


Summer 2009

# An Analytical Framework and Model Formulation for Measuring Risk in Engineering Enterprise Systems: A Capability Portfolio Perspective

Paul Raphael Garvey  
*Old Dominion University*

Follow this and additional works at: [https://digitalcommons.odu.edu/emse\\_etds](https://digitalcommons.odu.edu/emse_etds)

 Part of the [Industrial Engineering Commons](#), [Operational Research Commons](#), and the [Systems Engineering Commons](#)

---

## Recommended Citation

Garvey, Paul R.. "An Analytical Framework and Model Formulation for Measuring Risk in Engineering Enterprise Systems: A Capability Portfolio Perspective" (2009). Doctor of Philosophy (PhD), dissertation, Engineering Management, Old Dominion University, DOI: 10.25777/k951-jw92  
[https://digitalcommons.odu.edu/emse\\_etds/65](https://digitalcommons.odu.edu/emse_etds/65)

This Dissertation is brought to you for free and open access by the Engineering Management & Systems Engineering at ODU Digital Commons. It has been accepted for inclusion in Engineering Management & Systems Engineering Theses & Dissertations by an authorized administrator of ODU Digital Commons. For more information, please contact [digitalcommons@odu.edu](mailto:digitalcommons@odu.edu).

**AN ANALYTICAL FRAMEWORK AND MODEL FORMULATION  
FOR MEASURING RISK IN ENGINEERING ENTERPRISE  
SYSTEMS: A CAPABILITY PORTFOLIO PERSPECTIVE**

by

Paul Raphael Garvey  
A.B. May 1978, Boston College  
M.Sc. June 1980, Northeastern University

A Dissertation Submitted to the Faculty of  
Old Dominion University in Partial Fulfillment of the  
Requirement for the Degree of

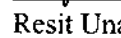
DOCTOR OF PHILOSOPHY  
ENGINEERING MANAGEMENT

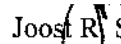
OLD DOMINION UNIVERSITY  
August 2009

Approved by:

 C. Ariel Pinto (Director)

  
Charles B. Keating (Member)

  
Resit Unal (Member)

  
Joost R. Santos (Member)

## **ABSTRACT**

# **AN ANALYTICAL FRAMEWORK AND MODEL FORMULATION FOR MEASURING RISK IN ENGINEERING ENTERPRISE SYSTEMS: A CAPABILITY PORTFOLIO PERSPECTIVE**

Paul Raphael Garvey  
Old Dominion University, 2009  
Director: Dr. C. Ariel Pinto

This work formulates an analytical framework and computational model for assessing risk in engineering enterprise systems. It addresses the engineering management problem of how to represent, model, and measure risk in large-scale, complex systems engineered to function in enterprise-wide environments.

The research in this dissertation extends current practice in the management of risk for traditional systems and creates new constructs and protocols for the management of risk in engineering large-scale, complex, and highly networked enterprise systems. This work advances engineering management theory and analytic practice as applied to the measurement and management of risk for enterprise systems engineered within capability portfolio paradigms.

This dissertation is dedicated to my wife Maura and daughters Alana and Kirsten.  
I also dedicate this work to the memory of my daughter Katrina  
and my parents Eva and Ralph.

*Ad Majorem Dei Gloriam*

## ACKNOWLEDGMENTS

Gratia est optimus attitude

*Gratitude is the best attitude - author unknown*

Although writing a dissertation is a singular endeavor, its contents develop from exchanges with many. With this, the author appreciatively acknowledges a number of distinguished professors and professionals who made this dissertation possible.

First, I thank Dr. Resit Unal, professor and Chair of the Department of Engineering Management and Systems Engineering. My pursuit of this doctorate came from a chance encounter with Dr. Unal at the National Institute of Aerospace, where I was invited to deliver the May 2006 Systems Analysis Series Lecture. His quiet but persistent encouragement is greatly appreciated.

Along with Dr. Unal, I thank the following members of my dissertation committee: namely, Dr. Charles B. Keating, Dr. Joost R. Santos (University of Virginia), and Dr. C. Ariel Pinto. From Dr. Keating, I became increasingly versed in the latest thinking on engineering systems, systems of systems, and research methods essential to doctoral studies. From Dr. Santos, I came to know the scholarship on Leontief-based methods applied to dependency analysis – a difficult and critical problem area in engineering systems. Dr. Santos' innovative research provided the groundwork for how I've addressed dependency problems as they occur at an enterprise scale.

Educator and Pulitzer Prize winning author Mark van Doren (1894–1972) wrote “*the art of teaching is the art of assisting discovery*”. Dr. C. Ariel Pinto, dissertation director, exemplifies such a teacher. Dr. Pinto assisted discovery by reading, reviewing, and critically challenging this research as it evolved over thirty months. It is with sincerest gratitude that I acknowledge Dr. Pinto's sanguine and expert advice that guided the depth and breadth of this work, as well as its early introduction to the engineering systems literature.

In addition to my dissertation committee, I wish to acknowledge the managerial excellence of Kim B. Sibson. As programs manager for the Department of Engineering Management and Systems Engineering, Ms. Sibson's expert advice and administrative assistance is greatly appreciated.

I also wish to acknowledge my appreciation to Mr. John J. Shottes, Dr. Richard A. Moynihan, and Mrs. Charlene J. McMahon for their participation in the industry assessment summarized in Appendix B. Their insights were instrumental in bringing practical considerations into the design of the risk analytic methods herein.

I appreciate permission from CRC Press, Taylor and Francis Group, to use materials in this dissertation from my book *Analytical Methods for Risk Management: A Systems Engineering Perspective*, which was published in 2008.

Last, I am sincerely appreciative to my family to whom this dissertation is dedicated. Once again, they encouraged me to pursue another intellectual and writing adventure – one that came after just finishing a second book. I promise to no longer say “*this is the last one*”.

## TABLE OF CONTENTS

|   | Page |
|---|------|
| LIST OF TABLES .....                                      | viii |
| LIST OF FIGURES.....                                      | x    |
| <br>Chapter   |      |
| I. INTRODUCTION .....                                     | 1    |
| ENGINEERING SYSTEMS RISK MANAGEMENT .....                 | 1    |
| COMMON PRACTICES .....                                    | 6    |
| NEW CHALLENGES .....                                      | 11   |
| LITERATURE REVIEW .....                                   | 12   |
| RESEARCH OBJECTIVES AND CONTRIBUTIONS.....                | 34   |
| II. ENGINEERING ENTERPRISE SYSTEMS.....                   | 40   |
| INTRODUCTION.....   | 40   |
| THE ENTERPRISE ENGINEERING PROBLEM SPACE .....            | 41   |
| CAPABILITY PORTFOLIO PERSPECTIVES .....                   | 44   |
| III. A RISK ANALYTIC FRAMEWORK.....                       | 48   |
| INTRODUCTION.....   | 48   |
| A FRAMEWORK FOR REPRESENTING CAPABILITY RISK.....         | 48   |
| AN ALGEBRA FOR COMPUTING CAPABILITY RISK .....            | 49   |
| INFORMATION NEEDS .....                                   | 64   |
| IV. AN INDEX TO MEASURE RISK CO-RELATIONSHIPS (RCR) ..... | 66   |
| INTRODUCTION.....   | 66   |
| RCR POSTULATES, DEFINITIONS, AND THEORY .....             | 66   |
| COMPUTING THE RCR INDEX.....                              | 75   |
| APPLICATION TO RESOURCE ALLOCATION DECISIONS .....        | 83   |
| SUMMARY .....   | 86   |
| V. FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA) .....    | 87   |
| INTRODUCTION.....   | 87   |
| FDNA FUNDAMENTALS AND POSTULATES.....                     | 88   |
| FDNA GENERAL EQUATION, PROPERTIES, AND THEOREMS .....     | 96   |
| A GENERAL THEORY OF DEPENDENCY .....                      | 119  |
| LINKING FDNA TO RISK REDUCTION INVESTMENT DECISIONS.....  | 145  |
| RELATIONSHIP OF FDNA TO OTHER METHODS .....               | 149  |
| SUMMARY .....   | 169  |

| Chapter  | Page |
|--|------|
| VI. PRIORITIZING RISK MANAGEMENT DECISIONS .....     | 172  |
| INTRODUCTION.....                                    | 172  |
| A PRIORITIZATION ALGORITHM .....                     | 172  |
| ILLUSTRATION .....                                   | 179  |
| VII. SUMMARY.....                                    | 182  |
| A UNIFYING RISK ANALYTIC FRAMEWORK AND PROCESS ..... | 182  |
| SUMMARY AND AREAS FOR FUTURE RSEARCH.....            | 189  |
| REFERENCES.....                                      | 190  |
| APPENDIXES   |      |
| A. TOPSIS ALGORITHM: CLASSICAL FORMULATION.....      | 195  |
| B. INDUSTRY PRACTITIONER ASSESSMENTS .....           | 201  |
| C. LITERATURE ASSESSMENT SUMMARY .....               | 245  |
| D. FDNA AND THE HILBERT MATRIX.....                  | 258  |
| E. FDNA AND THE MARKOV MATRIX.....                   | 261  |
| VITA .....   | 264  |

## LIST OF TABLES

| Table  | Page |
|--|------|
| 1 A Sample Constructed Scale: Supplier Node Impacts .....                    | 53   |
| 2 Example 4.3 Data and Computations: The Influence of Risk Inheritance ..... | 80   |
| 3 The Influence of Risk Inheritance on C-Node Risk Scores.....               | 81   |
| 4 P-Node Input Matrix.....   | 84   |
| 5 P-Node Solution Matrix.....  | 85   |
| 6 A First Operability Analysis of a 2,1,1-Node FDNA Graph.....               | 113  |
| 7 A Second Operability Analysis of a 2,1,1-Node FDNA Graph.....              | 115  |
| 8 An Operability Analysis of the Capability Portfolio in Figure 50.....      | 118  |
| 9 An Operability Analysis of a 2,1,1,R-Node FDNA Graph, in Range .....       | 139  |
| 10 An Operability Analysis of a 2,1,1,R-Node FDNA Graph, not in Range .....  | 141  |
| 11 An Operability Analysis of a 2,1,1,R-Node FDNA Graph, in Range .....      | 142  |
| 12 An FDNA Operability Analysis of the Infrastructure Systems Scenario ..... | 161  |
| 13 An FDNA Operability Analysis of the IIM 4-Matrix in Example 5.22 .....    | 169  |
| 14 A Traditional Decision or Performance Matrix of Alternatives .....        | 175  |
| 15 A Decision Matrix That Yields an Undefined Entropy Weight .....           | 178  |
| 16 Capability Node Risk Management Decision Matrix.....                      | 179  |
| 17 A TOPSIS-Derived Capability Risk Prioritization.....                      | 180  |
| 18 A Traditional Decision or Performance Matrix of Alternatives .....        | 196  |
| 19 A Risk Event Decision Matrix.....   | 199  |
| 20 An Illustrative Risk Event Decision Matrix .....                          | 199  |
| 21 Risk Event TOPSIS Scores.....   | 200  |



| Table  | Page |
|--|------|
| 22 Industry Assessment Summary Findings.....                     | 207  |
| 23 Industry Question 1-15 Analysis Summary Cards .....           | 208  |
| 24 Industry Respondent Summaries .....                           | 223  |
| 25 Literature Assessment Relative to Research Problem Areas..... | 248  |
| 26 An FDNA Operability Analysis Involving a Hilbert Matrix.....  | 260  |
| 27 An FDNA Operability Analysis Involving a Markov Matrix .....  | 263  |

## LIST OF FIGURES

| Figure   | Page |
|--|------|
| 1 Pressures on a Program Manager's Decision Space .....                      | 7    |
| 2 Steps Common to a Risk Management Process.....                             | 9    |
| 3 Dissertation Research: Literature Map Dimensions .....                     | 12   |
| 4 Literature Map: Engineering Systems.....                                   | 14   |
| 5 Literature Map: Risk and Decision Theory, Engineering Risk Management..... | 21   |
| 6 A Swiss Silver Thaler, Zurich, 1727 .....                                  | 22   |
| 7 Daniel Bernoulli's Logarithmic Utility Function.....                       | 23   |
| 8 Families of Risk Attitude or Utility Functions.....                        | 25   |
| 9 Families of Power-Additive Utility Functions.....                          | 30   |
| 10 Research Problem Area Relationships .....                                 | 38   |
| 11 Dissertation Research Contributions.....                                  | 39   |
| 12 Dissertation Organization .....   | 39   |
| 13 An Enterprise and its Environment .....                                   | 41   |
| 14 Nested Nature of Enterprises .....  | 42   |
| 15 An Enterprise and its Capability Portfolios .....                         | 44   |
| 16 A Capability Portfolio for Network Operations.....                        | 45   |
| 17 A Supplier-Provider View .....  | 46   |
| 18 A Tier 3 Capability from the Portfolio in Figure 17 .....                 | 50   |
| 19 Capability 3.2 Supplier Risk Set.....                                     | 51   |
| 20 EWXT Technology Program Risk Set.....                                     | 52   |
| 21 A Value Function for Occurrence Probability .....                         | 52   |

| Figure  | Page |
|---|------|
| 22 Example Risk Scores for EWXT Program Risks.....                      | 55   |
| 23 An Example Max Average Weighting Function.....                       | 56   |
| 24 Overall EWXT Program Risk Score and Color Rating .....               | 56   |
| 25 Supplier Node Risk Measures to Functionality 3.22 .....              | 57   |
| 26 Risk Measure Derived for Functionality 3.22.....                     | 58   |
| 27 Risk Measures for Capability 3.2 Functionality Nodes .....           | 59   |
| 28 Risk Measure for Capability 3.2: Critical Average Rule .....         | 60   |
| 29 Information Assurance: A Tier 2 Capability Area.....                 | 60   |
| 30 Information Assurance: Capability Risk Measures.....                 | 61   |
| 31 Information Assurance: Capability Risk Measures.....                 | 62   |
| 32 Network Operations Capability Portfolio-Level Risk Measure.....      | 62   |
| 33 An RCR Graph: Program-to-Capability Node Risk Co-Relationships.....  | 71   |
| 34 An RCR Graph: A Risk Event Inheritance View .....                    | 72   |
| 35 Example 4.1 RCR Graph .....  | 77   |
| 36 Example 4.2 RCR Graph .....  | 78   |
| 37 Example 4.3 RCR Graph: Non-Inherited and Inherited Risk Events ..... | 79   |
| 38 Example 4.3 Nodes: An RCR Index View .....                           | 82   |
| 39 An FDNA Graph: A Capability Portfolio Context .....                  | 88   |
| 40 A 2- and 3-Node FDNA Graph.....                                      | 89   |
| 41 A 2-Node FDNA Graph: Strength of Dependency (SOD) View.....          | 90   |
| 42 A 2-Node FDNA Graph: View by SOD Fraction and BOL .....              | 91   |
| 43 A 2-Node FDNA Graph: Criticality of Dependency View.....             | 92   |

| Figure  | Page |
|---|------|
| 44 A 2-Node FDNA Graph: Strength and Criticality of Dependency View .....       | 93   |
| 45 A Value Function for the Operability Node $P_j$ .....                        | 97   |
| 46 A 2,1,1-Node FDNA Graph .....  | 98   |
| 47 A 3,2,1-Node FDNA Graph .....  | 98   |
| 48 A 3,3,2-Node FDNA Graph .....  | 99   |
| 49 A 5,6,3-Node FDNA Graph .....  | 100  |
| 50 An FDNA Graph: From a Capability Portfolio Perspective .....                 | 101  |
| 51 A 2,1,1-Node FDNA Graph .....  | 112  |
| 52 Table 6 and Table 7 Operability Analysis Comparison .....                    | 116  |
| 53 Operability Analysis for Varying $\beta_{ij}$ (Tables 6, 7 Data) .....       | 116  |
| 54 An FDNA Constituent Node Defined by Five Components .....                    | 119  |
| 55 A Single Dimensional Value Function for the Operability Level of $P_j$ ..... | 120  |
| 56 Component SDVFs for Constituent Node $P_i$ .....                             | 121  |
| 57 A Constituent Node with $\kappa$ Components .....                            | 122  |
| 58 A 2,2,1-Node FDNA Graph with Constituent Node $P_i$ .....                    | 122  |
| 59 A 2,1,1-Node FDNA Graph: Constituent Node, Single Component Node .....       | 123  |
| 60 A 2,1,1-Node FDNA Graph: Single Component Node, Constituent Node .....       | 124  |
| 61 A 2,2,2-Node FDNA Graph .....  | 124  |
| 62 A 3,4,3-Node FDNA Graph: Constituent and Single Components Nodes .....       | 125  |
| 63 Specification Levels, Dependence, Constituent Nodes, and Components .....    | 127  |
| 64 A 2,1,1,R-Node FDNA Graph: Regulated SOD Fraction .....                      | 128  |
| 65 A 3,3,2,R-Node FDNA Graph, with Regulation .....                             | 143  |

| Figure  | Page |
|---|------|
| 66 FDNA Graph and SOD Equations for Example 5.18 .....                    | 146  |
| 67 An MRR View of the FDNA Graph in Example 5.18.....                     | 146  |
| 68 An FDNA Graph for Example 5.19.....                                    | 147  |
| 69 A Design Structure Matrix (DSM).....                                   | 149  |
| 70 Physical Connections Between Components.....                           | 155  |
| 71 An FDNA Graph and its Weighted Adjacency Matrix.....                   | 156  |
| 72 A Weighted FDNA Graph and its Adjacency Matrix.....                    | 156  |
| 73 A System-Subsystems Scenario: IIM and FDNA Relationship.....           | 157  |
| 74 An Infrastructure Systems Scenario: IIM and FDNA Relationship.....     | 157  |
| 75 A 4,6,4-Node FDNA Graph of the Infrastructure Systems Scenario.....    | 160  |
| 76 An IIM $A$ -Matrix with Weighted FDNA Graph .....                      | 165  |
| 77 Weighted FDNA Graph with $(\alpha, \beta)$ Parameters.....             | 166  |
| 78 Component Feeder-Receiver Relationships (Example 5.22, Presumed) ..... | 167  |
| 79 Component Connections and Feeders/Receivers (Integrated View).....     | 168  |
| 80 Euclidean Distances to Positive and Negative Ideal Solutions.....      | 174  |
| 81 A Traditional Risk Management Process.....                             | 182  |
| 82 Risk Analytic Methods Related to Risk Identification .....             | 184  |
| 83 Risk Analytic Methods Related to Risk Impact Assessment.....           | 185  |
| 84 Risk Analytic Methods Related to Risk Prioritization Analysis.....     | 186  |
| 85 Risk Analytic Methods Related to Risk Mitigation Planning.....         | 186  |
| 86 A Risk Analytical Framework and Model Formulation .....                | 187  |
| 87 Euclidean Distances to Positive and Negative Ideal Solutions.....      | 195  |

| Figure   | Page |
|--|------|
| 88 Industry Assessment Approach: An Inductive Analysis Pyramid ..... | 202  |
| 89 A View Into a Network Operations Capability Portfolio.....        | 205  |
| 90 Dissertation Research: Literature Map Dimensions .....            | 246  |
| 91 The Determinant of a Hilbert Matrix .....                         | 258  |
| 92 An FDNA Graph With a Hilbert Matrix.....                          | 259  |
| 93 An FDNA Graph With a Markov Matrix.....                           | 262  |

## CHAPTER I

### INTRODUCTION

#### **ENGINEERING SYSTEMS RISK MANAGEMENT**

Risk is a driving consideration in decisions that determine how engineering systems are developed, produced, and sustained. Critical to these decisions is an understanding of risk and how it affects the engineering of systems. What do we mean by risk?

In its common usage, risk means the possibility of loss or injury. Risk is an event that, if it occurs, has unwanted consequences. In the context of engineering management, risk can be described as answering the question “What can go wrong with my system or any of its parts?” [Kaplan, Garrick, 1981, p. 11]. In the past three-hundred years, a theory of risk has grown from connections between the theories of probability and economics.

In probability theory, risk is defined as the probability an unwanted event occurs [Hansson, 2007]. In economics, risk is characterized by the way a person evaluates the monetary worth of participation in a lottery or a gamble – any game whose monetary outcome is determined by chance. We say a person is risk averse if he is willing to accept with certainty an amount of money less than the expected amount he might receive from a lottery.

There is a common, but subtle, inclusion of loss or gain in these definitions of risk. Probability theory studies risk by evaluating the chances unwanted events occur. What makes an event unwanted? In economics, this question is answered in terms of a person’s monetary perspective or value structure. In general, “unwanted” is an adjective that needs human interpretation and value judgments specific to a situation.

Thus, the inclusion of probability and loss (or gain) in the definition of risk is important. Defining risk by these two fundamental dimensions enables tradeoffs between them with respect to decision-making and course-of-action planning. This is essential in the systems engineering community, which traditionally considers risk in terms of its probability and consequence (e.g., cost, safety, or performance impacts). Understanding these dimensions and their interactions often sets priorities for whether, how, and when risks are managed in the engineering of systems.

What does it mean to manage risk? From a systems engineering perspective, risk management is a formal process used to continuously identify, analyze, and adjudicate events that, if they occur, have unwanted impacts on a system’s ability to achieve its outcome objectives [Garvey, 2008]. Applied early, risk management can expose potentially crippling areas of risk in the engineering of systems. This provides management time to define and implement corrective strategies. Moreover, risk management can bring realism to technical and managerial decisions that define a system’s overall engineering strategy.

---

This dissertation is formatted in the style of the *Publication Manual of the American Psychological Association*, 5th edition.

Successfully engineering today's systems requires deliberate and continuous attention to the management of risk. Managing risk is an activity designed to improve the chance these systems will be completed within cost, on time, and meet safety and performance objectives.

Engineering today's systems is more sophisticated and complex than ever before. Increasingly, systems are engineered by bringing together many separate systems which, as a whole, provide an overall capability otherwise not possible. Many systems no longer physically exist within clearly defined boundaries and specifications, a characteristic of traditional systems.

Today, systems are increasingly characterized their ubiquity and lack of specifications. Such systems are present everywhere and in many places simultaneously. They operate as an enterprise of interactions between technologies and users in a dynamic that behaves in often unpredictable ways.

Enterprise systems involve and evolve webs of users, technologies, systems, and systems-of-systems through environments that offer cross-boundary access to a wide variety of resources, systems, and information repositories. Examples of enterprise systems include the National Airspace System, a university's information infrastructure, or the Internet.

Enterprise systems create value by delivering capabilities over time that meet user needs for increased flexibility, robustness, and scalability rather than by specifying, *a-priori*, firm and fixed requirements. Thus, enterprise system architectures must always be open to allow the insertion of innovation, at strategic junctures, which advance the efficacy of the enterprise and its delivery of capabilities and services to users.

Engineering enterprise systems involves much more than discovering and employing innovative technologies. Engineering designs must be adaptable to change and the evolving demands of user enclaves. In addition, designs must be balanced with respect to expected performance while continuously risk managed throughout an enterprise system's evolution.

Engineers and managers must develop a holistic understanding of the social, political, and economic environments within which an enterprise system operates. Failure to fully consider these dimensions, as they influence engineering and management decisions, can be disastrous. Consider the case of Boston's Central Artery/Tunnel Project, informally known as the "Big Dig".

#### **Boston's Central Artery/Tunnel (CA/T)**

Boston's Central Artery/Tunnel (CA/T) project began in 1991 and was completed in 2007. Its mission was to rebuild the city's main transportation infrastructure such that more than 10 hours of traffic congestion each day would be markedly reduced.

At its peak, the Big Dig involved 5,000 construction personnel, more than 100 separate engineering contracts, and saw an expenditure rate reach 3 million dollars a day. When completed, the CA/T project built 161 lane miles of highway in a 7.5 mile corridor (half in tunnels) and included 200 bridges and 4 major highway interchanges [Massachusetts Turnpike Authority, *Big Dig*, retrieved from <http://www.massturnpike.com/bigdig/background/facts.html>].



The Big Dig was an engineering and management undertaking on an enterprise scale – a public works project that rivaled in complexity with the Hoover dam<sup>\*</sup>. From the lens of history, design and engineering risks, though significant, were dwarfed by the project's social, political, environmental, and management challenges. Failure to successfully address aspects of these dimensions not only led to a 12 billion dollar increase in completion year costs but also to serious operational safety failures – one which caused loss of life.

Case studies will be written about the CA/T project for many years. The successes and failures of Boston's Big Dig offer a rich source for understanding risks associated with engineering large-scale, complex, enterprise systems. The following summarizes key lessons from the Big Dig and relates them to similar challenges being seen on other enterprise engineering projects.

Research into the management of risk for large-scale infrastructure projects is limited, but some findings are emerging from the community. A study by Reilly and Brown [2004] identifies three significant areas of risk that persistently threaten infrastructure projects that are enterprise in scale, such as the Big Dig. These areas are as follows.

#### **Risk Area: System Safety**

This area refers to the risk of injury or catastrophic failure with the potential for loss of life, personal injury, extensive material and economic damage, and loss of credibility for those involved [Reilly, Brown, 2004].

#### **Experience from the Big Dig**

On 10 July 2006, twelve tons of cement ceiling panels fell onto a motor vehicle traveling through one of the new tunnels. The collapse resulted in the loss of life. The accident occurred in the D-Street portal of the Interstate 90 connector tunnel in Boston to Logan Airport. One year later, the National Transportation Safety Board (NTSB) determined "the probable cause of the collapse was the use of an epoxy anchor adhesive with poor creep resistance, that is, an epoxy formulation that was not capable of sustaining long-term loads" [NTSB, 10 July 2007, p. 107]. The safety board summarized its findings as follows:

"Over time, the epoxy deformed and fractured until several ceiling support anchors pulled free and allowed a portion of the ceiling to collapse. Use of an inappropriate epoxy formulation resulted from the failure of Gannett Fleming, Inc., and Bechtel/Parsons Brinckerhoff to identify potential creep in the anchor adhesive as a critical long-term failure mode and to account for possible anchor creep in the design, specifications, and approval process for the epoxy anchors used in the tunnel.

The use of an inappropriate epoxy formulation also resulted from a general lack of understanding and knowledge in the construction community about creep in adhesive anchoring systems. Powers Fasteners, Inc. failed to provide the Central Artery/Tunnel project with sufficiently complete, accurate, and detailed information about the suitability of the company's Fast Set epoxy for sustaining long-term tensile loads. Contributing to the accident was the failure of Powers Fasteners, Inc., to determine that the anchor displacement that was found in

---

<sup>\*</sup> See: Stern, S. (2003), *The Christian Science Monitor*, [www.csmonitor.com](http://www.csmonitor.com).

the high occupancy vehicle tunnel in 1999 was a result of anchor creep due to the use of the company's Power-Fast Fast Set epoxy, which was known by the company to have poor long-term load characteristics. Also contributing to the accident was the failure of Modern Continental Construction Company and Bechtel/Parsons Brinckerhoff, subsequent to the 1999 anchor displacement, to continue to monitor anchor performance in light of the uncertainty as to the cause of the failures. The Massachusetts Turnpike Authority also contributed to the accident by failing to implement a timely tunnel inspection program that would likely have revealed the ongoing anchor creep in time to correct the deficiencies before an accident occurred" [NTSB/HAR-07/02, 2007, p. 107].

#### **Risk Area: Design, Maintainability, Quality**

This area refers to the risk of not meeting design, operational, maintainability, and quality standards [Reilly, Brown, 2004].

##### **Experience from the Big Dig**

In many ways a system's safety is a reflection on the integrity of its design, maintainability, and quality. In light of the catastrophic failure just described, of note is an article from *City Journal* in their story *Lessons of Boston's Big Dig* by [Gelinis, 2007]. Relevant to this risk area the author writes the following:

"As early as 1991, the state's inspector general warned of the 'increasingly apparent vulnerabilities... of (Massachusetts's) long-term dependence on a consultant' whose contract had an 'open-ended structure' and 'inadequate monitoring'. The main deficiency, as later IG reports detailed, was that Bechtel and Parsons – as 'preliminary designer,' 'design coordinator,' 'construction coordinator,' and 'contract administrator' – were often in charge of checking their own work. If the team noticed in managing construction that a contract was over budget because of problems rooted in preliminary design, it didn't have much incentive to speak up" [Gelinis, 2007, retrieved from [http://www.city-journal.org/html/17\\_4\\_big\\_dig.html](http://www.city-journal.org/html/17_4_big_dig.html)].

#### **Risk Area: Cost-Schedule Realism**

This area refers to the risks of significant increase in project and support costs; risks of a significant delay to project completion and start of revenue operations [Reilly, Brown, 2004].

##### **Experience from the Big Dig**

The completion cost of the Big Dig was 14.8 billion dollars. Its original estimate was 2.6 billion dollars. The project's completion cost was 470 percent larger than its original estimate. If the impacts of unwanted events are measured by cost, then risks realized on the Big Dig were severe.

Numerous investigations have been made into the reasons why Big Dig costs increased to this magnitude. A key finding was lack of cost-schedule realism in the project's initial stages. This was driven by many factors. Among these were incompleteness in cost scope, ignoring the impacts of inflation, overreliance on long-term federal political support (at the expense of building local political and community advocacy), and failure to incorporate risk into cost-schedule estimates.

Sadly, news reporting cited concerns over cost overruns as a factor that contributed to the collapse of cement ceiling tiles in the new tunnel. Consider the following excerpt from *City Journal's* story *Lessons of Boston's Big Dig* [Gelinas, 2007].

“This problem of murky responsibility came up repeatedly during the Big Dig, but most tragically with the ceiling collapse. Designers engineered a lightweight ceiling for the tunnel in which Milena del Valle died. But Massachusetts, annoyed by cost overruns and cleanliness problems on a similar ceiling, and at the suggestion of federal highway officials, decided to fit the new tunnel with a cheaper ceiling, which turned out to be heavier.

Realizing that hanging concrete where no built-in anchors existed to hold it would be a difficult job, the ceiling's designer, a company called Gannett Fleming, called for contractors to install the ceiling with an unusually large built-in margin for extra weight. Shortly after contractors installed the ceiling using anchors held by a high strength epoxy (as Gannett specified) workers noticed it was coming loose.

Consultants and contractors decided to take it apart and reinstall it. Two years later, after a contractor told Bechtel that ‘several anchors appear to be pulling away from the concrete,’ Bechtel directed it to ‘set new anchors and retest.’ After the resetting and retesting, the tunnel opened to traffic, with fatal consequences” [Gelinas, 2007, retrieved from [http://www.city-journal.org/html/17\\_4\\_big\\_dig.html](http://www.city-journal.org/html/17_4_big_dig.html)].

The paper “Management and Control of Cost and Risk for Tunneling and Infrastructure Projects” [Reilly, Brown, 2004] offers reasons from Fred Salvucci (former Massachusetts Secretary of Transportation) for the project's schedule slip and cost growth. Quoting from that work:

“The reasons had much to do with Governmental policies, local and national politics, new requirements not planned for in the beginning and, political and management transitions that disrupted continuity. Technical complexity was a factor – but it was not the major cause of the schedule slip and cost growth” [Reilly, Brown, 2004, p. 1].

### **Summary**

The engineering community should study and learn from the successes and failures of Boston's Central Artery/Tunnel project. The technical and engineering successes of the Big Dig are truly noteworthy, but sadly so are its failures. Project failures often trace back to judgments unduly influenced by cost, schedule, and socio-political pressures. Adherence to best practices in the management of engineering projects is often minimized by these pressures.

Clearly, the emergence of enterprise systems makes today's engineering practices even more challenging than before. Projects at this scale, as experienced on the Big Dig, necessitate the tightest coupling of engineering, management and socio-political involvement in unprecedented ways, so success becomes the norm and failure the exception. Risks can never be eliminated. However, their realization and consequences can be minimized by the continuous participation of independent boards, stakeholder communities, and well-defined lines of management authority.

## **COMMON PRACTICES**

Engineering risk management is a program management process. At its core, engineering risk management is program management.

The objectives of engineering risk management are the early and continuous identification, management, and resolution of risks such that engineering a system is accomplished within cost, delivered on time, and meets user needs [Garvey, 2008]. Why is engineering risk management important? There are many reasons. The following are five key considerations.

### **Early and Continuous Risk Identification**

An engineering risk management program fosters the early and continuous identification of risks so options can be considered and actions implemented before risks seriously threaten a system's outcome objectives.

### **Risk-Based Program Management**

Engineering risk management enables risk-informed decision-making and course-of-action planning throughout a program's development life cycle and particularly when options, alternatives, or opportunities need to be evaluated.

### **Estimating and Justifying Risk Reserve Funds**

An engineering risk management program enables identified risk events to be mapped into a project's work breakdown structure. From this, the cost of their ripple effects can be estimated. Thus, an analytical justification can be established between a project's risk events and the amount of risk reserve (or contingency) funds that may be needed.

### **Resource Allocation**

The analyses produced from an engineering risk management program will identify where management should consider allocating limited (or competing) resources to the most critical risks on an engineering system project.

### **Situation Awareness and Risk Trends**

Engineering risk management can be designed to provide management with situational awareness in terms of a project's risk status [Garvey, 2008]. This includes tracking the effectiveness of courses-of-action and trends in the rate that risks are closed with those newly identified and those that remain unresolved.

What are risks? Risks are events that, if they occur, cause unwanted change in the cost, schedule, or technical performance of an engineering system. The occurrence of risk is an event that has negative consequences on an engineering system project. Risk is a probabilistic event; that is, risk is an event that may occur with probability  $p$  or may not occur with probability  $(1 - p)$  [Garvey, 2008].

Why are there risks? Pressures to meet cost, schedule, and technical performance are the practical realities in engineering today's systems [Haimes, 2004]. Risk is present when expectations in these dimensions push what is technically or economically feasible. Managing risk is managing the inherent contention that exists within and across all these dimensions, as shown in Figure 1.

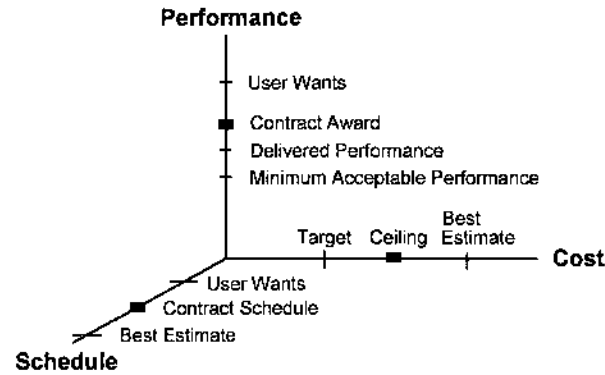


Figure 1. Pressures on a Program Manager's Decision Space [Garvey, 2008]

What is the goal of engineering risk management? As mentioned earlier, the goal is to identify cost, schedule, and technical performance risks early and continuously, such that control in any of these dimensions is not lost or the consequences on them are well-understood.

Risk management strives to enable risk-informed decision-making throughout an engineering system's life cycle. Engineering risk management process and practice varies greatly from very formal to very informal. The degree of formality is governed by management style, commitment, and a project team's attitude towards risk identification, analysis, and management. Next, we present two basic definitions.

**Definition 1.1:** Risk is an event that, if it occurs, adversely affects the ability of an engineering system project to achieve its outcome objectives [Garvey, 2008; Haimes, 2004].

From this, a risk event has two aspects. The first is its occurrence probability. The second is its impact (or consequence) to an engineering system project. A general expression for this is given by Equation 1.1 [Garvey, 2008; Bahnmaier, 2003; Haimes, 2004].

$$Risk = F(Probability, Consequence) \quad (1.1)$$

**Definition 1.2:** An event is uncertain if there is indefiniteness about its outcome [Garvey, 2008].

There is a distinction between the definition of risk and the definition of uncertainty. Risk is the chance of loss or injury. In a situation that includes favorable and unfavorable events, risk is the probability an unfavorable event occurs. Uncertainty is the indefiniteness about the outcome of a situation. Uncertainty is sometimes classified as aleatory or epistemic.

Aleatory derives from the Latin *aleatorius* (gambler). Aleatoric uncertainty refers to inherent randomness associated with some events in the physical world [Ayyub, 2001]. For example, the height of waves is aleatoric. Epistemic is an adjective that means *of or pertaining to knowledge*. Epistemic uncertainty refers to uncertainty about an event due to incomplete knowledge [Ayyub, 2001]. For example, the cost of engineering a future system is an epistemic uncertainty.

We analyze uncertainty for the purpose of measuring risk. In an engineering system, the analysis might involve measuring the risk of failing to achieve performance objectives, over-running the budgeted cost, or delivering the system too late to meet user needs [Garvey, 2008; Bahnmaier, 2003; Haimes, 2004].

Why is the probability formalism used in risk management? Since risk is a potential event, probability is used to express the chance the event will occur. However, the nature of these events is such that objectively derived measures of occurrence probabilities are typically not possible. Risk management necessarily relies (in part) on probabilities that stem from expert judgment. These are known as measures of belief or subjective probabilities. Are such measures valid?

In 1933, Russian mathematician Kolmogorov established a definition of probability in terms of three axioms\*. They define probability as a measure – one that is independent of objective and subjective interpretations of probability. Known as the axiomatic definition, it is the view of probability adopted in this dissertation.

Under this definition, it is assumed for each random event  $A$ , in a sample space  $\Omega$  there is a real number  $P(A)$  that denotes the probability of  $A$ . In accordance with Kolmogorov's axioms, probability is simply a numerical measure that satisfies the following:

**Axiom 1**  $0 \leq P(A) \leq 1$  for any event  $A$  in  $\Omega$

**Axiom 2**  $P(\Omega) = 1$

**Axiom 3** For any sequence of mutually exclusive events  $A_1, A_2, \dots$

defined on  $\Omega$  it follows that  $P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$

For any finite sequence of mutually exclusive events

$A_1, A_2, \dots, A_n$  defined on  $\Omega$  it follows that  $P(\bigcup_{i=1}^n A_i) = \sum_{i=1}^n P(A_i)$

The first axiom states the probability of any event is a non-negative number in the interval zero to one. The second axiom states a *sure event* is certain to occur. In probability theory, the sample space  $\Omega$  is referred to as the *sure event*; therefore, we have  $P(\Omega)$  equal to one. The third axiom states for any infinite or finite sequence of mutually exclusive events, the probability of at least one of these events occurring is the sum of the probabilities associated with each event  $A_i$ .

From this, it is possible for probability to reflect a measure of belief in an event's occurrence. For instance, an engineer might assign a probability of 0.70 to the event "the radar software for the Advanced Air Traffic Control System (AATCS) will not exceed 100K source instructions." Clearly, this event is non-repeatable. The AATCS cannot be built  $n$  times (and under identical conditions) to objectively determine if this probability is indeed 0.70. When an event such as this appears, its probability may be subjectively assigned.

---

\* A. N. Kolmogorov, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Ergeb. Mat. und ihrer Grenz., vol. 2, no. 3, 1933. Translated into English by N. Morrison, *Foundations of the Theory of Probability*, New York (Chelsea), 1956.

Subjective probabilities should be based on available evidence and previous experience with similar events. They must be plausible and consistent with Kolmogorov's axioms and the theorems of probability.

What about consequence? What does consequence mean and how can it be measured? As mentioned earlier, a risk event's consequence is typically expressed in terms of its impact on an engineering system's cost, schedule, and technical performance. However, there are often other important dimensions to consider. These include programmatic, political, and economic impacts.

There are many ways consequence can be measured. Common measurement methods include techniques from value or utility function theory, which are presented later in this dissertation. These formalisms enable risk events that impact a project in different types of units (e.g., dollars, months, processing speed) to be compared along normalized, dimensionless, scales. This is especially necessary when risk events are rank-ordered or prioritized on the basis of their occurrence probabilities and consequences.

Assessing a risk event's occurrence probability and its consequence are only parts of an overall process of managing risk on an engineering system project. In general, risk management can be characterized by the process illustrated in Figure 2. The following describes each step.

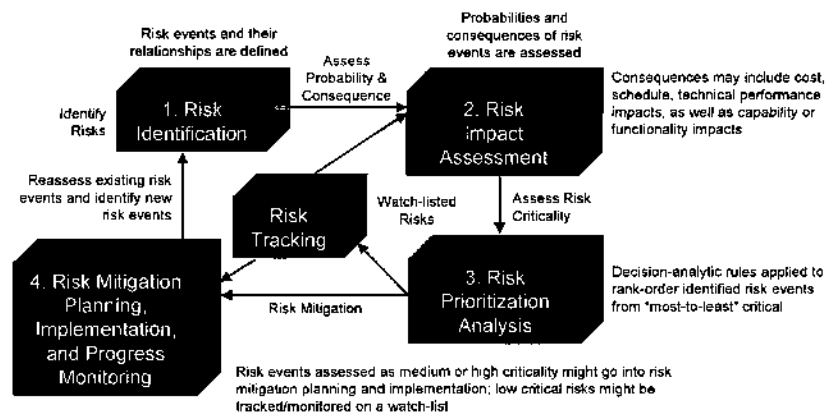


Figure 2. Steps Common to a Risk Management Process

### Risk Identification

Risk identification is the critical first step of the risk management process. Its objective is the early and continuous identification of risks, to include those within and external to the engineering system project. As mentioned earlier, these risks are events that, if they occur, have negative impacts on the project's ability to achieve its outcome goals.

### Risk Impact (Consequence) Assessment

Here, an assessment is made of the impact each risk event could have on the engineering system project. Typically, this includes how the event could impact cost, schedule, or technical performance objectives. Impacts are not limited to these criteria. Additional criteria such as political or economic consequences may require consideration – a topic discussed later in this dissertation.

An assessment is also made of the probability each risk event will occur. As mentioned previously, this often involves subjective probability assessments particularly if circumstances preclude a direct evaluation of probability by objective methods.

### **Risk Prioritization Analysis**

At this step the overall set of identified risk events, their impact assessments, and their occurrence probabilities are processed to derive a ranking of the most- to least-critical risks. Decision analytic techniques such as utility theory, value function theory, or ordinal methods are formalisms often used to derive this ranking.

A major purpose for prioritizing (or ranking) risks is to form a basis for allocating critical resources. These resources include the assignment of additional personnel or funding (if necessary) to focus on resolving risks deemed most critical to the engineering system project.

### **Risk Mitigation Planning and Progress Monitoring**

This step involves the development of mitigation plans designed to manage, eliminate or reduce risk to an acceptable level. Once a plan is implemented, it is continually monitored to assess its efficacy with the intent to revise its courses-of-action if needed.

### **Summary**

This section presented an introduction to systems engineering risk management as a fundamental engineering and program management practice. Core concepts were discussed to provide context and to set the stage for their extension to systems engineered to operate in an enterprise space.

Systems engineering practices often necessitate the use of historical experience and expert subjective judgments. These aspects should be properly addressed when designing and applying formal methods to engineering systems problems.

In recognition of this, the analytical methods developed herein derive from formalisms designed for situations where quantitative data is the exception rather than the rule. Specifically, value and utility function theory will be used to represent and measure risk and its effects on engineering systems. These formalisms originate from the von Neumann and Morgenstern axioms of expected utility theory [von Neumann, Morgenstern, 1944] and from modern works on preference theory [Keeney, Raiffa, 1976].

Thoughts on these formalisms are given by R. L. Keeney in his book *Value-Focused Thinking: A Path to Creative Decision Making*. In this work, Keeney writes the following [Keeney, 1992]:

“The final issue concerns the charge that value (utility) models are not scientific or objective. With that, I certainly agree in the narrow sense. Indeed values are subjective, but they are undeniably a part of decision situations. Not modeling them does not make them go away. It is simply a question of whether these values are included implicitly and perhaps unknowingly in a decision process or whether there is an attempt to make them explicit and consistent and logical. In a broader sense, the systematic development of a model of values is definitely scientific and objective. It lays out the assumptions on which the model is based, the logic supporting these assumptions, and the basis for data (that is, specific value judgments). This



makes it possible to appraise the implications of different value judgments. All of this is very much in the spirit of scientific analysis. It certainly seems more reasonable – even more scientific – to approach important decisions with the relevant values explicit and clarified rather than implicit and vague” [Keeney, 1992, p. 154].

This view reflects the author’s philosophy and the analytic school of thought in this dissertation. It is in this spirit that the formalisms herein were developed to address the very real and complex management problems in engineering today’s advanced enterprise systems.

## NEW CHALLENGES

As mentioned earlier, today’s systems are increasingly characterized by their *ubiquity* and lack of specification. Systems like the internet are unbounded, present everywhere, and in places simultaneously. They are an *enterprise* of systems and systems-of-systems. Through the use of advanced network and communications technologies, these systems continuously operate to meet the demands of globally distributed and uncountable many users and communities.

Engineering enterprise systems is an emerging discipline that encompasses and extends traditional systems engineering to create and evolve webs of systems and systems of systems. They operate in a network-centric way, to deliver capabilities via services, data, and applications through richly interconnected networks of information and communications technologies.

More and more defense systems, transportation systems, and financial systems connect across boundaries and seamlessly interface with users, information repositories, applications, and services. These systems are an enterprise of people, processes, technologies, and organizations.

Thinking about how to design, engineer, and manage enterprise systems is at the cutting edge of modern systems thinking and engineering. Lack of clearly defined boundaries and diminished hierarchical control are significant technical and managerial challenges. Along with this, the engineering management community needs to establish methods for identifying, analyzing, and managing risks in systems engineered to operate in enterprise contexts.

What makes managing risks in engineering enterprise systems more challenging than managing risks in engineering traditional systems? How does the delivery of capability to users affect how risks are identified and managed in engineering enterprise systems?

With regard to the first question, the difference is principally a matter of scope. From a high-level perspective, the basic risk management process (shown in Figure 2) is the same. The challenge comes from implementing and managing this process across a large-scale, complex, enterprise – where contributing systems may be in different stages of maturity and where managers, users, and stakeholders may have different capability needs and priorities.

With regard to the second question, an enterprise system is often planned and engineered to deliver capabilities through a series of time-phased increments or evolutionary builds. Thus, risks can originate from many different sources and threaten enterprise capabilities at different points in time. Furthermore, these risks must align to the capabilities they potentially affect and the

scope of their consequences must be understood. In addition, the extent to which enterprise risks may have unwanted collateral effects on other dependent capabilities must be carefully examined.

A final distinguishing challenge in engineering enterprise systems is not only their technologies but also the way users interface with them and each other. Today, the engineering and social science communities are joining in ways not previously seen when planning and evolving the design, development, and operation of enterprise systems [Allen, Nightingale, Murman, 2004].

The goal of this research is the design of formal methods that provide a holistic understanding of risks in engineering enterprise systems, their potential consequences, dependencies, and rippling effects across the enterprise space. Ultimately, risk management in this context aims to establish and maintain a complete view of risks across the enterprise, so capabilities and performance objectives are achieved via risk-informed resource and investment decisions.

## LITERATURE REVIEW

This dissertation presents an analytical framework and computational model for assessing risk in engineering large-scale, highly networked, enterprise systems. Engineering management methods in general, and risk management practices in particular, are in their infancy with respect to engineering enterprise systems.

The literature in this field has only begun to address the complexities and multidisciplinary nature of this problem space (refer to Appendix C). However, foundational perspectives on ways to view this space exist in the literature and in the scientific community. Many of these perspectives originate from *general systems theory* [von Bertalanffy, 1968], a topic discussed throughout this section.

Figure 3 shows the major academic disciplines applied in this research and presents them as dimensions that form a *literature map*. Three axes are shown. They are *engineering systems*, *risk and decision theory*, and *engineering risk management*. General systems theory provides a foundation for how aspects of these disciplines are applied to the research in this dissertation.

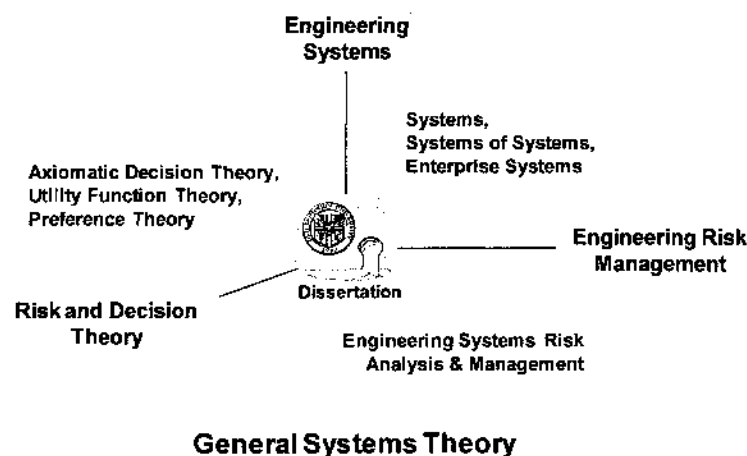


Figure 3. Dissertation Research: Literature Map Dimensions

## General Systems Theory and Engineering Systems Literature

*"Systems Everywhere"*

Karl Ludwig von Bertalanffy (1901 – 1972)

General systems theory views systems as "everywhere" [von Bertalanffy, 1968, p. 3]. Natural laws and social behaviors are parts of highly complex, interdependent, systems and elements. General systems theory is a philosophy that considers how to view and pursue scientific inquiry. Its concepts provide a basis for aspects of the research approach carried out for this dissertation.

General systems theory is a phrase coined forty years ago; however, systems and systems thinking have long been part of man's history. Anthropological evidence reveals the creation of hunting systems by Paleolithic human cultures that lived more than 50,000 years ago.

Cro-Magnon artifacts demonstrate the increasing sophistication of their hunting devices and hunting systems to capture large and dangerous game from safer and safer distances. One such device was a thrower. The thrower operated like a sling-shot. When inserted with a spear and thrown, the thrower device increased the spear's speed, range, and lethality. This enabled hunters to attack from distances that lessened their risk of injury. These understandings were learned from empirical observations and not, at that time, from formal understandings of the laws of motion.

Let's review this from a general systems theory perspective. Here, three elements came together to make the Cro-Magnon's weapon – the arrow head, a long thick stick, and the thrower device. Independently, these elements were ineffective as a weapon for capturing prey. However, when integrated as a whole system the spear's potential was deadly. Potential is used because the spear itself is inert. A human thrower is needed for the spear's effectiveness to be realized.

In this sense, the human thrower is the weapon system and the spear is the weapon. When multiple human throwers are engaged in a coordinated attack they operate as a system-of-weapons systems engaged on a target. Here, the spears are the individual weapon systems that operate together to form an even more powerful assault on a target than realized by a single human thrower acting as a single weapon system.

It took systems thinking to integrate the weapon's three elements. It took even greater systems thinking to improve the weapon's effectiveness by launching it simultaneously at targets through group attack strategies. This is one of many examples of systems, systems thinking, and even system of systems thinking in early human culture.

This discussion highlights a view that systems are not only everywhere but have always been everywhere. They are ubiquitous throughout nature and society. Forty years ago Karl Ludwig von Bertalanffy (1968) authored the book *General Systems Theory: Foundations, Development, Applications*. He conjectured a theory of systems as "a general science of wholeness" [von Bertalanffy, 1968, p. 37], where "the whole is more than the sum of its parts" [von Bertalanffy, 1968, p. 18]. Illustrated above, these ideas were already well-understood by our early ancestors.

Next, we fast forward from Paleolithic times to the Industrial Revolution. Historians generally associate the Industrial Revolution with mid- to late-eighteenth century England. Here,

mechanical innovations moved agriculturally-based economies to economies driven by the mass-production of manufactured goods. With this, society experienced dramatic population shifts from rural farm life to cities where factories and factory jobs were plentiful.

Historians refer to the Industrial Revolution in two phases. The first phase involved mechanical innovations that replaced manual labor with machine-driven mass-production of goods. The second phase brought many of these innovations into more and more complex applications, some that included the use of electrification.

Consider steam power. In the first phase of the Industrial Revolution, steam power powered many types of manufacturing machines that operated in factories – especially in factories where water power was absent. However, steam power would soon be recognized as a way to drive shipping and railway systems. Ultimately, these innovations led to electro-mechanical technologies that enabled wide-scale transportation systems to be built and operated across the expanse of a nation's land and sea territories. Thus, one can trace the beginnings of modern day engineering systems to those innovations, inventions, and processes that appeared more than a century ago.

Today, engineering systems continue to advance, but they do so within another revolution – the Digital or Information Age. Unlike engineering systems built during the height of the Industrial Revolution, today's systems are focused less on enabling the mass-production of physical goods and more on enabling global connectivity. With this, engineering systems now make possible the instantaneous transport of digital information around the world. With an understanding of the past and a perspective on today, the literature for this dissertation was researched, reviewed, and summarized in the discussion that follows.

Figure 4 presents the literature reviewed for this research as it maps to modern scholarship on systems theory and the engineering of systems, systems of systems, and enterprise systems. We begin with Bertalanffy and his seminal work on general systems theory.

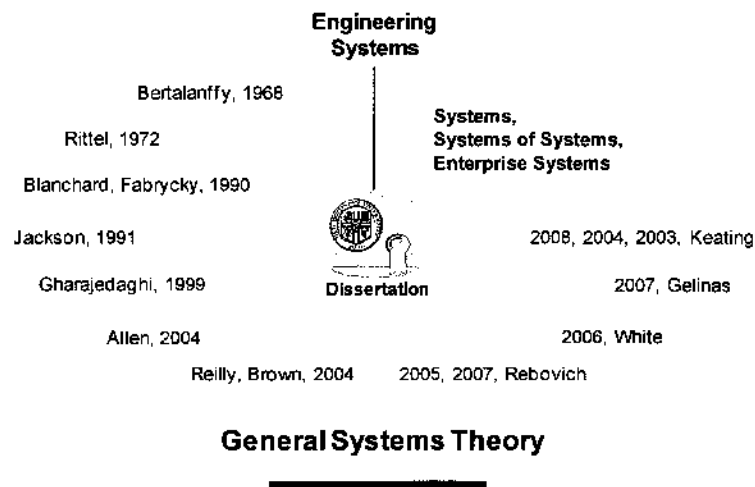


Figure 4. Literature Map: Engineering Systems

### General Systems Theory

Karl Ludwig von Bertalanffy proposed forty years ago a general theory of systems to explain fundamental commonalities that seem to underlie natural and socio-behavioral phenomena. He theorized that natural phenomena and social behavior at their elemental levels, are systems comprised of entities that operate and interact in open and continually dynamic ways.

Bertalanffy (1968) argues a closed system\*, such as an urn containing red and blue marbles, eventually tends toward a state of most probable distribution and this tendency reflects a tendency toward maximum disorder. A system might be closed at certain macro-levels of organization with behaviors predictable with certainty; however, at lower and lower levels of organization the system eventually becomes more and more open, disordered, and with behaviors not predictable with certainty. "Thus a basic problem posed to modern science is a general theory of organization" [von Bertalanffy, 1968, p. 34] with general systems theory as a framework within which the behavior and interaction of entities operating within an organization can be discovered.

Bertalanffy regarded general systems theory as a "general science of wholeness" [von Bertalanffy, 1968, p. 37]. He saw the incompleteness of trying to understand "observable phenomena" [von Bertalanffy, 1968, p. 36] as a collection of entities that could be studied "independently of each other" [von Bertalanffy, 1968, p. 37]. Systems are fundamentally organizations made of entities "not understandable by investigation of their respective parts in isolation" [von Bertalanffy, 1968, p. 37] but in how they assemble, react, and interact as a whole. Thus, the behavior of a system (an organization) is not simply the sum of the behaviors of its parts.

Bertalanffy's insights were profound. He foresaw not only the challenges in engineering today's complex systems but also ways to view and study their dynamics, interactions, and behaviors. Others also expressed views consistent with Bertalanffy when planning and designing engineering systems. For example, Rittel (1972) wrote on the importance of "grasping the whole of a system" rather than viewing it in "piecemeal" and since a system has many "facets" planning its design is necessarily multidisciplinary [Rittel, 1972, p. 390].

Bertalanffy and Rittel each recognized the need for many different specialties to work together to engineer systems as they evolved from single-purpose machines, like a steam engine, to highly complex machines like space vehicles [von Bertalanffy, 1968; Rittel, 1972]. Throughout most of the Industrial Revolution, single-purpose machines were built by engineers trained in their underlying technologies. These machines were made of components similar to each other to the extent they were within the training of the engineer's technical disciplines. As the industrial age moved into its second phase, and especially in today's information age, engineering systems required the assemblage of more and more technologies that are unlike each other (e.g., encryption hardware technologies are unlike database technologies). Hence, many different specialties are now needed to successfully design, build, and field information age systems.

What are these specialties? They are indeed the traditional engineering sciences but also include management, economics, cost analysis and other analytical areas such as reliability and logistics

---

\* A closed system is isolated from its environment [von Bertalanffy, 1968]. An open system is one that is not closed.

analyses, modeling and simulation, and human factors. In the past twenty-five years, authors like Blanchard and Fabrycky (1990) brought these and related areas into the modern study of systems engineering. With this, systems engineering has become the principal discipline from which to address the depth and breadth of the socio-technical challenges in engineering today's advanced systems.

What is meant by socio-technical challenges? They range from how a system affects society to how a society affects a system. With regard to the former, we discussed how the Industrial Revolution changed society from an agricultural economy to one driven by automation and the mass-production of goods. With regard to the latter, we discussed how social-political attitudes affected technical decisions on Boston's Central Artery/Tunnel (CA/T) project [Gelinas, 2007; Reilly, Brown, 2004; NTSB, 2007]. Thus, socio-technical challenges stem from how systems interact with people and how people interact with systems.

Social interactions with systems, as enabled by their technologies, are innumerable. They produce desirable and undesirable effects. For example, the ability to easily purchase goods from around the world via networked systems and services led to the emergence of cyber-based commerce and the economic opportunities that provides. Unfortunately, opportunities often come with risks. Consider the risks posed by cybercrime to electronic commerce. Cybercrime is a socially-initiated undesirable behavior that intentionally exploits vulnerabilities in a system's technologies.

In both cases, electronic commerce and cybercrime illustrate a property called emergent behavior. Emergent properties derive from "the whole of a system and not the properties of its parts; nor can it be deduced from the properties of its parts" [Gharajedaghi, 1999, p. 45]. Emergent behavior has always been possible in systems. However, emergent behaviors in industrial age systems could be better anticipated and addressed than systems engineered in the current age. Emergent behaviors in today's systems are often so subtle, or originate so deeply in layers of architecture, that their effects or origins can go unnoticed. Thus, there is a persistence of uncertainty and unpredictability in the performance and behavior of information age systems.

Why is this? A simple answer is because of networks and networked computing.

#### *Complex Systems, Systems of Systems, and Enterprise Systems*

The computer was a closed system before the advent of networks in ways similar to single-purpose machines of the Industrial Revolution. Network technologies brought isolated computers into an open system of globally connected machines, where information dissemination and collaboration is nearly instantaneous.

Networks became the enabling technology of information age systems. With this, separate and autonomous computers could now form into systems of networked computers and computing that grew in scale, complexity, and purpose.

Thus, in today's literature the terms *complex systems*, *systems of systems*, and *enterprise systems* are commonly found. What do these terms mean and how are they related?

It is important to note the systems engineering community is not settled on answers to these questions. These are cutting edge topics in engineering systems and system research. However, convergence of thought is beginning to emerge. The following discusses this further.

We begin with the term *complex system*. Keating et al. (2003) describe complex systems as those having attributes characterized by Jackson (1991). These are:

- Large number of variables or elements; rich interactions among elements;
- Difficulty in identifying attributes and emergent properties;
- Loosely organized (structured) interaction among elements;
- Probabilistic, as opposed to deterministic, behavior in the system;
- System evolution and emergence over time;
- Purposeful pursuit of multiple goals by system entities or subsystems (pluralistic);
- Possibility of behavioral influence or intervention in the system;
- Largely open to the transport of energy, information, or resources from/to across the system boundary to the environment.

Examples of complex systems include the space shuttle, a nuclear power plant, or a magnetic resonance imaging scanner.

More recently, and consistent with the above, White (2006) defines a complex system as “an open system with continually cooperating and competing elements – a system that continually evolves and changes its behavior according to its own condition and its external environment. Changes between states of order and chaotic flux are possible. Relationships between elements are imperfectly known and difficult to understand, predict, or control” [White, 2006, p. 5].

Engineering systems today are challenged when complex systems become more and more networked in ways that create metasystems – *systems of systems* “comprised of multiple embedded and interrelated autonomous complex subsystems” [Keating, 2004, p. 4]. Similarly, White (2006) defines a system of systems (SoS) as “a collection of systems that function to achieve a purpose not achievable by the individual systems acting independently. Each system can operate independently and accomplish its own separate purpose” [White, 2006, p. 5]. In a system of systems their whole is indeed more than the sum of their parts; however, it can’t exist without them.

Systems of systems form from integrations of multiple subsystems, where each subsystem can be a complex system. Examples of systems of systems include the Ballistic Missile Defense System (BMDS), the international earth observer program known as GEOSS (Global Earth Observation System of Systems), and navigation systems such as the Global Positioning System (GPS).

Building systems of systems like these is an enormous engineering and management challenge. If those challenges aren't enough, engineering systems of networked systems of systems is an even greater challenge and the newest being faced in engineering systems.

Systems of networked systems of systems are sometimes called *enterprise systems*. Enterprise systems such as the Internet, the Department of Defense Global Information Grid (GIG), or the Federal Aviation Administration's National Airspace Systems (NAS) are the cutting edge of information age computing and global communications.

The literature is very young on engineering enterprise systems. However, scholarship has begun to emerge from academia and industry. Writings by Allen (MIT, 2004) and Rebovich (MITRE, 2005) reflect thought trends from academic and industry perspectives, respectively.

In the monograph "Engineering Systems: An Enterprise Perspective" Allen et al. (2004) reflects on the nature of an enterprise and its effects on design and engineering solutions. "Such designs are no longer purely technical. In many cases, the enterprise issues are far more difficult than the technical ones to solve; moreover, there must be adaptation on both sides of the relationship between system and enterprise" [Allen, et al., 2004, p. 2]. Moreover, Allen identifies the critical and sometimes orthogonal relationships and goals of the multiple stakeholders in the design of an enterprise system. In this monograph Allen writes:

"An enterprise perspective on system design makes us aware of the fact that most such designs engage multiple stakeholders. These can range from shareholders to suppliers to members of the workforce to customers to society. What impact can this far-reaching effect have on system design? First of all, stakeholders' interests are not always in alignment.

System design may have to take this into account, balancing the interests of the various stakeholders. As a result, the design process is far more complex than one would be led to believe from the engineering science model that we teach to undergraduate engineering students. The best technical solution to a design may very well not be the best overall solution. In fact, it seldom is, and there may not even be a best technical design.

Take for example the current F-35 aircraft design. With several customers, each having different missions for this system, the designers cannot optimize the design for any one of the customers' desires. In addition, since recruiting customers in different countries often means engaging suppliers from those countries, adaptations may need to be made in the design to match the capabilities of those suppliers" [Allen, et al., 2004, p. 3].

Allen's insights echoed Bertalanffy's which recognized that systems, such as the F-35 or Boston's Big Dig, are fundamentally organizations made of entities (e.g., people) understood by "studying them not in isolation" but in how they assemble, react, and interact as a whole. Rebovich (2005, 2007), and other systems thinkers at MITRE, offer a view on what is meant by an enterprise and what is fundamentally different. They write the following:

"By enterprise we mean a network of interdependent people, processes and supporting technology not fully under control of any single entity. In business literature an enterprise



frequently refers to an organization, such as a firm or government agency; in the computer industry it refers to any large organization that uses computers.

Our definition emphasizes the interdependency of individual systems and **even systems of systems**. We include firms, government agencies, large information-enabled organizations and any network of entities coming together to collectively accomplish explicit or implicit goals. This includes the integration of previously separate units. The enterprise displays new behaviors that emerge from the interaction of the parts” [MITRE, 2007, p. 1].

### **What is fundamentally different?**

“A mix of interdependency and unpredictability, intensified by rapid technology change, is driving the need for new systems engineering techniques. When large numbers of systems are networked together to achieve some collaborative advantage, interdependencies spring up among the systems. Moreover, when the networked systems are each individually adapting to both technology and mission changes, then the environment for any given system becomes essentially unpredictable. The combination of massive interdependencies and unpredictability is fundamentally different. Systems engineering success is defined not for an individual known system, but for the network of constantly changing systems” [MITRE, 2007, p. 1].

From this, a key differentiator of an enterprise system is diminished control over its engineering by a centralized authority. Centralized or hierarchical control over design decisions is a feature in engineering systems of systems and traditional, well-bounded, systems (e.g., an airplane or an automobile). Systems of systems are, in most cases, engineered in accordance with stated specifications. These may be shaped by multiple stakeholders, but they are managed by a centralized authority with overall responsibility for engineering and fielding the system of systems.

This is not the case in engineering enterprise systems. An enterprise system is not characterized by firm and fixed specifications under the control of a centralized authority and agreed to by all participants throughout their organizational levels. The envelop that captures stakeholders affected by, or involved with, an enterprise system is so broad that centralized or hierarchical control over its engineering is generally not possible and perhaps not even desirable.

Given these challenges and considerations, how is engineering an enterprise planned? The short answer, given what we’ve seen so far, is through a continual and evolutionary development of capability. What is meant by capability? Based on experiences to date, planners of enterprise systems define capability as the *ability to achieve an effect to a standard under specified conditions using multiple combinations of means and ways to perform a set of tasks* [Office of the Secretary of Defense (OSD), 2005].

An enterprise is essentially a society of connected users with competing needs, interests, and behaviors. Thus, an enterprise system is characterized more by the capabilities it must field than by the specifications within which they must operate. Moreover, capabilities are constrained by the readiness of technology, availability of technology suppliers, and the operational limits of the systems and systems of systems that enable them.

An enterprise system must be adaptable to evolving missions, changing capability needs, and the dynamics of human behaviors that interact within the enterprise. Rebovich writes “Enterprise capabilities evolve through largely unpredictable technical and cultural dimensions. Enterprise capabilities are implemented by the collective effort of organizations whose primary interests, motivations, and rewards come from successfully fielding system capabilities” [Rebovich, 2007, p. 3]. He further writes:

“Enterprise engineering is an emerging discipline for developing enterprise capabilities. It is a multidisciplinary approach that takes a broad perspective in synthesizing technical and nontechnical (political, economic, organizational, operational, social and cultural) aspects of an enterprise capability.

Enterprise engineering is directed towards enabling and achieving enterprise-level and cross-enterprise operations outcomes. Enterprise engineering is based on the premise that an enterprise is a collection of entities that want to succeed and will adapt to do so. The implication of this statement is that enterprise engineering processes are more about shaping the space in which organizations develop systems so that an organization innovating and operating to succeed in its local mission will – automatically and at the same time – innovate and operate in the interest of the enterprise.

Enterprise engineering processes are focused more on shaping the environment, incentives and rules of success in which classical engineering takes place. Enterprise engineering coordinates, harmonizes and integrates the efforts of organizations and individuals through processes informed or inspired by natural evolution and economic markets. Enterprise engineering manages largely through interventions [innovations] instead of [rigorous/strict] controls” [Rebovich, 2007, p. 3].

### **Summary**

This literature review covered a lot of ground. First and foremost, the literature on systems and systems theory will continue to evolve. Systems science is endless. The more we explore, the more our present day understandings are shaped and further challenged. The more we advance in technology and global connectedness, the more open, complex, and virtual become the enabling systems.

Engineering and managing the development of enterprise systems necessitates, as never before, an openness and adaptability of process, practice, and procedure. Engineering methodologies appropriate today might not be appropriate tomorrow. Engineering management practices that scale today might not scale tomorrow. Because we cannot see beyond our line of sight, we should reserve judgment on the finality of any one process or practice at this stage of understanding.

It is with this view the risk analytical methods presented in this dissertation were designed. The analytic philosophy was to approach risk analysis in the enterprise space from a “whole systems” perspective. A perspective with roots in the writings of Bertalanffy (1968) and one influenced by recognizing the whole of an enterprise is not just more than the sum of its parts – but one wholly and continually shaped, expanded, or diminished by them.

## Risk, Decision Theory, and Engineering Risk Management Literature

*"I think there's a difference  
between a gamble and a calculated risk"*  
Edmund Hall North, American Screenwriter (1911 – 1990)

The literature in risk and decision theory is vast. Its foundations are deeply rooted in mathematics and economics. Risk and decision theory has been a field of study for at least 300 years and one with a rich history of cross-domain applications. The engineering, management, and behavioral sciences all apply and advance aspects of risk and decision theory in their problem spaces.

The study of risk is the study of chance and the study of choice. Risk is the chance an unwanted event occurs. Taking a risk is a choice to gamble on an event whose outcome is uncertain. Risk is the probability an unfavorable outcome is realized. However, a favorable or unfavorable outcome is a personal determination – one governed by a person's or a society's concept of value or worth.

Probability theory is the formalism to study chance. Decision theory is the formalism to study choice. Together, they provide the formalism to study risk. The importance of joining the study of chance and the study of choice was recognized by Swiss mathematician Daniel Bernoulli in his 1738 essay "Exposition of a New Theory on the Measurement of Risk" [Bernoulli, 1738] \*.

The following presents a focused review of risk and decision theory literature as it applies to the research in this dissertation. Figure 5 identifies authors of the literature reviewed. We'll begin with Bernoulli and his seminal 1738 essay, which proposed a mathematical relationship between chance and choice. We'll end with a return to Bertalanffy and his insights on the importance of this topic to general systems theory.

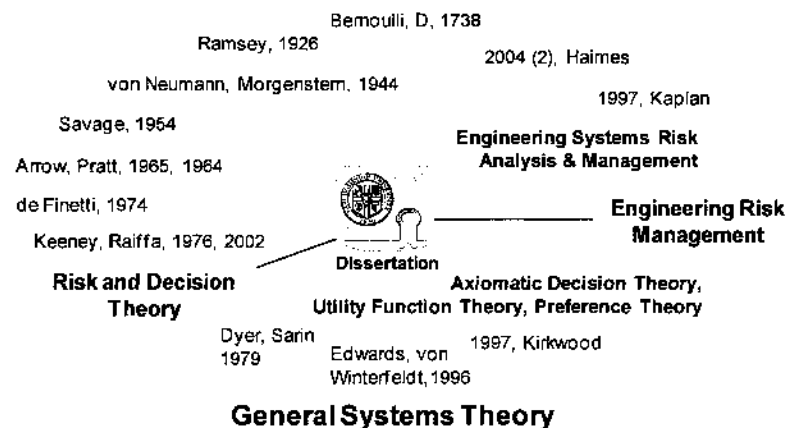


Figure 5. Literature Map: Risk and Decision Theory, Engineering Management

\* "Specimen theoriae novae de mensura sortis" in *Commentarii Academiae Scientiarum Imperialis Petropolitanae* (Papers of the Imperial Academy of Sciences in Petersburg) Vol. 5, 175-192, 1738. Translated as "Exposition of a New Theory on the Measurement of Risk", by Prof. L. Sommer, American University, for *Econometrica* Vol. 22 (1954).

Daniel Bernoulli published one of the most influential essays on a theory of risk and its measurement. He formed the idea that valuing monetary loss or gain from a gamble or lottery should be measured in context of a player's personal circumstance *and existing wealth*. It was the first time a person's affluence was directly considered in how they value an amount of money won or lost, instead of just its absolute numerical sum (e.g., 1,000 dollars)\*.

"To do this the determination of the value of an item must not be based on its price, but rather on the utility it yields. The price of the item is dependent only on the thing itself and is equal for everyone; the utility, however, is dependent on the particular circumstances of the person making the estimate. Thus, there is no doubt that *a gain of one thousand ducats is more significant to a pauper than to a rich man though both gain the same amount*" [Bernoulli, para. 3, 1738].



Figure 6. A Swiss Silver Thaler, Zurich, 1727\*\*

"Meanwhile, let us use this as a fundamental rule: If the utility of each possible profit expectation is multiplied by the number of ways in which it can occur, and we then divide the sum of these products by the total number of possible cases, a mean utility [*moral expectation*] will be obtained, and the profit which corresponds to this utility will equal the value of the risk in question" [Bernoulli, para. 4, 1738].

"Thus, it becomes evident that no valid measurement of the *value of a risk can be obtained without consideration being given to its utility*, that is to say, the utility of whatever gain accrues to the individual or, conversely, how much profit is required to yield a given utility. However it hardly seems plausible to make any precise generalizations since the utility of an item may change with circumstances. *Thus, though a poor man generally obtains more utility than does a rich man from an equal gain*" [Bernoulli, para. 5, 1738].

\* Daniel Bernoulli's essay was part of correspondences on a problem that became known as the St. Petersburg paradox. The paradox was one of five problems posed by Daniel's cousin Nicolas Bernoulli (1687-1759) to Pierre Raymond de Montmort (1678-1719) – a French mathematician who wrote a treatise on probability theory and games of chance. In a 1728 letter to Nicolas Bernoulli, Swiss mathematician Gabriel Cramer (1704-1752) independently developed concepts similar to those in Daniel Bernoulli's essay. Like Daniel Bernoulli, Cramer wrote "*mathematicians estimate money in proportion to its quantity, and men of good sense in proportion to the usage that they may make of it*". Cramer went on to propose a square root function to represent "proportion of usage", where Daniel Bernoulli derived a logarithmic function. Recognition of Cramer's thoughts as remarkably similar to his own is nicely acknowledged and written by Daniel Bernoulli at the close of his 1738 essay [reference: Bernoulli, 1738].

\*\* MONETA REIPUBLICÆ TIGURINÆ, oval city coat-of-arms within ornate frame supported by lions rampant, one holding palm, the other sword. DOMINI CONSERVA NOS IN PACE, aerial view of city along the Limmat River with boats; date in ornate cartouche [from source: <http://commons.wikimedia.org/wiki/Thaler>]. Image source from CNG coins [<http://www.cngcoins.com>, permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation license, Version 1.2].

With this, Bernoulli introduced the idea of *expected utility theory* and the logarithmic utility function (Figure 7) to represent decision-making under uncertainty. It was a formalism that directly captured personal or subjective measures of value (or worth) into a risk calculus.

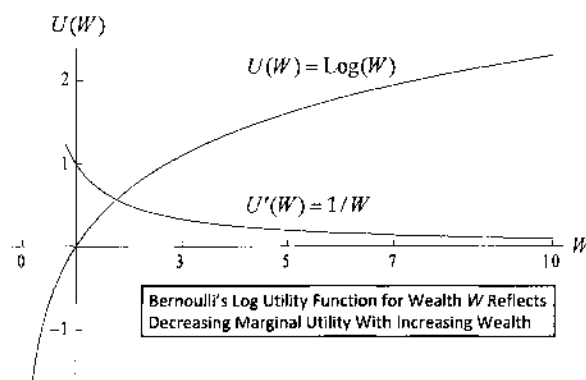


Figure 7. Bernoulli's Log Utility Function

Seen in Figure 7, Bernoulli's log utility function is concave. Concave functions always appear "hill-like". The log utility function exhibits a property known as *diminishing marginal utility*<sup>\*</sup>. This means for every unit increase in wealth, there is a corresponding decrease in the rate of additional utility with respect to that change in wealth.

Concave utility functions are always associated with a risk-averse person. A risk-averse person is willing to accept, with certainty, an amount of money less than the expected amount that might be received from a lottery or gamble. Bernoulli's risk measurement theory assumed all persons are risk averse. This assumption was reasonable given the socio-economic realities of 18th century Europe.

Despite the newness of Bernoulli's theory, it would be 200 years before John von Neumann and Oskar Morgenstern (1944) extended its ideas to a set of axioms known as the *axioms of expected utility theory*<sup>\*\*</sup>. The axioms of expected utility theory state conditions that must exist for rational decision-making in the presence of uncertainty.

Subject to these conditions, a rational individual will choose (or prefer) the option from a set of options (with uncertain outcomes) with maximum expected utility. With this, von Neumann and Morgenstern define a utility function over options with uncertain outcomes, lotteries, or gambles instead of over wealth as offered by Bernoulli.

Before presenting these axioms, it is important to mention that decision theorists treat individual preferences as *primitives*. In decision theory, a primitive is that not derived from other conditions [Garvey, 2008]. Decision theory is a calculus that operates on primitives to make visible which

<sup>\*</sup> Also known as "Bernoulli's *increasing-at-a-decreasing-rate* thesis, which economists would later term *diminishing marginal utility of wealth*" [Fishburn, P. C., 1989].

<sup>\*\*</sup> The axioms of expected utility are sometimes called the *axioms of choice* or the *preference axioms*.

option among competing options is the rational choice instead of interpreting why an individual prefers one option more than others.

How are preferences expressed? This can be illustrated by the following two examples.

- A person strictly prefers the color red more than the color black ( $\text{red} \succ \text{black}$ )\*
- A person *weakly* prefers 5 *A*-widgets more than 9 *B*-widgets ( $5 \text{ A-widgets} \succeq 9 \text{ B-widgets}$ )

The principle axioms of von Neumann-Morgenstern (vNM) expected utility theory are as follows:

#### **Completeness Axiom**

Given lottery *A* and lottery *B*, a person can state *A* is strictly preferred to *B* ( $A \succ B$ ) or *B* is strictly preferred to *A* ( $B \succ A$ ) or the person is indifferent between them ( $A \sim B$ )

#### **Transitivity Axiom**

If a person prefers lottery *A* more than lottery *B* and lottery *B* more than lottery *C*, then lottery *A* is preferred to lottery *C*.

#### **Continuity Axiom**

If a person prefers lottery *A* more than lottery *B* and lottery *B* more than lottery *C*, then there is a probability *p* such that this person is *indifferent* between receiving lottery *B* with *certainty* and receiving a compound lottery\*\* with probability *p* of receiving lottery *A* and probability  $(1 - p)$  of receiving lottery *C*.

The continuity axiom means a person is willing to act on an event that has a favorable or unfavorable outcome if the probability the unfavorable outcome occurs is reasonably small. Another way to view this axiom is as follows: a slight change in an outcome's occurrence probability *p* does not change a person's preference ordering of these outcomes. The continuity axiom implies a continuous utility function exists that represents a person's preference relation.

#### **Independence Axiom**

If a person prefers lottery *A* more than lottery *B*, then a compound lottery that produces lottery *A* with probability *p* and lottery *C* with probability  $(1 - p)$  is preferred to a compound lottery that produces lottery *B* with probability *p* and lottery *C* with probability  $(1 - p)$ .

The independence axiom means a person's preference order for any pair of lotteries, *A* and *B*, is preserved when *A* and *B* are mixed with a third lottery *C*, provided lottery *A* and lottery *B* are produced with probability *p* and lottery *C* is produced with probability  $(1 - p)$ .

---

\* The notation  $\succ$  is a preference relation notation. Here,  $A \succ B$  means a person **strictly** prefers outcome *A* more than outcome *B*;  $A \succeq B$  means a person **weakly** prefers outcome *A* more than outcome *B* (the outcome from *A* is at least as good as the outcome from *B*);  $A \sim B$  means a person is **indifferent** between outcome *A* or outcome *B*.

\*\* A compound lottery is one whose possible outcomes are themselves simple lotteries; a simple lottery is a gamble or risky prospect whose outcomes are determined by chance.

Thus, in vNM utility theory if an individual's preferences obey these axioms then they act rationally in choosing the option that has maximum expected utility from a set of options whose outcomes are uncertain.

The vNM axiomatization of utility furthered a formal theory of risk with respect to choices under uncertainty. From this, the existence of utility functions could be claimed and their shapes could be associated with a person's attitude for risk averse, risk seeking, or risk neutral behavior.

In a situation where gains are preferred to losses, a risk averse person is one willing to accept a gain with certainty that is less than the expected amount received from a lottery. The opposite characterizes a risk seeking person. A risk seeking person is one willing to accept a loss greater than the expected amount received from a lottery. A risk neutral person is one who is neither risk averse nor risk seeking. Such a person would be willing to accept a gain or a loss equal only to the expected amount received from a lottery.

There is a class of utility functions that model attitudes with respect to risk averseness, risk seeking, and risk neutral behaviors. A family of such functions is shown in Figure 8.

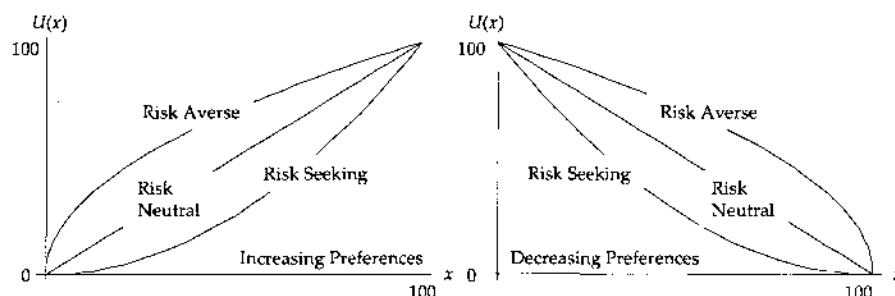


Figure 8. Families of Risk Attitude or Utility Functions [Garvey, 2008]

Concave utility functions model risk averse attitudes. When gains are preferred to losses, concave utility functions show for every unit increase in  $x$  there is a slower rate of increase in utility. Convex utility functions model risk seeking attitudes. When gains are preferred to losses, convex utility functions show for every unit increase in  $x$  there is a faster rate of increase in utility. Linear utility functions model risk neutral attitudes. Here, for every unit increase in  $x$  there is a constant rate of increase in utility regardless of whether gains are preferred to losses.

From this, utility theorists began to measure a person's degree of risk averseness by the steepness of their utility function. From calculus, the second derivative of a function provides information about its curvature. Since a vNM utility function  $U(x)$  is monotonic and continuous on a close interval  $a \leq x \leq b$ , from differential calculus  $U(x)$  is concave if  $U''(x) < 0$  and convex if  $U''(x) > 0$  for all  $x$  such that  $a \leq x \leq b$ . So, can  $U''(x)$  provide a measure of a person's degree of risk averseness? Not by itself.

A key property of vNM utility functions is they are unique up to an affine transformation. They are cardinal functions. Preference differences between points along their curves have meaning in

accordance with cardinal interval scales\*. Unfortunately,  $U''(x)$  is not invariant under an affine transformation.

However, two theoretical economists K. J. Arrow [Arrow, 1965] and J. W. Pratt [Pratt, 1964] created an index that used  $U''(x)$  and preserved the preference structure of  $U(x)$ . This became known as the Arrow-Pratt risk aversion index. The index is defined as follows:

$$R_A = -\frac{U''(x)}{U'(x)}$$

Using the Arrow-Pratt risk aversion index, it can be shown that the Bernoulli log utility function has decreasing absolute risk aversion; that is,

$$R_A = -\frac{U''(W)}{U'(W)} = -\frac{(-1/W^2)}{1/W} = \frac{1}{W} = U'(W)$$

if  $U(W) = \text{Log}(W)$  and  $W$  denotes wealth. Thus, the Bernoulli log utility function has decreasing absolute risk aversion and decreasing marginal utility with increasing wealth, as shown in Figure 7. This means the amount of wealth a person is willing to risk increases as wealth increases.

The works of Daniel Bernoulli, John von Neumann, Oskar Morgenstern, and others brought about ways to study rational decisions relative to risk and risk taking. A theory of risk emerged where a person's choice to engage in events with uncertain outcomes could be represented by bounded and monotonic functions called utility functions – mathematical expressions which capture preferences, measures of worth, or degrees of risk aversion *unique* to an individual.

In many ways, utility theory as a basis for a theory of risk was a revolution in the growth of mathematical thought. Prior to Daniel Bernoulli's 1738 essay on the St. Petersburg paradox, mathematics was principally applied to problems in natural sciences. By 1738, however, mathematics was intersecting with problems in social sciences and most prominently with the study of economics. Economics provided the ideal problem environment to evolve theories of rational choice, as reflected in a person's decision to invest in options with uncertain outcomes.

---

\* An interval scale is a measurement scale in which attributes are assigned numbers such that differences between them have meaning. The zero point on an interval scale is chosen for convenience and does not necessarily represent the absence of the attribute being measured. Examples of interval scales are the Fahrenheit (F) or Celsius (C) temperature scales. The mathematical relationship between these scales is an *affine transformation*; that is,  $F = (9/5) \cdot C + 32$ . The zero point in a temperature scale does not mean the absence of temperature. In particular, zero degrees Celsius is assigned as the freezing point of water.

Because distances between numbers in an interval scale have meaning, addition and subtraction of interval scale numbers is permitted; however, because the zero point is arbitrary, multiplication and division of interval scale numbers is not permitted. For example, we can say that 75 degrees Fahrenheit is 25 Fahrenheit degrees hotter than 50 degrees Fahrenheit; but, we cannot say 75 degrees Fahrenheit is 50 percent hotter than 50 degrees Fahrenheit. However, ratios of differences can be expressed meaningfully; for example, one difference can be one-half or twice or three-times another.



Around the same time von Neumann and Morgenstern were forming an axiomatic basis for a theory of rational choice, mathematicians were revisiting views on the nature of probability and its meaning as a measure. As mentioned earlier, the study of risk is the study of chance **and** the study of choice; thus, the dual concepts of probability and choice are integral to a theory of risk.

In 1926, F. P. Ramsey of the University of Cambridge wrote “Truth and Probability” [Ramsey, Mellor (editor), 1990]. In this work, Ramsey produced some of the earliest arguments and proofs on the logical consistency of subjective utility and subjective probability as measures of value and chance; the latter which he proved follows the laws of probability.

