RELIABILITY, MULTI-STATE FAILURES AND SURVIVABILITY OF SPACECRAFT AND SPACE-BASED NETWORKS

A Dissertation
Presented to
The Academic Faculty

By

Jean-François Castet

In Partial Fulfillment
Of the Requirements for the Degree
Doctor of Philosophy in the
School of Aerospace Engineering

Georgia Institute of Technology

December 2012

RELIABILITY, MULTI-STATE FAILURES AND SURVIVABILITY OF SPACECRAFT AND SPACE-BASED NETWORKS

Approved by:

Dr. Joseph H. Saleh, Advisor
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Eric M. Feron
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Vitali V. Volovoi
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Paul Kvam
School of Industrial and Systems Engineering
Georgia Institute of Technology

Mr. John C. Day
Technical Group Supervisor, Autonomy and Fault Protection
Jet Propulsion Laboratory

Date Approved: October 19, 2012

To my parents, grand-mother and So Young

ACKNOWLEDGEMENTS

First and foremost, I wish to thank my advisor, Dr. Joseph H. Saleh for his guidance and constant support through this difficult but enriching endeavor. Dr. Saleh was always available for our research discussions, and offered pointed and extremely helpful advice and guidance. Without his support, this dissertation would not have seen the light of day. In addition, Dr. Saleh has a brilliant mind and wonderful work ethics I truly admire. I am also very grateful for all the opportunities he has given me, such as presenting my work at various conferences or writing with him several journal papers. He also gave me the exceptional opportunity to co-author a book with him, and I am deeply grateful and proud of this accomplishment. In addition to our fruitful research interactions, I got the chance to discuss with him about a wide range of subjects, and his depth and variety of knowledge never cease to amaze me.

I would also like to extend my thanks to all the members of my Ph.D. committee: Dr. Eric M. Feron, Dr. Vitali V. Volovoi, Dr. Paul Kvam and Mr. John C. Day. I thank them for the thought-provoking discussions and expertise that allowed this dissertation to come to fruition.

I would like to express my gratitude to Dr. Jeff Jagoda for his essential support during these years. Without his help and the teaching assistantships he kindly offered me, I would not have been able to pursue this program.

My years as a graduate student would not have been as fun and interesting without my fellow labmates in the Space Systems Design Lab, particularly Greg Dubos, Jarret Lafleur, Joy Brathwaite, and Loïc Brevault for their willingness to discuss research ideas, but also for the less serious sides of student life. I also want to thank other graduate students in the lab, Zarrin Chua, Grégory Lantoine, Nitin Arora, Brad Steinfeldt, and Francesca Favaro. A particular thank to Jenna Stahl, who help smooth the rough edges of my English when I first arrived in the US, and Gi Yun Chung, who had to put up with me during lunch for all these years. I also would like to thank my dear friends in France: Hervé Kelmant, Jean-François and Mayalen Sallaberry, Florian Duport, and all the members of the “Bouliste” from SUPAERO for their support even from far, far away.

Finally, I want to thank So Young Kim for her irreplaceable support, encouragement and understanding. My deepest gratitude goes to my parents Pierre and Anne-Marie and my grand-mother Louise for their unconditional love and enduring support of my decision of continuing my studies. Without them, I would not have gone as far as I am today. I also want to extend this to my entire family and family friends for their unwavering support for my studies abroad.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

In Appendices:

LIST OF SYMBOLS

$.^{F}$	quantity related to the failed state
$.^{m}$	quantity related to the minor degradation state
$.^{M}$	quantity related to the major degradation state
$.^{MF}$	quantity related to the major–failed state (or severe degradation state)
$.^{mMF}$	quantity related to minor–major–failed state (or degraded state)
A_l	adjacency matrix of layer l
C	interlayer matrix
$\|E\|$	cardinality of set E (number of elements in E)
E_k	set of interlayer edges representing the kill effect
E_l	set of edges (or links) in G_l
E_L	set of functionally redundant layers
E_p	set of interlayer edges representing the precursor effect
f	mapping function
G_l	graph of layer l
H_l	matrix in layer l in precursor effect propagation
$\mathbf{k_1}$	killer vector for the kill effect
$\mathbf{k_2}$	killer vector for the precursor effect
L	number of layers in an IMLN
$\mathbf{m}_l$	column vector derived from H_l
$\mathbf{N}$	set of natural numbers (non-negative integers)
$\mathbf{N}^{*}$	set of natural numbers excluding zero

$\mathbf{N}_n^*$	set of integers from 1 to n
N	network
n	total number of vertices in a network N
n_{A_l}	number of elements in adjacency matrix A_l
n_C	number of elements in interlayer matrix C
n_{E_l}	number of edges in layer l
n_i	number of item functioning right before $t_{(i)}$ (Part 1)
n_l	total number of vertices in G_l (Part 2)
n_S	number of spacecraft in the network N
$\overline{P}$	sample probability mean
P_0	probability associated with an architecture with a perfect networkable subsystem
P_F	probability of being in a failed state
$\hat{p}_i$	conditional probability of surviving an infinitesimal time after $t_{(i)}$
P_{ij}	conditional probability of transitioning from state i to state j
$\hat{P}_{ij}$	estimate of P_{ij}
P_m	probability of being in a minor degradation state
P_M	probability of being in a major degradation state
P_{MF}	probability of being in a major–failed state (or severe degradation state)
P_{mMF}	probability of being in a minor–major–failed state (or degraded state)
P_P	probability associated with the payload subsystem
P_S	probability associated with the supporting subsystems

$P_{S_{v1}}$	probability of being in a virtual state 1
$P_{S_{v2}}$	probability of being in a virtual state 2
$P_{\mathrm{U}i}^{F}$	probability of failure of the wireless unit *i*
$R(t)$	reliability, or survivor function
$\widehat{R}(t)$	Kaplan-Meier estimated of the reliability function
R^2	coefficient of determination in a regression analysis
r_j	percent contribution of subsystem *j* to the probability of failure of the spacecraft
s	sample standard deviation
S_i	State *i* in the transition diagram
$t_{(i)}$	i^{th} failure time
T_F	time to failure
$T_{F,\mathrm{vertex}\ i}$	time to failure of vertex *i*
$T_{F,\mathrm{edge}\ j\to i}$	time to failure of edge between vertex *j* and vertex *i*
T_{ij}	transition between the state *i* and state *j*
T_m	time to minor degradation state
T_M	time to major degradation state
T_{MF}	time to major–failed state (or severe degradation state)
T_{mMF}	time to minor–major–failed state (or degraded state)
$T_{S_{v1}}$	time to virtual state 1
$T_{S_{v2}}$	time to virtual state 2
T_U	time to unavailability

T_U^k time to unavailability due to the kill effect

T_U^m minimum time to unavailability after the the kill effect

T_U^p time to unavailability due to the precursor effect

T_U^r time to unavailability considering the functional redundancy

$\mathbf{v_1}$ victim vector for the kill effect

$\mathbf{v_2}$ victim vector for the precursor effect

V_i set of vertices (or nodes) in G_i

α_F probability of failure of the networkable subsystem

α_m probability of being in a minor degradation state for the networkable subsystem

α_M probability of being in a major degradation state for the networkable subsystem

α_{MF} probability of being in a major–failed state for the networkable subsystem

α_{mMF} probability of being in a minor–major–failed degradation state for the networkable subsystem

$\alpha_{\cdot}^{15}$ value of $\alpha_{\cdot}$ at t = 15 years (*F*, *m*, *M*, *MF*, *mMF*)

α_j weighting coefficient in mixture distribution function

β Weibull shape parameter

γ_F relative failure growth

Δ net gain of the network

Δ_0 maximum net gain of the network

ΔP performance degradation

η network efficiency

θ	Weibull scale parameter
λ	exponential rate parameter
μ	exponential mean parameter
υ_F	probability of failure of the wireless link

LIST OF ABBREVIATIONS

AOCS	Attitude and Orbit Control Susbsytem
ASAT	Anti-Satellite Weapon
Battery	Battery / Cell subsystem
Beam	Beam / Antenna Operation / Deployment subsystem
CI	Confidence Interval
CP	Control Processor subsystem
DH	Data Handling subsystem
DoD	US Department of Defense
ED	Electrical Distribution subsystem
EPS	Electrical Power Subsystem
GPS	Global Positioning System
Gyro	Gyro / Sensor / Reaction Wheel subsystem
iid	Independent and identically distributed
IMLN	Interdependent Multi-Layer Network
MC	Monte Carlo, or Markov Chain, depending on context
Mechanisms	Mechanisms / Structures / Thermal subsystem
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MLE	Maximum Likelihood Estimation
Payload	Payload Instrument / Amplifier / On-board Data / Computer / Transponder subsystem

RAM	Random-Access Memory
S/C	Spacecraft
SAD	Solar Array Deployment subsystem
SAO	Solar Array Operating subsystem
SBN	Space-Based Network
SPN	Stochastic Petri Net
SubS*i*	Subsystem State *i*
SysS*i*	System State *i*
Thruster	Thruster / Fuel subsystem
TTC	Telemetry, Tracking and Command subsystem
US	United States

SUMMARY

Spacecraft fulfill a myriad of critical functions on orbit, from defense and intelligence to science, navigation, and telecommunication. Spacecraft can also cost several hundred millions of dollars to design and launch, and given that physical access for maintenance remains difficult if not impossible to date, designing high reliability and survivability into these systems is an engineering and financial imperative.

While reliability is recognized as an essential attribute for spacecraft, little analysis has been done pertaining to actual field reliability of spacecraft and their subsystems. This thesis fills the gap in the current understanding of spacecraft failure behavior on orbit through extensive statistical analysis and modeling of anomaly and failure data, and then leverages these results to develop a theoretical basis and algorithmic tools for the analysis of survivability of spacecraft and space-based networks.

This thesis consists of two parts. The first part provides extensive statistical results of recent on-orbit anomaly and failure data of Earth-orbiting spacecraft. Nonparametric reliability results are derived, and parametric models, including Weibull and mixture distributions, of spacecraft and spacecraft subsystems are developed. These analyses are then extended to multi-state failures, accounting for and modeling spacecraft subsystems' degraded states and partial failures. Culprit subsystems driving spacecraft unreliability are identified, including major contributors to infant mortality and anomaly, and it is suggested that these would benefit most from a revision of their current testing protocol

and burn-in procedures. The second part builds on these results to develop a novel theoretical basis and algorithmic tools for the analysis of survivability of spacecraft and space-based networks. Space-based networks (SBNs) allow the sharing of on-orbit resources, such as data storage, processing, and downlink. Spacecraft in SBNs can have different subsystem composition and functionality, thus resulting in node heterogeneity (each spacecraft being a node in the network). Current tools for network survivability analysis assume homogeneous nodes, and as such, they are not suited for the analysis of space-based networks. This thesis proposes that heterogeneous networks can be modeled with a new approach termed interdependent multi-layer networks, which is then adapted for their survivability analysis. The multi-layer aspect enables the breakdown of spacecraft according to common functionalities and allows the emergence of homogeneous sub-networks, while the interdependency aspect constrains the network to capture the physical characteristics of spacecraft. Formal characterization of interdependent multi-layer networks, as well as algorithmic tools for the analysis of failure propagation across the network are developed and illustrated with space applications and proof of concepts. The SBN applications considered consist of several networked spacecraft that can tap into other’s Command and Data Handling subsystem (C&DH), in case of degradation or failure of its own, including Telemetry, Tracking and Command, Control Processor or Data Handling sub-subsystems. Results indicate and quantify the incremental survivability improvement of the SBN over the traditional monolith architecture. A trade-space analysis is then conducted using non-descriptive networkable subsystems/technologies to explore survivability characteristics of space-based networks and help guide design choices. The trade studies provide important

insights into design and architectural choices for enhancing survivability of heterogeneous networks in general, and space-based networks in particular. For example, it is shown that such networks shield in priority the system from the most severe failures, and their incremental survivability decreases with decreasing severity of subsystems anomalies at comparable occurrence. Also, network survivability benefits most from increasing number of nodes for networkable subsystems with increasingly problematic failure behavior. The analysis also demonstrates the criticality of the wireless link reliability, and highlights the importance of rooting out infant mortality of this link to enable any survivability improvements for space-based networks.

CHAPTER 1

INTRODUCTION

“*Tempus edax rerum*”
“Time, devourer of all things”

Ovid, AD 8
Metamorphoses, XV, 234

1.1. A Brief Historical Perspective and Motivation

On October 4, 1957, a small beeping spacecraft, Sputnik, heralded the beginning of the Space Age. From this humble start, the space industry grew into an impressive $100+ billion industry. Around 6500 spacecraft were launched in the five decades after Sputnik. And although the launch rate has been highly variable (Hiriart and Saleh, 2010), a rough estimate would set it at present around 80 to 100 spacecraft launched per year. Spacecraft today fulfill a myriad of functions, from Defense and Intelligence missions (early warning, reconnaissance, etc.), to Science missions (Earth observation, interplanetary probes), Communication functions (Direct-To-Home, Fixed Satellite Services, and Mobile Satellite Services) and Navigation services (GPS).

Spacecraft can cost several hundred millions of dollars to design and launch[1], and as such reliability is essential for these systems. More generally, reliability is a critical design attribute for high-value systems operating in remote or inhospitable environments such as spacecraft or sub-sea installations. Since physical access to these assets is difficult or impossible, maintenance cannot be relied upon to compensate for substandard reliability (Rausand and Høyland, 2004). As a result, designing high reliability into these systems is an essential engineering and financial imperative.

By an unexpected accident of history, the official birth of reliability engineering and the onset of the Space Age took place the same year (1957), and **the first part of this dissertation is at the intersection of these two developments by bringing reliability engineering to bear on space systems**. Reliability engineering is founded on several essential ingredients such as probability and statistics, theoretically formalized in the seventeen century by Blaise Pascal and Pierre de Fermat, or the concept of mass production, popularized by Henri Ford but already existing for several years with the use of standardized, interchangeable parts. The idea of the stochastic nature of the time to failure was not immediately accepted by production engineers, but the stark unreliability of the vacuum tube during World War II acted as the catalyst that accelerated the coming of reliability engineering, through studies launched by the US Department of Defense. A more detailed review of the history of reliability engineering can be found in Saleh and Marais (2006) and Saleh and Castet (2011).

[1] Except for micro-satellites, which are typically in the $10 – $50 million range, and on-going efforts are seeking to significantly reduce this price tag. Whether useful functions can be performed on orbit below this range remains to be seen.

In the case of space systems, statistical analysis of actual flight data would provide useful feedback to the space industry, in relation to part selection, redundancy allocation, testing programs, etc. In addition, a better understanding of spacecraft failures, and the determination of the existence of infant mortality among spacecraft subsystems is an important endeavor for the space industry. Indeed, infant mortality can be traced back to design flaws and manufacturing defects, and as such it can be reduced or eliminated through proper equipment testing or burn-in. Robertson and Stoneking (2003) however warn against over-testing parts that could lead to a decrease in the overall subsystem reliability. This raises interesting questions of how to do pre-flight testing, and at what level of integration, of subsystems whose components exhibit different failure behaviors (e.g., infant mortality for some and wear-out failure for others).

In its traditional understanding, reliability analysis considers only two states: operational and failed. Consequently, the system under consideration is only perceived as being in one of these two states. In reality, engineering artifacts can experience partial degradations, and not necessary only catastrophic failures. To account for this progression from fully operational towards complete loss, **multi-state failure analysis** introduces “degraded states”, and thus provides more insights through finer resolution into the degradation behavior of an item. As such, following a reliability analysis of spacecraft subsystems, this dissertation provides a theoretical formalization of multi-state failure analysis and applies it on spacecraft subsystems.

Finally, endogenous failures are a subset of the failures a spacecraft can experience: exogenous failures such as collisions with orbital debris or attacks from anti-satellite

(ASAT) weapons can trigger degradation in functionality, potentially leading to a total loss. This broader picture of failure analysis falls in the realm of **survivability analysis** and is applied to spacecraft and space-based networks (SBNs). SBNs are related to a novel concept recently introduced in the space industry termed fractionation: by physically distributing functions in multiple orbiting modules wirelessly connected to each other, this new architecture allows the sharing of resources on-orbit, such as data processing, data storage, and downlinks.

To summarize, spacecraft and space-based networks, as engineering artifacts, degrade and fail in time; just how they do so, a particular aspect of their relationship with time, is explored in this thesis, and the remainder of this dissertation is organized as follows.

1.2. Outline and Anticipated Contributions

This dissertation is articulated in two parts. The first part is a descriptive analysis of reliability and multi-state failures of spacecraft and spacecraft subsystems based on statistical data analyses (Chapter 2 and Chapter 3). The second part introduces a prescriptive or normative analysis of survivability bearing on spacecraft and space-based networks (Chapter 4 and following). It also brings a theoretical contribution to this thesis by proposing a novel method to represent and analyze networks with node heterogeneity.

Chapter 2 presents a statistical analysis of spacecraft failure data. As mentioned earlier, spacecraft reliability analysis are recognized as important for the space industry, but unfortunately, limited empirical data and statistical analyses of spacecraft reliability exist in the literature. A **brief literature review of early studies of spacecraft failures** is conducted and highlights their limitations. This chapter fills the gap by providing a **formal reliability analysi**s based on a large sample and **nonparametric spacecraft reliability results** are presented. In addition, **parametric analyses** are conducted and single Weibull as well as mixture distribution models are derived. Finally, the statistical failure analysis is extended to **spacecraft subsystems**, and the relative contribution of spacecraft subsystems to the global spacecraft unreliability is examined, **highlighting problematic subsystems that would benefit most from reliability improvements**.

Chapter 3 extends the previous analyses of reliability, in its traditionally binary-state understanding, to account for spacecraft anomalies and failures of various severity. Partial failures constitute a significant portion of anomalous events a spacecraft can experience on-orbit, and as such their analysis is critical to obtain a complete picture of the spacecraft and spacecraft subsystems' failure behavior. This chapter introduces a **formal multi-state failure analysis of spacecraft subsystems**, and **provides practical implications for the space industry**.

Chapter 4 is a turning point in this dissertation as considerations of **survivability analysis** are brought on **spacecraft** and the newly introduced concept of **space-based networks**. Chapter 4 provides a literature review on survivability analysis, as well as on network analysis. A **formal survivability framework** is introduced and limitations of the current network analysis to represent and analyze space-based networks are demonstrated. To overcome these limitations, **a new framework is presented and termed interdependent multi-layer network approach**.

Chapter 5 is devoted to the derivation of the **anomaly and failure propagation for the interdependent multi-layer network approach** introduced in this thesis. Several algorithms are introduced and illustrated with a case study space-based network.

Chapter 6 presents the analyses conducted to **validate** the failure propagation for interdependent multi-layer networks introduced in the previous chapter. This validation procedure is important so that the survivability results can be trusted and properly analyzed. Chapter 6 also evaluate the **precision** of the model results, by comparing them with results obtained with an alternative modeling technique, namely stochastic Petri nets, as well as limited analytical solutions. Finally, Chapter 6 investigates the potential **scalability** of the interdependent multi-layer network modeling.

Chapter 7 puts to use the validated interdependent multi-layer network approach proposed in this dissertation to **derive survivability analysis of selected space-based network architectures**. This chapter then leverages these results to obtain **insights on design and architectural choices for future space systems**.

Finally, Chapter 8 concludes this works and provides several recommendations for future research.

PART 1

STATISTICAL ANALYSIS OF SPACECRAFT RELIABILITY

AND MULTI-STATE FAILURES

CHAPTER 2

RELIABILITY OF SPACECRAFT AND SPACECRAFT SUBSYSTEMS

For space systems, statistical analysis of flight data, in particular of actual on-orbit (field) anomaly and failure data, would provide particularly useful feedback to spacecraft designers. For example, such analyses can help guide parts selection and provide an empirical basis for subsystem redundancy and reliability growth plans. Analyzing spacecraft failure behavior on orbit, and identifying their subsystems' actual reliability profiles, not their reliability requirements—how they actually degrade and fail on-orbit, not how they should or are expected to—can help spacecraft manufacturers prioritize and hone in on problematic subsystems that would benefit most from reliability improvements. Reliability improvements can be achieved through redundancy, increased testing prior to launch, or better design and parts selection, and these efforts would result in a decreased likelihood of spacecraft experiencing failure events. In addition, identifying whether specific spacecraft subsystems experience infant mortality for example would provide a clear opportunity for spacecraft manufacturers and equipment providers to develop burn-in procedures for weeding out early failures in said subsystems.

Statistical analysis of on-orbit failure and spacecraft reliability can also provide important and actionable information to stakeholders other than spacecraft manufacturers. For example spacecraft operators may be particularly interested in the reliability profiles of their on-orbit assets, for planning and risk mitigation purposes, and insurers evidently rely on such analysis and information to set up their policy and insurance premiums.

The importance of statistical analysis of on orbit failure data was recognized early in the advent of the space age. The following subsections provide a brief overview of past spacecraft reliability studies.

2.1. On Spacecraft and Reliability: Early Studies

A few years after the launch of the first spacecraft, statistical analyses of spacecraft reliability and on-orbit failures began to appear. As discussed by Bean and Bloomquist (1968), statistical analyses based on empirical data from spacecraft on-orbit were an essential undertaking for the aerospace industry, for two reasons: gathering data from spacecraft and determining the failure behavior of satellites or satellite subsystems 1) provides feedback to the industry on the performance ("strengths" or "weaknesses") of designed and manufactured parts and components, and allows efficient reliability improvement programs, and 2) allows improving the estimation of "parameters commonly used in reliability predictive techniques" by comparing estimated and observed reliability/failure rates. One of the earliest reliability studies, according to Leventhal *et al*. (1969), was published in 1962, and it analyzed the failure behavior of 16 spacecraft launched before November 1961 (ARINC, 1962). Over the years, similar analyses would be conducted with larger sample sizes or spacecraft population. For example, Bean and Bloomquist (1968) analyzed the failure behavior of 225 spacecraft; Timmins and Heuser (1971), and Timmins (1974; 1975) analyzed the failure behavior of 57 spacecraft; and Hecht and Hecht (1985) and Hecht and Fiorentino (1987; 1988) analyzed the failure behavior of some 300 spacecraft.

More recent studies revolved around specific spacecraft subsystems. For example Cho

(2005) and Landis *et al*. (2006) focused on failures in spacecraft power subsystem, Brandhorst and Rodiek (2008) on solar arrays failures, and Roberston and Stoneking (2003) on the attitude control subsystem failures. Sperber (2002) and Tafazoli (2009) analyzed not a single subsystem's failures but the comparative contribution of various subsystems to spacecraft on orbit failures. And instead of spacecraft subsystems, Bedingfield *et al*. (1996) focused on spacecraft failures only due to the natural space environment.

Early spacecraft reliability studies assumed an exponential distribution and constant failure rate (Leventhal *et al*., 1969; Bean and Bloomquist, 1968; Binckes, 1983). In some of these studies however, discrepancies between the values of the observed reliability and the predicted reliability of the spacecraft already started to appear: Bean and Bloomquist (1968), for example, concluded that observed failures rates were lower than expected from prediction. The exponential assumption was challenged by Timmins and Heuser (1971) who showed that, for their small sample of 57 NASA Goddard Space Flight Center spacecraft, the failure rate was in fact not constant but higher in the early days on orbit:

> "*The number of failures per spacecraft were abnormally high for the first 30 days in space. The number of first-day failures departed even more from the longer trend*."

This finding of spacecraft infant mortality and decreasing failure rate was repeated in subsequent studies (Timmins, 1974; 1975), and led Baker and Baker (1980) to comment that "those spacecraft that last, last on and on," which in effect reflects for these authors the absence of wear-out failures in spacecraft.

Hecht and Hecht (1985) analyzed a different population of spacecraft than the one used in the previous four studies (the 57 NASA spacecraft). Their sample consisted of some 300 spacecraft launched between 1960 and 1984, and covered 96 different space programs. Their analysis also found decreasing failure rate in their spacecraft sample, and they took issue with the constant failure rate models proposed in the military reliability handbook, MIL-HDBK-217 as unrealistic for system reliability predictions. MIL-HDBK-217 was first developed in 1961 and revised several times afterwards. Similar conclusions were advanced by Krasich (1995) and Sperber (1990; 1994) who noted a qualitative agreement in prior studies "that as the mission goes on, risk per unit time to surviving spacecraft decreases."

To better represent this non constant failure rate, several models have been explored, and several studies chose the Weibull distribution as suitable for spacecraft or spacecraft subsystem reliability (Norris and Timmins, 1976; Baker and Baker, 1980; Hecht and Hecht, 1985; Hecht and Fiorentino, 1987; Krasich, 1995). However, given the significant technological changes in spacecraft design in the last decades, these models suffer from obsolescence and are of limited relevance for today's spacecraft. As for the more recent studies mentioned earlier, they reported failure numbers but they did not provide reliability models. Consequently there is a gap in the literature for recent reliability models for spacecraft and a need for a thorough statistical analysis of recent flight data to answer this fundamental question: **How reliable spacecraft and spacecraft subsystems have been?**

2.2. Nonparametric Reliability Analysis of Spacecraft Failure Data

2.2.1. Database and Data Description

The SpaceTrak database (see References) was adopted for the purpose of this thesis. This database is used by many of the world's launch providers, spacecraft insurers, operators, and spacecraft manufacturers. The database provides a history of on-orbit spacecraft failures and anomalies, as well as launch histories since 1957. It should be pointed out that this database is not necessarily "complete" in a statistical sense since some military or intelligence spacecraft may not have their failures reported. Similarly, the database cannot be considered "complete" with respect to anomalies or partial failures since spacecraft operators may not report all partial failures, especially, the ones that can be recovered from in a timely manner. This being said, the database is considered as one of the authoritative databases in the space industry with failure and anomaly data for over 6400 spacecraft. The statistical analysis in this work is enabled by, and confined to, the failure and anomaly information provided in this database.

The sample analyzed in this section consists of 1584 spacecraft. The sample was restricted to Earth-orbiting spacecraft successfully launched between January 1990 and October 2008. The observation window has been chosen to obtain a spacecraft sample as large as possible, while limiting the effect of technology heterogeneity and obsolescence. A failure leading to the spacecraft retirement is identified in the database as a Class I failure, that is, a complete failure leading to the loss of the spacecraft. In addition, as will be detailed later, eleven spacecraft subsystems are identified in the database. If the cause of a Class I failure is identified and traced back to a particular subsystem, that “culprit” subsystem is noted in the database. When the culprit subsystem, whose failure led to the spacecraft failure, could not be identified, the failure of the spacecraft is ascribed to an “unknown” category in the database. This categorization was used for analyzing the relative contribution of each subsystem to the overall spacecraft failures.

For each spacecraft in the sample, the following information was collected: 1) its launch date; 2) its failure date, if failure occurred; 3) the subsystem identified as having caused the spacecraft failure, hereafter referred to as the culprit subsystem; and 4) the censored time, if no failure occurred. This last point is further explained in the following subsection, where data censoring and the Kaplan–Meier estimator are discussed. The data collection template and sample data for the analysis are shown in Table 2.1.

Table 2.1. Data collection template and sample data for the statistical analysis of spacecraft reliability

Sample unit number*	Launch date	Failure date (if failure occurred)	Culprit subsystem	Censored time (if no failure occurred)
Spacecraft #1	11/06/1998	11/15/1998	TTC	–
Spacecraft #2	03/01/2002	–	–	10/02/2008
…	…	…	…	…
Spacecraft #1584	04/26/2004	03/28/2006	Mechanisms	–

* Note that spacecraft are not necessarily arranged/shown in chronological order

2.2.2. Nonparametric Analysis of Spacecraft Failure Data

Censoring occurs when life data for statistical analysis of a set of items is “incomplete”. This situation occurs frequently in multiple settings (e.g., medical and engineering contexts) and can happen because some items in the sample under study are removed prior to failure or because the test or observation window ends prior to all items failing. By contrast, a life data set is said to be “complete” if one observes the actual time to failure of all the items in the sample under study, that is, if no censoring occurs within the data. Censoring introduces particular difficulties in statistical analysis which, if not addressed and accounted for, can significantly bias the results. There are multiple classifications and types of censoring and different statistical techniques for dealing with them. The reader interested in extensive detail is referred to three excellent books on the subject: Lawless (2003), Ansell and Phillips (1994) and Meeker and Escobar (1998). In the particular case of this study, the sample analyzed is right-censored (random censoring) with staggered entry. This means the following: 1) the units in the sample are activated at different points in time (i.e. the spacecraft are launched at different calendar dates), but all activation times in the sample are known; 2) failures dates and censoring are stochastic; and 3) censoring occurs either because a unit (spacecraft) is retired from the sample before a failure occurs or because the spacecraft is still operational at the end of the observation window (October 2008). This situation is illustrated in Figure 2.1.

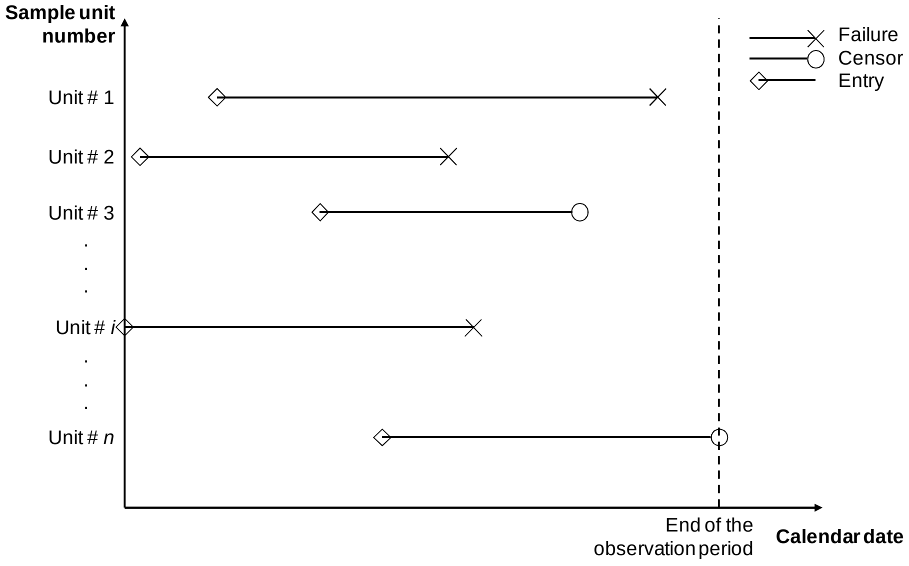


Figure 2.1. Censored data with staggered entry

Staggered entries are easily handled by shifting all the activation times to $t = 0$, which changes the approach, and the x-axis in Figure 2.1, from a calendar-time to a clock-time analysis of spacecraft reliability. Therefore spacecraft reliability is investigated as a function of time following successful orbit insertion.

Censoring of data requires particular attention. Deriving a reliability function from censored life data is not trivial, and it is important that is it done properly if the results are to be meaningful and unbiased. In this work, the powerful Kaplan–Meier estimator (Kaplan and Meier, 1958) is adopted, as it is best suited for handling the type of censoring in the sample.

Starting with n operational units, and because of censoring, only m time to failure ($m < n$) are collected. Assuming no ties between failures times, let

$$t_{(1)} < t_{(2)} < \ldots < t_{(m)} \tag{2.1}$$

be the failure times organized in ascending order. The goal is to estimate the reliability function, defined with respect to the random variable T_F (time to failure) as:

$$R(t) \equiv P(T_F > t) \tag{2.2}$$

The Kaplan–Meier estimator of the reliability function with censored data is given by:

$$\hat{R}(t) = \prod_{\substack{\text{all } i \text{ such} \\ \text{that } t_{(i)} \leq t}} \hat{p}_i = \prod_{\substack{\text{all } i \text{ such} \\ \text{that } t_{(i)} \leq t}} \frac{n_i - 1}{n_i} \tag{2.3}$$

where:

$$\begin{aligned} n_i &= \text{number of operational units right before } t_{(i)} \\ &= n - [\text{number of censored units right before } t_{(i)}] \\ &\quad - [\text{number of failed units right before } t_{(i)}] \end{aligned} \tag{2.4}$$

The complete derivation of the Kaplan-Meier estimator and the treatment of ties in the data are provided in Castet and Saleh (2009a) and Saleh and Castet (2011). Also in these references are provided details about the construction of confidence intervals for the Kaplan-Meier estimate (here using the Greenwood's formula, with alternative methods in Kalbfleisch and Prentice (1980) and Lawless (2003)).

The on-orbit spacecraft reliability from the censored data set can now be analyzed. For the 1584 spacecraft in the sample, there are 98 failures times and 1486 censored times. The (ordered) failure times are provided in Table 2.2.

Table 2.2. Failure times (in days) of spacecraft launched between January 1990 and October 2008

1	1	1	1	2	3	3	4	4	5	5
7	9	12	15	15	16	16	23	36	51	53
64	68	73	79	89	102	107	123	128	131	167
190	197	221	229	237	252	271	309	314	317	334
364	465	515	696	701	713	722	724	787	1053	1073
1122	1146	1167	1184	1233	1256	1347	1458	1551	1637	1778
1797	1836	1967	2009	2091	2097	2098	2181	2191	2237	2429
2434	2472	2577	2580	2624	2702	2917	2947	2963	3038	3077
3159	3268	3455	3684	3759	4192	4324	4909	5043	5207	

The data is then treated with the Kaplan-Meier estimator (Eq. (2.3)), and the Kaplan-Meier plot of spacecraft reliability shown in Figure 2.2 is obtained, with 95% confidence intervals (that is, a 95% likelihood that the actual reliability will fall between these two bounds, with the Kaplan-Meier analysis providing the most likely estimate).

Figure 2.2 reads as follows: For example, after two years on-orbit, spacecraft reliability will be between 95.4% and 97.8% with a 95% likelihood—these values constitute the lower and upper bounds of the 95% confidence interval at t = 2 years. In addition, the most likely estimate of spacecraft reliability at this point in time is $\hat{R}$ = 96.4%. More precisely:

$$\widehat{R}(t) = 0.964 \qquad \text{for} \qquad 1.982\ \text{years} \le t < 2.155\ \text{years}$$

Spacecraft reliability then drops to approximately 94% after 6 years on-orbit. Past 12 years, spacecraft reliability lies roughly between 90% and 91%. Complete tabular data are given in Castet and Saleh (2009a) and Saleh and Castet (2011). Comments about the confidence interval spread are made in Chapter 3.

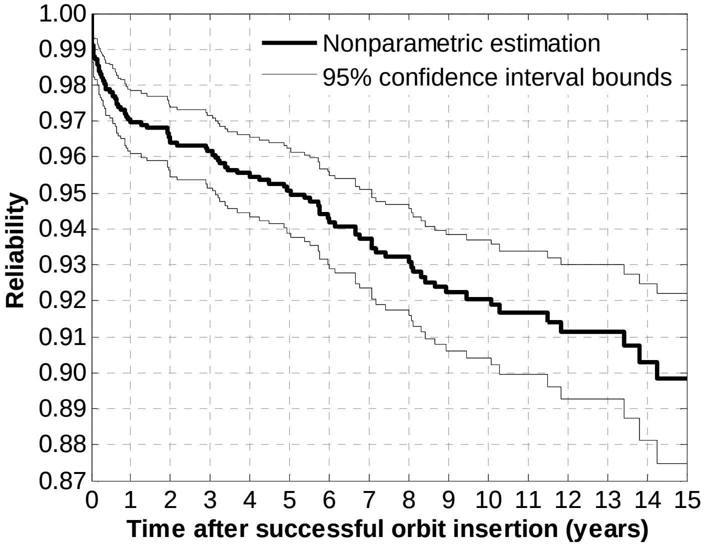


Figure 2.2. Kaplan-Meier plot of spacecraft reliability with 95% confidence intervals

These are actual (field) spacecraft reliability results, not reliability specifications, and they provide a first answer to “how reliable spacecraft have been?” (between 1990 and 2008). Several trends can be seen in Figure 2.2, the most noticeable one being the steep drop in reliability during the first year of spacecraft operation, which is indicative of infant mortality. These trends are better captured further with parametric models.

2.2.3. Parametric Analysis and Weibull Modeling of Spacecraft Reliability

Nonparametric analysis provides powerful results since the reliability calculation is unconstrained to fit any particular pre-defined lifetime distribution. However, this flexibility makes nonparametric results neither easy nor convenient to use for various purposes often encountered in engineering design (e.g., reliability-based design optimization). In addition, some failure trends and patterns are more clearly identified and recognizable with parametric analysis. Several methods are available to fit parametric distributions to the nonparametric reliability results (as provided for example by the Kaplan-Meier estimator), or to derive parametric reliability distributions directly from the failure and censored times. Probability plotting is used to illustrate that spacecraft reliability can be reasonably approximated by a Weibull distribution, and the Maximum Likelihood Estimation (MLE) method is used to calculate the parameters of the Weibull distribution. However, as discussed below, several trends are present in the nonparametric result of spacecraft reliability that can be better captured by more complex models, such as mixtures of Weibull distributions.

Weibull distributions and mixtures. The Weibull distribution is one of the most commonly used distribution in reliability analysis. The reason for its wide adoption is that it is quite flexible, and with an appropriate choice of one of its two parameters (the shape parameter), it can model different kinds of failure behaviors. The Weibull distribution has two parameters: the shape parameter β and the scale parameter θ. Its failure rate can be written as follows:

$$\lambda(t) = \frac{\beta}{\theta}\left(\frac{t}{\theta}\right)^{\beta-1} \text{ with } \theta > 0, \beta > 0, t \geq 0 \tag{2.5}$$

The shape parameter β is dimensionless, and the scale parameter θ is expressed in units of time. Its probability density function can be expressed as follows:

$$R(t) = \exp\left[-\left(\frac{t}{\theta}\right)^{\beta}\right] \tag{2.6}$$

The parametric reliability model with a mixture of Weibull distributions can be expressed as follows:

$$R(t) = \sum_{j=1}^{k} \alpha_j \exp\left[-\left(\frac{t}{\theta_j}\right)^{\beta_j}\right] \tag{2.7}$$

where:

$$\begin{cases} k \text{ is the number of distributions in the mixture} \\ 0 \leq \alpha_j \leq 1 \\ \sum_{j=1}^{k} \alpha_j = 1 \end{cases} \tag{2.8}$$

Weibull models for spacecraft reliability. Probability plots constitute a simple and visually appealing graphical estimation procedure for fitting a parametric distribution to nonparametric data. This procedure is based on the fact that some parametric models such as the Exponential or Weibull distribution can have their reliability function linearized using a particular mathematical transformation. This transformation for the Weibull distribution is presented in Castet and Saleh (2009a) and Saleh and Castet (2011). In the case of the estimated spacecraft reliability obtained above, its resulting Weibull plot is shown in Figure 2.3.

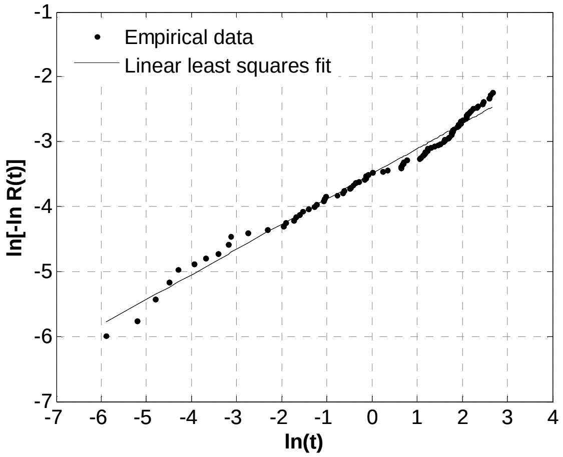


Figure 2.3. Weibull plot of spacecraft reliability

The data points are well aligned (R^2 = 0.9835) and this provides a first indication that the Weibull fit is indeed a good one, and that spacecraft reliability can be justifiably approximated by a Weibull distribution. The Maximum Likelihood Estimation (MLE) method provides more precise parametric fits than graphical estimation, as long as the sample size is not exceedingly small (e.g., in the single digits). The MLE method is analytically more involved than the graphical estimation techniques, and requires 1) determining the right formulation of the Likelihood function for a chosen distribution and type of censoring, as will be shown shortly, and, 2) searching for an optimum of this function, which can be accomplished through various computational or analytical techniques. The values of unknown parameters of the distribution parameters that maximize the Likelihood Function are termed the Maximum Likelihood Estimates and the method is known as the MLE. The complete analytical derivation of the MLE in the case of a Weibull distribution is provided in Saleh and Castet (2011). The resulting Weibull reliability function for spacecraft is given as follows:

$$R(t) = \exp\left[-\left(\frac{t}{2607}\right)^{0.4521}\right], \ t \text{ in years} \tag{2.9}$$

The shape parameter of the Weibull distribution (β = 0.4521) is smaller than 1, which indicates that spacecraft **infant mortality** is a robust finding.

In addition to the Weibull distribution to parametrically model spacecraft reliability, other distributions were investigated, and in particular an MLE lognormal fit was also conducted, and the resulting p.d.f. is:

$$f(t;\mu,\sigma) = \frac{1}{t\sigma\sqrt{2\pi}} e^{\frac{-(\ln(t)-\mu)^2}{2\sigma^2}} \tag{2.10}$$

with $\mu = 9.7646$ and $\sigma = 5.2209$ for *t* in years

The residuals of the lognormal distribution indicate that although it is a relatively accurate representation of the nonparametric (benchmark) satellite reliability results, the lognormal distribution is less precise and a more biased fit of satellite reliability than the Weibull distribution. As a conclusion, the Weibull distribution is retained for the remainder of this dissertation.

In the case of a 2-Weibull mixture distribution, the MLE method yields the following (method and step-by-step derivation of the MLE for Weibull mixtures provided in Saleh and Castet (2011). Also in that reference are provided alternative methods based on

Dempster, *et al*. (1977), or McLachlan and Krishnan (2008), Titterington, *et al*. (1985) and Kvam and Vidakovic (2007)):

$$R(t) = 0.9725\exp\left[-\left(\frac{t}{14310.1}\right)^{0.3760}\right] + 0.0275\exp\left[-\left(\frac{t}{9.3}\right)^{2.9937}\right], \; t \text{ in years} \qquad (2.11)$$

Note that the first Weibull shape parameter $\beta_1 < 1$ captures spacecraft infant mortality, whereas the second Weibull shape parameter $\beta_2 > 1$ captures spacecraft wear-out failures. These two parametric models of the spacecraft reliability are shown in Figure 2.4 and Figure 2.5, superimposed on the nonparametric reliability results.

It can be observed that both parametric models provide relatively precise approximation of the nonparametric reliability as can been seen from Figure 2.4 and Figure 2.5. However, upon closer inspection, it is clear that the 2-Weibull mixture distribution follows with a higher accuracy the trends present in the nonparametric spacecraft reliability. To quantify this difference in accuracy, a detailed analysis of the residuals of both parametric models is conducted with respect to the nonparametric reliability, as shown in Figure 2.6. Figure 2.6 presents two box-plots for the residuals of the single Weibull and the 2-Weibull mixture distributions. Recall that the box-plot reads as follows: the lower boundary of the “box” is determined by the first quartile (25th percentile) of the residuals, and the upper boundary by the third quartile (75th percentile). The line within the box corresponds to the median value, and the “whiskers” outside the box represent the minimum and maximum of the residuals.

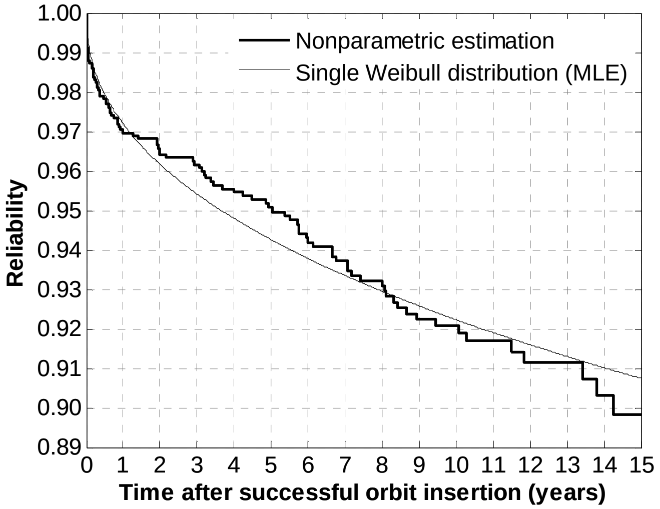


Figure 2.4. Nonparametric and single Weibull reliability

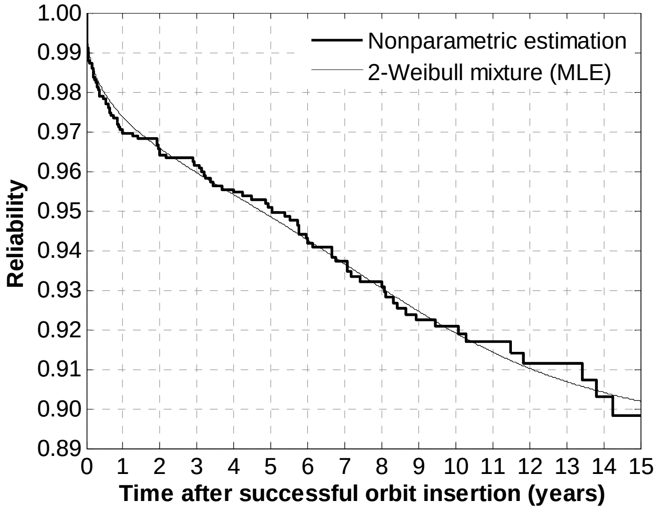


Figure 2.5. Nonparametric and 2-Weibull mixture reliability

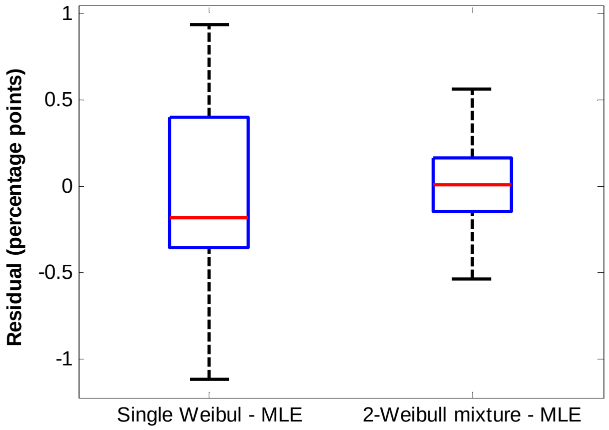


Figure 2.6. Box plots of the residuals between the Weibull fits and the nonparametric reliability over 15 years

Figure 2.6 confirms the higher precision of the mixture of distributions over 15 years. The residuals of the mixture distribution have a smaller spread than those of the single-function parametric fit:

- The 25th and 75th percentile are less dispersed for the mixture distribution (i.e., smaller box);
- The extreme values are less spread (i.e., shorter whiskers);
- The residuals of the 2-Weibull mixture distribution are clearly more symmetrically dispersed that those of the single Weibull. In addition, the residuals between the 2-Weibull and the nonparametric reliability results are quasi-normally distributed which is a good indication that no bias remains in the parametric mixture model and all failure trends have been captured by the 2-Weibull mixture distribution. This last comment also indicates that it is superfluous to fit higher order mixture distributions ($k > 2$).

As a conclusion, the following suggestions are made for researchers and industry professionals should they wish to use these spacecraft reliability results. First, the use the nonparametric results is recommended as the most accurate reflection of actual spacecraft reliability. However, if the context of the study is not amenable to manipulating or using nonparametric results, then the use of the 2-Weibull mixture fit is recommended. The single Weibull MLE fit can be used if simplicity is sought and the study does not require a high level of precision.

2.2.4. Discussion and Limitations

A discussion is in order regarding the challenges and limitations of statistical analysis of spacecraft reliability in general, and the analysis and results in the previous section in particular. First note that the results here provided represent the “collective” failure behavior of Earth-orbiting spacecraft launched between 1990 and 2008. It can be argued however that no two spacecraft are truly alike, and that every spacecraft operates in a distinct environment, in different orbits or even within the same orbit, where spacecraft, unless they are co-located, are exposed to different space environment conditions. The situation of the space industry is different from that for example of the semi-conductor industry where data on, say, thousands of identical transistors operating under identical environmental conditions are available for statistical analysis, or other industries with items for which failure data can be easily obtained from accelerated testing or field operation. The consequence is that in the absence of “spacecraft mass production,” statistical analysis of spacecraft failure and reliability data faces the dilemma of choosing between calculating precise “average” spacecraft reliability or deriving a possibly uncertain “specific” spacecraft platform reliability. This dilemma is explained in the following two possible approaches.

The first approach is to lump together different spacecraft and analyze their “collective” on-orbit failure behavior, assuming that the failure times of the spacecraft are independent and identically distributed (*iid*). The advantage of doing so is that one can work with a relatively large sample (a few hundred or thousand of units), as done in this section, and thus obtain some precision and a narrow confidence interval for the “collective” reliability analyzed (a single-digit percentage point dispersion). The disadvantage is that the *iid* assumption can be challenged, and the “collective” reliability calculated (with precision) may not reflect the specific reliability of a particular type of spacecraft in a particular orbit.

The second approach is to specialize the data, for example for specific spacecraft platform or mission type, or for spacecraft in particular orbits. The advantage of doing so is that the reliability analyzed is specific to the type of spacecraft considered (it is no longer a “collective” on-orbit reliability). The disadvantage is that the sample size is reduced, and as a consequence, the confidence interval expands. Given the available number of spacecraft (a few thousands), inappropriate data specialization, which could reduce the sample size to say fewer than a hundred data points, will result in significantly large confidence intervals, and thus highly dispersed and uncertain “specific” spacecraft reliability results.

This section provided results based on the first approach, the “collective” failure behavior of spacecraft recently launched. The second approach is adopted in Castet and Saleh (2009b), Hiriart, *et al*. (2009), and Dubos, Castet and Saleh (2010), where reliability results based on careful data specialization by spacecraft mission type, orbit type, and mass category are derived.

2.2.5. Spacecraft Subsystem Reliability and Comparative Contribution to Spacecraft Unreliability

In this subsection, , the previous statistical analysis of spacecraft reliability is extended to include spacecraft subsystems, that is, the analysis is narrowed down from the system-level to the subsystem-level failures, and reliability results, nonparametric and parametric, are derived for spacecraft subsystems. The two broad questions addressed here are, 1) **what are the reliability profiles of various spacecraft subsystems?** And 2) **to what extent does each subsystem contribute to the overall failures of spacecraft?** The answer to the second question constitutes a comparative analysis of subsystems failure, from an actuarial perspective, and allows for example the identification of culprit subsystems driving spacecraft unreliability. The results here provided should prove helpful to spacecraft manufacturers by allowing them to hone in on problematic subsystems that would benefit most from increased testing and reliability improvements.

Spacecraft subsystem identification. The statistical failure data analysis at the subsystem level is enabled by, and confined to, the subsystems identified in the database:

1. Gyro / Sensor / Reaction Wheel (hereafter referred to as Gyro)
2. Thruster / Fuel (Thruster)
3. Beam / Antenna Operation / Deployment (Beam)
4. Control Processor (CP)
5. Mechanisms / Structures / Thermal (Mechanisms)
6. Payload Instrument / Amplifier / On-board Data / Computer / Transponder (Payload)
7. Battery / Cell (Battery)
8. Electrical Distribution (ED)
9. Solar Array Deployment (SAD)
10. Solar Array Operating (SAO)
11. Telemetry, Tracking and Command (TTC)

Descriptions of these subsystems can be found in textbooks on spacecraft systems engineering such as in Fortescue *et al*. (2003) or Wertz and Larson (1999). When the culprit subsystem that led to the failure of the spacecraft could not be identified, the failure of the spacecraft is ascribed to an “Unknown” category in the database. Only the Beam/Antenna operation/deployment subsystem exhibits no Class I failure in the dataset. Thus the following study is confined to the 10 remaining subsystems plus the unknown category.

Nonparametric reliability of spacecraft subsystems. The subsystem failure data is treated with the Kaplan-Meier estimator (Eq. (2.3)), and the Kaplan-Meier plots of the reliability of all the spacecraft subsystems along with 95% confidence intervals are shown in Figure 2.7 and Figure 2.8.

Figure 2.7 and Figure 2.8 read as follows. Consider the “Gyro” subsystem, its reliability is shown in the upper-left corner of Figure 2.7. After a successful launch, the reliability of this subsystem drops to approximately 99.5% after four years on-orbit. More precisely :

$$\begin{aligned} \widehat{R}(t) = 0.9948 \quad & \text{for} \quad 1146 \text{ days} \le t < 1967 \text{ days} \\ & \text{that is} \quad 3.137 \text{ years} \le t < 5.385 \text{ years} \end{aligned}$$

In addition, the reliability of this subsystem will fall between 99.1% and 99.9%, its 95% confidence interval, over this period of time.

This same “reading grid” regarding the estimated reliability $\widehat{R}(t)$ and confidence interval applies to all the other subsystems of Figure 2.7 and Figure 2.8. Notice the particular nonparametric reliability of the Solar Array Deployment, a constant, which is due to the one-shot nature of this “subsystem” (or more precisely, to this phase of the solar array subsystem).

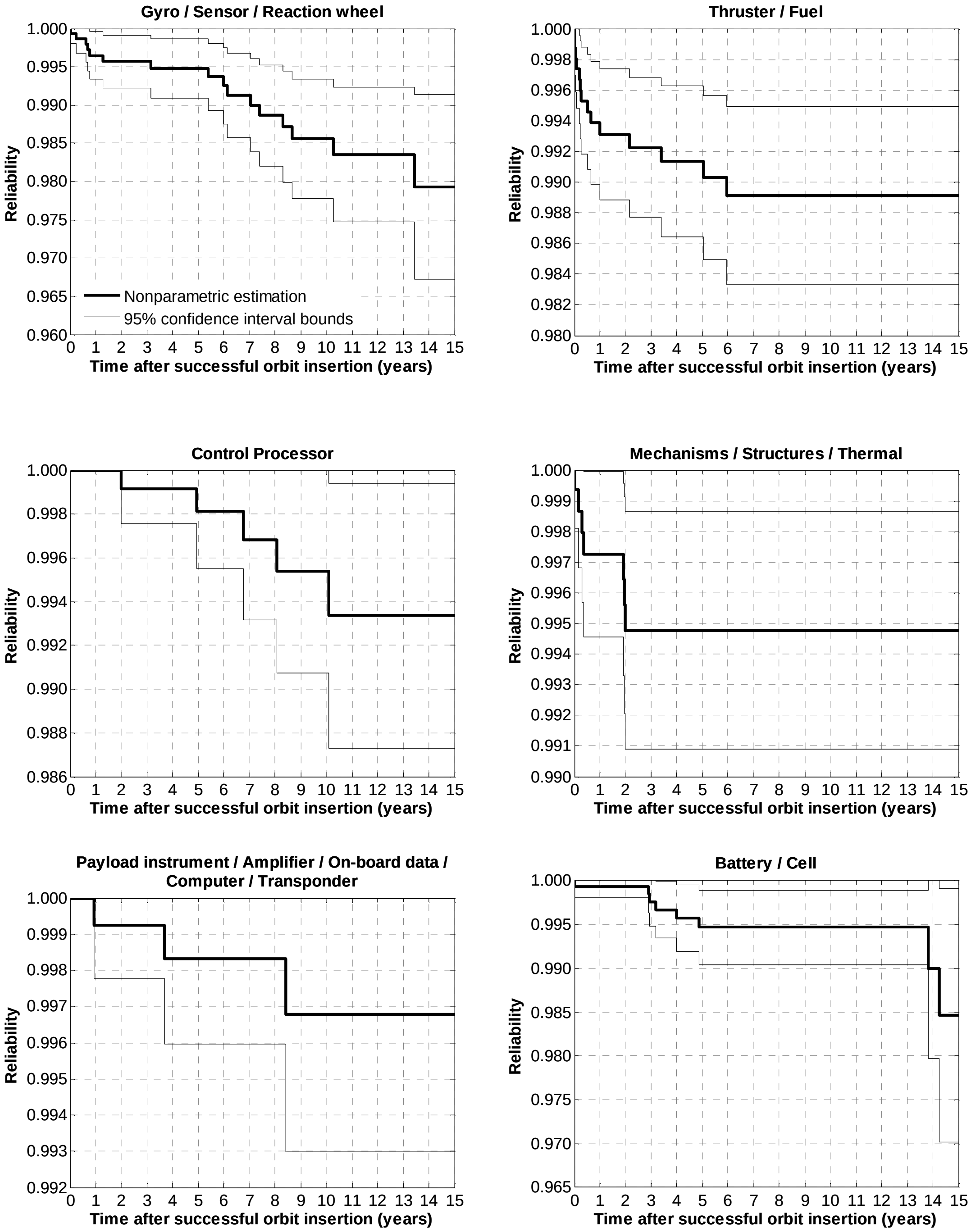


Figure 2.7. Spacecraft subsystems reliability with 95% confidence intervals (1/2)

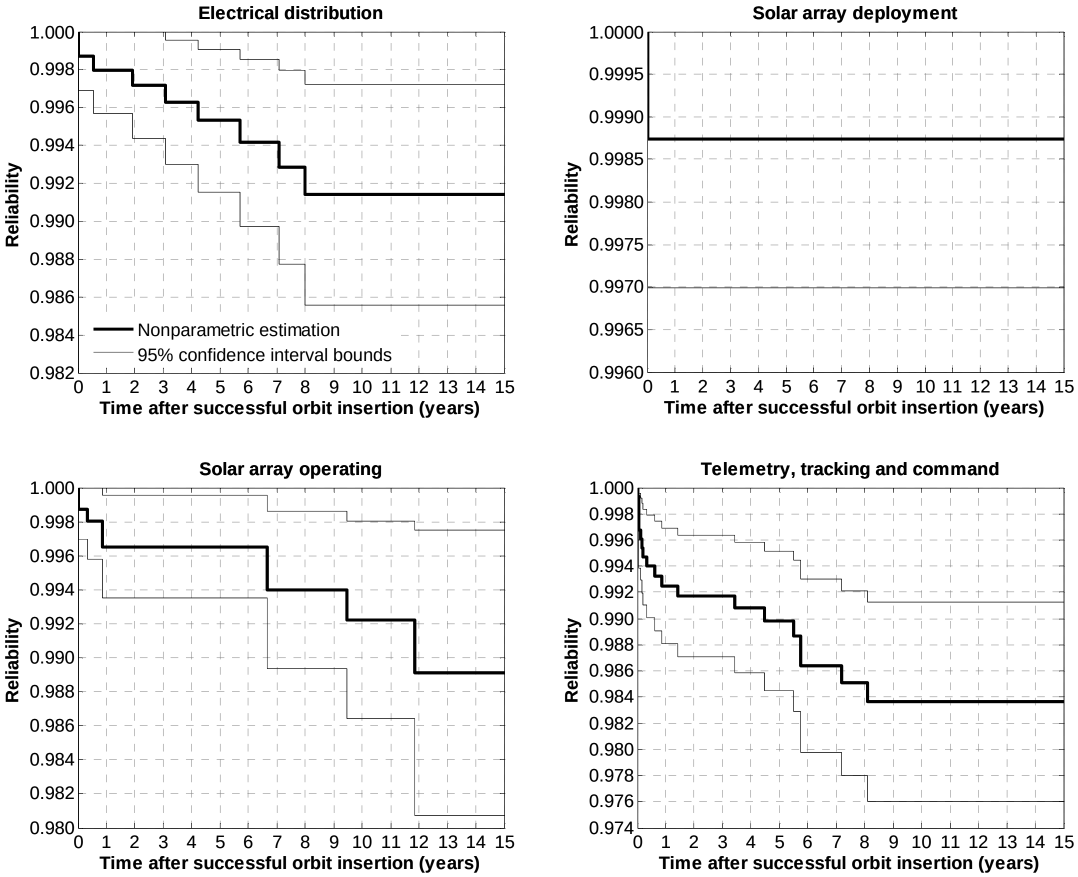


Figure 2.8. Spacecraft subsystems reliability with 95% confidence intervals (2/2)

A general observation can be made regarding these nonparametric reliability results, namely that spacecraft subsystems all maintain reliability above than 98% after 15 years on orbit (and above 97% for the lower bound of the 95% confidence interval). However, the collective failure contributions of these subsystems lead to spacecraft reliability in the 80% to 90% range as seen in the previous subsection, a costly situation, considering that these high-value assets often cost several hundred millions of dollars to design and launch, and they do not benefit from physical access and maintenance to remedy on orbit failures. Consequently, improvements to spacecraft subsystem reliability are warranted, and the nonparametric results in Figure 2.7 and Figure 2.8. provide a first indication of possible subsystem failure patterns to target and remedy. Notice for example the distinct and marked infant mortality failures of the Thruster / Fuel and the TTC subsystems, which could be eliminated through improved testing or burn-in procedures.

Weibull modeling of spacecraft subsystem reliability. Weibull distributions have been shown previously to be adequate for modeling spacecraft reliability. The same observation can be extended to spacecraft subsystems as demonstrated in Castet and Saleh (2009c) and Saleh and Castet (2011). The resulting models from the MLE methods are given in Table 2.3. It is shown in these two references that the resulting Weibull distributions are a good fit for the nonparametric results. Improved accuracy, if needed, can be obtained as done previously through the use of mixture distributions.

Table 2.3. Maximum Likelihood Estimates of the Weibull parameters for subsystem reliability

Subsystem	$\boldsymbol{\beta}$	$\boldsymbol{\theta}$
		years
Gyro / Sensor / Reaction Wheel	0.7182	3831
Thruster / Fuel	0.3375	6,206,945
Control Processor	1.4560	408
Mechanisms / Structures / Thermal	0.3560	2,308,746
Payload Instrument / Amplifier / On-board Data / Computer / Transponder	0.8874	7983
Battery / Cell	0.7460	7733
Electrical distribution	0.5021	169,272
Solar Array Deployment	–	–
Solar Array Operating	0.4035	1,965,868
Telemetry Tracking and Command	0.3939	400,982

Note that no values of the Weibull parameters are provided for the Solar Array Deployment subsystem. As discussed previously, the “Solar Array Deployment” is a one-shot “subsystem” and a Weibull fit is not meaningful in this case. A Weibull fit can also be conducted on the data assigned to the "Unknown" category. The resulting Weibull parameters are β = 0.4011 and θ = 5836474 years.

The important result in Table 2.3 is that **all spacecraft subsystems, with the exception of the Control Processor, suffer from infant mortality** (shape parameter $\beta < 1$). This finding has important implications for the space industry and should prompt serious considerations for improved subsystem testing and burn-in procedures.

Comparative analysis of subsystem failures. A comparative analysis of subsystem failure is provided in this section and the culprit subsystems driving spacecraft unreliability are identified. More specifically, the relative contribution of each subsystem to the failure of the spacecraft in the sample is quantified. In addition, a time dimension is added to this analysis by investigating the evolution over time of the relative contribution of each subsystem to the loss of spacecraft. The derivation of the percentage contribution of subsystem j to the failure of a spacecraft, named r_j, is not trivial and the complete original derivation is available in Saleh and Castet (2011) and an illustrative example is shown in Kim, Castet and Saleh (2012).

Deriving r_j for all subsystem addresses the second question of this subsection, namely to what extent each subsystem contributes to the overall failures of spacecraft. The results of the analysis can be displayed in one figure, showing all the r_j for j = 1 to 11 as a function of time. Doing so however would result in an exceedingly cluttered figure. For readability purposes, the results are split into four panels in Figure 2.9.

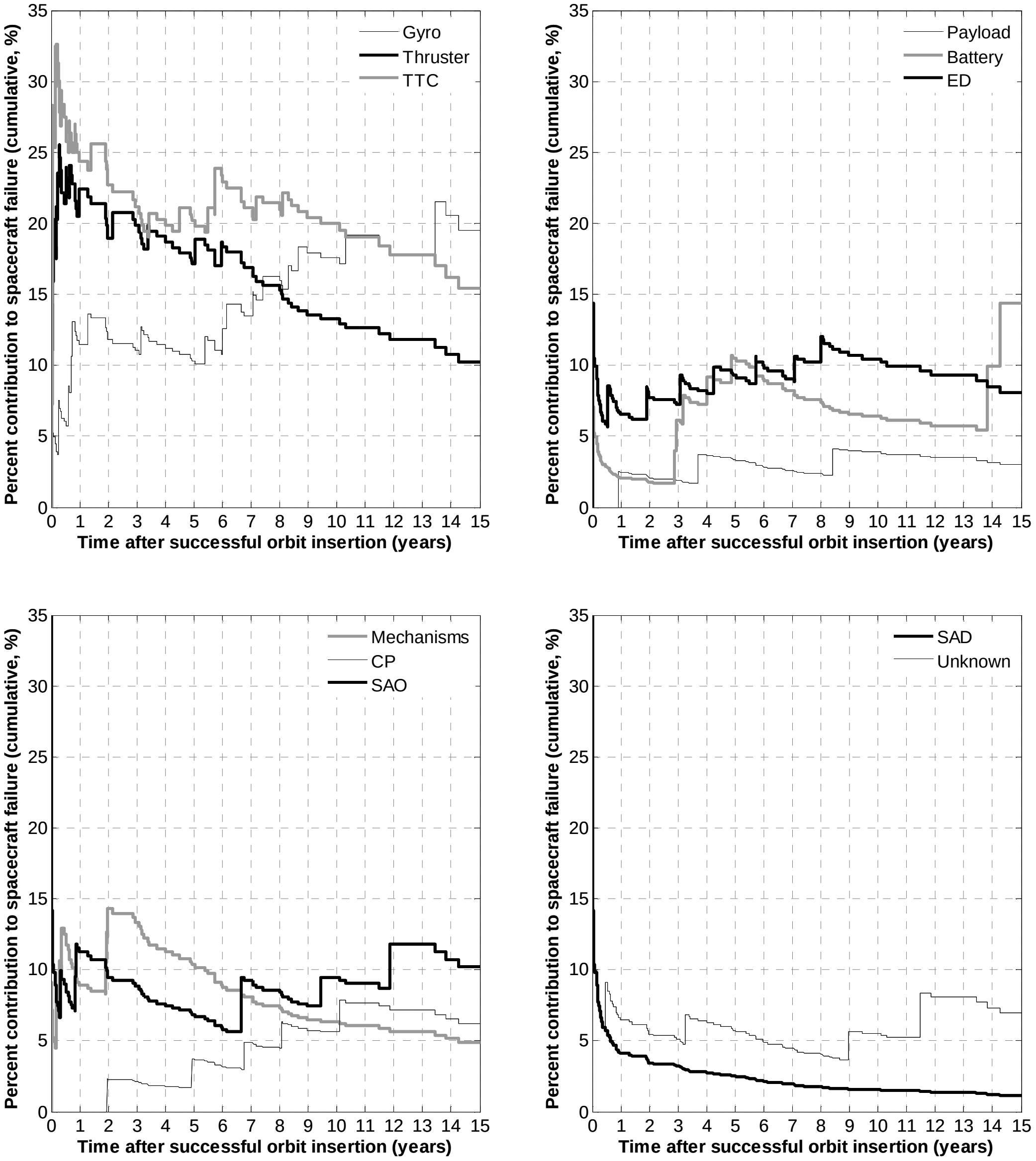


Figure 2.9. Relative contribution of various subsystems to spacecraft failure

Figure 2.9 shows the evolution over time of the contribution of each subsystem to the loss of spacecraft. For example, it can be seen in the lower-left quadrant of Figure 2.9, that the Control Processor (CP) contributes approximately 6% to the total failures of spacecraft over 15 years. Similarly in the upper-left quadrant of Figure 2.9, it is observed that the

Gyro and TTC are the major contributors to spacecraft failures with respectively 20% and 15% of spacecraft failures due to these subsystems over a period of 15 years.

