ABSTRACT

Title of Document:	APPLYING RELIABILITY ANALYSIS TO DESIGN ELECTRIC POWER SYSTEMS FOR MORE-ELECTRIC AIRCRAFT
	Baozhu Zhang, Master of Science, 2014
Directed By:	Research Assistant Professor Huan Xu, Aerospace Engineering and Institute for Systems Research

The More-Electric Aircraft (MEA) is a type of aircraft that replaces conventional hydraulic and pneumatic systems with electrically powered components. These changes have significantly challenged the aircraft electric power system design. This thesis investigates how reliability analysis can be applied to automatically generate system topologies for the MEA electric power system. We first use a traditional method of reliability block diagrams to analyze the reliability level on different system topologies. We next propose a new methodology in which system topologies, constrained by a set reliability level, are automatically generated. The path-set method is used for analysis. Finally, we interface these sets of system topologies with control synthesis tools to automatically create correct-by-construction control logic for the electric power system.

APPLYING RELIABILITY ANALYSIS TO DESIGN ELECTRIC POWER SYSTEMS FOR MORE-ELECTRIC AIRCRAFT

By

Baozhu Zhang

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Master of Science
2014

Advisory Committee:
Research Assistant Professor Huan Xu, Chair
Associate Professor Mark Austin
Associate Professor Gang Qu

Acknowledgements

I will like to express my most sincere gratitude to Dr. Huan Xu, my academic advisor, whose attitude and genius has gotten me thus far. Her support was not only limited to providing me with guidance, but also included giving me the freedom to pursue my own interests. She acted as a mentor by sharing her vast insight and wisdom that guided me to the right direction. Dr. Huan Xu is also a friend who has giving me encouragement at all times - weekdays and weekends, day and night. She has been always there for me when I encounter any trouble or questions. Without her supervision and constant help, this thesis will not have been possible.

I will also like to thank my defense committee members, Dr. Mark Austin and Dr. Qang Qu, for their helpful commentary and feedback. Dr. Austin had been my instructor for two different courses. During these two courses, Dr. Austin did his best to help and support me with my thesis work. His door has been always open whenever I needed help, and I am truly grateful to have been his student.

Another special thanks to my best friends Kathleen Seay, Beserat Debebe, Angela Ng and other friends who helped and supported me in finishing this thesis.

Finally, I want to thank my lovely parents and my brother who have always supported me continuing my education. My lovely mother has always cooked and cleaned for me so that I have enough time to work on my school works and eat nutritious food. I dedicate this thesis to her. Without her dedication, I would not be where I am now.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction and Background

1.1<u>Thesis Overview</u>

Increasing reliance on electric power systems has recently become popular in overall aircraft design. The increasing used of electric power systems in aircraft design had increased the level of Safety-criticality in an aircraft electric power system. Unlike traditional hydraulic systems, the electric power system is more flexible in design and weighs less, thus reducing fuel consumption. More subsystems now rely on electric power, demanding we guarantee the safety of every aircraft while at the same time trying to design a system that is much more complex. This thesis investigates how reliability analysis can be applied to the automatically generated candidate system topologies for the More-Electric Aircraft (MEA) electric power system. Topologies are linked to control synthesis techniques that automatically construct controllers to actuate contactors in order to provide power to buses and loads. this design a controller to actuate contactors in order to provider power to the buses and loads. The goal of this thesis is to select a reliable number of electric components and the connectivity between electric power components that will produce a consistent reliability level. Reliability is the ability of a system or a product to operate under calculated operating conditions for a designed life cycle [19]. In the next section, we describe MEA and how they differ from the traditional aircraft.

1.2 <u>More-Electric Aircraft (MEA)</u>

The MEA replaces traditional hydraulic and pneumatic systems with electrically powered components [3, 18]. The electrical systems offer more design flexibility than the hydraulic and pneumatic system. Instead of controlling the system with hydraulic, pneumatic and mechanical systems, the MEA is controlled by high-speed electric motors [3]. When the plane is lighter, it requires less fuel to maintain the operation. This also means it can fly faster and be more fuel efficient (because less thrust is required to balance this smaller drag from less weight) [12]. Current MEA models include the F-35 Fighter, Airbus A380, and Boeing 787 [37].

The concept of the electric aircraft has been around since the 1940’s but due to the lack of electric power capabilities, it did not become popular until recently [10]. Figure 1 compares the electric generation and distribution on a traditional aircraft with a MEA (Boeing 787). As it can be seen from Figure 1, the traditional airplane has only one generator on each of the two main engines and one generator on the auxiliary power unit [5]. Boeing 787 has two generators on each engine and two generators on the auxiliary power unit.

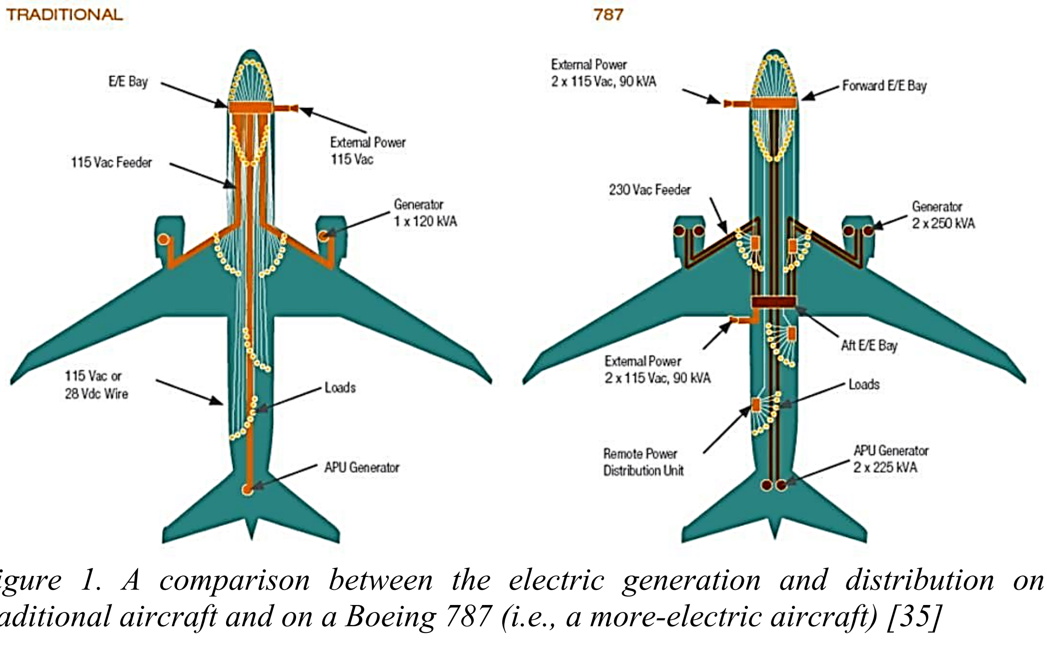


Figure 1. A comparison between the electric generation and distribution on a traditional aircraft and on a Boeing 787 (i.e., a more-electric aircraft) [35]

Despite MEA's benefits, it also creates new uncertainties. Replacing the hydraulic pneumatic system, mechanical system and subsystem with the electric equivalents system, there is more components need to be controlled, and more subsystems interact with each other because they all rely on electric power. Finding errors, or sequences of events leading to errors, is difficult.

In summary, to compare the traditional and the more advanced electric system, we will examine the differences electric power system between Boeing 777 and Boeing 787.

1.2.1 Traditional Power System

On a traditional airplane, the power is extracted from the engines in two different ways:

- Engine-driven generators, which power the electrical system.
- Diverting hot, high-energy air from the engines into the pneumatic system.

Each engine has one generator, which spins when the engine is running to produce electrical power. The pneumatic system, also known as a "bleed-air" system, bleeds air off the engines to power other systems [37].

For example, Boeing 777 has a twin engine with each engine having a 120-kVA generator. This is one 120-kVA Auxiliary Power Unit (APU) driven generator with one 7.5 kVA Ram air turbine.

1.2.2 More-Electric Power System

The 787 Dreamliner uses electricity, not pneumatics, to power airplane systems and relies on electricity more than any other Boeing airplane [37]. Unlike other models, electricity on board the 787 powers things such as environmental controls, engine start-up, hydraulics and wing ice prevention [37]. This innovative “bleedless” system provides many benefits over pneumatic systems. These benefits include: (i) Eliminates heavy ducts, valves and controls, (ii) Eliminates maintenance associated with pneumatic systems, and (iii) Extracts significantly less energy from the engines.

For example, Boeing 787 has adopted the three-phase 230 VAC electric-power instead of the conventional three-phase 115 VAC arrangement that Boeing usually uses. This increases the voltage by a 2:1 factor and decreases the feeder losses in the electrical distribution system, which allows significant wiring reduction. There are two 250 kVA generators per engine and two 225 kVA APU mounted generators. In addition, Boeing 787 also powers 230 VAC loads and the electrical power is converted into 115 VAC and 28 VDC power to feed into other sub-systems that need power supplies [20].

Because there are thousands of components in an aircraft, the connectivity between components can be very complex. In this thesis, our primary goal is to generates topologies with a given reliability level. In the next section, we present the electric power components that we consider in this thesis.

1.3 Electric Power System Components

Depending on the manufacturer, each electric power system component has various reliability rates, and placing them in different positions at the electrical circuits can lead to different reliability of the eclectic power system. Placing the components in a different position implies connecting the components in different way. We considered having the components connected with others in a series, parallel or complex format. A complex system is one that is neither series nor parallel, nor parallel-series.

A main focus of this thesis is to study the different reliability levels that result from different connectivity of the components. The topologies formed by the electric power components were mainly connected as a complex system, which included components both in series and parallel. The topologies here in this thesis were composed of a set of components with different component combinations. Although an MEA had thousands of components, in this thesis, for the purpose of simplicity we scaled down the number of components to ranges of six to eight components. The following is a brief description of the electric power components found in an electric power system.

Generators: Generators are connected to engines and can operate in high or low voltages. For example, the AC generator for Boeing 787 is 235 VAC while the DC generators are 270 VDC.

Buses: Buses deliver power to loads or power conversion equipment. More sophisticated electrical systems usually include multiple voltage systems with a combination of AC and DC buses to power various aircraft components [35, 36].

Contactors: A contactor is an electrically controlled switch used to switch a power circuit. Contactors provide the actuation for reconfiguration of the topology's electric power system; hence, changing the paths through which power is delivered from generators to loads depends on the contingencies [35,36].

Transformer Rectifier Units: Transformers will step down a voltage level. Rectifiers will convert AC power to DC power. A transformer rectifier unit can do both.

Batteries: Batteries are used to provide emergency backup power to avionics equipment and provide ground power capability for maintenance and preflight checkouts.

RAM Air Turbine: The RAM Air Turbine (RAT) is an emergency device that provides backup electrical and hydraulic power when there is a loss of multiple main generators [35].

Overall this section introduces the different type of electric power component and each component is part of the system. Placing each component in different position can affect the overall system's reliability level. In this section, we introduced all the components in an electric power system, and this is the reliability rate for the overall system calculated. In the next section, we describe the system requirements and how it affects the safety.

1.4 Reliability Requirements

The basic reliability requirement for the designer is that no single failure can cause the loss of an aircraft. The electric power system design needs to be able to demonstrate a capability that fulfills a probability of failure less than 10^{-9} per flight hours, which mean no single failure can occur within 10^{-9} flight hours. In this thesis, we mainly focus on the catastrophic failure. This means that the system designer will be required to implement fail-safe features in the design, and it will have to demonstrate the appropriate analysis that the design is capable of meeting or exceeding a probability of failure less than 10^{-9} per flight hours [20, 24]. Examples of catastrophes will be the loss of an aircraft, wings cut off, cabin pressurization, etc. – anything that prevents a pilot from saving the aircraft.

Calculating correctly the reliability level plays an important role in designing the electric power systems. In the next section, we present the reliability analysis methods we used in this thesis.

1.5 Reliability Analysis Methods

We performed the system reliability analysis into two different procedures. In the first procedure, different reliability methods were used to calculate a given electric power system topology. The second procedure automatically generated candidate system topologies that could potentially meet the reliability requirement. In these two design procedures, we applied RBD and path-set method to the calculations.

In the traditional method calculation, we primarily used the Reliability Block Diagram (RBD) to develop topologies. RBD's are models that are used to analyze the performance of the system, and RBD primarily depends on its physical arrangements.

During the proposed method calculation, we used a method call 'path-set' to calculate the reliability, and 'path-set' was part of the complex system methods.

1.5.1 General Equations to Calculate MTBF

Calculations of MTBF assume that a system is ‘renewed’, i.e. fixed, after each failure, and then returned to service immediately after failure [19]. The average time between failing and being returned to service is termed Mean Down Time. As shown in Figure 2, the definition of MTBF is the sum of the operational period (“start of down time” subtract “start of up time”) divided by the number of observed failures.

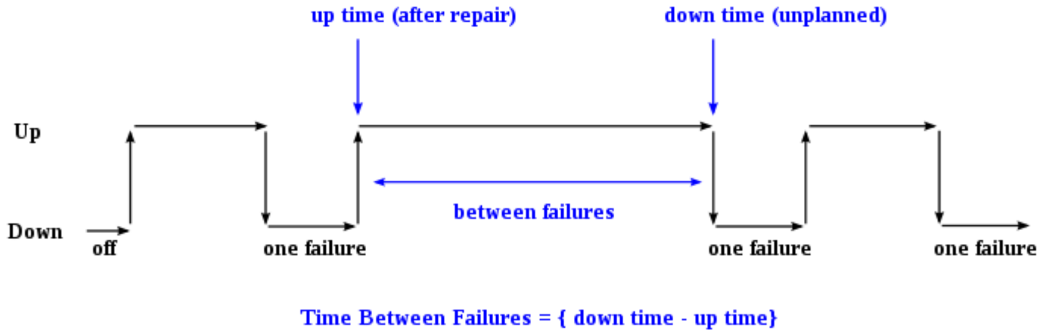


Figure 2. Definition of Mean Time between Failures (where MTBF is the sum of the operational period (“Start of down time” subtract “start of up time”) divided by the number of observed failures)

We can express the MTBF in a formula as

$$MTBF = \frac{\sum(T_d - T_u)}{\sum(F_i)},$$

Where T_d is the start of down time, T_u is the start of up time and $\mathrm{F_i}$ was the number of observed failures.

1.5.2 Reliability Black Diagram

A Reliability Block Diagram (RBD) performs the system reliability and availability analysis on large and complex systems using block diagrams to show network relationships. It has frequently been used to model the effect of a failure item on a system’s performance. We can separate Reliability Block Diagrams into three different types [19]:

a. In series (when all of the blocks work, the system works):

b. In parallel (System fails when all blocks fail)

c. *Complex systems* – parallel-series system, but most systems are a combination of the two.