Ramsey wrote that measuring a person’s degree of belief in the truth of a proposition can be determined from the odds a person would accept when gambling on an uncertain outcome. Thus, Ramsey connected an individual’s decision to engage in a bet with their previous knowledge or experience on whether the outcome would likely be in their favor or in their disfavor. This is essentially a lottery, which von Neumann and Morgenstern would later make fundamental to their theory of rational choice.

Ramsey’s view of probability became increasingly the modern interpretation. Independent of Ramsey’s essay, Italian mathematician B. de Finetti (1974) went so far to say “probability does not exist” [Nau, 2002, p. 90] – meaning that probability has only a subjective meaning [de Finetti, 1974]. “This definition neatly inverts the objectivistic theory of gambling, in which probabilities are taken to be intrinsic properties of events (e.g., propensities to happen or long-run frequencies) and personal betting rates are later derived from them. Of course, subjective probabilities may be informed by classical, logical, or frequentist reasoning in the special cases where they apply” [Nau, 2002, p. 90].

Like Ramsey, de Finetti associated probability with the “rate at which an individual is willing to bet on the occurrence of an event. Betting rates are the primitive measurements that reveal your probabilities or someone else’s probabilities, which are the only probabilities that really exist” [Nau, 2002, p. 90]. Thus, de Finetti, like Ramsey, viewed probability as dependent on the state of a person’s knowledge.

In 1954, Savage further extended the ideas of Ramsey, von Neumann and Morgenstern, and de Finetti to ultimately form a Bayesian approach to statistical theory [Savage, 1954]. In particular, Savage described a relationship between probability and preference as follows:

“Moreover, a utility function  $u$  is unique up to a positive affine (linear) transformation, and the subjective probability  $\pi$  is unique. The relation between probability and preference revealed by the representation is

$$\pi(A) > \pi(B) \underset{\text{iff}}{\Leftrightarrow} \{x \text{ if } A, y \text{ if not } A\} \succ \{x \text{ if } B, y \text{ if not } B\}$$

whenever outcome  $x$  is preferred to outcome  $y$ . Thus, for Savage, you regard  $A$  as more probable than  $B$  if you would rather bet on  $A$  than  $B$  for the preferred outcome” [Fishburn, 1989, p. 388].

Despite continuing debates on the interpretation of probability throughout the 20th century, the issue was essentially settled in 1933. About ten years prior to the vNM axioms of utility, Russian mathematician A. N. Kolmogorov<sup>\*</sup> presented a definition of probability in terms of three axioms.

The first axiom states the probability of any event is a non-negative number in the interval zero to unity. The second axiom states the sure or certain event has probability equal to one. The third axiom states for any sequence of mutually exclusive events, the probability of at least one of these events occurring is the sum of the probabilities associated with each event.

Thus, probability need only be a numerical measure that behaves according to these axioms. This encompassed all competing interpretations on its nature and allowed objective and subjective probabilities to be part of the “Laplacian” calculus.

### Modern Decision Theory

Decision theory has much of its modern theoretical basis in the classic text *Decisions with Multiple Objectives: Preferences and Value Tradeoffs* by R. L. Keeney and H. Raiffa (1976). In this work, Keeney and Raiffa extend the ideas of value and vNM expected utility theory into a modern theory of preference. Preference theory has become the theoretical foundation for most of today’s engineering systems risk analysis methods, as well as for the work in this dissertation.

Howard Raiffa has written extensively on subjective probability theory, the need for consistency with Kolmogorov’s axioms, and its role in Bayesian statistical inference – particularly with decision-making under conditions of uncertainty. Raiffa introduced concepts of preferential and utility independence – key to examining tradeoffs between alternatives and their performance across multiple criteria. The study of tradeoffs led to a theory of multiattribute utility – whose extensive development Raiffa credits to Ralph Keeney, his doctoral student at that time.

Where tradeoffs under conditions of uncertainty are captured by multiattribute utility, tradeoffs under conditions of certainty are captured by multiattribute value theory. Keeney and Raiffa (1976) write the following:

“The multiattribute value problem is one of value tradeoffs. If there is no uncertainty in the problem, if we know the multiattribute consequence of each alternative, the essence of the issue is, *How much achievement on objective 1 is the decision-maker willing to give up to improve achievement on objective 2 by some fixed amount?* If there is uncertainty in the problem, the tradeoff issue remains, but difficulties are compounded because it is not clear what the consequences of each alternative will be. The tradeoff issue often becomes a personal value question and, in those cases, it requires the subjective judgment of the decision-maker. There may be no right or wrong answers to these value questions and, naturally enough, different individuals may have different value structures” [Keeney, Raiffa, 1976, pp. 66-67].

Although, Keeney and Raiffa extended the theoretical foundations of vNM utility theory, it was Krantz et al. (1971) and Dyer and Sarin (1979) who developed value functions as formalisms to

---

<sup>\*</sup> A. N. Kolmogorov, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, *Ergeb. Mat. und ihrer Grenz.*, vol. 2, no. 3, 1933. Translated into English by N. Morrison, *Foundations of the Theory of Probability*, New York (Chelsea), 1956.

capture a person's *strength of preference*. A value function is a real-valued function defined over an evaluation criterion (or attribute) that represents an alternative's (or option's) measure of goodness over the levels of the criterion. A measure of "goodness" reflects a decision-maker's judged value in the performance of an alternative (or option) across the levels of a criterion (or attribute).

Like a utility function, a value function<sup>\*</sup> is usually designed to vary from zero to one over the range of levels (or scores) for a criterion. In practice, the value function for a criterion's least preferred level (or score) (i.e., the least preferred option or alternative) takes the value zero. The value function for a criterion's most preferred level (or score) (i.e., the most preferred option or alternative) takes the value one.

Dyer and Sarin (1979) introduced the concept of a *measurable value function*. A measurable value function is one where the value difference between any two levels (or scores) within a criterion (or attribute) represents a decision-maker's strength of preference between them – also referred to as preference differences.

A measurable value function<sup>\*\*</sup> is monotonic in preferences and where value differences represent relative strength of preference. Large value differences between options (alternatives) indicate the difference in preference between them is greater than the difference in preference between other options (alternatives). Furthermore, the numerical amount of this difference represents the relative amount of preference difference. The concept of value differences is also a "primitive concept" in decision theory; that is, it is a concept not derived from other conditions.

One way to address tradeoff problems is found in *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets* [Kirkwood, 1997]. In this work, he writes "if a decision-maker is multiattribute risk averse, then it is necessary to determine a utility function to convert values calculated using a multiattribute value function into utilities. This utility function can then be used to rank alternatives that have uncertainty about their outcomes."

Kirkwood (1997) presents a utility function known as the *power-additive utility function*. It is an exponential utility function that is a function of a multiattribute value function. With the power-additive utility function, Kirkwood connects utility theory to preference theory and to the concept of multiattribute risk averseness (or risk tolerance).

Although the power-additive utility function has many useful theoretical properties, its strengths are in its practical aspects. Its shape is fully determined by a single parameter that reflects the risk averseness of a decision-maker. This parameter is known as *multiattribute risk tolerance*  $\rho_m$ .

One way to determine  $\rho_m$  is for the decision-maker to select the value that reflects his/her risk attitude. Where increasing preferences apply, an extremely risk averse decision-maker might

---

<sup>\*</sup> A utility function is a value function but a value function is not necessarily a utility function [Keeney, Raiffa, 1976].

<sup>\*\*</sup> The vertical axis of a measurable value function is a cardinal interval scale measure of the strength of a decision-maker's preferences. For this reason, a measurable value function is also referred to as a cardinal value function (refer to Dyer and Sarin (1976) and Kirkwood (1997)).

select  $\rho_m$  in the interval  $0.05 \leq \rho_m \leq 0.15$ . A less risk averse decision-maker might select  $\rho_m$  in the interval  $0.15 < \rho_m \leq 1$ . As  $\rho_m$  becomes increasingly large the decision-maker becomes increasingly risk neutral and the power-additive utility function approaches a straight line. Here, the expected value of the value function can be used to rank alternatives\*. Figure 9 presents families of power-additive utility functions for various  $\rho_m$  and for increasing preferences.

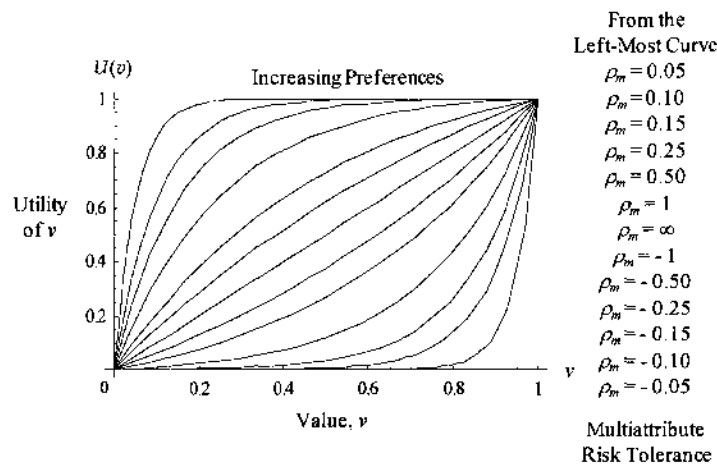


Figure 9. Families of Power-Additive Utility Functions [Garvey, 2008]

Preference theory and subjective expected utility theory grew in prominence as a mathematical foundation for a theory of rational choice. With this, it became increasingly necessary to understand its conjunction with human behavior relative to decision-making under uncertainty.

By the 1950s, decision theory joined with behavioral science through the works of Ward Edwards and his graduate student Detlof von Winterfeldt. Two influential papers written by Edwards in 1954 and 1961 introduced vNM utility theory for the first time to the field of psychology.

From these papers, an entirely new branch of study called behavioral decision theory emerged. Behavioral scientists began to study whether human behavior followed the views of vNM utility theory. Today, the findings remain somewhat mixed. Nonetheless, Edward's brought a behavioral science view to the topic of rational choice and human decision-making. His many contributions included identifying that persons have preference structures for probabilities and not just for utilities [von Winterfeldt, Edwards, 1986]. Consider the following from Fishburn (1989).

"In early work on the psychology of probability, Edwards observed that people's betting behavior reveals preferences among probabilities. For example, given monetary gambles with equal expected values, subjects consistently liked bets with win probability 1/2 and avoided bets with win probability 3/4. Moreover, these probability preferences were reversed in the loss domain, were insensitive to the amounts involved, and could not be explained by curved utility functions" [Fishburn, 1989, p. 391].

\* This is where the expected value of an outcome would equal its expected utility; hence, either decision rule would be a rational basis for the choice under consideration.

### Engineering Risk Management

The intellectual groundwork just described has natural extensions to engineering systems, how they are managed and their risks assessed. Successfully engineering today's systems requires deliberate and continuous attention to the management of risk. Managing risk is an activity designed to improve the chance these systems will be completed within cost, on time, and meet safety and performance objectives.

As mentioned earlier, the study of risk is the study of chance and the study of choice. In engineering a system, risk is the chance an event occurs with unwanted consequences on the system's cost, schedule, or performance. Furthermore, choices must be made on where to allocate resources to manage risks such that, if they occur, their consequences to the system are eliminated or reduced to acceptable levels.

Until the mid-1970's, risk analyses in engineering systems were often informal and characterized by ad hoc collections of qualitative approaches. However, by 1975 qualitative approaches began to be replaced with increasingly insightful quantitative methods. One such method became known as Quantitative Risk Assessment (QRA)\*.

A founder of QRA was Stan Kaplan, an engineer and applied mathematician who first used the technique to analyze risks associated with engineering and operating nuclear power plants. For this, Kaplan gave a definition of "risk" consistent with past scholarship but in a context specific to engineering systems. Kaplan (1997) states that risk analyses in general, and specifically in engineering systems, really involve answering three questions [Kaplan, 1997, p. 408]. They are:

*"What can happen?"*

*"How likely is that to happen?"*

*"If it happens what are the consequences?"*

These questions became known as Kaplan's triplet. This is represented by the expression

$$Risk = \langle Scenario, Probability, Consequence \rangle$$

where *Scenario*, *Probability*, and *Consequence* reflect these first, second, and third questions, respectively.

A hallmark of QRA is the idea of evidence-based decision-making. Here, Kaplan writes when dealing with an expert one should never ask for his opinion. Instead, we want his experience, his information, and his evidence [Kaplan, 1997]. This includes expert-driven evidence-based probabilities, the second component of Kaplan's triplet.

The impetus for this aspect of QRA is rooted in the views of probability expressed by Ramsey, de Finetti, and Savage, as well as from E. T. Jaynes who wrote extensively on probability as a theory of logic.

---

\* Quantitative Risk Assessment (QRA) is also known as Probabilistic Risk Assessment (PRA).

“Probabilities need not correspond to physical causal influences or propensities affecting mass phenomena. Probability theory is far more useful if we recognize that probabilities express fundamentally logical inferences pertaining to individual cases” [Jaynes, 1988, p. 1].

“In our simplest everyday inferences, in or out of science, it has always been clear that two events may be physically independent without being logically independent; or put differently, they may be logically dependent without being physically dependent. From the sound of raindrops striking my window pane, I infer the likely existence of clouds over-head

$$P(Clouds | Sound) \approx 1$$

although the sound of raindrops is not a physical causative agent producing clouds. From the unearthing of bones in Wyoming we infer the existence of dinosaurs long ago:

$$P(Dinosaur | Bones) \approx 1$$

although the digging of the bones is not the physical cause of the dinosaurs. Yet conventional probability theory cannot account for such simple inferences, which we all make constantly and which are obviously justified. As noted, it rationalizes this failure by claiming that probability theory expresses partial physical causation and does not apply to the individual case” [Jaynes, 1988, p. 14].

“But if we are to be denied the use of probability theory not only for problems of reasoning about the individual case; but also for problems where the cogent information does not happen to be about a physical cause or a frequency, we shall be obliged to invent arbitrary *ad hoc* theories for dealing with virtually all real problems of inference; as indeed the orthodox school of thought has done. Therefore, if it should turn out that probability theory used as logic is, after all, the unique, consistent tool for dealing with such problems, a viewpoint which denies this applicability on ideological grounds would represent a disastrous error of judgment, which deprives probability theory of virtually all its real value and even worse, deprives science of the proper means to deal with its problems” [Jaynes, 1988, p. 14].

The QRA approach emphasized the importance of scenario-driven risk analyses and the integration of probability and consequence measures with cost-benefit-risk tradeoffs to derive optimal risk reduction choices among competing courses-of-action. Early QRA applications focused on quantifying risks to public safety by certain types of engineering systems, such as nuclear power systems. As QRA methods improved, so did the breadth of their applications to broader types of engineering systems.

The text *Risk Modeling, Assessment, and Management* [Haines, 1998, 2004] was a major contribution in the extension of risk analysis methods to the broader engineering systems community. Innovations by Haines were many. Among them were extensions of Keeney-Raiffa decision theory to enable the study of tradeoffs between risks with multi-consequential impacts to an engineering system. In addition, Haines was an early author of engineering risk management methods and ways for them to integrate into the processes and practices of project management.

## Summary

*"You've got to be very careful if you don't know  
where you're going, because you might not get there"*  
Lawrence Peter "Yogi" Berra, American Baseball Player (b. 1925)

The literature on risk and decision analysis has deep roots in philosophies of logic, probability, and theories of rational choice. Despite discordant views on elemental issues (i.e., *Does probability exist? Can utility functions represent human preference?*) it nonetheless illuminates the merits of competing alternatives, especially where interactions and tradeoffs between them would otherwise not be visible.

Bertalanffy recognized vNM utility theory as concerned with the "behavior of supposedly "rational" players to obtain maximal gains and minimal losses by appropriate strategies against the other player (or nature). Hence, it concerns essentially a "system" of antagonistic "forces" with specifications" [Bertalanffy, 1968, p. 22].

One can apply Bertalanffy's view to risk management in engineering systems. Here, risk management is concerned with the behavior of supposedly rational decision-makers to field systems that maximally achieve outcome objectives and while minimizing failure to do so. Appropriate strategies (i.e., risk mitigation approaches) are taken against risks ("the other player") that threaten success. Hence, an engineering system's manager is always concerned with managing successfully through a "system" of antagonistic "forces".

Thus, one may view risk and decision analysis as very much a systems science, as recognized by Bertalanffy. It follows that risk management in engineering systems is also a systems science – one that necessitates taking and benefits from a "whole systems" perspective. Such a perspective is needed not only for systems of systems and enterprise systems but for traditional systems as well.

Built upon this view, this research formulates an analytical framework and computational model for assessing risk in engineering enterprise systems from a whole systems perspective. It's a topic at the interface between risk management methods in engineering traditional systems with those needed in engineering enterprises.

Recognizing this interface and addressing its risk analytic challenges is a key contribution of this research. It is an essential step in creating new methods and new practices uniquely designed to successfully manage risk in engineering enterprise systems.

N. W. Dougherty, president of the American Society for Engineering Education (1954 – 1955), once said *"the ideal engineer is a composite.. he is not a scientist, he is not a mathematician, he is not a sociologist or a writer; but he may use the knowledge and techniques of any or all of these disciplines in solving engineering problems"*. That was true then and is even truer in engineering today's sophisticated, complex, and highly networked engineering systems.

## RESEARCH OBJECTIVES AND CONTRIBUTIONS

The objective of this research is to address the engineering management problem of how to represent, model, and measure risk in large-scale, complex, systems engineered to function in enterprise-wide environments. This was accomplished by formulating an analytical framework and computational model for assessing risk in engineering enterprise systems.

Achieving this objective extends current practice in the management of risk for traditional systems and created new constructs and new protocols for the management of risk in engineering enterprise systems. This work advances engineering management theory and practice in ways that include the following:

- Structuring the enterprise systems engineering problem space that enables capability-based risk analyses to be conducted by representing this space via a supplier-provider metaphor.
- Developing mathematical protocols for measuring risk within structures of capability portfolios, where portfolios collectively deliver capability to users served by the enterprise. This includes new ways to compose risk probability and consequence assessments into utility measures that will also permit traceability of risk-driving events affecting the enterprise.
- Applying advanced decision-theoretic algorithms to measure risk criticality as a function of these measures and capability dependencies present in a portfolio.
- Designing new measurement protocols to capture capability dependency risks and risk co-relationships that may exist in an enterprise. These protocols are called the Risk Co-Relationship (RCR) Index and the Functional Dependency Network Analysis (FDNA) approach. They are distinguished as follows:

*The Risk Co-Relationship (RCR) Index is a new management metric that measures and traces risk inheritance and its collateral effects across an enterprise.*

*The Functional Dependency Network Analysis (FDNA) approach is a new technique employing graph theory concepts to measure the operability/inoperability of capability if, due to risks, one or more enabling suppliers in the supplier-provider chains degrade, fail, or are eliminated.*

- Demonstrating how these formalisms integrate with investment decision methods that determine optimum, or satisficing, strategies on where resources are best allocated to reduce (or eliminate) risks that threaten capability outcome objectives.

## Dissertation Research Problem Areas

This dissertation focused on five core problem areas. Solution approaches were developed for each area in the form of analytic methodologies.

There is an implied sequence to each problem area. The first establishes a framework within which to study systems engineering risk theory and how it extends to the enterprise problem.



Solutions to subsequent problem areas are built upon this framework. These results then come together to form an overall analytical framework and computational model designed to measure risk in large-scale, complex, systems engineered to function in enterprise-wide environments.

### **Problem Area 1**

Describe and structure the risk management problem space as it relates to engineering enterprise systems from a capability portfolio perspective.

This area focused on bringing conceptual understandings of engineering enterprise systems into a framework where risk management theory and practice can be studied and new formalisms created. This problem area falls at the interface between traditional approaches and frameworks developed for engineering systems of systems and enterprise systems.

Describing and structuring the enterprise engineering problem space in ways that enable capability-based risk analyses is an original contribution to current risk management practice. Viewing this space via a supplier-provider metaphor and formulating risk measurement protocols within that structure takes advantage of an existing management paradigm that breaks capability portfolios into mission-to-task decomposition trees.

Although the use of a decomposition tree is an existing framework in portfolio analyses its use in risk management is new. However, instead of creating mission-to-task trees this research builds capability-to-supplier trees which are essentially mathematical graphs. Algorithms are then designed to operate on these graphs that produce various measures of capability risk.

### **Problem Area 2**

Develop mathematical protocols for measuring risk within structures of capability portfolios, where these portfolios collectively deliver capability to consumers served by the enterprise. Create measurement formalisms that account for, and track, multiple sources where risks to capabilities originate.

This area focused on creating specific measurement scales, computational algebras, and unique value function formulations to measure capability risk. Elements from mathematical graph theory are used to represent a capability portfolio's supplier-provider topology. Developing these protocols advances engineering management theory and practice as it relates to the objectives of this dissertation. Presently, there are no published protocols for quantifying capability risk in the context of portfolios that define an enterprise.

### **Problem Area 3**

Apply decision-theoretic algorithms for ranking risk criticality as a function of the measures developed in Problem Area 2 and capability dependencies in a portfolio. This area focused on applying advanced ranking algorithms to capture each risk's multi-consequential impacts and dependencies that may exist across an enterprise.

The significance of solutions to this problem area is the innovation in applying advanced ranking protocols for managing risk in engineering enterprise systems. This provides decision-makers a

logical and rational basis for addressing the choice problem of selecting which capability risks to lessen, or eliminate, as a function of their criticality to the portfolio and to the enterprise.

#### **Problem Area 4**

Develop protocols for capturing and measuring vertical and horizontal dependencies between capabilities within a portfolio and across a portfolio's supplier-provider topology.

This area focused on developing ways to represent and measure capability dependencies in engineering enterprise systems as a critically important aspect of enterprise risk management. The importance of this problem is many-fold. Primary is enabling management to study ripple effects of failure in one capability on other dependent capabilities. Offering ways to study these effects enables engineers to design for minimizing dependency risks that, if realized, have cascading negative impacts on the ability of an enterprise to deliver services to consumers.

This work introduces to the community a new management metric called the Risk Co-Relationship (RCR) index. The index provides a way to address the question: *How risk-dependent are capabilities so threats to them can be discovered before contributing programs (e.g., suppliers) degrade, fail, or are eliminated?* Its purpose is to signal where risk reducing opportunities exist to minimize dependency risks that, if realized, can have cascading negative effects on the ability of an enterprise to deliver capabilities and services to users.

This work also introduces to the community a new technique called Functional Dependency Network Analysis (FDNA). The FDNA approach enables the engineering community to address the question: *What is the effect on the operability of capability if one or more contributing program (e.g., suppliers) or supplier-provider chains degrade, fail, or are eliminated?*

#### **Problem Area 5**

Bring together research and solution approaches developed in the preceding problem areas into a coherent approach for representing, modeling, and measuring risk in engineering large-scale, complex, systems designed to function in enterprise-wide environments.

With the completion of this problem, the engineering management and systems engineering community has a generalized framework and computational model for the analysis of risk in engineering enterprise systems. This provides decision-makers formal ways to model and measure enterprise-wide risks, their potential multi-consequential impacts, dependencies, and their rippling effects within and beyond enterprise "boundaries". Management is enabled with analytic methods to develop holistic views of risks so capabilities and enterprise-wide outcomes can be achieved.

### Research Problem Area Relationships

This section explains why these problem areas were chosen for the dissertation, how they relate to each other, and how they relate to processes common to traditional systems engineering risk management. Consider Figure 10.

In Figure 10, these research problems provide a bridge between risk management processes common to traditional systems with those needed for, non-traditional, enterprise systems. Problem Area 1 is the base of the research. From an enterprise engineering risk management perspective, Problem Area 1 is a close equivalent to the process for *identifying risk* in engineering traditional systems.

Shown later, Problem Area 1 applies a supply-chain metaphor to represent an enterprise by capability portfolios. Here, each portfolio is expressed as mathematical graph. This graph shows how capabilities, provided to the enterprise by a specific portfolio, are enabled by contributions from specific programs and technologies. These programs and technologies are the suppliers in this chain. They are also a major source for identifying risks to capabilities, since capability risks that may negatively affect an enterprise are driven, in large part, by risks faced by their suppliers.

Problem Areas 2 and 4 combine into the next level up the diagram, in Figure 10. From an enterprise engineering risk management perspective, these areas form a close equivalent to the process for *analyzing risk* in engineering traditional systems.

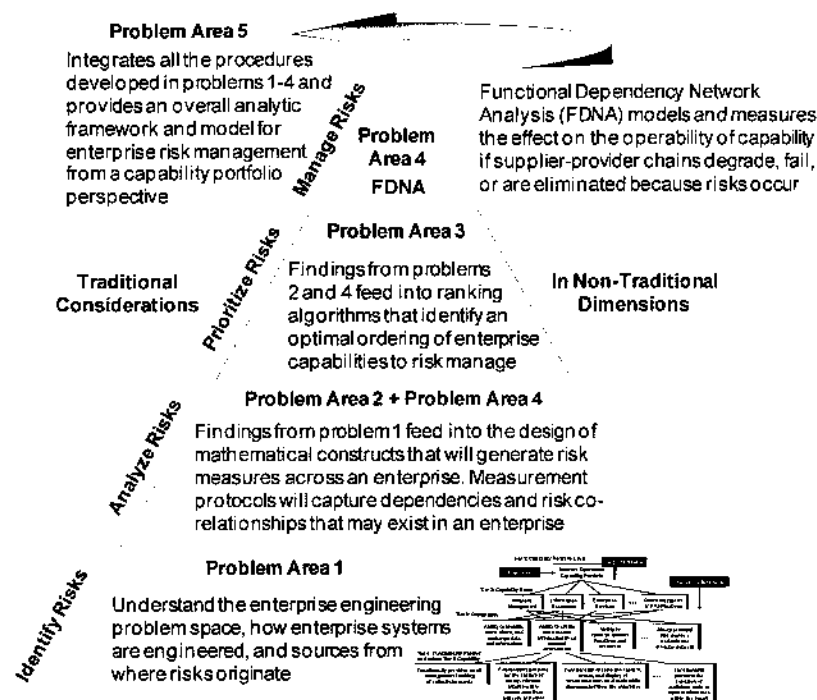
Problem Areas 2 and 4 apply findings from Problem Area 1 to design mathematical formulas that generate measures of capability risk for each capability in the “supplier-provider” graph of an enterprise’s portfolio. Dependency relationships associated with risk inheritance and capability operability interactions are also captured.

Problem Area 3 is the next level up the diagram, in Figure 10. From an enterprise engineering risk management perspective, Problem Area 3 is a close equivalent to the process for *prioritizing risk* in engineering traditional systems.

Problem Area 3 uses capability risk measures, just discussed, as inputs into advanced ranking algorithms to isolate which capabilities, in a portfolio, are most risk-threatened. This enables management to target risk reduction resources in ways that optimally reduce threats posed by risks to critical enterprise capabilities.

Problem Area 4 is at the top of Figure 10. From an enterprise engineering risk management perspective, Problem Area 4 is a close equivalent to the process for *managing risk* in engineering traditional systems. Problem Area 4 models and measures the critical consideration of dependencies in engineering enterprise systems. As mentioned earlier, two types of dependencies exist in this problem space.

**Integration Path of Problem Area Research:  
Leads to Overall Analytic Framework**



**Figure 10. Research Problem Area Relationships**

One dependency is risk inheritance; that is, *how risk-dependent are capabilities so threats to them can be discovered before contributing programs (e.g., suppliers) degrade, fail, or are eliminated?* The other dependency is operational dependence; that is, *what is the effect on the operability of capability if one or more contributing program (e.g., suppliers) or supplier-provider chains degrade, fail, or are eliminated?*

Factoring dependency considerations into the protocols presented in this dissertation enables the proper management of enterprise risk; specifically, investment decisions on where to target risk reduction resources in ways that optimally reduce threats posed by dependencies between risks, and capability operability, within and across portfolios of an enterprise.

Problem Area 5 is the completion of this research. It is outside the “pyramid” in Figure 10 because it is an “integrating activity” of the preceding problems; that is, Problem Area 5 integrates the findings and analytics developed in Problem Areas 1-4 into a coherent analytical framework for risk analysis and management in the context of engineering enterprise systems.

### Dissertation Research Contributions Summary

This research contributes to the engineering systems community across three dimensions; namely, General, Technical, and Literature. A summary of these contributions is shown in Figure 11.

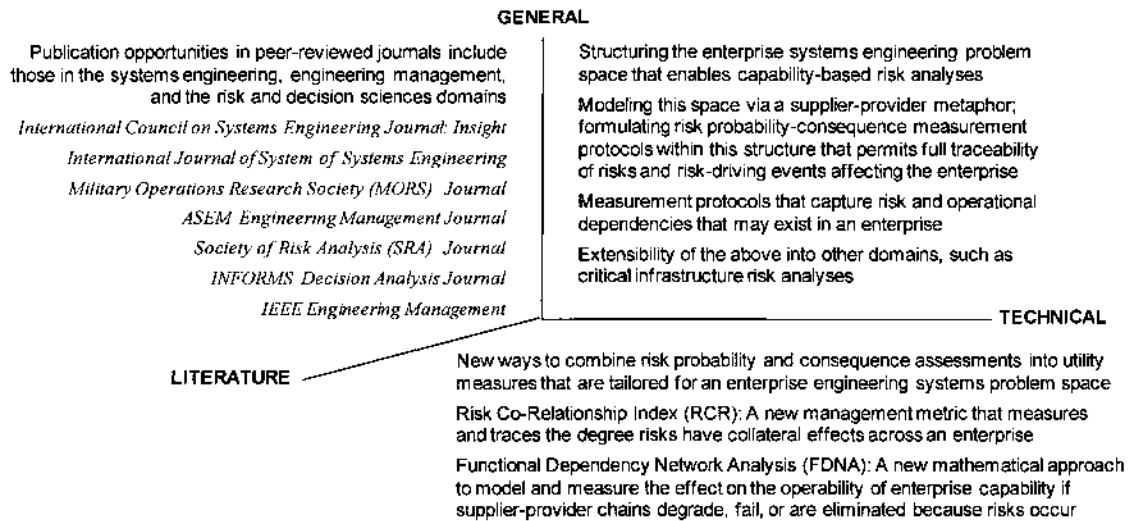


Figure 11. Dissertation Research Contributions

### Dissertation Organization

Figure 12 shows the dissertation's organization by problem areas and chapter.

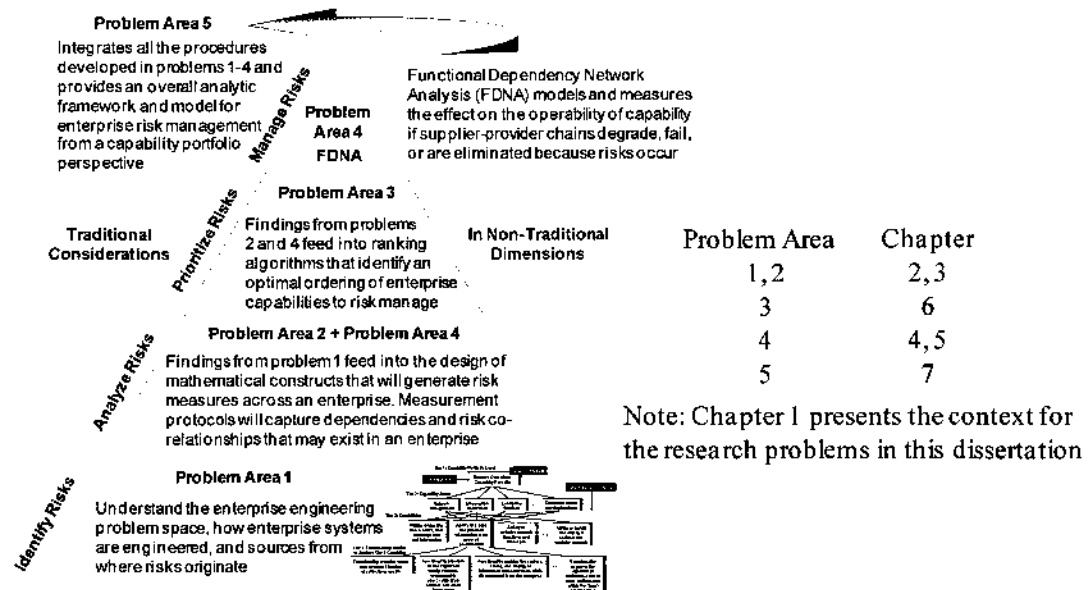


Figure 12. Dissertation Organization

## **CHAPTER II**

### **ENGINEERING ENTERPRISE SYSTEMS**

#### **INTRODUCTION**

The section introduces enterprise systems, how their engineering is planned, and the environments within which they operate. This provides context for discussions about risk in engineering enterprise systems and how risk management theory and practice apply.

Enterprise systems engineering (ESE) is an emerging discipline. It encompasses and extends traditional systems engineering (TSE) to create and evolve webs of systems that deliver capabilities via services, data, and applications through a rich network of information and communications technologies. Enterprise environments (such as the internet) offer users ubiquitous, cross-boundary, access to a wide-variety of services, applications, and information repositories.

Today, we're in the early stage of understanding how systems engineering, engineering management, and social science weave together to create systems that live and evolve in enterprise environments. This section discusses some of these understandings, specifically as they pertain to risk management. The analytical practices discussed will themselves evolve as the community gains experience and knowledge about engineering in the enterprise problem space.

Engineering today's systems is a sophisticated, complex, and resource intensive undertaking. Increasingly, systems are being engineered by bringing together many separate systems which, as a whole, provide an overall capability otherwise not possible. Many systems no longer physically exist within clearly defined boundaries; rather, systems are more and more geographically and spatially distributed and interconnected through a rich and sophisticated set of networks and communications technologies.

These large-scale enterprise systems operate to satisfy large, and dynamically changing, user populations, stakeholders, and communities of interest. It is no longer enough to find just technology solutions to the engineering of these systems. Solutions must be adaptable to change in the enterprise, balanced with respect to expected capability outcomes and performance, while also considering the social, political, and economic constraints within which they'll operate and change over time.

In an enterprise context, risk management is envisioned as an integration of people, processes, and tools that together ensure the early identification and resolution of risks. The goal is to provide decision-makers an enterprise-wide understanding of risks, their potential consequences, interdependencies, and rippling effects within and beyond enterprise boundaries. Ultimately, risk management aims to establish and maintain a holistic view of risks across the enterprise, so capabilities and performance objectives are achieved via risk-informed resource and investment decisions.

## THE ENTERPRISE ENGINEERING PROBLEM SPACE

As mentioned earlier, today's systems are continually increasing in scale and complexity. Today, more and more defense systems, transportation systems, financial systems, and human services systems network ubiquitously across boundaries and seamlessly interface with users, information repositories, applications, and services. These systems can be considered, in one sense, an enterprise of people, processes, technologies, and organizations.

A distinguishing feature of enterprise systems is not only their technologies but the way users interface with them and each other. New challenges are present in how to design and engineer these systems, and their interfaces, from human, social, political, and managerial dimensions [Allen, Nightingale, Murman, 2004]. To address these challenges the engineering and social sciences are joining together in ways not previously seen, when planning and evolving the design, development, and operation of these large-scale and highly networked systems.

This section discusses the enterprise problem space and systems thinking within that space. The materials that follow derive from a perspectives paper on enterprise engineering, written by George Rebovich, Jr. of The MITRE Corporation\*.

### The Enterprise [Rebovich, 2005]

In a broad context, an enterprise is an entity comprised of interdependent resources that interact with each other and their environment to achieve goals. A way to view an enterprise is illustrated in Figure 13.

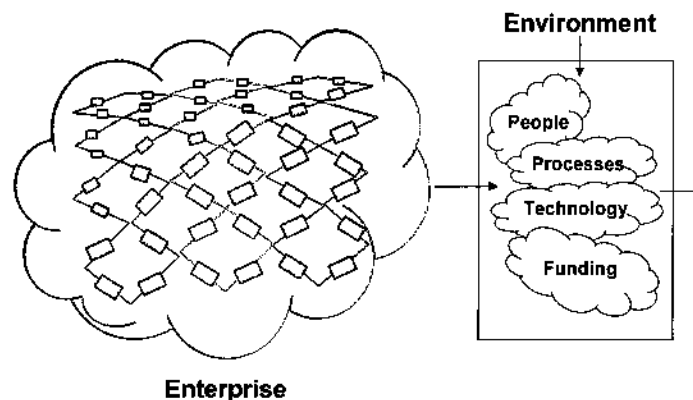


Figure 13. An Enterprise and its Environment

Here, resources include people, processes, organizations, technologies, and funding. Interactions include coordinating functions or operations, exchanging data or information, accessing applications or services.

Historically, systems engineering has focused on the technologies which have enabled the development of the piece parts – the systems and subsystems embedded in the enterprise. Modern

\* Permission has been granted to excerpt materials from the paper "Enterprise Systems Engineering Theory and Practice, Volume 2: Systems Thinking for the Enterprise: New and Emerging Perspectives", authored by Rebovich, George, Jr., MP 050000043, November 2005. © 2005 The MITRE Corporation, All Rights Reserved.

systems thinkers [Gharajedaghi, 1999] are increasingly taking a holistic view of an enterprise. Here, an enterprise can be characterized by the following:

- A multi-minded, socio-cultural entity, comprised of a voluntary association of members who can choose their goals and means,
- An entity whose members share values embedded in a (largely common) culture,
- Having the attributes of a purposeful entity, and
- An entity whose performance improves through alignment of purposes across its multiple levels.

There is a nested nature to many enterprises. At every level, except at the very top and bottom, an enterprise itself is part of a larger enterprise and contains sub-enterprises, each with its own people, processes, technologies, funding and other resources. Nesting within an enterprise can be illustrated by a set of US Air Force programs shown in Figure 14. Here, the family of Airborne Early Warning and Control (AEW&C) systems is an enterprise which is nested in the Command and Control (C2) Constellation enterprise which is nested in the Air Force C2 enterprise.

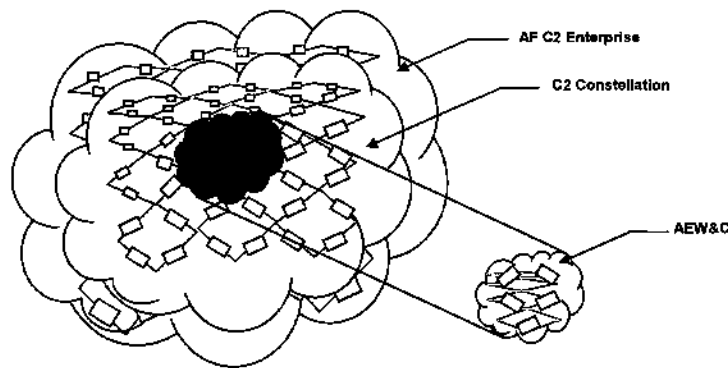


Figure 14. Nested Nature of Enterprises

Alignment of purposes across the levels of the enterprise can improve overall enterprise performance. The sub-enterprises contribute to the outcomes or goals of the containing enterprise. This view has profound implications for how systems engineers must think about their activities – that they are inexorably linked to the enterprise and its operations as a whole.

For example, at the AEW&C system program level, the view must be that an AEW&C system builds an air picture that serves the higher goal of achieving situation awareness within the C2 Constellation. This requires the AEW&C systems engineer to ask (and answer) how the AEW&C piece parts being developed serve situation awareness in the C2 Constellation in addition to how they serve the AEW&C system specification.



At the next level, the view must be that the C2 Constellation develops integrated capabilities to serve the higher goal of providing net-centric C2 for the Air Force C2 Enterprise. The implication is that the systems engineer must address how the C2 Constellation piece parts serve the Air Force C2 Enterprise, in addition to how they serve the C2 Constellation.

At the highest level in this example the view must be that the Air Force C2 Enterprise develops Air Force net-centric capabilities to serve the higher goal of providing net-centric C2 for the Joint/Coalition C2 Enterprise. The implication is that the systems engineer must address how the Air Force C2 Enterprise piece parts serve joint and coalition net-centric C2 in addition to how they serve the Air Force C2.

This discussion leads to an operational definition of enterprise viewed from the perspective of an individual (system engineer or other participant) or team in the enterprise. It aims to answer the question, “what is my (our) enterprise?” The enterprise, then, can be viewed as a set of interdependent elements (systems and resources) that a participating actor or actors either control or influence.

This definition of enterprise is a virtual construct that depends on the make-up, authority, and roles of the participating actors in a community of interest. For example, the program team of a system managed by one organization may have virtual control of most engineering decisions being made on the system’s day-to-day development activities. If the system is required to be compliant with technical standards developed by an external agency, the program team may have representation on the standards team but that representation is one voice of many and so the standard is a program element or variable the program team can influence but not control.

The implication is that all actors or teams in an enterprise setting should know their enterprise and be aware of which enterprise elements or variables they control, which they influence, and which they neither control nor influence. In general, environmental elements or factors cannot be controlled or influenced. But the individual or project team may very well need to be aware of and understand the implications of such environmental factors.

In an enterprise context, risk management is an integration of people, processes, and tools that ensure the early and continuous identification and resolution of risks that threaten enterprise capabilities or user-accessed services. The goal is to provide decision-makers an enterprise-wide understanding of capability risks\*, their potential consequences, interdependencies, and rippling effects within and beyond enterprise boundaries. Ultimately, risk management aims to establish and maintain a holistic view of risks across the enterprise, so capabilities and performance objectives are achieved via risk-informed resource and investment decisions.

---

\* Societal consequences of risks realized from engineering systems (e.g., nuclear, transportation, financial systems) have been studied and published by Murphy and Gardoni [Murphy, Gardoni, 2006]. Their work relates notions of capability risks to their potential impacts on the capacity of socio-political structures to operate and on the ability of individuals to function within their respective social-political environments.

## CAPABILITY PORTFOLIO PERSPECTIVES

What events threaten the delivery of capabilities needed to successfully advance enterprise goals and mission outcomes? If these events occur, how serious are their impacts? How can the progress of management plans, aimed at minimizing their impacts, be monitored? How can risk be considered in resource planning and investment decision-making?

Questions such as these arise when planning, executing, and managing the engineering of large-scale, enterprise-wide, systems. Addressing these questions involves not only engineering and technology dimensions but human-social-system interactions as well.

Enterprise risk management differs from traditional systems engineering risk management in the expanse of the consequence space within which risks affect enterprise goals, mission outcomes, or capabilities. In a traditional system, the consequence space is usually focused on the extent risks negatively affect the system's cost, schedule, and technical performance. Enterprise risk management necessitates broadening the scope of this space. Identifying and evaluating higher-level effects (or consequences) are critical considerations in decisions on where to allocate resources to manage enterprise risks.

### A Capability Portfolio View

One way management plans for engineering an enterprise is to create capability portfolios of technology programs and initiatives that, when synchronized, will deliver time-phased capabilities that advance enterprise goals and mission outcomes. Thus, a capability *portfolio* is a *time dynamic organizing construct* to deliver capabilities across specified epochs.

Creating capability portfolios is a complex management and engineering analysis activity. In the systems engineering community, there is a large body of literature on *portfolio analysis and investment decision management* applied to the acquisition of today's advanced systems. This topic, however, is outside the scope of this dissertation. Instead, the following is focused on applying risk management practices within a generic model of capability portfolios, already defined to deliver capabilities to an enterprise. Figure 15 presents a view of such a model.

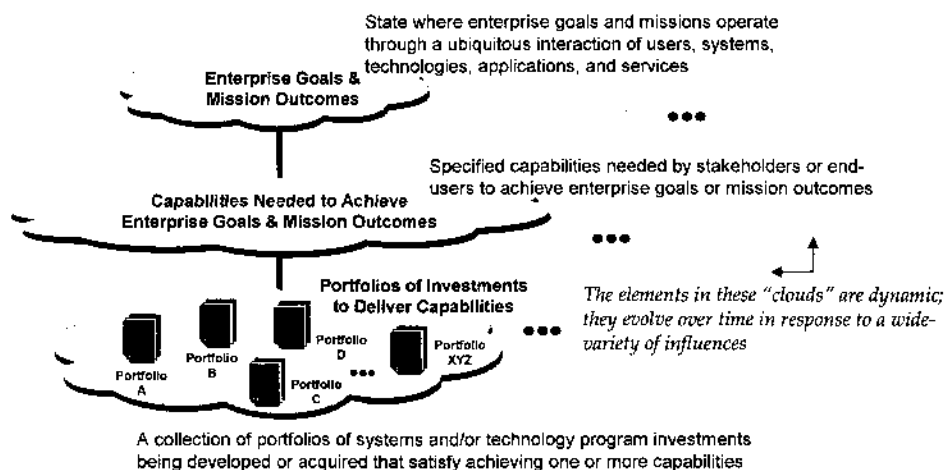


Figure 15. An Enterprise and its Capability Portfolios

In Figure 15, the lowest-level is the family of capability portfolios. What does a capability portfolio look like?

An example is shown in Figure 16. Presented is an inside-look at a capability portfolio from a capability-to-functionality view. Figure 16 derives from a capability portfolio for network operations [OSD, 2005]. This is one among many capability portfolios designed to deliver capabilities to the Department of Defense (DOD) Global Information Grid [Government Accountability Office (GAO), 2004].

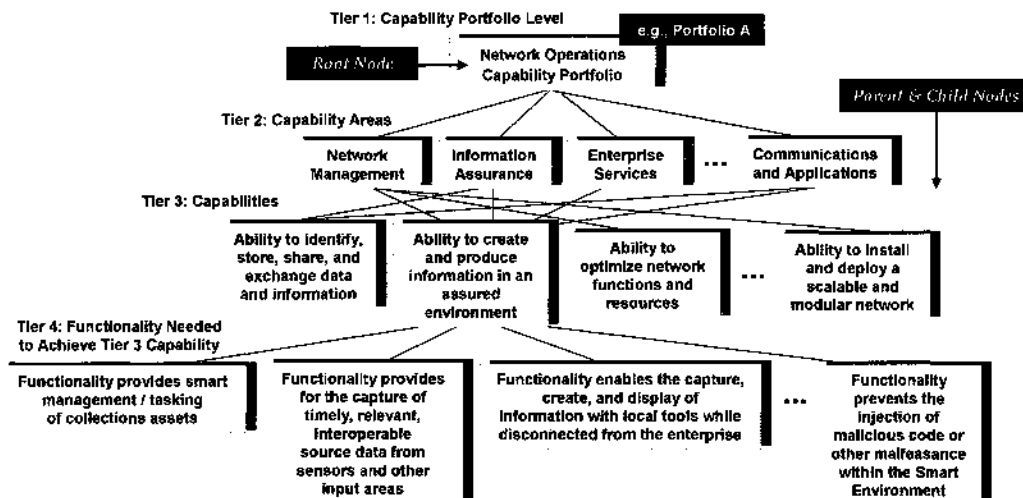


Figure 16. A Capability Portfolio for Network Operations [OSD, 2005]  
(e.g., Capabilities Delivered by 20xx)

Given this, a capability portfolio can be represented in a hierarchical structure. At the top is the capability portfolio itself. Consider this the Tier 1 level. The next tier down the hierarchy presents capability areas, such as Network Management, Information Assurance, and so forth.

These Tier 2 elements depict the functional domains which characterize the capability portfolio. Tier 3 is the collection of capabilities the portfolio must deliver by a specified epoch (e.g., 20xx). Here, a capability can be defined as *the ability to achieve an effect to a standard under specified conditions using multiple combinations of means and ways to perform a set of tasks* [OSD, 2005]. Tier 4 is the functionality that must integrate together to achieve capability outcomes.

For example, consider the capability portfolio in Figure 16. The Tier 3 capability *Ability to create and produce information in an assured environment* refers to the ability to collect data and transform it into information, while also providing end-to-end protection to assure the availability of information and validating its integrity [OSD, 2005].

Suppose this capability advances toward outcome goals when functionality is delivered that ensure the *Capture of timely, relevant, interoperable source data from sensors and other input areas*. Suppose this functionality contributes to this capability's outcome when the *Time for information change to be posted and/or subscribers notified* "< 1 minute" [OSD, 2005].

Later, we will use this information and show how a hierarchical representation of a capability portfolio can be used as a modeling framework within which risks can be assessed and capability portfolio risk measures derived. In preparation for this, we first consider a capability portfolio from a supplier-provider context.

### Supplier-Provider Concept

Once a capability portfolio's hierarchy and its elements are defined it is managed by a team to ensure its collection of technology programs and technology initiatives combine in ways to deliver one or more capabilities to the enterprise. Thus, one can take a supplier-provider view of a capability portfolio. This is illustrated in Figure 17.

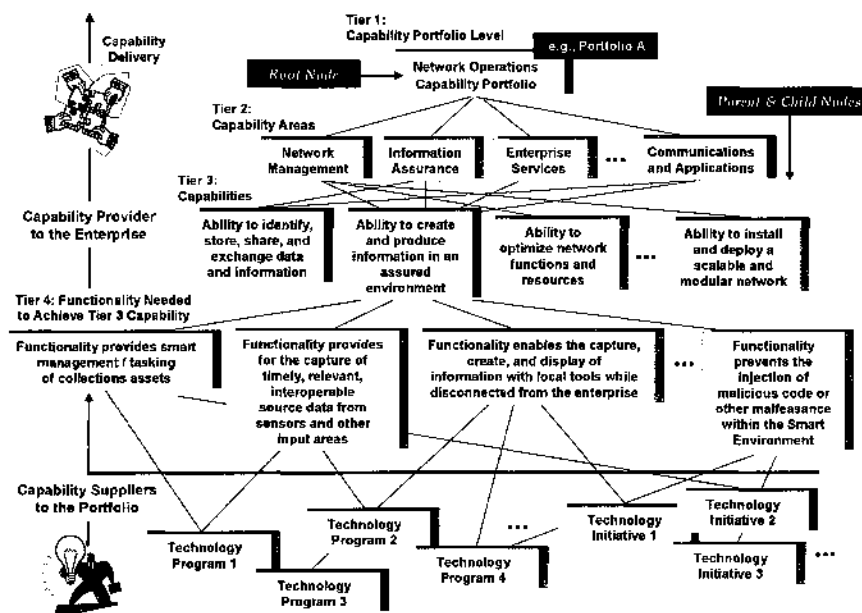


Figure 17. A Supplier-Provider View  
(e.g., Capabilities Delivered by 20xx)

Here, a capability portfolio can be viewed as the provider charged with delivering time-phased capabilities to the enterprise. Technology programs and technology initiatives aligned to, and synchronized with, the capability portfolio supply the functionality needed to achieve the provider's capability outcomes.

The supplier-provider view offers a way to examine a capability portfolio from a risk-perspective. Look again at Figures 15, 16, and 17. We have enterprise goals and mission outcomes dependent on capability portfolios successfully delivering required capabilities. Next, we have capability portfolios dependent on programs and technologies successfully delivering functionality that enables these capabilities. Thus, major sources of risk originate from the suppliers to these capability portfolios.

Supplier risks include unrealistic schedule demands placed on them by portfolio needs or placed by suppliers on their vendors. Supplier risks include premature use of technologies, including the deployment of technologies not adequately tested.

Dependencies amongst suppliers can generate a host of risks, especially when a problem with one supplier generates a series of problems with others. Economic conditions can always threaten business stability or the business viability of suppliers and vendors. Unfavorable funding or political influences outside an enterprise can adversely affect its capability portfolios, its suppliers, or the supplier-vendor chains in ways that threaten the realization of enterprise goals and mission outcomes.

These issues are important risk considerations to any engineering system. However, they are a more present and persistent concern in the management of risk in engineering enterprise systems, especially those acquired by supplier-provider models.

The research in this dissertation will use these views or structures and show how a hierarchical representation of a capability portfolio can serve as a modeling or analytical framework within which risks can be assessed and capability portfolio risk measures derived.

The following presents an analytical framework within which to structure capability portfolio risk assessments. This framework can be extended to a generalized logical-model – one where capability portfolio risk assessments combine to measure and trace their integrative effects on engineering an enterprise system.

## CHAPTER III

### A RISK ANALYTIC FRAMEWORK

#### INTRODUCTION

This chapter describes the structure of the risk management problem space as it relates to engineering enterprise systems from a capability portfolio perspective. It presents a solution approach to Problem Areas 1 and 2, as defined in Chapter I.

This aspect of the dissertation's research is at the interface between risk analytic approaches for engineering traditional systems with those needed for engineering enterprise systems. Addressing this area is a necessary first step.

Shown in this chapter, the enterprise problem space is represented by a supplier-provider metaphor in the form of a mathematical graph. This graph is a topology of nodes that depict supplier-provider-capability relationships unique to a capability portfolio.

Within this topology, mathematical rules are designed that operate on these relationships to generate measures of capability risk. A definition of capability risk is provided that considers the occurrence probabilities and consequences of risks that threaten capability. In this context, consequence is evaluated according to a capability's *ability to achieve its outcome objectives* for the portfolio and ultimately for the enterprise.

#### A FRAMEWORK FOR REPRESENTING CAPABILITY RISK

When a capability portfolio can be represented in a hierarchical structure it offers a modeling framework within which risks can be assessed and capability risk measures derived. Examples are shown by the hierarchies in Figure 16 and Figure 17. What is meant by capability risk? In the context of a capability portfolio, we define *capability risk as a measure of the chance and the consequence that a planned capability, defined within a portfolio's envelope, will not meet intended outcomes by its scheduled delivery date.*

First, we'll design algebraic rules for computing risk measures within a segment of a capability portfolio's hierarchy. Then, we will show how to extend these computations to operate across a capability portfolio's fully specified hierarchy. This will involve a series of roll-up calculations. Shown will be risk measure (risk score) computations that originate from leaf nodes, which will then roll-up to measure the risks of parent nodes, which will then roll-up to measure the risk of the capability portfolio itself (i.e., the root node level).

When a capability portfolio can be represented in the form of a hierarchy, decision-makers are provided the trace basis and the event drivers behind all risk measures derived for any node at any level in the hierarchy. From this, management has visibility and supporting rationales for identifying where resources are best allocated to reduce (or eliminate) risk events that threaten the success of the capability portfolio's goals and capability outcome objectives.

## AN ALGEBRA FOR COMPUTING CAPABILITY RISK

In a capability portfolio's hierarchical structure, each element in the hierarchy is referred to as a node. The top-most node is the *root node*. In Figure 16 or Figure 17 the root node represents the capability portfolio itself, which, in this case, is the Network Operations Capability Portfolio. A *parent node* is one with lower-level nodes coming from it. These lower-level nodes are called *child nodes* to that parent node. Nodes that terminate in the structure are called *leaf nodes*. Leaf nodes are terminal nodes in that they have no children coming from them.

In the context of a hierarchy, leaf nodes are terminal nodes that originate from supplier nodes. Here, leaf nodes are risk events associated with supplier nodes. Thus, the risk measures (risk scores) of leaf nodes drive the risk measures of supplier nodes. The risk measures (risk scores) of supplier nodes drive the risk measures of their parent nodes. The risk measures (risk scores) of parent nodes drive the risk measures of their parent nodes, and so forth. Hence, risk measures (risk scores) computed for all nodes originate from risk measures derived for leaf nodes. This *ripple-in-the-pond* effect is reflective of capability portfolio risk management when taking a supplier-provider view.

Risks that trace to suppliers are a major source of risk to the portfolio's ability to deliver capability to the enterprise. However, it is important to recognize that suppliers are not the only source of risk. Risks external to a capability portfolio's supplier-provider envelope are very real concerns. Risk sources outside this envelope must also be considered when designing and implementing a formal risk management program for a capability portfolio or family of capability portfolios.

Figure 18 shows a Tier 3 capability from the portfolio in Figure 17. For convenience we've numbered the nodes as shown. Figure 18 shows three supplier nodes responsible for contributing to Functionality 3.22 – one of four functions needed for Capability 3.2 to be delivered as planned. Functionality node 3.22 is a parent node to the supplier nodes EWXT, QSAT, and S-RAD.

Two of these supplier nodes are technology programs. One supplier node is a technology initiative. In practice, this distinction can be important. A technology program is often an engineering system acquisition – one characterized by formal contracting, well-defined requirements, and adherence to engineering standards and program management protocols. A technology initiative is often targeted at developing a specific technology for an engineering system or for an appropriate user community. An example might be the development of advanced encryption technology for the information assurance community.

Whether supplier nodes are technology programs or technology initiatives, they exist in a capability portfolio because of their contributions to parent nodes. Seen from the portfolio perspectives in Figure 17 and Figure 18, functionality nodes are the parent nodes to these supplier nodes. Here, supplier node contributions integrate in ways that enable functionality nodes. Functionality nodes integrate in ways that enable their corresponding capability nodes – capabilities the portfolio is expected to successfully deliver to the enterprise.

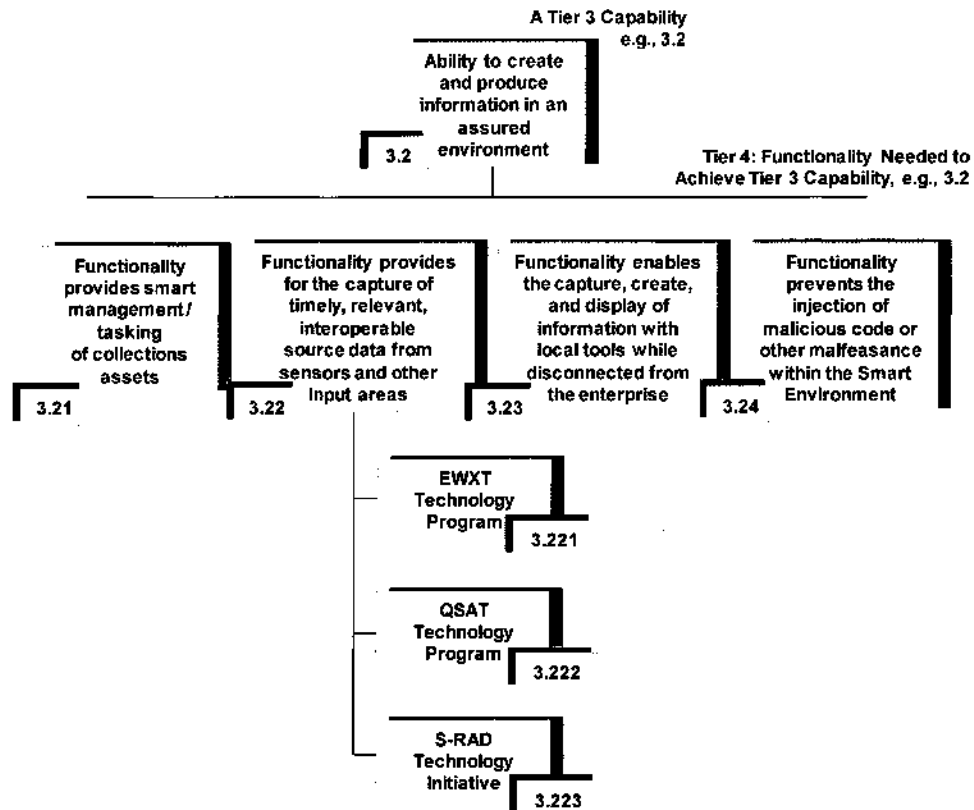


Figure 18. A Tier 3 Capability From the Portfolio in Figure 17

At the supplier-level, we define *contribution* by a supplier node as *that which advances the capability portfolio's ability to provide capability that meets the needs of the portfolio's consumers*. A supplier's contribution to its parent node (e.g., a functionality node) could be in many forms and include technologies, engineering analyses, or software applications.

At the supplier-level, risk events can have adverse consequences on the cost, schedule, or technical performance of the supplier's contribution(s) to its parent node, such as a functionality node in Figure 18. Risk events can also negatively affect a supplier's programmatic efforts.

Programmatic efforts refer to technical or program-related work products as they support the supplier's business, engineering, management, or acquisition practices needed to advance the outcome objectives of the supplier's contribution to its parent node (e.g., a functionality node). Technical or program-related work products include architecture frameworks, engineering analyses, organizational structures, governance models, and engineering, program, and acquisition management plans.

In addition, supplier nodes can be negatively affected by political risks, budgetary risks, business, economic risks, or supplier/vendor viability. These risks not only threaten suppliers but they can *directly* threaten functionality or capability nodes at those levels in the capability portfolio's hierarchy. Thus, risk events from a capability portfolio perspective are of multiple types with the potential for multi-consequential impacts on parent nodes located at any level in the hierarchy.



Figure 19 shows leaf nodes intended to represent supplier node risk events. These leaf nodes are labeled R1, R2, R3, etc. These nodes denote risk events that, if they occur, would negatively affect the supplier node's contribution to its parent node (Functionality 3.22, in this case).

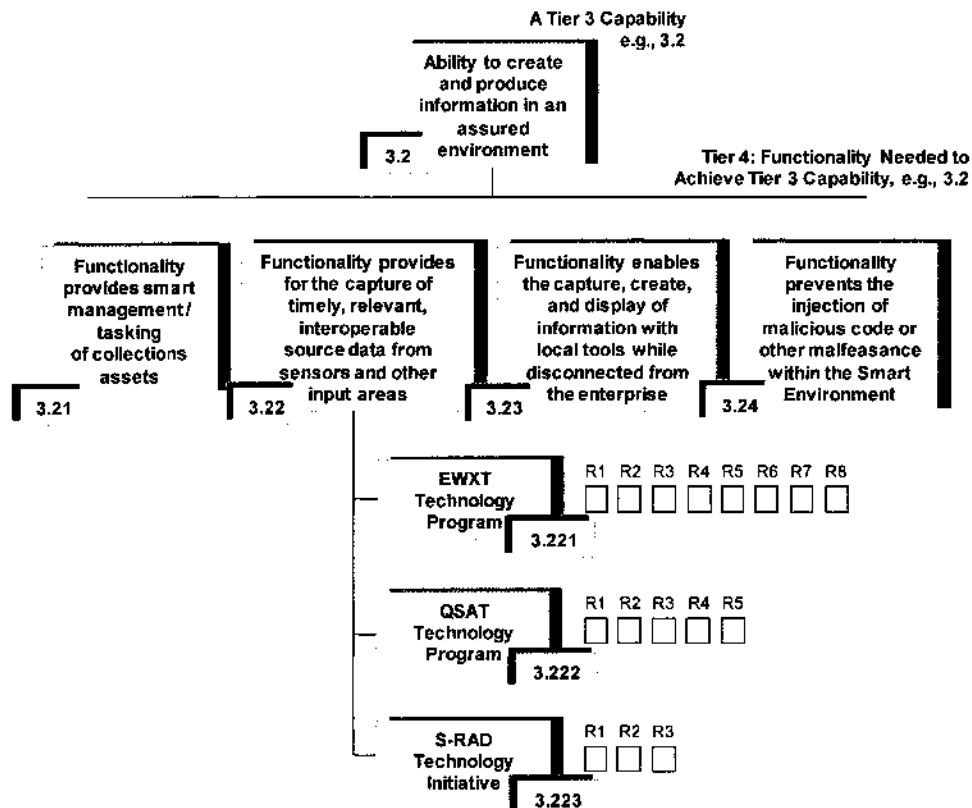


Figure 19. Capability 3.2 Supplier Risk Set

Risks that threaten supplier node contributions to Functionality 3.22 have “*ripple-in-the-pond*” effects on the portfolio’s delivery expectations for Capability 3.2. As we’ll see, risks that affect Capability 3.2 can have horizontal and vertical effects elsewhere in the portfolio.

Next, we’ll look at the EWXT Technology Program. Suppose eight risks have been identified – R1, R2,..., R8. From a capability portfolio perspective, these are *only* the risk events originating from the EWXT Program that, if they occur, have negative consequences on the EWXT Program’s contribution to Functionality 3.22. In this sense, they may not be all the risk events on the EWXT Program.

In Figure 20, each EWXT risk event is given a color. The color reflects a measure of the risk event’s severity. In Figure 20, each risk event happens to be either Red (R) or Yellow (Y). Suppose the basis for each color derives from a function of each risk event’s occurrence probability and its impact or consequence.

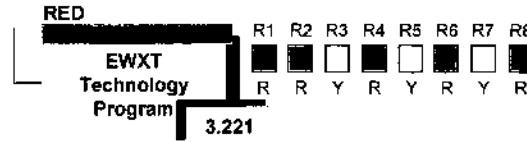


Figure 20. EWXT Technology Program Risk Set (R = Red, Y = Yellow)

Suppose this function is given by Equation 3.1, where the risk measure (or risk score) of risk event  $R_i$  ( $i = 1, 2, 3, \dots, n$ ) is defined by

$$0 \leq \text{Risk Score}(R_i) = RS_{R_i} = u_1 \text{Prob}(R_i) + u_2 V_{\text{Impact}}(R_i) \leq 100 \quad (3.1)$$

In Equation 3.1, the first term is an assessment of the risk event's occurrence probability. The second term is an assessment of its impact severity, assuming the risk occurs, on the contribution the EWXT Program (a supplier node) is making to Functionality 3.22 (its parent node). The coefficients  $u_1$  and  $u_2$  are non-negative weights that sum to one.

In Equation 3.1, both terms can be represented as value functions. For example, values for the first term in Equation 3.1 can derive from a value function for a risk event's occurrence probability. Suppose a linear relationship is assumed, as shown in Figure 21. Non-linear relationships are also possible.

Table 1 offers a value function for the second term in Equation 3.1. This is shown in the form of a table known as a constructed scale.

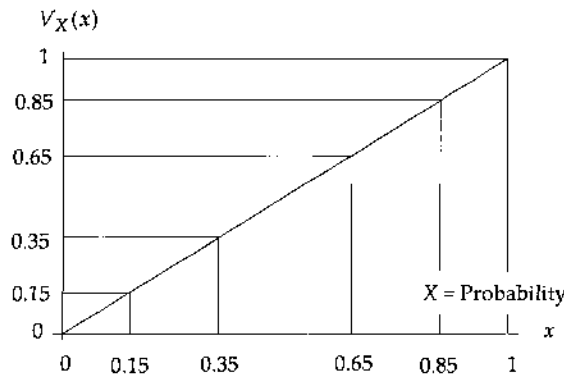


Figure 21. A Value Function for Occurrence Probability

Next, we will discuss ways to combine these measures into an overall measure of risk for a supplier node. Then, we will discuss ways to combine supplier node risk measures into an overall measure of risk for its parent node (e.g., Functionality 3.22). For this, we introduce the idea of criticality – that is, considering the criticality of a supplier node's contribution to its parent node when measuring that parent node's risk.

**Definition/Context: Risk Event Impacts on a  
Supplier Node's Contribution to its Parent Node**

*Ref: Meister, David (1985). Behavioral Analysis and Measurement Methods, John Wiley & Sons, New York, New York, ISBN 0471896403.*

**Context:** This table is used to assess the consequences or impacts of risks to a supplier node's contribution to its parent node.

**Scale Type:** In decision analysis, this table is known as a *constructed scale*. Constructed scales are frequently created when natural measurement scales either do not exist or cannot be commonly defined for the problem at hand. With this scale resides an accompanying value function/measure applied later in the analysis.

**Scale Definitions:** The linguistic definitions shown for each scale level derives, in part, from measurement research by D. Meister (see above reference). Meister derived sets of linguistic phrases, commonly used to indicate an entity's measure of value or goodness, in a manner that reflects an "ordered-metric". Ordered-metric in this context means these phrases are at least one standard deviation apart and have parallel wording or that intervals (levels) between these phrases are as nearly equal as possible.

**Basis of Assessment (BOA):** All rating assessments **shall** be accompanied by a written Basis of Assessment (BOA) that justifies the reasons for the chosen selections. The BOA must be written such that it (1) clearly and concisely justifies the team's rationale and (2) enables this justification to be objectively reviewed by "peers".

**Quantified Consequences:** If metrics have been developed or are available that provide context for a risk event's impact(s), then these measures **shall** be reported (and included) in the justification narratives (the BOA) that support the basis for the selection of a specific rating level.

Below, the phrase *The nature of the risk is..* is intended to allow for cost, schedule, technical performance, or programmatic risks. It is also intended to allow for risks that fall outside these traditional categories to be included. This includes political risks, budgetary risks, funding risks, economic risks, or business/vendor viability risks, etc.

This table provides a *constructed scale* from which an accompanying value function can be developed. Value functions can also be developed for each type of risk according to its nature; that is, whether it is a cost or schedule risk, a political risk, an economic risk, etc.

Doing this depends on the level of analytic detail desired by the analysis team. *At a minimum, it is recommended that each risk be tagged by its nature so that tracking risk by its type can be done as part of the analysis.*

**Table 1. A Sample Constructed Scale: Supplier Node Impacts**

| Ordinal Scale/ Level (Score) | Definition/Context:<br>Risk Event Impacts on a Supplier Node's Contribution to its Parent Node   | Cardinal Interval Scale/Level (Score) |
|------------------------------|--|---------------------------------------|
| 5                            | A risk event that, if it occurs, impacts the supplier node to the extent that its contribution to its parent node is severely degraded or compromised. The nature of the risk is such that outcome objectives for the supplier node's contribution are either not met or are <b><i>extremely unacceptable</i></b> (e.g., fall well-below minimum acceptable levels). | e.g.,<br>80 to 100                    |
| 4                            | A risk event that, if it occurs, impacts the supplier node to the extent that its contribution to its parent node is marginally below minimum acceptable levels. The nature of the risk is such that outcome objectives for the supplier node's contribution are <b><i>moderately unacceptable</i></b> .   | e.g.,<br>60 to < 80                   |
| 3                            | A risk event that, if it occurs, impacts the supplier node to the extent that its contribution to its parent node falls well-below stated objectives but remains enough above minimum acceptable levels. The nature of the risk is such that outcome objectives for the supplier node's contribution are <b><i>borderline acceptable</i></b> .                       | e.g.,<br>40 to < 60                   |
| 2                            | A risk event that, if it occurs, impacts the supplier node to the extent that its contribution to its parent node falls below stated objectives but falls well-above minimum acceptable levels. The nature of the risk is such that outcome objectives for the supplier node's contribution are <b><i>reasonably acceptable</i></b> .                                | e.g.,<br>20 to < 40                   |
| 1                            | A risk event that, if it occurs, impacts the supplier node to the extent that its contribution to its parent node is negligibly affected. The nature of the risk is such that outcome objectives for the supplier node's contribution are <b><i>completely acceptable</i></b> , but regular monitoring for change is recommended.                                    | e.g.,<br>0 to < 20                    |

Table 1. A Sample Constructed Scale: Supplier Node Impacts (Concluded)

Returning to Figure 20, Equation 3.1 will produce a risk score for each identified risk event  $R_i$ . For convenience, suppose each EWXT risk event's risk score *was already computed* (e.g., by Equation 3.1) and is given in Figure 22.

In Figure 22, risk event R1 has a risk score of 85; risk event R2 has a risk score of 90; risk event R3 has a risk score of 60 and so forth. Given these eight risk scores for the EWXT Technology Program, what is an overall measure of the risk EWXT poses to Functionality 3.22? The following is one way to formulate this measure.

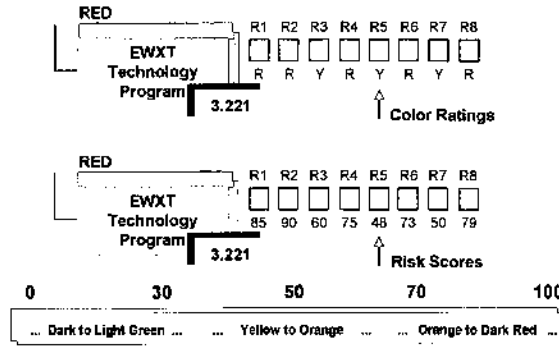


Figure 22. Example Risk Scores for EWXT Program Risks  
(R = Red, Y = Yellow)

### Maximum “Max” Average

Here, we introduce a new measure called the “max” average\*. The max average is an algorithm that can be used to measure and rank-order risks in a set of identified risk events. The max average is defined as follows:

**Definition 3.1:** The max average of  $\{x_1, x_2, x_3, \dots, x_n\}$  where  $0 \leq x_i \leq 100$ ,  $i = 1, 2, 3, \dots, n$ , is

$$Max Ave = \lambda m + (1 - \lambda) Average\{x_1, x_2, x_3, \dots, x_n\} \quad (3.2)$$

where  $m = Max\{x_1, x_2, x_3, \dots, x_n\}$  and  $\lambda$  is a weighting function.

Suppose the capability portfolio’s management decided to use the weighting function in Figure 23. Now, in the context of this discussion the  $x_i$ ’s in Equation 3.2 equate to the  $R_i$ ’s (the risk scores) in Figure 22. Thus, from Equation 3.2 we have

$$Risk Score(EWXT) = RS_{3.221} = \lambda(90) + (1 - \lambda)Average\{85, 90, 60, 75, 48, 73, 50, 79\}$$

where  $m = Max\{85, 90, 60, 75, 48, 73, 50, 79\} = 90$ . It follows (from Figure 23) that  $\lambda = 0.70$ . From this, we have

$$Risk Score(EWXT) = RS_{3.221} = (0.70)(90) + (0.30)(70) = 84$$

Thus, the EWXT Technology Program (a supplier node) has a high risk score. According to the scale convention in Figure 22, EWXT falls in the “RED R” color band.

In summary, the EWXT Technology Program is contributing a high degree of risk towards Functionality 3.22, which threatens Capability 3.2. Furthermore, it can be shown that R1, R2, R4, R6, and R8 are responsible for 93 percent of the EWXT Program’s risk score.

\* The max average was created by Dr. Bruce W. Lamar (MITRE, 2005) and published by The MITRE Corporation in the paper *Min-Additive Utility Functions*, MP080070-1, April 2008, ©2008, All Rights Reserved.

These five risk-driving events signal areas in the EWXT Program where increased management focus and risk mitigation planning may be warranted. Figure 24 offers a summary view of the EWXT Program risks.

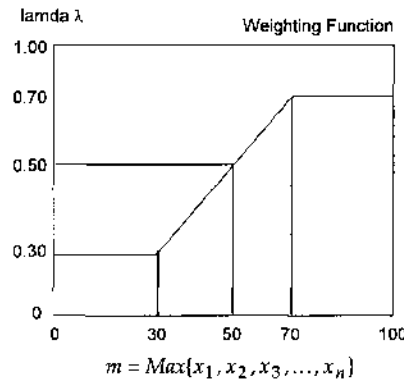


Figure 23. An Example Max Average Weighting Function\*

In summary, the EWXT Technology Program is contributing a high degree of risk towards Functionality 3.22, which threatens Capability 3.2. Furthermore, it can be shown that R1, R2, R4, R6, and R8 are responsible for 93 percent of the EWXT Program's risk score. These five risk-driving events signal areas in the EWXT Program where increased management focus and risk mitigation planning may be warranted. Figure 24 offers a summary view of the EWXT Program risks.

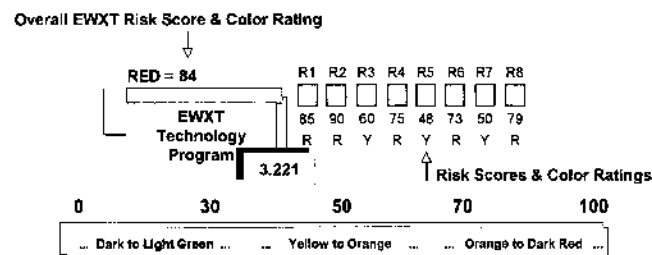


Figure 24. Overall EWXT Program Risk Score & Color Rating  
(Max Ave, R = Red, Y = Yellow)

### Measuring “Up”: How Supplier Risks Affect Functionality

The preceding discussion presented one way to derive a risk measure (i.e., the risk score) of the EWXT Program, as a function of its eight identified risk events. However, EWXT is just one of three supplier nodes to Functionality 3.22. What about the other supplier nodes? How might their risk measures combine into an overall measure of risk to Functionality 3.22? What ripple effects do supplier risks have on all dependent higher level nodes in the capability portfolio's hierarchy? The following will address these and related questions.

\* The shape of the weighting function can have a significant influence on scores generated by the max average rule. In practice, its shape should be designed to model the team's (or decision-maker's) preferences for how much the maximum score should influence the overall score.

Suppose risk measures for the other two supplier nodes to Functionality 3.22 are shown in Figure 25. These are the QSAT Program and the S-RAD Technology Initiative. Suppose their risk measures were also derived by the max average rule given by Equation 3.2. From this, how can we combine the risk measures from all three supplier nodes, in Figure 25, into an overall measure of risk to Functionality 3.22?

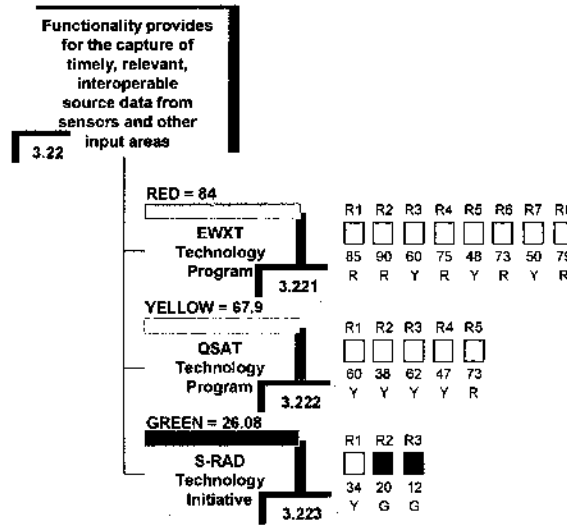


Figure 25. Supplier Node Risk Measures to Functionality 3.22

### Critical Average

Here, we introduce a new measure called the *critical average*. The critical average is a variation of the max average. It can be applied to a set of supplier node risk scores. The critical average is defined as follows:

**Definition 3.2:** Suppose a parent node has  $n$  child nodes and  $\{x_1, x_2, x_3, \dots, x_n\}$  is the set of scores of these child nodes. If  $A$  is a subset of  $\{x_1, x_2, x_3, \dots, x_n\}$  that contains *only* the scores of the child nodes deemed critical\* to the parent node, then the critical average of  $\{x_1, x_2, x_3, \dots, x_n\}$  is defined as follows:

$$Crit Ave = \lambda Max\{A\} + (1 - \lambda) Average\{x_1, x_2, x_3, \dots, x_n\} \quad (3.3)$$

where  $0 \leq x_i \leq 100$  for all  $i = 1, 2, 3, \dots, n$  and  $\lambda$  is a weighting function, such as the weighting function in Figure 23.

Next, we'll apply the critical average to the nodes in Figure 25 as the rule to measure the risk to Functionality 3.22. Suppose the EWXT Program is deemed the *only* critical supplier to Functionality 3.22; thus,  $A = \{RS_{3.221}\}$  in this case. From this, it follows that

\* A child node's contribution to its parent node is critical if, without the contribution, the parent node's outcome objectives are not achieved or are unacceptably degraded.

$Risk\ Score(Functionality\ Node_{3.22}) = RS_{3.22}$

$$= \lambda \text{Max}\{A\} + (1 - \lambda) \text{Average}\{RS_{3.221}, RS_{3.222}, RS_{3.223}\} \quad (3.4)$$

where  $\lambda$  is a weighting function. For convenience, use the weighting function in Figure 23. Then, from the risk scores in Figure 25 and Equation 3.4 we have

$$RS_{3.22} = (0.70)(84) + (1 - 0.70) \text{Average}\{84, 67.9, 26.08\} = 76.6$$

Thus, Functionality 3.22 has a high risk score, denoted by  $RS_{3.22}$ . A picture of this result is illustrated in Figure 26.

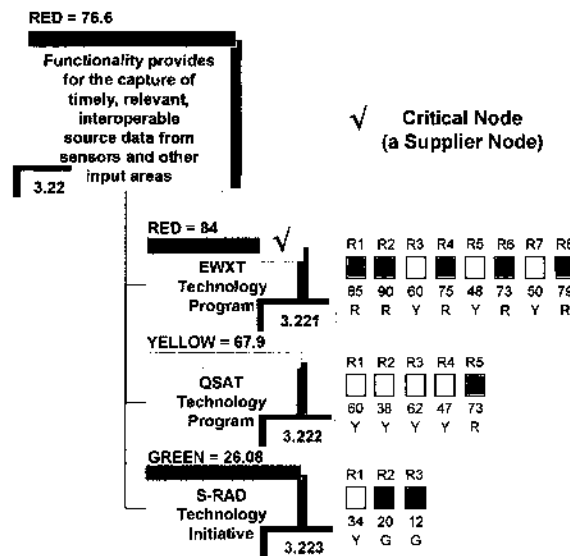


Figure 26. Risk Measure Derived for Functionality 3.22

The high risk score for Functionality 3.22 is driven by the importance of the EWXT Program. According to the scale convention in Figure 22, Functionality 3.22 would also fall in the “RED” color band, as shown in Figure 26.

It is important that various analyses be conducted to examine the risk-drivers to Functionality 3.22. It can be shown that 88 percent of the high risk score of Functionality 3.22 ( $RS_{3.22}$ ) is driven by the high risk score of the EWXT Technology Program ( $RS_{3.221}$ ). The high risk score of the EWXT Program is driven by R1, R2, R4, R6, and R8. These five risk events collectively account for 93 percent of the EWXT Program’s risk score ( $RS_{3.221}$ ).

These risk events signal where management attention is needed with respect to reducing the risk to Functionality 3.22. Improperly managing these risks, or not targeting them for management consideration, will further contribute to negative effects at higher dependency levels in the capability portfolio’s hierarchy.



### Measuring “Up”: How Functionality Risks Affect Capability

The preceding presented ways to derive a measure of Functionality 3.22 risk as a function of its supplier risks. Shown in Figure 19, Functionality 3.22 is one of four functionality nodes to Capability 3.2. What about the other functionality nodes? How might their risk measures combine into an overall measure of risk to Capability 3.2? What ripple effects do these Tier 4 functionality risks have on dependent higher level capability nodes in the capability portfolio’s hierarchy? The following will address these and related questions.

Suppose risk measures for the other three functionality nodes to Capability 3.2 are shown along Tier 4 in Figure 27. These nodes are Functionality 3.21, 3.23, and 3.24. Suppose their risk measures were also derived as a function of the risks their supplier nodes face, according to the same process just described. For convenience, we defer showing their supplier nodes to keep Figure 27 less visually complicated.

Next, we address a way to combine risk measures from all four functionality nodes, in Figure 27, into an overall measure of risk to Capability 3.2? Here, we can again apply the critical average rule across the four Tier 4 functionality nodes to derive a measure of risk faced by Capability 3.2 – a Tier 3 node.

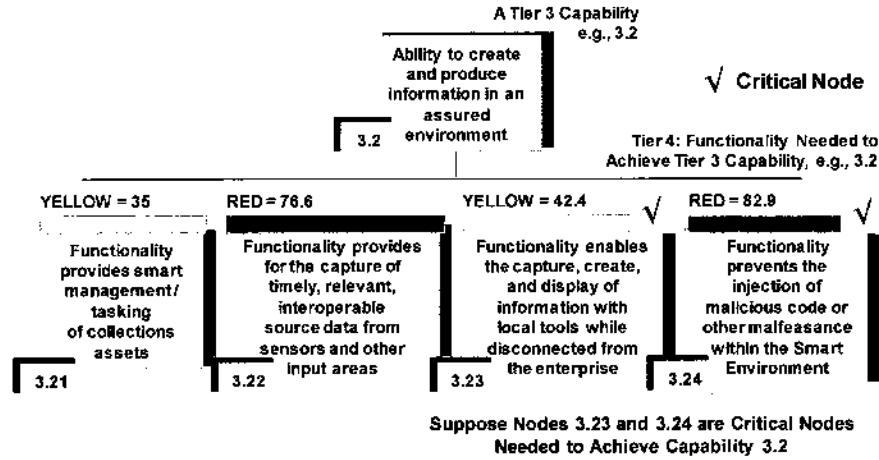


Figure 27. Risk Measures for Capability 3.2 Functionality Nodes

In Figure 27, suppose (in this case) Functionality 3.23 and 3.24 are deemed the critical functions to achieving Capability 3.2; thus,  $A = \{RS_{3.23}, RS_{3.24}\}$  in this case. From this, it follows that

$$\begin{aligned}
 Risk\ Score(Capability\ Node_{3.2}) &= RS_{3.2} \\
 &= \lambda Max\{A\} + (1 - \lambda) Average\{RS_{3.21}, RS_{3.22}, RS_{3.23}, RS_{3.24}\} \quad (3.5)
 \end{aligned}$$

where  $\lambda$  is a weighting function. For convenience, use the weighting function in Figure 23. Then, from the risk scores in Figure 27 and Equation 3.5 we have

$$RS_{3.2} = (0.70)(82.9) + (1 - 0.70)Average\{35, 76.6, 42.4, 82.9\} = 75.8$$

Thus, we conclude that Capability 3.2 has a high risk score. This is driven by the importance of Functionality 3.24. According to the scale convention in Figure 23, Capability 3.2 would fall in the “RED” color band. The results of this discussion are illustrated in Figure 28.