These results clearly mark the **TTC, Gyro, and Thruster/Fuel subsystems as the major culprits driving spacecraft unreliability** and the ones that would benefit most from reliability improvements. The Gyro and the Thruster/Fuel are the two subsystems of the macro spacecraft subsystem Attitude and Orbit Control Subsystem (AOCS). As a side node, if the Battery/Cell, ED, SAD and SAO are considered together within the larger **Electrical Power Subsystem** (EPS), their combined contributions to spacecraft unreliability class them as major protagonists for spacecraft complete loss, as shown in Kim, Castet and Saleh (2012). A complete discussion of the results presented in Figure 2.9 is available in Saleh and Castet (2011). As a conclusion, Figure 2.9 provides some **guidance to engineers working on spacecraft design and corresponding reliability testing programs**.

Figure 2.10 provides a more readable version of Figure 2.9. Instead of the evolution over time of r_j, Figure 2.10 provides a snapshot or static picture of the subsystems' contributions to spacecraft failures at four discrete points in time, after 30 days, after 1 year, after 5 years, and after 10 years on-orbit. Figure 2.10 in effect represents vertical cuts across Figure 2.9, and while the dynamical information portrayed in this figure is lost, readability and accuracy (or finer resolution) is gained at the discrete points in time selected.

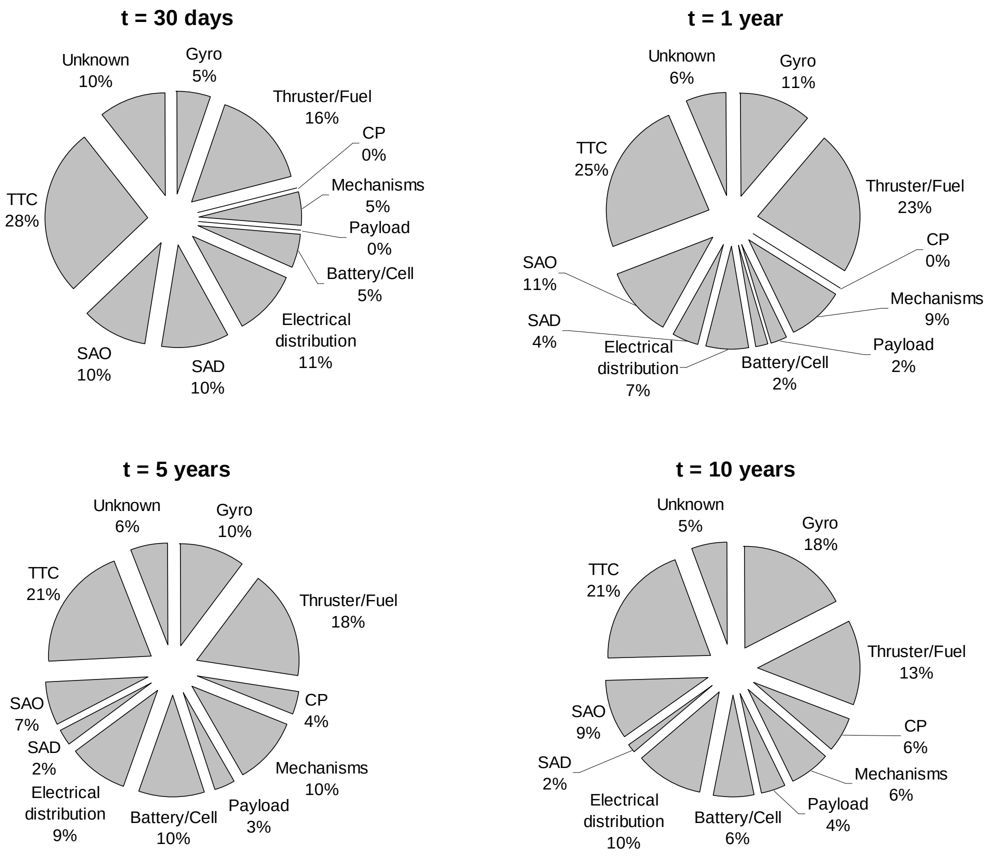


Figure 2.10. Subsystem contributions to spacecraft failures after 30 days, 1 year, 5 years, and 10 years on-orbit

Similar observation can be made on Figure 2.10. In addition, note in the upper-left quadrant of Figure 2.10 that the Solar Array (Deployment and Operating) and TTC account respectively for 20% and 28% of the failures of the first 30 days on-orbit. Thus spacecraft infant mortality is driven to a large extent by these two subsystems, followed by the Thruster/Fuel subsystem, during the first month on orbit.

2.3. Summary

The technical literature has long recognized the importance of spacecraft reliability, but little analysis based on actual extensive flight data has been conducted. The present chapter helps to fill this gap by 1) conducting a thorough statistical analysis of recent on-orbit spacecraft reliability data and on a significantly large sample, 2) fitting parametric models to the actual/observed reliability and 3) deriving reliability profiles of spacecraft subsystems and quantifying their relative contribution to satellite failures, enabling the identification of the subsystems that drive spacecraft unreliability.

Fundamental results or this chapter includes the following: the spacecraft failures examined in this thesis exhibit a clear infant mortality trends, as well most subsystem failures (with the exception of the control processor). It was shown that the Weibull distribution is an appropriate model (single or mixture) for spacecraft reliability. Finally, particular subsystems such as the TTC or the Gyro were outlined as major contributors to spacecraft failures, and the time-dependence contribution of each subsystem was clearly identified. As such, the TTC and the solar array drive a significant part of the infant mortality. These analyses provides helpful feedback to the space industry in providing results, but also reproducible reliability methods for redesigning spacecraft and spacecraft subsystems, their test and screening programs, and providing an empirical basis for subsystem redundancy allocation and reliability growth plans. In the subsequent chapter, a more detailed approach to the degradation behavior of spacecraft subsystems is developed by accounting for and analyzing their anomalies and partial failures, i.e., failures of different severities, not just Class I (total) failures.

CHAPTER 3

MULTI-STATE FAILURE ANALYSIS OF SPACECRAFT SUBSYSTEMS

3.1. Introduction

The previous section dealt with reliability of spacecraft and spacecraft subsystems, a critical design attribute for high value assets. The events considered were catastrophic failures (Class I) that lead to the complete loss of the spacecraft. As a result, only two states were considered, *operational* and *failed*, and the (sub)systems were analyzed and modeled as being in one of these two states. In reality, many engineering artifacts, spacecraft included, can experience failure events of varying severities, and thus transition from fully operational to various states of partial degradations, not necessarily complete failures. Indeed, the database used for the statistical analysis in the present work identifies four classes of anomaly and failure for each spacecraft subsystem: three degraded states, and one failed state (complete failure):

- Class IV: minor/temporary/repairable failure that does not have a significant permanent impact on the operation of the spacecraft or its subsystems;
- Class III: major non-repairable failure that causes the loss of redundancy to the operation of a spacecraft or its subsystems on a permanent basis;
- Class II: major non-repairable failure that affects the operation of a spacecraft or its subsystems on a permanent basis;

- Class I: subsystem failure causing spacecraft retirements. This effectively means the total failure of the spacecraft due to a (dramatic) subsystem failure.

All the anomalies and failure events experienced by the spacecraft in the sample were collected, and their distribution across the different classes is shown in Figure 3.1.

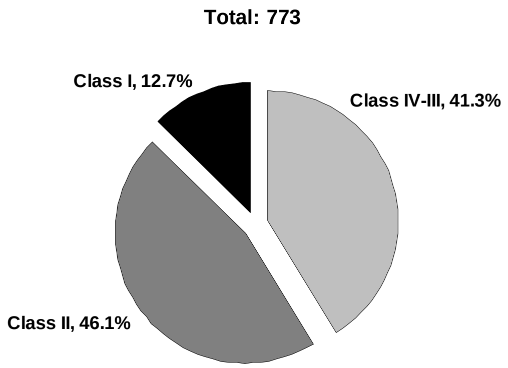


Figure 3.1. Distribution of anomaly and failure events by severity for spacecraft successfully launched between January 1990 and October 2008

Partial failures of different severities constitute a significant portion of anomalous events spacecraft experience on orbit, and as such their analysis provides additional and important pieces of information toward the understanding of spacecraft and subsystems' failure behavior and propensity. The numbers presented in Figure 3.1 should not be overly interpreted beyond the important message that they convey, namely that focusing solely on the reliability of spacecraft, defined as the probability of being in an operational (not total failure) state, misses an important part of spacecraft on orbit degradation and failure behavior. This leads to the following questions: **How can the functionality degradation of an item be analyzed?** and **How does specific spacecraft subsystems functionality degrade in time?**

3.2. Setting the Stage for Multi-State Failure Analysis

To answer these questions, the investigation of failures of spacecraft subsystems is extended in a new direction beyond the binary concept of reliability to the analysis of anomalies and multi-state failures, or failure events of different severities, as shown in Figure 3.2. Multi-state failure analysis introduces “degraded states” or partial failures, and thus provides more insights through finer resolution into the degradation behavior of an item, and its progression towards complete failure.

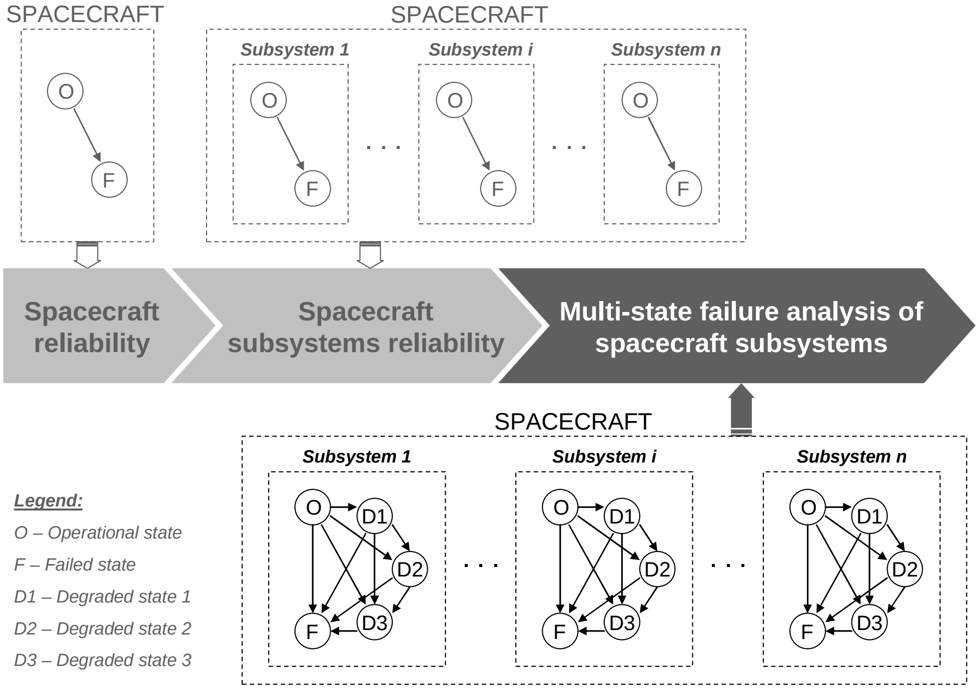


Figure 3.2. Progression in the statistical analysis of spacecraft and spacecraft subsystem failures

The failure state diagram for each subsystem is shown in Figure 3.3. State 1 (Class I failure) is referred to in stochastic modeling as an absorbing state: it cannot be recovered from, and as such no outbound transitions emanate from it. No transitions are shown on

Figure 3.3 from a partially failed state towards a higher functional state (i.e., no directed arc from S*i* to S(*i*+1) for $i \neq 1$). In reality, few transitions (3.6%) in the database occur in this "healing" direction. Incidentally, the argument in support of on-orbit servicing can be made in relation to these "healing" state transitions. This subject however is beyond the scope of the present work (see Saleh, *et al*. (2003) for details about on-orbit servicing).

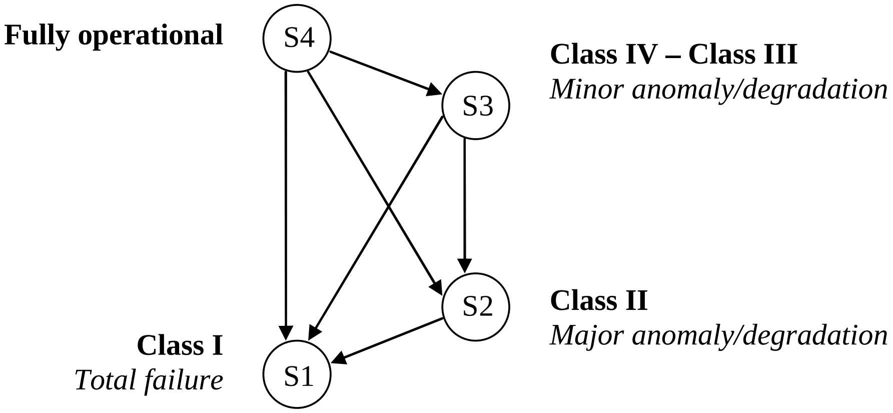


Figure 3.3. Multi-state and transition diagram for spacecraft subsystem failure behavior

Consider the following notations:

T_{ij}: transition between the state *i* and state *j*

P_{ij}: conditional probability of transitioning from state *i* to state *j*

For example the transition for a subsystem from a fully operational state (S4) to a major anomaly (S2) is labeled T_{42}, and the probability of transitioning between these two states is P_{42}. How to calculate these probabilities of transitioning is the focus of the next section.

3.3. Multi-State Failure Analysis: Theoretical Development and Application to Spacecraft Subsystems

3.3.1. Nonparametric Analyses of Subsystems' Multi-State Failures

In this section, the failure and anomaly data from all the states previously defined are used to compute the probability of transitioning from one state to another for all the spacecraft subsystems. The following data is collected for each subsystem and each state transition (*i*,*j*): 1) its date of arrival in state *i*; 2) its date of leaving state *i* to state *j*, if this transition occurred; and 3) the "censored time" if the state transition (*i*,*j*) did not occurred.

Particular attention is required in handling censoring. In addition, beyond the procedure for handling right-censored data in the binary case of reliability analysis described in the previous chapter, multi-state failures introduce an additional subtlety in the definition of censored data and its handling. The dataset is still random-censored with staggered entry, meaning the following:

- The subsystems in the sample are activated (arriving date in state *i* or launch date for $i = 4$) at different points in time, but all these activation times are known.
- Departure dates from state *i* to state *j* are stochastic (and so is censoring).
- Censoring occurs because a spacecraft is retired from the sample before T_{ij} occurs or because the end of the observation window is reached (October 2008) without the subsystem experiencing to the transition T_{ij}. In addition, in multi-state failure analysis, when studying T_{ij} for a given subsystem, censoring also occurs when the

> subsystem transitions to a state *k* different from state *j*. In this case, T_{ik} with $k \neq j$ is considered censoring for the calculation of T_{ij}. For example, when studying T_{43}, that is, the transition of a subsystem from the fully operational state to the minor anomaly/degradation state, T_{43} is censored by T_{42} and T_{41}, the transitions to state 2 and state 1 (major anomaly/degradation and total failure).

Accordingly, the Kaplan-Meier estimator needs to be adapted to estimate the conditional probability P_{ij} of transitioning from state *i* to state *j* in the context of multi-state failures with their distinct censoring. To illustrate this point, consider the transition diagram shown in Figure 3.4. The following focuses on estimating the probability of transitioning from state *i* to state *j*, P_{ij}. This in effect is a conditional probability, which means if the item is in state *i*, it is P_{ij} likely to have transitioned to state *j* by the time *t*. Recall that censoring in the binary reliability analysis implies that an item has been removed from observation (for various reasons) prior to the occurrence of failure. In multi-state failure analysis, any transition to another state than the one of interest, in the example from state *i* to state *j*, is also considered censoring. For example, in Figure 3.4, the transitions from the state *i* to the state *r* or *s* ($r \neq j$ and $s \neq j$) are considered censoring for the calculation of P_{ij}.

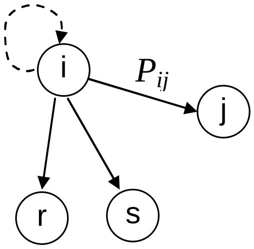


Figure 3.4. Censoring of P_{ij}

The estimate $\hat{P}_{ij}$ of P_{ij} is written as:

$$\hat{P}_{ij}(t) = 1 - \prod_{\substack{\text{all k such} \\ \text{that } t_{ij(k)} \leq t}} \hat{p}_{ij,k} = \prod_{\substack{\text{all k such} \\ \text{that } t_{ij(k)} \leq t}} \frac{n_{ij,k} - 1}{n_{ij,k}} \tag{3.1}$$

where:

$t_{ij(k)}$: time to k^{th} departure from state i to state j (arranged in ascending order)

$$\begin{aligned} n_{ij,k} &= \text{number of units in state } i \text{ right before } t_{ij(k)} \\ &= n - [\text{number of censored units right before } t_{ij(k)}] \\ &\quad - [\text{number of units having transitioned to state } j \text{ right before } t_{ij(k)}] \end{aligned} \tag{3.2}$$

The treatment of ties in the data in the context of multi-state failures is provided in Castet and Saleh (2010) and Saleh and Castet (2011). Also in these references are provided details about the construction of confidence intervals for multi-state failure analysis.

With the background information, the multi-state failure analysis of spacecraft subsystems can now be applied to the on-orbit anomaly and failure data of the 1584 spacecraft in the sample to obtain the nonparametric estimations $\hat{P}_{ij}$ of P_{ij}.

How many nonparametric calculations and $\hat{P}_{ij}$ are there? The combinatorics of the multi-state problem involves the following:

- The multi-state analysis covers 11 spacecraft subsystems and 4 states for each subsystem (plus one unknown category).
- Therefore theoretically, for each subsystem, we should calculate $4^2 = 16$ transition probabilities. This number however is reduced because of the following two reasons:
    - The probability P_{ii} is a dependent variable on all P_{ij} $(i \neq j)$ and does not require a dedicated nonparametric calculation. The consequence is that we are left with $4^2 - 4 = 12$ transition probabilities $\hat{P}_{ij}$ to estimate (i.e., no estimation of $\hat{P}_{ii}$)
    - With the additional assumption of no transition in the healing direction, the transitions from a partially failed state towards a higher functional state are eliminated, and $12 - (3 + 2 + 1) = 6$ transition probabilities $\hat{P}_{ij}$ are left to estimate for each subsystem, as shown in Figure 3.3.

With 11 subsystems and 6 possible state transitions for each subsystem to calculate, there are 66 nonparametric probabilities to estimate (excluding the unknown category). In addition, two (nonparametric) calculations for each transition probability are required to estimate the 95% confidence interval. As a result, 198 nonparametric calculations are needed to fully characterize the multi-state failure behavior of the satellites in the sample, given the number of subsystems and the classes of failures identified. This proliferation of transition probabilities is in effect one of the main difficulties in statistically handling multi-state failures compared to the simple (binary) reliability analysis, and is rightfully described as the “dimension damnation” by Lisnianski and Levitin (2003). However, the insights that emerge from multi-state failure analysis are significantly worth this added complexity, as will be shown shortly.

Figure 3.5 provides an example of the nonparametric calculations. Shown are the six transition probabilities of the Gyro / Sensor / Reaction wheel subsystem. Figure 3.5 reads as follows. For example, after four years on-orbit, the Gyro subsystem is roughly 4.8% likely to have transitioned from state 4 to state 3 (minor anomaly; additionally P_{43} will fall between 3.5% and 6.0% with 95% confidence), 1.3% likely to have transitioned from state 4 to state 2 (major anomaly), and 0.3% likely to have transitioned from state 4 to state 1 (total failure). The probabilities of transitioning P_{41}, P_{31} and P_{21} provide a finer resolution in the mechanisms leading to the total loss of the spacecraft, as opposed to traditional reliability analyses that lump together these transitions.

Several transitions between states for various subsystems are not present in the dataset here analyzed. For example, for the Thruster / Fuel subsystem has no transition that occurred on orbit between a minor anomaly (State 3) and a complete failure (State 1) in the dataset. As a result, this transition is not subject to statistical analysis. Other transitions also do not occur in the dataset, thus reducing the total number of transitions to 48 and a total of 144 nonparametric calculations (excluding the unknown category). The absent transitions can be seen in Table 3.1 and Table 3.2 noted as “NA”. All the 144 calculations are not shown here for convenience, but more are provided in Castet and Saleh (2010) and Saleh and Castet (2011). The parametric fits for all these transition probabilities are provided next.

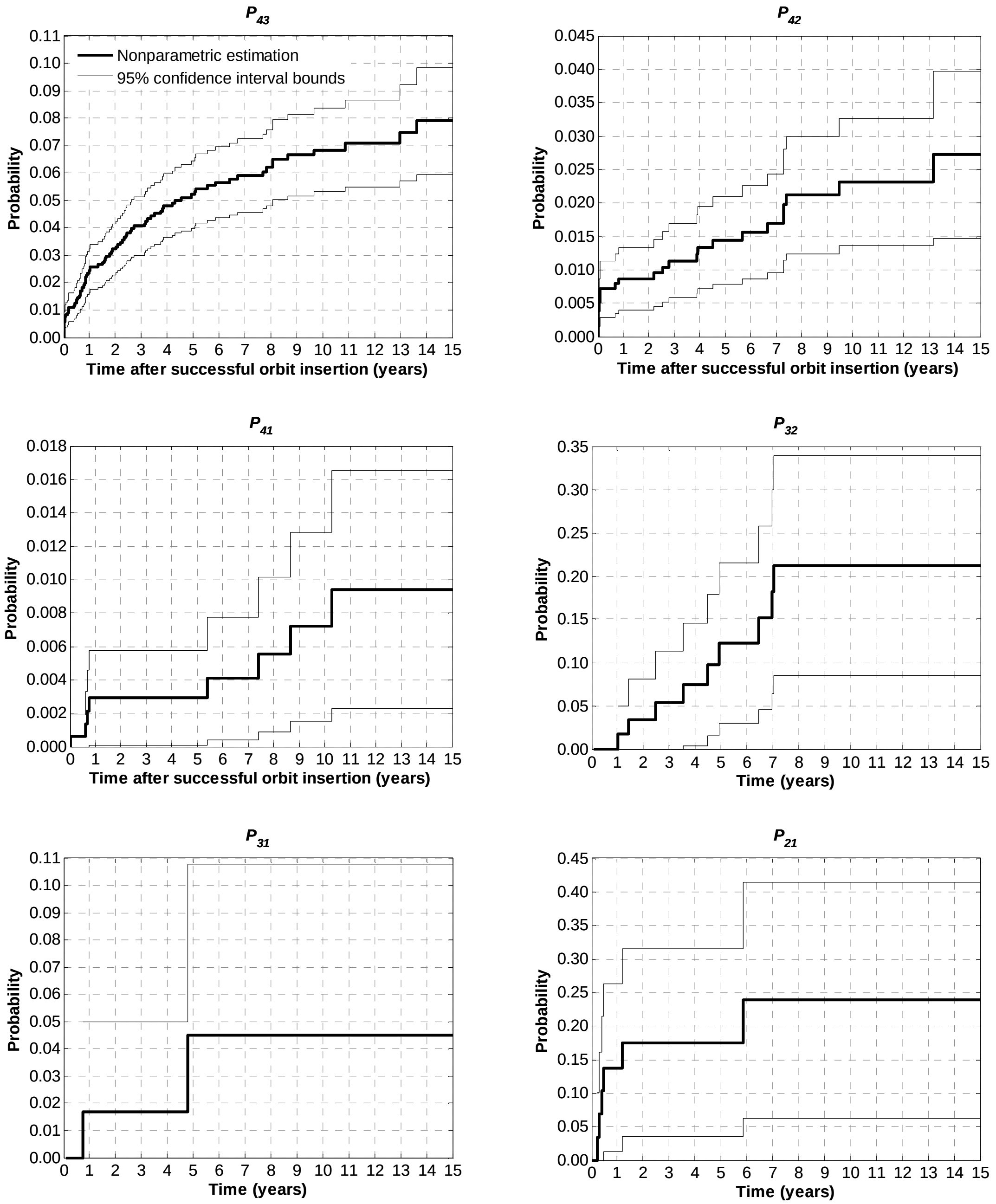


Figure 3.5. Probabilities of transitioning for the Gyro subsystem

3.3.2. Weibull Parametric Models

Since the interest herein is in the cumulative failure likelihood (the transition to a degraded state), the shape and scale parameter of the following are calculated with the MLE procedure, and given in and Table 3.1 and Table 3.2:

$$P_{ij}(t) = 1 - \exp\left[-\left(\frac{t}{\theta}\right)^{\beta}\right] \tag{3.3}$$

Table 3.1. Weibull parameters for the spacecraft subsystems P_{ij} (β is dimensionless, θ is given in years)

Gyro / Sensor / Reaction wheel			**Thruster / Fuel**			**Beam / Antenna operation / deployment**		
P_{ij}	β	θ	P_{ij}	β	θ	P_{ij}	β	θ
P_{43}	0.4731	2758	P_{43}	0.3827	171879	P_{43}	0.0019 *	
P_{42}	0.3685	336231	P_{42}	0.4763	8591	P_{42}	0.2468	436409190
P_{41}	0.5635	65547	P_{41}	0.3114	29975357	P_{41}	NA	
P_{32}	1.1950	33	P_{32}	0.6052	46	P_{32}	NA	
P_{31}	0.7551	546	P_{31}	NA		P_{31}	NA	
P_{21}	0.4653	134	P_{21}	0.2632	589300	P_{21}	NA	
Control Processor			**Mechanisms / Structures / Thermal**			**Payload Instrument / Amplifier / On-board data / Computer / Transponder**		
P_{ij}	β	θ	P_{ij}	β	θ	P_{ij}	β	θ
P_{43}	0.6585	3562	P_{43}	0.3840	4952368	P_{43}	0.4474	4065
P_{42}	NA		P_{42}	0.0060 *		P_{42}	0.4691	3170
P_{41}	NA		P_{41}	0.3572	19794952	P_{41}	0.6701	119171
P_{32}	0.5487	1056	P_{32}	NA		P_{32}	0.6647	38
P_{31}	0.7231	45	P_{31}	NA		P_{31}	NA	
P_{21}	1 *		P_{21}	NA		P_{21}	0.2513	169439610

* Due to the constant form of the nonparametric curve, a Weibull fit is not meaningful in these cases. The values are the probabilities of transitioning over 15 years.

Table 3.2. Weibull parameters for the spacecraft subsystems P_{ij} (β is dimensionless, θ is given in years)

Battery / Cell			Electrical distribution			Solar array deployment		
P_{ij}	β	θ	P_{ij}	β	θ	P_{ij}	β	θ
P_{43}	0.3855	9946825	P_{43}	0.3663	13753674	P_{43}	0.0015 *	
P_{42}	0.4134	357357	P_{42}	0.3526	11893973	P_{42}	0.0040 *	
P_{41}	0.9239	4431	P_{41}	0.5215	144569	P_{41}	0.0013 *	
P_{32}	NA		P_{32}	1.1329	38	P_{32}	NA	
P_{31}	NA		P_{31}	NA		P_{31}	NA	
P_{21}	0.2353	1936	P_{21}	0.4618	376	P_{21}	NA	

Solar array operating			Telemetry, Tracking and Command[2]			Unknown		
P_{ij}	β	θ	P_{ij}	β	θ	P_{ij}	β	θ
P_{43}	0.3216	3237079	P_{43}	0.3668	205920	P_{43}	NA	
P_{42}	0.4724	4313	P_{42}	0.5249	19577	P_{42}	0.3766	1471383
P_{41}	0.2527	3.45E10	P_{41}	0.3098	29482835	P_{41}	0.4020	5578316
P_{32}	0.7268	16	P_{32}	0.2273	390440	P_{32}	NA	
P_{31}	0.5935	646	P_{31}	NA		P_{31}	NA	
P_{21}	0.4307	4501	P_{21}	0.3374	87	P_{21}	NA	

* The Solar Array Deployment is a one-shot “subsystem” and a Weibull fit is not meaningful in this case. Thus these are the probabilities of transitioning over 15 years.

Figure 3.6 shows the nonparametric curves (with the 95% confidence interval) for the $\hat{P}_{43}$ of the Gyro subsystem, and the $\hat{P}_{42}$ of the Thruster / Fuel subsystem, superimposed on their respective MLE Weibull fits. Figure 3.6 provides a visual confirmation that the Weibull distributions with the MLE parameters provided in Table 3.1 are good fits for the $\hat{P}_{43}$ of the Gyro subsystem and the $\hat{P}_{42}$ of the Thruster / Fuel subsystem. Similar results are obtained for the other probabilities of transitioning of the spacecraft subsystems using the Weibull parameters given in Table 3.1 and Table 3.2.

[2] These results exclude the endemic failures of the TTC subsystem of the GLOBALSTAR fleet (47 Class II failures).

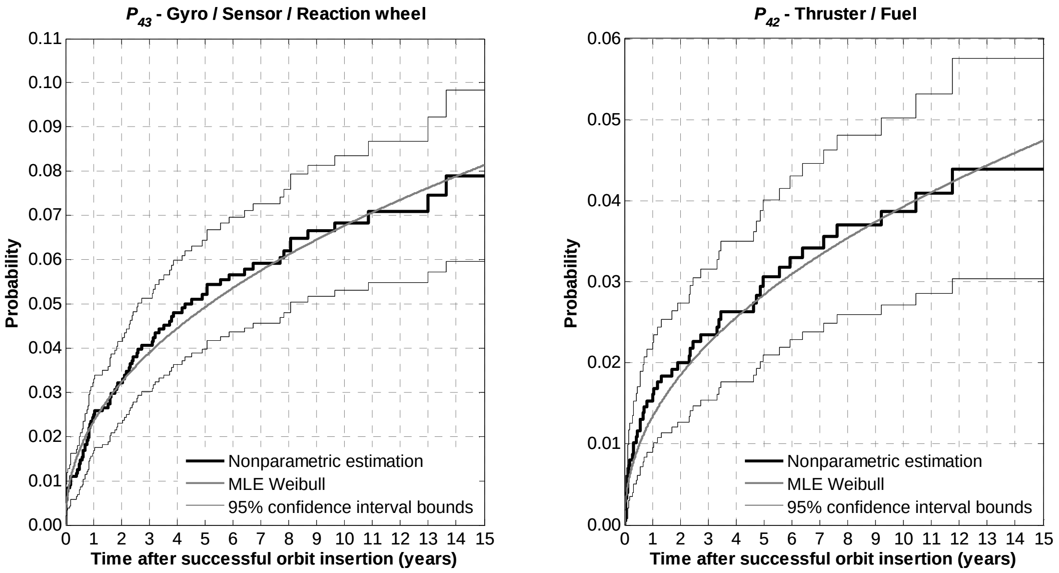


Figure 3.6. Examples of nonparametric probabilities of transitioning and Weibull fits

Given the relative complexity of subsystem models, several tests were devised to verify that the parametric models were properly derived, and that they reflected actual on-orbit data. This validation procedure is presented in Castet and Saleh (2010) and Saleh and Castet (2011). The conclusion of the validation is that the parametric models are appropriate and exhaustive.

3.3.3. Discussion about Uncertainty and Confidence Interval Spread

For reliability or multi-state analyses, the uncertainty that arises from the censoring in the data (or the lack of a complete data set) is captured by the confidence intervals. Indeed, the Kaplan-Meier estimator (for reliability or the adapted one for the probabilities of transitioning) provides a maximum likelihood estimate, but does not inform about the dispersion around that estimate. As a consequence, it is necessary to build confidence intervals to display the uncertainty associated with the best estimate, and their analysis yields interesting observations. Note that the confidence interval spread increases with time, as seen for example in Figure 2.2 (spacecraft reliability), Figure 2.7 and Figure 2.8 (spacecraft subsystems reliability) and Figure 3.5 (probabilities of transitioning between states for the Gyro subsystem). For example, in Figure 2.2, after two years on-orbit, the spacecraft reliability is dispersed over a 2 percentage point interval (with 95% confidence), whereas after 12 years on-orbit, the satellite reliability is dispersed over a 3.7 percentage point interval. In the case of the multi-state analysis, the probability of transitioning between the fully operational state and the minor anomaly state, P_{43}, for the Gyro subsystem is dispersed over a 1.6 percentage point interval after 1 year on orbit, while it is dispersed over 3.9 percentage point interval after 15 years on orbit. This is a direct result of the decreasing sample size with time and how it is handled in Eq. (2.3) for reliability analysis as more spacecraft fail or are retired from the sample due to censoring effects or in Eq. (3.1) for multi-state analysis as more spacecraft transition to the state of interest or are retired from the sample due to censoring effects. The spread of the confidence intervals remains small and shows that these reliability and multi-state failure results are precise.

Another observation about uncertainty in multi-state analysis can be seen in Figure 3.5: in the case of the Gyro subsystem, the confidence interval spread is larger for P_{32}, P_{31} and P_{21} than for any probabilities of transitioning out of the fully operational state S4 (P_{43}, P_{42} and P_{41}). For example, the maximum confidence interval spread is about 11 percentage points for P_{31}, while the maximum spread for P_{42} is about 2.5 percentage points. This is a direct consequence of the difference in sample size for deriving probabilities of transitioning: for the transitions out of S4, the sample consists of all the 1584 spacecraft in the sample used in Chapter 2, while the samples for the transitions out of S3 and S2 are reduced to the spacecraft among the 1584 spacecraft that effectively transitioned to these states in the original sample. In the case of the Gyro, 62 spacecraft transitioned to a minor degradation state (S3) and 30 to a major degradation state (S2). A similar trend can be observed for all the spacecraft subsystems under consideration in this thesis. The impact of this uncertainty on the probabilities of residency in degraded states is lessened due to the small number of spacecraft that are subjected to these transitions. Decreasing the uncertainty (decreasing confidence interval spread) could be obtained by collecting more precise and complete data about the degradation and failure behavior of spacecraft subsystems for these states, with improved spacecraft state of health (SOH) monitoring, or running accelerated life testing (ALT).

The multi-state results and further simulations in this thesis are confined to the best estimates of these probabilities. Propagating their uncertainties to the final results could bring an additional piece of information to the degradation and failure behavior of the different space systems considered, and could be a fruitful avenue for future improvements.

3.4. Comparative Reliability and Multi-State Failure Analyses of Spacecraft Subsystem: the Thruster/Fuel Subsystem Example

In this section, complete multi-state failure results are provided, resulting from simulations, for a specific spacecraft subsystem: the Thruster / Fuel subsystem. This subsystem was chosen in part because it was identified in the previous chapter as a major culprit driving spacecraft unreliability. In addition, this subsystem was chosen because its multi-state failure analysis clearly identifies key insights that cannot be captured by the traditional (binary) reliability analysis. However, multi-state analyses have been conducted for all subsystems, and plots are presented in the appendix of this chapter. Analyses of more subsystems (e.g., the Gyro or the TTC) are presented in Castet and Saleh (2010) and Saleh and Castet (2011).

The Thruster/Fuel subsystem is a major contributor to spacecraft failures, especially over the early years of the spacecraft service life. For example, over the first 10 years on orbit, 13% of all spacecraft failures are due to the Thruster/Fuel subsystem, and for the first year on orbit, 20% of all spacecraft failures are due to this subsystem. Figure 3.7 shows on the left the reliability curve and the probability of being in state 4, that is, the probability of being fully operational for the Thruster/Fuel subsystem. The reliability curve, or survivor function, represents the probability of the subsystem not being in the failed state 1. On the right of Figure 3.7 are shown the different probabilities of being in degraded states, from state 1 to state 3.

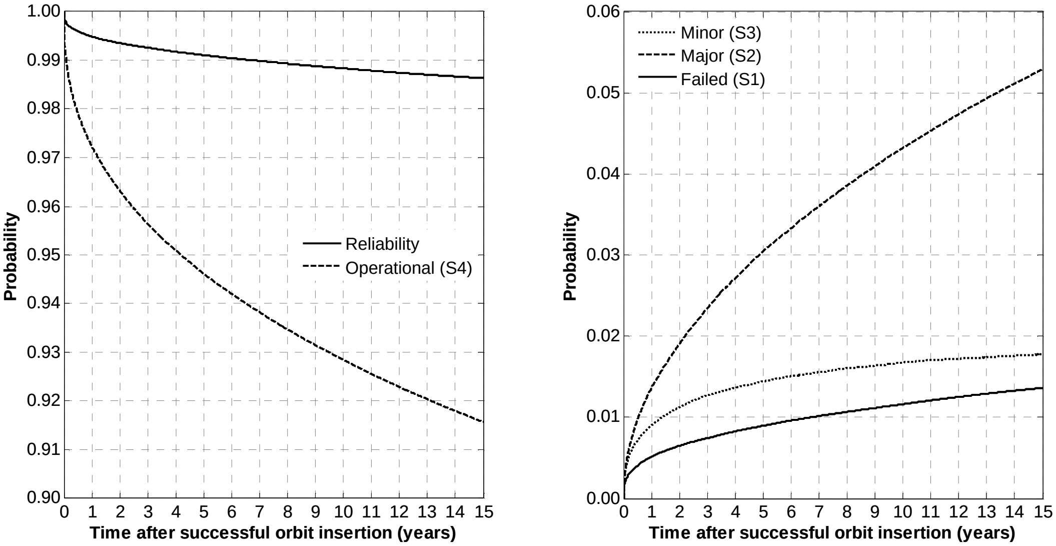


Figure 3.7. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Thruster / Fuel subsystem

Figure 3.7 highlights an important distinction that is made in multi-state failure analysis but that cannot be captured by the traditional (binary) reliability analysis, namely the distinction between being in a fully operation state and being in the non-total failure state. To clarify this point, consider the following. The two left curves in Figure 3.7 are separated by a distinct and growing gap, with roughly 7 percentage point difference at *t* = 15 years. The upper reliability curve indicates that the subsystem is 98.5% reliable after 15 years, that is, the subsystem is 98.5% likely to be operational (not broken), whereas the multi-state failure analysis (lower curve) indicates that the subsystem is only 91.5% likely to be fully operational after 15 years.

The difference is not negligible and can have important consequences, the most important probably being that a 98.5% reliable subsystem after 15 years may not trigger any engineering action whereas a 91.5% fully operational subsystem may prompt a careful analysis of the subsystem (partial) failure modes and support improvement efforts.

The distinction between these two probabilities of a subsystem occupying different states (fully operational versus non-total failure states) lies of course in the partial failures that are introduced and probed by the multi-state failure analysis. The probabilities of occupying any one of the failure states over 15 years are shown on the right of Figure 3.7, and read as follows. For example, at *t* = 10 years, there is a 1.7% probability that the subsystem is in a minor anomaly state (S3), 4.4% that the subsystem is in a major anomaly state (S2)—these states and probabilities are not visible to the traditional reliability analysis—and a 1.1% that the subsystem is totally failed (S1). This last probability is in effect the complement of the reliability of the subsystem (the failed curve on the right of Figure 3.7 is the complement of the reliability curve on the left of Figure 3.7).

The most interesting feature of the multi-state failure analysis of this subsystem is the dynamics of the degraded states, and especially the probability of being in the major anomaly state (S2). The probability of being in a minor anomaly is low (less than 2%), whereas the probability of being in a major anomaly state is significantly higher, continuously increasing over the years to eventually reach approximately 5% after 15 years. The fast increase in the probability of transitioning to state 3 (major anomaly) in the early years can be termed “infant severe degradation” of the Thruster/ Fuel subsystem, as the multi-state analog of the infant mortality concept in traditional reliability analysis.

In summary, when the Thruster/ Fuel subsystem (partially) fails, it is likely to “fail hard”, i.e., with a transition to a major anomaly/degradation state (S2). The Thruster/ Fuel subsystem has previously been identified as one of the major culprits driving spacecraft failures. The present multi-state failure analysis also shows that this subsystem experiences significant degradations in its functionality on-orbit. This provides an additional indication for spacecraft manufacturers and equipment providers to focus their attention on improving the Thruster / Fuel subsystem, and more generally on subsystems that either drive spacecraft failures or that have a high propensity for major degradations.

3.5. Summary

This chapter provided multi-state failure analyses of spacecraft subsystems as an extension of the previous chapter results on spacecraft and spacecraft subsystems reliability. Multi-state failure analysis introduces “degraded states” or partial failures and provides additional insights on the failure and degradation behavior of an item. In this chapter, a formal theoretical framework was established to conduct multi-state failure analyses, and applied to gather information about the degradation of spacecraft subsystems. The models obtained were shown to appropriately capture the multi-state failure characteristics of the subsystems. The results provided by the multi-state failure analysis can thus be used to prompt further detailed investigation into the “physics of anomaly and failure” of particular spacecraft subsystems and guide technical efforts towards the identification of subsystem failure modes and their elimination.

3.A. Appendix: Multi-State Failure Analysis of Remaining Subsystems

Gyro / Sensor / Reaction wheel

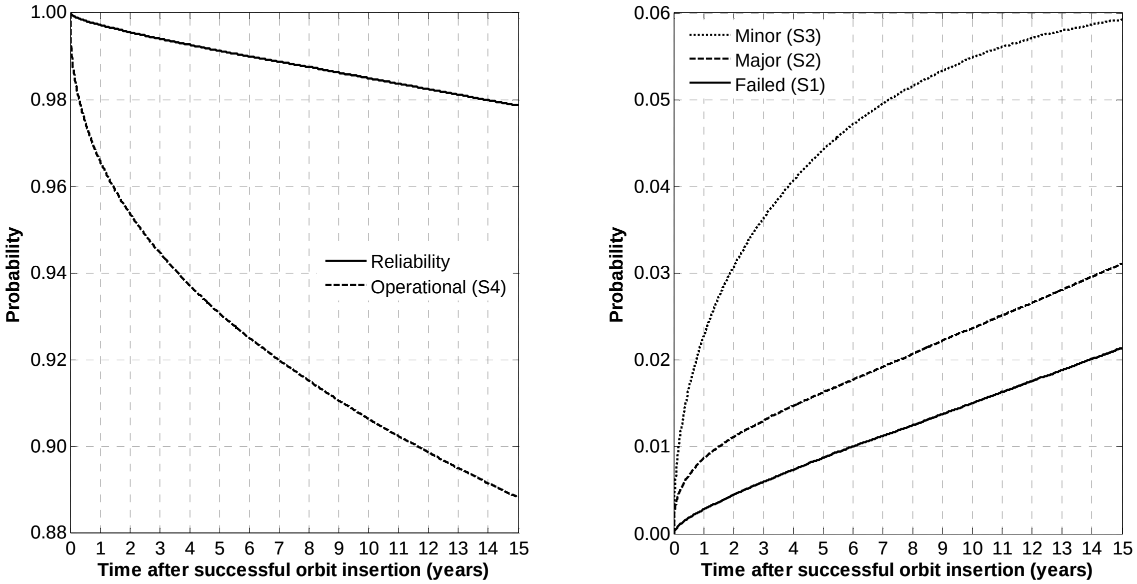


Figure 3.A. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Gyro / Sensor / Reaction wheel subsystem

Beam / Antenna operation / deployment

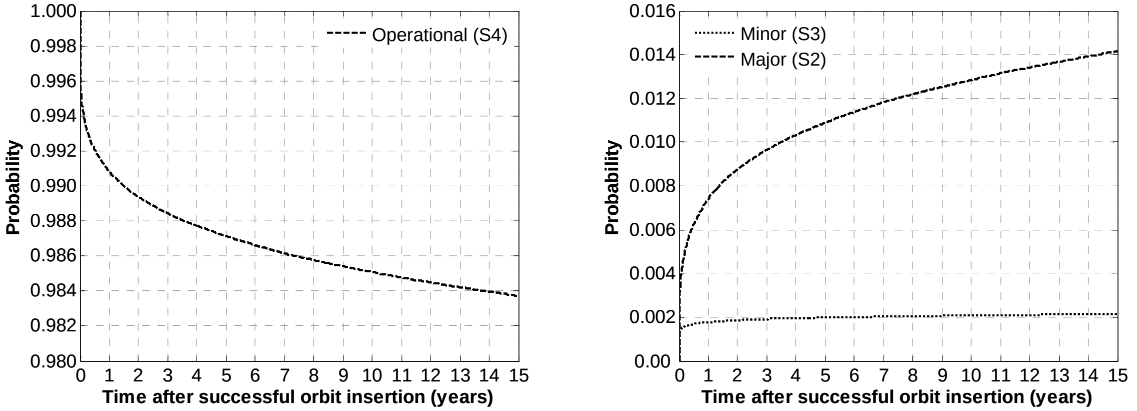


Figure 3.B. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Beam / Antenna operation / deployment subsystem

Control processor

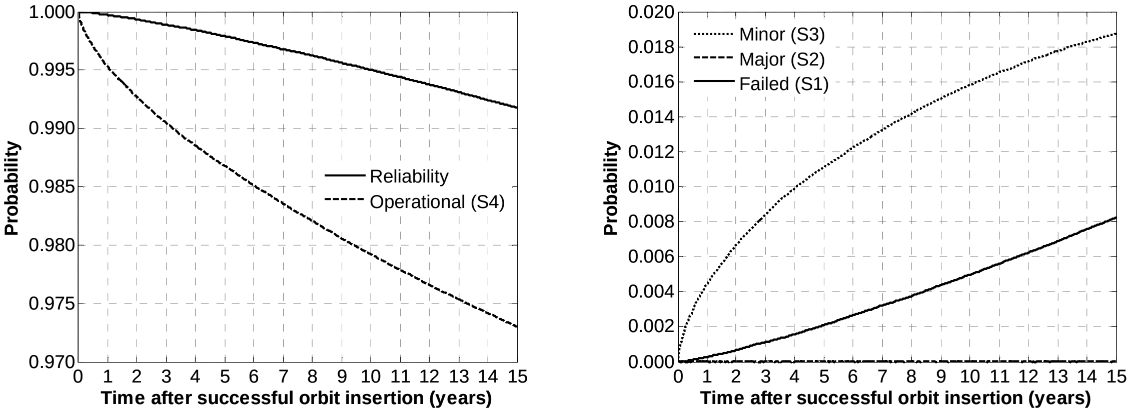


Figure 3.C. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Control processor subsystem

Mechanisms / Structures / Thermal

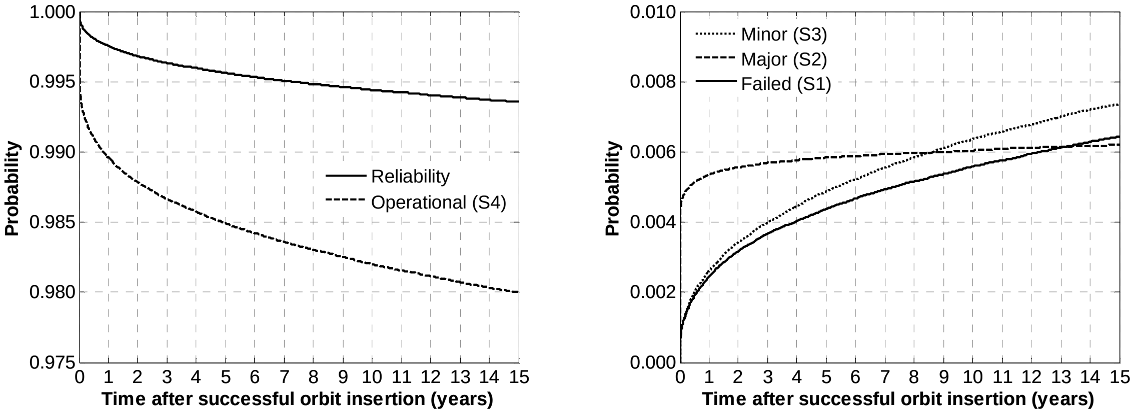


Figure 3.D. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Mechanisms / Structures / Thermal subsystem

Payload instrument / Amplifier / On-board data / Computer / Transponder

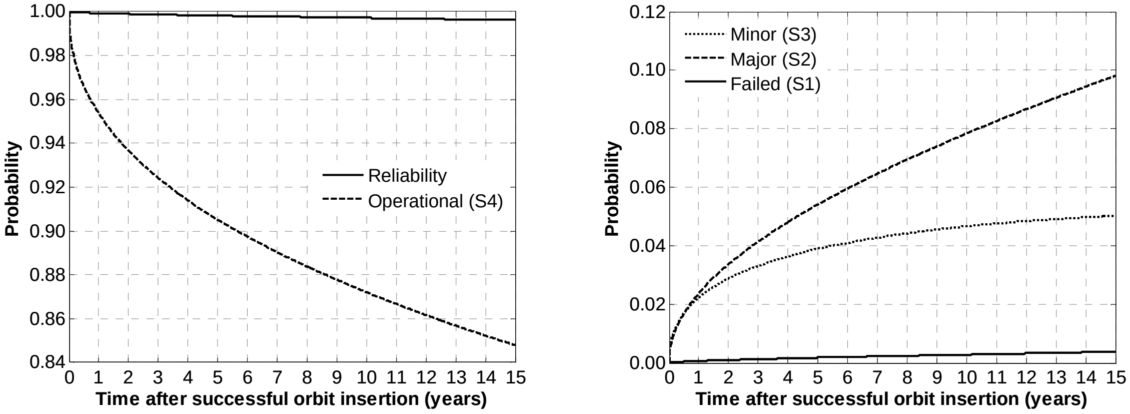


Figure 3.E. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Payload instrument / Amplifier / On-board data / Computer / Transponder subsystem

Battery / Cell

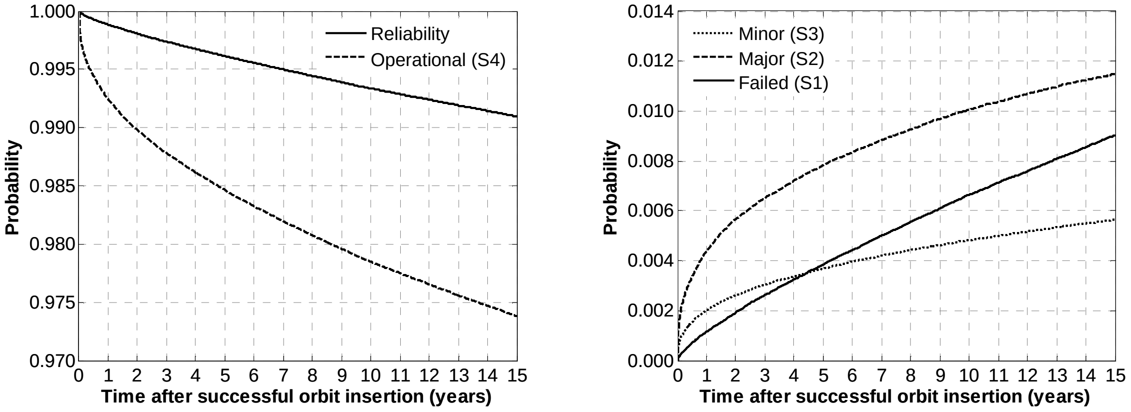


Figure 3.F. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Battery / Cell subsystem

Electrical distribution

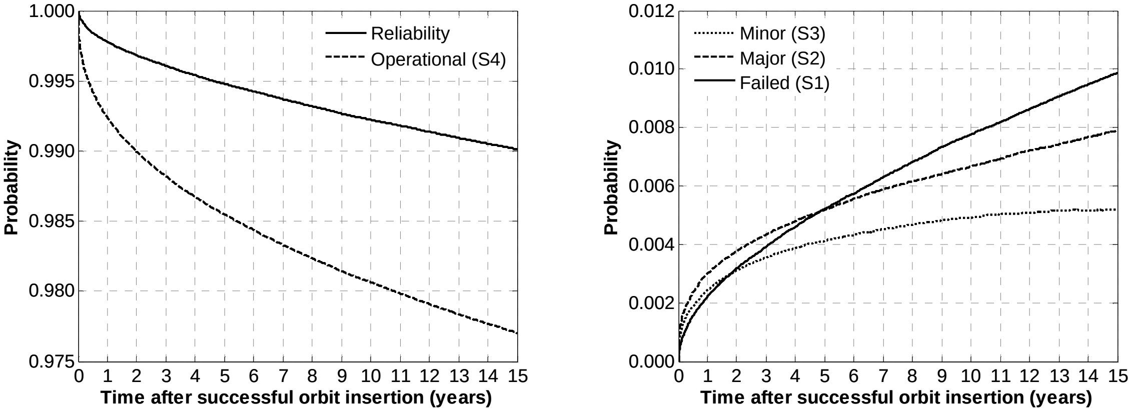


Figure 3.G. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Electrical distribution subsystem

Solar array deployment

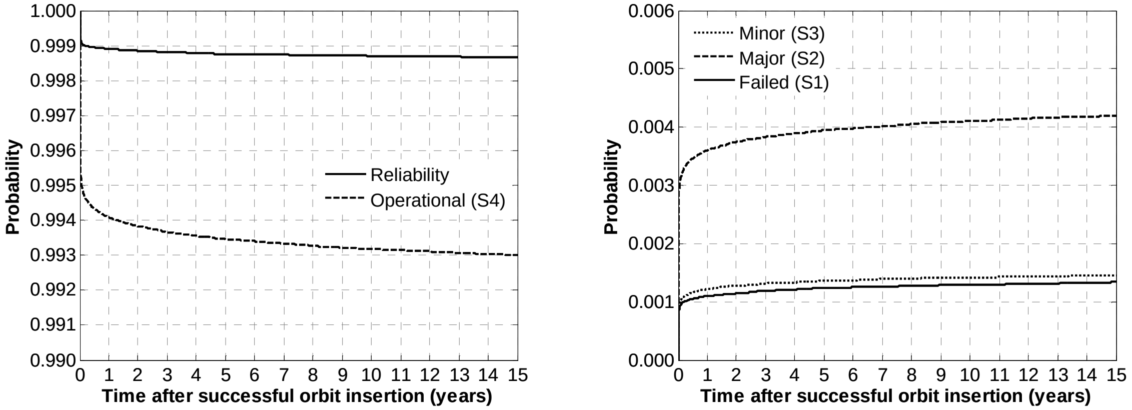


Figure 3.H. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Solar array deployment subsystem

Solar array operating

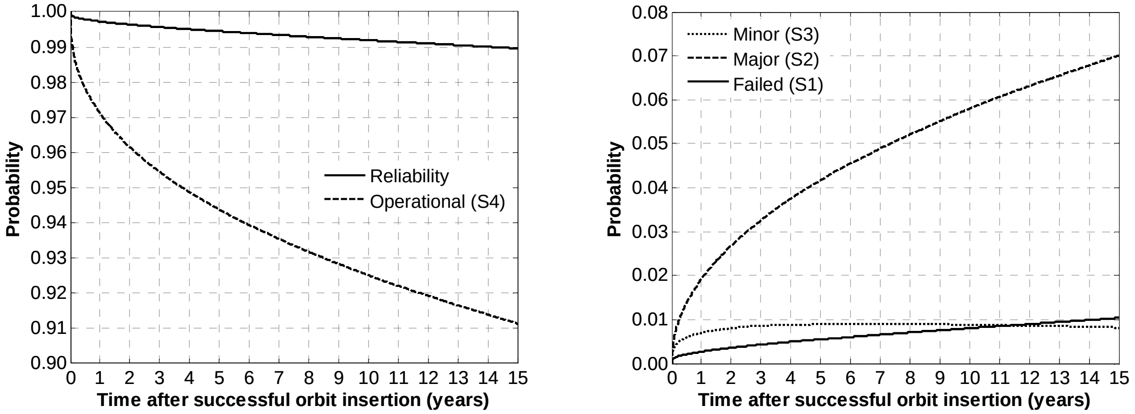


Figure 3.I. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Solar array operating subsystem

Telemetry, Tracking and Command

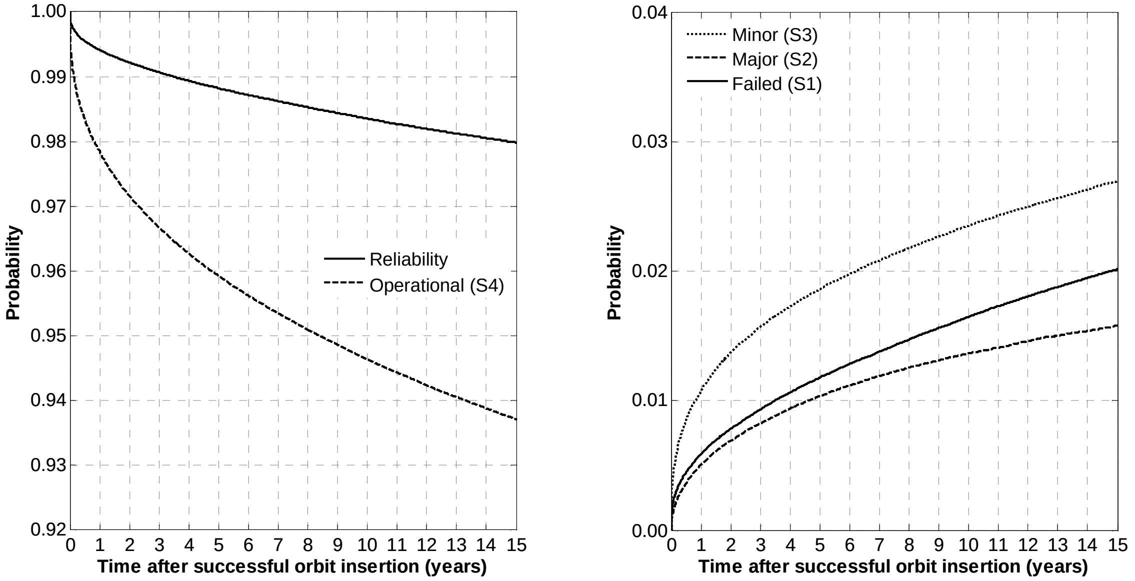


Figure 3.J. (left) Reliability and probability of being fully operational and (right) degraded states probabilities for the Telemetry, Tracking and Command subsystem

PART 2

SURVIVABILITY OF SPACECRAFT AND SPACE-BASED NETWORKS

CHAPTER 4

SURVIVABILITY AND INTERDEPENDENT MULTI-LAYER NETWORKS: SETTING A NOVEL FRAMEWORK FOR ANALYSIS

Modeling, analyzing, and predicting failures is a central focus to many engineering disciplines dealing with system design and operations, such as civil, aerospace, and electrical engineering. Given the design and development of increasingly complex and interconnected systems, it has become even more important to analyze the propensity to failures of said systems and whether they would experience catastrophic failures or graceful degradations following node or component failures for example. These failures may be triggered by endogenous or exogenous causes (e.g., attacks), and the analysis would assess, among other things, how localized failures or disruptions would propagate throughout the system. These concerns fall within the realm of survivability analysis.

In this second part, the survivability assessment of spacecraft and what is termed in this work Space-Based Networks (SBNs) is sought. SBNs are related to a novel concept recently introduced in the space industry termed fractionation (Brown and Eremenko, 2006a; 2006b). By physically distributing functions in multiple orbiting modules wirelessly connected to each other, this new architecture allows the sharing of resources on-orbit, such as data processing, data storage, and downlinks. Preliminary analysis suggests that such an architecture, under certain conditions and despite some initial overhead, offers several advantages over the traditional monolith spacecraft design in terms of utility versus cost (details can be found in Dubos and Saleh, 2011).

As mentioned above, survivability analysis considers system component failures, and among them, endogenous failures. As a consequence, the knowledge from the failure models of spacecraft subsystems developed in Part 1 is leveraged in this second part to assess the survivability of spacecraft and space-based networks and answer the following questions: **How can the survivability of spacecraft and SBNs be assessed**? and **What insights for design and architectural choices of spacecraft and SBNs can arise from survivability analyses**?

Before describing this thesis' proposed model for survivability assessment of spacecraft and SBNs, an overview of the survivability concept is presented first. The survivability framework is then followed by literature highlights on network analysis for introducing a new modeling technique for space-based networks.

4.1. Survivability: Literature Highlights

In this section, a brief overview of the concept of survivability is provided. Survivability is extensively used in the technical literature as multi-disciplinary concept in a variety of contexts and often with different meanings.

4.1.1. Military Context

Survivability as a system attribute has always been important to the military, and its experimental and analytical assessment was probably heightened since the 1960's (Ball and Atkinson, 1995). Survivability in a military context is applied to platforms (e.g., aircraft), people, systems (e.g., military network), and nowadays more generally to missions. Several articles show this evolution, from one of the first attempts to assess survivability of an aircraft in 1967 (Atkinson, *et al.*, 1969; Ball and Atkinson, 1995) to some more general definitions (MIL-STD-2069, 1961; MIL-HNBK-336-1, 1982; MIL-HDBK-2069, 1997; DoD Regulation 5000.2-R, 1999) as the one provided by the DoD Regulation 5000.2-R (1999): "[survivability is] the capability of a system and crew to avoid or withstand a man-made hostile environment without sustaining an impairment of its ability to accomplish its designated mission. Survivability consists of susceptibility, vulnerability, and recoverability." Susceptibility is "the degree to which a weapon system is open to effective attack because of one or more inherent weakness"; vulnerability is "the characteristic of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform its designated mission) as a result of having being subjected to a certain (defined) level of effects in an unnatural (man-made) hostile environment"; recoverability is "the ability, following combat damage, to take emergency action to prevent the loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities." In addition, several publications addressed the issue of survivability of military communication networks, a growing area of interest and research since the 1990's, and for which survivability of the network is defined as the "ability to maintain communication among the nodes when it is subject to deliberate destruction" (Haizhuang Kang, *et al.*, 1998).

4.1.2. Engineering Context

Following its initial analysis within a military context, the concept of survivability spread to other areas than the military, especially to electrical engineering with an emphasis on software, telecommunications, and information systems. In particular, survivability has become of major interest for network systems designers since society has become significantly dependent on a variety of networks, leading to severe consequences in the case of network system disruptions or failures. While the use of "survivability" is widespread within the technical community, no definition is unanimously adopted. Westmark (2004) compiled 53 definitions of survivability from different publications and synthesized the following definition: survivability, according to Westmark, is "the ability of a given system with a given intended usage to provide a pre-specified minimum level of service in the event of one or more pre-specified threats." One of the more cited definitions of survivability is provided by Ellison *et al*. (1999): survivability, according to Ellison *et al*., is the "capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents". Knight *et al*. (2003), while focusing on survivability in a telecommunications and network context, found previous definitions not precise enough, and proposed a formal definition of survivability based on six quantitative parameters (or sextuple). He characterized a system as "survivable if it complies with its survivability specification," and the survivability specification is mathematically defined, gathering all acceptable levels of service from the system, the associated services values and relative values (perceived by the user), its probabilistic requirements and its possible transitions in a specified operating environment. Accordingly, survivability definitions teeter between the informal and the formal, and occasionally, they include probabilistic terms. But, as the previous definitions indicate, survivability is context-specific, related to the system studied and its environment, the services it provides to users, and the requirements that have been set for it. This specificity explains why often survivability seems to be a more generic word defined or measured in terms of other notions, like availability, performance, traffic capacity, connectivity, etc.

4.1.3. Survivability Concept Summary

Since the definition of survivability is context-specific, the environment, the threat(s), and the performance index have to be specified each time an analysis is conducted. Figure 4.1 provides a notional representation of a system response facing a shock or disruption. The survivability of the system is related to the performance degradation[3] ΔP. The extent of the performance drop depends on the survivability features of the system: the more survivable (with respect to the defined threat), the smaller the drop (in the performance metric of interest). The response of the system after the shock characterizes the recoverability of the system, which in simple terms can be thought of as the time needed for the system to return within a certain percentage of its initial level of performance. However, the study of the system recoverability is out of the scope of the thesis and will not be addressed in the following.

[3] As a side note, graceful degradation, which is particularly desirable for systems with high-availability requirements, allows a system to keep operating and providing some level of service by staging the system's performance degradation over time.

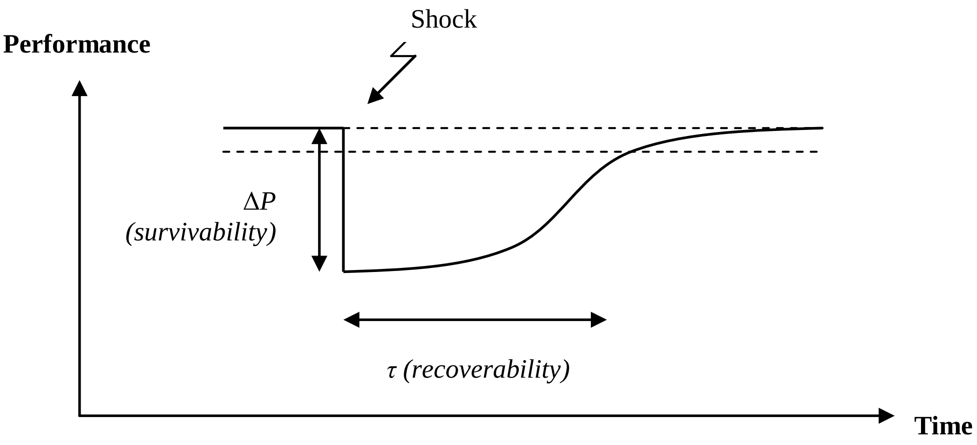


Figure 4.1. Notional system response following a shock

4.2. Survivability Framework

This dissertation introduces a notional **framework for survivability analysis** is shown in Figure 4.2 and this framework captures the different steps through which survivability analysis proceeds.

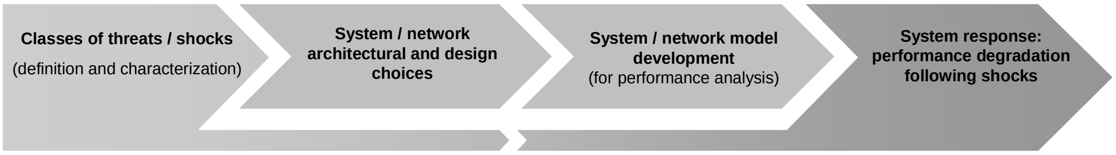

Classes of threats / shocks
(definition and characterization)
System / network architectural and design choices
System / network model development
(for performance analysis)
System response: performance degradation following shocks

Figure 4.2. Survivability framework

Figure 4.2 starts to the left with the definition or delineation of the classes of threats or types of disruptions the analyst is interested in assessing the system's survivability with respect to. Survivability, like the concept to optimization, remains ill-defined unless an additional information is provided: what the system is optimized with respect to for the latter, and what the system is survivable with respect to for the former. The characterization of the classes of threats or types of disruptions of interest constitutes the first step in a survivability analysis. The second step in Figure 4.2 is design-centric and seeks to characterize the architecture of the system under consideration, its (functional) structure and design choices (e.g., modularity, coupling, redundancy, etc.), in particular the features that pertain to its performance. The third step in Figure 4.2 transforms the previous step into an analytical or computational model of the system to assess its survivability with respect to the classes of threats or types of disruptions of interest. Finally the last step in Figure 4.2 consists in assessing the system's performance degradation—its survivability assessment—following disruptions, using the system model previously developed and the characterization of the classes of threats or types of disruptions of interest (step 1).

Step 3 requires the modeling of the architecture for which a survivability assessment is desired. This thesis is particularly interested in investigating the survivability features of spacecraft and space-based networks. Modeling space-based networks falls in the realm of network analysis, and a brief literature review of network analysis is provided next. This literature highlights the limitations of the application of current models and tools for space-based networks in particular, and stresses the need of introducing a new approach to remedy the underlined shortcomings.

4.3. Networks: Literature Highlights and Limitations for Space-Based Networks

Networks have been widely studied (Newman, 2010; Albert and Barabási, 2002), as they can describe a large number of technical, biological or social systems: the World Wide Web and the Internet, power grids, telecommunications systems, social relationships, food webs, to cite a few. Graph theory and analyses of real networks allowed a better understanding of network properties (random graphs, scale-free networks, etc.) and the definition of metrics to describe network characteristics (Newman, 2010; Albert and Barabási, 2002).