We can analyze a complex system or parallel-series system by dividing it into its basic parallel and series modules and then determining the reliability function for each module. Figure 3 shows a simplified RBD for an aircraft electric power system.

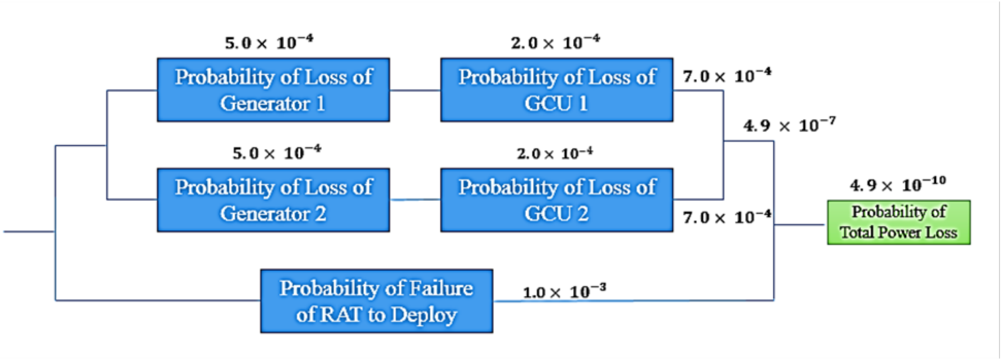

5.0×10^{-4}
Probability of Loss of Generator 1
2.0×10^{-4}
Probability of Loss of GCU 1
7.0×10^{-4}
4.9×10^{-7}
5.0×10^{-4}
Probability of Loss of Generator 2
2.0×10^{-4}
Probability of Loss of GCU 2
7.0×10^{-4}
4.9×10^{-10}
Probability of Total Power Loss
Probability of Failure of RAT to Deploy
1.0×10^{-3}

Figure 3. Simplified RBD for an Aircraft Electric Power System

We used different type of complex system method in our proposed method, and this type of complex system is either parallel or series, but exhibits some hybrid combination of the two. This type of system uses a more computationally intensive method to determine the reliability involved with the use of path-set and cut-set methods [19], and in this thesis, we will be looking at path-set method only.

Compared cut-set and path-set methods, path-set method makes calculation simpler in this thesis. RBD suitable apply to topologies that are neatly laid out in series, parallel or parallel-series only. Topologies generated in our proposed method displays hybrid combination of series and parallel. Therefore we used path-set methods for calculations.

A path-set is a set of units that forms a connection between input and output when traversed in the direction of the reliability block diagram arrows. Thus, a set merely represents a "path" through the graph. A cut set is a set of system elements that, when removed from the system, interrupts all connections between the input and output ends of the system. A minimum cut sets contains no other cut sets within it [19].

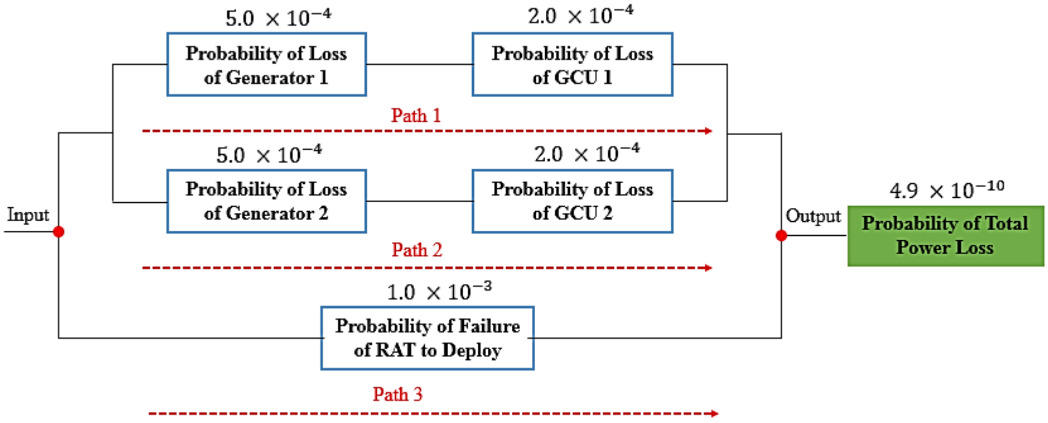

5.0×10^{-4}
Probability of Loss of Generator 1
2.0×10^{-4}
Probability of Loss of GCU 1
Path 1
5.0×10^{-4}
Probability of Loss of Generator 2
2.0×10^{-4}
Probability of Loss of GCU 2
Input
Output
4.9×10^{-10}
Probability of Total Power Loss
Path 2
1.0×10^{-3}
Probability of Failure of RAT to Deploy
Path 3

Figure 4. Simplified Path-Set for an Aircraft Electrical Power System

As shown in Figure 4, there are three paths that can go from input to output and each path follows the direction of an arrow. Path one passes through generator 1 and Generator control unit (GCU) 1 while path two passes through generator 2 and GCU 2. Path three passes through Ram Air Turbine (RAT) only. The RAT generates power from the airstream by ram pressure due to the speed of the aircraft. Each of these paths has their own reliability level, and we can find it on the system reliability level by multiplying it.

After going through different type of reliability analysis methods, we are now ready to apply these methods to our designs. In the following chapter, we present the two different methodologies we used in this thesis.

1.6 Thesis Outline

In this thesis, we present different methods to investigate system topology options for MEA electric power system. We use a traditional methodology to calculate the reliability rate for an electric power system, and propose a new methodology to generate topologies for a given reliability level. We also present the different reliability methods to find the reliability level for different topologies. The reliability method in the traditional methodology is RBD, while we apply put-set methods in the proposed methodology. MATLAB and Python are used for calculations in the two methodologies. Chapter 2 presents the methods in both traditional and proposed methodologies while Chapter 3 and 4 describe the step-by-step procedure for both methods. Chapter 5 discusses the formal specification in synthesizing the control protocols and distributed controller for selected cases. Discussion, evaluation and conclusion are in Chapter 6.

Chapter 2: System Design Methodologies

In our design methodologies, we consider two processes, which are the traditional and the new proposed process. In the traditional design method, we look at the requirement for an aircraft's electric power system and then select the electric power components. Within those electric power components, different brand's components have different reliability values. In this thesis, the reliability value for each type of component is a constant. Selecting the number of components becomes very important when we calculate the overall reliability level for the electric power system. Failure of one component can cause a failure of the entire system. In addition, the connectivity of the components plays an important role in calculating reliability. Placing each component in series or parallel, it affects its overall reliability level. We applied the RBD into the analysis and calculations. For the topologies that did not meet the FAA reliability level requirement, we redesigned them. In this process of design, we aimed to develop a topology that would be the reliable choice for the number of components and their connectivity.

For the proposed design method, we looked at the overall reliabilities for the electric power system and automatically generated a set of candidate topologies that met the reliability level. We applied complex system method into the analysis and calculations of the reliability level. We created a set of candidate topologies by using all the possible combinations of component quantities. Within the set of candidate topologies, we then applied constraints to the topologies. The first constraints limited the values of each type of components in a combination. This meant that at least one component from each type of electric power component was required (e.g. at least one generator was required for each topology). There were also constraints on the connection points between components, such as a generator that cannot connect to another generator.

2.1 Traditional Methodology

The traditional way to determine the reliability level of a system, such as cars, aircrafts and buildings, is by testing the reliability level of each components system and their behaviors in the system. Knowing the reliability values of each component, we can calculate the reliability level of the whole system. In this thesis, the reliability values come from industry tested values obtained from numerous tests, which have increased the reliability of the values [20]. Next, it is to develop topologies, here we are determining the reliability level of a topology by placing the components in different positions, such as in series, parallel or a mix of series and parallel. We then calculate the reliability level of each topology. In this procedure, we applied the Reliability Black Diagram (RBD) to the analysis and used MATLAB as our tool to calculate the reliability. If the overall reliability level does not reach the required level of safety determined by the FAA, then the topology must be redesigned.

2.1.1 Reliability Values

The reliability level of each component in this thesis has been selected based on its reasonable value from industries, since different providers have provided different reliability levels for each component. The reliability level used for each component is shown in the table below:

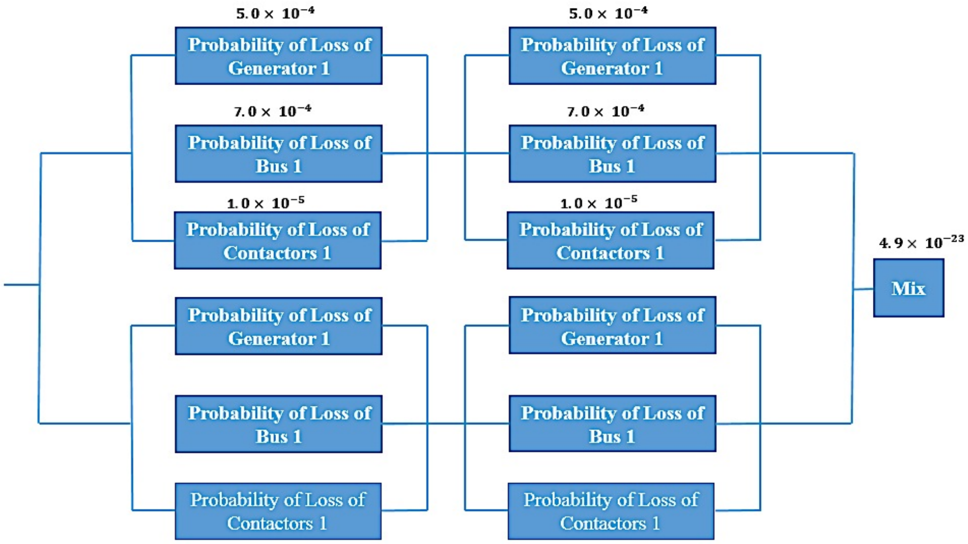
Table 1. MTBF values for components [20]

Component	Symbol	MTBF Value (per flight hours)
Generator	G/g	$5.0{\times}10^{-4}$
Bus	B/b	$7.0\ {\times}10^{-4}$
Conactor	C/c	$1\ {\times}10^{-5}$
Group power units	GCU	$2.0\ {\times}10^{-4}$
Rectifier	R	$1.0\ {\times}10^{-6}$

2.1.2 Designed in Redundancy

Redundancy is a common approach to improve the reliability and availability of a system. In system design, redundancy duplicated the components or functions of a system; this increased the reliability level of the safety-critical system. For electric power system design, applying redundancy in the electric power system means having more than one components of each electric component (e.g. two generators) in the system to increase the reliability of the system. In many safety-critical systems, such as hydraulic systems in the aircraft, it will be applied the triply which is formally termed triple modular redundancy. Within the existing aircraft, Boeing 787 and Airbus 380 applied the triple redundant in their hydraulic system. In a triply redundant system, the system has three sub components, all three of which must fail before the system fails [29]; which increased the reliability level.

Adding redundancy into the design, however, increase the cost and complexity of the system. Yet, if the cost of failure is high enough, redundancy may be an option to the system design. Figure 5 is an example of a topology that has applied redundancy into the design and the final outcome of the topology is $4.9\ {\times}10^{-23}\ per\ flight\ hours$. It means that the failure rate of the system is $4.9\ {\times}10^{-23}$ per flight hours. It also means that the MTBF is $2.04\ {\times}10^{22}$ hours. While this topology meets the reliability requirement, the values also imply that the system has extra components. Overlooking other constraints by focusing on only the MTBF values, we will like to get a topology that has a MTBF value that can be as close to the requirement ($MTBF = 1 \times 10^{-9}\, per\ flight\ hours$) as possible. From this, we come to conclusion that the topology we design should apply redundancy in our electric power system design. This means that we should have at least two components for each important electric power components (e.g. two generators).



5.0×10^{-4}
Probability of Loss of Generator 1
7.0×10^{-4}
Probability of Loss of Bus 1
1.0×10^{-5}
Probability of Loss of Contactors 1
5.0×10^{-4}
Probability of Loss of Generator 1
7.0×10^{-4}
Probability of Loss of Bus 1
1.0×10^{-5}
Probability of Loss of Contactors 1
4.9×10^{-23}
Mix
Probability of Loss of Generator 1
Probability of Loss of Bus 1
Probability of Loss of Contactors 1
Probability of Loss of Generator 1
Probability of Loss of Bus 1
Probability of Loss of Contactors 1

Figure 5. Sample Topology Design in Redundancy

The traditional method was presented in this section. In the next section, we present the opposite direction method which is proposed method.

2.2 Proposed Methodology

In the new proposed process, instead of developing topologies and determining their reliability level, we consider the overall required reliability level and a set of candidate topologies that satisfies the requirements. To begin with, we generate a set of all possible combination topologies, which means generating all different combinations for the chosen number of components. After we generate all combinations, we will eliminate the one that has zero components of any electric power components. Next, based on the characteristic of each electric power components, we define its behavior constraints. For example, we want to avoid connections between two generators, and generator connecting to bus or bus connecting to generator. Right after we apply the behavior constraints to the components, we select the number of connections between components. The more edges in a topology, the better its reliability level. Therefore, we want to correctly select the number of connections between components.

Last but not least, we apply path-set methods to calculate the reliability level of each topology. To do this, we first want to define the input and output components, followed by finding all possible paths between input and output. Each path represents a level of reliability and the more paths a topology has, the higher its reliability level. Python is used to generate topologies and calculate reliability levels.

Within the reliable topologies, we also want to eliminate the topologies that have worsening effects for the overall system. The worsening effect means increasing the weight of the aircraft and the cost of the system. In general, the reliability level is proportional to the cost as shown in Figure 6, the higher the reliability, the higher cost will be [24]. The topologies generated by the tool not only look at its reliability level but also the topology that is low in cost. Comparing the cost with the reliability level, the total cost gets higher as the reliability level increases. The lowest cost happens with a reliability system level right at the reliability index, which comprehensive the required reliability level and total cost. The best sets of topologies are the ones balanced in cost and reliability level.

