DISSERTATION

SYSTEM LEVEL RISK ANALYSIS OF ELECTROMAGNETIC ENVIRONMENTAL EFFECTS AND LIGHTNING EFFECTS IN AIRCRAFT – STEADY STATE AND TRANSIENT

Submitted by

James Y. Lee

College of Engineering

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2017

Doctoral Committee:

Advisor: George J. Collins

John M. Borky
James L. Cale
Christopher J. Ackerson

ABSTRACT

SYSTEM LEVEL RISK ANALYSIS OF ELECTROMAGNETIC ENVIRONMENTAL EFFECTS AND LIGHTNING EFFECTS IN AIRCRAFT – STEADY STATE AND TRANSIENT

This dissertation is an investigation of the system level risk of electromagnetic and lightning effects in aircraft. It begins with an analysis to define a system, and a discussion of emergence as a characteristic of a system. Against this backdrop, risk is defined as an undesirable emergent property of a system. A procedure to translate the system level non-functional attributes to lower level functional requirements is developed. With this foundation, a model for risk analysis, resolution and management is developed by employing the standard risk model. The developed risk model is applied to evaluation of electromagnetic environmental effects and lightning effects in aircraft. Examples are shown to demonstrate the validity of the model. Object Process Methodology and systems thinking principles are used extensively throughout this work. The dissertation concludes with a summary and suggestions for additional work.

ACKNOWLEDGMENTS

I would like to express my special appreciation and thanks to my advisor Professor Dr. George J. Collins, for his unfailing guidance, instructions and support throughout my Ph.D. program. His timely advice on research and continuous encouragement have been invaluable to the success of the program. Thank you.

I would also like to thank my committee members, Professor John M. Borky, Professor James L. Cale, and Professor Christopher J. Ackerson, for their kind support and helpfulness.

Lastly, I wish to thank Colorado State University for providing me with an ideal setting for the research.

PREFACE

This work investigates the system level risk analysis of electromagnetic effects and lightning effects in aircraft. The risks of electromagnetic and lightning environmental effects in aircraft systems have been one of the major safety concerns to aircraft manufacturers and airlines since the early days of aviation. These safety concerns are regulated by governmental authorities such as the Federal Aviation Administration (FAA) or the European Aviation Safety Agency (EASA) with certification processes, and aircraft manufacturers have obligation to prove the safety of manufactured aircraft from these hazardous effects in order to sell the aircraft to airlines, government, and individual customers. It is noteworthy that these electromagnetic concerns have been exacerbated in recent years due to (1) increased electromagnetic footprint in aircraft since the early 1990s with the introduction of portable electronic devices and passengers activities such as emailing, web browsing, text messaging, and mobile audio/video service usage, (2) growing application of composite materials for airframes, which do not provide protection against electromagnetic effects as well as aluminum material does, and (3) modern aircraft's increasing dependency on electronics for communications, navigation and surveillance functions, and flight control functions (fly-by-wire). For these reasons, the need to assess, evaluate, mitigate and manage electromagnetic and lightning risks has been growing and is greater than ever.

Considering the complex, inter-related, global, and dynamic nature of electromagnetic environmental and lightning effects, we find application of systems engineering to these electromagnetic risks necessary, useful and beneficial. In particular, in our research, we utilize the standard risk model as a main tool in conjunction with the computer aided fault tree analysis tool for systems risk analysis. The standard risk model is an internationally recognized risk analysis method and provides benefits of clearly expressed causality and event drivers which let us conduct risk mitigation and management activities in a logical manner. Based on this model, several example studies are performed to validate the model. The methodology developed in this dissertation provides a comprehensive risk modeling, which can be used widely in many aviation risk analysis situations. Another practical reason for the need of systems engineering in this area is the current organizational trend of aerospace companies of becoming a systems integration and testing house. Thus there are concerted efforts in aerospace industry to use systems engineering approach for engineering issues in general and the electromagnetic and lightning issues in particular.

The primary purpose of this work is to provide clarity to the fundamental nature of system level risk and to develop a risk analysis methodology with increased rigor. A secondary purpose is to show how the developed methodology can be used to analyze specific problems of electromagnetic and lightning risks. This work leverages prior works of several authors who did research in the area of system level risk analysis of electromagnetic interference. However, this work goes beyond prior works by incorporating the systems risk analysis principles fully in all areas of electromagnetic environmental effects including lightning. Risk is discussed in this work as an emergent property of systems. Emergence as a system characteristic has been studied carefully in the past by many authors and we clarify the meaning of risk in the context of emergence theory. We may call this approach an ontological view. The ontological view on risk is stimulating and productive when it is applied to concrete aviation situations. This view led the author to adopt Object Process Methodology (OPM) modeling language for this work, which was originally developed with a similar ontological motivation. Several systems thinking principles are introduced and expanded. These systems thinking principles play a significant role in developing ideas and approaches in this work. The OPM system modeling language and systems thinking principles are used extensively for this research project.

It is noted that there has been a cultural gap between the electromagnetics community and systems engineering community, and collaborative research activities of the two disciplines are rarely found. Because of the systemic effects of electromagnetic energy, and maturity of systems engineering and electromagnetics engineering, significant results would be generated when the two disciplines are considered together. This work is one of the first serious attempts to bridge the gap between the two disciplines via risk analysis. It is expected that streamlining the engineering electromagnetic risk analysis processes using the method expounded in this research will help the aviation industry and improve the risk management effectiveness over the engineering lifecycle. Employing the model developed in this work should significantly enhance the safety of aircraft against electromagnetic environmental threats.

The discussion is introduced in Chapter 1 which provides definition and various properties of a system. Emergence characteristic of a system is discussed and system level risk is defined as an undesirable emergent property of a system. Processes of how system level quality attributes can be translated into requirements at the subsystem and component level are shown in Chapter 2. Development of a general risk analysis and mitigation model is presented in Chapter 3. Chapter 4 shows the details of electromagnetic environmental risk analysis in aircraft. The lightning risk analysis in aircraft is conducted in Chapter 5. The test procedures and results for lightning risk mitigation are given in Chapter 6. Further validation of the developed risk analysis approach is presented in Chapter 7. This work concludes in Chapter 8 with a summary and recommendation.

DEDICATION

Dedicated to my family – my late father Won-Shik Lee, my mother Kap-Choon Kim, my wife Kum-Ja, and my daughters Adrienne and Katherine, for their unending love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. Introduction

The topic of the dissertation is the system level risk analysis of electromagnetic environmental effects and lightning effects in aircraft for both steady state and transient events. The risk of electromagnetic and lightning threats has been known and of concern since the early days of aviation [1]. Although the risk analysis of electromagnetic interference at a system level has been performed by several authors in the past [2,3,4,5], a comprehensive risk study of both electromagnetic and lightning effects at an aircraft system level has not been accomplished in public literature. The aircraft structure and behavior are quite complex, and so are the effects of electromagnetic threats in aircraft [6]. In order to evaluate such complexity adequately, a systems engineering approach is desired and necessary. Systems engineering is an application of the general systems theory to engineering architectures [7,8]. We note that application of systems theory and systems thinking is quite helpful not only to the design and development of aircraft but also to the effective risk evaluation, resolution, and management. To understand how systems thinking can be helpful in this context, we must understand what a system is [9]. Even though we generally have an intuitive understanding of what the term means, it is prudent to make the term explicitly clear in order to use the systems theory and systems thinking properly.

1.1 System and Emergence

System is an integrated collection of parts or subsystems that is highly organized to accomplish an overall goal. The system may receive various inputs, which go through certain processes in the system to produce outputs, which ideally produce overall desired goals. A system is usually made up of many smaller subsystems or components. A complex entity may be made up of many structures, functions, services, products, groups and individuals. If one part of the system is changed, the nature of the overall system could be changed as well. Thus the changes in the system is systemic, meaning the changes affect the entire system.

Systems range widely. For example, there are mechanical systems such as an air-conditioning unit, biological systems such as a heart, human/mechanical systems such as a boy riding a bicycle, ecological systems such as animals living in a forest, and social systems such as schools, churches, or economic activities. In engineering world, we can classify systems into two groups: technical computer-based systems and socio-technical systems. A technical computer-based system includes hardware and software but operators and operational processes are not part of the system. A technical computer-based system is not self-aware. A socio-technical system includes technical computer-based systems but it also includes operational processes and people who use and interact with the technical systems. A socio-technical system is self-aware. Complex systems are comprised of numerous subsystems and components. The transportation systems shown in Fig. 1 are examples of socio-technical systems. The transportation system evolution in

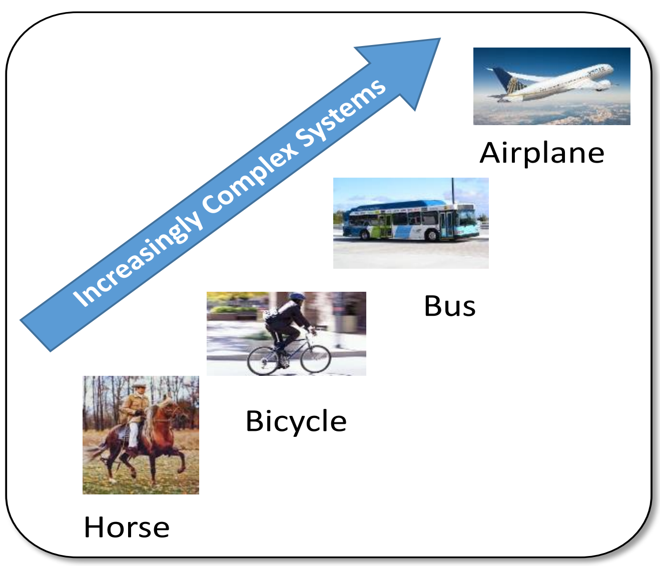

Figure 1. Evolution of a transportation system: complex socio-technical system

Fig. 1 illustrates that a system may evolve from a simple system to a complex system with multiple subsystems. Subsystems or components are arranged in hierarchies and organized to accomplish the overall goals of the system. Each subsystem or component has its modularity property, and includes various inputs, processes, and outputs that achieve the goals of the subsystem. Complex systems usually interact with their environments and are, thus, open systems.

A high-functioning system continually operates on a feedback among its various parts to ensure they remain aligned and focused on achieving the goals. If any of the parts or activities in the system are weakened or misaligned, the system makes necessary adjustments to achieve its goals. Thus a pile of dirt is not a system. If you remove a piece of dirt, you still have a pile of dirt. However, a functioning airplane is a system. Remove the engines and you no longer have a working airplane. An airplane is a system because of new functions an airplane possesses, such as a function of transporting people and cargo. This function is only found in an aircraft as a system and is not found in elements or entities when they are individually considered. This new function, emerged only as a system, is the power and magic of a system. The new emergent function is what makes a system greater than the sum of parts. This feature of a system was stated by the Greek philosopher Aristotle more than two thousand years ago as follows: "The whole is something beside the parts [10]." Thus we may summarize it by saying that a system is comprised of entities and their relationships, and the new functionality as a system is greater than the sum of the functions of individual entities considered separately. This notion of a system indicates the following two important points:

1. A system is comprised of entities that interact or are interrelated.

2. When the entities interact together, a function appears that is other than or greater than the functions of the individual entities.

The first point above is simply about the composition of a system being entities and their relationships. The second point above is about the characteristic of a system: a functionality of a system is other than or greater than sum of functions of individual entities. This describes what is called *emergence* [11,12,13]. Emergence appears when a system operates. Engineers build systems to obtain desired emergence [14,15,16] and the goal of systems thinking is to understand emergence of a system. Thus the essential feature of a system is that new functions emerge from the designed engineering system. Sand and a glass tube are shown in Fig. 2. Sand is material found in nature and does not have any function as is. The funnel shaped glass tube simply constricts a flow of fluid. However, when two are brought together, a new function appears: timekeeping. Individual element when considered separately does not show any trace of a timekeeping function. When they are together, a new informational system emerges by design. The second category of emergence is performance. We may consider the timekeeping performance of the hourglass such as how accurately the hourglass keeps time. This performance property is considered an emergence of the system. The third category of emergence is a set of operational attributes such as maintainability, reliability, safety or operability. These attributes are called the "ilities." Whereas function and performance create values immediately, the ilities tend to appear over the lifecycle

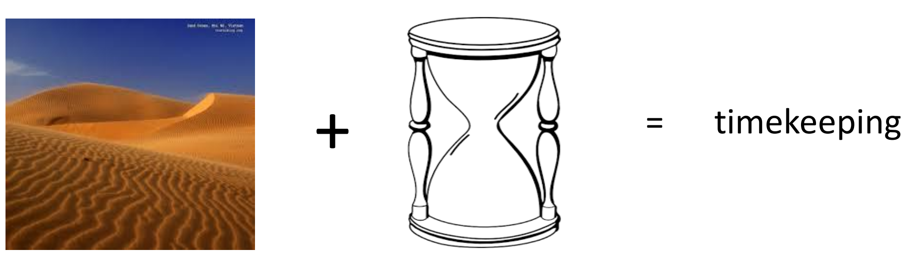

Figure 2. Emergent function from sand and a funnel

of a system. The final category of emergence is called an undesirable emergent properties (UEPs) which are an undesirable and unanticipated emergence. UEP as emergence of a system is illustrated in Fig. 3 for A320-200. On September 14, 1993, Lufthansa Flight 2904, Airbus A320-200, tried to land on the runway at Warsaw International Airport on a bad weather. To overcome reported crosswind, the right wing was lowered, resulting in a single wheel landing. For safety, the software system was designed not to deploy the thrust reversers and spoilers if weight on both wheels and wheel rotation above 72 knots are not detected. Left landing gear did not touch the ground for about 9 seconds after the landing. The computer software commanded thrust reversers and spoilers not be deployed and as a consequence, the aircraft hit the barrier and crashed. The braking subsystem behaved exactly as specified but the system failed. This is an example of a system failure. A reliable software system was unsafe. Safety ility requirement was not met.

It is noted that the function of timekeeping for the hourglass system does not have meaning without a user. The emerged function has meaning only to a user or an operator. This brings up an important point of the role of an operator in the study of emergence. Emergence in systems makes us pay attention to the role of an observer. Then, we ask, if an emergent functionality has meaning

Figure 3. A320 crash showing UEP as an emergence in a system

only with an observer, if the emergence exists only in the mind of an observer, does it mean that emergence does not have an independent existence? This question about subjective quality of emergence has been discussed by several authors. For instance, Crutchfield [17] considered the properties of complexity to be subjective qualities determined by the observer. He believed defining structure and detecting the emergence of complexity are inherently subjective scientific activities. On the other hand, Peter Corning [18] asked, "Must the synergies be perceived/observed in order to qualify as emergent effects, as some theorists claim? Most emphatically not. The synergies associated with emergence are real and measurable, even if nobody is there to observe them." When we consider the emergence in engineering domain, we acknowledge both qualities to be present. In socio-technical systems, we cannot do away with either the role of stakeholders or the objective reality of emerged values.

One of the first remarks of emergence in a historical context was made by Galileo [19]. A column of marble was stored on two supports at either end as shown in Fig. 4. The masons knew these columns could break under their own weight so they placed another support at mid-section of the beam. One of the end supports decayed over time while the middle support has remained

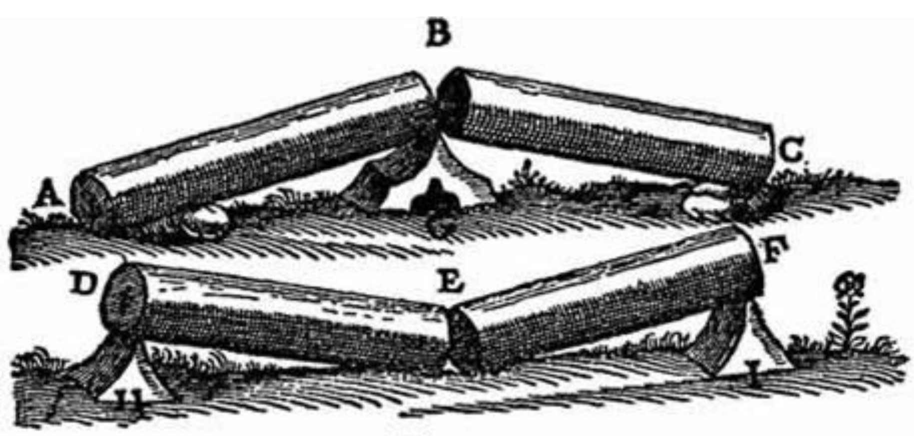

Figure 4. Galileo's broken marble column for emergent property illustration

hard as illustrated in Fig. 4. The half of the beam projected into the air without support. Consequently the column broke at the mid-point. Galileo remarked "it is a very remarkable and thoroughly unexpected accident, especially if caused by placing that new support in the middle." H. Petroski [20] commented that it is, to this day, considered a model of failure analysis.

When we conduct a risk analysis which is the main topic of this work, it is required to define and understand risk clearly. Risk is defined to be the potential that something will go wrong as a result of an event or a series of events. Functionality as emergence of a system is listed in Table 1. The corresponding properties as applicable to risk definition are shown in Table 2. The undesirable and unanticipated emergence, called UEP (undesirable emergent property), fits the definition of risk. The desired and anticipated functionality category also fits the definition of risk if the desired functionality does not happen or is degraded [21,22]. Undesirable and anticipated functionality could be categorized as risk as well since we have to control and monitor the undesirable functionality for opportunity to improve the situation.

Table 1. Functionality as an emergence property of aircraft

	Anticipated	Unanticipated
Desirable	Function, performance and ilities	Sense of freedom
Undesirable	Electromagnetic effects	Anomalies or accidents

Table 2. Risk as an emergent property of aircraft

	Anticipated	Unanticipated
Desirable	Degradation of ilities	N/A
Undesirable	EMI with known probability	Potential of failure

This categorization provides an ontological flavor to functionality and risk discussion [23]. We may sum up the discussion up to this point as follows:

1. The power of an engineering system is in emergence.
2. Emergence is manifest by functionality – function, performance, ilities and UEP (undesirable emergent property). UEP is an emergence with negative consequences.
3. Emergence provides values or meaning to an operator or a user or an observer. This emphasizes the role of an operator, a user or an observer.
4. Risk is defined as an emergent property of a system [24]. It is an emergence with a potential of negative consequences.

Above discussion about systems and emergent property of a system is applicable to a general system. Since the system in this work is restricted to engineering systems, the following definition of systems in ISO/IEC/IEEE 15288 is useful [25]:

"[5.2.1] Systems are man-made, created and utilized to provide products or services in defined environments for the benefit of users and other stakeholders."

Thus an engineering system is a purposeful collection of inter-related components working together to achieve a common objective, and it may include software, mechanical, electrical and electronic hardware. For engineering systems, people are responsible for its installation and operation and systems are procured, owned and operated by organizations.

In summary, a system is made up of entities that interact or are interrelated, and the properties and behavior of system components are inexplicably inter-mingled and form a whole. This forming of a whole with interrelated parts generally leads to a complex system. The main characteristics of such formed systems are new emergent functionality. A system is greater than, or other than, the functions of the individual entities considered separately.

1.2 System and Perspectives

A system, being a complex entity, may be viewed from many perspectives. An example of systems perspectives is given as follows: a sign of 55 MPH maximum speed on a freeway in Fig. 5 may be perceived in several different ways. Professor James C. Maxwell would think of an electromagnetic theory of colors, and Professor Einstein might start speculating on a special relativity theory. A mechanical engineer may perceive the sign from a metallurgical mechanical theory for strength of matter. An artist may pay particular attention to the shapes and shades and how they impress our senses. A systems engineer may perceive that the speed sign is only a final product and note that there were thoughts about the sign initially. It might have been a vague idea, based on a need analysis and requirements. The vague idea evolves into conceptual design through operational and logical perspectives, considering all the system aspects including city ordinances, laws and local government policies to determine whether it is appropriate to the city. Then a detail design in physical perspectives emerged, which turned into an actual physical implementation with activities such as integration, testing, production, distribution and servicing of the products.

So among physicists, a mechanical engineer, an artist, and a systems engineer, whose approach or perception is right? The answer is it depends on the goal: The systems engineering

Figure 5. A speed limit sign on a freeway system may be viewed from several perspectives

approach is the right one for architecting of the engineering product. However, a physicist's perspective is also right if the goal was to investigate the physical property of the sign. Thus a system may be viewed from several different perspectives, and some perspectives are more appropriate than others depending on the goal of the project under discussion. Views and perspectives are as important as the physical system itself if not more. The role of views in the context of architectural development cycle is illustrated in Fig. 6, where several views such as operational, logical or functional, and physical view are shown over the architectural lifecycle [26]. Application of this "perspectives" to engineering systems is discussed next.

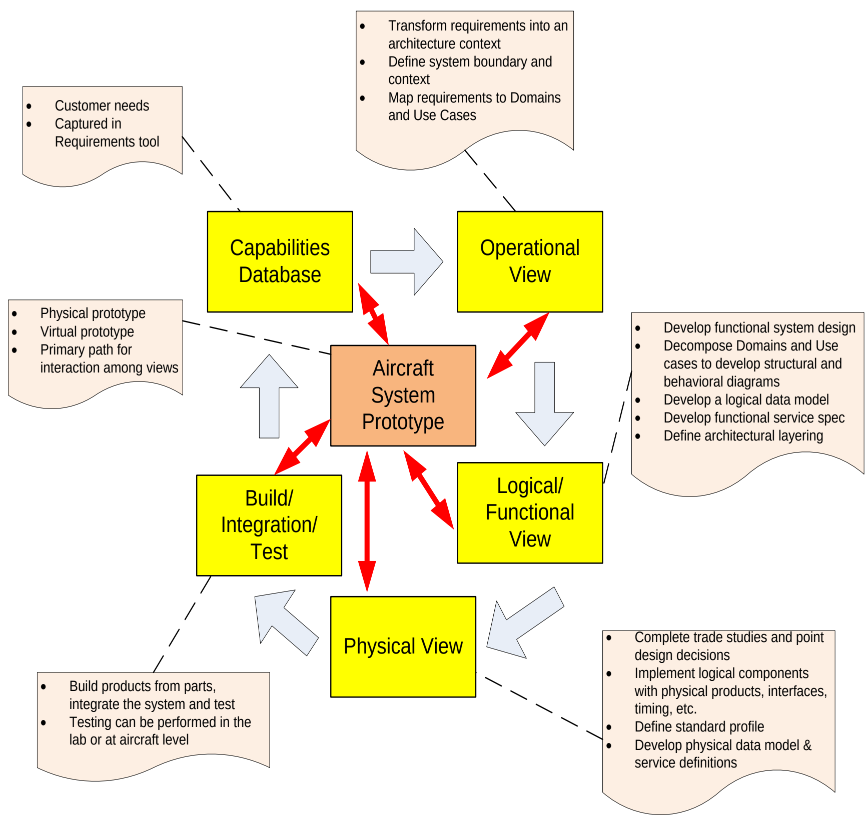

Figure 6. Role of views in architectural development cycle

1.3 System Architecture and Principles

The importance of views and perspectives in engineering systems is illustrated by discussing the systems architecture taxonomy developed by J. M. Borky [27]. A system taxonomy is shown in Fig. 7. We first note that architecture may have the following definitions:

1) In IEEE Std 610,12, architecture is defined as “the organizational structure of a system or component [28].”
2) In the ISO/IEC/IEEE 24765 International Standard, it is defined as “fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design ad evolution … the organizational structure of a system and its implementation guidelines [29].”
3) In [30], authors define architecting as “the process of structuring the components of a system, their interrelationships, and their evolution over time.”

System Taxonomy in Fig. 7 shows three architecture axes [31]. The axis of abstraction indicates the levels of system architecture in terms of abstraction that may progress from operational view,

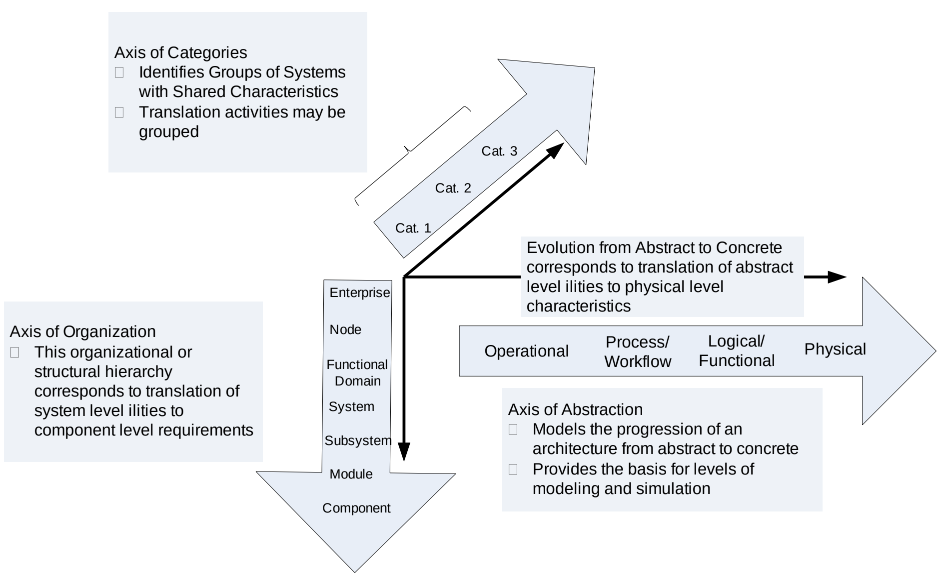

Figure 7. System architecture taxonomy and quality attributes translation

to logical/functional view, and to physical view. The axis of organization refers to the degree of organizational extent from an enterprise level to a component level. The axis of categories refers to the groups of the system identified to have shared characteristics. We are particularly interested in the axis of abstraction since it provides the background of translation of system quality attributes into requirements at subsystem level. The details of the translation process are discussed fully in Chapter 2. System taxonomy helps us to understand the system in a logical way.

Systems thinking may be done with system architecture principles. Systems thinking is thinking about problems explicitly considered as a system. Systems thinking is used for understanding behavior of an existing system and for imagining improved system changes. We use several principles for system thinking. For engineering systems the following principles in Table 3 may be used, which follows the table in [32] with seven added principles. Each principle is discussed below.

1) *The principle of emergence*: As a system is formed by putting elements together, due to interaction between elements, function, behavior, performance, and UEPs emerge.
2) *The principle of holism*: Every system is a part of a large system and is a system of smaller systems.

Table 3. Principles of system architecture

1. Emergence	12. Stress of modern practice	23. Apparent complexity
2. Holism	13. Architectural decision	24. Hierarchy
3. Focus	14. Reuse of legacy elements	25. Second law
4.Perspective	15. Product evolution	26. Decomposition
5. Dualism	16. Beginning	27. Leadership and management
6. Coherence	17. Balance	28. 2 Down, 1 up
7. Benefit delivery	18. System problem statement	29. Elegance
8. Values and architecture	19. Boundary adjustment	30. Robustness of architecture
9. Solution neutral function	20. Ambiguity and goals	31. Coupling & organization of architectural decision
10. Role of the architect	21. Creativity	32. Dualism of function risk
11. Ambiguity	22. Essential complexity	33. Unpredictability

3) *The principle of focus*: The number of identifiable issues of a system at any point is beyond one's ability to understand. Identify and focus on the most critical and consequential issues.

4) *The principle of Perspective*: System architecture may be viewed from many different perspectives. All systems are viewed from perspectives for proper understanding.

5) *The principle of dualism*: All built systems exist in the physical domain as well as in the informational domain.

6) *The principle of coherence:* This principle is closely related to the principle of dualism. The physical domain and the information domain should be coherent from each other.

7) *The principle of benefit delivery*: Good architectures must deliver benefits by focusing on the emergence of functions, delivered across the system boundary at an interface.

8) *The principle of value and architecture:* Architecture is function enabled by form. Benefit is delivered by function, and form is associated with cost. Value is benefit at cost.

9) *The principle of Solution-Neutral Function*: Poor system specifications may lead the architect to a narrower set of potential options.

10) *The principle of Role of the Architect*: To resolve ambiguity, simplify complexity and enhance creativity, which are the architect's role.

11) *The principle of Ambiguity*: Great ambiguity characterizes the early phase of a system design. The architect strives to resolve this ambiguity and produce, and continuously update goals for the team.

12) *The principle of stress of the modern practice*: Modern product development processes should be employed, which include concurrency, distributed teams, and supplier engagement, and having a good architecture.

13) *The principle of architectural decisions*: Architectural decisions must be made carefully. It should be done with enough time taken and upfront because of its criticality.

14) *The principle of reuse of legacy elements*: Use legacy systems fully. Their emergent properties should be studied and selected features are transferred to the new architecture.

15) *The principle of product evolution*: Place importance to interfaces, since the architecture itself evolves and may lose competitive edges.

16) *The principle of beginning*: The stakeholders for both internal and external influence the architecture. Their impact should be considered at the beginning.

17) *The principle of balance*: Be balanced about numerous factors so the factors that satisfy stakeholders are addressed.

18) *The principle of System Problem Statement*: The statement of the problem is where the architecting starts. The problem statement must be studied fully until we are satisfied.

19) *The principle of boundary adjustment*: In order to treat and understand a system properly, it is necessary to set up boundaries wisely.

20) *The principle of Ambiguity and Goals*: Resolve ambiguity and produce representative and consistent goals. The process may go through several cycles.

21) *The principle of creativity*: Resolve tensions to produce good architecture and ensure that creativity emerges.

22) *The principle of apparent complexity*: Keep the apparent complexity within the range of human understanding via abstraction and decomposition.

23) *The principle of Essential complexity*: Pay attention to functionality which drives and forms essential complexity. Choose a concept that produces low grade complexity.

24) *The principle of hierarchy*: All complex systems have hierarchy. Typical hierarchy taxonomy is comprised of organization hierarchy and abstraction hierarchy.

25) *The principle of second law*: Since the actual complexity of the system exceeds the essential complexity, make decisions to reduce the essential complexity to the level of essential complexity.

26) *The principle of decomposition*: Make active choices for decomposition, which affects performance measurement and organization and supplier value capturing.

27) *The principle of leadership and management*: System work is done by project management, and leadership is an important aspect for project management.

28) *The principle of 2 down, 1 up:* Be attentive on the sequence between decomposition at Level 1 and the relationships identified at Level 2.

29) *The principle of elegance*: Low essential complexity and a decomposition that aligns many planes produce elegance in architecting.

30) *The principle of robustness of architecture*: Be attentive to the change which affects robustness and adaptability.

31) *The principle of coupling and organization of architectural decision:* Be sensitive about the metrics to the decisions as well as the degree of connectivity of decisions.

32) *The principle of dualism of function and risk:* Function and risk emerge together.

33) *The principle of unpredictability:* It is difficult to predict emergent properties from physics only, even though no physical laws are violated for emergence.

Among these principles, some of the important principles for the system level risk mitigation work are those of focus (No. 3), dualism (No. 5) and coherence (No. 6). We note a complex system may be analyzed by dividing it into the physical domain and informational domain (dualism), put certain elements under study (focus) and check the coherence between the physical elements and informational elements (coherence).

While we incorporate systems thinking as discussed above into our system architecture consideration, we note that systems thinking has the tendency to cover the object of interest in its entirety, which is the principle of holism. Thus there is a need to balance it out with the focused (centricity) thinking which helps us to give proper attention to the part or aspect of the system under study. This focus is then checked against the background or context for coherence. Thus we may propose the following primary actions: action of principle of focus (centricity) and principle of coherence [33]. In consideration of system architecture, we recognize the principle of focus brings in the limits required for the research, and the principle of coherence brings in the test required to ascertain the correctness of the part within the context of the system. Let's consider an example of aircraft system under electromagnetic threats. The electromagnetic threats affect the entire aircraft, thus the entire system should be examined in accordance with the holism systems thinking principle. However, we may apply the principle of focus to each individual component or subsystem to conduct our research into the subsystem or the component. Subsequently, we apply the principle of coherence to check if our research of the individual component is in coherency with the rest of the system. We can say the line of boundary we draw around the part is not a solid line but is a dotted line tentatively distinguishing the part under discussion from the rest of the system for convenience.

The electromagnetic risk analysis work is heavily electromagnetics-oriented. There is a tendency for an electromagnetics specialist to fall into a trap of concentrating on the narrow area and not seeing the big picture, i.e., seeing trees but not the forest. This defect is corrected by application of these two principles. The view, perspective or the frame is provided for the electromagnetics specialists by systems engineers.

1.4 Conceptual System and Physical System

We wish to explore the topic of conceptual system in this section. We note that a system has the following meaning [34]:

"An integrated set of elements, sub-systems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, and firmware), processes, people, information, techniques, facilities, services, and other support elements. A combination of interacting elements organized to achieve one or more stated purposes."

The above definition refers to both physical systems in the real world and a conceptual system, a mental representation of the actual system [35]. As such, the systems engineer must distinguish between the real world system and the conceptual system.

It is noted Blanchard and Fabrycky [36] made a clear distinction between a conceptual system and a physical system in their general discussion of systems. The importance of this insight has not been appropriately emphasized in public literature. From the detailed analysis of the abstraction hierarchy, we note how widely spread the conceptual system is in engineering systems as well as in systems found in many other areas. The conceptual system exists in the form of written and spoken languages, thoughts, electromagnetic transmission in the air, electrical and non-electrical signals, and data in communication systems and computers, etc., which are also

Table 4. Conceptual system and physical system

		Can concept/information exist without physical system?	
		Yes	**No**
Can physical exist without concept?	**Yes**	Dualism	Materialism
	No	Idealism	Neutral Monism

called an information system or a thought system [37,38]. If we allow ourselves to consider deeper meaning of two systems and their implication, we find that this question has been explored for a long time throughout the western intellectual history. The relationship between a conceptual system and a physical system as shown in Table 4 has parallel to mind and matter problem in philosophy. A 17th century French philosopher Rene Descartes differentiated matter and mind by imagining God's mind and treating the rest of the world as a world of matter. The distinction was made that matter has extension and the mind does not. The mind and matter exist separately and they interact in a mysterious way in human mind. Idealists believe all things are imbued with mind, and matter can exist only with mind. Materialists believe the opposite that matter can exist by itself but mind cannot. Neutral Monists believe all things have mind and matter coexisting as one. We note that the dualism we discussed before in the context of the systems thinking principle is different from the philosophical dualism in Table 4. We acknowledge the two systems of a conceptual system and a physical system exist, but we do not believe a conceptual system may exist by itself. Our position is rather close to materialism and the dualism in the engineering principle of dualism is rather a working hypothesis for engineering purposes. In engineering systems, the conceptual system exists in the form of drawings, diagrams, documents, meeting logs, test data, etc. The artifacts may be understood from this system point of view. Initially there was a concept of an engineering product (aircraft as an example). That concept grew to have extensive ramifications since the concept transforms into to sub-concepts for many parts of the engineering product (wings, fuselage, flight control, engine, power, etc.). Each sub-concept generated respective drawings. Each drawing produced corresponding part. Integration of the parts produced the engineering product (aircraft). In some way this process is similar to the growth of organisms.