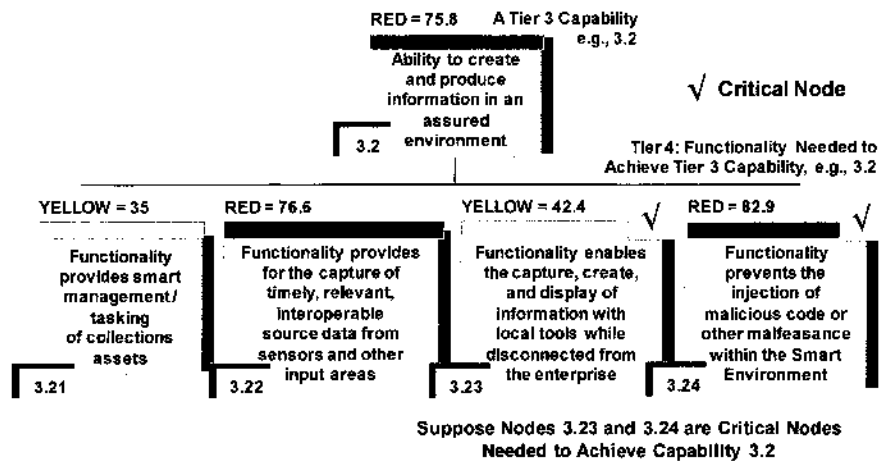


Figure 28. Risk Measure for Capability 3.2: Critical Average Rule

### Measuring “Up”: How Capability Risks Affect the Capability Portfolio

The preceding discussion presented ways to derive a measure of Capability 3.2 risk as a function of its Functionality risks. Shown in Figure 29, Capability 3.2 is one of four capability nodes to Information Assurance, a Tier 2 capability area. What about the other capability nodes? How might their risk measures combine into an overall measure of risk to Tier 2 Information Assurance? What ripple effects do these Tier 3 capability risks have in the capability portfolio’s hierarchy? The following will address these and related questions.

Suppose risk measures for the other three capability nodes to the Tier 2 node Information Assurance are shown in Figure 29. These nodes are Capability 3.1, 3.3, and 3.4.

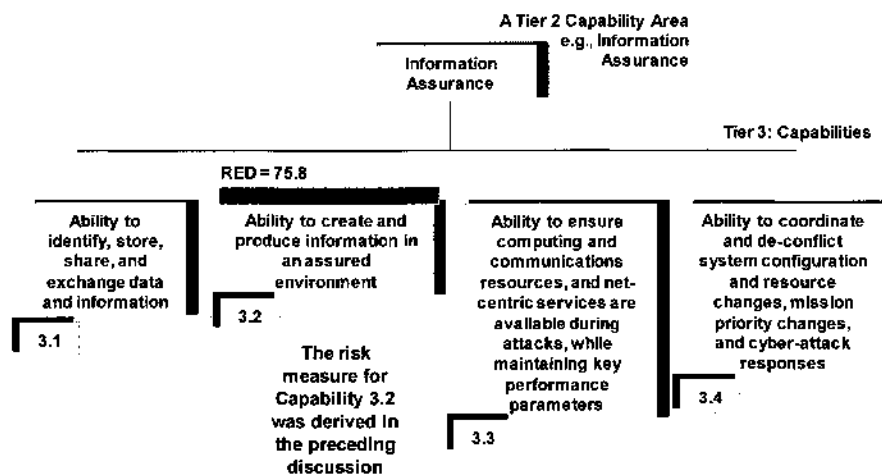


Figure 29. Information Assurance: A Tier 2 Capability Area

Suppose their risk measures were also derived as a function of the risks their functionality nodes face, according to the same process just described. For convenience, we defer showing their functionality nodes to keep Figure 29 less visually complicated.

We will again apply the critical average rule to combine risk measures from all four capability nodes, in Figure 30. This will produce an overall measure of risk to the Tier 2 node Information Assurance.

In Figure 30, suppose (in this case) Capability 3.1, 3.3, and 3.4 are deemed the critical capabilities to achieving Tier 2 Information Assurance. Given this, and applying the critical average rule, set  $A$  is equal to  $A = \{RS_{3.1}, RS_{3.3}, RS_{3.4}\}$ . From this, the max of set  $A$  is

$$\text{Max}\{A\} = \text{Max}\{RS_{3.1}, RS_{3.3}, RS_{3.4}\} = 38.1$$

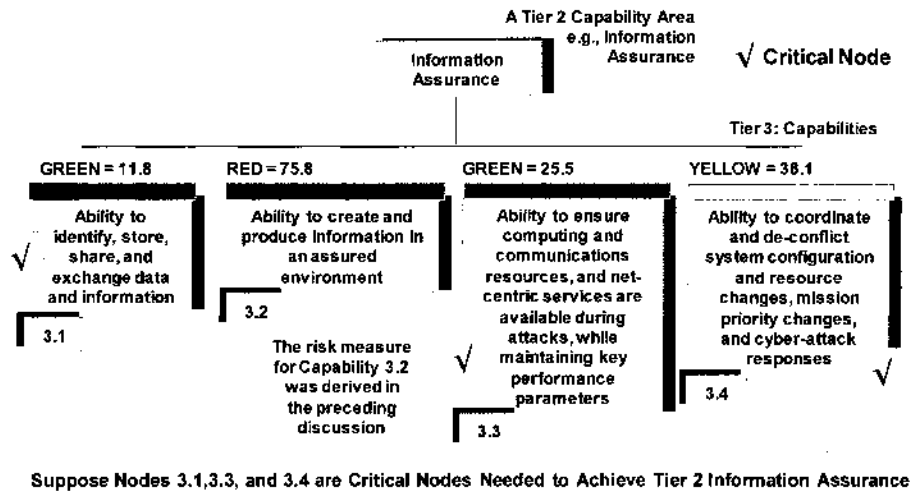


Figure 30. Information Assurance: Capability Risk Measures

Thus, from Equation 3.3 we have

$$\begin{aligned} \text{Risk Score}(\text{Information Assurance Node}) &= RS_{IA} \\ &= \lambda \text{Max}\{A\} + (1 - \lambda) \text{Average}\{RS_{3.1}, RS_{3.2}, RS_{3.3}, RS_{3.4}\} \end{aligned} \quad (3.6)$$

where  $\lambda$  is a weighting function. For convenience, use the weighting function in Figure 23. Then, from the risk scores in Figure 30 and Equation 3.6 we have

$$RS_{IA} = (0.381)(38.1) + (1 - 0.381) \text{Average}\{11.8, 75.8, 25.5, 38.1\} = 38$$

We conclude the Tier 2 Information Assurance capability area has a moderate risk score. This is driven by the importance of Capability 3.4. According to the scale convention in Figure 23, the Tier 2 Information Assurance capability area would fall in the YELLOW color band. The results of this discussion are illustrated in Figure 31.

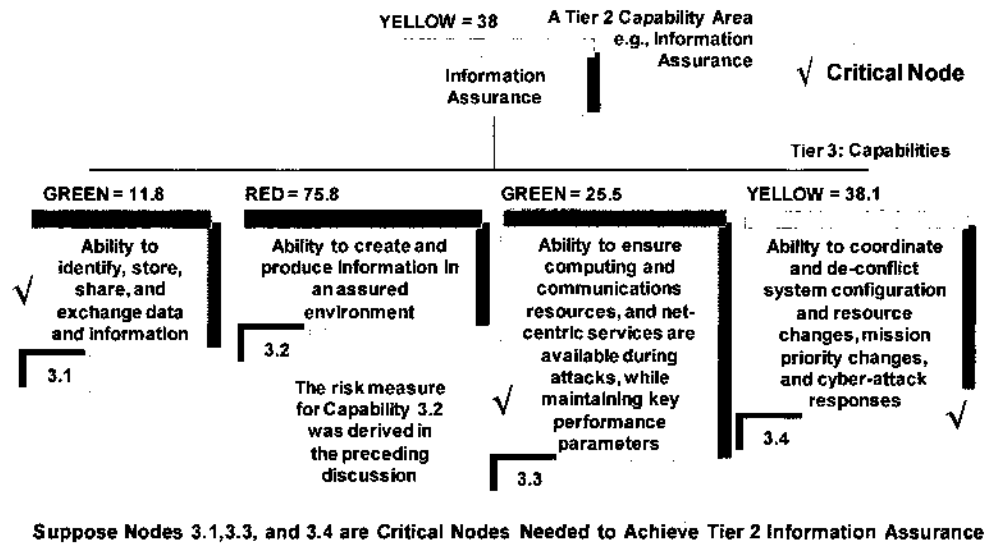


Figure 31. Information Assurance: Capability Risk Measures

Suppose risk measures for the other three Tier 2 capability areas are shown in Figure 32. These nodes are Network Management, Enterprise Services, and Communications and Applications. Suppose their risk measures were derived as a function of the risks their Tier 3 capability nodes face, according to the same process just described.

We can apply the critical average rule to combine risk measures from all four Tier 2 capability areas into an overall measure of risk to the capability portfolio. Assume all four Tier 2 capability areas are critical to the portfolio. The result of this computation is shown in Figure 32.

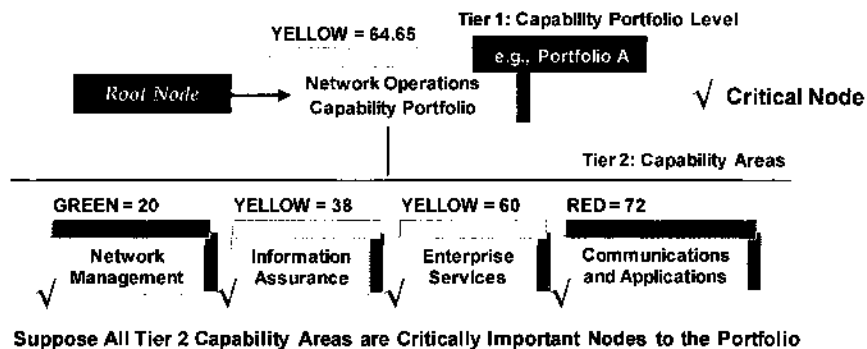


Figure 32. Network Operations Capability Portfolio-Level Risk Measure

Hence, we see the Network Operations Capability portfolio is facing an overall moderate level of risk with a risk measure of 64.65. According to the scale convention in Figure 23, the capability portfolio's overall risk measure places it in the YELLOW color band.

The preceding discussion presented an algebra designed to measure risk, at any node in a capability portfolio, when risk events originate from a capability portfolio's supplier levels. Computational rules were defined and illustrated to show how risk measures derive, in part, from a series of roll-up calculations. Risk measures derived from leaf nodes were rolled-up to measure the risks of parent nodes. Risk measures derived for parent nodes were rolled-up to measure the risk of the capability portfolio itself.

In the context of this formalism, the *number* of risk events associated with a supplier node does not fully drive the magnitude of its risk measure. Consider the max average rule. This rule is purposefully designed to weight more heavily risk events, in a set of events, with higher risk measures (risk scores) than those in the set with lower risk measures. Although risk scores of all risk events associated with a supplier node are included in the max average, *their effect on the node's overall risk measure is controlled by the shape or form of the weighting function  $\lambda$* . Because of this, each risk event does not necessarily contribute equally to the supplier node's overall risk measure. A supplier node with a set of five risk events can have a higher risk measure than one with a set containing more than five risk events *and vice versa*.

Thus, with the max average rule it is important to design the shape or form of its weighting function to capture the team's (or decision-maker's) preferences for the degree the maximum score should influence the overall score. One weighting function is shown in Figure 23. Many other shapes are possible [Garvey, 2008].

The *max average* rule applied in the context of Figure 24 operates, under certain conditions, as a decision-maker's "alert function". In Figure 24, the supplier node's risk measure was 84 given the eight risks R1 through R8. Suppose management actions were taken such that R3 through R8 were eliminated from this supplier node's risk set. With this, the EWXT Technology Program would now have a risk measure of 89.25.

Why did this supplier node's risk measure increase despite the elimination of all but two of its risks? The answer includes the following: (1) management actions eliminated R3 through R8 – but they did not eliminate the two most serious risks, R1 and R2, from the node's risk set (2) the max average rule operates only on the risk set presented; so, even though R3 through R8 were eliminated the max average rule only "sees" a supplier node with two serious risks R1 and R2.

The fact that the risk measure increased is noteworthy, but not as important as the result that the node remained in the Red risk color band in this example. Thus, the max average rule can be *tuned* to alert management when a supplier node still faces a high-degree of risk because of the presence of even just a few very serious risks – despite the elimination of less serious ones from the set.

What about risks to capabilities when risk events originate from non-supplier-related sources or conditions? How can these risks be considered in a capability portfolio risk assessment? Risks that threaten capabilities to be delivered by a capability portfolio can originate from sources other than those that affect only the portfolio's suppliers. These events can directly attack one or more capability nodes in a capability portfolio's hierarchy. For example, uncertainties in geo-political landscapes may impact operational demands on capabilities that stress planned performance.

Dependencies between capability portfolios in families of portfolios, such as those that constitute an enterprise, are also potential risk sources. Here, outcome objectives for capabilities delivered by one capability portfolio may depend on the performance of capabilities delivered by another capability portfolio. Identifying risk events from non-supplier-related sources and capturing their contribution to a capability node's risk measure is an important consideration in a capability portfolio's risk assessment and analysis process.

This process, as described, provides ways to separate, track, and report risks faced by capability nodes, as a function of the many sources of risk affecting the nodes and ultimately the capability portfolio. In practice, it is recommended that supplier and non-supplier measures of capability risk be separately derived, tracked, and reported to the capability portfolio's management team. In addition, each risk should be tagged according to its type (or nature) and tracked in the capability portfolio's overall risk "population".

If this is done, then a variety of management indicators can be developed. These include (1) the frequency with which specific types of risk affect capability nodes and (2) the degree a capability node's risk measure is driven by supplier versus non-supplier source conditions, including understanding the nature and drivers of these conditions.

We end this discussion with a summary of the information needed to implement capability portfolio risk management. The chapter concludes with a perspective on capability portfolio risk management and its relationship to the management of risk in engineering the enterprise.

### **INFORMATION NEEDS**

Risk management in a capability portfolio context has unique and thought challenging information needs. These needs can group into two categories. The first addresses capability value. The second category addresses supplier contributions, criticality, and risks as they relate to enabling the portfolio to deliver capability.

Information needs that address capability value include the following:

- For each Tier 3 capability, shown in Figure 16, what standard (or outcome objective) must each capability meet by its scheduled delivery date?
- For each Tier 3 capability, what is the source basis for its standard (or outcome objective)? Does it originate from user-driven needs, policy-driven needs, model-derived values, a combination of these, or from other sources?
- For each Tier 3 capability, what extent does the standard (or outcome objective) for one capability depend on others meeting their standards (or outcome objectives)?

Information needs that *address supplier contributions, criticality, and risks* include the following:

- For each Tier 3 capability, which Technology Programs and Technology Initiatives are contributing to that capability?

- For each Tier 3 capability, what (specifically) are the contributions of its suppliers?
- For each Tier 3 capability, how do supplier contributions enable the capability to achieve its standard (or outcome objective)?
- For each Tier 3 capability, which Technology Programs and Technology Initiatives are critical contributors in enabling the capability to achieve its standard (or outcome objective)?
- Given this, what risks originate from (or are associated with) suppliers that, if these events occur, negatively affect their contributions to capability?

A similar set of information needs can be crafted for risk events that originate from non-supplier-related sources or conditions.

Measuring, tagging, and tracking risk events in the ways described aids management with identifying courses of action. Specifically, whether options exist to attack risks directly at their sources or to engage them by deliberate intervention actions – actions aimed at lessening or eliminating their potential capability consequences.

Process tailoring, socialization, and establishing governance protocols are critical considerations in engineering risk management. Ensuring these aspects succeed is time well-spent. With this, effective and value-added engineering management practices can be institutionalized – practices that enable capability portfolio outcomes, and ultimately those of the enterprise, to be achieved via risk-informed resource and investment management decisions.

To conclude, the approach presented for capability portfolio risk management provides a number of beneficial and actionable insights. These include the following:

- Identification of risk events that threaten the delivery of capabilities needed to advance goals and capability outcome objectives.
- A measure of risk for each capability derived as a function of each risk event's occurrence probability and its consequence.
- An analytical framework and logical model within which to structure capability portfolio risk assessments – one where assessments can be combined to measure and trace their integrative effects on engineering the enterprise.
- Through the framework, ways to model and measure risk as capabilities are time-phased across incremental capability development approaches.
- Decision-makers provided the trace basis and the event drivers behind all risk measures derived for any node at any level of the capability portfolio's hierarchy. With this, capability portfolio management has visibility and supporting rationales for identifying where resources are best allocated to reduce (or eliminate) risk events that threaten achieving goals and capability outcome objectives.

## CHAPTER IV

### AN INDEX TO MEASURE RISK CO-RELATIONSHIPS (RCR)

#### INTRODUCTION

Chapter III described a way to structure the risk management problem space in engineering enterprise systems from a capability portfolio perspective. A representation of this space by a supplier-provider metaphor in the form of a mathematical graph was developed. This graph is a topology of nodes that depict supplier-provider-capability relationships unique to a capability portfolio. From this, capturing dependencies between nodes is clearly a critical aspect in the analysis and management of risk in engineering enterprise systems.

In this dissertation, we posit two types of dependencies that affect risk in engineering capabilities for an enterprise system. One is risk inheritance; that is, how risk-dependent are capabilities so threats to them can be discovered *before* contributing programs (e.g., suppliers) degrade, fail, or are eliminated? The other is operational dependence; that is, what is the effect on the operability of capability if, *due to the realization of risk*, one or more contributing programs (e.g., suppliers) or supplier-provider chains degrade, fail, or are eliminated? This chapter addresses the first type of dependency. Chapter V addresses the second type of dependency.

The following introduces the community to a new management metric called the Risk Co-Relationship (RCR) index. The RCR index measures risk inheritance between supplier programs and its ripple effects across a capability portfolio. The index identifies and captures directional impacts of risk inheritance, across supplier-provider chains, as this increases the threat that risks with one supplier program may adversely affect others and ultimately their contributions to their associated capabilities. The purpose of the RCR index is to signal where risk reducing opportunities exist to minimize dependency risks that, if realized, have cascading negative effects on the ability of an enterprise to deliver capabilities and services to users.

#### RCR POSTULATES, DEFINITIONS, AND THEORY

The development of the RCR index is based on a set of postulates. They are definitional to the index in terms of its behavior and the problem context of engineering enterprise systems by capability portfolios.

The RCR postulates are expressed in the context of a mathematical graph, which represents the supplier-provider metaphor previously described. As such, these postulates assume a parent-child relationship between a capability node (C-node) and the set of supplier program nodes that contribute to enabling that capability. First, we begin with a definition of *risk inheritance*.

##### **Definition 4.1:** Risk Inheritance

A risk co-relationship exists between program nodes *if and only if* one program node inherits one or more risk events from one or more other program nodes and the inherited risks have nonzero consequences on the inheriting program node's ability to deliver its contribution to its respective capability node.



Inheritance occurs when risks from one or more supplier program nodes transmit an increased risk to other dependent nodes along a connecting path of neighboring nodes through the graph.

Risk co-relationships only directly exist between P-nodes; that is, only P-nodes can directly inherit risk events. Risk co-relationships indirectly exist between C-nodes when P-nodes associated with them have risk co-relationships with other P-nodes in the capability portfolio.

**Postulate 4.1: Capability Node Risk Score**

A capability node's risk score is a function of the risk scores of its supplier program nodes.

**Postulate 4.2: Capability Node RCRs Are Indirect**

A capability node's risk co-relationships are indirect. They derive only from risk co-relationships that directly exist between supplier program nodes across the capability portfolio.

**Postulate 4.3: Inheritance Bounds**

The risk score of a program node with non-inherited risk events that then inherits one or more risks from one or more other program nodes cannot be lower than its risk score prior to the inheritance.

**Postulate 4.4: Probability Invariant With Inheritance**

A risk event's occurrence probability is invariant with respect to inheritance.

**Postulate 4.5: Impacts Can Vary With Inheritance**

An inherited risk event's impact (or consequence) on a receiving program node can be different from its impact (or consequence) on the sending program node.

**Postulate 4.6: Impacts Assessed Against Capability**

A risk event inherited by a program node shall have its impacts assessed in terms of how the risk, if it occurs, has negative consequences to that program node's ability to deliver its contribution to its associated capability node.

**Postulate 4.7: Inherited Risk Events Have Resolution Priority**

Inherited risk events are "first" targets for resolution or elimination by management.

Inherited risk events have, by their nature, extended their threat to other programs beyond their source program nodes. This complicates coordination, collaboration, and risk resolution planning between management and stakeholders across all levels of the portfolio. Impacts to multiple stakeholders, users, and outcome goals of affected program nodes must be jointly and carefully considered when planning, executing, and managing resolution strategies for inherited risks.

Next, we establish important notation pertaining to the RCR Index. This is followed by a set of definitions that govern its computation.

**Notation 4.1**

Let  $E$  denote a risk event.

**Notation 4.2**

Let  $[[E]]$  denote a risk event inherited by one program node from another program node.

**Notation 4.3**

Let  $\sim I = \{E_{i1}, E_{i2}, E_{i3}, \dots, E_{im}\}$  denote a finite set of  $j = 1, \dots, m$  non-inherited risk events associated with program node  $P_i$ . Let  $\sim I$  denote the notation for not-inherited.

**Notation 4.4**

Let  $I = \{[[E_{i,x,q}]], [[E_{i,y,r}]], [[E_{i,z,s}]], \dots, [[E_{i,\bullet,u}]]\}$  denote a finite set of inherited risk events that program node  $P_i$  receives from one or more other program nodes in the capability portfolio. Let subscripts  $x, y$ , and  $z$  denote the subscripts of the sending program nodes. Let subscripts  $q, r, s$ , and  $u$  denote the subscripts of the risk events inherited by  $P_i$  from the sending program nodes. Let  $I$  denote notation for inherited.

For example, the set  $\{[[E_{1,2,6}]]\}$  indicates program node  $P_1$  receives or inherits risk event  $E_6$  from program node  $P_2$ . The set  $\{[[E_{1,2,6}]], [[E_{1,2,4}]], [[E_{1,2,5}]], [[E_{1,3,9}]]\}$  indicates program node  $P_1$  receives or inherits four risk events from four other P-nodes in the capability portfolio. These events are  $E_6, E_4$ , and  $E_5$  from program node  $P_2$  and  $E_9$  from program node  $P_3$ .

**Notation 4.5**

Let  $\{RS(E_{i1}), RS(E_{i2}), RS(E_{i3}), \dots, RS(E_{im})\}$  denote a finite set of non-inherited risk event risk scores associated with program node  $P_i$ , where, in general,

$$0 < Risk\ Score(E) = RS(E) = u_1 Prob(E) + u_2 V_{Impact}(E) \leq 100 \quad (4.1)$$

where coefficients  $u_1$  and  $u_2$  are non-negative weights that sum to one. The first term is a value function for the risk event's occurrence probability. The second term is a value function for the risk event's overall impact on a program node's ability to deliver its contribution to its respective capability node. Higher risk event risk scores have higher criticality to management.

**Notation 4.6**

Let  $\{RS([[E_{i,x,q}]]), RS([[E_{i,y,r}]]), RS([[E_{i,z,s}]]), \dots, RS([[E_{i,\bullet,u}]]])\}$  denote a finite set of inherited risk event risk scores associated with program node  $P_i$ , where, in general,

$$0 < Risk\ Score([[E]]) = RS([[E]]) = u_1 Prob(E) + u_2 V_{Impact}([E]) \leq 100 \quad (4.2)$$

We assume a risk event's occurrence probability is invariant with respect to inheritance, but an inherited risk event's impact  $V_{Impact}([E])$  on a receiving program node can be different than its impact on the sending program node; so,  $V_{Impact}([E])$  does not necessarily equal  $V_{Impact}(E)$ .

Last, we establish the set of definitions that govern the RCR index computations.

**Definition 4.2: Risk Event Risk Score**

The risk score  $RS$  of risk event  $E$  is given by

$$0 < Risk\ Score(E) = RS(E) = u_1 Prob(E) + u_2 V_{Impact}(E) \leq 100$$

where coefficients  $u_1$  and  $u_2$  are non-negative weights that sum to one. The first term is a value function for the risk event's occurrence probability. The second term is a value function for the risk event's overall impact on a program node's ability to deliver its contribution to its respective capability node. A risk event with a high risk score has high criticality to management.

**Definition 4.3: Program Node Risk Score (Non-Inherited Risk Events)**

The risk score of the  $i$ -th program node's set of non-inherited risk events is given by

$$RS(P_i | \sim I) = MaxAve(\{RS(E_{i1}), RS(E_{i2}), RS(E_{i3}), \dots, RS(E_{im})\}) \quad (4.3)$$

where  $0 < RS(P_i | \sim I) \leq 100$ ,  $\sim I$  indicates program node  $P_i$ 's set of non-inherited risk events, and  $MaxAve$  is a special weighted average operator on the set of risk event risk scores  $\{RS(E_{i1}), RS(E_{i2}), RS(E_{i3}), \dots, RS(E_{im})\}$ . Chapter III presented the  $MaxAve$  operator.

**Definition 4.4: Program Node Risk Score (Inherited Risk Events)**

The risk score of the  $i$ -th program node's set of inherited risk events is given by

$$RS(P_i | I) = MaxAve(\{RS([E_{i,x,q}]), RS([E_{i,y,r}]), RS([E_{i,z,s}]), \dots, RS([E_{i,\bullet,u}])\}) \quad (4.4)$$

where  $0 < RS(P_i | I) \leq 100$  and  $I$  indicates program node  $P_i$ 's set of inherited risk events.

**Definition 4.5: Program Node Risk Score (Non-Inherited and Inherited Risk Events)**

The risk score of program node  $P_i$ , when  $P_i$  is characterized by a finite set of non-inherited and inherited risk events is denoted by  $RS(P_i | \sim I \wedge I)$  and is defined below

$$RS(P_i | \sim I \wedge I) = \begin{cases} RS(P_i | \sim I) & \text{if } Z_1 \text{ is true} \\ MaxAve(RS(P_i | \sim I), RS(P_i | I)) & \text{if } Z_2 \text{ is true} \end{cases} \quad (4.5)$$

where,  $Z_1$  is when  $P_i$  has non-inherited and inherited risk events and  $RS(P_i | I) \leq RS(P_i | \sim I)$  (in accordance with Postulate 4.3);  $Z_2$  is when  $P_i$  has non-inherited and inherited risk events and  $RS(P_i | \sim I) < RS(P_i | I)$ . From Definition 4.3 the risk score of any risk event is greater than zero; otherwise the event would not be a risk.

The expression associated with  $Z_2$  is referred to as the *MaxAve chain rule*. This rule is activated when  $Z_2$  is true; that is, when a program node  $P_i$  contains non-inherited and inherited risk events and the risk score of  $P_i$  with respect to its inherited risk events is greater than the risk score of its non-inherited risk events. The following describes the MaxAve chain rule.

Recall that  $\sim I = \{E_{i1}, E_{i2}, E_{i3}, \dots, E_{im}\}$  denotes a finite set of non-inherited risk events associated with program node  $P_i$ . This set of risk events excludes any events inherited from one or more other P-nodes in the capability portfolio. Recall that

$$I = \{[[E_{i,x,q}]], [[E_{i,y,r}]], [[E_{i,z,s}]], \dots, [[E_{i,\bullet,u}]]\}$$

denotes a finite set of inherited risk events that program node  $P_i$  receives from one or more other P-nodes in the capability portfolio.

If program node  $P_i$  contains non-inherited and inherited risk events, then (in accordance with Equation 4.5) the overall risk score of  $P_i$  is computed by “chaining” the max average rule if condition  $Z_2$  is met; specifically,

$$RS(P_i | \sim I \wedge I) = \text{MaxAve} (RS(P_i | \sim I), RS(P_i | I)), \text{ where}$$

$$RS(P_i | \sim I) = \text{MaxAve} (RS(E_{i1}), RS(E_{i2}), RS(E_{i3}), \dots, RS(E_{im})), \text{ and}$$

$$RS(P_i | I) = \text{MaxAve}(RS([E_{i,x,q}]), RS([E_{i,y,r}]), RS([E_{i,z,s}]), \dots, RS([E_{i,\bullet,u}]))$$

where  $RS(P_i | \sim I)$  and  $RS(P_i | I)$  are described in Definition 4.3 and Definition 4.4, respectively. The max average chain rule applies only to program nodes that contain non-inherited risk events and risk events inherited from one or more other program nodes in the portfolio, subject to condition  $Z_2$  being met.

The practical philosophy behind the max average chain rule is as follows. If a program node’s set of inherited risk events has a higher overall risk score than the node’s set of non-inherited risk events, then the node’s overall risk score should be driven by the impacts of inheritance.

The complement of the above must also be true. If a program node’s set of non-inherited risk events has a higher overall risk score than the node’s set of inherited risk events, then the node’s overall risk score should be driven by the impacts of non-inheritance – as these are the more threatening events to the program node’s ability to deliver its contribution to its capability node. The max average chain rule, when invoked, ensures the direction of these outcomes is preserved.

**Definition 4.6: Capability Node Risk Score**

The risk score  $RS$  of a capability node (e.g., the  $k$ -th C-node enabled by contributions from its  $h$  supplier program nodes) is the max average of its individual program node risk scores *that include (if present) the influence of risk event inheritance in accordance with Definition 4.5.*

$$0 < \text{Risk Score}(C_k) = RS(C_k)$$

$$= \text{MaxAve}(\{RS(P_{k1}), RS(P_{k2}), RS(P_{k3}), \dots, RS(P_{kh})\}) \leq 100 \quad (4.6)$$

**Definition 4.7: Program Node RCR Index**

If program node  $P_i$  contains non-inherited risk events and risk events inherited from one or more other program nodes in the capability portfolio, then the risk co-relationship (RCR) index of  $P_i$  is defined as follows:

$$0 \leq RCR(P_i) = \frac{RS(P_i | \sim I \wedge I) - RS(P_i | \sim I)}{RS(P_i | \sim I \wedge I)} < 1 \quad (4.7)$$

where the risk scores in the RCR index must all be greater than zero. If inheritance is not present between program nodes then  $RCR(P_i)$  is equal to zero by definition.

**Definition 4.8: Capability Node RCR Index**

If capability node  $C_k$  contains one or more program nodes that have risk co-relationships with other program nodes in the capability portfolio, then the risk co-relationship (RCR) index of capability node  $C_k$  is defined as follows:

$$0 \leq RCR(C_k) = \frac{RS(C_k | \sim I \wedge I) - RS(C_k | \sim I)}{RS(C_k | \sim I \wedge I)} < 1 \quad (4.8)$$

where  $RS(C_k | \sim I \wedge I)$  is the risk score of capability node  $C_k$  computed over its set of P-node risk scores that include (if present) the influence of risk event inheritance in accordance with Definition 4.5. The term  $RS(C_k | \sim I)$  is the risk score of capability node  $C_k$  computed over its set of P-node risk scores that do not include the influence of inheritance.

Last, recall from Postulate 4.2 that a capability node's risk co-relationships are indirect. They derive only from risk co-relationships that exist directly between supplier program nodes in the portfolio. So, a capability node's RCR index is really a response measure – one that derives from the effects of risk event inheritance between P-nodes that comprise the supplier dimension of the capability portfolio. This is illustrated in Figure 33, whose interpretation is discussed next.

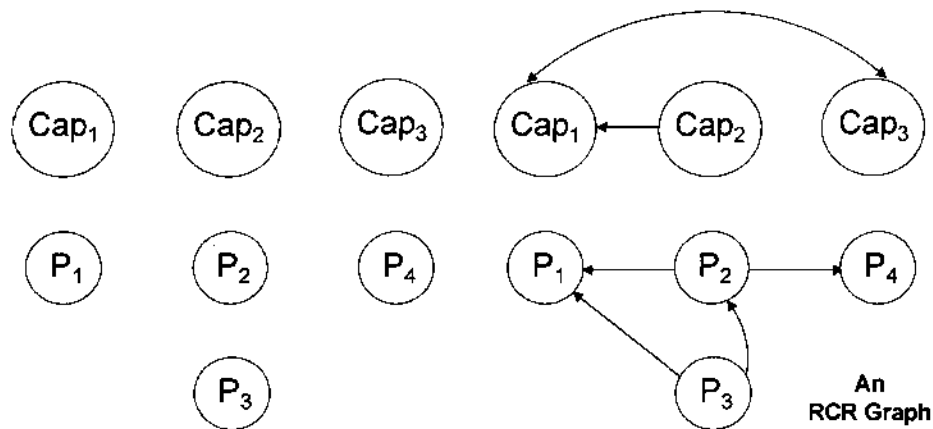


Figure 33. An RCR Graph: Program-to-Capability Node Risk Co-Relationships

Suppose Figure 33 illustrates a capability portfolio that consists of three capability nodes (C-nodes) and four supplier program nodes (P-nodes). The left-most assemblage of nodes shows an alignment of P-nodes under each C-node. Let this alignment indicate which supplier programs are responsible to deliver technologies that enable the associated capability. In Figure 33, we see that capability node  $Cap_2$  is dependent on two supplier program nodes  $P_2$  and  $P_3$  for it to achieve its intended outcomes.

In Figure 33, the right-most picture shows arrows between the C-nodes and the P-nodes on the left. These arrows signal that risk co-relationships exist between them. The right-most picture in Figure 33 is called an RCR graph. In an RCR graph, risk co-relationships are always indicated by arrows\*. Figure 34 shows the RCR graph in Figure 33 with the inheritance flow of risk events from one node to another node.

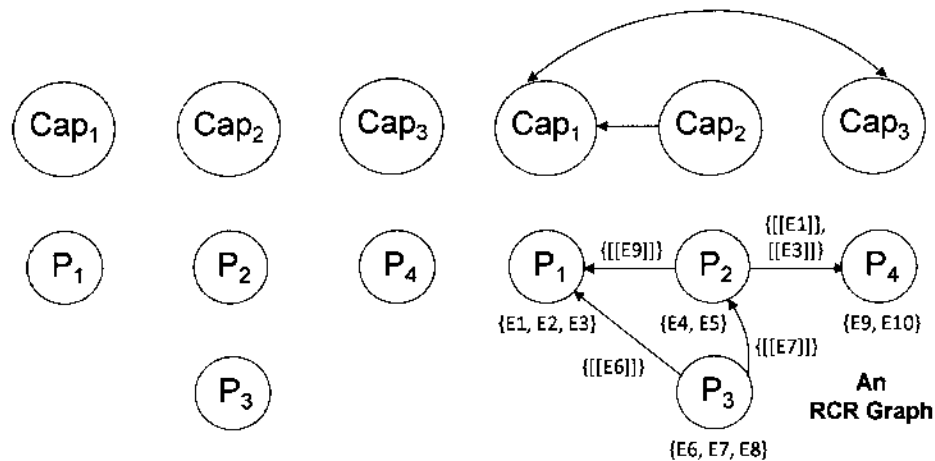


Figure 34. An RCR Graph: A Risk Event Inheritance View

On the right side of Figure 34, a collection of risk events are shown under each program node. Recall that a risk event is one that, if it occurs, has unwanted consequences for the respective program node's ability to deliver its contribution to its respective capability node.

From Definition 4.1, a risk co-relationship exists between P-nodes if and only if one P-node inherits one or more risk events from one or more other P-nodes, and the inherited risks have nonzero consequences on the inheriting P-node's ability to deliver its contribution to its respective capability node. When risk co-relationships are present, they only exist directly between P-nodes. Risk co-relationships between C-nodes are indirect; that is, they occur in response to the presence of direct P-node risk co-relationships. In Figure 33 and Figure 34, this is indicated by the arched arrow above the C-nodes.

\* In Chapter V, arrows are used to indicate the direction of operational dependencies between nodes in a mathematical graph that represents a capability portfolio. In Chapter V, such a graph is called a Functional Dependency Network Analysis (FDNA) graph. In this chapter, arrows are used to indicate (1) a risk co-relationship exists between two nodes and (2) the direction of the risk inheritance in terms of the inheritance feeding node and the inheritance receiving node. When arrows on a graph indicate risk inheritance then it is called an RCR graph. When arrows on a graph indicate operational dependence then it is called an FDNA graph. This is indicated in this dissertation by labeling the graph or the figure as an RCR graph or an FDNA graph. With this, arrows on these graphs are interpreted accordingly.

In Figure 34, let  $E$  denote a risk event. Let  $[[E]]$  denote a risk event inherited by one P-node from another P-node. Let  $\sim I = \{E_{i1}, E_{i2}, E_{i3}, \dots, E_{im}\}$  denote a finite set of  $j = 1, \dots, m$  non-inherited risk events associated with program node  $P_i$ . The notation  $\sim I$  denotes not-inherited.

Let  $I = \{[[E_{i,x,q}]], [[E_{i,y,r}]], [[E_{i,z,s}]], \dots, [[E_{i,\bullet,u}]]\}$  denote a finite set of inherited risk events that program node  $P_i$  receives from one or more other P-nodes in the capability portfolio. Let subscripts  $x, y$ , and  $z$  denote the subscripts of the sending P-nodes. Let subscripts  $q, r, s$ , and  $u$  denote the subscripts of the risk events inherited by  $P_i$  from the sending P-nodes. The notation  $I$  denotes inherited.

The RCR index behaves in accordance with a set of properties summarized below. These properties follow from the preceding postulates and definitions.

**Property 4.1**

If program node  $P_i$  has non-inherited and inherited risk events and  $RS(P_i|I) \leq RS(P_i|\sim I)$ , then  $RCR(P_i) = 0$ . Note, if inheritance is not present between program nodes then  $RCR(P_i)$  is equal to zero by Definition 4.7.

**Proof**

Program node  $P_i$  is given to have non-inherited and inherited risk events, and it is given that  $RS(P_i|I) \leq RS(P_i|\sim I)$ . From Postulate 4.3, it then follows that  $RS(P_i|\sim I \wedge I) = RS(P_i|\sim I)$ ; thus,

$$RCR(P_i) = \frac{RS(P_i|\sim I \wedge I) - RS(P_i|\sim I)}{RS(P_i|\sim I \wedge I)} = \frac{RS(P_i|\sim I) - RS(P_i|\sim I)}{RS(P_i|\sim I)} = 0$$

This completes the proof. Property 4.1 reflects the following: if the risk co-relationship between  $P_i$  and another program node is zero, then inheritance has no increase on the magnitude of the risk score of  $P_i$ . The program node maintains its score (e.g., its value remains high or low) despite the inheritance of one or more risk events from one or more other P-nodes. This derives from Postulate 4.3 which states: *The risk score of a P-node with non-inherited risk events that then inherits one or more risks from one or more other P-nodes cannot be lower than its risk score prior to the inheritance.*

**Property 4.2**

The RCR index can never equal or exceed one.

**Proof**

The RCR index can only equal one when  $RS(P_i|\sim I) = 0$ ; however, from Equation 4.1, the risk score of a risk event must always be strictly greater than zero; otherwise, the event would not be a risk. Since  $RS(P_i|\sim I) > 0$  it follows that the RCR index can never equal or exceed one.

**Property 4.3**

The RCR index always falls within the interval  $0 \leq RCR(P_i) < 1$

**Proof**

From Property 4.1, it was shown under what conditions  $RCR(P_i) = 0$ . From Property 4.2, it was shown why the RCR index can never equal or exceed one. To show the RCR index is otherwise between zero and one, we proceed as follows. From Equation 4.7 we have

$$0 \leq RCR(P_i) = \frac{RS(P_i | \sim I \wedge I) - RS(P_i | \sim I)}{RS(P_i | \sim I \wedge I)} < 1$$

where the risk scores in the RCR index must all be greater than zero. The risk co-relationship index will be less than one when  $RS(P_i | \sim I \wedge I) > RS(P_i | \sim I)$ . From Equation 4.5

$$RS(P_i | \sim I \wedge I) = \text{MaxAve}(RS(P_i | \sim I), RS(P_i | I))$$

when program node  $P_i$  has non-inherited and inherited risk events and  $RS(P_i | \sim I) < RS(P_i | I)$ . When  $RS(P_i | \sim I) < RS(P_i | I)$  it follows that

$$RS(P_i | \sim I \wedge I) = \text{MaxAve}(RS(P_i | \sim I), RS(P_i | I)) > RS(P_i | \sim I)$$

From this, suppose we let

$$RS(P_i | \sim I \wedge I) = \text{MaxAve}(RS(P_i | \sim I), RS(P_i | I)) > RS(P_i | \sim I) = RS(P_i | \sim I) + \varepsilon, \quad \varepsilon > 0$$

From this, we can write

$$RCR(P_i) = \frac{RS(P_i | \sim I) + \varepsilon - RS(P_i | \sim I)}{RS(P_i | \sim I) + \varepsilon} = \frac{\varepsilon}{RS(P_i | \sim I) + \varepsilon}$$

Since  $RS(P_i | \sim I) > 0$  (from Equation 4.1) and  $\varepsilon > 0$  it follows that  $RS(P_i | \sim I) + \varepsilon > \varepsilon$ ; hence

$$RCR(P_i) = \frac{RS(P_i | \sim I) + \varepsilon - RS(P_i | \sim I)}{RS(P_i | \sim I) + \varepsilon} = \frac{\varepsilon}{RS(P_i | \sim I) + \varepsilon} < 1$$

This completes the proof. Property 4.3 bounds the interval within which the RCR index takes values. The closer the index is to one the greater the influence of risk inheritance on program node  $P_i$ .



**Theorem 4.1**

If program node  $P_i$  has non-inherited and inherited risk events and  $RS(P_i|\sim I) < RS(P_i|I)$  then

$$RS(P_i|\sim I) < RS(P_i|\sim I \wedge I) < RS(P_i|I)$$

**Proof**

Given that program node  $P_i$  contains non-inherited and inherited risk events and

$$RS(P_i|\sim I) < RS(P_i|I)$$

it follows from Equation 4.5 that

$$RS(P_i|\sim I \wedge I) = \text{MaxAve}(RS(P_i|\sim I), RS(P_i|I))$$

Given  $RS(P_i|\sim I) < RS(P_i|I)$  it follows that

$$\text{MaxAve}(RS(P_i|\sim I), RS(P_i|I)) > RS(P_i|\sim I)$$

and

$$\text{MaxAve}(RS(P_i|\sim I), RS(P_i|I)) < RS(P_i|I)$$

since, in general, if  $a$  and  $b$  are real numbers and  $a < b$ , then  $a < \text{MaxAve}(a, b) < b$ . Thus,

$$RS(P_i|\sim I) < RS(P_i|\sim I \wedge I) < RS(P_i|I)$$

This concludes the development and discussion of the RCR index and its theoretical properties. The following illustrates computing the index and highlights aspects of its properties.

**COMPUTING THE RCR INDEX**

The following describes each step associated with measuring risk co-relationships in a capability portfolio. Numerical examples are then provided to illustrate how the RCR index is computed.

**Step 1****Model an Enterprise as a Portfolio of Capabilities**

In this step, we model the management of engineering an enterprise by defining a portfolio of the capabilities it must deliver. Illustrated in Figure 17, a capability portfolio can be expressed by building blocks of programs and technologies that, when integrated, incrementally provide user-services that enables enterprise outcome objectives to be achieved over time. Creating capability portfolios is a complex engineering and management process, as discussed in Chapters II and III.

**Step 2****Model Each Capability as a Supplier-Provider System Made up of Program Nodes**

In this step, we represent the capability portfolio by a mathematical graph. These can be seen in the preceding chapters; however, to simplify its visualization consider the capability portfolio's supplier-provider graph in Figure 34.

In Figure 34, we have a portfolio of three capability nodes (C-nodes) and four supplier program nodes (P-nodes). The left-most graph shows an alignment of P-nodes under each C-node. Let this alignment indicate those supplier programs delivering technologies that enable the associated capability. In Figure 34, capability node  $Cap_2$  is dependent on supplier program nodes  $P_2$  and  $P_3$  for it to achieve its intended outcomes.

The right-most collection of nodes shows where risk co-relationships exist between them. These are indicated by the arrows.

### Step 3

#### Describe Each Program Node's Risk Events

In this step, we describe each program node in terms of its non-inherited and inherited risk events. Refer to Figure 34. On the right-side, a collection of risk events is shown under each program node. A risk co-relationship exists between P-nodes if and only if one P-node inherits one or more risk events from one or more other P-nodes, and the inherited risks have nonzero consequences on the inheriting P-node's ability to deliver its contribution to its respective capability node.

When risk co-relationships are present, they only exist directly between P-nodes. Risk co-relationships between C-nodes are indirect; that is, they occur in response to the presence of direct P-node risk co-relationships.

In Figure 34, let  $E$  denote a risk event. Let  $[[E]]$  denote a risk event inherited by one P-node from another P-node. For instance,  $P_1$  has set of non-inherited risk events  $\sim I = \{E_1, E_2, E_3\}$  and a set of inherited risk events  $I = \{[[E_9]], [[E_6]]\}$  from nodes  $P_2$  and  $P_3$ , respectively.

### Step 4

#### Compute Risk Co-Relationship Indices

In this step, we compute the risk co-relationship index for each program node and each capability node. Formulas to compute these indexes are given by Equation 4.7 and Equation 4.8, respectively. This will be illustrated in the examples that follow.

### Step 5

#### Manage Risk Events

Managing risk events involves a host of decisions and considerations. This includes determining the optimal assignment of resources to P-nodes that offer the maximum reduction in the effects of risk inheritance, given resources or funding constraints.

Once determined, this enables portfolio management to time-history monitor reductions in capability risk, as driven by inheritance and non-inheritance, when more and more risk reduction dollars are judiciously applied in optimally decision-theoretic ways. This will be illustrated in the forthcoming section.

**Example 4.1:** From the information in Figure 35, compute the risk co-relationship index for program node  $P_1$ .

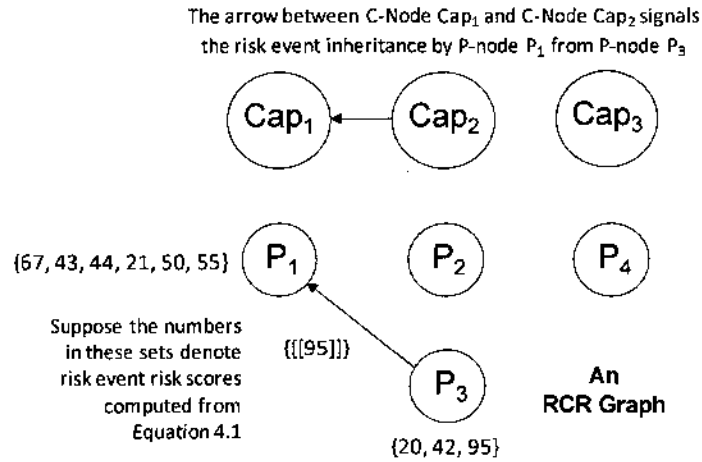


Figure 35. Example 4.1 RCR Graph

From Equation 4.3 we have

$$RS(P_1 | \sim I) = \text{MaxAve} (67, 43, 44, 21, 50, 55) = 60.29$$

From Equation 4.4 we have

$$RS(P_1 | I) = \text{MaxAve} ([95]) = 95$$

From Equation 4.5 we have

$$RS(P_1 | \sim I \wedge I) = \text{MaxAve} (60.29, 95) = 89.7935 \text{ since } RS(P_1 | \sim I) < RS(P_1 | I)$$

In the above max average calculation suppose the weighting function in Figure 23 was used.

From Equation 4.7 we have

$$0 \leq RCR(P_1) = \frac{RS(P_1 | \sim I \wedge I) - RS(P_1 | \sim I)}{RS(P_1 | \sim I \wedge I)} = \frac{89.7935 - 60.29}{89.7935} = 0.32857 < 1$$

The influence of the inherited risk event's risk score on program node  $P_1$  accounts for approximately 33 percent of its risk score. This would certainly be noteworthy to report to the engineering system's program manager or its management team.

**Example 4.2:** From the information in Figure 36, compute the risk co-relationship index for program node  $P_1$ .

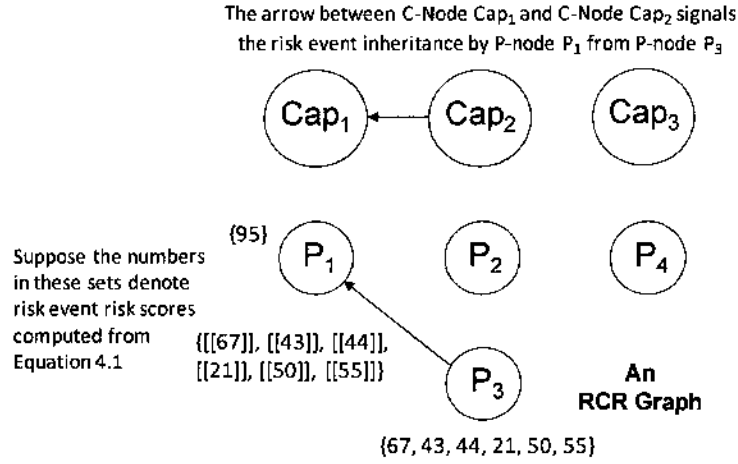


Figure 36. Example 4.2 RCR Graph

From Equation 4.3 we have

$$RS(P_1 | \sim I) = \text{MaxAve} (95) = 95$$

From Equation 4.4 we have

$$RS(P_1 | I) = \text{MaxAve} ([67], [43], [44], [21], [50], [55]) = 60.29$$

From Equation 4.5 we have

$$RS(P_1 | \sim I \wedge I) = RS(P_1 | \sim I) = 95 \text{ since } RS(P_1 | I) < RS(P_1 | \sim I)$$

In the above max average calculation suppose the weighting function in Figure 23 was used.

From Equation 4.7 we have

$$0 \leq RCR(P_1) = \frac{RS(P_1 | \sim I \wedge I) - RS(P_1 | \sim I)}{RS(P_1 | \sim I \wedge I)} = \frac{95 - 95}{95} = 0$$

The inherited risk event's risk score on program node  $P_1$  has no influence on its risk score, in accordance with Postulate 4.3. Recall this states: *The risk score of a program node with non-inherited risk events that then inherits one or more risks from one or more other program nodes cannot be lower than its risk score prior to the inheritance.*

**Example 4.3:** Compute the risk co-relationship indexes for all nodes in Figure 37.

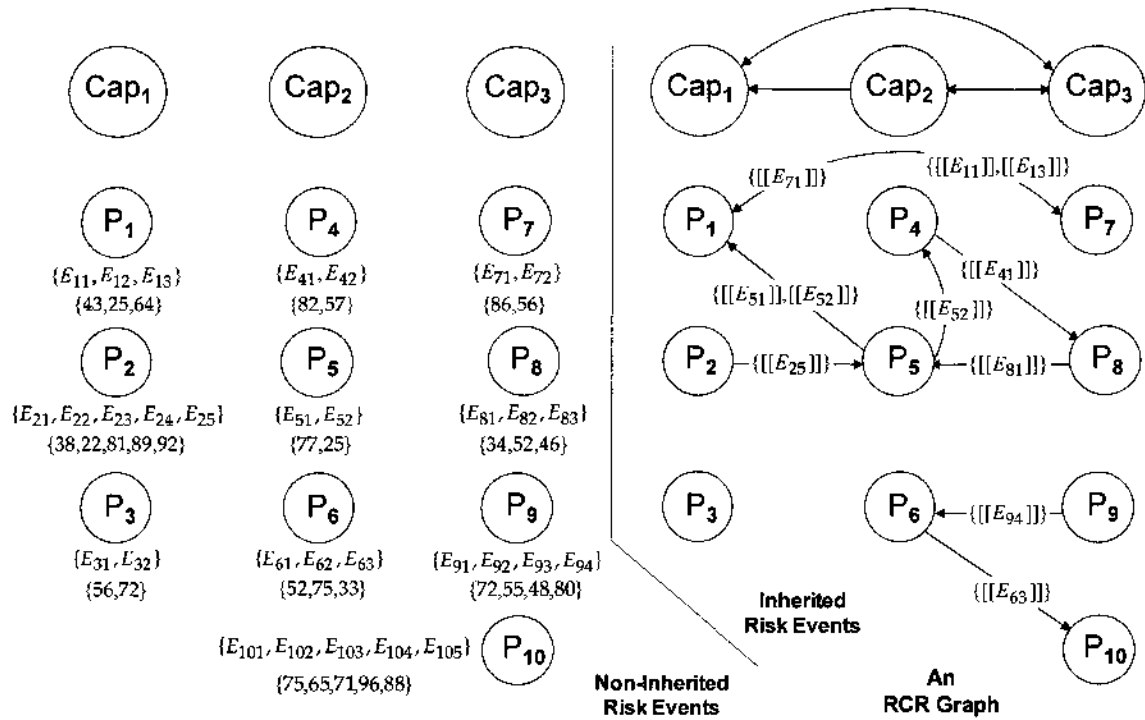


Figure 37. Example 4.3 RCR Graph: Non-Inherited and Inherited Risk Events

Figure 37 shows ten supplier program nodes providing contributions to three capability nodes. Here, program nodes within a capability node need not be unique to that capability. In practice, the same program node may appear beneath multiple capability nodes if the technology program represented by that node is supplying multiple contributions to those capabilities. For example, program node  $P_2$  might be the same technology program as program node  $P_6$ , but it is supplying multiple contributions to capability node  $Cap_1$  and  $Cap_2$ .

In Figure 37 and Table 2 observe that program node  $P_1$  has three non-inherited risk events  $E_{11}$ ,  $E_{12}$ , and  $E_{13}$  and three inherited risk events  $[[E_{71}]]$ ,  $[[E_{51}]]$ , and  $[[E_{52}]]$ . These inherited events come from program nodes  $P_5$  and  $P_7$ . Suppose risk scores for these six risk events are given below and were computed by Equation 4.1.

$$\{RS(E_{11}), RS(E_{12}), RS(E_{13})\} = \{43, 25, 64\}$$

$$\{RS([[E_{71}]]), RS([[E_{51}]]), RS([[E_{52}]])\} = \{86, 77, 25\}$$

| Program Node | Non-Inherited Risk Event Risk Scores | Inherited Risk Event Risk Scores | $RS(P_i \sim I)$ | $RS(P_i I)$ | $RS(P_i \sim I \wedge I)$ | $RCR(P_i)$ |
|--------------|--------------------------------------|----------------------------------|------------------|-------------|---------------------------|------------|
| $P_1$        | {43, 25, 64}                         | {86, 77, 25}                     | 56.8             | 79          | 75.67                     | 0.249      |
| $P_2$        | {38, 22, 81, 89, 92}                 | None                             | 83.72            | —           | —                         | 0*         |
| $P_3$        | {56, 72}                             | None                             | 69.6             | —           | —                         | 0*         |
| $P_4$        | {82, 57}                             | {25}                             | 78.25            | 25          | 78.25                     | 0          |
| $P_5$        | {77, 25}                             | {92, 34}                         | 69.2             | 83.3        | 81.185                    | 0.148      |
| $P_6$        | {52, 75, 33}                         | {80}                             | 68.5             | 80          | 78.275                    | 0.125      |
| $P_7$        | {86, 56}                             | {43, 64}                         | 81.5             | 60.22       | 81.5                      | 0          |
| $P_8$        | {34, 52, 46}                         | {82}                             | 48.16            | 82          | 76.924                    | 0.374      |
| $P_9$        | {72, 55, 48, 80}                     | None                             | 75.125           | —           | —                         | 0*         |
| $P_{10}$     | {75, 65, 71, 96, 88}                 | {33}                             | 90.9             | 33          | 90.9                      | 0          |

\* By Definition 4.7, if inheritance is not present between program nodes then  $RCR(P_i)$  is defined to equal zero.

Table 2. Example 4.3 Data and Computations: The Influence of Risk Inheritance

From Equation 4.3 and Equation 4.4, program node  $P_1$ 's risk scores are as follows:

$$RS(P_1|\sim I) = \text{MaxAve}(\{RS(E_{11}), RS(E_{12}), RS(E_{13})\}) = \text{MaxAve}(\{43, 25, 64\}) = 56.8$$

$$RS(P_1|I) = \text{MaxAve}(\{RS([E_{71}]), RS([E_{51}]), RS([E_{52}])\}) = \text{MaxAve}(\{86, 77, 25\}) = 79$$

From Equation 4.5, the risk score of program node  $P_i$ , when  $P_i$  is characterized by a finite set of non-inherited and inherited risk events is

$$RS(P_i|\sim I \wedge I) = \begin{cases} RS(P_i|\sim I) & \text{if } Z_1 \text{ is true} \\ \text{MaxAve}(RS(P_i|\sim I), RS(P_i|I)) & \text{if } Z_2 \text{ is true} \end{cases}$$

where,  $Z_1$  is when  $P_i$  has non-inherited and inherited risk events and  $RS(P_i|I) \leq RS(P_i|\sim I)$  (in accordance with Postulate 4.3);  $Z_2$  is when  $P_i$  has non-inherited and inherited risk events and  $RS(P_i|\sim I) < RS(P_i|I)$ .

From the above, since  $RS(P_1|\sim I) < RS(P_1|I)$  the combined risk score of program node  $P_1$  is

$$RS(P_1|\sim I \wedge I) = \text{MaxAve}(56.8, 79) = 75.67$$

Thus, the risk co-relationship index of  $P_1$  is

$$RCR(P_1) = \frac{RS(P_1|\sim I \wedge I) - RS(P_1|\sim I)}{RS(P_1|\sim I \wedge I)} = \frac{75.67 - 56.8}{75.67} = 0.249$$

The computations shown in Table 2 for the other nine program nodes were completed in a similar manner. To the capability portfolio manager, and to the portfolio's individual program managers, inherited risks are first targets for resolution or elimination. Seen in Figure 37, inherited risk events extend their threat to other programs beyond their originating program nodes.

Inheritance complicates program-to-portfolio cross-coordination, collaboration, and resolution planning. Multiple stakeholders, users, and outcome goals of affected program and capability nodes must be jointly considered when planning and executing resolution strategies for inherited risks. Thus, from a criticality perspective inherited risk events are signaled as prime targets for early management attention and intervention.

Table 3 shows the computational results of each capability node's risk score as a function of the relationships shown in Figure 37 and the program node risk scores derived in Table 2.

| Capability Node | Program Node Risk Score Set  | Capability Node Risk Score $RS(C_k)$ | $RCR(C_k)$ |
|-----------------|------------------------------|--------------------------------------|------------|
| $C_1$           | {75.67, 83.72, 69.6}         | 81.503                               | 0.02315    |
| $C_2$           | {78.25, 81.185, 78.275}      | 80.601                               | 0.0525     |
| $C_3$           | {81.5, 76.924, 75.125, 90.9} | 87.964                               | 0.0245     |

Table 3. The Influence of Risk Inheritance on C-Node Risk Scores

For example, the risk score and the risk co-relationship index for capability node  $C_2$  are formulated from Equation 4.6, Equation 4.8, Figure 37, and Table 2 as follows:

$$Risk\ Score\ (C_2) = RS(C_2) = MaxAve\ (\{RS(P_4|\sim I \wedge I), RS(P_5|\sim I \wedge I), RS(P_6|\sim I \wedge I)\})$$

$$= RS(C_2|\sim I \wedge I) = MaxAve\ (\{78.25, 81.185, 78.275\}) = 80.601$$

Here,  $RS(C_2|\sim I \wedge I)$  is the risk score of capability node  $C_2$  computed over its set of P-node risk scores that include the influence of inheritance (Table 2). The risk co-relationship index of capability node  $C_2$  is then computed, from Equation 4.8, as follows:

$$RCR(C_k) = \frac{RS(C_k|\sim I \wedge I) - RS(C_k|\sim I)}{RS(C_k|\sim I \wedge I)}$$

$$RCR(C_2) = \frac{RS(C_2|\sim I \wedge I) - RS(C_2|\sim I)}{RS(C_2|\sim I \wedge I)} = \frac{80.601 - \text{MaxAve}(\{78.25, 69.2, 68.5\})}{80.601}$$

$$RCR(C_2) = \frac{RS(C_2|\sim I \wedge I) - RS(C_2|\sim I)}{RS(C_2|\sim I \wedge I)} = \frac{80.601 - 76.37}{80.601} = 0.0525$$

Observe that a capability node's risk co-relationships are *indirect*. They derive only from risk co-relationships that exist *directly* between supplier program nodes in the portfolio. So, a capability node's RCR index is really a *response measure* – one that derives from the effects of risk event inheritance between P-nodes that comprise the supplier dimensions of the capability portfolio.

Figure 38 presents the nodal topology of Example 4.3 visualized by RCR indices between the program and capability nodes. With this, management can view time-history changes to these indices and quickly see where high risk co-relationships exist or remain between program and capability nodes. A rank-ordering from highest-to lowest-RCR index by program and capability nodes affected by inheritance can also be generated and monitored over time.

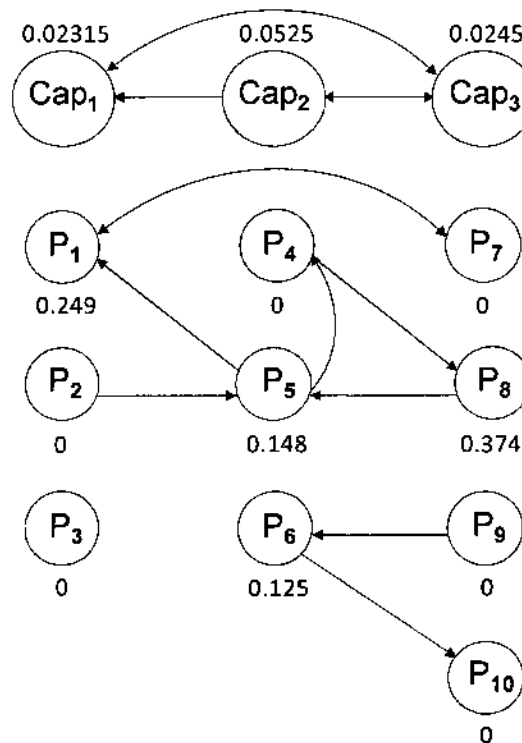


Figure 38. Example 4.3 Nodes: An RCR Index View



## APPLICATION TO RESOURCE ALLOCATION DECISIONS

This section illustrates an application of the RCR index to resource allocation decisions. Here, we integrate an operations research optimization algorithm into the theory of risk inheritance and the RCR index. The aim is to demonstrate a formal and analytically-traceable investment-decision protocol. This protocol works to identify which combination of program nodes offer the maximum reduction in capability risk when allocated risk resolution assets from a constrained risk resolution budget. These nodes will be the best among other program node candidates for management intervention and the investment of limited risk resolution funds.

The optimization algorithm discussed below falls into a class known as constrained optimization algorithms. It is informally known as the *knapsack model*.

### The Knapsack Optimization Algorithm

The knapsack problem is a classic problem in operations research. One form of this problem can be described as follows. Suppose you have a finite collection of items you want to pack into your knapsack. Suppose the knapsack has limited capacity so it is not possible to include all items. Suppose each item has a certain value (or utility) to you. Given this, which items can be included in the knapsack such that the value of its collection of items is maximized but does not exceed the knapsack's capacity?

### A Knapsack Problem Formulation

A classic knapsack problem can be mathematically formulated as follows.

$$\begin{aligned} &\text{Maximize } v_1x_1 + v_2x_2 + v_3x_3 + \dots + v_nx_n \\ &\text{subject to } w_1x_1 + w_2x_2 + w_3x_3 + \dots + w_nx_n \leq K \end{aligned}$$

where  $x_i$  for  $i = 1, 2, 3, \dots, n$  takes the value 0 if item  $x_i$  is not included in the knapsack and takes the value 1 if item  $x_i$  is included in the knapsack. The parameter  $w_i$  is the weight (e.g., in pounds) of item  $x_i$  and  $K$  is the overall weight capacity of the knapsack.

The first equation is called the objective function. The second equation is called the constraint (or constraint equation). Solving the knapsack problem involves *integer programming* – a specialized optimization technique. The Microsoft® Excel Solver program can be used to find solutions to the knapsack problem. The following illustrates this in the problem context of this dissertation.

Instead of a knapsack, let's think of the problem of choosing which P-nodes to include in a risk resolution portfolio. However, suppose this portfolio is defined by a fixed budget for funding P-nodes to resolve their risks. The decision problem is to select those P-nodes that have the highest threat to their associated capability while not exceeding the overall risk resolution budget. As mentioned above, we can think of this as a knapsack problem. The mathematical set up is as follows.

Let  $j = \{1, 2, 3, \dots, n\}$  be a set indexing the candidate P-nodes (*note: subscripts here are local to this knapsack formulation*). Let

$$x_j = \begin{cases} 0 & \text{if } j\text{th P-node is not in the risk resolution portfolio} \\ 1 & \text{if } j\text{th P-node is in the risk resolution portfolio} \end{cases}$$

Here, we want to

$$\begin{aligned} &\text{Maximize } v_1x_1 + v_2x_2 + v_3x_3 + \dots + v_nx_n \\ &\text{subject to } c_1x_1 + c_2x_2 + c_3x_3 + \dots + c_nx_n \leq C \end{aligned}$$

where  $v_j$  is the RCR index of  $j$ -th P-node,  $c_j$  is the cost to resolve the risk events that comprise the  $j$ -th P-node, and  $C$  is the total risk resolution budget.

Table 4 illustrates this application in the context of ten P-nodes described in Example 4.3. Table 2 presents the risk scores of these P-nodes. Suppose the columns of the Table 4 are the ten P-nodes all competing for limited risk resolution resources. Suppose the total risk resolution budget is 20 million dollars. However, the cost to resolve the risks in all ten P-nodes is just over 36 million dollars (36.225 million dollars).

Furthermore, suppose management decided the risk resolution budget should only be allocated to P-nodes with risk scores greater than or equal to 70. The reasoning being that P-nodes with risk scores equal to or higher than 70 fall into a “RED” color zone and, as such, are those that most threaten capability.

Given this, which P-nodes should be included in the “risk resolution portfolio” such that they collectively offer the maximum reduction in potential threat to capability while not exceeding the 20 million dollar budget and maintaining a risk score equal to or greater than 70?

| Optimization Input Matrix                   | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID |
|---|-----------------|-----------------|-----------------|-----------------|-----------------|
|   | 1               | 2               | 3               | 4               | 5               |
| Objective Function: P-Node RCR Index        | 0.249           | 0               | 0               | 0.000           | 0.148           |
| Subject To Constraint: Risk Resolution Cost | 5900            | 2300            | 4321            | 7656            | 2132            |
| Optimization Input Matrix                   | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID |
|   | 6               | 7               | 8               | 9               | 10              |
| Objective Function: P-Node RCR Index        | 0.125           | 0               | 0.374           | 0               | 0               |
| Subject To Constraint: Risk Resolution Cost | 6241            | 1325            | 3127            | 2112            | 1111            |

Table 4. P-Node Input Matrix

To find the optimal collection of P-nodes to include in the risk resolution portfolio, given the above conditions, we can model this situation as a “knapsack” problem. Here, the coefficients of the objective function are the RCR indexes of the P-nodes. The coefficients of the constraint equation are the resolution costs (in dollars-thousands) of these P-nodes. For example, P-node 1 has an RCR index of 0.249 and a risk resolution cost of 5.9 million dollars.

Here, we use the Microsoft® Excel Solver program to solve this optimization problem. The results from Solver are shown in Table 5. The P-nodes indicated by a “1” in the solution matrix are those to be funded. The P-nodes indicated by a “0” in the solution matrix are those not to be funded. Here, P-nodes 1, 5, 6, 7, 8, and 10 are the optimal collection of P-nodes to include in the risk resolution portfolio. Program nodes 2, 3, 4, and 9 are not funded.

This mix of funded P-nodes is the optimal combination of P-nodes to allocate resources that (1) offer the largest reduction in effects of risk co-relationships in the capability portfolio and (2) comes as close as possible, while not exceeding, the total risk resolution budget of 20 million dollars. The risk resolution costs for all P-nodes selected for investment sum to 19.836 million dollars. The values in row three of Table 5 are the P-node risk scores, as derived and summarized in Table 2.

| Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID | Program Node ID |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| 1               | 2               | 3               | 4               | 5               | 6               | 7               | 8               | 9               | 10              |
| 1               | 0               | 0               | 0               | 1               | 1               | 1               | 1               | 0               | 1               |
| 75.670          | 83.720          | 69.600          | 78.250          | 81.185          | 78.275          | 81.500          | 76.924          | 75.125          | 90.900          |
| 0.249           | 0               | 0               | 0               | 0.148           | 0.125           | 0               | 0.374           | 0               | 0               |
| 5900            | 2300            | 4321            | 7656            | 2132            | 6241            | 1325            | 3127            | 2112            | 1111            |

Table 5. P-Node Solution Matrix

The approach described in this section illustrates a formal way to allocate limited risk resolution resources to P-nodes considered most threatening to capability. Analytical approaches such as these are valuable “first-filters” that *support* decision-making.

They are not replacements for human judgment or creative crisis or intervention management. Leadership should always look at results such as these and consider additional tradeoffs, options, or creative ways to address critically impacting P-nodes, given constraints such as a fixed risk resolution budget. One way to use this analysis is to let it form the basis for debating why, where, and when increased resources are needed. This approach reveals not only those P-nodes that can be included in a budget but those that, without relaxing constraints or finding workarounds, must be excluded.

## SUMMARY

Developing ways to represent and measure capability dependencies in the engineering of enterprise systems is a critically important aspect of enterprise risk management. The importance of this problem is many-fold. Primary is enabling management to study ripple effects of failure in one capability on other dependent capabilities. Offering ways to study these effects enables engineers to design for minimizing dependency risks that, if realized, have cascading negative effects on the ability of an enterprise to deliver services to consumers.

The problem investigated herein focused on one form of dependency – risk inheritance between supplier programs in a capability portfolio. This work investigated and rigorously developed an index for measuring risk inheritance among supplier programs and capabilities. The risk co-relationship index identifies and captures the impacts of this type inheritance dependency on the increased risk that program nodes will fail to deliver their contributions to their associated capabilities.

Mathematical graph theory offers a useful representation formalism for capturing and analyzing risk inheritance in engineering enterprise systems. Within the concept of a graph, algorithms and new theorems were created to produce the risk co-relationship index. As shown, this index measures the influence of risk inheritance between program nodes supplying technologies to capabilities. The risk co-relationship index is fully generalized with respect to permitting risk events to be horizontally or vertically inherited between supplier program nodes. The risk co-relationship index, and ways to measure risk inheritance across a capability portfolio, is an original contribution to the engineering management community.

Last, connecting the mathematical theory developed for the risk co-relationship index with that of investment decision management enables decision-makers to optimally assign resources to just those P-nodes that offer the maximum reduction in inheritance effects, given funding constraints. This enables portfolio management to time-history monitor reductions in capability risk, as driven by inheritance, when more and more risk reduction dollars are judiciously applied in optimally decision-theoretic ways.

## CHAPTER V

### FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA)

#### INTRODUCTION

Critical considerations in engineering enterprise systems are identifying, representing, and measuring dependencies between suppliers of technologies and providers of services to consumers and users. The importance of this problem is many-fold. Primary is enabling the study of ripple effects of failure in one capability on other dependent capabilities across the enterprise. Providing mechanisms to anticipate these effects early in design enables engineers to minimize dependency risks that, if realized, can have cascading negative effects on the ability of an enterprise to deliver services to users.

The approach to this problem, described herein, is built upon concepts from graph theory. Graph theory enables (1) a visual representation of complex interrelationships between entities and (2) the design of analytical formalisms that trace the effects of dependencies between entities as they affect many parts and paths in a graph.

In this context, a capability portfolio is represented as a *directed graph* whose entities are nodes that depict the direction, strength, and criticality of supplier-provider relationships. Algorithms are designed to measure capability operability (or inoperability) due to degraded performance (or failure) in supplier and program nodes within a capability portfolio.

Capturing and analyzing dependencies is not new in systems engineering. New is tackling this problem (1) in an enterprise systems engineering context where horizontal and vertical dependencies can exist at many levels in a capability portfolio and (2) by creating a flexible analysis and measurement approach applicable to any capability portfolio, whose supplier-provider relationships can be represented by graph theoretic formalisms.

In Chapter IV, the Risk Co-Relationship (RCR) index was developed and presented. The RCR index is a management metric that measures risk inheritance between supplier programs and its ripple effects across a capability portfolio. The index identifies and captures horizontal and vertical impacts of risk inheritance, as it increases the threat that risks on one supplier program may adversely affect others and ultimately their contributions to their associated capabilities.

The higher the RCR index the greater the degree risks are co-related between supplier-programs. The lower the RCR index the lesser the degree risks are co-related between supplier programs. Thus, to the capability portfolio manager inherited risks might be “first” targets for resolution or elimination.

The methodology in this chapter is named *Functional Dependency Network Analysis* (FDNA). Its formulation is motivated, in part, by concepts from Leontief Matrices, Inoperability Input-Output Models (IIM), and Failure Modes and Effects Analysis (FMEA). These concepts are described in Y. Y. Haimes (2004).

The FDNA is a methodology that enables management to study and anticipate the ripple effects of losses in supplier-program contributions on dependent capabilities before risks that threaten these suppliers are realized. Where the RCR index identifies which supplier programs face high risk (incorporating effects of risk inheritance) in delivering their contributions to capability, the FDNA analysis identifies whether the level of operability loss, if such risks occur, is acceptable. This enables management to better target risk resolution resources to those supplier programs that face high risk and are most critical to the operational capabilities of a portfolio.

Together, the RCR index and the FDNA methodology address the following:

*How risk-dependent are capabilities so threats to them can be discovered **before** contributing programs (e.g., suppliers) degrade, fail, or are eliminated?*

and

*What is the effect on the operability of capability **if**, due to the realization of risks, one or more contributing programs or supplier-provider chains degrade, fail, or are eliminated?*

### FDNA FUNDAMENTALS AND POSTULATES

This section introduces the Functional Dependency Network Analysis (FDNA) methodology and its essential ideas on ways to model and measure operational dependencies in a portfolio.

The idea behind FDNA is best illustrated by the graph in Figure 39. Here, a simple capability portfolio is shown. It consists of three capability nodes and six program nodes. Mathematically, Figure 39 illustrates a special type of graph known as a directed graph.

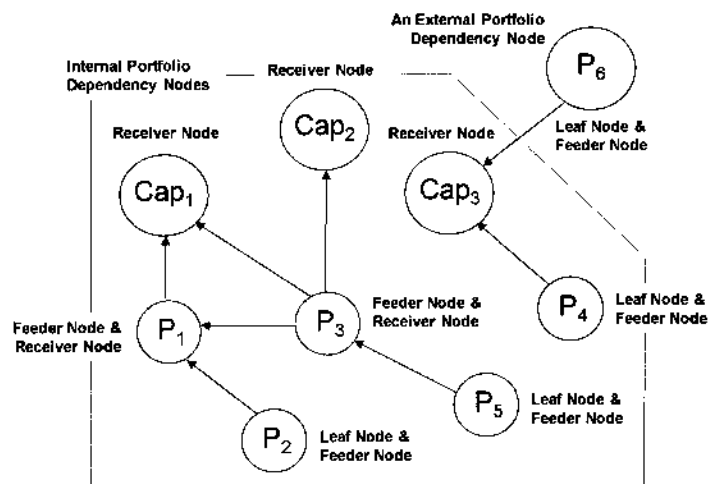


Figure 39. An FDNA Graph: A Capability Portfolio Context

In general, a graph is defined as a collection of points and lines connecting some (possibly empty) subset of them. The points of a graph are known as vertices or nodes. The lines connecting the vertices are known as edges or arcs\*.

\* Reference: This text excerpted from <http://mathworld.wolfram.com/Graph.html>.

The lines of graphs can have directedness. Arrows on one or both endpoints of a graph indicate directedness. Such a graph is said to be *directed*. A graph or directed graph together with a function which assigns a positive real number to each line is known as a *network*<sup>\*</sup>. An FDNA graph is a directed graph and later we'll see it is also a network.

A graph may also be viewed in terms of parent-child relationships. A *parent node* is one with lower-level nodes coming from it. These nodes are called *child nodes* to that parent node. Nodes that terminate in a network are sometimes called *leaf nodes*. Leaf nodes are terminal nodes in that they have no children coming from them [Garvey, 2008].

Next, we'll take a closer look at the graph in Figure 39. From this we'll introduce key FDNA definitions and behavioral properties of supplier-provider dependencies.

### FDNA Fundamentals

We begin with a discussion of dependence and what it means in the FDNA methodology. In an FDNA graph, dependence is a condition that exists between two nodes when the operability of one node relies, to some degree, on the operability of another node. What is meant by operability?

In FDNA, operability is a measure of the value of a node's output. It is a vNM utility measure expressed as "utils". For example, a node that produces 60 widgets per hour might have this level of performance valued at 50 utils; or equivalently, its operability level is 50.

In FDNA, a node's operability level is defined to range from 0 to 100 utils. A node is wholly inoperable if its operability level is 0 utils. A node is wholly operable if its operability level is 100 utils. In FDNA, as a node's operability level increases so does the utility of its output.

An FDNA graph can be viewed as a topology of receiver-feeder node relationships. A receiver node is one whose operability level relies, to some degree, on the operability level of at least one feeder node. In FDNA, a node may be a feeder and a receiver node as shown in Figure 40.

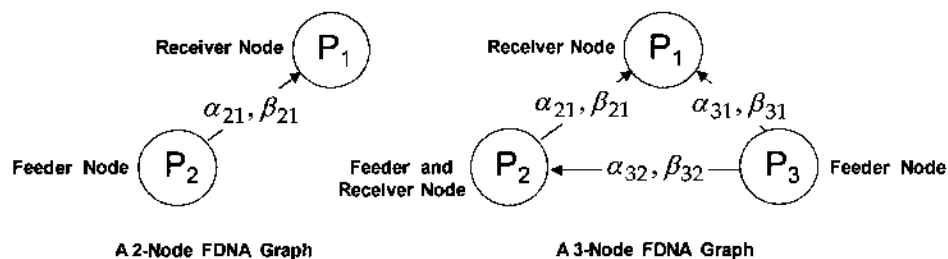


Figure 40. A 2- and 3-Node FDNA Graph

In FDNA, a receiver node's operability level is influenced by two types of dependencies. The first type is the strength with which a receiver node's operability level relies, to some degree, on the operability level of a feeder node. The second is the criticality of the feeder node's contribution to the receiver node for it to ultimately achieve its operability level objectives.

<sup>\*</sup> Reference: This text excerpted from <http://mathworld.wolfram.com/Graph.html>.

We call these types of dependencies the *strength of dependency* and the *criticality of dependency*. They are governed by two parameters  $\alpha_{ij}$  and  $\beta_{ij}$ , respectively. Here,  $i$  is the index of a feeder node that a receiver node of index  $j$  depends on.

Strength of dependency and criticality of dependency capture different aspects of feeder-to-receiver node relationships. Each is important and both influence receiver node operability levels and the achievement of the utility of the node's overall outcome.

### Strength of Dependency (SOD)

**Definition 5.1:** Strength of dependency is the operability level (utils) a receiver node relies on receiving from a feeder node for the receiver node to *continually increase* its baseline operability level and ensure the receiver node is wholly operable when its feeder node is wholly operable.

The strength of dependency with which receiver node  $P_j$  relies on feeder node  $P_i$  is governed by the parameter  $\alpha_{ij}$ , where  $0 < \alpha_{ij} \leq 1$ . This parameter will also be referred to as the *strength of dependency fraction*. If  $\alpha_{ij} = 1$ , then receiver node  $P_j$  is wholly dependent on feeder node  $P_i$  for its operability. In this case, the operability level of the receiver node is equal to the operability level of its feeder node – the receiver node has no operability independent of the operability of its feeder node. The parameter  $\alpha_{ij}$  is always greater than zero; otherwise, no dependency would exist between receiver node  $P_j$  and feeder node  $P_i$ .

Figure 41 shows a 2-node strength of dependency view of an FDNA graph. Here, receiver node  $P_j$  is  $\alpha_{ij}$ -dependent on feeder node  $P_i$ . The greater the value of  $\alpha_{ij}$  the greater the strength of dependency that  $P_j$  has on  $P_i$  and the less  $P_j$ 's operability level is independent of  $P_i$ 's level. The smaller the value of  $\alpha_{ij}$  the lesser the strength of dependency that  $P_j$  has on  $P_i$  and the more  $P_j$ 's operability level is independent of  $P_i$ 's level.

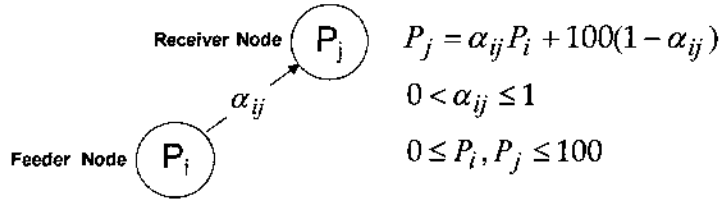


Figure 41. A 2-Node FDNA Graph: Strength of Dependency (SOD) View

An equation that behaves with these properties is given by Equation 5.1.

$$P_j = \alpha_{ij} P_i + 100(1 - \alpha_{ij}), \quad 0 \leq P_i, P_j \leq 100, \quad 0 < \alpha_{ij} \leq 1 \quad (5.1)$$

Equation 5.1 is the *Strength of Dependency* equation of receiver node  $P_j$  on feeder node  $P_i$ . The first term  $\alpha_{ij} P_i$  is the amount of feeder node  $P_i$ 's operability (utils) that receiver node  $P_j$  depends on receiving for  $P_j$ 's operability (utils) to improve the baseline utility of its outputs. The second term  $100(1 - \alpha_{ij})$  is expressed in utils. It is defined as  $P_j$ 's baseline operability level (BOL) prior to receiving feeder node  $P_i$ 's operability, in terms of added utility. Thus, from a strength of dependency view, a receiver node will *always* increase in operability above its BOL whenever its feeder node has an operability level greater than zero.



From the preceding discussion, the terms in Equation 5.1 can be viewed as shown in Figure 42.

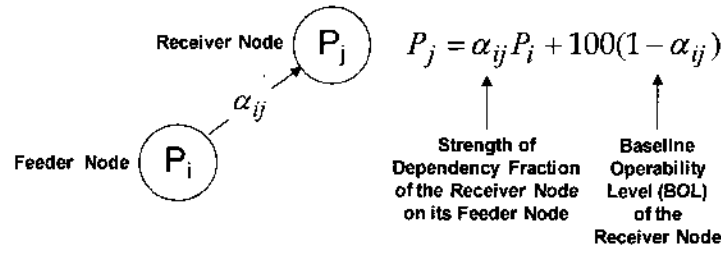


Figure 42. A 2-Node FDNA Graph: View by SOD Fraction  $\alpha_{ij}$  and BOL

In Equation 5.1, if receiver node  $P_j$ 's baseline operability level is zero then  $P_j$ 's operability level is wholly dependent on feeder node  $P_i$ 's operability level. This implies  $\alpha_{ij} = 1$  since  $100(1 - \alpha_{ij}) = 0$  utils, in this case. With this, Equation 5.1 reduces to

$$P_j = 1 \cdot P_i + 100(1 - 1) = P_i, \quad 0 \leq P_i, P_j \leq 100$$

When receiver node  $P_j$  is wholly dependent on feeder node  $P_i$  the strength of dependency parameter  $\alpha_{ij}$  is at its maximum; that is,  $\alpha_{ij} = 1$ . Here, we have the condition "as  $P_i$  goes so goes  $P_j$ ".

In Equation 5.1, if feeder node  $P_i$  is wholly inoperable ( $P_i = 0$ ) then the receiver node's operability level is equal to its baseline level; that is,

$$P_j = 100(1 - \alpha_{ij}) = BOLP_j \text{ utils}$$

If feeder node  $P_i$  is wholly operable ( $P_i = 100$ ) then receiver node  $P_j$  is wholly operable since

$$P_j = \alpha_{ij}(100) + 100(1 - \alpha_{ij}) = 100 \text{ utils}$$

which is in accordance with Definition 5.1. From this, we see that the lower a receiver node's baseline operability level the higher its strength of dependency on contributions from feeder nodes to achieve an operability level of 100 utils. Likewise, the higher a receiver node's baseline operability level the lower its strength of dependency on contributions from feeder nodes to achieve an operability level of 100 utils.

In FDNA, the strength of dependency equation between a receiver node and a feeder node is defined by an increasing linear function of their operability levels. A linear function was chosen for this first version of FDNA because of its "utility-neutral" qualities. Future research into non-linear monotonically increasing functions could be explored.

Is the strength of dependency equation all that is needed in an FDNA operability analysis? What if a receiver node degrades from its baseline operability level unless its feeder node achieves a specified level of operability? Next, we introduce into the FDNA calculus a concept called *criticality of dependency*.

### Criticality of Dependency (COD)

First, we will motivate the concept of criticality of dependency with a story. This will be followed by a technical discussion of criticality of dependency and how this influence is incorporated into the FDNA methodology. Consider the 2-node FDNA graph in Figure 43.

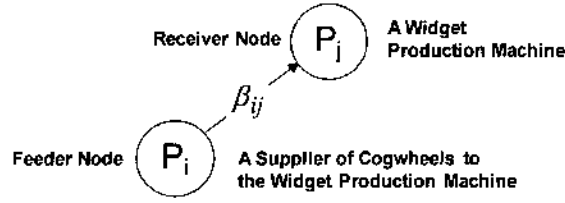


Figure 43. A 2-Node FDNA Graph: Criticality of Dependency View

Suppose receiver node  $P_j$  is a widget production machine. Suppose feeder node  $P_i$  manufactures new cogwheels ideal for lowering mechanical stress and increasing the output of the widget production machine.

With the contribution from  $P_i$  suppose this machine can produce up to 90 widgets per hour and at this level of performance the machine is wholly operable. This means

$$P_j(90) = 100 \text{ utils}$$

Without the contribution from  $P_i$  suppose the machine can produce 60 widgets per hour and the value or worth of this level of performance is 50 utils. This means

$$P_j(60) = 50 \text{ utils} = BOLP_j$$

Suppose the widget production machine is old and without these new cogwheels the machine's parts will wear and its ability to produce 60 widgets per hour will degrade. Furthermore, suppose the machine's degraded level of performance is accompanied by a decline in its baseline operability level. Because of this, we say a criticality of dependency exists between receiver node  $P_j$  and its feeder node  $P_i$ .