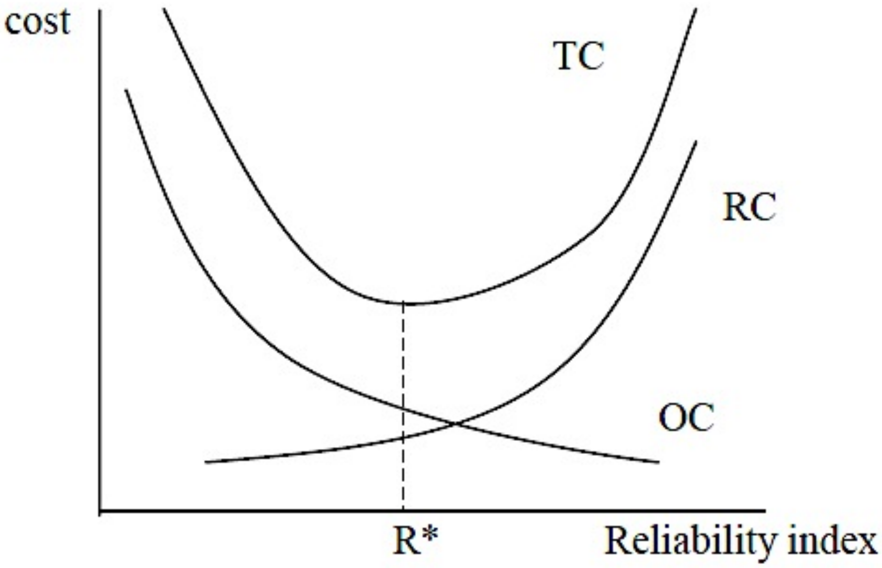


Figure 6. Total Reliability costs where the investment and operating costs can be represented by curve RC, outage cost represented by curve OC. The total cost curve TC is the sum of the individual cost overs RC and OC. Total cost presents a minimum at R, which determines the optimal levels of reliability. [23]*

Chapter 3: Traditional Design Method Using RBD

In this chapter, our primary focus is to determine the total number and combination of components that gives a reliability level that meets the FAA reliability requirement ($10^{-9}\, per\ flight\ hours$). Also, we want to define the reliability difference when placing the components in different positions. We begin by looking at the reliability values for each component and develop topologies that meet the FAA reliability requirement. In order to simplify the procedure, the electric power components selected are generators, buses, and contactors. Also, in order to simplify the calculation, we consider the reliability values for the same type of components that remain the same throughout the entire thesis work. For example, we consider the reliability value of a generator is 5.0×10^{-4} (MTBF is 2000 flight hours). All generators in this thesis use 5.0×10^{-4} as a reliability value.

In electric circuits, parallel circuit is safer and more reliable than series connections [19]. Selecting the best number of components that give a reliability level to meet the requirement and at the same time weighing the least also plays an important role in this thesis. In finding topologies, we apply Reliability Black Diagram (RBD) into the analysis. If the overall reliability level does not reach the required level of safety determined by the FAA, the topology must be redesigned.

In the below MATLAB code, first, we give an abbreviation for all electric components, such as using **G** abbreviated generator, **B** abbreviated bus, **C** abbreviated contactor, **GCU** abbreviated group power unit and the final reliability value abbreviated by R. In this example, there are two generators and two group power units; we define the first generator as **G1** while the second generator as **G2**. We did the same for the other components. For components in series, we add them together; while those components in parallel, we multiply them. Finally, reliability for the simple calculation of an aircraft electrical power system is shown in the last row, which is equal to 4.9 e -10 ($MTBF = 4.9 \times 10^{-10}$ per flight hours). This matches the reliability value we find in the RBD. Now, we are ready to conduct the next step, which is to develop topologies that fulfill the reliability requirements. In the next section, we present sample topologies that develop by applying reliability methods and show in RBD.

3.1 Sample Topologies

Figures 7 to 12 show the sample topologies that we create. All topologies from this set meet the reliability requirements with some exceeding the reliability level. As can be seen from Figure 7 to 12, placing the components in parallel format increases the reliability level while placing the components in a series format leads to a lower reliability level. Comparing topologies from Figure 7 and 8, they both lay in a parallel-series format, and the reliability values for both topologies are met the reliability level. In these two topologies, we place the components in parallel; this guarantees the reliability level. For example, system failures only occur if all components in a same branch (such as all generators or buses) have failures. The only difference between Topology A and B was that Topology B has one less generator than Topology A. Comparing topologies A and B, Topology B was better than topology A due to two facts. One, Topology B has a value that was closer to the FAA requirement, which means that it is closer to the reliability index. Two, both Topology A and B meet the FAA requirements while Topology B has a lighter weight. In aircraft design, we want to minimize all unnecessary extra material. A regular generator weighs around 200 to 300 pounds. An extra generator increases the cost and weight. However, several generators can supply a bigger load, but the minimum of two generators is necessary to maintain a successful operation.

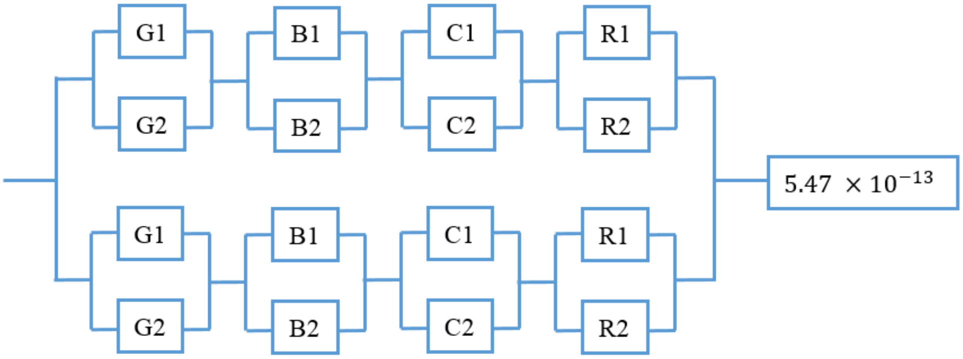


Figure 7. Topology A

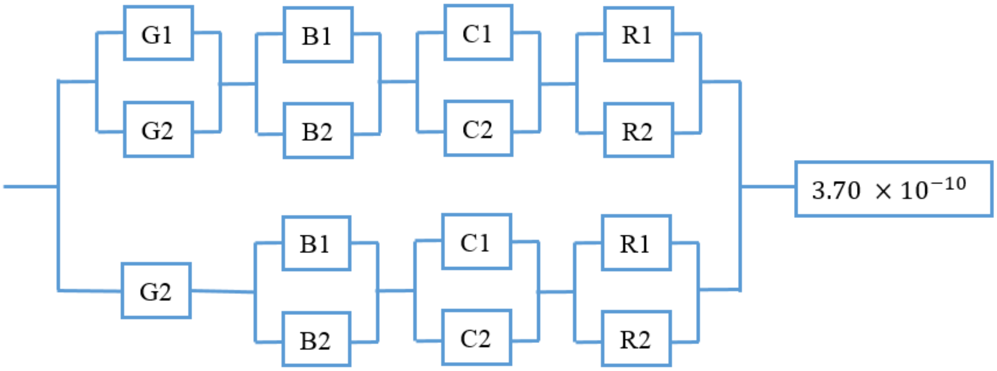


Figure 8. Topology B

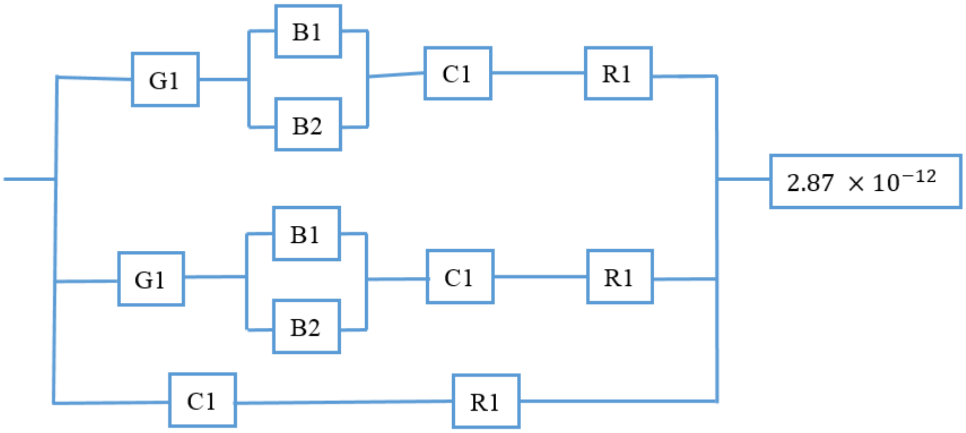


Figure 9. Topology C

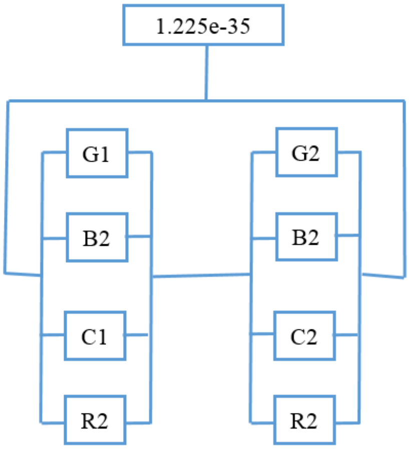


Figure 10. Topology D

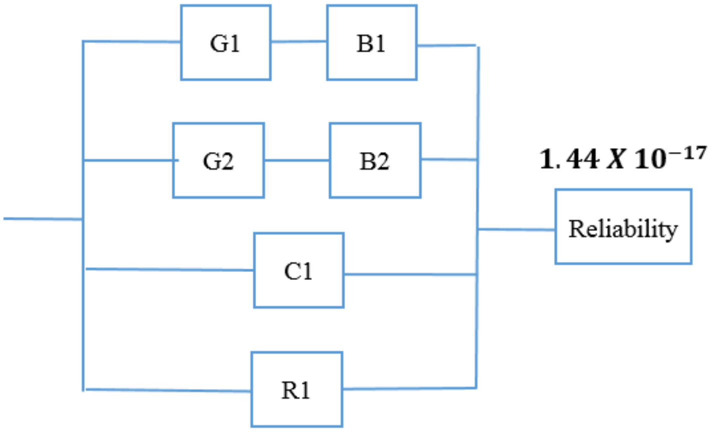


Figure 11. Topology E

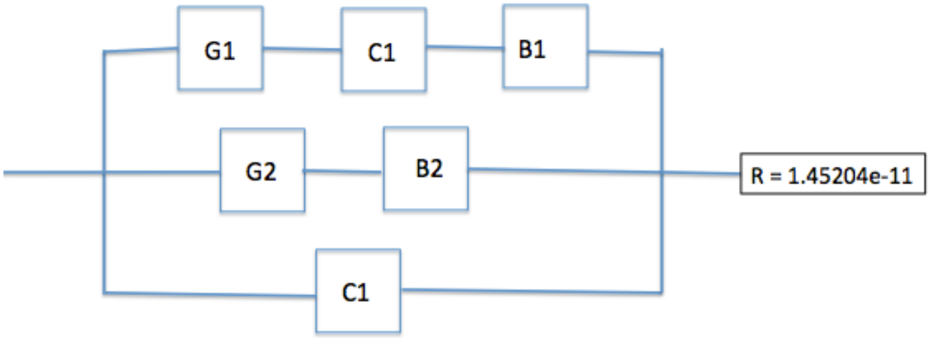


Figure 12. Topology F

Comparing topologies in Figure 8 and 9 (topology C with topology B), we reduce a set of components in topology C and still place them in a series-parallel format. Even though C has fewer components, its reliability level is higher B. The main reason topology C had a higher reliability than topology B was topology C has applied the *triplicate redundancy* into the design while topology is not. Topologies in Figure 10, 11, and 12, topology D, E and F are simply applied in a complex system to all components with the reliability level at the highest level when the system has the highest number of components in the parallel. As is mentioned in Chapter 2, system design, reliability level and total cost are relatively, higher reliability means the higher the cost. Therefore a good desirable topology is the one that meets its system requirement but at the same time uses the least value of components in a complex system.

Chapter 4: Proposed Design Procedure Using Python and Path-set Method

In this chapter, we investigate a "set of topologies" option for the electric power system. These topologies were automatically generated using NetworkX. NetworkX is a Python software package that studies graphs and networks [40]. Each graph is a collection of nodes connected with edges. Consider a topology as a graph ***G = (N, E)*** where ***N*** is the nodes and ***E*** is the edges. The set ***N*** of nodes in the graph contains the following components: generator (***g***), buses (***b***) and contactors (***c***). The set ***E*** are the solid wire links between components [43]. Sample topologies generated by NetworkX are shown below in Figure 13.

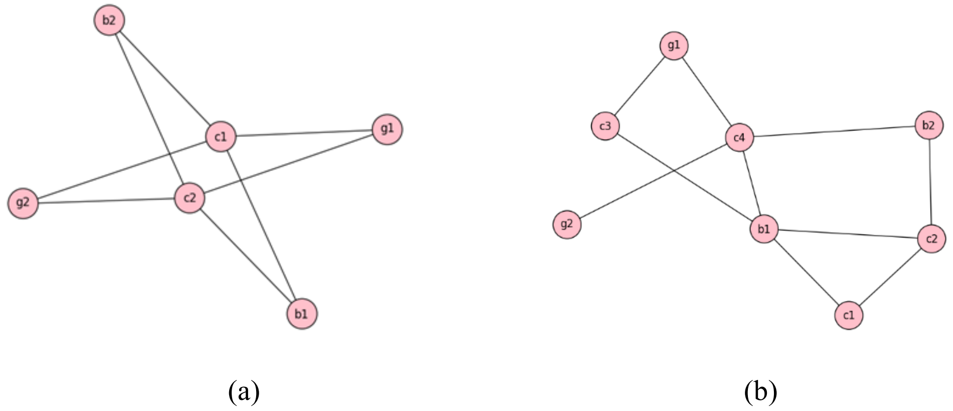


Figure 13. Sample Topologies Generated by NetworkX. (a) Six components with eight edges – two generators, three buses and two contactors. (b) Eight components with ten edges – two generator, two buses and four contactors.

In the topologies of this thesis, we were interested in the reliability level of the generators, buses and contactors. These electrical components represent some of the key features of the aircraft's electric power system, and fewer components simplified the procedure. The reliability values for these components are obtained from the industries as shown in [20]. These values can be varied based on the different brand of components. There are thousands of electric components in an aircraft, for clarity of analysis and ease for the reader, we aimed to develop a set of topologies that had the least number of components but that resulted in a reliability level that met the FAA requirements. Therefore, we scale down the number of components and mainly focused on the six and eight components combinations in the process.

4.1 Constraints

In order to eliminate any physically impossible or unsuitable topologies, we include a set of additional constraints into the design process.

4.1.1 Components (nodes)

We initially input the total number of components. Within these set of combinations, we eliminated the combinations in which there were zero elements of one particular component. For example, for the combination that has zero generator, bus or contactor, we will eliminate that combination. This will leave us with a set of component combinations with at least one component of each electric power component. For example, in the six components event, there are a total of 28 sets of combinations, and these combinations are 015, 420, 501, 222, and etc.

In each combination, where the first position denotes the number of generator, the second position denotes the number of bus and the third position denotes the number of contractor.

- e.g. 015 = 0 generator; 1 bus and 5 contractors

- e.g. 222 = 2 generators, 2 buses and 2 contractors

From this, we eliminated the set of combination from 28 sets to 10 sets for the six components event.