The hierarchy of abstraction can be best understood fundamentally by considering the significance of the conceptual system. Concepts eventually are implemented and materialized in the form of a physical system. Lifecycles in systems engineering may be recast as a process of this transformation of a conceptual system into a physical system [39]. In a way we may say all written and spoken activities in engineering are of a conceptual system because concept formation in such activities is a typical way we conduct engineering. We may equally say all activities in engineering are of a physical system since for every conceptual system, there is a corresponding physical system. As we discussed before, this aspect of the relation between the two systems may be called a principle of duality [40], but it is different from the Cartesian dualism. As commented before, we take a position of materialism on this issue that an information domain in the form of concepts, design, drawing, past lessons is based on a physical system which is in the form of hardware and test equipment. A distinction between the conceptual system and the physical system is possible, but we may say they are generally two sides of the same coin. Take an aerospace company as an example of a system organized by concepts. We have the concept of the company's existence and structure. This concept of common understanding ties together the enterprise headquarters, engineering offices, manufacturing facilities and test labs. What we consider an aerospace company is entirely organized by this conceptual system. Without this conceptual system, people wouldn't know what they are supposed to do and how all these facilities as a physical system are related to each other. Thus the conceptual system is at the core of the company, and company's changes and evolution are based on the conceptual system. Projects or product development at a company start with a conceptual system on an abstract level and then progresses into logical/functional and to a physical system eventually. Again we emphasize that the dualism in system architecture is different from the dualism in metaphysics developed by the French

Philosopher Rene Descartes [41] who advocated demarcation between God's mind and matter. The system architecture is a physical system which is designed, iterated and monitored by the engineering mind which is a conceptual system in the informational domain. In engineering, we take the position that mind always has the material basis of neurophysiological system and is never a separate entity on its own. The separate existence of mind was the position of Rene Descartes who placed the mind in God, which was the dominant thinking in the 17th century. We view that engineering mind always has a physical basis, thus materialism would be the best description of our position.

The way of interaction between the two is another interesting question with a long history in the theory of knowledge or truth. Thus we wish to discuss this principle of dualism for the relation between the two systems. The main question is, when we have the conceptual system and the physical system, how we ascertain the physical system is correctly materialized per the conceptual system and how the conceptual system represents the physical system correctly. This question has been treated in the epistemology as a theory of knowledge [42]. According to the theory of knowledge, there are three theories on truth: (1) correspondence theory, (2) coherence theory, and (3) pragmatist theory. These three theories take different approaches as to what constitute the truth and relation between knowledge and reality. In engineering domain, we take all three theories to be relevant depending on situations, context and goals. The engineering drawings match the engineered artifacts, testing per conceptual system coherently matches the outcome in the physical system, and the conceptual system as well as the physical system provide practical values. Views are one of the key concepts in systems architecture. The main components of the conceptual system are the views or representations. These two systems, conceptual and physical, are internally related and one flows to the other in one movement.

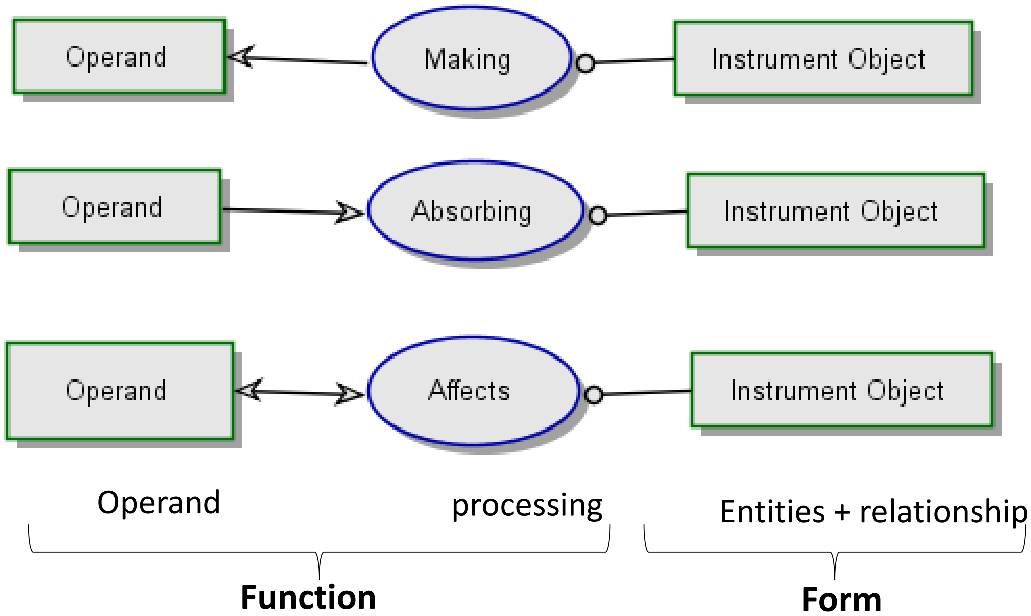

Figure 8. OPM representation of canonical system architecture

The fundamental structures of conceptual system and physical system may be modeled with Object Process Methodology (OPM, ISO 19450, 2015) developed by Professor Dori [43]. The modeling language was created on the ontological basis and the canonical structures are illustrated in Fig. 8 and Fig. 9.

Creation of OPM language is based on an ontological thinking about general existence. It recognizes that the universe may be described with objects and processes (thus the name object-process methodology). This structure is similar to the transformational grammar being subject-verb-object structure as expounded by Noam Chomsky. The correspondence of subject to instrument, verb to processing, and object to operand is apparent. This canonical structure is fundamental to all systems and this is perhaps the way our brains operate as well. The canonical system model in Fig. 8 shows a form and function relationship. The form belongs to a physical system and function belongs to a conceptual system. A form is comprised of entities and their

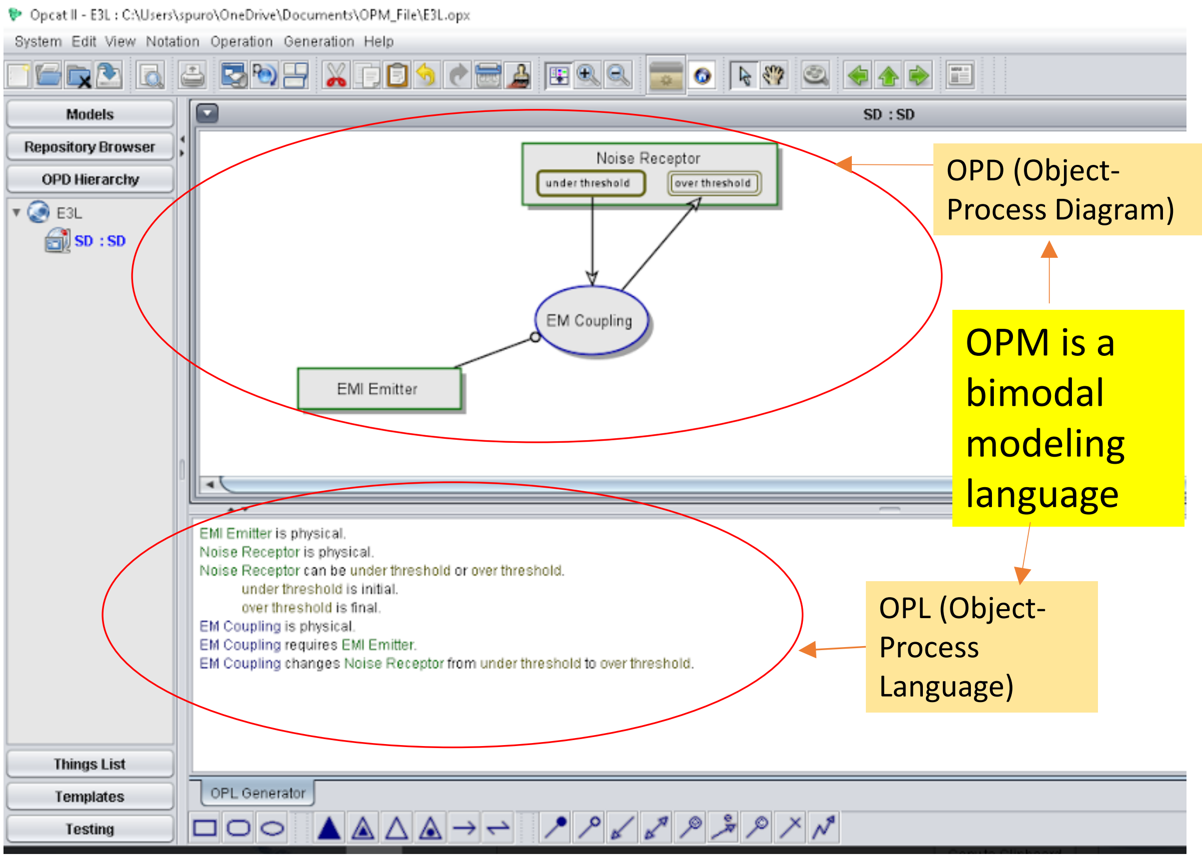

Figure 9. OPCAT suite for EMI energy coupling model

relationships and a function is comprised of processes and operands. Processing works on the operands and operands are the targets of the processing.

This simple yet powerful diagram is an ontological representation of systems. Form is comprised of entities and relationship between them. There are three types of processing: creation of operand (making), destroying of operand (absorbing) and affecting of operand. Affecting means state changes of the operand. The platform for the modeling tool is shown in Fig. 9. It shows that OPM can be created in the OPCAT suite and the OPM language is a bimodal language with OPD (object process diagram) and OPL (object process language). OPM is appropriate for ontological modeling, thus is appropriate when risk analysis is viewed ontologically.

1.5 System and Risk

We defined risk as an emergence or degradation of emergent functionality already in the previous section. We wish to continue to consider risk in general within the context of systems. Risk is defined as a potential that something will go wrong as a result of an event or a series of events [44]. To discuss the relationship between risk and issues, let's consider the burnt circuit in Fig. 10. The burnt circuit is an issue since the lavatory control function is disabled because of this anomaly. However, before the circuit was burned, the situation was at risk. After the circuit was burnt, the circuit for all other airplanes of the same model became at risk. Thus issues and risks are closely related in this sense. The scope of risks goes beyond the technical nature and includes marketing, sourcing, regulatory and management [45]. In the context of discussing electromagnetic effect risks, we are primarily interested in the technical risks. Specifically, to

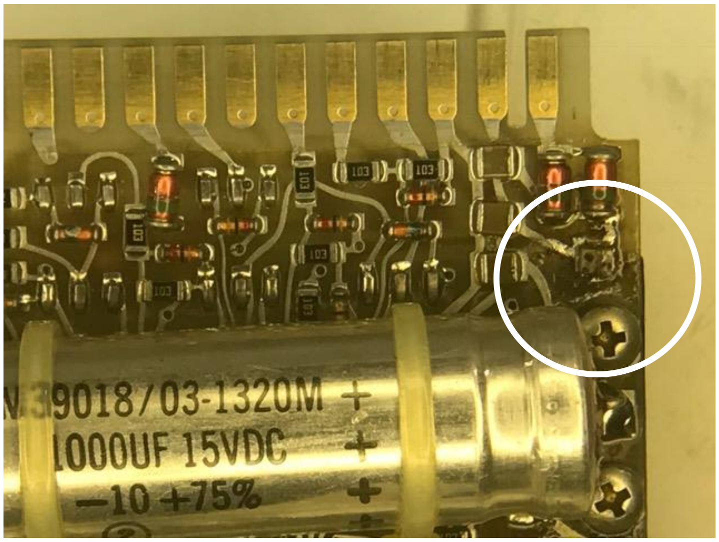

Figure 10. Burnt circuit in lavatory drain control logic represents issues and risk

discuss system level risks, we first want to examine the systems architecture. A system architecture may be treated from several perspectives: structural perspective, behavioral perspective, service perspective and data perspective, which are further elaborated in the architecture methodology called the model-based system architecture process (MBSAP) [46]. So we may say risks may reside in structural, behavioral, service and data perspectives. When electromagnetic risks or threats are examined carefully, we find risks exist in all four perspectives. A direct lightning effect that may affect the aircraft fuselage is an example of a structural risk. An indirect lightning or high intensity radiated fields (HIRF) affecting aircraft equipment operation is an example of a behavioral risk. Electromagnetic interference (EMI) affecting flight control computer data streams is an example of data risk. Portable electronic devices (PEDs) introduced into aircraft by passengers affecting airborne internet communication services would be an example of service risk. A risk is a potential event, expressed by probability values.

Risks may exist at many different organizational levels and it is necessary to be able to address risks at all levels. Wherever we find functions, we also need to talk about risks. This is because we have to be prepared for the worst case as engineers. Discussions of risks at system level and at subsystem level can be found in Chapter 2. The discussion includes details of how non-functional properties such as safety or reliability may be passed down and translated into subsystem level requirements such as the probability specification of fuel subsystem explosion due to lightning strikes. Electromagnetic risks are high when the electromagnetic energy flow are impeded. Risk mitigation techniques such as conductive bonding or grounding enhance the energy flow. The details of how electromagnetic and lightning risks are identified, analyzed and mitigated are shown in Chapters 4 and 5.

1.6 Challenges and Contributions of this Work

This work deals with the following challenges and offers the contributions below.

(1) It is noted that there is a lack of systematic, logical, and disciplined approach to the electromagnetic environmental effects in aircraft. Systematic evaluation of the electromagnetic effects on aircraft equipment is best approached by system level risk analysis and we find that adoption of the standard risk modeling as done in this work to be the best approach.

(2) The approach used in industry to evaluate electromagnetic and lightning effects is testing in the lab. The test results produce fixed values, which means the electromagnetic effects are considered deterministic. As Keith Armstrong strongly argued [47,48], the current reliance on "testing" implies this hazard is deterministic. However, the risks of electromagnetic and lightning effects (susceptibility) are actually probabilistic. The risk analysis in this research sees this susceptibility as "probabilistic." The nature of susceptibility is probabilistic because the threat levels are never completely known, and only the range of the threat levels are estimated. It is not prudent to always choose the worst case and test the susceptibility at the worst case level because if one chooses that route for lightning test, one will always test the lightning "direct" effect test with 200 kA. One can't and one should adjust the level to a reasonable level and use the probabilistic approach. Also we note that testing is not a deterministic endeavor. Testing in the lab has many implications and it can be done in many different ways. We note there are many variations on how to configure the test setup geometry as far as the radiating antennas and test articles are concerned. The distance, angle and the whole configuration could be subject of discussion. The exact

spot which the radiating antenna is pointing at is also a subject of discussion: at connectors, or wires, horizontally or vertically. Lab environment should be also discussed. Fans may be in operation in the lab, and there could be connections to the console outside lab, since test computers in console might generate noises and affect the susceptibility test. The point is there are just too many variables in the test and it is not practically possible to figure out all the factors in deterministic way. Thus the most sensible approach would be the probabilistic approach. The system level risk analysis we perform in this work is designed to accomplish this goal. Risk is expressed as a probabilistic quantity and this risk analysis work is fundamentally probabilistic.

(3) Schism exists between the electromagnetics community and the systems engineering community. The tendency of EMI/EMC engineers is to investigate the details of electromagnetic fields and current distributions at the parts of concern. While this investigation at the component level is one of the necessary steps, the ultimate goal of assessing and mitigating the electromagnetic risks is to understand their impact at the system level. A typical electromagnetics specialist is not well trained in the systems engineering, but it is believed that application of systems engineering to electromagnetics engineering is an extremely important and valuable activity. There may be cultural and historical reasons for the schism between the two disciplines but it doesn’t have to be that way. This work is one of the first serious attempts to bridge the gap between the two disciplines. The combining of the two disciplines should generate synergy that will be proven significantly productive because electromagnetic energy is fundamentally propagative and global and so study of its effect on electronic modules and systems should be conducted from the systems engineering perspectives.

1.7 Chapter Conclusions

In order to provide increased rigor to the system level risk analysis, we examined the definitions of systems and emergence. We have noted that emergence is one of the most important characteristics of a system. The categorization of emergence in terms of desirability and predictability has been performed. Defining systems with emergent properties led us to the definition of risk in a natural way as undesirable emergent properties of systems. The nature of risk is discussed within the categorization table of emergence. This ontological approach was found to be best served by using the Object Process Methodology (OPM) for modeling purposes. OPM modeling is appropriate and applicable to the electromagnetic risk analysis. The OPM modeling platform, OPCAT suite, has been introduced. Numerous principles of system architecture and systems thinking were given and discussed. In addition to 26 principles found in public literature, seven new principles have been newly introduced in our research. The OPM modeling language and the discussed principles of systems thinking are used extensively throughout this work.

2. Translation of System Quality Attributes to Subsystem Requirements

As a background for the system level risk analysis, we would like to consider how the system level quality attributes may be passed down to subsystem and component level and translated into functional requirements. The main quality attribute of this work, safety or risk, is considered to be a non-functional property of a system. We already have shown that ilities are emergent properties of a system in Chapter 1. Safety is one of the ilities which aircraft customers view to be the most important ones. Without aircraft safety ensured, all other values will have very little meaning. The safety ility is declared to be the most important value in the FAA value statement [49] and aircraft manufacturers and airlines also declare similar value statements. This Chapter describes how such quality attributes or ilities may be passed down to subsystems and translated into requirements.

In consideration of the use of ilities for systems engineering of subsystems and components, we note prior work on ilities has emphasized or restricted their application to system level non-functional properties. The premise of this work is that ilities can be applied with benefit, and in some cases of necessity, to lower levels of systems as well. The veracity of this premise is established by pointing to an example that demonstrates how safety is passed as a non-functional property of electrical and structural subsystems in commercial airliners. It is further demonstrated that passing ilities down to the subsystem level is not only a useful practice for systems engineers, but it can be an essential step to ensure that customer needs are actually met by the system. Systems engineers often lack the detailed knowledge of the subsystems or components required to translate ilities into functional requirements. Thus the system ilites are passed down and translated by subject matter experts from non-functional to functional requirements. We recast the ilities translation process using expanded SoS architecting with ilities (SAI) method. The relation of the ilities translation process to classical system engineering processes is discussed. This chapter paves a way to explore the possibility of applying systems engineering principles to electromagnetics engineering, filling the gap between the two disciplines.

2.1 Introduction

Ilities are a way for systems engineers to capture customer needs early in the system lifecycle prior to the development of functional requirements. They are the developmental, operational, and support requirements a program must address. Examples are reliability, quality, flexibility, safety, durability, manufacturability, and testability as shown in Fig. 11 and Table 5, to name a few [50]. They are not specific requirements of the system. Rather, they are properties of

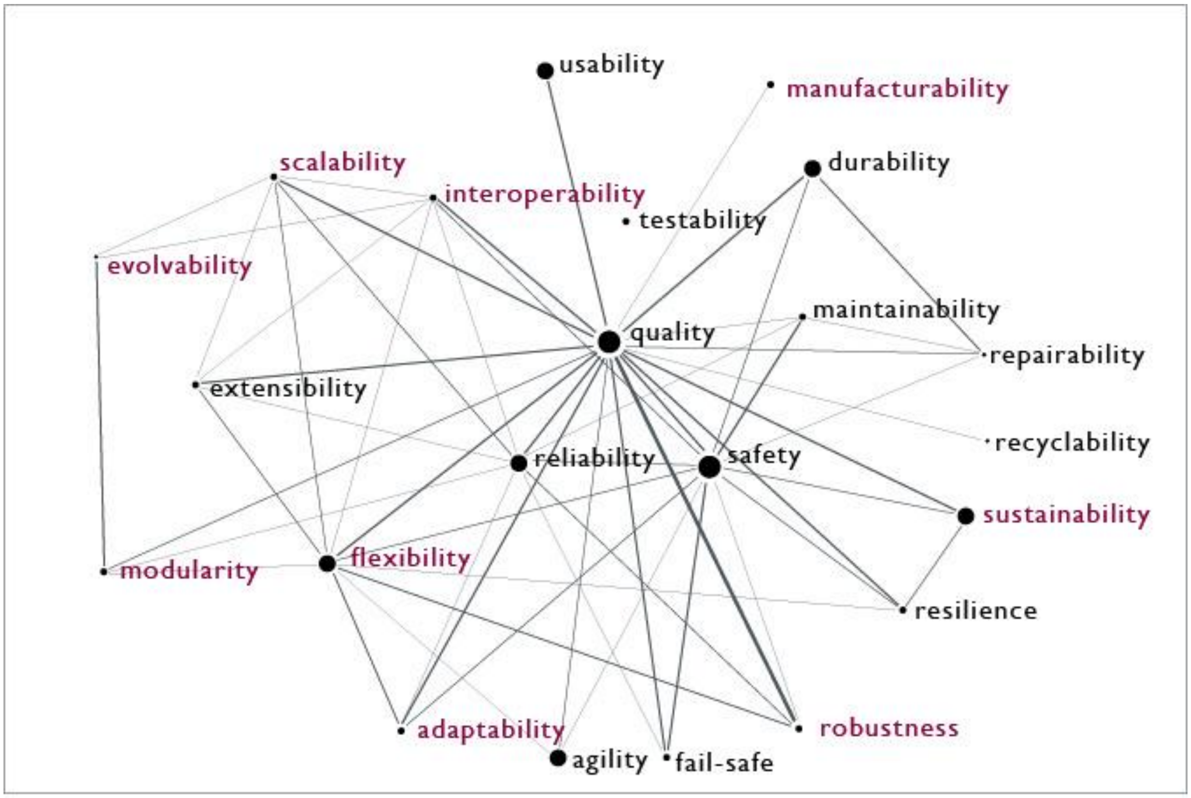

Figure 11. Diagram of ilities

Table 5. List of ilities

Quality	Reliability	Safety	Flexibility	Robustness
Durability	Scalability	Adaptability	Usability	Interoperability
Sustainability	Maintainability	Testability	Modularity	Resilience

the system that are important to customers and other stakeholders. Each ility may have a variable level of importance to each stakeholder and one function of the systems engineer is to work with the team chartered with implementing the system to develop a solution that balances all stakeholder interests. The ilities are then translated to functional requirements.

A more restrictive definition of ilities limits them to only system level non-functional requirements. For instance, they have been defined as "desired properties of systems, such as flexibility or maintainability … these properties are not the primary functional requirements of a system's performance, but typically concern wider system impacts with respect to time and stakeholders [51]." On this understanding, ilities are limited to system level descriptions. A similar definition of ilities was used in [52] where ilities were restricted to stakeholders' needs in relation to the level of service. In their approach, ilities are used in a quality function deployment (QFD) matrix which transforms the qualitative user demands into quantitative parameters. This approach provides a valuable tool to systems engineers in managing ilities, but it is applied only at a top system level and does not flow ilities to lower parts of the system.

This same approach of limiting ilities to system level analysis exists in software development. For instance, this approach is taken in [53] which uses non-functional requirements for software architecting. On their approach, each ility is listed in a table which can be used to assess the ability of the architecture to achieve desired system aspects for space mission flight software. While this is a valuable tool for software development, the ilities are only applied at the system architecting level.

The central proposal in this work is that for complex systems, ilities can be applied with benefits to not only system level properties, but also to subsystems as well. The veracity of this premise is established by pointing to an example that demonstrates how safety is passed down as a non-functional property to electrical subsystems in commercial airliners. Examples of an emergency light subsystem and lightning related subsystems are shown. A secondary point of this work is that passing ilities down to subsystem level is not only a useful practice for systems engineers, but it can be an essential step to ensure customer needs are actually met by the system. This is due to the fact that systems engineers often lack the detailed knowledge of subsystems or components required to translate ilities into functional requirements. As a result, for complex systems, ilites are passed down so they can be translated by experts from non-functional to functional requirements which ensures that customer needs are met. The idea that ilities can be used not only at a system level, but also at a subsystem level for complex systems is the central focus of this work.

This work is divided into seven sections. Section 2.2 proposes a working definition of ilities which accounts for their use in subsystems and components. Section 2.3 considers the place and implication of conceptual system in systems engineering. Section 2.4 provides examples for how ilities for complex systems are passed down to subsystem or components in the system. The point of this section is to establish the legitimacy of the premise. Section 2.5 describes the expanded SoS Architecting with Ilities (SAI) method to be used when ilities are passed down. Section 2.6 discusses the correlation between translation process and the development process in classical systems engineering. Section 2.7 provides a summary and suggestions for additional work

2.2 Definition and Scope of Ilities

The proposed definition of ilities builds upon prior work, but expands it. It includes their use in lower levels of systems such as subsystems and components. We don't propose a redefinition of ilities, but rather a redefinition of their scope of use. That ilities describe system level properties is not disputed. Users and most stakeholders are concerned about system level properties and are much less concerned about the subsystems used to achieve them.

The contention of this work is that it is incorrect to confuse stakeholder ility concerns with how systems engineers and architects use ilities. Instead of ilities being converted from system level non-functional requirements to system level function requirements only, they can be passed to lower levels in the system for conversion to functional specifications. In other words, just because stakeholders view ilities as system level properties they are concerned with does not mean that the use of ilities by developers must be restricted to only the system level. Instead, for complex systems, ilities can be passed down to lower levels in the system such as subsystems and components for conversion to functional requirements. This practice frees up certain restrictions existing in ilities engineering and offers significant benefits for paving a way to apply systems engineering principles to subsystems and components engineering. In this paper, we apply this approach to engineering electromagnetics. Other benefit of the expansion of scope of ilities is that it increases the tools available to systems engineers and architects. This is because it allows them to perform ilities trade studies not only at the system level, but also at the subsystem level. This can be an important benefit since it allows trade studies at the lower levels of the system prior to conversion of non-functional properties to functional requirements.

The translation may be viewed from an architectural hierarchy viewpoint such as of abstraction or organizational [54]. It is illustrated in Fig. 12 that translation can be performed either in the hierarchy of abstraction or organization. Typically ilities are considered at the system of systems (SOS) or systems level and the translation is performed at a lower level. A similar translation may be performed in the hierarchy of abstraction. The ilities are placed at highly abstract level such as operational viewpoint and are translated at a less abstract level. Thus the translation covers the flow from an operational viewpoint to a functional/logical viewpoint and to a physical viewpoint. In this context, consideration of conceptual system provides the key to fundamental understanding.

2.3 Place of a Conceptual System in Systems Engineering

Blanchard and Fabrycky [55] made a clear distinction between a conceptual system and a physical system in their general discussion of systems. The importance of this insight has not been appropriately emphasized in public literature. From the detailed analysis of abstraction hierarchy, we note how widely spread the conceptual system is in engineering systems as well as in systems found in many other areas. The conceptual system exists in the form of written and spoken

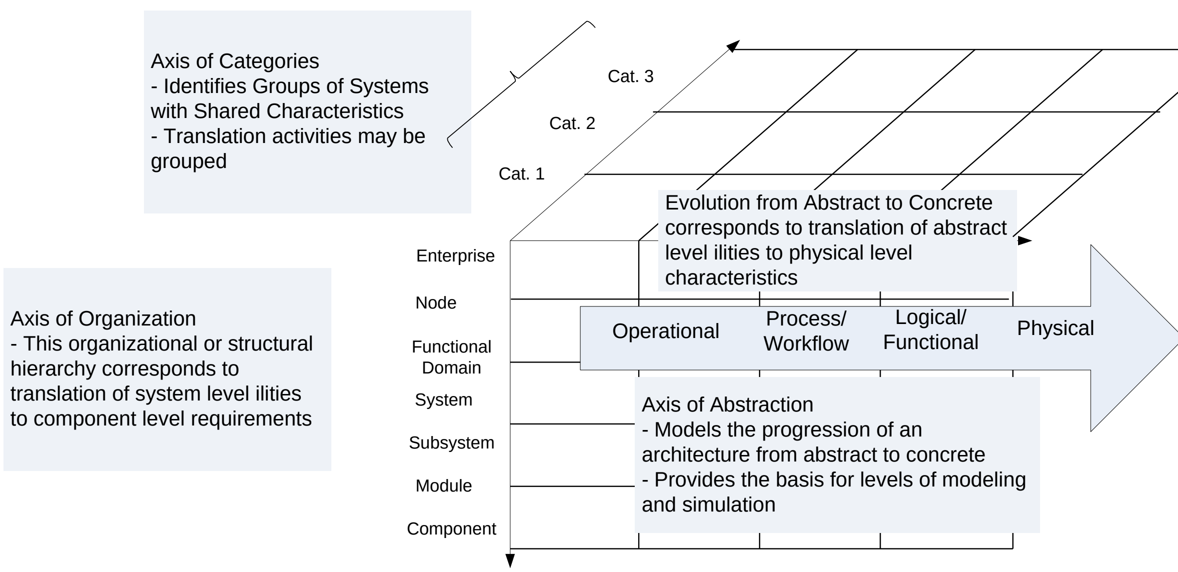

Figure 12. Ilities translation in the context of architecture hierarchy

languages, thoughts, learning, planning, electromagnetic transmission in the air, electrical and non-electrical signals, data in communication systems and computers, and others [56]. In engineering systems, the conceptual system exists in the form of specifications, drawings, diagrams, documents, meeting logs, test data, procedures, reports, and others. The hierarchy of abstraction can be best understood fundamentally by considering the significance of the conceptual system. Concepts eventually are implemented and materialized in the form of a physical system.

Lifecycles in systems engineering [57] may be recast as a process of this transformation of a conceptual system into a physical system. The hierarchy of abstraction can also be recast from this point of view [58]. In a way, we may say all written and spoken activities in engineering are of a conceptual system because concept formation in such activities is a typical way we conduct engineering activities. We may equally say all activities in engineering are of a physical system since for every conceptual system, there is a corresponding physical element or system. This aspect of the relation between the two systems is called a principle of dualism [59]. A distinction between conceptual system and physical system is possible, but we may say they are generally two sides of the same coin. Take an aerospace company as an example of a system organized by concepts. We have the concept of the company's existence and structure. This concept of common understanding ties together the enterprise headquarters, engineering offices, manufacturing facilities and test labs. What we consider an aerospace company is entirely organized by this conceptual system. Without this conceptual system, people wouldn't know what they are supposed to do and how all these facilities as a physical system are related to each other. Thus the conceptual system is at the core of the company and changes and evolution are based on the conceptual system. Projects or product development at a company start with a conceptual system on an abstract level and then progresses into logical/functional and to a physical system eventually.

2.4 Ilities Translation in Aircraft Electromagnetic Environment

In Section 2.1, we proposed the idea that ilities can be applied with benefit to not only system level properties, but also to subsystems as well with proper translation. In this section, we intend to describe an example of how the ilitiy of safety is passed down to the electrical subsystem of a commercial airliner. Specifically, the electromagnetic environmental effects (E^3) will be used as an example [60,61]. Safety as a top level system ility comes from stakeholders such as the FAA, the EASA, aircraft manufacturers, and airliners. We note that safety is a primary issue in aircraft operation as the following value statement of the FAA attests:

"Our continuing mission is to provide the safest, most efficient aerospace system in the world … Safety is our passion. We work so all air and space travelers arrive safely at their destinations [62]." (FAA Value Statement 2015)

This is a major motivating factor for every policy and regulation decision made by the FAA. This emphasis on safety is also shared by the manufacturers of commercial airliners. For instance, the vision statement of Boeing emphasizes:

"We value human life and health above all else and take action accordingly to maintain the safety of our workplaces, products and services." [63].

Airliners also understand that the future of their company depends upon producing products that maintain the safety of their airliners. Based on these considerations, Safety is introduced to aviation industry as one of the most critical ilities that cover the system level needs. We propose the translation of the system level ilitiy of safety into the requirements at the subsystems level be done for various environmental threats to aircraft [64]. Safety as an ility is a non-functional system property which stakeholders understand is critical to customer needs.

Firstly, safety is passed down from the system to the subsystem. Subsequently, the subsystem experts translate the requirement of safety into functional requirements.

Consider, for instance, how safety is applied to electromagnetic environmental threats on aircraft. The aircraft subsystem engineer will apply a context diagram for threat environment categories. It is shown in Fig. 13 which describes the electromagnetic environment of aircraft such as lightning, HIRF, PEDs, P-static and EMI/EMC. [65]

- Lightning: These are lighting strikes on the aircraft body during flight or while on the ground [66].
- HIRF: These are High Intensity Radiated Fields from sources such as radar systems, radio transmitting towers, to name a few [67,68].
- PEDs: These are Portable Electronic Devices such as mobile phones, lap tops, and tablets which can radiate electromagnetic energy when taken onboard an aircraft [69, 70].
- P-Static: This is Precipitation Static caused by friction between air particles and the surface of aircraft.
- EMI/EMC: These are electromagnetic interference and compatibility among electrical and electronic equipment.

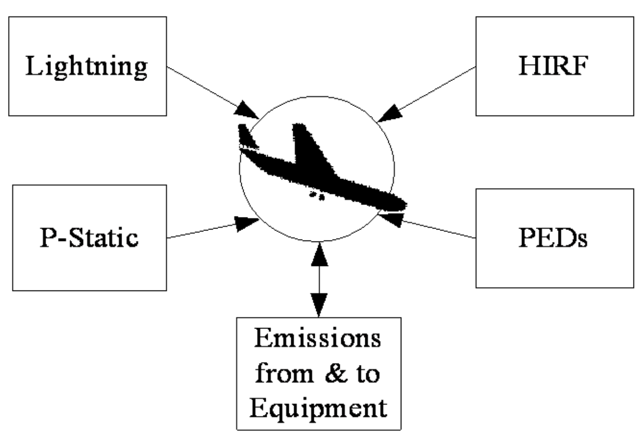

Figure 13. Aircraft electromagnetic context diagram

These electromagnetic effects are directly related to safety of aircraft and they may be effectively used in discussing the level of effects in aircraft. Safety value is absorbed by the subsystem experts and used as a guide for decisions, specifications, and processes. The subsystem engineer will consider the recipients of these electromagnetic threats in an aircraft as shown in Fig, 9 and translate the system level safety concerns into subsystem or component level consideration. Translation requires specific knowledge of the subsystems that can be affected by electromagnetic threats.

This process of translation occurs when the subsystem and component experts develop testing methods, requirements, and qualification processes. The goal of safety is not quantified; it is a non-functional system property which the experts understand is critical to customer needs. Therefore, safety ility becomes a guide standard.

Next we wish to review the translation process in detail. Lightning strike attachments generate both direct and indirect hazardous effects to aircraft safety. Lightning direct effect events are as follows [71,72].

(1) Lightning direct effects:

a. Melt-through damage for metal or non-metal skins (of fuel tank skin, trailing edge, painted skin, and radome).
b. Resistive heating damage (bonding strap heating or exploding wires for a navigation light on a plastic vertical fin cap, diverter straps, pitot probe air tube, and radome) Magnetic force effects (slamming together of two metal air pressure tubes in a radome mounted pitot system, in wing tip trailing edges, bent bond straps).
c. Arcing across bonds (over riveted joints with corrosion inhibiting coating, over fasteners or bonding jumpers with inadequate current carrying capacity, over fasteners

in secondary structures such as wing tips, tail cones, wheel well doors, and flight control surfaces, over adhesive bonds, over hinges and bearings resulting in pitting or welding).

d. Sparking over structural joints.

e. Punctures or flash-over over nonconductive composite material (radomes, composite material skin).

f. Damage of windshields, canopies, windows (direct or swept channel attachment to heating elements and damaging the connected power circuits).

g. Damages on electrically conductive composites (carbon fiber composite skins in Zone 1 and 2 by lightning stroke currents by mechanism of pyrolysis and shock wave; primary structures, engine nacelle and pylon, flight control surface, leading edge devices, avionics bay, wing and empennage tips, fuel tank skin).

h. Damage of propulsion system (engine cowlings or nacelles, propeller and rotor blades, gear boxes damaged by lightning attachments).

i. Rain erosion of conductive lightning protection strip (degradation of conductive frame on wings and empennage).