In Figure 43, the parameter  $\beta_{ij}$  denotes a criticality of dependency exists between a receiver node  $P_j$  and its feeder node  $P_i$ . It is also the operability level (utils) a receiver node decreases to without its feeder node contribution. This story illustrated the concept of criticality of dependency. We now proceed with its formal definition.

**Definition 5.2:** Criticality of dependency is the operability level  $\beta_{ij}$  (utils) a receiver node degrades to from its baseline operability level without receiving its feeder node's contribution.

The criticality of dependency with which receiver node  $P_j$  relies on feeder node  $P_i$  is governed by the parameter  $\beta_{ij}$ , where  $\beta_{ij}$  is in utils and  $0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ . Observe that  $\beta_{ij}$  is bounded above by the BOL of receiver node  $P_j$ . Later, we will derive this result. Meanwhile, why is this intuitive?

If  $\beta_{ij} = 100(1 - \alpha_{ij})$  then receiver node  $P_j$  improves its baseline operability level whenever the operability level of feeder node  $P_i$  is greater than zero. Recall this is a characteristic property of strength of dependency. However, when  $\beta_{ij} = 100(1 - \alpha_{ij})$  we shall see the strength of dependency and criticality of dependency between  $P_j$  and  $P_i$  are no longer distinguishable and either will determine the operability level of  $P_j$ . What does the minimum value of  $\beta_{ij}$  mean?

When  $\beta_{ij} = 0$  a maximum criticality of dependency exists with respect to the extent that receiver node  $P_j$  relies on feeder node  $P_i$ . Maximum criticality of dependency means the operability level of receiver node  $P_j$  is equal to the operability level of its feeder node  $P_i$ . Here, we have the condition “as  $P_i$  goes so goes  $P_j$ ”. Earlier, we saw this was possible under a strength of dependency when  $\alpha_{ij} = 1$ . This same condition can occur under a criticality of dependency when  $\beta_{ij} = 0$ .

An equation that behaves with these properties is given by Equation 5.2.

$$P_j = P_i + \beta_{ij}, \quad 0 \leq P_i, P_j \leq 100, \quad 0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij}) \quad (5.2)$$

Equation 5.2 is the *Criticality of Dependency* equation of  $P_j$  on feeder node  $P_i$ .

If a criticality of dependency exists between receiver node  $P_j$  and feeder node  $P_i$  then, from Equation 5.2, if  $P_i = 0$  then  $P_j = \beta_{ij}$ . Thus, if feeder node  $P_i$  is wholly inoperable then receiver node  $P_j$ 's operability level is equal to  $\beta_{ij}$ , which at most is equal to its BOL. If  $P_i = 100$  then  $P_j = 100 + \beta_{ij} = 100$  since  $0 \leq P_i, P_j \leq 100$ . Thus, if feeder node  $P_i$  is wholly operable then receiver node  $P_j$  is wholly operable, which is also consistent with Definition 5.1.

In FDNA, if a receiver node's operability relies (to some degree) on contributions from a feeder node, then a SOD is present between them. However, the presence of a SOD between a receiver node and a feeder node does not imply a criticality of dependency (COD) exists between them. From Definition 5.2, a COD is present between a receiver node and a feeder node only when the receiver degrades from its baseline operability level without receiving its feeder node's contribution.

#### Determining $\alpha_{ij}$ and $\beta_{ij}$

The following illustrates how  $\alpha_{ij}$  and  $\beta_{ij}$  can be determined from their respective definitions. For this, refer to the FDNA graph in Figure 44. We begin with  $\alpha_{ij}$ .

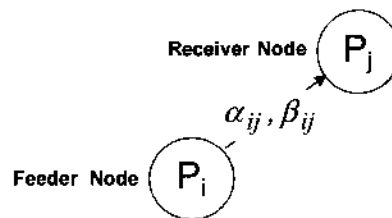


Figure 44. A 2-Node FDNA Graph: Strength and Criticality of Dependency View

With respect to Figure 44, to determine  $\alpha_{ij}$  one can ask the following question.

**SOD Question:** *What is the receiver node's baseline operability level (utility) prior to receiving its feeder node's contribution?*

If the answer is 0 utils, then  $\alpha_{ij} = 1$ . If the answer is 50 utils, then  $\alpha_{ij} = 0.50$ . If the answer is 70 utils, then  $\alpha_{ij} = 0.30$  and so forth. Thus,  $\alpha_{ij}$  can be solved from the expression

$$100(1 - \alpha_{ij}) = x$$

where  $x$  is the receiver node's baseline operability level (BOL) prior to receiving its feeder node's contribution.

With respect to Figure 44, to determine  $\beta_{ij}$  one can ask the following questions.

**COD Questions:** *If the feeder node's contribution is equal to zero in operational utility to the receiver node, then will the receiver node degrade from its baseline operability level (utility)? If yes, then to what operability level (utility) will the receiver node decline? If no, then no criticality of dependency exists between the receiver node and its feeder node.*

From Definition 5.2, recall that criticality of dependency is the operability level  $\beta_{ij}$  (utils) a receiver node degrades to without receiving its feeder node's contribution, where

$$0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$$

If the COD questions are **yes** "receiver node  $P_j$  **will degrade** from its BOL if  $P_i = 0$ ", then  $\beta_{ij}$  is set equal to the level of operability to which  $P_j$  will (or is anticipated to) decline. For instance, if  $\beta_{ij} = 0$  utils then the operability level of receiver node  $P_j$  is equal to the operability level of its feeder node  $P_i$ . Once again we see the condition "as  $P_i$  goes so goes  $P_j$ ", however, instead of seeing this through the earlier SOD perspective with  $\alpha_{ij} = 1$  we now see it from a COD perspective, with  $\beta_{ij} = 0$ . If  $\beta_{ij} = 20$  utils, then receiver node  $P_j$  degrades from its baseline operability level to 20 utils if feeder node  $P_i = 0$ . Note these examples are consistent with Equation 5.2.

If the COD question is **no** "receiver node  $P_j$  **will not degrade** from its BOL if  $P_i = 0$ ", then the operability level of  $P_j$  is determined solely by its strength of dependency on the operability level of  $P_i$ . This can be seen from the general SOD equation (Equation 5.1). From Equation 5.1, recall that

$$P_j = \alpha_{ij}P_i + 100(1 - \alpha_{ij}), \quad 0 \leq P_i, P_j \leq 100, \quad 0 < \alpha_{ij} \leq 1$$

If  $P_i = 0$  then the operability level of  $P_j$  is equal to  $100(1 - \alpha_{ij})$ . This is  $P_j$ 's BOL. Thus, when a dependency relationship is such that there is no degradation from  $P_j$ 's BOL when  $P_i = 0$  it follows there is only a strength of dependency between them. Finally, in a SOD relationship as feeder node  $P_i$  increases in operability ( $P_i > 0$ ) then receiver node  $P_j$  also increases in operability above its BOL by amounts governed by  $\alpha_{ij}$ , where  $0 < \alpha_{ij} \leq 1$ .

In summary, two types of dependencies have been discussed. They are *strength of dependency* and *criticality of dependency*. Each type captured different effects of receiver-feeder node relationships on their operability levels. Strength of dependency captured the effects of dependency relationships that improved baseline operability levels. Criticality of dependency captured whether dependency relationships could, in some situations, cause their baselines to degrade. FDNA permits this dualism to compete within its calculus to model positive or negative effects that complex receiver-feeder node interactions can have across a topology of multi-nodal relationships.

### **FDNA Postulates**

#### **Postulate 5.1: Operational Performance**

*All nodes can be characterized by a measure that expresses the achievement of a node's output.*

This may be a cardinal or ordinal measure of performance (MOP). For example, a communications node that achieves a data connectivity rate of 54 Mbps has a cardinal measured value (54 Mbps). A node that achieves a level of performance assessed by a rating level on a semantic differential scale (e.g., a "3" on a 1 – 5 Likert scale) has an ordinal measured value.

#### **Postulate 5.2: Operability**

*Operability is a state where a node is operationally performing.*

#### **Postulate 5.3: Operability Level**

*All nodes can be characterized by a measure of the value or worth of the outputs from their operational performance. This measure is a node's operability level.*

The operability level of a node is equivalent to a vNM utility measure. It can be considered a measure of effectiveness (MOE). Refer to Postulate 5.4 for an additional discussion.

#### **Postulate 5.4: Dependency and Acyclic Relationships**

*A dependency relationship exists between nodes when the operational performance of one node relies, to some degree, on the operational performance of other nodes. All FDNA graphs are acyclic\*.*

In this postulate, reliance refers to contributions to the dependent node from other nodes. Contributions are context specific to the nature of the supplying nodes. A contribution might be the delivery of widgets at a given production rate or the delivery of  $n$  electronic devices to a distribution node. How do we express contribution by a measure?

A contribution results from the achievement of an output by a node that reflects the operational performance of that node. For example, suppose a node manufactures widgets at a production rate of 60 widgets per hour. This rate is a measure of performance (MOP). Now, suppose this node's MOP translates to an operability level of 50 utils. This level is a measure of effectiveness (MOE). Thus, a node's MOP will have an accompanying measure of effectiveness (MOE). The MOE reflects the operability level, value, or worth of the output the node achieves.

---

\* A cycle relationship exists between nodes when there is a closed path between them (i.e., a path with the same first and last node). Acyclic graphs are graphs without cycles.

The following presents a set of key FDNA postulates.

**Postulate 5.5: Feeder Node**

*A feeder node is one that "feeds" contributions to one or more receiver nodes.*

**Postulate 5.6: Receiver Node**

*A receiver node is one that depends, to some degree, on contributions from one or more feeder nodes.*

**Postulate 5.7: Feeder and Receiver Node**

*A node can be a feeder node and a receiver node.*

**Postulate 5.8: Leaf Node**

*Leaf nodes are strictly feeder nodes.*

**Postulate 5.9: Not a Leaf Node**

*A node that is a feeder node and a receiver node is not a leaf node.*

**Postulate 5.10: Inoperable/Operable Node**

*A node is wholly inoperable if its operability level is zero. A node is wholly operable if its operability level is one-hundred.*

**Postulate 5.11: Receiver Node Operability**

*A receiver node may become wholly operable before its feeder node is wholly operable.*

**Postulate 5.12: Baseline Operability Level**

*The lower a receiver node's baseline operability level the higher its strength of dependency on feeder nodes to become wholly operable. Conversely, the higher a receiver node's baseline operability level the lower its strength of dependency on feeder nodes to become wholly operable.*

**FDNA GENERAL EQUATION, PROPERTIES, AND THEOREMS**

This section presents the FDNA fundamental equation used to determine a node's operability level. In addition, its formulation as a *composition of dependency functions* is illustrated from a simple 2-node FDNA graph to increasingly complex multi-nodal topologies.

**FDNA Fundamental Equation**

The FDNA fundamental equation is a formulation that jointly captures the operability level of receiver node  $P_j$  as a function of its strength of dependency and its criticality of dependency on feeder node  $P_i$  and the operability level of  $P_i$ . Its general expression is given by

$$P_j = F(\alpha_{ij}, \beta_{ij}, P_i) \quad 0 \leq P_i, P_j \leq 100 \quad (5.3)$$

where  $\alpha_{ij}$  and  $\beta_{ij}$  are, respectively, the strength and criticality of dependency parameters with which receiver node  $P_j$  relies on feeder node  $P_i$ . Equation 5.3 is called the *FDNA Dependency Function* (FDF). What form does this function take?

In accordance with Postulate 5.3,  $F(\alpha_{ij}, \beta_{ij}, P_i)$  is a vNM utility function. It can take a variety of functional forms that reflect increasing levels of operability of receiver nodes with increasing levels of operability in their feeder nodes. Some examples are shown in Figure 9.

This dissertation presents FDNA for the first time. As such, a linear form was selected for the FDF. As mentioned earlier, a linear form was chosen because of its “utility-neutral” qualities. Linear utility is a member of a class of functions known as power-additive utility functions [Kirkwood, 1997]. Families of power-additive utility functions are illustrated in Figure 9. Seen there, the linear form has a multiattribute risk tolerance of  $\rho_m = \infty$ . The linearity of FDF provides a point-of-departure for future research, where nonlinear monotonically increasing functions such as those in Figure 9 could be explored.

### An FDNA Dependency Function (FDF)

As mentioned above, we present the FDNA dependency function as a linear function of increasing operability (utils). Although the FDF is linear, it is defined by individual functions that can be nonlinear. Thus, the FDF can be a linear combination of nonlinear value functions\*.

Figure 45 illustrates a nonlinear value function for the operability level of an FDNA node. Suppose the node represents a widget production machine. The vertical axis is the machine’s operability level (utils) or MOE. The horizontal axis is the operational performance the machine achieves, as measured by the widget production rate. This axis reflects the node’s MOP.

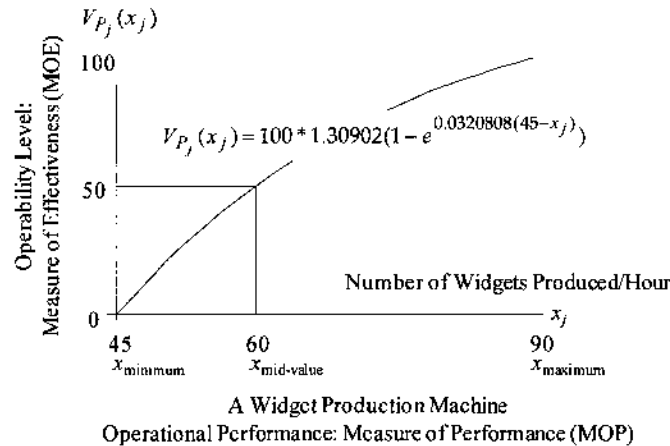


Figure 45. A Value Function for the Operability of Node  $P_j$

Figure 45 illustrates how an FDNA node’s operability level is a function of its operational performance. This demonstrates the relationship between these two measures, as discussed in Postulate 5.1 and Postulate 5.3. The following illustrates forming FDNA dependency functions for increasingly complex FDNA graphs by a *composition of functions* approach.

\* From a decision theory perspective, the FDF is technically a value function [Keeney, Raiffa, 1976]. A value function is a real-valued mathematical function defined over an evaluation criterion (or attribute) that represents an option’s measure of goodness over the levels of the criterion. A measure of goodness reflects a decision-maker’s judged value in the performance of an option across the levels of a criterion (or attribute) [Garvey, 2008].

**Example 5.1:** Formulating a 2,1,1-Node FDF

Figure 46 shows a 2-node FDNA graph with 1-dependency point and 1-receiver node. Let this be indicated by the notation 2,1,1-node.

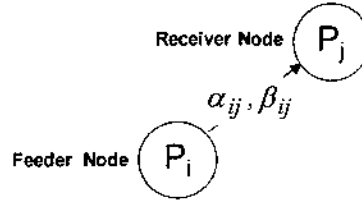


Figure 46. A 2,1,1-Node FDNA Graph

The FDNA dependency function formed for this relationship is given by Equation 5.4.

$$P_j = \text{Min} (SODP_j, CODP_j) = \text{Min} (\alpha_{ij}P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij}) \quad (5.4)$$

where  $\alpha_{ij}$  and  $\beta_{ij}$  are strength and criticality of dependency,  $P_i$  is the operability level of the receiver node's feeder node and  $0 < \alpha_{ij} \leq 1$ ,  $0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ , and  $0 \leq P_i, P_j \leq 100$ .

Equation 5.4 follows a principle known as the *weakest link*<sup>\*</sup>. In FDNA, the weakest link principle means the operability level of a receiver node is determined by the operability level derived from its weakest feeder node's strength of dependency or criticality of dependency.

**Example 5.2:** Formulating a 3,2,1-Node FDF

Figure 47 shows a 3-node FDNA graph with 2-dependency points and 1-receiver node. Let this be indicated by the notation 3,2,1-node.

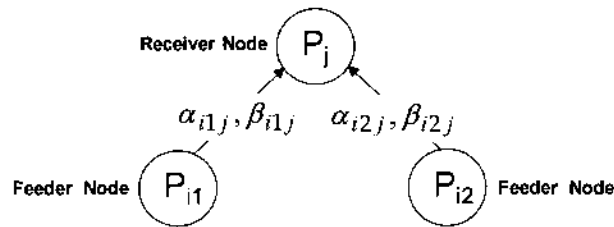


Figure 47. A 3,2,1-Node FDNA Graph

<sup>\*</sup> The weakest link principle asserts *no chain is stronger than its weakest link (non fortiter catena quam anulus debilissimus* [Rescher, 2006]). In philosophical logic it means "the status of a conclusion is that of the weakest premise" [Rescher, 2006]. Weakest link is known as a probative principle of rational cogency [Rescher, 2006].

The weakest link principle originates in Greek philosophy. It is attributed to Aristotle's pupil Theophrastus, who lived from 372 – 287 BC. Theophrastus was a Greek Peripatetic philosopher who became head of the Lyceum in Athens founded by Aristotle [Encyclopædia Britannica. Retrieved October 12, 2008, from Encyclopædia Britannica Online: <http://www.britannica.com/EBchecked/topic/590974/Theophrastus>]. For more on Theophrastus refer to *New World Encyclopedia*, <http://www.newworldencyclopedia.org>.



The FDNA dependency function formed for this relationship is given by Equation 5.5.

$$P_j = \text{Min} (\text{Average} (SODP_{ji1}, SODP_{ji2}), CODP_{ji1}, CODP_{ji2})$$

$$P_j = \text{Min} \left( \frac{\alpha_{i1j}P_{i1}}{2} + \frac{\alpha_{i2j}P_{i2}}{2} + 100(1 - (\frac{\alpha_{i1j} + \alpha_{i2j}}{2})), P_{i1j} + \beta_{i1j}, P_{i2j} + \beta_{i2j} \right) \quad (5.5)$$

where

$\alpha_{i1j}$  is the strength of dependency fraction between  $P_{i1}$  and  $P_j$

$\alpha_{i2j}$  is the strength of dependency fraction between  $P_{i2}$  and  $P_j$

$\beta_{i1j}$  is the criticality of dependency between  $P_{i1}$  and  $P_j$

$\beta_{i2j}$  is the criticality of dependency between  $P_{i2}$  and  $P_j$

$0 < \alpha_{i1j} \leq 1, 0 < \alpha_{i2j} \leq 1$

$0 \leq \beta_{i1j} \leq 100(1 - \alpha_{i1j}), 0 \leq \beta_{i2j} \leq 100(1 - \alpha_{i2j})$

$0 \leq P_{i1}, P_{i2}, P_j \leq 100$

**Example 5.3:** Formulating a 3,3,2-Node FDF

Figure 48 shows a 3-node FDNA graph with 3-dependency points and 2-receiver nodes. Let this be indicated by the notation 3,3,2-node.

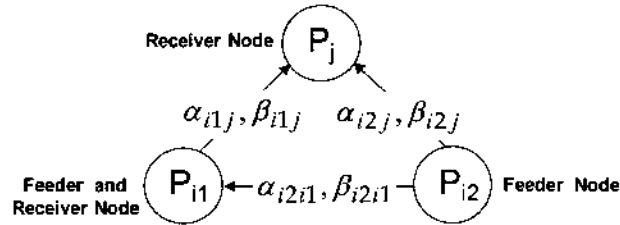


Figure 48. A 3,3,2-Node FDNA Graph

The FDNA dependency function formed for this relationship is given by Equation 5.6

$$P_j = \text{Min} \left( \frac{\alpha_{i1j}P_{i1}}{2} + \frac{\alpha_{i2j}P_{i2}}{2} + 100(1 - (\frac{\alpha_{i1j} + \alpha_{i2j}}{2})), P_{i1} + \beta_{i1j}, P_{i2} + \beta_{i2j} \right) \quad (5.6)$$

$$P_{i1} = \text{Min}(\alpha_{i2i1}P_{i2} + 100(1 - \alpha_{i2i1}), P_{i2} + \beta_{i2i1}) \quad (5.7)$$

where

$\alpha_{i1j}$  is the strength of dependency fraction between  $P_{i1}$  and  $P_j$

$\alpha_{i2j}$  is the strength of dependency fraction between  $P_{i2}$  and  $P_j$

$\alpha_{i2i1}$  is the strength of dependency fraction between  $P_{i1}$  and  $P_{i2}$

$$\begin{aligned}
&\beta_{i1j} \text{ is the criticality of dependency between } P_{i1} \text{ and } P_j \\
&\beta_{i2j} \text{ is the criticality of dependency between } P_{i2} \text{ and } P_j \\
&\beta_{i2i1} \text{ is the criticality of dependency between } P_{i1} \text{ and } P_{i2} \\
&0 < \alpha_{i1j} \leq 1, 0 < \alpha_{i2j} \leq 1, 0 < \alpha_{i2i1} \leq 1 \\
&0 \leq \beta_{i1j} \leq 100(1 - \alpha_{i1j}), 0 \leq \beta_{i2j} \leq 100(1 - \alpha_{i2j}), 0 \leq \beta_{i2i1} \leq 100(1 - \alpha_{i2i1}) \\
&0 \leq P_{i1}, P_{i2}, P_j \leq 100
\end{aligned}$$

For this FDNA graph there are two dependency equations. These are given by Equation 5.6 and Equation 5.7. Why does this graph have two equations?

In an FDNA graph, the number of dependency equations is equal to the number of receiver nodes. The FDNA graph in Figure 48 has two receiver nodes. These are  $P_j$  and  $P_{i1}$ . The operability level of  $P_j$  is a function of the operability level of  $P_{i1}$  and the operability level of  $P_{i2}$ . The operability level of  $P_{i1}$  is also a function of the operability level of  $P_{i2}$ . Hence, we have two dependency equations for this graph.

The preceding examples lead to the following notation definition.

**Definition 5.3:** The notation  $q,r,s$ -node denotes an FDNA graph with  $q$ -nodes,  $r$ -dependency points, and  $s$ -receiver nodes where  $q$ ,  $r$ , and  $s$  are positive integers.

**Example 5.4:** Formulating a 5,6,3-Node FDF

Figure 49 shows a 5-node FDNA graph with 6-dependency points and 3-receiver nodes. Let this be indicated by the notation 5,6,3-node.

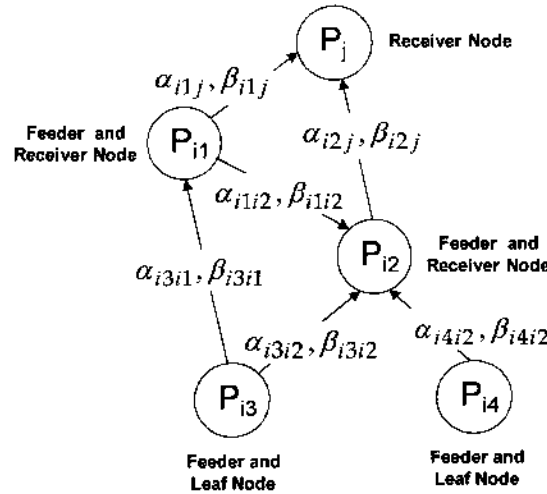


Figure 49. A 5,6,3-Node FDNA Graph

The FDNA dependency function formed for this relationship is given by Equation 5.8.

$$P_j = \text{Min} \left( \frac{\alpha_{i1j}P_{i1}}{2} + \frac{\alpha_{i2j}P_{i2}}{2} + 100(1 - (\frac{\alpha_{i1j} + \alpha_{i2j}}{2})), P_{i1} + \beta_{i1j}, P_{i2} + \beta_{i2j} \right) \quad (5.8)$$

$$P_{i1} = \text{Min}(\alpha_{i3i1}P_{i3} + 100(1 - \alpha_{i3i1}), P_{i3} + \beta_{i3i1}) \quad (5.9)$$

$$P_{i2} = \text{Min}(A, B) \quad (5.10)$$

$$A = \frac{\alpha_{i1i2}P_{i1}}{3} + \frac{\alpha_{i3i2}P_{i3}}{3} + \frac{\alpha_{i4i2}P_{i4}}{3} + 100(1 - (\frac{\alpha_{i1i2} + \alpha_{i3i2} + \alpha_{i4i2}}{3}))$$

$$B = \text{Min}(P_{i1} + \beta_{i1i2}, P_{i3} + \beta_{i3i2}, P_{i4} + \beta_{i4i2})$$

In this example, we have three receiver nodes and hence three dependency equations (Equations 5.8-5.10). The following presents the last example of formulating an FDF. This is presented from a capability portfolio context.

**Example 5.5: Formulating an FDF: A Capability Portfolio Perspective**

Figure 50 shows a simple capability portfolio. It consists of three capability nodes that have a mix of dependency relationships on six program nodes. Figure 50 can also be considered a 9,8,5-node FDNA graph.

Suppose program nodes supply various technologies that enable capabilities. Five of these program nodes fall within the capability portfolio's management authority, as indicated by nodes  $P_1$  through  $P_5$  in the "box". The node  $P_6$  illustrates that dependency relationships can also be external to the authority envelope of a portfolio. External dependencies can have as much influence on the operability of a capability as those from internal dependencies.

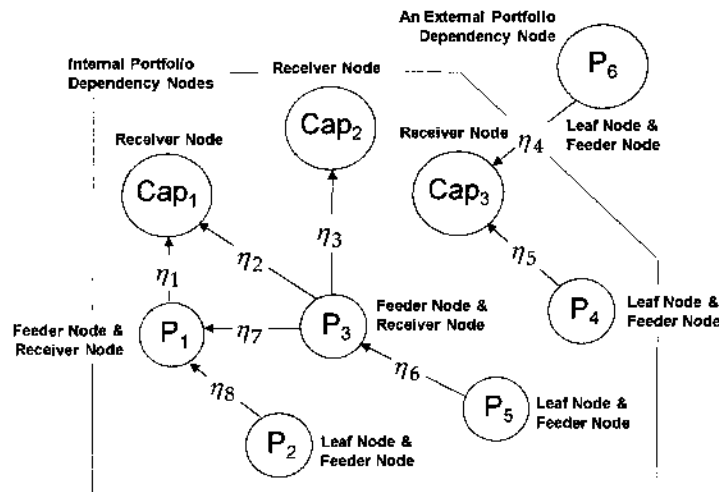


Figure 50. An FDNA Graph: From A Capability Portfolio Perspective

Figure 50 shows the symbol  $\eta$  on each arrow. This is for notational convenience to keep the figure less crowded. Let  $\eta$  indicate equivalence to the following FDNA parameters:

$$\begin{aligned}\eta_1 &\equiv \alpha_{P_1 Cap_1}, \beta_{P_1 Cap_1} & \eta_2 &\equiv \alpha_{P_3 Cap_1}, \beta_{P_3 Cap_1} \\ \eta_3 &\equiv \alpha_{P_3 Cap_2}, \beta_{P_3 Cap_2} & \eta_4 &\equiv \alpha_{P_6 Cap_3}, \beta_{P_6 Cap_3} \\ \eta_5 &\equiv \alpha_{P_4 Cap_3}, \beta_{P_4 Cap_3} & \eta_6 &\equiv \alpha_{P_5 P_3}, \beta_{P_5 P_3} \\ \eta_7 &\equiv \alpha_{P_3 P_1}, \beta_{P_3 P_1} & \eta_8 &\equiv \alpha_{P_2 P_1}, \beta_{P_2 P_1}\end{aligned}$$

Since this is a 9,8,5-node FDNA graph we form the following five FDF equations.

$$P_1 = \text{Min} \left( \frac{\alpha_{P_2 P_1} P_2}{2} + \frac{\alpha_{P_3 P_1} P_3}{2} + 100(1 - (\frac{\alpha_{P_2 P_1} + \alpha_{P_3 P_1}}{2})), P_2 + \beta_{P_2 P_1}, P_3 + \beta_{P_3 P_1} \right) \quad (5.11)$$

$$P_3 = \text{Min}(\alpha_{P_5 P_3} P_5 + 100(1 - \alpha_{P_5 P_3}), P_5 + \beta_{P_5 P_3}) \quad (5.12)$$

$$Cap_1 = \text{Min} \left( \frac{\alpha_{P_1 Cap_1} P_1}{2} + \frac{\alpha_{P_3 Cap_1} P_3}{2} + 100(1 - (\frac{\alpha_{P_1 Cap_1} + \alpha_{P_3 Cap_1}}{2})), P_1 + \beta_{P_1 Cap_1}, P_3 + \beta_{P_3 Cap_1} \right) \quad (5.13)$$

$$Cap_2 = \text{Min}(\alpha_{P_3 Cap_2} P_3 + 100(1 - \alpha_{P_3 Cap_2}), P_3 + \beta_{P_3 Cap_2}) \quad (5.14)$$

$$Cap_3 = \text{Min} \left( \frac{\alpha_{P_4 Cap_3} P_4}{2} + \frac{\alpha_{P_6 Cap_3} P_6}{2} + 100(1 - (\frac{\alpha_{P_4 Cap_3} + \alpha_{P_6 Cap_3}}{2})), P_4 + \beta_{P_4 Cap_3}, P_6 + \beta_{P_6 Cap_3} \right) \quad (5.15)$$

The FDNA graph in this example is a topology of multiple receiver-feeder node relationships. Here, five receiver node operability levels rely on the operability levels of a mix of other feeder-receiver nodes.

Example 5.5 is a simple capability portfolio. In practice, one can imagine a portfolio with a highly complex and intricate nodal topology. The power of the FDNA approach is its ability to operate across topologies of any complexity with only two defining parameters – strength and criticality of dependency between dependent nodes.

The preceding illustrated how the weakest link FDNA dependency function is formulated from a *composition of dependency relationships* in an FDNA graph. This leads to the following definition.

**Definition 5.4:** A Weakest Link Composition of the FDNA Dependency Function

The operability level of node  $P_y$  that is dependent on the operability levels of  $h$  other nodes  $P_1, P_2, P_3, \dots, P_h$  is given by

$$0 \leq P_y = \text{Min} (SODP_y, CODP_y) \leq 100 \quad (5.16)$$

where

$$SODP_y = \text{Average} (SODP_{y1}, SODP_{y2}, SODP_{y3}, \dots, SODP_{yh})$$

$$SODP_{yl} = \alpha_{ly} P_l + 100(1 - \alpha_{ly}), \quad 0 \leq P_l, P_y \leq 100, \quad 0 < \alpha_{ly} \leq 1, \quad l = 1, 2, 3, \dots, h$$

$$CODP_y = \text{Min} (CODP_{y1}, CODP_{y2}, CODP_{y3}, \dots, CODP_{yh})$$

$$CODP_{yl} = P_l + \beta_{ly}, \quad 0 \leq \beta_{ly} \leq 100(1 - \alpha_{ly})$$

From Equation 5.3, recall that the FDNA fundamental equation is given by

$$P_j = F(\alpha_{ij}, \beta_{ij}, P_i) \quad 0 \leq P_i, P_j \leq 100$$

The weakest link FDF defined by Equation 5.16 is a specific form of  $F(\alpha_{ij}, \beta_{ij}, P_i)$ ; that is,

$$P_j = F(\alpha_{ij}, \beta_{ij}, P_i) = \text{Min} (SODP_j, CODP_j) \quad (5.17)$$

In summary, FDNA can isolate nodes that drive loss of operability due to the realization of risks on supplier-provider chains. FDNA generates outputs that can be directly linked to an investment decision process. From a capability portfolio perspective, FDNA will identify which supplier nodes offer the highest rates-of-return when risk reduction investments in these nodes are made. This enables optimum investment choices to be made before unacceptable levels of operability loss occur. A detailed discussion of this analytical feature is presented later in this chapter. The following presents a set of fundamental properties of FDNA.

#### FDNA Fundamental Properties and Theorems

There are a number of fundamental properties and theorems associated with FDNA. The following presents these properties as they derive from *the weakest link FDF*.

**Property 5.1:** In an FDNA graph, if node  $P_j$  has maximum strength of dependency on node  $P_i$ , then  $P_j$  has maximum criticality of dependency on  $P_i$ 's contribution to  $P_j$ 's operability.

#### Proof

Since it is given that  $P_j$  has maximum strength of dependency on  $P_i$  it follows from Equation 5.1 the dependency fraction  $\alpha_{ij}$  is maximum; thus,  $\alpha_{ij} = 1$ . From Equation 5.2, criticality of dependency is governed by  $\beta_{ij}$ , where  $0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ . Since  $\alpha_{ij} = 1$ , it follows that

$$0 \leq \beta_{ij} \leq 0 \Rightarrow \beta_{ij} = 0$$

From Definition 5.2, criticality of dependency is the operability level  $\beta_{ij}$  (in utils) to which  $P_j$  degrades from its baseline operability level without receiving its contribution from  $P_i$ . If  $\beta_{ij} = 0$  then  $P_j$  degrades to zero utility; that is,  $P_j$  is wholly inoperable without  $P_i$ . Moreover, when  $\beta_{ij} = 0$  the operability level of  $P_j$  is equal to the operability level of  $P_i$  for  $0 \leq P_i \leq 100$ .

This can be seen from Equation 5.2 (criticality of dependency) where

$$P_j = P_i + \beta_{ij} = P_i + 0 = P_i, \text{ if } \beta_{ij} = 0$$

Thus,  $P_j$ 's operability level cannot be higher or lower than  $P_i$ 's operability level when  $\beta_{ij} = 0$ , where  $0 \leq P_i, P_j \leq 100$ . Therefore,  $P_j$  is maximally critically dependent on  $P_i$  for its operability. This result can also be seen from Equation 5.1 (strength of dependency) where

$$P_j = \alpha_{ij}P_i + 100(1 - \alpha_{ij}) = 1 \cdot P_i + 100(1 - 1) = P_i$$

since, when  $\beta_{ij} = 0$  it immediately follows that  $\alpha_{ij} = 1$ .

**Property 5.2:** In an FDNA graph, if  $P_j$  has a dependency relationship with  $P_i$  and  $P_j$  has a baseline operational utility level equal to zero then  $P_j$  has a maximum criticality of dependency on  $P_i$ .

**Proof**

From the strength of dependency discussion, recall the baseline operability level of  $P_j$  with a dependency relationship on  $P_i$  is given by  $100(1 - \alpha_{ij})$  utils. If

$$100(1 - \alpha_{ij}) = 0 \Rightarrow \alpha_{ij} = 1$$

From Property 5.1, if  $\alpha_{ij} = 1$  then  $\beta_{ij} = 0$  and, from Property 5.1, it follows that  $P_j$  has maximum criticality of dependency on feeder node  $P_i$ .

**Property 5.3: COD/SOD Cross-Over Point**

If  $P_j$  has a dependency relationship with  $P_i$  that is neither a maximum strength nor a maximum criticality of dependency, then when  $P_i$  reaches an operability level of

$$100 - \frac{\beta_{ij}}{1 - \alpha_{ij}} \text{ utils}$$

the operability level of  $P_j$  will cross-over from being determined by  $CODP_j$  to being determined by  $SODP_j$  where  $0 < \alpha_{ij} < 1$ ,  $0 < \beta_{ij} < 100(1 - \alpha_{ij})$ , and  $0 \leq P_i, P_j \leq 100$ .

**Proof**

Since  $P_j$  has neither a maximum strength nor a maximum criticality of dependency on  $P_i$  it follows that  $\alpha_{ij} \neq 1$  and  $\beta_{ij} \neq 0$ . From Equation 5.16, we have

$$P_j = \text{Min}(SODP_j, CODP_j) = \text{Min}(\alpha_{ij}P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij})$$

The operability level of  $P_j$  is strictly determined by  $CODP_j$  when

$$P_i + \beta_{ij} < \alpha_{ij} P_i + 100(1 - \alpha_{ij})$$

$$\Rightarrow P_i < 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})}$$

The operability level of  $P_j$  is strictly determined by  $SODP_j$  when

$$\alpha_{ij} P_i + 100(1 - \alpha_{ij}) < P_i + \beta_{ij}$$

$$\Rightarrow P_i > 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})}$$

When

$$P_i = 100 - \frac{\beta_{ij}}{1 - \alpha_{ij}} \quad (5.18)$$

we can write this as

$$(1 - \alpha_{ij})P_i = 100(1 - \alpha_{ij}) - \beta_{ij} \Rightarrow P_i - \alpha_{ij}P_i = 100(1 - \alpha_{ij}) - \beta_{ij}$$

$$\Rightarrow P_i + \beta_{ij} = \alpha_{ij}P_i + 100(1 - \alpha_{ij}) \Rightarrow CODP_j = SODP_j$$

since  $CODP_j = P_j + \beta_{ij}$  and  $SODP_j = \alpha_{ij}P_i + 100(1 - \alpha_{ij})$  in accordance with the definition of the weakest link FDNA dependency function. The value of  $P_i$  produced by Equation 5.18 is called the *COD/SOD cross-over point*.

In general, if a COD/SOD cross-over point exists, then there must be an operability level for  $P_i$  where  $CODP_j(P_i) = 100$  (its maximum) but  $SODP_j(P_i) < 100$ . Furthermore, it is always true that  $CODP_j = P_j + \beta_{ij} = 100$  when  $P_i = 100 - \beta_{ij}$  and  $SODP_j(100 - \beta_{ij}) = 100 - \alpha_{ij}\beta_{ij}$  when  $P_i = 100 - \beta_{ij}$ . From this, it follows that

$$100 - \alpha_{ij}\beta_{ij} < 100$$

$$\Rightarrow SODP_j(P_i) < 100 = CODP_j(P_i)$$

when  $P_i = 100 - \beta_{ij}$ ,  $0 < \alpha_{ij} < 1$ , and  $0 < \beta_{ij} < 100(1 - \alpha_{ij})$ . Thus, subject to these conditions, a cross-over point will exist and be contained in the interval  $0 \leq P_i, P_j \leq 100$ .

In Property 5.3,  $\beta_{ij}$  was restricted to the interval  $0 < \beta_{ij} < 100(1 - \alpha_{ij})$ . If  $\beta_{ij} = 0$ , then a maximum criticality of dependency exists with  $P_j$  on  $P_i$  and the operability level of  $P_j$  is strictly determined by  $CODP_j$  for  $0 \leq P_i \leq 100$ . No COD/SOD cross-over point exists when this condition is present. In fact, from Equation 5.2

$$P_j = CODP_j = P_i + \beta_{ij} = P_i + 0 = P_i$$

when  $\beta_{ij} = 0$ . As discussed earlier, this is the condition “as  $P_i$  goes so goes  $P_j$ ”.

In Property 5.3,  $\beta_{ij}$  was also not permitted to equal  $100(1 - \alpha_{ij})$ . If  $\beta_{ij} = 100(1 - \alpha_{ij})$ , then from Equation 5.16 we can write the following:

$$\begin{aligned} P_j &= \text{Min}(SODP_j, CODP_j) = \text{Min}(\alpha_{ij}P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij}) \\ \Rightarrow P_j &= \text{Min}(\alpha_{ij}P_i + 100(1 - \alpha_{ij}), P_i + 100(1 - \alpha_{ij})) \end{aligned}$$

Thus, the operability level of  $P_j$  is strictly determined by  $SODP_j$ . No COD/SOD cross-over point exists when this condition is present.

**Definition 5.5:** Minimum Effective Operational Level (MEOL)

The minimum effective operational level (MEOL) of a node is the utility associated with the minimum level of performance the node must achieve for its outputs to be minimally acceptable to stakeholders.

The MEOL is to recognize not all nodes need to be wholly operable for their outputs to have utility to stakeholders. In general, a node's baseline operability level is less than or equal to its minimum effective operational level; that is,

$$BOLP_j \leq MEOLP_j$$

**Property 5.4: Beta Anchor Point**

Suppose  $P_j$  has a dependency relationship with  $P_i$  and a COD/SOD cross-over point exists. Suppose  $MEOLP_j$  denotes the minimum effective operational level of  $P_j$ . If

$$\beta_{ij} < \frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j)$$

then the minimum effective operational level of  $P_j$  is achieved by  $CODP_j$ . If

$$\beta_{ij} > \frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j)$$

then the minimum effective operational level of  $P_j$  is achieved by  $SODP_j$ . The value produced when

$$\beta_{ij} = \frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j)$$

is called the **beta anchor point**.



### Proof

Since  $P_j$  has a dependency relationship with  $P_i$  we can write

$$P_j = \text{Min}(SODP_j, CODP_j) = \text{Min}(\alpha_{ij}P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij})$$

If the minimum effective operational level of  $P_j$  is achieved by  $CODP_j$  then

$$MEOLP_j = P_i + \beta_{ij} \Rightarrow P_i = MEOLP_j - \beta_{ij} \text{ and } \alpha_{ij}P_i + 100(1 - \alpha_{ij}) > MEOLP_j$$

This implies

$$\begin{aligned} \alpha_{ij}(MEOLP_j - \beta_{ij}) + 100(1 - \alpha_{ij}) &> MEOLP_j \\ \Rightarrow \beta_{ij} &< \frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j) \end{aligned}$$

If the minimum effective operational level of  $P_j$  is achieved by  $SODP_j$  then

$$MEOLP_j = \alpha_{ij}P_i + 100(1 - \alpha_{ij}) \text{ and } P_i + \beta_{ij} > MEOLP_j$$

This implies  $\beta_{ij} > MEOLP_j - P_i$  and this implies

$$\begin{aligned} \beta_{ij} > MEOLP_j - P_i = MEOLP_j - \left[ \frac{MEOLP_j - 100(1 - \alpha_{ij})}{\alpha_{ij}} \right] \\ \Rightarrow \beta_{ij} &> \frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j) \end{aligned}$$

From this, it follows that the value produced when

$$\beta_{ij} = \frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j) \quad (5.19)$$

is called the **beta anchor point**.

Recall from Definition 5.5 the minimum effective operational level (MEOL) of a node is the utility associated with the minimum level of performance the node must achieve for its outputs to be minimally acceptable to stakeholders. The MEOL is to recognize not all nodes need to be wholly operable for their outputs to have utility to stakeholders. Even though more operability is

better than less, it may be economically prohibitive, in some cases, to require a node be wholly operable before its outputs have utility to stakeholders.

The beta anchor point is the level of operability  $P_j$  achieves (in utils) in  $0 \leq P_j \leq 100$  around which the  $MEOLP_j$  is achieved by  $CODP_j$  or by  $SODP_j$ . From this, we have the following.

If the criticality of dependency parameter  $\beta_{ij}$  is chosen to be less than the beta anchor point, then  $MEOLP_j$  is achieved by  $CODP_j$ . If the criticality of dependency parameter  $\beta_{ij}$  is chosen to be greater than the beta anchor point, then  $MEOLP_j$  is achieved by  $SODP_j$ . If the criticality of dependency parameter  $\beta_{ij}$  is chosen to be equal to the beta anchor point, then  $MEOLP_j$  is achieved by  $CODP_j$  or by  $SODP_j$ ; that is,  $CODP_j = MEOLP_j$  and  $SODP_j = MEOLP_j$  in this case.

The location of the beta anchor point is important. It identifies whether the rate by which a dependent node achieves its minimum effective operational level is driven by COD or by SOD. Under the weakest link FDF, when  $0 < \alpha_{ij} < 1$  the rate by which a node increases its operability level is faster under COD than under SOD. The rate is the same if  $\alpha_{ij} = 1$ .

From this discussion, one could ask the following: *What operability level must a feeder node  $P_i$  achieve for its dependent node  $P_j$  to achieve its minimum effective operational level?* This question can be answered from Property 5.4. Consider the following.

If the minimum effective operational level of  $P_j$  is achieved by  $CODP_j$  then from Property 5.4 we can write

$$MEOLP_j = P_i + \beta_{ij} \Rightarrow P_i = MEOLP_j - \beta_{ij}$$

If the minimum effective operational level of  $P_j$  is achieved by  $SODP_j$  then from Property 5.4 we can write

$$MEOLP_j = \alpha_{ij} P_i + 100(1 - \alpha_{ij})$$

$$\Rightarrow P_i = \frac{MEOLP_j - 100(1 - \alpha_{ij})}{\alpha_{ij}}$$

or equivalently,

$$P_i = \frac{MEOLP_j - BOLP_j}{\alpha_{ij}}$$

**Property 5.5: Beta Bounds**

If  $P_j$  has a dependency relationship on  $P_i$  then  $0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ .

**Proof**

Since  $P_j$  has a dependency relationship on  $P_i$  we can write

$$P_j = \text{Min} (SODP_j, CODP_j) = \text{Min} (\alpha_{ij}P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij})$$

If  $P_j = CODP_j$  with  $\alpha_{ij} \neq 1$  then

$$P_i + \beta_{ij} < \alpha_{ij}P_i + 100(1 - \alpha_{ij})$$

$$\Rightarrow P_i < 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})}$$

If  $P_j = SODP_j$  with  $\alpha_{ij} \neq 1$  then

$$\alpha_{ij}P_i + 100(1 - \alpha_{ij}) < P_i + \beta_{ij}$$

$$\Rightarrow P_i > 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})}$$

By definition  $0 \leq P_i \leq 100$ ; thus,

$$0 \leq 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})} \leq 100 \quad (\text{with } \alpha_{ij} \neq 1)$$

whether  $P_j = CODP_j$ ,  $P_j = SODP_j$ , or  $P_j = CODP_j = SODP_j$  (Property 5.3). This means

$$0 \leq 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})} \quad \text{and} \quad 100 - \frac{\beta_{ij}}{(1 - \alpha_{ij})} \leq 100 \quad (\text{with } \alpha_{ij} \neq 1)$$

$$\Rightarrow \beta_{ij} \leq 100(1 - \alpha_{ij}) \quad \text{and} \quad 0 \leq \beta_{ij}$$

$$\Rightarrow 0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$$

This result is intuitive. If  $\beta_{ij} \geq 100(1 - \alpha_{ij})$  then the operability level of  $P_j$  is strictly determined by  $SODP_j$ . When  $P_j = SODP_j$ , for all  $0 \leq P_i \leq 100$ , the operability level of  $P_j$  will not fall below its baseline level of  $100(1 - \alpha_{ij})$ . Here, no criticality of dependency exists between feeder node  $P_i$  and receiver node  $P_j$ . However, if a criticality of dependency exists between  $P_i$  and  $P_j$  then  $P_j \neq SODP_j$  for all  $0 \leq P_i \leq 100$ . In this situation, it follows that  $0 \leq \beta_{ij} < 100(1 - \alpha_{ij})$ .

**Theorem 5.1:** The operability level of a receiver node is bounded above by the measure of its strength of dependency on its feeder node.

**Proof**

First, we'll prove this theorem for a receiver node with a single feeder node dependency. Then, we'll extend this result to a receiver node with dependency relationships on  $n$  feeder nodes.

*Single Node Dependency*

Suppose  $P_j$  is a receiver node with a dependency relationship on a single feeder node  $P_i$ . To prove this theorem, we want to show the operability level of  $P_j$  is bounded above by  $SODP_j$ .

From the weakest link FDF (Equation 5.16) we have the following:

$$P_j = \text{Min} (SODP_j, CODP_j) = \text{Min} (\alpha_{ij} P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij})$$

From this, only one of two outcomes can occur:

$$\alpha_{ij} P_i + 100(1 - \alpha_{ij}) \leq P_i + \beta_{ij} \text{ or } P_i + \beta_{ij} \leq \alpha_{ij} P_i + 100(1 - \alpha_{ij})$$

From either condition it follows that

$$P_j = \text{Min} (SODP_j, CODP_j) \leq SODP_j$$

Thus, the operability level of a receiver node is bounded above by the measure of its strength of dependency on its feeder node.

*Multiple Node Dependencies*

Suppose  $P_j$  is a receiver node with dependencies on  $h$  feeder nodes  $P_1, P_2, P_3, \dots, P_h$ . From the weakest link FDF (Equation 5.16) we have the following:

$$P_j = \text{Min} (SODP_j, CODP_j)$$

where

$$SODP_j = \text{Average} (SODP_{j1}, SODP_{j2}, SODP_{j3}, \dots, SODP_{jh})$$

$$SODP_{jl} = \alpha_{lj} P_l + 100(1 - \alpha_{lj}), \quad 0 \leq P_l, P_j \leq 100, \quad 0 < \alpha_{lj} \leq 1, \quad l = 1, 2, 3, \dots, h$$

$$CODP_j = \text{Min} (CODP_{j1}, CODP_{j2}, CODP_{j3}, \dots, CODP_{jh})$$

$$CODP_{jl} = P_l + \beta_{lj}, \quad 0 \leq \beta_{lj} \leq 100(1 - \alpha_{lj})$$

From this, only one of two outcomes can occur; either

$$CODP_j \leq SODP_j \text{ or } CODP_j \geq SODP_j$$

From either condition it follows that

$$P_j = \text{Min} (SODP_j, CODP_j) \leq SODP_j$$

Thus, the operability level of a receiver node with dependencies on  $h$  feeder nodes can never exceed its strength of dependency measure.

**Theorem 5.2:** If receiver node  $P_j$  has a maximum strength of dependency on  $h$  feeder nodes, then its operability level is equal to the minimum operability level of the feeder node in this set.

### Proof

This theorem is a generalization of Property 5.1 to the case of  $h$  feeder nodes. We're given that  $P_j$  is a receiver node with dependencies on  $h$  feeder nodes, say  $P_1, P_2, P_3, \dots, P_h$ . We're also given that  $P_j$  has a maximum strength of dependency on each feeder node; thus,

$$\alpha_{1j} = \alpha_{2j} = \alpha_{3j} \dots = \alpha_{hj} = 1$$

From Property 5.1 this implies

$$\beta_{1j} = \beta_{2j} = \beta_{3j} \dots = \beta_{hj} = 0$$

From the weakest link FDF, the operability level of  $P_j$  given these conditions is:

$$P_j = \text{Min} \left( \frac{P_1 + P_2 + \dots + P_h}{h}, P_1, P_2, P_3, \dots, P_h \right)$$

This can be written as follows:

$$P_j = \text{Min} \left( \frac{P_1 + P_2 + \dots + P_h}{h}, \text{Min} (P_1, P_2, P_3, \dots, P_h) \right)$$

Now, the average of a finite set of real numbers is greater than or equal to the minimum of the set. We will prove this for three real numbers  $a, b$ , and  $c$ . The proof is readily extensible to a finite set of  $m$  real numbers.

Suppose we have three real numbers  $a, b$ , and  $c$ . We want to prove that

$$\frac{a + b + c}{3} \geq \text{Min}(a, b, c)$$

This can be written as

$$a + b + c \geq 3\text{Min}(a, b, c)$$

Suppose  $\text{Min}(a, b, c) = b$ . Then, it follows that

$$a + b + c \geq 3\text{Min}(a, b, c) \Rightarrow a + b + c \geq 3b \Rightarrow a + c \geq 2b$$

Since we've assumed  $\text{Min}(a, b, c) = b$  then  $a \geq b$  and  $c \geq b$ . Furthermore, suppose

$$a \geq b \text{ by } \varepsilon_a \geq 0 \text{ and } c \geq b \text{ by } \varepsilon_c \geq 0$$

Then, we can write

$$a = b + \varepsilon_a \text{ and } c = b + \varepsilon_c \text{ where } \varepsilon_a, \varepsilon_c \geq 0$$

This implies

$$a + c \geq 2b \Rightarrow (b + \varepsilon_a) + (b + \varepsilon_c) \geq 2b \Rightarrow \varepsilon_a + \varepsilon_c \geq 0$$

since  $\varepsilon_a, \varepsilon_c \geq 0$ . A similar argument holds if  $\text{Min}(a, b, c) = a$  or  $\text{Min}(a, b, c) = c$ .

Thus, the average of a set of three real numbers is always greater than or equal to the minimum of the set. Proving this result for a finite set of  $m$  real numbers is similarly approached. Therefore,

$$\frac{P_1 + P_2 + \dots + P_h}{h} \geq \text{Min}(P_1, P_2, P_3, \dots, P_h)$$

Thus,

$$P_j = \text{Min}(P_1, P_2, P_3, \dots, P_h)$$

Therefore, if receiver node  $P_j$  has a maximum strength of dependency on  $n$  feeder nodes, then its operability level is equal to the minimum operability level of the feeder node in this set. Note this is consistent with the philosophy of weakest link/weakest chain theory.

This concludes a discussion of key fundamental properties and theorems in the FDNA methodology. The following offers two numerical examples to illustrate aspects of FDNA theory described thus far.

**Example 5.6:** Figure 51 shows a dependency relationship between two nodes  $P_j$  and  $P_i$ . As we've discussed, this is a 2,1,1-node FDNA graph.

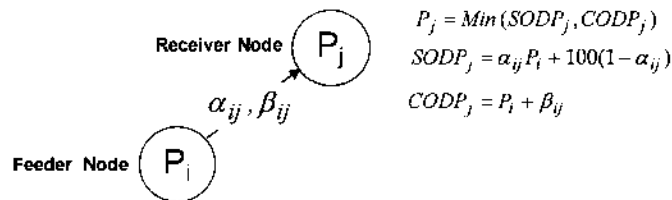


Figure 51. A 2,1,1-Node FDNA Graph

Table 6 is an operability analysis of a 2,1,1-node dependency relationship in Figure 51. Here, the calculations are in accordance with the weakest link FDF, given by Equation 5.16, and the FDNA properties previously described.

**A 2-Node FDNA Graph: 1-Dependency Point, 1-Receiver Node  $P_j$** 

| <b>INPUT:</b> MEOLP <sub>j</sub>             | <b>80</b>         | Definition 5.5  |  |  |
|--|-------------------|---|--|--|
| <b>INPUT:</b> BOLP <sub>j</sub>              | <b>50</b>         | Figure 5.4  |  |  |
| COMPUTED: $\alpha$ -Dependency Fraction      | <b>0.50</b>       | Figure 5.4  |  |  |
| COMPUTED: Beta Anchor Point                  | <b>20.0</b>       | Property 5.4  |  |  |
| COMPUTED: Beta Upper Bound                   | <b>50</b>         | Property 5.5  |  |  |
| <b>INPUT:</b> Beta Assigned/Setting          | <b>10</b>         | Assigned/Set  |  |  |
| Feeder Node $P_i$                            | SODP <sub>j</sub> | CODP <sub>j</sub>   | $P_j$ Operability Level =<br>Min(SODP <sub>j</sub> , CODP <sub>j</sub> ) | $P_j$ Operability Level<br>Determined By |
| 0  | 50                | 10  | 10   | COD                                      |
| 5  | 52.5              | 15  | 15   | COD                                      |
| 10   | 55                | 20  | 20   | COD                                      |
| 15   | 57.5              | 25  | 25   | COD                                      |
| 20   | 60                | 30  | 30   | COD                                      |
| 25   | 62.5              | 35  | 35   | COD                                      |
| 30   | 65                | 40  | 40   | COD                                      |
| 35   | 67.5              | 45  | 45   | COD                                      |
| 40   | 70                | 50  | 50   | COD                                      |
| 45   | 72.5              | 55  | 55   | COD                                      |
| 50   | 75                | 60  | 60   | COD                                      |
| 55   | 77.5              | 65  | 65   | COD                                      |
| 60   | 80                | 70  | 70   | COD                                      |
| 65   | 82.5              | 75  | 75   | COD                                      |
| 70   | 85                | 80  | 80   | COD                                      |
| 75   | 87.5              | 85  | 85   | COD                                      |
| 80   | 90                | 90  | 90   | COD/SOD                                  |
| 85   | 92.5              | 95  | 92.5   | SOD                                      |
| 90   | 95                | 100   | 95   | SOD                                      |
| 95   | 97.5              | 105   | 97.5   | SOD                                      |
| 100  | 100               | 110   | 100  | SOD                                      |
| <b>Cross Over Point For <math>P_i</math></b> | <b>80</b>         | <b>From This Point SODP<sub>j</sub> Determines <math>P_j</math>'s Operability Level</b> |  |  |
| <b>Cross Over Score for <math>P_j</math></b> | <b>90</b>         |   |  |  |

**Table 6. A First Operability Analysis of a 2,1,1-Node FDNA Graph**

A second operability analysis was conducted, where the degree of criticality  $\beta_{ij}$  was relaxed from a value of 10 to a value of 30. These results are presented later in Table 7.

Three inputs are shown in Table 6. These are  $MEOLP_j$ ,  $BOLP_j$ , and the criticality of dependency parameter  $\beta_{ij}$ . Here, receiver node  $P_j$  must reach a minimum operability level of 80 utils. However, its current baseline operability level is 50 utils. So, receiver node  $P_j$  relies on contributions from feeder node  $P_i$  to improve its baseline operability to the minimum effective level required by stakeholders. Table 6 also shows that  $P_j$ 's reliance on contributions from  $P_i$  is significantly critical. Here, the criticality of dependency parameter is set at 10. This value is near the maximum criticality of dependency point ( $\beta_{ij} = 0$ ) in the range  $0 \leq \beta_{ij} \leq 50$ .

Three outputs are shown in the upper left corner of Table 6. These are the strength of dependency fraction  $\alpha_{ij}$ , the beta anchor point, and the beta upper bound. These outputs were computed from the inputs in Table 6; specifically,

The  $\alpha_{ij}$ -dependency fraction:  $100(1 - \alpha_{ij}) = BOLP_j = 50 \Rightarrow \alpha_{ij} = 0.50$

The beta anchor point:  $\frac{(1 - \alpha_{ij})}{\alpha_{ij}}(100 - MEOLP_j) = \frac{(1 - 0.50)}{0.50}(100 - 80) = 20$

The beta upper bound:  $0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij}) \Rightarrow \beta_{ij} \leq 100(1 - \alpha_{ij}) \Rightarrow \beta_{ij} \leq BOLP_j = 50$

The last set of outputs in Table 6 show the operability level of  $P_j$  as a function of the operability level of  $P_i$ , for  $0 \leq P_i, P_j \leq 100$ . The following are a few observations:

(1) Feeder node  $P_i$  must achieve an operability level of 70 utils for receiver node  $P_j$  to achieve its MEOL. From Property 5.4, since the criticality of dependency parameter was set at 10, and this is less than the beta anchor point,  $P_j$  achieves its MEOL under a rate governed by  $CODP_j$ .

(2) The COD/SOD cross-over point occurs when feeder node  $P_i$  achieves 80 utils; that is, from Equation 5.18 we have

$$P_i = 100 - \frac{\beta_{ij}}{1 - \alpha_{ij}} = 100 - \frac{10}{1 - 0.50} = 80$$

From this point, the operability improvement in receiver node  $P_j$  transitions from being determined by  $CODP_j$  to being determined by  $SODP_j$ . Receiver node  $P_j$  continues to improve in operability with increasing operability in  $P_i$  but it will now improve at a rate slower than it did when its operability level was determined by  $CODP_j$ .

(3) If feeder node  $P_i$ 's contribution is equal to zero in operational utility to receiver node  $P_j$  then  $P_j$  will degrade from its baseline operability level of 50 utils to 10 utils, rendering  $P_j$  virtually inoperable.

**Example 5.7:** Here, we look at a slight variation of the input data in Table 6. Suppose the data in Table 7 is for the 2,1,1-node dependency relationship in Figure 51.

Now, instead of 10 as the value assigned for the criticality of dependency parameter (in Table 6) suppose the value assigned is 30. This value is farther from the maximum criticality of dependency point ( $\beta_{ij} = 0$ ) than it was in Table 6. Although  $P_i$ 's contribution to the operability of  $P_j$  remains critical, its level of criticality is less in this case than it was for the case in Table 6.

In Table 7,  $\beta_{ij}$  remains in the range  $0 \leq \beta_{ij} \leq 50$ . Table 7 presents the results of this operability analysis.



**A 2-Node FDNA Graph: 1-Dependency Point, 1-Receiver Node  $P_j$**

| <b>INPUT:</b> MEOL $P_j$                       | <b>80</b>   | Definition 5.5   |  |  |
|--|-------------|--|--|--|
| <b>INPUT:</b> BOL $P_j$                        | <b>50</b>   | Figure 5.4   |  |  |
| <b>COMPUTED:</b> $\alpha$ -Dependency Fraction | <b>0.50</b> | Figure 5.4   |  |  |
| <b>COMPUTED:</b> Beta Anchor Point             | <b>20.0</b> | Property 5.4   |  |  |
| <b>COMPUTED:</b> Beta Upper Bound              | <b>50</b>   | Property 5.5   |  |  |
| <b>INPUT:</b> Beta Assigned/Setting            | <b>30</b>   | Assigned/Set   |  |  |
| Feeder Node $P_i$                              | SOD $P_j$   | COD $P_j$  | $P_j$ Operability Level =<br>Min{SOD $P_j$ , COD $P_j$ } | $P_j$ Operability Level<br>Determined By |
| 0  | 50          | 30   | 30   | COD                                      |
| 5  | 52.5        | 35   | 35   | COD                                      |
| 10   | 55          | 40   | 40   | COD                                      |
| 15   | 57.5        | 45   | 45   | COD                                      |
| 20   | 60          | 50   | 50   | COD                                      |
| 25   | 62.5        | 55   | 55   | COD                                      |
| 30   | 65          | 60   | 60   | COD                                      |
| 35   | 67.5        | 65   | 65   | COD                                      |
| 40   | 70          | 70   | 70   | COD/SOD                                  |
| 45   | 72.5        | 75   | 72.5   | SOD                                      |
| 50   | 75          | 80   | 75   | SOD                                      |
| 55   | 77.5        | 85   | 77.5   | SOD                                      |
| 60   | 80          | 90   | 80   | SOD                                      |
| 65   | 82.5        | 95   | 82.5   | SOD                                      |
| 70   | 85          | 100  | 85   | SOD                                      |
| 75   | 87.5        | 105  | 87.5   | SOD                                      |
| 80   | 90          | 110  | 90   | SOD                                      |
| 85   | 92.5        | 115  | 92.5   | SOD                                      |
| 90   | 95          | 120  | 95   | SOD                                      |
| 95   | 97.5        | 125  | 97.5   | SOD                                      |
| 100  | 100         | 130  | 100  | SOD                                      |
| <b>Cross Over Point For <math>P_i</math></b>   | <b>40</b>   | <b>From This Point SOD<math>P_j</math> Determines <math>P_j</math>'s Operability Level</b> |  |  |
| <b>Cross Over Score for <math>P_j</math></b>   | <b>70</b>   |  |  |  |

Table 7. A Second Operability Analysis of a 2,1,1-Node FDNA Graph

In this case, receiver node  $P_j$  achieves its minimum effective operational level (MEOL) when feeder node  $P_i$  reaches 60 utils instead of 70 utils (as in Table 6). Thus,  $P_i$  doesn't have to contribute as much utility to  $P_j$  for  $P_j$  to reach its minimum effective operational level than it does for the data in Table 6. This is because the criticality of  $P_i$ 's contribution to  $P_j$ 's operability is more relaxed than it was for the case represented by Table 6.

The operability analysis in Table 7 reveals that  $P_j$  achieves its MEOL under a rate governed by SOD $P_j$ . This illustrates Property 5.4. Here, the criticality of dependency parameter was set at 30. Since this value is greater than the beta anchor point (in Table 7) Property 5.4 states that  $P_j$  will achieve its MEOL under a rate governed by SOD $P_j$ .

The opposite was seen for the data in Table 6. There, the criticality of dependency parameter is set at 10. Since this is less than the beta anchor point,  $P_j$  achieves its MEOL under a rate governed by COD $P_j$ , in accordance with Property 5.4. Figure 52 presents a visual comparison of the operability analysis conducted with the datasets from Table 6 and Table 7, respectively.

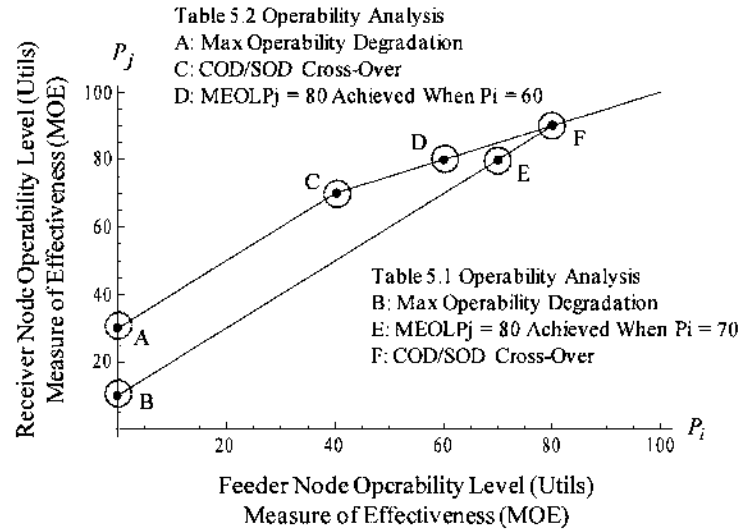
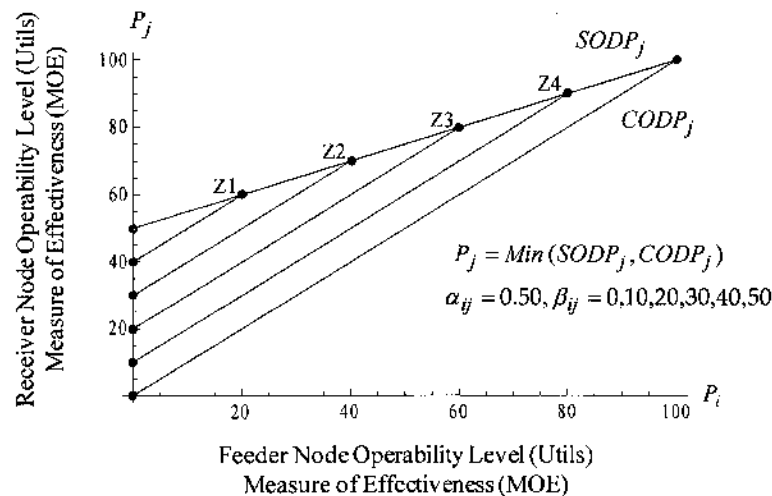


Figure 52. Table 6 and Table 7 Operability Analysis Comparison

Figure 53 presents a further operability analysis of the dependency relationship in Figure 51. Shown is the operability level of  $P_j$  as a function of the operability level of  $P_i$  for varying degrees that  $P_j$  has a critical dependency on  $P_i$ . Six curves are shown in Figure 53.

Figure 53. Operability Analysis for Varying  $\beta_{ij}$  (Tables 6, 7 Data)

A number of observations can be seen from Figure 53. These include the following:

- Top-Most Line: The operability level of  $P_j$  is strictly determined by  $SODP_j$  since the criticality of dependency parameter  $\beta_{ij} = 50 = BOLP_j$ . Also, there is **no degradation** in the operability level of  $P_j$  if the operability level of  $P_i$  is zero. As discussed earlier, this is expected in cases where  $\beta_{ij} = BOLP_j$ . Because the operability level of  $P_j$  is strictly determined by  $SODP_j$  there is no COD/SOD cross over point.

- **Bottom-Most Line:** The operability level of  $P_j$  is strictly determined by  $CODP_j$  since the criticality of dependency parameter  $\beta_{ij} = 0$  (maximum criticality of dependency). Also, there is **complete degradation** in the operability level of  $P_j$  if the operability level of  $P_i$  is zero. As discussed earlier, this is expected in cases where  $\beta_{ij} = 0$ . From Property 5.1, recall that if  $\beta_{ij} = 0$  then  $\alpha_{ij} = 1$ .

Thus,  $CODP_j$  strictly drives the operability level of  $P_j$ , in this case. Moreover, the operability level of  $P_j$  is equal to the operability level of  $P_i$ . Because the operability level of  $P_j$  is strictly determined by  $CODP_j$  there is no COD/SOD cross over point.

- **Between Lines:** The marks Z1, Z2, Z3, and Z4 indicate COD/SOD cross-over points for  $\beta_{ij} = 40, 30, 20$ , and  $10$ , respectively, and where  $0 < \alpha_{ij} < 1$  and  $0 < \beta_{ij} < 100(1 - \alpha_{ij})$ . Unlike the top-most or bottom-most lines,  $P_j$  in these in-between lines has neither a maximum strength nor a maximum criticality of dependency on  $P_i$ . Thus, when  $\alpha_{ij} \neq 1$  and  $\beta_{ij} \neq 0$  a COD/SOD cross-over point always exists. This was shown in Property 5.3.
- Figure 53 illustrates Theorem 5.1; that is, the operability of a receiver node  $P_j$  is bounded above by  $SODP_j$  and bounded below by  $CODP_j$ .

#### Summary: FDNA Fundamental Equations

1. **Weakest Link FDNA Dependency Function:** The operability level of node  $P_y$  that is dependent on the operability levels of  $h$  other nodes  $P_1, P_2, P_3, \dots, P_h$  is given by

$$0 \leq P_y = \text{Min} (SODP_y, CODP_y) \leq 100$$

$$SODP_y = \text{Average} (SODP_{y1}, SODP_{y2}, SODP_{y3}, \dots, SODP_{yh})$$

$$SODP_{yl} = \alpha_{ly} P_l + 100(1 - \alpha_{ly}), \quad 0 \leq P_l, P_y \leq 100, \quad 0 < \alpha_{ly} \leq 1, \quad l = 1, 2, 3, \dots, h$$

$$CODP_y = \text{Min} (CODP_{y1}, CODP_{y2}, CODP_{y3}, \dots, CODP_{yh})$$

$$CODP_{yl} = P_l + \beta_{ly}, \quad 0 \leq \beta_{ly} \leq 100(1 - \alpha_{ly})$$

$$2. \text{ The COD/SOD cross-over point: } P_i = 100 - \frac{\beta_{ij}}{1 - \alpha_{ij}}$$

$$3. \text{ The beta anchor point: } \beta_{ij, \text{Anchor Point}} = \frac{(1 - \alpha_{ij})}{\alpha_{ij}} (100 - MEOLP_j)$$

$$4. \text{ The } \alpha_{ij} \text{-dependency fraction: } \alpha_{ij} = 1 - \frac{BOLP_j}{100}, \text{ where } BOLP_j = 100(1 - \alpha_{ij})$$

$$5. \text{ The beta bounds: } 0 \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$$

Last, the result from these summary equations applied to the multi-nodal dependency topology of a capability portfolio is shown. For this, we apply FDNA to the portfolio in Figure 50. Table 8 is the resulting operability analysis *as feeder nodes lose operability over time t1, t2, and t3*.

| FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA)                                    |        |  |        |  |        |                   |      |
|--|--------|--|--------|--|--------|-------------------|------|
| A CAPABILITY PORTFOLIO: 9,8,5-NODE FDNA GRAPH                                    |        |  |        |  |        |                   |      |
| INPUT: $\alpha_{ij}$ Strength of Dependency (SOD)                                |        |  |        | $\alpha_{ij}$ Within Range ... T/F                                     |        |                   |      |
| $\alpha_{P1Cap1}$  | 0.90   | $\alpha_{P4Cap3}$  | 0.85   | $\alpha_{P1Cap1}$  | TRUE   | $\alpha_{P4Cap3}$ | TRUE |
| $\alpha_{P3Cap1}$  | 0.45   | $\alpha_{P5P3}$  | 0.30   | $\alpha_{P3Cap1}$  | TRUE   | $\alpha_{P5P3}$   | TRUE |
| $\alpha_{P3Cap2}$  | 0.65   | $\alpha_{P3P1}$  | 0.15   | $\alpha_{P3Cap2}$  | TRUE   | $\alpha_{P3P1}$   | TRUE |
| $\alpha_{P6Cap3}$  | 0.90   | $\alpha_{P2P1}$  | 0.28   | $\alpha_{P6Cap3}$  | TRUE   | $\alpha_{P2P1}$   | TRUE |
| INPUT: $\beta_{ij}$ Criticality of Dependency (COD)                              |        |  |        | $\beta_{ij}$ Within Range ... T/F                                      |        |                   |      |
| $\beta_{P1Cap1}$   | 10.00  | $\beta_{P4Cap3}$   | 15.00  | $\beta_{P1Cap1}$   | TRUE   | $\beta_{P4Cap3}$  | TRUE |
| $\beta_{P3Cap1}$   | 55.00  | $\beta_{P5P3}$   | 70.00  | $\beta_{P3Cap1}$   | TRUE   | $\beta_{P5P3}$    | TRUE |
| $\beta_{P3Cap2}$   | 35.00  | $\beta_{P3P1}$   | 85.00  | $\beta_{P3Cap2}$   | TRUE   | $\beta_{P3P1}$    | TRUE |
| $\beta_{P6Cap3}$   | 10.00  | $\beta_{P2P1}$   | 72.00  | $\beta_{P6Cap3}$   | TRUE   | $\beta_{P2P1}$    | TRUE |
| INPUT: IF these feeder nodes are functioning at these operability levels ...     |        |  |        |  |        |                   |      |
| Time t1: If operability levels of feeder nodes P2, P5, P4, and P6 are:           |        | Time t2: If operability levels of feeder nodes P2, P5, P4, and P6 are: |        | Time t3: If operability levels of feeder nodes P2, P5, P4, and P6 are: |        |                   |      |
| P2   | 100    | P2   | 75     | P2   | 50     |                   |      |
| P5   | 100    | P5   | 75     | P5   | 50     |                   |      |
| P4   | 100    | P4   | 75     | P4   | 50     |                   |      |
| P6   | 100    | P6   | 100    | P6   | 100    |                   |      |
| OUTPUT: Then these receiver nodes are functioning at these operability levels... |        |  |        |  |        |                   |      |
| P3   | 100.00 | P3   | 78.75  | P3   | 57.50  |                   |      |
| P1   | 100.00 | P1   | 87.47  | P1   | 74.94  |                   |      |
| Cap1   | 100.00 | Cap1   | 84.80  | Cap1   | 67.50  |                   |      |
| Cap2   | 100.00 | Cap2   | 93.63  | Cap2   | 87.25  |                   |      |
| Cap3   | 100.00 | Cap3   | 98.13  | Cap3   | 96.25  |                   |      |
| COD portion of receiver node operability level                                   |        |  |        |  |        |                   |      |
| P3   | 115.00 | P3   | 90.00  | P3   | 65.00  |                   |      |
| P1   | 135.00 | P1   | 113.75 | P1   | 92.50  |                   |      |
| Cap1   | 110.00 | Cap1   | 88.75  | Cap1   | 67.50  |                   |      |
| Cap2   | 170.00 | Cap2   | 148.75 | Cap2   | 127.50 |                   |      |
| Cap3   | 172.00 | Cap3   | 160.00 | Cap3   | 135.00 |                   |      |
| SOD portion of receiver node operability level                                   |        |  |        |  |        |                   |      |
| P3   | 100.00 | P3   | 78.75  | P3   | 57.50  |                   |      |
| P1   | 100.00 | P1   | 87.47  | P1   | 74.94  |                   |      |
| Cap1   | 100.00 | Cap1   | 84.80  | Cap1   | 69.60  |                   |      |
| Cap2   | 100.00 | Cap2   | 93.63  | Cap2   | 87.25  |                   |      |
| Cap3   | 100.00 | Cap3   | 98.13  | Cap3   | 96.25  |                   |      |

Table 8. An Operability Analysis of the Capability Portfolio in Figure 50

## A GENERAL THEORY OF DEPENDENCY

The preceding sections introduced FDNA by a foundational set of postulates, properties, and theorems. From these, a calculus was built that measures how the operability of one node affects the operability of other nodes that connect across a network of complex relationships. From this, FDNA can be viewed as a framework for a *general theory of dependency* – one extensible to other problem contexts and into greater levels of generality. The following discusses this further.

Thus far, the FDNA calculus addressed dependency relationships between nodes that produce a single component, such as the node illustrated in Figure 55. What if a node produces multiple components? How is the operability of a node that produces multiple components determined? How is the operability of other nodes affected by nodes whose operability depends on the operability of multiple components? This section will address these and related questions.

Following this, the next topic in this section describes how the FDNA fundamental equation and its weakest link formulation can be *regulated*. The form of the FDNA dependency function is such that it can be attuned, if necessary, to the realities of a specific dependency relationship. Regulating the FDNA dependency function is a generalization from its fundamental form.

### Multiple Component FDNA Nodes

This topic involves extending the FDNA analytics to accommodate nodes characterized by multiple components. To begin, we start with the following definition.

#### Definition 5.6: Constituent Node, Single Component Node

In FDNA, a node characterized by two or more components is a *constituent node*. A node that is not a constituent node is a *single component node*. A single component node is one that is defined by one and only one component.

What does a constituent node look like? Figure 54 provides an example.

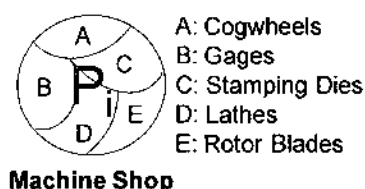


Figure 54. An FDNA Constituent Node Defined by Five Components

Suppose  $P_1$  is a machine shop that manufactures five components: cogwheels, gages, stamping dies, lathes, and rotor blades. In the language of FDNA,  $P_1$  is a *constituent node*.

Thus, a constituent node is always separable into two or more distinct components. Nodes in the preceding discussions were not separable into distinct components. They delivered to, or received from, single component nodes. If the node in Figure 54 produced only cogwheels then it is a *single component node*.

A constituent node can be a feeder to, or a receiver from, other nodes in an FDNA graph. These may be other constituent nodes or other single component nodes. Furthermore, a component within a constituent node can be a feeder to, or a receiver from, other components in the same node (an intra-component dependency), or to other components in other constituent nodes, or to other constituent nodes (as a whole), or to other single component nodes (as a whole) in an FDNA graph.

#### *Computing the Operability of a Constituent Node*

The preceding discussion introduced the constituent node in FDNA and discussed how it differs from a single component node. The difference is not only interpretive but also affects how the operability of these node types is computed.

If an FDNA node is a single component node then its operability can be represented by a single dimensional value function (SDVF)\*. Figure 55 shows a nonlinear SDVF for the operability of a widget production machine. The vertical axis is the machine's operability level (utils). The horizontal axis is the operational performance the machine achieves, as measured by the widget production rate.

So, the operability of single component nodes can be represented by single dimensional value functions to determine the operability levels their single component achieves. This is trickier but possible to do for constituent nodes. We discuss this next.

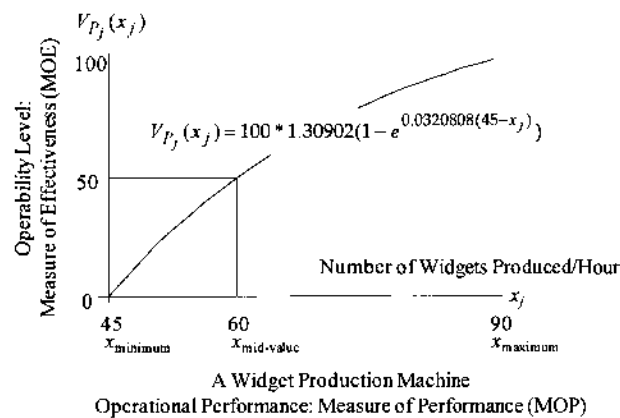


Figure 55. A Single Dimensional Value Function for the Operability Level of Single Component Node  $P_j$

\* A single dimensional value function (SDVF) is an established construct in modern decision theory [Kirkwood, 1997]. A *value function* is a real-valued mathematical function defined over an evaluation criterion that represents an option's measure of "goodness" over the levels of the criterion. A measure of "goodness" reflects a judged value in the performance of an option across the levels of a criterion.

The SDVFs in this dissertation all feature a preference ordering and strength of preference between the criterion's levels (or scores). When these features are present the SDVF is known as a *measurable value function*. In a measurable value function the value difference between any two levels (or scores) within a criterion represents a person's strength of preference between the two levels (or scores). The vertical axis of a measurable value function is a *cardinal interval scale* measure of the strength of a person's preferences. For this reason, a measurable value function is also referred to as a *cardinal value function*.

If an FDNA node is a constituent node, then its operability level is a function of the operability levels of its components. The operability of each component is represented by its own SDVF. If the components in the constituent node meet independence conditions\* then, by a theorem in decision theory, the overall operability function of the constituent node is a linear additive sum of the component SDVFs. The following illustrates this further.

Consider Figure 56. Suppose components  $A$ ,  $B$ , and  $C$  define constituent node  $P_i$ .

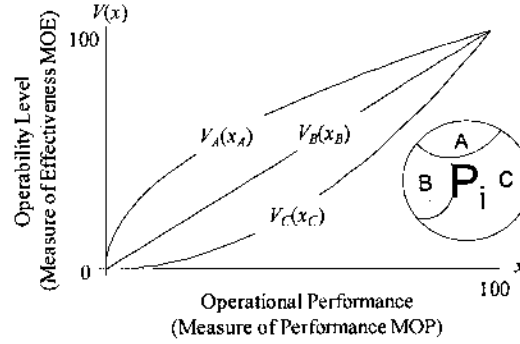


Figure 56. Component SDVFs for Constituent Node  $P_i$

Suppose the operability functions for  $A$ ,  $B$ , and  $C$  are given by single dimensional value functions  $V_A(x_A)$ ,  $V_B(x_B)$ , and  $V_C(x_C)$ , respectively. From this, the operability function of  $P_i$  is

$$P_i = w_A V_A(x_A) + w_B V_B(x_B) + w_C V_C(x_C) \quad (5.20)$$

where  $w_A + w_B + w_C = 1$  and  $0 \leq P_i, V_A(x_A), V_B(x_B), V_C(x_C) \leq 100$ . Equation 5.20 is a form of the additive value function in decision theory [Keeney, Raiffa, 1976; Kirkwood, 1997].

**Definition 5.7: Constituent Node Operability Function**

The operability level of constituent node  $P_y$  that contains  $\kappa$  components  $A_1, A_2, A_3, \dots, A_\kappa$  is given by

$$P_y = \sum_{i=1}^{\kappa} w_i V_{A_i}(x_i) \quad (5.21)$$

where  $w_1 + w_2 + w_3 + \dots + w_\kappa = 1$ ,  $V_{A_i}(x_i)$  is the single dimensional value function for  $A_i$ , and  $0 \leq P_y, V_{A_i}(x_i) \leq 100$ .

If a component in constituent node  $P_y$  has a dependency relationship with another component (internal or external to  $P_y$ ) then the value function for this component in Equation 5.21 is replaced by its FDF formulation, as defined by Equation 5.16.

\* The additive value function comes from a theorem in decision theory that states if a set of criteria are mutually preferentially independent, then an evaluator's preferences can be represented by a weighted linear combination of the single dimensional value functions for each criterion contained in the set [Keeney, Raiffa, 1976].

Equation 5.21 is a classical form of the Keeney-Raiffa additive value function. Figure 57 offers a visualization of Definition 5.6 and Definition 5.7.

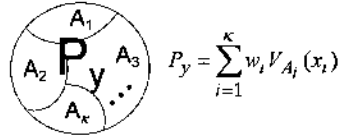


Figure 57. A Constituent Node With  $\kappa$  Components

The following examples illustrate how FDNA equations are formulated for various situations that may occur between constituent nodes and single component nodes.

**Example 5.8:** Formulate the FDNA equations for the graph in Figure 58.

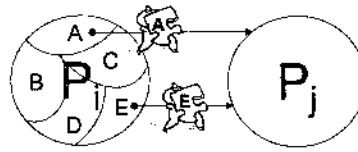


Figure 58. A 2,2,1-Node FDNA Graph With Constituent Node  $P_i$

Figure 58 consists of two nodes  $P_i$  and  $P_j$ , two dependency points, and one receiver node  $P_j$ . Node  $P_i$  is a constituent node feeding its components  $A$  and  $E$  to receiver node  $P_j$ .

The FDNA dependency function for this graph is given by Equations 5.22 and 5.23.

$$P_j = \text{Min} (\text{Ave} (\text{SODP}_{jA}, \text{SODP}_{jE}), \text{CODP}_{jA}, \text{CODP}_{jE}) \quad (5.22)$$

$$P_j = \text{Min} \left( \frac{\alpha_{Aj} A}{2} + \frac{\alpha_{Ej} E}{2} + 100 \left( 1 - \left( \frac{\alpha_{Aj} + \alpha_{Ej}}{2} \right), A + \beta_{Aj}, E + \beta_{Ej} \right) \right) \quad (5.23)$$

where  $\alpha_{Aj}$ ,  $\alpha_{Ej}$ ,  $\beta_{Aj}$ , and  $\beta_{Ej}$  are strength and criticality of dependency parameters with respect to components  $A$  and  $E$  that are feeder nodes to  $P_j$ . The terms  $A$  and  $E$ , in Equation 5.23, are the operability levels\* of  $A$  and  $E$ . Finally, Equation 5.23 is subject to

$$0 < \alpha_{Aj}, \alpha_{Ej} \leq 1, 0 \leq \beta_{Aj} \leq 100(1 - \alpha_{Aj}), 0 \leq \beta_{Ej} \leq 100(1 - \alpha_{Ej}), \text{ and } 0 \leq A, E, P_i, P_j \leq 100$$

\* Notational Comment: All node-related terms in an FDNA equation are measures of operability levels that range from zero to one-hundred. Shown in Figure 45 or Figure 55, operability levels can originate from single dimensional value functions. Capturing this from a strict notational perspective would reduce the ease with which FDNA equations appear. For example, in Figure 58,  $A$  is a component contained in  $P_i$ . It is also a feeder to  $P_j$ . When  $A$  appears as a term in Equation 5.23, it is assumed that  $0 \leq A \equiv V_A(x_A) \leq 100$ . This term is  $A$ 's operability level derived from its single dimensional value function  $V_A(x_A)$ . This convention was adopted for ease of presentation so readers could view FDNA equations more from their structural contexts than from a strictly rigorous notational one.