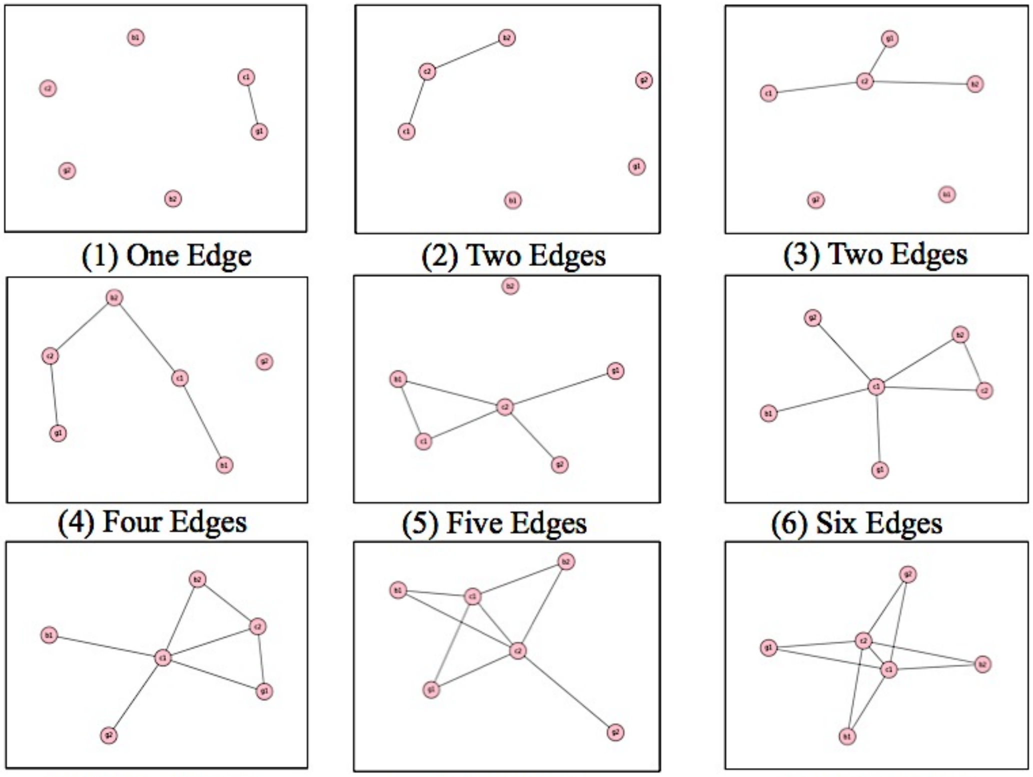
4.1.2 Edges

Edges between components determine connectivity and the flow of electricity. Generally, we do not want to connect two generators in a series. We want generators connect it in parallel. Connecting two generators in parallel allows one generator to continue its operation even if the other generator failed. This increased the reliability level of the electric power system [41]. Contactors are power switches that controlled the flow of power and establish the connections between components while the electricity is output at the buses. As a result, we want contactors in between generators and buses [16, 32, 35]. Combined with the previous electric power components characteristics, we had defined a set of false edges. The edges that connect the components that we did not want to be connected were defined as false edges. These false edges were:

i. Edges between generator and generator
ii. Edges between generator and bus

Possible edges are ones that connect generators with contactors, contactors with contactors, and contactors with buses. Each set of components have a maximum number of possible edges. For example, for a combination that has two generators, two buses, and two generators, the maximum possible edges are nine. In this thesis, we select different numbers of edges and calculate the reliability level for each event;

and the highest number of edges we can use is the maximum possible edges for that example. Within the different numbers of edges, it generates a different set of topologies. Within the same conditions, it generates a number of possible topologies. Figure 14 shows the sample topologies that are connected by different number of edges for the two generators, two buses and two contactors event.



(1) One Edge (2) Two Edges (3) Two Edges

(4) Four Edges (5) Five Edges (6) Six Edges

(7) Seven Edges (8) Eight Edges (9) Nine Edges

Figure 14. Example topologies for the two generators, two buses, and two contactors events connected with different number of edges.

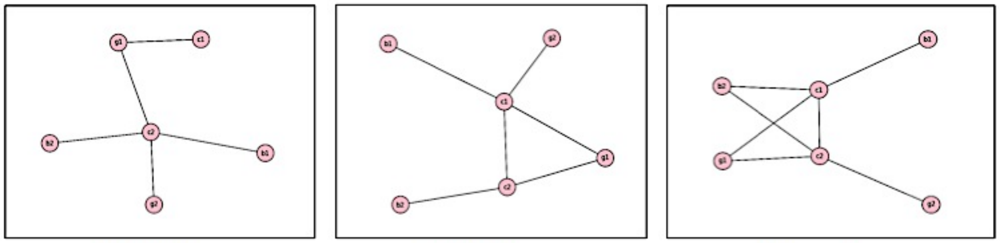
From the example topologies shown in Figure 14, we identified that for the six components events, we needed at least six edges to connect all components together. While we calculated the reliability level, we ensured that we did not have any topologies that had components that were not connected with other components (e.g. (1) to (5) in Figure 14). The edges in each topology that physically function as wires will connect to each electric power component. Electricity cannot flow to the components that are not connected. In this thesis, we applied path-set method to calculate the reliability level. In reliability analysis, path-set is a method where we find all paths through the topology starting from the input to the output. Different number of edges generates different set of paths, and the more paths a topologies forms, the higher the reliability level reached. Next, we compared the reliability level of different topologies that were composed by different number of edges and components.

4.2 Reliability Calculations

In this section, we first presented topologies that were composed by different number of edges with the same number of components (*e.g. five, six, seven, eight, and nine edges for the events to have two generators, two buses and two contactors*). Subsequently, we compared the topologies with the same total number of components but different number of each type of components (*e.g. two generators, two buses, and two contactors are compared with events that have two generators, three buses and one contactor*). Following, we presented topologies that were composed by different total number of components (*e.g. six components vs. eight components*). Lastly, we presented topologies that were composed with same number of components, same edges but different connectivity. In order to calculate the reliability level for each topology, we applied the path-set method into the analysis. As mention previously in this chapter, the electricity that flows through the generators and output at the buses. Therefore, generators are the inputs while the buses are the outputs.

Each topology can have more than one path-set; while each path-set can have multiple paths that can pass through from input to output. The number of generators and buses determines the number of path-sets. For instance, a topology has a set of components that have two generators and one bus; this topology will have two path-sets (i.e. $g1$ to $b1$ and $g2$ to $b1$). The reliability for each path-sets are independent from each other; consequently, we want to select a topology that has multiple path-sets and that each path-sets meet the requirement reliability level ($Reliability\ (R) = 10^{-9}\ per\ flight\ hours$) or higher.

To start, we compared the reliability level composed by different number of edges. Figure 15 shows topologies with a total number of six components (*two generator, two buses and two contactors*) connected with different number of edges. The paths for each topology are generated by Python codes, and the Python outputs are shown below each topology.



(1) Five Edges

```
Output from Python codes:
All paths from g1 to b1 are:
['g1', 'c2', 'b1']
R = 0.0012
 All paths from g1 to b2 are:
['g1', 'c2', 'b2']
R = 0.0012
 All paths from g2 to b1 are:
['g1', 'c2', 'b1']
R = 0.0012
All paths from g2 to b2 are:
['g2', 'c2', 'b2']
R = 0.0012
```

(2) Six Edges

```
Output from Python codes:
 All paths from g1 to b1 are:
['g1', 'c2', 'c1', 'b1']
['g1', 'c1', 'b1']
R = 1.476e-06
 All paths from g1 to b2 are:
['g1', 'c2', 'b2']
['g1', 'c1', 'c2', 'b2']
R = 1.476e-06
 All paths from g2 to b1 are:
['g1', 'c2', 'c1', 'b1']
['g1', 'c1', 'b1']
R = 1.476e-06
 All paths from g2 to b2 are:
['g2', 'c1', 'c2', 'b2']
['g2', 'c1', 'g1', 'c2', 'b2']
R = 2.098 e-06
```

(3) Seven Edges

```
Output from tool:
 All paths from g1 to b1 are:
['g1', 'c2', 'c1', 'b1']
['g1', 'c2', 'b2', 'c1', 'b1']
['g1', 'c1', 'b1']
R = 2.834e-09
 All paths from g1 to b2 are:
['g1', 'c2', 'c1', 'b2']
['g1', 'c2', 'b2']
['g1', 'c1', 'c2', 'b2']
['g1', 'c1', 'b2']
R = 2.179e-12
 All paths from g1 to b1 are:
['g1', 'c2', 'c1', 'b1']
['g1', 'c2', 'b2', 'c1', 'b1']
['g1', 'c1', 'b1']
R = 2.834e-09
 All paths from g2 to b2 are:
['g2', 'c2', 'c1', 'b2']
['g2', 'c2', 'g1', 'c1', 'b2']
['g2', 'c2', 'b2']
R = 2.8343e-09
```

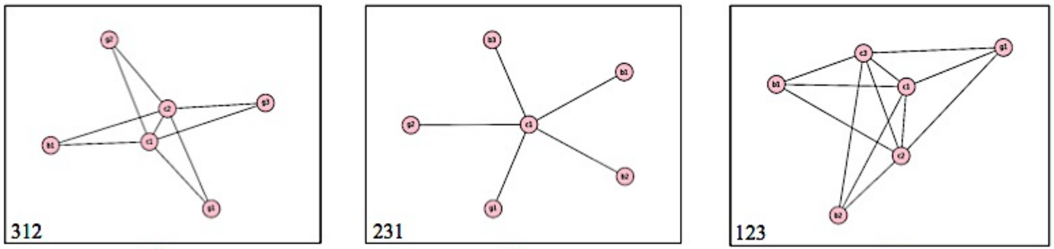
Figure 15. Topologies with two generators, two buses and two contactors (1) with five edges; (2) with six edges; (3) with seven edges. The paths for each topology are shown below where R is the reliability level for each path-sets

Topology in Figure 15 (1) Five Edges, it was compose of two generators, two buses and two contactors and was connected by five edges. This topology had four path-sets (*i.e. g1 to b1, g1 to be, g2 to b1 and g2 to b2*), and in each path-set had one path. The reliability value for each path-sets were $R_1 = R_2 = R_3 = R_4 = 0.0012$, which did not meet the FAA requirement ($R = 10^{-9}$).

Topology in Figure 15 (2) Six Edges, it was also compose by two generators, two buses and two contactors and was connected by six edges. The topology also had four path-sets, but each path-sets had two paths. The reliability values for each path-sets were $R_1 = R_2 = R_3 = 1.47\ e - 06$ and $R_4 = 2.089\ e - 06$, which did not meet the reliability requirement.

Topology in Figure 15 (3) Seven Edges, it was compose by the same set of components as the topology in Figure 15 (1) and (2), but it was connected by seven edges. Since they are composed by same set of components, it computed four path-sets as well. Each path-set had three or four paths, and the reliability values for each path were $R_1 = R_3 = R_4 = 2.834\ e - 09$ and $R_2 = 2.17\ e - 012$ which had meet the reliability level. By comparing the three topologies in Figure 15, we recognized that the same set of components, the topologies with more edges gives more options to the paths. The number of paths determines the reliability values.

After we compared the topologies with the same set of components but with different number of edges, we compared the topologies with different set of components but with the same total number of components (*i.e. three generators, one bus and two contactors or two generators, three buses and one contactor or one generator, two buses and three contactors are with the same number of component, which is with six components*).



(1)

```
Output from Python codes:
Max_edge = 9
All paths from g1 to b1 are:
['g1', 'c2', 'c1', 'b1']
['g1', 'c2', 'g3', 'c1', 'b1']
['g1', 'c2', 'g2', 'c1', 'b1']
.
.
.
R = 1.907e -23
All paths from g2 to b1 are:
['g2', 'c2', 'c1', 'b1']
['g2', 'c2', 'g3', 'c1', 'b1']
.
.
.
R = 1.907e -23
All paths from g3 to b1 are:
['g3', 'c2', 'c1', 'b1']
['g3', 'c2', 'g2', 'c1', 'b1']
.
.
.
R = 1.907e -23
```

(2)

```
Output from Python codes:
Max_edge = 5
All paths from g1 to b1 are:
['g1', 'c1', 'b1']
R = 0.0012
All paths from g1 to b2 are:
['g1', 'c1', 'b2']
R = 0.0012
All paths from g1 to b3 are:
['g1', 'c1', 'b3']
R = 0.0012
All paths from g2 to b1 are:
['g2', 'c1', 'b1']
R = 0.0012
All paths from g2 to b2 are:
['g2', 'c1', 'b2']
R = 0.0012
All paths from g2 to b3 are:
['g2', 'c1', 'b3']
R = 0.0012
```

(3)

```
Output from Python codes:
Max_edge = 12
All paths from g1 to b1 are:
['g1', 'c3', 'c2', 'c1', 'b1']
['g1', 'c3', 'c2', 'b2', 'c1', 'b1']
.
.
.
R=4.78e -94
All paths from g1 to b2 are:
['g1', 'c3', 'c2', 'c1', 'b2']
['g1', 'c3', 'c2', 'c1', 'b2']
.
.
.
R=4.78e -94
```

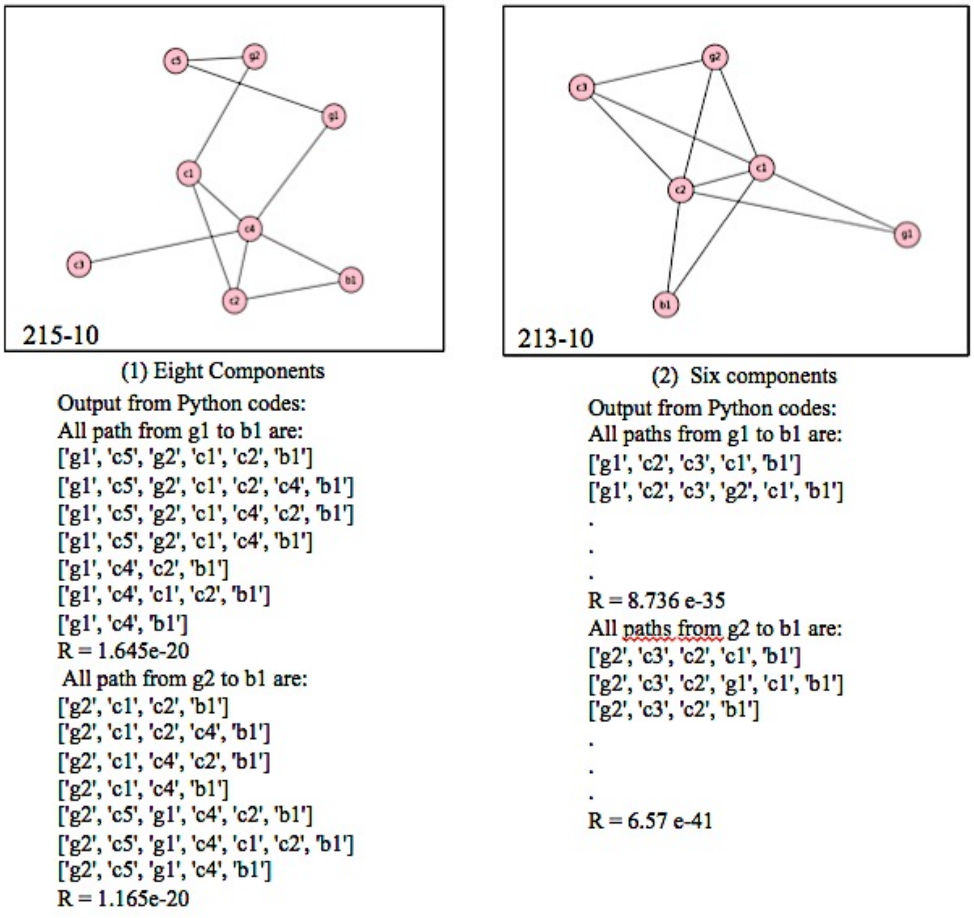
Figure 16. Topologies with same number of components (1) three generators, one bus and two contactors with nice edges; (2) two generators, three buses and one contactor with five edges; (3) one generator, two buses and three generators with twelve edges. The paths for each topology are shown below where R is the reliability level for each path-sets

Topology in Figure 16 (1) consisted of three generators, one bus and two contactors. It was connect by its maximum number of edges, which were nice edges. This topology had three path-sets (*i.e. g1 to b1, g2 to b1 and g3 to b1 where g1, g2 and g3 were the input components and b1 is the output component*). Each path-set had a total of eight paths. The reliability value for each path-set was $R_1 = \ R_2 = 1.907\ e - 23$, which met the FAA reliability requirement ($R = 10^{-9}$ per flight hours). Topology in Figure 16 (2) contained two generators, three buses and one contactor, and it was connect by its maximum number of edges, which were five edges. This topology had six path-sets (*i.e. g1 to b1, g2 to b1, g3 to b1, g1 to b2, g2 to b2, g3 to b2 where g1, g2 and g3 were the input components and b1, b2 and b3 were the output components*); each path-set had only one path. The reliability values for each paths-sets were $R_1 = R_2 = R_3 = R_4 = 0.0012$, which did not met the FAA reliability requirement.