(2) Lightning indirect effect events for which the following systems of concern fail:

a. Full authority digital engine control (FADEC).

b. Full authority electronic flight control (Fly-by-wire).

c. Supervisory control systems capable of initiating control inputs that could endanger flight safety.

d. Fully or highly integrated cockpit instruments and displays.

e. Electronic flight instrumentation system (EFIS).

f. Aircraft electric power control and distribution system.

g. Electrical and avionics systems that include externally mounted apparatus, such as air data probes, heaters, actuators, and antennas.

(3) Fuel tank ignition or fire due to lightning strikes.

As we examine the lightning threats in aircraft, we note specific components must be included in resolving the issues. In other words, discussions of the damage and effects due to lightning strikes encompass the system level safety concerns as well as the subsystem and component level inspection of the damages and risk resolution. This process is applicable to many safety/risk situations. Table 6 illustrates subsystems for the example and corresponding subsystem parameters. Thus we may say the safety as an ility is introduced at a system of systems (SoS) or systems level. When this ility is passed down to the fuel subsystem level, fuel subsystem engineers or subject matter experts examine the safety parameters of the subsystem such as fuel tank explosion probability and develop specific requirements such as fuel tank explosion probability

Table 6. Translated ilities at subsystem level for lightning effects

System Ility	Subsystem Ility	Subsystem (Category)	Subsystem Parameters
Safety	Safety	Fuselage (DLE)	Melt-through damage
Safety	Safety	Navigation Light /Pitot tube (DLE)	Resistive heating damage
Safety	Safety	Wing tip/Tail cone (DLE)	Arcing across bonds
Safety	Safety	Structural joints (DLE)	Sparking
Safety	Safety	Radome (DLE)	Puncture
Safety	Safety	Windshield, canopy, window (DLE)	Mechanical damage
Safety	Safety	Composite (DLE)	Damage
Safety	Safety	Propulsion system (DLE)	Mechanical and thermal damage
Safety	Safety	Conductive strip on rudder (DLE)	Rain erosion
Safety	Safety	Full authority digital engine control (DLE)	Anomaly in engine control
Safety	Safety	Full authority electronic flight control (DLE)	Flight control error
Safety	Safety	Supervisory control systems (DLE)	Erroneous control
Safety	Safety	Fully or highly integrated cockpit instruments and displays (ILE)	Flickering in display
Safety	Safety	Electronic flight instrumentation system (ILE)	Error with instrumentation
Safety	Safety	Aircraft electric power control and distribution system (ILE)	Unpredictable Power shedding
Safety	Safety	Electrical and avionic systems (ILE)	Air data malfunction
Safety	Safety	Fuel Tank (FTI)	Tank Flammability

DLE: direct lightning effects
ILE: indirect lightning effects
FTI: fuel tank ignition

requirement of 10E-9 per flight hour. Fuel tank component engineers conduct researches into components such as fuel tank gaskets and might develop new design of components. Role of the Systems Engineer after Ilities are Passed Down The systems engineer and system architect can use ilities at the system or lower levels to perform trade studies to optimize value delivery to users and other stakeholders. In addition, once ilities are passed down to subsystem or component developers, the role of the systems engineer is to ensure that the correct emphasis is placed on ilities during the translation to models and functional requirements [73]. In other words, if the ilities are properly managed, then stakeholder needs prioritize the ilities and the role of the systems engineer is to ensure continuity of the priorities. As a result, the system engineer must be involved in the process of translating the ilities to subsystem or component functional requirements.

There are several methods to use ilities for conceptual design. One approach useful for systems of systems is called the expanded system of system architecting with ilities (SAI) method which is an expanded version of the published SAI method [74]. Another method uses non-functional requirements and quality function deployment (QFD) matrix to rank each of the ilities [75]. For our analysis here, we have focused on the expanded SAI method which is established

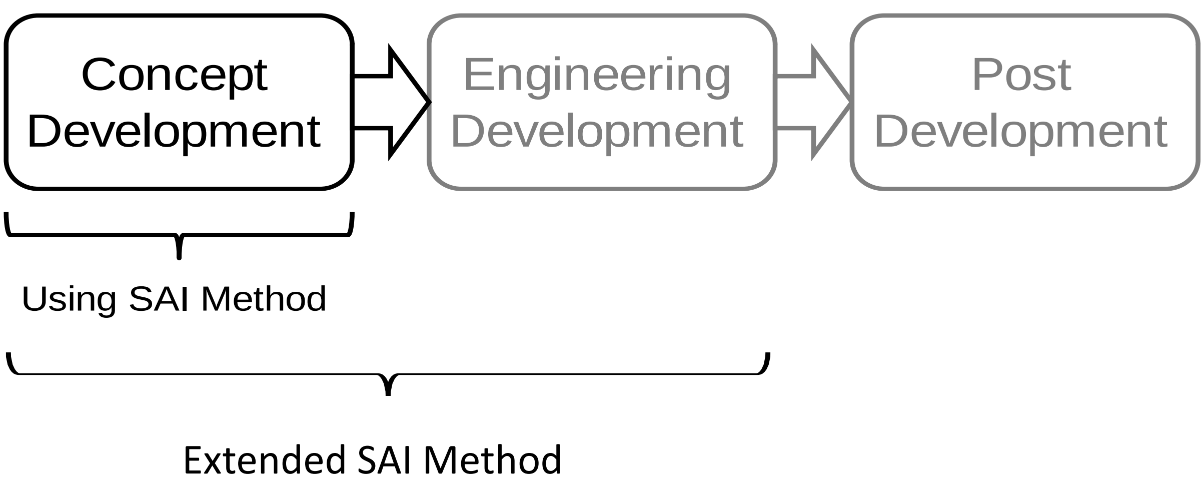

Figure 14. Extended SAI in engineering lifecycle

for system of systems. The extended SAI method is illustrated in Fig. 14. The SAI method covers the concept development and the extended portion covers the engineering development. As a whole the extended SAI method addresses the concept development and the engineering development and it is correspondent to the translation of the system level quality attributes to the subsystem level parameters or the requirements. The advantage of having the translation process correspond to the SAI method is that the powerful SAI techniques become available by having this correspondence. Thus the ility translation process can have the strong foundation and the tools within the SAI method become available for the process. This argument can also be used for correspondence to the traditional systems engineering with similar benefits..

The 12 steps of the extended SAI method in Fig. 15 are elaborated below.

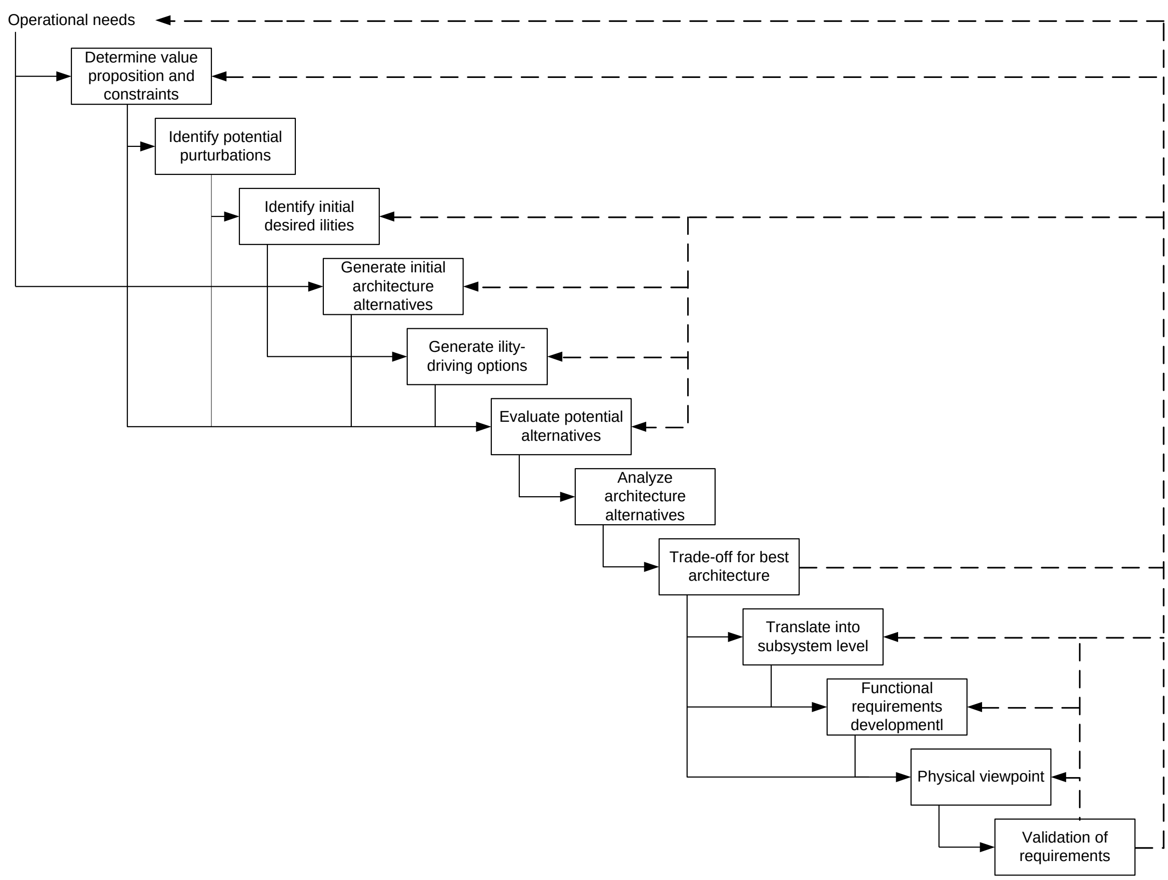

Figure 15. Extended SAI method flow diagram

(1) In this first step, we wish to explore constraints and value proposition: this involves identification, understanding, and capturing of the overall value proposition for the SoS architecture. The interactions with key stakeholders and their needs are identified, and design constraints are also noted.

(2) Potential perturbations are studied and identified: using various techniques, potential perturbations in the context and needs of system that can possibly interfere with SoS value registry are identified and listed.

(3) Initial desired ilities are studied: list ilities that promote the desired long-term behavior of the SoS using a variety of analytical tools (e.g., ilities hierarchies, semantic basis tool, and others). Note information about relevant perturbations can lead to high interest in certain ilities over other ilities.

(4) Initial architecture alternatives are set up: the purpose of this step is to suggest various value-driven architecture for the value proposed in step 1. SoS architecture alternatives in terms of operational and design variables, with associated concepts of operations.

(5) Illity-driving options are produced: this step is concerned with selection and generation of options to include in the initial architecture that will eventually result in enabling desired ilities (identified in step 3). These options form the linkage to the emergence of lifecycle properties over time, because they are the change enablers or resistance to change in the SoS when exogenous perturbations threaten SoS value delivery, or when opportunities to enhance value delivery arise. Options can also be latent in a given architecture.

(6) Potential alternatives are evaluated: a model is built and executed to evaluate different SoS architecture alternatives in terms of various metrics, including performance (i.e. attributes and costs) and illity metrics.

(7) Analyze architecture alternatives: the analysis in this step is aimed at developing insight and understanding in the trade-offs between static value and ility behaviors within various SoS architectures in terms of design and operations choices. Various analytical techniques – such as Multi-Epoch Analysis, Era Analysis, and the Valuation Approach for Strategic Changeability (VASC) – are employed in this step.

(8) Trade-off and select “best” architecture with ilities: in the final step, selection criteria for nominating the “best” architecture with ilities are justified and documented, and ilities requirements are generated.

(9) Translation into subsystem requirements: The system level quality attributes are passed down and translated at the subsystem level and subsystem architecture. This step can proceed linearly or iteratively. In this step, the systems engineers examine the desired ilities at the subsystem level. Several or many ilities may be considered at this step depending on the value register. Thus certain judgment and intimate familiarity of the choices made during previous steps are needed.

(10) Development of functional and logical requirements based on ilities: The subsystem experts convert the passed down ilties into functional and logical requirements.

(11) Physical viewpoint implementation: actual realization of an increment of capabilities.

(12) Validation of achievement of the passed down ility: the subsystem engineers perform requirement analysis and characterization against the physical implementation, which validate the subsystems achieve the requirements from the system level desired ility.

These steps comprise the complete procedure from SoS architecting to translation of ilities to subsystem requirements and provides insight on risk analysis as well.

Table 7. Ilities trade-off for emergency light subsystem

Ility	Value	Lights
Safety	Certification	8 lights
Quality	Customer Need	12 lights
Reliability	Airline Maintenance	No defect, long lasting

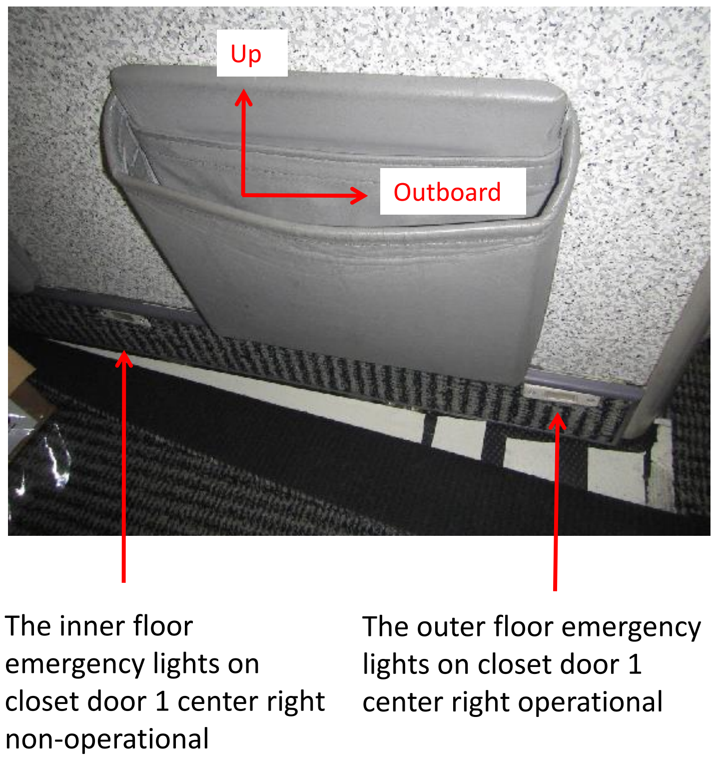

Figure 16. Emergency lights for the galley closet

Table 7 provides an example of identifying desired ilities. We may consider three ilities as following: safety, quality and reliability. FAA might be interested in safety ility for emergency lights on a galley closet. The quality ility may lead to drawing packages of 12 emergency lights as shown in Fig. 16 and Fig. 17. However, the four lights in aft location may not be required for the purpose of safety. It is possible airlines may dispatch aircraft without the aft lights. Also the lights may be analyzed with reliability ility. Thus we could see the roles played by trade-off of several ilities and the summary of ilities trade-off is shown in Table 7.

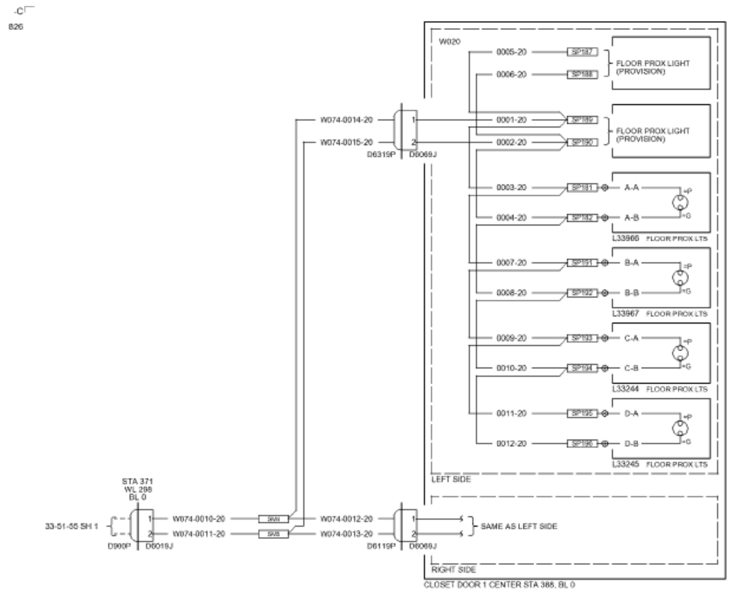

Figure 17. Wiring diagram of emergency floor proximity light system

2.5 Ilities Translation in the Context of Classical Systems Engineering Processes

We note this translation of the system level ilities to subsystem level requirements has strong correlation to traditional systems engineering processes [76]. This is an important point because the similarity allows the tools available in systems engineering to be utilized for the processes of ilities translation. We examine the similarity in detail in this section. Typical systems engineering processes are shown in Fig. 18 and Fig. 19. The flow of rectangular blocks in Fig. 18 indicates the typical systems engineering lifecycle of requirements analysis, functional definition, physical definition, and design validation. In the system development process, this lifecycle is repeatedly used for needs analysis phase, concept exploration phase, concept definition phase, advanced development phase, and engineering design phase during concept development stage as well as engineering development stage. Thus Fig. 18 is the details of the spiral cycle of Fig. 19 and the two figures should be read in tandem.

The systems engineering method is an application of the scientific method in an organized and systematic way to develop and architect complex systems. The flow diagram in Fig. 18 starts with inputs from the previous phase. Predecessor system, functional building blocks, and previous analysis are shown as inputs to the blocks. The inputs to the needs analysis, synthesis of functions

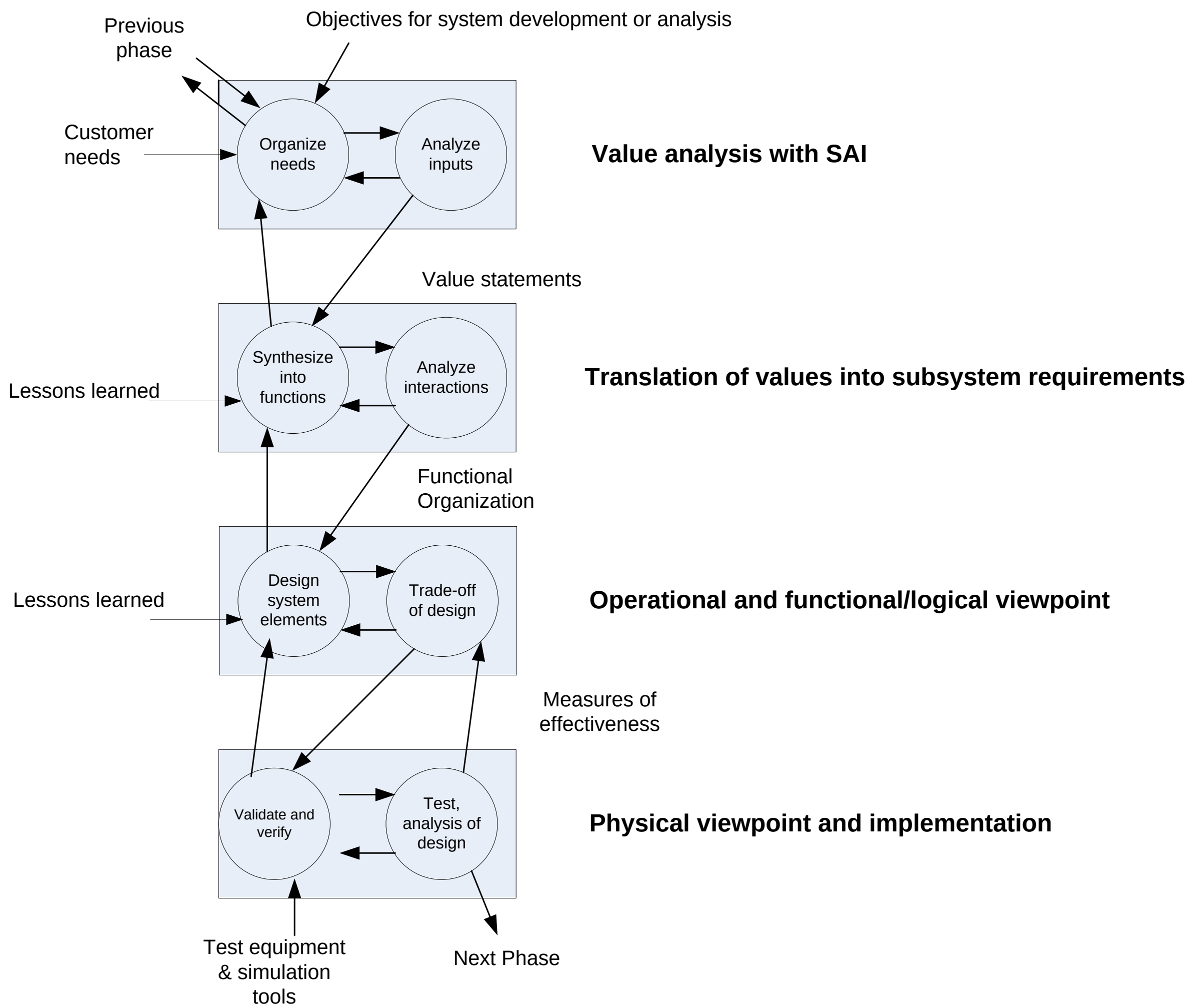

Figure 18. Quality attributes translation within the systems engineering processes

X

Phase Axis

Y

Step Axis	Needs Analysis	Concept Exploration	Concept Definition	Advanced Development	Engineering Design	Integration Evaluation
Rqmts Analysis	Analyze needs	Analyze operational rqmts	Analyze performance rqmts	Analyze functional rqmts	Analyze design rqmts	Analyze rqmts
Functional Definition	Define system functions	Define subsystem functions	Define component functions	Define subcomponent functions	Define part functions	Define functional tests
Physical Definition	Visualize subsystems	Visualize components	Select components	Specify component	Specify subcomponent	Specify test equipment
Design Validation	Validate needs, feasibility	Validate performance rqmts	Validate systems effectiveness	Test critical subsystems	Validate component construction	Test & evaluate system

Figure 19. Axes of abstraction and organization in the systems engineering lifecycle

are indicated. Also shown are inputs from systems engineering methodology such as partitioning criteria, trade-off criteria, measures of effectiveness, and tools and methodologies.

Representations of key processes are shown as circles in side each block. Information flow, feedbacks and iteration are shown with arrows.

The steps 1 to 8 in extended SAI process includes the needs analysis and requirements analysis in the systems engineering method flow diagram. Passing down the ilities and translation of ilities into subsystem requirements are performed during the flow from requirement analysis to functional definition.

Passing down the requirements from subsystem level to component level for steps 9 to 12 corresponds to systems engineering method flow from functional definition to physical definition. During the design validation phase, the component level requirements from ilities translation are validated and verified.

The needs analysis and requirements analysis are necessary to increase the understanding of the problem situation and to scope any expansion or corrections needed. In the initial stage of a system development process, ideas are in flux and many assumptions are made and ilities are the main topic to be discussed. This discussion is important for providing the backdrop for considering operational needs and technological opportunities and to flow the high level requirements from ilities to increasingly specific representations of requirements and system design. Frequently at this stage, the system models, which identifies and describes all design choices, are studied with consideration of ilities.

Functional definition block refers to functional analysis and allocation and is needed to ensure a disciplined approach to an effective configuration of the functions and selection of implementation that best balances the desired characteristics of system such as performance and cost. This block corresponds to translation of the system level architecture into subsystem architecture and the development of functional requirements block. The basic building block is a subsystem that performs a single significant function with single set of signals, data, energy or material. A subsystem is consisted of elements that perform lower level functions which aggregates into a subsystem function. After the component level requirements are implemented, the design validation is performed, which corresponds to validation of designed architecture for the passed down ilities. In development of a complex system, the steps of the design definition may have been accomplished in full compliance with requirements. However, the validation step is still needed for an explicit validation of the design before moving to the next phase. It is our experience that there are too many opportunities for undetected errors without explicit validation, verification and evaluation. Such validation includes modeling of the system environment, and tests and test data analysis.

2.6 Chapter Conclusions

In this chapter we have shown that the non-functional requirements typically manifest as ilties can be and should be translated into functional requirements at the subsystems and components level. In order to achieve this goal, we expanded the SoS architecting with ilities (SAI) method, where steps that aid the concrete and specific engineering development at the subsystem and component level are incorporated. An example of translation of the safety ility into subsystem level parametric development was discussed to demonstrate the value of this approach. Electromagnetic environmental threats and lightning effects in aircraft systems were discussed. The ilities translation process was discussed in the context of architectural hierarchy. Importance of the conceptual system needed for fundamental understanding of architectural processes was emphasized. Ilities translation was discussed from the viewpoint of classical systems engineering processes. Our approach in this paper follows this tradition and translates the ilities research into a dissertation that is congruent with the traditional systems engineering lifecycle of product approach.

3. Risk Analysis Model Development

The risk analysis and mitigation is approached from a project management point of view. We define the risk and risk management project formally in this chapter. The risk is expressed in mathematical terms. Then the charter, scope and methodology of the project are presented [77].

3.1 Mathematical Expression of Risk

Risk is generally related to the probability of a hazardous event and the severity of the event. As such we may express risk as a set of two elements [78]:

$$R_i = \{C_i, p(C_i)\}, \quad i = 1,2,\ldots,N \tag{1}$$

Where:

R_i = Risk of the ith hazardous event,

C_i = Severity of the event (consequence)

$p(C_i)$ = Probability of consequence

i = Event index

N = Maximum number of events

If there are multiple of events to be considered, the final risk is the summation of each risk.

$$R = \sum_{i=1}^{N} C_i, p(C_i), \quad i = 1,2,\ldots,N \tag{2}$$

Consequences are defined as the overall results of a hazardous event. Typically the consequence is expressed by financial loss or impact of the event on the overall functionality of the system under consideration. A typical way to describe this impact in electromagnetic environment is to classify the impact from criticality point of view as follows:

(1) No effect or no consequence (undisturbed)

(2) Interference (limited)

(3) Degradation (severe)

(4) Loss of main function/mission kill (very severe)

(5) Loss of system (catastrophically)

The electromagnetic environment and the effects depend on the parameters of the source, the set up, and the course of action during the event. The event scenario is defined as a set of parameters as follows:

$$S = \{C_s, L_s, D\}. \quad (3)$$

Where:

S = The scenario

C_s = Category of the source

L_s = Location of the electromagnetic source

D = Duration of the scenario

It is customary in the standard risk model to separate the probability of a consequence into the likelihood of the event and the conditional probability of the consequence given the event occurrence as follows:

$$p(C_i) = p(S_k) \cdot p(C_i|S_k). \quad (4)$$

Where:

$p(S_k)$ = Likelihood of the scenario S_k

$p(C_i|S_k)$ = Conditional probability of C_i given S_k

If there are multiple scenarios leading to the same consequence, then (4) may be extended to (5):

$$p(C_i) = \sum_{k=1}^{K} p(S_k) \cdot p(C_i|S_k). \quad (5)$$

It is also noted that As long as risk is related to uncertainty, risk may also be equated to a variance of probability distribution. Our treatment of risk implies risk is logical operation AND of risk event probability and risk consequence scale. In some literature it is expressed as logical operation OR. Generally AND gate is used and that is the convention we adopt in our work.

3.2 Charter and Scope of Risk Management Project

3.2.1 Charter of the project

For our project, the charter would be to investigate the risk management of electromagnetic environmental threats to aircraft with an integrated approach based on the long history of safety study of aircraft by employing the latest systems engineering methodology. This research task is urgent and strongly motivated by the fact that the electromagnetic environmental effects on aircraft have been exacerbated in recent years due to modern aircraft's increasing dependence on electronic devices for communication, navigation and flight control, and growing use of composite materials for airframes. The approach includes the management approach and technical approach, and the constraints include time constraints, budget constraints, and safety regulations.

3.2.2 Scope of the project

The scope of the project includes overview and purpose being the innovative method and techniques for system level risk management of electromagnetic environmental threats to aircraft and the following items:

- Methodology of Risk Mitigation technique
- Concrete examples of how the risks are mitigated in the area of electromagnetic threats and lightning threats
- Test procedures for the technology and methodology
- Test results for the validation of the approach

Table 8. Principles used for risk analysis

Principle	Utility for this work	Note
Emergence	Risk characterization	Risk considered as emergent property
Holism	System perspective	Electromagnetic issues are at systems level
Dualism	Information domain and physical domain	Risk mitigation information should be represented by physical form
Focus	Identify high risk events	Focus on high criticality or expected loss
Coherence	Criteria of validation and verification	Testing, analysis, or simulation to check coherence
Dualism of F/R	Understanding nature of risk	Function and risk on equal footing

- Analysis tools such as computerized fault tree analysis which demonstrates the innovative technology
- A final report that summarizes the details of the risk mitigation technology

The principles in Table 8 may be used in risk study. The project scope also covers the schedule, milestones, project approach, and management of issues, changes, communication, procurement, resource, outstanding issues, approvals, deliverables, quality objectives, and quality control activities. Although not all of these items are applicable to the current project, it is important to understand all aspects of project management since engineering projects typically emerges in response to customer needs and management is essential part of the engineering projects. These principles are selected from the system architecture principles discussed in Chapter 1. These principles are adapted for electromagnetic risk analysis which is discussed in the next chapter. The principle of emergence is used for affirmation that risk has the ontological basis by being degradation of emergent behavior. The principle of holism is especially adequate for E^3 risk analysis due to its global nature. The principle of dualism lets us be attentive to the relation between conceptual analysis and physical phenomenon. The principles of focus and .coherence are used for conducting the work for risk mitigation.

3.3 Identification of Risks

In Figure 20 below, risk management steps are shown. The first step is the identification of risks. A list of possible on the register are noted and analyzed [79]. The requirements and scope for the project are listed and if these change, opportunity may increase. Deliverables and activities in the work breakdown structure (WBS) may be analyzed for potential risks so that comprehensive risk analysis can be performed. Project resources may also be analyzed. Other areas that could be analyzed include cost, availability, delivery, quality, and expertise for risk identification.

Costs and budgets deserve attention for potential risks to add to risk register. The risk level requirements or quality procedures from the sponsor or organization provide opportunities for

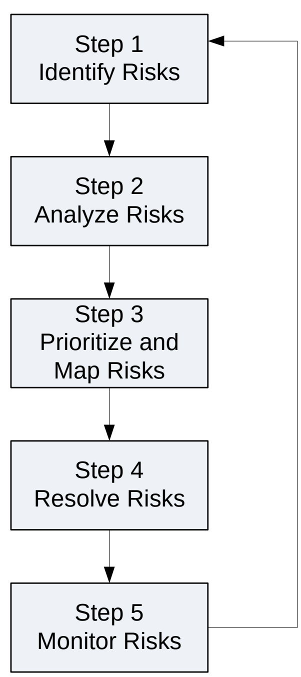

Figure 20. Risk management process

identifying potential risks. Communications planning, procurement and managing of project including cost, duration and resources also need to be analyzed.

3.4 Qualitative Risk Analysis

Qualitative risk analysis is performed after the identification of the risks. This activity includes assessment of the probability and impact of each risk on the risk register list. As discussed in the previous section, risk probability contains the element of likelihood of the event and the element of consequences to the project in terms of cost or time. This process could be subjective but one has to do the best one can to attach certain numbers to the likelihood and the consequences. The qualitative criticality can be assessed based on Table 9.

The likelihood and consequence of each risk may be determined through discussions by the stakeholders and unbiased subject matter experts or risk analysts. Then, a risk score is calculated by multiplying the likelihood by the consequences to derive a risk score. Then the ranking can be derived from the risk scores. Modern risk management science does not always treat the risks negatively. Some of the risks may be treated as opportunities and so certain discretion is required. Then the goal is to maximize the opportunities or the positive risks and minimize the threats or the negative risks. After the risk analysis has been completed, we give attention to the risks in the upper portions of the risk list. Risk management planning includes determination of the threshold above which one has to manage the risks.

Table 9. Risk event criticality level

Criticality (Total Loss) Level	**Description**
1	No effect or no consequence (undisturbed)
2	Interference (limited)
3	Degradation (severe)
4	Loss of main function/mission kill (very severe)
5	Loss of system (catastrophically)

3.5 Quantitative analysis

This step requires special attention since it is difficult to perform quantitative analysis. One wishes to determine the expected loss of each high-priority risk. From this analysis, we can anticipate the cost of the risk in terms of lost or saved time or money. We usually perform quantitative risk analysis on the risks which are located above the threshold on the risk list. We engage subject matter experts to perform this quantitative analysis. For the expected loss, use the formula listed below.

$$Expected\ loss = Likelihood\ \times Total\ Loss$$

The value of the total loss is what is expected for the loss, or gain if a particular risk event occurs. The probability is the likelihood for the event to occur and risk assessment is conducted as shown in Fig. 21.