What is the operability function for  $P_i$ ? Since  $P_i$  is a constituent node, from Definition 5.7

$$P_i = w_A V_A(x_A) + w_B V_B(x_B) + w_C V_C(x_C) + w_D V_D(x_D) + w_E V_E(x_E) \quad (5.24)$$

where

$$w_A + w_B + w_C + w_D + w_E = 1$$

$$V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), \text{ and } V_E(x_E)$$

are single dimensional value functions for  $A, B, C, D$ , and  $E$ , respectively,  $0 \leq P_i, \leq 100$  and

$$0 \leq V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), V_E(x_E) \leq 100$$

In this chapter, we adopted a notational simplification explained in the preceding footnote. Using this convention, we can simplify the notation in Equation 5.24 as follows:

$$P_i \equiv w_A A + w_B B + w_C C + w_D D + w_E E \quad (5.25)$$

where

$$A = V_A(x_A), B = V_B(x_B)$$

$$C = V_C(x_C), D = V_D(x_D), \text{ and } E = V_E(x_E)$$

Throughout this chapter, Equation 5.24 and Equation 5.25 are considered notationally equivalent.

**Example 5.9:** Formulate the FDNA equations for the graph in Figure 59.

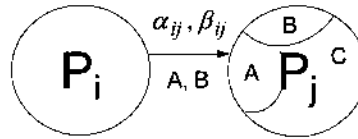


Figure 59. A 2,1,1-Node FDNA Graph:  
Constituent Node Dependency on a Single Component Node

The FDNA graph in Figure 59 consists of two nodes  $P_i, P_j$ , one dependency point, and one receiver node  $P_j$ . Node  $P_i$  is a single component node. Node  $P_j$  is a constituent node defined by three components  $A, B$ , and  $C$ . Constituent node  $P_j$  has a dependency relationship on node  $P_i$ .

In Figure 59, the  $A, B$  below the arrow means only components  $A$  and  $B$  in  $P_j$  depend on single component node  $P_i$ . With this, we can form the FDNA equations as follows:

$$P_j = w_A A + w_B B + w_C C$$

$$A = \text{Min} (\alpha_{ijA} P_i + 100(1 - \alpha_{ijA}), P_i + \beta_{ijA})$$

$$B = \text{Min} (\alpha_{ijB} P_i + 100(1 - \alpha_{ijB}), P_i + \beta_{ijB})$$

where  $w_A + w_B + w_C = 1$ ,  $C = V_C(x_C)$ , and  $0 \leq V_C(x_C) \leq 100$ , and  $0 \leq P_i, P_j \leq 100$ .

**Example 5.10:** Formulate the FDNA equations for the graph in Figure 60.

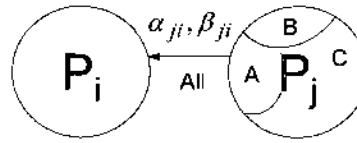


Figure 60. A 2,1,1-Node FDNA Graph:  
Single Component Node Dependency on a Constituent Node

The FDNA graph in Figure 60 consists of two nodes  $P_i$ ,  $P_j$ , one dependency point, and one receiver node  $P_j$ . Node  $P_i$  is a single component node. Node  $P_j$  is a constituent node defined by three components  $A$ ,  $B$ , and  $C$ . Single component node  $P_i$  has a dependency relationship on constituent node  $P_j$ .

In Figure 60, the “All” below the arrow means single component node  $P_i$  depends on all the components in  $P_j$ . With this, we can form the FDNA equations as follows:

$$P_i = \text{Min} (\alpha_{ji}P_j + 100(1 - \alpha_{ji}), P_j + \beta_{ji})$$

$$P_j = w_A A + w_B B + w_C C$$

where

$$w_A + w_B + w_C = 1, \quad A = V_A(x_A), \quad B = V_B(x_B), \quad C = V_C(x_C)$$

and

$$0 \leq V_A(x_A), V_B(x_B), V_C(x_C) \leq 100, \text{ and } 0 \leq P_i, P_j \leq 100.$$

**Example 5.11:** Formulate the FDNA equations for the graph in Figure 61

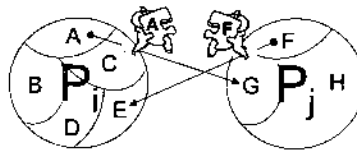


Figure 61. A 2,2,2-Node FDNA Graph

The graph in Figure 61 consists of two nodes  $P_i$  and  $P_j$ , two dependency points, and one receiver node  $P_j$ . Nodes  $P_i$  and  $P_j$  are constituent nodes. Component  $A$  in constituent node  $P_i$  is a feeder to component  $G$  in constituent node  $P_j$ . Component  $F$  in constituent node  $P_j$  is a feeder to component  $E$  in constituent node  $P_i$ .

The FDNA dependency function for this graph is given by the following equations.

$$P_i \equiv w_A A + w_B B + w_C C + w_D D + w_E E \quad (5.26)$$

$$P_j \equiv w_F F + w_G G + w_H H \quad (5.27)$$

where  $E = \text{Min}(\text{SODE}_F, \text{CODE}_F) = \text{Min}(\alpha_{FE} F + 100(1 - \alpha_{FE}), F + \beta_{FE}) \quad (5.28)$

$$G = \text{Min}(\text{SODG}_A, \text{CODG}_A) = \text{Min}(\alpha_{AG} A + 100(1 - \alpha_{AG}), A + \beta_{AG}) \quad (5.29)$$

$$w_A + w_B + w_C + w_D + w_E = 1, \quad w_F + w_G + w_H = 1$$

$$A = V_A(x_A), \quad B = V_B(x_B), \quad C = V_C(x_C), \quad D = V_D(x_D), \quad \text{and} \quad F = V_F(x_F)$$

are single dimensional value functions for  $A, B, C, D$ , and  $F$ , respectively, where

$$0 \leq V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), V_F(x_F) \leq 100 \quad \text{and} \quad 0 \leq P_i, P_j \leq 100$$

**Example 5.12:** Formulate the FDNA equations for the graph in Figure 62.

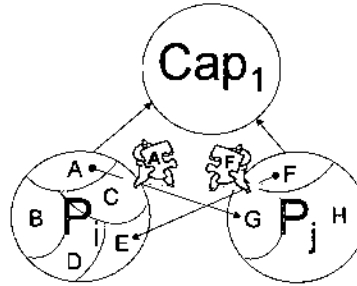


Figure 62. A 3,4,3-Node FDNA Graph: Constituent and Single Component Nodes

The graph in Figure 62 consists of three nodes  $P_i$ ,  $P_j$ , and  $Cap_1$ , four dependency points, and three receiver nodes  $P_i$ ,  $P_j$ , and  $Cap_1$ . Nodes  $P_i$  and  $P_j$  are constituent nodes. Component  $A$  in constituent node  $P_i$  is a feeder to component  $G$  in constituent node  $P_j$ . Component  $F$  in constituent node  $P_j$  is a feeder to component  $E$  in constituent node  $P_i$ .

The FDNA dependency function for this graph is given by the following equations.

$$Cap_1 = \text{Min}(\text{Ave}(\text{SODCap}_{1i}, \text{SODCap}_{1j}), \text{CODCap}_{1i}, \text{CODCap}_{1j})$$

$$Cap_1 = \text{Min}\left(\frac{\alpha_{iCap_1} P_i}{2} + \frac{\alpha_{jCap_1} P_j}{2} + 100(1 - (\frac{\alpha_{iCap_1} + \alpha_{jCap_1}}{2})), P_i + \beta_{iCap_1}, P_j + \beta_{jCap_1}\right)$$

where, from Example 5.11, we have

$$P_i \equiv w_A A + w_B B + w_C C + w_D D + w_E E \quad (5.30)$$

$$P_j \equiv w_F F + w_G G + w_H H \quad (5.31)$$

$$E = \text{Min}(\text{SODE}_F, \text{CODE}_F) = \text{Min}(\alpha_{FE} F + 100(1 - \alpha_{FE}), F + \beta_{FE}) \quad (5.32)$$

$$G = \text{Min}(\text{SODG}_A, \text{CODG}_A) = \text{Min}(\alpha_{AG} A + 100(1 - \alpha_{AG}), A + \beta_{AG}) \quad (5.33)$$

where

$$w_A + w_B + w_C + w_D + w_E = 1, \quad w_F + w_G + w_H = 1$$

$$A = V_A(x_A), \quad B = V_B(x_B), \quad C = V_C(x_C), \quad D = V_D(x_D), \quad \text{and} \quad F = V_F(x_F)$$

are single dimensional value functions for  $A$ ,  $B$ ,  $C$ ,  $D$ , and  $F$ , respectively, where,

$$0 \leq V_A(x_A), V_B(x_B), V_C(x_C), V_D(x_D), V_F(x_F), P_i, P_j, \text{Cap}_1 \leq 100$$

In FDNA, capturing dependence between pairs of nodes involves more than identifying a joint relationship exists. It is necessary to identify *why* the operability of one node depends on the operability of the other (and vice-versa) and *what* drives their relationship.

In general, a node's operability is really a "summation" or a "reflection" of the operability of its underlying components. The following illustrates the importance of this, especially in situations where dependencies are present between nodes and components in an FDNA graph.

**Example 5.13: Specification of Dependence**

This example illustrates the importance of specification between dependent nodes and especially when a mutual (cycle) dependence is present. Specification seeks to identify why a dependency exists and what these dependent nodes rely on from each other. The following demonstrates the specification of dependence through a simple example of the relationship of hands-to-body. This example illustrates concepts instead of a full depiction of the intricacies of this dependency.

It is reasonable to assert the operability of hands relies on the operability of the body. If the body must be self-reliant, then the operability of the body relies on the operability of the hands. We now have mutual dependence between hands and body. But what does this really mean? To answer this, it is necessary to specify *why* the operability of the hands depends on the operability of the body (and vice-versa) and *what* drives their mutual relationship. Consider Figure 63.

In Figure 63, we see that dependence can involve three levels of specification. The first level is identifying a dependency exists between two nodes (e.g., Hands and Body). In this case, the dependency is mutual. The next level is the component view of the dependency. This view begins to specify the "why" for the relationship. Here, level 2 shows two components for Hands – the Finger System (FS) and the Hand Skeletal System (HSS). Likewise, three components are shown for the Body – the Circulation System (CS), the Central Nervous System (CNS), and the Motor Grasp System (MGS).

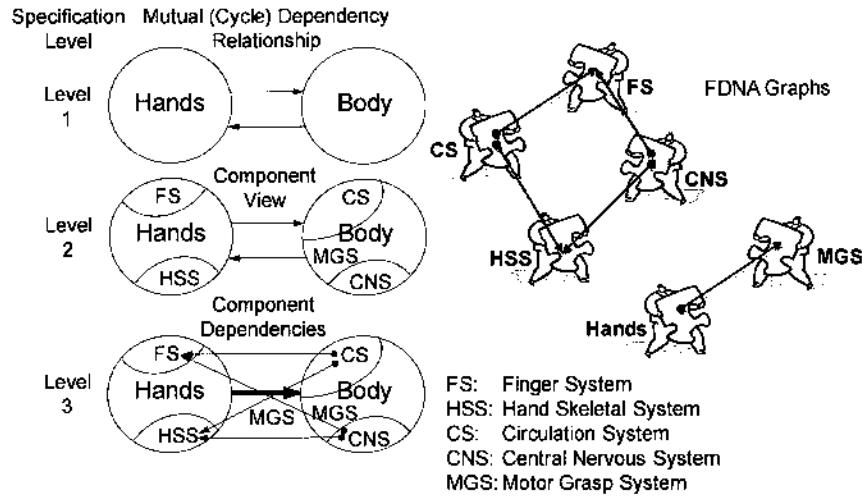


Figure 63. Specification Levels, Dependence, Constituent Nodes, and Components

Level 3 shows the component dependencies. This further addresses the “why” and now the “what” of the mutual dependence (in this case) between Hands and Body.

In Figure 63, suppose the operability of the Finger System depends on (1) the operability of the Body’s Circulation System (CS) for blood flow and (2) the operability of the Body’s Central Nervous System (CNS) for movement. Suppose the Hand Skeletal System (HSS) depends on the operability of the Body’s CS and CNS for the same reasons. In Figure 63, suppose the thick arrow indicates the operability of the Body’s Motor Grasp System (MGS) depends on the operability of the Hands for the Body to be operationally self-reliant, as required.

In Figure 63, the right-most side is an FDNA graph of the dependency relationships derived from the Level 3 specification shown at the left. From the FDNA graph, we can then build the FDNA equations for the dependencies between Hands and Body. These are as follows:

$$FS = \text{Min} \left( \frac{\alpha_{CSFS} CS}{2} + \frac{\alpha_{CNSFS} CNS}{2} + 100(1 - (\frac{\alpha_{CSFS} + \alpha_{CNSFS}}{2})), CS + \beta_{CSFS}, CNS + \beta_{CNSFS} \right)$$

$$HSS = \text{Min} \left( \frac{\alpha_{CSHSS} CS}{2} + \frac{\alpha_{CNSHSS} CNS}{2} + 100(1 - (\frac{\alpha_{CSHSS} + \alpha_{CNSHSS}}{2})), CS + \beta_{CSHSS}, CNS + \beta_{CNSHSS} \right)$$

$$\text{Hands} = H = w_1 FS + w_2 HSS$$

$$\text{Body} = B = u_1 CS + u_2 CNS + u_3 MGS$$

where  $MGS = \text{Min}(\alpha_{HB} H + 100(1 - \alpha_{HB}), H + \beta_{HB})$  and  $w_1 + w_2 = 1$ ,  $u_1 + u_2 + u_3 = 1$ ; and,  $CS = V_{CS}(x_{CS})$ ,  $CNS = V_{CNS}(x_{CNS})$  are single dimensional value functions for CS and CNS, respectively, where,  $0 \leq V_{CS}(x_{CS}), V_{CNS}(x_{CNS}), FS, HSS, MGS, H, B \leq 100$ .

### FDNA Dependency Function Regulation

This discussion demonstrates how the FDNA dependency function can be regulated to model the realities of a specific dependency relationship. It is an elaboration on Postulate 5.11, which states *a receiver node may become wholly operable before its feeder node is wholly operable*.

Thus far, FDNA equations had the property that a receiver node becomes wholly operable when its feeder node is wholly operable. Although this property is reasonable, situations might arise where a receiver node can become wholly operable when its feeder node achieves less than full operability. Capturing this situation in the FDNA calculus is called *regulation*.

Regulation is an FDNA calibration process. It involves adjusting the strength of dependency fraction  $\alpha_{ij}$  above its computed value\* to enable a receiver node to increase in operability at a rate faster than the rate governed by  $\alpha_{ij}$ . The parameter  $\alpha'_{ij}$  denotes the adjusted  $\alpha_{ij}$ . It is called the *regulated strength of dependency fraction* and is restricted to the interval  $0 < \alpha_{ij} \leq \alpha'_{ij} \leq 1$ .

#### Weakest Link FDNA Dependency Function Under Regulation

The following presents a general formulation of the weakest link FDNA dependency function under *regulation*. For convenience, we restrict this formulation to a receiver node  $P_j$  with a single feeder node  $P_i$  – the 2,1,1,R FDNA graph\*\* shown in Figure 64. Extension of this graph to a multi-feeder node scenario (under regulation) is straightforward.

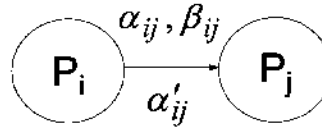


Figure 64. A 2,1,1,R FDNA Graph:  
Regulated SOD Fraction  $\alpha'_{ij}$

#### Definition 5.8: Weakest Link FDNA Dependency Function Under Regulation

Under regulation, the operability level of receiver node  $P_j$  that is dependent on the operability level of feeder node  $P_i$  is given by

$$0 \leq P_j = \text{Min} (\alpha'_{ij} P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij}) \leq 100 \quad (5.34)$$

where  $0 < \alpha_{ij} \leq \alpha'_{ij} \leq 1$ ,  $100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ ,  $BOLP_j = 100(1 - \alpha_{ij})$

and (1)  $0 \leq P_j \leq 100$  with  $0 \leq P_i \leq 100 - \beta_{ij}$  if  $P_j(100 - \beta_{ij}) = 100$

or (2)  $0 \leq P_j \leq 100$  with  $0 \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$  if  $P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$

\* Refer to the *SOD Question Protocol* in Chapter V for computing  $\alpha_{ij}$  from  $BOLP_j$ .

\*\* The "R" indicates  $\alpha'_{ij}$  is a regulation parameter in the FDNA equations developed for the respective FDNA graph.

**Theorem 5.3: COD/SOD Cross-Over Point Under Regulation**

Suppose receiver node  $P_j$  has a dependency relationship on feeder node  $P_i$ . Suppose the operability level of  $P_j$  is given by the weakest link FDNA dependency function under regulation.

**Part A**

If

$$P_j(100 - \beta_{ij}) < P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then the operability level of  $P_j$  will cross-over from being determined by  $CODP_j$  to being determined by  $SODP_j$  when

$$P_i = \frac{1}{1 - \alpha'_{ij}} (BOLP_j - \beta_{ij}) \text{ utils} \quad (5.35)$$

where  $0 \leq P_j \leq 100$ , with

$$0 \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}}, \quad 0 < \alpha_{ij} \leq \alpha'_{ij} < 1, \quad 100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}), \quad BOLP_j = 100(1 - \alpha_{ij}).$$

Equation 5.35 is called the **COD/SOD cross-over point under regulation**.

Prior to the cross-over point, the operability level of  $P_j$  is determined by  $CODP_j$  in the interval

$$0 \leq P_i \leq \frac{1}{1 - \alpha'_{ij}} (BOLP_j - \beta_{ij})$$

Subsequent to the cross-over point, the operability level of  $P_j$  is determined by  $SODP_j$  in the interval

$$\frac{1}{1 - \alpha'_{ij}} (BOLP_j - \beta_{ij}) \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \leq 100$$

and  $P_j$  becomes wholly operable when  $P_i = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$ .

**Part B**

If

$$P_j(100 - \beta_{ij}) > P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then the operability level of  $P_j$  is determined strictly by  $CODP_j$  and  $P_j$  becomes wholly operable when

$$P_i = 100 - \beta_{ij}$$

where  $0 \leq P_j \leq 100$  with

$$0 \leq P_i \leq 100 - \beta_{ij}, 0 < \alpha_{ij} \leq \alpha'_{ij} < 1, 100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}), BOLP_j = 100(1 - \alpha_{ij}).$$

### Part C

If

$$P_j(100 - \beta_{ij}) = P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then  $CODP_j = SODP_j = 100$  when  $P_j$  becomes wholly operable at

$$P_i = 100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

where  $0 \leq P_j \leq 100$  with

$$0 \leq P_i \leq 100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

and

$$0 < \alpha_{ij} \leq \alpha'_{ij} < 1, 100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}), BOLP_j = 100(1 - \alpha_{ij}).$$

### Proof

Throughout this proof, receiver node  $P_j$  has a dependency relationship with feeder node  $P_i$  with the weakest link FDNA dependency function under regulation. The following presents a proof for each part of Theorem 5.3.

### Part A

First, we establish general results that derive from Definition 5.8\*. We then use these results to prove Part A.

In general, the operability level of  $P_j$  is strictly determined by  $CODP_j$  when

$$P_i + \beta_{ij} < \alpha'_{ij} P_i + 100(1 - \alpha_{ij})$$

---

\* These results are analogous to, and consistent with, Property 5.3 (COD/SOD Cross-Over Point) in Chapter V.



$$\Rightarrow P_i < \frac{1}{(1 - \alpha'_{ij})} (BOLP_j - \beta_{ij}) \quad (5.36)$$

In general, the operability level of  $P_j$  is strictly determined by  $SODP_j$  when

$$\begin{aligned} \alpha'_{ij} P_i + 100(1 - \alpha_{ij}) &< P_i + \beta_{ij} \\ \Rightarrow P_i &> \frac{1}{(1 - \alpha'_{ij})} (BOLP_j - \beta_{ij}) \end{aligned} \quad (5.37)$$

In general, when

$$P_i = \frac{1}{1 - \alpha'_{ij}} (BOLP_j - \beta_{ij}) \quad (5.38)$$

we can write this as

$$\begin{aligned} (1 - \alpha'_{ij}) P_i &= (BOLP_j - \beta_{ij}) \\ \Rightarrow (1 - \alpha'_{ij}) P_i &= 100(1 - \alpha_{ij}) - \beta_{ij} \\ \Rightarrow P_i - \alpha'_{ij} P_i &= 100(1 - \alpha_{ij}) - \beta_{ij} \\ \Rightarrow P_i + \beta_{ij} &= \alpha'_{ij} P_i + 100(1 - \alpha_{ij}) \\ \Rightarrow CODP_j &= SODP_j \end{aligned}$$

since  $CODP_j = P_i + \beta_{ij}$  and  $SODP_j = \alpha'_{ij} P_i + 100(1 - \alpha_{ij})$  in accordance with the definition of the weakest link FDNA dependency function. The value of  $P_i$  produced by Equation 5.38 is called the *COD/SOD cross-over point*. From inequalities 5.37 and 5.38, we have  $P_j = SODP_j$  for all  $P_i$  in the interval

$$\frac{1}{1 - \alpha'_{ij}} (BOLP_j - \beta_{ij}) \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \leq 100$$

where  $0 \leq P_j \leq 100$ . To complete the proof of Part A, we need only establish a COD/SOD cross-over point exists when

$$P_j (100 - \beta_{ij}) < P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

Once this is done, the above results directly follow and will complete the proof. If the following inequality is true

$$P_j(100 - \beta_{ij}) < P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then

$$100 - \beta_{ij} < 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

since  $P_j$  is a monotonically increasing function of  $P_i$ . Next, we can write

$$100 - \beta_{ij} < 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \Rightarrow 100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}} - \varepsilon \text{ for some } \varepsilon > 0$$

$$\Rightarrow (100 - \beta_{ij}) + \varepsilon = 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \text{ for some } \varepsilon > 0$$

If  $P_i = 100 - \beta_{ij}$  then

$$COP_j(100 - \beta_{ij}) < COP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

Since

$$COP_j(100 - \beta_{ij}) = (100 - \beta_{ij}) + \beta_{ij} = 100$$

$$COP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = (100 - \beta_{ij} + \varepsilon) + \beta_{ij} = 100 + \varepsilon, \varepsilon > 0$$

Thus,

$$COP_j(100 - \beta_{ij}) < COP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) \text{ since } \varepsilon > 0$$

If  $P_i = 100 - \beta_{ij}$  then

$$SOP_j(100 - \beta_{ij}) < SOP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

Since

$$SOP_j(100 - \beta_{ij}) = \alpha'_{ij}(100 - \beta_{ij}) + 100(1 - \alpha_{ij})$$

$$SOP_j(100 - \beta_{ij}) = \alpha'_{ij} \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} - \varepsilon \right) + 100(1 - \alpha_{ij})$$

$$SODP_j(100 - \beta_{ij}) = 100 - \alpha'_{ij}\varepsilon, \quad 0 < \alpha_{ij} \leq \alpha'_{ij} < 1, \quad \varepsilon > 0$$

$$SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = \alpha'_{ij} 100 \frac{\alpha_{ij}}{\alpha'_{ij}} + 100(1 - \alpha_{ij}) = 100$$

Thus,

$$SODP_j(100 - \beta_{ij}) < SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) \text{ since } \varepsilon > 0$$

Combining these results, we have

$$SODP_j(100 - \beta_{ij}) < CODP_j(100 - \beta_{ij}) = 100$$

since  $100 - \alpha'_{ij}\varepsilon < 100$  where  $0 < \alpha_{ij} \leq \alpha'_{ij} < 1, \quad \varepsilon > 0$ . From this, at  $P_i = 100 - \beta_{ij}$

$$P_j = \text{Min}(SODP_j(100 - \beta_{ij}), CODP_j(100 - \beta_{ij})) = \text{Min}(SODP_j(100 - \beta_{ij}), 100)$$

$$\Rightarrow P_j = SODP_j(100 - \beta_{ij}) = 100 - \alpha'_{ij}\varepsilon < 100 = CODP_j(100 - \beta_{ij})$$

In general, if a COD/SOD cross-over point exists, then there must be an operability level for  $P_i$  where  $CODP_j(P_i) = 100$  (its maximum) but  $SODP_j(P_i) < 100$ . Seen above, and in Property 5.3, it is always true that  $CODP_j = P_i + \beta_{ij} = 100$  when  $P_i = 100 - \beta_{ij}$ . Given the conditions in Part A, we have shown that  $SODP_j(100 - \beta_{ij}) = 100 - \alpha'_{ij}\varepsilon < 100 = CODP_j(100 - \beta_{ij})$ ,  $\varepsilon > 0$ . Thus, subject to the conditions in Part A, a cross-over point will exist and be contained in the interval

$$0 < P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

Finally,

$$P_j = SODP_j \text{ for } \frac{1}{1 - \alpha'_{ij}}(BOLP_j - \beta_{ij}) \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \leq 100$$

and  $P_j$  becomes wholly operable when  $P_i = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$ , where  $0 \leq P_j \leq 100$  with

$$0 \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \text{ and } 0 < \alpha_{ij} \leq \alpha'_{ij} < 1, \quad 100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}),$$

$$BOLP_j = 100(1 - \alpha_{ij})$$

This completes the proof of Part A.

**Part B**

If the following inequality is true

$$P_j(100 - \beta_{ij}) > P_j\left(100 \frac{\alpha_{ij}}{\alpha'_{ij}}\right)$$

then  $100 - \beta_{ij} > 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$

since  $P_j$  is a monotonically increasing function of  $P_i$ . Next, we can write

$$100 - \beta_{ij} > 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \Rightarrow 100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}} + \varepsilon \text{ for some } \varepsilon > 0$$

If  $P_i = 100 - \beta_{ij}$  then

$$CODP_j(100 - \beta_{ij}) > CODP_j\left(100 \frac{\alpha_{ij}}{\alpha'_{ij}}\right)$$

Since

$$CODP_j(100 - \beta_{ij}) = (100 - \beta_{ij}) + \beta_{ij} = 100$$

$$CODP_j\left(100 \frac{\alpha_{ij}}{\alpha'_{ij}}\right) = (100 - \beta_{ij} - \varepsilon) + \beta_{ij} = 100 - \varepsilon, \varepsilon > 0$$

Thus,

$$CODP_j(100 - \beta_{ij}) > CODP_j\left(100 \frac{\alpha_{ij}}{\alpha'_{ij}}\right) \text{ since } \varepsilon > 0$$

If  $P_i = 100 - \beta_{ij}$  then

$$SODP_j(100 - \beta_{ij}) > SODP_j\left(100 \frac{\alpha_{ij}}{\alpha'_{ij}}\right)$$

Since

$$SODP_j(100 - \beta_{ij}) = \alpha'_{ij}(100 - \beta_{ij}) + 100(1 - \alpha_{ij})$$

$$SODP_j(100 - \beta_{ij}) = \alpha'_{ij}\left(100 \frac{\alpha_{ij}}{\alpha'_{ij}} + \varepsilon\right) + 100(1 - \alpha_{ij})$$

$$SODP_j(100 - \beta_{ij}) = 100 + \alpha'_{ij}\varepsilon, \quad 0 < \alpha_{ij} \leq \alpha'_{ij} < 1, \quad \varepsilon > 0$$

$$SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = \alpha'_{ij} 100 \frac{\alpha_{ij}}{\alpha'_{ij}} + 100(1 - \alpha_{ij}) = 100$$

Thus, 
$$SODP_j(100 - \beta_{ij}) > SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) \text{ since } \varepsilon > 0$$

Combining these results, we have

$$SODP_j(100 - \beta_{ij}) > CODP_j(100 - \beta_{ij})$$

since  $100 + \alpha'_{ij}\varepsilon > 100$  where  $0 < \alpha_{ij} \leq \alpha'_{ij} < 1$ ,  $\varepsilon > 0$ . Therefore, if

$$P_j(100 - \beta_{ij}) > P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then the operability level of  $P_j$  is determined strictly by  $CODP_j$  and  $P_j$  becomes wholly operable when

$$P_i = 100 - \beta_{ij}$$

where  $0 \leq P_j \leq 100$  with

$$0 \leq P_i \leq 100 - \beta_{ij}, \quad 0 < \alpha_{ij} \leq \alpha'_{ij} < 1, \quad 100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}), \quad BOLP_j = 100(1 - \alpha_{ij}).$$

This completes the proof of Part B.

### Part C

If the following is true

$$P_j(100 - \beta_{ij}) = P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then 
$$100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

since  $P_j$  is a monotonically increasing function of  $P_i$ . Next, we can write

$$100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \Rightarrow \alpha'_{ij} = \frac{100\alpha_{ij}}{100 - \beta_{ij}} \text{ or } \beta_{ij} = 100 \left( 1 - \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

If  $P_i = 100 - \beta_{ij}$  then

$$CODP_j(100 - \beta_{ij}) = SODP_j(100 - \beta_{ij}) = 100$$

since

$$CODP_j(100 - \beta_{ij}) = (100 - \beta_{ij}) + \beta_{ij} = 100$$

$$SODP_j(100 - \beta_{ij}) = \alpha'_{ij} P_i + 100(1 - \alpha_{ij})$$

$$SODP_j(100 - \beta_{ij}) = \left( \frac{100\alpha_{ij}}{100 - \beta_{ij}} \right) (100 - \beta_{ij}) + 100(1 - \alpha_{ij}) = 100$$

Therefore

$$CODP_j(100 - \beta_{ij}) = SODP_j(100 - \beta_{ij}) = 100$$

If  $P_i = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$  then

$$CODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$$

since

$$CODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100 \frac{\alpha_{ij}}{\alpha'_{ij}} + \beta_{ij}$$

$$CODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100 \frac{\alpha_{ij}}{\alpha'_{ij}} + 100 \left( 1 - \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$$

$$SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = \alpha'_{ij} 100 \frac{\alpha_{ij}}{\alpha'_{ij}} + 100(1 - \alpha_{ij}) = 100$$

Therefore

$$CODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$$

Combining these results, we have

$$SODP_j(100 - \beta_{ij}) = CODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$$

$$CODP_j(100 - \beta_{ij}) = SODP_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$$

Therefore, if

$$P_j(100 - \beta_{ij}) = P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

then  $CODP_j = SODP_j = 100$  when  $P_j$  becomes wholly operable at

$$P_i = 100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

where  $0 \leq P_j \leq 100$  with

$$0 \leq P_i \leq 100 - \beta_{ij} = 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$$

and

$$0 < \alpha_{ij} \leq \alpha'_{ij} < 1, 100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}), BOLP_j = 100(1 - \alpha_{ij}).$$

This completes the proof of Part C.

Last, we note if

$$\alpha_{ij} = \alpha'_{ij}$$

then the COD/SOD cross-over point under regulation reduces to the classic COD/SOD cross-over point presented by Property 5.3. This is intuitive and easy to show. This completes the proof of Theorem 5.3.

In Theorem 5.3, the strength of dependence fraction interval  $0 < \alpha_{ij} \leq \alpha'_{ij} < 1$  is tighter than in Definition 5.8, where  $0 < \alpha_{ij} \leq \alpha'_{ij} \leq 1$ . What happens when  $\alpha'_{ij} = 1$ ? This is discussed next.

**Theorem 5.4: Maximum Regulation**

Suppose receiver node  $P_j$  has a dependency relationship on feeder node  $P_i$  with the weakest link FDNA dependency function under regulation. If  $P_j$  has a maximum regulated strength of dependency on  $P_i$  then the operability level of  $P_j$  is strictly determined by  $CODP_j$ , where  $P_i$  operates in the interval  $0 \leq P_i \leq 100 - \beta_{ij}$ .

**Proof**

Since receiver node  $P_j$  has a dependency relationship on feeder node  $P_i$  with the weakest link FDNA dependency function under regulation, from Definition 5.8 we can write

$$0 \leq P_j = \text{Min}(\alpha'_{ij}P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij}) \leq 100$$

where  $0 < \alpha_{ij} \leq \alpha'_{ij} \leq 1$ ,  $100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ ,  $BOLP_j = 100(1 - \alpha_{ij})$

and (1)  $0 \leq P_j \leq 100$  with  $0 \leq P_i \leq 100 - \beta_{ij}$  if  $P_j(100 - \beta_{ij}) = 100$

or (2)  $0 \leq P_j \leq 100$  with  $0 \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$  if  $P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$

Since  $P_j$  has a maximum regulated strength of dependency on  $P_i$ , we have  $\alpha'_{ij} = 1$ ; thus,

$$P_j = \text{Min}(1 \cdot P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij}) = \text{Min}(P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij})$$

where  $0 < \alpha_{ij} \leq \alpha'_{ij} \leq 1$ ,  $100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ ,  $BOLP_j = 100(1 - \alpha_{ij})$ . From this, it follows that

$$(1) P_j = P_i + \beta_{ij} = CODP_j \text{ if } P_i + \beta_{ij} \leq P_i + 100(1 - \alpha_{ij})$$

or (2)  $P_j = P_i + 100(1 - \alpha_{ij}) = SODP_j$  if  $P_i + 100(1 - \alpha_{ij}) \leq P_i + \beta_{ij}$

Outcome (1) is always true since  $P_i + \beta_{ij} \leq P_i + 100(1 - \alpha_{ij})$  implies  $\beta_{ij} \leq 100(1 - \alpha_{ij})$ . From the Property 5.5, we know  $\beta_{ij}$  is always bounded above by  $100(1 - \alpha_{ij})$ . From Property 5.5, we know outcome (2) is impossible since  $\beta_{ij}$  cannot be greater than  $100(1 - \alpha_{ij})$ . Thus, if  $P_j$  has a maximum regulated strength of dependency on  $P_i$  then the operability level of  $P_j$  is strictly determined by  $CODP_j$ . The following is another approach to this proof.

Under regulation, it can be shown that  $100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ . From this, if  $\alpha'_{ij} = 1$  then  $100(1 - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij})$ . This implies  $\beta_{ij} = 100(1 - \alpha_{ij})$ . Thus, if  $\alpha'_{ij} = 1$  then

$$P_j = \text{Min}(P_i + 100(1 - \alpha_{ij}), P_i + \beta_{ij}) = \text{Min}(P_i + \beta_{ij}, P_i + \beta_{ij}) = P_i + \beta_{ij} = CODP_j$$

The following presents computational examples that illustrate some of the theory presented in these theorems. Each involves the use of regulation in the FDNA graph and equations.



**Example 5.14:** Suppose the data in Table 9 is for the 2,1,1,R-node dependency relationship in Figure 64. An operability analysis is conducted and summarized in the lower-half of Table 9.

**A 2-Node FDNA Graph: 1-Dependency Point, 1-Receiver Node  $P_j$ , With Regulation**

|  |       |  |
|--|-------|--|
| INPUT: MEOLP <sub>j</sub>                        | 85    | Definition 5.5                           |
| INPUT: BOLP <sub>j</sub>                         | 50    | Figure 5.4                               |
| COMPUTED: $\alpha$ -Dependency Fraction          | 0.50  | Figure 5.4                               |
| COMPUTED: Beta Anchor Point (Regulated)          | 26.67 | Property 5.4 But Modified For Regulation |
| COMPUTED: Beta Lower Bound                       | 10    | Property 5.5 But Modified For Regulation |
| COMPUTED: Beta Upper Bound                       | 50    | Property 5.5                             |
| INPUT: $\alpha$ -Dependency Fraction (Regulated) | 0.60  | Definition 5.8                           |
| INPUT: Beta Assigned/Setting                     | 20    | Assigned/Set                             |

| Feeder Node $P_i$          | SODP <sub>j</sub> | CODP <sub>j</sub> | $P_j$ Operability Level =<br>Min{SODP <sub>j</sub> , CODP <sub>j</sub> } | $P_j$ Operability Level<br>Determined By |
|----------------------------|-------------------|-------------------|--|--|
| 0                          | 50                | 20                | 20   | COD                                      |
| 5                          | 53                | 25                | 25   | COD                                      |
| 10                         | 56                | 30                | 30   | COD                                      |
| 15                         | 59                | 35                | 35   | COD                                      |
| 20                         | 62                | 40                | 40   | COD                                      |
| 25                         | 65                | 45                | 45   | COD                                      |
| 30                         | 68                | 50                | 50   | COD                                      |
| 35                         | 71                | 55                | 55   | COD                                      |
| 40                         | 74                | 60                | 60   | COD                                      |
| 45                         | 77                | 65                | 65   | COD                                      |
| 50                         | 80                | 70                | 70   | COD                                      |
| 55                         | 83                | 75                | 75   | COD                                      |
| 60                         | 86                | 80                | 80   | COD                                      |
| 65                         | 89                | 85                | 85   | COD                                      |
| 70                         | 92                | 90                | 90   | COD                                      |
| 75                         | 95                | 95                | 95   | COD/SOD                                  |
| 80                         | 98                | 100               | 98   | SOD                                      |
| 83.33333333                | 100               | 103.3333          | 100  | SOD                                      |
| Cross Over Point For $P_i$ | 75                |                   |  |  |
| Cross Over Score for $P_j$ | 95                |                   |  |  |

From This Point SODP<sub>j</sub> Drives  $P_j$ 's Operability Level

**Table 9. An Operability Analysis of a 2,1,1,R-Node FDNA Graph:  
COD/SOD Cross-Over Point in Range**

Four inputs are shown in Table 9. These are  $MEOLP_j$  and  $BOLP_j$ , the regulated  $\alpha$ -dependency fraction, and the criticality of dependency parameter  $\beta_{ij}$ . Here, receiver node  $P_j$  must reach a minimum operability level of 85 utils. However, its current baseline operability level is 50 utils. So, receiver node  $P_j$  relies on contributions from feeder node  $P_i$  to improve its baseline operability to the minimum effective level required by stakeholders.

Table 9 shows a regulated  $\alpha$ -dependency fraction of 0.60 and that  $P_j$ 's dependence on contributions from  $P_i$  is somewhat critical. Here, the criticality of dependency parameter is set at 20 in the range  $10 \leq \beta_{ij} \leq 50$ .

The outputs in the upper left corner of Table 9 are the strength of dependency fraction  $\alpha_{ij}$ , the beta anchor point, and the beta lower and upper bounds. These outputs were computed from the inputs in Table 9; specifically,

The  $\alpha_{ij}$ -dependency fraction:  $100(1 - \alpha_{ij}) = BOLP_j = 50 \Rightarrow \alpha_{ij} = 0.50$

The beta anchor point **under regulation**, which is easily derived, is

$$MEOLP_j \frac{(\alpha'_{ij} - 1)}{\alpha'_{ij}} + 100 \frac{(1 - \alpha_{ij})}{\alpha'_{ij}} = 26.67$$

The beta lower and upper bounds **under regulation**, which is easily derived, is:

$$100(\alpha'_{ij} - \alpha_{ij}) \leq \beta_{ij} \leq 100(1 - \alpha_{ij}) \Rightarrow 10 \leq \beta_{ij} \leq 50$$

The last set of outputs in Table 9 show the operability level of  $P_j$  as a function of the operability level of  $P_i$ , for  $0 \leq P_i, P_j \leq 100$ . The following are a few observations:

(1) Feeder node  $P_i$  must achieve an operability level of 65 utils for receiver node  $P_j$  to achieve its MEOL. Here,  $P_j$  achieves its MEOL under a rate governed by  $CODP_j$ .

(2) From Theorem 5.3, a COD/SOD cross-over point exists in  $0 \leq P_i, P_j \leq 100$  since

$$P_j(100 - \beta_{ij}) < P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

and, from Definition 5.8  $P_j(100 - \beta_{ij}) = P_j(80) = \text{Min}(0.60(80) + 100(1 - 0.50), 80 + 20) = 98$

$$P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = P_j(83.33) = \text{Min}(0.60(83.33) + 100(1 - 0.50), 83.33 + 20) = 100$$

From Theorem 5.3, the cross-over point occurs when feeder node  $P_i$  achieves

$$P_i = \frac{1}{1 - \alpha'_{ij}} (BOLP_j - \beta_{ij}) = \frac{1}{1 - 0.60} (50 - 20) = 75$$

From this point, the operability improvement in receiver node  $P_j$  transitions from being determined by  $CODP_j$  to being determined by  $SODP_j$ . Receiver node  $P_j$  continues to improve in operability with increasing operability in  $P_i$  but it will now improve at a rate slower than it did when its operability level was determined by  $CODP_j$ .

(3) If feeder node  $P_i$ 's contribution is equal to zero in operational utility to receiver node  $P_j$  then  $P_j$  will degrade from its baseline operability level of 50 utils to 20 utils, rendering  $P_j$  somewhat inoperable.

**Example 5.15:** Suppose the data in Table 10 is for the 2,1,1,R-node dependency relationship in Figure 64. An operability analysis is conducted and summarized in the lower-half of Table 10.

| A 2-Node FDNA Graph: 1-Dependency Point, 1-Receiver Node $P_j$ , With Regulation |       |  |  |  |  |
|--|-------|--|--|--|--|
| INPUT: MEOLP <sub>j</sub>  | 85    | Definition 5.5                           |  |  |  |
| INPUT: BOLP <sub>j</sub>   | 50    | Figure 5.4                               |  |  |  |
| COMPUTED: $\alpha$ -Dependency Fraction  | 0.50  | Figure 5.4                               |  |  |  |
| COMPUTED: Beta Anchor Point ( <b>Regulated</b> )                                 | 35.00 | Property 5.4 But Modified For Regulation |  |  |  |
| COMPUTED: Beta Lower Bound   | 20    | Property 5.5 But Modified For Regulation |  |  |  |
| COMPUTED: Beta Upper Bound   | 50    | Property 5.5                             |  |  |  |
| INPUT: $\alpha$ -Dependency Fraction ( <b>Regulated</b> )                        | 0.70  | Definition 5.8                           |  |  |  |
| INPUT: Beta Assigned/Setting   | 20    | Assigned/Set                             |  |  |  |

| Feeder Node $P_i$ | SODP <sub>j</sub> | CODP <sub>j</sub> | $P_j$ Operability Level =<br>Min(SODP <sub>j</sub> , CODP <sub>j</sub> ) | $P_j$ Operability Level<br>Determined By |
|-------------------|-------------------|-------------------|--|--|
| 0                 | 50                | 20                | 20   | COD                                      |
| 5                 | 53.5              | 25                | 25   | COD                                      |
| 10                | 57                | 30                | 30   | COD                                      |
| 15                | 60.5              | 35                | 35   | COD                                      |
| 20                | 64                | 40                | 40   | COD                                      |
| 25                | 67.5              | 45                | 45   | COD                                      |
| 30                | 71                | 50                | 50   | COD                                      |
| 35                | 74.5              | 55                | 55   | COD                                      |
| 40                | 78                | 60                | 60   | COD                                      |
| 45                | 81.5              | 65                | 65   | COD                                      |
| 50                | 85                | 70                | 70   | COD                                      |
| 55                | 88.5              | 75                | 75   | COD                                      |
| 60                | 92                | 80                | 80   | COD                                      |
| 65                | 95.5              | 85                | 85   | COD                                      |
| 70                | 99                | 90                | 90   | COD                                      |
| 75                | 102.5             | 95                | 95   | COD                                      |
| 80                | 106               | 100               | 100  | COD                                      |

Table 10. An Operability Analysis of a 2,1,1,R-Node FDNA Graph:  
COD/SOD Cross-Over Point Not in Range

Table 10 has the same data as in Table 9 with one exception. Table 10 shows a regulated  $\alpha$ -dependency fraction of 0.70 instead of 0.60. Because of this, a COD/SOD cross-over point does not exist in  $0 \leq P_i, P_j \leq 100$  since, in accordance with Theorem 5.3 we have

$$P_j(100 - \beta_{ij}) > P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right)$$

When this occurs, the operability level of  $P_j$  is determined strictly by  $CODP_j$  and  $P_j$  becomes wholly operable, in accordance with Theorem 5.3, when  $P_i = 100 - \beta_{ij} = 100 - 20 = 80$ .

**Example 5.16:** Suppose the data in Table 11 is for the 2,1,1,R-node dependency relationship in Figure 64. An operability analysis is conducted and summarized in the lower-half of Table 11. These results are compared to those in Table 6.

| A 2-Node FDNA Graph: 1-Dependency Point, 1-Receiver Node $P_j$ , With Regulation |                   |   |  |  |
|--|-------------------|---|--|--|
| INPUT: MEOLP <sub>j</sub>  | 80                | Definition 5.5  |  |  |
| INPUT: BOLP <sub>j</sub>   | 50                | Figure 5.4  |  |  |
| COMPUTED: $\alpha$ -Dependency Fraction  | 0.50              | Figure 5.4  |  |  |
| COMPUTED: Beta Anchor Point (Regulated)  | 25.45             | Property 5.4 But Modified For Regulation                            |  |  |
| COMPUTED: Beta Lower Bound   | 5                 | Property 5.5 But Modified For Regulation                            |  |  |
| COMPUTED: Beta Upper Bound   | 50                | Property 5.5  |  |  |
| INPUT: $\alpha$ -Dependency Fraction (Regulated)                                 | 0.55              | Definition 5.8  |  |  |
| INPUT: Beta Assigned/Setting   | 10                | Assigned/Set  |  |  |
| Feeder Node $P_i$  | SODP <sub>j</sub> | CODP <sub>j</sub>   | $P_j$ Operability Level =<br>Min(SODP <sub>j</sub> , CODP <sub>j</sub> ) | $P_i$ Operability Level<br>Determined By |
| 0  | 50                | 10  | 10   | COD                                      |
| 5  | 52.75             | 15  | 15   | COD                                      |
| 10   | 55.5              | 20  | 20   | COD                                      |
| 15   | 58.25             | 25  | 25   | COD                                      |
| 20   | 61                | 30  | 30   | COD                                      |
| 25   | 63.75             | 35  | 35   | COD                                      |
| 30   | 66.5              | 40  | 40   | COD                                      |
| 35   | 69.25             | 45  | 45   | COD                                      |
| 40   | 72                | 50  | 50   | COD                                      |
| 45   | 74.75             | 55  | 55   | COD                                      |
| 50   | 77.5              | 60  | 60   | COD                                      |
| 55   | 80.25             | 65  | 65   | COD                                      |
| 60   | 83                | 70  | 70   | COD                                      |
| 65   | 85.75             | 75  | 75   | COD                                      |
| 70   | 88.5              | 80  | 80   | COD                                      |
| 75   | 91.25             | 85  | 85   | COD                                      |
| 80   | 94                | 90  | 90   | COD                                      |
| 85   | 96.75             | 95  | 95   | COD                                      |
| 90   | 99.5              | 100   | 99.5   | SOD                                      |
| 90.5   | 99.775            | 100.5   | 99.775   | SOD                                      |
| 90.6   | 99.83             | 100.6   | 99.83  | SOD                                      |
| 90.7   | 99.885            | 100.7   | 99.885   | SOD                                      |
| 90.8   | 99.94             | 100.8   | 99.94  | SOD                                      |
| 90.9   | 99.995            | 100.9   | 99.995   | SOD                                      |
| 90.9090909   | 100               | 100.90909   | 100  | SOD                                      |
| Cross Over Point For $P_i$   | 88.889            | From This Point SODP <sub>j</sub> Drives $P_j$ 's Operability Level |  |  |
| Cross Over Score for $P_j$   | 98.889            |   |  |  |

Table 11. An Operability Analysis of a 2,1,1,R-Node FDNA Graph:  
COD/SOD Cross-Over Point in Range

Given the data in Table 11, the condition in Theorem 5.3 is met for a COD/SOD cross-over point to occur in the interval  $0 \leq P_i \leq 100$ . From Theorem 5.3, the cross-over point is computed to occur when feeder node  $P_i = 88.89$ . At this value, receiver node  $P_j$  achieves an operability level of 98.9 utils. This is a 4.7 percent increase in  $P_j$ 's level of operability than seen at  $P_i = 88.89$  in Table 6, where no regulation on the strength of dependency fraction was considered.

In Table 11, observe that  $P_i$  need only reach an operability level of 90.9 utils for  $P_j$  to become wholly operable. This is in contrast to Table 6, where  $P_j$  became wholly operable only when  $P_i$  became wholly operable. Throughout Table 11, the rate of operability gain in  $P_j$  is higher than the rate in Table 6. This is because a regulated strength of dependency fraction  $\alpha'_{ij} = 0.55$  has been factored in this analysis. This was not the case in Table 6, where only the classic strength of dependency fraction  $\alpha_{ij} = 0.50$  was considered.

**Example 5.17:** Formulating a 3,3,2,R-Node FDF

Figure 65 shows a 3-node FDNA graph under regulation with 3-dependency points and 2-receiver nodes. Let this be indicated by the notation 3,3,2,R-node.

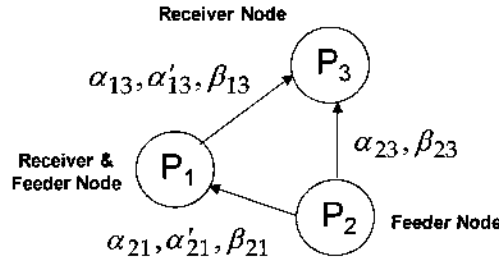


Figure 65. A 3,3,2,R-Node FDNA Graph, With Regulation on  $\alpha'_{13}$  and  $\alpha'_{21}$

The FDNA dependency function for this relationship is given by the following equations.

$$P_3 = \text{Min} \left( \frac{\alpha'_{13}P_1}{2} + \frac{\alpha_{23}P_2}{2} + 100(1 - (\frac{\alpha_{13} + \alpha_{23}}{2})), P_1 + \beta_{13}, P_2 + \beta_{23} \right)$$

$$P_1 = \text{Min}(\alpha'_{21}P_2 + 100(1 - \alpha_{21}), P_2 + \beta_{21})$$

where  $\alpha'_{13}$  : Regulated strength of dependency fraction between  $P_1$  and  $P_3$

$\alpha_{13}$  : Strength of dependency fraction between  $P_1$  and  $P_3$

$\alpha_{23}$  : Strength of dependency fraction between  $P_2$  and  $P_3$

$\alpha'_{21}$  : Regulated strength of dependency fraction between  $P_1$  and  $P_2$

$\alpha_{21}$  : Strength of dependency fraction between  $P_1$  and  $P_2$

$\beta_{13}$  : Criticality of dependency between  $P_1$  and  $P_3$

$\beta_{23}$  : Criticality of dependency between  $P_2$  and  $P_3$

$\beta_{21}$  : Criticality of dependency fraction between  $P_1$  and  $P_2$

$$0 < \alpha_{13} \leq \alpha'_{13} \leq 1, 0 < \alpha_{23} \leq 1, 0 < \alpha_{21} \leq \alpha'_{21} \leq 1$$

$$100(\alpha'_{13} - \alpha_{13}) \leq \beta_{13} \leq 100(1 - \alpha_{13})$$

$$0 \leq \beta_{23} \leq 100(1 - \alpha_{23})$$

$$100(\alpha'_{21} - \alpha_{21}) \leq \beta_{21} \leq 100(1 - \alpha_{21})$$

and (1)  $0 \leq P_j \leq 100$  with  $0 \leq P_i \leq 100 - \beta_{ij}$  if  $P_j(100 - \beta_{ij}) = 100$

or (2)  $0 \leq P_j \leq 100$  with  $0 \leq P_i \leq 100 \frac{\alpha_{ij}}{\alpha'_{ij}}$  if  $P_j \left( 100 \frac{\alpha_{ij}}{\alpha'_{ij}} \right) = 100$

for  $ij = 13, 21$  and  $0 \leq P_i, P_j \leq 100$  for  $ij = 23$ .

### Summary

This section presented FDNA as a *general theory of dependency* for capturing and measuring how the operability of one node affects the operability of other nodes across a topology of any complexity. FDNA is built upon a set of postulates. From them, a general structure has emerged such that dependency relationships can be modeled by simple algebraic functions and visualized by mathematical graph theory.

The extension of FDNA from single component nodes to constituent nodes is one generalization of its calculus. With this, FDNA can address mutual (cycle) dependencies between nodes. A mutual dependency is dealt with by specifying *why* the operability of one node depends on the operability of the other (and vice-versa) and *what* drives their mutual reliance. This is called specification (illustrated in Example 5.13).

Specification seeks to resolve mutual (cycle) dependencies by identifying the underlying mutually independent components between nodes. If this cannot be identified, then it signals the nodes are indistinguishable from each other. In such cases, they should be joined into a single (new) node – one with a revised interpretation that stems from their unification.

This section also demonstrated how the FDNA dependency function can be regulated to model the realities of a specific dependency relationship. Under regulation, the FDNA equations can now support the property that *a receiver node may become wholly operable before its feeder node is wholly operable*.

Although FDNA is developed to address dependency problems associated with engineering capabilities for an enterprise, its underlying algorithms are applicable to a variety of problem spaces. These include inflows and outflows of economic consumption and demand, flows through logistic supply chains, or critical infrastructure risk analyses. Interpretations of FDNA applied in these domains, especially the meaning of node-to-node relationships, are specific to the nature of the dependency problem addressed. A discussion of FDNA with respect to its relationship with other dependency analysis methods is provided later and will close this chapter.

The following presents one of many possible applications of FDNA. Shown is how FDNA outputs can be used to identify which nodes in a graph offer the highest rates of operational improvement when risk reduction investments in them are made.

## LINKING FDNA TO RISK REDUCTION INVESTMENT DECISIONS

An FDNA analysis can be extended to a number of decision-making contexts. This section illustrates one of them. Specifically, we'll show how FDNA can aid in investment decisions aimed at reducing operability loss due to the potential realization of unwanted events.

### Determining Risk Reduction Targets by Marginal Rates of Return (MRR)

This discussion presents how FDNA can identify which nodes in an FDNA graph offer the highest marginal rates of return (MRR) if risk reduction investments in them are made. Determining each node's MRR allows decision-makers to tradeoff the desirability of an investment in one node against the merits of doing so in other nodes. The objective is to identify where to target risk reduction resources, such that the marginal rate of operability improvement is maximized across an FDNA graph\*. We begin with the following definitions.

#### Definition 5.9: Marginal Rate of Return

The marginal rate of return is the rate with which a receiver node changes in operability (utils) with every unit change in the operability (utils) of its feeder node.

#### Definition 5.10: Strict Receiver Node

A *strict receiver node* is one that does not feed any other node in an FDNA graph.

The marginal rate of return of a strict receiver node is one. If an FDNA graph has  $n$  strict receiver nodes, then each of these nodes has an MRR equal to  $1/n$ . For any other node  $x$  with receiver node  $y$ , the marginal rate of return of  $x$  is

$$MRR_x = MRR_y \cdot \frac{\partial y}{\partial x} \quad (5.39)$$

If node  $x$  has receiver nodes  $y_1, y_2, y_3, \dots, y_k$ , then the marginal rate of return of  $x$  is

$$MRR_x = MRR_{y_1} \cdot \frac{\partial y_1}{\partial x} + MRR_{y_2} \cdot \frac{\partial y_2}{\partial x} + MRR_{y_3} \cdot \frac{\partial y_3}{\partial x} + \dots + MRR_{y_k} \cdot \frac{\partial y_k}{\partial x} \quad (5.40)$$

**Example 5.18:** Determine the MRR of each node in Figure 66.

In Figure 66, we have two receiver nodes  $P_1$  and  $P_3$ ; here,  $P_3$  is a strict receiver node. We want to compute the rate with which  $P_1$  and  $P_3$  change in operability, with every unit change in the operability of their feeder nodes. In this graph,  $P_2$  is a feeder node to node  $P_1$  and node  $P_3$  while  $P_1$  is both a feeder and a receiver node.

From Equation 5.39 and Equation 5.40, respectively, we have the following:

---

\* The approach herein is an application of an original idea by Dr. Brian K. Schmidt, The MITRE Corporation, for computing marginal rates of return on mathematical graphs associated with investment portfolio analysis and optimization problems [Moynihan, Schmidt, et al., 2008].

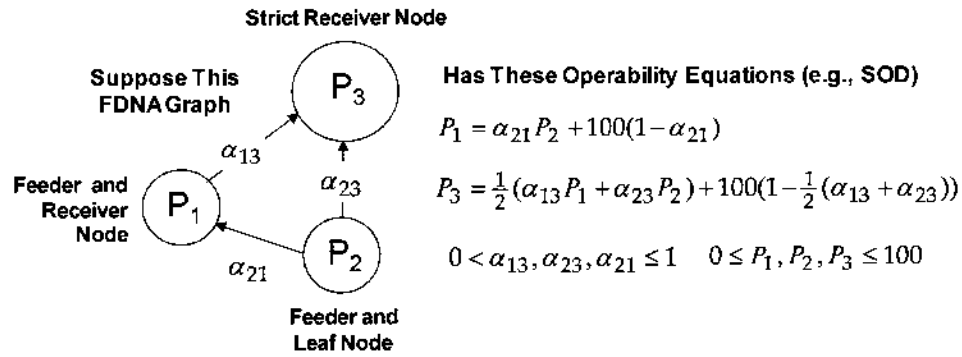


Figure 66. FDNA Graph and SOD Equations for Example 5.18

$$MRRP_1 = MRRP_3 \cdot \frac{\partial P_3}{\partial P_1} = 1 \cdot \frac{\alpha_{13}}{2} = \alpha_{13}/2 \quad (5.41)$$

$$MRRP_2 = MRRP_1 \cdot \frac{\partial P_1}{\partial P_2} + MRRP_3 \cdot \frac{\partial P_3}{\partial P_2} = \frac{\alpha_{13}}{2} \cdot \alpha_{21} + 1 \cdot \frac{\alpha_{23}}{2} = (\alpha_{13}\alpha_{21} + \alpha_{23})/2 \quad (5.42)$$

Figure 67 shows the FDNA graph in Figure 66 in terms of its marginal rates of return. If  $\alpha_{13} = 1/3$ ,  $\alpha_{23} = 2/3$ , and  $\alpha_{21} = 1/4$  then the marginal rates of return for  $P_1$  and  $P_2$  are  $1/6$  and  $3/8$ , as shown in Figure 67. Thus, node  $P_2$  has the highest MRR in this case.

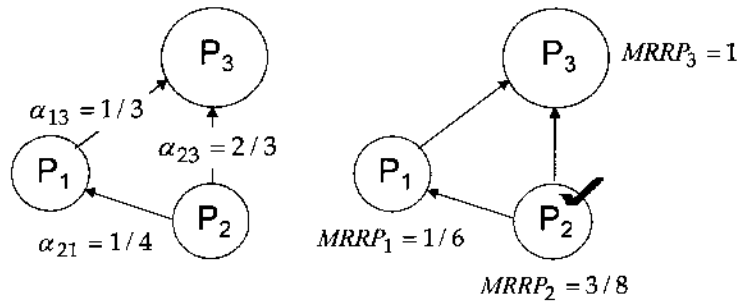


Figure 67. An MRR View of the FDNA Graph in Example 5.18

These rates of return mean a 1-util increase in the operability of node  $P_1$  produces an increase in operability of  $\alpha_{13}/2$  utils in  $P_3$ . A 1-util increase in the operability of node  $P_2$  produces an increase in operability of  $(\alpha_{13}\alpha_{21} + \alpha_{23})/2$  utils in  $P_3$ . Thus, in this FDNA graph, node  $P_2$  offers the highest marginal rate of return from an investment of risk reduction resources.

The following illustrates computing the MRR for an FDNA graph with multiple strict receiver nodes and the weakest link FDF. This is presented as Example 5.19.



**Example 5.19:** Determine the MRR of each node in Figure 68.

In Figure 68, we have three receiver nodes  $P_1$ ,  $P_3$ , and  $P_4$ ; here,  $P_3$  and  $P_4$  are strict receiver nodes. We want to compute the rate with which  $P_1$ ,  $P_3$ , and  $P_4$  change in operability, with every unit change in the operability of their feeder nodes. In this graph,  $P_2$  is a feeder node to node  $P_1$ ,  $P_3$ , and  $P_4$  while  $P_1$  is both a feeder and a receiver node.

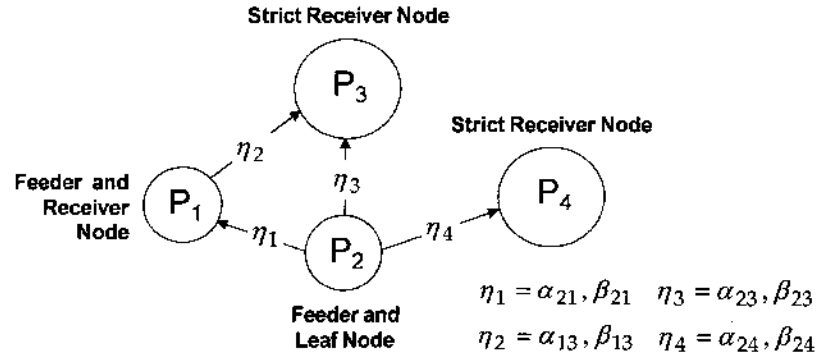


Figure 68. FDNA Graph for Example 5.19

Applying the weakest link FDF, from Definition 5.4, we can write the following equations for the FDNA graph in Figure 68.

$$P_1 = \text{Min}(\alpha_{21}P_2 + 100(1 - \alpha_{21}), P_2 + \beta_{21}) \quad (5.43)$$

$$P_3 = \text{Min}\left(\frac{\alpha_{13}P_1}{2} + \frac{\alpha_{23}P_2}{2} + 100\left(1 - \left(\frac{\alpha_{13} + \alpha_{23}}{2}\right)\right), P_1 + \beta_{13}, P_2 + \beta_{23}\right) \quad (5.44)$$

$$P_4 = \text{Min}(\alpha_{24}P_2 + 100(1 - \alpha_{24}), P_2 + \beta_{24}) \quad (5.45)$$

From Equation 5.39 and Equation 5.40 we have the following:

$$MRRP_1 = MRRP_3 \cdot \frac{\partial P_3}{\partial P_1} = \frac{1}{2} \frac{\partial P_3}{\partial P_1} \quad (5.46)$$

$$MRRP_2 = MRRP_1 \cdot \frac{\partial P_1}{\partial P_2} + MRRP_3 \cdot \frac{\partial P_3}{\partial P_2} + MRRP_4 \cdot \frac{\partial P_4}{\partial P_2} \quad (5.47)$$

$$= MRRP_1 \cdot \frac{\partial P_1}{\partial P_2} + \frac{1}{2} \cdot \frac{\partial P_3}{\partial P_2} + \frac{1}{2} \cdot \frac{\partial P_4}{\partial P_2} \quad (5.48)$$

where

$$MRRP_3 = 1/2 \text{ and } MRRP_4 = 1/2$$

since this FDNA graph has  $n = 2$  strict receiver nodes  $P_3$ , and  $P_4$ . From this, the MRR formulations are completed as follows:

$$MRRP_1 = MRRP_3 \cdot \frac{\partial P_3}{\partial P_1} = \frac{1}{2} \frac{\partial P_3}{\partial P_1} \quad (5.50)$$

$$= \frac{1}{2} \cdot \begin{cases} \frac{\alpha_{13}}{2} & \text{if the operability of } P_3 \text{ is determined by } SODP_3 \\ 1 & \text{if the operability of } P_3 \text{ is determined by } CODP_3 \end{cases} \quad (5.51)$$

From Equation 5.47 we have

$$MRRP_2 = MRRP_1 \cdot \frac{\partial P_1}{\partial P_2} + MRRP_3 \cdot \frac{\partial P_3}{\partial P_2} + MRRP_4 \cdot \frac{\partial P_4}{\partial P_2}$$

where the first term is

$$MRRP_1 \cdot \frac{\partial P_1}{\partial P_2} = MRRP_1 \cdot \begin{cases} \alpha_{12} & \text{if the operability of } P_1 \text{ is determined by } SODP_1 \\ 1 & \text{if the operability of } P_1 \text{ is determined by } CODP_1 \end{cases} \quad (5.52)$$

with  $MRRP_1$  is given by Equation 5.51. The remaining two terms in  $MRRP_2$  are as follows:

$$MRRP_3 \cdot \frac{\partial P_3}{\partial P_2} = \frac{1}{2} \cdot \begin{cases} \frac{\alpha_{23}}{2} & \text{if the operability of } P_3 \text{ is determined by } SODP_3 \\ 1 & \text{if the operability of } P_3 \text{ is determined by } CODP_3 \end{cases} \quad (5.53)$$

$$MRRP_4 \cdot \frac{\partial P_4}{\partial P_2} = \frac{1}{2} \cdot \begin{cases} \alpha_{24} & \text{if the operability of } P_4 \text{ is determined by } SODP_4 \\ 1 & \text{if the operability of } P_4 \text{ is determined by } CODP_4 \end{cases} \quad (5.54)$$

Combining Equations 5.52 through 5.54 in accordance with Equation 5.47 yields  $MRRP_2$ .

## RELATIONSHIP OF FDNA TO OTHER METHODS

This section discusses FDNA in relation to three other dependency analysis methods in the systems engineering community. These are the Dependency Structure Matrix (DSM), Failure Modes and Effects Analysis (FMEA), and the Inoperability Input-Output Model (IIM). We begin with DSM and FMEA. This is followed by a discussion of FDNA's relationship to its close analytic neighbor – the Inoperability Input-Output Model (IIM) [Jiang, Santos, Haimes, 2004].

### Design Structure Matrix

Design structure matrix is a technique used in systems analysis and project management. It originated as a system decomposition method and has grown in application as a way to design and manage interrelationships within complex projects.

Applied to systems engineering and design, DSM is a two dimensional way to visualize and represent interrelationships between entities at any level of a system's architecture. This can be at a system-level, a sub-system-level, or a module-level. Once specified, entity relationships can be analyzed by techniques such as cluster analysis to determine hidden dependency structures, optimal task sequencing, and information exchange relationships and requirements.

Applied to project management, the DSM provides a way to sequence activities from a scheduling perspective, identify activity dependencies and precedence relationships, and model feedback loops where rework or cycles are needed.

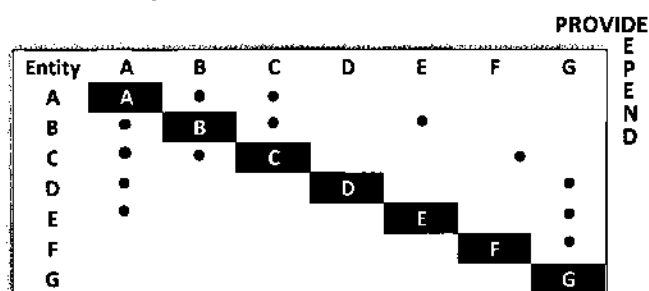


Figure 69. A Design Structure Matrix (DSM)

In Figure 69, entities are shown along the diagonal of the matrix. Dependencies between entities are shown in the off-diagonal elements. In a DSM, the rows *provide* and the columns *depend*. For instance, entity B provides something to entities A, C, and E, but entity B also depends on something from entities A and C.

Distinguishing characteristics between DSM and FDNA include the following:

- In DSM, dependencies between entities are expressed in the off-diagonal elements. An FDNA adjacency matrix corresponding to its graph permits intra-dependencies within its diagonal elements. This allows for increased flexibility across nodal or entity relationships.
- DSM allows strength of dependency to be indicated in the matrix by a number between zero and one, where one represents an extremely strong dependency. FDNA employs a similar construct but one that allows strength and criticality of dependency to be modeled.

### **Failure Modes and Effects Analysis**

Failure Modes and Effects Analysis (FMEA) is among a class of techniques that come from the quality assurance and system safety communities. The main objective of FMEA is to identify potential failure events early in a system's design, such that operational reliability and safety requirements are achieved.

Failure analyses within an FMEA rely on the availability and use of a system's block diagram or a control /data flow diagram or an operational view of how a system transports information between nodes, entities, or elements. Identified failure events, if they occur, are analyzed in terms of their ripple effects within and across a system's architecture. Thus, the correct capture of interrelationships within a system is a critical aspect of FMEA.

It is often recommended an FMEA be augmented by a Fault-Tree Analysis (FTA) or a Probabilistic Risk Analysis (PRA) to aid in the capture of interrelationships within a system. FTA and PRA are methods that emerged from, and have been refined, by the nuclear engineering community, where system safety is paramount. In recent years, FMEA has been extended to include a criticality analysis. This is called a FMECA, where the C stands for criticality. The criticality analysis includes an assessment of failure mode probabilities and consequences, with the aim of identifying failure mode events whose occurrences would result in severe or catastrophic outcomes.

Distinguishing characteristics between FMEA and FDNA include the following:

- FMEA is primarily a risk identification and assessment technique, where FDNA is an analysis of the effects of risk, if it occurs, on the operability of a system.
- FMEA computes a risk priority number (RPN) on the basis of three variables; these are the failure event's severity, its occurrence probability, and its chance of failure detection.

The RPN is computed by multiplying these variables on ordinal scales. This operation is impermissible because there is no meaningful distance metric between numbers on an ordinal scale. FDNA does not compute a risk measure explicitly; rather, its calculus measures operability loss or gain in a system's functionality that come from undesirable or desirable events.

- An FMEA generally relies on a team of engineers to identify failures events. Thus, small probability but high consequence events can be missed or possibly dismissed.
- An FDNA could be integrated into a FMEA in ways similar to doing so with FTA or PRA. In theory, an FDNA graph could be modeled from a system's block diagram. From this, failure events and their impacts on operability and operability dependencies across the nodes of a system could explicitly evaluated.

The following presents a detailed discussion of FDNA as it relates to its analytic neighbor – the Inoperability Input-Output Model (IIM).

### Inoperability Input-Output Model

The Inoperability Input-Output Model (IIM) [Jiang, Haimen, 2004; Santos, Haimen, 2004] was developed as a way to study the effects of degraded operations in critical infrastructures on nodes dependent on their availability. As the name implies, IIM is an input-output (I/O) model developed in the spirit of input-output models born out of economic science.

In economics, input-output models study how changes in inflows and outflows of goods and services affect consumers and suppliers that depend on them and each other. German-born economist Wassily Leontief (1905-1999) is credited with developing the underlying theory of input-output models, for which he won the Nobel memorial prize in economic sciences in 1973.

In critical infrastructure risk analysis, IIM studies how changes in the operability of systems such as power systems, financial systems, or transportation systems affect each other and entities that depend on some or all of them. IIM measures how loss of operability in one node (a critical infrastructure) affects the operability of entities that depend on it and concomitant ripple effects along dependency chains.

As mentioned earlier, IIM is a close analytic neighbor to FDNA. Before discussing their relationship we begin with an introduction to Leontief input-output models and IIM.

#### *The Leontief Input-Output Model*

At its core, Leontief's input-output model captures relationships between intra- and inter-dependent sectors (or industries) of an economy with respect to consumption and demand. Its fundamental equation is as follows:

$$X - AX = D \quad (5.55)$$

where  $X$  is the total output needed to meet consumer demand  $D$  given input-output matrix  $A$ . Let's take a look at the input-output matrix. Suppose  $A$  is given by the following matrix.

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{matrix} S_1 \\ S_2 \end{matrix} \quad (5.56)$$

The elements in matrix  $A$  are always non-negative. If these elements represent prices, then they can mean the following. Element  $a_{11}$  is the percentage of one dollar (input) needed to produce (output) one dollar worth of product (an economic good) in sector  $S_1$ . This is an economic intra-dependency or internal consumption within  $S_1$ . Element  $a_{12}$  is the percentage of one dollar it takes from sector  $S_1$  to produce one dollar worth of product in sector  $S_2$ . This is an economic interdependency between  $S_1$  and  $S_2$ .

Likewise, element  $a_{21}$  is the percentage of one dollar it takes from sector  $S_2$  to produce one dollar worth of product in sector  $S_1$ . This is an economic interdependency between  $S_2$  and  $S_1$ . Element  $a_{22}$  is the percentage of one dollar it takes to produce one dollar worth of product in sector  $S_2$ . This is an economic intra-dependency or the internal consumption within  $S_2$ .

In Equation 5.55,  $D$  is consumer demand for products produced by  $S_1$  and  $S_2$ . Demand is a vector whose elements are in dollars. Since  $A$  is a two dimensional matrix (here)  $D$  is a two dimensional vector; that is,  $D=[d_1, d_2]$  where  $d_1$  is consumer demand in dollars worth of product from sector  $S_1$  and  $d_2$  is consumer demand in dollars worth of product from sector  $S_2$ .

Given this, Leontief's model solves for how many dollars of product from sector  $S_1$  and sector  $S_2$  must be produced to meet consumer demand. This is determined by solving Equation 5.55 for  $X$ , where

$$X = (I - A)^{-1} D \quad (5.57)$$

In Equation 5.57,  $I$  is the identity matrix and  $X$  is a vector. Since  $A$  is a two dimensional matrix (in this discussion)  $X$  is a two dimensional vector; that is,  $X=[x_1, x_2]$  where  $x_1$  is the amount of dollars worth of product sector  $S_1$  must produce to meet consumer demand and  $x_2$  is the amount of dollars worth of product sector  $S_2$  must produce to meet consumer demand, while simultaneously considering the intra- and inter- sector dependencies represented in matrix  $A$ .

The Leontief input-output model is subject to certain mathematical conditions for solutions to Equation 5.57 to be meaningful in an economics context. In mathematical economics, it has been proved the Leontief equation  $(I - A)X = D$  has a non-negative solution ( $X \geq 0$ ) for every non-negative  $D$  ( $D \geq 0$ ) if and only if the Leontief matrix  $(I - A)$  satisfies the *Hawkins-Simon* condition. What is the Hawkins-Simon condition?

A square matrix, such as  $(I - A)$ , satisfies the Hawkins-Simon condition *if and only if* its leading principal minors (e.g., its principal sub-matrices along the diagonal) are positive. With this, the determinant of  $(I - A)$  is greater than zero; hence  $(I - A)$  is nonsingular and thus invertible.

**Definition 5.11:** The Hawkins-Simon Condition for  $(I - A)$  is defined as follows:

$$\det \begin{vmatrix} 1 - a_{11} & -a_{12} & \cdots & -a_{1k} \\ -a_{21} & 1 - a_{22} & \cdots & -a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{k1} & -a_{k2} & \cdots & 1 - a_{kk} \end{vmatrix} > 0 \quad \text{for } k = 1, \dots, n \quad (5.58)$$

where  $I$  is the  $n \times n$  identity matrix and  $A$  is an  $n \times n$  matrix.

**Example 5.20:** Hawkins-Simon Condition Check

Suppose  $A$  is given by the following  $3 \times 3$  matrix. Determine whether  $(I - A)$  satisfies the Hawkins-Simon condition given by Equation 5.58.

$$A = \begin{pmatrix} 0 & 0.10 & 0.20 \\ 0 & 0.05 & 0.20 \\ 0.20 & 0.01 & 0.10 \end{pmatrix}$$

### Solution

Given  $A$ , the Leontief matrix  $(I - A)$  is

$$I - A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0.10 & 0.20 \\ 0 & 0.05 & 0.20 \\ 0.20 & 0.01 & 0.10 \end{pmatrix} = \begin{pmatrix} 1 & -0.10 & -0.20 \\ 0 & 0.95 & -0.20 \\ -0.20 & -0.01 & 0.90 \end{pmatrix}$$

The determinants of the principal minors of  $(I - A)$  are

$$\det |1| = 1 > 0, \det \begin{vmatrix} 1 & -0.10 \\ 0 & 0.95 \end{vmatrix} = 0.95 > 0, \det \begin{vmatrix} 1 & -0.10 & -0.20 \\ 0 & 0.95 & -0.20 \\ -0.20 & -0.01 & 0.90 \end{vmatrix} = 0.811 > 0$$

These determinants are all positive; thus,  $(I - A)$  satisfies the Hawkins-Simon condition. Therefore, for  $A$  given in Example 5.20, the Leontief equation  $(I - A)X = D$  is guaranteed to have a non-negative solution  $X$  for every non-negative  $D$ . This concludes the example.

Not all Leontief matrices satisfy the Hawkins-Simon condition. For example, it can be shown if  $A$  is given by the following matrix, then the principal minors of  $(I - A)$  are not all positive. Thus, the Leontief equation  $(I - A)X = D$  is **not** guaranteed to have a non-negative solution for every non-negative  $D$ . Given  $A$ , in this case, the components of the solution vector  $X$  are all negative.

$$A = \begin{pmatrix} 0.95 & 0.20 & 0.10 \\ 0.10 & 0.40 & 0.20 \\ 0.10 & 0.10 & 0.30 \end{pmatrix}$$

### The Inoperability Input-Output Model

As mentioned earlier, the Inoperability Input-Output Model (IIM) was developed as a way to study the effects of degraded operations in critical infrastructures on entities with intra- and inter-dependencies on their operability. IIM captures how changes in the operability of infrastructure systems such as power systems, financial systems, or transportation systems affect each other and entities that depend on some or all of them.

Where Leontief I/O models capture how many dollars worth of product economic sectors must produce to meet demand, IIM measures the loss of operability in critical infrastructure “sectors” when their ability to meet demand is perturbed by natural or man-made events. The following provides a very simple illustration of IIM to demonstrate its core relationship with Leontief I/O modeling. Example 5.21 is from Haimes (2004).

#### **Example 5.21:** IIM Illustration [Haimes, p. 712, 2004]

Suppose we have a system with two subsystems. The inoperability of these two subsystems is given by  $x_1$  and  $x_2$ , respectively. Now, suppose a failure at subsystem 2 will lead subsystem 1 to be 80 percent inoperable. Suppose a failure at subsystem 1 will lead subsystem 2 to be 20 percent

inoperable. If subsystem 2 loses 60 percent of its operability due to an external perturbation what is the resultant effect on the operability of subsystem 1 and subsystem 2?

The IIM approach is illustrated by addressing this question. Equations 5.59 and 5.60 show the clear contrast between the Leontief I/O model and the IIM.

$$\text{Leontief I/O Model} \quad X - AX = D \quad (5.59)$$

$$\text{Inoperability I/O Model} \quad X - AX = C \quad (5.60)$$

In Equation 5.60,  $X$  is the inoperability vector of each subsystem,  $A$  is the inoperability input-output matrix between these subsystems, and  $C$  is the demand-side perturbation in the operability of subsystem 1 and subsystem 2 from a natural or man-made event. In IIM,  $A$  is also called the *interdependency matrix*.

From the information in this example, matrix  $A$  is as follows:

$$A = \begin{pmatrix} S_1 & S_2 \\ 0 & 0.80 \\ 0.20 & 0 \end{pmatrix} \begin{matrix} S_1 \\ S_2 \end{matrix} \quad (5.61)$$

where  $S_1$  and  $S_2$  denote subsystem 1 and subsystem 2, respectively. From this we can write

$$X - \begin{pmatrix} 0 & 0.80 \\ 0.20 & 0 \end{pmatrix} X = \begin{bmatrix} 0 \\ 0.60 \end{bmatrix} \quad (5.62)$$

where  $C = [0, 0.60]$ . The solution to Equation 5.62 is  $X = [0.571, 0.714]$ . This means the inoperability of subsystem 1 and subsystem 2 is, respectively,  $x_1 = 0.571$  and  $x_2 = 0.714$ . In IIM, an entity is wholly (flawlessly) operable if  $x = 0$  and wholly inoperable if  $x = 1$ .

Even though subsystem 1 was not perturbed, it realized an inoperability of 0.571 because of its connectedness with subsystem 2. Even though subsystem 2 lost 60 percent of its operability from an external perturbation, its overall inoperability worsened to 71.4 percent because of its connectedness to subsystem 1.

The IIM is subject to the same mathematical conditions previously described for Leontief input-output models. In IIM,  $(I - A)X = C$  has a non-negative solution for every non-negative  $C$  if and only if the IIM matrix  $(I - A)$  satisfies the Hawkins-Simon condition.

In summary, this example illustrates how dependence between pairs of entities (e.g., critical infrastructures) is captured in IIM and how it derives from the originating ideas of Leontief input-output economic models.



### Relationship of FDNA to IIM and its Distinctions

An assumption in IIM is that each system “performs a uniquely defined function; that is, no two systems perform the same function” [Haimes, 2004]. Dependencies between systems can be identified by understanding their physical connections, to include information exchange by virtual or cyber mechanisms. This is equivalent to the role of constituent nodes in FDNA, as illustrated in Figure 59 and shown below for convenience.

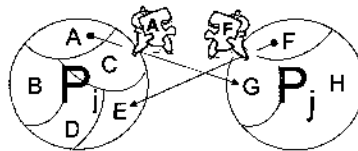


Figure 70. Physical Connections Between Components:

The IIM  $A$ -matrix is an *interdependency matrix*. It captures the degree of coupling between pairs of entities (e.g., infrastructures, industry sectors) as they affect the operability of each other. The elements in the  $A$ -matrix range from zero to one. If element  $a_{kj}$  is nonzero, then an operability dependency exists with the  $k$ -th entity on the  $j$ -th entity. Specifically, the interpretation is as follows: complete failure of the  $j$ -th entity leads to a level of inoperability in the  $k$ -th entity. If element  $a_{kj} = 1$ , then a complete failure of the  $j$ -th entity leads to a complete failure of the  $k$ -th entity. If element  $a_{kj} = 0$ , then a complete failure of the  $j$ -th entity has no impact on the operability of the  $k$ -th entity [Haimes, 2004].

FDNA captures these same dependency relationships through algebraic functions that model entity interactions. These functions are uniquely formulated from their specific mathematical graphs instead of a matrix protocol.

From a mathematical viewpoint, all matrices are graphs and all graphs are matrices. Next, we take a closer look at this in general and then from an IIM/FDNA perspective.

### Graphs and Matrices

A *mathematical graph* is a collection of points and lines connecting some (possibly empty) subset of them. The points of a graph are known as vertices or nodes. The lines connecting the vertices are known as edges or arcs\*. In general, a matrix is a two dimensional array of a mathematical graph. In graph theory, such an array is called an *adjacency matrix*. An adjacency matrix is one whose elements  $a_{ij} = 1$  when  $(i, j)$  is a line (edge),  $a_{ij} = 0$  when  $(i = j)$ , and  $a_{ij} = \infty$  otherwise.

The lines of graphs can have directedness. Arrows on one or both endpoints of a graph indicate directedness. Stated previously, such a graph is said to be *directed*. A graph or a directed graph together with a function which assigns a positive real number to each line is known as a *network*\*. An FDNA graph is a directed graph. It is also a network. Figure 71 illustrates an FDNA graph and its adjacency matrix.

\* Reference: This text excerpted from <http://mathworld.wolfram.com/Graph.html>.

Figure 71 shows the FDNA graph from Example 5.4 on the left and its adjacency matrix representation on the right.

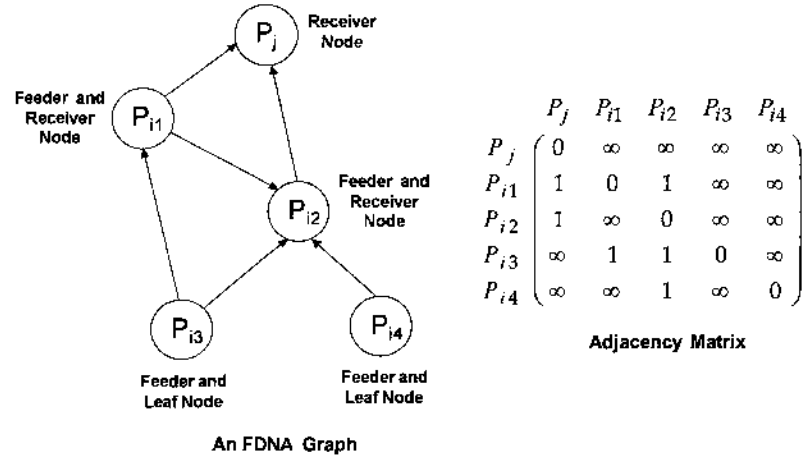


Figure 71. An FDNA Graph and its Adjacency Matrix

In Figure 71, the adjacency matrix contains 1's, 0's, and  $\infty$ 's. When one node is adjacent to another the adjacency is indicated by the value one. A node adjacent to itself is indicated by the value zero. Thus, the diagonal elements in an adjacency matrix are always zero. The symbol  $\infty$  is used to signal no path exists between two nodes; a zero can also be used.

If a graph is undirected, then its adjacency matrix is symmetric. If the graph is directed, then the adjacency matrix is not necessarily symmetric. Adjacency matrices are always square. Next, we introduce the concept of a weighted directed graph and a weighted adjacency matrix. These are the types seen in FDNA and IIM.

A *weighted directed graph* is a directed graph with a number assigned along its lines or edges. Numbers can represent a variety of effects, such as the distance between nodes. A *weighted adjacency matrix* is the adjacency matrix of a weighted directed graph. An example is shown in Figure 72.