Topology in Figure 16 (3), was composed by one generator, two buses and three contactors, and connected by its maximum number of edges, which were twelve edges. This topology had two path-sets (*i.e. g1 to b1 and g1 to b2 where g1 was the input component and b1 and b2 were the output components)*, and each path-set had thirty-three paths. The reliability values for each path-sets were $R_1 = R_2 = 4.78\,e - 49$, which met the FAA reliability requirement.

By comparing the three topologies in Figure 16, we recognized that the topologies with the same total number of components (*e.g. all topologies had six components*), but with different number of each type of electric power components (*e.g. one generator, two generator*) could generate different maximum edges. Topologies with the highest number of paths computed would have higher reliability values. Based on the edges constraints we applied on each component (*i.e. no edges allowed between generator and generator, bus and bus, and generator and bus*), contactor was the only one component that did not had any constraints. Therefore, contactor was the freest components that created more paths for each topology. Topologies had least number of contactor; it computed least number of paths. As it shown in Figure 16 (3), it had the most number of contactor between the topologies in Figure 16. It computed the most paths between these three topologies.

After we compared the topologies with the same number of components, we compared the topologies with the same number of edges but with different total number of components (*i.e. six components and eight components with ten edges*).



(1) Eight Components

```
Output from Python codes:
All path from g1 to b1 are:
['g1', 'c5', 'g2', 'c1', 'c2', 'b1']
['g1', 'c5', 'g2', 'c1', 'c2', 'c4', 'b1']
['g1', 'c5', 'g2', 'c1', 'c4', 'c2', 'b1']
['g1', 'c5', 'g2', 'c1', 'c4', 'b1']
['g1', 'c4', 'c2', 'b1']
['g1', 'c4', 'c1', 'c2', 'b1']
['g1', 'c4', 'b1']
R = 1.645e-20
 All path from g2 to b1 are:
['g2', 'c1', 'c2', 'b1']
['g2', 'c1', 'c2', 'c4', 'b1']
['g2', 'c1', 'c4', 'c2', 'b1']
['g2', 'c1', 'c4', 'b1']
['g2', 'c5', 'g1', 'c4', 'c2', 'b1']
['g2', 'c5', 'g1', 'c4', 'c1', 'c2', 'b1']
['g2', 'c5', 'g1', 'c4', 'b1']
R = 1.165e-20
```

(2) Six components

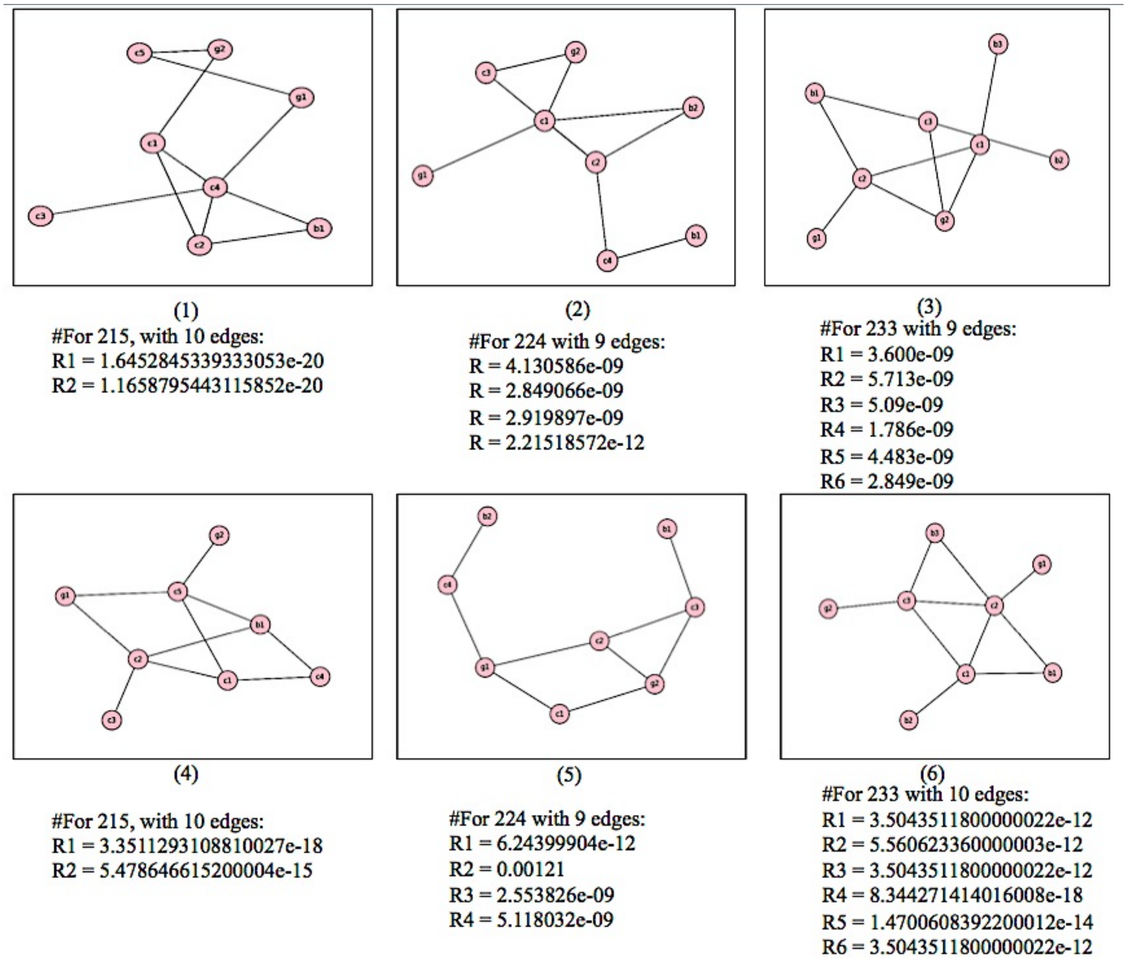
```
Output from Python codes:
All paths from g1 to b1 are:
['g1', 'c2', 'c3', 'c1', 'b1']
['g1', 'c2', 'c3', 'g2', 'c1', 'b1']
.
.
.
R = 8.736 e-35
All paths from g2 to b1 are:
['g2', 'c3', 'c2', 'c1', 'b1']
['g2', 'c3', 'c2', 'g1', 'c1', 'b1']
['g2', 'c3', 'c2', 'b1']
.
.
.
R = 6.57 e-41
```

Figure 17. Topologies with same number of edges: (1) Eight components - two generators, one bus and five contactors with ten edges; (2) Six components - two generators, one bus and three contactors with ten edges; the paths for each topology are shown below where R is the reliability level for each path-sets

Topology in Figure 17 (1) consisted of two generators, one bus and five contactors. It was connected by ten edges. This topology had two path-set (*i.e. g1 to b1 and g2 to* *b1 where g1and g2 were the input components and b1 was the output component)*, and each path-set had seven paths. The reliability values for each path-sets were $R_1 = 1.645\, e - 20$ and $R_2 = 1.165\, e - 20$, which both met the FAA reliability requirement.

Topology in Figure 17 (2) contained two generators, one bus and three contactors, and it also connected by ten edges. This topology also had two path-sets (*i.e. g1 to b1 and g2 to b1 where g1and g2 were the input components and b1 was the output component)*, and each path-set had twelve paths. The reliability values for each path-sets were $R_1 = R_2 = 6.57e - 41$, which both also met the FAA reliability requirement.

Comparing the topologies in Figure 17 with the assumption of two topologies with the same number of path-set (*i.e. same number of input and output*), we recognized that topologies with different total number of components (*e.g. six and eight components*) but with the same number of edges, the least number of components can generate more paths. With mean topologies with the same number of edges, the less number of component lean to compute more paths with higher reliability level. After comparing the different topologies for the set of six components, we move forward to compare the topologies for eight components.



(1)
#For 215, with 10 edges:
R1 = 1.6452845339333053e-20
R2 = 1.1658795443115852e-20

(2)
#For 224 with 9 edges:
R = 4.130586e-09
R = 2.849066e-09
R = 2.919897e-09
R = 2.21518572e-12

(3)
#For 233 with 9 edges:
R1 = 3.600e-09
R2 = 5.713e-09
R3 = 5.09e-09
R4 = 1.786e-09
R5 = 4.483e-09
R6 = 2.849e-09

(4)
#For 215, with 10 edges:
R1 = 3.3511293108810027e-18
R2 = 5.478646615200004e-15

(5)
#For 224 with 9 edges:
R1 = 6.24399904e-12
R2 = 0.00121
R3 = 2.553826e-09
R4 = 5.118032e-09

(6)
#For 233 with 10 edges:
R1 = 3.5043511800000022e-12
R2 = 5.560623360000003e-12
R3 = 3.5043511800000022e-12
R4 = 8.344271414016008e-18
R5 = 1.4700608392200012e-14
R6 = 3.5043511800000022e-12

Figure 18. Topologies with eight components

Topologies in Figure 18 are with eight components, and the reliability levels are different in each topology. Both (1) and (4) have two generators, one bus and five contactors, both connected with ten edges. However, the reliability values are different for these two, even though they have the same number of edges and components. (2) and (5) have two generators, two buses and four contactors, both connected with nice edges. The reliability values for these two also different. (3) and (6) have two generators, three buses and three contactors, while (3) is connected with nine edges and (6) is connected with ten edges. The reliability value for the ten edges is higher than the topology connected with nine edges. Comparing (1) (2) and (3), the number of each type of electric power components are different, but the one with more edges lean to have a higher reliability values. This result is the same as the event that occurs with six components where the topologies have more edges to give higher reliability level. At the same time, topologies in Figure 18 also show us that, topologies with same features (same number edges and components), the reliability level could be different. This tells us that we cannot guarantees all topologies meet the reliability requirement with same features. As it shown in Figure 18 (2) and (5), while they have the same number of components and edges, the reliability level in (2) met the FAA requirement but (5) is not.

In this chapter, we examine the set of combinations with six and eight components, while in each set of combinations. There is total number of possible combinations (*e.g. for the six components events, there is total of ten sets*). On each set of components, we applied different number of edges to each event. After going through all possible number of edges, we found that within the same set of component, the more edges we applied to the topologies, the higher the reliability level it got. Then, we looked into examples that had the same total number of components with the same edges number (as it show in Figure 15), but with different number of each type of components (*e.g. one generator, two generator, or three generators*). Within the assumption we established in this thesis (using the path-sets method and constraints for components), topologies with higher number of contactors have higher reliability values. After going through all the possible examples for six components, we did the same procedures for the eight component events. The results show topologies with six or eight components, their behaviors are the same. In this procedure, we used the path-set method for our calculations. In the next section, we applied our proposed method to calculate the reliability values for the AC electrical systems architecture of the aircraft found in [46] as show in Figure 19.

4.3 Application of the Proposed Method

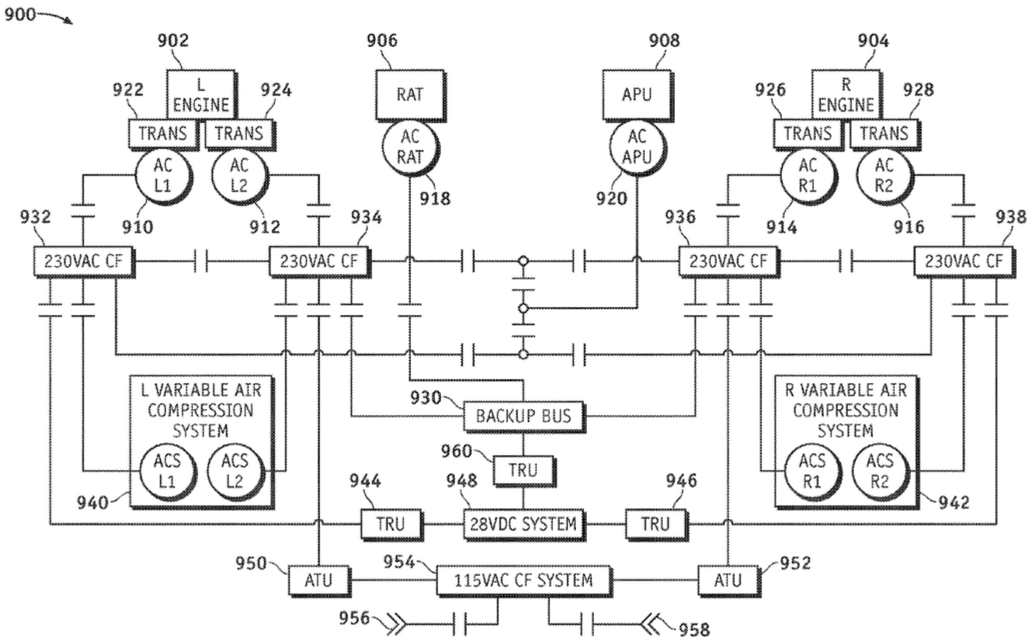


Figure 19. AC Electrical systems architecture for an aircraft [46]

In this section, we take a single-line diagram as shows in Figure 19. We consider only the AC electrical systems in this architecture of an aircraft and we use the python code to generate candidate topologies. Each topology has a total of six generators, five buses and twenty-five contactors; a sample topology shows in Figure 20.