Networks have also been studied with respect to failure propagation and cascading failures (Motter and Lai, 2002; Crucitti, *et al*., 2004; Ash and Newth, 2007; Kurant and Thiran, 2007; Buldyrev, *et al*., 2010; Zio and Sansavini, 2011; to cite a few). A simple model for cascading failures in communication/transportation network was to dynamically redistribute the flow on the network after the failure of a node, this redistribution leading to the overload of other nodes in a cascading fashion (Crucitti, *et al*., 2004). More recent analyses pointed that the failure behavior of a significant number of modern networks could not be independently studied as these networks are coupled together: for example, the electrical power network and the Internet network rely on each other for communication and control on one hand, and electricity supply on the other hand (Buldyrev, *et al*., 2010). Such analyses showed that while an independent single network will break down after the removal of a significant number of nodes, interdependent networks can fail catastrophically after the removal of a small fraction. This approach led to the introduction of interdependent network analyses to characterize properties of networks (e.g., Rinaldi, 2004; Newman, *et al*., 2005; Kurant and Thiran, 2006; Knippel and Lardeux, 2006; Wong-Jiru, *et al*., 2007; Buldyrev, *et al*., 2010; Donges, *et al*., 2011; Xu *et al*., 2011). More particularly, Kurant and Thiran (2006) introduced the concept of a two-layered network to study the dynamics of a transportation system: they noted that the representation of such systems as a single network was inappropriate as it did not allow both the modeling of the physical topology of the network and the traffic flow on it. Also, Xu *et al*. (2011) introduced the concept of interconnecting bilayer networks, where networks on both layer could share some common nodes (e.g., the networks of scientists and musicians can share similar persons, as a person can both be a scientist and a musician).

However, these analyses and tools cannot be directly applied to the study of space-based networks for a fundamental reason pertaining to the nature of SBNs. These analyses usually assume homogeneous (or identical) nodes in the networks, while spacecraft in an SBN can have different components due to the fractionation of the functionality, resulting in **node heterogeneity**.

To illustrate this, let us take the example that is going to be a case study later in this dissertation: the space-based network (SBN) here considered is simple and consists of two networked spacecraft that can tap into the other spacecraft's TTC in case of damage or failure of its own TTC. This architecture is shown in Figure 4.3. In essence, the wirelessly connectivity in the SBN enables a new type of redundancy – functional redundancy – of the TTC between the two spacecraft in the network. Each spacecraft is composed of the following subsystems:

- The first spacecraft, S/C#1 contains all subsystems described in Part 1. For an easier representation, S/C#1 is composed of three "components": a payload component (generating utility), a TTC component, and a "supporting subsystems component" composed of the remaining subsystems (AOCS, EPS, Beam, CP, Mechanisms plus Unknown) necessary for the operation of the spacecraft.

- The second spacecraft, S/C#2, is composed of a TTC component and a supporting subsystems component (equivalent of the one of S/C#1). Note that S/C#2 has no payload component, as it is envisioned as a backup for S/C#1's TTC.

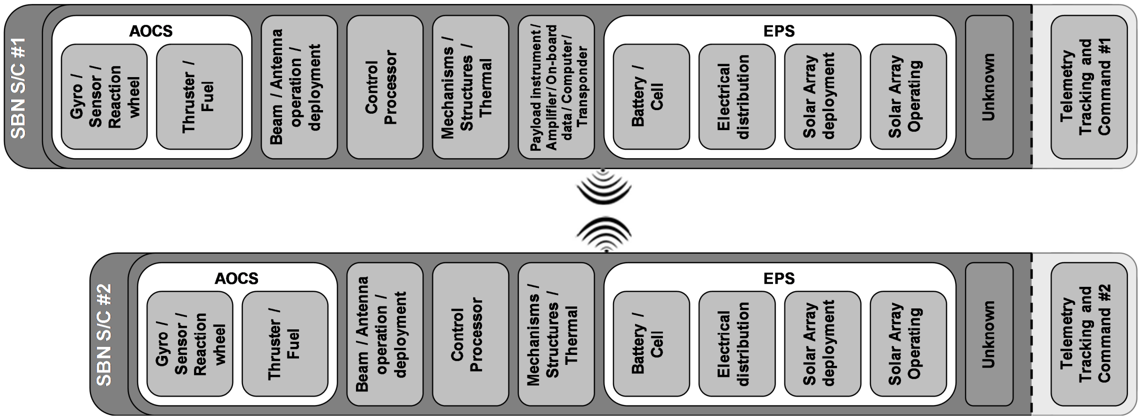

SBN S/C #1
AOCS
Gyro / Sensor / Reaction wheel
Thruster / Fuel
Beam / Antenna operation / deployment
Control Processor
Mechanisms / Structures / Thermal
Payload instrument / Amplifier / On-board data / Computer / Transponder
EPS
Battery / Cell
Electrical distribution
Solar Array deployment
Solar Array Operating
Unknown
Telemetry Tracking and Command #1
SBN S/C #2
AOCS
Gyro / Sensor / Reaction wheel
Thruster / Fuel
Beam / Antenna operation / deployment
Control Processor
Mechanisms / Structures / Thermal
EPS
Battery / Cell
Electrical distribution
Solar Array deployment
Solar Array Operating
Unknown
Telemetry Tracking and Command #2

Figure 4.3. Example of a space-based network

It is immediately clear that if we were to represent this particular SBN as shown in Figure 4.4, the nodes could not be considered as identical, as S/C#1 possesses a payload component, while S/C#2 does not. The representation shown in Figure 4.4 could be adequate at a high-level representation, indicating that S/C#1 and S/C#2 are networked, but would be meaningless and misleading for any other purposes: for example, what would the link represent from the payload's perspective?

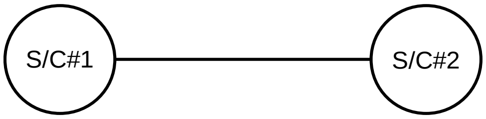


Figure 4.4. Inadequate representation of the case study SBN

Some attempts at considering heterogeneous nodes have been conducted in the literature, but are too limited to properly model SBNs. For example, some studies considered nodes with different capacities (Motter and Lai, 2002; Crucitti, *et al*., 2004), but the function of the nodes remains identical, when a SBN might have spacecraft with different functionalities. The Internet network has raised questions about heterogeneity as it is the union of different networks (wireless devices, computers, routers, etc.). However, the efforts in these studies were put on the transmission of data among the nodes rather than a modeling of heterogeneity in networks. As a consequence, a first question must be answered before analyzing the survivability of SBNs: **how can networks with heterogeneous nodes be represented and analyzed?**

4.4. Introduction to Interdependent Multi-Layer Networks

Building on the concepts of interdependency and layers in network presented in the literature review, we propose in this thesis to represent a network with heterogeneous nodes as an **interdependent multi-layer network** (IMLN), where each layer corresponds to a particular node characteristic or functionality and is represented as a network with homogeneous (or identical) nodes. The following paragraphs aim to introduce and present this new concept, as well as to provide a formal mathematical characterization in the next section.

To illustrate the proposed concept, let us go back to the case study example: the three identified functionalities in that particular SBN are: the payload, the TTC and the supporting subsystems. Three layers are then created to represent each of these functionalities, and homogeneous networks can be created on each of the layers: a link is present between two nodes in the same layer if there is a relationship of sort between these nodes (e.g., flow of data, or in this dissertation, a node that provides resources to another one). A link can be directed (from the node that provides the resources to the receiver node) or undirected (which can be conceived as two opposite directed arcs). A multi-layer network representation of the SBN illustrating the previous step is shown in Figure 4.5. Note that in each layer, the nodes are now "identical". However, this representation is incomplete because some nodes across the layers physically belong to the same spacecraft and are not independent as pictured in Figure 4.5.

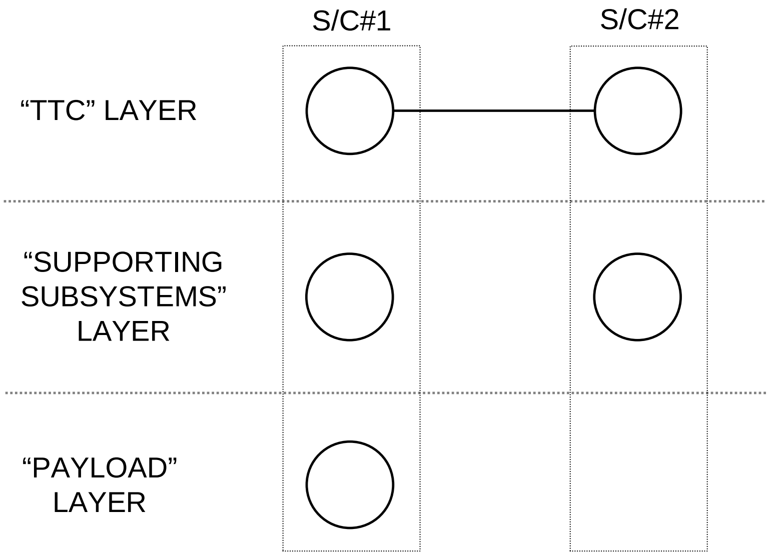


Figure 4.5. Incomplete representation of the case study SBN

A complete representation is obtained by adding **interdependencies** between layers to capture the breakdown of S/C#1 and S/C#2. Several types of interdependencies can be conceived between layers. In the present case, two types of interdependencies exit[4]:

- The failure of the supporting subsystems results in the immediate failure of the whole spacecraft, leading to the unavailability of other nodes (TTC, payload) in different layers belonging to that spacecraft. In this thesis, this effect is called the "kill effect" and is represented with solid directed arcs from the "killer node" to the "victim node".
- The failure of the TTC does not necessarily result in the immediate failure of the spacecraft. Indeed, the functional redundancy on the TTC can allow the survival of the spacecraft if it can tap in the TTC of the other spacecraft. This is possible if, in the TTC layer, both the link to another TTC node and that TTC node are both functioning. In this thesis, this effect is called the "precursor effect" and is represented with dashed directed arcs from the "killer node" to the "victim node".

In the case of S/C#1, the "supporting systems" node failure renders unavailable the "TTC" node and the "payload" node through the "kill effect"; the "TTC" node renders unavailable the "supporting subsystems" node and the "payload" node through the "precursor effect". The "payload" node failure has no impact on the other nodes as the loss of the payload does not doom the spacecraft, only its ability to generate utility.

In the case of S/C#2, "supporting systems" node failure renders unavailable the "TTC" node through the "kill effect"; the "TTC" node renders unavailable the "supporting

[4] Similar or other types of interdependencies between layers have been used in the literature: for example, Zio and Sansavini (2011) used interdependency links to transfer loads from a failed node, or Gu *et al*. (2011) used interdependent links to model cooperation between sub-networks. The interdependency scheme used by Buldyrev *et al*. (2010) is similar to the kill effect described in this thesis.

subsystems” node through the “precursor effect”.

The complete representation of this SBN as an interdependent multi-layer network is shown in Figure 4.6.

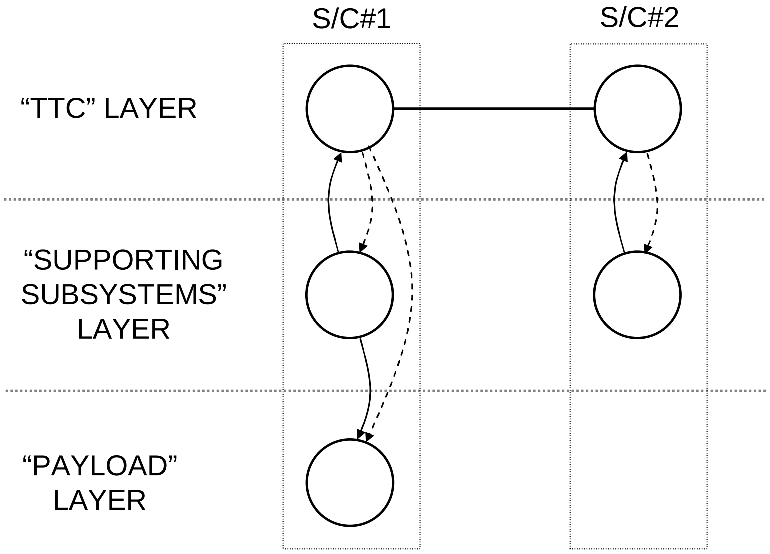


Figure 4.6. Interdependent multi-layer network representation for the case study SBN

One last component in the IMLN representation is what is called in this thesis a “virtual node”. Let illustrate this node with an example: consider the addition of another spacecraft, S/C#3 to the current space-based network. However, this new spacecraft has a payload component and a “supporting subsystems” component, but does not have a TTC component. S/C#3 can however be operational by tapping into the TTC of the other two spacecraft. A node must be added in the “TTC” layer to represent this, but the node does not correspond to a physical subsystem, hence called a “virtual node”. Also this node is peculiar as S/C#3 does not provide any TTC resources to the other spacecraft, as shown by the directed arcs towards that node in the “TTC” layer. This “virtual node” is represented by a dashed circle and this space-based network is shown in Figure 4.7.

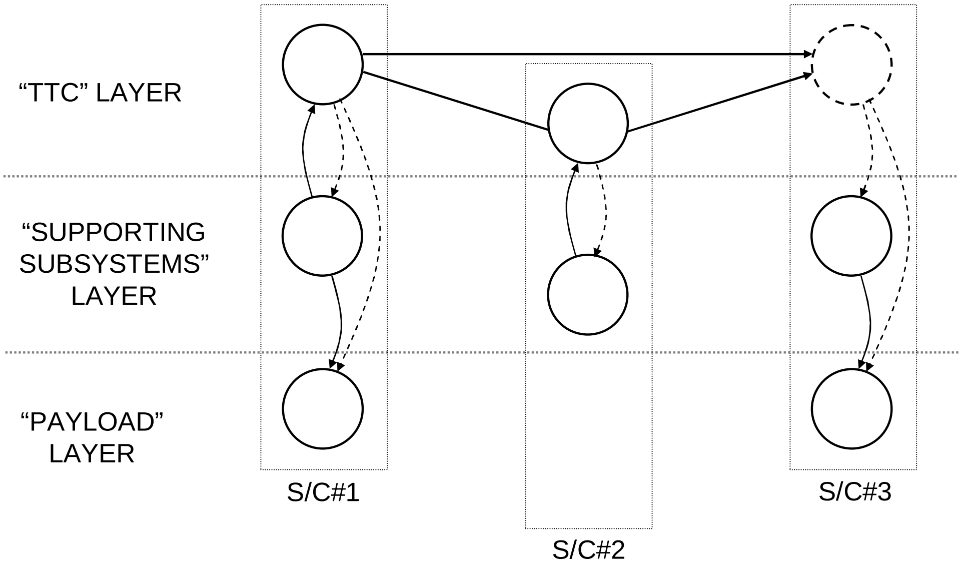


Figure 4.7. Illustration of a "virtual node"

In summary, the IMLN representation consists of nodes placed on several layers representing different types of functionality. Within a layer, nodes form a network by connecting to other nodes with directed or undirected links. Arcs also connect nodes across layers to capture the physical reality of spacecraft and model two types of interdependencies related to the kill and precursor effect. A formal definition of interdependent multi-layer networks is presented next.

4.5. Formal Definition of Interdependent Multi-Layer Networks

4.5.1. IMLN Representation Using Graphs

Building on the notation of Gu *et al*. (2011), the interdependent multi-layer network *N* is defined as $N(G_1,\ldots,G_L,E_k,E_p)$, where:

$$\begin{cases} L \text{ is the number of layers, each numbered sequentially from 1 to } L \\ G_1,\ldots,G_L \text{ are the graphs on each layer} \\ \qquad \forall l \in [1,\ldots,L], G_l = (V_l, E_l) \text{ with:} \\ \qquad\qquad V_l \text{ is the set of } n_l \text{ vertices (or nodes) in } G_l \\ \qquad\qquad E_l \text{ is the set of edges (or links) in } G_l \\ E_k \text{ is the set of interlayer edges representing the “kill effect”} \\ E_p \text{ is the set of interlayer edges representing the “precursor effect”} \end{cases} \tag{4.1}$$

The total number of vertices in N is $n = \sum_{l=1}^{L} n_l$, and the vertices are numbered uniquely and sequentially from 1 to n. As indicated in Newman (2010), “it does not matter which vertex gets which label, only that each label is unique so that we can use the labels to refer to any vertex unambiguously.” However, it is shown later in this chapter that a particular scheme for numbering vertices leads to a more efficient way of representing IMLNs.

Figure 4.8 presents the vertices numbered in the case of the case study SBN presented in Figure 4.6. For that particular case, the interdependent multi-layer network is $N(G_1, G_2, G_3, E_k, E_p)$ where:

- $G_1 = (V_1, E_1)$ with $V_1 = \{1,4\}$ and $E_1 = \{(1,4),(4,1)\}$ is the graph for the “TTC” layer;
- $G_2 = (V_2, E_2)$ with $V_2 = \{2,5\}$ and $E_2 = \varnothing$ is the graph for the “supporting subsystems” layer;
- $G_3 = (V_3, E_3)$ with $V_3 = \{3\}$ and $E_3 = \varnothing$ is the graph for the “payload” layer;

- $E_k = \{(2,1),(2,3),(5,4)\}$
- $E_p = \{(1,2),(1,3),(4,5)\}$

The set of functionally redundant layers E_L is defined as:

$$E_L = \left\{ l \in \mathbf{N}_L^* \middle| \; E_l \neq \text{Ø} \right\} \tag{4.2}$$

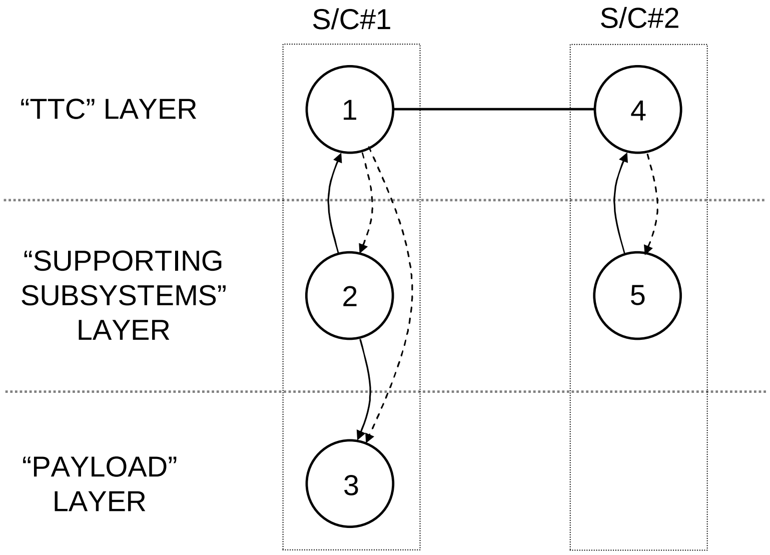


Figure 4.8. Interdependent multi-layer network with numbered vertices for the case study SBN

4.5.2. IMLN Representation Using Matrices

A more practical representation of *N* is given by using 1) classic adjacency matrices $A_1,\ldots,A_L$ for the respective graphs $G_1,\ldots,G_L$, 2) what is introduced in this thesis as the "interlayer" matrix *C*, and 3) a mapping function *f*.

As said before, the vertices are numbered from 1 to n: this numbering scheme is called in this thesis the "*overall numbering*". An additional numbering of the vertices is introduced, called the "*layer numbering*": for each layer l, the vertices are numbered sequentially from 1 to n_l. The function f maps the labels k_O of each node in the "overall numbering" scheme to a pair of integers (l, k_L) where l is the layer number, and k_L is the label of the node in the "layer numbering". Note that indices in the "overall numbering" scheme have a subscript "*O*", while the indices in the "overall numbering" scheme have a subscript "*L*".

For example, in the case of the case study SBN:

- In the "TTC" layer, numbered layer 1, the node 1 in the "overall numbering" is given the "layer number" 1, while the node 4 in the "overall numbering" is given the "layer number" 2;
- In the "supporting subsystems" layer, numbered layer 2, the node 2 in the "overall numbering" is given the "layer number" 1, while the node 5 in the "overall numbering" is given the "layer number" 2;

In the "payload" layer, numbered layer 3, the node 3 in the "overall numbering" is given the "layer number" 1. Then the mapping function f is:

$$\begin{cases} f(1) = (1,1) \\ f(2) = (2,1) \\ f(3) = (3,1) \\ f(4) = (1,2) \\ f(5) = (2,2) \end{cases} \tag{4.3}$$

Because of the layers and the nodes in both numbering schemes are numbered uniquely, the function *f* is bijective. As a consequence, the inverse mapping function f^{-1} is also defined.

For each layer *l*, the graph G_l can be represented by the associated adjacency matrix $A_l = \left[a^l_{i_L\, j_L}\right]_{n_l \times n_l}$ such that:

$$\begin{cases} a^l_{i_L\, j_L} = 1 \text{ if there is an edge from vertex } j_L \text{ to } i_L \\ a^l_{i_L\, j_L} = 0 \text{ otherwise} \end{cases} \tag{4.4}$$

In the case study SBN example:

- The adjacency matrix A_1 for the "TTC" layer (layer 1) is defined as follows:

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.5}$$

- The adjacency matrices A_2 for the "supporting subsystems" layer (layer 2) and A_3 for the "payload" layer (layer 3) are trivial as there is no edge in these layers:

$$A_2 = 0_{2\times 2} \text{ and } A_3 = 0_{1\times 1} \tag{4.6}$$

The “interlayer” matrix $C = \left[c_{i_O\, j_O}\right]_{n\times n}$ is defined as follows:

$$\begin{cases} c_{i_O\, j_O} = 1 \text{ if there is an edge from vertex } j_O \text{ to } i_O \text{ belonging to } E_k \\ \qquad\qquad \text{(kill effect)} \\ c_{i_O\, j_O} = 2 \text{ if there is an edge from vertex } j_O \text{ to } i_O \text{ belonging to } E_p \\ \qquad\qquad \text{(precursor effect)} \\ c_{i_O\, j_O} = 0 \text{ otherwise} \end{cases} \tag{4.7}$$

In the case study example, the interlayer matrix *C* is as follows:

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix} \tag{4.8}$$

As mentioned earlier, the overall numbering scheme can be chosen to facilitate the representation of the IMLN, and in particular the interlayer matrix C. Indeed, if the “overall numbering” is chosen such that vertices belonging to the same spacecraft were numbered sequentially (vertices 1, 2 and 3 belongs to S/C#1, and vertices 4 and 5 to S/C#2) as in the present case study, the interlayer matrix *C* can be reduced to a block diagonal form:

$$C = \begin{bmatrix} \begin{matrix} 0 & 1 & 0 \\ 2 & 0 & 0 \\ 2 & 1 & 0 \end{matrix} & 0_{3\times 2} \\ 0_{2\times 3} & \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} \end{bmatrix} \tag{4.9}$$

As the number of spacecraft increases in the space-based network, the interlayer matrix growth can be alleviated using this numbering scheme, as only the blocks around the diagonal need to be populated. Also, from a computational point of view, this can allow for the matrix to be saved as a scarce matrix and save memory during the simulation. Examples of larger networks will be shown later in the dissertation.

The sets E_k, E_p and E_L can also be defined from the adjacency matrices and interlayer matrix as follows:

$$E_k = \{(j,i) \mid c_{ij} = 1\} \tag{4.10}$$

$$E_p = \{(j,i) \mid c_{ij} = 2\} \tag{4.11}$$

$$E_L = \{l \mid A_l \neq 0_{n_l \times n_l}\} \tag{4.12}$$

As a conclusion, the interdependent multi-layer network N can be uniquely defined as $N(G_1, \ldots, G_L, E_k, E_p)$ or $N(A_1, \ldots, A_L, C, f)$, as the two characterizations are equivalent.

4.6. Summary

This chapter discussed the concept of survivability, from its origin in the military context to its expansion to engineering systems. Building on the works published in the literature, this thesis introduced a framework for the study of the survivability of engineering systems in general, and applied to space systems in this dissertation. The chapter then discussed the state of the academic study of network analysis and its practical use for understanding real-world network. However, it was highlighted that the classic network representation failed to capture an essential aspect of space-based networks, namely, the potential heterogeneity in their respective functionalities. To enable the modeling of such architectures, a new concept was introduced and this approach describes the space-based networks as “interdependent multi-layer networks”. A formal definition of the IMLN representation was then introduced. However, one question was not addressed in conjunction with the survivability considerations discussed earlier in the chapter: how can this new representation be used for survivability analyses? This topic is the subject of the following chapter dedicated to the study and modeling of the failure propagation across an IMLN.

CHAPTER 5

FAILURE PROPAGATION IN INTERDEPENDENT MULTI-LAYER NETWORKS: FORMAL ANALYSIS AND THEORETICAL DEVELOPMENT

Modeling the space-based networks through interdependent multi-layer network has been presented in the previous chapter. However, assessing the survivability features of such networks requires estimating an objective function related to the failure times of the network nodes. Due to the interdependencies in the model, this estimation is not trivial and requires understanding the propagation of failures through the network. Part of the failure propagation is due to the kill and precursor effects introduced earlier. The following sections are dedicated to study these effects, but note that other cascading mechanisms such as the ones described in the literature review can be easily added and implemented. **How does the failure of one node propagate in the interdependent multi-layer network through the kill and precursor effect?**

The proposed method comprises three steps:

1. Generate the times to failures T_F for each vertex and edge[5].
2. Propagate failures through the kill effect
3. Propagate failures through the precursor effect

[5] In the following, the following convention is adopted: $T_{F,\text{ vertex } i}$ refers to the time to failure of vertex i in the overall numbering scheme. Also, T_F represents the random variable time to failure, while t_F represents an instantiation of the random variable T_F.

Let characterize mathematically the last two steps. Suppose that the interdependent multi-layer network of interest has been defined as $N(A_1, \ldots, A_L, C, f)$.

The remainder of this chapter is split in two sections: the first section investigates the propagation across the network of catastrophic failures only; the second section builds onto this propagation scheme and expands the established algorithm for the more complex treatment of multi-state failures (minor and major anomalies).

5.1. Complete Failure Simulation

5.1.1. Time to Failure Generation

To propagate failures through the network, one must first generate times to failures for the different objects in the space-based network: the vertices and the edges. Using the cumulative distribution functions representing the failure behavior of each vertex, random times to failure for the vertices $T_{F,\text{vertex } i}$ ($i \in \mathbf{N}_n^*$) can be generated[6]. Note that it is not necessary for each node in a common layer to share the same failure behavior.

Two steps are needed to generate the times to failure for the edges $T_{F,\text{edge } j \to i}$: the link between two spacecraft is established through a wireless unit embedded in each spacecraft. For the link to function, both units need to be operational, the failure of one leading to the failure of the link.

[6] In the case of a virtual node, its failure time is considered as null.

- Generate the times to failure of the wireless units on each spacecraft using predetermined cumulative distribution functions;
- Generate the times to failures for each edge $T_{F,\text{edge } j\rightarrow i}$ by taking the minimum of the time to failures of the two associated wireless units (unit *i* and unit *j*).

5.1.2. Failure Propagation Through the "Kill Effect"

The information about the kill effect is contained in the interlayer matrix *C*, and the first step consists in extracting from *C* the pairs of "killer" and "victim" vertices. As shown in the previous chapter, E_k can be defined from *C* as follows:

$$E_k = \left\{ (j,i) \middle| \, c_{ij} = 1 \right\} \tag{5.1}$$

Define the "killer" vector $\mathbf{k_1}$ and the "victim" vector $\mathbf{v_1}$ such that:

$$\begin{cases} \mathbf{k_1}, \mathbf{v_1} \in \mathbf{N}^{|E_k|} \\ \forall q \in \mathbf{N}^*_{|E_k|}, \left(\mathbf{k_1}(q), \mathbf{v_1}(q)\right) \in E_k \\ \forall r, s \in \mathbf{N}^*_{|E_k|} \text{ and } r \neq s, \left(\mathbf{k_1}(r), \mathbf{v_1}(r)\right) \neq \left(\mathbf{k_1}(s), \mathbf{v_1}(s)\right) \end{cases} \tag{5.2}$$

The last step consists in computing time to unavailability $T_U^{k,F}$ of the "victim" vertex using the time to failure of the "killer" vertex. Mathematically, this is expressed as:

$$\forall q \in \mathbf{N}^*_{|E_k|}, T^{k,F}_{U,\text{ vertex } \mathbf{v_1}(q)} = T_{F,\text{ vertex } \mathbf{k_1}(q)} \tag{5.3}$$

In the case that a victim vertex has several killers, $T^{k,F}_U$ is equal to the minimum of the times to failure of the killer vertices.

5.1.3. Failure Propagation Through the "Precursor Effect"

As for the killer effect, the information about the precursor effect is contained in the interlayer matrix *C*, and *C* is used to extract the pairs of "killer" and "victim" vertices. As defined in the previous chapter, E_p is defined as follows:

$$E_p = \{(j,i) \mid c_{ij} = 2\} \tag{5.4}$$

The "killer" vector $\mathbf{k_2}$ and the "victim" vector $\mathbf{v_2}$ are defined as:

$$\begin{cases} \mathbf{k_2}, \mathbf{v_2} \in \mathbf{N}^{|E_p|} \\ \forall q \in \mathbf{N}^*_{|E_p|}, (\mathbf{k_2}(q), \mathbf{v_2}(q)) \in E_p \\ \forall r, s \in \mathbf{N}^*_{|E_p|} \text{ and } r \neq s, (\mathbf{k_2}(r), \mathbf{v_2}(r)) \neq (\mathbf{k_2}(s), \mathbf{v_2}(s)) \end{cases} \tag{5.5}$$

Computing the time to unavailability due to the precursor effect is not as straightforward as for the kill effect. Indeed, the failure of a vertex that has a functional redundancy will not necessarily propagate immediately to the vertices belonging to the same entity (here, spacecraft). The time at which the function represented by the vertex will become unavailable depends on the time to failure of the vertex itself, but also on the times to failure of the other vertices and edges part of the same layer. For example, in the case study SBN, the failure of node 1 will propagate to nodes 2 and 3 if node 1 is not able to tap into the resources of node 4, i.e., if either the link between node 4 and 1, or node 4 has failed. Hence it is necessary to compare the time to failure of the node, to the ones of the pairs link/node it is connected to. Several steps are needed and are described below.

1. To know when a vertex becomes unavailable after the kill effect, the "minimum time to unavailability" $T_U^{m,F}$ is introduced and is defined as:

$$\forall q \in \mathbf{N}_n^*, \begin{cases} T_{U,\,\text{vertex}\,q}^{m,F} = \min\left[T_{F,\,\text{vertex}\,q}, T_{U,\,\text{vertex}\,q}^{k,F}\right] \text{ if } T_{U,\,\text{vertex}\,q}^{k,F} \text{ exists} \\ T_{U,\,\text{vertex}\,q}^{m,F} = T_{F,\,\text{vertex}\,q} \quad \text{else} \end{cases} \tag{5.6}$$

2. To compare the time to failure of the vertex *i* and the ones of the pairs edge (*j*→*i*)/vertex *j* it is connected to (i.e., edges *towards* that vertex *i*) , a useful object is introduced – the matrix $H_l^F = \left[h_{i\,j}^{l,F}\right]_{n_l \times n_l}$ defined as follows for $l \in E_L$:

$$\forall l \in E_L, \begin{cases} \text{if } i = j, h_{i\,j}^{l,F} = T_{U,\,\text{vertex}\,f^{-1}(l,i)}^{m,F} \\ \text{if } i \neq j, \begin{cases} \text{if } a_{i\,j}^l = 1, h_{i\,j}^{l,F} = \min\left[T_{F,\,\text{edge}\,f^{-1}(l,j)\to f^{-1}(l,i)}, T_{U,\,\text{vertex}\,f^{-1}(l,j)}^{m,F}\right] \\ \text{if } a_{i\,j}^l = 0, h_{i\,j}^{l,F} = 0 \end{cases} \end{cases} \tag{5.7}$$

This matrix H is helpful as it presents in line the time to failure of the vertex, and the ones of the pairs edge/vertex it is connected to.

3. The time to unavailability considering the functional redundancy $T_U^{r,F}$ of the vertex of interest can be found as the maximum time to failure in the associated line. Consider the column vector $\mathbf{m}_l^F = \left[m_i^{l,F}\right]_{n_l \times 1}$ defined for $l \in E_L$ as:

$$\forall l \in E_L, m_i^{l,F} = \max_j h_{ij}^{l,F} \tag{5.8}$$

4. $T_U^{r,F}$ can now be computed as:

$$\forall l \in E_L, \forall i \in \mathbf{N}_{n_l}^*, T_{U,\text{ vertex } f^{-1}(l,i)}^{r,F} = m_i^{l,F} \tag{5.9}$$

5. The same process than for the kill effect can be now applied, that is, the propagation of the “failure” of a node across layers to nodes belonging to the same entity. This step consists in computing time to unavailability $T_U^{p,F}$ of the “victim” vertex using the time to failure of the “killer” vertex. Mathematically, this is expressed as:

$$\forall q \in \mathbf{N}_{|E_p|}^*, T_{U,\text{ vertex } \mathbf{v_1}(q)}^{p,F} = T_{U,\text{ vertex } \mathbf{k_1}(q)}^{r,F} \tag{5.10}$$

In the case that a victim vertex has several killers, $T_U^{p,F}$ is equal to the minimum of the times $T_U^{r,F}$ of the killer vertices.

6. Due to the fact that several layers of redundancy can be considered concurrently, the interdependence of the precursor effect between vertices belonging to the same spacecraft but in different layers can require an iterative scheme for unavailability times to converge to their correct values. The following condition indicates if more iterations are required: if $T_{U,\,\mathrm{vertex}\,q}^{m,F} \leq T_{U,\,\mathrm{vertex}\,q}^{p,F}$, the failure propagation due to the precursor effect is complete (skip step 7). If not, continue to next step.

7. While $T_{U,\,\mathrm{vertex}\,q}^{m,F} > T_{U,\,\mathrm{vertex}\,q}^{p,F}$, set $T_{U,\,\mathrm{vertex}\,q}^{m,F} = T_{U,\,\mathrm{vertex}\,q}^{p,F}$ and repeat steps 2–5.

5.1.4. Combination of All Effects

Finally, for each vertex in the interdependent multi-layer network, the time to unavailability is obtained as:

$$\forall q \in \mathbf{N}_n^*, T_{U,\,\mathrm{vertex}\,q}^{F} = \min\left[\max\left(T_{F,\,\mathrm{vertex}\,q}, T_{U,\,\mathrm{vertex}\,q}^{r,F}\right), T_{U,\,\mathrm{vertex}\,q}^{k,F}, T_{U,\,\mathrm{vertex}\,q}^{p,F}\right] \tag{5.11}$$

where $T_{U,\mathrm{vertex}\,q}^{r,F}$, $T_{U,\mathrm{vertex}\,q}^{k,F}$ and $T_{U,\mathrm{vertex}\,q}^{p,F}$ are included in if they exist

5.1.5. Summary of the Failure Propagation Algorithm

Below is a summary of the algorithmic process used to propagate catastrophic failures across the network. The following inputs are required: the adjacency matrices and interlayer matrix, the mapping function (these three elements defining a network architecture), and the c.d.f.s for the failure distribution of the vertices and edges.

1. Generate for each vertex i $T_{F,\text{vertex } i}$ (section 5.1.1)
2. Generate for each edge $T_{F,\text{edge } j\to i}$ (section 5.1.1)
3. Compute E_k using Eq. (5.1)
4. Compute $\mathbf{k_1}$ and $\mathbf{v_1}$ using Eq. (5.2)
5. Compute $T_U^{k,F}$ for each victim vertex using Eq. (5.3)
6. Compute E_p using Eq. (5.4)
7. Compute $\mathbf{k_2}$ and $\mathbf{v_2}$ using Eq. (5.5)
8. Compute $T_U^{m,F}$ for each vertex using Eq. (5.6)
9. For all $l \in E_L$, compute H_l^F using Eq. (5.7)
10. For all $l \in E_L$, compute $\mathbf{m}_l^F$ using Eq. (5.8)
11. Compute $T_U^{r,F}$ for each vertex for all layers $l \in E_L$ using Eq. (5.9)
12. Compute $T_U^{p,F}$ for each victim vertex using Eq. (5.10)
13. Repeat steps 9–12 until $T_{U,\text{ vertex } q}^{m,F} \le T_{U,\text{ vertex } q}^{p,F}$ for all victim vertices q in the precursor effect
14. Compute T_U^F for each vertex using Eq. (5.11)

5.1.6. Failure Propagation Examples

The first example uses the TTC functional redundancy case study, and the IMLN under consideration is shown in Figure 4.8. To illustrate how the algorithm is working, deterministic times to failures for the nodes and links will be used in this example. These times to failures are given in Table 5.1, and shown in Figure 5.1 for clarity purposes.

Table 5.1. Times to failure of the nodes and link in the case study example

	Time to failure
	years
Spacecraft #1	
TTC	2
Supporting subsystems	6
Payload	7
Spacecraft #2	
TTC	9
Supporting subsystems	8
Link between spacecraft	12

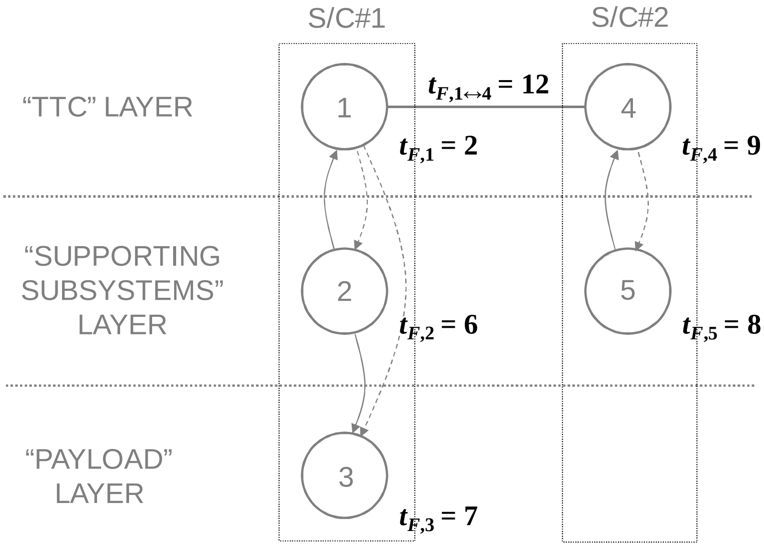


Figure 5.1. IMLN representation with node and link times to failure

If spacecraft #1 was to be by itself, it would have failed at 2 years, when the TTC failed. However, in this network configuration, the second spacecraft can help maintaining the functionality up to 6 years on-orbit. How this number was obtained is explained below using the 14 steps given in section 5.1.5. Steps 1 and 2 are already completed as the times to failure for the nodes and link are given in this example.

3. According to section 4.5.1,

$$E_k = \{(2,1),(2,3),(5,4)\} \tag{5.12}$$

4. Then,

$$\mathbf{k_1} = (2 \quad 2 \quad 5) \text{ and } \mathbf{v_1} = (1 \quad 3 \quad 4) \tag{5.13}$$

5. Propagating the kill effect yields:

$$\begin{cases} t_{U,1}^{k,F} = t_{F,2} = 6 \\ t_{U,3}^{k,F} = t_{F,2} = 6 \\ t_{U,4}^{k,F} = t_{F,5} = 8 \end{cases} \tag{5.14}$$

6. According to section 4.5.1,

$$E_p = \{(1,2),(1,3),(4,5)\} \tag{5.15}$$

7. Then,

$$\mathbf{k}_2 = \begin{pmatrix}1 & 1 & 4\end{pmatrix} \text{ and } \mathbf{v}_2 = \begin{pmatrix}2 & 3 & 5\end{pmatrix} \tag{5.16}$$

8. The minimum time to unavailability after the kill effect is given as:

$$\begin{cases} t_{U,1}^{m,F} = \min\left[t_{F,1}, t_{U,1}^{k,F}\right] = \min[2,6] = 2 \\ t_{U,2}^{m,F} = t_{F,2} = 6 \\ t_{U,3}^{m,F} = \min\left[t_{F,3}, t_{U,3}^{k,F}\right] = \min[7,6] = 6 \\ t_{U,4}^{m,F} = \min\left[t_{F,4}, t_{U,4}^{k,F}\right] = \min[9,8] = 8 \\ t_{U,5}^{m,F} = t_{F,5} = 8 \end{cases} \tag{5.17}$$

9. The only functionally redundant layer in this IMLN is the TTC layer. The associated *H* matrix is expressed as:

$$H_1^F = \begin{bmatrix} t_{U,1}^{m,F} & \min\left[t_{F,4\to1}, t_{U,4}^{m,F}\right] \\ \min\left[t_{F,1\to4}, t_{U,1}^{m,F}\right] & t_{U,4}^{m,F} \end{bmatrix} = \begin{bmatrix} 2 & \min[12,8] \\ \min[12,2] & 8 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 2 & 8 \end{bmatrix} \tag{5.18}$$

10. Then,

$$\mathbf{m}_1^F = \begin{bmatrix} \max[2,8] \\ \max[2,8] \end{bmatrix} = \begin{bmatrix} 8 \\ 8 \end{bmatrix} \tag{5.19}$$

11. The times to unavailability for the TTCs due to the functional redundancy are expressed as:

$$\begin{cases} t_{U,1}^{r,F} = m_{11}^{1,F} = 8 \\ t_{U,4}^{r,F} = m_{12}^{1,F} = 8 \end{cases} \tag{5.20}$$

12. Propagating the precursor effect yields:

$$\begin{cases} t_{U,2}^{p,F} = t_{U,1}^{r,F} = 8 \\ t_{U,3}^{p,F} = t_{U,1}^{r,F} = 8 \\ t_{U,5}^{p,F} = t_{U,4}^{r,F} = 8 \end{cases} \tag{5.21}$$

13. The convergence condition is met in this particular example, so the algorithm continues to the final step.
14. Combining all the effect, the final times to unavailability for the nodes are:

$$\begin{cases} t_{U,1}^{F} = \min\left[\max\left(t_{F,1}, t_{U,1}^{r,F}\right), t_{U,1}^{k,F}\right] = \min\left[\max(2,8),6\right] = 6 \\ t_{U,2}^{F} = \min\left[t_{F,2}, t_{U,2}^{p,F}\right] = \min[6,8] = 6 \\ t_{U,3}^{F} = \min\left[t_{F,3}, t_{U,3}^{k,F}, t_{U,3}^{p,F}\right] = \min[7,6,8] = 6 \\ t_{U,4}^{F} = \min\left[\max\left(t_{F,4}, t_{U,4}^{r,F}\right), T_{U,4}^{k,F}\right] = \min\left[\max(9,8),8\right] = 8 \\ t_{U,5}^{F} = \min\left[t_{F,5}, t_{U,5}^{p,F}\right] = \min[8,8] = 8 \end{cases} \tag{5.22}$$

5.2. Multi-State Failure Simulation

In the case of a multi-state failure approach, some additions must be made to the algorithm presented in the previous section. Let’s consider two degraded states for each vertex and edge: a minor degradation state and a major degradation state. The respective time to event random variable is noted T_m and T_M. It is shown below that modeling directly the probability distributions of these two random variables is not practical, and two related random variables are used instead in the modeling process: T_{MF} and T_{mMF}. The former represents the time at which a vertex or edge is in either the major degradation state or the complete failure state; the latter represents the time at which the vertex or edge experience any degradation event (minor, major or catastrophic).

5.2.1. Generation of the Times to Failure and Degradation

Instantiations to the time to failure T_F and the two times to degradation T_{MF} and T_{mMF} cannot be generated independently. Knowing T_F, how can instantiations to T_{MF} be generated? And knowing T_F and T_{MF}, how can instantiations to T_{mMF} be generated? This subsection is presenting a possible solution to generate these times concurrently.

A event leads to the major-failed state (*MF*) either if this event is a major degradation or a complete failure of the (sub)system under consideration. As such, there is a competition between these two types of severity for which will occur first. A transition diagram of this failure and degradation behavior is shown in Figure 5.2a. Both the probabilities of being in the failed state (*F*) and the major-failed state (*MF*) can be modeled using cumulative distribution functions as they are absorbing states. However, the probability of being in a major state cannot be modeled similarly: as time goes to infinity, the probability of being in that state goes to zero. To get around this problem, an equivalent representation for the failed state and the major-failed state is shown in Figure 5.2b. The major state (*M*) has been replaced by a virtual state (S_{v1}) where the probability of being in that state is represented by a c.d.f. The major-failed state can now be thought as the failed state and the virtual state in series from a block diagram point of view. As a consequence, the probability of being in the major-failed state can be expressed as:

$$P_{MF} = 1 - (1 - P_F)(1 - P_{S_{v1}}) \tag{5.23}$$

Rearranging the terms yields:

$$P_{S_{v1}} = 1 - \frac{(1 - P_{MF})}{(1 - P_F)} \tag{5.24}$$

Then, the random variables for the time to complete failure (T_F), major degradation or complete failure (T_{MF}) and time to the virtual state ($T_{S_{v1}}$) are related as follows:

$$T_{MF} = \min(T_F, T_{S_{v1}}) \tag{5.25}$$

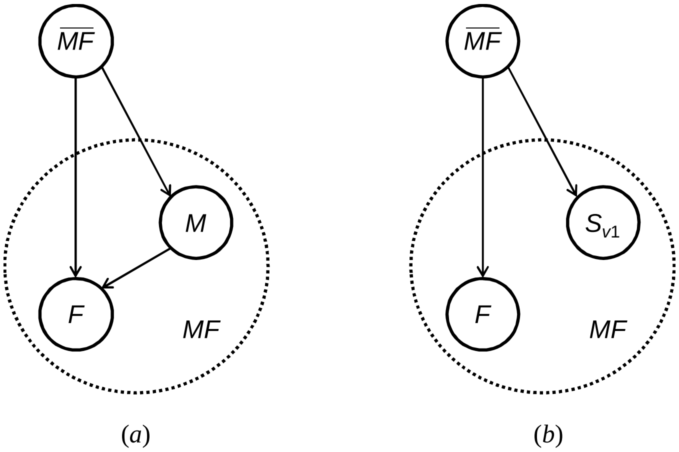


Figure 5.2. Transition diagram for the major-failed state (*a*) and its equivalent model (*b*)

Let us examine the expression of $P_{S_{v1}}$ for different types of distribution for T_F and T_{MF}.

- ***Exponential distributions***:

Consider that both T_F and T_{MF} are modeled as exponential distributions and their c.d.f.s are expressed as:

$$P_F = 1 - \exp(-\lambda_F \cdot t) \tag{5.26}$$

$$P_{MF} = 1 - \exp(-\lambda_{MF} \cdot t) \tag{5.27}$$

Using these expressions in Eq. (5.24) yields:

$$P_{S_{v1}} = 1 - \frac{\exp(-\lambda_{MF} \cdot t)}{\exp(-\lambda_F \cdot t)} \tag{5.28}$$

Simplifying Eq. (5.28) leads to

$$P_{S_{v1}} = 1 - \exp[-(\lambda_{MF} - \lambda_F)t] \tag{5.29}$$

Note that the resulting probability is also exponential with a parameter equal to $(\lambda_{MF} - \lambda_F)$. Generating random times to the virtual state is straightforward and given by:

$$t_{S_{v1}} = \frac{\ln(1 - P_{S_{v1}})}{\lambda_F - \lambda_{MF}} \tag{5.30}$$

- ***Weibull distributions with the same shape parameter***:

Consider that both T_F and T_{MF} are modeled as Weibull distributions sharing the same Weibull shape parameter β. Their c.d.f.s can be expressed as follows:

$$P_F = 1 - \exp\left[-\left(\frac{t}{\theta_F}\right)^{\beta}\right] \tag{5.31}$$

$$P_{MF} = 1 - \exp\left[-\left(\frac{t}{\theta_{MF}}\right)^{\beta}\right] \tag{5.32}$$

Substituting these functions in Eq. (5.24) yields:

$$P_{S_{v1}} = 1 - \exp\left[\left(\frac{t}{\theta_F}\right)^{\beta} - \left(\frac{t}{\theta_{MF}}\right)^{\beta}\right] \tag{5.33}$$

As shown in Volovoi and Vega (2012), Eq. (5.33) can be reduced to a single Weibull distribution characterized by the shape parameter β and the following scale parameter $\theta_{S_{v1}}$:

$$\theta_{S_{v1}} = \frac{1}{\left[\frac{1}{(\theta_{MF})^{\beta}} - \frac{1}{(\theta_{F})^{\beta}}\right]^{\left(\frac{1}{\beta}\right)}} \tag{5.34}$$

Also in this case, generating random times to the virtual state is straightforward:

$$t_{S_{v1}} = \theta_{S_{v1}} \left[-\ln\left(1 - P_{S_{v1}}\right)\right]^{\left(\frac{1}{\beta}\right)} \tag{5.35}$$

- ***General Weibull distributions***:

In the case of two different Weibull distributions for T_F and T_{MF},

$$P_F = 1 - \exp\left[-\left(\frac{t}{\theta_F}\right)^{\beta_F}\right] \tag{5.36}$$

$$P_{MF} = 1 - \exp\left[-\left(\frac{t}{\theta_{MF}}\right)^{\beta_{MF}}\right] \tag{5.37}$$

the resulting expression for $P_{S_{v1}}$ given in Eq. (5.38) cannot be reduced to an equivalent single Weibull distribution.

$$P_{S_{v1}} = 1 - \exp\left[\left(\frac{t}{\theta_F}\right)^{\beta_F} - \left(\frac{t}{\theta_{MF}}\right)^{\beta_{MF}}\right] \tag{5.38}$$

As a consequence, there is no closed-form solution for the time to the virtual state (as seen above, a closed-form solution exists if $\beta_F = \beta_{MF}$). Generating random times requires solving for t in Eq. (5.38). In this thesis, a root-finding algorithm (MATLAB *fzero* function) was used and the initial guess was determined by fitting $P_{S_{v1}}$ with a single Weibull distribution using a non-linear least-square regression.

Algorithm for T_F and T_{MF}. In this thesis, the times to failure and severe degradation T_F and T_{MF} for each vertex and edge are modeled as Weibull distributions that might or might not have the same Weibull shape parameter (Eqs (5.36) and (5.37)). Consequently, instantiations to T_F and T_{MF} are generated concurrently as follows:

1. Using Eq. (5.36), generate randomly an instantiation to T_F, namely, t_F;
2. If $\beta_F = \beta_{MF}$, generate randomly an instantiation to $T_{S_{v1}}$, namely, $t_{S_{v1}}$ using the straightforward Eq. (5.35). If $\beta_F \neq \beta_{MF}$, then numerically solve Eq**.** (5.38) for $t_{S_{v1}}$ as described above;
3. From Eq. (5.25), calculate t_{MF} as follows:

$$t_{MF} = \min\left(t_F, t_{S_{v1}}\right) \tag{5.39}$$

4. To obtain a representative sample, repeat n_{MC} times steps 1–3 in a Monte Carlo simulation.

After the Monte Carlo simulation, the c.d.f.s for T_F and T_{MF} (P_F and P_{MF}) can be recreated and P_M can be obtained as follows:

$$P_M = P_{MF} - P_F \tag{5.40}$$

Generation of instantiations of T

Generation of instantiations of T_{mMF}. Knowing T_{MF}, the same process can be applied to generate an instantiation of T_{mMF}. A similar equivalent representation involving the MF state and another virtual state (S_{v2}) leads to modify Eq. (5.23) as follows:

$$P_{mMF} = 1 - (1 - P_{MF})(1 - P_{S_{v2}}) \tag{5.41}$$

Similarly, Eq. (5.24) is modified, yielding:

$$P_{S_{v2}} = 1 - \frac{(1 - P_{mMF})}{(1 - P_{MF})} \tag{5.42}$$

In addition, the random variables for the time to major degradation or complete failure (T_{MF}), the time to degradation (T_{mMF}) and time to the virtual state ($T_{S_{v2}}$) are related as follows:

$$T_{mMF} = \min(T_{MF}, T_{S_{v2}}) \tag{5.43}$$

Similarly, assuming that T_{MF} and T_{mMF} are modeled using Weibull distributions, $P_{S_{v2}}$ can be expressed as follows:

$$P_{S_{v2}} = 1 - \exp\left[\left(\frac{t}{\theta_{MF}}\right)^{\beta_{MF}} - \left(\frac{t}{\theta_{mMF}}\right)^{\beta_{mMF}}\right] \qquad (5.44)$$

In general, $t_{S_{v2}}$ must be solved numerically. If $\beta_{MF} = \beta_{mMF} = \beta$, $P_{S_{v2}}$ has a closed-form solution given by:

$$t_{S_{v2}} = \theta_{S_{v2}} \left[-\ln\left(1 - P_{S_{v2}}\right)\right]^{\left(1/\beta\right)} \qquad (5.45)$$

where:

$$\theta_{S_{v2}} = \frac{1}{\left[\dfrac{1}{(\theta_{mMF})^{\beta}} - \dfrac{1}{(\theta_{MF})^{\beta}}\right]^{\left(1/\beta\right)}} \qquad (5.46)$$

General algorithm for T_F, T_{MF} and T_{mMF}. Assuming Weibull distribution for these random variables, instantiations for T_F, T_{MF} and T_{mMF} are obtained as follows:

1. Using Eq. (5.36), generate randomly an instantiation to T_F, namely, t_F;
2. If $\beta_F = \beta_{MF}$, generate randomly an instantiation to $T_{S_{v1}}$, namely, $t_{S_{v1}}$ using the straightforward Eq. (5.35). If $\beta_F \neq \beta_{MF}$, then numerically solve Eq. (5.38) for $t_{S_{v1}}$ as described above;
3. From Eq. (5.25), calculate t_{MF} as follows:

$$t_{MF} = \min\left(t_F, t_{S_{v1}}\right) \tag{5.47}$$

4. If $\beta_{MF} = \beta_{mMF}$, generate randomly an instantiation to $T_{S_{v2}}$, namely, $t_{S_{v2}}$ using the straightforward Eq. (5.45). If $\beta_{MF} \neq \beta_{mMF}$, then numerically solve Eq**.** (5.44) for $t_{S_{v2}}$ as described above;
5. From Eq. (5.43), calculate t_{mMF} as follows:

$$t_{mMF} = \min\left(t_{MF}, t_{S_{v2}}\right) \tag{5.48}$$

6. To obtain a representative sample, repeat n_{MC} times steps 1–5 in a Monte Carlo simulation.

5.2.2. Algorithm Modification for Failure Propagation in the Multi-State Case

Both propagations through the kill effect and through the precursor effect need to be expanded to take into account the multi-state failures occurring at the vertices and edges. Once T_F, T_{MF} and T_{mMF} have been generated for each vertex and edge as described in the previous subsection, the kill effect and the precursor effect are derived as follows.

Kill effect. E_k, $\mathbf{k_1}$ and $\mathbf{v_1}$ are derived as previously using Eqs. (5.1) and (5.2). The time to unavailability for the failed case (F) for the victim vertices is given by Eq. (5.3), as recalled below:

$$\forall q \in \mathbf{N}^{*}_{|E_k|}, T^{k,F}_{U,\text{ vertex }\mathbf{v_1}(q)} = T_{F,\text{ vertex }\mathbf{k_1}(q)} \tag{5.49}$$

Similarly, the time to unavailability for the major degradation or complete failure case (*MF*) and for the degradation case (*mMF*) are derived as:

$$\forall q \in \mathbf{N}^{*}_{|E_k|}, T^{k,MF}_{U,\text{ vertex }\mathbf{v_1}(q)} = T_{MF,\text{ vertex }\mathbf{k_1}(q)} \tag{5.50}$$

$$\forall q \in \mathbf{N}^{*}_{|E_k|}, T^{k,mMF}_{U,\text{ vertex }\mathbf{v_1}(q)} = T_{mMF,\text{ vertex }\mathbf{k_1}(q)} \tag{5.51}$$

In the case that a victim vertex has several killers, $T_U^{k,MF}$ and $T_U^{k,mMF}$ are equal to the minimum of the times of the killer vertices.

Precursor effect. E_p, $\mathbf{k_2}$ and $\mathbf{v_2}$ are derived as previously using Eqs. (5.4) and (5.5). After the kill effect, a victim node becomes unavailable for the failed case as given by Eq. (5.6) and rewritten below:

$$\forall q \in \mathbf{N}^{*}_{n}, \begin{cases} T^{m,F}_{U,\text{ vertex }q} = \min\left[T_{F,\text{ vertex }q}, T^{k,F}_{U,\text{ vertex }q}\right] & \text{if } T^{k,F}_{U,\text{ vertex }q} \text{ exists} \\ T^{m,F}_{U,\text{ vertex }q} = T_{F,\text{ vertex }q} & \text{else} \end{cases} \tag{5.52}$$

However, in the case of the *MF* and *mMF* states of the victim vertices, the functionality is truly lost only due to the complete failure of the killer vertex (T_{MF} and T_{mMF} have no impact on the functionality of the victim vertex). As a consequence, the equivalent expression for $T_U^{m,MF}$ and $T_U^{m,mMF}$ are modified as follows:

$$\forall q \in \mathbf{N}_n^*, \begin{cases} T_{U,\,\text{vertex}\,q}^{m,MF} = \min\left[T_{MF,\,\text{vertex}\,q}, T_{U,\,\text{vertex}\,q}^{k,F}\right] \text{ if } T_{U,\,\text{vertex}\,q}^{k,F} \text{ exists} \\ T_{U,\,\text{vertex}\,q}^{m,MF} = T_{MF,\,\text{vertex}\,q} \quad \text{else} \end{cases} \tag{5.53}$$

$$\forall q \in \mathbf{N}_n^*, \begin{cases} T_{U,\,\text{vertex}\,q}^{m,mMF} = \min\left[T_{mMF,\,\text{vertex}\,q}, T_{U,\,\text{vertex}\,q}^{k,F}\right] \text{ if } T_{U,\,\text{vertex}\,q}^{k,F} \text{ exists} \\ T_{U,\,\text{vertex}\,q}^{m,mMF} = T_{mMF,\,\text{vertex}\,q} \quad \text{else} \end{cases} \tag{5.54}$$

The matrices $H_l^{MF} = \left[h_{i\,j}^{l,MF}\right]_{n_l \times n_l}$ and $H_l^{mMF} = \left[h_{i\,j}^{l,mMF}\right]_{n_l \times n_l}$ are defined for $l \in E_L$ in the same fashion than H_l^F in Eq. (5.7):

$$\forall l \in E_L, \begin{cases} \text{if } i = j, h_{i\,j}^{l,MF} = T_{U,\,\text{vertex } f^{-1}(l,i)}^{m,MF} \\ \text{if } i \neq j, \begin{cases} \text{if } a_{i\,j}^l = 1, h_{i\,j}^{l,MF} = \min\left[T_{MF,\,\text{edge } f^{-1}(l,j) \to f^{-1}(l,i)}, T_{U,\,\text{vertex } f^{-1}(l,j)}^{m,MF}\right] \\ \text{if } a_{i\,j}^l = 0, h_{i\,j}^{l,F} = 0 \end{cases} \end{cases} \tag{5.55}$$

$$\forall l \in E_L, \begin{cases} \text{if } i = j, h_{i\,j}^{l,mMF} = T_{U,\,\text{vertex } f^{-1}(l,i)}^{m,mMF} \\ \text{if } i \neq j, \begin{cases} \text{if } a_{i\,j}^l = 1, h_{i\,j}^{l,mMF} = \min\left[T_{mMF,\,\text{edge } f^{-1}(l,j) \to f^{-1}(l,i)}, T_{U,\,\text{vertex } f^{-1}(l,j)}^{m,mMF}\right] \\ \text{if } a_{i\,j}^l = 0, h_{i\,j}^{l,mMF} = 0 \end{cases} \end{cases} \tag{5.56}$$

In the same fashion, $\mathbf{m}_l^{MF} = \left[m_i^{l,MF}\right]_{n_l \times 1}$ and $\mathbf{m}_l^{mMF} = \left[m_i^{l,mMF}\right]_{n_l \times 1}$ for $l \in E_L$ are defined as $\mathbf{m}_l^F$ using Eq. (5.8):

$$\forall l \in E_L, m_i^{l,MF} = \max_j h_{ij}^{l,MF} \tag{5.57}$$

$$\forall l \in E_L, m_i^{l,mMF} = \max_j h_{ij}^{l,mMF} \tag{5.58}$$

The times of unavailability due to the functional redundancy in the *MF* and *mMF* cases ($T_U^{r,MF}$ and $T_U^{r,mMF}$ respectively) can now be computed as:

$$\forall l \in E_L, \forall i \in \mathbf{N}_{n_l}^*, T_{U,\text{ vertex } f^{-1}(l,i)}^{r,MF} = m_i^{l,MF} \tag{5.59}$$

$$\forall l \in E_L, \forall i \in \mathbf{N}_{n_l}^*, T_{U,\text{ vertex } f^{-1}(l,i)}^{r,mMF} = m_i^{l,mMF} \tag{5.60}$$

Finally, the times to unavailability due to the precursor effect for the *MF* and *mMF* cases are:

$$\forall q \in \mathbf{N}_{|E_p|}^*, T_{U,\text{ vertex } \mathbf{v_1}(q)}^{p,MF} = T_{U,\text{ vertex } \mathbf{k_1}(q)}^{r,MF} \tag{5.61}$$

$$\forall q \in \mathbf{N}_{|E_p|}^*, T_{U,\text{ vertex } \mathbf{v_1}(q)}^{p,mMF} = T_{U,\text{ vertex } \mathbf{k_1}(q)}^{r,mMF} \tag{5.62}$$

Once again, in the case that a victim vertex has several killers, $T_U^{p,MF}$ and $T_U^{p,mMF}$ are equal to the minimum of the times of the killer vertices.

Similarly to the failed case (F), the convergence condition of the algorithm is given by $T_{U,\text{ vertex } q}^{m,MF} \leq T_{U,\text{ vertex } q}^{p,F}$ and $T_{U,\text{ vertex } q}^{m,mMF} \leq T_{U,\text{ vertex } q}^{p,F}$ for all victim vertices q in the precursor effect. While these conditions are not met, set $T_{U,\text{ vertex } q}^{m,MF} = T_{U,\text{ vertex } q}^{p,F}$ and $T_{U,\text{ vertex } q}^{m,mMF} = T_{U,\text{ vertex } q}^{p,F}$ (precursor times for the failed case for similar reasons with T_U^m in Eqs. (5.53) and (5.54)) and repeat the precursor effect process outlined above.

Combination of all effects. The final times to unavailability in the *MF* and *mMF* cases are derived in a similar way than Eq. (5.11):

$$\forall q \in \mathbf{N}_n^*, T_{U,\text{ vertex } q}^{MF} = \min\left[\max\left(T_{MF,\text{ vertex } q}, T_{U,\text{ vertex } q}^{r,MF}\right), T_{U,\text{ vertex } q}^{k,MF}, T_{U,\text{ vertex } q}^{p,MF}\right] \tag{5.63}$$

$$\forall q \in \mathbf{N}_n^*, T_{U,\text{ vertex } q}^{mMF} = \min\left[\max\left(T_{mMF,\text{ vertex } q}, T_{U,\text{ vertex } q}^{r,mMF}\right), T_{U,\text{ vertex } q}^{k,mMF}, T_{U,\text{ vertex } q}^{p,mMF}\right] \tag{5.64}$$

where $T_{U,\text{vertex} q}^{r,MF}$, $T_{U,\text{vertex} q}^{k,MF}$, $T_{U,\text{vertex} q}^{p,MF}$, $T_{U,\text{vertex} q}^{r,mMF}$, $T_{U,\text{vertex} q}^{k,mMF}$ and $T_{U,\text{vertex} q}^{p,mMF}$ are included in if they exist.

5.2.3. Summary of the Anomaly and Failure Propagation Algorithm

Below is a summary of the algorithmic process used to propagate multi-state failures across the network. The following inputs are required: the adjacency matrices and interlayer matrix, the mapping function (these three elements defining a network architecture), and the c.d.f.s for the anomaly and failure distributions of the vertices and edges.

1. Generate for each vertex *i* $T_{F,\text{vertex}\ i}$, $T_{MF,\text{vertex}\ i}$, and $T_{mMF,\text{vertex}\ i}$ (section 5.2.1)
2. Generate for each edge $T_{F,\text{edge}\ j\to i}$, $T_{MF,\text{edge}\ j\to i}$, and $T_{mMF,\text{edge}\ j\to i}$ (section 5.2.1)
3. Compute E_k using Eq. (5.1)
4. Compute $\mathbf{k_1}$ and $\mathbf{v_1}$ using Eq. (5.2)
5. Compute $T_U^{k,F}$, $T_U^{k,MF}$ and $T_U^{k,mMF}$ for each victim vertex using Eqs. (5.3), (5.50) and (5.51)
6. Compute E_p using Eq. (5.4)
7. Compute $\mathbf{k_2}$ and $\mathbf{v_2}$ using Eq. (5.5)
8. Compute $T_U^{m,F}$, $T_U^{m,MF}$ and $T_U^{m,mMF}$ for each vertex using Eqs. (5.6), (5.53) and (5.54)
9. For all $l \in E_L$, compute H_l^F , H_l^{MF} and H_l^{mMF} using Eqs. (5.7), (5.55) and (5.56)
10. For all $l \in E_L$, compute $\mathbf{m}_l^F$, $\mathbf{m}_l^{MF}$ and $\mathbf{m}_l^{mMF}$ using Eqs. (5.8), (5.57) and (5.58)
11. Compute $T_U^{r,F}$, $T_U^{r,MF}$ and $T_U^{r,mMF}$ for each vertex for all layers $l \in E_L$ using Eqs. (5.9), (5.59) and (5.60)
12. Compute $T_U^{p,F}$, $T_U^{p,MF}$ and $T_U^{p,mMF}$ for each victim vertex using Eqs. (5.10), (5.61) and (5.62)
13. Repeat steps 9–12 for victim vertices *q* in the precursor effect until $T_{U,\,\text{vertex}\,q}^{m,F} \le T_{U,\,\text{vertex}\,q}^{p,F}$, $T_{U,\,\text{vertex}\,q}^{m,MF} \le T_{U,\,\text{vertex}\,q}^{p,F}$ and $T_{U,\,\text{vertex}\,q}^{m,mMF} \le T_{U,\,\text{vertex}\,q}^{p,F}$
14. Compute T_U^F , T_U^{MF} and T_U^{mMF} for each vertex using Eqs. (5.11), (5.63) and (5.64)

5.2.4. Failure Propagation Example in the Multi-State Case

Let us revisit the first example presented in section 5.1.6 by considering the *MF* case additionally (the *mMF* case can be applied in a similar fashion). The times to failures (T_F) and to *MF* state (T_{MF}) are given in Table 5.2, and shown in Figure 5.3 for clarity purposes.

Table 5.2. Times to failure and degradation of the nodes and link in the case study example

	Time to failure T_F	**T_{MF}**
	years	years
Spacecraft #1		
TTC	2	1
Supporting subsystems	6	6
Payload	7	5
Spacecraft #2		
TTC	9	4
Supporting subsystems	8	0.5
Link between spacecraft	12	11

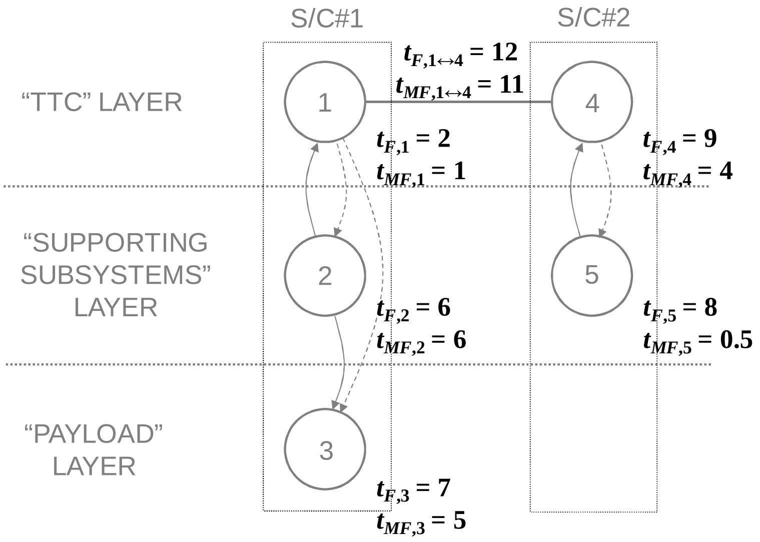


Figure 5.3. IMLN representation with node and link times to failure and degradation

If spacecraft #1 was to be by itself, it would have failed at 2 years and been in a *MF* state at 1 year, when the TTC failed and degraded. However, in this network configuration, the second spacecraft can help maintaining the functionality up to 6 years on-orbit for a non-failed state, and 4 years for a non-*MF* state. How these numbers were obtained is explained below using the 14 steps given in section 5.2.2. Steps 1 and 2 are already completed as the times to failure for the nodes and link are given in this example.