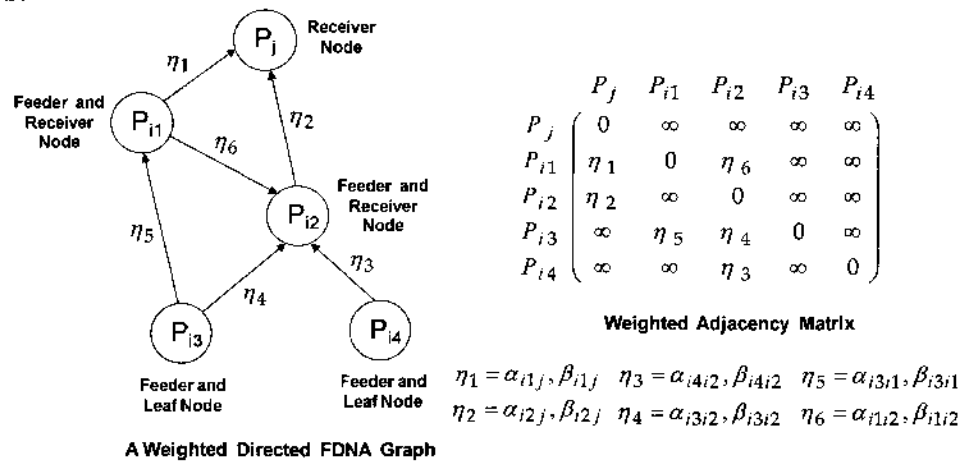


Figure 72. A Weighted FDNA Graph and its Weighted Adjacency Matrix

Seen in the preceding figure, FDNA graphs are weighted directed graphs that can be represented by weighted adjacency matrices. In FDNA, weights might be the strength of dependency parameter, referred to as  $\alpha$ . They may also be operability or inoperability levels of nodes. This is the case in IIM. In fact, the interdependency matrix in IIM (the  $A$ -Matrix) is simply a weighted adjacency matrix from a corresponding graph.

For example, the  $A$ -matrix in Example 5.21 is for a system with two subsystems  $S_1$  and  $S_2$  [Haimes, 2004]. From this, the weighted FDNA graph can be written as shown in Figure 73.

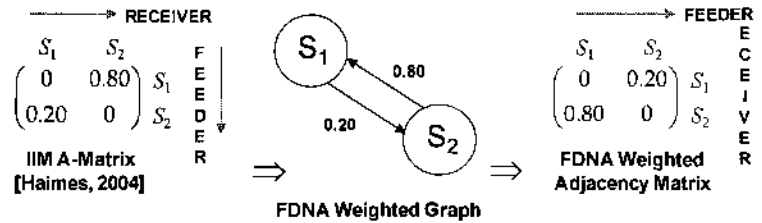


Figure 73. A System-Subsystems Scenario  
IIM Interdependency Matrix and FDNA Relationship

Figure 74 illustrates an  $A$ -matrix for an infrastructure scenario [Haimes, 2004]. Here, and in Figure 73, the IIM  $A$ -matrix implicitly contains a “feeder-receiver” metaphor. Furthermore, there is a transpose relationship between the IIM  $A$ -matrix and the FDNA weighted adjacency matrix; specifically,

$$a_{kj} = \alpha_{jk} \text{ for } j, k = 1, \dots, n$$

The  $A$ -matrix elements  $a_{kj}$  in IIM follow a receiver-feeder pattern by row( $k$ )-column( $j$ ), respectively. The weighted adjacency matrix elements  $\alpha_{jk}$  in FDNA follow a feeder-receiver pattern by row( $j$ )-column( $k$ ), respectively.

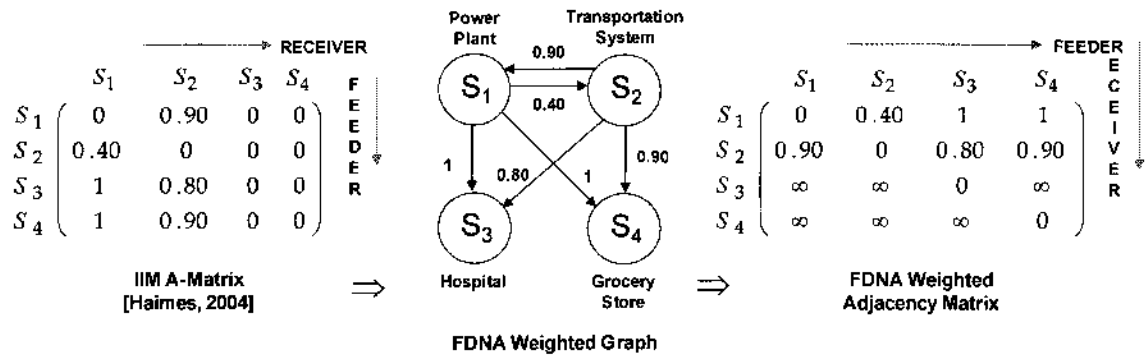


Figure 74. An Infrastructure Systems Scenario  
IIM Interdependency Matrix and FDNA Relationship

In IIM, each element ( $k, j$ ) of its  $A$ -matrix is interpreted as follows: “a complete failure of the  $j$ -th entity leads to a level of inoperability in the  $k$ -th entity”. In FDNA, this is equivalent to the strength of dependency fraction  $\alpha_{jk}$  between feeder node  $P_j$  and receiver node  $P_k$ . Recall that strength of dependency is the operability level (utils) a receiver node relies on receiving from a

feeder node for the receiver to *continually increase* its baseline operability level **and** ensure the receiver node is wholly operable when its feeder node is wholly operable.

In FDNA, if a feeder node provides zero utility to its receiver node then the receiver at most operates at its baseline operability level  $BOLP_k$ . From Equation 5.1,  $BOLP_k = 100(1 - \alpha_{jk})$ . For example, in Figure 74 the IIM  $A$ -matrix element  $(1, 2) = 0.90$  means “a complete failure of infrastructure system  $S_2$  results in an operability level of  $100(1 - 0.90) = 10$  percent for infrastructure system  $S_1$ . Thus, IIM  $A$ -matrix element  $(k, j)$  is equivalent to the FDNA strength of dependency fraction  $\alpha_{jk}$ , where receiver node  $P_k$  relies on feeder node  $P_j$  and  $0 < \alpha_{jk} \leq 1$ .

Thus, a direct link exists between FDNA and IIM and ultimately to the Leontief Input-Output model approach itself. Their distinctions are in the calculus by which they generate measures of operability, inoperability, or economic loss or gain. These distinctions are important. As mentioned earlier, IIM/Leontief models must meet certain matrix algebra conditions for solutions to exist – conditions FDNA is not subject to because of its algebraic, non-matrix-based, calculus.

Next, we present an IIM and FDNA analysis of the infrastructure scenario in Figure 74. First, we apply the IIM approach to the  $A$ -matrix in Figure 74. Here, the IIM is the solution to

$$S - AS = C \quad (5.63)$$

where  $S$  is the inoperability vector of infrastructures  $S_1, S_2, S_3$ , and  $S_4$  (defined in Figure 74),  $A$  is the inoperability input-output matrix given below

$$\begin{array}{c} S_1 \quad S_2 \quad S_3 \quad S_4 \\ \begin{array}{l} S_1 \\ S_2 \\ S_3 \\ S_4 \end{array} \begin{pmatrix} 0 & 0.90 & 0 & 0 \\ 0.40 & 0 & 0 & 0 \\ 1 & 0.80 & 0 & 0 \\ 1 & 0.90 & 0 & 0 \end{pmatrix} \end{array}$$

and  $C$  is the demand-side perturbation in the operability of  $S_1, S_2, S_3$ , and  $S_4$  from a natural or man-made event. Suppose a storm destroys 50 percent of the functionality of the transportation system infrastructure  $S_2$  [Haimes, 2004]; thus,  $C = [0, 0.50, 0, 0]$ . From Equation 5.63 we have

$$S - \begin{pmatrix} 0 & 0.90 & 0 & 0 \\ 0.40 & 0 & 0 & 0 \\ 1 & 0.80 & 0 & 0 \\ 1 & 0.90 & 0 & 0 \end{pmatrix} S = \begin{bmatrix} 0 \\ 0.50 \\ 0 \\ 0 \end{bmatrix} \quad (5.64)$$

From Equation 5.64, we can form the following system of linear equations.

$$S_1 = 0.90S_2 \quad (5.65)$$

$$S_2 = 0.40S_1 + 0.50 \quad (5.66)$$

$$S_3 = S_1 + 0.80S_2 \quad (5.67)$$

$$S_4 = S_1 + 0.90S_2 \quad (5.68)$$

The solution to this linear system is  $S = [0.703125, 0.78125, 1.32813, 1.40625]$ . Inoperability cannot be greater than one; therefore, the convention in IIM is to modify the solution vector as

$$S = [0.703125, 0.78125, 1, 1]$$

Thus, due to the interdependencies between  $S_1$ ,  $S_2$ ,  $S_3$ , and  $S_4$ , a 50 percent loss in the functionality of the transportation system infrastructure  $S_2$  brings with it increased inoperability in the power plant  $S_1$ , the hospital  $S_3$ , and the grocery store  $S_4$ . In fact, the latter two entities  $S_3$  and  $S_4$  are now wholly inoperable. Is this reasonable? We will re-visit this question later.

Does the IIM matrix in this discussion satisfy the Hawkins-Simon condition? Here, the Leontief matrix  $(I - A)$  is

$$I - A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0.90 & 0 & 0 \\ 0.40 & 0 & 0 & 0 \\ 1 & 0.80 & 0 & 0 \\ 1 & 0.90 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -0.90 & 0 & 0 \\ -0.40 & 1 & 0 & 0 \\ -1 & -0.80 & 1 & 0 \\ -1 & -0.90 & 0 & 1 \end{pmatrix}$$

The determinants of the principal minors of  $(I - A)$  are

$$\det |1| = 1 > 0 \quad \det \begin{vmatrix} 1 & -0.90 \\ -0.40 & 1 \end{vmatrix} = 0.64 > 0$$

$$\det \begin{vmatrix} 1 & -0.90 & 0 \\ -0.40 & 1 & 0 \\ -1 & -0.80 & 1 \end{vmatrix} = 0.64 > 0 \quad \det \begin{vmatrix} 1 & -0.90 & 0 & 0 \\ -0.40 & 1 & 0 & 0 \\ -1 & -0.80 & 1 & 0 \\ -1 & -0.90 & 0 & 1 \end{vmatrix} = 0.64 > 0$$

These determinants are all positive, so  $(I - A)$  satisfies the Hawkins-Simon condition. Thus, given the interdependency matrix in this discussion the Leontief/IIM equation  $(I - A)S = C$  is guaranteed to have a non-negative solution for every non-negative  $C$ . This concludes the IIM analysis of the infrastructure systems scenario in Figure 74. Next, we'll evaluate this scenario by the FDNA approach.

In Figure 74, we saw that IIM implicitly subscribes to a "feeder-receiver" metaphor. Moreover, we saw the IIM  $A$ -matrix is really an adjacency matrix of interdependencies which, by definition, has an equivalent mathematical graph. In particular, we demonstrated how this directly relates to an FDNA graph.

Figure 75, shows the FDNA graph associated with the infrastructure systems scenario. Observe this is a 4-node FDNA graph with 6-dependency points and 4-receiver nodes. A mutual dependence also exists between nodes  $S_1$  and  $S_2$ . As discussed in Example 5.13, when mutual dependence between nodes is present it is necessary to specify the **why** and **what** of their joint relationship. In FDNA this is called specification. In IIM, this is identifying their physical connections.

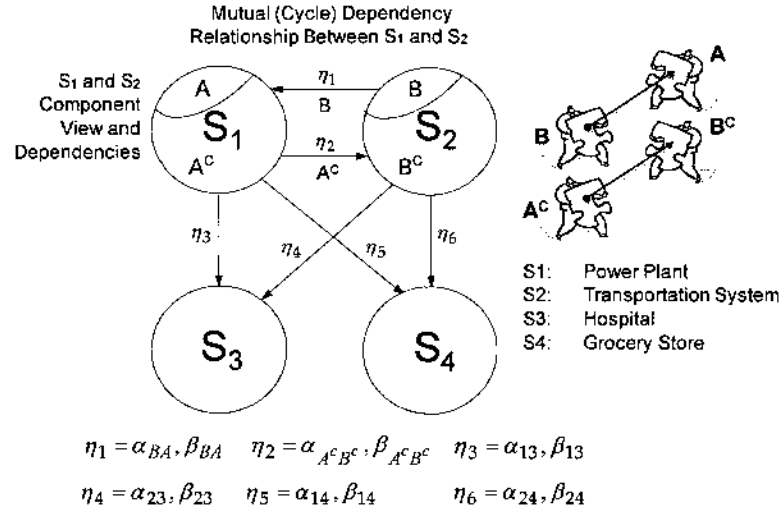


Figure 75. A 4,6,4-Node FDNA Graph of the Infrastructure Systems Scenario

As mentioned earlier, an assumption in IIM is each system “performs a uniquely defined function; that is, no two systems perform the same function” [Haimes, 2004]. Dependencies between systems can be identified by understanding their physical connections. Identifying the physical connections between nodes is equivalent to the concept of constituent nodes in FDNA, as discussed earlier.

Figure 75 is an expanded view of the FDNA graph in Figure 74. This includes a hypothetical decomposition of constituent nodes  $S_1$  and  $S_2$  into their components. Suppose  $S_1$  has components  $A$  and  $A^c$  (all components in  $S_1$  that are not  $A$ ). Suppose  $S_2$  has components  $B$  and  $B^c$  (all components in  $S_2$  that are not  $B$ ). Suppose components  $A$ ,  $A^c$ ,  $B$ , and  $B^c$  define the **why** and **what** of the joint relationship between nodes  $S_1$  and  $S_2$ . From the FDNA graph in Figure 75, we can build the set of FDNA equations as follows:

$$A = \text{Min}(\alpha_{BA}B + 100(1 - \alpha_{BA}), B + \beta_{BA}) = \text{Min}(0.90B + 10, B + \beta_{BA})$$

$$B^c = \text{Min}(\alpha_{A^c B^c}(A^c) + 100(1 - \alpha_{A^c B^c}), A^c + \beta_{A^c B^c}) = \text{Min}(0.40A^c + 60, A^c + \beta_{A^c B^c})$$

$$S_3 = \text{Min} \left( \frac{\alpha_{13}S_1}{2} + \frac{\alpha_{23}S_2}{2} + 100 \left( 1 - \left( \frac{\alpha_{13} + \alpha_{23}}{2} \right) \right), S_1 + \beta_{13}, S_2 + \beta_{23} \right)$$

$$S_3 = \text{Min} \left( \frac{S_1}{2} + \frac{2S_2}{5} + 10, S_1 + \beta_{13}, S_2 + \beta_{23} \right)$$

$$S_4 = \text{Min} \left( \frac{\alpha_{14}S_1}{2} + \frac{\alpha_{24}S_2}{2} + 100 \left( 1 - \left( \frac{\alpha_{14} + \alpha_{24}}{2} \right) \right), S_1 + \beta_{14}, S_2 + \beta_{24} \right)$$

$$S_4 = \text{Min} \left( \frac{S_1}{2} + \frac{9S_2}{20} + 5, S_1 + \beta_{14}, S_2 + \beta_{24} \right)$$

where

$$S_1 = w_1 A + w_2 A^c$$

$$S_2 = u_1 B + u_2 B^c$$

$$w_1 + w_2 = 1, \text{ and } u_1 + u_2 = 1$$

and  $A^c = V_{A^c}(x_{A^c})$  and  $B = V_B(x_B)$  are single dimensional value functions for  $A^c$  and  $B$ , respectively, with  $0 \leq A, A^c, B, B^c, V_{A^c}(x_{A^c}), V_B(x_B), S_1, S_2, S_3, S_4 \leq 100$ . Table 12 presents an operability analysis of this scenario given the equations above.

| FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA)   |                   |               |                   |                                    |                   |               |       |
|---|-------------------|---------------|-------------------|------------------------------------|-------------------|---------------|-------|
| An FDNA Operability Analysis of the Infrastructure Scenario                               |                   |               |                   |                                    |                   |               |       |
| INPUT: $\alpha_{ij}$ Strength of Dependency (SOD)   |                   |               |                   | $\alpha_{ij}$ Within Range ... T/F |                   |               |       |
| $\alpha_{BA}$   | 0.90              | $\alpha_{23}$ | 0.80              | $\alpha_{BA}$                      | TRUE              | $\alpha_{23}$ | TRUE  |
| $\alpha_{A^C B^C}$  | 0.40              | $\alpha_{14}$ | 1.00              | $\alpha_{A^C B^C}$                 | TRUE              | $\alpha_{14}$ | TRUE  |
| $\alpha_{13}$   | 1.00              | $\alpha_{24}$ | 0.90              | $\alpha_{13}$                      | TRUE              | $\alpha_{24}$ | TRUE  |
| INPUT: $\beta_{ij}$ Criticality of Dependency (COD)                                       |                   |               |                   | $\beta_{ij}$ Within Range ... T/F  |                   |               |       |
| $\beta_{BA}$  | 10.00             | $\beta_{23}$  | 20.00             | $\beta_{BA}$                       | TRUE              | $\beta_{23}$  | TRUE  |
| $\beta_{A^C B^C}$   | 60.00             | $\beta_{14}$  | 0.00              | $\beta_{A^C B^C}$                  | TRUE              | $\beta_{14}$  | TRUE  |
| $\beta_{13}$  | 0.00              | $\beta_{24}$  | 10.00             | $\beta_{13}$                       | TRUE              | $\beta_{24}$  | TRUE  |
| Assume $w_1$ and $w_2$ are equally weighted. Assume $u_1$ and $u_2$ are equally weighted. |                   |               |                   |                                    |                   |               |       |
| If $A^C$ and B operability levels at time $t_1$ , $t_2$ , and $t_3$ are:                  |                   |               |                   |                                    |                   |               |       |
| Time $t_1$  |                   | Time $t_2$    |                   | Time $t_3$                         |                   |               |       |
| A   | Function of B     | A             | Function of B     | A                                  | Function of B     |               |       |
| $A^C$   | 100               | $A^C$         | 75                | $A^C$                              | 50                |               |       |
| B   | 100               | B             | 75                | B                                  | 50                |               |       |
| $B^C$   | Function of $A^C$ | $B^C$         | Function of $A^C$ | $B^C$                              | Function of $A^C$ |               |       |
| OUTPUT: Then these receiver nodes are functioning at these operability levels...          |                   |               |                   |                                    |                   |               |       |
| S1  | 100.00            | Power Plant   | S1                | 76.25                              | Power Plant       | S1            | 52.50 |
| S2  | 100.00            | Transp Syst   | S2                | 82.50                              | Transp Syst       | S2            | 65.00 |
| S3  | 100.00            | Hospital      | S3                | 76.25                              | Hospital          | S3            | 52.50 |
| S4  | 100.00            | Grocery Store | S4                | 76.25                              | Grocery Store     | S4            | 52.50 |

Table 12. An FDNA Operability Analysis of the Infrastructure Systems Scenario

### Comparisons and Considerations

The following offers some comparative comments and observations on IIM and FDNA. We begin by comparing the model and solution results produced by IIM and FDNA for *the infrastructure scenario case*. This case was illustrated in Figure 74 and analyzed by IIM and FDNA, respectively, in the preceding discussions.

- **Mutual Dependence:** The infrastructure scenario involved a mutual (cycle) dependency relationship between the power plant  $S_1$  and the transportation system  $S_2$ . IIM and FDNA each address mutual dependence between nodes in similar ways. The following discusses how this is done.

In IIM, identifying the physical connections between nodes is required. IIM also assumes each node performs a “uniquely defined function” [Haimes, 2004]. If each node has a distinct function, then it must consist of one or more components that collectively enable its uniqueness. For this, these components must be mutually independent within each node and across other nodes in the graph. From this, it follows that mutual dependence between nodes (when present) can be resolved by identifying their mutually independent physical connections, as defined by the distinct components that enable their unique functions. A similar thesis is true in FDNA.

In FDNA, physical connections between nodes means specifying their dependency relationships in concrete ways. FDNA also assumes each node performs a uniquely defined function. In FDNA, if each node has a distinct function then it must consist of one or more components that collectively enable its uniqueness. In FDNA, a node with two or more components is called a constituent node. Components contained in constituent nodes are also mutually independent within the node and across other nodes in the FDNA graph. From this, it follows that mutual dependence between nodes (when present) can also be resolved by identifying their mutually independent physical connections, defined by the distinct components that enable their unique functions. With this, cycle relationships can be expressed by acyclic ones.

- **Infrastructure Scenario: Operability Analysis Comparison:** In the infrastructure scenario, IIM and FDNA produced different levels of inoperability for  $S_1$ ,  $S_2$ ,  $S_3$ , and  $S_4$  if a weather event caused the transportation system  $S_2$  to lose 50 percent of its operability. The IIM results are shown prior to the FDNA analysis, summarized in Table 12.

In IIM, the effect of the weather perturbation on the operability of  $S_2$  produced operability losses within itself and in the power plant  $S_1$ , the hospital  $S_3$ , and the grocery store  $S_4$ . This is due to the interdependencies between them as expressed by the  $A$ -matrix. Shown in the IIM solution to this scenario, the operability declined to (1) 30 utils for the power plant (2) 22 utils for the transportation system (3) 0 utils for the hospital and (4) 0 utils for the grocery store. In this case, the hospital and grocery store became wholly inoperable, in fact their inoperability levels exceeded the maximum value allowed in IIM. The true IIM solution vector for the infrastructure scenario is

$$S = [0.703125, 0.78125, 1.32813, 1.40625]$$

Since inoperability cannot be greater than one, the convention in IIM is to modify the solution vector as

$$S = [0.703125, 0.78125, 1, 1]$$



However, such a truncation implies the modified vector  $S = [0.703125, 0.78125, 1, 1]$  is no longer a true solution to the specific IIM system of equations. This may not be an issue in a stationary IIM. It could be an issue in a nonstationary IIM, where inoperability measures derived for the  $t$ -th state may depend on their values derived for the preceding state.

The rate of operability loss may not always be realistic. In the infrastructure scenario, is it realistic for the grocery store to become 140 percent inoperable just because the transportation system loses 50 percent of its functionality? In fact, one can show the grocery store becomes 100 percent inoperable when the transportation system suffers only a 36 percent loss of functionality.

Should a grocery store have such a criticality of dependency on the transportation system? Perhaps. Nonetheless, the FDNA analysis summarized in Table 12 shows the grocery store losing about 48 percent of its operability if the transportation system experiences a 50 percent decline in functionality. Here, FDNA computes operability loss or gain by a weakest link formulation of its dependency function. Specifying such a function enables analysts to modulate the rate of operability loss or gain deemed appropriate to the nature of a dependency relationship.

- **Non-Negative Solutions:** Non-negative solutions to an IIM model are determined by whether the Leontief matrix  $(I - A)$  meets the Hawkins-Simon condition (Definition 5.11). If this condition is met, then  $(I - A)$  is nonsingular (invertible) and solutions to the IIM system of equations  $(I - A)S = C$  are non-negative for every non-negative vector  $C$ . Although Hawkins-Simon guarantees non-negative solutions, it does not guarantee they are always less than or equal to one. Elements of the solution vector  $S$  may greatly exceed the maximum inoperability level, as evidenced in the infrastructure scenario. Hence, for these elements a forced truncation to a value of one is needed.

Unfortunately, even if the Leontief matrix  $(I - A)$  meets the Hawkins-Simon condition it may be *ill-conditioned*. An ill-conditioned matrix signals that solutions to its equivalent linear system may be highly sensitive to small changes in elements of the matrix. In linear algebra, an index known as the *condition number*<sup>\*</sup> measures the degree a matrix is ill-conditioned. The condition number of a matrix is always greater than or equal to one.

The farther from one the condition number of a matrix (say  $(I - A)$ ) the greater the instability of solutions to its equivalent linear system – seemingly minor changes in elements of  $(I - A)$  or the vector  $C$  can produce large changes in IIM system solutions. Stable solutions to linear systems have their coefficient matrices with condition numbers close to one. A matrix is singular (non-invertible) if its condition number is infinite.

The Hilbert matrix nicely illustrates an increasingly ill-conditioned matrix. The Hilbert matrix is a symmetric matrix whose elements  $h_{ij}$  are fractions and has the following general form.

---

<sup>\*</sup> The condition number of matrix  $A$  is equal to the norm of  $A$  times the norm of  $A^{-1}$ , where the norm of  $A$  is defined as

$$\|A\|_{\infty} = \max_i \sum_{j=1}^n |a_{ij}|.$$

$$H_{ij} = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \dots \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \dots \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \text{ where } h_{ij} = \frac{1}{i+j-1}$$

Solutions to linear systems with Hilbert coefficient matrices become rapidly unstable as the number of equations in the system increase. A Hilbert coefficient matrix for  $n = 2, 3, 4, 5$ , and  $6$  linear equations in a system has condition numbers  $27, 748, 28375, 943656$ , and  $29070279$ , respectively. Thus, systems of linear equations with Hilbert coefficient matrices quickly become unstable with each unit increase in the number of equations in a system.

The stability of solutions to Leontief/IIM systems of equations can also be determined by the modulus of the eigenvalues of  $(I - A)$ . If the modulus of each eigenvalue of  $(I - A)$  is less than one, then the matrix  $(I - A)$  is stable. In this case, all eigenvalues of  $(I - A)$  fall within the unit circle\*. If the modulus of any eigenvalue of  $(I - A)$  is greater than one, then the matrix  $(I - A)$  is unstable. In this case, one or more eigenvalues of  $(I - A)$  fall outside the unit circle. If, say, the modulus of one eigenvalue of  $(I - A)$  is equal to one but the others each have modulus less than one, then the matrix  $(I - A)$  might be considered weakly stable.

The IIM analysis of the infrastructure scenario illustrates a characteristic of ill-conditioned matrices. Here, the solution to the IIM system of equations is affected by which element of the  $C$ -vector is affected by the perturbing event. Instead of a storm destroying 50 percent of the functionality of the transportation system infrastructure  $S_2$ , suppose the hospital  $S_3$  loses 100a percent of its functionality. The  $C$ -vector then changes from  $C = [0, 0.50, 0, 0]$  to  $C = [0, 0, a, 0]$ . The IIM equation would then be

$$S \begin{pmatrix} 0 & 0.90 & 0 & 0 \\ 0.40 & 0 & 0 & 0 \\ 1 & 0.80 & 0 & 0 \\ 1 & 0.90 & 0 & 0 \end{pmatrix} S = \begin{bmatrix} 0 \\ 0 \\ a \\ 0 \end{bmatrix} \quad (5.69)$$

From Equation 5.69, the resultant IIM system of equations is

$$S_1 = 0.90S_2 \quad (5.70)$$

$$S_2 = 0.40S_1 \quad (5.71)$$

$$S_3 = S_1 + 0.80S_2 + a \quad (5.72)$$

$$S_4 = S_1 + 0.90S_2 \quad (5.73)$$

---

\* The unit circle is the contour in the complex plane, with the modulus  $|z| = \sqrt{a^2 + b^2} = 1$ .

This system now has only a trivial solution with  $S = [0, 0, a, 0]$  compared to the original solution vector  $S = [0.703125, 0.78125, 1.32813, 1.40625]$ . A similar result is seen if an event has impacts on multiple elements of the  $C$ -vector. For instance, if an event simultaneously perturbs  $S_3$  and  $S_4$  with  $C = [0, 0, a, b]$  then the resultant IIM system of equations has the solution vector  $S = [0, 0, a, b]$ . These solution vectors are very different from the original solution vector.

Unsteady behavior in a solution signals the coefficient matrix of the associated linear system may be ill-conditioned. The  $(I - A)$  matrix, in this scenario, passes the Hawkins-Simon condition. Its condition number is 17.2. However, the moduli of three of its four eigenvalues lie outside the unit circle. Thus,  $(I - A)$  is unstable; therefore, solutions to its system of linear equations will not converge to fixed solution vector.

In summary, IIM is subject to solvability issues such as these because its computational basis is rooted in matrix algebra. Although all FDNA graphs can be represented by matrices, FDNA equations are constructed from these graphs in ways that enable solutions to be derived by a composition of functions approach. This strategy avoids matrix algebra and the issues that come with that formalism. Furthermore, from Postulate 5.4 recall that all FDNA graphs are acyclic. This further enables the algebraic solvability of FDNA equations because of a process called *specification*<sup>\*</sup>. The following illustrates this for an FDNA graph of intra- and interdependent nodes whose  $(I - A)$  matrix fails the Hawkins-Simon condition, but is solvable by FDNA.

**Example 5.22: FDNA With Intra- and Interdependent Nodes**

Conduct an FDNA operability analysis of the IIM  $A$ -matrix in Figure 76.

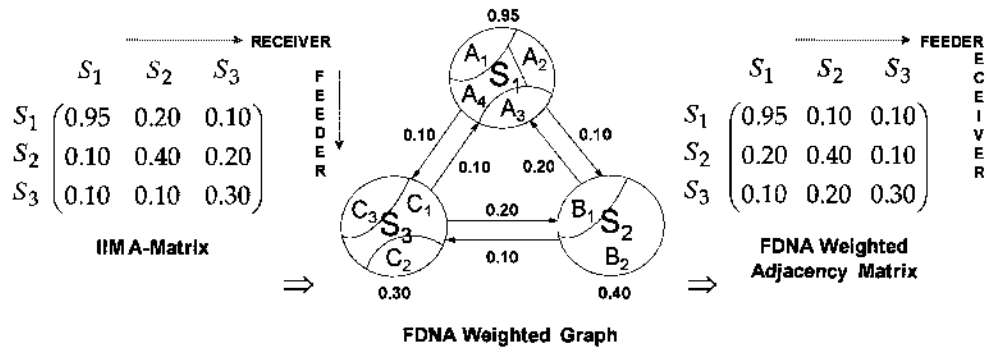


Figure 76. An IIM  $A$ -Matrix With Weighted FDNA Graph

First, we look at the principal minors of  $(I - A)$  to determine if  $(I - A)$  meets the Hawkins-Simon condition. Given  $A$ , the determinants of the principal minors of  $(I - A)$  are as follows:

$$\det |0.05| = 0.05 > 0 \quad \det \begin{vmatrix} 0.05 & -0.20 \\ -0.10 & 0.60 \end{vmatrix} = 0.01 > 0 \quad \det \begin{vmatrix} 0.05 & -0.20 & -0.10 \\ -0.10 & 0.60 & -0.20 \\ -0.10 & -0.10 & 0.70 \end{vmatrix} = -0.005 < 0$$

<sup>\*</sup> Refer to the discussion on constituent nodes, components, and mutual dependence in Chapter V and Example 5.12.

Since these determinants are not all positive, it follows that  $(I - A)$  fails to meet the Hawkins-Simon condition. Thus, the Leontief/IIM equation  $(I - A)S = C$  is not guaranteed to have a non-negative solution for every non-negative  $C$ , even though  $(I - A)$ , in this case, is a stable matrix. However, an FDNA operability analysis can be done since it uses a different calculus than one rooted in the matrix algebra of IIM. This is illustrated in the following discussion.

Explained earlier, the IIM  $A$ -matrix is transpose equivalent to an adjacency matrix of an FDNA graph. From this, the left-most image in Figure 77 is the FDNA graph associated with the IIM  $A$ -matrix in Figure 76. In Figure 77, the arrows follow the FDNA feeder-receiver row-column path.

In Figure 77, the left-most graph is a cycle graph. In accordance with Postulate 5.4, FDNA graphs must be acyclic. FDNA, like IIM, models the physical connections between nodes. This means specifying their dependency relationships in concrete ways. Like IIM, FDNA also assumes each node performs a uniquely defined function. Thus, if each node has a distinct function then it must consist of one or more components that collectively enable its uniqueness.

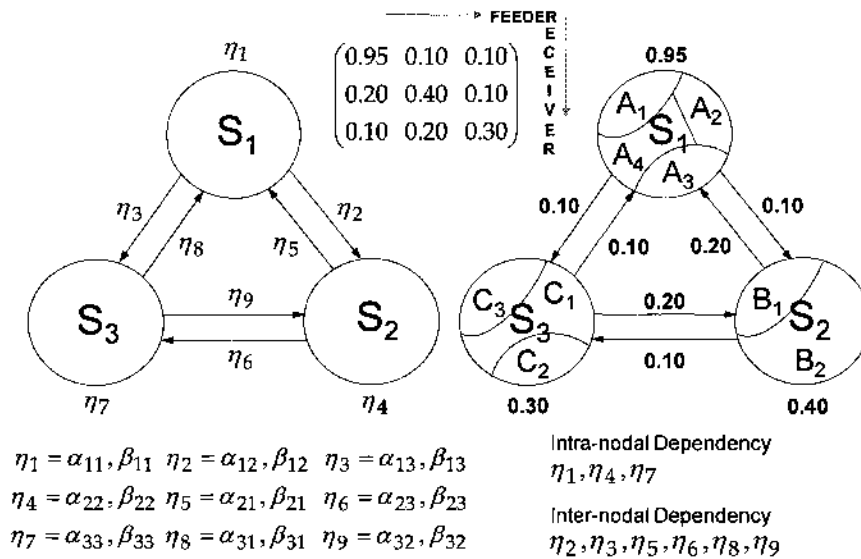


Figure 77. Weighted FDNA Graph With  $(\alpha, \beta)$  Parameters

In FDNA, recall that a node with two or more components is called a constituent node. Components contained in constituent nodes are also mutually independent within the node and across other nodes in the FDNA graph. From this, it follows that mutual dependence between nodes (when present) can be resolved by identifying their mutually independent physical connections defined by the distinct components that enable their unique functions. With this, cycle relationships can be expressed by acyclic connections. The right-most side of Figure 77 shows a breakout (presumed) of the left-most graph into its constituent nodes and components. Let's suppose node  $S_1$  is specified by four components, node  $S_2$  is specified by two components, and node  $S_3$  is specified by three components.

Example 5.22 illustrates the ability of FDNA to handle intra-nodal dependencies. In an FDNA graph, intra-nodal dependencies indicate one or more nonzero diagonals exist in the graph's

weighted adjacency matrix. In Example 5.22, three diagonal elements of the  $A$ -matrix are nonzero.

Figure 78 illustrates intra- and interdependencies between the components of the FDNA graph in Figure 77. These component feeder-receiver relationships are presumed with the intent to illustrate results from a *specification process*. This process drives an FDNA cycle graph into an acyclic one (required by Postulate 5.4)\*. The alpha values in Figure 78 originate from the  $A$ -matrix in Example 5.22.

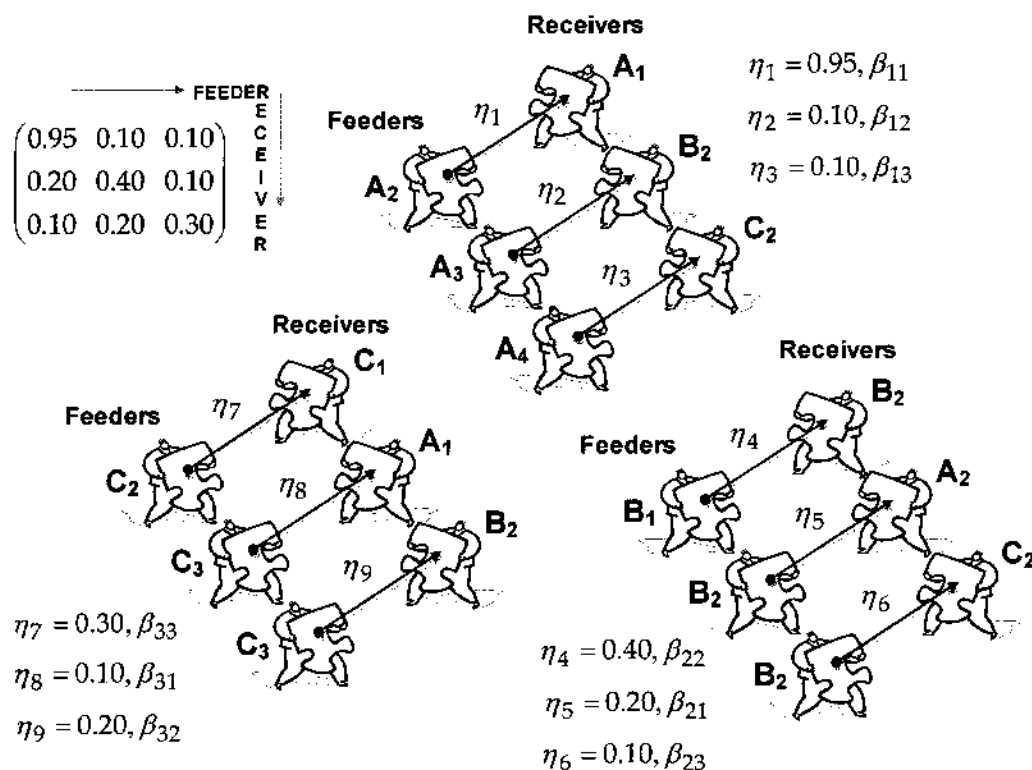


Figure 78. Component Feeder-Receiver Relationships (Example 5.22, Presumed)

Figure 79 presents an integration of the pair-wise component connections shown in Figure 78. These are the feeder-receiver pairs that when connected reveal which components are strictly leaf nodes, which are feeder and receiver nodes, and which are strictly receiver nodes.

\* As mentioned earlier, IIM implicitly requires cycle relationships to be expressed by acyclic ones by identifying the physical connections between nodes, where nodes in IIM perform unique functions. In the IIM infrastructure scenario, recall that nontrivial solutions to the linear system became trivial solutions when the  $C$ -vector changed from  $[0, 0.50, 0, 0]$  to  $[0, 0, a, b]$ . This change resulted in a cycle relationship forming between  $S_1$  and  $S_2$  that was previously not there. This can be seen in the first two equations of the IIM linear system given by Equations 5.70 through 5.73.

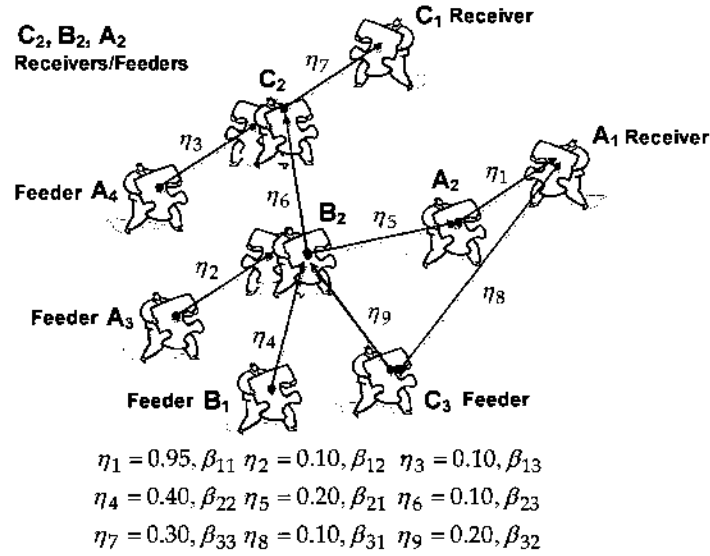


Figure 79. Component Connections and Feeders/Receivers (Integrated View)

From the last three figures, we can build the FDNA equations for the problem in Example 5.22. They are as follows:

$$S_1 = w_1 A_1 + w_2 A_2 + w_3 A_3 + w_4 A_4, \quad \text{where } w_1 + w_2 + w_3 + w_4 = 1$$

$$S_2 = u_1 B_1 + u_2 B_2, \quad \text{where } u_1 + u_2 = 1$$

$$S_3 = r_1 C_1 + r_2 C_2 + r_3 C_3, \quad \text{where } r_1 + r_2 + r_3 = 1$$

$$C_1 = \text{Min}(\alpha_{33} C_2 + 100(1 - \alpha_{33}), C_2 + \beta_{33})$$

$$C_2 = \text{Min} \left( \frac{\alpha_{13} A_4}{2} + \frac{\alpha_{23} B_2}{2} + 100(1 - (\frac{\alpha_{13} + \alpha_{23}}{2})), A_4 + \beta_{13}, B_2 + \beta_{23} \right)$$

$$B_2 = \text{Min}(X, Y) \text{ where}$$

$$X = \frac{\alpha_{12} A_3}{3} + \frac{\alpha_{22} B_1}{3} + \frac{\alpha_{32} C_3}{3} + 100(1 - (\frac{\alpha_{12} + \alpha_{22} + \alpha_{32}}{3}))$$

$$Y = \text{Min}(A_3 + \beta_{12}, B_1 + \beta_{22}, C_3 + \beta_{32})$$

$$A_2 = \text{Min}(\alpha_{21} B_2 + 100(1 - \alpha_{21}), B_2 + \beta_{21})$$

$$A_1 = \text{Min} \left( \frac{\alpha_{11} A_2}{2} + \frac{\alpha_{31} C_3}{2} + 100(1 - (\frac{\alpha_{11} + \alpha_{31}}{2})), A_2 + \beta_{11}, C_3 + \beta_{31} \right)$$

where  $A_4$ ,  $A_3$ ,  $B_1$ , and  $C_3$  are feeder (leaf) nodes as seen in Figure 79. All variables in these equations are single dimensional value functions, explained in earlier discussions. Table 13 presents an operability analysis of this case (Example 5.22) using the preceding equations.

| FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA)   |        |  |       |                                    |      |               |      |
|---|--------|--|-------|------------------------------------|------|---------------|------|
| An FDNA Operability Analysis of the IIM A-Matrix in Example 5.22                            |        |  |       |                                    |      |               |      |
| INPUT:  |        | $\alpha_{ij}$ Strength of Dependency (SOD)   |       | $\alpha_{ij}$ Within Range ... T/F |      |               |      |
| $\alpha_{11}$   | 0.95   | $\alpha_{21}$                                | 0.20  | $\alpha_{11}$                      | TRUE | $\alpha_{21}$ | TRUE |
| $\alpha_{12}$   | 0.10   | $\alpha_{22}$                                | 0.40  | $\alpha_{12}$                      | TRUE | $\alpha_{22}$ | TRUE |
| $\alpha_{13}$   | 0.10   | $\alpha_{23}$                                | 0.10  | $\alpha_{13}$                      | TRUE | $\alpha_{23}$ | TRUE |
| SOD values come from the IIM A-Matrix   |        | $\alpha_{31}$                                | 0.10  |                                    |      | $\alpha_{31}$ | TRUE |
|   |        | $\alpha_{32}$                                | 0.20  |                                    |      | $\alpha_{32}$ | TRUE |
|   |        | $\alpha_{33}$                                | 0.30  |                                    |      | $\alpha_{33}$ | TRUE |
| INPUT:  |        | $\beta_{ij}$ Criticality of Dependency (COD) |       | $\beta_{ij}$ Within Range ... T/F  |      |               |      |
| $\beta_{11}$  | 5.00   | $\beta_{21}$                                 | 80.00 | $\beta_{11}$                       | TRUE | $\beta_{21}$  | TRUE |
| $\beta_{12}$  | 80.00  | $\beta_{22}$                                 | 60.00 | $\beta_{12}$                       | TRUE | $\beta_{22}$  | TRUE |
| $\beta_{13}$  | 90.00  | $\beta_{23}$                                 | 90.00 | $\beta_{13}$                       | TRUE | $\beta_{23}$  | TRUE |
| Suppose we have these COD values  |        | $\beta_{31}$                                 | 90.00 |                                    |      | $\beta_{31}$  | TRUE |
|   |        | $\beta_{32}$                                 | 80.00 |                                    |      | $\beta_{32}$  | TRUE |
|   |        | $\beta_{33}$                                 | 70.00 |                                    |      | $\beta_{33}$  | TRUE |
| Assume equally weighted components in each constituent node S1, S2, and S3                  |        |  |       |                                    |      |               |      |
| If the operability levels of these components of S1, S2, and S3 at time t1, t2, and t3 are: |        |  |       |                                    |      |               |      |
| Time t1   |        | Time t2                                      |       | Time t3                            |      |               |      |
| A4  | 100    | A4   | 75    | A4                                 |      | 50            |      |
| A3  | 100    | A3   | 75    | A3                                 |      | 50            |      |
| B1  | 100    | B1   | 75    | B1                                 |      | 50            |      |
| C3  | 100    | C3   | 75    | C3                                 |      | 50            |      |
| OUTPUT: Then these nodes are functioning at these operability levels...                     |        |  |       |                                    |      |               |      |
| S1  | 100.00 | S1   | 87.15 | S1                                 |      | 74.30         |      |
| S2  | 100.00 | S2   | 84.58 | S2                                 |      | 69.17         |      |
| S3  | 100.00 | S3   | 91.00 | S3                                 |      | 82.00         |      |
| C2  | 100.00 | C2   | 98.46 | C2                                 |      | 96.92         |      |
| C1  | 100.00 | C1   | 99.54 | C1                                 |      | 99.08         |      |
| B2  | 100.00 | B2   | 94.17 | B2                                 |      | 88.33         |      |
| A2  | 100.00 | A2   | 98.83 | A2                                 |      | 97.67         |      |
| A1  | 100.00 | A1   | 99.77 | A1                                 |      | 99.53         |      |

Table 13. An FDNA Operability Analysis of the IIM A-Matrix in Example 5.22

## SUMMARY

This chapter introduced a new formalism for the analysis of dependencies. This formalism is called Functional Dependency Network Analysis (FDNA). FDNA is an approach and a calculus for capturing and measuring operability-inoperability relationships between entities in engineering or operating an enterprise.

The importance of the dependency problem in enterprise engineering is many-fold. Primary is enabling the study of ripple effects of failure in one capability on the operability of other dependent capabilities across an enterprise. Providing mechanisms to anticipate these effects early in design enables engineers to minimize dependency risks that, if realized, may have cascading negative effects on the ability of an enterprise to deliver services to users.

The risk analysis community has published many scholarly papers involving methods to capture dependencies between entities in various problems contexts. A list of recent publications is shown in the footnote below\*. A prominent method in the community is the Inoperability Input-Output Model (IIM), discussed in the preceding sections. The motivation for FDNA came from the need to further generalize the underlying mathematics that defines input-output (I/O) models in economic science and IIM in particular.

The Leontief I/O model is the classical formalism of input-output economics. Its mathematical protocols are based on matrix algebra. As such, the Leontief model will not produce meaningful solutions if the *Hawkins-Simon condition* on principal minors is not met.

For this dissertation, it was initially thought Leontief's original input-output model [Leontief, 1966] could be leveraged onto the dependency problem herein. However, matrix algebra restrictions (e.g., the Hawkins-Simon condition) occurred too often when its original formulation was applied in this research context.

Thus, it became necessary to think further about dependencies and what mutual relationships between entities really mean, whether these entities are economic sectors, critical infrastructures, or receiver-feeder nodes in an FDNA graph. As mentioned earlier, FDNA equations are constructed from mathematical graphs in ways that enable solutions to be derived by a composition of functions; that is, FDNA equations are algebraically formulated by a composition of functional dependency relationships across a mathematical graph. This strategy avoids matrix algebra and linear system solution issues that can (on occasion) come with Leontief's original input-output model\*\*.

The FDNA structure is visualized by graph theory to represent and model a range of complex dependency relationships between entities. FDNA has the potential to be a generalized modeling approach for a variety of dependency problems, including those in the domains of input-output economics, critical infrastructure risk analysis, and nonstationary dependency analysis problems.

---

\* Santos, J. R., Haimés, Y. Y., 2004. "Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures", *Risk Analysis*, Vol. 24, No. 6.

Jiang, P., Haimés, Y. Y., 2004. "Risk Management for Leontief-Based Interdependent Systems", *Risk Analysis*, Vol. 24, No. 5.

Crowther, K. G., Haimés, Y. Y., Taub, G., 2007. "Systemic Valuation of Strategic Preparedness Through Application of the Inoperability Input-Output Model with Lessons Learned from Hurricane Katrina", *Risk Analysis*, Vol. 27, No. 5.

Santos, J. R., Haimés, Y. Y., Lian, C., 2007. "A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies", *Risk Analysis*, Vol. 27, No. 5.

Lian, C., Santos, J. R., Haimés, Y. Y., 2007. "Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors", *Risk Analysis*, Vol. 27, No. 4.

Ayyub, B. M., McGill, W. L., Kaminsky, M., 2007. "Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework", *Risk Analysis*, Vol. 27, No. 4.

Cox, L. A., 2009. "Improving Risk-Based Decision Making for Terrorism Applications", *Risk Analysis*, Vol. 29, No. 3.

\*\* Today, the United States Department of Commerce, Bureau of Economic Analysis (BEA), is a primary data source for Leontief input-output analyses. Data from the BEA are empirically derived and purposefully designed so that the Leontief  $(I - A)$  matrix meets (almost always) the Hawkins-Simon condition, with stable solutions to the associated linear system of equations.



In addition, FDNA's calculus could be expanded to account for changes in operability levels as a function of time. Building temporal features into FDNA and incorporating them into a modeling environment (e.g., a systems dynamics tool environment) is a rich area to further explore.

Protocols could also be developed to conduct sensitivity analyses within the FDNA approach. This includes elicitation procedures for specifying uncertainty distributions (e.g., triangular distributions) around key FDNA parameters, such as  $\alpha_{ij}$  and  $\beta_{ij}$ . Discrete or probabilistic simulations could then be run to identify Pareto optimal tradeoffs between system improvements, investment costs, and anticipated reductions in operability risks.

In summary, and with respect to this dissertation, FDNA is a methodology that enables management to study and **anticipate** the ripple effects of losses in supplier-program contributions on dependent capabilities **before** risks that threaten these suppliers are realized. Where the RCR index (Chapter IV) identifies which supplier programs face high risk (incorporating effects of risk inheritance) in delivering their contributions to capability, FDNA identifies whether the level of operability loss, if such risks occur, is acceptable. This enables management to better target risk resolution resources to those supplier programs that face high risk **and** are most critical to the operational capabilities of a portfolio.

## CHAPTER VI

### PRIORITIZING RISK MANAGEMENT DECISIONS

#### INTRODUCTION

This chapter presents a decision-theoretic approach for prioritizing risk management decisions as a function of the risk measures and analysis procedures developed in the previous chapters. These measures are integrated into advanced ranking algorithms to isolate and prioritize which capabilities are most risk-threatened and qualify for deliberate management attention. This methodology enables decision-makers to target risk reduction resources in ways that optimally reduce threats posed by risks to critical capability outcome objectives.

#### A PRIORITIZATION ALGORITHM

Management decisions often involve choosing the “best” or “most-preferred” option among a finite set of competing alternatives. Similar selection decisions exist in risk management. Instead of choosing the most-preferred alternative, risk management decisions involve choosing the most-preferred risks to reduce, or eliminate, because of their threats to capability. In either situation, the common question is “*How to identify selecting the best option from a finite set of competing alternatives*”? Addressing this is the focus of rational decision-making, supported by a variety of analytical formalisms developed in the last three-hundred years.

In general, selection algorithms produce rankings of options from a finite set of competing alternatives as a function of how each performs across multiple evaluation criteria. Algorithms that produce ordered-rankings fall into two classes. These are ordinal methods and cardinal methods. Ordinal methods apply scales to rate the performance of alternatives by numbers that represent order. Ordinal scales are common in the social sciences, where they are often used for attitude measurement. However, only the ordering of numbers on these scales is preserved. The distance between them is indeterminate (not meaningful). Arithmetic operations beyond “greater-than”, “less-than”, or “equal-to” are impermissible. Thus, ordinal ranking algorithms isolate which alternative in a finite set of competing alternatives is more critical than the others. However, they cannot measure the distance between ranked alternatives.

Cardinal methods apply scales to rate the performance of alternatives by numbers that represent an ordered-metric. This means the distance between numbers on a cardinal scale is determinate (meaningful). Examples of numbers on a cardinal scale include the probability measure or degrees centigrade. For purposes of this research, we employ a cardinal-based approach to this ranking problem. This provides analytic flexibility to integrate optimization protocols with ranking algorithms when (or if) optimal assignments of risk reduction resources, under a variety of constraints, need to be determined at a later point.

As mentioned above, there are many algorithms in decision analysis that can be tailored to address the problem of ranking risks (say) from most- to least-critical to an engineering system. Many have their origins in vNM expected utility theory [von Neumann, Morgenstern, 1944].

From utility theory, a well-established algorithm known as the linear additive model is a popular approach [Keeney, Raiffa, 1976]. A form of the linear additive model is given by Equation 6.1 [Garvey, 2008]. Furthermore, it has been proved if the criteria in a selection problem are mutually preferentially independent then the evaluator's preferences can be represented by an additive value function [Keeney, Raiffa, 1976].

### Linear Additive Model

A value function  $V_Y(y)$  is an additive value function if there exists  $n$  single dimensional value functions  $V_{X_1}(x_1)$ ,  $V_{X_2}(x_2)$ ,  $V_{X_3}(x_3)$ , ...,  $V_{X_n}(x_n)$  satisfying

$$V_Y(y) = w_1 V_{X_1}(x_1) + w_2 V_{X_2}(x_2) + w_3 V_{X_3}(x_3) + \dots + w_n V_{X_n}(x_n) \quad (6.1)$$

where  $w_i$  for  $i = 1, \dots, n$  are non-negative weights (importance weights) whose values range between zero and one and where  $w_1 + w_2 + w_3 + \dots + w_n = 1$ .

The linear additive model is representative of a class of decision rules known as compensatory models. Compensatory models allow tradeoffs to compete between attributes (or criteria). For instance, an alternative with low scores on some attributes (or criteria) can improve in its attractiveness to a decision-maker if this is compensated by high values on other attributes; hence, the average or expected-value effect that can come from compensatory decision models.

There is another class of decision rules known as compromise solution models. These rules assume that choice among alternatives depends on a reference point (e.g., an ideal set of outcomes on all attributes) and attempts to minimize the distance between alternatives and the reference point [Malczewski, 1999].

More commonly referred to as ideal point methods, these approaches generate a complete ranking of alternatives as a function of their relative distance from the hypothetical ideal (the alternative characterized by attributes with all ideal values). "Ideal point methods treat alternatives and their attributes as inseparable bundles, all competing for closeness in similarity to the ideal alternative" [Malczewski, 1999].

The ideal point represents a hypothetical alternative that consists of the most desirable weighted normalized levels of each criterion across the set of competing alternatives. The alternative closest to the ideal point solution performs best in the set. Separation from the ideal point is measured geometrically by a Euclidean distance metric.

Ranking algorithms that derive from vNM decision theory are rooted in maximizing expected utility. In contrast, those that derive from ideal point methods are rooted in maximizing similarity to the ideal solution. The best alternative is the compromise solution relative to that reference point.

Seen in the previous chapters, complex dependency relationships are the norm and not the exception in engineering an enterprise. Entities such as supplier-provider nodes play key roles in planning, engineering, and managing an enterprise. Their effects on the success or failure of delivering capabilities to users are such that tradeoffs between them might not be realistic or even

advisable. For this reason, we approach the ranking problem in this chapter by way of a compromise model. This does not preclude the use of compensatory models, if and when tradeoffs between entities are reasonable. This is a fruitful area of continued research.

### Compromise Models

Figure 80 illustrates the motivation for the development of compromise solution models. Two alternatives  $A_1$  and  $A_2$  are shown in relation to two benefit criteria or attributes (Attribute 1 and Attribute 2). In Figure 80, observe that  $A_1$  is closest to the ideal solution  $A^*$  but  $A_2$  is farthest from the negative ideal solution  $A^-$ . Given this, which alternative do you choose?

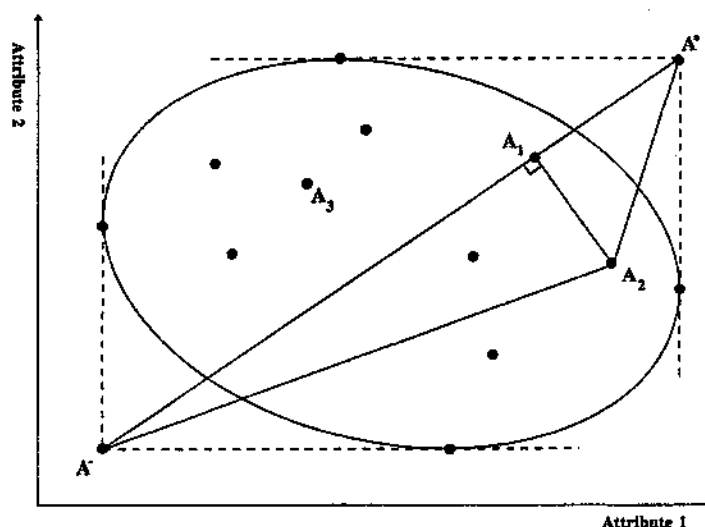


Figure 80\*. Euclidean Distances to Positive and Negative Ideal Solutions

An ideal point method that reconciles this question is TOPSIS – *Technique for Order Preference by Similarity to Ideal Solution* [Hwang, Yoon, 1995]. TOPSIS is an ideal point method that ensures the chosen alternative is simultaneously closest to the ideal solution and farthest from the negative ideal solution. TOPSIS chooses the alternative whose performance across all criteria maximally matches those that comprise the ideal solution.

TOPSIS assumes each attribute (or criterion) can be characterized by either monotonically increasing or decreasing utility. Here, we seek to maximize attributes that offer a benefit and minimize those that incur a cost. TOPSIS generates an index that rank-orders competing alternatives from most-to-least-desired on the relative distance of each to the ideal solution.

The TOPSIS algorithms operate on a generalized decision matrix of alternatives as shown in Table 14. Here, the performance of an alternative is evaluated across competing criteria. The attractiveness of an alternative to a decision-maker is a function of the performance of each alternative across these criteria.

\* Reprinted by permission of Sage Publications, Inc. [Hwang, Yoon, 1995].

| Decision<br>Alternative | Criteria & Weights |                 |                 |     |                 |
|-------------------------|--------------------|-----------------|-----------------|-----|-----------------|
|                         | C <sub>1</sub>     | C <sub>2</sub>  | C <sub>3</sub>  | ... | C <sub>n</sub>  |
|                         | w <sub>1</sub>     | w <sub>2</sub>  | w <sub>3</sub>  | ... | w <sub>n</sub>  |
| A <sub>1</sub>          | x <sub>11</sub>    | x <sub>12</sub> | x <sub>13</sub> | ... | x <sub>1n</sub> |
| A <sub>2</sub>          | x <sub>21</sub>    | x <sub>22</sub> | x <sub>23</sub> | ... | x <sub>2n</sub> |
| A <sub>3</sub>          | x <sub>31</sub>    | x <sub>32</sub> | x <sub>33</sub> | ... | x <sub>3n</sub> |
| ...                     | ...                | ...             | ...             | ... | ...             |
| A <sub>m</sub>          | x <sub>m1</sub>    | x <sub>m2</sub> | x <sub>m3</sub> | ... | x <sub>mn</sub> |

**A Decision Matrix**

Table 14. A Traditional Decision or Performance Matrix of Alternatives

Applying TOPSIS consists of the following steps and equations.

### Step 1

Normalize the decision matrix of alternatives (Table 14). One way is to compute  $r_{ij}$  where

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^m x_{ij}^2}} \quad i = 1, \dots, m; \quad j = 1, \dots, n \quad (6.2)$$

### Step 2

Compute a matrix of weighted normalized values according to  $v_{ij}$ ,

$$v_{ij} = w_j r_{ij} \quad i = 1, \dots, m; \quad j = 1, \dots, n \quad (6.3)$$

where  $w_j$  is weight of the  $j$ -th attribute (criterion).

### Step 3

Derive the positive  $A^*$  and the negative  $A^-$  ideal solutions, where

$$A^* = \{v_1^*, v_2^*, \dots, v_j^*, \dots, v_n^*\} = \{(\max_i v_{ij} \mid j \in J_1), (\min_i v_{ij} \mid j \in J_2) \mid i = 1, \dots, m\} \quad (6.4)$$

$$A^- = \{v_1^-, v_2^-, \dots, v_j^-, \dots, v_n^-\} = \{(\min_i v_{ij} \mid j \in J_1), (\max_i v_{ij} \mid j \in J_2) \mid i = 1, \dots, m\} \quad (6.5)$$

where  $J_1$  is the set of benefit attributes and  $J_2$  is the set of cost attributes.

### Step 4

Calculate separation measures between alternatives, as defined by the  $n$ -dimensional Euclidean distance metric. The separation from the positive-ideal solution  $A^*$  is given by

$$S_i^* = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^*)^2} \quad i = 1, \dots, m \quad (6.6)$$

The separation from the negative-ideal solution  $A^-$  is given by

$$S_i^- = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^-)^2} \quad i = 1, \dots, m \quad (6.7)$$

#### Step 5

Calculate similarities to positive-ideal solution, as follows:

$$0 \leq C_i^* = \frac{S_i^-}{(S_i^* + S_i^-)} \leq 1 \quad i = 1, \dots, m \quad (6.8)$$

#### Step 6

Choose the alternative in the decision matrix with the maximum  $C_i^*$  or rank these alternatives from most-to least-preferred according to  $C_i^*$  in descending order. The closer  $C_i^*$  is to unity the closer it is to the positive-ideal solution. The farther  $C_i^*$  is from unity the farther it is from the positive-ideal solution.

In summary, the optimal compromise solution produced from these steps is given by

$$\text{Max } \{C_1^*, C_2^*, C_3^*, \dots, C_n^*\}$$

The alternative with the maximum  $C_i^*$  will be closest to the ideal solution and concurrently farthest from the least ideal solution.

#### Criteria Weights

Weighting the importance of each criterion in a decision matrix is a key consideration that influences the outcomes of a decision analysis. In the TOPSIS algorithm, criteria weights are entered at Step 2. How are weights determined?

The literature presents many ways to derive criteria weights [Clemen, 1996; Kirkwood, 1997]. These include subjective weighting methods, objective weighting methods, and a mix of these approaches. Subjective weighting involves an opinion-based specification of criteria weights. Objective weighting emphasizes the use of facts rather than thoughts or opinions in the specification of criteria weights. Because of this, objective weighting has the desirable feature of letting the “data” say which criterion, in the set of criteria, is most important, which is next most important, and so forth.

The canonical approach to objective criteria weighting is the *entropy method*. Entropy\* is a concept found in information theory that measures the uncertainty associated with the expected information content of a message. It is also used in decision science to measure the amount of decision information contained and transmitted by a criterion.

---

\* In information theory, entropy measures the uncertainty associated with the expected information content of a message. The classical work in information entropy is in *A Mathematical Theory of Communication*, written by Claude E. Shannon, Bell System Technical Journal, 1948.

The amount of decision information contained and transmitted by a criterion is driven by the extent the performance (i.e., “score”) of each alternative is distinct and differentiated by that criterion. When alternatives (in a decision matrix) all have the same performance for a criterion, we say the criterion is unimportant. It can be dropped from the analysis because it is not transmitting distinct and differentiating information. The more distinct and differentiated the performance of competing alternatives on a criterion, the greater the amount of decision information contained and transmitted by that criterion; hence, the greater its importance weight.

In decision science, entropy is used to derive objective measures of the relative importance of each criterion (i.e., its weight) as it influences the performance of competing alternatives. If desired, prior subjective weights can be folded into objectively-derived entropy weights. The following steps present the equations for computing entropy-derived objective weights used to derive the “most-preferred” alternative in a decision matrix.

**Step 1:** From the decision matrix in Table 14, compute  $p_{ij}$  where

$$p_{ij} = \frac{x_{ij}}{\sum_{i=1}^m x_{ij}} \quad i = 1, \dots, m; j = 1, \dots, n \quad (6.9)$$

**Step 2:** Compute the entropy of attribute (criterion)  $j$  as follows:

$$0 \leq E_j = -\frac{1}{\ln(m)} \sum_{i=1}^m p_{ij} \ln p_{ij} \leq 1 \quad i = 1, \dots, m; j = 1, \dots, n \quad (6.10)$$

**Step 3:** Compute the degree of diversification  $d_j$  of the information transmitted by attribute (criterion)  $j$  according to  $d_j = 1 - E_j$ .

**Step 4:** Compute the entropy-derived weight  $w_j$  as follows:

$$w_j = \frac{d_j}{\sum_{j=1}^n d_j} \quad j = 1, \dots, n \quad (6.11)$$

If the decision-maker has prior subjective importance weights  $\lambda_j$  for each attribute (criterion), then this can be adapted into  $w_j$  as follows:

$$w_j^* = \frac{\lambda_j w_j}{\sum_{j=1}^n \lambda_j w_j} \quad j = 1, \dots, n \quad (6.12)$$

In Step 2, observe that entropy weighting involves the use of the natural logarithm. Thus, weights derived from this approach require all elements in the decision matrix be strictly greater than zero; otherwise, for some  $ij$  the term  $p_{ij} \ln p_{ij}$  in the expression (see Equation 6.10)

$$0 \leq E_j = -\frac{1}{\ln(m)} \sum_{i=1}^m p_{ij} \ln p_{ij} \leq 1 \quad i = 1, \dots, m; j = 1, \dots, n$$

takes the indeterminate form  $0 \cdot \infty$ . In mathematics, this is one of seven indeterminate forms involving 0, 1, and  $\infty$  whose overall limit is unknown. Table 15 shows a decision matrix where this condition will arise, where suppose a true zero exists as indicated by the arrow.

| Capability Node | C-Node Risk Score | C-Node Risk Mitigation Dollars |
|-----------------|-------------------|--------------------------------|
| C-Node 1        | 96.3              | 5.5                            |
| C-Node 2        | 54.7              | 7.8                            |
| C-Node 3        | 45.3              | 12.3                           |
| C-Node 4        | 77.8              | 0 ←                            |
| C-Node 5        | 21.3              | 11.2                           |
| C-Node 6        | 66.9              | 9.3                            |
| C-Node 7        | 90.0              | 2.5                            |

Table 15. A Decision Matrix That Yields an Undefined Entropy Weight

However, it can be shown if  $p \rightarrow 0$  (in the limit) then the expression  $p \ln p$  approaches zero; hence, entropy calculations often use the convention  $0 \cdot \ln 0 = 0$ .

An alternative to objective weighting by the entropy measure is the variance-to-mean ratio (VMR). Like entropy, the variance-to-mean ratio is a measure of the uncertainty or dispersion of a distribution. Distributions characterized by data with VMRs less than one are considered less random (more uniform) than those with VMRs greater than one. A probability distribution's VMR is often compared to the VMR of a Poisson distribution, whose VMR is exactly one. If alternatives in a decision matrix all have the same performance on a criterion, then the criterion's VMR is zero. Thus, the criterion can be dropped from the analysis because it is not transmitting distinct and differentiating information. Recall this is also a property of the entropy measure.

Deriving objective weights for criteria by the VMR statistic\* is done as follows:

$$w_j = \frac{\sigma_j^2 / \mu_j}{\sum_{j=1}^n \sigma_j^2 / \mu_j} \quad \mu_j \neq 0, j = 1, \dots, n \quad (6.13)$$

If a decision-maker has prior subjective importance weights  $\lambda_j$  for each criterion, then this can be adapted into  $w_j$  by  $w_j^*$  in the same way shown in Step 4 of the entropy weighting method.

\* Note the VMR statistic requires the mean of a dataset be nonzero.



## ILLUSTRATION

This section illustrates how the TOPSIS algorithm can be used to prioritize risk management decisions. Suppose we have the following information in Table 16.

| Capability Node | C-Node Risk Score | C-Node FDNA | C-Node Risk Mitigation Dollars | C-Node Risk Reduction Benefit | C-Node Criticality Level |
|-----------------|-------------------|-------------|--------------------------------|-------------------------------|--------------------------|
| C-Node 1        | 96.3              | 5.0         | 5.5                            | 85.0                          | 3.0                      |
| C-Node 2        | 54.7              | 2.1         | 7.8                            | 44.0                          | 4.0                      |
| C-Node 3        | 45.3              | 3.2         | 12.3                           | 78.0                          | 3.0                      |
| C-Node 4        | 77.8              | 4.1         | 8.5                            | 45.0                          | 2.0                      |
| C-Node 5        | 21.3              | 0.1         | 11.2                           | 56.0                          | 1.0                      |
| C-Node 6        | 66.9              | 5.3         | 9.3                            | 76.0                          | 2.0                      |
| C-Node 7        | 90.0              | 3.3         | 2.5                            | 25.0                          | 5.0                      |

Table 16. Capability Node Risk Management Decision Matrix

Table 16 presents characteristics on seven capability nodes (C-Nodes) across five criteria. These are *C-Node Risk Score*, *C-Node FDNA*, *C-Node Risk Mitigation Dollars*, *C-Node Risk Reduction Benefit*, and *C-Node Criticality Level*. They are defined as follows:

### ***C-Node Risk Score***

A value between zero and one-hundred that quantifies the C-Node's risk. The data for this criterion derives from the risk score equations, measures, and risk inheritance considerations developed throughout Chapter III and Chapter IV.

### ***C-Node FDNA***

The quantified effect on a C-Node's operability if, due to the realization of risks, one or more contributing programs or supplier-provider chains degrade, fail, or are eliminated. The data for this criterion are expressed as a percentage below the minimum effective operational level (MEOL) defined in Chapter V.

### ***C-Node Risk Mitigation Dollars***

The dollars (in millions) estimated to mitigate a C-Node's risks.

### ***C-Node Risk Reduction Benefit***

A C-Node's risk reduction benefit expected from expending its risk mitigation dollars. Here, benefit is expressed as the percent reduction in the C-Node's risk score.

### ***C-Node Criticality Level***

This criterion represents a C-Node's mission criticality with respect to the outcome objectives of the portfolio. The levels range from one (least critical) to five (most criticality). For convenience, assume these levels reflect numbers defined along a cardinal interval scale.

Given the above, suppose the management question is: *What is the most favorable ordering of C-Nodes in Table 16 that maximally reduces capability risk and minimizes the expense of risk mitigation dollars?* The TOPSIS algorithm can be applied to address this question. The algorithm's computational steps and results are shown and summarized in Table 17.

| Capability Node Risk Management Prioritization |                   |             |                                |                               |                          |
|--|-------------------|-------------|--------------------------------|-------------------------------|--------------------------|
| Capability Node                                | C-Node Risk Score | C-Node FDNA | C-Node Risk Mitigation Dollars | C-Node Risk Reduction Benefit | C-Node Criticality Level |
| C-Node 1                                       | 96.3              | 5.0         | 5.5                            | 85.0                          | 3.0                      |
| C-Node 2                                       | 54.7              | 2.1         | 7.8                            | 44.0                          | 4.0                      |
| C-Node 3                                       | 45.3              | 3.2         | 12.3                           | 78.0                          | 3.0                      |
| C-Node 4                                       | 77.8              | 4.1         | 8.5                            | 45.0                          | 2.0                      |
| C-Node 5                                       | 21.3              | 0.1         | 11.2                           | 56.0                          | 1.0                      |
| C-Node 6                                       | 66.9              | 5.3         | 9.3                            | 76.0                          | 2.0                      |
| C-Node 7                                       | 90.0              | 3.3         | 2.5                            | 25.0                          | 5.0                      |
| Sum  | 452.29            | 23.10       | 57.10                          | 409.00                        | 20.00                    |
| Root Sum of Squares                            | 182.742           | 9.770       | 23.083                         | 163.728                       | 8.246                    |
| Normalized Matrix                              | C-Node Risk Score | C-Node FDNA | C-Node Risk Mitigation Dollars | C-Node Risk Reduction Benefit | C-Node Criticality Level |
| C-Node 1                                       | 0.5272            | 0.5118      | 0.2383                         | 0.5192                        | 0.3638                   |
| C-Node 2                                       | 0.2992            | 0.2149      | 0.3379                         | 0.2687                        | 0.4851                   |
| C-Node 3                                       | 0.2480            | 0.3275      | 0.5329                         | 0.4764                        | 0.3638                   |
| C-Node 4                                       | 0.4256            | 0.4197      | 0.3682                         | 0.2748                        | 0.2425                   |
| C-Node 5                                       | 0.1168            | 0.0102      | 0.4852                         | 0.3420                        | 0.1213                   |
| C-Node 6                                       | 0.3660            | 0.5425      | 0.4029                         | 0.4642                        | 0.2425                   |
| C-Node 7                                       | 0.4922            | 0.3378      | 0.1083                         | 0.1527                        | 0.6063                   |
| Norm of Normalized Cols                        | 1.000             | 1.000       | 1.000                          | 1.000                         | 1.000                    |
| Entropy Matrix                                 | C-Node Risk Score | C-Node FDNA | C-Node Risk Mitigation Dollars | C-Node Risk Reduction Benefit | C-Node Criticality Level |
| C-Node 1                                       | 0.2130            | 0.2165      | 0.0963                         | 0.2078                        | 0.1500                   |
| C-Node 2                                       | 0.1209            | 0.0909      | 0.1366                         | 0.1076                        | 0.2000                   |
| C-Node 3                                       | 0.1002            | 0.1385      | 0.2154                         | 0.1907                        | 0.1500                   |
| C-Node 4                                       | 0.1720            | 0.1775      | 0.1489                         | 0.1100                        | 0.1000                   |
| C-Node 5                                       | 0.0472            | 0.0043      | 0.1961                         | 0.1369                        | 0.0500                   |
| C-Node 6                                       | 0.1479            | 0.2294      | 0.1629                         | 0.1858                        | 0.1000                   |
| C-Node 7                                       | 0.1989            | 0.1429      | 0.0438                         | 0.0611                        | 0.2500                   |
| Sum  | 1.000             | 1.000       | 1.000                          | 1.000                         | 1.000                    |
| Entropy Measure                                | 0.9589            | 0.9092      | 0.9577                         | 0.9666                        | 0.9496                   |
| Diversification Measure                        | 0.0411            | 0.0908      | 0.0423                         | 0.0334                        | 0.0504                   |
| Entropy Weights                                | 0.1592            | 0.3521      | 0.1640                         | 0.1294                        | 0.1953                   |
| Entropy Weight Sum Check                       | 1.0000            |             |                                |                               |                          |
| Entropy Weighted Normalized Matrix             | C-Node Risk Score | C-Node FDNA | C-Node Risk Mitigation Dollars | C-Node Risk Reduction Benefit | C-Node Criticality Level |
| C-Node 1                                       | 0.0839            | 0.1802      | 0.0391                         | 0.0672                        | 0.0711                   |
| C-Node 2                                       | 0.0476            | 0.0757      | 0.0554                         | 0.0348                        | 0.0947                   |
| C-Node 3                                       | 0.0395            | 0.1153      | 0.0874                         | 0.0616                        | 0.0711                   |
| C-Node 4                                       | 0.0678            | 0.1478      | 0.0604                         | 0.0356                        | 0.0474                   |
| C-Node 5                                       | 0.0186            | 0.0036      | 0.0796                         | 0.0442                        | 0.0237                   |
| C-Node 6                                       | 0.0583            | 0.1910      | 0.0661                         | 0.0600                        | 0.0474                   |
| C-Node 7                                       | 0.0784            | 0.1189      | 0.0178                         | 0.0198                        | 0.1184                   |

Table 17. A TOPSIS-Derived Capability Risk Prioritization

|   |                          |                    |                                       |                                      |                                 |                 |                 |
|---|--------------------------|--------------------|---------------------------------------|--------------------------------------|---------------------------------|-----------------|-----------------|
| <b>A*</b> Positive-Ideal Soln (Ideal Vector)            | <b>C-Node Risk Score</b> | <b>C-Node FDNA</b> | <b>C-Node Risk Mitigation Dollars</b> | <b>C-Node Risk Reduction Benefit</b> | <b>C-Node Criticality Level</b> |                 |                 |
|   | 0.0839                   | 0.1910             | 0.0178                                | 0.0672                               | 0.1184                          |                 |                 |
| <b>A<sup>-</sup></b> Negative-Ideal Soln (Nadir Vector) | 0.0186                   | 0.0036             | 0.0874                                | 0.0198                               | 0.0237                          |                 |                 |
| <b>S*</b> Euclidean Separation Distance                 | <b>C-Node 1</b>          | <b>C-Node 2</b>    | <b>C-Node 3</b>                       | <b>C-Node 4</b>                      | <b>C-Node 5</b>                 | <b>C-Node 6</b> | <b>C-Node 7</b> |
|   | 0.0531                   | 0.1328             | 0.1218                                | 0.1000                               | 0.2296                          | 0.0900          | 0.0865          |
| <b>S<sup>-</sup></b> Euclidean Separation Distance      | <b>C-Node 1</b>          | <b>C-Node 2</b>    | <b>C-Node 3</b>                       | <b>C-Node 4</b>                      | <b>C-Node 5</b>                 | <b>C-Node 6</b> | <b>C-Node 7</b> |
|   | 0.2056                   | 0.1111             | 0.1301                                | 0.1573                               | 0.0257                          | 0.1983          | 0.1752          |

|   |                 |                 |                 |                 |                 |                 |                 |
|---|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| <b>Ranking Result</b>                                     |                 |                 |                 |                 |                 |                 |                 |
| <b>Relative Closeness to Ideal Solution: TOPSIS Score</b> | <b>C-Node 1</b> | <b>C-Node 2</b> | <b>C-Node 3</b> | <b>C-Node 4</b> | <b>C-Node 5</b> | <b>C-Node 6</b> | <b>C-Node 7</b> |
|   | 0.7949          | 0.4554          | 0.5165          | 0.6114          | 0.1007          | 0.6880          | 0.6696          |

Table 17. A TOPSIS-Derived Risk Management Decision Prioritization

Table 17 shows the C-Node TOPSIS scores given the input data in Table 16. The C-Node with the largest TOPSIS score is most favorable with respect to the one that *maximally reduces capability risk and minimizes the expense of risk mitigation dollars*. The C-Node with the next largest TOPSIS score is the next most favorable, and so forth. Also, the criterion with the largest weight has the most influence on the overall C-Node ranking. The criterion with the next largest weight has the next most influence on the overall C-Node ranking, and so forth.

## CHAPTER VII

### SUMMARY

#### A UNIFYING RISK ANALYTIC FRAMEWORK AND PROCESS

The preceding chapters covered a great deal of ground. New risk analytic methods have been developed to address engineering an enterprise system from a capability portfolio perspective. The aim of this chapter is to describe how these methods relate and unify into a practical model for the analysis of risk in engineering today's enterprise systems.

#### A Traditional Process With Non-Traditional Methods

In general, managing risk in engineering systems can be characterized by the process shown in Figure 81 [Blanchard and Fabrycky, 1990; Bahnmaier, 2003]. Although this process grew from engineering traditional systems, its execution involves non-traditional methods, when applied to engineering an enterprise. Why is this?

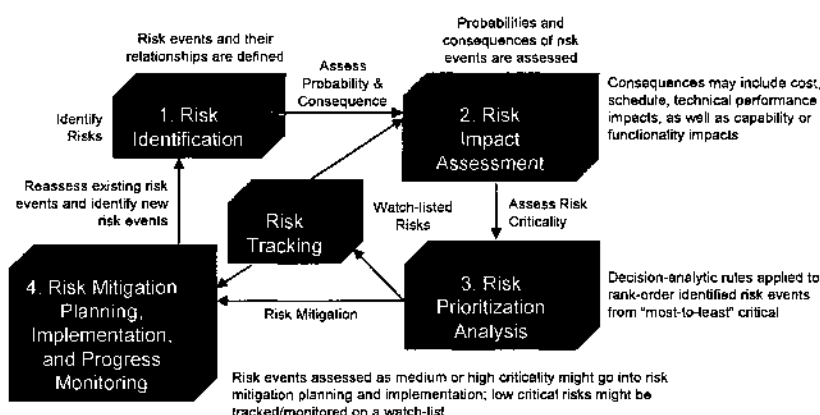


Figure 81. A Traditional Risk Management Process

As discussed earlier, today's information-age systems are more and more characterized by their *ubiquity* and lack of specification. Systems like the internet are unbounded, present everywhere, and in places simultaneously. They are an *enterprise* of systems and systems-of-systems. By the use of advanced network and communications technologies, these systems continuously operate to meet the demands of globally distributed and uncountable many users and communities.

Engineering enterprise systems is an emerging discipline that encompasses and extends "traditional" systems engineering to create and evolve "webs" of systems and systems of systems. They operate in a network-centric way to deliver capabilities via services, data, and applications through richly interconnected networks of information and communications technologies. More and more defense systems, transportation systems, and financial systems globally connect across

\* Traditional systems are generally regarded as systems characterized by well-defined requirements and technical specifications, predictable operational performance, adherence to engineering standards and manufacturing processes, and centralized management authority.

boundaries and seamlessly interface with users, information repositories, applications, and services. These systems are an enterprise of people, processes, technologies, and organizations.

As discussed in Chapters II and III, an enterprise system is often planned to deliver capabilities through portfolios of time-phased increments or evolutionary builds. Thus, risks can originate from many different sources (e.g., suppliers) and threaten enterprise capabilities at different points in time. Furthermore, these risks (and their sources) must align to the capabilities they potentially affect and the scope of their consequences understood. In addition, the extent enterprise risks may have unwanted collateral effects on other dependent capabilities must be captured and measured when planning where to allocate risk reducing investments.

From a high-level perspective, the process for analyzing and managing risk in engineering enterprise systems is similar to engineering traditional systems. Scale, ubiquity, and decentralized authority in engineering enterprise systems drive the need for non-traditional risk analytic methods within each of the traditional process steps in Figure 81.

Recognizing and researching these distinctions has produced the formal methods herein. They aim to enable a holistic understanding of risks in engineering enterprise systems, their potential consequences, dependencies, and rippling effects across the enterprise space. When implemented, these methods provide engineering management a complete view of risks across an enterprise, so capabilities and performance objectives can be achieved via risk-informed resource and investment decisions.

### **A Model Formulation for Measuring Risk in Engineering Enterprise Systems**

The following describes how the risk analytic methods in this dissertation form a practical model for the analysis of risk in engineering today's enterprise systems. We will relate this model formulation to the fundamental process steps shown in Figure 81.

#### **Step 1: Risk Identification**

In engineering a traditional system, risk identification is the critical first step of the risk management process. Its objective is the early and continuous identification of risks, to include those within and external to the engineering system project. As mentioned earlier, these risks are events that, if they occur, have negative impacts on the project's ability to achieve its outcome goals.

In engineering an enterprise system, risk identification needs to consider supplier risks. Supplier risks include unrealistic schedule demands placed on them by portfolio needs or placed by suppliers on their vendors. Supplier risks include premature use of technologies, including the deployment of technologies not adequately tested. Dependencies amongst suppliers can generate a host of risks, especially when a problem with one supplier generates a series of problems with others. Economic conditions can always threaten business stability or the business viability of suppliers and vendors. Unfavorable funding or political influences outside an enterprise can adversely affect its capability portfolios, its suppliers, or the supplier-vendor chains in ways that threaten the realization of enterprise goals and mission outcomes.

Risks that trace to “suppliers” are a major source of risk to the portfolio’s ability to deliver capability to the enterprise. However, it is important to recognize that suppliers are not the only source of risk. Risks that threaten capabilities to be delivered by a portfolio can originate from sources other than those that affect only the portfolio’s suppliers. These events can directly attack one or more capability nodes in a capability portfolio’s hierarchy. For example, uncertainties in geo-political landscapes may impact operational demands on capabilities that stress planned performance.

Risk identification also needs to consider dependencies. Dependencies between capability portfolios in families of portfolios, such as those that constitute an enterprise, are also potential risk sources. Here, outcome objectives for capabilities delivered by one capability portfolio may depend on the performance of capabilities delivered by another capability portfolio. Identifying risk events from non-supplier-related sources and capturing their contribution to a capability node’s risk measure is an important consideration in a capability portfolio’s risk assessment.

Figure 82 illustrates the risk analytic methods developed in this dissertation that relate to this process step. Methods from Chapters II and III are applicable at this stage. Here, the capability portfolio is defined and expressed as a mathematical graph. This graph is used as a modeling “framework” within which risks can be assessed and capability risk measures derived. In this step, effort is spent defining capability in measurable contexts (refer to guidance in Chapter II) and aligning capability suppliers as they enable the portfolio to deliver capability.

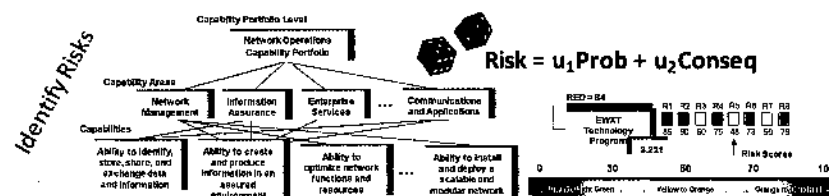


Figure 82. Risk Analytic Methods Related Risk Identification

## Step 2: Risk Impact (Consequence) Assessment

In engineering a traditional system, an assessment is made of the impact each risk event could have on the engineering system project. Typically, this includes how the event could impact cost, schedule, or technical performance objectives. An assessment is also made of the probability each risk event will occur. This often involves subjective probability assessments, particularly if circumstances preclude a direct evaluation of probability by objective methods.

In engineering an enterprise system, findings from Step 1 feed into mathematical constructs that generate capability risk measures across an enterprise. These measures are determined by the calculus created in Chapter III, where the enterprise problem space is represented by a supplier-provider metaphor in the form of a mathematical graph. This graph is a topology of nodes that depict supplier-provider-capability relationships unique to a capability portfolio.

Within this topology, mathematical rules have been developed that operate on these relationships to generate measures of capability risk. Here, a definition of capability risk is provided that

considers the occurrence probabilities and consequences of risks that threaten capability. In this context, consequence is broadened beyond cost, schedule, and technical performance dimensions; risk consequence is evaluated according to a capability's *ability to achieve its outcome objectives* for the portfolio and ultimately for the enterprise.

Next, dependencies and risk co-relationships that may exist in the enterprise are captured. Chapters IV and V provide formalisms for analyzing dependency relationships and their affects on engineering and planning an enterprise system. Critical considerations in engineering enterprise systems are identifying, representing, and measuring dependencies between suppliers of technologies and providers of services to consumers and users.

The importance of dependency analysis in engineering an enterprise is many-fold. A primary concern is enabling the study of ripple effects of failure in one capability on other dependent capabilities across the enterprise. Providing mechanisms to anticipate these effects early in design enables engineers to minimize dependency risks that, if realized, can have cascading negative effects on the ability of an enterprise to deliver services to users.