Expected loss may be added to contingency reserve. By doing similar calculations for each high-priority risk, we can estimate the amount of money to be considered for the contingency

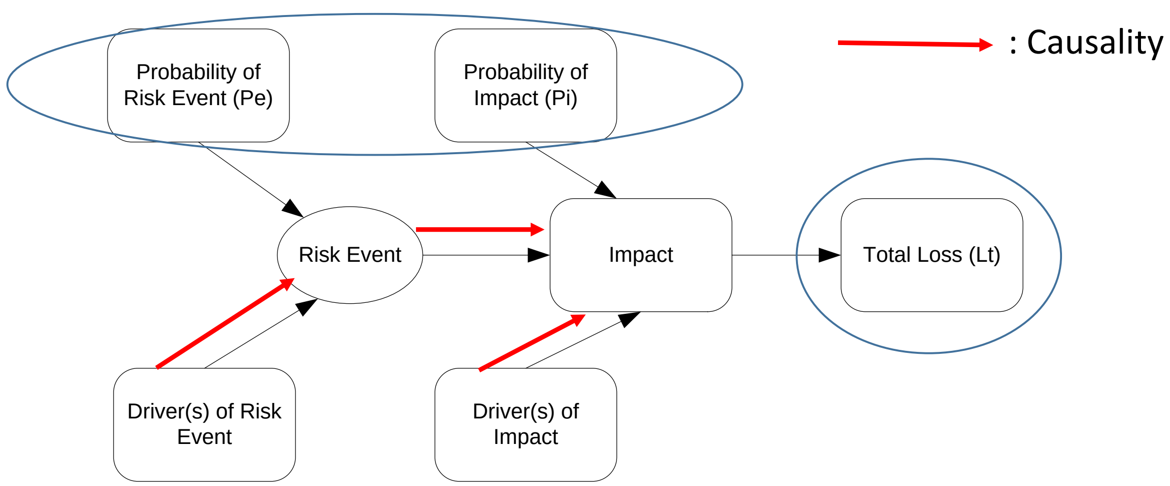

Figure 21. Standard risk model with causality paths specified

reserve. Similar calculations work for time, allowing one to add contingencies to the schedule. Other techniques for quantitative risk analysis include using Monte Carlo analysis, standard deviations or distribution charts. Resorting the list may be conducted for the expected loss

3.6 Risk Mitigation

Following the approach planning for handling risk, potential risks identification, and performed qualitative and quantitative risk analysis performance, one devise a method for risk management, one plans for risk evaluation for each of these top ranked risks as shown in Fig. 22 and the risk resolution steps are shown in Fig. 23. The two figures are showing the same steps but the focus for each diagram is different. The first step is to evaluate the risk, which means the probability of the events and probability of the impacts should be calculated or estimated. The risk mitigation is to resolving the risk with prevention of risk event or planning contingency plans for the impact. In other words the risks are resolved actively with scientific methods. The four general strategies in PMBOK® are shown in Table 10:

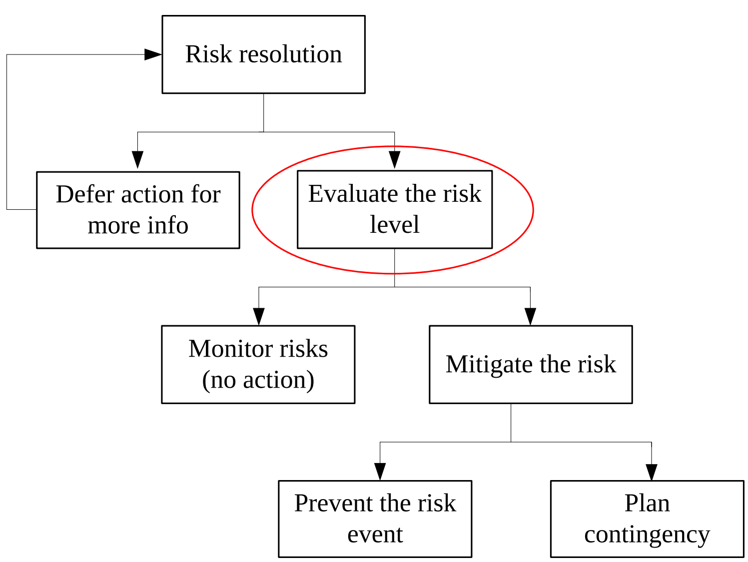

Figure 22. Risk resolution flow diagram for risk level evaluation

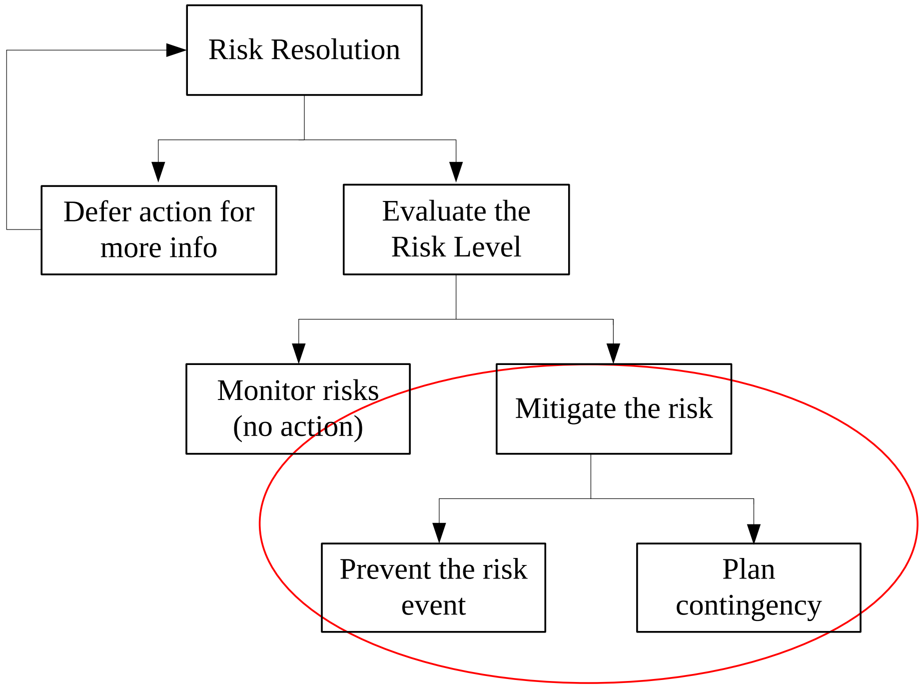

Figure 23. Risk resolution flow diagram for risk mitigation

Table 10. Risk resolution strategy for negative and positive risks (PMBOK®)

Negative Risks	**Positive Risks**
Avoid	Exploit
Transfer	Share
Mitigate	Enhance
Accept	Accept

The strategy depends, in part, upon organization's culture. Risk resolution strategies include the expected loss of the risk, subject matter experts' opinions and the timing of the potential risk. The chosen strategy help determine the specific mitigation plan for each of the top-ranked risks. It is important to have a contingency plan (plan A) and a fallback plan (plan B) for the highest ranked risks. Budget and schedule should be considered for the mitigation activities. It is important to know the time when the risk might happen and to have the responsible personnel for the risks.

Based on these risk analysis discussions, the overall flow diagrams are developed. The flow diagram in Fig. 24 shows that the work starts when there are customer requests or challenges that need to be addressed. This is similar to the customer needs in systems engineering

The requests or needs are examined against the backdrop of understanding of the nature of the risks, systems architecture, risk analysis, or the electromagnetic coupling diagrams. Then the problem is sent over to the standard risk model. This is shown in Fig. 25, where the standard risk model is elaborated. When the standard risk model is carefully analyzed, we obtain the following insights:

(1) The standard risk model shows the causality relation between event drivers and event, impact drivers and impact, and the event and the impact,

(2) The standard risk model shows the event may occur at a system level or at a component level, but the impact generally occurs at a system level.

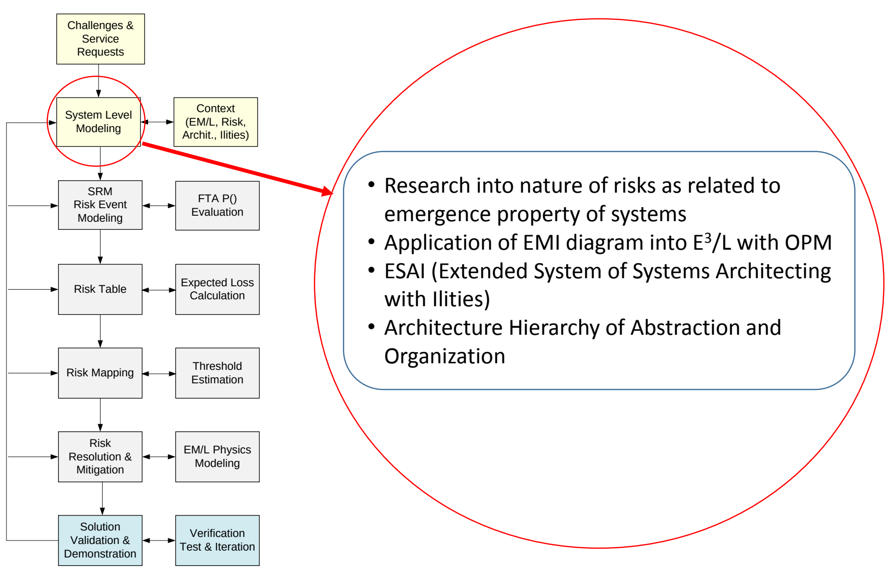

Figure 24. Outline of overall risk analysis flow with details of context block shown

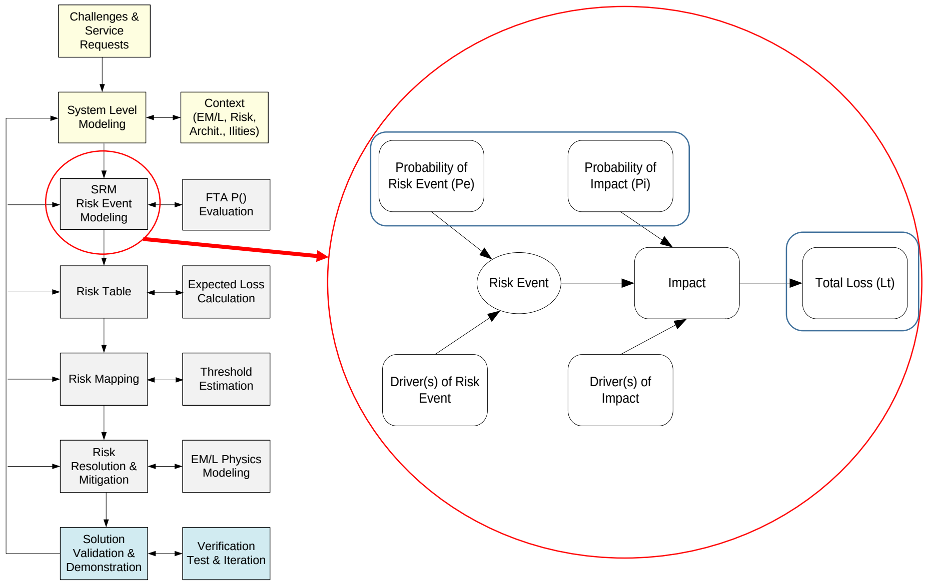

Figure 25. Outline of overall risk analysis flow with details of risk event modeling shown

(3) The standard risk model shows the risk event prevention is possible by examining the event drivers. Likewise, the impact contingency is possible by carefully examining the impact drivers. This process is similar to the root cause analysis and the corrective action activity.

(4) The standard risk model shows two factors are needed for risk analysis: likelihood and total loss. Likelihood represents the total probability of the event and the total loss represents the criticality of the event.

Once these insights were obtained by examining the standard risk model, they led to the development of the risk analysis and mitigation methodology in Fig. 24 and Fig. 25. In other words, when the implication within the standard risk model was unfolded, the meaning became manifest as the risk analysis and mitigation flow diagram. Thus this is an example of how a model leads to another model. As the challenges or the customer requests are understood in the context of architecture, systems engineering, and risk analysis, the problem is given to and analyzed by the standard risk model. It is noted the principles of holism, focus, and dualism in discussed in Chapter 1 are employed at this stage.

3.7 Monitoring and Controlling Risks

In order to deal with many changes such as scope, cost, and time, resources, management, project teams, one monitors and controls the risks. There is correlation between the monitoring and controlling processes since as changes occur to the project, changes occur to the risks. Changes may add additional risks. Monitoring and controlling involve tracking the risks, evaluating the effect of the implemented risk mitigations, identifying new risks, and changing the rankings as needed. Monitoring and controlling risk includes reserve analysis for the amount of time and money, and comparing them to the remaining risks.

3.8 Risk Management Process Documents

The risk management processes call for excellent documentation. For example, documents such as technical documents, assumptions log updates, and recommended corrective and preventative actions are to be written and preserved. Also the project management plan requires the documents shown in Table 11 below:

Table 11. Documents for project management plan

Project management plan document	Need for the document
Product quality management plan	Standards for the product quality
Expenses management plan	Expenses for the project managed
Scheduling management plan	Time aspect of the project
Team staffing management plan	Member recruitment and organization
Supplier management plan	Supplier and procurement management
Work breakdown structure plan	Structure of work activities organized
Baseline plan for schedule and expense	Baseline requirements to establish

The project management processes requires that changes for one aspect affect other components of the project. Changes in certain risks may affect other risks as well. Thus risk monitoring is an important aspect of risk management. Documenting plays a critical part in managing the changes in risk levels.

3.9 Chapter Conclusions

We have defined the risk in mathematical terms in this chapter. Risks were discussed from the project management point of view. Systems engineering approach means dealing with all aspects of risk management. It is critical to understand risk management requires integrated systems approach. By going through the risk analysis steps from identification of risks, the risk analysis, prioritization and mapping of risks, resolving the risks, and finally, monitoring of risks, risk analysis modeling flow diagram emerged. This flow diagram is the result of having insights from the standard risk model. Thus this is an example of one model being unfolded from internal structure enfolded in another model. The implication was in the standard risk model and that implication was unfolded into the risk modeling flow diagram. Another way of describing this is that the new flow diagram emerged from the standard risk model. Emergence and unfolding are two aspects of the same phenomenon.

4. Risk Analysis of Electromagnetic Environmental Effects in Aircraft

Risk Analysis of electromagnetic environmental effects in aircraft systems is performed in this chapter. The system level consideration of electromagnetic environmental effects (E^3) in aircraft is one of the major concerns to aviation industry. Discussion of hazardous electromagnetic environmental effects in aircraft systems includes lightning, high intensity radiated fields (HIRF), precipitation-static (P-static), portable electronic devices (PEDs), and electromagnetic compatibility (EMC) issues, and canonical structure of electromagnetic energy coupling shown in Fig. 26 is developed in this chapter for discussions. This model is based on the three-component modeling in EMC discipline [80], but the actual modeling is accomplished by using Object Process Methodology (OPM) modeling language. The electromagnetic environmental effects on aircraft have been exacerbated in recent years due to modern aircraft's increasing dependence on electronic devices for communication, navigation and flight control, and growing use of composite materials for airframe. In this chapter, we review electromagnetic environmental effects in aircraft from a systems engineering perspective. Considering the complex, interrelated, and dynamic nature of electromagnetic phenomenon in aircraft, we find the systems engineering application to electromagnetic effects discussion appropriate and beneficial. In particular, we judge that risk

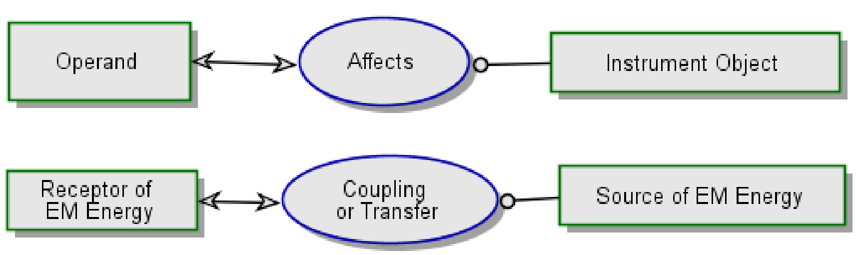

Figure 26. Basic electromagnetic energy coupling diagram with OPM

analysis methodology is an underutilized but well-suited tool for understanding and mitigation of electromagnetic hazardous effects in aircraft systems.

Herein we first introduce the Standard Risk Model (SRM), and then apply the model to electromagnetic risk events and impacts, and follow through with illustrative prioritized identifications. We next develop drivers for each risk event and impact, and finally we present the baseline risk prevention plans and associated impact contingency plans. We conclude with a summary of our findings and present future work suggestions for systems engineering application to aircraft electromagnetic environmental study and mitigation of the hazardous effects.

4.1 Introduction

The electromagnetic (EM) environmental effects in aircraft systems have been of continuing concern to aviation industry since radios were first installed on aircraft in the 1920s. The EM energy coupling diagram is shown in Fig. 26, where the EM problem situation is parsed into three fundamental components: EM energy source, transfer path, and receptor [81]. The first component in this diagram, the source of EM energy, encompasses a variety of natural and man-made environmental sources. Typical EM energy sources for aircraft include lightning stroke attachment, high intensity radiated fields (HIRF) from airport radars and broadcast transmitters, portable electronic devices (PEDs), precipitation static (P-static), and emissions from equipment within the aircraft as illustrated in the E^3 context diagram of Fig.27. The mathematics for EM energy coupling is readily available in public literature [82]. For electromagnetic interference (EMI) and electromagnetic compatibility (EMC) considerations, the general convention is that both the source and receptor are located within the aircraft. However, some authors include lightning and HIRF in the broad category of EMC discussion [83]. We consider it is a matter of personal preference. The EM sources for modern aircraft have become progressively more severe

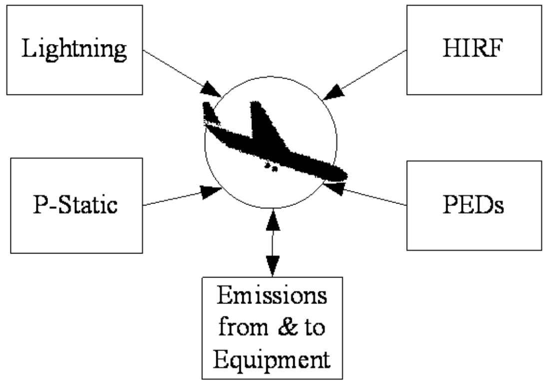

Figure 27. Aircraft electromagnetic effect context diagram

in recent years. Although the natural environment of lightning and P-static has not changed, the man-made EM environment in aircraft has changed for the worse with the introduction of new PEDs such as mobile phones, email, web browsing, text messaging, and mobile audio/video services since the early 1990s [84,85]. This PEDs energy coupling is modeled in Fig. 28 showing some details. The transmitting power of HIRF sources such as airport radars and radio transmitters has been increasing. The second component in Fig. 26, the transfer path of EM energy, has also been changing for the worse due to growing application of composite materials in airframe, which

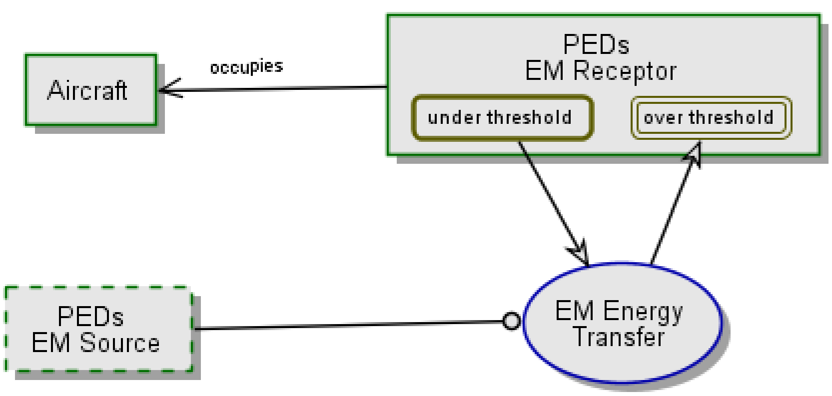

Figure 28. Portable electronic device energy coupling diagram with OPM modeling. PEDs EM sources are part of the environment with dotted lines

Figure 29. EMI energy coupling diagram with OPM modeling. Note the crosstalk emitter is part of the system with solid lines

Figure 30. Lightning energy coupling diagram with OPM modeling. Note the lightning source is part of environment with dotted lines

Figure 31. HIRF energy coupling diagram with OPM modeling. HIRF energy source is part of the environment with dotted lines

are relatively transparent to EM energy transmission and provides less protection to aircraft [86]. The ever-increasing density of electronics in modern aircraft makes the third component in the Fig. 26 diagram, the receptor, more susceptible to EM energy. Coupling diagrams for other E^3 threats are shown in Figures 28, 29, 30, and 31. These are modeled with OPM as shown in Fig. 32. Modeling of EM energy coupling is important since the communication, navigation and surveillance (CNS) functions and flight control functions (fly-by-wire) in modern aircraft are performed entirely by electronics [87], increasing their vulnerability to EM energy.

The phenomenon of EM effects in aircraft is complex, interrelated, dynamic, and open, which means EM problems are best addressed by systems approach [88,89]. The EM effects are complex because aircraft structure represents complicated EM boundary conditions; are

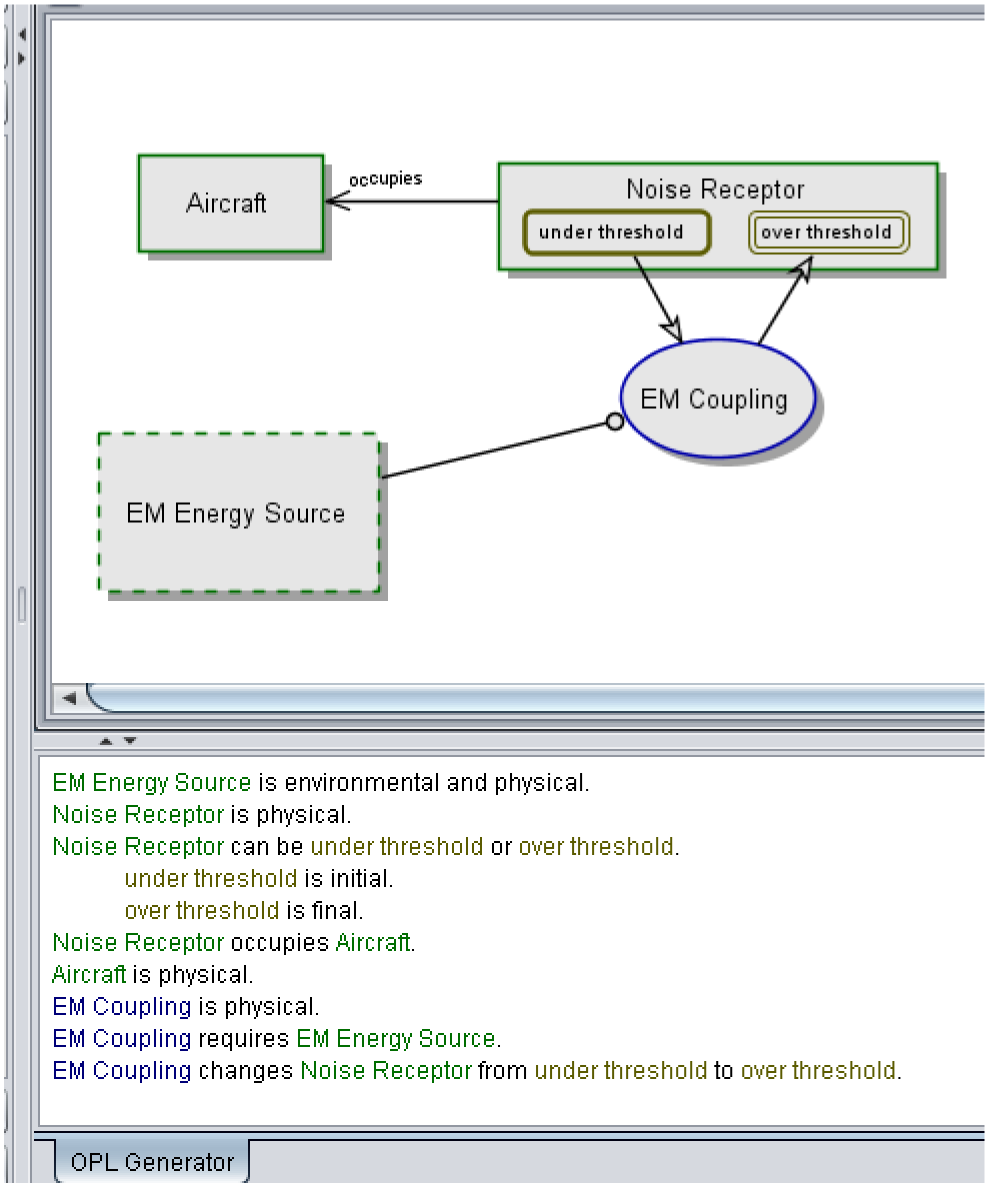

Figure 32. Modeling of EM energy source coupling to receptor with OPM in OPCAT suite

interrelated because of intricate mutual dependency among electric field, magnetic field and electric current; are dynamic because of time dependency of governing Maxwell's equations; and are open because the aircraft is an open system with its electromagnetic environment. This complexity of EM environment was illustrated in Fig. 27 with at least five EM threats to aircraft. EM effects in aircraft fit the definition of system, and research of EM issues using system concept

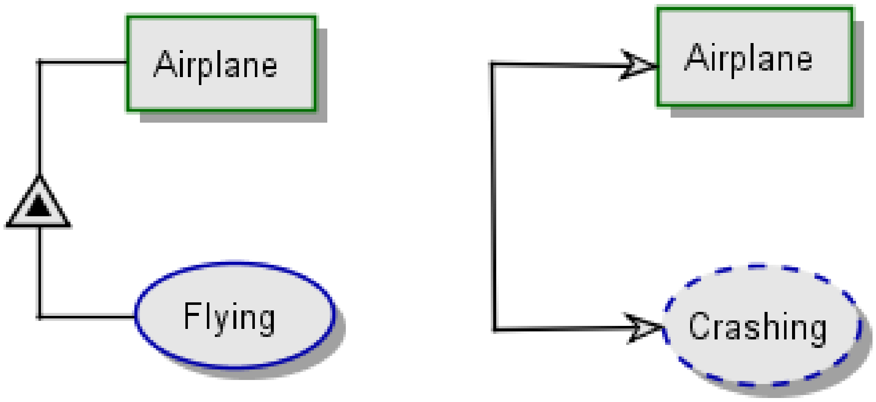

Figure 33. Modeling of emergent properties of flying (Left) and crashing (Right) with OPM

is appropriate and beneficial. Risk analysis is a discipline formally recognized in systems engineering standards [90]. Risk analysis and management is one of the essential tasks of systems engineering, which requires a broad knowledge of the system and its critical elements as a whole. Risk can be viewed as degradation in emergence of systems. The electromagnetic risks occur at a system or at a subsystem level. Risks are either absence or degradation of emergent functionality such as function, performance, or ilities. Risk may also be viewed as an undesirable emergent property. For the emergence at the subsystem level, risks also emerge at the subsystem level. For the function at the component level, risk may occur at the component level. However this risk at the component level is different than the one for the system level. In summary, risks may occur at all levels just like functions may operate at all levels. In particular, systems engineering is crucial to the decision of how to achieve the best balance in risk management [91]. Risk modeling is illustrated in Fig. 33. Desirable flying function which is a designed functionality is shown on the left side in Fig. 33. Undesirable and unanticipated occurrence of crashing is shown on the right side in Fig. 33. The potential of this occurrence was there before the crashing, which represents risk as an emergent property of a system. This risk should be identified and managed by risk analysis modeling and processes. Table 12 lists some of the desirable emergent properties and undesirable properties of aircraft.

Risk analysis is essential when we deal with safety or threat issues of any system. EM threat in aircraft is a safety issue regulated by governmental agencies such as Federal Aviation Administration (FAA), or European Aviation Safety Agency (EASA). The governing FAA regulations of EMC are 14 CFR Part 25.1353(a) and 25.1431(c), which state that any electrical interference likely to be present in the airplane must not result in hazardous effects on the airplane or its systems.

In public literature, EM risk analysis has been conducted quite extensively. It has been applied to electronic systems [92,93,94,95], high power electromagnetics [96], medical systems [97], and space systems [98]. However, these papers do not utilize the Standard Risk Model. Also

Table 12. Emergent properties of aircraft

Emergent property	**Note**
Transportation of passengers and crew (emergent feature)	Emergent feature
Flight performance	Part of functionality
Stability and control	Performance emergence
Cost	Economic emergence
Aerodynamics	Function emergence
Ilities (Safety, reliability, maintainability)	Emergence over lifecycle
Anomalies or accidents	Undesirable unanticipated
Volume	Emergent feature

they do not emphasize the need for systems engineering perspective. We intend to fill this gap in this paper and develop system level EM risk analysis in aircraft.

We first discuss the system concept with respect to the aircraft EM concerns in Section 4.2. Next, we describe the Standard Risk Modeling process [99] in Section 4.3 and identify the risk events, impacts, and drivers of EM effects in aircraft in Section 4.4. Then we discuss the EM risk mitigation in aircraft by developing risk monitoring plans with a risk map, risk as well as the event prevention and impact contingency plans. We conclude with a summary and future work suggestions.

4.2 Applicability of System Concept

The meaning of "system" is broad and diverse. Blanchard and Fabrycky defines system as an assemblage or combination of functionally related elements or parts forming a unitary whole [100]. In Systems Engineering, a system refers to a complex engineered entity that requires combined inputs of specialists representing a wide variety of engineering and related disciplines, of which power system of Fig. 34 is one example. Against the backdrop of this discussion, we may

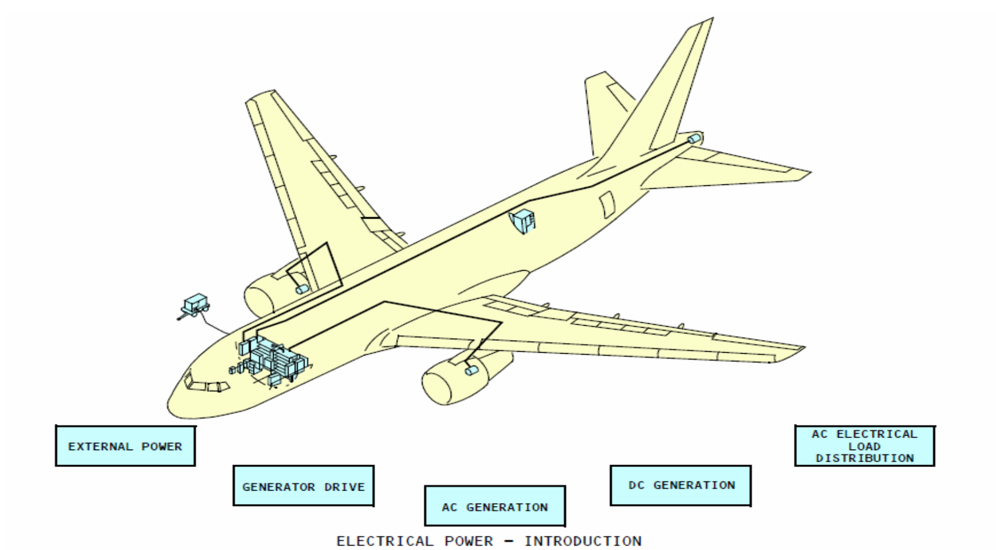

Figure 34. Airplane power system

consider all of the subtle, complex, integrated electromagnetic interactions in and around aircraft as a whole, a system. This electromagnetic system is the subject of our discussion. We note that a systems approach involves "perspective" of how one sees the entity. Aircraft may be viewed from various perspectives such as aerodynamic, propulsion, structure, or electromagnetic [101]. In our case, EM system is an aspect of an aircraft which includes any subsystem and components which interact with EM energy emanating from outside and within aircraft [102].

Since the risk analysis is performed at the system level, it is necessary to review the aircraft subsystems that are relevant to this risk analysis work. In particular the power subsystem in Fig. 34 and the power distribution system in Fig. 35 are important since they often become the source of electromagnetic interference.

For in-flight operations, power comes from an integrated drive generator (IDG) on each engine or from the APU generator as shown in Fig. 34. A hydraulic motor generator (HMG) system operates as a back-up source if there is a loss of all main electrical power. The HMG does not have a time limit for operation [103].

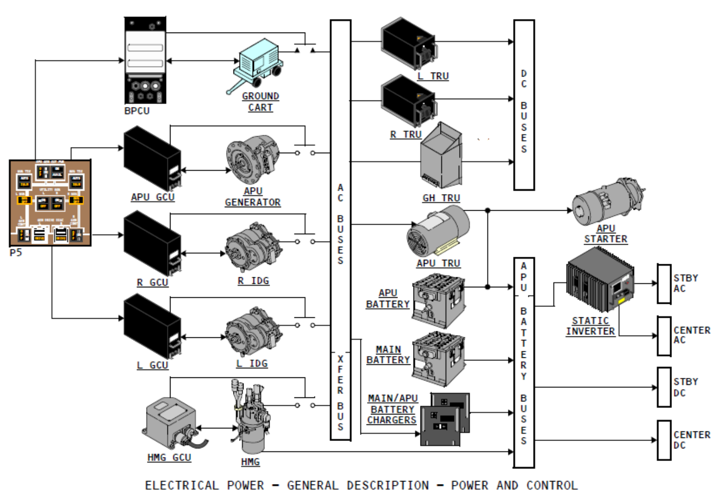

Figure 35. Airplane power distribution system

Electrical power comes through the ac and dc distribution systems as in Fig. 35. The ac distribution system has these buses: The IDG connects to its bus through the closed generator circuit breaker (GCB). The power output of the APU generator or external power cart can also connect to the ac buses through the closed auxiliary power breaker (APB) or external power contactor (EPC). The operation of the related bus tie breaker (BTB) prevents parallel operation of the IDGs or two sources on the main buses. The ground service bus gets power from the right main ac bus when the right bus has power. If the right bus is off, the ground service bus can get power from external power or the APU generator when you push the ground service switch. If external and APU power are available, external power supplies power to the bus.

There are two transfer buses, the captain and the first officer. The captain transfer bus usually gets power from the left ac bus. If the left ac bus does not have power, the instrument transfer bus gets power from the right ac bus. The first officer transfer bus usually gets power from the right ac bus but changes to the left ac bus if there is a loss of right ac bus power.

The left and right transfer buses usually get power from their main bus. The transfer buses get power from the hydraulic motor generator (HMG) if the two main ac buses have a power loss in flight or during a maintenance test of the HMG. The center ac bus receives power from the left main bus. During autoland operations the center ac bus receives power from the static inverter. During autoland the static inverter receives power from the hot battery bus. This bus isolation makes sure the autopilots are on three isolated ac sources. The standby ac bus gets power from the left transfer bus but changes to the static inverter when these are all true: Two utility buses get power from their main ac bus through a utility bus relay (UBR). If the electrical load is more than the generation capacity, the UBRs open and remove utility loads from the generators. Next we would like introduce a standard risk analysis modeling for electromagnetic environmental effects.

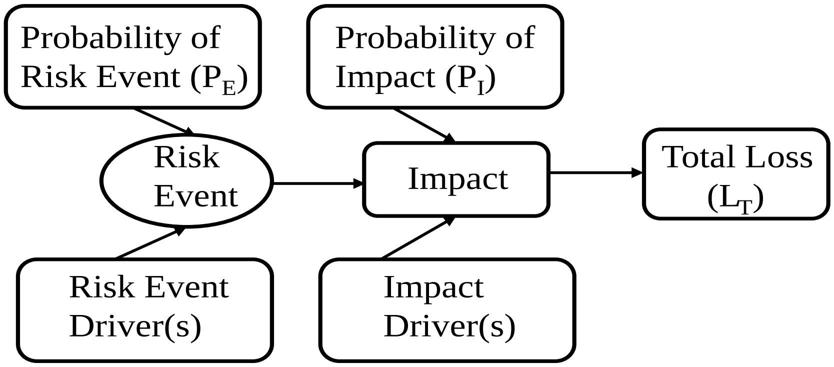

Figure 36. Standard risk model to be used for electromagnetic effects analysis

4.3 Standard Risk Model for E[3]

Risk is defined as the potential that something will go wrong as a result of an event or a series of events. [104]. We find the standard risk model (SRM) illustrated in Fig. 36 to be the one most helpful to understand risks and to develop mitigation methods of risks. The standard risk model in Fig. 36 in EM situation has several components [105]:

(1) Risk event: The happening or state that "triggers" a loss in safety or economic value. The risk events may be specific and concrete EM hazards or incidents.

(2) Risk event driver: Something existing in the event environment that leads one to believe that a particular risk event such as EM incident could occur.

(3) Impact of a risk: The consequence or potential loss that might result if a risk event occurs. In a complicated situation such as an EM problem situation, the impact may not be a simple consequence, but impact itself may have system-subsystem-component structure.

(4) Impact driver: Something existing in the problem situation that leads one to believe that a particular impact such as system level EM damage or upset could occur.

(5) Total loss: The magnitude of the actual loss value accrued when a risk event occurs; it could be measured in days or money, but in complex situations, level of safety or function

criticality must be considered, preventing simplistic monetary value representation. In other words, it may be qualitative rather than quantitative and can be evaluated by levels of criticality.