3. According to section 4.5.1,

$$E_k = \{(2,1),(2,3),(5,4)\} \tag{5.65}$$

4. Then,

$$\mathbf{k_1} = (2 \quad 2 \quad 5) \text{ and } \mathbf{v_1} = (1 \quad 3 \quad 4) \tag{5.66}$$

5. Propagating the kill effect yields:

$$\begin{cases} t_{U,1}^{k,F} = t_{F,2} = 6 \\ t_{U,3}^{k,F} = t_{F,2} = 6 \\ t_{U,4}^{k,F} = t_{F,5} = 8 \end{cases} \tag{5.67}$$

And:

$$\begin{cases} t_{U,1}^{k,MF} = t_{MF,2} = 6 \\ t_{U,3}^{k,MF} = t_{MF,2} = 6 \\ t_{U,4}^{k,MF} = t_{MF,5} = 0.5 \end{cases} \tag{5.68}$$

6. According to section 4.5.1,

$$E_p = \{(1,2),(1,3),(4,5)\} \tag{5.69}$$

7. Then,

$$\mathbf{k}_2 = \begin{pmatrix}1 & 1 & 4\end{pmatrix} \text{ and } \mathbf{v}_2 = \begin{pmatrix}2 & 3 & 5\end{pmatrix} \tag{5.70}$$

8. The minimum time to unavailability after the kill effect is given as:

$$\begin{cases} t_{U,1}^{m,F} = \min\left[t_{F,1}, t_{U,1}^{k,F}\right] = \min[2,6] = 2 \\ t_{U,2}^{m,F} = t_{F,2} = 6 \\ t_{U,3}^{k,F} = \min\left[t_{F,3}, t_{U,3}^{k,F}\right] = \min[7,6] = 6 \\ t_{U,4}^{k,F} = \min\left[t_{F,4}, t_{U,4}^{k,F}\right] = \min[9,8] = 8 \\ t_{U,5}^{m,F} = t_{F,5} = 8 \end{cases} \tag{5.71}$$

And:

$$\begin{cases} t_{U,1}^{m,MF} = \min\left[t_{MF,1}, t_{U,1}^{k,F}\right] = \min[1,6] = 1 \\ t_{U,2}^{m,MF} = t_{MF,2} = 6 \\ t_{U,3}^{k,MF} = \min\left[t_{MF,3}, t_{U,3}^{k,F}\right] = \min[5,6] = 5 \\ t_{U,4}^{k,MF} = \min\left[t_{MF,4}, t_{U,4}^{k,F}\right] = \min[4,8] = 4 \\ t_{U,5}^{m,MF} = t_{MF,5} = 0.5 \end{cases} \tag{5.72}$$

9. The only functionally redundant layer in this IMLN is the TTC layer. The associated *H* matrices are expressed as:

$$H_1^F = \begin{bmatrix} t_{U,1}^{m,F} & \min\left[t_{F,4\to1}, t_{U,4}^{m,F}\right] \\ \min\left[t_{F,1\to4}, t_{U,1}^{m,F}\right] & t_{U,4}^{m,F} \end{bmatrix} = \begin{bmatrix} 2 & \min[12,8] \\ \min[12,2] & 8 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 2 & 8 \end{bmatrix} \tag{5.73}$$

And:

$$H_1^{MF} = \begin{bmatrix} t_{U,1}^{m,MF} & \min\left[t_{MF,4\to1}, t_{U,4}^{m,MF}\right] \\ \min\left[t_{MF,1\to4}, t_{U,1}^{m,MF}\right] & t_{U,4}^{m,MF} \end{bmatrix} = \begin{bmatrix} 1 & \min[11,4] \\ \min[11,1] & 4 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 1 & 4 \end{bmatrix} \tag{5.74}$$

10. Then,

$$\mathbf{m}_1^F = \begin{bmatrix} \max[2,8] \\ \max[2,8] \end{bmatrix} = \begin{bmatrix} 8 \\ 8 \end{bmatrix} \tag{5.75}$$

And:

$$\mathbf{m}_1^{MF} = \begin{bmatrix} \max[1,4] \\ \max[1,4] \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \end{bmatrix} \tag{5.76}$$

11. The times to unavailability for the TTCs due to the functional redundancy are expressed as:

$$\begin{cases} t_{U,1}^{r,F} = m_{11}^{1,F} = 8 \\ t_{U,4}^{r,F} = m_{12}^{1,F} = 8 \end{cases} \tag{5.77}$$

And:

$$\begin{cases} t_{U,1}^{r,MF} = m_{11}^{1,MF} = 4 \\ t_{U,4}^{r,MF} = m_{12}^{1,MF} = 4 \end{cases} \tag{5.78}$$

12. Propagating the precursor effect yields:

$$\begin{cases} t_{U,2}^{p,F} = t_{U,1}^{r,F} = 8 \\ t_{U,3}^{p,F} = t_{U,1}^{r,F} = 8 \\ t_{U,5}^{p,F} = t_{U,4}^{r,F} = 8 \end{cases} \tag{5.79}$$

And:

$$\begin{cases} t_{U,2}^{p,MF} = t_{U,1}^{r,MF} = 4 \\ t_{U,3}^{p,MF} = t_{U,1}^{r,MF} = 4 \\ t_{U,5}^{p,MF} = t_{U,4}^{r,MF} = 4 \end{cases} \tag{5.80}$$

13. The convergence condition is met in this particular example, so the algorithm continues to the final step.
14. Combining all the effect, the final times to unavailability for the nodes are:

$$\begin{cases} t_{U,1}^{F} = \min\left[\max\left(t_{F,1}, t_{U,1}^{r,F}\right), t_{U,1}^{k,F}\right] = \min\left[\max(2,8),6\right] = 6 \\ t_{U,2}^{F} = \min\left[t_{F,2}, t_{U,2}^{p,F}\right] = \min[6,8] = 6 \\ t_{U,3}^{F} = \min\left[t_{F,3}, t_{U,3}^{k,F}, t_{U,3}^{p,F}\right] = \min[7,6,8] = 6 \\ t_{U,4}^{F} = \min\left[\max\left(t_{F,4}, t_{U,4}^{r,F}\right), T_{U,4}^{k,F}\right] = \min\left[\max(9,8),8\right] = 8 \\ t_{U,5}^{F} = \min\left[t_{F,5}, t_{U,5}^{p,F}\right] = \min[8,8] = 8 \end{cases} \tag{5.81}$$

And:

$$\begin{cases} t_{U,1}^{MF} = \min\left[\max\left(t_{MF,1}, t_{U,1}^{r,MF}\right), t_{U,1}^{k,MF}\right] = \min\left[\max(1,4),6\right] = 4 \\ t_{U,2}^{MF} = \min\left[t_{MF,2}, t_{U,2}^{p,MF}\right] = \min[6,4] = 4 \\ t_{U,3}^{MF} = \min\left[t_{MF,3}, t_{U,3}^{k,MF}, t_{U,3}^{p,MF}\right] = \min[5,6,4] = 4 \\ t_{U,4}^{MF} = \min\left[\max\left(t_{MF,4}, t_{U,4}^{r,MF}\right), T_{U,4}^{k,F}\right] = \min\left[\max(4,4),0.5\right] = 0.5 \\ t_{U,5}^{MF} = \min\left[t_{MF,5}, t_{U,5}^{p,MF}\right] = \min[0.5,4] = 0.5 \end{cases} \tag{5.82}$$

5.3. Summary

This chapter was entirely dedicated to the study of the anomaly and failure propagation across interdependent multi-layer networks. This chapter developed several contributions:

- The formal description of the mechanisms that enable the propagation of failures and anomalies across the network, supporting a complete survivability analysis of the network under consideration;
- The establishments of several algorithms for:
    - the propagation of complete failures of nodes and links across the network;
    - the concurrent generation of times to failure and degradation in the context of multi-state failures;
    - the concurrent propagation of multi-state failures across the network.
- The illustration of the failure propagation process through case-study examples.

The following chapter aims to validate the modeling and simulation tool presented in this chapter, quantify its precision and its scalability.

CHAPTER 6

VALIDATION AND SCALABILITY OF INTERDEPENDENT MULTI-LAYER NETWORK MODELING

6.1. Introduction

The previous chapters have introduced the need of the interdependent multi-layer approach and developed the necessary tools to tackle survivability analyses for space-based networks. This chapter aims to test that the proposed tool correctly perform what it is designed for, as well as quantify the simulation output precision and evaluate the scalability of the model.

The first objective will be tackled using an alternative modeling scheme, namely the stochastic Petri nets, as well as analytical solutions that can exceptionally be derived for simple forms of networks: the output probabilities of the IMLN approach will be compared to the output of these two alternative ways of obtaining them, and it will be shown that the IMLN results are in excellent agreement with the other two set of results as shown in sections 6.2 and 6.3. Consequently, the IMLN output can be trusted for further analysis in the following chapter (Chapter 7).

The second objective arises from the fact that the results from the IMLN approach are obtained by running Monte Carlo simulations. As a consequence, there is an inherent variability in the probabilities outputted by the simulation associated with the number of runs selected for the Monte Carlo. Section 6.4 investigates the spread of the confidence intervals and ways to maintain the precision of the IMLN results. This discussion is continued in section 6.5.

Finally, section 6.5 also addresses questions relative to the scalability of the IMLN approach, such as: how does precision requirements affect the simulation time? How flexible is the IMLN representation in handling large network size? How does this network size affect the simulation time?

6.2. Stochastic Petri Nets

6.2.1. Overview of Stochastic Petri Nets

Petri nets were introduced in 1962 by the German computer scientist, Carl Adam Petri (1926–2010). A Petri net is a bipartite directed graph used to model discrete-event systems that can display concurrent or asynchronous processes (Peterson, 1977). The Petri net graph has 2 disjoint sets of vertices (or nodes): places and transitions. Directed arcs are drawn between a place and a transition (called input arc) or conversely between a transition and a place (called output arc). Places connected to a transition by input arcs are called input places of that transition, and conversely places connected to a transition by output arcs are called output places of that transition. In addition to places, transitions, and directed arcs, Petri nets also have “tokens”, or markings that can be associated with each place.

As explained by Peterson (1977), a Petri net has “static” and “dynamic” properties: the Petri net graph describes its “static properties”, and its “dynamic properties [...] result from its execution”. The evolution of the Petri net is marked by the movement of the tokens from places to places, through the “firing” of transitions. However, the firing of a transition occurs only if this transition has been “enabled” beforehand, i.e., if tokens are present in all the input places of the transition. The firing rules of the transitions define the dynamic behavior of the system, and the combination of the locations of the tokens, called the marking, characterizes the current state of the system. Thus, places model particular “conditions” of the system (e.g., subsystem X experienced a major anomaly), while transitions model “events” affecting the system (e.g., failure of subsystem X). The condition associated with a place is realized when one (or several) token(s) are in that place. Formal mathematical definitions of Petri nets can be found in Peterson (1977; 1981) or Haas (2002).

Stochastic Petri Nets (SPNs) are a subfamily of Petri nets, and they add a stochastic behavior to the modeling scheme by introducing randomness in the firing of transitions, modeled for example with exponential, Weibull, or lognormal distributions. Details about stochastic Petri nets, or other Petri net subfamilies (e.g., colored or hierarchical Petri nets) can be found in Haas (2002), or Ajmone Marsan (1989).

Two additional types of arcs exist in Petri net modeling, the inhibitor and the enabler arcs. The inhibitor arc prevents a transition from firing when a token is present in the place linking the transition and the place. Its usefulness will be shown in an example shortly. Conversely, the enabler arc is a “negative inhibitor” (Volovoi, 2006) that enables or forces the transition to occur. In essence, the inhibitor and enabler arcs “override” the stochastic nature of a transition in an SPN model (or a deterministic temporal delay in a regular Petri Net).

To better understand the construction and evolution of a Petri net, consider the following example. A system is composed of two subsystems, and each can be in two states: operational or failed. After a failure, each subsystem can be repaired and brought back to the operational state, but only one subsystem at a time. In other words, only one subsystem can be repaired at a time. This system is shown in Figure 6.1.

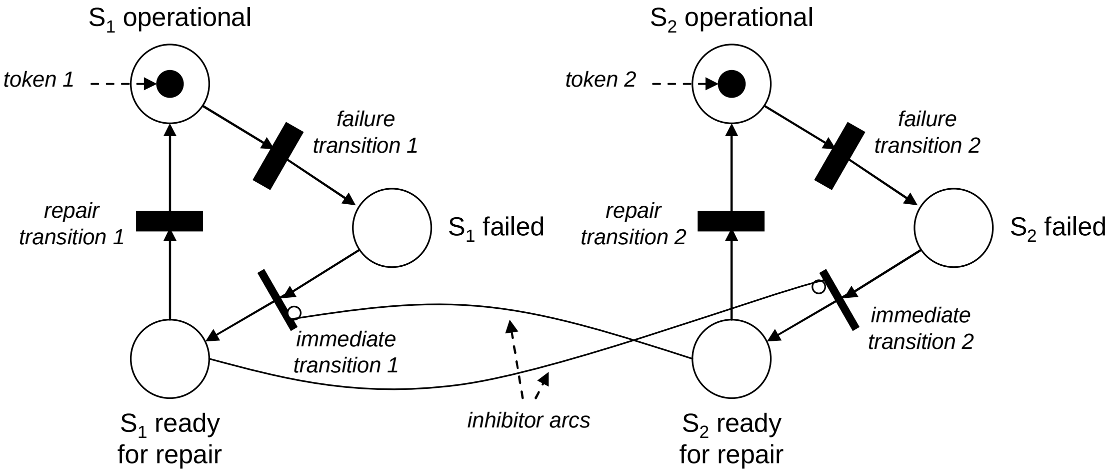


Figure 6.1. Two-subsystem system with repair queue

(*initial configuration with subsystem 1 (S_1) and subsystem 2 (S_2) both operational*)

All the elements previously mentioned can be seen in Figure 6.1:

- six places (shown as circles) representing the possible “states” the subsystems can evolve towards;

- two tokens initially in the operational places for the subsystems, indicating that initially the systems is in this configuration/state;
- the failure and repair transitions are displayed as large black rectangles and represent the stochastic or deterministic laws governing the failure and the repair time of the subsystems; the immediate transitions are represented differently here (with thin black rectangles) to ensure the clarity of the model.
- These immediate transitions can be overridden by the inhibitor arcs to ensure than only one subsystem get repaired at a time: if subsystem 1 (S_1) fails first for example, the token 1 initially in the place labeled "S_1 operational" transitions to the place labeled "S_1 failed", and as the subsystem 2 is still operational, the immediate transition is enabled and the token 1 immediately transitions to the place labeled "S_1 ready for repair". Since now a token is present in that place, the inhibitor arc overrides the immediate transition 2. As a consequence, if the subsystem 2 fails while the immediate transition 2 is still inhibited, the token 2 will stay in the place labeled "S_2 failed" until the token 1 transitions back to the place labeled "S_1 operational."[7]

6.2.2. Stochastic Petri Nets for Multi-State Failure and Survivability Modeling

In multi-state failure or survivability analyses, the finer resolution into the degradation and failure behavior of systems introduces additional complexity compared with the traditional reliability analysis, and requires as a consequence more advanced analytical

[7] As a side note, enabler arcs could have been used instead of inhibitor arcs in this example: an enabler arc between "S_1 operational" and the immediate transition 2, and another one between "S_2 operational" and the immediate transition 1 would have modeled the same behavior.

techniques for modeling and analysis, such as the IMLN framework proposed in this thesis, Markov chains or more broadly stochastic timed automata.

SPNs have several advantages over Markov chains for modeling and analyzing multi-state systems. One argument in support of this statement is the following: consider a simple example, where a system is composed of *k* subsystems and each subsystem can be in *m* different states. In the case of a Petri net modelization, “only” *km* places are necessary to model the state evolution of this system (the presence of tokens in places will reflect which state the system is in). However, with a Markovian approach, m^k states are necessary. The ratio of the number of states necessary for a Markovian approach to the number of places required in a Petri net approach is plotted in Figure 6.2. The figure shows this ratio with respect to the number of subsystems *k*, and for 4 different values of the number of states per subsystem, *m*, (*m* = 2 for the lowest curve to *m* = 5 for the uppest curve). The figure is plotted with a logscale *y*-axis due to the explosion of this ratio for higher values of *k* and *m*.

Figure 6.2 reads as follows: for example, for *k* = 5 and *m* = 5 (the upper-most curve), a Marvokian model requires 125 more states than places in a Petri net model. The proliferation of states or places when *k* or *m* increases is rightfully described as the “dimension damnation” of multi-state failure analysis by Lisnianski and Levitin (2003), but is significantly more acute in the case of the Markovian approach. Figure 6.2 also shows for example that for systems with 7 or more components, even in the case of the traditional binary reliability analysis, Markov Chains require at least an order of magnitude more states to model the system than places in an equivalent Petri net. More broadly, this feature of Markov chains—their (acute) dimension damnation—results from the fact that Markovian modeling requires “global states” and a “global clock” for the system to run the state evolution against. That is, the system can be in only one state at a time, and this state describes the status of all the subsystems evolving in time with respect to the unique “global” clock. In contrast, Petri nets allow local modeling (places per subsystem) and local clocks, where each subsystem evolves with its own token(s) and the system state is given by the marking of the Petri net.

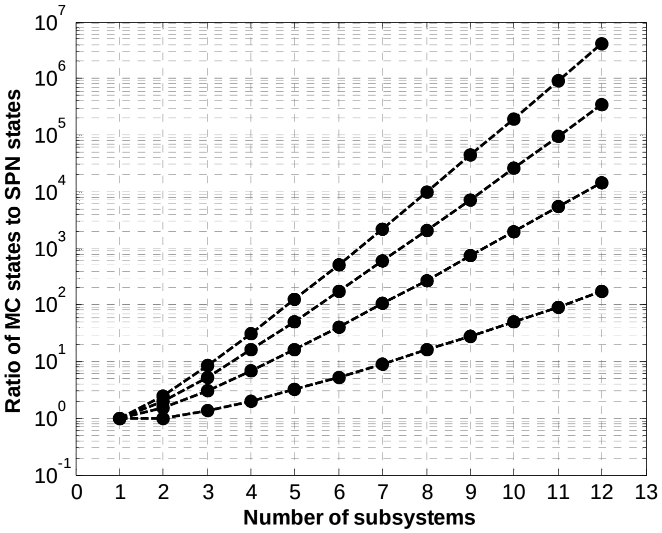


Figure 6.2. Numbers of states in Markov Chains versus Petri nets

(*the lower curve represents subsystems with 2 states, and the upper curve represents subsystems with 5 states*)

Another advantage of SPNs is their intrinsic ability to handle any distribution for the time to transition, for example non-exponential transitions such as the Weibull or the lognormal, as opposed to the Markovian approach which would require more complex and involved operations to manage time-varying failure rate (e.g., systems exhibiting infant mortality or wear-out behavior).

Although initially used for the modeling and analysis of manufacturing systems and computer networks, stochastic Petri Nets are slowly but increasingly being adopted for reliability studies, as well as for maintenance and risk analysis, because of the many advantages they provide over Markov chains for example (Volovoi, 2004). The adoption of SPN is still hampered however by the limited availability of Petri net software, especially when compared with the widespread availability of software tools for other modeling approaches. In this thesis, the software SPN@ (Volovoi, 2006) was used.

In the space application developed in this work, we consider 12 subsystems on-board spacecraft, and each of these subsystems can be in 4 different states of functionality. Thus 48 places are necessary in the case of a Petri net to capture the overall state of only one spacecraft, whereas more than 16 million states are necessary in a Markovian approach. The state space for a Markov chain (or a semi-Markov model) would make it unmanageable and impossible to visualize. Also, the number of transition laws to calculate and populate in the model would be unmanageable.

6.2.3. Stochastic Petri Net Representation of a Spacecraft and of the Case Study Space-Based Network

The traditional monolith and the case study SBN architectures were introduced in previous chapters but are recalled here for readability purposes. The monolith architecture consists of a single spacecraft with the 11 subsystems introduced in Chapter 2 and Chapter 3, plus the unknown category:

1. Gyro / Sensor / Reaction Wheel (hereafter referred to as Gyro)
2. Thruster / Fuel (Thruster)
3. Beam / Antenna Operation / Deployment (Beam)
4. Control Processor (CP)
5. Mechanisms / Structures / Thermal (Mechanisms)
6. Payload Instrument / Amplifier / On-board Data / Computer / Transponder (Payload)
7. Battery / Cell (Battery)
8. Electrical Distribution (ED)
9. Solar Array Deployment (SAD)
10. Solar Array Operating (SAO)
11. Telemetry, Tracking and Command (TTC)

The Gyro and Thruster subsystems can be lumped together into a macro-subsystem called Attitude and Orbit Control Subsystem (AOCS), and the Battery, ED, SAD and SAO subsystems are part of the macro-subsystem named Electrical Power Subsystem (EPS).

The traditional monolith architecture is presented in the upper part of Figure 6.3. The case study space-based network consists of two spacecraft (S/C #1 and S/C#2): S/C #1 is similar to the spacecraft in the monolith architecture, while S/C #2 possesses all the subsystems but the payload. The two spacecraft are networked wirelessly together to provide a functional redundancy for the TTC. This SBN is shown in the bottom part of Figure 6.3.

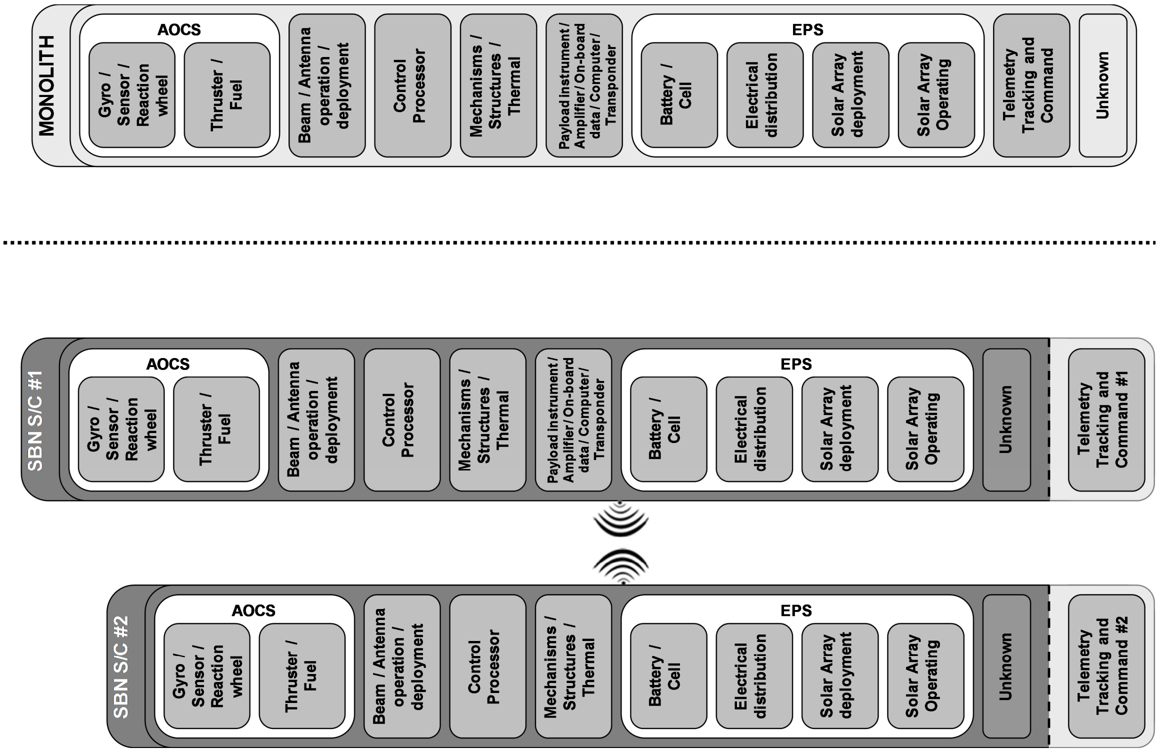

MONOLITH
AOCS
Gyro / Sensor / Reaction wheel
Thruster / Fuel
Beam / Antenna operation / deployment
Control Processor
Mechanisms / Structures / Thermal
Payload instrument / Amplifier / On-board data / Computer / Transponder
EPS
Battery / Cell
Electrical distribution
Solar Array deployment
Solar Array Operating
Telemetry Tracking and Command
Unknown
SBN S/C #1
Telemetry Tracking and Command #1
SBN S/C #2
Telemetry Tracking and Command #2

Figure 6.3. Architecture of the monolith spacecraft (top) and the case study SBN (bottom)

As developed in Chapter 3, four classes of failure events were recognized and analyzed for each subsystem:

- Subsystem state 4 (SubS4): fully operational
- Subsystem state 3 (SubS3): minor anomaly/degradation
- Subsystem state 2 (SubS2): major anomaly/degradation
- Subsystem state 1 (SubS1): total failure

Each subsystem can transition to a more severe state of degradation or failure and the associated probabilities of transitioning were derived in Chapter 3 as Weibull distributions.

To evaluate the survivability of these two architectures, four states were considered by the author at the system level:

- System state 4 (SysS4): fully operational: 0 – 5% performance loss
- System state 3 (SysS3): minor degradation: 5 – 35% performance loss
- System state 2 (SysS2): major degradation: 35 – 85% performance loss
- System state 1 (SysS1): total failure: 85 – 100% performance loss

These states determine the level of precision for the survivability analysis of the models. Additional precision can be obtained by defining additional states, which comes at the cost of increased analytical and computational complexity, as discussed previously. The probabilities of being in these four states are the output of the SPN model. Comparisons between the probabilities obtained provide the comparative survivability analysis of these two architectures, as will be shown shortly.

In the case of the monolith spacecraft, the following rules are used to link the subsystem and system levels of degradations and failures:

- The system is in the operational state (SysS4) if all the subsystems are in their operational states (SubS4);
- The system is in the failed state (SysS1) if one subsystem is in its failed state (SubS1);
- SubS3 state of the subsystems does not have a direct effect on the system level;

- The SubS2 state can lead to minor, major degradation or failed system states (SysS3, SysS2 and SysS1 respectively) according to conditional probabilities peculiar to each subsystem, as given in Table 6.1 (actual on-orbit data derived from the database). The probabilities given in Table 6.1 are "conditional" since they represent the probability that the system will transition to a degraded state given that a particular subsystem is in SubS2 state. For example, for the Gyro / Sensor / Reaction wheel subsystem, given that this subsystem is in SubS2 (major anomaly), there is 25.7% chance that the system transitions to a minor degradation state (SysS3), 54.3% chance to a major degradation state (SysS2) and 20% chance to a failed state (SysS1).

Table 6.1. Impact on the system level of subsystem major degradation (conditional probabilities)

Subsystem	Conditional probability that a SubS2 state leads to system:		
	minor degradation	**major degradation**	**total failure**
Gyro / Sensor / Reaction wheel	25.7%	54.3%	20%
Thruster / Fuel	50.9%	47.3%	1.8%
Beam / Antenna operation / deployment	70.6%	23.5%	5.9%
Control processor	0%	0%	100%
Mechanisms / Structures / Thermal	100%	0%	0%
Payload instrument / Amplifier / On-board data / Computer / Transponder	33.4%	59.1%	7.5%
Battery / Cell	56.2%	18.8%	25%
Electrical distribution	40%	40%	20%
Solar array deployment	40%	60%	0%
Solar array operating	61%	31.2%	7.8%
Telemetry Tracking and Command	43.5%	34.8%	21.7%
Unknown	58.4%	33.3%	8.3%

A summary of the subsystem and system states, and the links between is provided in Table 6.2.

Table 6.2. Summary of subsystem and system state and transitions

	States	**Transitions between states**
Subsystem level	For each subsystem, four states based on *subsystem anomalies and failures*: SubS4: operational SubS3: minor anomaly SubS2: major anomaly SubS1: total failure derived from the classes of events present in the database (see Chapter 3)	Weibull distributions derived from statistical data analysis (see Chapter 3)
System level	Four states based on the *performance degradation of the system*: SysS4: operational SysS3: minor degradation SysS2: major degradation SysS1: total system failure defined in this dissertation	Transitions between system states depend on subsystems states: *If a subsystem transitions to…* *then the system transitions to…* SubS3 → no transition (no impact on system states) SubS2 → SysS3 or SysS2 or SysS1 (see Table 6.1) SubS1 → SysS1

Given the stochastic transition laws between the different states summarized in Table 6.2, the SPN model of a monolith spacecraft facing on-orbit failures and anomalies was developed (using SPN@ (Volovoi, 2006)) and is shown in Figure 6.4. To clarify this model and enable an easy identification of its different parts, Figure 6.5 is provided showing the overall SPN model, the spacecraft architecture, the various subsystem models, and the system transition diagram. In addition, a zoom-in or enlargement of two subsystems SPN models is shown in Figure 6.5, those of the Gyro, and the TTC subsystems. The system level states are clearly identified and illustrated by a schematic transition diagram. The remaining states are labeled “intermediary states” and are used to link the subsystem level to the system level according to the empirical data and the previously stated rules.

A similar SPN model has been developed for the case study SBN, and is provided in the appendix of this chapter instead of the main body for readability purposes. Its derivation is presented in detail in Castet and Saleh (2012) and Saleh and Castet (2011). Also explained in these references is the extensive testing done to validate these SPN models.

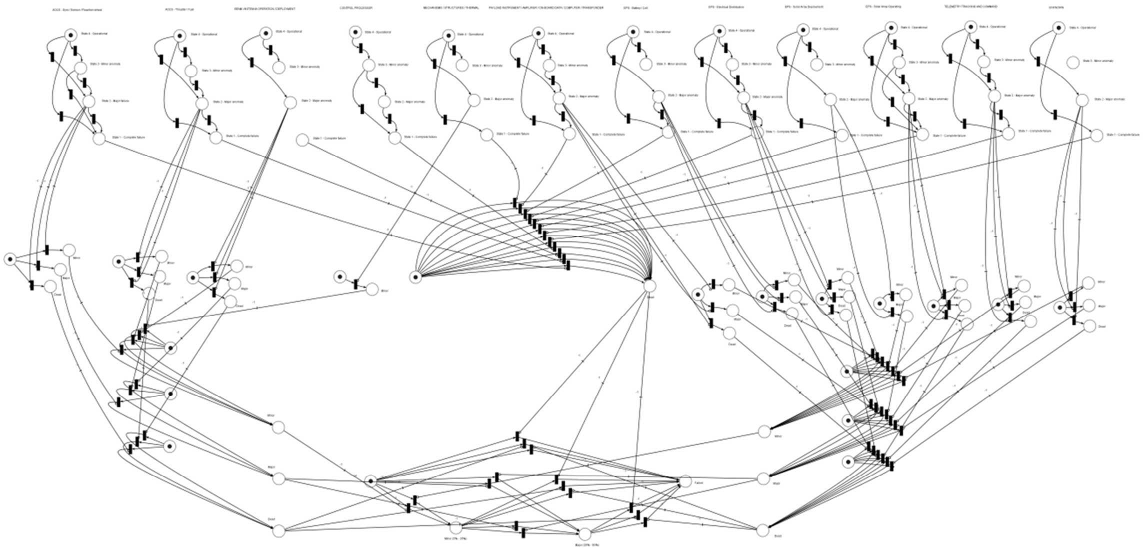

ADCS - Gyro / Sensor / Reaction wheel
ADCS - Thruster / Fuel
BEAM / ANTENNA OPERATION / DEPLOYMENT
CONTROL PROCESSOR
MECHANISMS / STRUCTURES / THERMAL
PAYLOAD INSTRUMENT / AMPLIFIER / ON-BOARD DATA / COMPUTER / TRANSPONDER
EPS - Battery / Cell
EPS - Electrical Distribution
EPS - Solar Array Deployment
EPS - Solar Array Operating
TELEMETRY TRACKING AND COMMAND
UNKNOWN
State 4 - Operational
State 3 - Minor anomaly
State 2 - Major failure
State 2 - Major anomaly
State 1 - Complete failure

Figure 6.4. SPN model of a monolith spacecraft

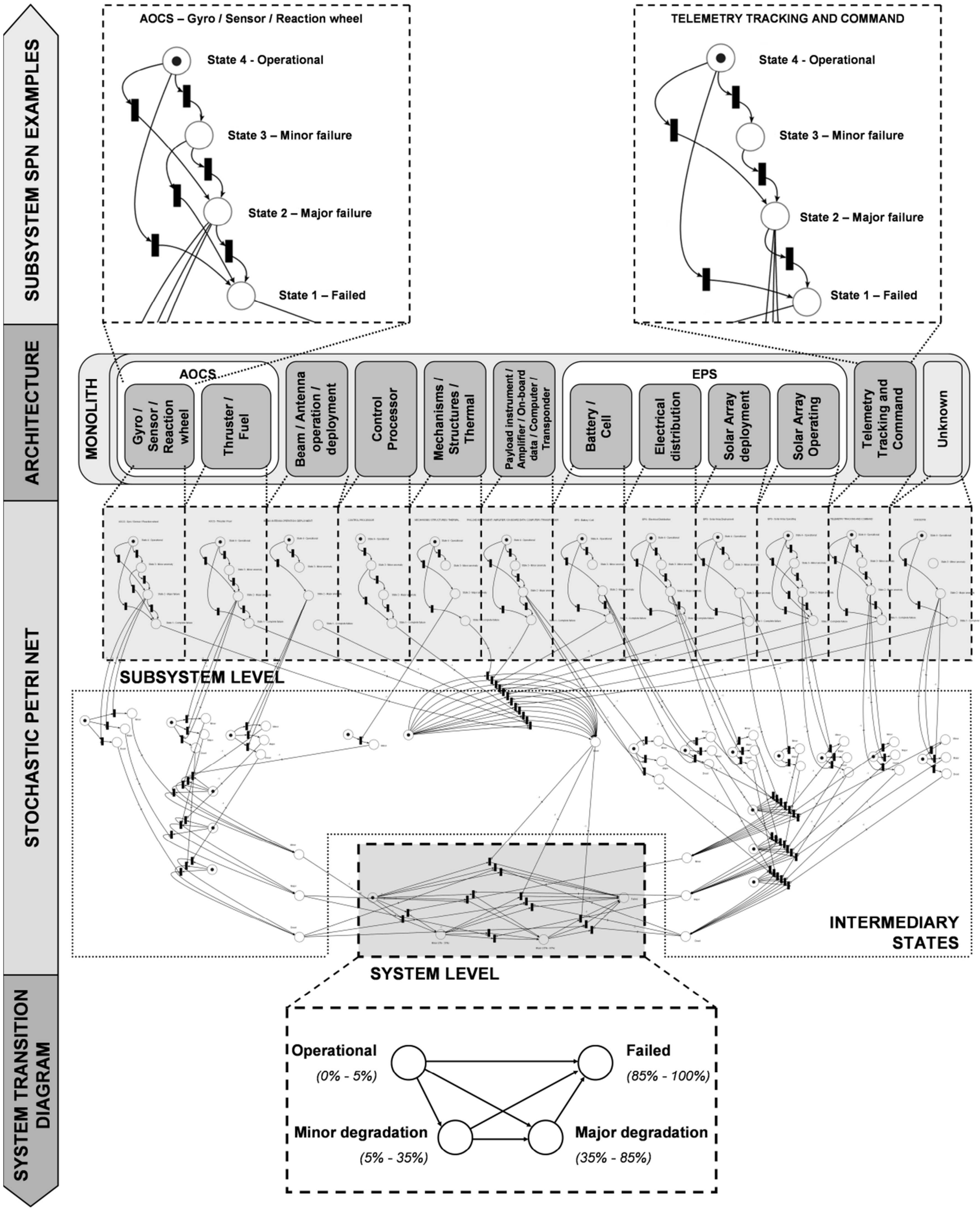


Figure 6.5. Construction clarification of the monolith spacecraft SPN model

Results. Running the Monte Carlo simulation of the SPN model in the case of the monolith spacecraft provides the evolution in time of the probabilities of the system being in operational or different failed states (i.e., operational, minor and major degradation, failed). Figure 6.6 presents these results, shown in two different plots for readability purposes given their different ranges on the *y*-axis.

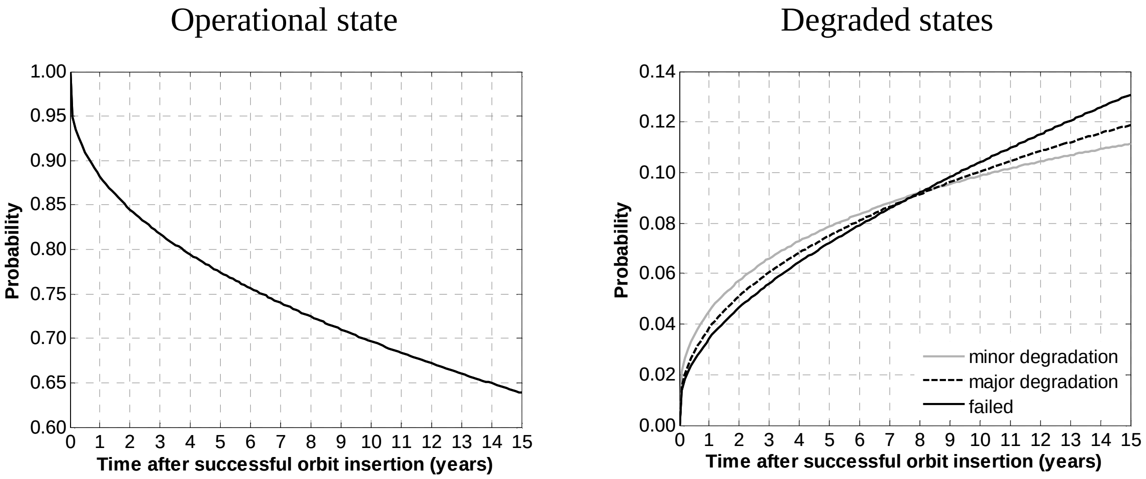


Figure 6.6. State probability results of the monolith spacecraft SPN model

Figure 6.6 reads as follows: for example after six years on-orbit, a monolith spacecraft has a 75.6% likelihood of being fully operational, 8.4% of being in minor degradation, 8.1% of being in major degradation state, and 7.9% of being in a failed state. Similarly, after 10 years for example, a spacecraft has only a 70% likelihood of being fully operational, that is, of not experiencing some form of anomaly or degradation. This result offers a significant opportunity, can be thought of as a call to arms, to improve spacecraft design and testing.

For the space-based network, running the simulation of its SPN model leads to the same kind of plots. This in turns allows the comparison of the probability of residency in each state for both architectures. Figure 6.7 for example displays the probability of residency in the operational and failed states for the monolith spacecraft and the space-based network.

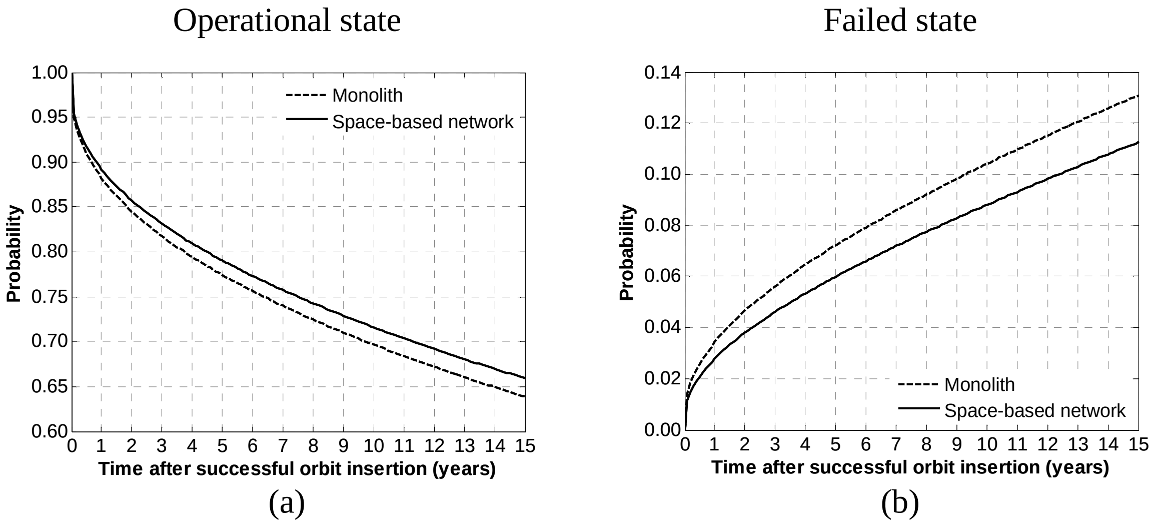


Figure 6.7. Comparison between the monolith spacecraft and the SBN for the fully operational (a) and failed (b) states

Figure 6.7a is confined to the operational state and clearly shows that the space-based network is more likely to be in an operational state than the traditional monolith spacecraft at any point in time, given stochastic on-orbit anomalies and failures. For example, after 15 years, there is a 65.9% likelihood that the space-based network will still be in the operational state, compared with 63.9% for the monolith spacecraft. This two-percentage point increment is provided by the networked nature of this architecture and the ability of one spacecraft to tap into a resource, in this case the TTC, of the second spacecraft. Similarly, Figure 6.7b shows that the space-based network is less likely to be in a failed state than the traditional monolith at any point in time. For example, after 15 years, there is 11.2% likelihood that the space-based network will be in the failed state, compared with 13.1% for the monolith spacecraft.

A detailed analysis of the implications for design and architectural choice of the results presented above is conducted in Chapter 7. As a side note, other space-based network architectures were modeled with stochastic Petri nets, as presented in Castet and Saleh (2011). As seen above, the SPN modeling allow the generation of probabilities of degradation and failure of the space-based network. One might wonder why SPNs were not chosen as the principal modeling tool for survivability analysis, in place of the proposed IMLN representation. A Petri net is by nature a graphical representation of processes, and the generation of even the monolith spacecraft model was complex, as attested by Figure 6.5. The simple case study space-based network also required a complex SPN model, created manually. In comparison, the IMLN approach only requires the creation of three sets of input: the adjacency matrices, the interlayer matrix and the mapping function. As explained in section 6.5.3, their determination can be quite simple and the algorithm presented to propagate failures is not specific to any type of network. Consequently, the survivability exploration of several architectures is conducted by varying inputs in the case of the IMLN framework, while a graph must be specifically created for each architecture in the case of the SPN approach. As a conclusion, the IMLN approach is superior in terms of generalization, complexity and practicality. The actual introduction and use of SPN in the context of the IMLN modeling is presented next.

6.2.4. Use of SPN Model to Partially Create and Validate the IMLN Model

The monolith and space-based network SPN were used to create inputs for the IMLN, as well as using SPN results to (partially) validate IMLN models.

IMLN input creation. Remember that the required inputs for the IMLN models are based on design and architectural choices of the network (adjacency matrices A_1, …, A_L, the interlayer matrix C and the mapping function f) as well as on the failure behaviors of the vertices and edges of the network. The formers are immediately defined from an arbitrary architecture, while the latters are not trivial in their derivation. In this dissertation, it was chosen to represent the failure behavior of the vertices and the edges using cumulative distributions functions of the random variables T_F, T_{MF} and T_{mMF} (all three of them for a complete multi-state failure simulation, or a subset for other simulations (e.g., a complete failure simulation requires only the c.d.f.s for T_F)). These c.d.f.s are represented parametrically here using single Weibull distributions characterized by two Weibull parameters each: β_F, θ_F, β_{MF}, θ_{MF}, β_{mMF} and θ_{mMF}.

In this dissertation, deriving β_F, θ_F, β_{MF}, θ_{MF}, β_{mMF} and θ_{mMF} is not trivial as the severity levels at the subsystem level do not match the severity of the impact at the system level. Indeed, as summarized in Table 6.2, a subsystem in a minor degradation state (SubS3) does not translate in the overall spacecraft transitioning to the system minor degradation state (SysS3) for example. However, the IMLN inputs characterize the impact of failure behavior of the vertices and nodes at the system level. Hence, for example in the case study, the Weibull c.d.f. for the total failure (P_F) of TTC vertex is not defined by the results derived in Chapter 3 (that correspond to probability of the TTC being in SubS1), as Table 6.1 and Table 6.2 clearly show that the spacecraft will experience a total failure (SysS1) due to the TTC if the TTC experiences a total failure (SubS1) or a major degradation event (SubS2) that leads to a system total failure in 21.7% of the occurrences of such event.

The SPN model of the monolith spacecraft becomes extremely helpful in determining the Weibull parameters of the c.d.f.s for T_F, T_{MF} and T_{mMF} of the vertices in the IMLN models. For example, in the case of the case study IMLN, the required c.d.f.s are the ones of the TTC vertex, the supporting subsystems vertex and the payload vertex. These probabilities can be obtained by running subsets of the SPN monolith model with the subsystems of interest and tracking the resulting system state probability output of the Monte Carlo simulation. For example, in the case of the supporting subsystems vertex, the subset of subsystem under consideration consists of the AOCS, EPS, Beam, Mechanisms and CP subsystems; the arcs in the SPN model for the remaining subsystems modeling their impact on the system level being disconnected. To obtain the Weibull parameters β_F, θ_F, β_{MF}, θ_{MF}, β_{mMF} and θ_{mMF}, a non-linear least-square regression is used to fit single Weibull distributions to the output of the SPN simulation. In this space application, these Weibull models are very precise: for example, in the case of the TTC vertex, the average errors of the Weibull models with respect to the probability output of the SPN simulation are 0.003, 0.02 and 0.04 percentage points for T_F, T_{MF} and T_{mMF} respectively. The resulting Weibull parameters for the case study are shown in Table 6.3.

Table 6.3. Weibull parameters for T_F, T_{MF} and T_{mMF} of vertices in the IMLN case study model

Vertex	P_F	P_{MF}	P_{mMF}
TTC	$\beta_F = 0.4650$ $\theta_F = 47700$ years	$\beta_{MF} = 0.4680$ $\theta_{MF} = 28040$ years	$\beta_{mMF} = 0.4402$ $\theta_{mMF} = 28210$ years
Supporting subsystems	$\beta_F = 0.5529$ $\theta_F = 918.5$ years	$\beta_{MF} = 0.5052$ $\theta_{MF} = 435.0$ years	$\beta_{mMF} = 0.4638$ $\theta_{mMF} = 203.6$ years
Payload[8]	$\beta_F = 0.5921$ $\theta_F = 30150$ years	$\beta_{MF} = 0.5561$ $\theta_{MF} = 1731$ years	$\beta_{mMF} = 0.5599$ $\theta_{mMF} = 813.3$ years

Partial validation of the IMLN model. Now that a subset of the SPN model has been used to create inputs for the IMLN model, it is possible to use the complete SPN model and its results to partially validate the IMLN simulation results.

A Monte Carlo simulation of the SPN model of the case study space-based network was run (5 million runs, as justified in Castet and Saleh (2012)), and the results are provided in Table 6.4. For example, according to the SPN model, after 5 years on-orbit, the probability that the space-based network has completely failed (P_F) is 6.0 percentage points, that it is in a major degradation state (P_M) is 7.3 percentage points, and that it is in a minor degradation state (P_m) is 7.7 percentage points.

The IMLN model using the Weibull distributions given in Table 6.3 and assuming a perfect link between spacecraft was run 100,000 times (see section 6.4 for more details about the number of runs). The results are also presented in Table 6.4. Similarly, according to the IMLN model, after 5 years on-orbit, the probability that the space-based

[8] In this particular example, the "payload" vertex consists of the payload instrument, as well as data handling components. These components will be analyzed separately later in the dissertation.

network has completely failed (P_F) is 6.1 percentage points, that it is in a major degradation state (P_M) is 7.4 percentage points, and that it is in a minor degradation state (P_m) is 7.7 percentage points.

Table 6.4 gives the full results for all degradation and failure states at four times in the lifetime of a spacecraft (1, 5, 10 and 15 years) for both models. Table 6.4 also provides the absolute difference (in percentage points) between the results of the two models. It can be seen that these results are similar, as the maximum error is 0.29 percentage point and the average error over all the results is 0.1 percentage point, a significantly small difference. A detailed analysis of the results is presented in Chapter 7.

Table 6.4. Results from the SPN and IMLN simulations of the case study and comparison (in percentage points)

Time	**SPN**			**IMLN**			**Absolute difference**		
on-orbit	P_F	P_M	P_m	P_F	P_M	P_m	F	M	m
1 year	2.78	3.70	4.36	2.53	3.50	4.34	0.24	0.19	0.02
5 years	5.96	7.32	7.66	6.09	7.38	7.69	0.12	0.07	0.03
10 years	8.78	9.89	9.71	8.79	9.88	9.74	0.01	0.04	0.03
15 years	11.22	11.78	11.04	10.93	11.66	11.00	0.29	0.13	0.04

The small, but existing differences can be explained from two sources:

- The IMLN model was simulated with 100,000 runs. Increasing the number of runs will increase the precision of the results, but at the cost of computing time. This source of error is investigated in the following section. Also the Monte Carlo simulation can introduce some variability in the SPN results, even if 5 million runs were chosen to reduce it as much as possible with a reasonable simulation time.

- The Weibull laws derived in Table 6.3 are close approximations of subsets of the SPN model, hence the fitting errors mentioned above are introduced in the IMLN simulation.

6.3. Comparison with Limited Analytical Solutions

In the case of the simple space-based network from the case study, a closed-form solution for the probabilities of being in a total failure state, a major degradation state or a minor degradation state can be derived analytically. Note that the existence of a closed-form solution is not generalizable to all space-based networks, justifying the need of the general interdependent multi-layer approach presented in this dissertation.

Assuming that the link is perfectly reliable, they can be expressed as:

$$P_F = 1 - \left(1 - P^{F}_{\text{supp. sub.}}\right)\left(1 - P^{F}_{\text{payload}}\right)\left\{1 - \left(1 - \left(1 - P^{F}_{\text{TTC}}\right)\left(1 - P^{F}_{\text{supp. sub.}}\right)\right)P^{F}_{\text{TTC}}\right\} \tag{6.1}$$

$$P_{MF} = 1 - \left(1 - P^{MF}_{\text{supp. sub.}}\right)\left(1 - P^{MF}_{\text{payload}}\right)\left\{1 - \left(1 - \left(1 - P^{MF}_{\text{TTC}}\right)\left(1 - P^{F}_{\text{supp. sub.}}\right)\right)P^{MF}_{\text{TTC}}\right\} \tag{6.2}$$

$$P_{mMF} = 1 - \left(1 - P^{mMF}_{\text{supp. sub.}}\right)\left(1 - P^{mMF}_{\text{payload}}\right)\left\{1 - \left(1 - \left(1 - P^{mMF}_{\text{TTC}}\right)\left(1 - P^{F}_{\text{supp. sub.}}\right)\right)P^{mMF}_{\text{TTC}}\right\} \tag{6.3}$$

Plugging in the Weibull models shown in Table 6.3, it is then possible to investigate the precision of the IMLN results from 100,000 runs. The numerical results from the equations are presented in Table 6.5. Note that these values differ from the SPN results presented in Table 6.4 as the $P_{\text{supp. sub.}}$, P_{payload} and P_{TTC} are modeled using the same Weibull distributions than the IMLN model. As a side node, the SPN results can be found by plugging instead the SPN simulated values.

Table 6.5. Results from the analytical and IMLN models of the case study and comparison (in percentage points)

Time	**Analytical solution**			**IMLN**			**Absolute difference**		
on-orbit	P_F	P_M	P_m	P_F	P_M	P_m	F	M	m
1 year	2.51	3.55	4.25	2.53	3.50	4.34	0.02	0.05	0.09
5 years	6.08	7.39	7.76	6.09	7.38	7.69	0.01	0.01	0.07
10 years	8.86	9.93	9.72	8.79	9.88	9.74	0.06	0.04	0.02
15 years	11.01	11.69	10.93	10.93	11.66	11.00	0.08	0.03	0.07

The IMLN simulation results are in good agreement with the analytical results: the maximum error for all degradation and failure states and for all time is 0.1 percentage point and the average error is 0.05 percentage point.

It results that the comparison of the IMLN results with the SPN and analytical results yields very good agreement, partially validating the IMLN approach and establishing trust for the IMLN outputs.

6.4. IMLN Model Precision

The IMLN results presented in Table 6.5 were obtained by using a Monte Carlo simulation with 100,000 runs. However, due to the variability associated with Monte Carlo simulations, these results are not fully representative of the precision of the IMLN model. This precision was investigated on the case study by running 10 times the same Monte Carlo simulation with 100,000 runs. Then confidence intervals can be built to characterize the variability associated with the IMLN simulation. For each on-orbit time (1, 5, 10 and 15 years) and for each degradation or failure state, a sample of 10 probabilities *P* is gathered: the sample mean is defined as $\overline{P}$ and the sample standard deviation is *s*. Then, using the Student's *t*-distribution with 9 degrees of freedom, the two-sided 95% confidence interval is expressed as:

$$\left[\overline{P} - \frac{s}{\sqrt{10}} t_{0.025,9} \quad , \quad \overline{P} + \frac{s}{\sqrt{10}} t_{0.025,9}\right] \tag{6.4}$$

where $t_{0.025,9} = 2.262$ as $P\left(-t_{0.025,9} \leq T \leq t_{0.025,9}\right) = 0.95$ for 9 degrees of freedom

The sample averages and the confidence interval spreads are provided in Table 6.6. The spread of the confidence interval is relatively small: the maximum spread is 0.15 percentage point and the average spread is 0.10 percentage point, with most of the analytical results falling between the confidence interval bounds.

Table 6.6. Confidence intervals for 100,000 runs results

Time	**Sample average**			**Confidence interval spread**		
on-orbit	P_F	P_M	P_m	*F*	*M*	*m*
1 year	2.48	3.54	4.21	0.08	0.10	0.08
5 years	6.03	7.40	7.76	0.11	0.13	0.07
10 years	8.79	9.91	9.77	0.11	0.13	0.08
15 years	10.94	11.68	10.99	0.13	0.15	0.07

Improving the accuracy of the results can be obtained by increasing the number of runs in the simulation, hence increasing the computational burden. This is discussed in more details in the following section.

6.5. Model Scalability

6.5.1. Confidence Interval and Simulation Time

For the case study IMLN (2-spacecraft network represented with 5 nodes), four series of Monte Carlo simulations were conducted to determine the accuracy improvement of the IMLN model results with the increase in the number of runs by tracking the spread of the confidence intervals, as well as the impact of this increase on the computational time. Each series of Monte Carlo consists in running 10 times the total failure simulation (no degradation states considered) in order to build confidence interval with that sample. The number of runs for each series is increasing from 10,000 runs for the first series to 100,000 runs for the second series, 500,000 runs for the third series and 1,000,000 runs for the fourth series. The resulting variation in confidence interval spread (average and maximum over four on-orbit dates: 1, 5, 10 and 15 years) is presented in Figure 6.8. Also shown on the secondary *y*-axis in Figure 6.8 is the time required for propagating the failures across the IMLN depending on the number of runs. The configuration used in this thesis consists of the MATLAB software running on an Intel Core 2 Duo 2.66 GHz processor with 2 GB of RAM.

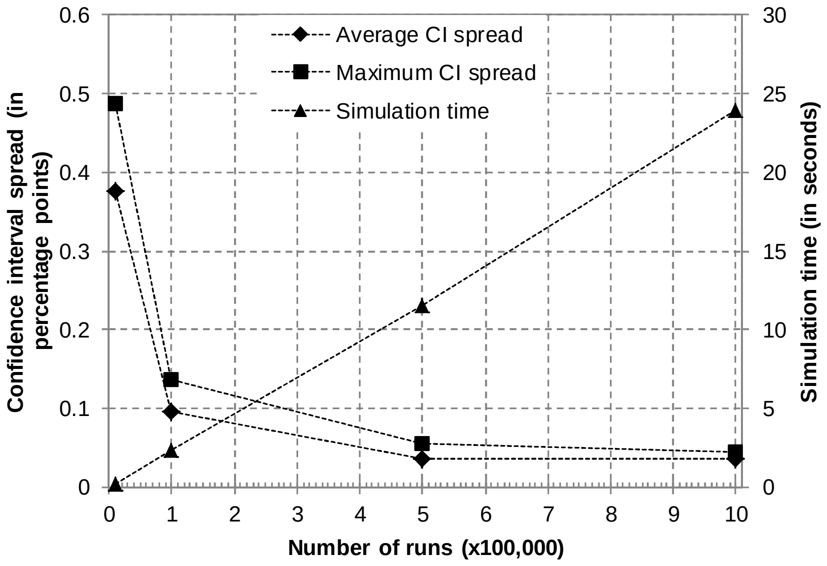


Figure 6.8. Confidence interval spread and simulation time variations with the number of runs for the case study IMLN

Figure 6.8 shows an exponential decrease in the spread of the confidence interval (both for the average and the maximum values) by increasing the number of runs, trend that can be translated in an increase in accuracy for the IMLN model. For example, the average confidence interval spread is 0.4 percentage point for 10,000 runs and 0.04 percentage point for 500,000 runs. Figure 6.8 suggests that choosing a too high number of runs will not translate in a significantly higher accuracy (plateau effect after 500,000 runs in this particular example). This is all the more significant as Figure 6.8 shows that the simulation time linearly increases with the number of runs, from 0.2 second for 10,000 runs to 24 seconds for 1 million runs. Consequently, a medium number of runs associated with most of the precision improvement and an acceptable computational time can be selected as a trade-off. The simulation times shown here remain low, but the IMLN under consideration consists of a small number of nodes. The next paragraph investigates how the simulation time increases with the complexity of the network.

6.5.2. Network Size and Simulation Time

Four different space-based network architectures are considered here, each with four layers: two layers of functional redundancy (layers 1 and 2), one layer of supporting subsystems (layer 3) and one layer for the payload (layer 4). The first network consists of 3 networked spacecraft (3-IMLN), the second of 4 spacecraft (4-IMLN), the third of 5 spacecraft (5-IMLN) and the fourth of 10 spacecraft (10-IMLN). These IMLNs are not intended to be realistic space architectures: they were chosen to increase the complexity of the failure propagation and observe its impact on the simulation time. The IMLN models (graph representation, adjacency matrices, interlayer matrix and mapping function) of these four architectures are shown in the Appendix of this chapter, instead of the main body for readability purposes. The number of vertices increases from 8 in the 3-IMLN, to 11 in the 4-IMLN, 14 in the 5-IMLN and 29 in the 10-IMLN. The simulation times necessary to propagate total failures (these are not multi-state failure simulations) across the networks during Monte Carlo simulations with 100,000 runs are given in Table 6.7. Even in the most complex IMLN (10 spacecraft), the simulation time for 100,000 runs remain low with a value of about 13 seconds. A shorter simulation time or the possibility of considering a higher number of runs could be obtained by using a more efficient programming language or a more powerful computer configuration.

Table 6.7. Simulation time variation with number of vertices

Network type	Number of vertices	Simulation time
		seconds
3-IMLN	8	4.8
4-IMLN	11	5.8
5-IMLN	14	6.9
10-IMLN	29	12.8

In addition to the results for the architectures considered above, the failure propagation took about 2.3 seconds for 100,000 runs in the case of the 2-IMLN case study as shown in Figure 6.8. The previous calculations were obtained for total failure simulations. In the case of a full multi-state analysis (here including the *MF* and *mMF* degraded states), the degradation and failure propagation takes about 5.4 seconds, short of three times the time necessary for the total failure simulation. As a consequence, the computational burden remains low even for the multi-state simulation.

However, an additional computational time exists for the generation of T_F, T_{MF} and T_{mMF} for the vertices (and edges). In the case of the total failure simulation, only T_F is required to be generated from Weibull distributions, and only a fraction of second (0.2 second) is added to the 2.3 seconds required for the failure propagation across the network in the 2-IMLN case. This is not the case for the multi-state approach, as T_F, T_{MF} and T_{mMF} need to be generated concurrently using the algorithm presented in section 5.2.1. In the case of the 100,000-run Monte Carlo simulation for the case study IMLN, 585 seconds are necessary to generate T_F, T_{MF} and T_{mMF} for the vertices (the link between spacecraft is assumed to be perfectly reliable). This generation is significantly time consuming for vertices with Weibull distributions for T_F, T_{MF} and T_{mMF} that do not share the same shape parameter and thus require the use of a potentially slow root-solving algorithm[9]. Increasing the number of runs to high levels with a high number of such vertices in the network might lead to a significantly high simulation time that might become prohibitive. To balance this problem, it was shown in Figure 6.8 that considering a too high number

[9] The vertices with Weibull distributions sharing the same shape parameters induce a low computational burden as T_F, T_{MF} and T_{mMF} can be generated using straightforward equations presented in 5.2.1.

of runs might not significantly improve the accuracy of the results. To help improve the time necessary for the generation of T_F, T_{MF} and T_{mMF}, several paths can be considered: using a more efficient programming language, using a more efficient root-finding algorithm, approximating the failure behavior models with Weibull with the same shape parameters as much as possible or using a more powerful hardware configuration. Also, one might consider creating in parallel a library of times to degraded states for pre-determined node and link anomaly and failure behaviors, so that the changes in the architecture and reruns of the simulations can be done within the order of times presented in Table 6.7 (i.e., uncoupling the generation of T_F, T_{MF} and T_{mMF} and the failure propagation algorithm).

6.5.3. Network Size and Scalability of Adjacency and Interlayer Matrices

Another consequence of scaling up the network size lies with the increasing size of the adjacency and interlayer matrices. This increase can pose significant issues for creating and stocking matrices as well as performing efficient matrix operations. However, it is shown below that most interlayer matrices can be considered as sparse matrices, as well as some adjacency matrices. A sparse matrix is a matrix mainly populated with zeros, and it is extremely useful for lowering the computational burden associated with large matrices, as only the non-zero elements need to be considered.

The maximum number of elements in an adjacency matrix grows as the square of the number of spacecraft n_S in the network: for example, in the case of the IMLN with $n_S = 4$ spacecraft (4-IMLN) presented in the appendix, the adjacency matrix A_1 has

$n_{A_1} = 4 \times 4 = 16$ elements (maximum possible size), while the A_2 matrix has $n_{A_2} = 2 \times 2 = 4$ elements. The actual size of the adjacency matrix depends on the number of nodes n_l in the associated layer l (bounded by the number of spacecraft), and the number of non-zero elements in it depends on the number of edges in that layer ($n_{E_l} = |E_l|$ with E_l defined in Eq. (4.1)). For undirected edges with no self-edges, the maximum number of edges is given by $n_{E_l,\max} = n_l(n_l - 1)/2$ (Newman, 2010). As a consequence, the associated adjacency matrix is symmetric, its diagonal only consists of zero, and there are $n_l(n_l - 1)/2$ remaining elements to fully define A_l. In the case of a low connectance (or density) of the layer (i.e., a low number of edges), A_l can be considered as a sparse matrix. For example in the case of the 10-IMLN presented in the appendix, the adjacency matrix A_1 has 100 elements, but only 5 elements are necessary to fully characterized it.

The number of elements n_C in the interlayer matrix C scales with the square of the number of vertices n in the network. For example, in the case of the 5-IMLN presented in the appendix, $n_C = 14 \times 14 = 196$ elements. This number can grow very quickly and determining, entering and stocking the interlayer matrix elements can pose significant practical and computational issues. However, the number of non-zero elements (n_C^*) in the interlayer matrix is generally relatively low. Table 6.8 shows for each of the architectures considered in the appendix the total number of elements in C, the total number of non-zero elements in C and the ratio of these two numbers. For example, in the case of the 10-spacecraft network, the interlayer matrix has 841 elements, but only 55 of them are non-zero: in other words, 7% of the elements in that specific matrix are non-zero. For all four of the architectures, this ratio stays below 20 %. As a consequence, the interlayer matrix *C* can be considered as a sparse matrix to improve the computational treatment of this matrix.

Also, as mentioned in section 4.5.1, a particular scheme of numbering the vertices in the network can help determining more easily elements of the interlayer matrix: if the vertices belonging to a same spacecraft are numbered in sequential order, the interlayer matrix can be written with a block diagonal form. It can be seen in the appendix that the interlayer matrix for the 10-IMLN architecture is simply written, despite its 29×29 size. Note that the seven 3×3 non-zero blocks are similar, as the two 2×2 blocks. To summarize, the fact that the interlayer matrix can be considered as a sparse matrix, and that an informed numbering scheme can significantly reduce the issues of scaling up the network size.

Table 6.8. The interlayer matrix as a sparse matrix

Network type	Number of vertices	Total number of elements in the C matrix (n_C)	Number of non-zero elements in the C matrix (n_C^*)	Ratio n_C^* / n_C
3-IMLN	8	64	13	20%
4-IMLN	11	121	19	16%
5-IMLN	14	196	25	13%
10-IMLN	29	841	55	7%

6.6. Summary

This chapter explored technical considerations related to the IMLN representation and simulation tool: (partial) validation of the IMLN outputs, relationship between precision and number of runs in the Monte Carlo simulation, and its impact on scalability through the simulation time and matrix size. It was demonstrated that the IMLN concept introduced in this thesis is able to handle properly the exploration of the design space of space-based networks. Indeed, the results from the IMLN simulation were shown to be in good agreement with results derived from an equivalent stochastic Petri net model, as well as analytical solutions, for a reasonable number of runs and simulation time. It was also shown that the precision of the results, through the proxy of the spread of confidence interval, is increasing (smaller confidence intervals) with the number of runs in the Monte Carlo simulation. However, the incremental benefits in precision are also decreasing with an increase in the number of runs, while the simulation time increases. A resulting compromise between precision and simulation time is necessary, but it was demonstrated that the failure propagation algorithm is sufficiently efficient so that the simulation time remains acceptable. Finally, through an informed way of numbering nodes in the network and the fact that most matrices considered are sparse, it was shown that the determination of the elements of the adjacency matrices and the interlayer matrix could be significantly simplified, allowing for the consideration of complex space-based networks.