One dependency is risk inheritance; that is, *how risk-dependent are capabilities so threats to them can be discovered before contributing programs (e.g., suppliers) degrade, fail, or are eliminated?* Chapter IV provides a protocol, the Risk Co-Relationship (RCR) index, for capturing and measuring risk inheritance in an enterprise. The RCR index is a new management metric that measures risk inheritance between supplier programs and its ripple effects across a capability portfolio. The index identifies and captures horizontal and vertical impacts of risk inheritance, as it increases the threat that risks on one supplier program may adversely affect others and ultimately their contributions to their associated capabilities.

The other dependency is operational dependence; that is, *what is the effect on the operability of capability if one or more contributing program (e.g., suppliers) or supplier-provider chains degrade, fail, or are eliminated?* Chapter V presents an entirely new formalism, called Functional Dependency Network Analysis (FDNA), for capturing and measuring operational dependence in an enterprise.

Factoring dependency considerations into the protocols presented in this dissertation enables the proper management of enterprise risk; specifically, investment decisions on where to target risk reduction resources in ways that optimally reduce threats to capabilities posed by dependencies. Figure 83 illustrates the risk analytic methods developed in this dissertation that relate to this process step.

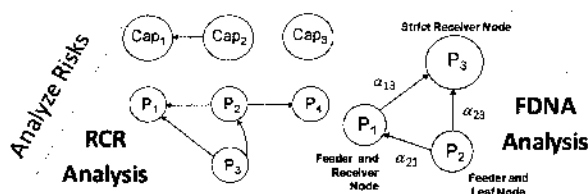


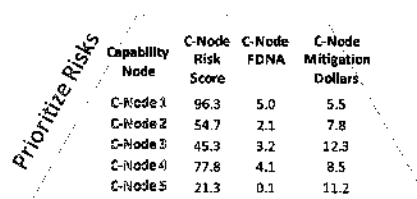
Figure 83. Risk Analytic Methods Related to Risk Impact Assessment

### Step 3: Risk Prioritization Analysis

At this step the overall set of identified risk events, their impact assessments, and their occurrence probabilities are “processed” to derive a ranking of the most- to least-critical risks. Decision analytic techniques such as utility theory, value function theory, or ordinal methods are formalisms often used to derive this ranking.

Findings from Steps 2 and 3 feed into ranking algorithms that identify an optimal ordering of enterprise capabilities to risk manage. In Chapter VI, a decision-theoretic approach for prioritizing risk management decisions as a function of the risk measures and analysis procedures developed in the previous chapters is provided. These measures are integrated into advanced ranking algorithms to isolate and prioritize which capabilities are most risk-threatened and qualify for deliberate management attention.

The outputs from these ranking algorithms enable decision-makers to target risk reduction resources in ways that optimally reduce threats posed by risks to critical capability outcome objectives. Figure 84 illustrates the risk analytic methods developed in this dissertation that relate to this process step.



| Capability Node | C-Node Risk Score | C-Node FDNA | C-Node Mitigation Dollars |
|-----------------|-------------------|-------------|---------------------------|
| C-Node1         | 96.3              | 5.0         | 5.5                       |
| C-Node2         | 54.7              | 2.1         | 7.8                       |
| C-Node3         | 45.3              | 3.2         | 12.3                      |
| C-Node4         | 77.8              | 4.1         | 8.5                       |
| C-Node5         | 21.3              | 0.1         | 11.2                      |

Figure 84. Risk Analytic Methods Related to Risk Prioritization Analysis

### Step 4: Risk Mitigation Planning and Progress Monitoring

This step involves the development of mitigation plans designed to manage, eliminate or reduce risk to an acceptable level. Once a plan is implemented, it is continually monitored to assess its efficacy with the intent to revise its courses-of-action if needed.

Step 4 results from the integration of all the risk analytic methods developed in Chapter II through Chapter VI. With this, decision-makers have a logical and rational basis for addressing the choice problem of selecting which capability risks to mitigate or reduce as a function of their criticality to the portfolio and to the enterprise as a whole. Figure 85 illustrates this step.



Figure 85. Risk Analytic Methods Related to Risk Mitigation Planning



In summary, these four process steps bring the research and solution approaches developed in this dissertation into a coherent structure for representing, modeling, and measuring risk in engineering large-scale, complex, systems designed to function in enterprise-wide environments.

With the completion of this research, the engineering management and systems engineering community has a generalized framework and computational model for the analysis of risk in engineering enterprise systems. This provides decision-makers formal ways to model and measure enterprise-wide risks, their potential multi-consequential impacts, dependencies, and their rippling effects within and beyond enterprise boundaries. Figure 86 visually summarizes the risk analytical framework and model formulation created by the research in this dissertation.

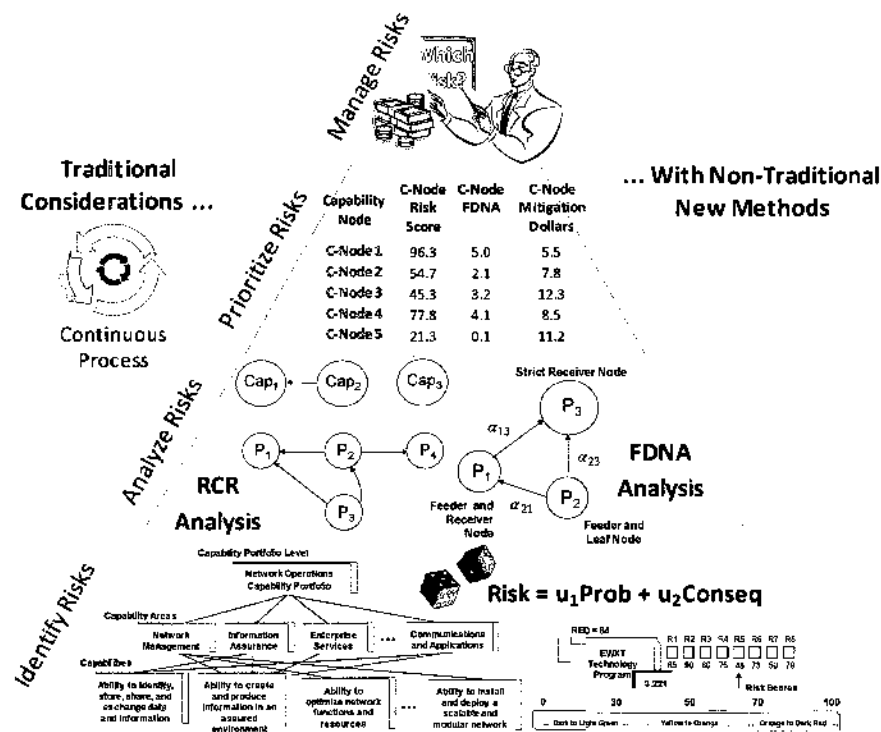


Figure 86. A Risk Analytical Framework and Model Formulation

Making operational the model shown in Figure 86 has unique and challenging information needs. These can be grouped into two categories. The first *addresses capability value*. The second *addresses supplier contributions, criticality, and risks* as they relate to enabling the portfolio to deliver capability.

Information needs to *address capability value* include the following:

- For each Tier 3 capability, shown in Figure 17, identify what performance standard (or outcome objective) each capability must meet by its scheduled delivery date.

- For each Tier 3 capability, identify the source basis for its performance standard (or outcome objective). Does it originate from user-driven needs, policy-driven needs, model-derived values, a combination of these, or from other sources?
- For each Tier 3 capability, identify to what extent the performance standard (or outcome objective) for one capability depends on others meeting their standards.

Information needs to *address supplier contributions, criticality, and risks* include the following:

- For each Tier 3 capability, identify which Technology Programs and Technology Initiatives are contributing to that capability.
- For each Tier 3 capability, identify what (specifically) are the contributions of its suppliers.
- For each Tier 3 capability, identify how supplier contributions enable the capability to achieve its performance standard (or outcome objective).
- For each Tier 3 capability, identify which Technology Programs and Technology Initiatives are critical contributors in enabling the capability to achieve its performance standard (or outcome objective).
- With the above, identify what risks originate from (or are associated with) suppliers that, if these events occur, negatively affect their contributions to capability.

Process tailoring, socialization, and establishing governance protocols are critical considerations in engineering risk management for enterprise systems. Overall, the risk analytic approaches in this dissertation provide the following:

- Identification of risk events that threaten the delivery of capabilities needed to advance goals and capability outcome objectives of the enterprise.
- A measure of risk for each capability derived as a function of each risk event's occurrence probability and its consequence.
- An analytical framework and logical model within which to structure capability portfolio risk assessments – one where assessments can be combined to measure and trace their integrative influence on engineering the enterprise.
- Through the framework, ways to model and measure risk as capabilities are time-phased across incremental capability development approaches.
- Analytic transparency, where the methods in this dissertation provide decision-makers the trace basis and the event drivers behind all risk measures derived for any node at any level of the capability portfolio's hierarchy. With this, capability portfolio management has visibility and supporting rationales for identifying where resources are best allocated to reduce (or eliminate) events that threaten achieving the enterprise's capability outcome objectives.

## SUMMARY AND AREAS FOR FUTURE RESEARCH

Managing risk in engineering today's complex systems is more sophisticated and challenging than ever before. Lack of clearly defined boundaries, diminished hierarchical control, network-centric information exchange, and ubiquitous services are significant technical and managerial challenges faced in engineering enterprise systems. Increased complexity contributes to increased risks of system and management failures – particularly in systems designed to employ advanced, network-centric, information technologies [Daniels, LaMarsh, 2007].

Few, if any, protocols exist for assessing and measuring risk in engineering enterprise systems from a capability portfolio perspective. Addressing this problem has been the aim and the objective of this research. The risk analytic methods herein provide a foundation from which to address a next set of hard problems. Areas for future research include the following:

- **Analytical Scalability:** Research how to approach risk analysis in engineering enterprise systems that consist of dozens of capability portfolios with hundreds of supplier programs.

Explore representing large-scale enterprises by domain capability portfolio clusters and investigate a concept for portfolio cluster risk management – include a social science perspective on the management of risk in engineering enterprise systems at this scale.

Explore the efficacies of alternative protocols for assessing and measuring risks from the supplier through the provider layers of a capability portfolio. Quality Function Deployment (QFD) or Balanced Scorecard (BSC) are protocols to consider, particularly for questions concerning the analytical scalability of the roll-up rules created herein.

- **Nonstationary Considerations:** Extend the FDNA calculus to address nonstationary dependency analysis problems. Explore how FDNA can expand and integrate into time-varying modeling and simulation environments, such as those provided in systems dynamics methods and tools.

- **Optimal Adaptive Strategies:** Research how to optimally adapt an engineering system's supplier-provider network to reconfigure its nodes to maintain operability if risks that threaten these nodes are realized. Consider this problem in stationary and nonstationary perspectives.

The research in this dissertation falls at the interface between risk management methods for engineering traditional systems with those needed for engineering enterprise systems. Recognizing this is an essential first step towards addressing these challenges and discovering new methods and new practices in engineering risk management and its related disciplines.

N. W. Dougherty\*, once said *"the ideal engineer is a composite... he is not a scientist, he is not a mathematician, he is not a sociologist or a writer; but he may use the knowledge and techniques of any or all of these disciplines in solving engineering problems"*. That was true then and is truer still in engineering today's sophisticated, complex, and highly networked enterprise systems.

---

\* President, 1954-1955, American Society for Engineering Education (ASEE).

## REFERENCES

- Allen, T., Nightingale, D., Murman, E., March 2004. "Engineering Systems an Enterprise Perspective", An Engineering Systems Monograph, Engineering Systems Division, The Massachusetts Institute of Technology.
- Arrow, K. J., 1965. "Aspects of the Theory of Risk Bearing", Yrjo Jahnsson Lectures, Helsinki, Finland: Yrjo Jahnssonin Saatio.
- Ayyub, B. M., 2001. *Elicitation of Expert Opinions for Uncertainty and Risks*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York.
- Ayyub, B. M., McGill, W. L., Kaminsky, M., 2007. "Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework", *Risk Analysis*, Vol. 27, No. 4.
- Bahnmaier, W. W., editor, 2003. *Risk Management Guide for DOD Acquisition*, 5th Edition, Version 2.0, Department of Defense Acquisition University Press, Fort Belvoir, Virginia, 22060-5565.
- Bernoulli, D., 1738. "Exposition of a New Theory on the Measurement of Risk", *Econometrica*, Vol. 22, No. 1 (Jan., 1954), pp. 23-36 Virginia, 22060-5565, The Econometric Society, [www.jstor.org/stable/1909829](http://www.jstor.org/stable/1909829).
- Blanchard, B. S., Fabrycky W. J., 1990. *Systems Engineering and Analysis*, 2nd ed. Englewood Cliffs, New Jersey, Prentice-Hall, Inc.
- Browning, T. R., Deyst, J. J., Eppinger, S. D., 2002. "Adding Value in Product Development by Creating Information and Reducing Risk", *IEEE Transactions on Engineering Management*, Vol. 49, No. 4.
- Chytka, T., Conway, B., Keating, C., Unal, R., 2004. "Development of an Expert Judgment Elicitation And Calibration Methodology for Risk Analysis in Conceptual Vehicle Design", Old Dominion University Project Number: 130012, NASA Grant NCC-1-02044, NASA Langley Research Center, Hampton, Virginia 23681.
- Clemen, R. T., 1996. *Making Hard Decisions An Introduction to Decision Analysis*, 2nd edition, Pacific Grove, California, Brooks/Cole Publishing Company.
- Cox, L. A., Babayev, D., Huber, W., 2005. "Some Limitations of Qualitative Risk Rating Systems" *Risk Analysis*, Vol. 25, No. 3.
- Cox, L. A., 2009. "Improving Risk-Based Decision Making for Terrorism Applications", *Risk Analysis*, Vol. 29, No. 3.
- Creswell, J. W., 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2nd ed.), Sage University Press, Thousand Oaks, California.
- Crowther, K. G., Haimes, Y. Y., Taub, G., 2007. "Systemic Valuation of Strategic Preparedness Through Application of the Inoperability Input-Output Model with Lessons Learned from Hurricane Katrina", *Risk Analysis*, Vol. 27, No. 5.
- Daniels, C. B. and LaMarsh, W. J., 2007. "Complexity as a Cause of Failure in Information Technology Project Management", *Proceedings of IEEE International Conference on System of Systems Engineering*, April, pp.1-7.
- de Finetti, B., 1974. *Theory of Probability*, Vol. 1., John Wiley & Sons, New York, NY.

- de Finetti, B (author), A. Mura, A. (editor), 2008. *Philosophical Lectures on Probability*: Springer-Science + Business Media B. V.
- Dyer, J. S., Sarin, R. K., 1979. "Measurable Multiattribute Value Functions", *Operations Research*, Vol. 27, No. 4, July-August.
- Edwards, J. E., Scott, J. C., Nambury, R. S., 2003. *The Human Resources Program-Evaluation Handbook*, Sage University Press, Thousand Oaks, California.
- Edwards, W., 1954. "The Theory of Decision Making", *Psychological Bulletin*, 41, 380-417.
- Edwards, W., 1961. "Behavioral Decision Theory", *Annual Review of Psychology*, 12, 473-498.
- Fishburn, P. C., "Foundations of Decision Analysis: Along the Way", *Management Science*, Vol. 35, No. 4, April 1989.
- GAO: Government Accountability Office, July 2004. "Defense Acquisitions: The Global Information Grid and Challenges Facing its Implementation", GAO-04-858.
- Garvey, P. R., Cho, C. C., Giallombardo, R., 1997. "RiskNav: A Decision Aid for Prioritizing, Displaying, and Tracking Program Risk", *Military Operations Research*, V3, N2.
- Garvey, P. R., 1999. "Risk Management", *Encyclopedia of Electrical and Electronics Engineering*, John Wiley & Sons, New York, NY.
- Garvey, P. R., 2000. *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), London, Boca Raton, New York; ISBN 0824789660.
- Garvey, P. R., 2001. "Implementing a Risk Management Process for a Large Scale Information System Upgrade – A Case Study", *INSIGHT*, Vol. 4, Issue 1, International Council on Systems Engineering (INCOSE).
- Garvey, P. R., Cho, C. C., 2003. "An Index to Measure a System's Performance Risk", *The Acquisition Review Quarterly (ARQ)*, Vol. 10, No. 2.
- Garvey, P. R., Cho, C. C., 2005. "An Index to Measure and Monitor a System of Systems' Performance Risk", *The Acquisition Review Journal (ARJ)*.
- Garvey, P. R., 2005. "System of systems Risk Management Perspectives on Emerging Process and Practice", The MITRE Corporation, MP 04B0000054.
- Garvey, P. R., 2008. *Analytical Methods for Risk Management: A Systems Engineering Perspective*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), London, Boca Raton, New York; ISBN 1584886374.
- Gelinas, N., 2007. "Lessons of Boston's Big Dig", *City Journal*.
- Gharajedaghi, J., 1999. *Systems Thinking Managing Chaos and Complexity – A Platform for Designing Business Architecture*, Woburn, Massachusetts, Butterworth-Heinemann.
- Haimes, Y. Y., 2004. *Risk Modeling, Assessment, and Management*, 2nd ed., John Wiley & Sons, New York, NY.
- Hansson, S. O., "Risk", *The Stanford Encyclopedia of Philosophy* (Winter 2008 Edition), Edward N. Zalta (ed.), URL = <<http://plato.stanford.edu/archives/win2008/entries/risk/>>.

- Hofstetter, P., Bare, J. C., Hammitt, J. K., Murphy, P. A., Rice, G. E., 2002. "Tools for Comparative Analysis of Alternatives: Competing or Complementary Perspectives?" *Risk Analysis*, Vol. 22, No. 5.
- Hwang, Ching-Lai, Yoon, K. Paul, 1995. *Multiple Attribute Decision Making: An Introduction*, Sage University Paper Series in Quantitative Applications in the Social Sciences, 07-104, Thousand Oaks, California, copyright 1995, by Sage.
- Jackson, M. C., 1991. *Systems Methodology for the Management Sciences*, New York: Plenum.
- Jaynes, E. T., 1988. "Probability Theory as Logic", Ninth Annual Workshop on Maximum Entropy and Bayesian Methods, Dartmouth College, New Hampshire, August 14, 1989. In the Proceedings Volume, *Maximum Entropy and Bayesian Methods*, Paul F. Fougere, Editor, Kluwer Academic Publishers, Dordrecht, Holland (1990).
- Jiang, P., Haimes, Y. Y., 2004. "Risk Management for Leontief-Based Interdependent Systems", *Risk Analysis*, Vol. 24, No. 5.
- Kaplan, S., Garrick, B., 1981. "On the Quantitative Definition of Risk", *Risk Analysis*, Vol. 1, No. 1, pp.11-27.
- Kaplan, S., 1997. "The Words of Risk Analysis", *Risk Analysis*, Vol. 4, No. 17.
- Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., Peterson, W., Rabadi, G., 2003. "System of Systems Engineering", *Engineering Management Journal*, Vol. 15, No. 3.
- Keating, C. B., Sousa-Poza, A., Mun, Ji Hyon, 2004. "System of Systems Engineering Methodology", Department of Engineering Management and Systems Engineering, Old Dominion University, ©2004, All rights reserved.
- Keating, C., Sousa-Poza, A., Kovacic, S., 2008. "System of Systems Engineering: An Emerging Multidiscipline", *Int. J. System of Systems Engineering*, Vol. 1, Nos. 1/2, pp. 1-17.
- Keeney, R. L., Raiffa, H., 1976. *Decisions with Multiple Objectives Preferences and Value Tradeoffs*, John Wiley & Sons, New York, NY.
- Keeney, R. L., 1992. *Value-Focused Thinking A Path to Creative Decision Making*, Harvard University Press, Cambridge, Massachusetts.
- Kirkwood, C. W., 1997. *Strategic Decision Making: Multiobjective Decision Analysis With Spreadsheets*, California, Duxbury Press.
- Krantz, D. H., Luce, R. D., Suppes, P., Tversky, A., 1971. *Foundations of Measurement, Additive and Polynomial Representations*, Volume 1., New York, Academic Press, Dover Publications.
- Leontief, W. W., 1966. *Input-Output Economics*, Oxford University Press, New York, NY.
- Lian, C., Santos, J. R., Haimes, Y. Y., 2007. "Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors", *Risk Analysis*, Vol. 27, No. 4.
- Malczewski, J., 1999. *GIS and Multicriteria Decision Analysis*, John Wiley & Sons, New York, NY.
- Mariampolski, H., 2001. *Qualitative Market Research: A Comprehensive Guide*, Sage University Press, Thousand Oaks, California.

Massachusetts Turnpike Authority (MTA), *Big Dig*, retrieved from <http://www.massturnpike.com/bigdig/background/facts.html>.

MITRE: 2007. "Evolving Systems Engineering", © 2007, The MITRE Corporation, All Rights Reserved, Distribution Unlimited, Case Number 07-1112.

Moynihan, R. A., Reining, R. C., Salamone, P. P., Schmidt, B. K., 2008. "Enterprise Scale Portfolio Analysis at the National Oceanic and Atmospheric Administration (NOAA)", *Systems Engineering*, International Council on Systems Engineering (INCOSE), 11 September 2008, © 2008 Wiley Periodicals, Inc.; [www3.interscience.wiley.com/journal/121403613/references](http://www3.interscience.wiley.com/journal/121403613/references).

Murphy, C., Gardoni, P., 2006. "The Role of Society in Engineering Risk Analysis: A Capabilities-Based Approach", *Risk Analysis*, Vol. 26, No. 4.

Nau, R. F., 2002. "de Finetti Was Right: Probability Does Not Exist", *Theory and Decision* 51: 89-124, 2001, ©2002, Kluwer Academic Publishers.

National Transportation Safety Board, 2007. Public Meeting, 10 July 2007; "Highway Accident Report: Ceiling Collapse in the Interstate 90 Connector Tunnel", Boston, Massachusetts, NTSB/HAR-07/02.

Office of the Secretary of Defense (OSD), 2005: *Net-Centric Operational Environment Joint Integrating Concept*, Version 1.0, Joint Chiefs of Staff, 31 October 2005, Joint Staff, Washington, D.C. 20318-6000; [www.dod.mil/cio-nii/docs/netcentric\\_jic.pdf](http://www.dod.mil/cio-nii/docs/netcentric_jic.pdf).

Pinto, C. A., Arora, A., Hall, D., Ramsey, D., Telang, R., 2004. "Measuring the Risk-Based Value of IT Security Solutions", *IEEE IT Professional*, v.6 no.6, pp. 35-42.

Pinto, C. A., Arora, A., Hall, D., Schmitz, E., 2006. "Challenges to Sustainable Risk Management: Case Example in Information Network Security", *Engineering Management Journal*, v.18, no.1, pp. 17-23.

Pratt, J. W., 1965. "Risk Aversion in the Small and in the Large", *Econometrica*, Vol. 32.

Ramsey, F. P. (author), Mellor, D. H. (editor), 1990. "F. P. Ramsey: Philosophical Papers", Cambridge University Press.

Rebovich, G., Jr., 2007. "Engineering the Enterprise", The MITRE Corporation; [www.mitre.org/work/tech\\_papers/tech\\_papers\\_07/07\\_0434/07\\_0434.pdf](http://www.mitre.org/work/tech_papers/tech_papers_07/07_0434/07_0434.pdf).

Rebovich, G., Jr., 2005. "Enterprise Systems Engineering Theory and Practice, Volume 2, Systems Thinking for the Enterprise New and Emerging Perspectives", The MITRE Corporation; [www.mitre.org/work/tech\\_papers/tech\\_papers\\_06/05\\_1483/05\\_1483.pdf](http://www.mitre.org/work/tech_papers/tech_papers_06/05_1483/05_1483.pdf).

Reilly, J., Brown, J., 2004. "Management and Control of Cost and Risk for Tunneling and Infrastructure Projects", *Proc. International Tunneling Conference*, Singapore.

Rescher, N., 2006. *Philosophical Dialectics: An Essay on Metaphilosophy*, SUNY Press, Albany, New York.

Rittel, H., 1972. "On the Planning Crisis: Systems Analysis of the First and Second Generations" The Institute of Urban and Regional Development, Reprint No. 107, University of California, Berkeley.

- Santos, J. R., Haimes, Y. Y., 2004. "Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures", *Risk Analysis*, Vol. 24, No. 6.
- Santos, J. R., Haimes, Y. Y., Lian, C., 2007. "A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies", *Risk Analysis*, Vol. 27, No. 5.
- Savage, L. J., 1954. *The Foundations of Statistics*, John Wiley & Sons, New York, NY.
- Shanteau, J., Weiss, D. J., Thomas, R., Pounds, J., 2001. "Performance-based Assessment of Expertise: How to Decide if Someone is an Expert or Not", *European Journal of Operations Research*, 136, 253-263.
- Stevens, S. S., 1946. "On the Theory of Scales of Measurement" *Science*, vol. 103, pp. 677-680.
- von Bertalanffy, L., 1968. *General Systems Theory, Foundations, Development, Applications*, University of Alberta, Edmonton, Canada, published by George Braziller, One Park Avenue, New York, New York, 10016.
- von Neumann J., Morgenstern O., 1944. *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, New Jersey 08540.
- von Winterfeldt D., and Edwards, W., 1986. *Decision Analysis and Behavioral Research*, Cambridge University Press, Cambridge, United Kingdom.
- White, B. E., 2006. "Fostering Intra-Organizational Communication of Enterprise Systems Engineering Practices", The MITRE Corporation, National Defense Industrial Association (NDIA), 9th Annual Systems Engineering Conference, October 23-26, 2006, Hyatt Regency Islandia, San Diego California.



## APPENDIX A

### TOPSIS ALGORITHM: CLASSICAL FORMULATION

#### INTRODUCTION

This appendix introduces a geometric approach that can be used to rank risk events on the basis of their performance across multiple evaluation criteria. This approach has a number of uniquely desirable features and it can be used in conjunction with value function approaches described in Chapter III.

#### Technique for Order Preference by Similarity to Ideal Solution

The geometric approach introduced in this appendix is known as TOPSIS [Hwang, Yoon, 1995]. The acronym stands for *Technique for Order Preference by Similarity to Ideal Solution*. TOPSIS is known in the decision sciences literature as an ideal point multiple criteria decision analysis method. It generates indices that order a set of competing alternatives from most-to least-preferred (or desirable) as a function of multiple criteria.

The ideal point represents a hypothetical alternative that consists of the most desirable weighted normalized levels of each criterion across the set of competing alternatives. The alternative closest to the ideal point performs best in the set. Separation from the ideal point is measured geometrically by a Euclidean distance metric. This is illustrated in Figure 87\*.

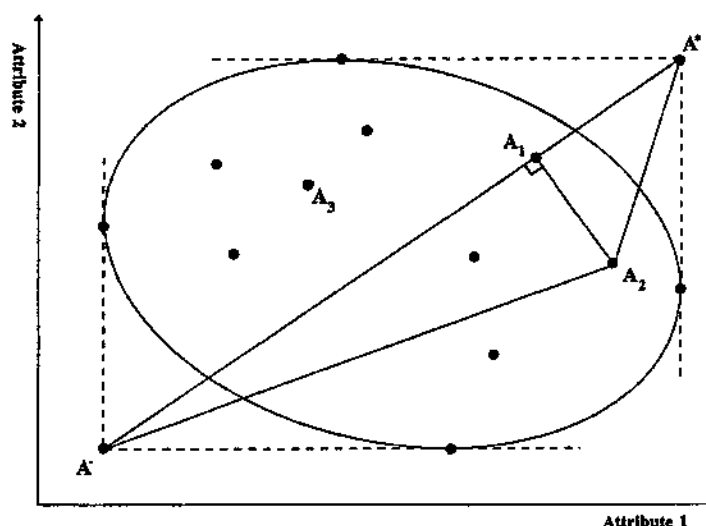


Figure 87. Euclidean Distances to Positive and Negative Ideal Solutions

\* Reprinted by permission of Sage Publications, Inc. [Hwang, Yoon, 1995].

Figure 87 shows two alternatives  $A_1$  and  $A_2$  in relation to two benefit criteria or attributes (Attribute 1 and Attribute 2). Here,  $A_1$  is closest to the ideal solution  $A^*$ , but  $A_2$  is farthest from the negative ideal solution  $A^-$ . So, which one do you choose?

TOPSIS is an ideal point method that ensures the chosen alternative is simultaneously closest to the ideal solution and farthest from the negative ideal solution. TOPSIS chooses the alternative whose performance across all criteria maximally matches those that comprise the ideal solution.

TOPSIS assumes each attribute (or criterion) can be characterized by either monotonically increasing or decreasing utility. Here, we seek to maximize attributes that offer a benefit and minimize those that incur a cost. TOPSIS generates an index that rank-orders competing alternatives, from most-to least-desired, on the relative distance of each to the ideal.

### Objective Weighting: The Entropy Method

Table 18 presents a generalized decision or performance matrix of alternatives. Here, the performance of an alternative is evaluated across competing criteria. The attractiveness of an alternative to a decision-maker is a function of the performance of each alternative across these criteria.

| Decision<br>Alternative | Criteria & Weights |                |                |     |                |
|-------------------------|--------------------|----------------|----------------|-----|----------------|
|                         | $C_1$<br>$w_1$     | $C_2$<br>$w_2$ | $C_3$<br>$w_3$ | ... | $C_n$<br>$w_n$ |
| $A_1$                   | $x_{11}$           | $x_{12}$       | $x_{13}$       | ... | $x_{1n}$       |
| $A_2$                   | $x_{21}$           | $x_{22}$       | $x_{23}$       | ... | $x_{2n}$       |
| $A_3$                   | $x_{31}$           | $x_{32}$       | $x_{33}$       | ... | $x_{3n}$       |
| ...                     | ...                | ...            | ...            | ... | ...            |
| $A_m$                   | $x_{m1}$           | $x_{m2}$       | $x_{m3}$       | ... | $x_{mn}$       |

**A Decision Matrix**

Table 18. A Traditional Decision or Performance Matrix of Alternatives

*Entropy*<sup>\*</sup> is a concept found in information theory that measures the uncertainty associated with the expected information content of a message. It is also used in decision science to measure the amount of decision information contained and transmitted by a criterion.

The amount of decision information contained and transmitted by a criterion is driven by the extent the performance (i.e., “score”) of each alternative is distinct and differentiated by that criterion. When alternatives all have the same performance for a criterion, we say the criterion is unimportant. It can be dropped from the analysis because it is not transmitting distinct and differentiating information. The more distinct and differentiated the performance of competing alternatives on a criterion, the greater the amount of decision information contained and transmitted by that criterion; hence, the greater its importance weight.

<sup>\*</sup> Entropy measures the uncertainty associated with the expected information content of a message [Shannon, Claude, E., 1948. *A Mathematical Theory of Communication*; [http://en.wikipedia.org/wiki/Claude\\_Elwood\\_Shannon](http://en.wikipedia.org/wiki/Claude_Elwood_Shannon), Bell System Technical Journal, 1948].

In decision science, entropy is used to derive objective measures of the relative importance of each criterion (i.e., its weight) as it influences the performance of competing alternatives. If desired, prior subjective weights can be folded into objectively-derived entropy weights. This is discussed later.

### Equations for the TOPSIS Method

Applying TOPSIS consists of the following steps and equations.

**Step 1.** Normalize the values in the decision matrix of alternatives (Table 18). One way to do this is to compute  $r_{ij}$  where

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^m x_{ij}^2}} \quad i = 1, \dots, m; \quad j = 1, \dots, n$$

**Step 2.** From step 1, compute weighted normalized values. This can be done by computing  $v_{ij}$ , where

$$v_{ij} = w_j r_{ij} \quad i = 1, \dots, m; \quad j = 1, \dots, n$$

and  $w_j$  is the weight of the  $j$ -th attribute (criterion). In this step,  $w_j$  could be replaced by the *entropy weight*, which is discussed next.

**Step 3.** Derive the positive  $A^*$  and the negative  $A^-$  ideal solutions, where

$$A^* = \{v_1^*, v_2^*, \dots, v_j^*, \dots, v_n^*\} = \{(\max_i v_{ij} \mid j \in J_1), (\min_i v_{ij} \mid j \in J_2) \mid i = 1, \dots, m\}$$

$$A^- = \{v_1^-, v_2^-, \dots, v_j^-, \dots, v_n^-\} = \{(\min_i v_{ij} \mid j \in J_1), (\max_i v_{ij} \mid j \in J_2) \mid i = 1, \dots, m\}$$

where  $J_1$  is the set of benefit attributes and  $J_2$  is the set of cost attributes.

**Step 4.** Calculate separation measures between alternatives, as defined by the  $n$ -dimensional Euclidean distance metric.

The separation from the positive-ideal solution  $A^*$  is given by

$$S_i^* = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^*)^2} \quad i = 1, \dots, m$$

The separation from the negative-ideal solution  $A^-$  is given by

$$S_i^- = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^-)^2} \quad i = 1, \dots, m$$

**Step 5.** Calculate similarities to positive-ideal solution, as follows:

$$0 \leq C_i^* = \frac{S_i^-}{(S_i^* + S_i^-)} \leq 1 \quad i = 1, \dots, m$$

**Step 6.** Choose the alternative in the decision matrix with the maximum  $C_i^*$  or rank these alternatives from most-to least-preferred according to  $C_i^*$  in descending order. The closer  $C_i^*$  is to unity the closer it is to the positive-ideal solution. The farther  $C_i^*$  is from unity the farther it is from the positive-ideal solution.

### Equations for the Entropy Weighting Method

The following steps present the equations for computing entropy-derived objective weights used to derive the “most-preferred” alternative in a decision matrix.

**Step 1.** From the decision matrix in Table 18, compute  $p_{ij}$  where

$$p_{ij} = \frac{x_{ij}}{\sum_{i=1}^m x_{ij}} \quad i = 1, \dots, m; j = 1, \dots, n$$

**Step 2.** Compute the entropy of attribute (criterion)  $j$  as follows:

$$0 \leq E_j = -\frac{1}{\ln(m)} \sum_{i=1}^m p_{ij} \ln p_{ij} \leq 1 \quad i = 1, \dots, m; j = 1, \dots, n$$

**Step 3.** Compute the degree of diversification  $d_j$  of the information transmitted by attribute (criterion)  $j$  according to  $d_j = 1 - E_j$ .

**Step 4.** Compute the entropy-derived weight  $w_j$  as follows:

$$w_j = \frac{d_j}{\sum_{j=1}^n d_j} \quad j = 1, \dots, n$$

If the decision-maker has prior subjective importance weights  $\lambda_j$  for each attribute (criterion), then this can be adapted into  $w_j$  as follows:

$$w_j^* = \frac{\lambda_j w_j}{\sum_{j=1}^n \lambda_j w_j} \quad j = 1, \dots, n$$

### Application of TOPSIS Ranking Risks

Here, we describe how TOPSIS and the entropy weighting method can be applied to derive a most-to least-critical risk ranking from a set of identified risk events. To begin, we first write the generalized decision matrix in Table 18 into the form given in Table 19.

In Table 19, we have a set of risk events instead of alternatives competing for the position of most-critical to a project. The most-critical risk event has the highest occurrence probability and the highest consequences (or impacts) to the project. Thus, the higher these indicators across the matrix in Table 19 the more critical is the associated risk event to the project.

| Set of<br>Risk Events   | Probability & Consequence Criteria |                 |                 |     |                 |
|-------------------------|------------------------------------|-----------------|-----------------|-----|-----------------|
|                         | Prob                               | C <sub>1</sub>  | C <sub>2</sub>  | ... | C <sub>n</sub>  |
|                         | w <sub>1</sub>                     | w <sub>2</sub>  | w <sub>3</sub>  | ... | w <sub>n</sub>  |
| Risk Event <sub>1</sub> | x <sub>11</sub>                    | x <sub>12</sub> | x <sub>13</sub> | ... | x <sub>1n</sub> |
| Risk Event <sub>2</sub> | x <sub>21</sub>                    | x <sub>22</sub> | x <sub>23</sub> | ... | x <sub>2n</sub> |
| Risk Event <sub>3</sub> | x <sub>31</sub>                    | x <sub>32</sub> | x <sub>33</sub> | ... | x <sub>3n</sub> |
| ...                     | ...                                | ...             | ...             | ... | ...             |
| Risk Event <sub>m</sub> | x <sub>m1</sub>                    | x <sub>m2</sub> | x <sub>m3</sub> | ... | x <sub>mn</sub> |

**A "Risk Event" Decision Matrix**

Table 19. A Risk Event Decision Matrix

Consider the following. Suppose we have seven risk events given in Table 20. Suppose the performance of these risks, in terms of their occurrence probabilities and consequences to a project, are given in the columns of Table 20. Suppose the consequence criteria values (in Table 20) derive from value functions. From these data, the TOPSIS equations will be applied to derive a score (or index) to rank-order each risk event from most-to least-critical to the project.

|              | Occurrence<br>Probability | Cost<br>Impact | Consequence Criteria |                                    |                        |
|--------------|---------------------------|----------------|----------------------|------------------------------------|------------------------|
|              |                           |                | Schedule<br>Impact   | Technical<br>Performance<br>Impact | Programmatic<br>Impact |
| Risk Event 1 | 0.75                      | 0.770          | 0.880                | 0.600                              | 0.789                  |
| Risk Event 2 | 0.95                      | 0.920          | 0.750                | 0.333                              | 0.474                  |
| Risk Event 3 | 0.55                      | 0.500          | 0.500                | 0.133                              | 0.211                  |
| Risk Event 4 | 0.25                      | 0.500          | 0.630                | 0.133                              | 0.474                  |
| Risk Event 5 | 0.45                      | 0.250          | 0.250                | 0.133                              | 0.789                  |
| Risk Event 6 | 0.15                      | 0.150          | 0.750                | 0.600                              | 0.474                  |
| Risk Event 7 | 0.90                      | 0.350          | 0.750                | 0.333                              | 0.211                  |

Table 20. An Illustrative Risk Event Decision Matrix

Applying each step of TOPSIS and the entropy weighting methods, described above, produces the scores in the right-most column in Table 21.

|                     | Occurrence<br>Probability | Cost<br>Impact | Consequence Criteria |                                    |                        | TOPSIS<br>Score |
|---------------------|---------------------------|----------------|----------------------|------------------------------------|------------------------|-----------------|
|                     |                           |                | Schedule<br>Impact   | Technical<br>Performance<br>Impact | Programmatic<br>Impact |                 |
| <b>Risk Event 1</b> | 0.75                      | 0.770          | 0.880                | 0.600                              | 0.789                  | 0.849           |
| <b>Risk Event 2</b> | 0.95                      | 0.920          | 0.750                | 0.333                              | 0.474                  | 0.668           |
| <b>Risk Event 3</b> | 0.55                      | 0.500          | 0.500                | 0.133                              | 0.211                  | 0.305           |
| <b>Risk Event 4</b> | 0.25                      | 0.500          | 0.830                | 0.133                              | 0.474                  | 0.267           |
| <b>Risk Event 5</b> | 0.45                      | 0.250          | 0.250                | 0.133                              | 0.789                  | 0.306           |
| <b>Risk Event 6</b> | 0.15                      | 0.150          | 0.750                | 0.600                              | 0.474                  | 0.463           |
| <b>Risk Event 7</b> | 0.90                      | 0.350          | 0.750                | 0.333                              | 0.211                  | 0.474           |

Table 21. Risk Event TOPSIS Scores

From Table 21, the most-to least-critical risk ranking can be seen as follows:

**Risk Event 4** (Least-Critical) < Risk Event 3 < Risk Event 5 <  
Risk Event 6 < Risk Event 7 < Risk Event 2 < **Risk Event 1** (Most-Critical)

Entropy weighting of these data revealed the criterion *Technical Performance Impact* transmitted the most distinct and differentiating information from all others (in this case). Thus, this criterion has the most weight or influence on the derivation of the risk event rank-order positions shown above.

## APPENDIX B

### INDUSTRY PRACTITIONER ASSESSMENTS

#### INTRODUCTION

This appendix presents an industry assessment of the risk analytic methods developed in this dissertation. The objectives of this assessment were to (1) obtain feedback from the engineering systems community on the logic and efficacy of these methods and (2) ascertain the relevance of this research to real-world practice in engineering complex, enterprise, systems.

The industry assessment was performed using qualitative research design principles and practices. These principles and practices are described in Creswell (2003) and Mariampolski (2001). The assessment method falls broadly into the case studies approach – an exploratory investigative technique that is “fundamentally interpretive” (Creswell, 2003).

Qualitative data was obtained from a survey defined by fifteen open-ended, non-directive, questions (Mariampolski, 2001). This encouraged findings to emerge from the assessment process. Face-to-face interviews allowed further probing of the data after the survey was returned by each respondent.

An inductive analysis of respondent data was performed. The analysis process consisted of four steps that followed the flow in Figure 88. The first step was the design and delivery of the survey instrument to identified industry participants. As stated above, fifteen open-ended questions were defined. They are listed in Table 22 and in subsequent tables throughout this appendix.

The second step involved an analysis of survey returns with the aim of inductively establishing themes or categories that characterized the responses from each respondent. The third step analyzed themes derived from the preceding step to look for broad patterns or generalizations that might be gleaned from the data. The fourth and last step fused these findings into a set of overall conclusions about the relevance, logic, and efficacy of the research in this dissertation from a practical real-world engineering systems perspective.

#### *Participant Selection and Qualifications*

Participant selection for the industry assessment followed guidance in the literature on criteria for identifying experts. Research by Ayyub (2001), Chytka (2004), and Edwards (2003) address this topic, which is briefly summarized below.

Ayyub (2003) defines an expert as “a very skillful person who had much training and has knowledge in some special field”. In addition, Ayyub (2003) emphasizes the importance that an expert’s knowledge be publicized at a level recognized by others in the community. This is consistent with studies by Edwards (2003) which identifies experts as persons characterized by academic degrees, training, experience, publications, position or rank, and special work-related appointments, studies, or assignments.

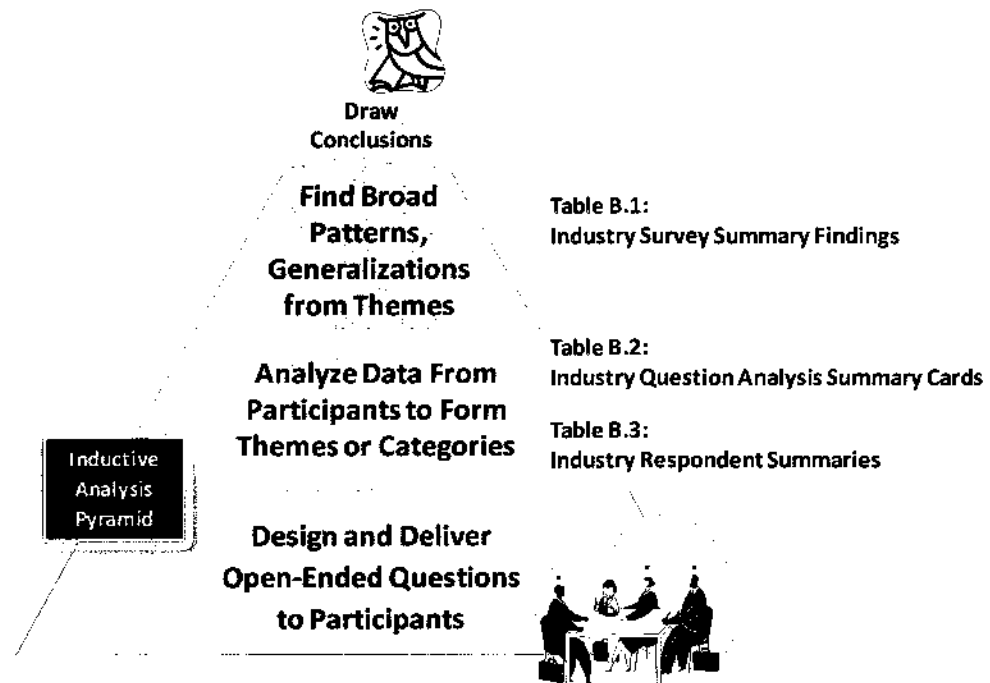


Figure 88. Industry Assessment Approach: An Inductive Analysis Pyramid

Chytka presents a set of criteria for the selection of experts that derives, in part, from Shanteau (2001) and Ayyub (2001). Chytka states “no one criterion should be used as a selection basis or disqualifier for the identification of an expert [Chytka, 2004]. Chytka further writes “the number of years of experience, educational background, and cognitive skills are criteria to be integrated in the selection process. Expertise is an integrated summation of characteristics (criteria)” [Chytka, 2004].

In 2001, research by Shanteau recognized that *discrimination* and *consistency* are two critical attributes in selecting an expert. Discrimination refers to “the ability to differentiate between similar but not identical cases. According to Shanteau’s research, discrimination is a “hallmark of expertise; that is, experts perceive and act on subtle distinctions that others miss”. Discrimination refers to a judge’s differential evaluation of different stimulus cases” (Shanteau, 2001). Consistency reflects “within-person reliability; it refers to a judge’s evaluation of the same stimuli over time; inconsistency is its complement” (Shanteau, 2001).

Participants selected for the industry assessment met or exceeded the above Shanteau/Chytka criteria in three relevant domains. These were systems engineering, risk/program management, and operations research. Qualification statements for these domains were written and are shown next. With these, experts different from the participants in this survey can later be identified to meaningfully partake in future evaluations of the risk analytic methods in this dissertation.



### **Systems Engineer Qualification**

A systems engineer is qualified to participate in this survey if he/she has at least 10 years of successful experience in engineering systems development and management. This should include technical leadership (e.g., a chief engineer) with engineering management experience of a comparable level with technical leadership responsibilities (e.g., a project leader). A key qualification is leadership experience that ranges from engineering traditional systems to complex engineering systems, to include systems of systems and enterprise systems. One or more advanced technical degrees is preferred in systems engineering or a closely relevant field.

### **Risk/Program Manager Qualification**

A risk/program manager is qualified to participate in this survey if he/she has at least 10-years of successful experience in the design and implementation of risk and program management processes and protocols on engineering systems developments. This should include analytical and/or engineering management leadership (e.g., a risk manager) that ranges from engineering traditional systems to complex engineering systems, to include systems of systems and enterprise systems. One or more advanced technical degrees is preferred in systems engineering or a closely relevant field.

### **Operations Research (OR) Analyst Qualification**

An operations research analyst is qualified to participate in this survey if he/she has at least 10-years of successful experience in the design and implementation of risk and decision-analytic methods that enable risk-informed decision-making on engineering systems developments. This should include analytical leadership (e.g., OR chief scientist) that ranges from engineering traditional systems to complex engineering systems, to include systems of systems and enterprise systems. One or more advanced technical degrees is preferred in mathematics, operations research, systems engineering, or a closely related highly quantitative field.

## **SUMMARY TABLE DESCRIPTIONS**

Before presenting the assessment summary findings, we first describe tables created from the industry survey data. Three tables were created. They are described below.

### **Table 22. Industry Assessment Summary Findings**

Table 22 provides an overall summary of the assessment's major themes. These are themes derived from the third step of the inductive analysis process shown in Figure 88. Table 22 is the third and final distillation of the data derived from the survey and forms the basis for the summary findings offered at the end of this section. Table 22 derives from Table 23.

### **Table 23. Industry Question 1-15 Analysis Summary Cards**

Table 23 is actually a set of fifteen tables with one "card" for each question. The information elements in Table 23 are defined as follows. The upper-half of each table results from an *inductive categorical analysis* of the respondent summaries. The lower-half of each table results from a *discourse analysis* of the respondent text. Discourse analysis is one way to conduct some quantitative text analysis on the information provided by respondents.

The discourse analysis looked at three areas. These areas are *most frequent words*, *key word frequency cloud*, and *phrase prominence*. The area *most frequent words* refers to the most recurrent relevant words reported across all respondents. The area *key word frequency cloud* expresses word frequency by font size. The more frequent the word the larger the font size and vice versa. The area *phrase prominence* refers to the most recurrent relevant phrase reported across all respondents.

A text analysis for *phrase prominence*, *key word frequency cloud*, and *most frequent words* aids in the identification of common themes or categories within and across respondent data. Table 23 is associated with the middle part of the inductive analysis pyramid in Figure 88. Table 23 derives from Table 24.

#### **Table 24. Industry Respondent Summaries**

Table 24 is a cross-comparison of respondent data by question. The information elements in Table 24 originates from the respondent raw data.

Finally, the information in these tables all stem from the respondent raw data. Subsequent distillations of these data were done in the order sequence given by Table 24, Table 23, and Table 22, respectively, and in accordance with the analysis flow shown in Figure 88.

### **INDUSTRY FINDINGS AND LESSONS BEING LEARNED**

Key findings from the industry assessment are discussed in this section and summarized in Table 22 (provided at the end of this section). Overall, participants cited the risk analytic methods in this dissertation found deficiencies in the engineering system's architectural design and captured risks associated with interactions and complex dependencies between entities that would otherwise have been missed. Participants also reported these methods required a moderate amount of training and socialization with engineers and stakeholders before they were accepted. This issue was driven by the newness of these techniques together with the present hard challenges in engineering enterprise systems.

With regards to socialization, a valuable lesson from the respondents was the importance of piloting and calibrating these risk analytic methods on smaller aspects of an engineering system. In this case, the system's architecture was chosen as the base case upon which to conduct the pilot. It was here the risk calculus created in Chapter III and the graph-theoretic methods designed in Chapters IV and V, for identifying and measuring risk co-relationships and risk dependencies, were found efficacious by the pilot. With this, the overall risk analysis approach in this dissertation went on to be more and more accepted and applied across additional aspects of the engineering system. Socialization by a well-planned, but gradual, infusion of these techniques into the engineering system's technical and managerial processes is the indicated way to proceed, especially when introducing new but needed engineering management methods into an already challenging and complex problem space.

The industry practitioner assessments also provided valuable insights into the information needed to drive the risk analytic methods in this dissertation and, more generally, to manage engineering an enterprise system from a capability portfolio perspective. The following summarizes key industry lessons *being* learned.

The analysis and management of risk in engineering an enterprise system has unique and thought challenging information needs. Respondents grouped these needs into two categories. The first *addresses capability value*. The second *addresses supplier contributions, criticality, and risks* as they relate to enabling the portfolio to deliver capability.

Information needs identified by industry practitioners to *address capability value* include the following:

- For each Tier 3 capability, shown in Figure 89\*, identify what performance standard (or outcome objective) each capability must meet by its scheduled delivery date.
- For each Tier 3 capability, identify the source basis for its performance standard (or outcome objective). Does it originate from user-driven needs, policy-driven needs, model-derived values, a combination of these, or from other sources?
- For each Tier 3 capability, identify to what extent the performance standard (or outcome objective) for one capability depends on others meeting their standards.

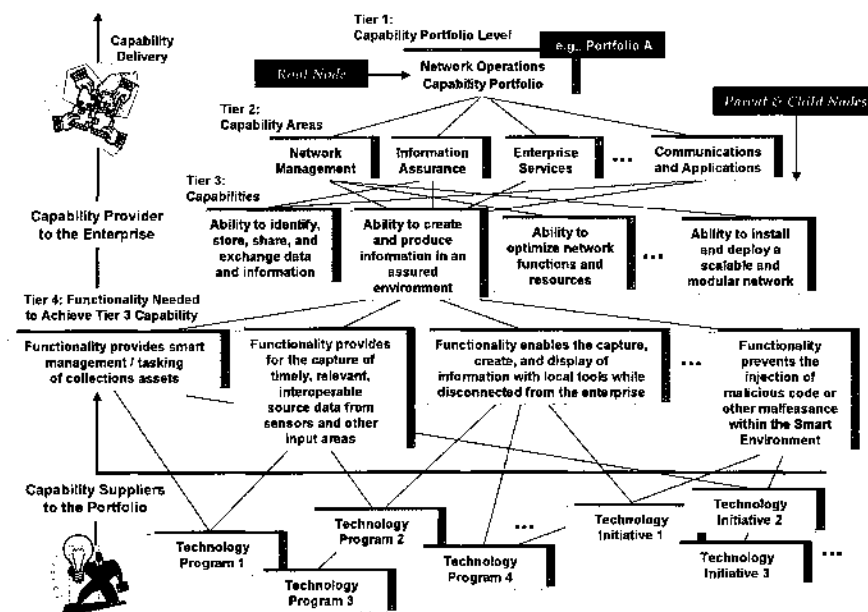


Figure 89. A View Into a Network Operations Capability Portfolio (e.g., Delivered by 20xx)

\* Presented in Chapters II and III, one way management plans for engineering an enterprise is to create capability portfolios of technology programs and initiatives that, when synchronized, will deliver time-phased capabilities that advance enterprise goals and mission outcomes. Once a capability portfolio's hierarchy and its elements are "defined" it is managed by a team to ensure its collection of technology programs and technology initiatives combine in ways to deliver one or more capabilities to the enterprise. Thus, one can take a supplier-provider view of a capability portfolio, as illustrated in Figure 89, where a capability portfolio can be viewed as the "provider" charged with delivering time-phased capabilities to the enterprise. Technology programs and technology initiatives aligned to, and synchronized with, the capability portfolio "supply" the functionality needed to achieve the provider's capability outcomes.

The supplier-provider view offers a way to examine a capability portfolio from a "risk-perspective". Enterprise goals and mission outcomes are dependent on capability portfolios successfully delivering required capabilities. Capability portfolios are dependent on programs and technologies successfully delivering functionality that enables these capabilities. Thus, major sources of risk originate from the "suppliers" to these capability portfolios.

Information needs identified by industry to *address supplier contributions, criticality, and risks* include the following:

- For each Tier 3 capability, identify which Technology Programs and Technology Initiatives are contributing to that capability.
- For each Tier 3 capability, identify what (specifically) are the contributions of its suppliers.
- For each Tier 3 capability, identify how supplier contributions enable the capability to achieve its standard (or outcome objective).
- For each Tier 3 capability, identify which Technology Programs and Technology Initiatives are critical contributors in enabling the capability to achieve its standard (or outcome objective).
- With the above, identify what risks originate from (or are associated with) suppliers that, if these events occur, negatively affect their contributions to capability.

Industry practitioners emphasized process tailoring, socialization, and establishing governance protocols as critical considerations in engineering risk management for enterprise systems. Overall, industry feedback indicates the risk analytic approaches herein provide beneficial and actionable insights. These include the following:

- Identification of risk events that threaten the delivery of capabilities needed to advance goals and capability outcome objectives of the enterprise.
- A measure of risk for each capability derived as a function of each risk event's occurrence probability and its consequence.
- An analytical framework and logical model within which to structure capability portfolio risk assessments – one where assessments can be combined to measure and trace their integrative influence on engineering the enterprise.
- Through the framework, ways to model and measure risk as capabilities are time-phased across incremental capability development approaches.
- The analytic transparency of the methods in this dissertation provide decision-makers the trace basis and the event drivers behind all risk measures derived for any node at any level of the capability portfolio's hierarchy. With this, capability portfolio management has visibility and supporting rationales for identifying where resources are best allocated to reduce (or eliminate) events that threaten achieving the capability outcome objectives of the enterprise.

How to design, engineer, and manage enterprise systems is at the cutting edge of modern systems thinking and engineering. Lack of clearly defined boundaries and diminished hierarchical control are significant technical and managerial challenges. Along with this, the engineering management community needs to establish methods for identifying, analyzing, and managing risks in systems engineered to operate in an enterprise space. Beginning to address this need has been the aim and objective of this research. It is clear from the industry assessment this objective has made positive gains but remains a work-in-progress. Table 22 presents an overall summary of the assessment findings. Details on each finding in Table 22 are found in Table 23 and Table 24.

| Industry Survey Question  | Respondent Summary Findings  |
|---|--|
| 1 What challenges characterized the engineering systems project where these methods were developed?               | Project Scope, Dependencies, Management Complexity   |
| 2 Were traditional engineering systems risk analysis methods appropriate? If yes, then why? If not, then why not? | Traditional Methods Alone not Fully Scalable; Traditional Methods Insufficient to Capture Complex Interactions |
| 3 What led to decisions to use the risk analytic methods in Chapter 3?  | Single System Risk Management Techniques Inadequate; Deeper Management Insights Needed                         |
| 4 What impact did these methods have on influencing decisions?  | System Architecture Deficiencies Corrected; A Risk's Spanning Space on Enterprise Capability Captured          |
| 5 Who benefited from these methods?   | Management, Engineers, Analysts  |
| 6 How were these methods actually implemented?  | Risk Analytic Methods Integrated With Engineering Processes; Instantiated Into Software                        |
| 7 How easy or complex were their implementations?   | Socialization Difficult; Software Instantiation Moderately Complex; Complex Problem Space                      |
| 8 How did participants feel about using these methods?  | Some Frustration With Newness of the Approach; Approach Met Needs  |
| 9 How did consumers of the outputs from these methods feel about their merits?                                    | Initial Reservations   |
| 10 Who do you feel are future participants and consumers of these methods?  | Peer Capability Portfolios; Government Programs Under Congressional Clinger-Cohen Mandates                     |
| 11 On a scale of 1 – 5 how analytically mature are these methods?   | Quite Good Maturity  |
| 12 What are the “pros” with these methods?  | Dependency Capture, Ripple Effects Identified and Modeled  |
| 13 What are the “cons” with these methods?  | Socialization Hurdle; Defining Capability in Cogent Ways   |
| 14 What factors will further shape the design of these methods?   | More Case Applications of the Risk Analytic Methods  |
| 15 Where should research be focused to further evolve these methods?  | Visualization Technologies; Cycle Dependencies   |

Table 22. Industry Assessment Summary Findings

## INDUSTRY SURVEY: QUESTION ANALYSIS “CARDS”

This section presents a summary analysis “card” for each industry survey question.

| Question 1  |   |
|---|---|
| What challenges characterized the engineering systems project where these methods were developed?   |   |
| <b>Inductive Categorical Analysis</b>   |   |
| The following themes derive from respondent narratives on this question.  |   |
| <b>Project Scope</b>  | Respondents directly or implicitly wrote that size and complexity of the system being engineered best characterized the project and drove the technical and managerial challenges. Size was described in terms of the system having to operate across an enterprise of users, while supporting the execution of complex missions by the integration and interaction of multiple capabilities. Managerial challenges were described by a portfolio manager with responsibility to deliver enterprise capabilities but without authority to manage the technology programs that enable them. This included the challenge of aligning the deployment of capabilities with the maturing of critical technologies. |
| <b>Dependencies</b>   | Respondents cited dependency relationships between the system’s moving parts needed to execute on an enterprise scale as a major challenge on this project. Dependency relationships involved not only the time synchronization of technology deliveries to schedule capability fielding but also funding relations and its continuity between competing needs of sponsors. Dependency challenges ran across the technical and socio-political landscapes.  |
| <b>Management Complexity</b>  | The supporting systems, systems of systems, and organizations to this engineering systems project were not directly reporting to the project’s capability manager, and the capabilities needed did not strictly align with a single capability area. Many capabilities expected to be delivered by this enterprise system fell outside the direct authority envelope of the capability portfolio manager. This increased the difficulties to build managerially meaningful and actionable program management plans, schedules, and deploy effective systems engineering and risk management practices.  |
| <b>Summary</b>  |   |
| Described above, respondents cited the key challenges on this project were scope, dependencies, and management complexity. Although these may be recognized as challenges common to any engineering systems project, the key in this case was their intensification by virtue of the enterprise scale with which they were felt and had to be addressed. Traditional systems engineering and management practices would not scale to this system’s level of complexity and the operational needs of an uncountable number of users across a world-wide landscape. |   |
| <b>Text Analysis of Respondent Narratives</b>   |   |
| The following are highlights from a text analysis of the narratives for this question across all respondents.   |   |
| <b>Most Frequent Words</b>  | Capability, Portfolio   |
| <b>Key Word Frequency Cloud</b>   | capability complexity dependencies portfolio programs<br>project risks sponsor system systems   |
| <b>Phrase Prominence</b>  | Size and complexity of the project/enterprise   |

Table 23. Industry Question 1 Analysis Summary Card

### Question 2

Were traditional engineering systems risk analysis methods appropriate? If yes, then why? If not, then why not?

#### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

##### Traditional Methods Alone Not Fully Scalable

Respondents cited traditional analysis methods for engineering systems are focused on how risk events impact a system's development cost, schedule, and technical performance. These dimensions alone don't fully span a risk event's consequence space when it affects an enterprise level. Here, management is ultimately concerned about events whose occurrences adversely affect the delivery of services to users.

##### Traditional Methods Insufficient to Capture Complex Interactions

Respondents cited how traditional methods do not adequately address the complex interactions that define an enterprise system, where synergy of operation among diverse systems is most important. Traditional methods do not capture dependency relationships between entities and how the occurrence of risks can have ripple effects across many others.

#### Summary

Traditional methods fail principally because of insufficient scope. From a high-level perspective, the basic risk management process is the same. The challenge comes from implementing and managing this process across a large-scale, complex, enterprise – where contributing systems may be in different stages of maturity and where managers, users, and stakeholders may have different capability needs and priorities.

An enterprise system is often planned and engineered to deliver capabilities through a series of time-phased increments or evolutionary builds. Thus, risks can originate from many different sources and threaten enterprise capabilities at different points in time. Furthermore, these risks (and their sources) must align to the capabilities they potentially affect and the scope of these consequences understood. In addition, the extent enterprise risks may have unwanted collateral effects on other dependent capabilities must be carefully examined.

#### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|                                 |   |
|---------------------------------|---|
| <b>Most Frequent Words</b>      | Risk, Impact, Traditional, Methods, Capability  |
| <b>Key Word Frequency Cloud</b> | capability consequence considerations dependencies enterprise;<br>traditional risk impact methods |
| <b>Phrase Prominence</b>        | Traditional risk analysis methods, enterprise systems   |

Table 23. Industry Question 2 Analysis Summary Card

| Question 3  |   |
|---|---|
| What led to decisions to use the risk analytic methods in Chapter III?  |   |
| <b>Inductive Categorical Analysis</b>   |   |
| The following themes derive from respondent narratives on this question.  |   |
| <b>Single System Risk Management Techniques Inadequate</b>  |   |
| Respondents cited the need to capture the size and complexity of a large portfolio of highly connected systems and systems of systems. Alone, single system risk management techniques were inadequate since a single risk in a particular system could significantly adversely impact the capability of the entire portfolio. Also, the risk analytic methodologies created in this dissertation can capture “over-arching” risks that might be missed by single-system risk management methods. |   |
| <b>Deeper Management Insights Needed</b>  |   |
| Similar to their response to Question 2, respondents cited the decision was driven by the complex nature of engineering this enterprise and the need for early alerts to the portfolio’s capabilities at risk. In addition, insights deeper than those possible from simple 5x5 risk matrices were needed by management to monitor and report achieving the capability roadmap and the delivery of critical services to users and consumers.  |   |
| <b>Summary</b>  |   |
| Respondents described the need to design of formal methods that provide a holistic understanding of risks in engineering enterprise systems, their potential consequences, inter-dependencies, and rippling effects across the enterprise space. Risk management for engineering enterprise systems aims to establish and maintain a complete view of risks across the enterprise, so capabilities and performance objectives are achieved via risk-informed resource and investment decisions.   |   |
| <b>Text Analysis of Respondent Narratives</b>   |   |
| The following are highlights from a text analysis of the narratives for this question across all respondents.   |   |
| <b>Most Frequent Words</b>  | Risk, Enterprise  |
| <b>Key Word Frequency Cloud</b>   | assessment of capability capture criticality-of-dependency<br>enterprise impact management of portfolio risk to roadmap |
| <b>Phrase Prominence</b>  | Single system risk management, enterprise risk management   |

Table 23. Industry Question 3 Analysis Summary Card



#### Question 4

What impact did these methods have on influencing decisions?

#### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

#### System Architecture Deficiencies Corrected

Respondents cited when the risk management methodologies developed in the dissertation were applied, architecture gaps and deficiencies were identified by virtue of how the risk methods captured linkages and dependencies between risks and entities. The risk management team joined forces with the system architecture team to evaluate the risk relationships to architectural entities; with this, gaps were identified early and which might have otherwise not been discovered until later in design. Timely corrections to deficiencies were made.

#### A Risk's Spanning Space on Enterprise Capability Captured

Respondents cited the methodologies herein enabled identifying risks whose impacts spanned multiple capability areas across the portfolio. How one risk event, if it occurred, would have multi-consequential effects on capabilities, or even create new risks, could be identified in ways that otherwise would be missed. A trace path could be established of how far (and where) each risk rippled throughout the portfolio.

#### Summary

Respondents cite that the risk analytic methods herein have been a key component in enabling capability-based portfolio investment analysis at an enterprise system level. With limited Government budgets, it is critical to understand how a mixture of various investments, acting in combination, best supports the operation of a broad mission or enterprise system. Moreover, it forces decision makers to evaluate and justify investment decisions based on their risks and mission impact, rather than on arbitrary performance parameters – such as bits-per-second for a communications system.

#### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|                                 |  |
|---------------------------------|--|
| <b>Most Frequent Words</b>      | Mission, System, Capability, Risks, Investments  |
| <b>Key Word Frequency Cloud</b> | architecture areas assessed <b>capability</b> capability-based capture engineering enterprise identify impact indirect influences interrelationships investment justify <b>mission</b> mixture optimization of options performance of portfolio representation resolution of risks |
| <b>Phrase Prominence</b>        | Capabilities, mission tree, enterprise system  |

Table 23. Industry Question 4 Analysis Summary Card

| Question 5   |  |
|--|--|
| Who benefited from these methods?  |  |
| <b>Inductive Categorical Analysis</b>  |  |
| The following themes derive from respondent narratives on this question.   |  |
| <b>Management, Engineers, and Analysts</b>   |  |
| Respondents cited senior management responsible for managing the engineering of this enterprise system benefited, as well as stakeholders with vested interests in using the capabilities the system would deploy. Of note was the extent leadership obtained better understandings of the overall impact that supplier program risks could have on higher-level capability needs, collateral risk consequences not initially visible, and ways to analytically tradeoff risks with investment decisions as they relate to mitigation courses of action. |  |
| <b>Summary</b>   |  |
| Respondents made clear that management, engineers, and analysts all benefited from the risk analytic methodologies developed in this dissertation. Senior leaders were provided breadth and depth of insight into how risks affect many parts and paths of engineering this enterprise. Engineers, technologists, and program analysts had early views into the interconnectedness of designs and the effects and influence of risks on them.  |  |
| <b>Text Analysis of Respondent Narratives</b>  |  |
| The following are highlights from a text analysis of the narratives for this question across all respondents.  |  |
| <b>Most Frequent Words</b>   | Program, risk  |
| <b>Key Word Frequency Cloud</b>  | interconnectedness; provide program risks recommendations                              |
| <b>Phrase Prominence</b>   | Management, engineers, and analysts all benefited from the risk analytic methodologies |

Table 23. Industry Question 5 Analysis Summary Card

| Question 6  |  |
|---|--|
| How were these methods actually implemented?  |  |
| <b>Inductive Categorical Analysis</b>   |  |
| The following themes derive from respondent narratives on this question.  |  |
| <b>Risk Analytic Methods Integrated With Engineering Processes</b>  |  |
| Respondents cited the risk analytic methods herein were integrated into an over-arching systems engineering process for managing the portfolio of capabilities this system was developing. The project director specifically defined tasks and procedures to develop an architecture, analyze the architecture, assess risks as they affected architectural entities and ultimately capabilities, and use these tools and techniques to make recommendations on managing the overall portfolio.   |  |
| <b>Instantiated Into Software</b>   |  |
| Respondents cited the risk analytic methods herein were instantiated into software in two key ways. First, a Microsoft Access database was created to capture all information related to identified risks and their impacts on the system. This included dependency considerations and collateral effects risks might have across multiple capabilities within the portfolio. Next, a visualization graphical interface was created via web technologies to allow for distributed inputs, outputs, and various management risk situation displays. Second, the analysis team integrated the risk analytics herein with investment optimization tools. This enabled risk-based investment tradeoffs to be made on a host of resource allocation decisions, such as where to invest in new capabilities or risk mitigation strategies to lessen the chances of capability/mission failures. |  |
| <b>Summary</b>  |  |
| Respondents made clear that management, engineers, and analysts all benefited from the risk analytic methodologies developed in this dissertation. Senior leaders were provided breadth and depth of insight into how risks affect many parts and paths of engineering this enterprise. Engineers, technologists, and program analysts had early views into the interconnectedness of designs and the effects and influence of risks on them.   |  |
| <b>Text Analysis of Respondent Narratives</b>   |  |
| The following are highlights from a text analysis of the narratives for this question across all respondents.   |  |
| <b>Most Frequent Words</b>  | Portfolio, Architecture, Capability  |
| <b>Key Word Frequency Cloud</b>   | architecture assessment capability dependencies portfolio risk roadmap rules |
| <b>Phrase Prominence</b>  | Risk analytic methods integrated into systems engineering process            |

Table 23. Industry Question 6 Analysis Summary Card

## Question 7

How easy or complex were their implementations?

### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

#### Socialization

Respondents cited the risk assessment methods herein are new. They took some initial orientation with participants who were entrenched in traditional cost, schedule, performance risk assessments; however, once a couple of risk assessments with the methods in this dissertation were conducted, participants quickly “caught on” to the ideas. They soon became comfortable with the risk analysis methods created for this enterprise engineering problem space.

#### Software Instantiation Moderately Complex

Respondents cited the moderate complexity of instantiating the risk analytic methodology into software. The database had to accommodate the many-to-many dependency relationships, risk assessments, and risk score roll-up schemas. The risk assessment input/output forms were more complex than traditional reporting. Here, it was necessary to tag a risk against any capability in the matrix and view the information sliced across capability by risk and by supplier program.

#### Complex Problem Space

Respondents cited the very complex nature of enterprise systems. The project’s engineering staff and risk management experts spent many hours understanding the complexity of the system, its environment, and the functional relationships within the architecture and the capability portfolio.

### Summary

The newness of the risk analysis methods, together with the very challenging enterprise engineering environment, necessitated more time than usual in socializing the ideas and the value of its outputs. After the risk analytic approaches were applied on a single aspect of the engineering system (e.g., the architectural design), participants then began to see the value of the methods. Full application of the approaches from Chapter III then proceeded in an organized and systematic way.

### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|                                 |  |
|---------------------------------|--|
| <b>Most Frequent Words</b>      | Risk, Assessment, Capability   |
| <b>Key Word Frequency Cloud</b> | architecture assessments capability complex dependency relationships<br>risk |
| <b>Phrase Prominence</b>        | Capability risk assessment   |

Table 23. Industry Question 7 Analysis Summary Card

| Question 8   |   |
|--|---|
| How did participants feel about using these methods?   |   |
| <b>Inductive Categorical Analysis</b>  |   |
| The following themes derive from respondent narratives on this question.   |   |
| <b>Some Frustration With Newness of the Approach</b>   |   |
| Respondents cited that participants experienced some frustration with these methods due (in-part) to the engineering complexity of the system/portfolio. However, the MITRE Director for the project was comfortable that quantifiable results could be demonstrated by first test-driving the risk analytic methods on the architectural design piece of the portfolio. Lessons-learned from that effort would then facilitate socialization and enable greater application of these techniques across more and more dimensions of the system's capability portfolio. |   |
| <b>Approach Met Needs</b>  |   |
| Respondents cited participants recognized FDNA, for example, could build on their previous analyses and put those results into a framework where additional insight and quantitative evaluation could be gleaned. This included their ultimate goal of providing a well-founded rationale for prioritizing risk mitigation investment options. Thus, the FDNA approach was not viewed as a new and unrelated analysis, but as a technique that would integrate and extend previous work.   |   |
| <b>Summary</b>   |   |
| In summary, respondents provided comments similar to those in Question 7. The capability risk assessment framework required orientation and socialization; however, after the new techniques were piloted on a piece of the program, the aims of and outputs from these methods became readily understood and valued by the project as a whole.  |   |
| <b>Text Analysis of Respondent Narratives</b>  |   |
| The following are highlights from a text analysis of the narratives for this question across all respondents.  |   |
| <b>Most Frequent Words</b>   | Complexity, framework   |
| <b>Key Word Frequency Cloud</b>  | quantifiable capability framework                                       |
| <b>Phrase Prominence</b>   | Quantifiable results; rational for risk mitigation investment decisions |

Table 23. Industry Question 8 Analysis Summary Card

| Question 9  |   |
|---|---|
| How did consumers of the outputs from these methods feel about their merits?  |   |
| <b>Inductive Categorical Analysis</b>   |   |
| The following themes derive from respondent narratives on this question.  |   |
| <b>Initial Reservations</b>   |   |
| As discussed in Question 8, respondents cited the sponsor had some reservations with regard to the results due to a perceived complexity of the tools and the newness of the risk analytic framework and processes. However, the outputs from these methods resulted in significant technical recommendations to change the system architecture. Such insights would have otherwise not been visible or caught as early as they were. Intermediate management levels used the results of the risk analyses. Synthesizing and summarizing findings from the analysis required some extra effort, but the risk analytic framework enabled drill-down to the singularly most risk-driving events threatening individual and overall capability goals of the portfolio. |   |
| <b>Summary</b>  |   |
| Overall, the engineers and analyst on this project had been searching for a risk analysis methodology that would enable them to establish a quantitative framework for their risk assessments and a basis for the selection of risk mitigation options. Participants felt the risk analytic framework and its various techniques (e.g., FDNA) suited their needs perfectly. Other customers have also been favorably impressed with these methods and FDNA in particular.   |   |
| <b>Text Analysis of Respondent Narratives</b>   |   |
| The following are highlights from a text analysis of the narratives for this question across all respondents.   |   |
| <b>Most Frequent Words</b>  | Reservations, newness   |
| <b>Key Word Frequency Cloud</b>   | newness risk methods  |
| <b>Phrase Prominence</b>  | Risk methods identified significant technical changes were needed |

Table 23. Industry Question 9 Analysis Summary Card

## Question 10

Who do you feel are future participants and consumers of these methods?

### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

#### Peer Capability Portfolios

Respondents cited peer portfolios within the government would benefit greatly from this methodology and, in fact, are already beginning to incorporate many aspects of these methods (e.g., FDNA). These approaches can be readily adopted by portfolio, enterprise, and capability managers conducting a risk assessment against enterprise-wide milestones or goals.

#### Government Programs Under Clinger-Cohen Compliance Mandates

Respondents cited future participants include those performing portfolio investment analyses, which focuses on maximizing overall mission capability while minimizing risks. This is a growing area of government effort, mandated by Congressional Directives such as the Clinger-Cohen Act and the DoD Joint Capabilities Integration Development System (JCIDS) Process.

### Summary

As mentioned previously, respondents cited the newness of the risk analysis methods, together with the very challenging enterprise engineering environment, necessitated more time than usual in socializing the ideas and value of the outputs. The same would be expected with peer portfolios. Training, presenting case studies, and providing lessons-learned from applying these methods would ease their acceptability by future participants.

### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|   |  |
|---|--|
| <b>Most<br/>Frequent<br/>Words</b>      | Portfolio  |
| <b>Key Word<br/>Frequency<br/>Cloud</b> | portfolio risk   |
| <b>Phrase<br/>Prominence</b>            | Peer portfolio managers would benefit from these methods |

Table 23. Industry Question 10 Analysis Summary Card

| Question 11  |                     |
|--|---------------------|
| On a scale of 1-5 how analytically mature are these methods?   |                     |
| <b>Inductive Categorical Analysis</b>  |                     |
| The following themes derive from respondent narratives on this question.   |                     |
| <b>Quite Good Maturity</b>   |                     |
| Two respondents assessed the maturity of the risk analysis structure as 4 – quite good maturity on the evidence that the analysis concepts have been implemented at least once. One respondent assessed the overall maturity as 5 – extremely good maturity.   |                     |
| <b>Summary</b>   |                     |
| Overall, respondents felt the risk analytic methodologies in this dissertation provided a good balance between capturing single-system risks that can impact the entire portfolio (or a significant portfolio capability) and over-arching enterprise-driving risks that do not appear in single-system assessments due to complex interdependencies. Maturity did not mean further refinements or advancements are not needed. Rather, that the analytics developed, thus far, derive from sound theory and their applications-to-date (even at this early stage) have clearly enabled meaningful/actionable decisions. |                     |
| <b>Text Analysis of Respondent Narratives</b>  |                     |
| The following are highlights from a text analysis of the narratives for this question across all respondents.  |                     |
| <b>Most Frequent Words</b>   | Maturity, good      |
| <b>Key Word Frequency Cloud</b>  | maturity            |
| <b>Phrase Prominence</b>   | Quite good maturity |

Table 23. Industry Question 11 Analysis Summary Card



## Question 12

What are the “pros” with these methods?

### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

#### Dependency Capture, Ripple Effects Identified and Modeled

Respondents cited the risk analytic methodologies (and especially FDNA) provided the ideal mechanism to capture the, possibly subtle, dependencies among a collection of interacting systems that support a mission enterprise. Capturing such dependencies is critical to identifying the source of capability performance risks in mission operations. The identification of such risks can then guide the optimal allocation of additional resources and system investments.

In addition, one respondent cited the FDNA approach can often integrate prior analyses that have been conducted on a program. For example, many government programs have a requirement to develop architectural “views” that capture various system, operational, and functional associations within a mission enterprise. However, these architectural views typically lack any expression of the relative importance and levels of dependency among the nodes within these taxonomies. FDNA equations can thus be introduced to support additional analyses that provide greater insight into mission capability dependencies and risks.

Another respondent cited one of the more interesting findings was the relationship and influence diagrams that come from the graph-theoretic representations in the risk methods (Chapter III); specifically, discovery of the secondary impacts of supplier-programs that were not fully understood prior to trying to map the relationships between them and their contributions to achieving capability. The secondary impact was the indirect impact of a dependency on a supplier of capability (e.g. the supplier to the supplier and the ripple effect of this relationship through the supplier-provider network shown in Chapter III).

### Summary

Respondents cited the ability to see the capability at risk and concomitant ripple effects were hallmarks of the methods in this dissertation. Beyond the traditional 5x5 probability-consequence matrix mentality, these new methods gave insight into what was in jeopardy of being achieved, not just that fact that there were high risks. Gaining insight into common contributors of risk to multiple areas across the desired capability space was beneficial. The ability to trace and track different risk impacts across many capability areas provided critical insights not easily visible (e.g., one single risk impacted 17 capability nodes).

### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|                                 |  |
|---------------------------------|--|
| <b>Most Frequent Words</b>      | Capability, risk, impact, mission  |
| <b>Key Word Frequency Cloud</b> | architectural areas <b>capability</b> dependencies have high <b>impact insight into mission risks supplier</b> |
| <b>Phrase Prominence</b>        | Analysis of mission enterprise; secondary impacts of risks captured  |

Table 23. Industry Question 12 Analysis Summary Card

## Question 13

What are the "cons" with these methods?

### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

#### Socialization Hurdle

Respondents continued to emphasize the importance of socializing these new methods in advance of their application. Convincing non-technical customers of the logic and merit of these approaches will continue to be a challenge, as it is with any new and sophisticated analytic method. It is important to illustrate the value of the methods in terms of how they help leadership make well-founded and rational decisions. Another hurdle is to secure the support of domain subject experts who have the insight and system knowledge necessary to characterize the inputs needed to execute the analysis and derive the benefits from its outputs.

#### Defining Capability in Cogent Ways

Respondents cited it was challenging to define capability in a particular timeframe to a satisfactory technical or operation level. Participants did not fully explore the contribution to capability of supplier-programs until the risk analytic methods herein really forced that understanding to take place. The risk analytic methods herein requires engineers reach consensus on the enterprise capability desired; that was tough in this context.

### Summary

Respondents made clear that socialization is, and will likely continue to be, the main hurdle. This will be true for many new engineering management methods for engineering enterprise systems via capability portfolio definition paradigms.

### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|                                 |   |
|---------------------------------|---|
| <b>Most Frequent Words</b>      | Capability, prioritization  |
| <b>Key Word Frequency Cloud</b> | Capability prioritization   |
| <b>Phrase Prominence</b>        | Socialization needed to derive the truly benefit from these risk analytic methods |

Table 23. Industry Question 13 Analysis Summary Card

### Question 14

What factors will further shape the design of these methods?

#### Inductive Categorical Analysis

The following themes derive from respondent narratives on this question.

#### More Case Applications

Respondents cited additional applications of these methods to engineering problems of an enterprise scale will ease and increase their acceptance by the community. Furthermore, more cases that demonstrate the positive technical impacts to decision making (seen so far) will enable the desire and intellectual energy to continuously advance the analytics developed-to-date.

#### Summary

Respondents made clear that more applications of these methods with enterprise engineering projects will undoubtedly expose new situations that will require further adaptation in these analytics. The risk analytic methods herein will adapt to capture unique relationships and mission architectures as engineering highly networked enterprise systems becomes more and more the norm of the information age.