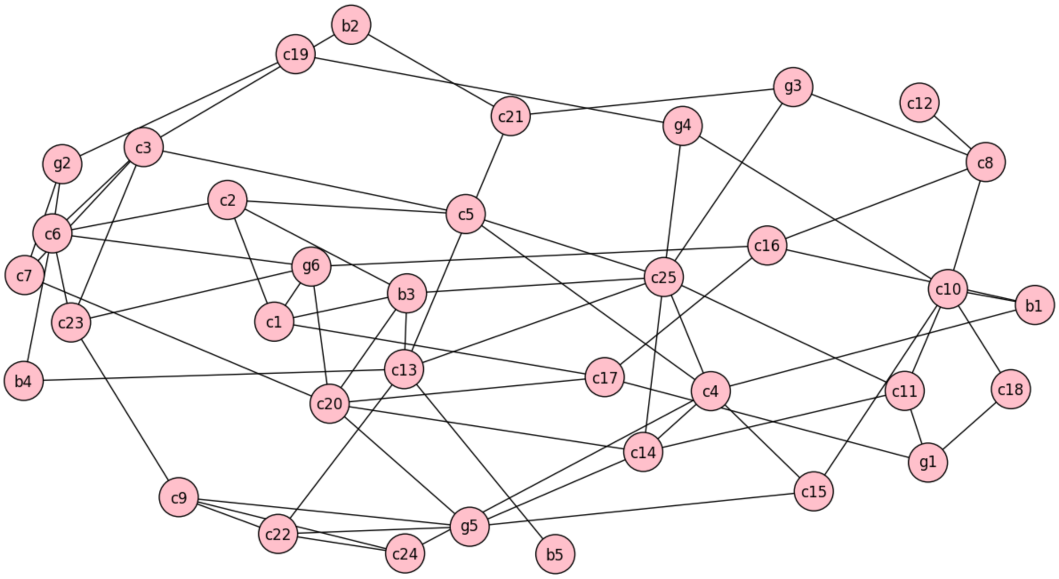


Figure 20. Topology for electric systems architecture of an aircraft

The topology in Figure 20 is composed of thirty-six components. These include six generators, five buses and twenty-five contactors. Using the path-set method to calculate the reliability value for this topology, it produces thirty different path-sets. The reliability values of each path-set are shown in Table 2. As it can be seen from table 2, the reliability values of each path-set for topology in Figure 20 are different. It varies from 10^{-10} to 10^{-74} per flight hours, which mean all values meet the FAA requirement. Based on the result of this example, we were able to develop topologies and calculated the reliability levels for any electric power system by using our proposed method. Within the same electric power system, this can produce different topologies and each topology having different reliability levels. From the difference of the reliability level, we know which path can produce better reliability by comparing them to each other. One advantage of using our propose method to study the electric power system was that we can create different topologies for the same electric power system and apply the topology with the highest reliability level to the design. In addition, an advantage of using path-set method to calculate the reliability level was that we were able to calculate all reliabilities between different input and outputs. For situation where we know which input and output the electricity is coming from and out, we can determine which path have higher reliability level by using path-set method.

Table 2. Reliability Values for AC electric systems architecture of an aircraft

Path-sets	Reliability Values	Path-sets	Reliability Values
From g1 to b1	2.070e-39	From g4 to b1	1.617e-41
From g1 to b2	1.474e-28	From g4 to b2	3.224e-36
From g1 to b3	4.217e-50	From g4 to b3	8.644e-17
From g1 to b4	1.462e-56	From g4 to b4	1.037e-51
From g1 to b5	1.229e-61	From g4 to b5	1.324e-56
From g2 to b1	1.854e-31	From g5 to b1	1.617e-13
From g2 to b2	4.706e-20	From g5 to b2	4.705e-20
From g2 to b3	4.547e-59	From g5 to b3	1.147e-25
From g2 to b4	4.973e-69	From g5 to b4	5.205e-54
From g2 to b5	8.463e-74	From g5 to b5	5.205e-54
From g3 to b1	3.661e-36	From g6 to b1	6.584e-54
From g3 to b2	2.662e-25	From g6 to b2	3.085e-10
From g3 to b3	7.6-6e-47	From g6 to b3	7.227e-16
From g3 to b4	1.189e-41	From g6 to b4	2.884e-44
From g3 to b5	9.589e-47	From g6 to b5	2.887e-44

In conclusion, by applying our propose method, we were able to design an electric power system with many different topologies. Using the path-set method, we were able to calculate the reliability level of each path-set. Therefore, applying the path-set with the highest reliability level to the aircraft design can increase the safety level of an aircraft.

Chapter 5: Control Synthesis

The topologies we found in Chapter 4 will be linked to a control synthesis, which design a controller to actuate contactors in order to provide power to buses and loads. For any selected topology, we first went through all possible faults and looked for environment conditions where the reliability level still met the FAA reliability requirement even with failure errors. We inputted a set of environment conditions to control synthesis and generated a controller that guaranteed the safety requirement.

The main function of the controller is sensing and reacting to the faults of the electric power system. The controller must be designed to guarantee that the safety is satisfied under all possible faults [28, 35]. For any given topology, generators can be unhealthy or healthy. The aim in this chapter is to find a control protocol to correctly actuate contactors in order to direct power from generators to buses, and guarantee that buses will never be unpowered for more than a set period of time. The resulting controller is made up from a specification language. This formal specification language was linear temporal logic (LTL) [28, 33, 35].

5.1 Linear Temporal Logic

LTL is a type of temporal logic that is suitable for describing the properties in which temporal ordering of events is important. LTL is a language that reasons propositions over an infinite sequence of states. LTL's main building block is the atomic proposition to which it has a unique truth-value [42, 43]. For example, the health status for generators $g1$ and $g2$ where $\{g1 = healthy\}$, and $\{g2 = unhealthy\}$ are atomic propositions [43].

LTL includes Boolean connectors: negation (¬), disjunction (∨), conjunction (^), material implication (→), and two basic temporal operators: *next* (**O**) and *unti*l ($\mathcal{U}$). By combining these operators, it is possible to specify requirements widely on the desired behavior of a system and environment assumptions. Formulas involving other operators can be derived from these basic ones, including *always* (□) and *eventually* (◊) [33, 35, 36]. Example of LTL includes invariance (□ **p**), reachability (□ ◊ **p**), recurrence (◊□**p**), response {□ **(p→q)}**, and next step response {□ **(p→ O** ◊ **q)}**.

Next, we review the formal method to link all the specifications to control synthesis. To synthesize the control logic that guarantees the reliability requirement, we will use a Python-based coded software, called the TuLiP [18, 33].

5.2 Introduction to TuLiP

The Temporal Logic Planning (TuLiP) toolbox is a collection of Python-based code used for automatic synthesis of correct-by-construction embedded control software [28, 33]. TuLiP is designed to synthesize discrete-state controllers for hybrid systems operating in an uncertain environment. There are three primary steps in using TuLiP. First, constructs a finite transition system ($\mathcal{D}$) that serves as an abstract model of S, where S is the state space of the continuous component of the system, which typically has infinitely many states. Second, it synthesizes a discrete planner that computes a discrete plan satisfying the specification φ based on the abstract, finite state model $\mathcal{D}$. Third, designs a continuous controller that implements the discrete plan [44].

Synthesis can be considered to be a two-player game, where the environment tries to make the system go into a “bad” state, and the controller tries to guarantee all requirements are met. Let $s = (e, p) \epsilon \ dom\ (E) \times dom\ (P)$ be the states of the system. Consider a LTL specification φ of assume guarantee form

$$\varphi = \varphi_{e} \rightarrow \varphi_{s}, \tag{1}$$

where φ_{e} is the conjunction of LTL specification that characterizes the assumptions on the environments and φ_{s} is the conjunction of LTL specification that characterizes the system requirements. TuLiP generates a finite automaton that represents all possible states of the systems and their transitions. If a strategy exists for the system to satisfy the specification, such as a controller exists, this means the specification φ is realizable [28, 33, 35, 36, 45].

5.3 Case Study Using TuLiP

The topology in Figure 19 was one of the topologies that was generated from the previous chapter. Using this sample topology, we linked it to control synthesis. For the sample topology, we first looked into the environment assumptions. For simplicity purpose, we considered that generators were the only type of variable capable of failing. Additional specifications were needed to instruct TuLiP on how to generate a controller for the sample topology. With all the specifications, a controller automaton was created. Each states in the automaton activity diagram shows the transitions behavior between each states. Lastly, for topology that is unrealizable, we provide details on how to redesign the topology.

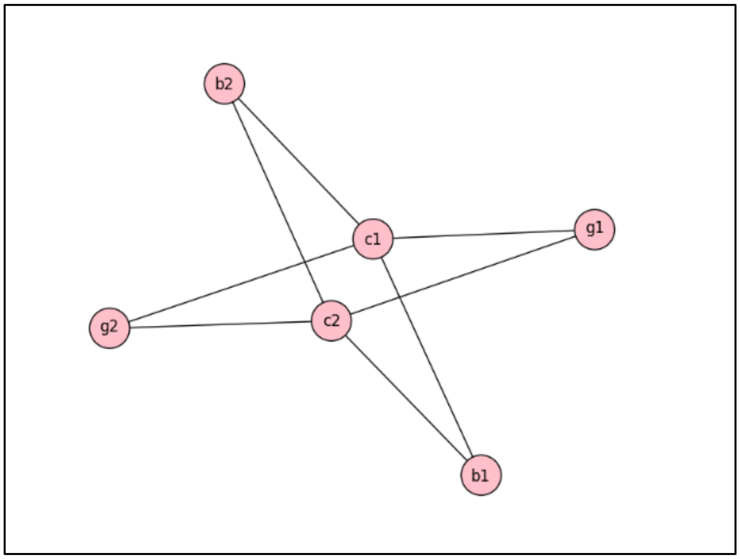


Figure 21. Topology with two generators, two buses and two contactors connected by eight edges

Since there is no control over the environment variables, the environment assumptions guarantee the system's feasibility. For a selected topology (shown in Figure 21), after going through all the possible faults in the existing examples, the path-sets (or the system reliability level) in each topology accommodate any possible combination of faults with a reliability level higher than 10^{-9} per flight hours are very few. For instance, the selected topology allows only two possible faults with reliability levels higher than 10^{-9} per flight hours. Therefore, we lowered the reliability level to 10^{-6} per flight hours. This way we could have more system variable activities in the environment specifications.

For selected topology, there are four total different path-sets. Given the four different environment equations, this can be written in specifications for the system variables with a compatible format for TuLiP as:

$$\begin{aligned}\varphi_{e1} = \rightarrow ((g1 = 1 \wedge g2 = 0 \wedge b1 = 1 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 1 \wedge g2 = 1 \wedge b1 = 1 \wedge b2 = 0 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 1 \wedge g2 = 0 \wedge b1 = 1 \wedge b2 = 0 \wedge c1 = 1 \wedge c2 = 0)\end{aligned} \tag{2}$$

$$\begin{aligned}\varphi_{e2} = \rightarrow ((g1 = 1 \wedge g2 = 0 \wedge b1 = 1 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 1 \wedge g2 = 1 \wedge b1 = 0 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 1 \wedge g2 = 0 \wedge b1 = 0 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1))\end{aligned} \tag{3}$$

$$\begin{aligned}\varphi_{e3} = \rightarrow ((g1 = 0 \wedge g2 = 1 \wedge b1 = 1 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 1 \wedge g2 = 1 \wedge b1 = 1 \wedge b2 = 0 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 0 \wedge g2 = 1 \wedge b1 = 1 \wedge b2 = 0 \wedge c1 = 1 \wedge c2 = 1))\end{aligned} \tag{4}$$

$$\begin{aligned}\varphi_{e4} = \rightarrow ((g1 = 0 \wedge g2 = 1 \wedge b1 = 1 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 1 \wedge g2 = 1 \wedge b1 = 1 \wedge b2 = 0 \wedge c1 = 1 \wedge c2 = 1)\\ \vee (g1 = 0 \wedge g2 = 1 \wedge b1 = 0 \wedge b2 = 1 \wedge c1 = 1 \wedge c2 = 1))\end{aligned} \tag{5}$$

Equation (2) to (5) are the outputs of the topology python code, where each specification represents a fault that occurs - but the reliability still meets the FAA requirement. Since there is a total of four path-sets for the selected topology, we have four environment assumption equations. Within these four environment equations (shown in equation 2 – 5), path-set one φ_{e1} allows five different fails while the other three allow only three fails. For example, as show in equation (5), if g1 fail, but g2, b1, b2 and c2 function regularly without any errors, the electric power system meets the FAA reliability requirement. Secondly, if b2 fails, but g1, g2, b1, c1 and c2 function regularly without any errors, the electric power system also meets the FAA reliability requirement. Finally, if g1 and b1 fails, but g2, b1, c1 and c2 function regularly without any errors, the electric power systems also meet the FAA reliability requirements.

In control synthesis, for simplicity, we consider generators (i.e. *g1* and *g2*) to be capable of failing. There are three acceptable environment behaviors for generators which including: g1 =1, g2 = 1; g1 = 1, g2 = 0 and g1 = 0, g2 = 0, where 1 = healthy and 0 = unhealthy. Written in LTL, the environment assumptions from equation (2) to (5) can reduce to the following:

$$\varphi_e = \square\{(g1 = 1 \ \wedge g2 = 1) \vee \ (g1 = 1 \ \wedge g2 = 0) \vee \ (g1 = 0 \ \wedge g2 = 1)\} \qquad (6)$$

The system variables are *b1, b2, c1* and *c2*, where they can take values of 0 or 1. For buses, a value of 0 means the bus in unpowered, while a value of 1 signifies that the bus is powered. A contactor with a value of 1 mean the contactors in closed. A value of 0 means the contactor is open.