6.A. Appendix

6.A.1. Stochastic Petri Net of the Case Study Space-Based Network

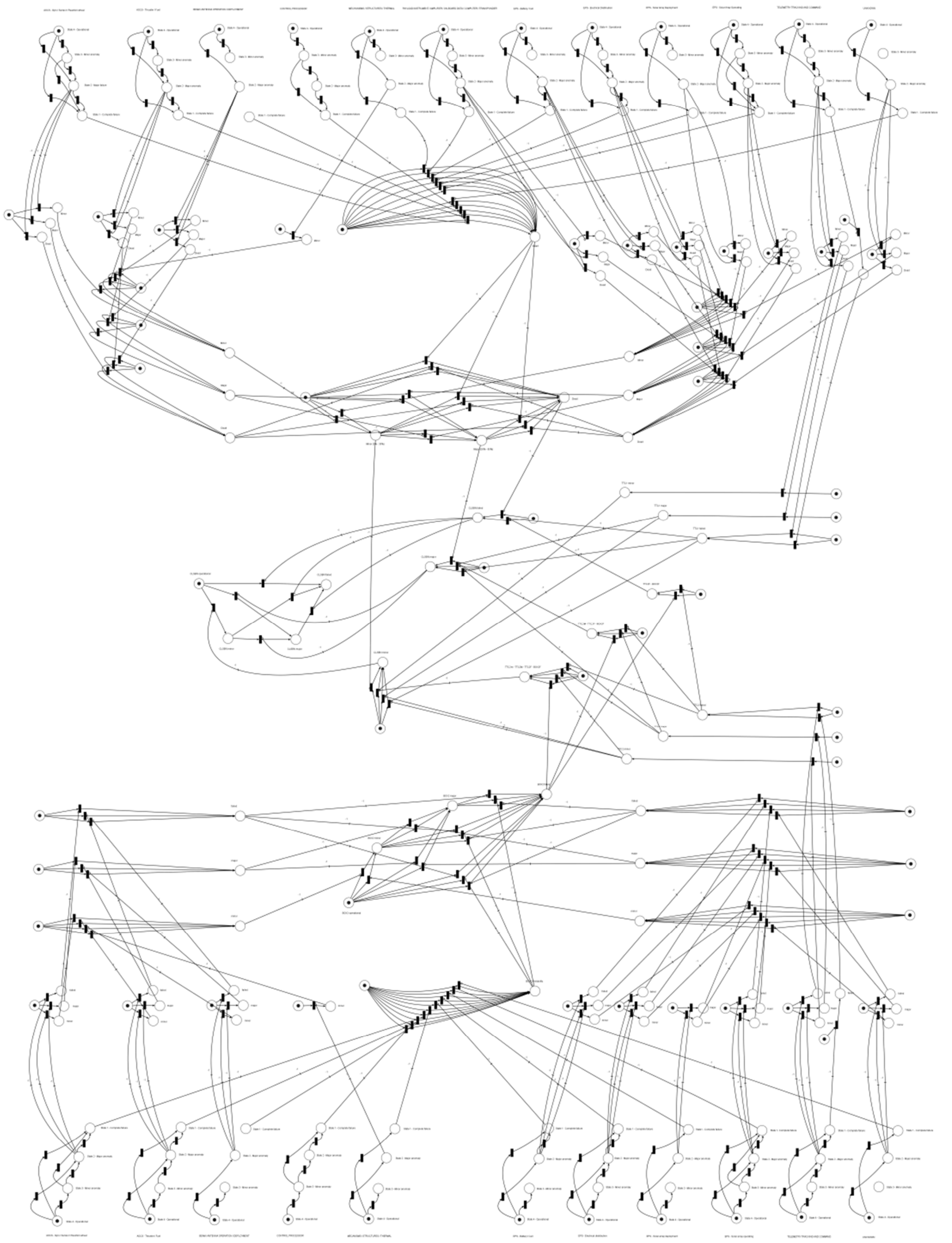


Figure 6.A. SPN model for the case study space-based network

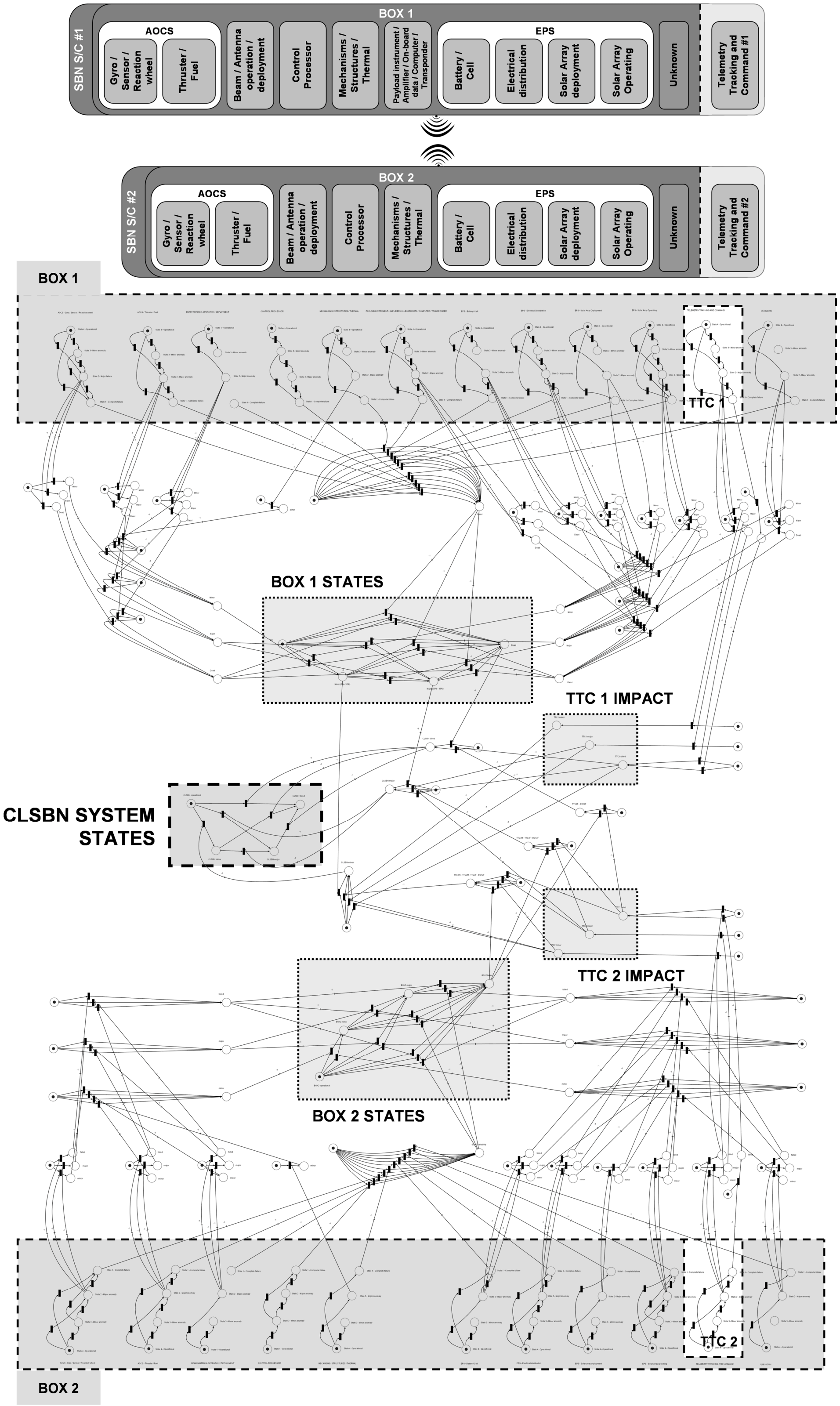


Figure 6.B. Construction clarification of the space-based network SPN model

6.A.2. IMLN Models of the Four Architectures in 6.5.3 3-IMLN architecture

3-IMLN architecture

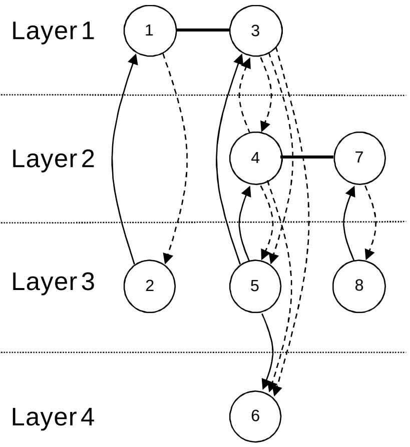


Figure 6.C. IMLN representation for the selected 3-IMLN architecture

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_3 = 0_{3\times3}$ and $A_4 = 0_{1\times1}$

- Interlayer matrix: $C = \begin{bmatrix} \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} & 0_{2\times4} & 0_{2\times2} \\ 0_{4\times2} & \begin{matrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 1 & 0 \end{matrix} & 0_{4\times2} \\ 0_{2\times2} & 0_{2\times4} & \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} \end{bmatrix}$

- (Inverse) mapping function[10]: $f^{-1} = \begin{bmatrix} 1 & 3 & NaN \\ 4 & 7 & NaN \\ 2 & 5 & 8 \\ 6 & NaN & NaN \end{bmatrix}$

[10] Using a matrix representation. For example, $f^{-1}(2,1) = 4$

4-IMLN architecture

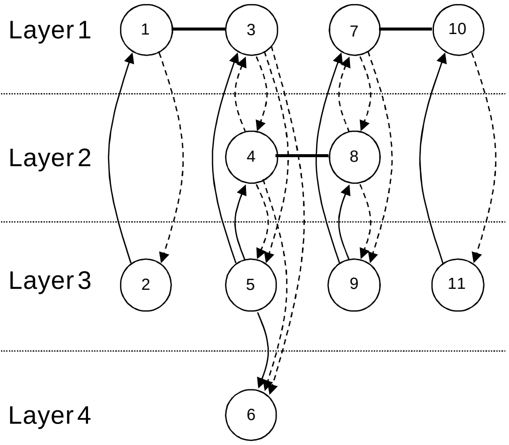


Figure 6.D. IMLN representation for the selected 4-IMLN architecture

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_3 = 0_{4\times4}$ and $A_4 = 0_{1\times1}$

- Interlayer matrix: $C = \begin{bmatrix} \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} & 0_{2\times4} & 0_{2\times3} & 0_{2\times2} \\ 0_{4\times2} & \begin{matrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 1 & 0 \end{matrix} & 0_{3\times3} & 0_{4\times2} \\ 0_{3\times2} & 0_{4\times4} & \begin{matrix} 0 & 2 & 1 \\ 2 & 0 & 1 \\ 2 & 2 & 0 \end{matrix} & 0_{3\times2} \\ 0_{2\times2} & 0_{2\times4} & 0_{2\times3} & \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} \end{bmatrix}$

- (Inverse) mapping function: $f^{-1} = \begin{bmatrix} 1 & 3 & 7 & 10 \\ 4 & 8 & NaN & NaN \\ 2 & 5 & 9 & 11 \\ 6 & NaN & NaN & NaN \end{bmatrix}$

5-IMLN architecture

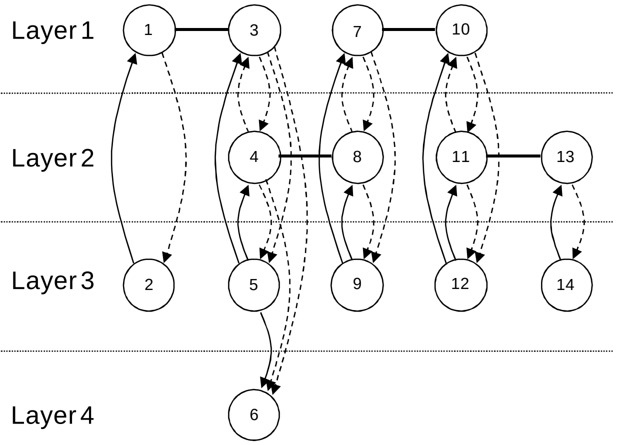


Figure 6.E. IMLN representation for the selected 5-IMLN architecture

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$, $A_3 = 0_{5\times5}, A_4 = 0_{1\times1}$

- Interlayer matrix: $C = \begin{bmatrix} \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} & 0_{2\times4} & 0_{2\times3} & 0_{2\times3} & 0_{2\times2} \\ 0_{4\times2} & \begin{matrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 1 & 0 \end{matrix} & 0_{4\times3} & 0_{4\times3} & 0_{4\times2} \\ 0_{3\times2} & 0_{3\times4} & \begin{matrix} 0 & 2 & 1 \\ 2 & 0 & 1 \\ 2 & 2 & 0 \end{matrix} & 0_{3\times3} & 0_{3\times2} \\ 0_{3\times2} & 0_{3\times4} & 0_{3\times3} & \begin{matrix} 0 & 2 & 1 \\ 2 & 0 & 1 \\ 2 & 2 & 0 \end{matrix} & 0_{3\times2} \\ 0_{2\times2} & 0_{2\times4} & 0_{2\times3} & 0_{2\times3} & \begin{matrix} 0 & 1 \\ 2 & 0 \end{matrix} \end{bmatrix}$

- (Inverse) mapping function: $f^{-1} = \begin{bmatrix} 1 & 3 & 7 & 10 & NaN \\ 4 & 8 & 11 & 13 & NaN \\ 2 & 5 & 9 & 12 & 14 \\ 6 & NaN & NaN & NaN & NaN \end{bmatrix}$

10-IMLN architecture

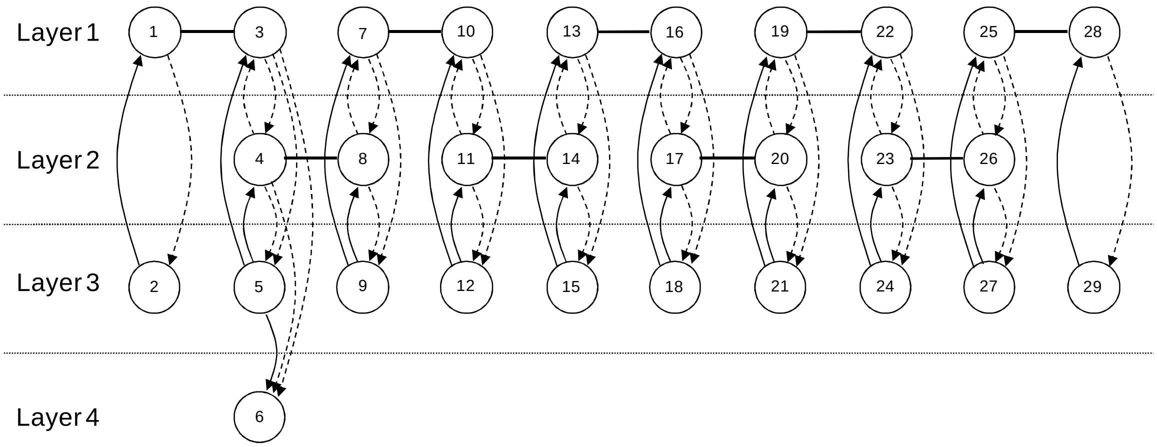


Figure 6.F. IMLN representation for the selected 10-IMLN architecture

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$,

$$A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \; A_3 = 0_{10\times 10} \text{ and } A_4 = 0_{1\times 1}$$

- Interlayer matrix:

$$C=\begin{bmatrix}
\begin{matrix}0&1\\2&0\end{matrix} & 0_{2\times4} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times2}\\
0_{4\times2} & \begin{matrix}0&2&1&0\\2&0&1&0\\2&2&0&0\\2&2&1&0\end{matrix} & 0_{4\times3} & 0_{4\times3} & 0_{4\times3} & 0_{4\times3} & 0_{4\times3} & 0_{4\times3} & 0_{4\times3} & 0_{4\times2}\\
0_{3\times2} & 0_{3\times4} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times2}\\
0_{3\times2} & 0_{3\times4} & 0_{3\times3} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times2}\\
0_{3\times2} & 0_{3\times4} & 0_{3\times3} & 0_{3\times3} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times2}\\
0_{3\times2} & 0_{3\times4} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times2}\\
0_{3\times2} & 0_{3\times4} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times3} & 0_{3\times3} & 0_{3\times2}\\
0_{3\times2} & 0_{3\times4} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times3} & 0_{3\times2}\\
0_{3\times2} & 0_{3\times4} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & 0_{3\times3} & \begin{matrix}0&2&1\\2&0&1\\2&2&0\end{matrix} & 0_{3\times2}\\
0_{3\times2} & 0_{2\times4} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & 0_{2\times3} & \begin{matrix}0&1\\2&0\end{matrix}
\end{bmatrix}$$

- (Inverse) mapping function:

$$f^{-1}=\begin{bmatrix}
1 & 3 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28\\
4 & 8 & 11 & 14 & 17 & 20 & 23 & 26 & NaN & NaN\\
2 & 5 & 9 & 12 & 15 & 18 & 21 & 24 & 27 & 29\\
6 & NaN & NaN & NaN & NaN & NaN & NaN & NaN & NaN & NaN
\end{bmatrix}$$

CHAPTER 7

RESULTS, ANALYSES AND INSIGHTS ON DESIGN AND ARCHITECTURAL CHOICES FOR SPACE-BASED NETWORKS

7.1. Introduction

Chapter 4 introduced a new concept to enable the modeling of space-based networks and Chapter 5 described a framework to assess the survivability of such architectures. Chapter 6 investigated the ability of this framework to properly capture subsystem anomaly and failure propagation across the network (a validation process) and its scalability. The objectives of this chapter are twofold: the first is to provide examples of application of the survivability framework and tools introduced in this dissertation through the evaluation of specific space-based networks as a proof of concept; the second is related to the purpose behind the introduction of this framework, that is, exploring the survivability features of a new concept for space systems, namely space-based networks, and their implications for conceptual design. Through the use of the survivability framework and the interdependent multi-layer network approach developed in this thesis, what insights can be gathered for the design and the architecture selection of space systems for which survivability is a metric of interest?

Before providing more details about the two objectives of this chapter, a caveat is in order to clarify the use of the tool introduced in this thesis, as well as the interpretation of the results provided in this chapter. This thesis does not advocate for or against the development of space-based networks by the space industry. This thesis introduces and develops a framework and tools to explore the survivability of space-based networks, in the case that space-based networks are under consideration by the designer due to particular drivers. This thesis enables the analysis of survivability implications of networks for design, and helps inform the design and architectural choices of space systems. The survivability tools and results presented here are not the only elements that will determine the design decision of the retained architecture: other considerations, such as cost, complexity, technology maturity, delivery schedule, customer requirements or shareholder risk tolerance, will also influence the designer's decision. In summary, this thesis provides the means to explore the survivability aspect and implications of space-based networks, if networks are one option amongst others on the design table, as part of a decision support process.

The first objective is tackled in section 7.2 where two particular cases of functional redundancy are explored, leveraging the subsystem probabilities of experiencing anomalies and failures derived earlier in this dissertation from a 1584-Earth orbiting spacecraft sample. The first case of functional redundancy is devoted to the Telemetry, Tracking and Command (TTC) subsystem: the role of the TTC is critical in the proper operation of a spacecraft as it links the spacecraft to the ground station and operators, enabling the proper tracking of the spacecraft, the monitoring of its subsystems and the upload of commands from the operators. The TTC function is a good candidate for fractionation, as the communication link with the ground can be distributed among neighboring spacecraft: through the network, the spacecraft could either pool their computing and communication capabilities or step up to support a networked spacecraft that lost its ability to communicate with the control center.

The second case builds on the TTC and adds two more subsystems for consideration of functional redundancy: the Control Processor subsystem (the computer "brain" of the spacecraft) and the Data Handling subsystem (the "hard-drive" of the spacecraft that stores and handles data). This aggregation of subsystems is termed the "Command and Data Handling subsystem" (C&DH) and Berget summarizes its function as the subsystem that "receives, validates, decodes, and distributes commands to other spacecraft systems and gathers, processes, and formats spacecraft housekeeping and mission data for downlink" (Berget, 1999). Consequently, the C&DH subsystem appears also as a good candidate for networking and sharing on-orbit resources among a constellation of co-located spacecraft. The TTC and C&DH examples are explored by considering specific types of networks, with two or three spacecraft, and serve as a proof of concept of the survivability evaluation process designed in this dissertation.

The second objective extends the survivability analysis of the TTC and C&DH in a more general direction in section 7.3, by considering a general non-descriptive networkable subsystem or technology and the parameterization of its anomaly and failure behavior to explore broader and more general survivability characteristics of space-based networks and insights gleaned for design and architectural choices of future space systems. Section 7.3 also demonstrates advanced capabilities of the modeling setup and simulation and introduces useful tools to the conceptual design analysis.

Before pursuing the stated objectives, the survivability framework and its application in four steps introduced in Chapter 4 is briefly recalled below:

- Step 1: definition of the classes of threats or types of disruptions for the survivability analysis;
- Step 2: functional characterization of the architecture of the system under consideration;
- Step 3: transformation of the functional characterization into an analytical or computational model of the system to assess its survivability with respect to the classes of threats or types of disruptions of interest;
- Step 4: assessment of the system's performance degradation—its survivability assessment—following disruptions, using the system model previously developed and the characterization of the classes of threats or types of disruptions of interest.

7.2. C&DH Survivability Analysis

7.2.1. Telemetry, Tracking and Command Functional Redundancy

The first space-based network considered in this first subsection is simple and is the case study model used in previous chapters (for example shown in Figure 6.3), which consists of a network of two spacecraft that can share their TTC resource. As seen in previous chapters, the TTC subsystem is a major driver of spacecraft unreliability. **The wireless connectivity in the SBN enables a type of redundancy in the TTC between the two spacecraft in the network**. This space-based network has already been discussed at length in previous chapters, but it was used in a specific fashion to illustrate the definition and construction of the IMLN modeling, its (partial) validation with stochastic Petri nets and analytical solutions, the IMLN modeling precision and its scalability. In this subsection, the focus is on showing the complete survivability analysis process, the results themselves, and their implications for design and architectural choices.

The four steps in the survivability analysis are presented below.

Step 1. The focus of this section is on endogenous failures, enabling the leverage of the studies conducted in earlier chapters on the anomaly and failure behavior of spacecraft subsystems. The models used to represent these behaviors are presented in step 3. As a consequence, the survivability results are limited to this particular class of threat, and they should not be extrapolated to other classes of on-orbit shocks.

Step 2. A compact representation of the SBN architecture is provided in Figure 7.1.

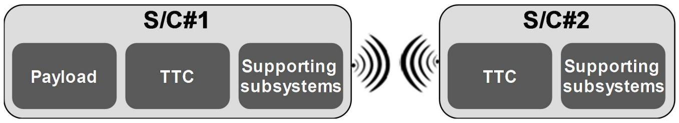


Figure 7.1. Simplified representation of the space-based network architecture

Step 3. The anomaly and failure behavior of the subsystem was derived in Chapter 6 (subsection 6.2.4), but the single Weibull models are recalled below in Table 7.1 for readability purposes.

Table 7.1. Weibull parameters for T_F, T_{MF} and T_{mMF} for the case study space-based network

Functionality	Severity level	Weibull shape parameter β	Weibull scale parameter θ
			years
Telemetry, Tracking, and Command (TTC)	total failure	0.4650	47,770
	severe degradation	0.4680	28,040
	any degradation	0.4402	28,210
Supporting subsystems	total failure	0.5529	918.5
	severe degradation	0.5052	435.0
	any degradation	0.4638	203.6
Payload[11]	total failure	0.5921	30,150
	severe degradation	0.5561	1731
	any degradation	0.5599	813.3

The IMLN representation of this space-base network is shown in Figure 7.2, and the different elements necessary to define the IMLN are listed below:

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_2 = 0_{2\times 2}$ and $A_3 = 0_{1\times 1}$;
- Interlayer matrix: $C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix}$;
- (Inverse) mapping function: $f^{-1} = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & NaN \end{bmatrix}$.

[11] In this particular example, the "payload" vertex consists of the payload instrument, as well as data handling components. These components will be analyzed separately later in the dissertation.

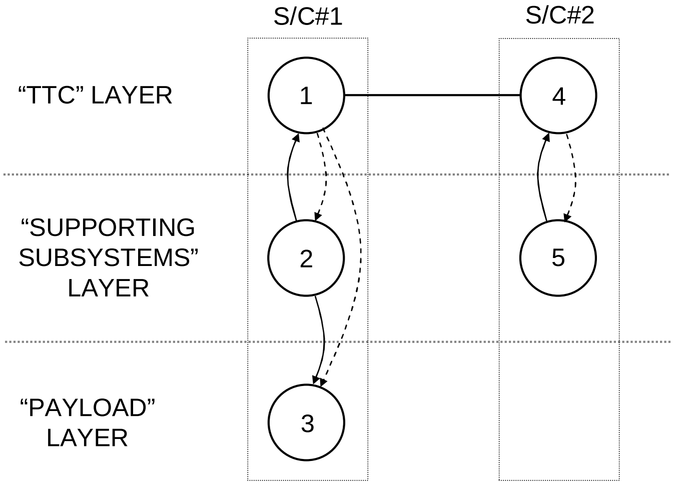


Figure 7.2. IMLN representation of the case study space-based network

Step 4. The survivability analysis here consists of investigating the utility generation capability of the space system, that is, the probability that the payload node (node 3) remains fully operational for full performance, or the probability that this node degrades or fails and results in performance degradation. As a consequence, the metrics of interest are $P\left(T_{U,3}^{F} < t\right)$, $P\left(T_{U,3}^{M} < t\right)$ and $P\left(T_{U,3}^{m} < t\right)$ (or the equivalent combination $P\left(T_{U,3}^{F} < t\right)$, $P\left(T_{U,3}^{MF} < t\right)$ and $P\left(T_{U,3}^{mMF} < t\right)$). Also here, the survivability results are limited to these specific metrics and should not be generalized to any other performance metrics.

After running a 500,000-run simulation, the resulting output is shown in Figure 7.3 for T_F, T_{MF} and T_{mMF}. The probabilities for being in the minor degradation state (T_m) and the major degradation state (T_M) are obtained by linear combinations of the previous results, and are shown along with the probability of total failure in Figure 7.4.

Figure 7.3 and Figure 7.4 share the same formatting. For example, Figure 7.4 reads as follows: after 5 years on orbit, the probability that the space-based network will have ceased to generate utility (failed state) is 6.08%, the probability that it will have a major degradation in performance is 7.38% and a minor degradation 7.69%. As a consequence, the complementary probability that the space system will be fully operational is 78.85% after 5 years on-orbit.

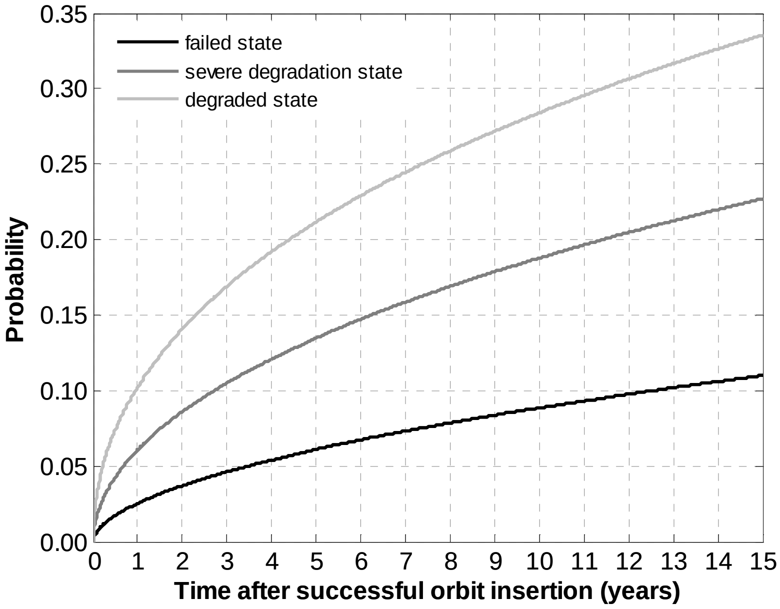


Figure 7.3. Output probabilities for T_F, T_{MF} and T_{mMF} of the payload node with TTC redundancy

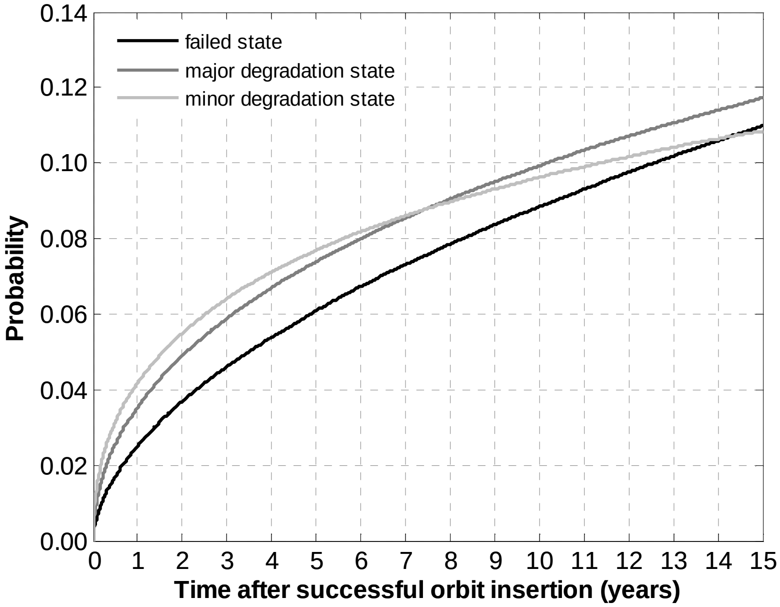


Figure 7.4. Processed probabilities for T_F, T_M and T_m of the payload node with TTC redundancy

The equivalent survivability analysis of the monolith architecture was conducted in the previous chapter and the results are recalled in Figure 7.5.

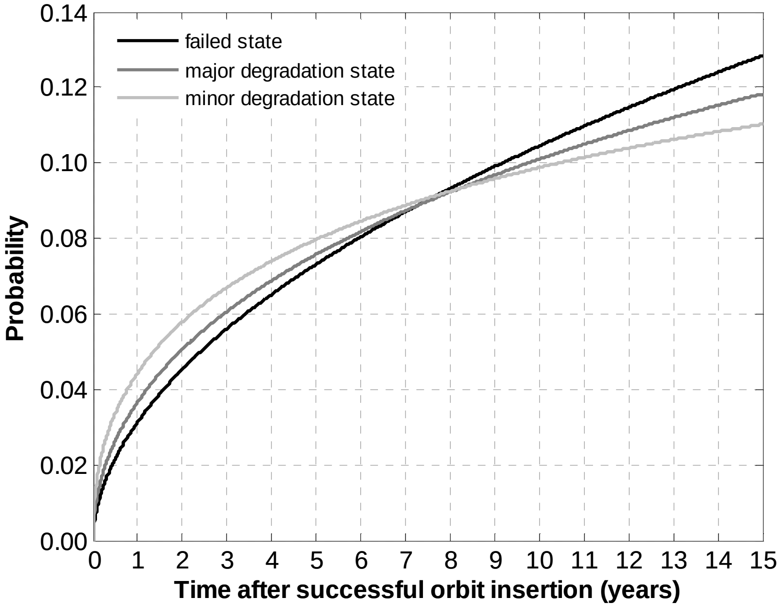


Figure 7.5. Survivability characteristics of the monolith architecture

At the same on-orbit time, the probability of the monolith space system will have ceased to generate utility (failed state) is 7.31%, the probability that it will have a major degradation in performance is 7.57% and a minor degradation 7.97%. As a consequence, the complementary probability that the space system will be fully operational is 77.15% after 5 years on-orbit.

The difference between the probability of residency in each state between the two architectures (P_{SBN} – P_{monolith}) and it can be computed to conduct a comparative survivability analysis. This is shown in Figure 7.6.

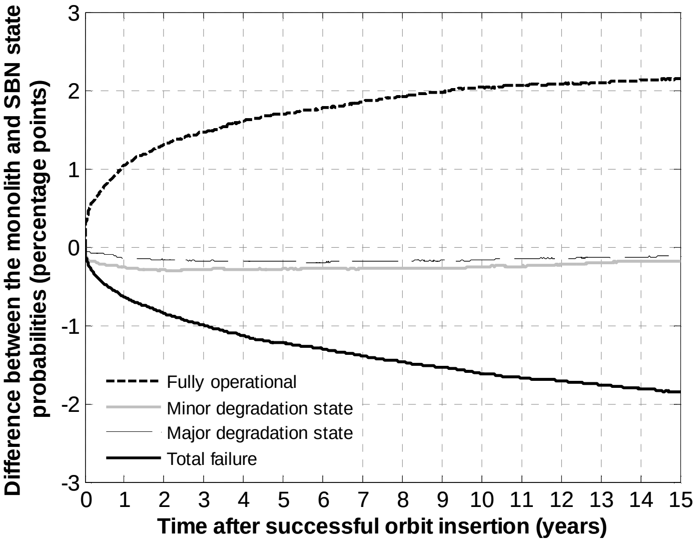


Figure 7.6. Survivability superiority of the space-based network with TTC redundancy over the monolith spacecraft

The important results than can be seen in Figure 7.6 are the following:

- The probability that, **in this specific case (TTC functional redundancy and endogenous failures), the space-based network will be able to generate utility at full capacity is higher at any point in time than the one of the monolith architecture** (the difference between the two is positive on Figure 7.6). After 15 years, the incremental likelihood is about 2 percentage points. A careful cost-benefit analysis should be conducted to assess whether this incremental probability of remaining fully operational is worth the cost of obtaining it. While such studies are beyond the scope of this dissertation, it is worth pointing out in this regard that communication satellites for example can generate in excess of $50 million per year and these increments in lowering the probability of failure can represent the equivalent of several months' worth of revenues. Similarly, it can be of significant importance for defense or intelligence space assets.
- Regarding the distribution of this incremental gain among the reduction in the probability of entering degraded states, the **major improvement was related to a decrease in the probability of total failure of the architecture** by about 1.9 percentage points. This **decrease represents a 14% variation** compared to the probability of total failure of the monolith architecture, which could be regarded as a significant improvement over the current design paradigm.
- A **significant share of the difference occurs early in the life of the space-based network**, consistent with the fact that most spacecraft subsystems suffer from infant mortality. This shows that the networking has a high efficiency as soon as the operational life starts (this notion of efficiency will be revisited later in the dissertation).

As a consequence, **adding a networked spacecraft to the traditional monolithic spacecraft will increase the survivability aspect the space system with respect to endogenous failures in the case of the TTC functional redundancy**.

The previous analysis was conducted with a network of 2 spacecraft (2-IMLN). The following explores the addition of a third spacecraft to the network (3-IMLN) in order to root out the anomaly and failure behavior of the TTC subsystem, as illustrated in Figure 7.7. Note that the S/C #2 and #3 do not communicate with each other. The associated IMLN representation is given in Figure 7.8.

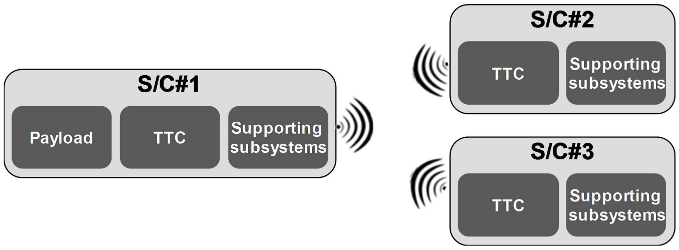


Figure 7.7. Architecture of the space-based network with 3 spacecraft (3-IMLN) for TTC redundancy

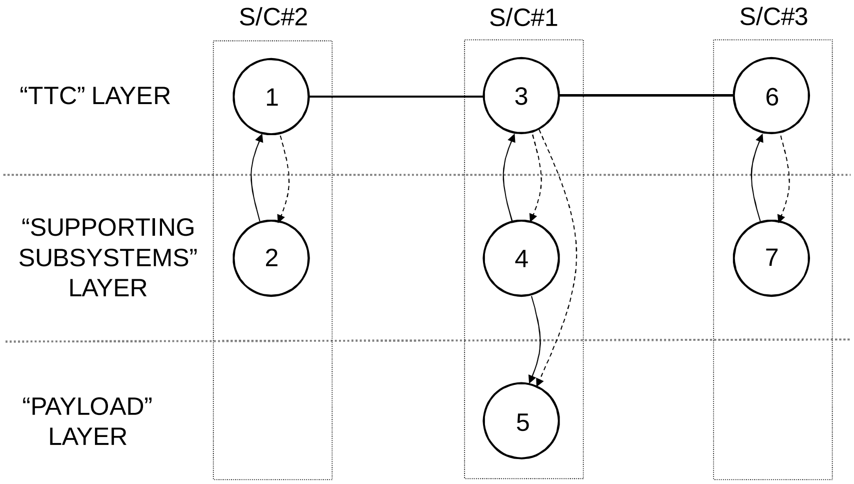


Figure 7.8. IMLN representation of the space-based network with 3 spacecraft for TTC redundancy

The different elements necessary to define the IMLN model are listed below:

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, $A_2 = 0_{3\times3}$ and $A_3 = 0_{1\times1}$;
- Interlayer matrix: $C = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{bmatrix}$;
- (Inverse) mapping function: $f^{-1} = \begin{bmatrix} 1 & 3 & 6 \\ 2 & 4 & 7 \\ 5 & NaN & NaN \end{bmatrix}$.

After running the IMLN simulation, the probabilities P_F, P_{MF} and P_{mMF} are obtained for the survivability features of the 3-IMLN, that is, features related to the performance degradation of the utility generation (Figure 7.9).

The probabilities shown in Figure 7.9 can be processed to obtain P_F, P_M and P_m for the payload node in the network. These probabilities are given in Figure 7.10.

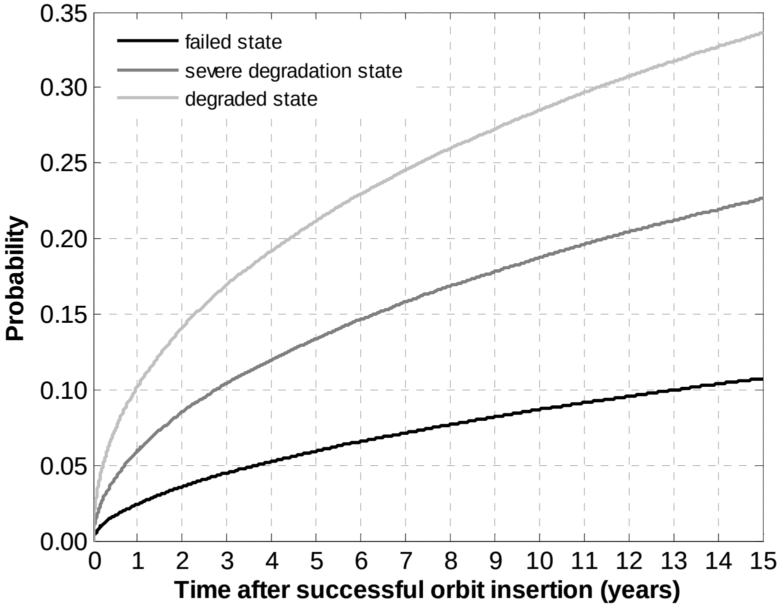


Figure 7.9. Output probabilities for T_F, T_{MF} and T_{mMF} of the payload node with TTC redundancy (3-IMLN case)

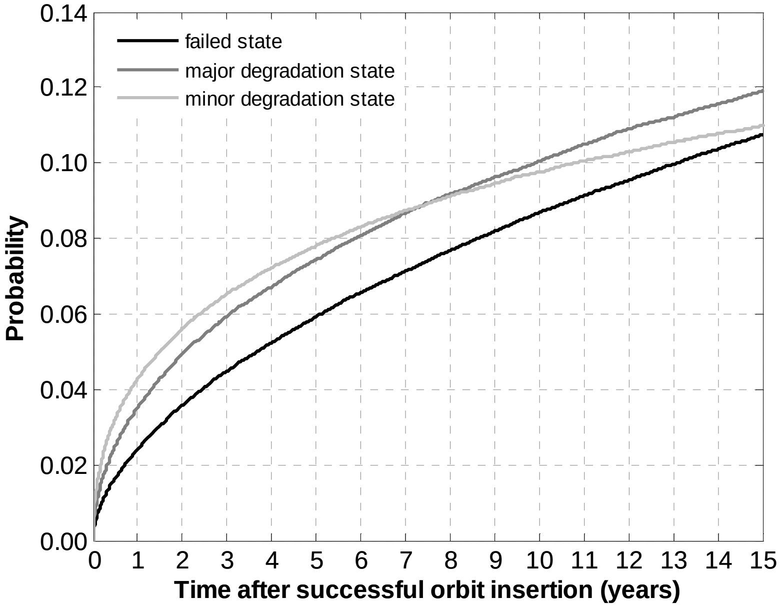


Figure 7.10. Processed probabilities for T_F, T_M and T_m of the payload node with TTC redundancy (3-IMLN case)

After 5 years on-orbit for example, the probability of the 3-IMLN space system will have ceased to generate utility (failed state) is 5.92%, the probability that it will have a major degradation in performance is 7.43% and a minor degradation 7.79%. As a consequence, the complementary probability that the space system will be fully operational is 78.86% after 5 years on-orbit. How does this 3-spacecraft network compare with the 2-spacecraft network? Figure 7.11 presents the probability of a total failure (total loss of utility due to the complete unavailability of the payload node) for the monolith architecture, the 2-IMLN and the 3-IMLN space systems. This probability is chosen as it is the one that presents the greatest difference with the monolith spacecraft.

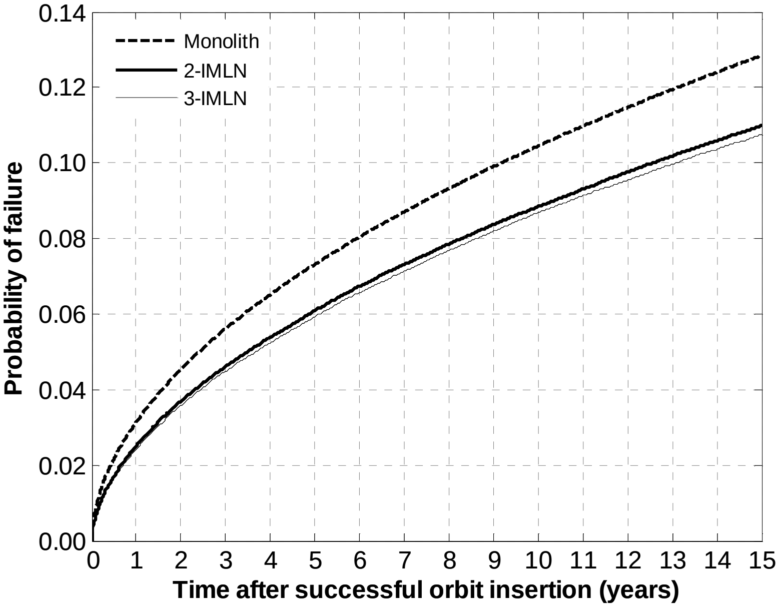


Figure 7.11. Comparison of the probability of unavailability of the payload for the monolith, 2-IMLN and 3-IMLN architectures

The greatest gap between the curves occurs at 15 years: after that duration on-orbit, the monolith spacecraft would have totally failed with 12.84% chance, the 2-IMLN with

10.98% chance and the 3-IMLN with a 10.74% chance. It is clear that the incremental benefit of adding a spacecraft to the 2-IMLN architecture decreases sharply compared to the benefit of networking a monolith spacecraft (2-IMLN): adding one spacecraft to the traditional monolith spacecraft for TTC functional redundancy improves by 1.86 percentage points the probability of payload unavailability, but adding two spacecraft to the monolith for the same purpose improves it only by an additional 0.24 percentage point. This indicates that, if networks are an option considered by the designer, **a three-spacecraft network for mitigating the TTC anomaly and failure behavior might not be worth it compared to the cheaper and slightly less survivable two-spacecraft network**. Note that this comment holds in the case of a perfectly reliable wireless link between spacecraft in the network. The impact of the link failures is treated later in the dissertation.

7.2.2. C&DH Functional Redundancy

Other spacecraft subsystems can be selected for sharing on-orbit resources: for example, the Control Processor (main computer of the spacecraft) can be a good candidate as spacecraft could pool their processing power, or one spacecraft could run processes and command another spacecraft if the Control Processor (CP) subsystem of that spacecraft failed, given that sufficient processing power margin is built into the supporting spacecraft. An additional fractionable subsystem could be the Data Handling subsystem (DH) (responsible for storing and exchanging data): for example, one spacecraft could be envisioned as the “hard drive” of the constellation, on which networked modules upload their data, data then sent to the ground station by the collector spacecraft.

The macro subsystem combining the TTC, the CP and DH is also referred to as the Command and Data Handling (C&DH) subsystem. The associated Weibull models are presented in Table 7.2.

Table 7.2. Weibull parameters for T_F, T_{MF} and T_{mMF} for the space-based network with C&DH redundancy

Functionality	Severity level	Weibull shape parameter β	Weibull scale parameter θ
			years
Control Processor (CP)[12]	total failure	1.251	691.2
	severe degradation	–	–
	any degradation	–	–
Data Handling (DH)	total failure	0.6266	350,000
	severe degradation	0.5603	119,900
	any degradation	0.5571	67,940
Telemetry, Tracking, and Command (TTC)	total failure	0.4650	47,770
	severe degradation	0.4680	28,040
	any degradation	0.4402	28,210
Supporting subsystems	total failure	0.5181	1405
	severe degradation	0.4856	543.5
	any degradation	0.4523	230.2
Payload[13]	total failure	0.5767	49,990
	severe degradation	0.5529	2117
	any degradation	0.5568	981.4

The IMLN model needs to account for these new separate functionalities: there are now five functionalities to represent: the CP, DH, TTC, supporting subsystems and payload. As a consequence, the IMLN representation will consist of five layers, one for each of the aforementioned functionalities. Two spacecraft are part of the network: the first spacecraft has all the subsystems, while the second has all the subsystems but the payload and acts as a functional redundancy for the first spacecraft for the CP, DHS and TTC. The associated IMLN representation is then shown in Figure 7.12.

[12] The CP subsystem only impacts the complete failure of the spacecraft: as such, $T_F = T_{MF} = T_{mMF}$.

[13] In this particular example, the "payload" vertex consists only of the payload instrument. Data handling components are analyzed separately in the DH layer.

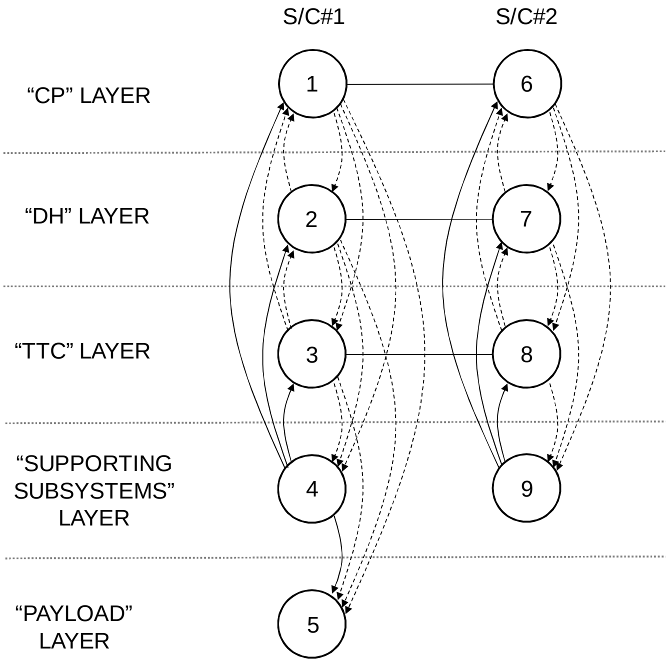


Figure 7.12. IMLN representation of the space-based network with C&DH redundancy

The different elements necessary to define the IMLN model are listed below:

- Adjacency matrices: $A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $A_4 = 0_{2\times 2}$ and $A_5 = 0_{1\times 1}$;

- Interlayer matrix: $C = \begin{bmatrix} 0 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 0 \end{bmatrix}$;

- (Inverse) mapping function: $f^{-1} = \begin{bmatrix} 1 & 6 \\ 2 & 7 \\ 3 & 8 \\ 4 & 9 \\ 5 & NaN \end{bmatrix}$.

Running a 500,000-run IMLN simulation yield the following results presented in Figure 7.13 for the probabilities P_F, P_{MF} and P_{mMF} for the payload node. The processed probabilities of residency in each degraded state (P_F, P_M and P_m) are shown in the following figure, Figure 7.14.

The difference in the probability of residency with the monolith spacecraft ($P_{\text{SBN}} - P_{\text{monolith}}$) can be computed and Figure 7.15 demonstrates the survivability improvements brought by the "networkness" introduced in the C&DH subsystems.

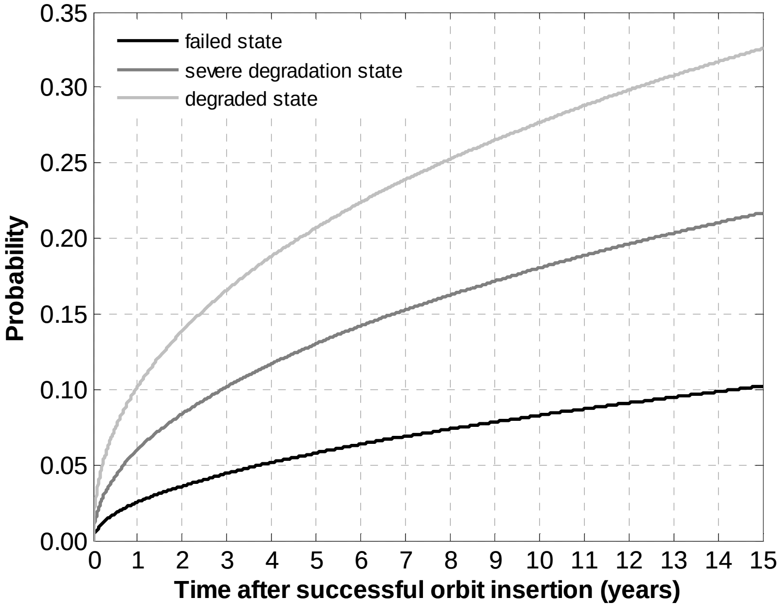


Figure 7.13. Output probabilities for T_F, T_{MF} and T_{mMF} of the payload node with C&DH redundancy

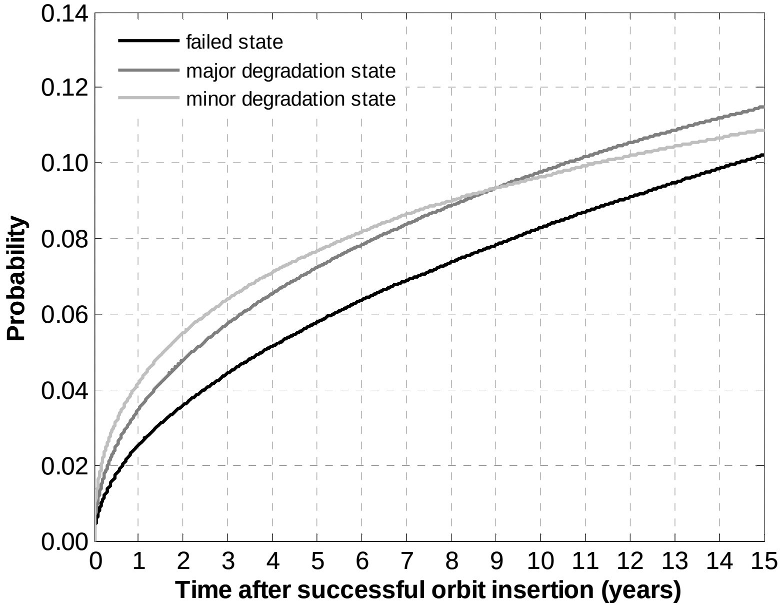


Figure 7.14. Processed probabilities for T_F, T_M and T_m of the payload node with C&DH redundancy

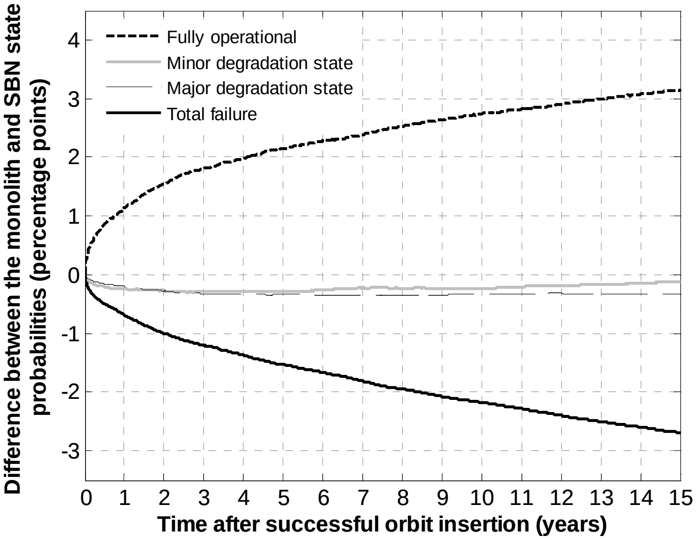


Figure 7.15. Survivability superiority of the space-based network with C&DH redundancy over the monolith spacecraft

For example, it can be seen in Figure 7.15 that after 15 years, the space-based network under consideration here has 3.1 percentage points more chance to be fully operational and generate utility at full performance than the monolith architecture. Regarding the total failure of the architectures, the network decreases the risk of payload unavailability by 2.6 percentage points. **This represents a 20.5% decrease compared to the monolith risk of losing payload utility (with respect to C&DH endogenous failures)**, and could be one of the elements justifying the consideration of space-based networks into the conceptual design process of the acquisition of a new space system. The fractionation of the three subsystems in the C&DH subsystem might be realized in upcoming space systems, but extending this paradigm shift to other subsystems such as the Electrical Power Subsystem or the Attitude and Orbit Control Subsystem might require technological breakthroughs. However, the results presented with the C&DH demonstrate certain survivability advantages of such architectures over the traditional monolithic design, but they should not be generalized to all designs of space-based networks or monolith architectures and they should not be extrapolated to other classes of on-orbit shocks. Also, survivability is one design aspect among others under consideration by the designers, and survivability advantages alone will not determine the final design decision. Complementary analyses on the cost and utility comparisons between space-based networks and monoliths can be found in Dubos and Saleh (2011).

7.3. General Subsystem/Technology Survivability Analysis

The previous section explored the survivability characteristics of specific subsystems associated with specific failure behavior derived from a 1584-Earth orbiting spacecraft sample. However, spacecraft designers might be interested in the impact of various subsystem or technology failure behaviors and links on design choices for the selection of networked architectures. To capture this variation, the anomaly and failure behavior of a general subsystem/technology, and further of the wireless link, is parameterized in this section, and the survivability characteristics of two architectures are explored. These two space-based networks are termed "2-IMLN" and "3-IMLN" in the remainder of this section and their complete representation is given below. The 2-IMLN and 3-IMLN architectures are similar to the ones used studied previously in the dissertation, and consist of two or three spacecraft networked to provide functional redundancy for the general subsystem/technology. Their representations are recalled in Figure 7.16 and Figure 7.17, and their adjacency matrices, interlayer matrices and mapping functions are given in section 7.2.1.

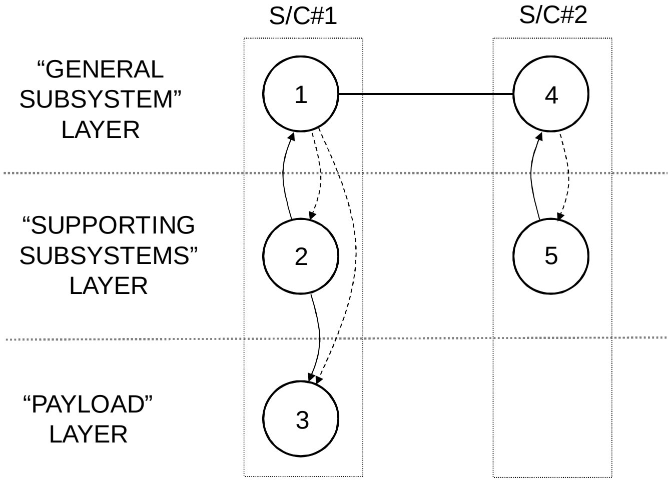


Figure 7.16. IMLN representation of the 2-IMLN

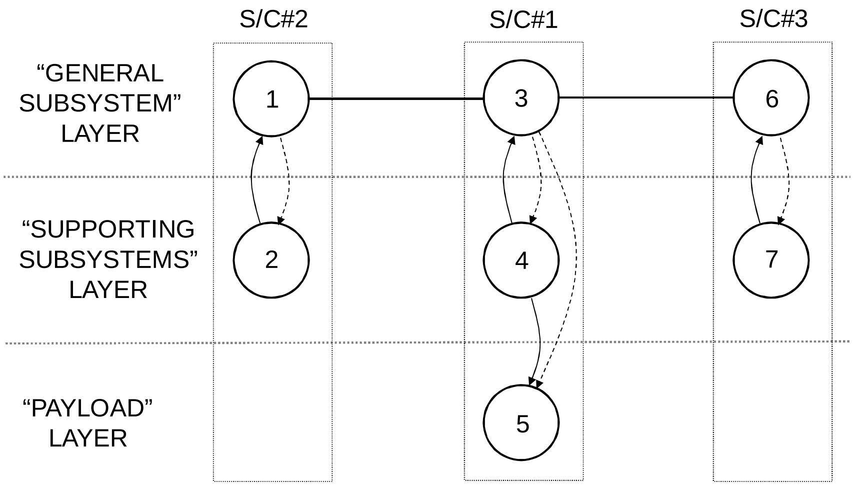


Figure 7.17. IMLN representation of the 3-IMLN

These specific architectures are simple but are extremely useful to explore the survivability trends of space-based networks in general as they illustrate the basic building blocks of a more complex network. The failure behavior of the supporting subsystems and payload functionality remain similar to the ones used previously and the Weibull distributions for their respective T_F, T_{MF} and T_{mMF} are recalled below in Table 7.3. Note that the sensitivity of the results obtained for the general subsystem/technology case will be investigated in this section.

Table 7.3. Weibull parameters for T_F, T_{MF} and T_{mMF} for the supporting subsystems and payload

Functionality	Severity level	Weibull shape parameter β	Weibull scale parameter θ
			years
Supporting subsystems	total failure	0.5181	1405
	severe degradation	0.4856	543.5
	any degradation	0.4523	230.2
Payload[14]	total failure	0.5767	49,990
	severe degradation	0.5529	2117
	any degradation	0.5568	981.4

[14] In this section, the "payload" vertex consists only of the payload instrument (no data handling).

As previously done, the survivability of each architecture is benchmarked by the traditional monolithic architecture, and the survivability metric is defined as the probability of being in a degraded state (P^F, P^M and P^m) for the payload node. As a consequence, the results and design implications provided next are limited to these choices.

7.3.1. Parameterization of Probability of Total Failure

The parameterization of the probability of failure of the networked subsystem/technology is conducted as follows. Let assume that the probability of failure is given by $\alpha_F(t)$. Five different failure behaviors are modeled in this dissertation, from a subsystem/technology that experiences few anomalies and failures to a subsystem/technology that is plagued by anomalies and failures. Let us first look into total failures. To characterize the different levels of severity of the failure behavior, the probability of total failure of the networked subsystem/technology after 15 years is used: $\alpha_F(t = 15\,\text{years}) = \alpha_F^{15}$. Five values of α_F^{15} are chosen here, from a low severity level to a high one: 0.01, 0.05, 0.10, 0.15 and 0.20.

In this dissertation, $\alpha_F(t)$ is modeled using a single Weibull distribution, with a fixed shape parameter β_F = 0.5, and a varying scale parameter θ_F to match the different α_F^{15} values. The choice of a single Weibull distribution is justified as this distribution type was shown in the previous chapters to be appropriate to model spacecraft subsystems. The shape parameter is chosen to be common to all distributions so that only one parameter in the Weibull distribution varies at a time, and its value is set at 0.5 as it is in the range of the shape parameters derived for most of the spacecraft subsystems in previous chapters. θ_F can be calculated using the expression of the Weibull c.d.f. as follows:

$$\theta_F = \frac{t}{\left[-\ln(1-\alpha_F(t))\right]^{\left(1/\beta_F\right)}} \tag{7.1}$$

Using Eq. (7.1), setting t = 15 years and β_F = 0.5 yields:

$$\theta_F = \frac{15}{\left[-\ln\left(1-\alpha_F^{15}\right)\right]^2} \tag{7.2}$$

The different values of θ_F are given in Table 7.4.

Table 7.4. Weibull scale parameter values for the networked subsystem/technology's failure behavior

$\boldsymbol{\alpha_F^{15}}$	**Scale parameter $\boldsymbol{\theta_F}$**
	years
0.01	148,501
0.05	5,701
0.10	1,351
0.15	568
0.20	301

The choice of a Weibull distribution affects the numerical results, but the IMLN models are general enough so that the reader can use and directly plug in different distributions to compute his own results.

7.3.2. IMLN Probability of Total Failure

The probabilities of catastrophic failure of the space-based networks under consideration are obtained by running the IMLN models, as well as using analytical expressions. Analytical expressions are possible in some cases here, but are already significantly complex for the relatively simple IMLN models presented in this section. Analytical expressions generally do not exist for interdependent multi-layer networks[15], and in the case they exit, they can be difficult to derive and use. Analytical expressions are used when possible in this section, as they provide insights complementary to the IMLN simulation on the survivability features of the space-based networks.

The probability of catastrophic failure of the traditional monolith architecture is given by:

$$P_{\text{monolith}}^{F} = 1 - \left(1 - P_{S}^{F}\right)\left(1 - P_{P}^{F}\right)\alpha_{F} \tag{7.3}$$

where: P_S^F is the probability of total failure of the supporting subsystems and P_P^F is the probability of total failure of the payload.

Similarly, the probabilities of catastrophic failure for the 2-IMLN and 3-IMLN architectures are given by:

[15] For example, in the case of the IMLN presented in Figure 7.12, no closed-form solution exists.

$$P^F_{\text{2-IMLN}} = 1 - \left(1 - P_S^F\right)\left(1 - P_P^F\right)\left\{1 - \left(1 - \left(1 - \alpha_F\right)\left(1 - P_S^F\right)\right)\alpha_F\right\} \tag{7.4}$$

$$P^F_{\text{3-IMLN}} = 1 - \left(1 - P_S^F\right)\left(1 - P_P^F\right)\left\{1 - \left(1 - \left(1 - \alpha_F\right)\left(1 - P_S^F\right)\right)^2 \alpha_F\right\} \tag{7.5}$$

Eqs. (7.3), (7.4) and (7.5) can be calculated for any time *t* spent on-orbit as shown in Figure 7.18. Also, for readability purposes here, four on-orbit times have been selected to compare architectures: 1 year, 5 years, 10 years and 15 years on-orbit. The probabilities of catastrophic failure (in percentage points) for the three architectures at these times are shown in Table 7.5. Note that no results are provided for the monolith architecture using the IMLN simulation as the interdependent multi-layer approach was proposed in this thesis for networked architectures (it is however possible to build a trivial model for the monolith case). The IMLN simulation results and the analytical results are in very good agreement, as the average error is 0.008 percentage point, a significantly low difference.

Table 7.5. Probabilities of failure for monolith and networked architectures (in percentage points)

α_F^{15}	**Architecture**	**P^F – IMLN simulation**				**P^F – Analytical results**			
		Time spent on-orbit (years)				Time spent on-orbit (years)			
		1	5	10	15	1	5	10	15
0.01	Monolith	–	–	–	–	2.76	6.26	8.85	10.82
	2-IMLN	2.51	5.73	8.16	10.00	2.51	5.74	8.16	10.01
	3-IMLN	2.50	5.71	8.11	9.93	2.50	5.71	8.11	9.93
0.05	Monolith	–	–	–	–	3.79	8.46	11.87	14.42
	2-IMLN	2.54	5.93	8.53	10.54	2.55	5.93	8.53	10.53
	3-IMLN	2.50	5.73	8.16	10.02	2.50	5.73	8.15	10.00
0.10	Monolith	–	–	–	–	5.12	11.28	15.68	18.93
	2-IMLN	2.63	6.30	9.23	11.54	2.63	6.31	9.24	11.56
	3-IMLN	2.51	5.77	8.27	10.21	2.51	5.78	8.27	10.22
0.15	Monolith	–	–	–	–	6.51	14.15	19.52	23.43
	2-IMLN	2.77	6.88	10.28	13.00	2.76	6.87	10.26	12.99
	3-IMLN	2.52	5.86	8.49	10.60	2.52	5.87	8.51	10.62
0.20	Monolith	–	–	–	–	7.96	17.11	23.42	27.94
	2-IMLN	2.94	7.63	11.61	14.84	2.93	7.62	11.60	14.83
	3-IMLN	2.54	6.04	8.91	11.27	2.54	6.03	8.90	11.26

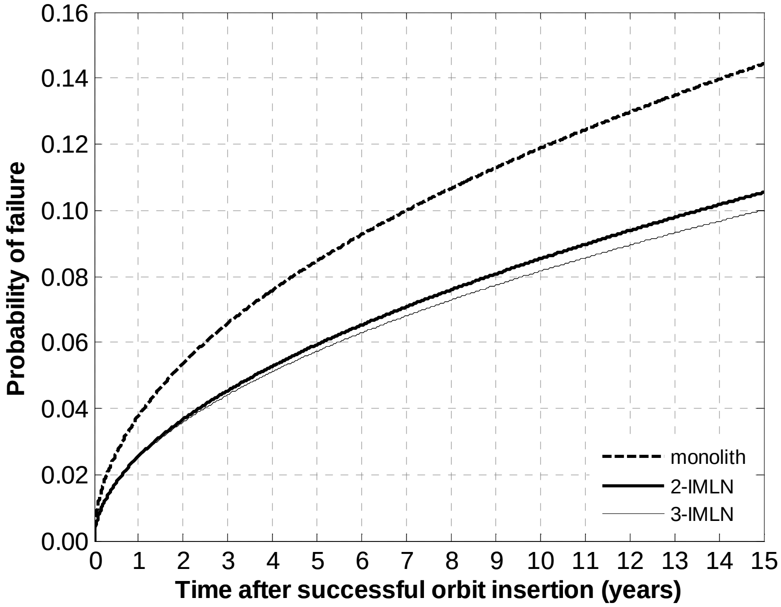


Figure 7.18. Probabilities of failure for monolith and networked architectures for $\alpha_F^{15} = 0.05$

Figure 7.19 provides a visual representation of Table 7.5 for the case $\alpha_F^{15} = 0.05$.

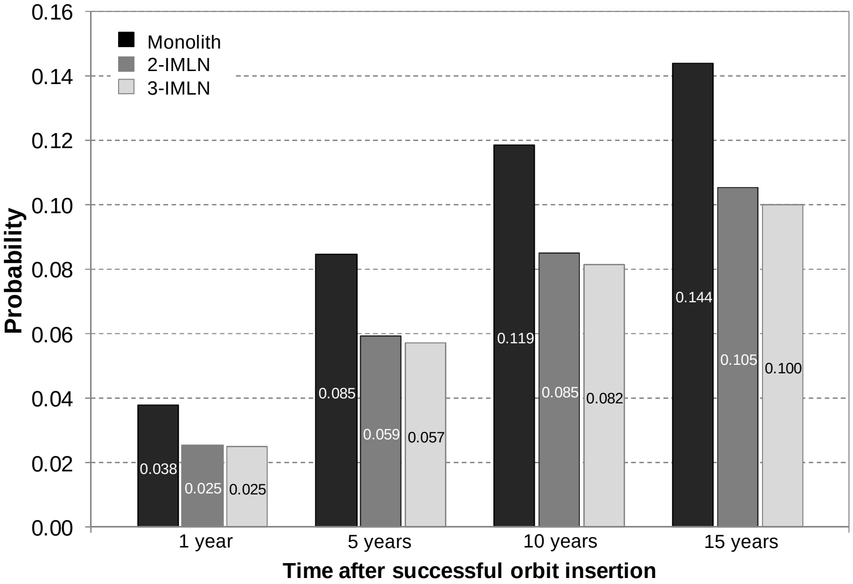


Figure 7.19. Snapshot of Figure 7.18 at four on-orbit times: 1, 5, 10 and 15 years

Figure 7.18 and Figure 7.19 read as follows: for example, after 5 years on-orbit, the probability of catastrophic failure is 0.085 for the monolith spacecraft (i.e., 8.5% chance of experiencing a catastrophic failure during the first 5 years on-orbit), 0.059 for the 2-IMLN architecture and 0.057 for the 3-IMLN architecture. In this particular example, the 2-IMLN architecture allows reducing the probability of a catastrophic failure during the first 5 years on-orbit by 2.53 percentage points and the 3-IMLN by 2.73 percentage points over the monolith architecture. These differences between the networked architectures and the monolith one is referred in this dissertation as the net gain and is labeled as Δ. **The net gain is an interesting indicator to the designer as it represents the absolute improvement or decline in survivability of one architecture with respect to another (with respect to the chosen performance metric and the class of threat of interest)**. It is mathematically defined as follows in the IMLN approach:

$$\Delta^F_{\text{2-IMLN}} = P^F_{\text{monolith}} - P^F_{\text{2-IMLN}} \tag{7.6}$$

$$\Delta^F_{\text{3-IMLN}} = P^F_{\text{monolith}} - P^F_{\text{3-IMLN}} \tag{7.7}$$

Developing the terms in Eqs. (7.3), (7.4) and (7.5) yields for the analytical solutions:

$$P^F_{\text{monolith}} = \alpha_F \left(1 - P^F_S\right)\left(1 - P^F_P\right) + 1 - \left(1 - P^F_S\right)\left(1 - P^F_P\right) \tag{7.8}$$

$$P^F_{\text{2-IMLN}} = \left(\alpha_F\right)^2 \left(1 - P^F_S\right)^2 \left(1 - P^F_P\right) + \alpha_F P^F_S \left(1 - P^F_S\right)\left(1 - P^F_P\right) + 1 - \left(1 - P^F_S\right)\left(1 - P^F_P\right) \tag{7.9}$$

$$\begin{aligned} P^F_{\text{3-IMLN}} &= (\alpha_F)^3 \left(1-P_S^F\right)^3 \left(1-P_P^F\right) + 2(\alpha_F)^2 P_S^F \left(1-P_S^F\right)^2 \left(1-P_P^F\right) \\ &\quad + \alpha_F \left(P_S^F\right)^2 \left(1-P_S^F\right)\left(1-P_P^F\right) + 1 - \left(1-P_S^F\right)\left(1-P_P^F\right) \end{aligned} \tag{7.10}$$

Substituting in Eqs. (7.6) and (7.7) results in:

$$\Delta^F_{\text{2-IMLN}} = \left(1-P_S^F\right)^2 \left(1-P_P^F\right)\left(1-\alpha_F\right)\alpha_F \tag{7.11}$$

$$\Delta^F_{\text{3-IMLN}} = \left(1-P_S^F\right)^2 \left(1-P_P^F\right)\left[-(\alpha_F)^2 \left(1-P_S^F\right) - 2\alpha_F P_S^F + 1 + P_S^F\right]\alpha_F \tag{7.12}$$

Figure 7.20 shows that for that particular setting and for this range of on-orbit time shown in Figure 7.19, the net gain increases in time. This suggests that the **longer the space architecture is planned to operate, the greater the benefit of the space-based architecture for survivability** in the case studied here. Indeed, if the architecture is designed to operate 1 year, then a networked architecture does not significantly improve over the traditional architecture (about 1 percentage point improvement), while an architecture designed to operate 15 years might benefit from the space-based network option (about 4 percentage points, to balance with the cost of adding spacecraft). Note that this trend is not valid for all times, as when time goes to infinity, Δ goes to zero. Also in this particular example, the difference between $\Delta_{\text{2-IMLN}}$ and $\Delta_{\text{3-IMLN}}$ is relatively small (0.53 percentage point after 15 years), suggesting that adding a third spacecraft to the network might not be the best option.