#### Text Analysis of Respondent Narratives

The following are highlights from a text analysis of the narratives for this question across all respondents.

|   |   |
|---|---|
| <b>Most<br/>Frequent<br/>Words</b>      | Implementation, acceptance                      |
| <b>Key Word<br/>Frequency<br/>Cloud</b> | refinements implementations                     |
| <b>Phrase<br/>Prominence</b>            | Continued applications will further refinements |

Table 23. Industry Question 14 Analysis Summary Card

| Question 15  |   |
|--|---|
| Where should research be focused to further evolve these methods?  |   |
| <b>Inductive Categorical Analysis</b>  |   |
| The following themes derive from respondent narratives on this question.   |   |
| <b>Visualization Technologies</b>  |   |
| Respondents cited “visualization” of the outputs generated from the methods herein as an area of focus.  |   |
| <b>Cyclic Dependencies</b>   |   |
| Respondents also cited cyclic dependencies between nodes as an area to explore further, particularly in the context of an FDNA graph.  |   |
| <b>Summary</b>   |   |
| Overall, respondents felt additional implementations of the methods in this dissertation, and the lessons learned, will identify new areas of research. Customer needs spawn the need for new methods or refinement to current methods. Customer needs also present new challenges. Respondents felt the risk analytic methods herein are flexible and will adapt to these needs in the near and longer terms. |   |
| <b>Text Analysis of Respondent Narratives</b>  |   |
| The following are highlights from a text analysis of the narratives for this question across all respondents.  |   |
| <b>Most Frequent Words</b>   | Visualization   |
| <b>Key Word Frequency Cloud</b>  | Visualization technology  |
| <b>Phrase Prominence</b>   | Additional implementations will present further bases for refinements |

Table 23. Industry Question 15 Analysis Summary Card

## INDUSTRY SURVEY: QUESTIONS AND RESPONDENT SUMMARIES

This section presents respondent answers to each industry survey question.

| Question<br>1   | Respondent<br>JS  | Respondent<br>DM   | Respondent<br>CM  |
|---|---|--|---|
| What challenges characterized the engineering systems project where these methods were developed? | <p>In my opinion, there were two major challenges to the methods employed on the project: 1) the size and complexity of the project and 2) acceptance by our sponsor of the results. Specifically, the size and complexity of the project had a tendency to "disguise" a true impact to the overall portfolio of systems.</p> <p>With regard to sponsor acceptance, the perceived complexity of our processes and tools led to an uncertainty in the utility of the results. Many hours of dialogue with our sponsor was needed to explain our process and tools.</p> | <p>Many enterprise systems are designed to support a particular military mission or business operation whose effective conduct depends on the interaction of a variety of diverse system functions.</p> <p>For example, a military search-and-rescue operation may rely on the coordinated interaction of radar sensors, radio communications, computer processors, and rescue vehicles. The interplay among these systems may be complex, with the poor performance of any one system having detrimental consequences on the overall mission.</p> <p>The FDNA methodology provides an ideal mechanism to capture the, possibly subtle, dependencies among such a collection of interacting systems. Capturing such dependencies is critical to identifying the source of any capability deficiencies and performance risks in mission operations. The identification of these areas can then guide the optimal allocation of additional resources and system investments.</p> | <p>The effort was in support of a capability portfolio manager. The responsibility is/was to foster capability development. The portfolio was comprised of Programs and organizations that contribute to the capability areas under the purview of the capability manager, but not management authority.</p> <p>The Programs and organizations were not directly reporting to the capability manager, nor were the capabilities strictly aligned with a single capability area (within or external to the portfolio). There were many challenges inherent in the alignment and understanding of the complex management space.</p> <p>The portfolio manager needed insight into areas of risks to achieving the capability desired, where to focus efforts to close gaps in capability, prioritize issues, and risks that crossed multiple capability areas, programs, organizations, and identify mitigation opportunities.</p> |

Table 24. Industry Respondent Summaries

| Question<br>2  | Respondent<br>JS  | Respondent<br>DM  | Respondent<br>CM   |
|--|---|---|--|
| <p>Were traditional engineering systems risk analysis methods appropriate? If yes, then why? If not, then why not?</p> | <p>Traditional engineering systems risk analysis methods had some applicability in places (e.g., a 5x5 risk matrix (probability versus consequence) of the risk analysis approach, however, the risks identified as part of a traditional method might not necessarily be evaluated in terms of how they impact overall risks and dependencies prevalent in the portfolio.</p> <p>The approach designed for this enterprise system has roots in traditional risk management methods but greatly expands or adds to them for the complexity of this problem space.</p> | <p>Traditional risk analysis methods tend to focus on individual systems (such as their readiness levels or ability to meet, often arbitrary, performance standards) and program processes (such as schedule and funding).</p> <p>However, these methods do not adequately address the complex interactions that define an enterprise system, where synergy of operation among diverse systems is most important.</p> | <p>Yes and no. Traditional risk analysis methods were appropriate in the sense of analyzing risks and evaluating the impact of the risks. A traditional risk matrix of probability and consequence could be derived and evaluated. The difference was that the programs and risks had to be evaluated against the strategic goals of the organization, the identification of programs contributing to, and risks to the 'picture of success,' risks that impact the ability to achieve the capability desired.</p> <p>The development of the analytic methods presented in these documents were leveraged to gain insight and understanding of risk impact beyond cost, schedule, and technical domain (to include those considerations), but needing to capture the impact to the capability and the consideration of dependencies, to evaluate the impact to the capabilities themselves, and the direct and indirect influence of Programs for portfolio considerations.</p> <p>Traditional cost, performance, and schedule risk scales were modified for capability assessment. The fact that a single program was off its schedule may or may not impact the portfolio. The evaluation of risk was not whether a Program was 2 weeks or 2 months late, instead the assessment was whether it presented risk to the capability delivery roadmap (timeframe of need).</p> |

Table 24. Industry Respondent Summaries (continued)

| Question<br>3   | Respondent<br>JS  | Respondent<br>DM  | Respondent<br>CM   |
|---|---|---|--|
| <p>What led to decisions to use the risk analytic methods in Chapter III?</p> | <p>The decision to use the Enterprise Risk Management methodology as described in this dissertation was made in an attempt to capture the impacts of the size and complexity of a large portfolio of highly connected systems. Single system risk management techniques alone were inadequate due to the fact that a single, significant risk in a particular system could adversely impact the capability of the entire portfolio. Also, Enterprise Risk Management methodologies capture “over-arching” risks that are missed by single-system risk management methods.</p> | <p>In a current analysis we were given a system risk assessment that identified vulnerabilities among lower level tasks within an enterprise system operation. Risk mitigation actions had also been recommended to reduce the potential impact of these vulnerabilities.</p> <p>However, there was no mechanism for prioritizing these mitigation actions, since the relative importance of the performance of the individual tasks had not been evaluated and captured. The FDNA approach provided a very effective and efficient means for implementing such an evaluation</p> <p>The application of FDNA provided a natural network structure for capturing the existing enterprise system taxonomy. Moreover, the FDNA equations could then be overlaid on the network hierarchy to capture the operational level of each node as a function of its lower-level feeder nodes. Subject-matter experts (SMEs) were consulted to establish both the strength-of-dependency (SOD) and criticality-of-dependency (COD) for these nodal relationships.</p> <p>The resulting enterprise level, FDNA-based, capability tree then allowed us to measure the impact of individual, and groups of, mitigation actions at an overall enterprise level.</p> | <p>As stated in response to Question 2, the complex nature of the task, and desire to ‘see’ the capabilities at risk to being achieved. To provide an assessment of the ability to achieve the capability roadmap, not strictly a two-dimensional risk matrix (consequence and probability) that didn’t give insight into what was at risk, instead that there were (and remain) high, medium, and low risks.</p> <p>Chapter V, FDNA, was developed to evaluate the first and second order impact of Program contribution to capability.</p> |

Table 24. Industry Respondent Summaries (continued)

| Question<br>4  | Respondent<br>JS   | Respondent<br>DM  | Respondent<br>CM  |
|--|--|---|---|
| What impact did these methods have on influencing decisions? | <p>The Enterprise Risk Management methodology, coupled with our representation of our system architecture in the portfolio, led to recommendations to improvements in the architecture as well as corrections of deficiencies in the systems involved.</p> | <p>The FDNA methods have been a key component in enabling capability-based portfolio investment analysis at an enterprise system level. With limited Government budgets, it is critical to understand how a mixture of various investments, acting in combination, best supports the operation of a broad mission or enterprise system. Moreover, it forces decision makers to evaluate and justify investment decisions based on their mission impact, rather than on arbitrary performance parameters – such as bits-per-second for a communications system.</p> <p>In particular, FDNA equations facilitate the conversion of engineering performance scales to “value functions” (on a 0-100 utility scale), following the approach of Keeney-Raiffa. The basis for selecting investment options has either been to enhance mission capabilities or to reduce system risks. In either case, my approach has utilized the construction of a mission tree hierarchy, often called a “strategy-to-task” mission decomposition. Within this mission tree hierarchy it is essential to capture the interrelationships and dependencies among the various tree nodes, starting at top-level mission objectives and flowing down to lower-level functions and tasks. I have found the FDNA methodology to be an ideal mechanism to capture these relationships.</p> <p>Having established such an FDNA-based network framework, it is then possible to map potential technology investments against associated mission nodes and use FDNA equations to measure their impact in improving capabilities or reducing risks. Optimization algorithms can then be applied to this overall framework in order to identify most cost-effective investment portfolios.</p> | <p>Chapter III, the capability risk assessment framework, enabled the team to identify common risks/issues to be assessed further by study teams.</p> <p>The risks that spanned capability areas were identified for coordinated effort to identify resolutions across capability domains.</p> <p>Chapter V, FDNA, was not fully implemented, but of the partial implementation the indirect influences were interesting, e.g. the program contributing to another program, thus indirectly impacting a capability they are not directly influencing.</p> |

Table 24. Industry Respondent Summaries (continued)



| Questions<br>5, 6, 7                            | Respondent<br>JS   | Respondent<br>DM  | Respondent<br>CM   |
|---|--|---|--|
| Who benefited from these methods?               | Our sponsor, as well as the DoD Services (Air Force, Army, Navy, and Marines) involved in this program.  | Program managers, decision-makers, and other stakeholders benefit from the FDNA approach by achieving a better understanding of the overall impact of system, capability risks and where their scarce investment dollars should be spent in mitigating these factors.   | In this case, the analysts benefited most, the ability to see the interconnectedness of risks and influence and provide recommendations for grouping of 'like' risks.  |
| How were these methods actually implemented?    | The risk management system was integrated into an over-arching systems engineering process for Portfolio Management. Specifically, our project set up efforts to develop an architecture, analyze the architecture, assess risk, and make recommendations with regard to the portfolio.  | The FDNA rules are easily implemented within a portfolio investment selection tool designed to capture a mission capability tree hierarchy wherein nodal dependencies can be specified by FDNA rules. A portfolio investment tool can then measure the impact of any set of investment options and apply an optimization algorithm to identify the most cost-effective portfolio at any budget level. | These methods were implemented via use of a MS Access database and .Net application to view the information; this included MS Excel spreadsheets and interviews of subject matter experts (SMEs). Architecture products and schedules proved useful as they evolved.   |
| How easy or complex were their implementations? | Enterprises or Portfolio of Systems are by their very nature very complex. Our engineering staff and our risk management experts spent many hours understanding the complex system and functional relationships within the architecture and portfolio.<br><br>With that said, once understood, the enterprise risk management implementation (described in Chapter III of this dissertation) proceeded in an organized and systematic way. The difficulty was in communicating the process, tools, and results to our sponsor. | The FDNA rules are easy to specify within a portfolio investment selection tool.<br><br>Most of the work lies in gathering SME judgments on dependency relationships that are then expressed by SOD and COD values.   | Moderately complex. The database had to accommodate the many to many relationships and assessments, and roll-up schemas. The risk assessment input/output forms for input were more complex than traditional (ability to tag a risk against any capability in the matrix, and view the information sliced across capability, by risk, by program, etc.). The development of the summary of information (e.g. the grouping of risks causing concern across the space) took time to evaluate.<br><br>The risk assessment facilitation of SMEs took some initial orientation to the context of the risk assessment, as the participants were more generally entrenched in cost, schedule, performance risk assessments, but once a couple of assessments were conducted, they quickly 'caught on' to the framework and were comfortable with the format of the assessment (probability and assessment against achieving the capability in the timeframe desired).<br><br>Without the full architectural understanding, the FDNA was more difficult. The specifics of the capability in the timeframe and the contribution were not flushed out to a level of fidelity for the FDNA structure. The SMEs said it seemed straight forward enough, the products and common understanding was not to the level needed for the capability contribution specificity. |

Table 24. Industry Respondent Summaries (continued)

| Questions<br>8, 9, 10  | Respondent<br>JS  | Respondent<br>DM  | Respondent<br>CM   |
|--|---|---|--|
| How did participants feel about using these methods?                         | The participants (technical staff actually using the tools/processes) might have experienced some frustration (because of the complexity of the portfolio and sponsor coordination), however, as the Director for this effort, I felt comfortable that I had quantifiable results based on a well-thought out set of tools and risk analytic processes. | In the most recent application (see response to question 3) the participants recognized that the FDNA and investment selection approach built on their previous analyses and put them in a framework where additional insight and quantitative evaluation could be applied, including their ultimate goal of providing a well-founded rationale for prioritizing risk mitigation options.<br><br>Thus the FDNA approach was not viewed as a new and unrelated analysis, but as a tool that integrated and extended their previous work. | See answer to Question 7. The capability risk assessment framework took some initial orientation (more work required), but was understood once the analysts walked through a risk assessment.<br><br>The FDNA sounded logical, but was more challenging to perform the assessment of contribution.   |
| How did consumers of the outputs from these methods feel about their merits? | As mentioned above, our sponsor had some reservations with regard to the results due to a perceived complexity of the tools and the newness of the risk analytic processes. However, the outputs from our processes resulted in significant technical recommendations to change the system architecture.  | In the most recent application (also see response to question 3) the participants had been searching for a methodology that would enable them to establish a quantitative framework for their risk assessment and selection of mitigation actions. They felt that the combined FDNA and investment selection approach suited their needs perfectly. Other customers have also been favorably impressed with the FDNA capabilities.  | Intermediate management levels used the risk information. The information was not shared with the most senior leadership. As with any method, the outputs were only as good as the inputs.<br><br>The risk information still required being summarized and synthesized for intermediate and senior leadership, but the framework enabled drill-down to the risk causing concern for the analysts.  |
| Who do you feel are future participants and consumers of these methods?      | There are peer portfolios within the government who would benefit greatly from this methodology, and in fact, are already incorporating some of these methods.  | The area of portfolio investment analysis focusing on maximizing overall mission capability and minimizing system risks is a growing area of Government concern, as evidenced by directives such as the Clinger-Cohen Act and the DoD Joint Capabilities Integration Development System (JCIDS) Process. As noted above, the FDNA methodology plays a key role in implementing these analyses and will continue to be a critical tool in our support to Government agencies.  | These approaches can be most readily adopted by Portfolio, enterprise, and capability managers, risk assessment against organizational goals.<br><br>Additionally, some of the concepts here can be applied to program and project management. Instead of just cost, schedule, technical, if there are specific capability or milestones the program or project must achieve, risks can be assessed and monitored against those planned achievements. FDNA can be applied to programs or organizations with first and second order contributors (e.g. contractors and sub-contractors or suppliers). |

Table 24. Industry Respondent Summaries (continued)

| Questions<br>11, 12   | Respondent<br>JS   | Respondent<br>DM  | Respondent<br>CM   |
|---|--|---|--|
| <p>On a scale of 1 – 5 how analytically mature are these methods?</p> <p>Analytical maturity refers to the degree these methods are fully developed to a complete or final stage. Explain the basis for your maturity rating.</p> | <p>5, Extremely good maturity. The methodology captures a good balance between capturing single-system risks that can impact the entire portfolio (or a significant portfolio capability) and over-arching risks that do not appear in single-system assessments due to complex interdependencies.</p> | <p>I would rate FDNA at level 4, based on my actual implementation of this approach with several customers, and their reaction regarding its suitability for addressing their problems.</p> <p>In particular, FDNA's ease of applicability within the portfolio investment selection tool, which itself has been successfully applied to support numerous customers over an eight year period, makes it a readily applicable methodology.</p>   | <p>4. The maturity of the analysis structure is 4 – quite good maturity. The concepts have been implemented at least once.</p>   |
| <p>What are the "pros" with these methods?</p>  | <p>Good project synergy due to project engineering staff and risk management experts understanding the complexity of the portfolio. High impact risks are identified</p>   | <p>As indicated above, the FDNA methodology provides an ideal mechanism to capture the, possibly subtle, dependencies among a collection of interacting systems that support a mission enterprise. Capturing such dependencies is critical to identifying the source of capability performance risks in mission operations. The identification of such risks can then guide the optimal allocation of additional resources and system investments.</p> <p>In addition, we have found that the FDNA approach can often integrate prior analyses that have been conducted on a program. For example, many Government programs have a requirement to develop architectural "views" that capture various system, operational, and functional associations within a mission enterprise.</p> <p>However, these architectural views typically lack any expression of the relative importance and levels of dependency among the nodes within these taxonomies. FDNA equations can thus be introduced to support additional analyses that provide greater insight into mission capability dependencies and sources of risk.</p> | <p>Ability to see the capability at risk. Beyond the 5x5 risk matrix mentality, this method gave insight into what was in jeopardy of being achieved, not just that fact that there were high risks.</p> <p>Gaining insight into common contributors of risk to multiple areas across the desired capability space was beneficial. The ability to tag different risk impacts across many capability areas provided insight (e.g. a single risk impacted 17 capability elements). Even without the capability contribution defined, there were many risks that could be defined to achieve the capability within the desired timeframe.</p> <p>One of the more interesting findings was the relationship and influence diagram; the secondary impact of Programs, not fully understood prior to trying to map out the relationships between the programs contributing to achieving capability. The secondary impact was the indirect impact of a dependency of a supplier of capability (e.g. the supplier to the supplier, and the ripple effect through the network).</p> |

Table 24. Industry Respondent Summaries (continued)

| Questions<br>13, 14, 15   | Respondent<br>JS   | Respondent<br>DM  | Respondent<br>CM  |
|---|--|---|---|
| What are the “cons” with these methods?                           | Time may be required to communicate the use of tools/processes to non-participants.  | <p>Convincing non-technical customers of the logic and merit of the FDNA approach will continue to be a challenge, as it is with any sophisticated analytic method.</p> <p>As with any other such tools, we need to be able to illustrate the value of the FDNA methodology in terms of how it will help the customer make well-founded and rational decisions.</p> <p>Another hurdle is to secure the support of domain SMEs who have the insight and system knowledge necessary to identify the dependency relationships used to establish the FDNA equations.</p>  | <p>The ability to define capability desired in a particular timeframe, within a particular area, to a satisfactory level was challenging. We did not fully explore the contribution to capability of programs because the initial step was not achieved to a level of detail desired.</p> <p>This method requires consensus/agreement as to the capability desired and that was tough in this context. Time needs to be devoted by the team to analyze the information for most meaningful results displays. There is not a clear-cut prioritization of top risks, we used multiple prioritization schemes for risk priority. Strictly max average resulted in too many ties and didn’t account for frequency of impact (ultimately we evaluated both).</p> |
| What factors will further shape the design of these methods?      | Acceptance by our sponsors and showing positive technical impact to the decision making process will enable the freedom to improve the tools/processes involved. | Application of the FDNA methodology with Government sponsors will undoubtedly expose us to new situations that will require further adaptation in this approach. New methods often undergone enhancements to address customer needs; so too will the FDNA methodology adapt to capture unique relationships within mission architectures.   | Refinements will occur with further implementation of these approaches. Both for language in the constructed scales and in ranking/prioritization rules.  |
| Where should research be focused to further evolve these methods? | Visualization or straight-forward explanations of the “inner workings” of the enterprise risk management methods developed in this dissertation.                 | <p>Issues that arrive during actual implementation of the FDNA methodology will certainly point to additional areas of research for this approach. Customer needs often present new challenges for any of our analytic methods and lead to creative adaptations that could not be otherwise anticipated.</p> <p>However, as one particular area of study that currently could use further development is the phenomenon of cyclic dependencies, e.g., node A feeds node B that, in turn, feeds node C that comes back to feed node A. This situation will surely arise in our future studies, such as in the analysis of critical infrastructure sectors, which include Energy, Transportation, Agriculture &amp; Food, Telecommunications, and Information Technology systems.</p> | Analysis and visualization of cluster effects. Consideration of mitigation resource trades in constrained and unconstrained environments.   |

Table 24. Industry Respondent Summaries (concluded)

## INDUSTRY SURVEY: RESPONDENT RAW DATA

This section presents each respondent's raw data.

### PART I. RESPONDENT'S BACKGROUND INFORMATION

*Please provide a brief summary of your professional background and responsibility for the task associated that led to the development of the risk analytic methods described herein.*

**Name:** John J. Shottes, Jr.; The MITRE Corporation

**Evaluation Reply Date:** 29 December 2008

**Professional Background:** *Briefly describe you academic and professional background. Include years of professional experience in the engineering systems community.*

I am currently the Director of a collaborative, knowledge sharing organization for a large agency within the Department of Defense (DoD). The principle domain of my current organization is in the field of Battle Management and Command and Control. In my current position, I am responsible for identifying risks and mitigation strategies, conducting independent technical assessments, identifying opportunities to share knowledge, and mentoring across a broad range of programs within a large enterprise. Prior to my current assignment, I served as a Project Director for a large expanse of systems within a Portfolio Management structure. In this capacity, I directed a team which provided critical support in the areas of systems engineering and integration, architecture development and analysis, risk management, and portfolio optimization.

I have been engaged in systems engineering with The MITRE Corporation since 1985. I earned my undergraduate degree at Boston University (Bachelor of Liberal Studies in Mathematics) and a Master of Science degree in Computer Engineering from the University of Massachusetts at Lowell. I am a Senior Member of the American Institute of Aeronautics and Astronautics and a Member of the Institute of Electrical and Electronics Engineers.

**Description of Work Responsibility:** *Without program(s) attribution, briefly describe your roles and responsibilities on the task or assignment that led to the development of the risk analytic method described in this dissertation.*

See above professional background description. Specifically, as a MITRE Project Director for a 30 Staff-Year Technical Project, I directed a team which provided critical support in the areas of systems engineering and integration, architecture development and analysis, risk management, and portfolio optimization.

## PART II. EVALUATION QUESTIONS

*The following are the questions that comprise this evaluation. Please provide short but sufficient answers to these questions with examples (where possible) that support and amplify your response. Please submit your answers to these questions electronically to the researcher on a separate document.*

*Henceforth “these methods” refer to the risk analytic methods in Chapter III and Chapter V of this dissertation.*

### **1. What challenges characterized the engineering systems project where these methods were developed?**

In my opinion, there were two major challenges to the methods employed on the project: 1) the size and complexity of the project and 2) acceptance by our sponsor of the results. Specifically, the size and complexity of the project had a tendency to “disguise” a true impact to the overall portfolio of systems. With regard to sponsor acceptance, the perceived complexity of our processes and tools led to an uncertainty in the utility of the results. Many hours of dialogue with our sponsor was needed to explain our process and tools.

### **2. Were traditional engineering systems risk analysis methods appropriate? If yes, then why? If not, then why not?**

Traditional engineering systems risk analysis methods had some applicability in places (e.g., like constructing a 5×5 risk matrix (probability versus consequence) of the risk analysis approach, however, the risks identified as part of a traditional method might not necessarily be evaluated in terms of how they impact overall risks and dependencies prevalent in the portfolio. The approach designed for this enterprise system has roots in traditional risk management methods but greatly expands or adds to them for the complexity of this problem space.

### **3. What led to decisions to use the risk analytic methods in Chapter III?**

The decision to use the Enterprise Risk Management methodology as described in this dissertation was made in an attempt to capture the impacts of the size and complexity of a large portfolio of highly connected systems. Single system risk management techniques alone were inadequate due to the fact that a single, significant risk in a particular system could adversely impact the capability of the entire portfolio. Also, Enterprise Risk Management methodologies capture “over-arching” risks that are missed by single-system risk management methods.

**4. What impact did these methods have on influencing decisions?**

The Enterprise Risk Management methodology, coupled with our representation of our system architecture in the portfolio, led to recommendations to improvements in the architecture as well as corrections of deficiencies in the systems involved.

**5. Who benefited from these methods?**

Our sponsor, as well as the DoD Services (Air Force, Army, Navy, Marines) involved in this program.

**6. How were these methods actually implemented?**

The risk management system was integrated into an over-arching systems engineering process for Portfolio Management. Specifically, our project set up efforts to develop an architecture, analyze the architecture, assess risk, and make recommendations with regard to the portfolio.

**7. How easy or complex were their implementations?**

Enterprises or Portfolio of Systems are by their very nature very complex. Our engineering staff and our risk management experts spent many hours understanding the complex system and functional relationships within the architecture and portfolio. With that said, once understood, the enterprise risk management implementation (described in Chapter III of this dissertation) proceeded in an organized and systematic way. The difficulty was in communicating the process, tools, and results to our sponsor.

**8. How did participants feel about using these methods?**

The participants (technical staff actually using the tools/processes) might have experienced some frustration (because of the complexity of the portfolio and sponsor coordination), however, as the Director for this effort, I felt comfortable that I had quantifiable results based on a well-thought out set of tools and risk analytic processes.

**9. How did consumers of the outputs from these methods feel about their merits?**

As mentioned above, our sponsor had some reservations with regard to the results due to a perceived complexity of the tools and the newness of the risk analytic processes. However, the outputs from our processes resulted in significant technical recommendations to change the system architecture.

**10. Who do you feel are future participants and consumers of these methods?**

There are peer portfolios within the government who would benefit greatly from this methodology, and in fact, are already incorporating some of these methods.

**11. On a scale of 1 – 5 how analytically mature are these methods? Analytical maturity refers to the degree these methods are fully developed to a complete or final stage. Explain the basis for your maturity rating.**

5, Extremely good maturity. The methodology captures a good balance between capturing single-system risks that can impact the entire portfolio (or a significant portfolio capability) and over-arching risks that do not appear in single-system assessments due to complex interdependencies.

**12. What are the “pros” with these methods?**

Good project synergy due to project engineering staff and risk management experts understanding the complexity of the portfolio.

High impact risks are identified

**13. What are the “cons” with these methods?**

Time may be required to communicate the use of tools/processes to non-participants.

**14. What factors will further shape the design of these methods?**

Acceptance by our sponsors and showing positive technical impact to the decision making process will enable the freedom to improve the tools/processes involved.

**15. Where should research be focused to further evolve these methods?**

Visualization or straight-forward explanations of the “inner workings” of the enterprise risk management methods developed in this dissertation.



## PART I. RESPONDENT'S BACKGROUND INFORMATION

*Please provide a brief summary of your professional background and responsibility for the task associated that led to the development of the risk analytic methods described herein.*

**Name:** Richard A. Moynihan; The MITRE Corporation

**Evaluation Reply Date:** 24 January 2009

**Professional Background:** *Briefly describe you academic and professional background. Include years of professional experience in the engineering systems community.*

Ph.D., Mathematics, concentration in Probability, University of Massachusetts/Amherst  
M.S., Operations Research, Cornell University  
A.B., Mathematics, Dartmouth College

I am a Principal Staff/Group Leader in the Economic and Decision Analysis Center (EDAC) at MITRE Corporation. I joined MITRE in 1977, after spending two years teaching college and conducting academic research in probability theory. My areas of expertise and responsibility include the following: Decision Analysis, Risk Analysis, Portfolio Investment Analysis, System Effectiveness Studies, Mathematical/Computer Modeling, and Operations/ Logistics Analysis.

**Description of Work Responsibility:** *Without program(s) attribution, briefly describe your roles and responsibilities on the task or assignment that led to the development of the risk analytic method described in this dissertation.*

Much of my recent work has involved developing and applying analytic methods to identify technology investments to support the missions of various Government organizations, including military services. The basis for selecting investment options has either been to enhance mission capabilities or to reduce system risks. In either case, my approach has utilized the construction of a mission tree hierarchy, often called a "strategy-to-task" mission decomposition. Within this mission tree hierarchy it is essential to capture the interrelationships and dependencies among the various tree nodes, starting at top-level mission objectives and flowing down to lower-level functions and tasks. I have found the FDNA methodology to be an ideal mechanism to capture these relationships. Having established such an FDNA-based network framework, it is then possible to map potential technology investments against associated mission nodes and use FDNA equations to measure their impact in improving capabilities or reducing risks. Optimization algorithms can then be applied to this overall framework in order to identify most cost-effective investment portfolios.

## PART II. EVALUATION QUESTIONS

*The following are the questions that comprise this evaluation. Please provide short but sufficient answers to these questions with examples (where possible) that support and amplify your response. Please submit your answers to these questions electronically to the researcher on a separate document.*

*Henceforth “these methods” refer to the risk analytic methods in Chapter III and Chapter V of this dissertation.*

### **1. What challenges characterized the engineering systems project where these methods were developed?**

Many enterprise systems are designed to support a particular military mission or business operation whose effective conduct depends on the interaction of a variety of diverse system functions. For example, a military search-and-rescue operation may rely on the coordinated interaction of radar sensors, radio communications, computer processors, and rescue vehicles. The interplay among these systems may be complex, with the poor performance of any one system having detrimental consequences on the overall mission. The FDNA methodology provides an ideal mechanism to capture the, possibly subtle, dependencies among such a collection of interacting systems. Capturing such dependencies is critical to identifying the source of any capability deficiencies and performance risks in mission operations. The identification of these areas can then guide the optimal allocation of additional resources and system investments.

### **2. Were traditional engineering systems risk analysis methods appropriate? If yes, then why? If not, then why not?**

Traditional risk analysis methods tend to focus on individual systems (such as their readiness levels or ability to meet, often arbitrary, performance standards) and program processes (such as schedule and funding). However, these methods do not adequately address the complex interactions that define an enterprise system, where synergy of operation among diverse systems is most important.

### **3. What led to decisions to use the risk analytic methods in Chapter III?**

In a current analysis we were given a system risk assessment that identified vulnerabilities among lower level tasks within an enterprise system operation. Risk mitigation actions had also been recommended to reduce the potential impact of these vulnerabilities. However, there was no mechanism for prioritizing these mitigation actions, since the relative importance of the performance of the individual tasks had not been evaluated and captured.

The FDNA approach provided a very effective and efficient means for implementing such an evaluation. The application of FDNA provided a natural network structure for capturing the existing enterprise system taxonomy. Moreover, the FDNA equations could then be overlaid on the network hierarchy to capture the operational level of each node as a function of its lower-level feeder nodes. Subject-matter experts (SMEs) were consulted to establish both the strength-of-dependency (SOD) and criticality-of-dependency (COD) for these nodal relationships. The resulting enterprise level, FDNA-based, capability tree then allowed us to

measure the impact of individual, and groups of, mitigation actions at an overall enterprise level.

**4. What impact did these methods have on influencing decisions?**

The FDNA methods have been a key component in enabling capability-based portfolio investment analysis at an enterprise system level. With limited Government budgets, it is critical to understand how a mixture of various investments, acting in combination, best supports the operation of a broad mission or enterprise system. Moreover, it forces decision makers to evaluate and justify investment decisions based on their mission impact, rather than on arbitrary performance parameters – such as bits-per-second for a communications system.

In particular, FDNA equations facilitate the conversion of engineering performance scales to “value functions” (on a 0-100 utility scale), following the approach of Keeney-Raiffa.

**5. Who benefited from these methods?**

Program managers, decision-makers, and other stakeholders benefit from the FDNA approach by achieving a better understanding of the overall impact of system, capability risks and where their scarce investment dollars should be spent in mitigating these factors.

**6. How were these methods actually implemented?**

The FDNA rules are easily implemented within portfolio investment selection tools. Such tools are designed to capture a mission capability tree hierarchy wherein nodal dependencies can be specified by FDNA rules. Portfolio investment tools can then measure the impact of any set of investment options and apply an optimization algorithm to identify the most cost-effective portfolio at any budget level.

**7. How easy or complex were their implementations?**

The FDNA rules are easy to specify within portfolio investment selection tools. Most of the work lies in gathering SME judgments on dependency relationships that are then expressed by SOD and COD values.

**8. How did participants feel about using these methods?**

In the most recent application (see response to question 3) the participants recognized that FDNA built on their previous analyses and put them in a framework where additional insight and quantitative evaluation could be applied, including their ultimate goal of providing a well-founded rationale for prioritizing risk mitigation options. Thus the FDNA approach was not viewed as a new and unrelated analysis, but as a tool that integrated and extended their previous work.

**9. How did consumers of the outputs from these methods feel about their merits?**

In the most recent application (also see response to question 3) the participants had been searching for a methodology that would enable them to establish a quantitative framework for their risk assessment and selection of mitigation actions. They felt that FDNA when combined with their mitigation selection approach suited their needs perfectly. Other customers have also been favorably impressed with the FDNA capabilities.

**10. Who do you feel are future participants and consumers of these methods?**

The area of portfolio investment analysis focusing on maximizing overall mission capability and minimizing system risks is a growing area of Government concern, as evidenced by directives such as the Clinger-Cohen Act and the DoD Joint Capabilities Integration Development System (JCIDS) Process. As noted above, the FDNA methodology plays a key role in implementing these analyses and will continue to be a critical tool in our support to Government agencies.

**11. On a scale of 1 – 5 how analytically mature are these methods? Analytical maturity refers to the degree these methods are fully developed to a complete or final stage. Explain the basis for your maturity rating.**

I would rate FDNA at level 4, based on my actual implementation of this approach with several customers, and their reaction regarding its suitability for addressing their problems. In particular, FDNA's ease of applicability within portfolio investment selection tools, which itself has been successfully applied to support numerous customers over an eight year period, makes it a readily applicable methodology.

**12. What are the “pros” with these methods?**

As indicated above, the FDNA methodology provides an ideal mechanism to capture the, possibly subtle, dependencies among a collection of interacting systems that support a mission enterprise. Capturing such dependencies is critical to identifying the source of capability performance risks in mission operations. The identification of such risks can then guide the optimal allocation of additional resources and system investments.

In addition, we have found that the FDNA approach can often integrate prior analyses that have been conducted on a program. For example, many Government programs have a requirement to develop architectural “views” that capture various system, operational, and functional associations within a mission enterprise. However, these architectural views typically lack any expression of the relative importance and levels of dependency among the

nodes within these taxonomies. FDNA equations can thus be introduced to support additional analyses that provide greater insight into mission capability dependencies and sources of risk.

**13. What are the “cons” with these methods?**

Convincing non-technical customers of the logic and merit of the FDNA approach will continue to be a challenge, as it is with any sophisticated analytic method. As with any other such tools, we need to be able to illustrate the value of the FDNA methodology in terms of how it will help the customer make well-founded and rational decisions. Another hurdle is to secure the support of domain SMEs who have the insight and system knowledge necessary to identify the dependency relationships used to establish the FDNA equations.

**14. What factors will further shape the design of these methods?**

Application of the FDNA methodology with Government sponsors will undoubtedly expose us to new situations that will require further adaptation in this approach. Just as new methods undergone enhancements to address customer needs, so too will the FDNA methodology adapt to capture unique relationships within mission architectures.

**15. Where should research be focused to further evolve these methods?**

Issues that arrive during actual implementation of the FDNA methodology will certainly point to additional areas of research for this approach. Customer needs often present new challenges for any of our analytic methods and lead to creative adaptations that could not be otherwise anticipated.

However, as one particular area of study that currently could use further development is the phenomenon of cyclic dependencies, e.g., node A feeds node B that, in turn, feeds node C that comes back to feed node A. This situation will surely arise in our future studies, such as in the analysis of critical infrastructure sectors, which include Energy, Transportation, Agriculture & Food, Telecommunications, and Information Technology systems.

## **PART I. RESPONDENT'S BACKGROUND INFORMATION**

*Please provide a brief summary of your professional background and responsibility for the task associated that led to the development of the risk analytic methods described herein.*

**Name:** Charlene J. McMahon; The MITRE Corporation

**Evaluation Reply Date:** 2 February 2009

**Professional Background:** *Briefly describe you academic and professional background. Include years of professional experience in the engineering systems community.*

B.S. Resource Economics, University of Massachusetts, Amherst, 1992

M.S. Information System Engineering, Northeastern University, 1999

1993 - Present. The MITRE Corporation, Bedford, Massachusetts.

I am a Group Leader, Principle Staff, in the Economic and Decision Analysis Center at The MITRE Corporation. The group I lead provides support to MITRE government sponsors in analyzing and managing risk, cost, and schedule. Since 2003, I have been the leader of the MITRE Center for Acquisition and Systems Analysis, Risk Analysis and Management Technical Team. I have supported a broad range of government programs, experiments, organizations, enterprise systems, system of systems, and capability portfolios. On these efforts, I have focused on the implementation of risk management processes and assessments, cost, and environmental considerations.

**Description of Work Responsibility:** *Without program(s) attribution, briefly describe your roles and responsibilities on the task or assignment that led to the development of the risk analytic method described in this dissertation.*

Task leader to provide risk analysis and management strategy and implementation for a Capability Portfolio.

## PART II. EVALUATION QUESTIONS

*The following are the questions that comprise this evaluation. Please provide short but sufficient answers to these questions with examples (where possible) that support and amplify your response. Please submit your answers to these questions electronically to the researcher on a separate document.*

**Henceforth “these methods” refer to the risk analytic methods in Chapter III and Chapter V of this dissertation.**

### **1. What challenges characterized the engineering systems project where these methods were developed?**

The effort was in support of a capability portfolio manager. The responsibility is/was to foster capability development. The portfolio was comprised of Programs and organizations that contribute to the capability areas under the purview of the capability manager, but not management authority. The Programs and organizations were not directly reporting to the capability manager, nor were the capabilities strictly aligned with a single capability area (within or external to the portfolio). There were many challenges inherent in the alignment and understanding of the complex management space. The portfolio manager needed insight into areas of risks to achieving the capability desired, where to focus efforts to close gaps in capability, prioritize issues, and risks that crossed multiple capability areas, programs, organizations, and identify mitigation opportunities.

### **2. Were traditional engineering systems risk analysis methods appropriate? If yes, then why? If not, then why not?**

Yes and no. Traditional risk analysis methods were appropriate in the sense of analyzing risks and evaluating the impact of the risks. A traditional risk matrix of probability and consequence could be derived and evaluated. The difference was that the programs and risks had to be evaluated against the strategic goals of the organization, the identification of programs contributing to, and risks to the ‘picture of success,’ risks that impact the ability to achieve the capability desired. The development of the analytic methods presented in these documents were leveraged to gain insight and understanding of risk impact beyond cost, schedule, and technical domain (to include those considerations), but needing to capture the impact to the capability and the consideration of dependencies, to evaluate the impact to the capabilities themselves, and the direct and indirect influence of Programs for portfolio considerations. Traditional cost, performance, and schedule risk scales were modified for capability assessment. The fact that a single program was off its schedule may or may not impact the portfolio. The evaluation of risk was not whether a Program was 2 weeks or 2 months late, instead the assessment was whether it presented risk to the capability delivery roadmap (timeframe of need).

### **3. What led to decisions to use the risk analytic methods in Chapter III?**

As stated in response to Question 2, the complex nature of the task, and desire to ‘see’ the capabilities at risk to being achieved. To provide an assessment of the ability to achieve the capability roadmap, not strictly a two-dimensional risk matrix (consequence and probability)

that didn't give insight into what was at risk, instead that there were (and remain) high, medium, and low risks. Chapter V, FDNA, was developed to evaluate the first and second order impact of Program contribution to capability.

**4. What impact did these methods have on influencing decisions?**

Chapter III, the capability risk assessment framework, enabled the team to identify common risks/issues to be assessed further by study teams. The risks that spanned capability areas were identified for coordinated effort to identify resolutions across capability domains. Chapter V, FDNA, was not fully implemented, but of the partial implementation the indirect influences were interesting, e.g. the program contributing to another program, thus indirectly impacting a capability they are not directly influencing.

**5. Who benefited from these methods?**

In this case, the analysts benefited most, the ability to see the interconnectedness of risks and influence and provide recommendations for grouping of 'like' risks.

**6. How were these methods actually implemented?**

These methods were implemented via use of a MS Access database and .Net application to view the information; this included MS Excel spreadsheets and interviews of subject matter experts (SMEs). Architecture products and schedules proved useful as they evolved.

**7. How easy or complex were their implementations?**

Moderately complex. The database had to accommodate the many to many relationships and assessments, and roll-up schemas. The risk assessment input/output forms for input were more complex than traditional (ability to tag a risk against any capability in the matrix, and view the information sliced across capability, by risk, by program, ...). The development of the summary of information (e.g. the grouping of risks causing concern across the space) took time to evaluate. The risk assessment facilitation of SMEs took some initial orientation to the context of the risk assessment, as the participants were more generally entrenched in cost, schedule, performance risk assessments, but once a couple of assessments were conducted, they quickly 'caught on' to the framework and were comfortable with the format of the assessment (probability and assessment against achieving the capability in the timeframe desired). Without the full architectural understanding, the FDNA was more difficult. The specifics of the capability in the timeframe and the contribution were not flushed out to a level of fidelity for the FDNA structure. The SMEs said it seemed straight forward enough, the products and common understanding was not to the level needed for the capability contribution specificity.

**8. How did participants feel about using these methods?**

See answer to Question 7. The capability risk assessment framework took some initial orientation (more work required), but was understood once the analysts walked through a risk assessment. The FDNA sounded logical, but was more challenging to perform the assessment of contribution.



**9. How did consumers of the outputs from these methods feel about their merits?**

Intermediate management levels used the risk information. The information was not shared with the most senior leadership. As with any method, the outputs were only as good as the inputs. The risk information still required being summarized/synthesized for intermediate and senior leadership, but the framework enabled drill-down to the risk causing concern for the analysts.

**10. Who do you feel are future participants and consumers of these methods?**

These approaches can be most readily adopted by Portfolio, enterprise, and capability managers, risk assessment against organizational goals. Additionally, some of the concepts here can be applied to program and project management. Instead of just cost, schedule, technical, if there are specific capability or milestones the program or project must achieve, risks can be assessed and monitored against those planned achievements. FDNA can be applied to programs or organizations with first and second order contributors (e.g. contractors and sub-contractors or suppliers).

**11. On a scale of 1 – 5 how analytically mature are these methods? Analytical maturity refers to the degree these methods are fully developed to a complete or final stage. Explain the basis for your maturity rating.**

4. The maturity of the analysis structure is 4 – quite good maturity. The concepts have been implemented at least once.

**12. What are the “pros” with these methods?**

Ability to see the capability at risk. Beyond the 5×5 risk matrix mentality, this method gave insight into what was in jeopardy of being achieved, not just that fact that there were high risks. Gaining insight into common contributors of risk to multiple areas across the desired capability space was beneficial. The ability to tag different risk impacts across many capability areas provided insight (e.g. a single risk impacted 17 capability elements). Even without the capability contribution defined, there were many risks that could be defined to achieve the capability within the desired timeframe. One of the more interesting findings was the relationship and influence diagram; the secondary impact of Programs, not fully understood prior to trying to map out the relationships between the programs contributing to achieving capability. The secondary impact was the indirect impact of a dependency of a supplier of capability (e.g. the supplier to the supplier, and the ripple effect through the network).

**13. What are the “cons” with these methods?**

The ability to define capability desired in a particular timeframe, within a particular area, to a satisfactory level was challenging. We did not fully explore the contribution to capability of programs because the initial step was not achieved to a level of detail desired. This method requires consensus/agreement as to the capability desired and that was tough in this context. Time needs to be devoted by the team to analyze the information for most meaningful results displays. There is not a clear-cut prioritization of top risks, we used multiple prioritization

schemes for risk priority. Strictly max average resulted in too many ties and didn't account for frequency of impact (ultimately we evaluated both).

**14. What factors will further shape the design of these methods?**

Refinements will occur with further implementation of these approaches. Both for language in the constructed scales and in ranking/prioritization rules.

**15. Where should research be focused to further evolve these methods?**

Analysis and visualization of cluster effects. Consideration of mitigation resource trades in constrained and unconstrained environments.

## APPENDIX C

### LITERATURE ASSESSMENT SUMMARY

#### INTRODUCTION

As discussed in Chapter 1, today's systems are increasingly characterized by their *ubiquity* and lack of specification. Systems like the internet are unbounded, present everywhere, and in places simultaneously. They are an *enterprise* of systems and systems-of-systems. Through the use of advanced network and communications technologies, these systems continuously operate to meet the demands of globally distributed and uncountable many users and communities.

Engineering enterprise systems is an emerging discipline that encompasses and extends traditional systems engineering to create and evolve webs of systems and systems of systems. They operate in a network-centric way, to deliver capabilities via services, data, and applications through richly interconnected networks of information and communications technologies.

More defense systems, transportation systems, and financial systems connect across boundaries and seamlessly interface with users, information repositories, applications, and services. These systems are an enterprise of people, processes, technologies, and organizations.

How to design, engineer, and manage enterprise systems is at the cutting edge of the literature on systems thinking and engineering. Lack of clearly defined boundaries and diminished hierarchical control are significant technical and managerial challenges. Along with this, the engineering management community needs to establish and publish methods for identifying, analyzing, and managing risks in systems engineered to operate in enterprise contexts.

What makes managing risks in engineering enterprise systems more challenging than managing risks in engineering traditional systems? How does the delivery of capability to users affect how risks are identified and managed in engineering enterprise systems?

With regard to the first question, the difference is principally a matter of scope. From a high-level perspective, the basic risk management process (refer to Figure 2) is the same. The challenge comes from implementing and managing this process across a large-scale, complex, enterprise – where contributing systems may be in different stages of maturity and where managers, users, and stakeholders may have different capability needs and priorities.

With regard to the second question, an enterprise system is often planned and engineered to deliver capabilities through a series of time-phased increments or evolutionary builds. Thus, risks can originate from many different sources and threaten enterprise capabilities at different points in time. Furthermore, these risks (and their sources) must align to the capabilities they potentially affect and the scope of their consequences understood. In addition, the extent enterprise risks may have unwanted collateral effects on other dependent capabilities must be carefully examined.

A final distinguishing challenge in engineering enterprise systems is not only their technologies but the way users interface with them and each other. Today, the engineering and social science communities are joining in ways not previously seen when planning and evolving the design, development, and operation of enterprise systems.

The goal of this research is the design of formal methods that provide a holistic understanding of risks in engineering enterprise systems, their potential consequences, dependencies, and rippling effects across the enterprise space. Ultimately, risk management in this context aims to establish and maintain a complete view of risks across the enterprise, so capabilities and performance objectives are achieved via risk-informed resource and investment decisions.

### LITERATURE ASSESSMENT

The literature in this field has only begun to address the complexities and multidisciplinary nature of this problem space. Foundational perspectives on ways to view this space exist in the literature. However, evident from the literature assessment summarized in Table 25 significant knowledge gaps exist on methods for identifying, analyzing, and managing risks in systems engineered to operate on an enterprise scale. Beginning to address this need has been the aim, objective, and contribution of this research. From the industry and literature assessments Appendix B and Appendix C, respectively, it is clear this objective has made positive gains but remains a work-in-progress.

Figure 90 shows the major academic disciplines relevant in this research and published literature. Three axes are shown. They are *engineering systems*, *risk and decision theory*, and *engineering risk management*. General systems theory provides a foundation and context for how aspects of these disciplines are applied to the research problems in this dissertation.

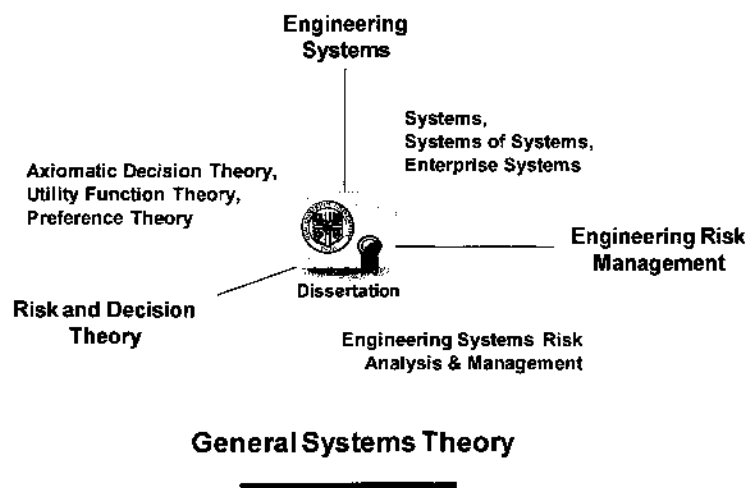


Figure 90. Dissertation Research: Literature Map Dimensions

### Relationship of Dissertation Research to Published Literature

This section identifies key publications related to engineering risk management and offers an assessment of this literature in relation to the research in this dissertation. In Chapter I, five problem areas were investigated. The first area established a framework within which to study systems engineering risk theory and how it extends to the enterprise problem space. This includes developing new methods and new risk-analytic formalisms. Solutions to subsequent problem areas built upon these findings. Chapter VII integrated these results to form an analytical framework and computational model to measure risk and its impacts in engineering enterprise systems.

#### Problem Area 1

Describe and structure the risk management problem space as it relates to engineering enterprise systems from a capability portfolio perspective.

#### Problem Area 2

Develop mathematical protocols for measuring risk within structures of capability portfolios, where these portfolios collectively deliver capability to consumers served by the enterprise. Create measurement formalisms that account for, and track, multiple-sources where risks to capabilities originate.

#### Problem Area 3

Develop decision-theoretic algorithms for measuring risk criticality as a function of the measures developed in Problem Area 2 and capability dependencies present in a portfolio.

#### Problem Area 4

Develop protocols for capturing and measuring dependencies among capabilities within a portfolio and across a family of portfolios that comprise an enterprise.

#### Problem Area 5

Bring together research and solution approaches developed in problem areas one through four into a coherent theory for representing, modeling, and measuring risk in engineering large-scale, complex, systems designed to function in enterprise-wide environments.

Table 25 presents an assessment of the literature with respect to these five problem areas and isolates where gaps in current scholarship are addressed by the research in this dissertation. For this, a color coding scheme was defined and presented below. The color code indicates the degree to which the dissertation research problem area is addressed in the referenced article or work.

#### COLOR CODING SCHEME

##### Red:

Problem area not addressed in the referenced article or work.

##### Yellow:

Problem area addressed to some extent in the referenced article or work; but, insufficient to meet this dissertation's research objectives.

##### Green:

Problem area addressed in the referenced article or work.

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Allen, T., Nightingale, D., Murman, E., March 2004. "Engineering Systems an Enterprise Perspective", an Engineering Systems Monograph, Engineering Systems Division, The Massachusetts Institute of Technology.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Arrow, K. J., 1965. "Aspects of the Theory of Risk Bearing", Yrjo Jahnsson Lectures, Helsinki, Finland: Yrjo Jahnssonin Saatio.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Ayyub, B. M., 2001. *Elicitation of Expert Opinions for Uncertainty and Risks*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Ayyub, B. M., McGill, W. L., Kaminsky, M., 2007. "Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework", Risk Analysis, Vol. 27, No. 4.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Bahnmaier, W. W., editor, 2003. *Risk Management Guide for DOD Acquisition*, 5th Edition, Version 2.0, Department of Defense Acquisition University Press, Fort Belvoir, Virginia, 22060-5565.

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
| RED | RED | RED | RED | RED |
|-----|-----|-----|-----|-----|

Bernoulli, D., 1738. "Exposition of a New Theory on the Measurement of Risk", *Econometrica*, Vol. 22, No. 1 (Jan., 1954), pp. 23-36 Virginia, 22060-5565, The Econometric Society, [www.jstor.org/stable/1909829](http://www.jstor.org/stable/1909829).

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Blanchard, B. S., Fabrycky W. J., 1990. *Systems Engineering and Analysis*, 2nd ed. Englewood Cliffs, New Jersey, Prentice-Hall, Inc.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Browning, T. R., Deyst, J. J., Eppinger, S. D., 2002. "Adding Value in Product Development by Creating Information and Reducing Risk", *IEEE Transactions on Engineering Management*, Vol. 49, No. 4.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Chytka, T., Conway, B., Keating, C., Unal, R., 2004. "Development of an Expert Judgment Elicitation And Calibration Methodology for Risk Analysis in Conceptual Vehicle Design", Old Dominion University Project Number: 130012, NASA Grant NCC-1-02044, NASA Langley Research Center, Hampton, Virginia 23681.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Clemen, R. T., 1996. *Making Hard Decisions An Introduction to Decision Analysis*, 2nd edition, Pacific Grove, California, Brooks/Cole Publishing Company.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Cox, L. A., Babayev, D., Huber, W., 2005. "Some Limitations of Qualitative Risk Rating Systems" Risk Analysis, Vol. 25, No. 3.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Cox, L. A., 2009. "Improving Risk-Based Decision Making for Terrorism Applications", Risk Analysis, Vol. 29, No. 3.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Creswell, J. W., 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2nd ed.), Sage University Press, Thousand Oaks, California.

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
| RED | RED | RED | RED | RED |
|-----|-----|-----|-----|-----|

Crowther, K. G., Haimes, Y. Y., Taub, G., 2007. "Systemic Valuation of Strategic Preparedness Through Application of the Inoperability Input-Output Model with Lessons Learned from Hurricane Katrina", Risk Analysis, Vol. 27, No. 5.

|     |        |     |       |     |
|-----|--------|-----|-------|-----|
| RED | YELLOW | RED | GREEN | RED |
|-----|--------|-----|-------|-----|

Daniels, C. B. and LaMarsh, W. J., 2007. "Complexity as a Cause of Failure in Information Technology Project Management", Proceedings of IEEE International Conference on System of Systems Engineering, April, pp.1-7.

|        |        |     |     |     |
|--------|--------|-----|-----|-----|
| YELLOW | YELLOW | RED | RED | RED |
|--------|--------|-----|-----|-----|

de Finetti, B., 1974. *Theory of Probability*, Vol. 1., John Wiley & Sons, New York, NY.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

de Finetti, B (author)., A. Mura, A. (editor), 2008. *Philosophical Lectures on Probability*: Springer-Science + Business Media B. V.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Dyer, J. S., Sarin, R. K., 1979. "Measurable Multiattribute Value Functions", *Operations Research*, Vol. 27, No. 4, July-August.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Edwards, J. E., Scott, J. C., Nambury, R. S., 2003. *The Human Resources Program-Evaluation Handbook*, Sage University Press, Thousand Oaks, California.

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
| RED | RED | RED | RED | RED |
|-----|-----|-----|-----|-----|

Edwards, W., 1954. "The Theory of Decision Making", *Psychological Bulletin*, 41, 380-417.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Edwards, W., 1961. "Behavioral Decision Theory", *Annual Review of Psychology*, 12, 473-498.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Fishburn, P. C., "Foundations of Decision Analysis: Along the Way", *Management Science*, Vol. 35, No. 4, April 1989.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

GAO: Government Accountability Office, July 2004. "Defense Acquisitions: The Global Information Grid and Challenges Facing its Implementation", GAO-04-858.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Garvey, P. R., Cho, C. C., Giallombardo, R., 1997. "RiskNav: A Decision Aid for Prioritizing, Displaying, and Tracking Program Risk", *Military Operations Research*, V3, N2.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Garvey, P. R., 1999. "Risk Management", *Encyclopedia of Electrical and Electronics Engineering*, John Wiley & Sons, New York, NY.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)



| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Garvey, P. R., 2000. *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), London, Boca Raton, New York; I; ISBN 0824789660.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Garvey, P. R., 2001. "Implementing a Risk Management Process for a Large Scale Information System Upgrade – A Case Study", *INSIGHT*, Vol. 4, Issue 1, International Council on Systems Engineering (INCOSE).

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Garvey, P. R., Cho, C. C., 2003. "An Index to Measure a System's Performance Risk", *The Acquisition Review Quarterly (ARQ)*, Vol. 10, No. 2.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Garvey, P. R., Cho, C. C., 2005. "An Index to Measure and Monitor a System of systems' Performance Risk", *The Acquisition Review Journal (ARJ)*.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Garvey, P. R., 2005. "System of Systems Risk Management Perspectives on Emerging Process and Practice", The MITRE Corporation, MP 04B0000054.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Garvey, P. R., 2008. *Analytical Methods for Risk Management: A Systems Engineering Perspective*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), London, Boca Raton, New York; ISBN 1584886374.

|       |        |        |     |     |
|-------|--------|--------|-----|-----|
| GREEN | YELLOW | YELLOW | RED | RED |
|-------|--------|--------|-----|-----|

Gelinas, N., 2007. "Lessons of Boston's Big Dig", *City Journal*.

|    |    |    |    |    |
|----|----|----|----|----|
| NA | NA | NA | NA | NA |
|----|----|----|----|----|

Gharajedaghi, J., 1999. *Systems Thinking Managing Chaos and Complexity – A Platform for Designing Business Architecture*, Woburn, Massachusetts, Butterworth-Heinemann.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Haimes, Y. Y., 2004. *Risk Modeling, Assessment, and Management*, 2nd ed., John Wiley & Sons, New York, NY.

|        |        |        |       |     |
|--------|--------|--------|-------|-----|
| YELLOW | YELLOW | YELLOW | GREEN | RED |
|--------|--------|--------|-------|-----|

Hofstetter, P., Bare, J. C., Hammitt, J. K., Murphy, P. A., Rice, G. E., 2002. "Tools for Comparative Analysis of Alternatives: Competing or Complementary Perspectives?" *Risk Analysis*, Vol. 22, No. 5.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Hwang, Ching-Lai, Yoon, K. Paul, 1995. *Multiple Attribute Decision Making: An Introduction*, Sage University Paper Series in Quantitative Applications in the Social Sciences, 07-104, Thousand Oaks, California, copyright 1995, by Sage.

|     |     |       |     |     |
|-----|-----|-------|-----|-----|
| RED | RED | GREEN | RED | RED |
|-----|-----|-------|-----|-----|

Jackson, M. C., 1991. *Systems Methodology for the Management Sciences*, New York: Plenum.

|        |        |     |     |     |
|--------|--------|-----|-----|-----|
| YELLOW | YELLOW | RED | RED | RED |
|--------|--------|-----|-----|-----|

Jaynes, E. T., 1988. "Probability Theory as Logic", Ninth Annual Workshop on Maximum Entropy and Bayesian Methods, Dartmouth College, New Hampshire, August 14, 1989. In the Proceedings Volume, *Maximum Entropy and Bayesian Methods*, Paul F. Fougere, Editor, Kluwer Academic Publishers, Dordrecht, Holland (1990).

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Jiang, P., Haimes, Y. Y., 2004. "Risk Management for Leontief-Based Interdependent Systems", *Risk Analysis*, Vol. 24, No. 5.

|        |        |     |       |     |
|--------|--------|-----|-------|-----|
| YELLOW | YELLOW | RED | GREEN | RED |
|--------|--------|-----|-------|-----|

Kaplan, S., Garrick, B., 1981. "On the Quantitative Definition of Risk", *Risk Analysis*, Vol. 1, No. 1, pp.11–27.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Kaplan, S., 1997. "The Words of Risk Analysis", *Risk Analysis*, Vol. 4, No. 17.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., Peterson, W., Rabadi, G., 2003. "System of Systems Engineering", *Engineering Management Journal*, Vol. 15, No. 3.

|        |        |     |     |     |
|--------|--------|-----|-----|-----|
| YELLOW | YELLOW | RED | RED | RED |
|--------|--------|-----|-----|-----|

Keating, C. B., Sousa-Poza, A., Mun, Ji Hyon, 2004. "System of Systems Engineering Methodology", Department of Engineering Management and Systems Engineering, Old Dominion University, ©2004, All rights reserved.

|        |        |     |     |     |
|--------|--------|-----|-----|-----|
| YELLOW | YELLOW | RED | RED | RED |
|--------|--------|-----|-----|-----|

Keating, C., Sousa-Poza, A., Kovacic, S., 2008. "System of Systems Engineering: An Emerging Multidiscipline", *Int. J. System of Systems Engineering*, Vol. 1, Nos. 1/2, pp. 1-17.

|        |        |     |     |     |
|--------|--------|-----|-----|-----|
| YELLOW | YELLOW | RED | RED | RED |
|--------|--------|-----|-----|-----|

Keeney, R. L., Raiffa, H., 1976. *Decisions with Multiple Objectives Preferences and Value Tradeoffs*, John Wiley & Sons, New York, NY.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Keeney, R. L., 1992. *Value-Focused Thinking A Path to Creative Decision Making*, Harvard University Press, Cambridge, Massachusetts.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Kirkwood, C. W., 1997. *Strategic Decision Making: Multiobjective Decision Analysis With Spreadsheets*, California, Duxbury Press.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Krantz, D. H., Luce, R. D., Suppes, P., Tversky, A., 1971. *Foundations of Measurement, Additive and Polynomial Representations*, Volume 1., New York, Academic Press, Dover Publications.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Leontief, W. W., 1966. *Input-Output Economics*, Oxford University Press, New York, NY.

|     |     |     |        |     |
|-----|-----|-----|--------|-----|
| RED | RED | RED | YELLOW | RED |
|-----|-----|-----|--------|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Lian, C., Santos, J. R., Haimes, Y. Y., 2007. "Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors", *Risk Analysis*, Vol. 27, No. 4.

|        |        |     |       |     |
|--------|--------|-----|-------|-----|
| YELLOW | YELLOW | RED | GREEN | RED |
|--------|--------|-----|-------|-----|

Malczewski, J., 1999. *GIS and Multicriteria Decision Analysis*, John Wiley & Sons, New York, NY.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Mariampolski, H., 2001. *Qualitative Market Research: A Comprehensive Guide*, Sage University Press, Thousand Oaks, California.

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
| RED | RED | RED | RED | RED |
|-----|-----|-----|-----|-----|

MITRE: 2007. "Evolving Systems Engineering", © 2007, The MITRE Corporation, All Rights Reserved, Distribution Unlimited, Case Number 07-1112.

|       |        |        |     |     |
|-------|--------|--------|-----|-----|
| GREEN | YELLOW | YELLOW | RED | RED |
|-------|--------|--------|-----|-----|

Moynihan, R. A., Reining, R. C., Salamone, P. P., Schmidt, B. K., 2008. "Enterprise Scale Portfolio Analysis at the National Oceanic and Atmospheric Administration (NOAA)", *Systems Engineering*, International Council on Systems Engineering (INCOSE), 11 September 2008, © 2008 Wiley Periodicals, Inc.; [www3.interscience.wiley.com/journal/121403613/references](http://www3.interscience.wiley.com/journal/121403613/references).

|       |        |        |     |     |
|-------|--------|--------|-----|-----|
| GREEN | YELLOW | YELLOW | RED | RED |
|-------|--------|--------|-----|-----|

Murphy, C., Gardoni, P., 2006. "The Role of Society in Engineering Risk Analysis: A Capabilities-Based Approach", *Risk Analysis*, Vol. 26, No. 4.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Nau, R. F., 2002. "de Finetti Was Right: Probability Does Not Exist", *Theory and Decision* 51: 89-124, 2001, ©2002, Kluwer Academic Publishers.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

National Transportation Safety Board, 2007. Public Meeting, 10 July 2007; "Highway Accident Report: Ceiling Collapse in the Interstate 90 Connector Tunnel", Boston, Massachusetts, NTSB/HAR-07/02.

|    |    |    |    |    |
|----|----|----|----|----|
| NA | NA | NA | NA | NA |
|----|----|----|----|----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Office of the Secretary of Defense (OSD), 2005: *Net-Centric Operational Environment Joint Integrating Concept*, Version 1.0, Joint Chiefs of Staff, 31 October 2005, Joint Staff, Washington, D.C. 20318-6000; [www.dod.mil/cio-nii/docs/netcentric\\_jic.pdf](http://www.dod.mil/cio-nii/docs/netcentric_jic.pdf).

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Pinto, C. A., Arora, A., Hall, D., Ramsey, D., Telang, R., 2004. "Measuring the Risk-Based Value of IT Security Solutions", *IEEE IT Professional*, v.6 no.6, pp. 35-42.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Pinto, C. A., Arora, A., Hall, D., Schmitz, E., 2006. "Challenges to Sustainable Risk Management: Case Example in Information Network Security", *Engineering Management Journal*, v.18, no.1, pp. 17-23.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Pratt, J. W., 1965. "Risk Aversion in the Small and in the Large", *Econometrica*, Vol. 32.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Ramsey, F. P. (author), Mellor, D. H. (editor), 1990. "F. P. Ramsey: Philosophical Papers", Cambridge University Press.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Rebovich, G., Jr., 2007. "Enterprise the Enterprise", The MITRE Corporation; [www.mitre.org/work/tech\\_papers/tech\\_papers\\_07/07\\_0434/07\\_0434.pdf](http://www.mitre.org/work/tech_papers/tech_papers_07/07_0434/07_0434.pdf).

|       |        |        |     |     |
|-------|--------|--------|-----|-----|
| GREEN | YELLOW | YELLOW | RED | RED |
|-------|--------|--------|-----|-----|

Rebovich, G., Jr., 2005. "Enterprise Systems Engineering Theory and Practice, Volume 2, Systems Thinking for the Enterprise New and Emerging Perspectives", The MITRE Corporation; [www.mitre.org/work/tech\\_papers/tech\\_papers\\_06/05\\_1483/05\\_1483.pdf](http://www.mitre.org/work/tech_papers/tech_papers_06/05_1483/05_1483.pdf).

|       |        |     |     |     |
|-------|--------|-----|-----|-----|
| GREEN | YELLOW | RED | RED | RED |
|-------|--------|-----|-----|-----|

Reilly, J., Brown, J., 2004. "Management and Control of Cost and Risk for Tunneling and Infrastructure Projects", *Proc. International Tunneling Conference*, Singapore.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

Rescher, N., 2006. *Philosophical Dialectics: An Essay on Metaphilosophy*, SUNY Press, Albany, New York.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Rittel, H., 1972. "On the Planning Crisis: Systems Analysis of the First and Second Generations" The Institute of Urban and Regional Development, Reprint No. 107, University of California, Berkeley.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

Santos, J. R., Haimes, Y. Y., 2004. "Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures", *Risk Analysis*, Vol. 24, No. 6.

|        |        |     |       |     |
|--------|--------|-----|-------|-----|
| YELLOW | YELLOW | RED | GREEN | RED |
|--------|--------|-----|-------|-----|

Santos, J. R., Haimes, Y. Y., Lian, C., 2007. "A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies", *Risk Analysis*, Vol. 27, No. 5.

|        |        |     |       |     |
|--------|--------|-----|-------|-----|
| YELLOW | YELLOW | RED | GREEN | RED |
|--------|--------|-----|-------|-----|

Savage, L. J., 1954. *The Foundations of Statistics*, John Wiley & Sons, New York, NY.

|        |     |     |     |     |
|--------|-----|-----|-----|-----|
| YELLOW | RED | RED | RED | RED |
|--------|-----|-----|-----|-----|

Shanteau, J., Weiss, D. J., Thomas, R., Pounds, J., 2001. "Performance-based Assessment of Expertise: How to Decide if Someone is an Expert or Not", *European Journal of Operations Research*, 136, 253-263.

|     |     |     |     |     |
|-----|-----|-----|-----|-----|
| RED | RED | RED | RED | RED |
|-----|-----|-----|-----|-----|

Stevens, S. S., 1946. "On the Theory of Scales of Measurement" *Science*, vol. 103, pp. 677-680.

|     |        |        |     |     |
|-----|--------|--------|-----|-----|
| RED | YELLOW | YELLOW | RED | RED |
|-----|--------|--------|-----|-----|

von Bertalanffy, L., 1968. *General Systems Theory, Foundations, Development, Applications*, University of Alberta, Edmonton, Canada, published by George Braziller, One Park Avenue, New York, New York, 10016.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (continued)

| Literature Assessment | Problem Area 1 | Problem Area 2 | Problem Area 3 | Problem Area 4 | Problem Area 5 |
|-----------------------|----------------|----------------|----------------|----------------|----------------|
|-----------------------|----------------|----------------|----------------|----------------|----------------|

von Neumann J., Morgenstern O., 1944. *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, New Jersey 08540.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

von Winterfeldt D., and Edwards, W., 1986. *Decision Analysis and Behavioral Research*, Cambridge University Press, Cambridge, United Kingdom.

|        |        |        |     |     |
|--------|--------|--------|-----|-----|
| YELLOW | YELLOW | YELLOW | RED | RED |
|--------|--------|--------|-----|-----|

White, B. E., 2006. "Fostering Intra-Organizational Communication of Enterprise Systems Engineering Practices", The MITRE Corporation, National Defense Industrial Association (NDIA), 9th Annual Systems Engineering Conference, October 23-26, 2006, Hyatt Regency Islandia, San Diego California.

|        |        |     |     |     |
|--------|--------|-----|-----|-----|
| YELLOW | YELLOW | RED | RED | RED |
|--------|--------|-----|-----|-----|

Table 25. Literature Assessment Relative to Research Problem Areas (concluded)

## APPENDIX D

### FDNA AND THE HILBERT MATRIX

#### THE HILBERT MATRIX

The Hilbert matrix is a symmetric matrix given by  $H_{ij}$ , where

$$H_{ij} = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \dots \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \dots \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Elements of a Hilbert matrix are fractions that take the form

$$h_{ij} = \frac{1}{i+j-1}$$

A Hilbert matrix has a number of interesting properties. These include the following:

- The inverse  $H_{ij}^{-1}$  exists in closed form and all elements of  $H_{ij}^{-1}$  are integers.
- Although the inverse of a Hilbert matrix theoretically exists, determining  $H_{ij}^{-1}$  becomes computationally intractable even for relatively small  $n$ .
- The determinant of an  $n \times n$  Hilbert matrix rapidly approaches zero with increasing  $n$ . This is illustrated in Figure 91 for a Hilbert matrix up to dimension  $10 \times 10$ .

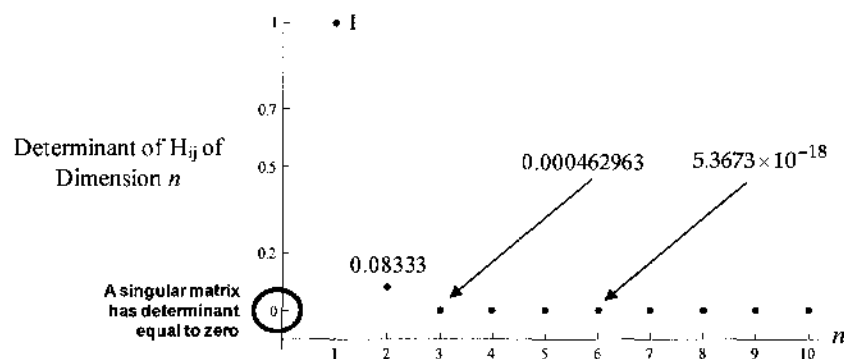


Figure 91. The Determinant of a Hilbert Matrix

\* As  $n$  increases, the elements of  $H_{ij}^{-1}$  become integers of extreme magnitudes. In a  $6 \times 6$  Hilbert matrix, the maximum element in  $H_{ij}^{-1}$  is 4,410,000. The minimum element is -3,969,000. These values occur at  $H_{55}^{-1}$  and  $H_{54}^{-1}$ , respectively. A dramatic change occurs in a  $10 \times 10$  Hilbert matrix. Here, the maximum element in  $H_{ij}^{-1}$  is 3,480,673,996,800. The minimum element is -3,363,975,014,400. These values occur at  $H_{77}^{-1}$  and  $H_{87}^{-1}$ , respectively.



- The solution to the linear system  $H_{ij}X = B$  becomes rapidly unstable with each unit increase in the number of equations in the system. For example, solutions to  $H_{ij}X = B$  evidence instability when  $H_{ij}$  is only a  $3 \times 3$  matrix.
- The above occurs because the Hilbert matrix is badly ill-conditioned. An ill-conditioned matrix  $A$  signals that solutions to the linear system  $AX = B$  may be highly sensitive to small changes in the elements of  $A$  or in the elements of  $B$ .

As discussed in Chapter V, an index known as the *condition number* measures the degree a matrix is ill-conditioned. The condition number is always greater than or equal to one. The farther from one the condition number of  $A$ , the greater the instability of solutions to the linear system  $AX = B$ . A matrix is singular if its condition number is infinite.

A linear system of  $n$  equations with coefficients from a Hilbert matrix of dimension  $n = 2, 3, 4, 5$ , and  $6$  has condition numbers  $27, 748, 28375, 943656$ , and  $29070279$ , respectively. Thus, linear systems of equations with Hilbert coefficient matrices quickly become unstable with each unit increase in the number of equations in the system.

### FDNA AND THE HILBERT MATRIX

If a dependency problem involves finding the solution to the linear system  $H_{ij}X = B$ , then doing so is very problematic if  $H_{ij}$  is a Hilbert matrix. For the reasons stated above, solutions to such a system are not only unstable but finding them also becomes computationally unwieldy for even relatively small  $n$ .

However, FDNA can generate solutions to dependency problems between nodes with features characterized by Hilbert matrices of any size  $n$ . Figure 92 illustrates an FDNA dependency problem characterized by a Hilbert matrix. This problem is Example 5.22 but with strength of dependency values that reflect the elements of a  $3 \times 3$  Hilbert matrix.

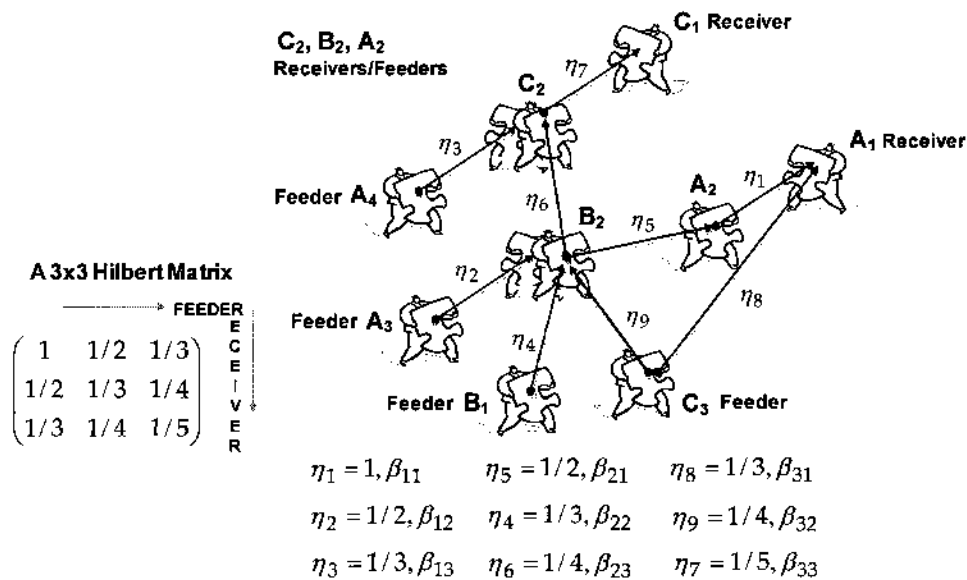


Figure 92. An FDNA Graph With a Hilbert Matrix

FDNA equations are algebraically formulated by a composition of functional dependency relationships across a mathematical graph. This composition of functions strategy avoids matrix algebra and linear system solution issues that can arise in some types of dependency problems. Table 26 presents an FDNA operability analysis of the dependency problem given in Figure 92.

| FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA)   |        |               |       |                                    |       |               |      |
|---|--------|---------------|-------|------------------------------------|-------|---------------|------|
| An FDNA Operability Analysis of Example 5.22 With a Hilbert SOD Matrix                      |        |               |       |                                    |       |               |      |
| INPUT: $\alpha_{ij}$ Strength of Dependency (SOD)   |        |               |       | $\alpha_{ij}$ Within Range ... T/F |       |               |      |
| $\alpha_{11}$   | 1.00   | $\alpha_{21}$ | 0.50  | $\alpha_{11}$                      | TRUE  | $\alpha_{21}$ | TRUE |
| $\alpha_{12}$   | 0.50   | $\alpha_{22}$ | 0.33  | $\alpha_{12}$                      | TRUE  | $\alpha_{22}$ | TRUE |
| $\alpha_{13}$   | 0.33   | $\alpha_{23}$ | 0.25  | $\alpha_{13}$                      | TRUE  | $\alpha_{23}$ | TRUE |
| Suppose SOD values come from a Hilbert Matrix   |        | $\alpha_{31}$ | 0.33  |                                    |       | $\alpha_{31}$ | TRUE |
|   |        | $\alpha_{32}$ | 0.25  |                                    |       | $\alpha_{32}$ | TRUE |
|   |        | $\alpha_{33}$ | 0.20  |                                    |       | $\alpha_{33}$ | TRUE |
| INPUT: $\beta_{ij}$ Criticality of Dependency (COD)   |        |               |       | $\beta_{ij}$ Within Range ... T/F  |       |               |      |
| $\beta_{11}$  | 0.00   | $\beta_{21}$  | 50.00 | $\beta_{11}$                       | TRUE  | $\beta_{21}$  | TRUE |
| $\beta_{12}$  | 50.00  | $\beta_{22}$  | 66.67 | $\beta_{12}$                       | TRUE  | $\beta_{22}$  | TRUE |
| $\beta_{13}$  | 66.67  | $\beta_{23}$  | 75.00 | $\beta_{13}$                       | TRUE  | $\beta_{23}$  | TRUE |
| Suppose we have these COD values  |        | $\beta_{31}$  | 66.67 |                                    |       | $\beta_{31}$  | TRUE |
|   |        | $\beta_{32}$  | 75.00 |                                    |       | $\beta_{32}$  | TRUE |
|   |        | $\beta_{33}$  | 80.00 |                                    |       | $\beta_{33}$  | TRUE |
| Assume equally weighted components in each constituent node S1, S2, and S3                  |        |               |       |                                    |       |               |      |
| If the operability levels of these components of S1, S2, and S3 at time t1, t2, and t3 are: |        |               |       |                                    |       |               |      |
| Time t1   |        | Time t2       |       | Time t3                            |       |               |      |
| A4  | 100    | A4            | 75    | A4                                 | 50    |               |      |
| A3  | 100    | A3            | 75    | A3                                 | 50    |               |      |
| B1  | 100    | B1            | 75    | B1                                 | 50    |               |      |
| C3  | 100    | C3            | 75    | C3                                 | 50    |               |      |
| OUTPUT: Then these nodes are functioning at these operability levels...                     |        |               |       |                                    |       |               |      |
| S1  | 100.00 | S1            | 85.81 | S1                                 | 71.61 |               |      |
| S2  | 100.00 | S2            | 82.99 | S2                                 | 65.97 |               |      |
| S3  | 100.00 | S3            | 89.55 | S3                                 | 79.10 |               |      |
| C2  | 100.00 | C2            | 94.70 | C2                                 | 89.41 |               |      |
| C1  | 100.00 | C1            | 98.94 | C1                                 | 97.88 |               |      |
| B2  | 100.00 | B2            | 90.97 | B2                                 | 81.94 |               |      |
| A2  | 100.00 | A2            | 95.49 | A2                                 | 90.97 |               |      |
| A1  | 100.00 | A1            | 97.74 | A1                                 | 95.49 |               |      |

Table 26. An FDNA Operability Analysis Involving a Hilbert Matrix

## APPENDIX E

### FDNA AND THE MARKOV MATRIX

#### THE MARKOV MATRIX

The Markov matrix is known as a *stochastic* or probability matrix. It is a square matrix whose elements  $m_{ij}$  are non-negative real numbers in the interval  $0 \leq m_{ij} \leq 1$ . In a Markov matrix, the row or column vectors represent probability distributions of discrete events. As such, the elements in each row or the elements in each column sum to one. A Markov matrix is called *doubly stochastic* if its row and column sums are both one.

The stochastic aspects of a Markov matrix has interesting implications in Leontief input-output economics. As discussed in Chapter V, Leontief's input-output model captures relationships between dependent sectors (or industries) of an economy with respect to consumption and demand. Leontief's fundamental equation is as follows:

$$X - AX = D$$

where  $X$  is the total output needed to meet consumer demand  $D$  given input-output matrix  $A$ .

A Leontief input-output model is *closed* when its  $A$ -matrix has Markov characteristics. Leontief argues a closed economy is one that consumes everything it produces. It cannot meet any outside consumer demand. Hence, the fundamental input-output equation  $X - AX = D$  becomes

$$X - AX = D = 0 \Rightarrow AX = X \Rightarrow (I - A)X = 0$$

A closed Leontief model means consumption is equal to production. The economy is balanced. It is in equilibrium. When consumption is equal to production, the elements in each column of  $A$  sum to one. The following theorem is now introduced.

**Brauer-Solow Theorem:** If  $A$  is a square, non-negative, matrix then if each row sum of  $A$  is less than one, or each column sum of  $A$  is less than one, then the Leontief matrix  $(I - A)$  is invertible, non-negative, and meets the Hawkins-Simon condition\*.

Thus, an economy that consumes everything it produces is one where the Brauer-Solow theorem is **not met** since

$$\sum_{i=1}^n m_{ij} = 1 \text{ for } j = 1, \dots, n \text{ or } \sum_{j=1}^n m_{ij} = 1 \text{ for } i = 1, \dots, n$$

in this case. Finally, it can be shown if  $A$  is a Markov matrix then the Leontief matrix  $(I - A)$  is not invertible (it is singular) and the largest eigenvalue of  $A$  will always equal one.

---

\* Refer to Chapter V, Definition 5.11.

### FDNA AND THE MARKOV MATRIX

If a dependency problem involves finding the solution to a Leontief system with a Markov  $A$ -matrix, then doing so is not possible for the reasons described above. However, FDNA can generate solutions to dependency problems between nodes with features characterized by Markov matrices of any size  $n$ .

Figure 93 illustrates an FDNA dependency problem characterized by a Markov matrix. This problem is Example 5.22 but with strength of dependency values that reflect the elements of a  $3 \times 3$  Markov matrix.

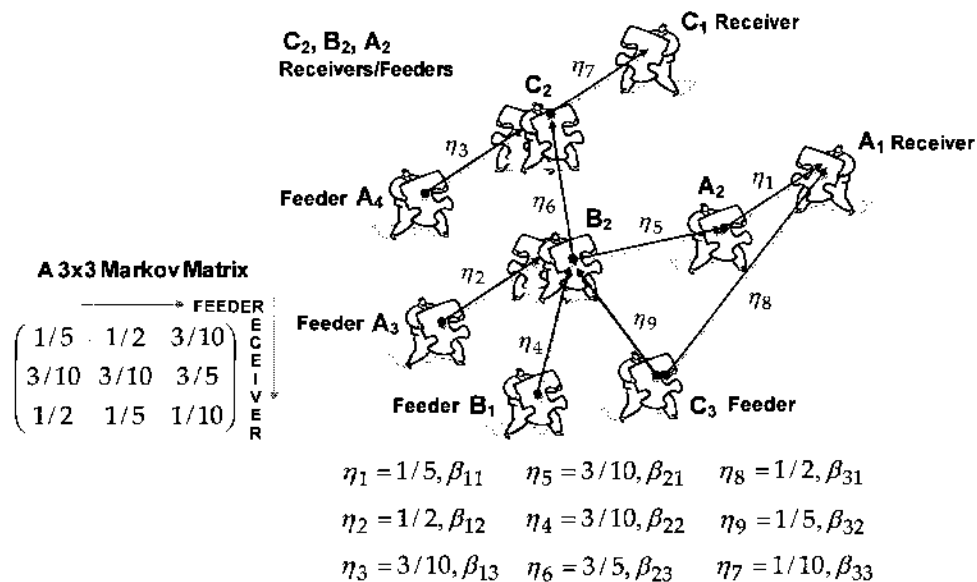


Figure 93. An FDNA Graph With a Markov Matrix

As mentioned previously, FDNA equations are algebraically formulated by a composition of functional dependency relationships across a mathematical graph. This composition of functions strategy avoids matrix algebra and linear system solution issues that can arise in some types of dependency problems. Table 27 presents an FDNA operability analysis of the dependency problem given in Figure 93.

| FUNCTIONAL DEPENDENCY NETWORK ANALYSIS (FDNA)   |        |               |       |                                    |       |               |      |
|---|--------|---------------|-------|------------------------------------|-------|---------------|------|
| An FDNA Operability Analysis of Example 5.22 With a Markov SOD Matrix                       |        |               |       |                                    |       |               |      |
| INPUT: $\alpha_{ij}$ Strength of Dependency (SOD)   |        |               |       | $\alpha_{ij}$ Within Range ... T/F |       |               |      |
| $\alpha_{11}$   | 0.20   | $\alpha_{21}$ | 0.30  | $\alpha_{11}$                      | TRUE  | $\alpha_{21}$ | TRUE |
| $\alpha_{12}$   | 0.50   | $\alpha_{22}$ | 0.30  | $\alpha_{12}$                      | TRUE  | $\alpha_{22}$ | TRUE |
| $\alpha_{13}$   | 0.30   | $\alpha_{23}$ | 0.60  | $\alpha_{13}$                      | TRUE  | $\alpha_{23}$ | TRUE |
| Suppose SOD values come from a Markov Matrix  |        | $\alpha_{31}$ | 0.50  |                                    |       | $\alpha_{31}$ | TRUE |
|   |        | $\alpha_{32}$ | 0.20  |                                    |       | $\alpha_{32}$ | TRUE |
|   |        | $\alpha_{33}$ | 0.10  |                                    |       | $\alpha_{33}$ | TRUE |
| INPUT: $\beta_{ij}$ Criticality of Dependency (COD)   |        |               |       | $\beta_{ij}$ Within Range ... T/F  |       |               |      |
| $\beta_{11}$  | 80.00  | $\beta_{21}$  | 70.00 | $\beta_{11}$                       | TRUE  | $\beta_{21}$  | TRUE |
| $\beta_{12}$  | 50.00  | $\beta_{22}$  | 70.00 | $\beta_{12}$                       | TRUE  | $\beta_{22}$  | TRUE |
| $\beta_{13}$  | 70.00  | $\beta_{23}$  | 40.00 | $\beta_{13}$                       | TRUE  | $\beta_{23}$  | TRUE |
| Suppose we have these COD values  |        | $\beta_{31}$  | 50.00 |                                    |       | $\beta_{31}$  | TRUE |
|   |        | $\beta_{32}$  | 80.00 |                                    |       | $\beta_{32}$  | TRUE |
|   |        | $\beta_{33}$  | 90.00 |                                    |       | $\beta_{33}$  | TRUE |
| Assume equally weighted components in each constituent node S1, S2, and S3                  |        |               |       |                                    |       |               |      |
| If the operability levels of these components of S1, S2, and S3 at time t1, t2, and t3 are: |        |               |       |                                    |       |               |      |
| Time t1   |        | Time t2       |       | Time t3                            |       |               |      |
| A4  | 100    | A4            | 75    | A4                                 | 50    |               |      |
| A3  | 100    | A3            | 75    | A3                                 | 50    |               |      |
| B1  | 100    | B1            | 75    | B1                                 | 50    |               |      |
| C3  | 100    | C3            | 75    | C3                                 | 50    |               |      |
| OUTPUT: Then these nodes are functioning at these operability levels...                     |        |               |       |                                    |       |               |      |
| S1  | 100.00 | S1            | 86.69 | S1                                 | 73.38 |               |      |
| S2  | 100.00 | S2            | 83.33 | S2                                 | 66.67 |               |      |
| S3  | 100.00 | S3            | 89.38 | S3                                 | 78.75 |               |      |
| C2  | 100.00 | C2            | 93.75 | C2                                 | 87.50 |               |      |
| C1  | 100.00 | C1            | 99.38 | C1                                 | 98.75 |               |      |
| B2  | 100.00 | B2            | 91.67 | B2                                 | 83.33 |               |      |
| A2  | 100.00 | A2            | 97.50 | A2                                 | 95.00 |               |      |
| A1  | 100.00 | A1            | 99.25 | A1                                 | 98.50 |               |      |

Table 27. An FDNA Operability Analysis Involving a Markov Matrix

## VITA

### Paul Raphael Garvey

Frank Batten College of Engineering and Technology  
Department of Engineering Management and Systems Engineering  
241 Kaufman Hall, Old Dominion University, Norfolk, VA 23529

Paul Raphael Garvey is Chief Scientist and a Director for the Center for Acquisition and Systems Analysis – a Division at The MITRE Corporation. Dr. Garvey is internationally recognized and widely published in systems cost analysis, cost uncertainty analysis, and in the application of decision analytic methods to problems in engineering systems risk analysis. He lectures frequently on these and related topics to government agencies and academic institutions in the United States and abroad.

Dr. Garvey authored three textbooks published by Chapman-Hall/CRC Press, a Taylor & Francis Group. They are *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective* (2000), *Analytical Methods for Risk Management: A Systems Engineering Perspective* (2008), and *Advanced Risk Analysis in Engineering Enterprise Systems* (2011). The latter work is co-authored with Prof. C. Ariel Pinto of Old Dominion University.

Dr. Garvey has also written over two-dozen technical articles that have appeared in books published by the IEEE Computer Society Press, Springer-Verlag's Economics and Mathematical Systems series, and John Wiley & Son's *Encyclopedia of Electrical and Electronics Engineering*. In addition, his articles have appeared in professional refereed journals such as *IEEE Software*, *Military Operations Research*, *The Journal of Cost Analysis*, and the *Acquisition Review Quarterly*, published by the Defense Acquisition University. Dr. Garvey is a four-time best paper award recipient from the United States Department of Defense Cost Analysis Symposium.

#### Education

Boston College, A.B., Mathematics, College of Arts & Sciences, College Honors Program, *cum laude*, May, 1978.

Northeastern University, M.Sc., Applied Mathematics, Graduate School of Arts & Sciences, June, 1980.

Old Dominion University, Ph.D., Engineering Management, Department of Engineering Management and Systems Engineering, Frank Batten College of Engineering and Technology, August, 2009.

Elected, Phi Kappa Phi National Honor Society