(6) Probability values: Probability values are assigned to EM risk events and impacts.

The Standard Risk Model is selected for the aircraft EM risk analysis because of the following advantages of the model:

(1) The Standard Risk Model is fairly simple to understand and captures the essence of resolving risks.

(2) It clearly separates risk events and their impact, thus, supporting cause and effect analysis.

(3) Separating risk and impact reinforces the notion of prevention or contingency planning for risks. The Standard Risk Model is supported by ISO 31000:2009 and it may be applied to any industry "regardless of its size, activity or sector" [106].

(4) By allocating the drivers related to a risk event, we can identify the threats and deal with those that contribute the most to risk events.

Because this is a standard model widely used internationally, it will be easier to compare the risks against known risks in other similar projects. This allows us to address similar risks with less resources, helps prioritize risks, and focuses us on unresolved risks. The risks are evaluated by computing expected loss, which is the average (mean) loss associated with a risk. Expected loss is

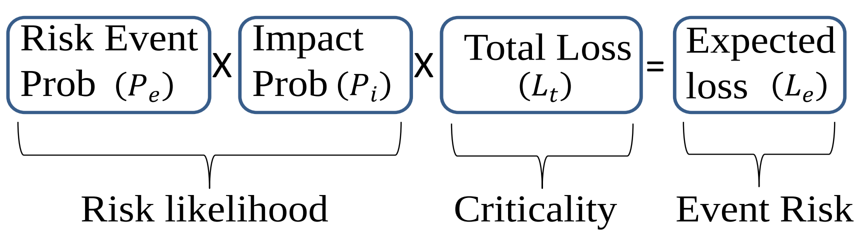

Figure 37. Expected loss calculation

calculated by multiplying the probabilities of risk event, probabilities of impact, and total loss as shown in Fig. 37. The significance of this diagram goes beyond simplistic quantification of risks and consequent losses. The essential insight in Fig. 37 is to recognize two important concepts in risk discussions: how likely is the risk (likelihood)? How critical is the consequence of the risk event (criticality)? We note these two concepts are common factors in most failure analysis or risk analysis methods.

The standard model process starts with risk identification, then proceeds to probability calculation of risks, prioritization of the risks, and resolution of risks. Lastly, the risk is continually monitored.

4.4 Electromagnetic Risk Events, Impacts and Drivers

In this Section, we identify electromagnetic risk events and their impacts in aircraft according to the Standard Risk Model.

Figure 38. Direct lightning effect due to swept strokes on aircraft

4.4.1 Risk Event Identification in Aircraft Electromagnetic Environment

We identified seven main risk event categories related to electromagnetic environment in aircraft as follows by carefully analyzing the electromagnetic threat situation:

(1) Direct lightning strike represents several risk events: (1.a) fuel tank explosion, (1.b) rudder conductive frame damage, (1.c) fasteners damage, (1.d) damage to bonding jumpers of main wing flight control surface or doors, (1.e) engine damage, (1.f) antenna damage, and (1.g) radome puncture. The direct lightning effect is illustrated in Fig. 38, where swept stroke attachment is shown. The lightning attachment was stationary but the aircraft continued moving forward, which resulted in sweeping of the lightning energy over the aircraft surface.

(2) Indirect lightning events occur when the lightning current on the aircraft surface generates magnetic fields which induce voltage on the wire bundles. The equipment these wires are connected to experience upsets or damages.

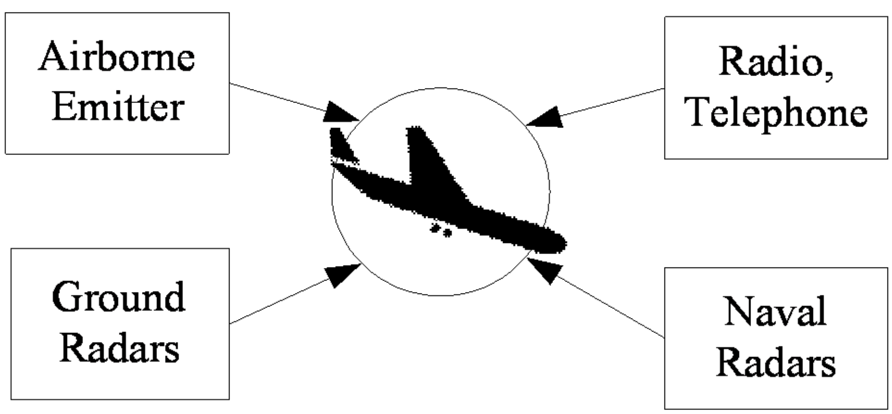

Figure 39. HIRF effect in aircraft context diagram

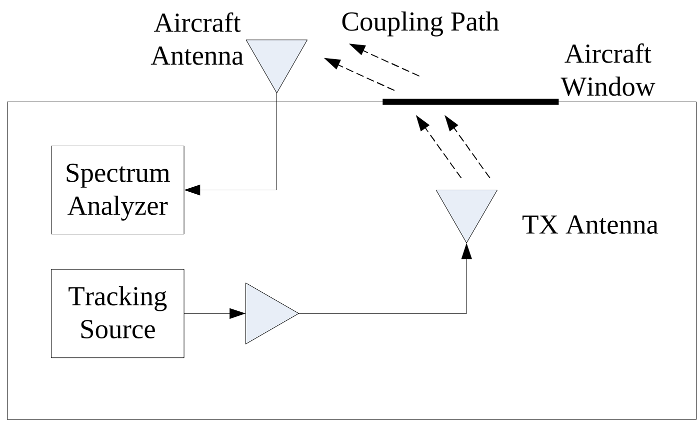

Figure 40. PEDs front door coupling

(3) HIRF events couple the energy from airport radars and radio transmitters to the wires located in un-pressurized area of aircraft. Fig. 39 shows the HIRF sources for aircraft.

(4) PEDs front door risk events represent EM energy coupling via aircraft antennas: The PEDs front door coupling measurement through windows is illustrated in Fig. 40.

(5) PEDs back door risk events occur due to EM energy back door coupling from PEDs emissions to aircraft wires as illustrated in Fig. 41.

(6) P-static risk events which affect radio communication and navi29ation of aircraft.

(7) Equipment to equipment interference events occurs when emitted EM emission energy is coupled to another equipment via wires or antennas.

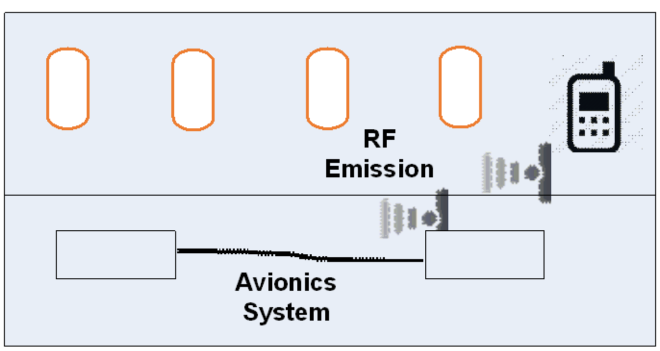

Figure 41. PEDs back door coupling

4.4.2 Drivers for Risk Events

Drivers for the seven risk events are identified as follows:

(1) Drivers for direct lightning risk events are: (1.a.1) flammable vapor in fuel tank, (1.a.2) triggering sparks from lightning stroke attachment around fuel tank, (1.a.3) vapor temperature, (b) to (g): improper grounding, damaged or missing bonding jumpers, corrosion which impedes lightning current flow, and conductive frame damage due to erosion by water ingress.

(2) Drivers for Indirect lightning events are: lack or inadequate grounding of equipment, corrosion of wire bundle over-braid and connectors due to water ingress, hydraulic fluid or airport de-icing fluid ingress.

(3) Drivers for HIRF energy coupling to equipment via wires in un-pressurized area of aircraft are: high impedance on connectors or over-braid of wire bundles. Corrosion and wire bundle defects are the major factors.

(4) Drivers for PEDs front door coupling risk events: unsatisfactory interference path loss (IPL) performance.

(5) Drivers for PEDS back door coupling risk events: close proximity of PEDs to wires, high susceptibility of equipment, and high level emission of PEDs.

(6) Drivers for P-static risk events: damaged or lack of static dischargers, inadequate anti-static paints

(7) Drivers for equipment to equipment: inadequate separation distance between power wires and sensor wires, inadequate isolation between antennas in terms of frequency, angle, polarization, and distance.

4.4.3 Impact Identification in Aircraft Electromagnetic Environment

We identify the impacts of these risk events as a next step. The risk events are specific and may be defined at the component level, whereas the impacts of risk events may have system level implication and, for the most part, are multi-leveled, meaning impacts occur at the system level as well as at the component level. This multi-level nature of impact may be cogently understood in terms of hierarchy discussion in the Systems Engineering discipline. Academic discourse of this subject has been well developed within the context of organizational hierarchy using axis of organization taxonomy concept in model-based systems engineering [107].

Impacts of direct lightning risk events are the total loss (fuel tank ignition), compromised flight controls due to damaged bonding jumpers at the rudder, or flight control surfaces, weakened structure due to fasteners damage, and compromised aircraft landing systems due to lightning damaged spoiler.

Impacts of indirect lightning risk events and HIRF are the disabled or upset flight control system or whichever system the risk event may occur at. The system level impact implication should be considered.

Impacts of PEDs risk events occur at the communications and navigation system level as well as at direct cross-coupling with wires. In other words, depending on the location or extent of the risk event, the specific system impacted by the risk event and system level implication of the impact should be examined.

Impacts of P-static risk events occur at the radio communication system level.

Impacts of equipment to equipment EM interference are temporary malfunction or permanent damage of each sensor or control system.

4.4.4 Drivers for Impacts

The impacts generally occur at the system level, and thus the drivers for each impact should be found at the system level as well. The example drivers for these system level impacts are inadequate error corrections, lack of redundancies, poor bonding and grounding schemes of aircraft, inadequate electrical wiring interconnection system (EWIS) configuration and antenna siting geometry. These are usually design configuration issues at the system level.

4.5 Risk Resolution

Fig. 42 describes several ways of risk resolution. In this Section, we discuss the risk resolution steps by creating and examining risk tables and risk maps. Risk levels are first evaluated and expressed as expected loss. The expected loss is obtained by multiplying the risk likelihood and total loss. The risk likelihood in turn is calculated by multiplying the risk event probability and the impact probability. These components are tabulated and a risk map is plotted from the

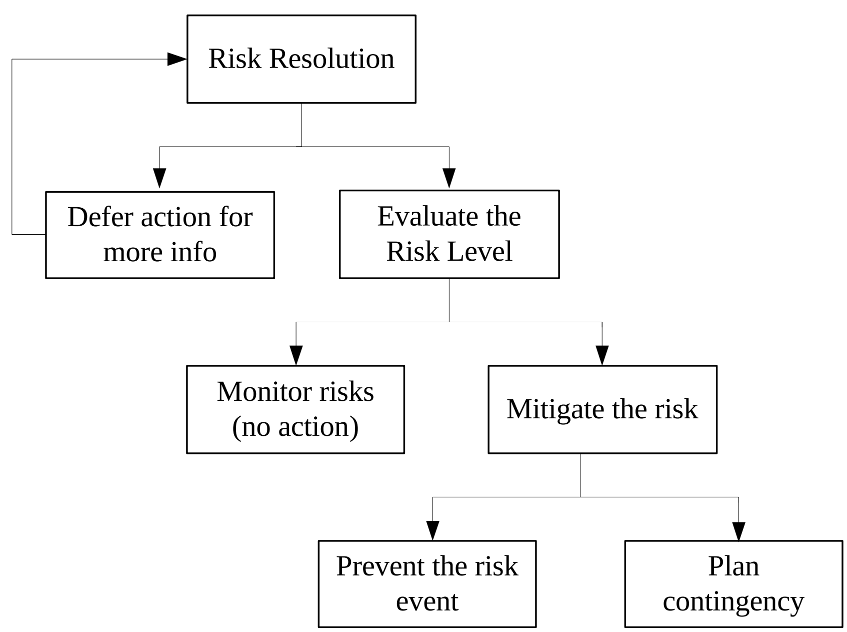

Figure 42. Risk resolution diagram

Table 13. Risk table for electromagnetic effects

Risk ID	Risk Event	Prob of Risk Event (Pe)	Prob of Impact (Pi)	Risk Likelihood	Total Loss ($M)	Expected Loss ($M)
1.a	Fuel tank explosion	1.0E-09	9.0E-01	9.0E-10	250	2.25E-07
1.b	Rudder damage	1.0E-06	1.0E-01	1.0E-07	0.1	1.0E-08
1.c	Fasteners damage	1.0E-05	5.0E-02	5.0E-07	0.2	1.0E-07
1.d	Compromised FCS	1.0E-06	1.0E-01	1.0E-07	0.3	3.0E-08
1.e	Engine damage	1.0E-07	5.0E-02	5.0E-09	1	5.0E-09
1.f	Antenna damage	1.0E-04	2.0E-01	2.0E-05	0.05	1.0E-06
1.g	Radome puncture	1.0E-05	3.0E-01	3.0E-06	0.25	7.5E-07
2	Ind lightning event	1.0E-04	2.5E-01	2.5E-05	0.1	2.5E-06
3	HIRF event	1.0E-04	1.0E-02	1.0E-06	0.1	1.0E-07
4	PEDs front door	1.0E-05	1.0E-05	1.0E-10	0.01	1.0E-12
5	PEDs back door	1.0E-05	1.0E-05	1.0E-10	0.01	1.0E-12
6	P-static	1.0E-03	1.0E-01	1.0E-04	0.01	1.0E-06
7	Equipment to equip	1.0E-03	2.0E-01	2.0E-04	0.01	2.0E-06

tabulated data. After the risk table and the risk map are developed, the risk levels of each risk event are examined with respect to a risk threshold. The risk threshold is a unique quantity for each project determined by the stakeholders. For the risks below the threshold curve, the risks are monitored but no actions may be taken. For risk events above the threshold curve, risk mitigation actions such as risk event prevention actions or impact contingency actions are taken. These processes are discussed in detail in the next three sections.

Table 14. EMI criticality category level

CAT 1	**Non-electronic equipment DC relays, DC solenoids, brushless induction motor**
CAT 2	Non-electronic equipment AC operated relays and solenoids
CAT 3	Electrical/Electronic equipment non-essential, susceptibility to wire-coupled or radiated EMI
CAT 4	Electrical/electronic Critical or essential, susceptibility to wire-coupled or EMI

4.5.1 Risk Evaluation and Monitoring Based on Risk Map

Risk evaluation sets the stage for the next actions in the way discussed above. As illustrated in Fig. 37, expected loss values are calculated by multiplying the risk even probability, impact probability and the total loss as the equation (1) below shows:

$$P_e \times P_i \times L_t = L_e \quad (1)$$

Where

P_e = Probability of risk event,
P_i = Probability of impact,
L_t = Total loss,
L_e= Expected loss

Based on the probabilities of risk events, probabilities of impact, and total loss in Tables 13, 14 and 15, a risk map is developed as shown in Fig. 43. The probability numbers are not specific to any aircraft model and they are presented as representation for illustration purposes. Note the y-axis, the Risk Likelihood, is in a logarithmic scale. Since the risk event (1.a), the fuel tank explosion, is an extreme outlier to the rest of the risk events, it is not included in Fig. 43. The way this risk map is developed is as follows: Firstly, we estimate the risk likelihood by multiplying the probability of the risk event and the probability of the impact. As an example, the risk event

Table 15. Criticality of EMI effects

EMC Category	Criticality	Failure Condition Classification	Development Assurance Level
4	Critical	Catastrophic	A
4	Essential	Hazardous/ Severe – Major	B
4	Essential	Major	C
3	Non-Essential	Minor	D/E
2	Any	Any	Any
1	Any	Any	Any

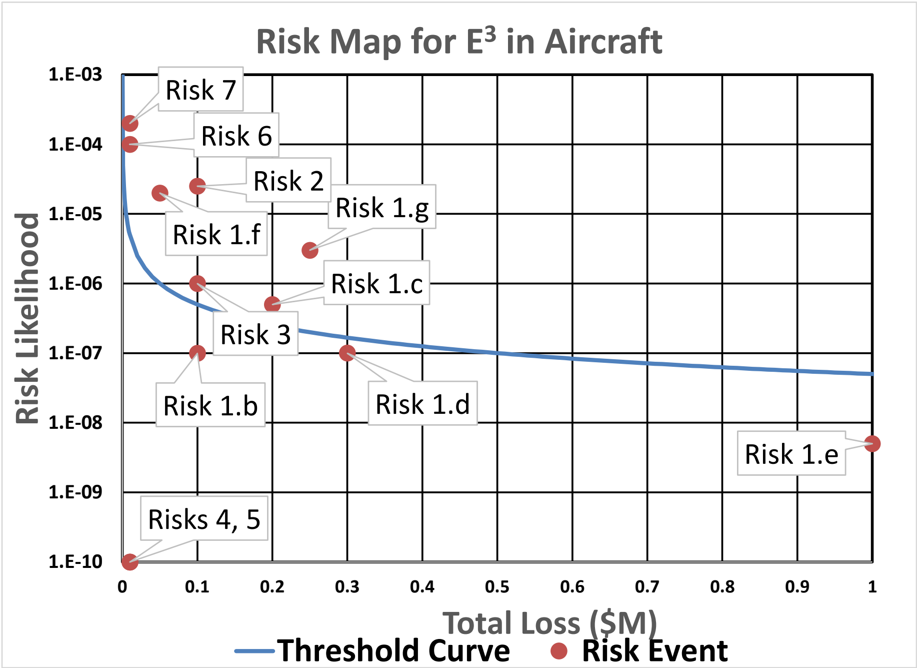

Figure 43. Risk map for electromagnetic effects in aircraft

probability of the rudder damage (risk event ID 1.b) is estimated to be 1×10^{-6} and the probability of the impact is estimated to be 1×10^{-1}. Thus the risk likelihood is calculated to be 1×10^{-7}. If this event is realized, the total cost of reaping the rudder is estimated to be $100,000, which is the total loss. Therefore, the expected loss is calculated to be one cent. This insignificant dollar figure is due to the extremely small probability of occurrence of the event.

All of the events listed in Table 13 are plotted in the Fig. 43 risk map by continual application of this process. The threshold was determined to be five cents in this example. By examining the risk map, the risk status of each risk event is clearly understood with respect to a threshold curve specific to an aircraft. We may accept the risk level of the risk events that are located below the threshold curve and choose not to address the risk events but simply monitor the risk level. By application of risk mitigation plans, we intend to move the risk events located above the threshold curve to locations below the threshold curve. After mitigation plans are implemented,

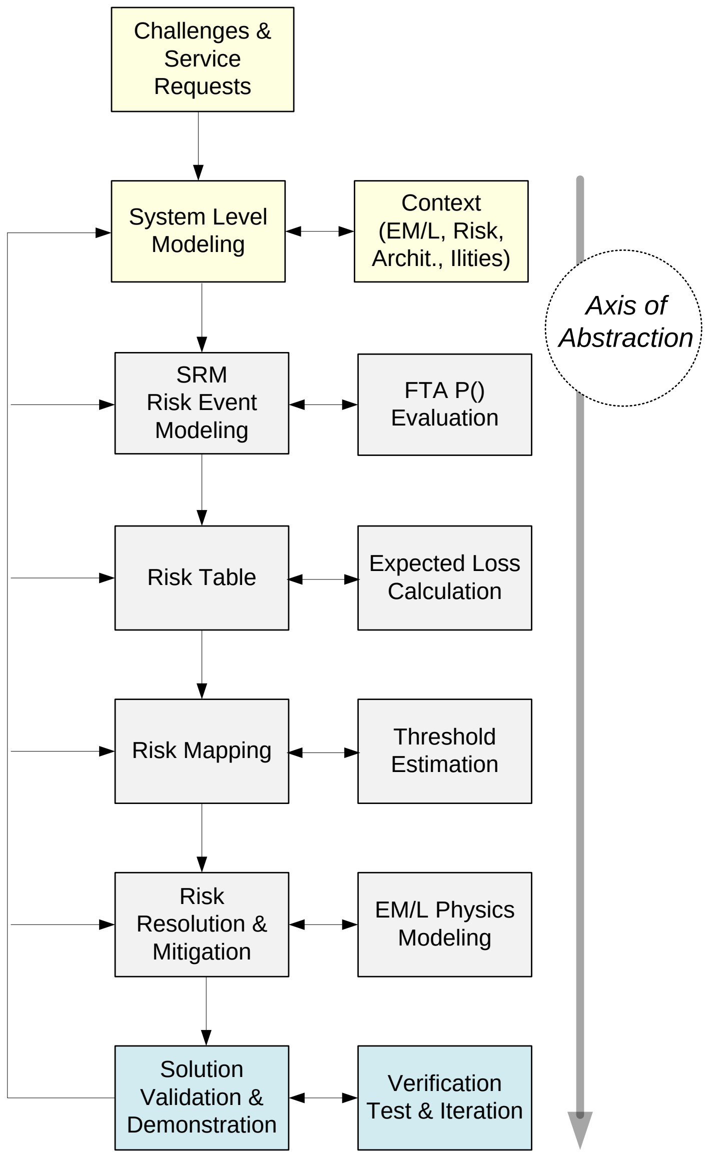

Figure 44. Flow diagram of E^3 risk analysis

the probabilities of risk events and probabilities of impacts should decrease and thus the expected loss values should be reduced. The essence of risk management is to monitor this movement of risk events on the risk map. The probabilities of risk events and impacts, total losses, and threshold values depend on the specific aircraft model under consideration. The risk modeling considered so far may be summarized as shown in Fig. 44. This flow diagram includes the entire processes and thus it represents the overall modeling of the whole risk analysis processes.

4.5.2 Risk Event Prevention Plan

As discussed previously, risk events are specific and concrete and may occur at the component level. Drivers of risk events are the facts that describe the causes of the events. Therefore the risk prevention comes out naturally by examining the risk event drivers carefully. For the direct lightning effects; examination of the (1.a.1) driver, the flammable vapors in fuel tank, leads one to the need for making the fuel tank vapor inflammable by using such equipment as nitrogen generating system (NGS). For (1.a.2) driver, sparking around the fuel tank suggests a good bonding and grounding scheme of the fuel tank. Examination of the (1.a.3) driver, high vapor temperature, leads one to the need to implementation of cooling mechanism around the fuel tank. This way we may develop the necessary preventive plan in a logical and systematic manner. Examination of the driver for events (b) to (g), damaged bonding jumpers and corrosion, leads one to establishment of the preventive plan of designing rugged and corrosion resistant bonding jumpers and wire bundles. For the indirect lightning and HIRF effects, review of the driver, the inadequate grounding, leads one to the need for a better grounding method of equipment and wire bundles. Review of the driver, and corrosion leads one to the need for protective design of wire bundles and connectors from corrosion.

For the PEDs front door electromagnetic coupling, review of the driver, high IPL (interference path loss), leads one to redesign consideration of aircraft windows and antennas siting geometry. Review of the back door coupling driver, high level electromagnetic coupling from PEDs to equipment wires, leads one to the need for adjusting separation distance and immunity improvement of aircraft equipment through EMI filters and better grounding.

For P-static risk event, review of the driver, inadequate static dischargers, leads one to consideration of better static dischargers such as the ones.

For the equipment to equipment EMC, review of the driver, inadequate wires separation and antennas isolation, leads one to re-design of wire installation and antenna configuration to meet the requirements of wire separation and antenna isolation.

4.5 3 Impact Contingency Plan

The impact and impact contingency plan occur at the system or subsystems level. The electromagnetic system can be subdivided into several subsystems such as flight control electromagnetic system, sensor electromagnetic system, fuel electromagnetic system, and others. For each subsystem, the contingency plan is achieved by examining the drivers for the impacts in the same way the risk event prevention plan was produced by examining the drivers for the risk events. Thus the concept of redundancy, error correction coding, software design, and system level grounding implementation including bonding jumper system level analysis is utilized to establish the impact contingency plan. The risk event prevention and impact contingency plan emerge in a systematic manner by carefully examining the risk event drivers and impact drivers with the standard risk model tool and systems engineering approach.

4.6 Chapter Conclusions

We have taken systems engineering approach and applied the standard risk model to electromagnetic environmental hazards analysis and mitigation in aircraft. The nature of electromagnetic energy interacting with aircraft and aircraft components lends itself well to systems engineering, risk analysis and risk management. Major risk events and impacts for aircraft electromagnetic hazards were identified and their drivers have been discussed. Risk prevention and impact contingency plans and risk monitoring methodology for aircraft electromagnetic hazards have been developed. We have shown that the systems engineering and standard risk model analysis for electromagnetic hazards in aircraft is appropriate and beneficial. Future work includes extending this approach to electromagnetic design details in aircraft to completion so that comprehensive electromagnetic database resource may become available to aviation industry. Quantification of risk event and impact probabilities in aircraft is quite a complex endeavor and further research based on analysis and testing is required.

5. Risk Analysis of Lightning Effects in Aircraft

The lightning effects in aircraft have been known since the early days of aviation, and still they are a subject of active research. Because the lightning issues in aircraft are of safety concern, governmental agencies require aircraft manufacturers to evaluate and mitigate the hazardous effects of lightning in aircraft and maintain high safety standards. In order to have commercial transportation aircraft be certified, aircraft manufacturers must prove they meet the strict governmental safety regulations. Thus conducting a risk analysis of lightning effects in aircraft is an essential task. Additionally, due to highly complex, dynamic and interrelated nature of the lightning strike effects on aircraft, it would be prudent to take a systems engineering approach to understand and address overall lightning effects in aircraft. In this paper, we intend to perform risk analysis of lightning hazardous effects in aircraft at a system level to assess and mitigate the lightning risks.

We examine the interaction of lightning with aircraft in Sections 5.1 and 5.2. We then introduce the Standard Risk Model in Section 5.3, and apply the model to lightning risk event and impact identification in Section 5.4. We next develop drivers for each lightning risk event and impact, and present the baseline of risk prevention and impact contingency plan for lightning hazard mitigation. We conclude with a summary and suggestions for the future work of aircraft lightning protection.

5.1 Introduction

It is well-known that an average of one lightning stroke attachment can be expected for each 3,000 hours of flight for any type of commercial transport aircraft [108]. The effects of these lightning strikes on aircraft have been a continuing concern to aviation industry since the early days of the aviation era. Because lightning hazards present aviation safety concerns, these issues are regulated by governmental rules such as the Title 14, Code of Federal Regulation (14 CFR) 25.581 and 25.981 for direct effects, 25.954 and 25.981 for fuel tanks, and 25.1316 for indirect effects. Regulation codes may vary for different aircraft models. CFR 25.581 states that the airplane must be protected against catastrophic effects from lightning, and CFR 25.954 states the fuel system must be designed and arranged to prevent the ignition of fuel vapor within the system by direct lightning, swept lightning, or corona and streamering at fuel vent outlets. The electrical and electronic system lightning protection regulation is found in CFR 25.1316.

The basic components of lightning energy transfer diagram are shown in Fig. 45, where the lightning problem situation is decomposed into three components: lightning energy source, transfer path for lightning energy, and receptor of the lightning energy. This diagram emphasizes the fact that the three-component framework commonly used in EMC discipline is equally applicable to lightning energy transfer [109].

The generation of lightning energy, the first component of the Fig. 45 diagram, occurs naturally, therefore the electromagnetic environment of lightning does not change significantly over time. However, there is a clear evidence that lightning flashes could be triggered by aircraft when aircraft is flown into clouds. A large percentage of lightning strikes to aircraft have evidently been triggered by and initiated at the aircraft, although the occurrence percentage of aircraft-triggered strikes is not known. An empirical study shows the necessary potential discontinuity

Figure 45. Lightning energy transfer model diagram

between an air vehicle and the adjacent atmosphere may reach 10^6 V before the lightning leader can be initiated from the vehicle [110]. The lightning strike probability of aircraft changes as a function of altitudes and weather conditions.

For a discussion of the second element in Fig. 45, the transfer path, we note the lightning energy is transferred to aircraft equipment via magnetically induced voltages. When a lightning stroke attaches to aircraft, subsequent current flow on the aircraft produces strong magnetic fields, which surround the conductive airframe and change rapidly as a function of the fast changing lightning stroke currents. Part of this magnetic flux could leak inside the aircraft through apertures, such as windows, composite fairings, door seams or joints. These internal fields couple through electrical wire circuits and induce voltages in them in proportion to the rate of change of the magnetic flux. The magnetically induced voltages could appear between wires of bundles as line-to-line voltages or between wire and airframe as common mode voltages. Resulting damages or upsets of electrical equipment by these induced voltages are referred to as indirect effects of lightning. Thus the lightning coupling paths are comprised of the aircraft surface and the affected wire bundles.

In order to investigate the indirect lightning effects further, lightning strike configurations may be examined. The lightning strike configurations refer to the lightning current path from the entry point to the exit point. The lightning entry and exit points may be understood in terms of zoning of the aircraft, which is discussed in Section 5.2. Probability of occurrence could be assessed for each strike configuration. The lightning strike configurations which commonly occur are the paths from an extremity point to another extremity point. Typical strike patterns used to test and assess the lightning effects at the aircraft level are available in public literature [111]: (1)

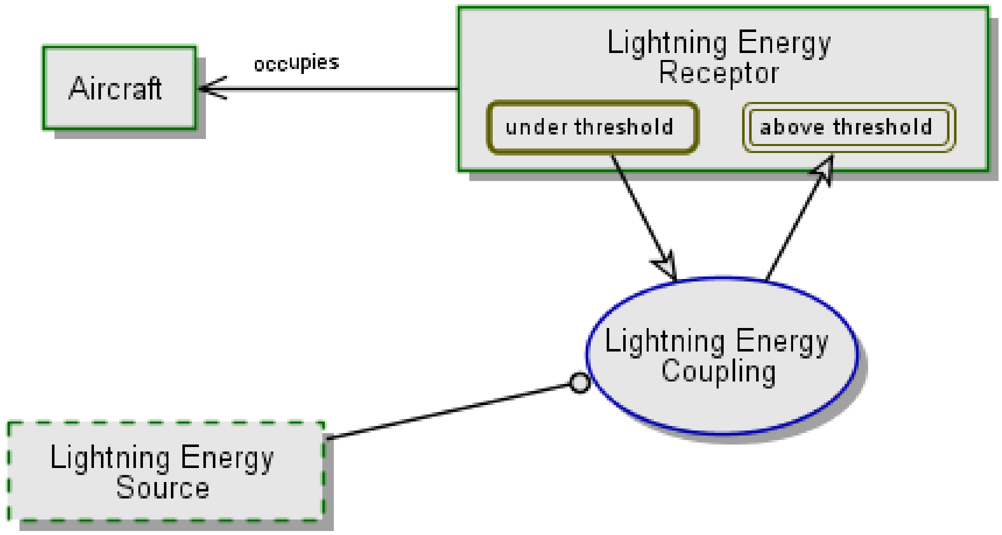

Figure 46. Lightning energy coupling modeling with OPM

nose radome to engine's aft, (2) nose radome to main landing gear, (3) nose radome to an extremity aft of nose, (4) nose radome to wing tip, (5) nose radome to tailcone, and (6) nose radome to horizontal /vertical stabilizer and elevator. Other severe lightning strike configurations include (7) wing tip to tail, (8) wing tip to wing tip, and (9) landing gear to tail. We selected such lightning strike configurations as typical examples knowing that they do not cover all possible lightning paths. Actual current paths depend on individual aircraft model and geometry. This lightning energy coupling can be modeled with OPM as shown in Fig. 46. The lightning energy is in the environment, not in the system, therefore is surrounded by dotted line. The lightning energy changes the state of the receptor electronics, which is shown as stage change in the diagram. The lightning energy receptor occupies the aircraft, which is also shown in Fig. 46.

We note that the airframe as a lightning energy transfer path has in recent years changed for the worse due to growing usage of composite material in its manufacturing. Composite material is not as conductive as aluminum is and it does not provide as good lightning protection to aircraft equipment as aluminum material does. In order to understand the role of wire bundles as lightning energy transfer path, we also need to consider wire bundle routing.

When the wire bundles are installed in parallel to the lightning strike configuration, the equipment connected to these wires are affected most significantly. The wires that are routed perpendicularly to the strike configuration are affected the least. This is due to the difference in energy coupling mechanism discussed earlier in this section.

Example wire routes that are parallel to the strike configurations listed above are as follows: (1) upper nose to engine, (2) lower nose to main landing gear, (3) lower nose to lower nose, (4) lower nose to main wheel well and wing trailing edge, (5) lower nose to aft stair, (6) lower nose to tailcone interfaces, (7) wing trailing edge to engine, (8) flight control wires, and (9) landing gear control wires. The energy transfer from current flow on the aircraft surface to wires occurs through lightning current diffusion, redistribution, or coupling through such apertures as cockpit and cabin windows, non-conductive access panels, wheel wells, wing aft cavities and weather sealed joints.

The third component of Fig. 45, the receptor of the lightning energy, is mainly the aircraft equipment on or inside the aircraft that are connected to the wire bundles mentioned in the previous paragraph [112]: (1) electronic engine control (EEC), (2) wheel speed transducer, (3) angle of attack, (4) position sensor of aileron, spoiler, flap, (5) aft stair up switching, (6) rudder position sensor, (7) fuel temp probe, (8) flight control sensors and actuators, and (9) landing gear control. When the received energy is greater than the equipment threshold, the receptor equipment act in an undesired manner, which constitutes interference. Impacts of the events due to malfunction of these equipment could be beyond the equipment level. The impacts may have the unit-subsystem-system structure.

The indirect effects discussed above are becoming more important because of (1) growing use of composite material in airframe, (2) trend toward miniaturization of electronics, (3) increasing use of electronics in communication, navigation and surveillance (CNS) and flight control (Fly-by-wire), and (4) more frequent flight through adverse weather conditions.

In regard to direct lightning effects, we note the lightning stroke attachments transfer energy to the aircraft skin, structure, equipment or bundles directly, causing damages as holes burned at metal skins, punctures or splinters of non-conductive parts, or welding of moveable hinges and bearings, and tearing, vaporization and blasting of aircraft structures. The receptors of the lightning energy for direct effect consideration are such aircraft structural components as nose radome, flight deck windows, fuselage, antennas, empennage, wings, wing tips, lights, engines, integrated drive generators (IDG), landing gears, and empennage tips.

There is another category of effects which is fuel tank explosion. This category is due to a combination of direct effects and indirect effects. The lightning strikes on or near the fuel tank area could cause a catastrophic events. Fuel tanks are located in zone 3 which is rarely hit by lightning. Thus it would be more likely that the effects will be indirect and the fuel tank may be subject to conducted currents. This cause sparking in the fastener area or gasket area in the fuel tank and that energy may get into the fuel tank. Thus a very careful design of fasteners, gaskets, and fuel tank structure are required to avoid such catastrophic events. Other consideration on this topic includes paint thickness. It is known that thicker paint may allow lightning energy to arrest for a longer time than thinner paint does.