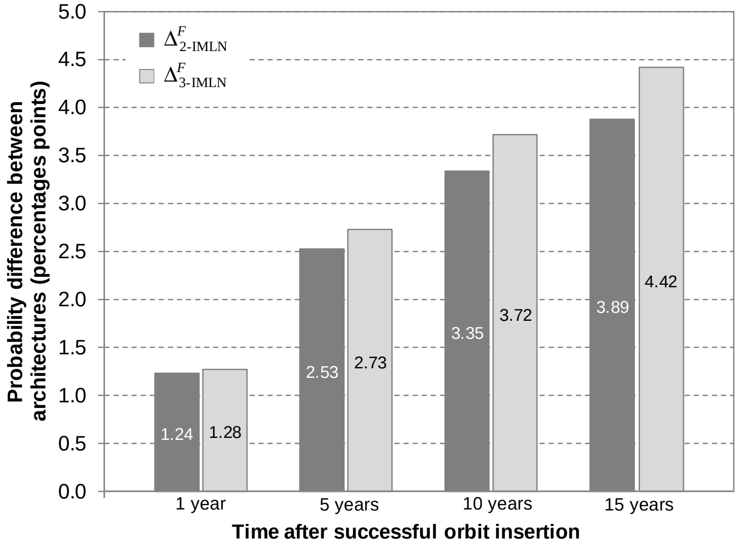


Figure 7.20. Net gain for the 2-IMLN and 3-IMLN compared to the monolith spacecraft for $\alpha_F^{15} = 0.05$

Another way to look at the data presented in Table 7.5 is to observe the impact of the failure behavior of the networked subsystem/technology on the probability of catastrophic failure of the monolith and networked architectures, i.e., its variation with α_F^{15}. Figure 7.21 shows this variation after 5 years on-orbit.

Figure 7.21 reads as follows: for example, after 5 years on-orbit, and for $\alpha_F^{15} = 0.05$, the monolith architecture has 11.3% chance of experiencing a catastrophic failure, while the 2-IMLN architecture has a 6.3% similar chance and the 3-IMLN a 5.8% chance.

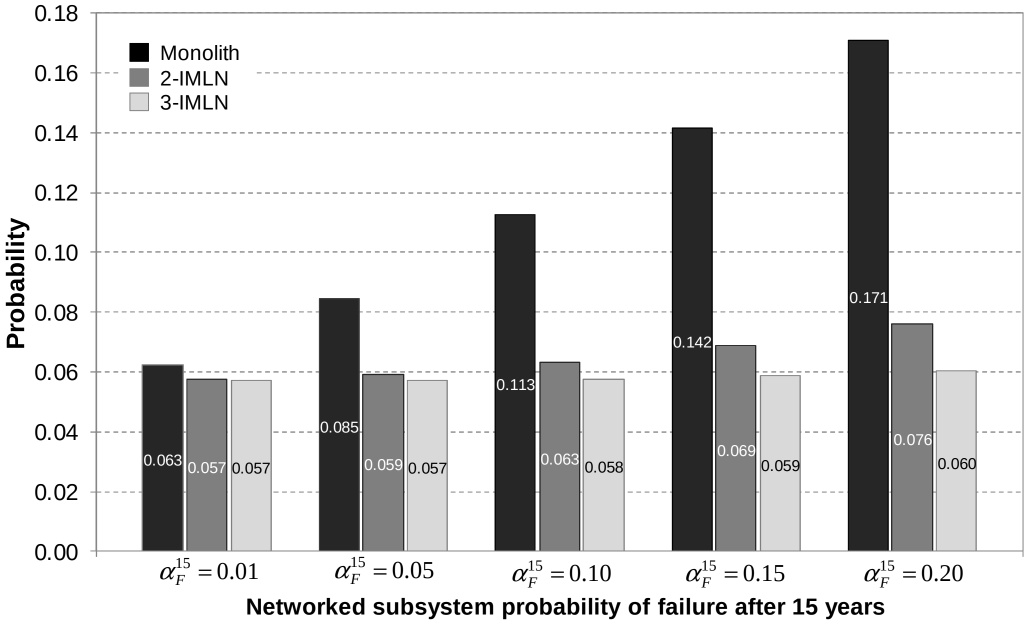


Figure 7.21. Variation of the probability of failure of architectures with α_F^{15}

As expected, the probability of a catastrophic failure at the system level increases with α_F^{15}. However, each architecture responds differently to the variation of α_F^{15}. The monolith architecture is significantly affected by its variation, while the networked architectures tend to be less affected: the probability of a catastrophic failure for the monolith architecture varies from 6.26% ($\alpha_F^{15} = 0.01$) to 17.11% ($\alpha_F^{15} = 0.20$); on the other hand, the probability of a catastrophic failure varies from 5.74% ($\alpha_F^{15} = 0.01$) to 7.62% ($\alpha_F^{15} = 0.20$) for the 2-IMLN, and from 5.71% ($\alpha_F^{15} = 0.01$) to 6.03% ($\alpha_F^{15} = 0.20$) for the 3-IMLN. To quantify this variation, let define the relative failure growth of the architecture as follows:

$$\gamma_F^5 = \frac{P_{\text{architecture}}^F(t = 5\text{ years}) - P_0^F(t = 5\text{ years})}{P_0^F(t = 5\text{ years})} \qquad (7.13)$$

where: $P_0^F(t)$ is the probability of a catastrophic failure for the architecture with a perfectly reliable networkable subsystem/technology ($\alpha_F = 0$)[16].

γ_F represents the relative error between a system with a perfectly reliable networkable subsystem/technology and the system under consideration with a networkable subsystem/technology prone to failures. In the present case, $P_0^F(t = 5\text{ years}) = 0.0571$, and using the values at 5 years presented in Table 7.5, the values for γ_F can be computed and are presented in Table 7.6. The results from Table 7.6 are also presented graphically in Figure 7.22. Table 7.6 results and Figure 7.22 confirm that the monolith architecture is severely affected by the failure behavior of the networkable subsystem/technology, with its probability of failure varying by 9.6% for a subsystem/technology failing little to almost 200% with a severely degrading subsystem/technology. On the other hand, the networked architectures handle better the failure of the networked subsystem/technology, as in the worst case considered here ($\alpha_F^{15} = 0.20$), the 2-IMLN architecture has a relative failure growth of 33.6% after 5 years, an order of magnitude lower than the one of the monolith spacecraft, and the 3-IMLN probability of catastrophic failure varies only by 5.7%, one additional order of magnitude lower.

[16] P_0^F is common to the three architectures

As a conclusion, **the networked architectures have a "shielding effect"** (in the sense that they shield the system from the failures of the networked subsystem/technology)**, and this effect grows stronger with the addition of spacecraft to the network**. Consequently, this positive behavior of the network can allow the design of a system with unproven subsystems or technologies, for example for technology testing, as it limits the sensitivity of the network to (potentially) problematic subsystems/technologies. Also, the relative failure growth can help informing the decision about the relevance of a networked architecture (and its number of spacecraft) according to shareholder risk tolerance.

Table 7.6. Relative failure growth (in percentage) of the architectures at *t* = 5 years

Architecture	γ_F^5					
	α_F^{15}:	0.01	0.05	0.10	0.15	0.20
Monolith		9.6%	48.2%	97.5%	147.9%	199.7%
2-IMLN		0.4%	3.8%	10.3%	20.5%	33.6%
3-IMLN		0.0%	0.4%	1.1%	2.6%	5.7%

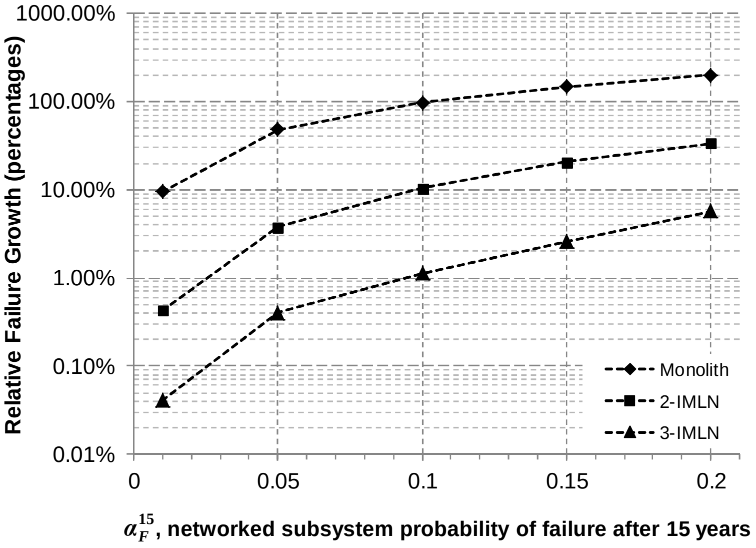


Figure 7.22. Relative failure growth after 5 years on-orbit with a logarithmic scale

7.3.3. Network Efficiency Relative To Failure

Another way to look at the shielding effect of the networked architecture is to investigate how efficiently they capture and eliminate catastrophic failures. **The network efficiency is an interesting indicator to the designer as it represents how much of the potential improvement (or decline) in survivability available is actually realized by the architecture** (with respect to the chosen performance metric and class of threat of interest). The maximum net gain a monolith can capture is limited to the complete elimination of the networkable subsystem/technology failures:

$$\Delta_0^F(t) = P_{\text{monolith}}^F(t) - P_0^F(t) \tag{7.14}$$

On the other hand, the net gain of a networked architecture over the monolith architecture is defined using Eqs. (7.11) and (7.12). The efficiency of the networked architecture compared to the monolith in rooting out failure is then defined in the ILMN approach as:

$$\eta^F(t) = \frac{P_{\text{monolith}}^F(t) - P_{\text{IMLN}}^F(t)}{P_{\text{monolith}}^F(t) - P_0^F(t)} = \frac{P_{\text{monolith}}^F(t) - P_{\text{IMLN}}^F(t)}{\Delta_0^F(t)} \tag{7.15}$$

Specifically for the 2-IMLN and 3-IMLN architectures:

$$\eta_{2-\text{IMLN}}^F(t) = \frac{\Delta_{2-\text{IMLN}}^F(t)}{\Delta_0^F(t)} \tag{7.16}$$

$$\eta^F_{3-\mathrm{IMLN}}(t) = \frac{\Delta^F_{3-\mathrm{IMLN}}(t)}{\Delta^F_0(t)} \tag{7.17}$$

As analytical expressions exist in this particular case of space-based networks, Eqs. (7.14), (7.16) and (7.17) can be expended using Eqs. (7.9), (7.11), (7.12) and the following:

$$P^F_0(t) = 1 - \left(1 - P^F_S\right)\left(1 - P^F_P\right) \tag{7.18}$$

Then:

$$\Delta^F_0(t) = \alpha_F \left(1 - P^F_S\right)\left(1 - P^F_P\right) \tag{7.19}$$

And:

$$\eta^F_{2-\mathrm{IMLN}}(t) = \frac{\Delta^F_{2-\mathrm{IMLN}}(t)}{\Delta^F_0(t)} = \frac{\left(1 - P^F_S\right)^2 \left(1 - P^F_P\right)\left(1 - \alpha_F\right)\alpha_F}{\alpha_F \left(1 - P^F_S\right)\left(1 - P^F_P\right)} = \left(1 - P^F_S\right)\left(1 - \alpha_F\right) \tag{7.20}$$

$$\begin{aligned}\eta^F_{3-\mathrm{IMLN}}(t) = \frac{\Delta^F_{3-\mathrm{IMLN}}(t)}{\Delta^F_0(t)} &= \frac{\left(1 - P^F_S\right)^2 \left(1 - P^F_P\right)\left[-\left(\alpha_F\right)^2 \left(1 - P^F_S\right) - 2\alpha_F P^F_S + 1 + P^F_S\right]\alpha_F}{\alpha_F \left(1 - P^F_S\right)\left(1 - P^F_P\right)} \\ &= \left(1 - P^F_S\right)\left[-\left(\alpha_F\right)^2 \left(1 - P^F_S\right) - 2\alpha_F P^F_S + 1 + P^F_S\right]\end{aligned} \tag{7.21}$$

These last two equations can be further manipulated to highlight the dependence on α_F:

$$\eta^{F}_{2\text{–IMLN}} = -\alpha_F \left(1 - P_S^F\right) + 1 - P_S^F \qquad (7.22)$$

$$\eta^{F}_{3\text{–IMLN}} = -\left(\alpha_F\right)^2 \left(1 - P_S^F\right)^2 - 2\alpha_F P_S^F \left(1 - P_S^F\right) + 1 - \left(P_S^F\right)^2 \qquad (7.23)$$

The IMLN simulation was run to determine the efficiencies of the two space-based networks, and the results at 4 points in time (as previously, 1, 5, 10 and 15 years) were selected for readability purposes. 100,000 runs were repeated 10 times to obtain average efficiencies and confidence intervals on the simulation results. In addition, plugging in the equations above the distributions for α_F and P_S, the efficiency of the 2-IMLN and 3-IMLN architectures is also obtained for all times up to 15 years in orbit, for comparison with the IMLN results. Figure 7.23 shows the efficiency of the 2-IMLN architecture and Figure 7.24 for the 3-IMLN, with the solid line showing the analytical results, and the x-mark showing the simulation results. The numerical values for the simulation are given in Table 7.7, along with their equivalents from the analytical formulas. Also Table 7.8 presents the confidence interval spread for the simulation results. The simulation and analytical results are well in agreement, with an average difference of 0.003 for the 2-IMLN and 0.001 for the 3-IMLN. Note that on Figure 7.23 the simulation results are following closely the solid lines for α_F^{15} from 0.05 to 0.20 (for the 0.01 case, the simulation results are less precise); similarly for the 3-IMLN in Figure 7.24, the simulation and analytical results are close for α_F^{15} from 0.10 to 0.20 (the cases 0.05 and 0.01 are less precise). The less precise results correspond to the simulation results with larger confidence intervals, and their precision could be largely improved by running simulations with higher numbers of runs (at the expense of time and hardware power, not done here as the absolute precision of the results is nevertheless high).

Table 7.7. Efficiency for the networked architectures

α_F^{15}	Architecture	η^F – IMLN simulation				η^F – Analytical results			
		Time spent on-orbit (years)				Time spent on-orbit (years)			
		1	5	10	15	1	5	10	15
0.01	2-IMLN	0.981	0.956	0.921	0.907	0.974	0.942	0.918	0.900
	3-IMLN	1.000	0.996	0.988	0.987	0.999	0.997	0.993	0.990
0.05	2-IMLN	0.969	0.922	0.888	0.862	0.964	0.920	0.888	0.864
	3-IMLN	0.999	0.992	0.984	0.979	0.999	0.994	0.987	0.981
0.10	2-IMLN	0.952	0.894	0.852	0.820	0.951	0.892	0.849	0.818
	3-IMLN	0.997	0.989	0.978	0.967	0.998	0.988	0.977	0.967
0.15	2-IMLN	0.934	0.861	0.809	0.772	0.937	0.863	0.811	0.773
	3-IMLN	0.996	0.982	0.966	0.949	0.996	0.981	0.964	0.948
0.20	2-IMLN	0.920	0.832	0.771	0.727	0.922	0.833	0.772	0.727
	3-IMLN	0.994	0.971	0.947	0.925	0.994	0.972	0.948	0.926

Table 7.8. Confidence intervals on the efficiency of the networks from the IMLN simulation

α_F^{15}	Architecture	Confidence interval spread on η^F IMLN simulation			
		Time spent on-orbit (years)			
		1	5	10	15
0.01	2-IMLN	0.058	0.036	0.046	0.048
	3-IMLN	0.025	0.040	0.034	0.029
0.05	2-IMLN	0.006	0.008	0.004	0.006
	3-IMLN	0.016	0.014	0.012	0.010
0.10	2-IMLN	0.008	0.006	0.004	0.004
	3-IMLN	0.008	0.004	0.004	0.004
0.15	2-IMLN	0.008	0.006	0.004	0.004
	3-IMLN	0.004	0.004	0.004	0.002
0.20	2-IMLN	0.006	0.004	0.004	0.004
	3-IMLN	0.004	0.002	0.004	0.004

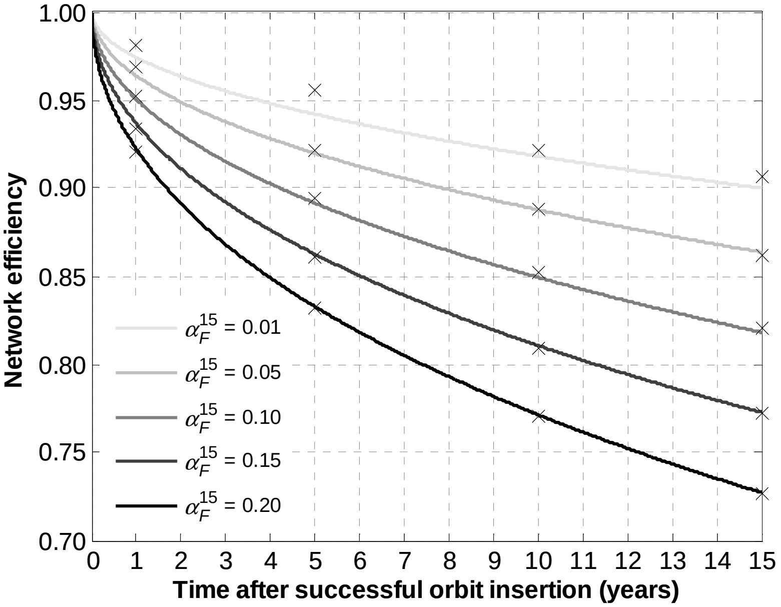


Figure 7.23. Efficiency of the 2-IMLN architecture

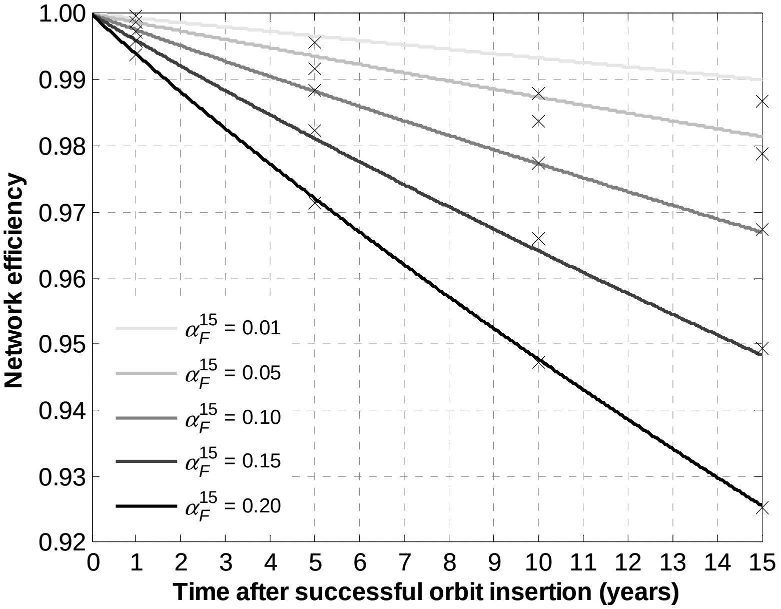


Figure 7.24. Efficiency of the 3-IMLN architecture

Figure 7.23 reads as follows: for example, after 10 years on-orbit and for $\alpha_F^{15} = 0.10$, the efficiency of the 2-IMLN architecture is about 0.85, i.e., the network was successful in capturing 85% of Δ_0^F. Similarly on Figure 7.24, for the same conditions, the efficiency of the 3-IMLN architecture is about 0.98. It can immediately be seen that in all the conditions explored here, **the architecture with a higher number of spacecraft has a higher efficiency**. Nevertheless here, as seen on Figure 7.23, the efficiency of the 2-IMLN remains relatively high for all times, even for the worse-case subsystem/technology failure under consideration here: the lowest efficiency recorded is about 0.73. This shows that the addition of a networked spacecraft to the traditional monolith spacecraft allows capturing at least 73% of the failure probability share of the networked subsystem/technology, which is quite significant. The 3-IMLN architecture performs even better, as the lowest efficiency recorded here is about 0.93. This could suggest that adding a fourth or more spacecraft to network would not be the best option in this case as the 3-IMLN almost capture all the failures that can be. However, a networkable subsystem/technology with a worse failure behavior than studied here could warrant more spacecraft for a more efficient network. As a consequence, **the efficiency can be a useful tool to the designer to select networked architectures depending on performance requirements**.

Several trends can be seen in both figures. First, the efficiency decreases with time: it means that the networks are more successful in shielding the system of failures early in the orbital life rather than later. Second, the efficiency also decreases with α_F^{15} increasing:

the networks are more efficient in shielding the system from a subsystem/technology failing little than from a heavily degrading subsystem/technology.

These two observations means that, **if an efficiency lower bound is fixed, then a time horizon exists for the network, and this horizon will occur earlier with major contributors to failure than with minor ones**. For example, considering two systems in a 2-IMLN configuration with $\alpha_F^{15} = 0.10$ and $\alpha_F^{15} = 0.20$ respectively, if a 85% efficiency threshold is required, then the first architecture meets this requirement for about 10 years on-orbit, while the second meets it only for the first 4 years. **This time horizon will also occur later for architectures with more spacecraft**. For example, considering $\alpha_F^{15} = 0.20$, if a 95% efficiency threshold is required, then the 2-IMLN architecture will meet this requirement for only half a year, while the 3-IMLN will meet it for 9.5 years.

It is mentioned above that the 3-IMLN architecture has a higher efficiency for the same α_F^{15}–level than the 2-IMLN architecture. Compares these two efficiencies after 15 years on orbit when varying α_F^{15}. This figure is obtained by a direct application of Eqs. (7.22) and (7.23): indeed, when t is fixed (here at 15 years), then P_S^F is also fixed, and the efficiency becomes only a function of α_F^{15} (linear effect for the 2-IMLN and quadratic for the 3-IMLN). Figure 7.25 clearly shows that the efficiency decreases with α_F^{15}, but more sharply for the 2-IMLN than the 3-IMLN in the 0–0.20 range (due to the quadratic effect, there is a range of high α_F^{15} for which the slope is higher for the 3-IMLN).

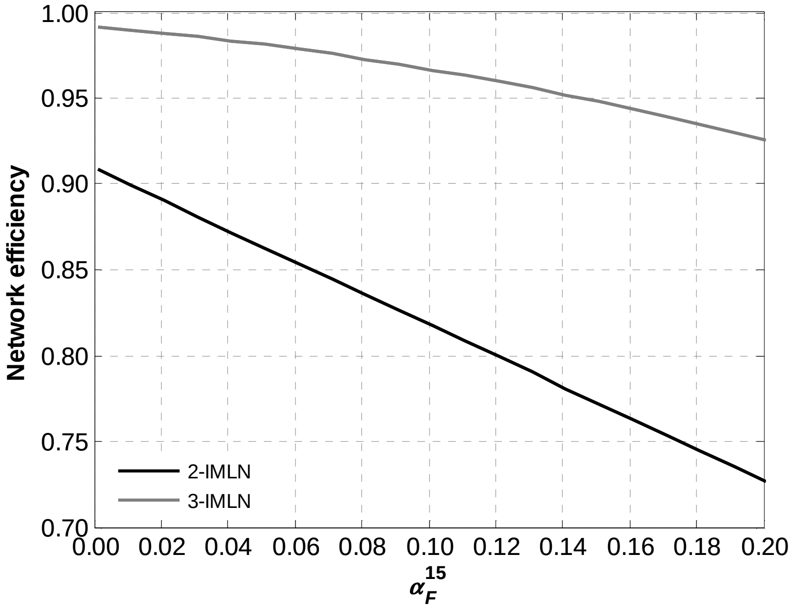


Figure 7.25. 2-IMLN versus 3-IMLN efficiency as a function of α_F^{15}

7.3.4. Efficiency Versus Net Gain

While it can be tempting to choose architectures with the highest efficiency, the net gain should also be considered in the decision process, as an architecture with a high efficiency but a very small net gain might not be the best candidate from a cost-benefit point of view. To combine both pieces of information, a new graph is introduced in this thesis and presents the network efficiency on the *x*-axis and the net gain from the network on the *y*-axis. Four notional areas can be envisioned on the η–Δ graph as shown in Figure 7.26, and some characteristics of the architectures can be deduced from their location on this graph (all the following survivability implications are considered with respect to the chosen performance metric and class of threat of interest):

- the area marked with a number 1 encircled corresponds to a network that has a high efficiency and a high net gain: it means that the monolith architecture failure behavior is such that a significant potential improvement exists and is fully captured by the space-based network under consideration. As a consequence, the architecture can be considered as insensitive to the failure of the networked subsystem/technology and is potentially a better choice than the monolith architecture for survivability considerations;
- the area marked with a number 2 encircled corresponds to a network that has a low efficiency and a high net gain: it means that the monolith architecture failure behavior is such that a significant potential improvement exists but the space-based network under consideration failed to capture a significant share of it. Contrary to the case in the previous point, the architecture is significantly affected by the failure of the networked subsystem/technology. Despite its low efficiency, the space-based network remains worth considering as it fares significantly better than the monolith architecture (high net gain) from a survivability point of view;
- the area marked with a number 3 encircled corresponds to a network that has a high efficiency and a low net gain: it means that the monolith architecture failure behavior is such that not much of a potential improvement exists in terms of reducing the probability of failure of the system; but however small is this improvement, it is fully captured by the space-based network under consideration. The failure behavior of the networked subsystem/technology is eradicated, but it was not affecting the monolith architecture in the first place;

- the area marked with a number 4 encircled corresponds to a network that has a low efficiency and a low net gain. Two possible cases arise: the potential improvement over the monolith architecture in terms of reducing the probability of failure of the system can be either low or high, but in both cases, the space-based network under consideration failed to capture it. In the first case, the space-based network might not be worth considering as the cost of adding a spacecraft does not buy a significantly better probability of failure. In the second case, the space-based network might be worth considering given some modifications to the network as explained in the following.

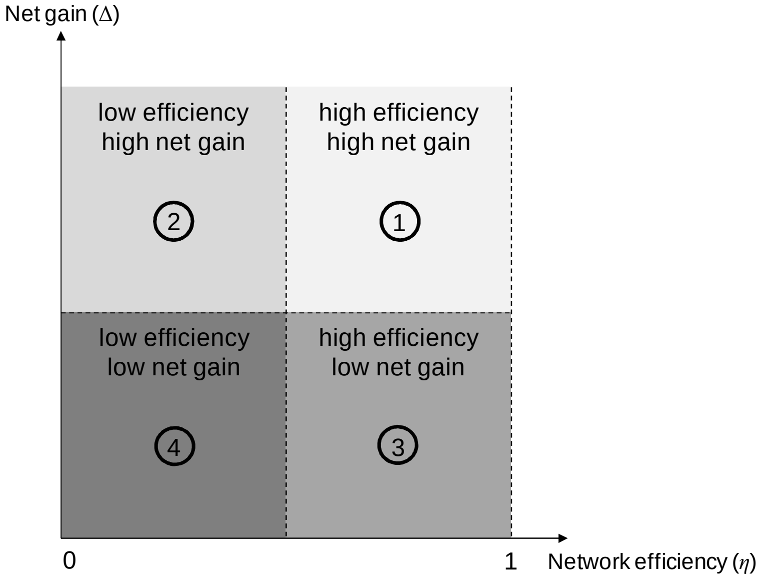
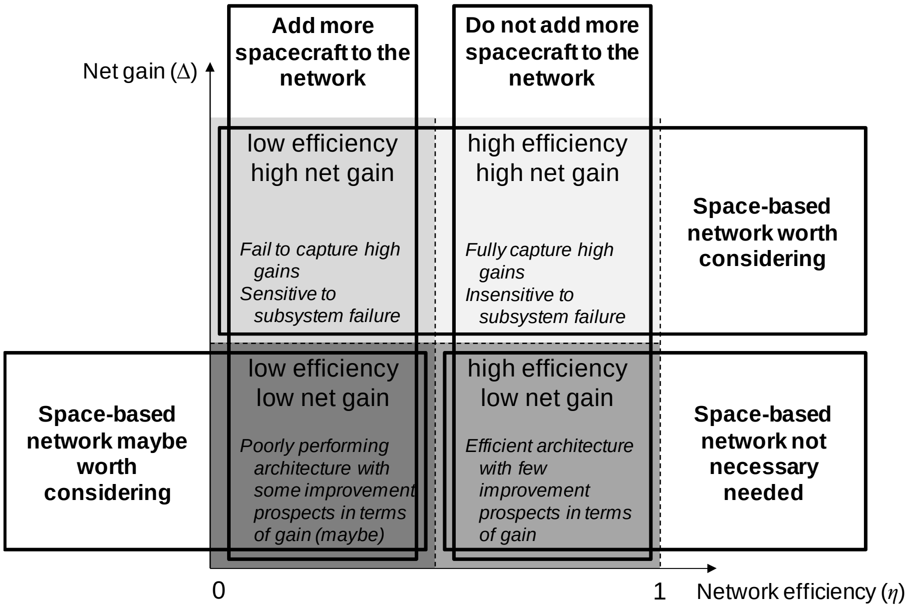


Figure 7.26. η–Δ graph with four types of architecture performance

The practical implications of the η–Δ graph are given below, and visually represented in Figure 7.27.

- **In the case of high efficiencies, the practical implication consists of not adding more spacecraft to the network for mitigating the failure of the networked subsystem(s)/technology(ies)** as the current architecture fully capture the shortcomings of the monolith architecture (areas 1 and 3 in the η–Δ graph). Removing some functionally redundant modules might also be an option to be considered according to the performance of that updated architecture.
- **The fact that a space-based network has a low efficiency should translate in considering the addition of functionally redundant modules for the networked subsystem(s)/technology(ies)**: as seen earlier, networks with a higher number of networked spacecraft have a higher efficiency (areas 2 and 4).
- **The previous two points should be adapted in function of the net gain**. A space-based network with high efficiency gains and high gain efficiency (area 1 in the η–Δ graph) does not require any improvement and can be considered as is: as a consequence, it should follow the "do not add spacecraft" implication. A space-based network high efficiency but with low gain (area 3) might not be cost-effective as is, and consequently no more spacecraft should be added to the network for the benefit of the networked subsystem/technology failure behavior (other modules such as payloads for example might be considered). The case of a space-based network with low efficiency but high gain (area 2) implies that a significant share of a high potential improvement is not captured by the current version of the network. More spacecraft should then be considered being added to the network. Finally, actions on space-based networks with low efficiencies but high gains (area 4) are not straightforward, as the potential improvement over a

monolith architecture is not readily observable due to the low efficiency of the network. If the potential improvement is high, then adding spacecraft to the network might result in significant gains; however if it is low, then the space-based network might not be a worthwhile alternative to the monolith spacecraft from a survivability point of view.



Add more spacecraft to the network
Do not add more spacecraft to the network
Net gain (Δ)
low efficiency high net gain
Fail to capture high gains
Sensitive to subsystem failure
high efficiency high net gain
Fully capture high gains
Insensitive to subsystem failure
Space-based network worth considering
Space-based network maybe worth considering
low efficiency low net gain
Poorly performing architecture with some improvement prospects in terms of gain (maybe)
high efficiency low net gain
Efficient architecture with few improvement prospects in terms of gain
Space-based network not necessary needed
0
1
Network efficiency (η)

Figure 7.27. Practical implications of the η–Δ graph for survivability considerations

7.3.5. η–Δ Graphs for 2- and 3-IMLN Architectures

Let us build the η–Δ graph for the 2-IMLN architecture defined earlier in this section. Recall that the efficiency and the net gain both vary with time and with α_F^{15}. The resulting graph for $\alpha_F^{15} = 0.05$ is presented in Figure 7.28, and the different lines and markers are explained in the caption of the figure.

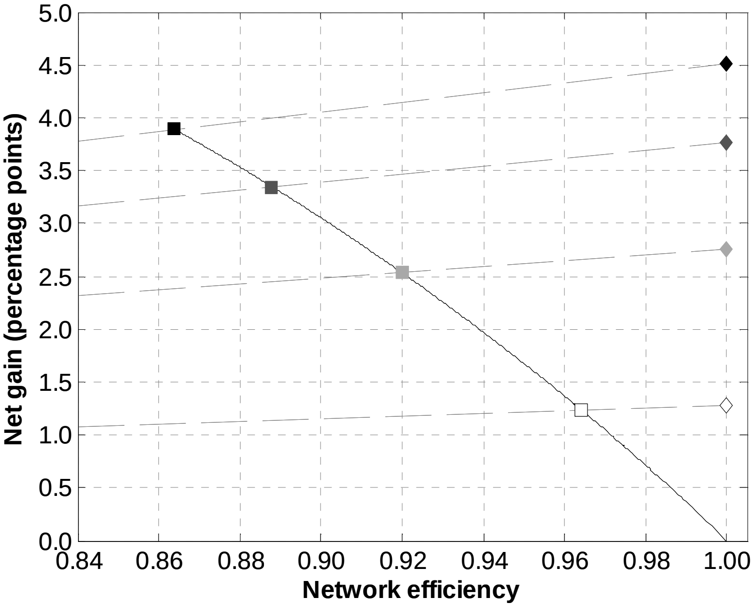


Figure 7.28. η–Δ graph for the 2-IMLN architecture as a function of time for $\alpha_F^{15} = 0.05$

(*the black solid line corresponds to the evolution in time of the efficiency and net gain of the 2-IMLN architecture, and the grey dashed lines correspond to instant in the orbital life of the system: 1, 5, 10 and 15 years from bottom to top. The square markers at the intersections of the solid line and dashed lines give (η,Δ) for the specified time (ageing from lighter to darker colors). The diamond-shaped markers represent the time-associated maximum net gains Δ_0 (also referred to as potential improvements from monoliths*)

Figure 7.28 reads as follows: after 5 years on orbit (light-grey square), the efficiency of the 2-IMLN is 0.92 and the associated net gain is 2.53 percentage points. The maximum net gain possible at the same time is 2.75 (light-grey diamond). Note that the numbers are consistent as $2.75 \times 0.92 = 2.53$. As observed previously, it can be seen that high gains come at the expense of efficiency and time. The η–Δ graph for the 3-IMLN for $\alpha_F^{15} = 0.05$ can be compiled in the same fashion, and is added to the 2-IMLN curve in Figure 7.29.

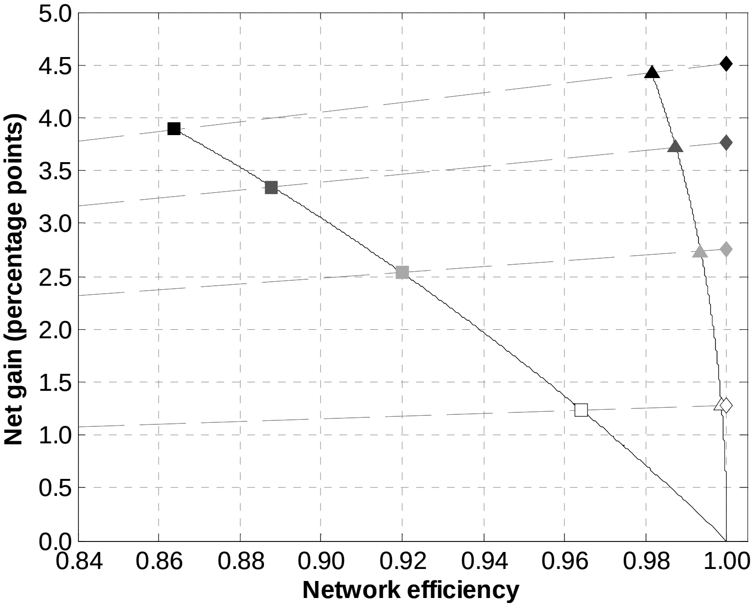


Figure 7.29. *η*–Δ graph for the 2-IMLN (square) and 3-IMLN (triangle) architectures as a function of time for $\alpha_F^{15} = 0.05$

(*Same formatting than the previous figure*)

Figure 7.29 shows that the 3-IMLN architecture has higher gains and higher efficiencies than the 2-IMLN for the same time. Also, the 3-IMLN curve stays closer to the “ideal” vertical curve at $\eta = 1$. A two-point comparison yields the following:

- After 5 years on-orbit, having added one spacecraft to the 2-IMLN architecture improves efficiency from 0.920 to 0.994, but the relative net gain associated is limited to 0.20 percentage point (from 2.53 to 2.73 percentage points).
- After 15 years on-orbit, the same operation yields an improved efficiency of 0.981 from 0.864, and the relative associated gain is 0.53 percentage point (from 3.89 to 4.42 percentage points).

A careful cost-benefit analysis should be conducted to assess whether these incremental improvements (from a monolith architecture to a 2-IMLN, and from a 2-IMLN to a 3-IMLN) are worth the cost of obtaining them.

Impact of $\boldsymbol{\alpha_F^{15}}$. Let us now vary α_F^{15}, that is, modify the failure behavior of the networked subsystem/technology (an increase in α_F^{15} translates in a networked subsystem/ technology more prone to failure). As previously, α_F^{15} varies from 0.01 to 0.20 and the resulting η–Δ graph is shown in Figure 7.30 for the 2-IMLN and Figure 7.31 for the 3-IMLN (the lowest curve has the lowest α_F^{15} and the highest curve the highest α_F^{15}).

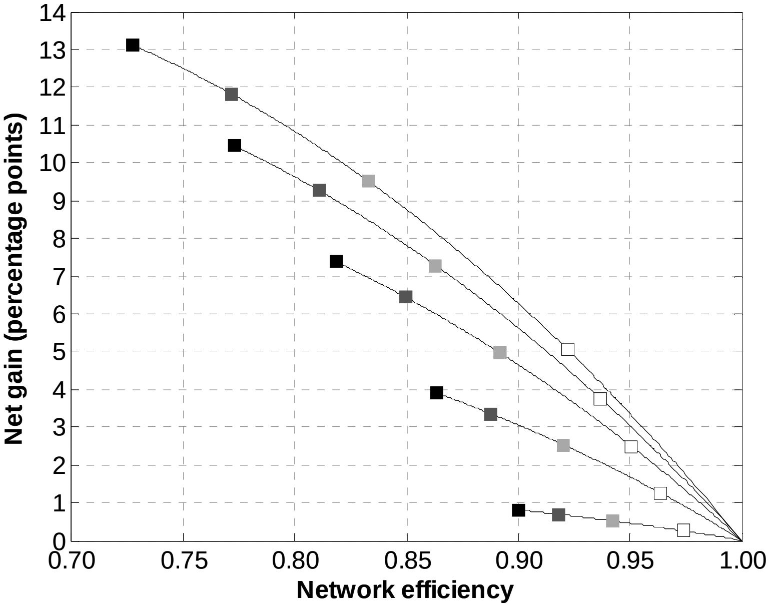


Figure 7.30. Variations of the 2-IMLN network efficiency and net gain with $\boldsymbol{\alpha_F^{15}}$

(*As previously, the color of the square markers corresponds to the on-orbit times, 1, 5, 10 and 15 years, from lighter to darker colors. The different curves correspond to the variation of* α_F^{15}*, from 0.01 in the bottom curve to 0.20 in the top curve*)

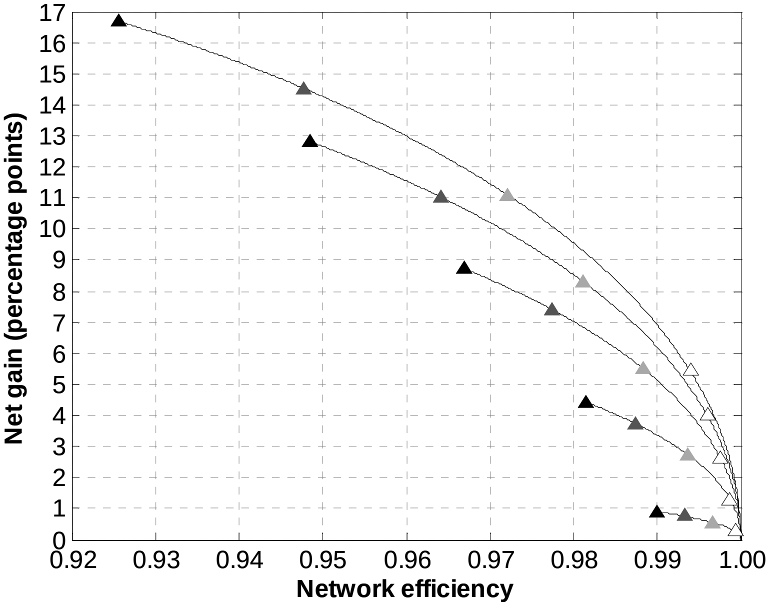


Figure 7.31. Variations of the 3-IMLN network efficiency and net gain with α_F^{15}

(*Same formatting than the previous figure*)

Several interesting trends can be seen on Figure 7.30 and Figure 7.31: increasing α_F^{15} results in increasing net gains at all times. For example, increasing α_F^{15} from 0.05 to 0.15 increases the net gain from 2.53 to 7.28 at 5 years for the 2-IMLN architecture, and from 2.73 to 8.28 for the same time for the 3-IMLN architecture. This trend comes from the fact that increasing α_F^{15} means that the probability of failure of the networked subsystem/technology increases and it results in higher potential net gains. Note that the 3-IMLN net gains are higher than the 2-IMLN as seen previously, and also that the relative net gain increase is higher in proportion for the 3-IMLN than for the 2-IMLN. Finally, in the case of a problematic subsystem/technology (such as $\alpha_F^{15} = 0.20$), the net gain reaches 13 percentage points after 15 years for the 2-IMLN and almost 17 points for the 3-IMLN, a significant improvement over the monolith architecture.

In parallel, increasing α_F^{15} results in decreasing efficiency at all times. Continuing the same example than above, the efficiency of the 2-IMLN architecture at 5 years decreases from 0.920 to 0.863, and from 0.994 to 0.981 for the 3-IMLN architecture by increasing α_F^{15} from 0.05 to 0.15. The 2-IMLN experienced a 6.2% loss in efficiency relative to the $\alpha_F^{15} = 0.05$ value, while the 3-IMLN limited its loss to 1.3%. This results is consistent with the fact the 3-IMLN architecture is more insensitive to the networked subsystem/technology failures than the 2-IMLN: in the worst case considered here, the efficiency lower bound for the 3-IMLN is a relatively high 0.926, when it is 0.727 for the 2-IMLN. Figure 7.32 presents a compact version of the trends discussed above.

Figure 7.32 clearly shows the impact of the networked subsystem/technology's probability of failure and the difference between the networks with 2 or 3 spacecraft here under consideration. Figure 7.32 highlights the potential interest in adding a spacecraft for networkable subsystems/technologies with a high probability of failure. For the range of times and α_F^{15} considered here, networks with more than 3 spacecraft for the same functionality are difficult to justify, as the 3-IMLN performance is significantly high in capturing the networkable subsystem/technology failures.

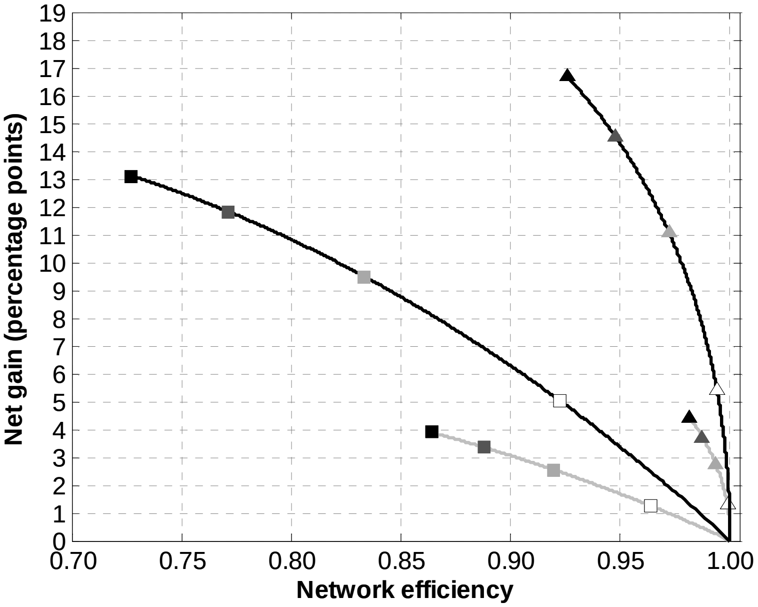


Figure 7.32. 2- and 3-IMLN comparison for $\alpha_F^{15} = 0.05$ and $\alpha_F^{15} = 0.20$

(*The grey curves correspond to* $\alpha_F^{15} = 0.05$ *and the black curves correspond to* $\alpha_F^{15} = 0.20$. *The square markers represent the 2-IMLN, and the triangle markers represent the 3-IMLN. As previously, the color of the markers represents the on-orbit times, 1, 5, 10 and 15 years from lighter to darker colors*)

By fixing the time (called here time horizon), the variations of the network efficiency and net gain are solely function of α_F as seen in Eqs (7.11), (7.12), (7.22) and (7.23). In the previous paragraph, only the 0.01–0.20 range was examined. The full range from 0 to 1 is examined in Figure 7.33 for the 2- and 3-IMLN architectures with a time horizon of 15 years (α_F becoming α_F^{15} in the equations mentioned above[17]).

[17] Generating Figure 7.33 for times other than 15 years here is more delicate, but feasible: the values of α_F at other times used in the equations need to be consistent with the Weibull distributions for α_F.

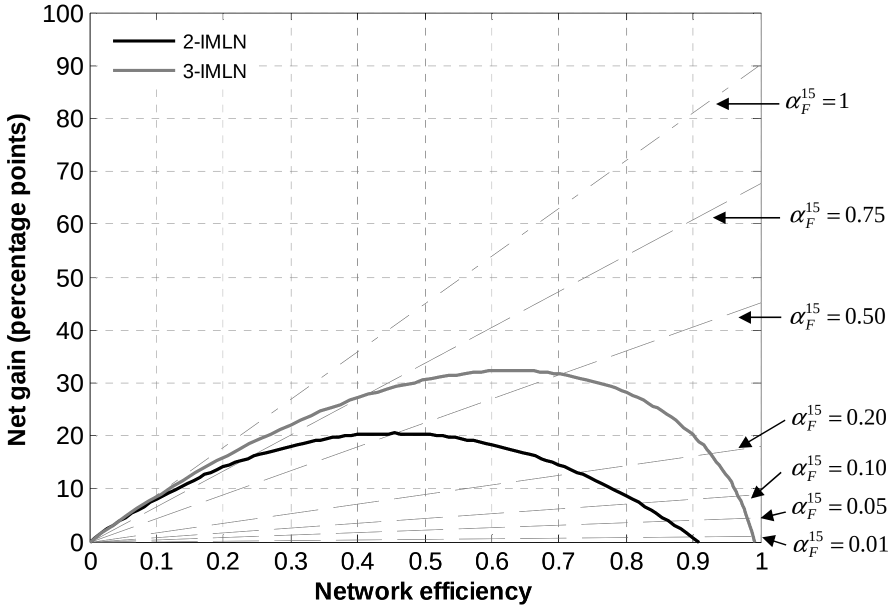


Figure 7.33. Variations of network efficiency versus net gain for a time horizon of 15 years

Figure 7.33 reads as follows: the black curve represents the 2-IMLN architecture, while the grey curve represents the 3-IMLN one. The dashed lines represent different values for α_F^{15}, the upper one being represented with a different type of dashed line as it is the limiting case. Indeed, a pair of network efficiency and net gain in the space above that line is not physically possible. Looking at the 0.50 dashed line, the values for the network efficiency and net gain for the 2-IMLN and 3-IMLN can be read: (0.455, 20.5) for the 2-IMLN and (0.703, 31.6) for the 3-IMLN.

If the probability of failure of the networkable subsystem/technology is known and fixed, then adding more spacecraft to the network make the pair (network efficiency, net gain) moves up and right along the associated dashed line for a specified time horizon.

Another effect can be noted on Figure 7.33: for each architecture, a unique maximum for the net gain exists for a specific value of α_F^{15}: 0.50 for the 2-IMLN maximum net gain of 20.5 percentage points (with an associated efficiency of 0.455) and 0.58 for the 3-IMLN maximum net gain of 32.3 percentage points (with an associated efficiency of 0.629). This means that **for a specific time horizon, space-based networks have a limiting capability to handle the failure of the networkable subsystem/technology (this limited capability increasing with the size of the network), over which the advantages of the network fade**. For example here, a probability of failure at 15 years superior to 0.50 for the networked subsystem/technology results in a net gain for the 2-IMLN smaller than the maximum value and on a decreasing trend (higher α_F^{15} will result in decreasing net gain values).

Families of curves for different types of network can be generated in the same fashion on Figure 7.33 and are of great help to inform the selection of a space architecture, by providing network efficiency and net gain trends and values. Indeed, these trends and values can be mapped to the risk tolerance of the shareholders and complementary cost studies can bring the last piece to choose an "optimal" solution.

7.3.6. Impact of Variations in the Probability of Failure of the Supporting Subsystems

In the subsections above, the probabilities of failure for the supporting subsystems and the payload were assumed to be equal to the ones derived from our sample of the SpaceTrak database (hereafter referred to as "nominal" case). However, these probabilities might be different for some specialized space platforms and this section investigates the impact on the efficiency of the network if these probabilities are changed. It can be seen in Eqs. (7.22) and (7.23) that the efficiency of the networks under consideration actually depends only on the probability of failure of the supporting subsystems, and not on the one of the payload. Assuming that the probability of failure of the supporting subsystems at 15 years varies by ±20% from the nominal case, while keeping the same shape parameter (β_S = 0.5181), the new values for the scale parameter are: $\theta_S^{F+} = 969$ years and $\theta_S^{F-} = 2202$ years. Generating again the network efficiencies for the 2-IMLN and 3-IMLN architectures for $\alpha_F^{15} = 0.05$ and $\alpha_F^{15} = 0.20$ yields the following results, shown in Figure 7.34 and Figure 7.35.

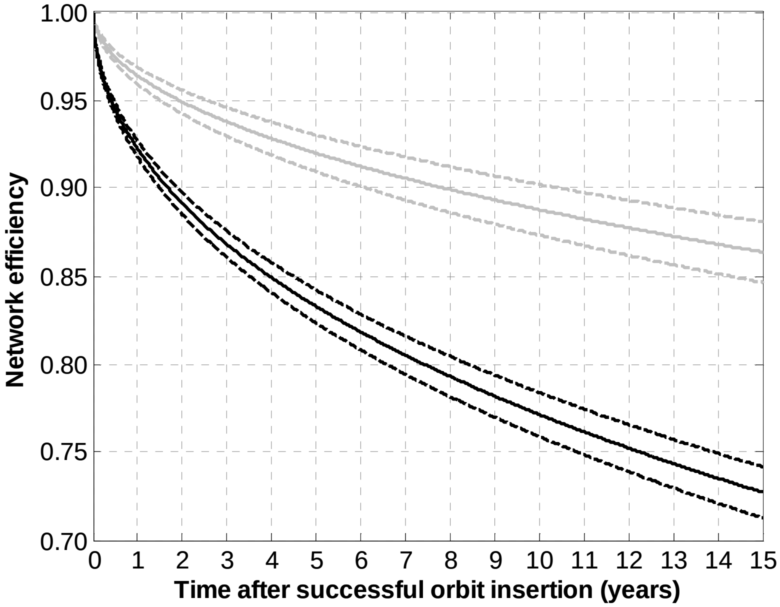


Figure 7.34. Effect of a ±20% variation in P_S^F on the 2-IMLN efficiency

(*The "nominal" case is represented with solid lines and the "perturbed" cases are represented with dashed lines. The family of grey curves represents the* $\alpha_F^{15} = 0.05$ *and the family of black curves corresponds to* $\alpha_F^{15} = 0.20$)

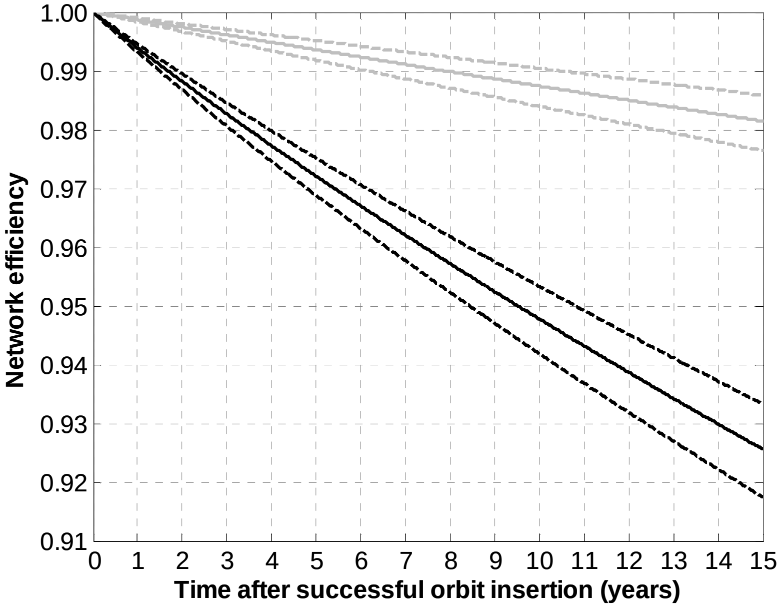


Figure 7.35. Effect of a ±20% variation in P_S^F on the 3-IMLN efficiency

(*Same formatting than the previous figure*)

The maximum deviation from the nominal case occurs at 15 years and is equal to 2% for the 2-IMLN and 0.4% for the 3-IMLN at $\alpha_F^{15} = 0.05$, 2% for the 2-IMLN and 0.8% for the 3-IMLN at $\alpha_F^{15} = 0.20$. As a consequence, the efficiency results change but remains close to the nominal case. Thus, the results presented in the previous section give a good approximation for the trends of the network efficiency.

7.3.7. Impact of the Probability of Failure of the Wireless Link Between Spacecraft

Another assumption made in the previous sections was related to the perfect reliability of the wireless link between spacecraft. In reality, this may not be the case, and, as a result, the survivability advantages of the space-based network over the monolith spacecraft may not be fully realizable. This section investigates the impact of an imperfect wireless link on the network efficiencies and net gains. Let assume that the wireless link between spacecraft is generated by two units in each spacecraft: the link works only if both units work (no link attenuation from distance for example is considered). The probability of failure of the link is labeled as $\upsilon_F(t)$, and the probability of failure of the unit i is labeled $P_{\mathrm{U}i}^{F}$. The two probabilities are related as follows:

$$\upsilon_F(t) = 1 - \left(1 - P_{\mathrm{U1}}^{F}\right)\left(1 - P_{\mathrm{U2}}^{F}\right) \tag{7.24}$$

Two types of distributions are considered for $P_{\mathrm{U}i}^{F}$: exponential and single Weibull. For the exponential distribution, the probability of failure of the unit is expressed as:

$$P_{\mathrm{U}i}^{F} = 1 - \exp\left(-\frac{t}{\mu_{F,i}}\right) \tag{7.25}$$

For a 2-IMLN with identical wireless units on both spacecraft:

$$\upsilon_F(t) = 1 - \exp\left(-\frac{t}{\left(\mu_F / 2\right)}\right) \tag{7.26}$$

As was done with α_F, υ_F is parameterized according to its values at 15 years, labeled υ_F^{15}: 0.05, 0.10, 0.20, 0.50, 0.90. The associated values for μ_F are given in Table 7.9.

Table 7.9. Exponential parameter values for the wireless link's failure behavior

$\boldsymbol{\upsilon_F^{15}}$	**Exponential mean parameter $\boldsymbol{\mu_F}$**
	years
0.05	584.8
0.10	284.8
0.20	134.4
0.50	43.28
0.90	13.02

The probability of failure given in Eq. (7.4) for the 2-IMLN can be modified to include the probability of failure of the link between the spacecraft as follows:

$$P^F_{\text{2-IMLN},\upsilon} = 1 - \left(1 - P_S^F\right)\left(1 - P_P^F\right)\left\{1 - \left(1 - \left(1 - \alpha_F\right)\left(1 - P_S^F\right)\left(1 - \upsilon_F\right)\right)\alpha_F\right\} \tag{7.27}$$

This equation can be reduced to (as done for Eq. (7.9)):

$$\begin{aligned} P^F_{\text{2-IMLN},\upsilon} = {} & \left(\alpha_F\right)^2\left(1 - P_S^F\right)^2\left(1 - P_P^F\right)\left(1 - \upsilon_F\right) + \alpha_F\left[1 - \left(1 - P_S^F\right)\left(1 - \upsilon_F\right)\right]\left(1 - P_S^F\right)\left(1 - P_P^F\right) \\ & + 1 - \left(1 - P_S^F\right)\left(1 - P_P^F\right) \end{aligned} \tag{7.28}$$

2-IMLN architecture's probability of complete failure – exponential case. Let us look at an example: assuming $\alpha_F^{15} = 0.05$, and $\upsilon_F^{15} = 0.50$ (the link has a 50% chance to be operational after 15 years), Figure 7.36 gives the probabilities of failure of the monolith architecture, of the 2-IMLN architecture with a perfect link ($\upsilon_F^{15} = 0$), and of the 2-IMLN with a 50% reliability link after 15 years ($\upsilon_F^{15} = 0.50$).

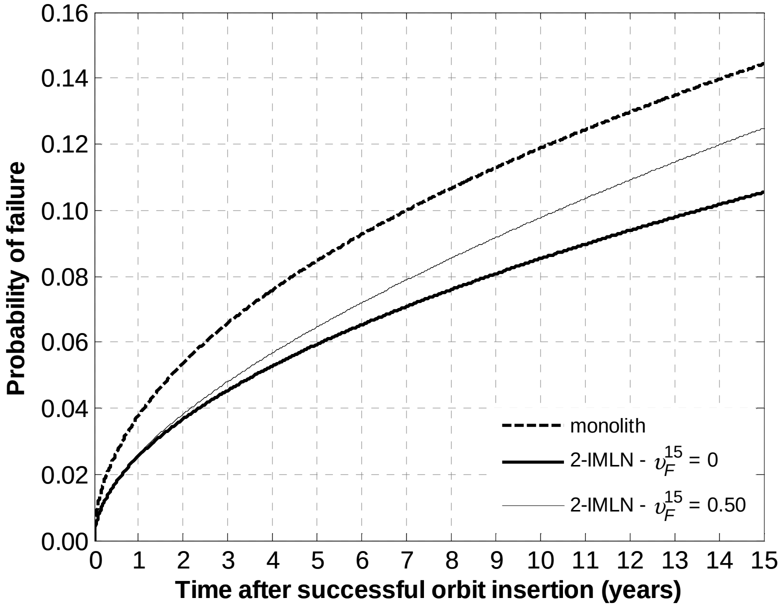


Figure 7.36. Impact of an imperfect link (exponential case)

Figure 7.36 clearly show that the probability of a complete failure is significantly impacted by the unreliability of the link: the two curves for the 2-IMLN architecture depart from each other from year 2 approximately. The gap continuously increases in time as the imperfect link curve tends towards the monolith curve. At 15 years, the probability of failure of the 2-IMLN with a 50% unreliable link is 0.125, compared to the perfect link case at 0.105. The monolith probability of total failure at 15 years is 0.144: as a consequence, of the 3.9 percentage point improvement by considering an ideal 2-IMLN, only 1.9 percentage points are effectively realized with a 50% reliable link.

2-IMLN architecture's net gain and efficiency – exponential case. Equations for the net gain and network efficiency can also be derived in this particular case as done previously:

$$\Delta^{F}_{\text{2-IMLN},\upsilon} = \left(1 - P_S^F\right)^2 \left(1 - P_P^F\right)\left(1 - \upsilon_F\right)\left(1 - \alpha_F\right)\alpha_F \tag{7.29}$$

$$\eta^{F}_{\text{2-IMLN},\upsilon} = \left(1 - P_S^F\right)\left(1 - \upsilon_F\right)\left(1 - \alpha_F\right)\alpha_F \tag{7.30}$$

Figure 7.37 shows the impact of an imperfect link on the network efficiency of the 2-IMLN architecture in the case $\alpha_F^{15} = 0.05$. For low values of υ_F^{15}, the efficiency remains close to its ideal value: for a link reliability around the same order of reliability of spacecraft subsystems, the efficiency slightly dropped to 0.821 for $\upsilon_F^{15} = 0.05$ from its ideal value of 0.864, or to 0.777 for $\upsilon_F^{15} = 0.10$. However, the efficiency dramatically drops with an significant increase in υ_F^{15}: with a 50% chance of link failure at 15 years ($\upsilon_F^{15} = 0.50$), the efficiency dropped to 0.432 from its ideal value of 0.864; in a more extreme case, with a 10% of still working after 15 years ($\upsilon_F^{15} = 0.90$), the efficiency is down to 0.086. As a consequence, the **reliability of the link is critical in capturing the survivability advantages of the space-based networks**.

The information about the net gain is also of interest to assess the interest of an architecture. Combing the results about the efficiency above with net gain calculations, the *η*–Δ graph can be generated and is given in Figure 7.38.

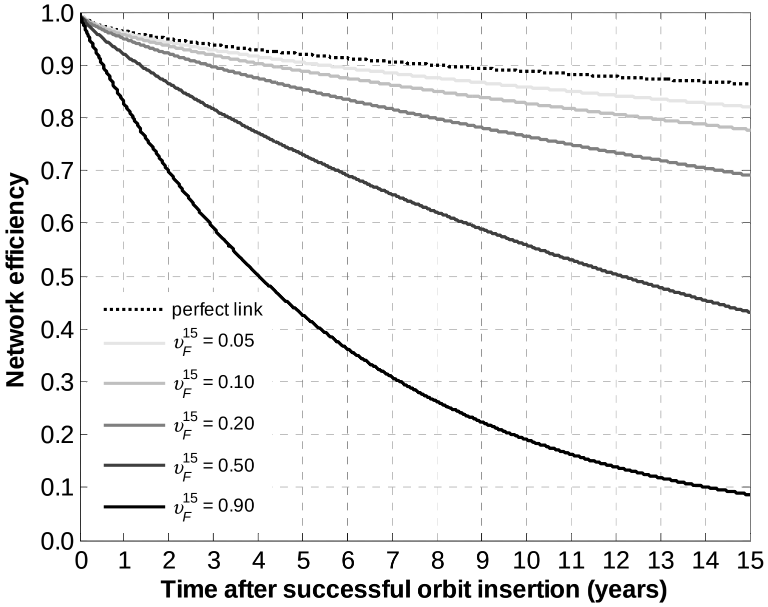


Figure 7.37. Impact of the link unreliability on the 2-IMLN efficiency ($\alpha_F^{15} = 0.05$)

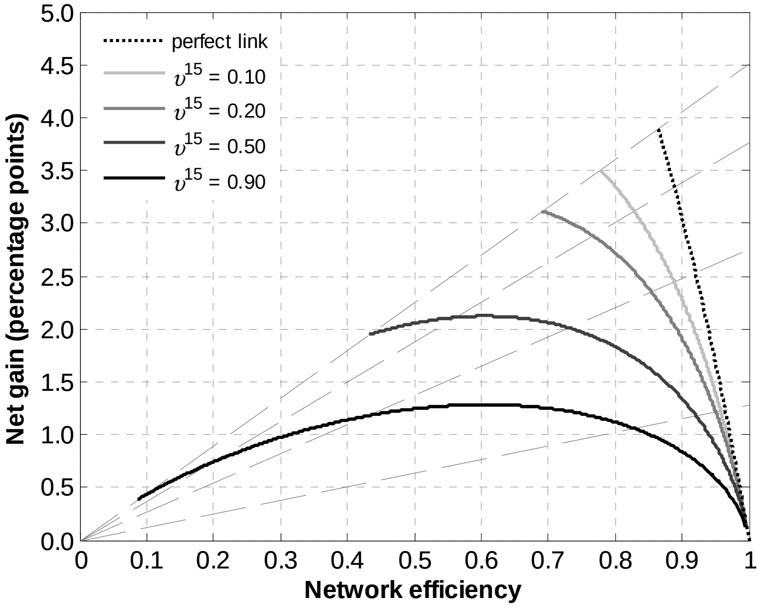


Figure 7.38. Variation of the probability of failure of the link (exponential, $\alpha_F^{15} = 0.05$)

Figure 7.38 shows a family of curves for the $\alpha_F^{15} = 0.05$ case with the dashed lines representing four on-orbit times: 1, 5, 10 and 15 years from the lower line to the upper one. Increasing υ_F^{15} results in a decrease in efficiency as seen in the previous figure. An additional piece of information yields with the net gain: the higher the probability of failure of the link, the smaller the net gain of the architecture. For the 0.10 and 0.20 cases, the maximum gain is obtained at 15 years, while the 0.50 maximum gain is reached at about 9 years and the 0.90 maximum gain at about 3 years. In the last two cases, the maximum gain is not reached at the end of the observation period, indicating a time horizon for an "effective performance" of the network. For example, in the case of $\upsilon_F^{15} = 0.90$, the network becomes less attractive past 3 years and the net gain captured continuously decline past that point.

2-IMLN architecture's probability of complete failure – Weibull case. The failure of the link was assumed to be exponential above. A more flexible distribution to model the link failure is the Weibull distribution. Two types of failure behavior are investigated in the following: an infant mortality behavior with a shape parameter equal to 0.5 (less than 1), and a wear-out behavior with a shape parameter of 3 (more than 1). In the case of the single Weibull distribution, the probability of failure of the unit can be expressed as:

$$P_{\mathrm{U}i}^F = 1 - \exp\left(-\left(\frac{t}{\theta_{\mathrm{U}i}^F} \right)^{\beta_{\mathrm{U}i}^F} \right) \tag{7.31}$$

For a 2-IMLN with identical wireless units on both spacecraft:

$$\upsilon_F(t) = 1 - \left[\exp\left(-\left(\frac{t}{\theta_U^F} \right)^{\beta_U^F} \right) \right]^2 \tag{7.32}$$

This can be further reduced to:

$$\upsilon_F(t) = 1 - \exp\left(-\left(\frac{t}{\left(\theta_U^F \big/ 2^{\left(1/\beta_U^F\right)} \right)} \right)^{\beta_U^F} \right) \tag{7.33}$$

An illustrative case is explored around $\upsilon_F^{15} = 0.50$: the values of the shape and scale parameter for the Weibull distribution are given in Table 7.10.