The power state for buses depends on healthy conditions of a generator. Buses are powered if there is a path between a bus and generator, and if all components along the path are healthy or closed. The specifications for initial grantees states for buses powered are

$$\varphi_{s1} = \square\{(g1 = 1 \ \wedge c1 = 1) \vee (g1 = 1 \wedge c2 = 1) \vee \ (g2 = 1 \ \wedge c1 = 1) \\ \vee (g2 = 1 \wedge c2 = 1) \rightarrow (b1 = 1)\} \qquad (7)$$

$$\varphi_{s2} = \square\{(g1 = 1 \ \wedge c1 = 1) \vee (g1 = 1 \wedge c2 = 1) \vee \ (g2 = 1 \ \wedge c1 = 1) \\ \vee (g2 = 1 \wedge c2 = 1) \rightarrow (b2 = 1)\} \qquad (8)$$

On the other hand, if none of the above conditions hold, the buses will be unpowered. This requirement is expressed as

$$\begin{aligned}\square \neg \{&(g1 = 1\ \wedge c1 = 1) \vee (g1 = 1\ \wedge c2 = 1) \vee (g2 = 1\ \wedge c1 = 1) \\ &\vee (g2 = 1\ \wedge c2 = 1) \rightarrow\ (b1 = 0)\}\end{aligned} \tag{9}$$

$$\begin{aligned}\square \neg \{&(g1 = 1\ \wedge c1 = 1) \vee (g1 = 1\ \wedge c2 = 1) \vee (g2 = 1\ \wedge c1 = 1) \\ &\vee (g2 = 1\ \wedge c2 = 1) \rightarrow\ (b2 = 0).\end{aligned} \tag{10}$$

We consider essential to be connected to safety-critical loads, and it can be never unpowered more than three time steps. Each transition represent an increment of time step, it will reset to zero when is powered. The safety specification for buses can be expressed as

$$\square\{\ (b1 = 0) \rightarrow (\mathbf{O}\ (counter\_1) = (counter\_1 + 1))\} \tag{11}$$

$$\square\{\ (b1 = 1) \rightarrow (\mathbf{O}\ (counter\_1) = (0))\} \tag{12}$$

$$\square\{\ (counter\_1 <= 3) \tag{13}$$

$$\square\{\ (b2 = 0) \rightarrow (\mathbf{O}\ (counter\_1) = (counter\_2 + 1))\} \tag{14}$$

$$\square\{\ (b2 = 1) \rightarrow (\mathbf{O}\ (counter\_2) = (0))\} \tag{15}$$

$$\square\{\ (counter\_2 <= 3) \tag{16}$$

Paralleling can occur if there exists a live path that connected all generators. To avoid paralleling, we never want to close all the contactors at the same time, which will lead to a live path between generators. This specification can expressed as

$$\square\{\ \neg\ (c1 = 1) \wedge (c2 = 1)\} \tag{17}$$

For a sample topology, there is a total of two generators and two buses, while each buses are connecting all generators. When generator (*g1 or g2*) become unhealthy, the contactors connected to that generator will become open. This specification can expressed as following

$$\square\{(g1 = 0) \rightarrow (c1 = 0 \wedge c2 = 0)\}, \tag{18}$$

$$\{(g2 = 0) \rightarrow (c1 = 0 \wedge c2 = 0)\}. \tag{19}$$

When Equations (18) and (19) holds this specification is unrealizable. In order to provide power to the buses, contactors must be closed. For the selected topology, if we want buses to be powered, we cannot have any generators to fail. We will address this issue later in this chapter. Thus, we deleted the specifications shown in (18) and (19) where *g1* or *g2* is unhealthy so that we can synthesize a controller for the selected topology. The resulting automaton is shown in Figure 22.

As shown in Figure 22, the status variables for generators are *g1* and *g2,* and the status variable for buses are b1 and b2 while the status variables for contactors are c1 and c2. Each state has a successor, which defines where the controller can transition depending on the current state. There are a total of 13 states where each state has four successors. For example, state 0 with successors: 1, 2, 3, and 4 means that the controller can transit from state 0 to state 1, 2, 3, or 4. For state 1, with successors: 5, 6, 7 and 8, it means that the controller can transit from state 1 to state 5, 6, 7, 8. Looking at the status for c2, we find out that c2 is always equal to 0 (open). In order to get more interesting behaviors for contractors, we add new specifications to the environment, it can written as

$$\square \lozenge (c1 = 1) \wedge \square \lozenge (c2 = 1) \tag{20}$$

By adding this new specification, a new automaton results as shown in Figure 23. With this new specification, depending on the status, c2 now can be open and closed. Comparing the two resulting automaton, the resulting automaton in Figure 21 creates more states. It has a total of 16 states.

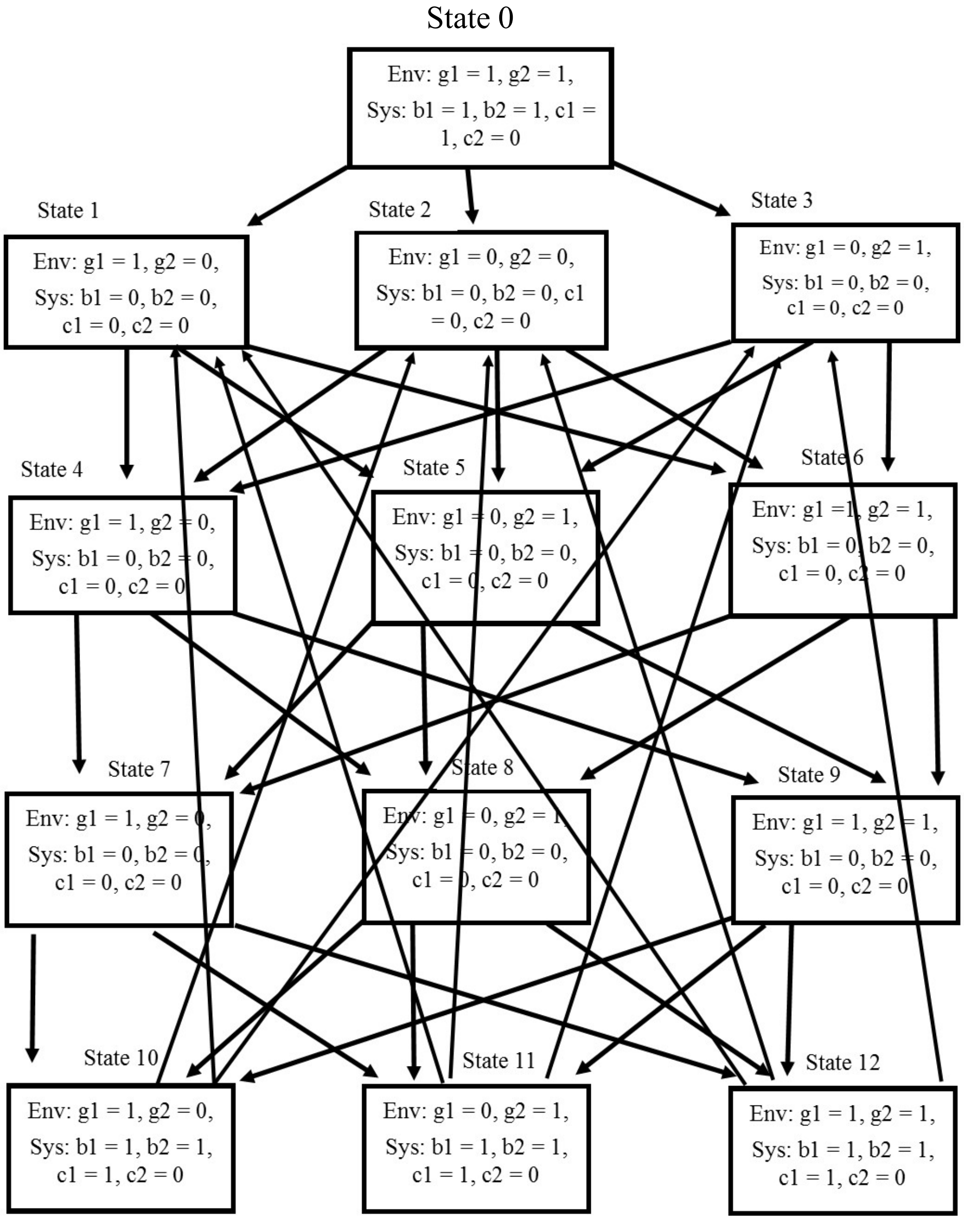

State 0
Env: g1 = 1, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0
State 1
Env: g1 = 1, g2 = 0,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 2
Env: g1 = 0, g2 = 0,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 3
Env: g1 = 0, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 4
Env: g1 = 1, g2 = 0,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 5
Env: g1 = 0, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 6
Env: g1 = 1, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 7
Env: g1 = 1, g2 = 0,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 8
Env: g1 = 0, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 9
Env: g1 = 1, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 10
Env: g1 = 1, g2 = 0,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0
State 11
Env: g1 = 0, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0
State 12
Env: g1 = 1, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0

Figure 22. Controller automaton output from TuLiP for topology in Figure 21 with original conditions

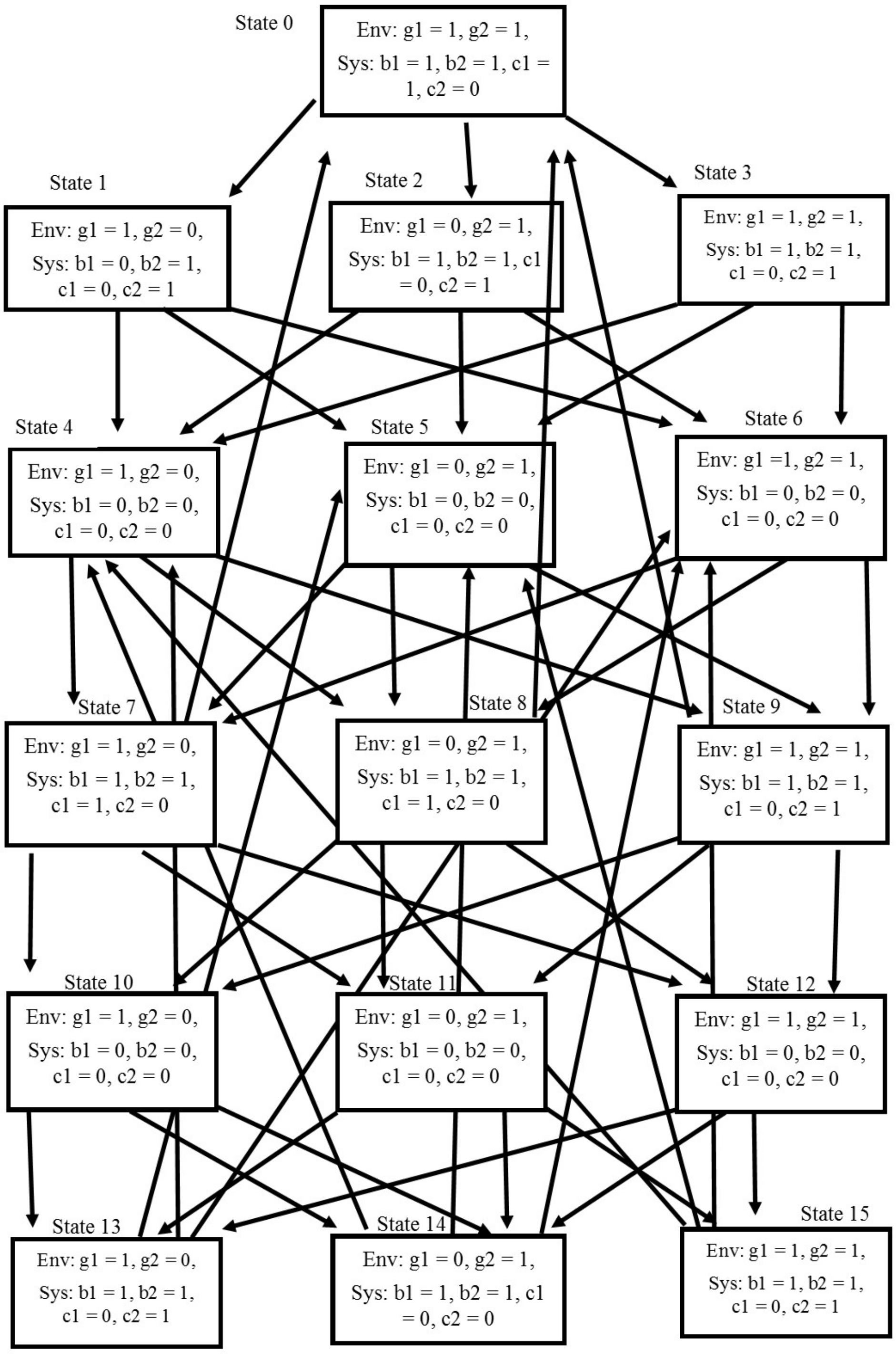

State 0
Env: g1 = 1, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0
State 1
Env: g1 = 1, g2 = 0,
Sys: b1 = 0, b2 = 1, c1 = 0, c2 = 1
State 2
Env: g1 = 0, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 0, c2 = 1
State 3
Env: g1 = 1, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 0, c2 = 1
State 4
Env: g1 = 1, g2 = 0,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 5
Env: g1 = 0, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 6
Env: g1 =1, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 7
Env: g1 = 1, g2 = 0,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0
State 8
Env: g1 = 0, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 1, c2 = 0
State 9
Env: g1 = 1, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 0, c2 = 1
State 10
Env: g1 = 1, g2 = 0,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 11
Env: g1 = 0, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 12
Env: g1 = 1, g2 = 1,
Sys: b1 = 0, b2 = 0, c1 = 0, c2 = 0
State 13
Env: g1 = 1, g2 = 0,
Sys: b1 = 1, b2 = 1, c1 = 0, c2 = 1
State 14
Env: g1 = 0, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 0, c2 = 0
State 15
Env: g1 = 1, g2 = 1,
Sys: b1 = 1, b2 = 1, c1 = 0, c2 = 1

Figure 23. Controller automaton output from TuLiP for topology in Figure 21 with modified conditions

5.4 <u>Redesign Topologies</u>

As previously discussed in previous section, when generators (*g1* or *g2*) become unhealthy, the contactors that are connected to that generator will become open. For selected topology in this chapter, when *g1* or *g2* fails, both contactors become open. Thus, buses cannot be powered and this is unrealizable. In situations like this, we have to go back and modify the topology, so it can guarantee all buses are powered. The first step we take is to increase the number of edges, but this does not solve the buses 'unpowered' problem. The next step we take is to increase the number of components.

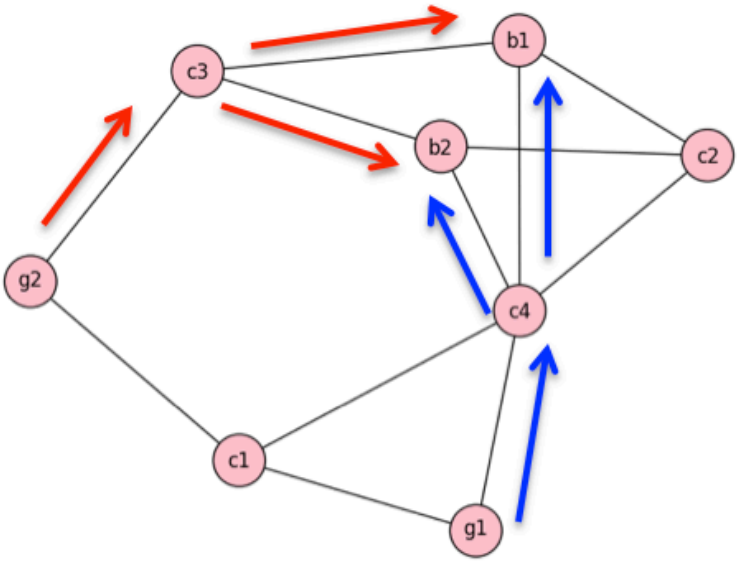


Figure 24. New topologies with two generators, two buses and four contactors, connected with twelve edges.