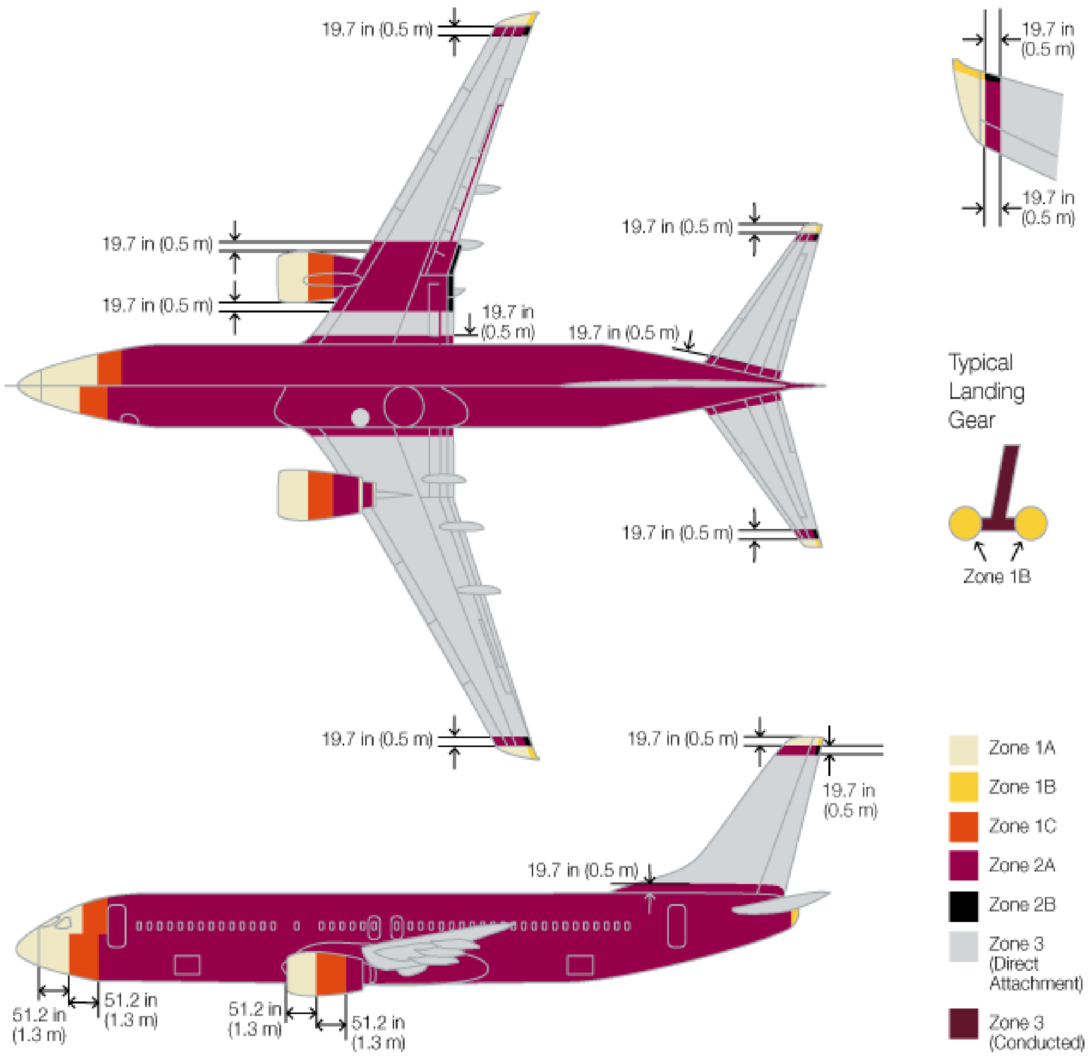

Figure 47. Lightning zone of aircraft

5.2 Lightning Attachment Zones

It is not possible to deterministically predict where on aircraft the next lightning strike will be attached. However, the general area where the lightning strokes attach may be estimated by examining lightning attachment zones on aircraft as shown in Fig. 47 [113]. SAE Aerospace published ARP 5414A which contains the following zone definitions as well as methods used to determine lightning zoning for aircraft [114]. Zones represent the external lightning strike environment as applied to the aircraft, and they often vary from one aircraft to another. Zone 1A refers to areas of aircraft surface where a first return stroke is likely during lightning channel attachment with a low expectation of flash hang on. Zone 1B refers to all areas of aircraft surface where a first return stroke is likely during lightning channel attachment with a high expectation of flash hang on. Zone 1C refers to all areas of aircraft surface where a first return stroke of reduced amplitude is likely during lightning channel attachment with a low expectation of flash hang on. Zone 2A refers to areas of aircraft surface where subsequent return stroke is likely to be swept with a low expectation of flash hang on. Zone 2B refers to areas of aircraft surface into which a lightning channel carrying a subsequent return stroke is likely to be swept with a high expectation of flash hang on. Zone 3 refers to the surface areas not in Zones 1A, 1B, 1C, 2A, or 2B, where any attachment of lightning channel is unlikely, and those portions of the aircraft that lie beneath or between the other zones and/or conduct substantial amount of electrical current between direct or swept stroke attachment points. Lightning attachments usually occur in Zone 1 but exit from a different Zone 1 area. As a continuous ionized channel is formed between charge centers, the ensuing currents that flow through the channel may persist for up to a second or more. The channel remains in its original location but the aircraft continues to move forward a significant distance during the life of the flash. Thus, in addition to initial entry and exit points, different final entry and final exit points form over the aircraft. The lightning currents are distributed widely throughout the surface of aircraft. In consideration of this wide current distribution and the global nature of the associated magnetic field effects, systems engineering approach in general, and a system risk analysis in particular, are taken in examining the lightning situation in aircraft [115, 116, 117].

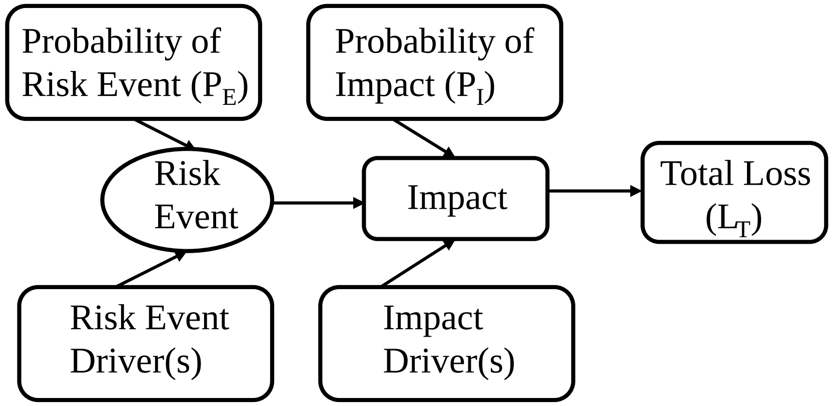

Figure 48. Standard risk model to use for lightning risk analysis

5.3 Standard Risk Model for Lightning

For the rest of the paper, we discuss definition, assessment and mitigation of lightning risks in aircraft. We find the standard risk model (SRM) illustrated in Fig. 48 to be the one most useful to understand risks and develop mitigation methods [118]. In the SRM illustrated in Fig. 48, risk is understood as the potential that something will go wrong as a result of an event or a series of events. SRM contains the following components in its risk evaluation process:

(1) Risk event: The happening or state that "triggers" a loss in safety or economic value. The risk events may be a specific and concrete lightning incident or a hazardous event.

(2) Driver of a risk event: Something existing in the event environment that leads one to believe that a particular risk such as lightning incidents could occur.

(3) Impact of a risk: The consequence or potential loss that might result if a risk event occurs. In a complicated situation such as a lightning stroke attachment to aircraft, the impact may not always be a damage isolated at a component level, but it could be a widespread effect at a system level.

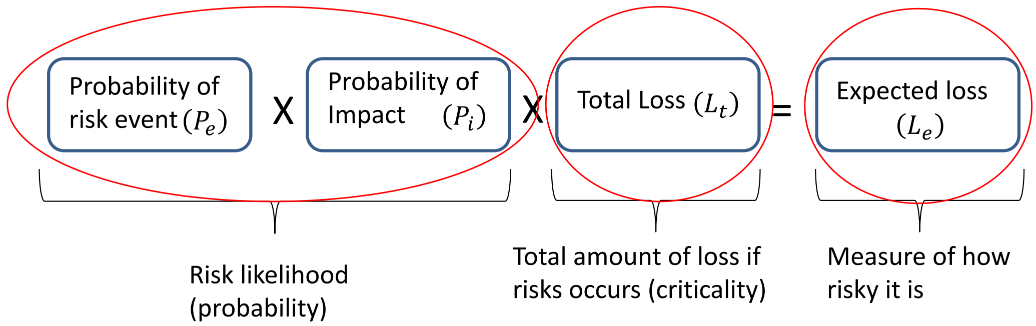

Figure 49. Expected loss calculation diagram

(4) Impact driver: Something existing in the lightning problem situation that leads one to believe that a particular impact such as a system level loss could occur.

(5) Total loss: The magnitude of the actual loss value accrued when a risk event occurs; it could be measured in days or money, but in complex situations, a simplistic monetary or time value representation may not be feasible. In other words, it may be represented qualitatively rather than quantitatively in terms of equipment criticality or failure condition classifications. The expected loss calculation using the total loss is shown in Fig. 49.

(6) Probability values: Probability values are assigned to lightning risk events and impacts.

The Standard Risk Model is used for the aircraft lightning risk analysis because of the following advantages of the model:

(1) The Standard Risk Model process is simple and easy to understand and it captures the essence of risk resolution.

(2) It separates risk events and impact, and supports cause and effect analysis.

(3) It evaluates the risk values enabling risk monitoring via risk maps possible.

SRM is a standard model widely accepted internationally, therefore it will be easier to compare the risks against known risks in other similar projects. This allows us to address similar

Figure 50. Lightning strikes in aircraft with entry point and exit point

risks with less resources, helps prioritize risks, and enables us to focus on unresolved risks. The risks are evaluated by computing expected loss, which is the average (mean) loss. A probabilistic risk analysis work with somewhat different approach from the present paper has been published for intentional electromagnetic interference (IEMI) situations [119]

5.4 Risk Events, Impacts and Drivers

We identify the lightning risk events, impacts and drivers in aircraft according to the Standard Risk Model. Even though aircraft manufacturers have made excellent progress in lightning protection, inspection and repair methods, lightning strikes still cause airlines costly interruptions for revenue flight services [120].

5.4.1 Risk Events for Lightning Effects

Lightning stroke attachments as illustrated in Fig. 50 generate both direct and indirect hazardous effects in aircraft. Typical risk events are listed below [121]:

Lightning direct effect event is illustrated in Fig. 50 and several such events are listed as follows:

(1) Melt-through damage for metal or non-metal skins (of fuel tank skin, trailing edge, painted skin, radome)

(2) Resistive heating damage (bonding strap heating or exploding wires for a navigation light on a plastic vertical fin cap, diverter straps, pitot probe air tube, and radome) Magnetic

force effects (slamming together of two metal air pressure tubes in a radome mounted pitot system, in wing tip trailing edges, bent bond straps)

(3) Arcing across bonds (over riveted joints with corrosion inhibiting coating, over fasteners or bonding jumpers with inadequate current carrying capacity, over fasteners in secondary structures such as wing tips, tail cones, wheel well doors, and flight control surfaces, over adhesive bonds, over hinges and bearings resulting in pitting or welding)

(4) Sparking over structural joints

(5) Punctures or flash-over over nonconductive composite material (radomes, composite material skin)

(6) Damage of windshields, canopies, windows (direct or swept channel attachment to heating elements and damaging the connected power circuits)

(7) Damages on electrically conductive composites (carbon fiber composite skins in Zone 1 and 2 by lightning stroke currents by mechanism of pyrolysis and shock wave; primary

Figure 51. Conductive strip in rudder may get lifted and damaged due to water ingress

structures, engine nacelle and pylon, flight control surface, leading edge devices, avionics bay, wing and empennage tips, fuel tank skin)

(8) Damage of propulsion system (engine cowlings or nacelles, propeller and rotor blades, gear boxes damaged by lightning attachments)

(9) Rain erosion of conductive lightning protection strip in Fig. 51 (degradation of conductive frame on wings and empennage)

Lightning indirect effect events for which the following systems of concern fail:

(1) Full authority digital engine control (FADEC)

(2) Full authority electronic flight control (Fly-by-wire)

(3) Supervisory control systems capable of initiating control inputs that could endanger flight safety

(4) Fully or highly integrated cockpit instruments and displays

(5) Electronic flight instrumentation system (EFIS)

(6) Aircraft electric power control and distribution system

(7) Electrical and avionics systems that include externally mounted apparatus, such as air data probes, heaters, actuators, and antennas

Fuel system fire or explosion due to lightning strikes

5.4.2 Drivers for Lightning Risk Events

Drivers for each event are: (a) insufficient skin thickness; lightning arc energy concentration, lack of protective layer; (b) lack of an alternate, parallel path for the lightning current, (c) magnetic force acting on two metal current paths, and bonding strap bending (d) corrosion inhibition coating may reduce the lightning current flow, design may force individual fastener to carry more than 5 kA component A stroke current, hinges and bearings may have a single point of contact, (e) inadequate design of joint or bonding resistance, 2.5 m□ is not always adequate, (f) no adequate electric path on radome, streamer development inside the radome, corona and charge formation for puncture, (g) electric field from lightning channel being swept across the windshield surfaces attaching to electric heating elements embedded, (h) inadequate material strength, lack of lightning current paths, degraded electrical conductivity, concentrated arc root (i) inadequate design of lightning protection for small airplanes and helicopters in terms of composite material lightning protection, (j) inadequate protection of conductive strips from rain erosion

Drivers for lightning indirect effects for events (a) to (g) are: lack of proper shielding of wires and connectors, improper grounding and bonding, equipment susceptibility higher than requirement due to design issues (lack of lightning protection devices, EMI filters and others). Drivers for fuel system risk event are: sparking generation from lightning due to inadequate fasteners, flammable fuel vapor, and high fuel tank temperature. Ignition sources may be provided by dielectric puncture, burn through, hot spot formation, ohmic heating, exploding conductors on fuel system joints, wires, access doors, and tank surfaces.

5.4.3 Impact Identification for Lightning Effects

We identify the impacts of these lightning effect risk events as a next step. A risk event is a specific occurrence and is identified at a component, whereas the impacts of risk events in general have a system level implication and, for the most part, are multi-leveled, meaning impacts occur at a component level as well as at a system level. This multi-level impact is understood in terms of organizational hierarchy which should be addressed by considering the axis of organization in an architecture framework or taxonomy in context of systems architecture engineering.

Impacts of direct lightning effect events are the compromised structural integrity, or compromised performance of the systems affected by the mechanical damages, thermal burns, or electrically degraded bonding and grounding resistance. Impacts of indirect lightning risk events are the system level effects due to the disabled or upset system. Impacts of fuel system risk event are ignition of fuel system which could result in a loss of the aircraft.

5.4 4 Drivers for the Lightning Impacts

Since the impacts generally occur at a system level, the drivers for each impact should be found at the system level as well. The example drivers for these system level impacts are; lack of redundancies, inadequate bonding and grounding schemes of electrical systems including electrical wiring interconnection system (EWIS), and absence of error corrections for subsystem electronics. These are the system configuration and design issues at the system level as well as at the unit level.

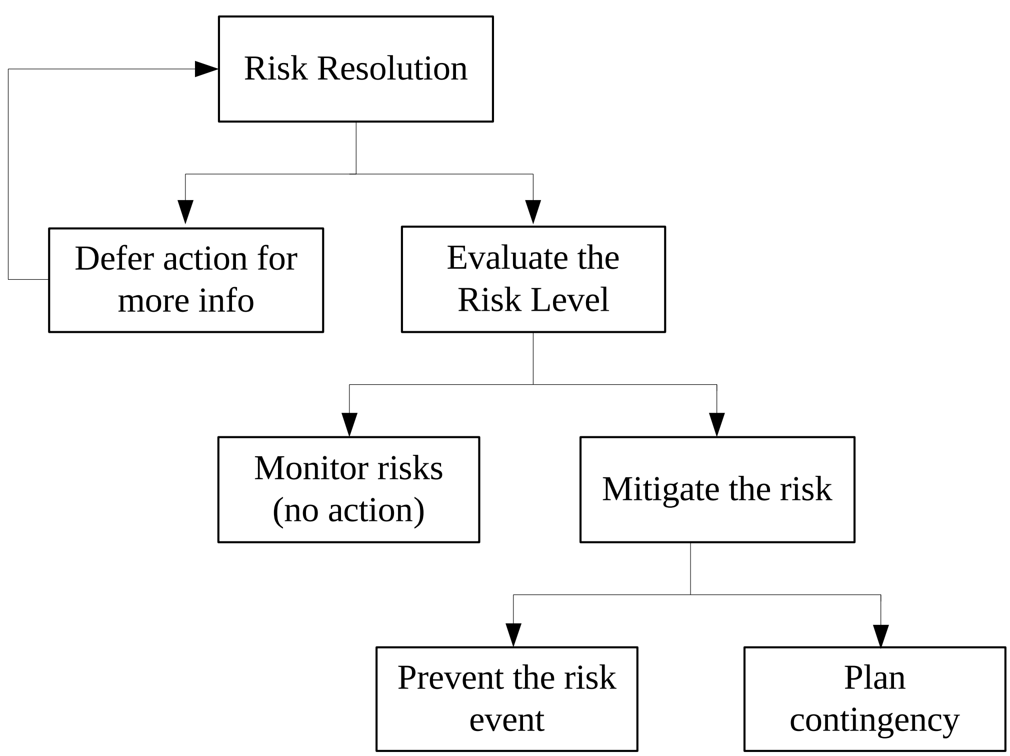

Figure 52. Risk resolution diagram to be used for electromagnetic risk mitigation

5.5 Lightning Risk Resolution

A lightning risk resolution process is shown in Fig. 52. Risk resolution is accomplished by developing risk action plans. In order to develop action plans, we examine the risk level of each risk event. If the risk level is higher than a predetermined threshold, then the risk mitigation actions such as risk event prevention actions or impact mitigation actions are performed. If the risk level is lower than the threshold, the risk is monitored but no immediate actions are required. A risk level is quantified by an expected loss value obtained by multiplying the risk event probability, impact probability, and total loss. Multiplication of the risk event probability and impact probability represents risk event likelihood and the total loss value represents the criticality of the affected system. These two entities, the likelihood and the criticality, are commonly found in risk or safety analysis procedures. Thus it is essential to assess the criticality of the lightning energy receptors in order to evaluate the risks. However, criticality may not always be quantifiable, and, in many cases, qualitative assessment of criticality may have to be used by categorizing the equipment into critical, essential, or non-essential. These criticality categories correspond to failure conditions of being catastrophic, hazardous (or major), and minor respectively.

(A) Risk Assessment and Risk Monitoring

The risk level of an event is assessed by calculating the expected loss value as follows:

$$P_e \times P_i \times L_t = L_e \qquad (1)$$

Where

P_e = Probability of lightning risk event,

P_i = Probability of lightning impact,

L_t = Total loss,

L_e= Expected loss

Table 16. Risk table for lightning effects in aircraft

Risk ID	Risk Event	Prob of Risk Event (Pe)	Prob of Impact (Pi)	Risk Likelihood	Total Loss ($M)	Expected Loss ($M)
1.a	Melt-through	1.0E-03	1.0E-04	1.0E-07	0.15	1.50E-08
1.b	Resistive heating	1.0E-04	5.0E-03	5.0E-07	0.25	1.25E-07
1.c	Magnetic force	1.0E-05	5.0E-05	5.0E-10	0.1	5.00E-11
1.d	Arcing across bond	1.0E-03	1.0E-03	1.0E-06	0.2	2.00E-07
1.e	Bonding resistance	1.0E-02	1.0E-03	1.0E-05	0.2	2.00E-06
1.f	Noncond comp	2.0E+00	3.0E-02	6.0E-02	0.5	3.00E-02
1.g	Window	1.0E-02	3.0E-03	3.0E-05	0.3	9.00E-06
1.h	Cond composite	1.0E-02	2.0E-02	2.0E-04	0.45	9.00E-05
1.i	Propulsion	5.0E-02	1.0E-02	5.0E-04	1	5.00E-04
1.j	Conductive strip	1.0E-02	1.0E-02	1.0E-04	0.25	2.50E-05
2.a	FADEC	1.0E-02	1.0E-02	1.0E-04	0.8	8.00E-05
2.b	FBW	1.0E-03	1.0E-02	1.0E-05	0.75	7.50E-06
2.c	Control	1.0E-02	1.0E-01	1.0E-03	0.6	6.00E-04
2.d	Cockpit display	2.0E-02	2.0E-01	4.0E-03	0.4	1.60E-03
2.e	EFIS	5.0E-02	4.0E-02	2.0E-03	0.4	8.00E-04
2.f	EPCD	1.0E-01	1.0E-01	1.0E-02	0.55	5.50E-03
2.g	Avionic	3.0E-02	6.0E-02	1.8E-03	0.45	8.10E-04
3	Fuel system	1.0E-09	5.0E-01	5.0E-10	250	1.25E-07

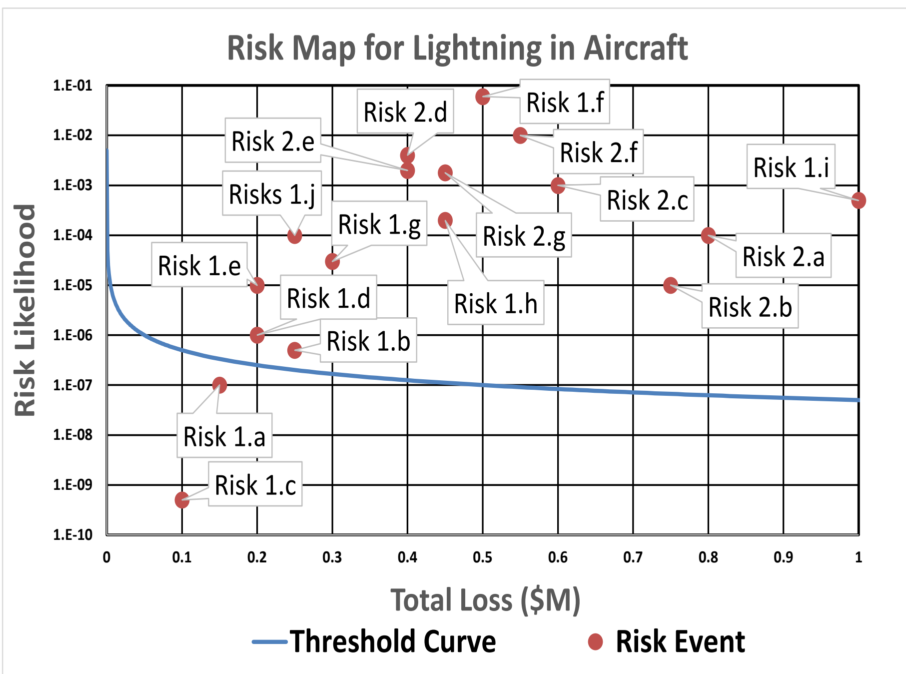

Figure 53. Risk map for lightning effects in aircraft

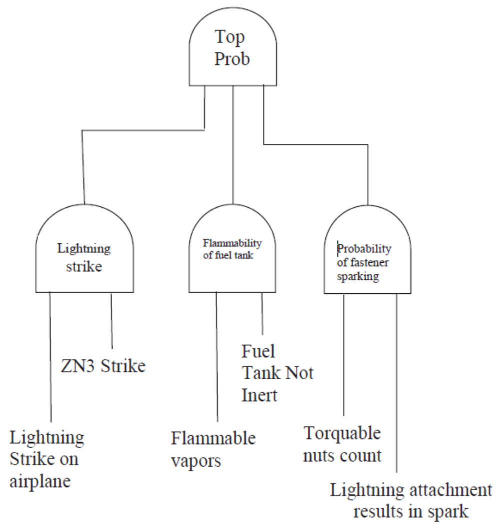

Figure 54. Top probability of lightning strike fault tree analysis

Table 16 is a summary of the probabilities of risk events, probabilities of impact, total loss, and expected loss, and a risk map is developed in Fig. 53 based on the risk table. These are representative and it has been produced for illustration purposes. A logarithmic scale is used for risk likelihood y-axis due to a widely varying range of the risk likelihood values. The way this lightning risk map is developed is as follows: Firstly, event probabilities are calculated as shown in Fig. 54. Then we estimate the risk likelihood by multiplying the probability of the risk event and the probability of the impact. As an example, the risk event probability of the resistance heating of a radome (risk event ID 1.b) is estimated to be 1×10^{-4} and the probability of the impact is estimated to be 5×10^{-3}. Thus the risk likelihood is calculated to be 5×10^{-7}. If this event is realized, the total cost of repairing or replacing the radome as well as the associated damaged electronics inside the radome is estimated to be $250,000, which is the total loss. The expected loss is obtained by multiplying the risk likelihood 5×10^{-7} and the total loss of $250,000, which results in 12.5 cents of expected loss. This minuscule dollar figure is due to the very small probability of the risk event occurrence.

The fuel system explosion risk calculation may be achieved by modeling the risk with the Fault Tree Analysis (FTA) as sown in Fig. 54. The Fault Tree includes three components that contribute to the fuel tank explosion: (1) Lightning strike event on or near fuel tank, (2) existence of flammable fuel vapor, (3) spark ignition source inside the fuel tank. Probability values for these three components are AND gated because these three conditions should exist independently and simultaneously for the fuel tank ignition to occur. The lightning strike event probabilities may be obtained from historical lightning data for each aircraft flight scenarios or patterns. Fuel tank door gaskets or fasteners are analyzed or tested for sparking conditions. The top level FTA risk probability is calculated by this way and it is included in Table 17.

Table 17. Lightning strike probability for each altitude segment

Altitude range (ft)	Probability
0 to 5,000	4.72E-10
5,000 to 10,000	7E-10
10,000 to 15,000	2.32E-09
15,000 to 20,000	1.83E-09
20,000 to 25,000	5.8E-10
25,000 to 30,000	3.9E-10
30,000 to 35,000	5.09E-10
35,000 to 40,000	1.36E-10
40,000 to 45,000	0
Total per flight	6.94E-09

All of the risk events listed in Table 16 are plotted in the Fig. 53 risk map by continual application of this process. The threshold was determined to be five cents in this example. The threshold values may vary for each aircraft model, the nature of the project, and requirements, which are discussed and determined by stakeholders. The status of each risk event is clearly shown in the map with respect to a threshold curve. Some risk levels under the threshold may be acceptable to the project and are just monitored, but no actions are taken. For the risk events above the threshold curve, risk event preventive actions and impact contingency plans are performed as discussed in the next two sections. As the risk event probabilities and impact probabilities are reduced to an adequate level, the likelihood probability values are also decreased in proportion and the overall expected loss values are decreased. Continuation of this action moves the risk events from the location above the threshold line to the location below the threshold line. All risks of lightning effects in aircraft are monitored and mitigated this way with the goal to reduce all risk levels to an optimum level.

(B) Risk Event Prevention for Lightning Strike Damage

Previously 18 lightning risk events were identified and the corresponding drivers were discussed. Risk event prevention is discussed below by examining the drivers for each risk event.

(a) The driver of this event, the inadequate skin thickness suggests a risk event prevention method of increasing the skin thickness. It is possible to determine the optimal thickness of the skin for unpainted aluminum skins and for painted skins by lab testing. (b) Likewise, the driver of lack of arc root dispersion suggests treatment of an exterior surface with an electrically conductive bumpy finish to enhance the arc root dispersion; the driver of lack of protective layer suggests laminating the skin with a protective layer of thin metal applied with a nonconductive adhesive, (b) the driver of lack of adequate current path suggests, as a prevention, to provide alternate current paths by making the corrosive inhibit coating even thinner and uniform, and to provide multiple conductive contacts, (c) the driver of two current paths in parallel suggests change in configuration design, and straighten the bonding straps and keep them short. In this manner, each driver suggests the following: (d) provide sufficient lightning current path through riveted joints or fasteners, control the thickness of adhesive bonds, provide multiple points of contact for hinges and bearings, (e) research into nature of bonding resistance including contact materials, shapes, surface areas, treatment of mating surfaces, and contact pressure, (f) installation of diverters or foil strips to intercept lightning flashes and divert them to nearby metal structure for radome, application of conductive material such as flame-sprayed metals over exterior of structures (other than radome), (g) test and select candidate windshield laminates, use of tough center ply, use of metal film heating element instead of fine embedded wires, employ surge suppression devices on power distribution circuits or buses, test candidate windshield and window design, bleed charges by anti-static coatings (h) strengthened material, provision of lightning current paths, arc root dispersion at multiplicity of points, use of expanded metal foil co-cured with the CFC laminate, (i) method of lightning protection for composite material for large aircraft may be used for small aircraft and helicopters, (j) study of conductive strip installation strength Next we wish to discuss risk mitigation based on the drivers examination.

(a) to (g): Lack of proper shielding of wires and connectors suggests adequate shielding design for wire bundles and EMI backshell, the driver of improper grounding and bonding suggest sturdy design of grounding and bonding, and the driver of equipment susceptibility higher than threshold suggests design and installation of lightning protection devices such as meal oxide varistors (MOVs) and prudent subsystem design with EMI filters and others.

The sparking driver for the fuel system ignition risk event suggests that prevention of sparking formation is required by fastener design improvement or by adding spark extinguishing sealant at the bottom end of the fasteners, the driver of flammable fuel vapor suggests necessity of installation of devices such as the nitrogen generation system (NGS) which fills the tank with nitrogen enriched air, the driver of high fuel tank temperature suggests advanced fuel cooling method implementation. We also may utilize guidance literatures such as FAA Advisory Circular 25.981-1C for information on compliance with the certification requirements about prevention of ignition sources within the fuel tanks of transport category aircraft.

(C) Impact Contingency Plan for Lightning Strike Damage

Impacts and impact contingency plans occur at the system level. Consideration of the system level impact drivers for lightning direct effects, indirect effects, and fuel system failures suggests revised design implementation for each electrical subsystem. In other words, for each electrical subsystem, the revised design plan is accomplished by examining the drivers for the impacts in the same way the risk event prevention plans were produced by examining the drivers for the risk events. Thus the concept of redundancy, error correction coding, software design, system level bonding and grounding implementation and new material development are naturally proposed to establish the impact contingency plan. We note the system level knowledge is necessary and critical in proposing the system level solutions. This way of careful examination of drivers for risk events as well as for impacts within the context of the Standard Risk Model enables emergence of risk event prevention and impact contingency plans in a systematic and logical manner.

5.6 Chapter Conclusions

Lightning risk analysis of aircraft systems has been performed from a systems engineering perspective. The Standard Risk Modeling approach was used for the analysis. Lightning currents propagate over the aircraft body from the entry point to exit point and affect the overall aircraft system directly as well as indirectly. Thus a system level approach to risk assessment and mitigation of lightning effects in aircraft is appropriate and beneficial. Typical lightning risk events were identified and their drivers have been discussed. Risk monitoring methodology as well as risk prevention and impact contingency plans for aircraft lightning hazards were developed. We have shown the risk analysis processes in detail so that this Standard Risk Model may be used for specific problem situations.

Future work includes applying this approach to specific aircraft models and extending it to all subsystems and modules so that comprehensive lightning risk database may be established to aid aviation industry. More accurate probability quantification of lightning risk events and impacts based on analytical means, lab and aircraft level testing, and historical statistical analysis is required. Further development of this system level lightning effects evaluation modeling of aircraft with increased rigor is necessary. The model based systems engineering (MBSE) has been proven to be successful in dealing with many system level issues [122]. Application of MBSE to this lightning effect evaluation for aircraft is recommended. Validation and demonstration of the approach through experimental testing for specific case is also desirable.

6. Testing of Lightning Effects on a Fuel Tank

The goal of this chapter is to show details of testing as a risk mitigation step for lightning risk event on fuel tanks. We have found fuel tank doors are vulnerable to lightning strike events. For this risk event, a driver-event study has been performed with the risk analysis model developed in Chapter 3. A major driver for the event we found was corrosion in the door gasket. We have set up a risk event prevention program which included a new design for the gaskets that are resistant to corrosion. This was an interdisciplinary work; it required lightning engineers, fuel engineers, material scientists and mechanical engineers. Design of the test waveform of lightning current is first presented. Then the lightning test background, test objective, approach conformity test are fully explained. The test procedure is developed. Test conduction, pass fail criteria discussion, and the test results are shown. This is an example of a specific case where the risk model is applied to obtain a solution to a risk event. The testing described in this chapter is a part of driver-event root cause analysis and risk mitigation activity. The risk model and approach are validated by showing some details of the risk analysis and mitigation via testing.

6.1 Design of Lightning Test Waveform Component

A lightning test is performed to verify and validate the methodology proposed in this work. In order to perform the test, the lightning waveform that are injected are investigated in this section. The power supply used for the test had 20kV, 0.1A rating, and lightning component A with 200kA peak and $2.5 \times 10^6 \, A^2sec$ action integral was desired. The capacitor bank was the design parameter. The test panel resistance was estimated to be 0.05 ohm.

The waveform generation may be described as follows where α and β are waveform design constants which to obtain the form we desire.

$$I = I_0\left(e^{-\alpha t} - e^{-\beta t}\right) \tag{1}$$

Initial current values from [123] are used.

I_0 = 218,810 A

α = 11,354 (1/s)

β = 647265 (1/s)

Energy conservation principle is applied. The initial energy contained in the capacitor is as follows where W_i is the initial energy, W_f:is the final energy, C is the capacitance, A_i is the action integral and $R$is the resistance of the test article.

$$W_i = \frac{1}{2}CV^2 = \frac{1}{2}C\,4\times 10^8 \tag{2}$$

The final energy is as follows:

$$W_f = A_i \times R = 2.5\times 10^6 \times 0.05 \tag{3}$$

Since

$$W_i = W_f \tag{4}$$

And

$$C = \frac{2.5\times 10^6\times 0.05}{2\times 10^8} = 6.25\times 10^{-4} = 625\ \mu F \tag{5}$$

Based on the calculated values, iteration was performed to get the value of α. With α = 9150, action integral = 2,507,184 was obtained which met the requirement. The component A waveform is plotted in Fig. 55 and is illustrated in Fig. 56: The design of waveform does not have to be done every time a test is conducted. However, in our work, we are establishing a risk analysis model and one of the steps is to gather all the background information necessary, thus it helps to understand the details of lightning waveforms. It also increases our understanding of the test and possible pitfalls of the test so that a proper testing can be conducted.

6.2 Lightning Test Background

One of the lightning hazardous conditions is corrosion on fuel tank access door components. Thus corrosion represents the driver for the event of lightning damage effects. There are other actors for the event, but corrosion is a typical driver and investigating and understanding of corrosion in detail helps with our effort of lightning even risk mitigation. Corrosion present high impedance path to lightning currents and possible explosion condition to the fuel tank. The fuel tank access door components include access plates, gaskets, fasteners, plate cut-outs, clamp-rings, and the wing skin. Special attention was placed on gaskets and fasteners since they are susceptible to corrosion and they could be the factors in the ignition of the fuel tanks. The lightning current affects the fuel by conducted currents in general rather than the direct strikes due to the fact the fuel tanks are located in zone 3 defined in Chapter 5.