Table 7.10. Weibull parameters values for the wireless link's failure behavior

$\boldsymbol{\upsilon_F^{15}}$	**Weibull shape parameter $\boldsymbol{\beta}$**	**Weibull scale parameter $\boldsymbol{\theta}$**
		years
0.50	0.5	124.88
	3	21.36

The probability of failure of the 2-IMLN architecture can be computed and is shown in Figure 7.39.

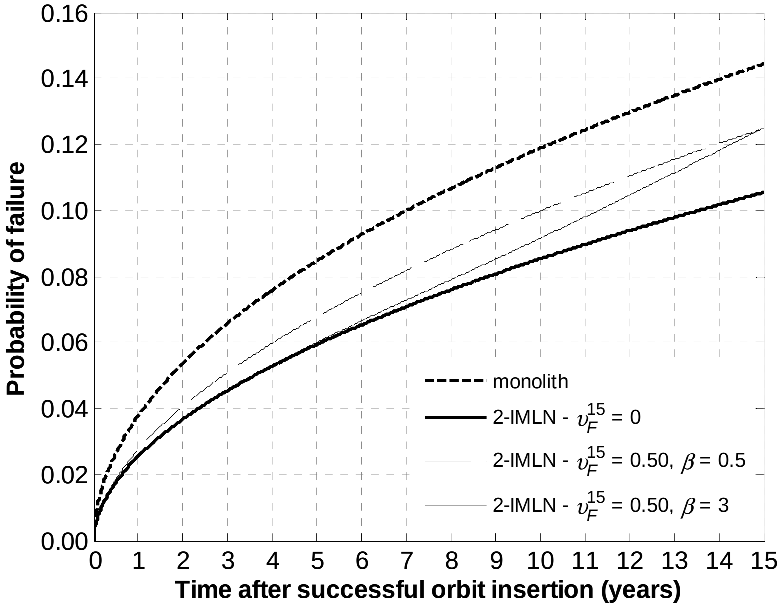


Figure 7.39. Impact of an imperfect link (Weibull case)

As it was the case above with the exponential failure distribution, the probability of failure for the 2-IMLN architecture with an imperfect link diverges from its ideal case, for both failure behavior (infant mortality and wear-out). The divergence however does not occur at the same time for the two failure behaviors: in the case of the infant mortality, the gap between the curves become noticeable before 1 year on-orbit, while in the case of a wear-out behavior, the divergence occurs between year 5 and 6. Thus it is clearly shown that an infant mortality behavior for the link will be significantly more problematic than the wear-out behavior. Despite the fact that at 15 years, both failure behaviors result in the same probability of failure, the wear-out case allowed to fully capture the survivability advantage of the space-based network for the first 5 years on orbit. As a consequence, **infant mortality failures in the link should be rooted out for the space-based network option to be of interest**.

2-IMLN architecture's net gain and efficiency – Weibull case. The trend mentioned above can also be shown with the evolution of network efficiency in time shown in Figure 7.40. Figure 7.40 presents the ideal 2-IMLN efficiency (link with a perfect reliability), the exponential link failure case (β = 1 makes the Weibull distribution equivalent to the exponential distribution), the infant mortality case (β = 0.5) and the wear-out failure case (β = 3). It can be seen on the figure that increasing the shape parameter β from 1 results in shifting the efficiency curve towards the right (hence retaining higher efficiency value at the same on-orbit time), while decreasing the shape parameter from 1 results in shifting the efficiency curve towards the left (and hence worsening the efficiency at a comparable on-orbit time).

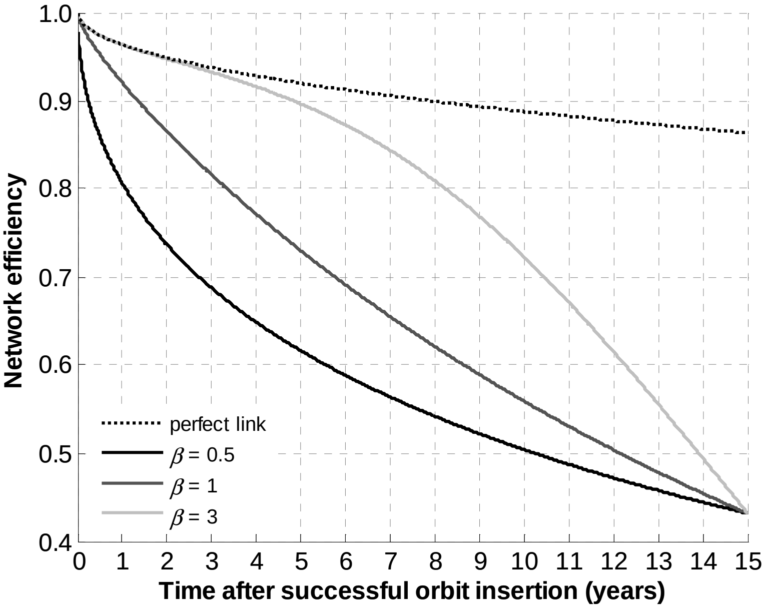


Figure 7.40. Impact of the link unreliability on the 2-IMLN efficiency ($\alpha_F^{15} = 0.05$ and $\upsilon_F^{15} = 0.50$)

Including the information about the net gain, the associated η–Δ graph can be generated as shown in Figure 7.41. Again, the dashed lines represent four on-orbit times: 1, 5, 10 and 15 years from the lower line to the upper one. An additional figure is given, Figure 7.42, to give a comparative case with a less problematic link ($\upsilon_F^{15} = 0.10$) relative to the case studied above ($\upsilon_F^{15} = 0.50$).

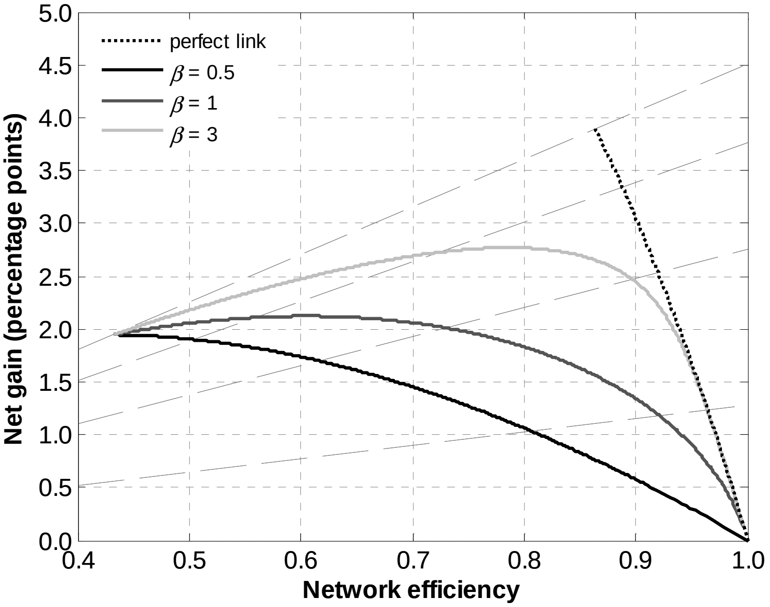


Figure 7.41. η–Δ graph for the 2-IMLN with an imperfect link, $\upsilon_F^{15} = 0.50$

(exponential and Weibull cases)

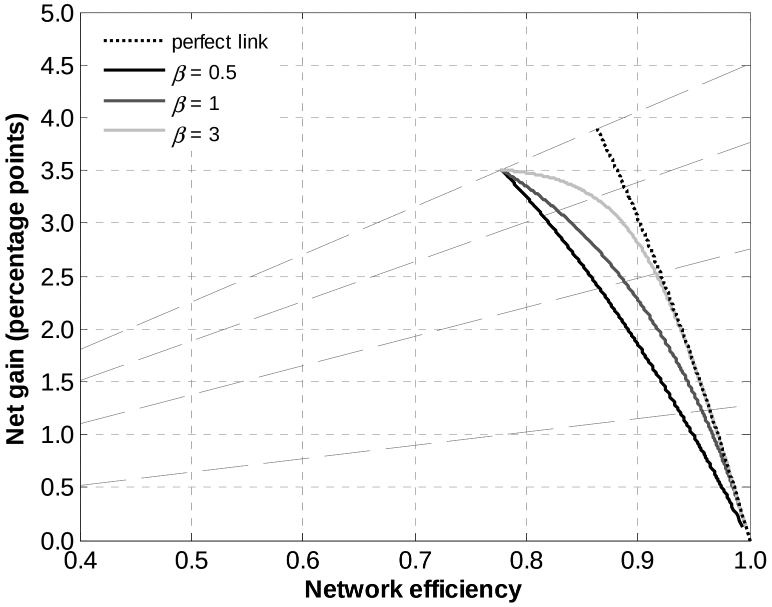


Figure 7.42. η–Δ graph for the 2-IMLN with an imperfect link, $\upsilon_F^{15} = 0.10$

Figure 7.41 and Figure 7.42 confirm that the infant mortality case is the worst in terms of network efficiency and net gain. However, in the case of a more problematic link (i.e., a link that fails more), the difference between the infant mortality case and the wear-out behavior is more pronounced (Figure 7.41 versus Figure 7.42). As a consequence, **the more the link fails, the more critical the infant mortality failures become**. In addition, note that in the $\upsilon_F^{15} = 0.50$ case, a maximum in the net gain appears for the wear-out and exponential cases around 9 years on-orbit. This could indicate that a time horizon for a true effective performance of the network can be defined in these cases. Finally, it can be seen that varying the failure behavior of the link from $\upsilon_F^{15} = 0.50$ to 0.10 results in shifting the end points of the efficiency–net gain curves along the 15-year dashed line, as seen in Figure 7.38.

All the figures above were generated such that the probability of failure of the networked subsystem/technology is equal to 0.05 after 15 years ($\alpha_F^{15} = 0.05$). A final examination of the behavior of the 2-IMLN network with respect to the link failure is to explore whether the sensitivity of the efficiency to the failure of the networked subsystem/technology is impacted by the failure of the link (exponential case), and this is shown in Figure 7.43.

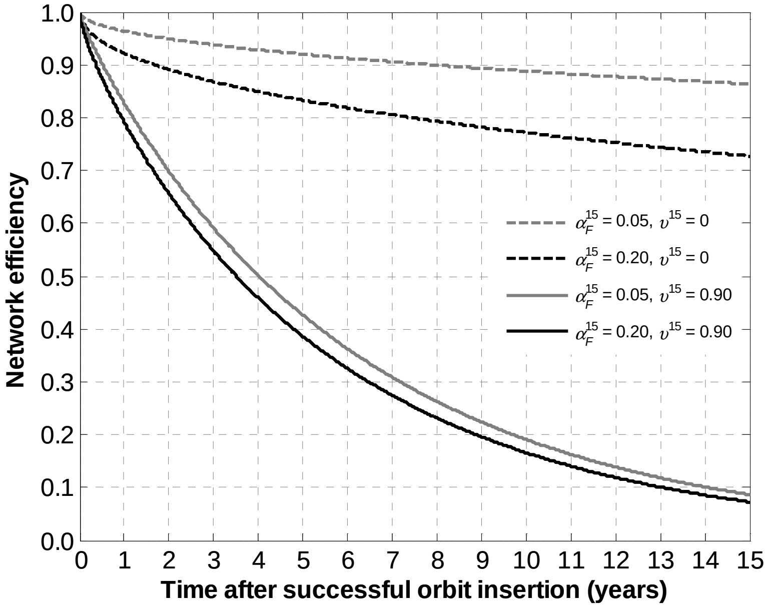


Figure 7.43. 2-IMLN efficiency variations due to the failures of the networked subsystem/technology and link

It can be seen in Figure 7.43 that in a perfect link situation, the 2-IMLN efficiency drops from 0.864 to 0.727 at 15 years due to the increase in the failure behavior of the networked subsystem/technology (α_F^{15} from 0.05 to 0.20), a 16% variation. Considering now a link that has a 90% chance of failing by 15 years, the same variation in α_F^{15} results in a drop from 0.086 to 0.073, a similar relative variation. However, the impact on the absolute numbers dramatically changed: the difference in efficiency for a network with a problematic link is smaller than for a healthy link. This is consistent with the fact that the more failure-prone the link is, the less networked the spacecraft are, and the less relevant the failure of the networked subsystem/technology is. Note that α_F and υ_F have a similar role on efficiency as shown in Eq. (7.30).

3-IMLN architecture. The previous results were generated for the 2-IMLN architecture. In the case of the 3-IMLN, the analytical solution is not obvious or possible, and the IMLN simulation is the only solution to generate the probability of failure of the network in presence of link failure. Indeed, the two links in the 3-IMLN do not fail independently: the failure of the wireless unit on board of the main spacecraft (with the payload) causes the failure of both links. Hence the time to failure of the links are computed by generating the times to failure of the 3 units, and taking the minimum of the times to failure of the two respective units for both links. The IMLN model handles very easily this computation and the probability of failure of the system, the network efficiency and the net gain can be simulated. In the case of $\alpha_F^{15} = 0.05$, three simulations were run, for υ_F^{15} equal to 0.20, 0.50 and 0.90 (exponential distributions with parameters given in Table 7.9) to obtain a representative sample of the impact of the link failures on the 3-IMLN architecture, presented in Figure 7.44.

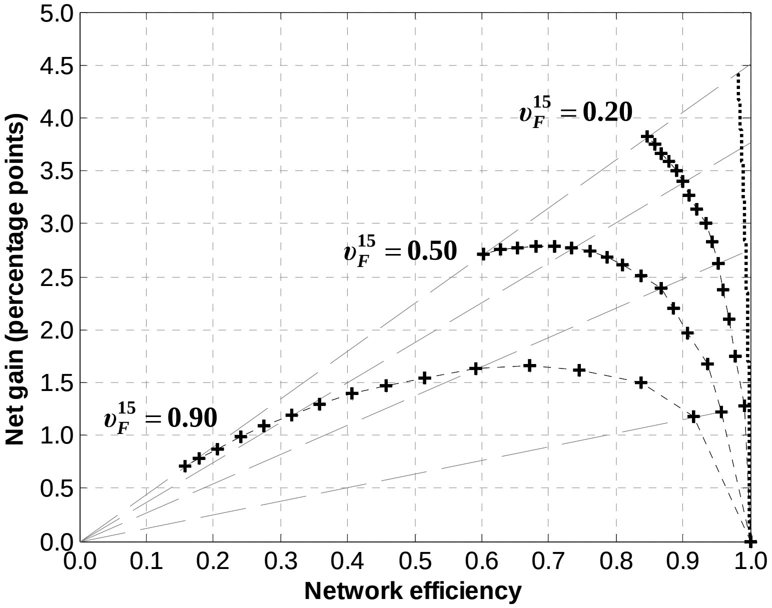


Figure 7.44. η–Δ graph for the 3-IMLN with an imperfect link (exponential case)

Figure 7.44 presents four curves: the black dotted line without “plus” markers is the perfect case (i.e., the links are perfectly reliable), and the curves with “plus” markers are the cases with links prone to failure. For readability purposes, it was chosen to output the results of the simulation every on-orbit year (15 markers per curve for 15 years spent on-orbit). The black short-dash lines link the markers on a curve, but do not represent results from the simulation (their unique purpose is to highlight the curve). Figure 7.44 shows that the 3-IMLN architecture is also affected by the failure of the links, although to a lesser extent than the 2-IMLN, as demonstrated in Figure 7.45 for $v_F^{15} = 0.50$.

Finally, Weibull distributions were considered for the link failure behavior, with the Weibull parameters given in Table 7.10. Similar comments than for the 2-IMLN can be made regarding the results of Figure 7.46.

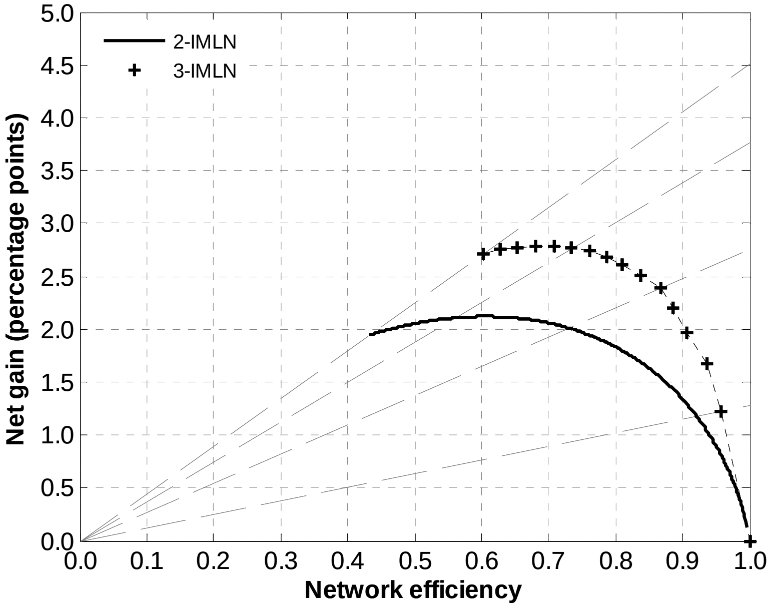


Figure 7.45. Comparison of the 2- and 3-IMLN architectures with link failures (exponential case)

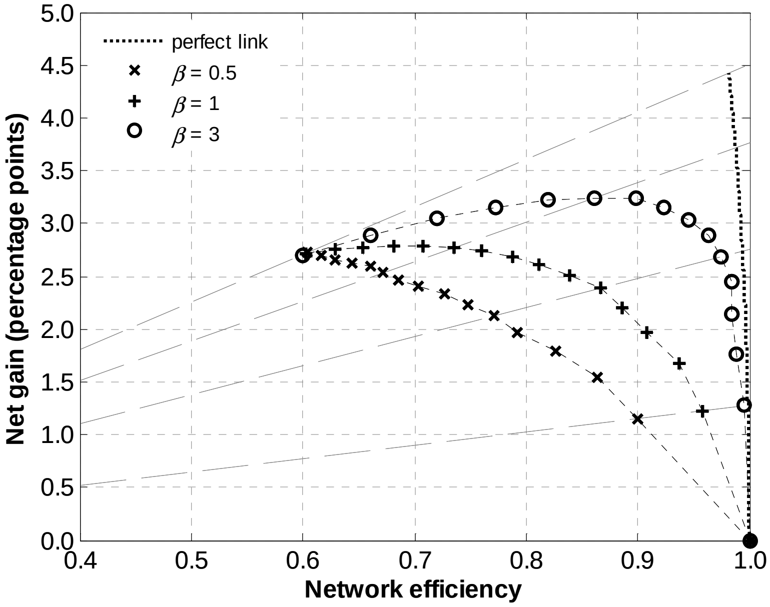


Figure 7.46. η–Δ graph for the 3-IMLN with an imperfect link, $\upsilon_F^{15} = 0.50$

(exponential and Weibull cases)

7.3.8. Multi-State Considerations: IMLN Behavior Facing Major Degradation

Up to this point, section 7.3 considered only the catastrophic failure of the monolith or space-based network architectures. However, as mentioned in earlier chapters and in section 7.2, other types of events can occur on-board the space systems that lead to a degradation of its functionality, and not necessary its complete loss. In this subsection, another level of severity in the performance degradation is investigated, namely, the major degradation state. Assuming that the probability of major degradation of the networked subsystem/technology is given by $\alpha_M(t)$, the impact of such an event is investigated in a similar fashion than for the complete failure, by parameterizing the value of the probability of major degradation at 15 years: $\alpha_M(t = 15\,\text{years}) = \alpha_M^{15}$. Four levels are explored in this subsection, with α_M^{15} equal to 0.05, 0.10, 0.15, 0.20.

This probability α_M is not directly useable in the IMLN model and simulation, as explained in Chapter 5. The state considered in the simulation is not the “major degradation” state directly, but the aggregation of the “major degradation” and “total failure” states into the “major–failed” state (also referred to as “severe degradation” state). The probability of being in a major degradation state for the space architecture is then calculated by taking the difference between the probability of being in the aggregated major–failed state, labeled $\alpha_{MF}(t)$, and the probability of being in the total failure state (simulated in the previous subsections), as evidenced by Eq. (5.40). In similar fashion, we have for α_F, α_M and α_{MF}:

$$\alpha_M(t) = \alpha_{MF}(t) - \alpha_F(t) \tag{7.34}$$

Note that the value of α_{MF} is bounded by 1, constraining the values α_F and α_M can take concurrently ($\alpha_F^{15} = 0.6$ and $\alpha_M^{15} = 0.7$ at the same time is not physically possible).

To investigate potential changes in the probability of major degradation for the space architecture due to variations in the probability of total failure of the networkable subsystem/technology, two levels for α_F^{15} were chosen, representative of subsystems/technologies with lower or higher tendency to complete failures: 0.05 and 0.20. Table 7.11 presents a summary of the levels used in the following simulations. It is interesting to note that the α_{MF}^{15} value of 0.25 can be obtained by two different combinations of α_F^{15} and α_M^{15} ((0.05, 0.20) and (0.20, 0.05) respectively).

Table 7.11. Parameterization of the failed, major and major–failed probabilities

$\boldsymbol{\alpha_F^{15}}$	$\boldsymbol{\alpha_M^{15}}$	$\boldsymbol{\alpha_{MF}^{15}}$
0.05	0.05	0.10
	0.10	0.15
	0.15	0.20
	0.20	0.25
0.20	0.05	0.25
	0.10	0.30
	0.15	0.35
	0.20	0.40

As done for the probability of failure of the networkable subsystem/technology, the probability of being in a major–failed state of the networkable subsystem/technology is modeled using single Weibull distributions (with a constant shape parameter $\beta = 0.5$), and the values of the scale parameters associated to the specified values are given in Table 7.12.

Table 7.12. Weibull scale parameter values for the α_{MF} distribution of the networked subsystem/technology

α_{MF}^{15}	Scale parameter θ_{MF}
	years
0.10	1,351
0.15	568
0.20	301
0.25	181
0.30	117.9
0.35	80.8
0.40	57.5

Using the IMLN models, simulations were run for each α_{MF}^{15} value, and generated as output the probability of being in a major–failed state of the space architecture (as previously: monolith, 2-IMLN and 3-IMLN). Also as done previously, analytical results can be found as the subscripts and superscripts "F" can be replaced by "MF" (except in some cases of the supporting subsystems probability[18]) in the equations derived for the probability of complete failure. They are modified as follows:

$$P_{\text{monolith}}^{MF} = 1 - \left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right)\alpha_{MF} \tag{7.35}$$

$$P_{\text{2-IMLN}}^{MF} = 1 - \left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right)\left\{1 - \left(1 - \left(1 - \alpha_{MF}\right)\left(1 - P_S^{F}\right)\right)\alpha_{MF}\right\} \tag{7.36}$$

[18] In the case of the functional redundancy, special attention must be given to the supporting subsystem state: the functional redundancy is inhibited only if the supporting subsystems fail completely, its major degradation having no impact in this representation.

$$P^{MF}_{\text{3-IMLN}} = 1 - \left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right)\left\{1 - \left(1 - \left(1 - \alpha_{MF}\right)\left(1 - P_S^{F}\right)\right)^2 \alpha_{MF}\right\} \tag{7.37}$$

For readability purposes again, four on-orbit times have been selected to compare architectures: 1 year, 5 years, 10 years and 15 years on-orbit. The probabilities of being in a major–failed state (in percentage points) for the three architectures at these times are shown in Table 7.13.

Table 7.13. Probabilities of being in a major–failed state for monolith and networked architectures (in percentage points)

α_{MF}^{15}	**Architecture**	P^{MF} **– IMLN simulation**				P^{MF} **– Analytical results**			
		Time spent on-orbit (years)				Time spent on-orbit (years)			
		1	5	10	15	1	5	10	15
0.10	Monolith	–	–	–	–	8.49	18.02	24.53	29.18
	2-IMLN	6.08	13.42	18.75	22.72	6.09	13.44	18.77	22.75
	3-IMLN	5.97	12.95	17.91	21.58	5.97	12.94	17.91	21.58
0.15	Monolith	–	–	–	–	9.83	20.68	27.97	33.12
	2-IMLN	6.20	13.94	19.67	23.98	6.21	13.95	19.69	24.00
	3-IMLN	5.98	13.04	18.12	21.93	5.98	13.03	18.12	21.92
0.20	Monolith	–	–	–	–	11.23	23.42	31.46	37.06
	2-IMLN	6.36	14.62	20.88	25.61	6.37	14.64	20.88	25.61
	3-IMLN	5.99	13.16	18.46	22.47	5.99	13.18	18.47	22.49
0.25	Monolith	–	–	–	–	12.70	26.22	34.98	41.00
	2-IMLN	6.58	15.49	22.35	27.56	6.59	15.52	22.37	27.58
	3-IMLN	6.04	13.41	18.99	23.31	6.02	13.40	18.99	23.31
0.30	Monolith	–	–	–	–	14.23	29.10	38.53	44.92
	2-IMLN	6.87	16.59	24.17	29.92	6.86	16.59	24.16	29.90
	3-IMLN	6.06	13.72	19.73	24.43	6.06	13.73	19.73	24.44
0.35	Monolith	–	–	–	–	15.86	32.07	42.15	48.86
	2-IMLN	7.20	17.90	26.25	32.58	7.21	17.89	26.26	32.58
	3-IMLN	6.13	14.20	20.72	25.92	6.12	14.19	20.72	25.92
0.40	Monolith	–	–	–	–	17.58	35.13	45.80	52.79
	2-IMLN	7.64	19.42	28.68	35.61	7.63	19.43	28.69	35.62
	3-IMLN	6.20	14.82	22.03	27.82	6.20	14.81	22.02	27.81

It can be seen in Table 7.13 that the results from the IMLN simulation and from analytical solutions are in strong agreement: the average difference is 0.01 percentage point and the maximum difference is 0.03 percentage point. As given by Eq. (5.40), combining the results from Table 7.13 and Table 7.5 (probability of complete failure), the probability of being in a major degradation state for the architecture under consideration can be computed, and the final result is given in Table 7.14.

Table 7.14. Probabilities of being in a major degradation state for monolith and networked architectures (in percentage points)

α_F^{15}	α_M^{15}	α_{MF}^{15}	Architecture	P^M – IMLN simulation				P^M – Analytical results			
				Time spent on-orbit (years)				Time spent on-orbit (years)			
				1	5	10	15	1	5	10	15
0.05	0.05	0.10	Monolith	–	–	–	–	4.70	9.56	12.66	14.76
			2-IMLN	3.53	7.49	10.23	12.18	3.54	7.51	10.25	12.21
			3-IMLN	3.46	7.22	9.75	11.56	3.46	7.21	9.76	11.57
	0.10	0.15	Monolith	–	–	–	–	6.04	12.22	16.10	18.69
			2-IMLN	3.66	8.02	11.14	13.44	3.66	8.02	11.16	13.46
			3-IMLN	3.47	7.31	9.96	11.91	3.47	7.30	9.97	11.92
	0.15	0.20	Monolith	–	–	–	–	7.44	14.95	19.59	22.63
			2-IMLN	3.82	8.70	12.35	15.07	3.82	8.71	12.36	15.07
			3-IMLN	3.49	7.43	10.30	12.45	3.49	7.45	10.32	12.48
	0.20	0.25	Monolith	–	–	–	–	8.91	17.76	23.11	26.57
			2-IMLN	4.04	9.56	13.82	17.02	4.04	9.59	13.85	17.05
			3-IMLN	3.53	7.68	10.83	13.29	3.51	7.67	10.84	13.31
0.20	0.05	0.25	Monolith	–	–	–	–	4.73	9.11	11.57	13.06
			2-IMLN	3.64	7.86	10.74	12.71	3.66	7.90	10.77	12.74
			3-IMLN	3.50	7.38	10.08	12.04	3.48	7.37	10.09	12.05
	0.10	0.30	Monolith	–	–	–	–	6.27	11.98	15.12	16.98
			2-IMLN	3.93	8.96	12.56	15.07	3.94	8.98	12.56	15.06
			3-IMLN	3.52	7.69	10.82	13.16	3.52	7.70	10.82	13.18
	0.15	0.35	Monolith	–	–	–	–	7.90	14.96	18.73	20.92
			2-IMLN	4.26	10.27	14.64	17.74	4.28	10.28	14.66	17.75
			3-IMLN	3.60	8.16	11.81	14.66	3.58	8.16	11.82	14.66
	0.20	0.40	Monolith	–	–	–	–	9.62	18.02	22.38	24.84
			2-IMLN	4.70	11.79	17.07	20.76	4.70	11.82	17.09	20.78
			3-IMLN	3.66	8.79	13.12	16.55	3.67	8.78	13.12	16.55

A more practical representation of the results presented in Table 7.5, Table 7.13 and Table 7.14 is shown in Figure 7.47, for the case $\alpha_{MF}^{15} = 0.10$ ($\alpha_F^{15} = 0.05$ and $\alpha_M^{15} = 0.05$) for example.

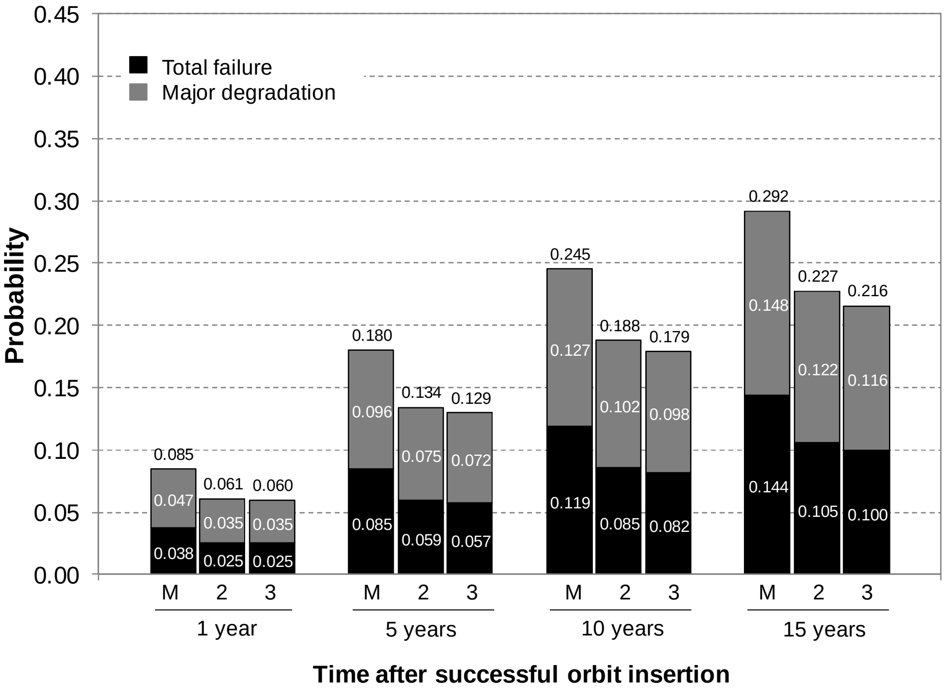


Figure 7.47. Probabilities of complete failure and major degradation for monolith and networked architectures

Figure 7.47 reads as follows. For each of the four on-orbit times, three bars are represented: the leftmost of the three represents the monolith architecture (“M” on the figure), the middle bar represents the 2-IMLN architecture (“2”) and the rightmost bar of the three represents the 3-IMLN architecture (“3”). The numbers associated with the black part of the stacked bars represent the probability of catastrophic failure of the associated architecture, while the grey part of the stacked bars represents the probability of being in a major degradation state for the associated architecture. As a consequence, the numbers on top of the bars resulting from the addition of the other two represent the probability of being in a major–failed state (or severe degradation state) for the architecture of interest. An example of the information read on the figure is, after 5 years on-orbit:

- The monolith architecture has a probability of being in a failed state (P^F) of 8.46%, a major degradation state (P^M) of 9.56% and a total probability of being in a severe degradation state (P^{MF}) of 18.02%;
- The 2-IMLN architecture has a probability of being in a failed state of 5.93%, a major degradation state of 7.51% and a total probability of being in a severe degradation state of 13.44%;
- The 3-IMLN architecture has a probability of being in a failed state of 5.73%, a major degradation state of 7.21% and a total probability of being in a severe degradation state of 12.94%.

In this particular case, the space-based networks improve on both the failed and the major degradation states, but with a small difference between the networks of 2 and 3 spacecraft.

The next step consists in looking at results in Table 7.13 and Table 7.14 obtained by increasing α_M^{15} while keeping α_F^{15} constant, to observe the effect of increasing the probability of being in a major degradation state for the networkable subsystem/technology on the system level. The resulting change is presented in Figure 7.48, with $\alpha_{MF}^{15} = 0.25$ ($\alpha_F^{15} = 0.20$ and $\alpha_M^{15} = 0.05$): α_M^{15} was increased from 0.05 to 0.20, while keeping α_F^{15} constant at 0.05.

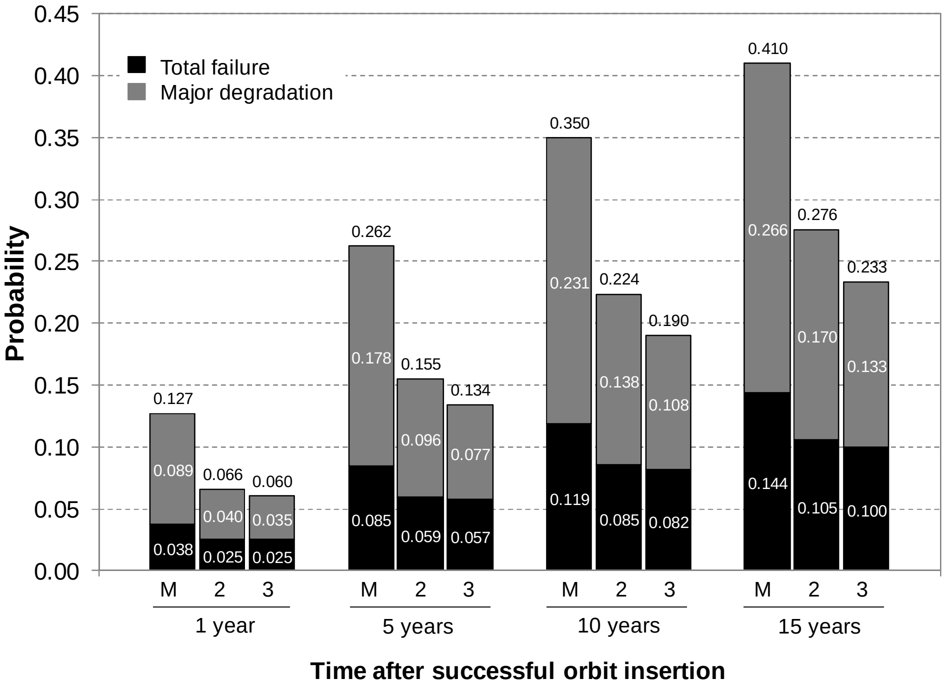


Figure 7.48. Increase in the probability of major degradation for the networkable subsystem/technology

As expected, the probability P^M (represented in grey) has increased while P^F (in black) remained constant: from Figure 7.47 where, at 5 years on-orbit, P^M for the monolith was equal to 9.56%, it is now 17.76%; in the case of the 2-IMLN, it went from 7.51% to 9.59% and for the 3-IMLN, it increased from 7.21% to 7.67%. Note that the increase was the most dramatic for the monolith spacecraft, while the 3-IMLN was the least affected. This result mirrors the behavior of the networks in the case of total failures. Also note that for higher α_M^{15}, the difference between architecture becomes more apparent: for example at 15 years, there is now a difference of 4.27 percentage points in P^{MF}, while it was only 1.17 percentage points for $\alpha_M^{15} = 0.05$.

Let investigate the complementary effect: keeping α_M^{15} fixed at 0.05 (as in Figure 7.47), let us increase α_F^{15} from 0.05 to 0.20. This is shown in Figure 7.49.

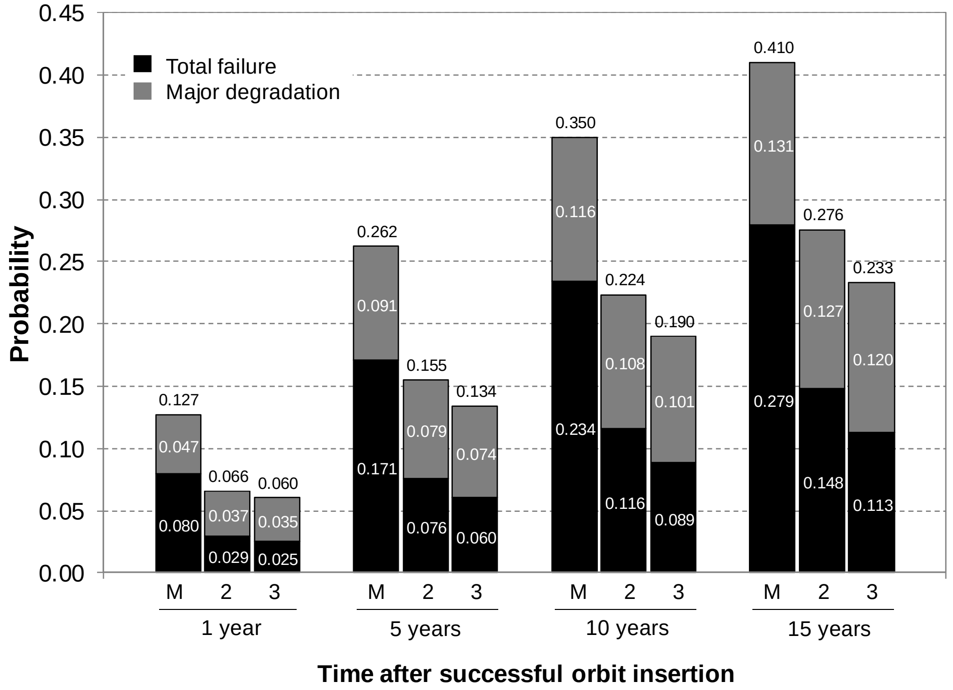


Figure 7.49. Increase in the probability of total failure for the networkable subsystem/technology

Several interesting phenomena occur in Figure 7.49. First, as the combination of α_F^{15} and α_M^{15} were chosen to add up to 0.25, the same α_{MF}^{15} than in Figure 7.48 (obtained with the reverse combination), the probabilities of being in a major–failed state (P^{MF}, given by the numbers on top of the stacked bars) for the three architectures are the same than in Figure 7.48. The splits between the black share and the grey share changed to accommodate for the new degradation and failure behavior of the networked subsystem/technology: P^F increased (in black) while P^M (in grey decreased). A more interesting finding lies in carefully examining Figure 7.47 and Figure 7.49: in both cases, $\alpha_M^{15} = 0.05$; the variable is

α_F^{15} which increased from 0.05 to 0.20. As expected, P^F increased, but P^M was also impacted: for example, after 15 years, the probability of major degradation for the monolith architecture shifted from 14.76% to 13.06%, from 12.21% to 12.74% for the 2-IMLN and from 11.57% to 12.05% for the 3-IMLN. This implies that for a constant probability of major degradation for the networkable subsystem/technology (α_M), the probability of major degradation of the complete architecture is affected by the variation in the probability of total failure of the networkable subsystem/technology (α_F). As a consequence, ***P*^{M} is not solely a function of α_M, but depends on both α_M and α_F**.

As mentioned above, and similarly for catastrophic failures, the space-based networks studied here are less sensitive to the variation in the degradation and failure behavior of the networkable subsystem/technology. This shielding effect from major anomalies and failures is clearly shown in Figure 7.50 (*t* = 5 years).

In the worst-case scenario here after 5 years on-orbit with $\left(\alpha_F^{15}, \alpha_M^{15}\right) = (0.20{,}0.20)$, P^M varies by 151% for the monolith (from an ideal value of 7.17% (perfect subsystem/technology, with no anomaly or failures, i.e., $\left(\alpha_F^{15}, \alpha_M^{15}\right) = (0{,}0)$) to 18.02%), by 65% for the 2-IMLN (from the ideal value of 7.17% to 11.82%) and by 22% for the 3-IMLN architecture (from the ideal value of 7.17% to 8.78%). Overall, the probability of severe degradation for the space system, P^{MF}, varies by 173% for the monolith, 51% for the 2-IMLN and 15% for the 3-IMLN. As a conclusion, **the networked architectures confirm their “shielding effect” for severe anomalies in addition to failures, and this effect grows stronger with the addition of spacecraft to the network**.

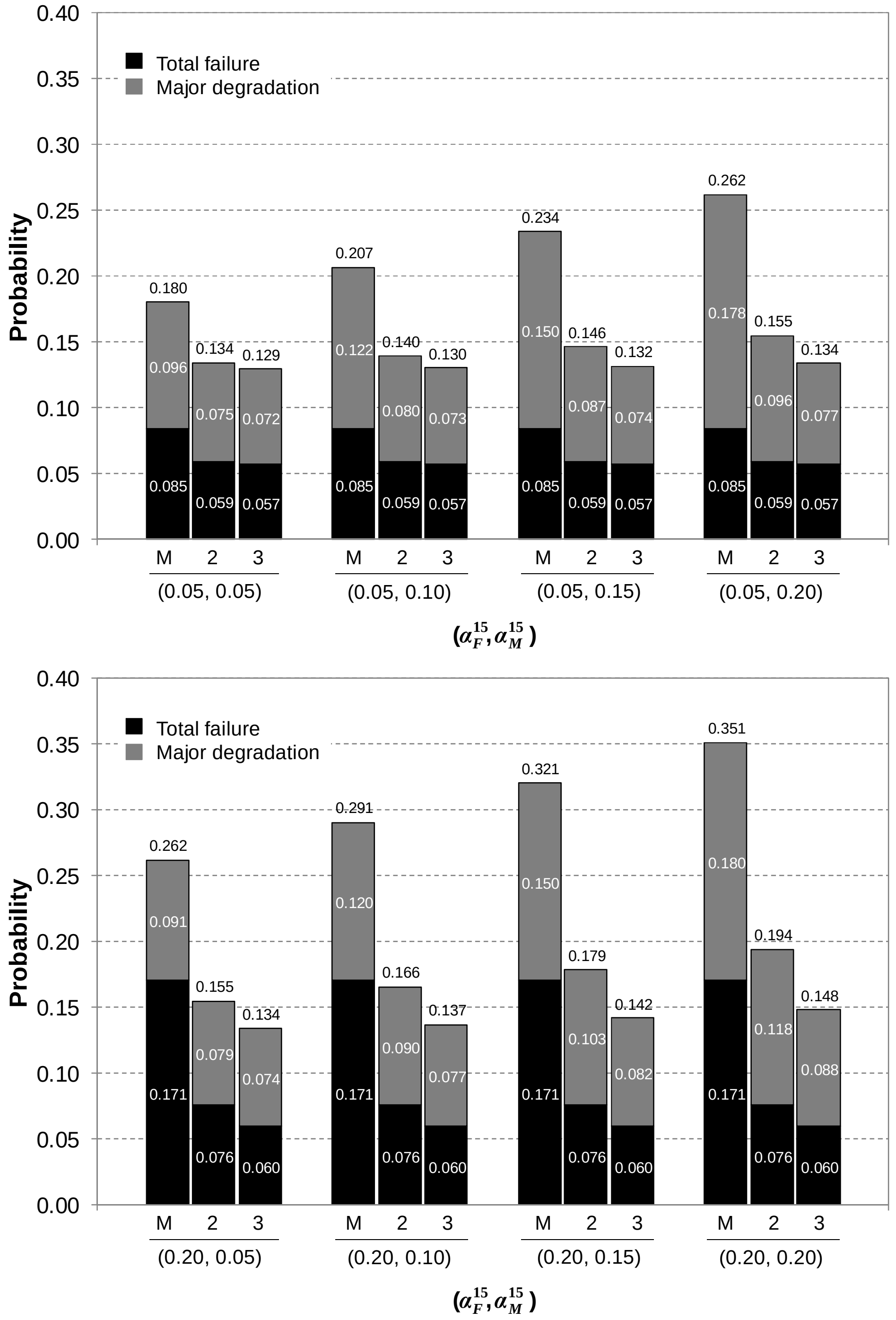


Figure 7.50. Sensitivity of the architectures to the anomaly and failure behavior of the networkable subsystem/technology (after 5 years on-orbit)

Net gain and network efficiency in the case of major anomalies. Net gains for the major–failed state Δ^{MF} can be defined for the IMLN approach in a similar fashion than for catastrophic failure as:

$$\Delta^{MF}_{\text{2-IMLN}} = P^{MF}_{\text{monolith}} - P^{MF}_{\text{2-IMLN}} \tag{7.38}$$

$$\Delta^{MF}_{\text{3-IMLN}} = P^{MF}_{\text{monolith}} - P^{MF}_{\text{3-IMLN}} \tag{7.39}$$

Using Eqs. (7.35), (7.36) and (7.37), these expressions can be manipulated to obtain:

$$\Delta^{MF}_{\text{2-IMLN}} = \left(1 - P_S^F\right)\left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right)\left(1 - \alpha_{MF}\right)\alpha_{MF} \tag{7.40}$$

$$\Delta^{MF}_{\text{3-IMLN}} = \left(1 - P_S^F\right)\left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right)\left[-\left(\alpha_{MF}\right)^2\left(1 - P_S^F\right) - 2\alpha_{MF} P_S^F + 1 + P_S^F\right]\alpha_{MF} \tag{7.41}$$

Due to the relationship between P^F, P^M and P^{MF} established in Eq. (5.40), the net gain for the major degradation state Δ^M can be computed from the knowledge of Δ^F and Δ^{MF}:

$$\Delta^{M}_{\text{2-IMLN}} = P^{M}_{\text{monolith}} - P^{M}_{\text{2-IMLN}} = \Delta^{MF}_{\text{2-IMLN}} - \Delta^{F}_{\text{2-IMLN}} \tag{7.42}$$

$$\Delta^{M}_{\text{3-IMLN}} = P^{M}_{\text{monolith}} - P^{M}_{\text{3-IMLN}} = \Delta^{MF}_{\text{3-IMLN}} - \Delta^{F}_{\text{3-IMLN}} \tag{7.43}$$

Note that the values of Δ^M are also dependent on the choice of α_F^{15}. In addition, network efficiency for major–failed state, η^{MF}, can also be defined for the IMLN approach in the same way than for catastrophic failures as:

$$\eta_{2\text{–IMLN}}^{MF} = \frac{\Delta_{2\text{–IMLN}}^{MF}}{\Delta_0^{MF}} \tag{7.44}$$

$$\eta_{3\text{–IMLN}}^{MF} = \frac{\Delta_{3\text{–IMLN}}^{MF}}{\Delta_0^{MF}} \tag{7.45}$$

with:

$$\Delta_0^{MF} = P_{\text{monolith}}^{MF} - P_0^{MF} \tag{7.46}$$

where $P_0^{MF}(t)$ is the probability of a major anomaly or catastrophic failure for the architecture with a networkable subsystem/technology without anomalies or failure (α_{MF} = 0). As:

$$P_0^{MF} = 1 - \left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right) \tag{7.47}$$

Eq. (7.46) can be manipulated to obtain:

$$\Delta_0^{MF} = \alpha_{MF}\left(1 - P_S^{MF}\right)\left(1 - P_P^{MF}\right) \tag{7.48}$$

Using Eqs. (7.40), (7.41) and (7.48), Eqs. (7.44) and (7.45) can be expressed as:

$$\eta_{2\text{–IMLN}}^{MF} = -\alpha_{MF}\left(1 - P_S^F\right) + 1 - P_S^F \tag{7.49}$$

$$\eta_{3\text{–IMLN}}^{MF} = -\left(\alpha_{MF}\right)^2\left(1 - P_S^F\right)^2 - 2\alpha_{MF} P_S^F\left(1 - P_S^F\right) + 1 - \left(P_S^F\right)^2 \tag{7.50}$$

Similarly, the network efficiency with respect to major degradation, η^M, can be obtained for the IMLN approach as:

$$\eta_{2\text{–IMLN}}^{M} = \frac{\Delta_{2\text{–IMLN}}^{M}}{\Delta_0^M} \tag{7.51}$$

$$\eta_{3\text{–IMLN}}^{M} = \frac{\Delta_{3\text{–IMLN}}^{M}}{\Delta_0^M} \tag{7.52}$$

where Δ^M are found in Eqs. (7.42) and (7.43) and Δ_0^M is simply computed as:

$$\Delta_0^M = \Delta_0^{MF} - \Delta_0^F \tag{7.53}$$

Note that the values of η^M and Δ_0^M are also dependent on the choice of α_F^{15}.

Net gain and network efficiency known, η–Δ graphs can be generated to investigate the reaction of the architecture to anomalies and failures in the networkable subsystem/technology. Let us start with the global major–failed state. Figure 7.51 presents the family of curves obtained from the variation of α_{MF}^{15} from 0.10 to 0.40 by 0.05 increments in the case of the 2-IMLN architecture.

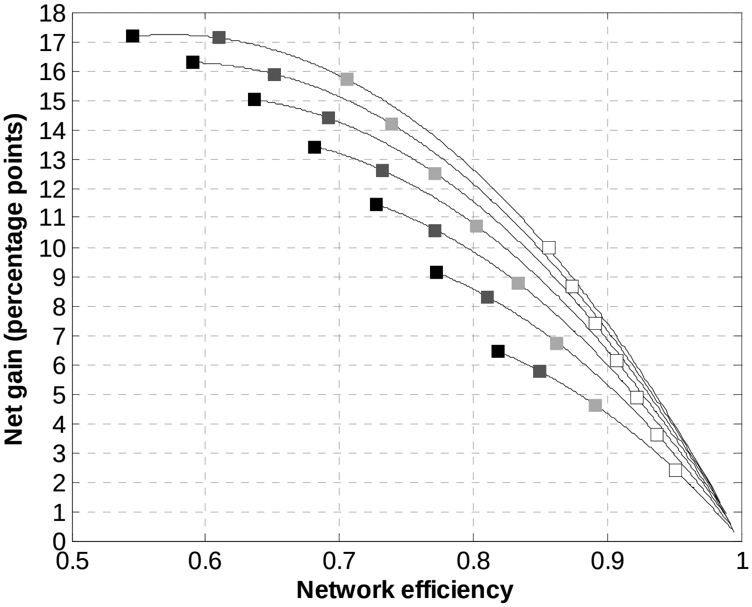


Figure 7.51. Network efficiency versus net gain for the major–failed state for the 2-IMLN

(*As previously, the color of the square markers corresponds to the on-orbit times, 1, 5, 10 and 15 years, from lighter to darker colors. The different curves correspond to the variation of* α_{MF}^{15} *, from 0.10 in the bottom curve to 0.40 in the top curve*)

It can be seen in Figure 7.51 that the η–Δ graph presents similar results for (η^{MF}, Δ^{MF}) than for (η^{F}, Δ^{F}): for the same on-orbit time, the efficiency decreases, but the net gain increases with α_{MF}^{15} increasing. Network efficiency continuously decreases as the spacecraft ages on-orbit, and the net gain initially increases, then decreases (the inflexion in the curve is only visible for the highest value of α_{MF}^{15}). Finally, the more severe the degradation is for the networkable subsystem/technology, the steeper the decrease in the network efficiency.

The 2-IMLN and 3-IMLN can also be compared for the severe degradation state, and this is shown in Figure 7.52. As previously seen for η^F and Δ^F, the 3-IMLN handles better the decrease in efficiency, as well as provides higher net gains.

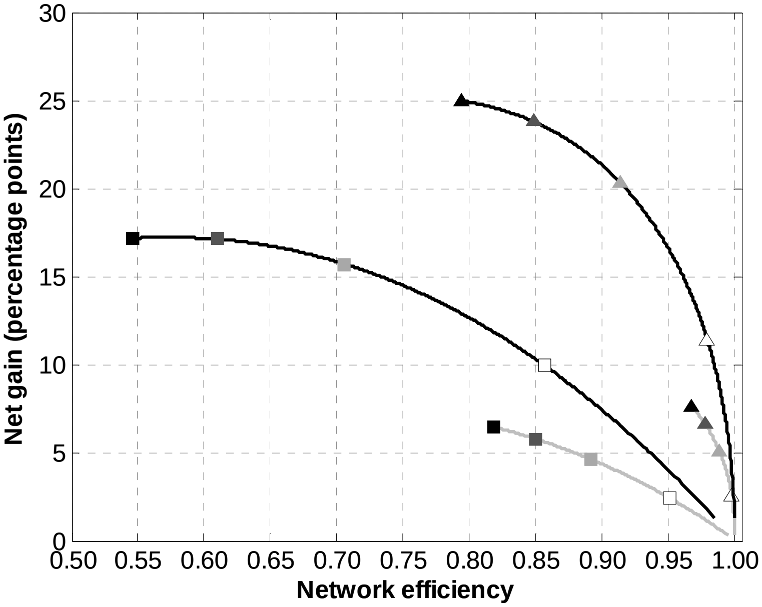


Figure 7.52. 2- and 3-IMLN comparison for $\alpha_{MF}^{15} = 0.10$ and $\alpha_{MF}^{15} = 0.40$

(*The grey curves correspond to $\alpha_{MF}^{15} = 0.10$ and the black curves correspond to $\alpha_{MF}^{15} = 0.40$. The square markers represent the 2-IMLN, and the triangle markers represent the 3-IMLN. As previously, the color of the markers represents the on-orbit times, 1, 5, 10 and 15 years from lighter to darker colors*)

How does compare the efficiency of space-based network in rooting catastrophic failures with major anomalies? This question is investigated in the following by considering equivalent values for α_F^{15} and α_M^{15}, at two levels (0.05 and 0.20). As such, the networkable subsystem/technology has an equal probability to be in a total failed state and in a major degradation state. Figure 7.53 shows the resulting network efficiencies η^F and η^M for the 2-IMLN architecture, and Figure 7.54 for the 3-IMLN architecture.

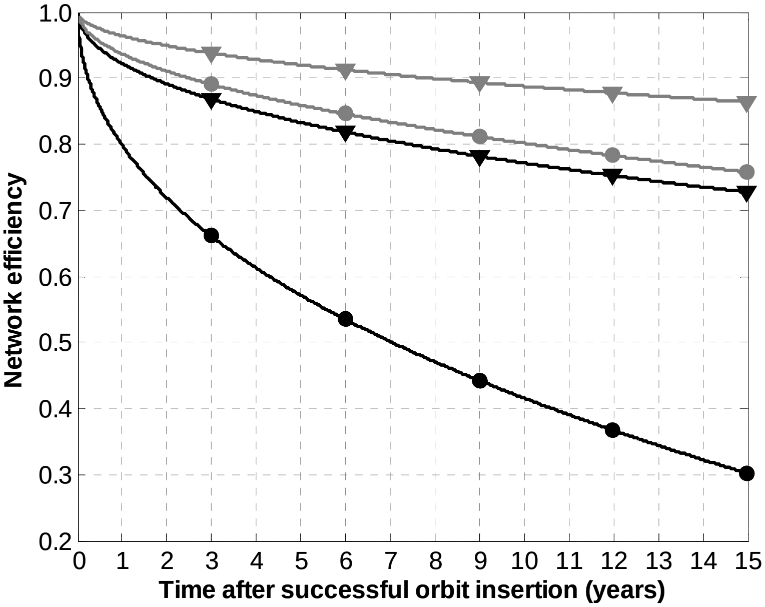


Figure 7.53. Comparison of η^F and η^M for the 2-IMLN architecture

(*The grey curves correspond to α_F^{15} and α_M^{15} equal to 0.05, while the black curves correspond to both parameters equal to 0.20. The triangle markers represent η^F (network efficiency for catastrophic failures), and the circle markers represent η^M (network efficiency for major anomalies)*)

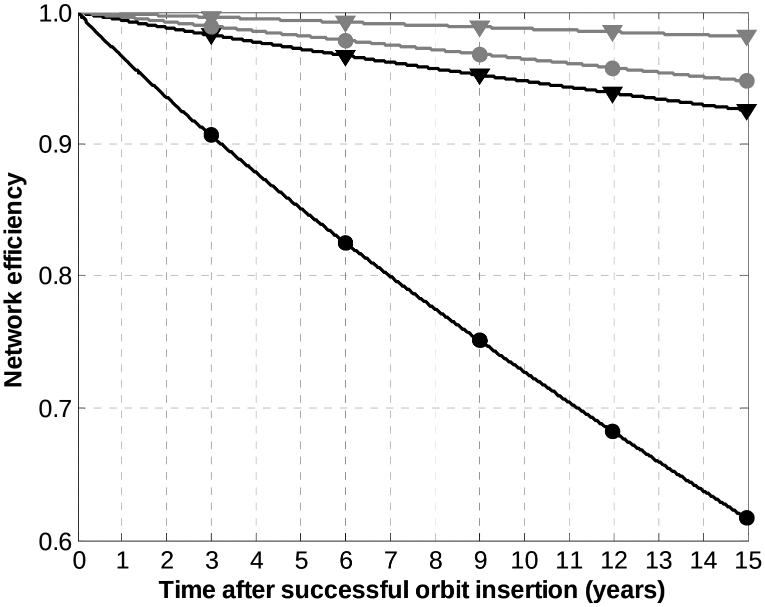


Figure 7.54. Comparison of η^F and η^M for the 3-IMLN architecture

(*Same formatting than the previous figure*)

It can be seen on Figure 7.53 that the 2-IMLN is more efficient at rooting out catastrophic failures than major anomalies in the networkable subsystem/technology (at both levels, 0.05 and 0.20): for example, after 15 years on orbit at the 0.05-level, the network efficiency η^F is equal to 0.864, while η^M is equal to 0.757, a value 12% lower. In the most problematic case considered here (α_F^{15} and α_M^{15} at 0.20), η^F is equal to 0.727, while η^M is equal to 0.302, a value 58% lower. This suggests that in the case of more and more problematic subsystem/technology, the space-based network concentrate more and more of its efforts on catastrophic failures, to the increasing detriment of major anomalies[19].

Figure 7.54 confirms a similar phenomenon for the 3-IMLN architecture: for example, after 15 years on orbit at the 0.05-level, the network efficiency η^F is equal to 0.981, while η^M is equal to 0.948, a value 3% lower. In the most problematic case considered here (α_F^{15} and α_M^{15} at 0.20), η^F is equal to 0.926, while η^M is equal to 0.616, a value 33% lower. However, the sacrifice of the major anomalies is less pronounced in the case of the 3-IMLN compared to the 2-IMLN architecture.

As a conclusion, the space-based networks demonstrate an interesting quality: **the networks attempt to eliminate anomalous events by decreasing levels of severity, catastrophic failures first, then major anomalies. This "sacrifice" is less pronounced in architectures with more networked spacecraft.**

[19] In the case of very high probability of failure of the networkable subsystem, the probability of being in a major degradation state for the space system can even increase between a monolithic architecture and a space-based network, leading to negative efficiencies. However, the overall probability of being in a major–failed state remains lower for the space-based network (the network completely sacrificed major anomalies to the advantage of catastrophic failures).

To complete this analysis, two more cases are studied for the 2-IMLN architecture with the same value of the probability of being in a major–failed state for the networkable subsystem/technology ($\alpha_{MF}^{15} = 0.25$): case 1 consists in a networkable subsystem/ technology that has a higher tendency to experience major anomalies over catastrophic failures ($\alpha_F^{15} = 0.05$ and $\alpha_M^{15} = 0.20$); case 2 consists in the reverse situation where the networkable subsystem/technology that has a higher tendency to experience catastrophic failures over major anomalies ($\alpha_F^{15} = 0.20$ and $\alpha_M^{15} = 0.05$). Figure 7.55 allows the comparison of the network efficiencies η^F and η^M resulting from cases 1 and 2.

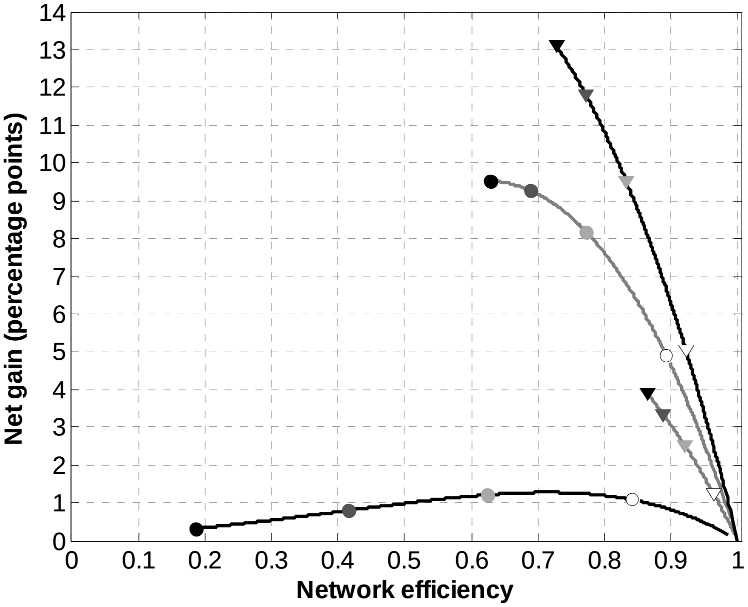


Figure 7.55. Comparison of η^F and η^M for the 2-IMLN architecture with $\alpha_{MF}^{15} = 0.25$

(The grey curves correspond to case 1(α_F^{15} and α_M^{15} equal to 0.05 and 0.20 respectively), while the black curves correspond to case 2 (α_F^{15} and α_M^{15} equal to 0.20 and 0.05 respectively). The triangle markers represent η^F (network efficiency for catastrophic failures), and the circle markers represent η^M (network efficiency for major anomalies))

Figure 7.55 confirms that the behavior of the network is different for catastrophic failures and major anomalies. For case 1 (grey curves), η^F is consistently higher than η^M at comparable on-orbit times (circle markers are always to the left of the triangle markers with the same color on the grey curves), but the net gains are higher in the case of major degradation compared to catastrophic failures (consistent with the fact that the networkable subsystem/technology is more prone to major anomalies). For case 2 (black curves), η^F is also consistently higher than η^M at comparable on-orbit times, but in this case the net gains are higher in the case of catastrophic failures (consistent with the fact that the networkable subsystem/technology is more prone to major anomalies). For the same α_{MF}^{15}–level, the network had the potential in case 1 to significantly help in terms of major degradation despite its associated lower efficiency, while in case 2, the network almost completely focused its efforts on rooting out catastrophic failures, resulting in a marginal improvement for the major degradation state.

7.3.9. Multi-State Considerations: IMLN Behavior Facing Minor Degradation

The last part of the multi-state analysis lies with the consideration of minor anomalies in the networkable subsystem/technology. As it was done for the major anomaly case, we assume that the probability of minor degradation of the networked subsystem/technology is given by $\alpha_m(t)$, the impact of such an event is investigated in a similar fashion, by parameterizing the value of the probability of major degradation at 15 years: $\alpha_m(t = 15\,\text{years}) = \alpha_m^{15}$. Only two levels are explored to give a sense of the type of analysis enabled by this dissertation: α_M^{15} equal to 0.05 and 0.20.

Again, the state considered in the simulation is not the “minor degradation” state directly, but the aggregation of the “minor degradation”, “major degradation” and “total failure” states into the “minor–major–failed” state (also simply referred to as “degraded” state). The probability of being in a minor degradation state for the space architecture is then calculated by taking the difference between the probability of being in the aggregated minor–major–failed state, labeled $\alpha_{mMF}(t)$, and the probability of being in the major degradation state and the total failure state (simulated in the previous subsections). As a consequence, we have for α_F, α_M, α_m, α_{MF} and α_{mMF}:

$$\alpha_{mMF}(t) = \alpha_F(t) + \alpha_M(t) + \alpha_m(t) = \alpha_{MF}(t) + \alpha_m(t) \tag{7.54}$$

Note that the value of α_{mMF} is bounded by 1, constraining the values α_F, α_M and α_m can take concurrently.

Three representative cases are investigated to expose trends associated with minor degradation:

- Case 1: $\alpha_F^{15} = 0.05$, $\alpha_M^{15} = 0.05$, $\alpha_m^{15} = 0.05$ and resulting in $\alpha_{MF}^{15} = 0.10$ and $\alpha_{mMF}^{15} = 0.15$;
- Case 2: $\alpha_F^{15} = 0.20$, $\alpha_M^{15} = 0.05$, $\alpha_m^{15} = 0.05$ and resulting in $\alpha_{MF}^{15} = 0.10$ and $\alpha_{mMF}^{15} = 0.30$: only α_m was increased from case 1;
- Case 3: $\alpha_F^{15} = 0.20$, $\alpha_M^{15} = 0.20$, $\alpha_m^{15} = 0.20$ and resulting in $\alpha_{MF}^{15} = 0.40$ and $\alpha_{mMF}^{15} = 0.60$: only α_{MF} was increased from case 2.

As done for the probability of failure and major anomaly of the networkable subsystem/technology, the probability of being in a minor–major–failed state of the networkable subsystem/technology is modeled using single Weibull distributions (with a constant shape parameter β = 0.5), and the values of the scale parameters associated to the specified values are given in Table 7.15.

Table 7.15. Weibull scale parameter values for the α_{mMF} distribution of the networked subsystem/technology

α_{mMF}^{15}	Scale parameter θ_{MF}
	years
0.15	568
0.30	117.9
0.60	17.87

Using the IMLN model, simulations were run for each α_{mMF}^{15} value, and generated as output the probability of being in a minor–major–failed state of the space architecture (as previously: monolith, 2-IMLN and 3-IMLN). Also as done previously, analytical results can be found as the subscripts and superscripts can be replaced by "mMF" (with the same exceptions than previously). The equations are modified as follows:

$$P_{\text{monolith}}^{mMF} = 1 - \left(1 - P_S^{mMF}\right)\left(1 - P_P^{mMF}\right)\alpha_{mMF} \qquad (7.55)$$

$$P_{\text{2-IMLN}}^{mMF} = 1 - \left(1 - P_S^{mMF}\right)\left(1 - P_P^{mMF}\right)\left\{1 - \left(1 - \left(1 - \alpha_{mMF}\right)\left(1 - P_S^{F}\right)\right)\alpha_{mMF}\right\} \qquad (7.56)$$

$$P_{\text{3-IMLN}}^{mMF} = 1 - \left(1 - P_S^{mMF}\right)\left(1 - P_P^{mMF}\right)\left\{1 - \left(1 - \left(1 - \alpha_{mMF}\right)\left(1 - P_S^{F}\right)\right)^2 \alpha_{mMF}\right\} \qquad (7.57)$$

For readability purposes again, four on-orbit times have been selected to compare architectures: 1 year, 5 years, 10 years and 15 years on-orbit. The probabilities of being in a major–failed state (in percentage points) for the three architectures at these times are shown in Table 7.16.

Table 7.16. Probabilities of being in a minor–major–failed state for monolith and networked architectures (in percentage points)

α_{mMF}^{15}	**Architecture**	P^{mMF} **– IMLN simulation**				P^{mMF} **– Analytical results**			
		Time spent on-orbit (years)				Time spent on-orbit (years)			
		1	5	10	15	1	5	10	15
0.15	Monolith	–	–	–	–	13.84	27.65	36.40	42.35
	2-IMLN	10.39	21.51	29.08	34.48	10.38	21.51	29.08	34.49
	3-IMLN	10.17	20.67	27.71	32.71	10.16	20.66	27.70	32.70
0.30	Monolith	–	–	–	–	18.05	35.32	45.72	52.52
	2-IMLN	11.00	23.92	33.04	39.58	11.01	23.91	33.03	39.58
	3-IMLN	10.24	21.32	29.14	34.88	10.24	21.30	29.12	34.87
0.60	Monolith	–	–	–	–	29.08	53.18	65.63	72.87
	2-IMLN	14.49	34.95	48.87	58.06	14.48	34.95	48.87	58.07
	3-IMLN	11.15	26.92	39.45	48.65	11.14	26.90	39.45	48.65

It can be seen in Table 7.16 that the results from the IMLN simulation and from analytical solutions are again in strong agreement: the average difference is less than 0.01 percentage point and the maximum difference is 0.02 percentage point.