Topologies in Figure 24 are composed with two generators, two buses, and four contactors, connected with twelve edges. For this topology, if g1 fails, c1 = c4 = 0, b1 and b2 can be powered from $g2$. The path would be $g2 \rightarrow c3 \rightarrow b1$ *or* $g2 \rightarrow c3 \rightarrow b2$. If g2 fails, c1 and c3 becomes open, b1 and b2 can power from $g1$, and the path would be $g1 \rightarrow c4 \rightarrow b1$ *or* $g1 \rightarrow c4 \rightarrow b2$.

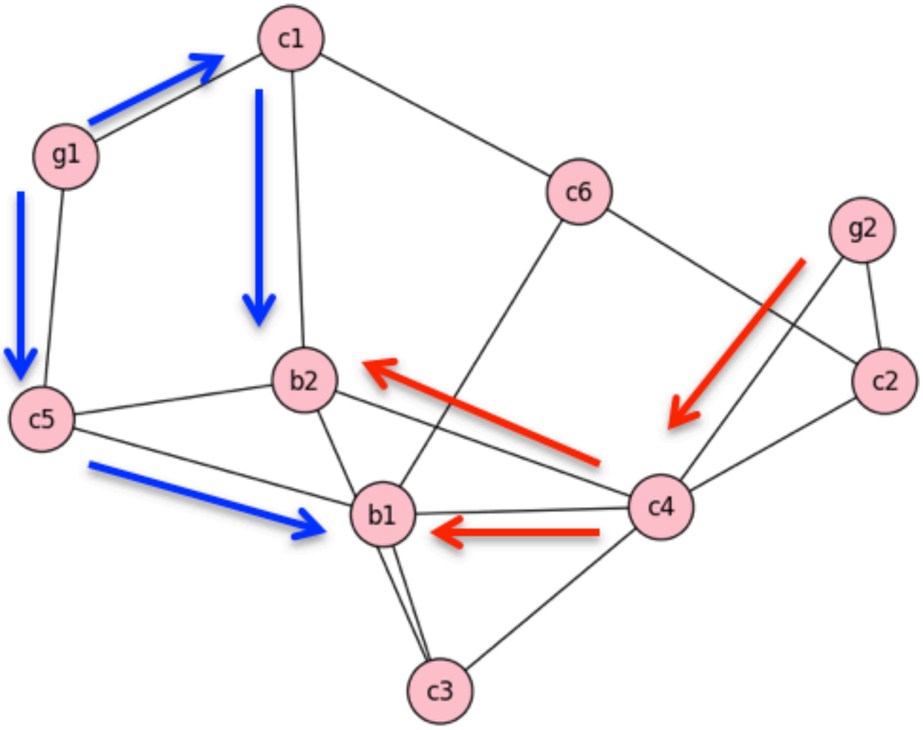


Figure 25. New topologies with two generators, two buses and six contactors, connected with sixteen edges.

For the topology in Figure 25, if g1 fails, then c1 = c5 = 0, and *b1 and b2* can be powered from $g2$, the path would be $g2 \rightarrow c4 \rightarrow b1$ *and* $g2 \rightarrow c4 \rightarrow b2$. If g2 fail, c2 = c4 = 0, and *b1 and b2* can be powered from$g1$, the path would be $g1 \rightarrow c5 \rightarrow b1$ *and* $g1 \rightarrow c1 \rightarrow b2$.

Comparing the topologies between Figure 24 and 25, both have given a satisfied solution to power the buses when one generator fails. However, the topology in

Figure 25 has to bring in extra components and edges. Extra components and edges increased the reliability level but in the same time increased the total cost. Good topologies are the ones balanced in cost and reliability level. Therefore, topology in Figure 24 has more advantage than topology in Figure 25. From the above topologies, we know that by increasing the number of contactors, it creates more paths for the electricity to flow from generators to buses. With enough edges and components, it increases the reliability level and guarantees the safety of the electric power systems. For topology that meet the reliability level but is unrealizable, we have to redesign it by increasing the number of components or edges.

Chapter 6: Conclusions and Future Work

6.1 *Summary*

This thesis investigated ways to analyze topologies for the MEA electric power system by using different reliability methodologies. The aim was to select a reliable number and connectivity of electric power components that could produce a reliable reliability value. Reliable reliability values were the reliability values that met the FAA required reliability level at 10^{-9} flight per hours and had the lowest total cost.

We demonstrated the traditional and new proposed methodologies in finding the reliability level for the electric power system. In the traditional method, we looked at the reliability values for each electric power component and calculated their reliability level. In our proposed method, we worked in the opposite direction and looked at the overall reliability level for electric power systems and generated topologies that met the reliability level. We used NetworkX, a Python software language, to compute candidate topologies. Each topology was composed of nodes and edges. Where nodes represented electric power components and edges represented the connections between each component. We applied a complex system reliability calculation method called the 'path-set method' to compute reliability levels for the candidate topologies.

Finally, we used TuLiP as the tool to automatically synthesize a controller that satisfied the safety requirement. The aim was create a controller that guarantees buses can be powered when failure occur. The formal language used to formulate the electric power system requirements was LTL. We demonstrated the procedures in formalizing a set of environmental conditions and system specifications to synthesize a controller automaton for a selected topology.

6.2 Future Work

Methodologies used in this thesis scaled down the number of electric power components and simplified changes in the reliability values. In future, we can increase the number and type of the electric power components. Having multiple reliability values for each type of electric power components definitely changes the reliability level for the electric power system. Furthermore, we also plan to expand the environment variables in TuLiP from the current two variables to four or more. Procedures input in the initial state and environment assumptions are complicated, expanding the variables directly and making the procedures into a much more complicated form.

Bibliography

[1] AA AbdElhafez and AJ Forsyth. A review of more-electric aircraft. In *Proceedings of The 13rd international conference on Aerospace Science and Aviation Technology conference*, pages 26–28, 2009.

[2] Federal Aviation Administration. *Aviation Maintenance Technician Handbook*. Indomitable Publications, 2008.

[3] David Blanding and Boeing Phantom Works. Subsystem design and integration for the more electric aircraft. In *5th International Energy Conversion Engineering Conference and Exhibit (IECEC)*, 2007.

[4] Barry W Boehm. Software engineering economics. 1981.

[5] A Boglietti, A Cavagnino, A Tenconi, and S Vaschetto. The safety critical electric machines and drives in the more electric aircraft: A survey. In *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE*, pages 2587–2594. IEEE, 2009.

[6] Reece A Clothier and Paul P Wu. A review of system safety failure probability objectives for unmanned aircraft systems. In *Proceedings of the 11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability (ESREL 2012) Conference.*, 2012.

[7] S Distefano and Liudong Xing. A new approach to modeling the system reliability: dynamic reliability block diagrams. In *Reliability and Maintainability Symposium, 2006. RAMS'06. Annual*, pages 189–195. IEEE, 2006.

[8] Salvatore Distefano. *System dependability and performances: Techniques, methodologies and tools*. PhD thesis, PhD thesis, University of Messina, 2005.

[9] Salvatore Distefano and Antonio Puliafito. Dependability evaluation with dynamic reliability block diagrams and dynamic fault trees. *Dependable and Secure Computing, IEEE Transactions on*, 6(1):4–17, 2009.

[10] A Emadi and M Ehsani. Aircraft power systems: technology, state of the art, and future trends. *Aerospace and Electronic Systems Magazine, IEEE*, 15(1):28–32, 2000.

[11] Guanghai Gong, Marcelo Lobo Heldwein, UweDrofenik, Johann Minibock, Kazuaki Mino, and Johann W Kolar. Comparative evaluation of three- phase high-power-factor ac-dc converter concepts for application in future more electric aircraft. *Industrial Electronics, IEEE Transactions on*, 52(3):727–737, 2005.

[12] Joel M Grasmeyer, Matthew T Keennon, et al. Development of the black widow micro air vehicle. *Progress in Astronautics and Aeronautics*, 195:519–535, 2001.

[13] Barringer H. Paul. Which reliability tool should I use? http://www.reliabilityweb.com/art07/reliability_tools.htm.

[14] Christopher Hart. The global aviation information network (gain). *Human Error, Safety and Systems Development*, pages 17–30, 2004.

[15] NicolaeJula, CostinCepisca, MirceaCovrig, CiprinRacuciu, and Tudor Ursu. Boolean applications in aircraft electric power systems reliability analysis. In *2nd European Computing Conference*, 2008.

[16] Wen-Shing Lee, DL Grosh, Frank A Tillman, and Chang H Lie. Fault tree

analysis, methods, and applications ? a review. *Reliability, IEEE Transactions on*, 34(3):194–203, 1985.

[17] Wei Lu and Wei-dong Peng. Analysis of use reliability on electrical power system of civil aviation training planes. In *Reston, VA: ASCEProceedings of the First International Conference on Transportation Information and Safety, June 30. July 2, 2011, Wuhan, China— d 20110000*. American Society of Civil Engineers, 2011.

[18] Cesar A Luongo, Philippe J Masson, Taewoo Nam, DimitriMavris, Hyun D Kim, Gerald V Brown, Mark Waters, and David Hall. Next generation more-electric aircraft: a potential application for hts superconductors. *Applied Superconductivity, IEEE Transactions on*, 19(3):1055–1068, 2009.

[19] Mohammad Modarres, Mark Kaminskiz, and VasiliyKrivstov. *Realiability Engineering and Risk Analysis: A Practical Guide*, volume 55. CRC press, 1999.

[20] Ian Moir and Allan Seabridge. *Aircraft systems: mechanical, electrical and avionics subsystems integration*, volume 21. Wiley. com, 2008.

[21] Guy Norris. Boeing’s seventh wonder. *Spectrum, IEEE*, 32(10):20–23, 1995.

[22] PIERLUIGI Nuzzo, HUAN Xu, NecmiyeOzay, JOHN B Finn, ALBERTO L Sangiovanni-Vincentelli, Richard M Murray, AlexandreDonze´, and SANJIT A Seshia. A contract-based methodology for aircraft electric power system design.

[23] Jose´ Fernando Prada. The value of reliability in power systems-pricing operating reserves. 1999.

[24] Maintainability Reliability. Availability (rma) handbook. *FAA HDBK-006*, 2006.

[25] Seung J Rhee and Kosuke Ishii. Using cost based fmea to enhance reliability and serviceability. *Advanced Engineering Informatics*, 17(3):179–188, 2003.

[26] Ryan Robidoux, HaipingXu, Liudong Xing, and MengChu Zhou. Automated modeling of dynamic reliability block diagrams using colored petri nets. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 40(2):337–351, 2010.

[27] GenainaNunes Rodrigues, David Rosenblum, and Jonas Wolf. Reliability analysis of concurrent systems using ltsa. In *Software Engineering- Companion, 2007. ICSE 2007 Companion. 29th International Conference on*, pages 63–64. IEEE, 2007.

[28] Robert Rogersten, HuanXu, NecmiyeOzay, UfukTopcu, and Richard M Murray. An aircraft electric power testbed for validating automatically synthesized reactive control protocols. In *Proceedings of the 16th international conference on Hybrid systems: computation and control*, pages 89–94. ACM, 2013.

[29] Joel R. Sklaroff. Redundancy management technique for space shuttle computers. *IBM Journal of Research and Development*, 20(1):20–28, 1976.

[30] Mark Wagner and Guy Norris. *Boeing 787 Dreamliner*. Zenith Imprint, 2009.

[31] Joseph A Weimer. Electrical power technology for the more electric aircraft. In *Digital Avionics Systems Conference, 1993. 12th DASC., AIAA/IEEE*, pages 445–450. IEEE, 1993.

[32] Joseph A Weimer. Electrical power technology for the more electric aircraft.

In *Digital Avionics Systems Conference, 1993. 12th DASC., AIAA/IEEE*, pages 445–450. IEEE, 1993.

[33] TichakornWongpiromsarn, UfukTopcu, NecmiyeOzay, HuanXu, and Richard M Murray. Tulip: a software toolbox for receding horizon temporal logic planning. In *Proceedings of the 14th international conference on Hybrid systems: computation and control*, pages 313–314. ACM, 2011.

[34] HaipingXu. *DRBD: Dynamic Reliability Block Diagrams for System Reliability Modelling*. PhD thesis, Citeseer, 2008.

[35] HuanXu. *Design, specification, and synthesis of aircraft electric power systems control logic*. PhD thesis, California Institute of Technology, 2013.

[36] HuanXu, UfukTopcu, and Richard M Murray. Specification and synthesis of reactive protocols for aircraft electric power distribution.

[37] Backgrounder, 787 Dreamliner Electrical System. Boeing Commercial Airplanes http://www.boeing.com.

[38] Safran. More Electric aircraft [Online]. Available: http://www.safran-group.com/site-safran-en/innovation-429/areas-of-expertise/more-electric-aircraft/?435.

[39] Fault Tree Analysis, Reliability Block Diagrams and BlockSim FTI Edition http://www.reliasoft.com/newsletter/2q2003/fta.htm.

[40] Hagberg, Aric, Pieter Swart, and Daniel S Chult. *Exploring network structure, dynamics, and function using NetworkX.* No. LA-UR-08-05495; LA-UR-08-5495. Los Alamos National Laboratory (LANL), 2008.

[41] YahiaBaghzouz. Synchronous Generators II http://www.egr.unlv.edu/~eebag/Sync%20Generators%20%20II.pdf

[42] Rehab Ashari and SaharHabib. Linear Temporal Logic (LTL) http://www.cs.colostate.edu/~france/CS614/Slides/Ch5-Summary.pdf

[43] Maillet, Quentin, Huan Xu, Necmiye Ozay, and Richard M. Murray. "Dynamic State Estimation in Distributed Aircraft Electric Control Systems via Adaptive Submodularity." In 52nd IEEE Conference on Decision and Control. 2013.

[44] *TuLip User's Guide*. http://tulip-control.sourceforge.net/doc/intro.html

[45] Nuzzo, P. I. E. R. L. U. I. G. I., Xu, H. U. A. N., Ozay, N., Finn, J. B., Sangiovanni-Vincentelli, A. L., Murray, R. M., ... & Seshia, S. A. A Contract-Based Methodology for Aircraft Electric Power System Design.

[46] *Electrical systems architecture for an aircraft, and related operating methods.* http://www.google.com/patents/US20090127855