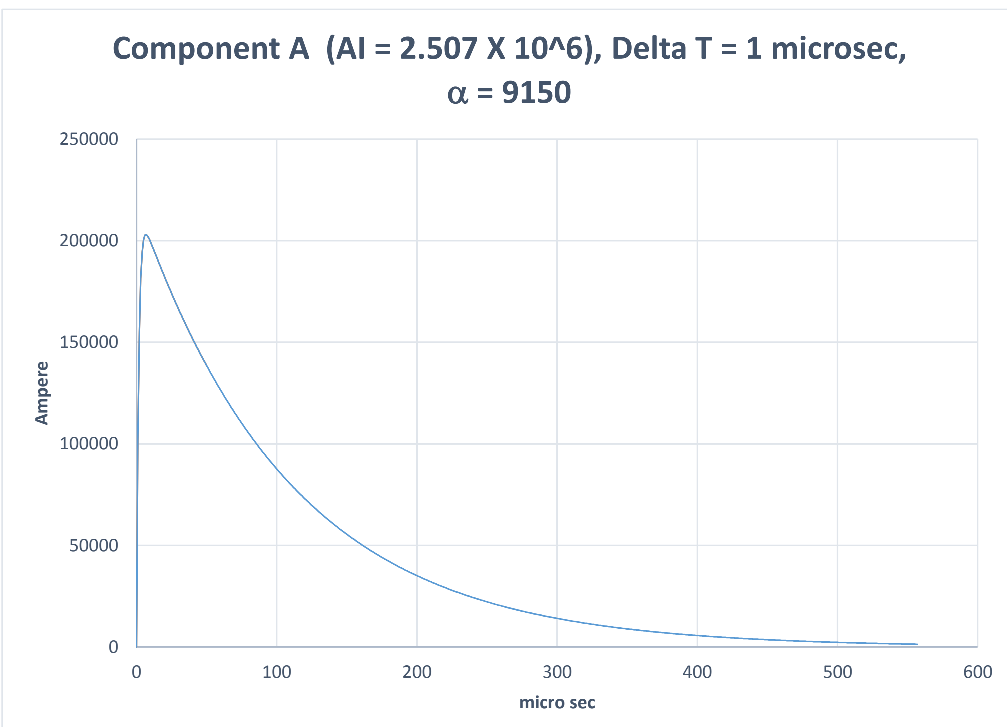

Figure 55. Design of lightning waveform for component A

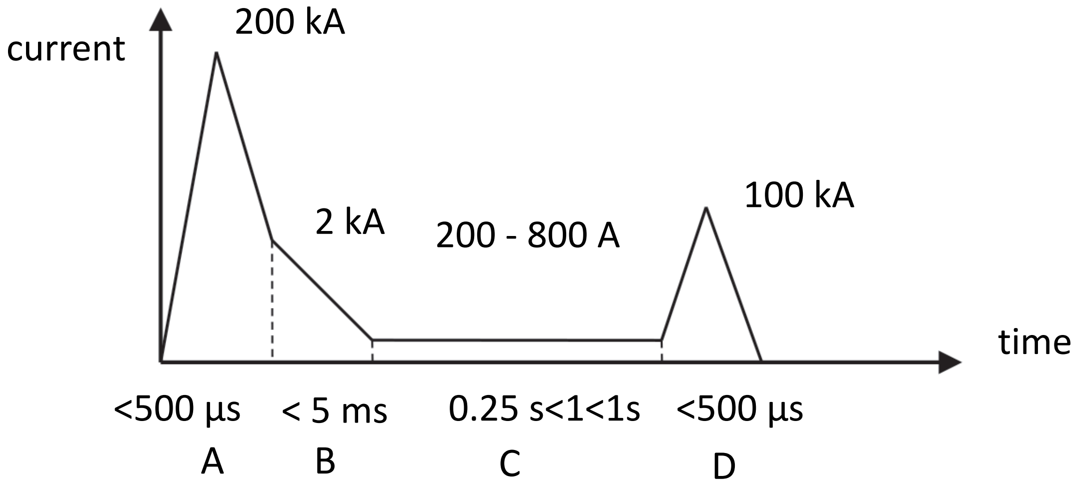

Figure 56. Lightning current waveform as a function of time

The standard risk model technique with event driver analysis has determined that the corrosion was caused by moisture ingress into the fuel access door and skin interface, which was attributed to the gasket not providing a durable moisture barrier over time in this dynamic environment. To address corrosion issues, the risk analysis and mitigation technique proposed a revised fuel access door assembly that incorporates a new fuel door gasket with an improved moisture seal material and profile. Further research indicated the Mobilgrease 33 material. This new mesh filling material was chosen based on extensive testing and it provide better corrosion resistance than the currently used gasket filling material. This new mesh filling Mobilgrease 33 material that has corrosion-inhibiting and lubricating properties along with a new rubber seal material and profile. This new gasket was determined to provide better corrosion protection than the current gasket. The gasket includes rubber around each of the attach fastener locations instead of mesh grommets. The mesh has been reduced to a single layer while maintaining the same thickness. The profile of the rubber seal part of the gasket has been increased in thickness and includes a bead to help seal out moisture. The seals are made from a new harder rubber material. The test objective is stated in italics:

"*The objective of this testing was to demonstrate that the installation of the fuel access doors with new gasket will not cause sparking within the fuel tank when Zone 3 lightning currents pass through this region.*"

6.3 Test Approach

This lightning-conducted current test was conducted in accordance with the Aerospace Recommended Practice (ARP) 5416 Rev New "Aircraft Lightning Test Methods [124]." Testing utilized production parts installed in sections of wing skin representing the actual installation. Several small sheet metal parts were fabricated and a test fixture was built to secure the test articles. The panel backside, installed in a light-tight box, was monitored for arcing/sparking by cameras recording absence or presence of light. Two fuel door sizes were tested, 8x18 and 10x18. Each door assembly used a new gasket with the new mesh filling material. The two test assemblies, one for each fuel door size were subjected to a reduced Zone 3 current level. The magnitude of the reduced current level was determined by the ratio of the full Zone 1 current level times the ratio of the wing cross sectional area at the fuel access door location to the test panel cross sectional area. Each of the test assemblies were subjected to one test shot except the high impact door configuration which was subjected to five shots. The test report gives a detailed description of this test.

6.4 Test Panel Configuration

The test fixtures for each of the two sizes of fuel door configurations were made from sections of the lower skin panel assemblies from the following locations. Fig. 57 shows a typical fuel tank door which was used for the testing.

Figure 57. Typical fuel tank door configuration

1. 10x18 high impact doors used between Ribs 3-6, regular doors used between Ribs 7-17
2. 8x18 doors used between Ribs 17-23 and 24-25

Each of the test fixtures were engineering supplied test parts and were made from sections of wing skin assembly approximately 20” wide by 24” long with a machined opening for a 10” x 18” or 8” x 18” fuel access door. The fixtures were made from scrapped wing skin assemblies from the wing factory or salvaged from airplanes in the fleet.

6.5 Conformity Test

For each of the test assembly, conformity was tested for the following items:

(1) Verification that FAA Form 8130-3 is completed for each test gaskets prior to their use in testing.
(2) Verification of fuel door part numbers.
(3) Verification of clamp-ring part numbers.
(4) Verification of assembly bolt part numbers.
(5) Verification that the skin sections (fixtures), fuel doors, and clamp-rings contact surfaces are clean.

(6) Verification the laminate sheet configuration requirements.

(7) Verification of door assembly.

(8) Verification of torqueing of bolts.

(9) Verification that the final test article (fixture, fuel door, clamp-ring, gasket and required laminate sheet) is mounted to a light-tight chamber.

(10) Verification of requirements of photographic testing for all test configurations.

6.6 Test Procedure

The test was performed in the Lightning Lab which has the capability of delivering the current waveforms specified in ARP 5412B Aircraft Lightning Environment and Related Test Waveforms [125]. Test panels were mounted on a shielded light-tight test chamber and conducted currents applied through the panels. The shop removed panel finishes to provide grounds as needed. Cameras recorded absence/presence of sparking on back side. These tests were performed at room temperature. The test panels were mounted on the test chamber on a nonconductive back plane. The generator output was attached to the test article as shown, so current was driven into the edge of the test article, the generator return was attached to the opposite side. Cameras recorded the absence/presence of sparking on the back side of the test panels. Test levels were appropriate for Zone 3; i.e., reduced waveforms, A + C per ARP 5412B Aircraft Lightning Environment and Related Test Waveforms. Each test panel, referred to as Unit Under Test (UUT), was mounted on a light- tight chamber provided by the laboratory. The chamber provides a conductive enclosure that represents surrounding substructure and a shielded enclosure to simulate the wing interior

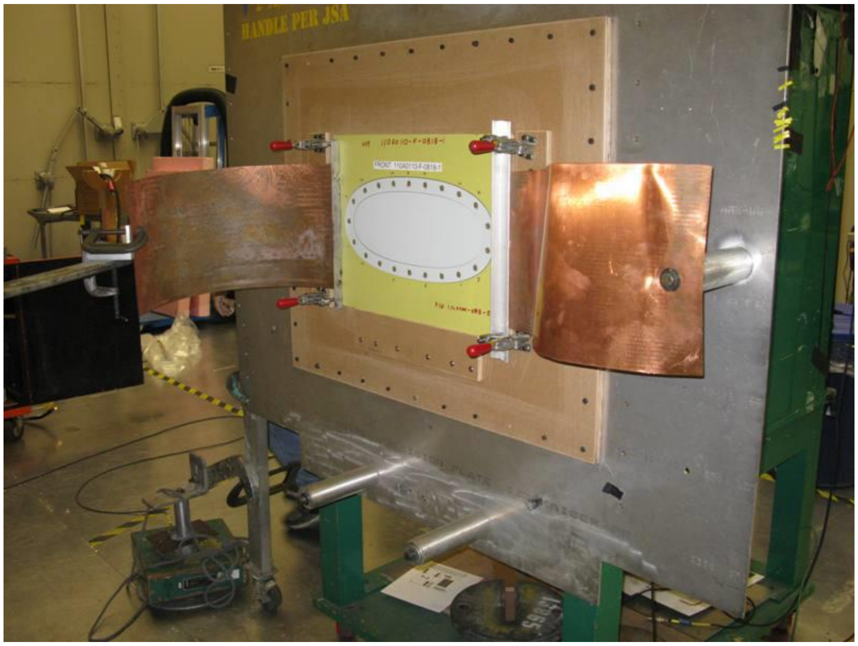

Figure 58. Test setup front view

environment. The test chamber has been designed to allow flexibility to adapt to various panels sizes. UUT is measured approximately 20 x 24 inches.

Prior to mounting the UUT on the light-tight chamber shown in Fig. 58, Fig. 59 and Fig. 60, these steps were followed:

- Resistance measurements were made from panel to access door on each UUT.
- The UUT was visually checked for any surface abnormalities.
- Pre Test photos were taken of both sides and recorded.
- Ground shots were taken to establish the required waveform.
- A verification (calibration) shot, for each new current probe setup was conducted with current probe cables disconnected from the probes, terminated in 50 ohms, and their outer conductor connected to the probe connector outer conductor. The oscilloscopes measured

and recorded the system noise level and confirm absence of significant stray current in the instrumentation.

Figure 59. Test set up inside view

Figure 60. Test set up side view

6.7 Test Conduction

Test conduction proceeded as follows:

(1) UUT was mounted on the light-tight chamber. Position of the UUT, vertical or horizontal, was shop discretion.

(2) No internal mirrors were arranged to view the test from various angles.

(3) Standard blackout checks using a strobe or similar with camera lenses open were run to show that the box is free of light leaks.

(4) Attached the generator output so the current was driven into the edge of the UUT. Attached the generator return in the same way but on the opposite side. The UUT was mounted on a non-conductive mounting plate.

(5) The UUT was subjected to a reduced Zone 3 current level. The magnitude of the reduced current level was determined by the full Zone 1A current level times the ratio of the UUT cross sectional area to the wing cross sectional area at the fuel access door location times 2.

(6) The following explains the test criteria and current levels methodology for the 8 x 18 fuel access doors:

a. Base on Zone 1A 200kA current level.

b. Wing minimum cross sectional area at Rib 25 including spar webs and upper and lower skins is 8.8 in^2.

c. UUT cross sectional area including the lower wing skin between stringers 6 and 8 (including the stringer lands) is3 in^2.

d. Drive is ratio of the UUT cross sectional area to Wing cross sectional area (0.34) times 200kA (68 kA) times 6db safety factor gives 136 kA.

e. Pass Criteria is there is no light on film.

(7) For the 8x18 access door, conducted current tests waveforms A, C were used.

The following explains the test criteria and current levels methodology for the 10 x 18 fuel access door tests:

(1) Base on Zone 1A 200kA current level.

(2) Wing minimum cross sectional area at Rib 17 including spar webs and upper and lower skins = $21.88\ in^2$.

(3) UUT cross sectional area including the lower wing skin between stringers 6 and 8 (including the stringer lands) = $4.0\ in^2$

(4) Drive is ratio of the UUT cross sectional area to Wing cross sectional area (0.18) times 200kA (36.56 kA) times 6db safety factor = 73.13 kA.

(5) Pass Criteria = no light on film

For the 10x18 access door, conducted current tests waveforms A, C were used. Test levels are +/- 10%. Verifying protection layers at these current levels was achieved by modifying the UUT by isolating approximately 50% of the door contact area with BMS7-335 Type VI grade B laminate sheet and loosening all the door fasteners 1/2-5/8 turn. In the event of a failure in this configuration, an unmodified UUT would be tested. Two Polaroid and one digital camera were set up to record any possible light within the box. A fast development type film, such as, Fujifilm FP3000B with 3000 ASA was used. The Polaroid cameras were set for F4.7 aperture, and were placed so that the lens was no more than 1.5 meters from the fuel door test panel being tested, as specified in SAE ARP5416. Following standard safety procedures, the appropriate capacitor bank was charged to the required level and fired. Immediately after the application of each waveform set, camera shutters were closed and followed by a review of Polaroid exposures and digital images. Any light observed on the photos was immediately reported to engineering. There were no failures to be reported to the EME AR. Waveforms were recorded and reviewed using the standard data acquisition system. Electronic versions were also maintained for later review. A detailed log was maintained that records plots and statistics for all shots taken. Resistance measurements were made at the completion of all the tests for that panel. Photos were taken of any unusual detail post test. Post Test Photos of the UUT were taken and documented. All tested panels are retained for disposition by Structures and EME engineering

6.8 Test Pass Fail Criteria

The test success criterion is no sparking and/or arcing within the light tight test chamber as shown in Fig. 61. Any detectable light on both Polaroid cameras would be a test failure. Detectable light on the digital camera was used as a means to confirm a failure, if light only shows on one Polaroid camera film. If light is observed on only one Polaroid camera film, then it was interpreted as a defect on the fast development type film.

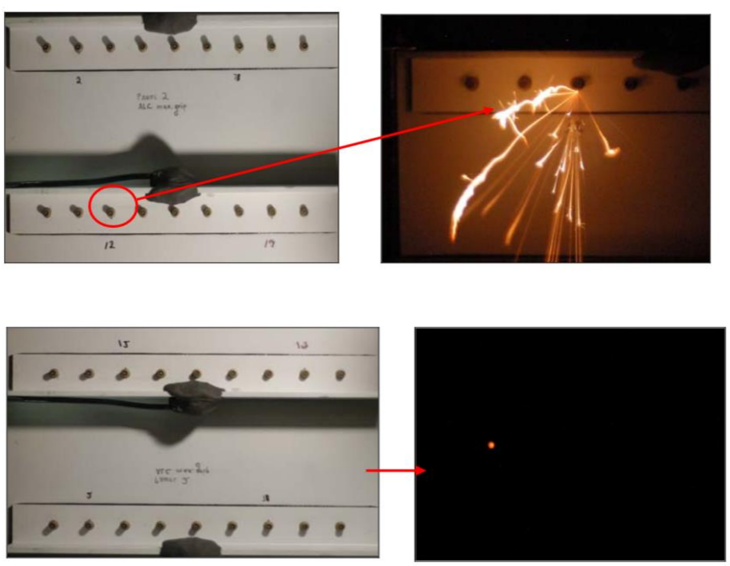

Figure 61. Test pass or fail criteria of light on film (LOF)

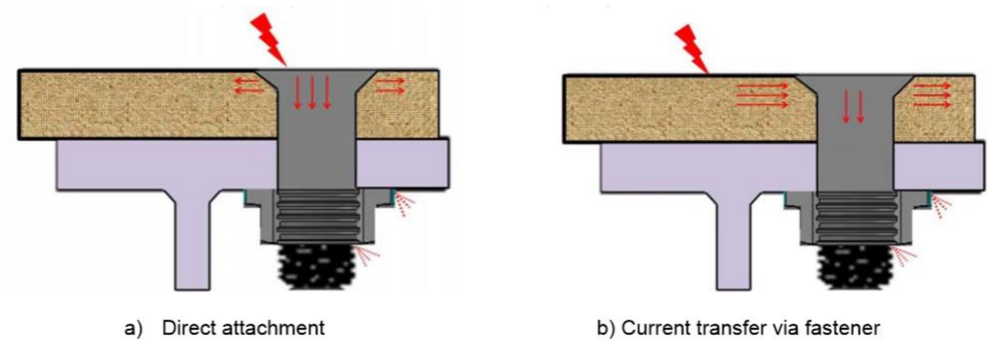

Figure 62. lightning attachment and ignition mechanism

The light on film mechanism is shown in Fig. 62 and Fig. 63. A direct current attachment and indirect current attachment are shown in Fig. 62. The arcing mechanism is shown in Fig. 63 where thermal sparking, outgassing and edge glow mechanisms are illustrated. Sparking occurs when there is an electrical breakdown of a gas that produces electrical discharge. The current through a normally nonconductive medium such as air produces a plasma and the plasma acts as a conductive path for arcing to occur.

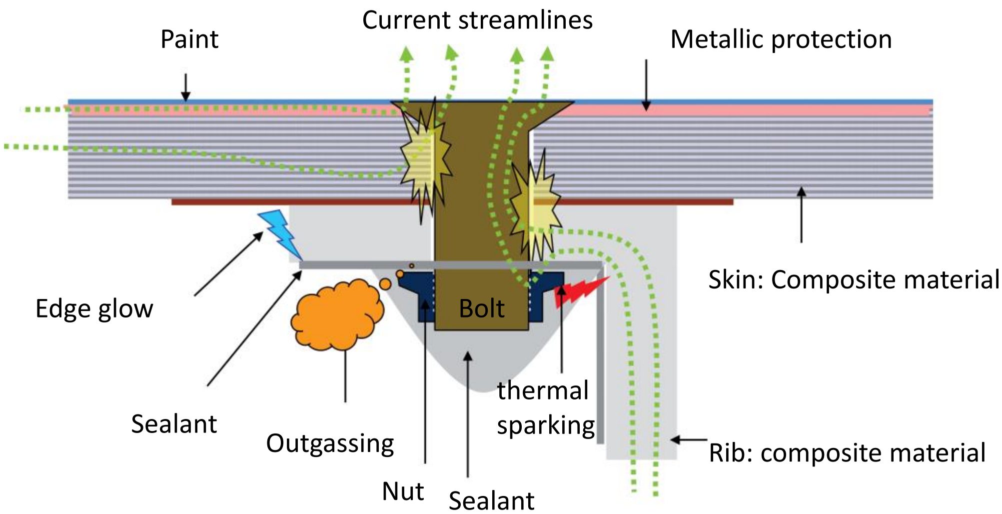

Figure 63. Sparking mechanism due to lightning current

6.9 Test Results

This test result includes all sections of the plan/procedure, a section of test results, and a section entitled conclusions. This section contains a summary of the test results with raw data included in the appendix. The data from the test equipment log and all FAA conformity documentation are also included in the appendix of this section. Three test assemblies for the 8 x 18 access door and three for the 10 x 18 access door were available for this test. Test Panels received one shot per panel. Pre and Post Test photos and resistance measurements were made and recorded. A ground shot and noise shot was performed and the test setup was conformed. The test panel to ground resistance measurement was made and recorded in the log book and setup photos were taken. The test levels were per the test plan. There were no failures to this first group of five test panels. The tested panels were returned to the shop for disassembly. Two 8 x 18 and three 10 x 18 test assemblies were reassembled, conformed and were labeled correctly. Test Panels received one shot per panel. Pre and Post Test photos and resistance measurements were made and recorded. A ground shot and noise shot was performed and the test setup was conformed. The test panel to ground resistance measurement was made and recorded in the log book and setup photos were taken. There were no failures to this second group of four test panels. Panel A (high impact fuel access door configuration) received five test shots. Pre- and post-test photos and resistance measurements were made and recorded. A ground shot was performed and the test setup was conformed. The test panel to ground resistance measurement was made and recorded in the log book and setup photos were taken. The test levels were per the test plan. There was no failure to both test panels. This null results represent successful outcome of the risk mitigation steps taken during this design and testing investigation.

6.10 Chapter Conclusions

The risk analysis and mitigation procedures are followed to investigate the mechanisms, causes, and prevention of possible fuel tank explosion risk. The driver-event analysis as developed in Chapter 3 and demonstrated in Chapters 4 and 5 are applied to the fuel tank doors. The drivers are identified to be corrosion of gaskets and fasteners. Thus the risk mitigation measure of having the fuel tank door free of corrosion is addressed with the risk model. The risk was viewed from the systems engineering point of view in the manner elaborated in Chapter 1. The standard risk modeling developed in Chapter 3 was used to identify, analyze the risk, develop mitigation techniques, and was verified by conducting a testing. This testing has demonstrated that the installation of the fuel access doors with the new gasket mesh filling material is the desired solution. The new material has corrosion-inhibiting and lubricating properties along with a new rubber seal material. The new gasket will not cause sparking within the fuel tank when Zone 3 lightning currents pass through this region even with a reduction of the electrical contact area and with all installed fasteners under torqued. In addition to the specific value obtained from this risk mitigation technique via testing, our motivation was to show how the overall risk analysis and mitigation approach works in combination with an actual testing in the lab as demonstrated in this chapter.

7. Validation of the Approach

7.1 Introduction

The risk analysis and mitigation model developed in this work has been applied to several situations related to lightning effects. Firstly, work has been done to assess the risk probability of lightning attachment at main wings. This assessment is an important step of the model and it provides the likelihood of the events. A summary list of important probabilities is shown in Table 18. The risk probability may be quantified by several ways. One way is to evaluate the events in the lab. Another way is to calculate the probability. Evaluation of risk level could be a very complicated matter in order to evaluate the fuel tank explosion probability, we need to have the following information.

Table 18. Summary of fuel tank explosion probability

Parameter	Numerical value
Attachment likelihood of lightning on aircraft per year	1×10^{-3}
Attachment likelihood per hour	4.2×10^{-7}
Attachment likelihood at zone 3	1×10^{-3}
Flammability of fuel tank	Variable
Defects on fasteners or gaskets	1×10^{-3}
Top level probability	1.08×10^{-9}

The calculation of the top level probability can be complicated since many factors must be considered. The most efficient way is to use the computer aided fault tree analysis program (CAFTA). In order to analyze the situation in more realistic way, each segments of altitude ranges were considered. Since the lightning strike probability values for each altitude segment are known, the flammability was also calculated over each segment of altitude. Then the lightning probability at each segment was multiplied with the flammability of the fuel tank system for each segment of altitude.

7.2 Lightning Risk Probability Calculation with FTA

It is noted that the probability calculation example shown below from Fig. 64 to Fig. 72 is a typical representation of lightning risk event probabilities for commercial transportation aircraft. Above fault tree calculation shows the probability calculation for the range of 0 ft to 5,000 ft. The top probability for this altitude range is 4.72E-10.

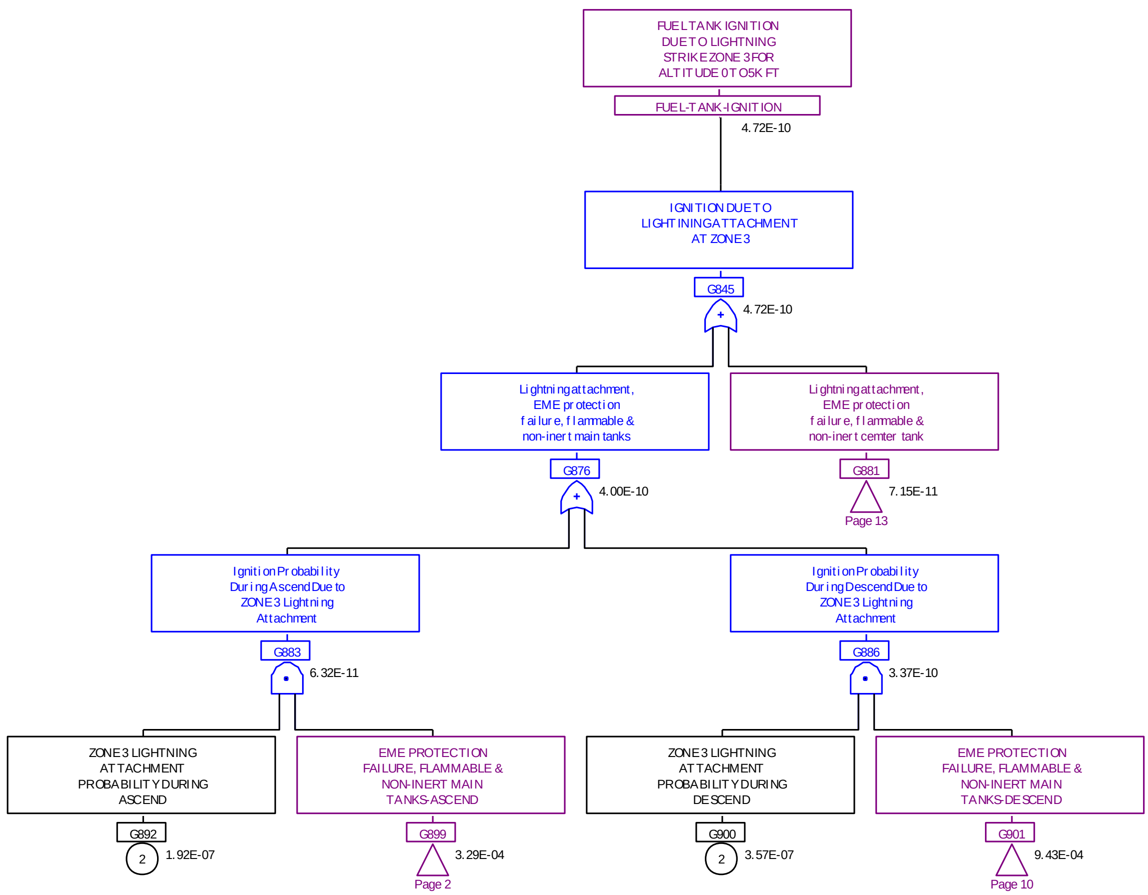

Figure 64. Fault Tree for the altitude range from 0 to 5000 ft

The fault tree in Fig. 65 shows the probability calculation for the range of 5000 ft to 10,000 ft. The top probability for this altitude range is 7.0E-10. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure.

The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system.

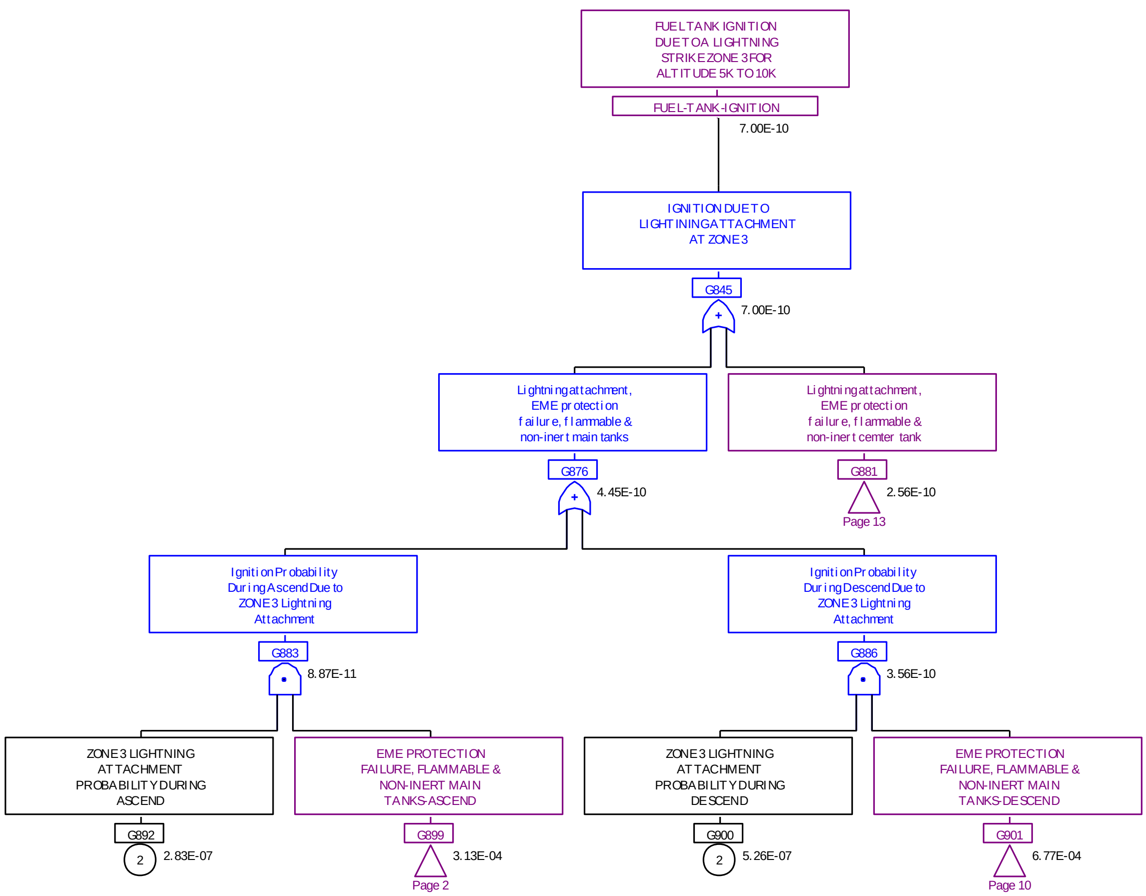

Figure 65. Fault tree for the altitude range from 5,000 to 10,000 ft

The fault tree in Fig. 66 shows the probability calculation for the range of 10,000 ft to 15,000 ft. The top probability for this altitude range is 2.32E-9. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure. The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system.

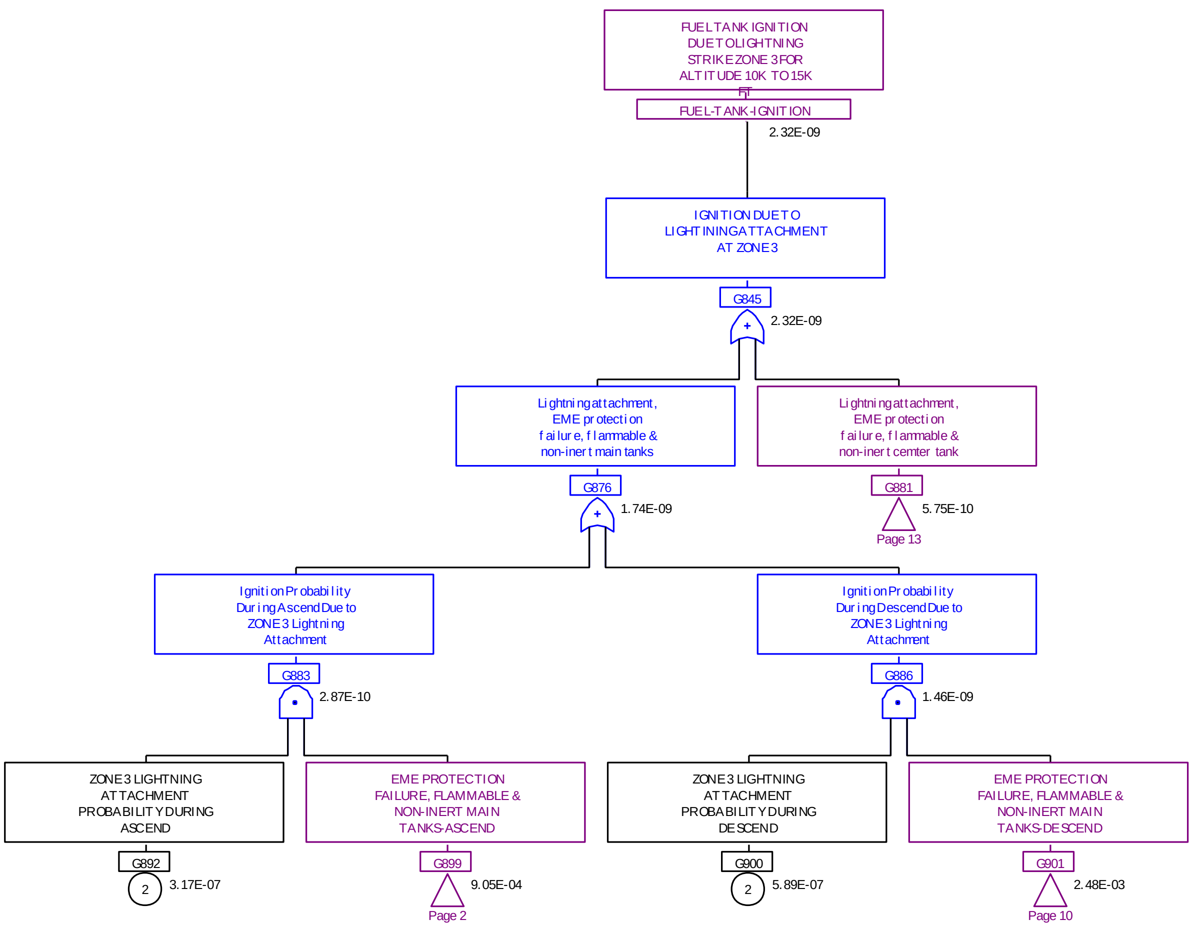

Figure 66. Fault tree for the altitude range from 10,000 to 15,000 ft

The fault tree in Fig. 67 shows the probability calculation for the range of 15,000 ft to 20,000 ft. The top probability for this altitude range is 1.83E-9. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure.

The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system.