In a similar fashion than for other severity levels, the probability of being in a minor degradation state for the architecture is given by:

$$P^{m} = P^{mMF} - P^{MF} \qquad (7.58)$$

From the results given in Table 7.13 and Table 7.16, it can be calculated and the results are shown in Table 7.17.

Table 7.17. Probabilities of being in a minor degradation state for monolith and networked architectures (in percentage points)

α_F^{15}	α_M^{15}	α_m^{15}	Architecture	P^m – IMLN simulation				P^m – Analytical results			
				Time spent on-orbit (years)				Time spent on-orbit (years)			
				1	5	10	15	1	5	10	15
0.05	0.05	0.05	Monolith	–	–	–	–	5.36	9.62	11.86	13.17
			2-IMLN	4.32	8.09	10.33	11.76	4.30	8.07	10.31	11.74
			3-IMLN	4.20	7.72	9.79	11.13	4.20	7.72	9.79	11.13
0.05	0.05	0.20	Monolith	–	–	–	–	9.57	17.30	21.19	23.34
			2-IMLN	4.93	10.50	14.28	16.86	4.93	10.48	14.25	16.83
			3-IMLN	4.27	8.37	11.22	13.30	4.28	8.36	11.21	13.29
0.20	0.20	0.20	Monolith	–	–	–	–	11.50	18.04	19.83	20.08
			2-IMLN	6.85	15.53	20.18	22.46	6.85	15.52	20.18	22.45
			3-IMLN	4.96	12.09	17.43	20.83	4.94	12.09	17.43	20.84

All the results regarding the total failure, major degradation and minor degradation can be presented in a more practical representation, for example for the case $\alpha_{mMF}^{15} = 0.15$ ($\alpha_F^{15} = 0.05, \alpha_M^{15} = 0.05$ and $\alpha_m^{15} = 0.05$) as shown in Figure 7.56.

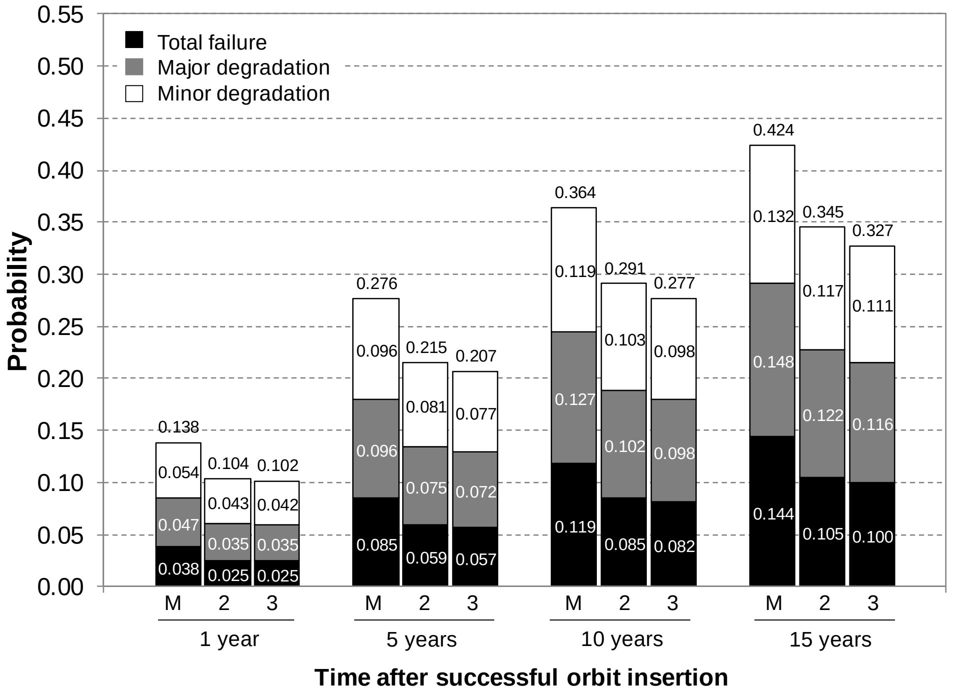


Figure 7.56. Probability of being in degraded states for the space architectures in case 1

Figure 7.56 represents the probability of total failure of the architecture in black, of major degradation in grey and minor degradation in white. The total probability to be in a degraded state (i.e., not fully operational) is shown at the top of the stacked bars. **Figure 7.56 gives a complete comparative survivability analysis of the architectures under consideration in the case of the considered endogenous failures and performance metric,** as all the degraded states are represented together. For example, it can be seen in Figure 7.56 that after 15 years on orbit, the probability of being in a degraded state has been reduced by 7.9 percentage points by considering a 2-IMLN architecture, and by 9.7 percentage points with a 3-IMLN. This reduction directly translates in a gain in the probability of being fully operational. In the same way than for total failures and major anomalies, the networked architectures behave better with respect to minor anomalies in this particular setting, with an advantage to networks with more spacecraft related to the networkable subsystem/technology.

The results for case 2 and case 3 are given Figure 7.57 and Figure 7.58 respectively.

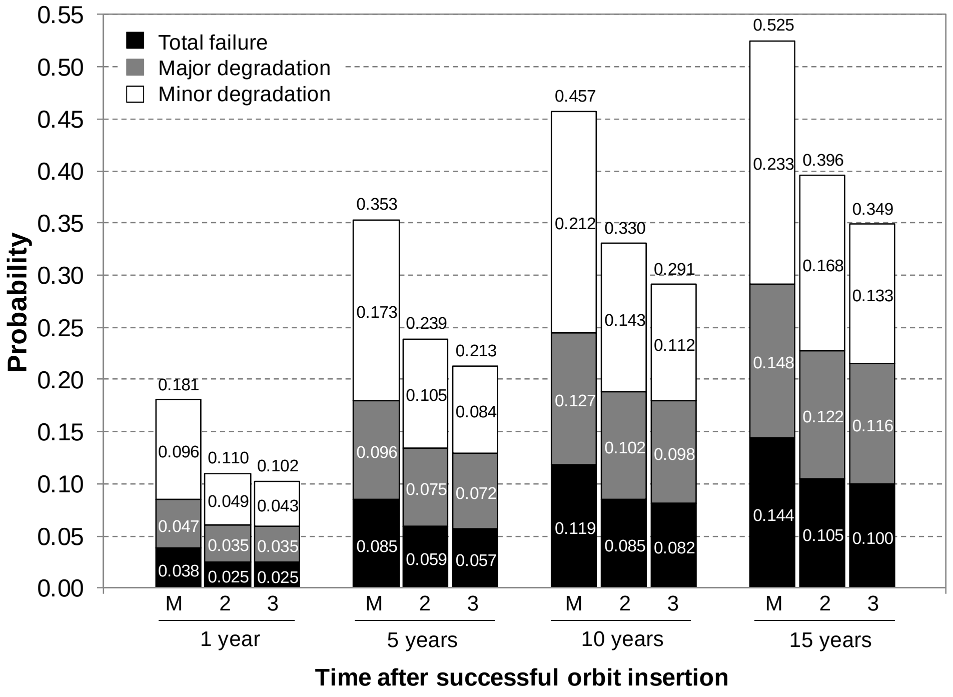


Figure 7.57. Probability of being in degraded states for the space architectures in case 2

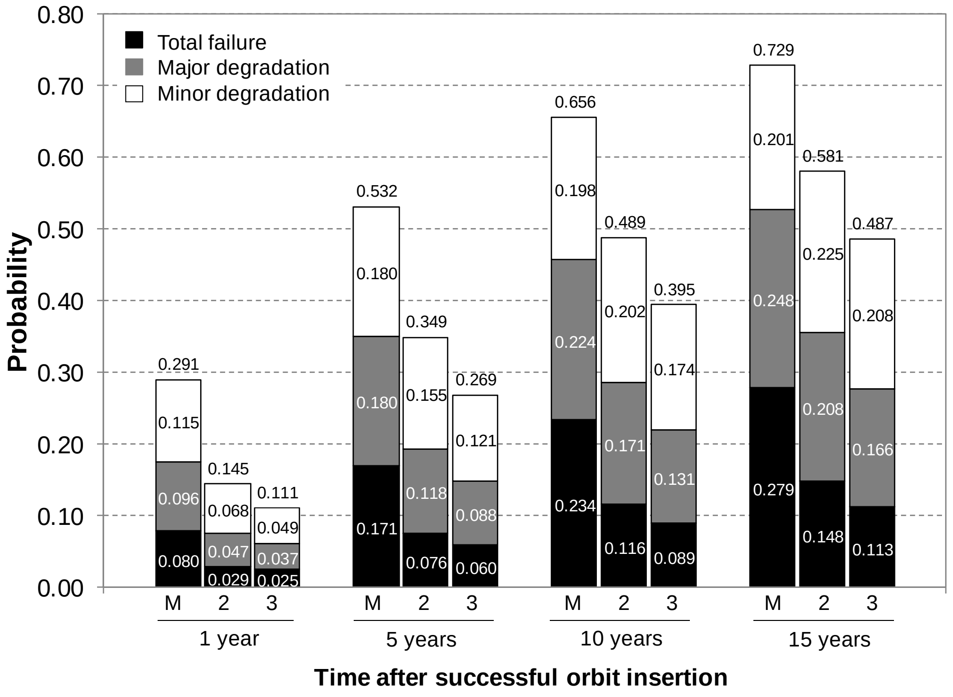


Figure 7.58. Probability of being in degraded states for the space architectures in case 3

In carefully examining Figure 7.57 and Figure 7.58, a familiar phenomenon can be observed, as it was the case for P^M: in both cases (case 2 and case 3), $\alpha_m^{15} = 0.20$; the variable is α_{MF}^{15} which increased from 0.10 to 0.40. As expected, P^F and P^M increased, but P^m was also impacted: for example, after 15 years, the probability of minor degradation for the monolith architecture shifted from 23.34% to 20.08%, from 16.83% to 22.45% for the 2-IMLN and from 13.29% to 20.84% for the 3-IMLN[20]. This implies that for a constant probability of minor degradation for the networkable subsystem/technology (α_m), the probability of minor degradation of the complete architecture is affected by the variation in the probability of being in a severe degradation state of the networkable subsystem/technology (α_{MF}). As a consequence, $\boldsymbol{P^m}$ **is not solely a function of** $\boldsymbol{\alpha_m}$**, but depends on** $\boldsymbol{\alpha_m}$**,** $\boldsymbol{\alpha_M}$ **and** $\boldsymbol{\alpha_F}$.

Net gain and network efficiency in the case of minor anomalies. Net gains for the minor–major–failed state Δ^{mMF} can be defined for the IMLN approach in a similar fashion than for other severity level.

$$\Delta_{\text{2-IMLN}}^{mMF} = P_{\text{monolith}}^{mMF} - P_{\text{2-IMLN}}^{mMF} \tag{7.59}$$

$$\Delta_{\text{3-IMLN}}^{mMF} = P_{\text{monolith}}^{mMF} - P_{\text{3-IMLN}}^{mMF} \tag{7.60}$$

Due to the relationship between P^F, P^M and P^m, the net gain for the minor degradation state Δ^m can be computed as:

[20] Note that the probabilities of being in a minor degradation state are higher for the space-based networks than for the monolith architecture. This phenomenon is commented in more depth later with efficiency considerations.

$$\Delta^{m}_{\text{2-IMLN}} = P^{m}_{\text{monolith}} - P^{m}_{\text{2-IMLN}} = \Delta^{mMF}_{\text{2-IMLN}} - \Delta^{MF}_{\text{2-IMLN}} \tag{7.61}$$

$$\Delta^{m}_{\text{3-IMLN}} = P^{m}_{\text{monolith}} - P^{m}_{\text{3-IMLN}} = \Delta^{mMF}_{\text{3-IMLN}} - \Delta^{MF}_{\text{3-IMLN}} \tag{7.62}$$

Note that the values of Δ^{m} are also dependent on the choice of α^{15}_{MF}.

In addition, network efficiency for minor–major–failed state, η^{mMF}, can also be defined as:

$$\eta^{mMF}_{\text{2–IMLN}} = \frac{\Delta^{mMF}_{\text{2–IMLN}}}{\Delta^{mMF}_{0}} \tag{7.63}$$

$$\eta^{mMF}_{\text{3–IMLN}} = \frac{\Delta^{mMF}_{\text{3–IMLN}}}{\Delta^{mMF}_{0}} \tag{7.64}$$

with:

$$\Delta^{mMF}_{0} = P^{mMF}_{\text{monolith}} - P^{mMF}_{0} \tag{7.65}$$

where $P^{mMF}_{0}(t)$ is the probability of an anomaly or failure for the architecture with a networkable subsystem/technology without anomalies or failure (α_{mMF} = 0).

Finally, the network efficiency with respect to major degradation, η^{m}, can be obtained as:

$$\eta^{m}_{\text{2–IMLN}} = \frac{\Delta^{m}_{\text{2–IMLN}}}{\Delta^{m}_{0}} \tag{7.66}$$

$$\eta^m_{3\text{–IMLN}} = \frac{\Delta^m_{3\text{–IMLN}}}{\Delta^m_0} \tag{7.67}$$

where:

$$\Delta^m_0 = \Delta^{mMF}_0 - \Delta^{MF}_0 \tag{7.68}$$

The network efficiency in the case of the minor–major–failed state (η^{mMF}) behaves in the same fashion than η^{MF} and η^{F} with their corresponding α^{15} : it decreases with α^{15}_{mMF} increasing. Let us concentrate instead on η^m: this efficiency represents how well the network tackles minor anomalies in the networkable subsystem/technology. Figure 7.59 presents the variations of η^m according to the anomaly and failure behavior of the networkable subsystem/technology.

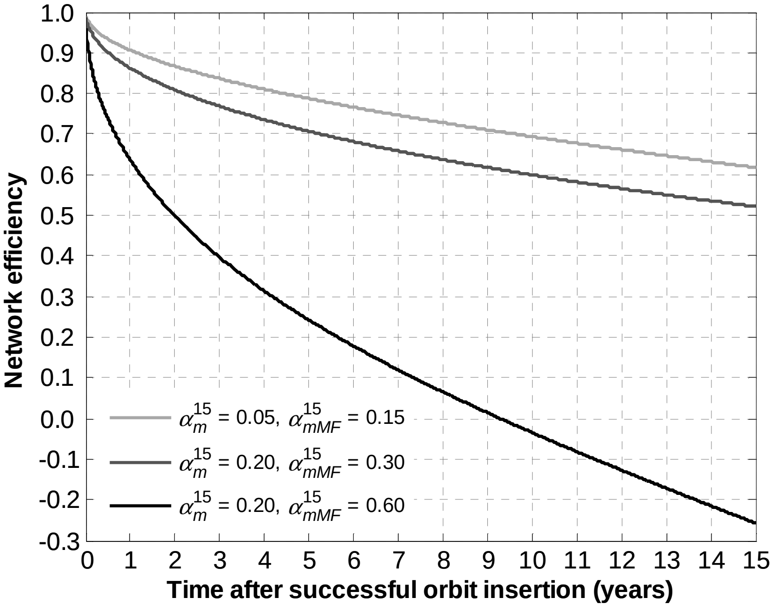


Figure 7.59. Network efficiency η^m for the 2-IMLN architecture

In Figure 7.59, the light grey curve corresponds to case 1, the dark grey curve corresponds to case 2 and the black curve to case 3. It can be seen that the network efficiency for minor degradation decreases between case 1 and case 2, where the probability of minor anomaly in the networkable subsystem/technology increases while keeping constant major anomaly and total failure probabilities. A more dramatic decrease occurs between case 2 and case 3: minor anomalies are kept at the same level of occurrence, but the major anomalies and total failures are drastically increased. It results in a large decrease in efficiency for rooting out minor anomalies. The efficiency even becomes negative for longer periods on-orbit, translating the fact that the space-based architecture has a higher probability of being in a minor degradation state than the monolith architecture at these times. This phenomenon can be observed in Figure 7.58 at 10 and 15 years on-orbit. This dependence of η^m with major anomalies and total failures mirrors the one for major anomalies with total failures. A similar effect is shown in Figure 7.60 for the 3-IMLN architecture, in a lesser way.

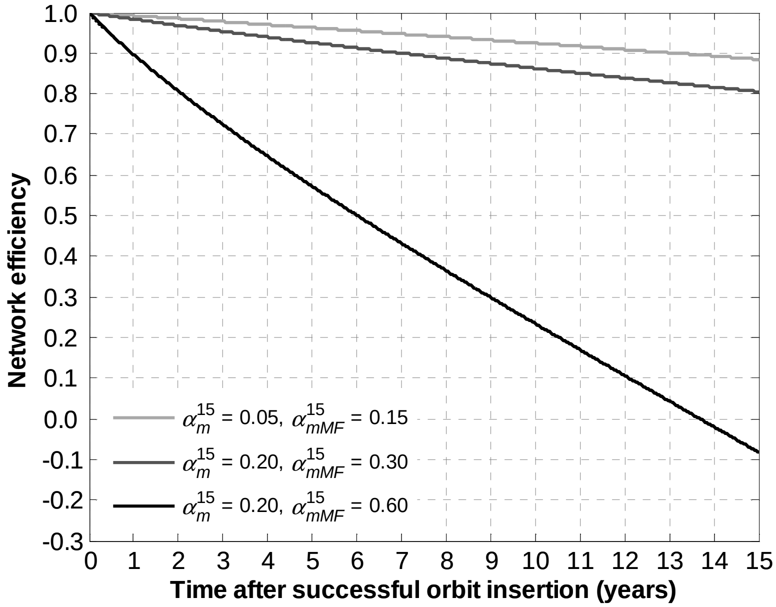


Figure 7.60. Network efficiency η^m for the 3-IMLN architecture

The variations observed in η^m are related to the fact that the networks extend their shielding priority rules to minor anomalies: it was seen earlier that networks shielded the architecture from catastrophic failures first, and then from major anomalies. Minor anomalies come last after major anomalies, as it can be seen in Figure 7.61 and Figure 7.62 for the 2-IMLN and 3-IMLN architectures respectively. For the same level of occurrence in all anomaly and failure types (α^{15} is equal to 0.05 for minor, major anomalies and total failures in case 1), the network efficiency are ranked by decreasing severity level: $\eta^F \geq \eta^M \geq \eta^m$. As a side note, the overall network efficiency for degraded state (η^{mMF}) is given as a reference of the overall performance of the network with respect to any anomalous event (dashed line in the figures).

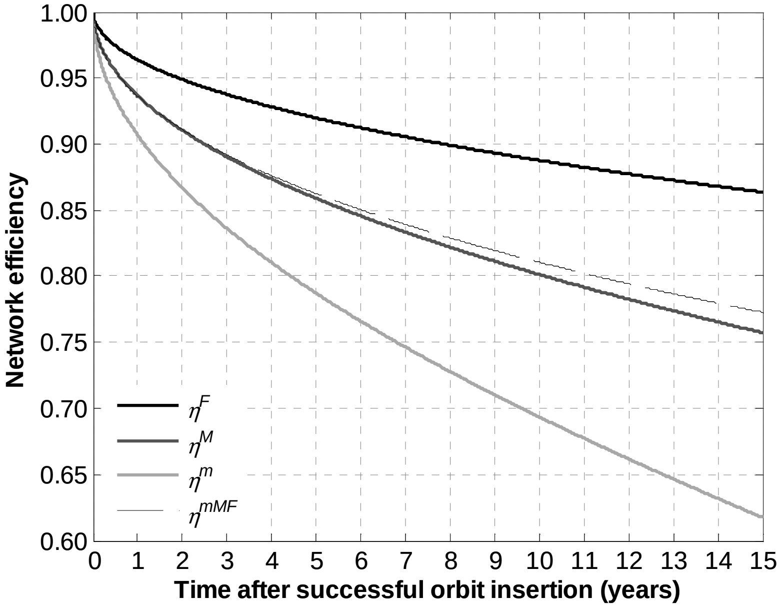


Figure 7.61. Comparison of network efficiencies of different severity levels for the 2-IMLN architecture in case 1

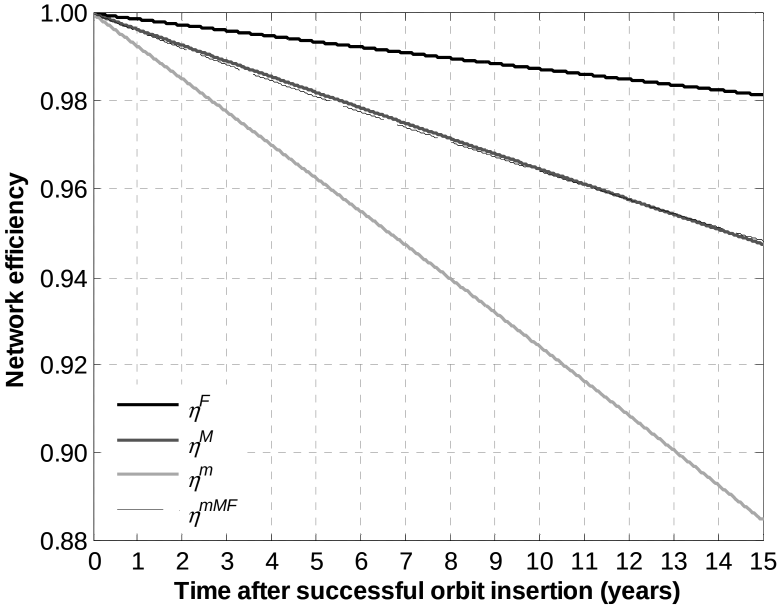


Figure 7.62. Comparison of network efficiencies of different severity levels for the 3-IMLN architecture in case 1

7.3.10. Survivability Analysis and Use of the η–Δ Graph

All the degradation states defined in this dissertation have been investigated in the previous subsections, and a global evaluation of the survivability of the architectures can be conceived through the *η*–Δ graph. Indeed, for a chosen performance metric, the *η*–Δ graph visualizes the potential gains or losses of an architecture under consideration with respect to the reference monolith architecture. In addition, if several architectures are under studied concurrently, the *η*–Δ graph allows a quick comparative analysis of the survivability characteristics of these architectures. As a consequence, the ***η*–Δ graph introduced in this thesis is a useful tool for the designers to explore the design space for survivability considerations and help inform architectural choices based on shareholder preferences**.

Some examples of the ways the *η*–Δ graph can be used are presented next by considering the three cases introduced in section 7.3.9. They are recalled below:

- Case 1: $\alpha_F^{15} = 0.05$, $\alpha_M^{15} = 0.05$, $\alpha_m^{15} = 0.05$ and resulting in $\alpha_{MF}^{15} = 0.10$ and $\alpha_{mMF}^{15} = 0.15$;
- Case 2: $\alpha_F^{15} = 0.20$, $\alpha_M^{15} = 0.05$, $\alpha_m^{15} = 0.05$ and resulting in $\alpha_{MF}^{15} = 0.10$ and $\alpha_{mMF}^{15} = 0.30$: only α_m was increased from case 1;
- Case 3: $\alpha_F^{15} = 0.20$, $\alpha_M^{15} = 0.20$, $\alpha_m^{15} = 0.20$ and resulting in $\alpha_{MF}^{15} = 0.40$ and $\alpha_{mMF}^{15} = 0.60$: only α_{MF} was increased from case 2.

For a given time and for each architecture, the net gains Δ^F, Δ^M, Δ^m, Δ^{MF} and Δ^{mMF}, as well as the associated network efficiencies η^F, η^M, η^m, η^{MF} and η^{mMF}. For the case 1 and at t = 5 years, the resulting η–Δ graph is shown in Figure 7.63.

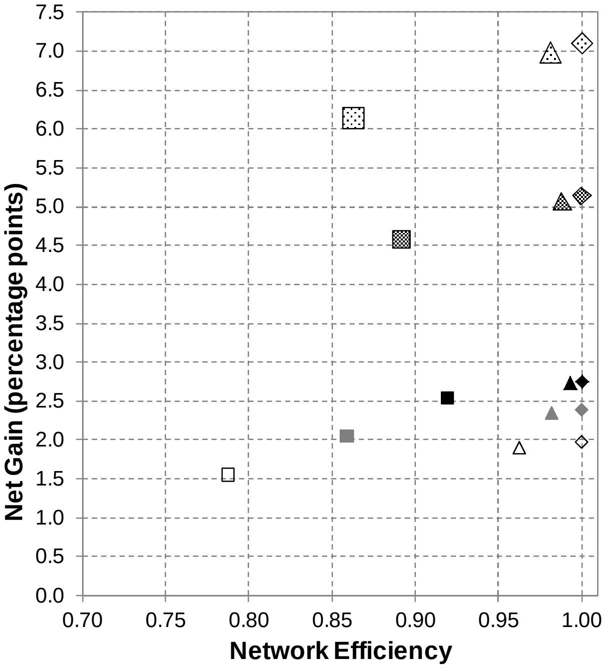


Figure 7.63. Complete η–Δ graph for 2-IMLN and 3-IMLN in case 1

Figure 7.63 is organized as follows:

- Marker shape:
    - The diamond markers represent the ideal case in which the networkable subsystem/technology does not experience anomalies or failures, and show the maximum net gain a space-based architecture can obtain. Referring to notations introduced earlier in the dissertation, the associated net gains correspond to Δ_0^F, Δ_0^M, Δ_0^m, Δ_0^{MF}, and Δ_0^{mMF};

    - The square markers represent the 2-IMLN architecture;
    - The triangle markers represent the 3-IMLN architecture.
- Marker color:
    - The white markers represent the network efficiencies and net gains associated with minor degradation, i.e., η^m and Δ^m;
    - The solid grey markers represent the network efficiencies and net gains associated with major degradation, i.e., η^M and Δ^M;
    - The black markers represent the network efficiencies and net gains associated with total failure, i.e., η^F and Δ^F;
    - The markers with dense dots represent the network efficiencies and net gains associated with major degradation or total failure, i.e., η^{MF} and Δ^{MF};
    - The markers with scarce dots represent the network efficiencies and net gains associated with any type of degradation, i.e., η^{mMF} and Δ^{mMF}.

As an example, it can be seen on Figure 7.63 for the 2-IMLN architecture that the network efficiencies and net gains (in percentage points) at 5 years on-orbit are:

- $(\eta^m, \Delta^m) = (0.787, 1.55)$;
- $(\eta^M, \Delta^M) = (0.859, 2.05)$;
- $(\eta^F, \Delta^F) = (0.920, 2.53)$;
- $(\eta^{MF}, \Delta^{MF}) = (0.892, 4.58)$;
- $(\eta^{mMF}, \Delta^{mMF}) = (0.863, 6.14)$;

This shows that, for example, the space-based network with two spacecraft improves the probability of experiencing a severe degradation (major degradation or total failure) of the on-orbit performance by 4.6 points with respect to the monolith architecture under the considered conditions. This architecture performs reasonably well for this level of severity as the associated efficiency is about 0.9.

In addition of assessing the survivability improvements related to the consideration of a 2-spacecraft network, Figure 7.63 allows the comparison with an additional architecture consisting of a 3-spacecraft network. It can be seen for example, that the 3-IMLN architecture provides an additional half percentage point on the net gain for the severe degradation state ($\Delta_{3-IMLN}^{MF} = 5.08$), with a much higher efficiency (about 0.99 compared to the 0.9 efficiency of the 2-IMLN). In the same fashion, the 3-IMLN adds an additional 0.8 percentage point ($\Delta_{3-IMLN}^{MF} = 6.98$) with a 0.98 efficiency. These high efficiencies do not translate in significantly higher gains, and as a consequence, adding a third spacecraft (or more) to the network might not be the best option from the survivability point of view in this particular case.

Let us now consider case 2: the probabilities of the networkable subsystem/technology experiencing a major anomaly and a total failure remain the same, but the probability of experiencing a minor anomaly increased significantly. The resulting η–Δ graph is shown in Figure 7.64.

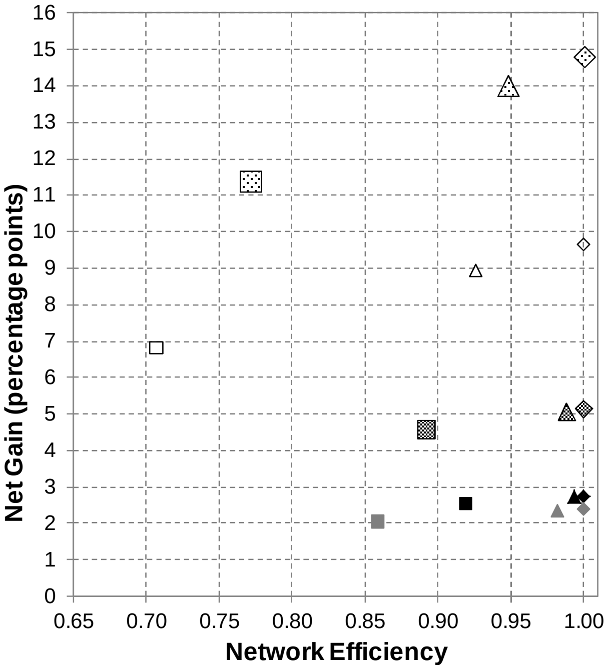


Figure 7.64. Complete η–Δ graph at 5 years for 2-IMLN and 3-IMLN in case 2

The formatting in Figure 7.64 is the same than for Figure 7.63. Note that the solid grey markers, black markers and markers with dense dots remain at the same location than in Figure 7.63: this is consistent with the fact that α_F^{15} and α_M^{15} did not change between case 1 and case 2. However, the locations of the white makers and the makers with scarce dots change, to reflect the change in α_m^{15}. The net gains at 5 years associated with the minor degradation state and the degraded state are now higher, for example for the 2-IMLN architecture:

- $(\eta^m, \Delta^m) = (0.707, 6.82)$;
- $(\eta^{mMF}, \Delta^{mMF}) = (0.771, 11.4)$;

As explained before, the associated network efficiencies are lower than in case 1 due to the increase in α_m^{15}. The difference between the 2-IMLN and 3-IMLN remains small for severe degradation states, but becomes potentially significant for any type of degradation: the 3-IMLN adds an additional 2.6 percentage points ($\Delta_{3-IMLN}^{MF} = 14.02$) with a 0.95 efficiency, only 0.8 percentage points from the ideal case. For stakeholders with high requirements on spacecraft to be fully operational, the 3-IMLN architecture might be a good candidate to consider. Adding more spacecraft to the network might not be interesting as the 3-IMLN performance is very close to the ideal case. Figure 7.64 clearly shows that the differences between 2-IMLN and 3-IMLN architectures mainly come from the minor anomalies in the networkable subsystem/technology.

The last case, case 3, is obtained from case 2 by increasing the probabilities of the networkable subsystem/technology experiencing major anomalies or total failures. The resulting η–Δ graph is shown in Figure 7.65.

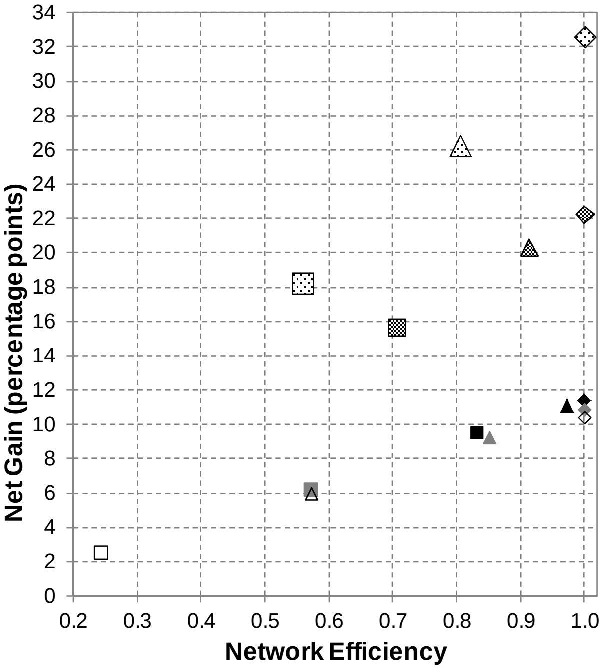


Figure 7.65. Complete *η*–Δ graph at 5 years for 2-IMLN and 3-IMLN in case 3

Figure 7.65 clearly shows a significant jump in net gains for the major degradation state, the total failure state, the severe degradation state (the sum of the previous two) and the degraded state. For example, the net gain at 5 years for the severe degradation state is 15.7 percentage points for the 2-IMLN architecture, with an associated efficiency of 0.71, while it is 20.3 points for the 3-IMLN architecture with an associated efficiency of 0.91. For this type of severity, the space-based network has a clear advantage over the monolith spacecraft (over 18 or 26 percentage point difference with the 2-IMLN and 3-IMLN for all types of anomalies and failures), with a significant edge for the 3-IMLN over the 2-IMLN. The 2-IMLN suffers from low efficiencies as it can be seen in Figure 7.65. Also note that the net gains and efficiencies for the minor degradation state are lower in case 2 than in case 3. This is consistent with previous findings that show that the networks prioritize their shielding effect to the most severe degradation type with higher

α^{15}. Finally, it can be observed that the results from the 3-IMLN are significantly different from the ideal case, indicating that networks with more spacecraft could be considered for survivability improvements.

The three η–Δ graphs shown above present interesting trends to the designer, especially when considered dynamically, as illustrated in Figure 7.66. This figure gathers the three previous figures and can be considered as the result of tweaking α_F^{15}, α_M^{15} and α_m^{15}. This could be for example integrated in a real-time simulation interface (see future work section for more details). Note that the scale has been altered so that it is common to all graphs for an easier visualization of the trends.

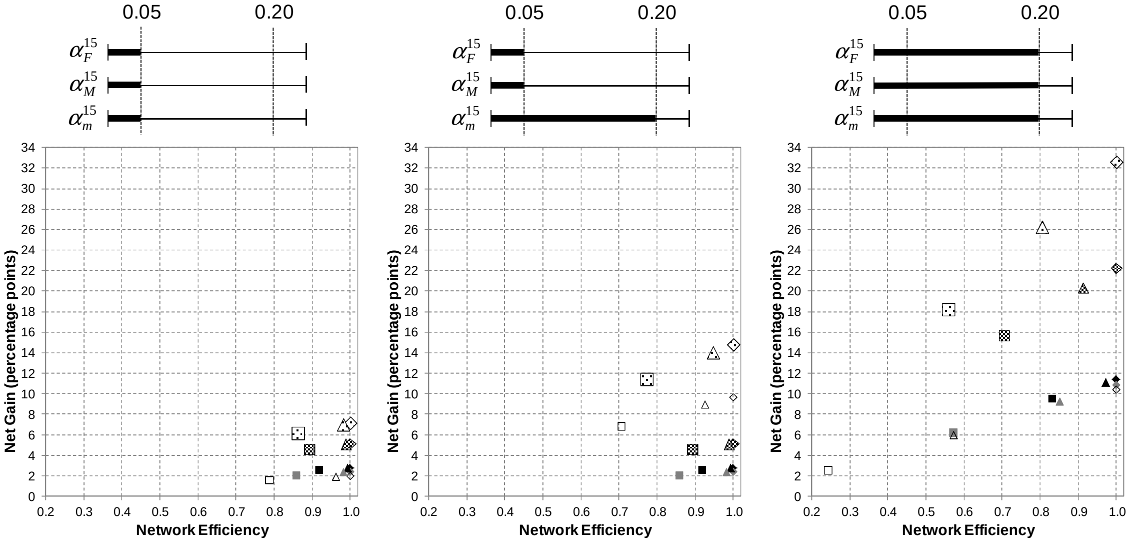


Figure 7.66. Evolution of the η–Δ graph at 5 years for 2-IMLN and 3-IMLN with the failure behavior of the networkable subsystem/technology

Another axis to study the behavior of the network is related to the time on-orbit. In the previous figures, the time was set to 5 years. A similar dynamic representation along the time axis is shown in Figure 7.67, for case 1, and it highlights all the trends discussed in the previous sections.

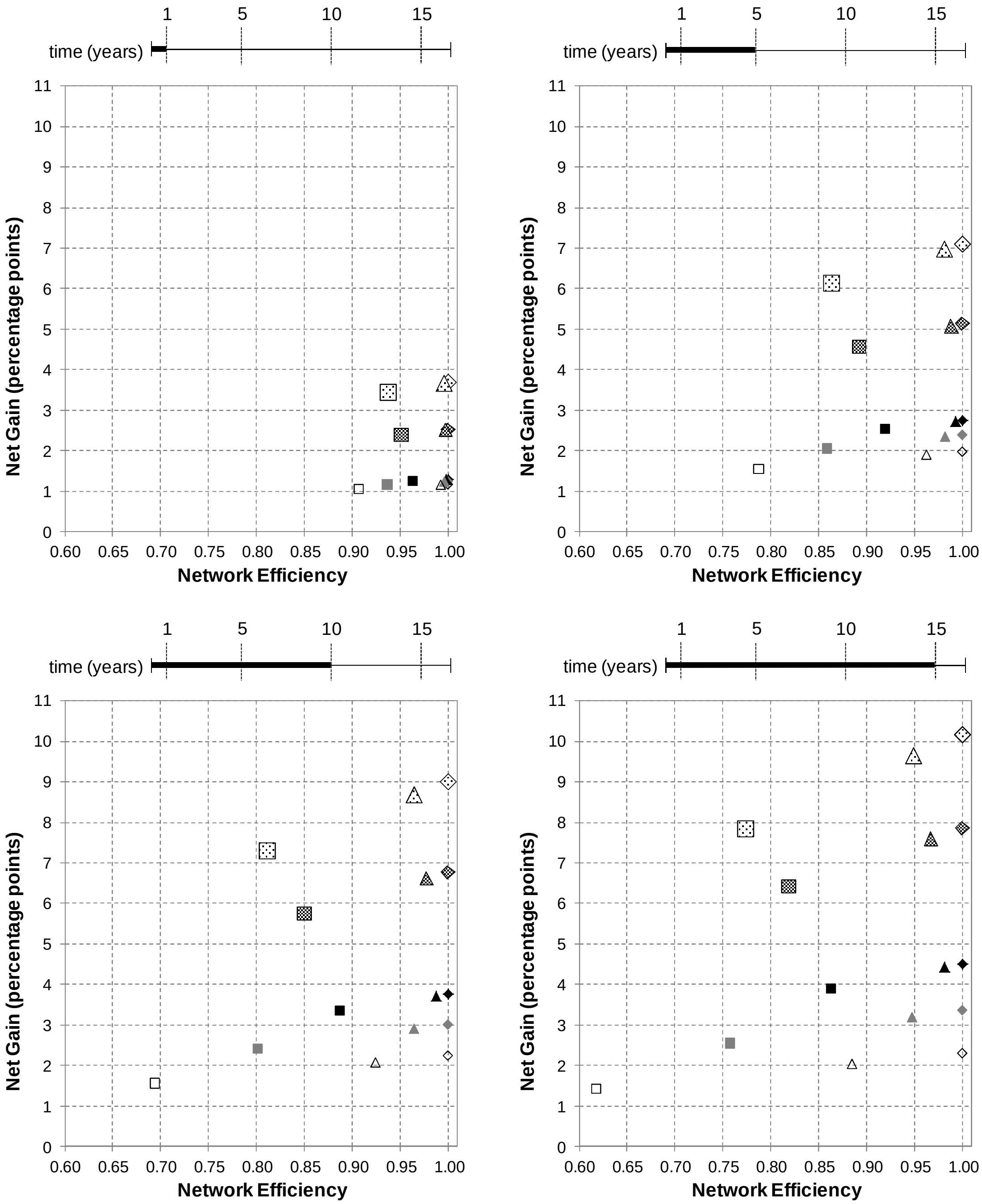


Figure 7.67. Evolution of the *η*–Δ graph for 2-IMLN and 3-IMLN with respect to on-orbit time

7.4. Summary of selected results

This chapter provided a significant amount of results and this conclusion summarizes a selected number of them. The first section investigated specific subsystems: the Telemetry, Tracking and Command (TTC) subsystem, and then proceeded to analyze the bigger Command and Data Handling (C&DH) subsystem. It was demonstrated that the consideration of a simple 2-spacecraft network provides a significant improvement in terms of survivability with respect to endogenous failures within these subsystems. Adding more spacecraft to the network for this purpose was shown to provide limited incremental benefits.

The following section then took a more general approach by considering a general non-descriptive networkable subsystem/technology and investigated the survivability characteristics of space-based networks chosen as they represent the building brick of more complex space-based networks. Several implications for space-based network design were observed, and a selected number is presented below. For example, it was shown that the worse degradation and failure behavior the networkable subsystem/technology has, the biggest benefit from a survivability point of view comes by adding more spacecraft to the network. It was also demonstrated that the space-based networks shield in priority from the worse failures, and then progress towards anomalies with decreasing levels of severity. A final example resides with the conclusion that the reliability of the wireless links in the network is critical to ripe all the survivability advantages enabled by the network, and especially infant mortality failures should be rooted out.

It is important to keep in mind the settings (e.g., class of threat, architecture functional structure, performance metric) of the survivability analysis to interpret the domain of applicability of the results provided in this chapter and not over-estimate their generalities. The results should not be generalized without proper analysis to all designs of space-based networks or monolith architectures and extrapolated to other classes of on-orbit shocks or threats to space systems. The survivability framework proposed in this thesis offers fruitful venue for further research and adaptation towards the survivability analysis of a broad range of architectural and design choices for space systems (and other engineering artifacts) and given different classes of shocks. Indeed, beyond survivability analyses pertaining to chosen architectures in this dissertation, this chapter introduced useful tools and metrics for the spacecraft designer to conduct his own conceptual design analyses, such as the net gain, the network efficiency and the dynamically evolving η–Δ graph. In conclusion, beyond specific results, this dissertation introduced a general framework and techniques that allow precisely quantifying survivability features of spacecraft and space-based networks.

CHAPTER 8

CONCLUSION AND RECOMMENDATIONS FOR FUTURE WORK

8.1. Summary

This dissertation explored the relationship of spacecraft and space-based networks with time, and more particularly how they degrade and fail in time. The focus of this dissertation was twofold: the first part dealt with reliability and multi-state failure analyses based on the statistical analysis of a large sample of Earth-orbiting satellites, when the second part introduced a novel framework for the survivability analysis of space-based networks.

Chapter 2 and Chapter 3 are the two installments of Part 1. Chapter 2 was devoted to spacecraft catastrophic failures and presented an extensive reliability analysis of spacecraft and spacecraft subsystems, through nonparametric studies, parametric model development and comparative analyses of subsystem contribution to spacecraft unreliability. Chapter 3 extended the reliability analysis beyond the binary approach of reliability analysis in its traditional understanding (an item being either operational or failed) to analyze anomalies (or partial failures that do not necessary result in the total loss of the spacecraft) of spacecraft subsystems. Chapter 3 presented both a theoretical approach to conduct multi-state analyses and its practical application to spacecraft subsystems. The results refined the comprehension of the progression towards complete failure of the spacecraft subsystems, and help identify problematic subsystems (in addition to the results in Chapter 2) for spacecraft designers to hone in.

As mentioned above, Part 2 was dedicated to the survivability analysis of space-based networks, a newly introduced concept in the space industry that promotes the sharing of on-orbit resources with neighboring orbiting spacecraft. After reviewing the survivability concept and the current state of network analysis, Chapter 4 introduced a survivability framework and proposed an approach to model space-based networks, namely the interdependent multi-layer network approach, to compensate for the perceived shortcomings of current tools. As survivability is the focus of this part, Chapter 5 established the theoretical basis for anomaly and failure propagation across the network interdependent multi-layer model. Chapter 6 was dedicated to the technical validation and characteristics of the survivability analysis using the interdependent multi-layer network modeling, by comparing its performance to alternative modeling techniques such as stochastic Petri nets, or by exploring the scalability of the proposed model. As the validation process demonstrated that the output of the interdependent multi-layer network modeling can be trusted, Chapter 7 presented survivability analyses of specific and non-descriptive subsystems/technologies, and then leveraged these results to provide insights into the conceptual design of future space systems, and potentially space-based networks, from a survivability point of view.

8.2. Contributions

In summary, the contributions of this thesis are as follows:

- Development of reliability models for spacecraft and spacecraft subsystems, in response of the identified need for recent and flight-based spacecraft reliability. This will provide a useful feedback to the space industry and help spacecraft manufacturers prioritize and hone in on problematic subsystems that would benefit most from reliability improvements;

- Development of formal techniques to evaluate multi-state failure behavior and their application to spacecraft subsystems, to improve the understanding of the spacecraft subsystems failure behavior beyond the traditional binary approach of reliability;

- Introduction of a survivability framework, as well as an interdependent multi-layer approach to represent and analyze networks with heterogeneous nodes;

- Development of theoretical foundations for the definition of interdependent multi-layer network proposed in this dissertation, for the anomaly and failure propagation across the network through algorithm, and its validation of for survivability analyses ;

- Leverage of the survivability results from the interdependent multi-layer network approach to gain insights for architectural choices of space-based networks.

8.3. Recommendations for future work

8.3.1. Spacecraft Failure Data, Further Reliability Analyses and Physics of Failure Considerations

As mentioned in the thesis, failure data for spacecraft is limited and the current publicly available databases are not complete, in particular with respect to minor or temporary failures. It is worth addressing a common argument, which is that competitive sensitivity is one reason for the lack of published data and statistical analysis of on-orbit reliability. Although this might be true for spacecraft manufacturers, it is not the case for spacecraft operators (private or government agencies) whose interests are better served by transparent reliability analyses of different spacecraft buses. Furthermore, spacecraft manufacturers could also benefit, in the long-term, in having spacecraft reliability analyzed and published. For example, such studies would constitute a transparent benchmark against which spacecraft manufacturers can compete and hence improve their products. The creation of such databases would allow using the tools presented in this thesis to improve the reliability and multi-state failure models. It could also be interesting to have access to the raw telemetry data, instead of the already processed information shown in current databases. Another reason for the incompleteness of spacecraft failure databases lies with the following: Chapter 2 showed that 5% to 10% of on orbit failures are ascribed to an “unknown” cause and subsystem. This is indicative of the extent of spacecraft State Of Health (SOH) monitoring and telemetry points. Spacecraft health monitoring and diagnostic issues deserve to be carefully analyzed and discussed in future work.

In this dissertation, it was implicitly assumed that subsystem failures are independent. In reality, some subsystems may have dependent anomalies and failures, for example the thermal and power subsystems. Unfortunately, the information available in the database, and sometimes in the satellite operator's incident report itself, does not explicitly address failure dependence. For example, a spacecraft Class I failure is ascribed to only one subsystem, and a partial failure of a subsystem has its timing and severity recorded. As noted previously, the statistical analysis in this work is enabled by and confined to the data available. As a result, common-cause and dependent anomalies and failures of spacecraft subsystems cannot be clearly identified and statistically analyzed. Such analyses however are of importance and constitute fruitful avenues for future research when the requisite data are collected.

Finally, the statistical approach adopted in this work pushed the limit in the development of actionable results of spacecraft reliability and subsystems multi-state failures. The next step ought to focus on and investigate the physics of failure of spacecraft and spacecraft subsystems—their actual failure modes and mechanisms.

8.3.2. Interdependent Multi-Layer Network Tool

This dissertation presented the theoretical foundations of the interdependent multi-layer networks, as well as the failure propagation across space-based networks. This thesis also introduced metrics and tools to efficiently gauge the survivability characteristics of the architectures under consideration. Future work on the subject could be related to the creation of an integrated software with a graphical interface to allow the quick building of the space-based network and dispense of the manual creation of the adjacency and interlayer matrices and the mapping function. This integrated tool could also be coded in a more performing language, such as C or Fortran, to compensate for the memory and speed shortcomings of MATLAB, used in this dissertation. The use of these languages could enable the use of Monte Carlo simulations with higher numbers of runs for an enhanced output precision, and bring the simulation time to allow quasi-real time network modifications. Finally, a graphic interface for the presentation of the simulation output, using the η–Δ graph dynamically by exploring different on-orbit time horizons, or subsystems failure behaviors as done in 7.3.10 could be a useful tool for the spacecraft designer.

8.3.3. Generalization and Extension of Applicability

In this thesis, non-repairable subsystems were considered: it can be seen in the multi-state failure diagram (Figure 3.3) as there is no arc towards less severe degradation states. This choice comes from the fact that maintenance is quasi-impossible on spacecraft (no easy physical access) and that very few actual transitions occurred in the "healing" direction in the spacecraft sample studied in this dissertation. In addition, the definition of some classes of events in the SpaceTrak database clearly specifies that the anomalies or failures pertaining to these classes were non-repairable. However, the multi-state approach presented in this thesis could be applied to repairable systems as part of future work by extending the process to derive their associated probabilities of transitioning (in the same fashion than for the transitions presented in this dissertation). Further work could also capture additional aspect of different repair policies (corrective versus preventive maintenance, or different types of repairs (e.g., as good as new)) by modulating the probability distributions. In the case of the interdependent multi-layer approach, repairs could also be handled by considering an additional effect that would re-enable the node functionality that was rendered unavailable through the interdependency effects.

Also in this thesis, all the nodes belonging to the same layer were assumed to share the same degradation and failure behavior. Dissimilar redundancy (i.e., the redundant node does not have the same degradation and failure behavior) can be considered in future work by implementing different probability distributions for the nodes of interest.

Finally, the interdependent multi-layer approach was applied to space-based networks and the modeling of the nodes and links, as well as the interdependency effects were tailored to this type of systems. However, the interdependent multi-layer approach has a potential broad appeal to the modeler, as it could be extended in future work to model different types of networks, or even other engineering systems (not necessary networks in the traditional sense) where clear functionalities can be defined and are distributed across the architecture: the proposed approach in this thesis can be adapted to these systems by properly defining the nodes and links, as well as introducing other interdependency schemes if need be. For example in the case of space systems, it is suggested that the interdependent multi-layer framework can be adapted to analyze redundancy within monolith spacecraft subsystems.

8.3.4. Multi-Criteria Analysis

In this dissertation, the survivability characteristics were studied by determining the probability of unavailability of the payload node. More complex architectures with several payloads for example, might require more advanced survivability metrics and part of the future work on space-based network survivability could be related to the investigation of appropriate metrics pertaining to these cases.

All the analyses conducted in this dissertation were done from a survivability point of view by considering endogenous failures, implying that the failures arising in the network were generated according to failure distributions internal to the spacecraft subsystems. However, recall that survivability can be defined as the "capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents" (Ellison, *et al.*, 1999). As a consequence, another aspect of the survivability of space-based networks is their ability to withstand targeted attacks, such as collisions with orbital debris, or anti-satellite (ASAT) attacks from antagonist entities. Exploring the space-based network response with respect to the modulation of the threat profile (random or targeted failures) might lead to interesting insights for the choice or design of architectures.

Also, survivability enhancements are usually coming at a cost. In the case study, the survivability improvement was obtained by designing, manufacturing and launching an additional spacecraft. Future work would be in the form of systematically evaluating the cost of space-based networks in addition to its survivability metrics.

The consideration of survivability metrics, cost and potentially other performance metrics for space-based networks paves the way for multi-criteria or multi-objective analyses, with the use of multi-criteria decision support tools for the spacecraft designer.

REFERENCES

Ajmone Marsan, M., “Stochastic Petri Nets: an Elementary Introduction,” In: *Advances in Petri Nets*, Berlin, Germany: Springer-Verlag, 1989, pp.1–29.

Albert, R., Barabási, A.-L., “Statistical Mechanics of Complex Networks,” *Reviews of Modern Physics*, Vol. 74, No. 1, 2002, pp. 47–97

Ansell, J. I., Phillips, M. J., *Practical Methods for Reliability Data Analysis*, Oxford, U.K.: Clarendon, 1994

ARINC Research Corporation, “Final Report, Satellite Reliability Spectrum,” Report No. 173-5-280, 30 January 1962

Ash, J., Newth, D., “Optimizing Complex Netwokrs for Resilience Against Cascading Failures,” *Physica A*, Vol. 380, 2007, pp. 673–683

Atkinson, D. B., *et al*., “Design of Fighter Aircraft for Combat Survivability,” *Society of Automotive Engineers, National Aeronautic and Space Engineering and Manufacturing Meeting*, Los Angeles, CA, 6–10 October 1969; paper 690706

Baker, J. C., Baker, G. A., “Impact of the Space Environment on Spacecraft Lifetime,” *Journal of Spacecraft and Rockets*, Vol. 17, No. 5, 1980, pp.479–480

Ball, R. E., Atkinson, D. B., “A History of the Survivability Design of Military Aircraft,” *AIAA/ASME/ASCE/AHS/ASC, 36th Structures, Structural Dynamics and Material Conference*. New Orleans, LA, 10–12 April 1995; paper AIAA-1995-1421

Bean, E. E., Bloomquist, C. E., “Reliability Data from In-Flight Spacecraft,” *15th Annual Symposium on Reliability*, 1968

Bedingfield, K. L., Leach, R. D., Alexander, M. B., “Spacecraft System Failures and Anomalies Attributed to the Natural Space Environment,” NASA Reference Publication 1390, 1996

Berget, R. T., “Command and Data Handling,” In: Wertz, J. R., Larson, W. J., *Space Mission Analysis and Design*, 3rd ed., Hawthorne, CA: Microcosm Press and New York, NY: Springer, 1999, pp. 395–407

Binckes, J. B., “Satellite Reliability Estimation: Past and Present Procedures,” *NATO ASI Series, Series F: Computer and Systems Sciences*, No. 3, 1983, pp. 333–335

Brandhorst, H. W., Rodiek, J. A., “Space Solar Array Reliability: a Study and Recommendations,” *Acta Astronautica*, Vol. 63, Nos. 11–12, 2008, pp.1233–1238

Brown, O., Eremenko, P., "The Value Proposition for Fractionated Space Architectures," In: *Proceedings of the AIAA Space 2006 Conference*, San Jose, California, USA, 19–21 September 2006, paper AIAA-2006-7506

Brown, O., Eremenko, P., "Fractionated Space Architectures: A Vision for Responsive Space," In: *Proceedings of the 4th Responsive Space Conference*, Los Angeles, CA, USA, 24–27 April 2006, paper RS4-2006-1002

Buldyrev, S. V., *et al.*, "Catastrophic Cascade of Failures in Interdependent Networks," *Nature*, Vol. 464, 15 April 2010, pp. 1025–1028

Castet, J.-F., Saleh, J. H., "Satellite Reliability: Statistical Data Analysis and Modeling," *AIAA Journal of Spacecraft and Rockets*, Vol. 46, No. 5, 2009, pp. 1065–1076

Castet, J.-F., Saleh, J. H., "Geosynchronous Communication Satellite Reliability: Statistical Data Analysis and Modeling," *27th IET and AIAA International Communications Satellite Systems Conference*, Edinburgh, UK, 1–4 June 2009

Castet, J.-F., Saleh, J. H., "Satellite and Satellite Subsystems Reliability: Statistical Data Analysis and Modeling," *Reliability Engineering and System Safety*, Vol. 94, No. 11, 2009, pp. 1718–1728

Castet, J.-F., Saleh, J. H., "Beyond Reliability, Multi-State Failure Analysis of Satellite Subsystems: a Statistical Approach," *Reliability Engineering and System Safety*, Vol. 95, No. 4, 2010, pp. 311–322

Castet, J.-F., Saleh, J. H., "Stochastic Petri Nets for System Survivability and Multi-State Failure Analyses with Application to Space Systems," AIAA-2011-1815, *52nd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, Denver, CO, Apr. 4-7, 2011

Castet, J.-F., Saleh, J. H., "On the Concepts of Survivability and Resiliency, with Application to Spacecraft and Space-Based Networks: Characterization, Stochastic Modeling, and Analysis," *Reliability Engineering and System Safety*, Vol. 99, 2012, pp. 123–138

Cho, M., "Failure Mechanisms and Protection Methods of Spacecraft Power System," *Proceeding of 2005 International Symposium on Electrical Insulating Materials*, Kitakyushu, Japan, 5–9 June 2005

Crucitti, P., Latora, V., Marchioori, M., "Model for Cascading Failures in Complex Networks," *Physical Review E*, Vol. 69, No. 4, 2004

Dempster, A. P., Laird, N. M., Rubin, D. B., "Maximum Likelihood from Incomplete Data via the EM Algorithm," *Journal of the Royal Statistical Society. Series B*, Vol. 39, No. 1, 1977, pp.1–38

DoD Regulation 5000.2-R, “Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs,” 11 May 1999

Donges, J. F., *et al*., “Investigating the Topology of Interacting Networks – Theory and Application to Coupled Climate Subnetworks,” *The European Physical Journal B*, 2011

Dubos, G. F., **Castet, J.-F.**, Saleh, J. H., “Statistical Reliability Analysis of Satellites by Mass Category: Does Spacecraft Size Matter?,” *Acta Astronautica*, Vol. 67, Nos. 5–6, 2010, pp. 584–595

Dubos, G. F., Saleh, J. H., “Comparative Cost and Utility Analysis of Monolith and Fractionated Spacecraft Using Failure and Replacement markov Models,” *Acta Astronautica*, Vol. 68, Nos. 1–2, 2011, pp.172–184

Ellison, B., *et al.*,“Survivable Network Systems: An Emerging Discipline,” Carnegie-Mellon Software Engineering Institute Technical Report CMU/SEI-97-TR-013, Pittsburgh, PA, May 1999 (1997 revised version)

Fortescue, P. W., Stark, J., Swinerd, G., *Spacecraft Systems Engineering*, 3rd ed., Hoboken, NJ: Wiley, 2003, p. 589

Gu, C.-G., *et al*., “Onset of Cooperation Between Layered Networks,” *Physical Review E*, Vol. 84, 2011

Haizhuang Kang, *et al.*, “A New Survivability Measure for Military Communication Networks”, *Military Communications Conference*, Vol. 1, IEEE, 1998, pp. 3–4

Haas, P., *Stochastic Petri Nets: Modelling, Stability, Simulation*. New York: Springer-Verlag, 2002

Hecht, M., Fiorentino, E., “Reliability Assessment of Spacecraft Electronics,” *Annual Reliability and Maintainability Symposium*, 1987

Hecht, M., Fiorentino, E., “Causes and Effects of Spacecraft Failures,” *Quality and Reliability Engineering International*, Vol. 4, No, 1, 1988, pp.11-20

Hecht, H., Hecht, M., “Reliability Prediction for Spacecraft. Rome Air Development Center Technical Report,” RADC-TR-85-229, 1985

Hiriart, T., Saleh, J. H., “Observations on the Evolution of Satellite Launch Volume and Cyclicality in the Space Industry,” *Space Policy*, Vol. 26, No. 1, 2010, pp. 53–60

Hiriart, T., **Castet, J.-F.**, Lafleur, J. M., Saleh, J. H., “Comparative Reliability of GEO, LEO, and MEO Satellites,” In: *Proceedings of the 60th International Astronautical Congress*, Republic of Korea: Daejeon, 12–16 October 2009

Kalbfleisch, J. D., Prentice, R. L., *The Statistical Analysis of Failure Data*, New York: John Wiley and Sons, 1980

Kaplan, E. L., Meier, P., “Nonparametric Estimation from Incomplete Observations,” *Journal of American Statistical Estimation*, Vol. 53, No. 282, 1958, pp. 457–481

Kim, S. Y., **Castet, J.-F.**, Saleh, J. H., “Spacecraft Electrical Power Subsystem: Failure Behavior, Reliability, and Multi-State Failure Analyses,” *Reliability Engineering and System Safety*, Vol. 98, 2012, pp. 55–65

Knight, J. C., Strunk, E. A., Sullivan, K. J., “Towards a Rigorous Definition of Information System Survivability,” *Proceedings of DARPA Information Survivability Conference and Exposition*, Vol. 1, 22–24 April 2003, pp. 78–89

Knippel, A., Lardeux, B., “The Multi-Layered Network Design Problem,” *European Journal of Operational Research*, Vol. 183, 2007, pp. 87–99

Krasich, M., “Reliability Prediction Using Flight Experience: Weibull Adjusted Probability of Survival Method,” NASA TR 20060041898, 1995

Kurant, M., Thiran, P., “Layered Complex Networks,” *Physical Review Letters*, Vol. 96, No. 13, 2006

Kurant, M., Thiran, P., “Error and Attack Tolerance of Layered Complex Networks,” *Physical Review E*, Vol. 76, No. 2, 2007

Kvam, P., Vidakovic, B., *Nonparametric Statistics with Applications to Science and Engineering*, New York: Wiley-Interscience, 2007

Landis, G. A., Bailey, S. G., Tischler, R., “Causes of Power-Related Satellite Failures,” *IEEE 4th World Conference on Photovoltaic Energy Conversion*, Waikaloa, HI, 8-12 May 2006

Lawless, J. F., *Statistical Models and Methods for Lifetime Data*, 2nd ed., New York: Wiley, 2003

Leventhal, A., Bloomquist, C. E., Joseph, J. A., “Spacecraft Failure Rates – Where Are We?,” *IEEE Proceedings of the Annual Symposium on Reliability*, Vol. 2, No. 1, 1969, pp. 444–452

Lisnianski, A., Levitin, G., *Multi-State System Reliability: Assessment, Optimization and Applications*, Singapore: World Scientific, 2003

McLachlan, G. J., Krishnan, T., *The EM Algorithm and Extensions*, 2nd ed., New York: Wiley-Interscience, 2008

Meeker, W. O., Escobar, L. A., *Statistical Methods for Reliability Data*, New York: Wiley, 1998

MIL-HDBK-217, *Military Handbook, Reliability Prediction of Electronic Equipment*, 1965-1995

MIL-HDBK-336-1, *Military Handbook, Survivability, Aircraft, Nonnuclear, General Criteria*, Vol. 1, 25 October 1982

MIL-HDBK-2069, *Military Handbook, Aircraft Survivability*, 10 April 1997

MIL-STD-2069, *Military Standard Requirements for Aircraft Nonnuclear Survivability Program*, 24 August 1961

Motter, A. E., Lai, Y.-C., "Cascade-Based Attacks on Complex Networks," *Physical Review E*, Vol. 66, 2002

Newman, D.E., *et al.*, "Risk Assessment in Complex Interacting Infrastructure Systems," *Proceedings of the 38th Hawaii International Conference on System Sciences*, 3–6 January 2005, Big Island, HI

Newman, M. E. J., *Networks, an Introduction*, Oxford University Press, 2010

Norris, H. P., Timmins, A. R., "Failure Rate Analysis of Goddard Space Flight Center Spacecraft Performance During Orbital Life," *Annual Reliability and Maintainability Symposium*, 1976

Peterson, J. L., "Petri Nets," *Computing Surveys*, Vol. 9, No. 3, 1977, pp. 223–252

Peterson, J L., *Petri Net Theory and the Modeling of Systems*, Englewood Cliffs, N.J.: Prentice Hall, 1981

Rausand, M., Høyland, A., *System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd ed, New York: Wiley-Interscience, 2004, pp.465–524

Rinaldi, S. M., "Modeling and Simulating Critical Infrastructures and Their Interdependencies," *Proceedings of the 37th Hawaii International Conference on System Sciences*, 5–8 January 2004, Big Island, HI

Robertson, B. and Stoneking, E., "Satellite GN&C Anomaly Trends," *AAS Guidance and Control Conference*, 2003

Saleh, J. H., **Castet, J.-F.**, *Spacecraft Reliability and Multi-State Failures: A Statistical Approach*, Chichester, U.K.: John Wiley & Sons, 2011

Saleh, J. H., Lamassoure, E., Hastings, D. E. and Newman, D. J., "Flexibility and the Value of On-Orbit Servicing: a New Customer-Centric Perspective," *Journal of Spacecraft and Rockets*, Vol. 40, No. 1, 2003, pp. 279–291

Saleh, J. H., Marais, K., "Highlights From the Early (and Pre-) History of Reliability Engineering," *Reliability Engineering and System Safety*, Vol. 91, No. 2, 2006, pp. 249–256

SpaceTrak, Ascend Worldwide [online database], http://www.ascendworldwide.com/what-we-do/ascend-data/space-data/space-trak.html [retrieved May 26, 2010]

Sperber, R., "Analysis of the Public Record of Spacecraft Anomalies," *13th AIAA International Communication Satellite Systems Conference and Exhibit (ICSSC)*, Los Angeles, CA, 11–15 March 1990, pp. 42–51

Sperber, R., "Better With Age and Experience – Observed Satellite In-Orbit Anomaly Rates," *15th AIAA International Communication Satellite Systems Conference and Exhibit (ICSSC)*, San Diego, CA, 28 February–3 March 1994, pp. 1162–1167

Sperber, R., "Hazardous Subsystems," *SatMax 2002: Satellite Performance Workshop*, Arlington, Virginia, 2002

Tafazoli, M., "A Study of On-Orbit Spacecraft Failures," *Acta Astronautica*, Vol. 64, Nos. 2–3, 2009, pp. 195–205

Timmins, A. R., "A Study of the First-Month Space Malfunctions," NASA Technical Report TN-D-7750, 1974

Timmins, A. R., "A Study of the Total Space Life Performance of GSFC Spacecraft," NASA Technical Report TN-D-8017, 1975

Timmins, A. R., Heuser, R. E., "A Study of First-Day Space Malfunctions," NASA Technical Report TN-D-6474, 1971

Titterington, D. M., Smith, A. F. M., Makov, U. E., *Statistical Analysis of Finite Mixture Distributions*, New York: John Wiley & Sons, 1985

Volovoi, V., "Modeling of System Reliability Petri Nets with Aging Tokens," *Reliability Engineering and System Safety*, Vol. 84. No. 2, 2004, pp. 149–161

Volovoi, V., "Stochastic Petri Nets Modeling SPN@," *Reliability and Maintainability Symposium (RAMS)*, Newport Beach, CA, 26–29 January 2006; paper 2006RM-166

Volovoi V., Vega, R., "On Compact Modeling of Coupling Effects in Maintenance Processes of Complex Systems," *International Journal of Engineering Science*, Vol. 51, 2012, pp. 193–210

Wertz, J., Larson, W., *Space Mission Analysis and Design*, 3rd ed., Torrence, CA: Microcosm Press, and Dordrecht, The Netherlands: Kluwer Academic, 1999

Westmark, V. R., “A Definition for Information System Survivability”, *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, 5–8 Jan. 2004

Wong-Jiru, A., *et al.*, “Graph Theoretical Analysis or Network Centric Operations Using Multi-Layer Models,” *Conference on System Engineering Research*, 14–16 March 2007, Hoboken, NJ

Xu, X.-L., *et al.*, “Interconnecting Bilayer Networks,” *Europhysics Letters*, Vol. 93, 2011

Zio, E., Sansavini, G., “Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins,” *IEEE Transactions on Reliability*, Vol. 60, No. 1, 2001, pp. 94–101

VITA

Jean-François Castet was born in Bayonne, France, and grew up on the French side of the Basque Country. He graduated summa cum laude from high school in 2003, and pursued a 2-year special program in mathematics and physics (preparatory classes) at Lyçée Michel Montaigne in Bordeaux, France, to prepare for competitive entrance exams of French engineering schools. In parallel, he obtained the equivalent of an Associate's degree in Sciences and Technologies, specialized in physics and engineering at Université de Bordeaux, Bordeaux, France. He was admitted in 2005 to SUPAERO (Ecole Nationale Supérieure de l'Aéronautique et de l'Espace, the French engineering School of Aeronautics and Space). In 2007, he was selected to purse a double-diploma program through an agreement between SUPAERO and the Georgia Institute of Technology, and moved to Atlanta to complete a Master of Science in Aerospace Engineering, which he obtained in May 2009. Jean-François then decided to remain in the School of Aerospace Engineering at Georgia Tech and continue his work with Dr. Joseph H. Saleh on spacecraft reliability, multi-state failures and survivability. During the summer of 2011, Jean-François got the opportunity to do a 3-month internship in the European Space Operations Center (ESOC), Darmstadt, Germany, a center of the European Space Agency (ESA).