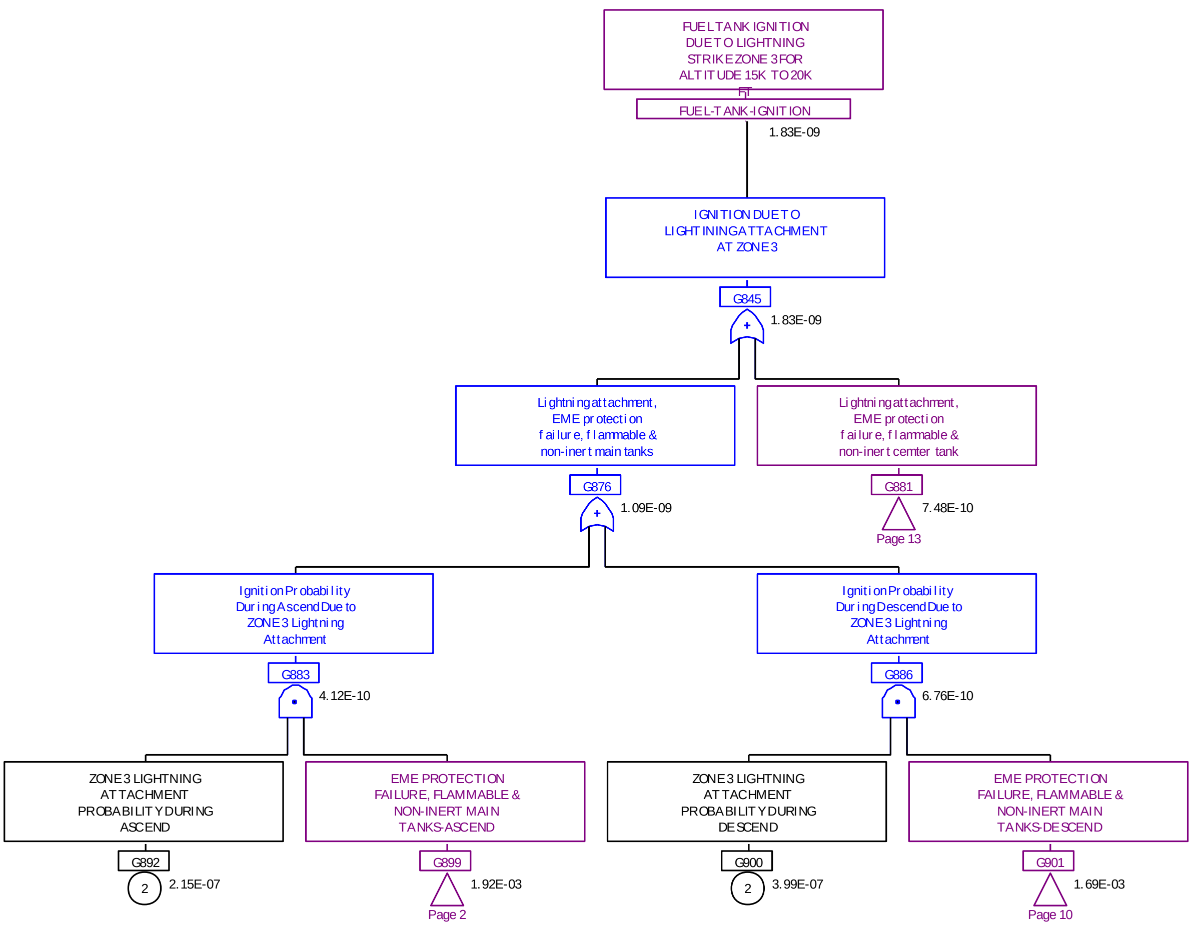

Figure 67. Fault tree for the altitude range from 15,000 to 20,000 ft

The fault tree in Fig. 68 shows the probability calculation for the range of 20,000 ft to 25,000 ft. The top probability for this altitude range is 5.8E-10. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure. The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system. These factors are calculated for different sections of the wings where the fuel tanks are located. Each factor for different sections of the wings are summed up to arrive the final probability numerical values for individual airplane.

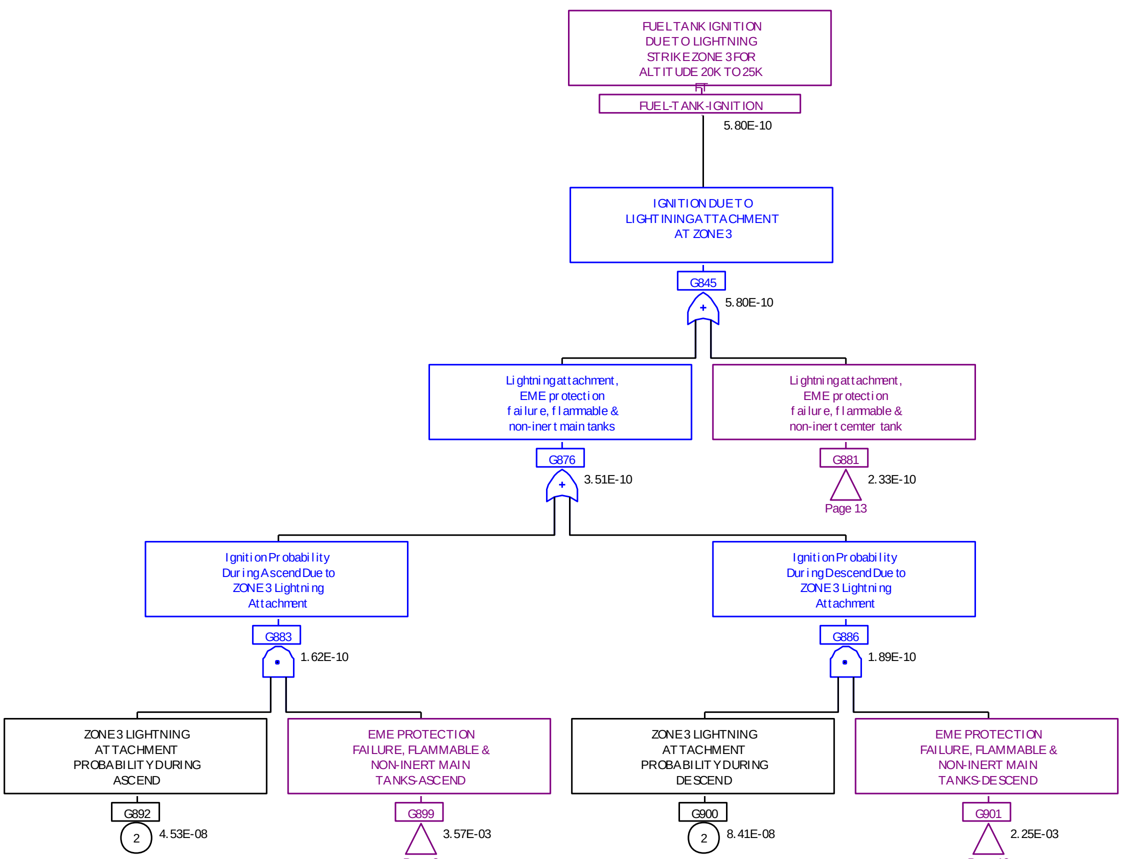

Figure 68. Fault tree for the altitude range from 20,000 to 25,000 ft

The fault tree in Fig. 69 shows the probability calculation for the range of 25,000 ft to 30,000 ft. The top probability for this altitude range is 3.9E-10. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure. The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system.

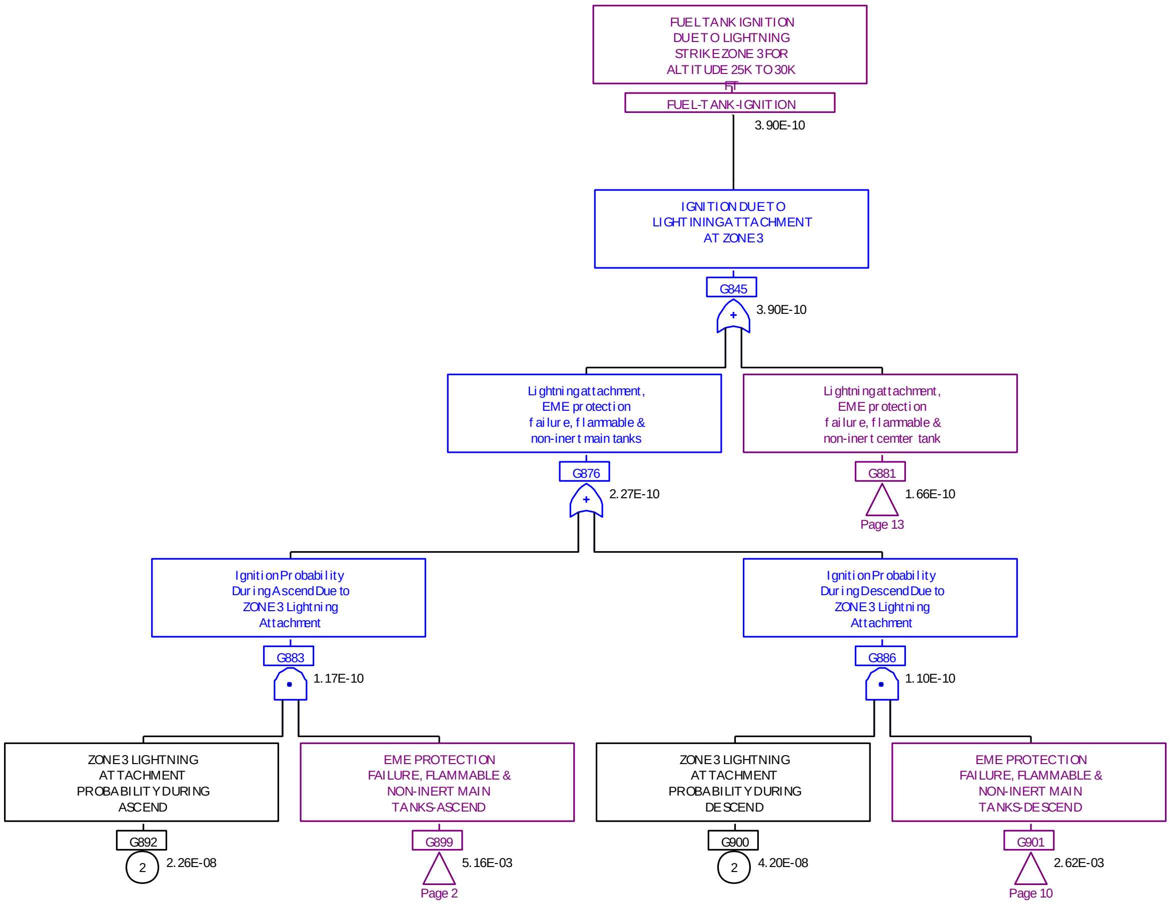

Figure 69. Fault tree for the altitude range from 25,000 to 30,000 ft

The fault tree in Fig. 70 shows the probability calculation for the range of 30,000 ft to 35,000 ft. The top probability for this altitude range is 5.09E-10. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure. The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system.

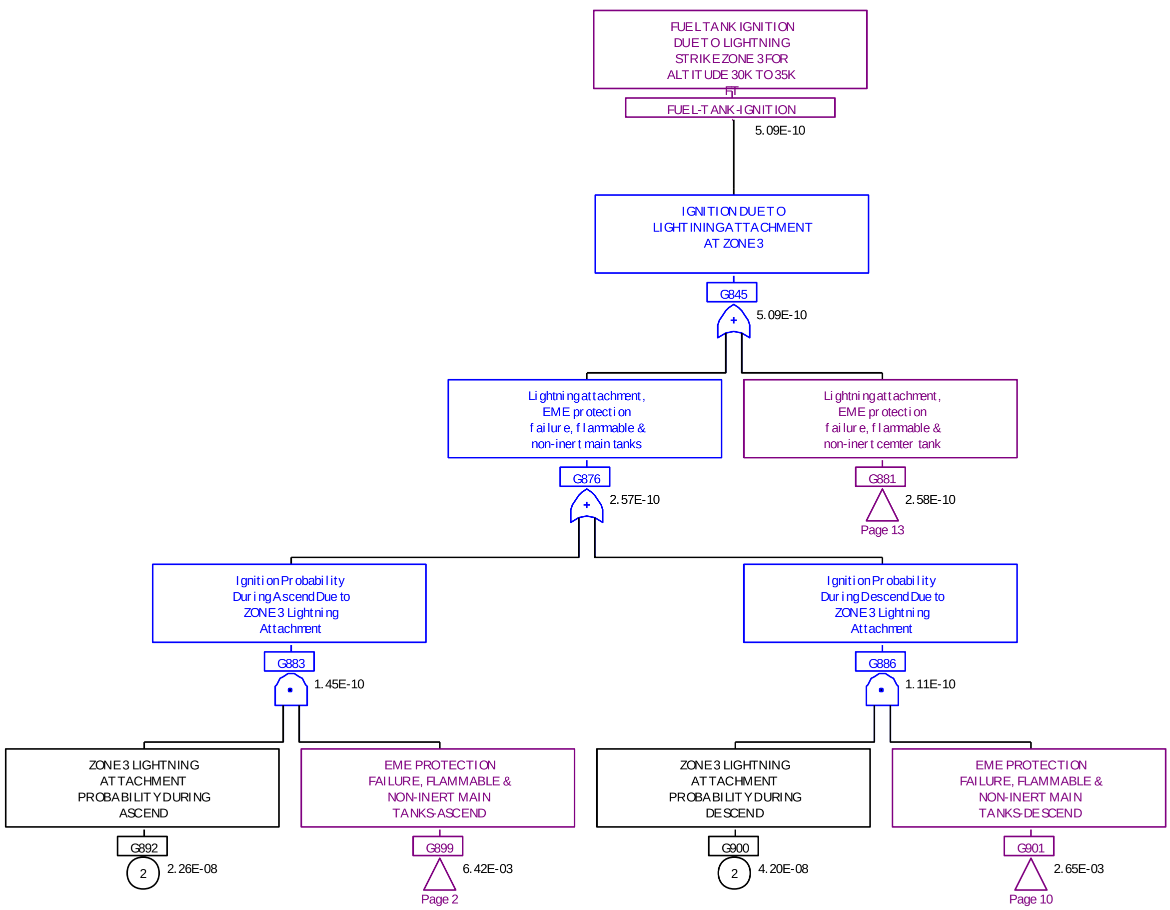

Figure 70. Fault tree for the altitude range from 30,000 to 35,000 ft

The fault tree in Fig. 71 shows the probability calculation for the range of 35,000 ft to 40,000 ft. The top probability for this altitude range is 1.36E-10. This probability is later summed up with the rest of the probability values to get the final individual probability. Note the probability is calculated per flight in this figure. The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system. These factors are calculated for different sections of the wings where the fuel tanks are located. Each factor for different sections of the wings are summed up to arrive the final probability numerical values for individual airplane.

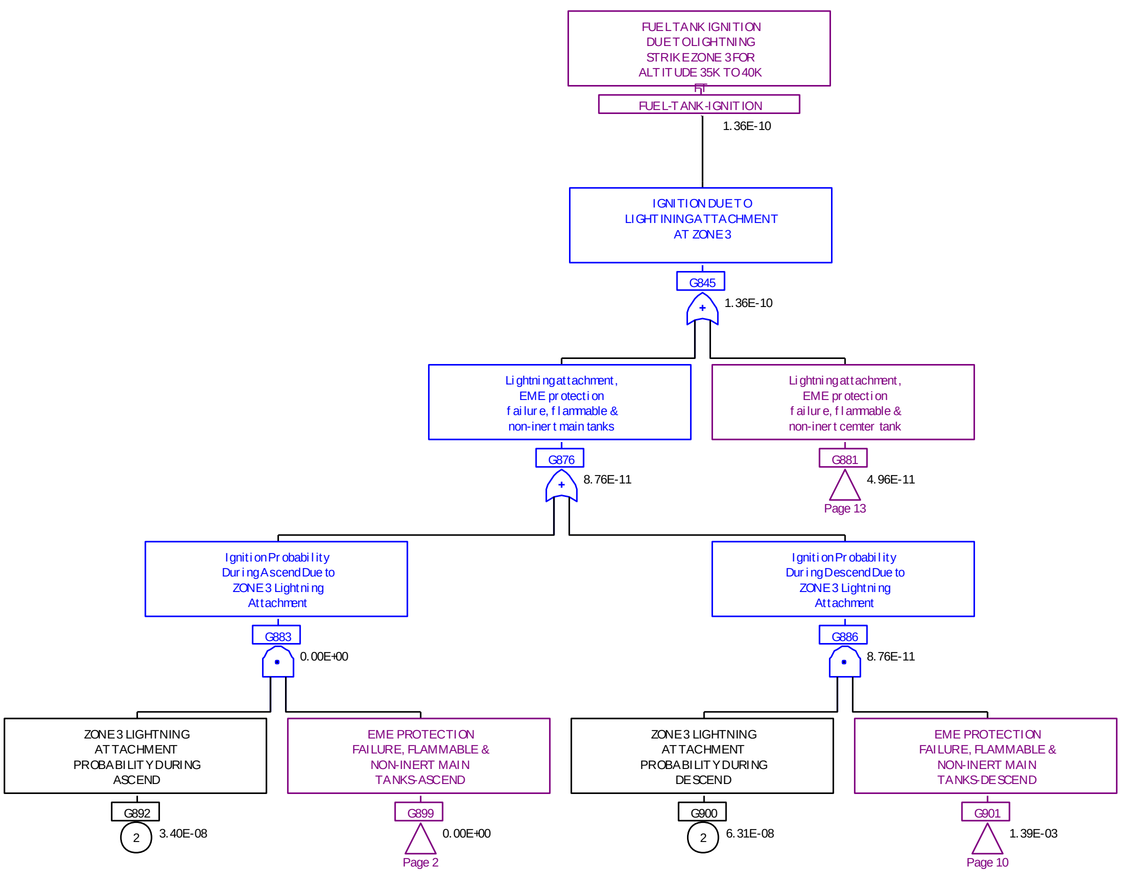

Figure 71. Fault tree for the altitude range from 35,000 to 40,000 ft

The fault tree in Fig. 72 shows the probability calculation for the range of 40,000 ft to 45,000 ft. The top probability for this altitude range is assumed to be zero since there is rarely a lightning strike over this range. Thus this probability does not affect the final individual probability. Note the probability is calculated per flight in this figure. The FTA calculation is done as a combination of the ignition probability during ascent, ignition probability during descent and contributions by the fuel tank being flammable, inadequate protection of fastens and other component around the fuel tank, and inadequate nitrogen generation system. These factors are calculated for different sections of the wings where the fuel tanks are located. Each factor for different sections of the wings are summed up to arrive the final probability numerical values for individual airplane.

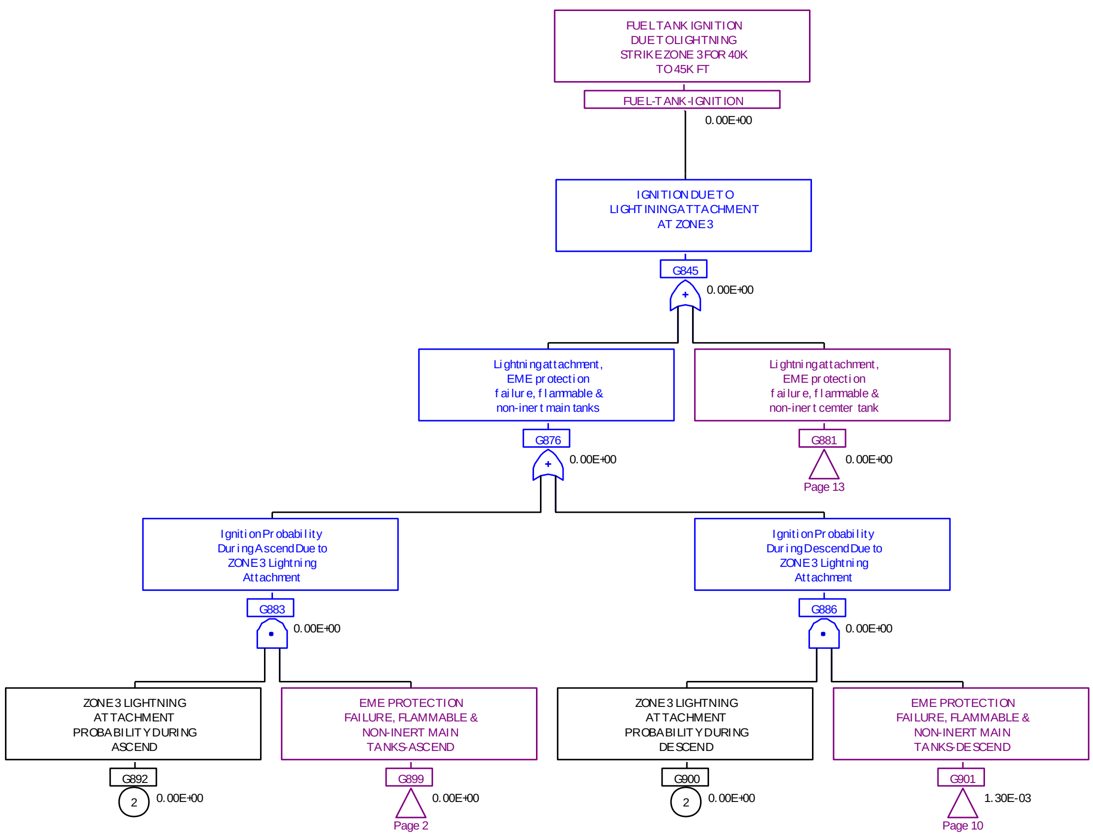

Figure 72. Fault tree for the altitude range from 40,000 to 45,000 ft

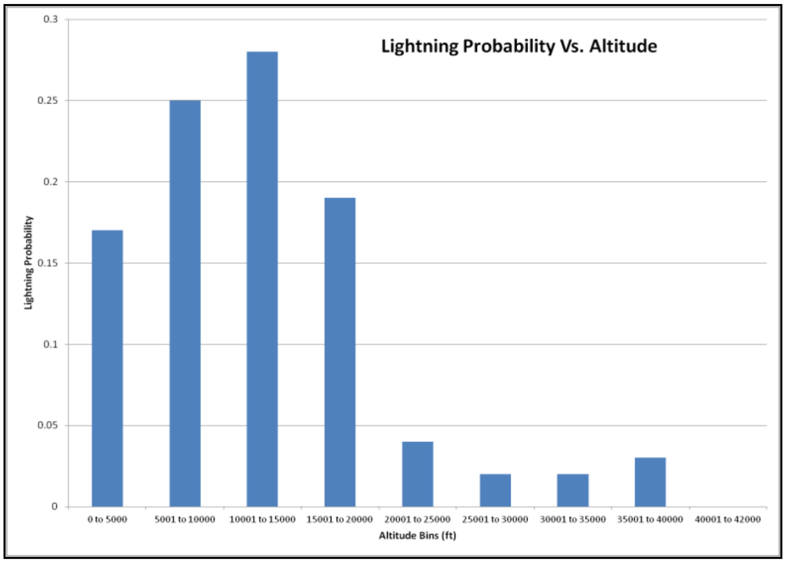

Figure 73. Lightning strike probability distribution over altitude ranges

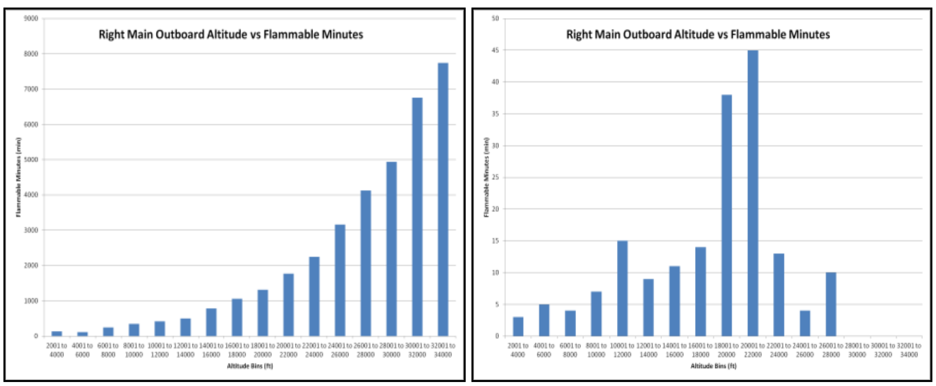

Figure 74. Flammable minutes vs. altitude ranges for right main outboard fuel tank for ascent phase (L) and descent phase (R)

The average lightning distribution is shown in Fig. 73. The average lightning strike distribution is the highest between 10,000 ft and 15,000 ft as shown. The average flammability distribution for the right main outboard fuel tank over the altitude ranges is shown in Fig. 74. The flammable minutes goes up as the altitude goes up. This opposite trend between the lightning probability and flammability implies the actual fuel tank explosion rate is lower than the calculated rate using simplistic assumption of constant lightning probability and flammability. After considerations of flammability, lightning strike probability and FTA calculation of fuel tank ignition with these factors, the final results are shown in Table 19 where the probabilities for each altitude range are summed up to produce the top level fuel tank ignition risk probability per flight and per hour.

Table 19. Top level probability based on altitude range consideration

Altitude range (ft)	Probability (per flight)
0 to 5,000	4.72E-10
5,000 to 10,000	7E-10
10,000 to 15,000	2.32E-09
15,000 to 20,000	1.83E-09
20,000 to 25,000	5.8E-10
25,000 to 30,000	3.9E-10
30,000 to 35,000	5.09E-10
35,000 to 40,000	1.36E-10
40,000 to 45,000	0
Total per flight	6.94E-09 (or 1.08E-09 per hour)

7.3 Risk Resolution Strategies

For the remaining chapter, various risk response strategies are discussed. The risk modeling gives options for difference responses for difference airplane scenarios.

Risks may be accepted if risks are determined to be tolerable and do not affect the safety of the airplanes. Airlines conduct inspection of the surface of airplane if there were reports of lightning strikes. If the inspection does not point out sever damage, the airplane may be dispatched without further repair until the airplane is located at a major repair facility (MRO). Another example of risk acceptance can be cited for a situation where walk around finds missing bonding jumpers. If there are redundant bonding jumpers next to the missing jumper location, the risk may be acceptable on a time-limited basis. The missing jumpers should be restored to the delivery configuration after a limited time elapses.

Risks may be mitigated. Lightning risks while airplane is parked in a tarmac can be mitigated by installing grounding cables. It is observed that the parked airplanes get hit with lightning strikes. Personnel safety may be compromised and airplane may get damaged. Grounding the airplane with cables reduce the risks by providing paths for the lightning currents to flow.

Risks may be acceptable and mitigated for the cases when the airplane is being worked on in the hangar.

Risks may be avoided. As airplanes fly the pre-determined path, if there are storm are reported, pilots may change the path and go around the storms.

Risks may be transferred. For instance, if there is module development that are highly technical, the technical risk may be transferred to the experts who works for suppliers.

Table 20 below summarized this discussion of various risk responses.

Table 20. Risk response strategies

Risk response strategy	**Airplane example**
Acceptance	Lightning inspection, and missing bonding jumpers for dispatch
Mitigation	Grounding while parked on tarmac (1 – 3 points)
Acceptance & Mitigation	Grounding while airplane is being worked on
Avoidance	Flying away from storms, lightning sensing devices
Transfer	Subcontracting to supplier

In the next section, several examples are shown for the risk responses such as risk acceptance, risk mitigation, risk avoidance and risk transfer which are shown in the Table 20.

7.4 Risk Acceptance and Mitigation for Airplane Grounding Policy

While airplanes are worked on for maintenance or repair purposes, questions arise about grounding practices of airplanes for safety. There are at least four situations as follows for grounding considerations:

(1) Risk is accepted when the airplane is parked or is being serviced during turnaround operation. Static grounding of the airplane by positive grounding means is not necessary. This does not include those situations where maintenance activities are being performed in or about the airplane.

(2) Risk is accepted when performing pressure refueling or pressure defueling of the airplane. Static grounding of the airplane by positive grounding means is not necessary.

(3) Risk should be mitigated when electrical bonding between the airplane and the refueling vehicle is required. Static grounding of the airplane by positive grounding means is recommended during overwing refueling or other fuel related activities.

(4) Risk should be mitigated when performing maintenance activities using devices such as lights, power tools, and instruments powered from external electrical power sources. Electrical bonding between the airplane and the refueling source is also required. Static grounding of the airplane by positive grounding means is required.

By having these risk responses in advance, airplane operations on tarmac and in hangar can be conducted efficiently for the optimum safety of airplanes and airplane operations.

7.5 Risk Mitigation by Bonding Jumper Design and Installation

To mitigate lightning and HIRF risks, bonding jumpers shown in Fig. 75 are frequently designed and installed on aircraft. This section covers the design principles for such bonding jumpers for lightning protection purposes.

Figure 75. Connection of the grounding cable from the landing gear to ground post in airport

Let's use 0.25 x 10^6 [A^2 s] for Zone 2 (component D) where the action integral is 0.56 x 10^6 for the 10 AWG wire with cross section 0.0526 cm^2

A design value k is defined and found below where ρ_{20} is resistivity at 20°C, A is the cross sectional area of the conductor in cm^2, I is the current though the conductor in ampere, c is the specific heat of the conductor, D is the density of the conductor in $\Omega{\cdot}cm$.

For copper:

$$k = \frac{0.2389\,\rho_{20}AI}{cDA^2} = \frac{0.2389 \times 1.72{\times}10^{-6}{\times}0.25{\times}10^{6}}{0.092 \times 8.89 \times 0.0526} = 2.387862 \quad (1)$$

$$\Delta\mathrm{T} = \frac{2.387862}{1-0.00393{\times}2.387862} = 2.410483 \quad (2)$$

For stainless steel:

$$k = \frac{0.2389\,\rho_{20}AI}{cDA^2} = \frac{0.2389 \times 72{\times}10^{-6}{\times}0.25{\times}10^{6}}{0.12 \times 7.9 \times 0.0526} = 86.23719 \quad (3)$$

$$\Delta\mathrm{T} = \frac{86.23719}{1-0.001{\times}86.23719} = 94.3759 \quad (4)$$

Although stainless steel or copper can handle this temperature rise, outer jackets may not. Determination of temperature rise on bonding jumpers is used as one of the design criteria.

7.6 Airplane Lightning Risk Mitigation with Multiple Wire Grounding

The bonding jumper design was discussed in the previous section, we want to discuss airplane lightning risk mitigation by using multiple wire grounding. A modeling of this situation is shown in Fig. 76 where the voltage development and temperature rise are the criteria for designing the multiple wire grounding. The voltage development is the result of two factors. The first factor is the inductance. The wire inductance is comprised of self-inductance as shown in equation (5) and mutual inductance as shown in equation (6). Wire resistance shown in equation (7) also contributes to the voltage development.

$$L = \frac{\mu_0}{2\pi}\left[\ln\frac{2h}{r_0}\right] \tag{5}$$

$$M = \frac{\mu_0}{2\pi} ln\left(\frac{d_G}{d_{GR}}\right) + \frac{\mu_0}{2\pi} ln\left(\frac{d_R}{r_{w0}}\right) \tag{6}$$

$$R = \rho l/A \tag{7}$$

Where L is self inductance, h is the distance above ground, r_0 is the radius of the conductor, d_G is the distance between generator and receptor wires, $d_{GR}$is the distacne betgween generator and reference wires, d_R is the distance between reference and test wires and r_{w0} is the raius of wires. ρ is the resistivity, l is the length of the wire, A is the area of the wire cross-section. These three factors in combination contribute to the voltage development as shown in equation (8).

$$V = L_T\frac{di}{dt} + iR \tag{8}$$

The equation (8) shows the totall volatage developed is due to the self inductance, mutual inductance and resistivity. This voltage development is shown in Fig. 76 with OPM modeling. It shows the form where this devlopment occurs, the process of voltage development and the state change in the cable for voltage and temperature.

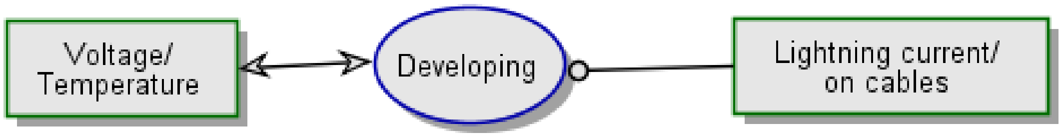

Figure 76. Voltage and temperature development due to lightning current flow on a cable

The voltage calculated is compared to the voltage for arcing condition generally available in literature. Generally inductive component contributes the most to the voltage development while the resistance component is not significant. Thus the length of the cable is a significant factor. Also the number of cables is inversely proportional to the voltage development. N number of cables in parallel will reduce the voltage by the factor N. Thus adequate number of grounding cables can be determined by considering the voltage developed and what is practically possible within the airport environment.

7.7 Risk Deferral with Lightning Damage Inspection

Risk deferral is another one of the risk resolution strategies. As an example for lightning strikes, inspection of aircraft after pilots report lightning strikes can be discussed. Airliners are required to have detailed inspections after pilots' reports. However it takes proper equipment and resources to do the detailed inspection. If initial inspection by binoculars does not show damages, repairs can be postponed for limited time which could be 5 to 10 flight cycles until the airplane is at a MRO (Maintenance, Repair and Overhaul) facility. Risk may be deferred but with some conditions:

(1) Performance of all of the external surface examinations specified, deferring the portion of the examinations of aircraft external surfaces that cannot be accessed above 8 meters.

(2) Supplementing of these inspections with examinations of upper and lower surfaces of all control surfaces and both left and right sides of the vertical stabilizer (including rudder,

rudder tab, and static dischargers) using binoculars from the most advantageous position possible.

(3) The balance of the external surface examinations to be completed within predetermined flights.

7.8 Risk Management of a Fleet as a System of Systems

In this section, we consider the fleet level risk analysis of airplanes. The question whether the fleet level airplanes may be treated as a system of systems (SoS) is also explored. We introduce the concept of system of systems first. It was Kenneth Boulding who used the term SoS first in 1956 in public literature [126]. Boulding imagined SoS as a "gestalt" in theoretical construction creating a "spectrum of theories" greater than the sum of its parts. The term SoS is defined to be a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers emergent activities. A fleet of airplanes is a loosely coupled SoS. A fleet of airplanes meet the SoS criteria because of the fleet actions by FAA and airplane manufacturers. Risk analysis is also done at the fleet level under FAA governance

A fleet of airplanes must meet compliance requirements by FAA for governance but not for management purposes. Fleet level risk or average risk is calculated for average conditions for tens of thousands cases for temperature and NGS availability via Monte Carlo analysis, represented by Risk Associated Compliance Period (RACP) determination. A specific risk is calculated for a single airplane at a specific condition and environment. We note that a fleet of a model (for instance, 777 fleet) is subject to the following activities:

(1) Service Bulletin published by Manufacturers

(2) AD issued by FAA

(3) Fleet Team meetings

(4) Fleet Team exchanges

(5) PEDs regulation is for model fleet

(6) Multi-operator messages

(7) Monitoring by Airplane Health Management System (AHMS) in real time and making parts ready for maintenance before landing

These conditions are the reasons for the possibility of airplane fleet to be a SoS. Airplanes in a fleet do not communicate or interact each other. However, as we will see in the next section, a system could be considered a SoS of loose coupling if there is a purposeful action on the fleet as a whole (collaborative) or each member of the system could participate in certain activities but they may withdraw anytime (virtual SoS of coalition type). The seven activities of a fleet stated above qualify a fleet for collaborative or virtual SoS. Thus a SoS concept is applicable to a fleet of airplanes and the tools available for SoS can be made available for a fleet of airplanes.

DoD system engineering guide in 2008 is shown in Fig. 77. Categories are in order of how tightly coupled the component systems are from loosely to tightly. According to this criteria, the fleet is a collaborative or a virtual SoS: There are purposeful activities for the fleet, but there is no

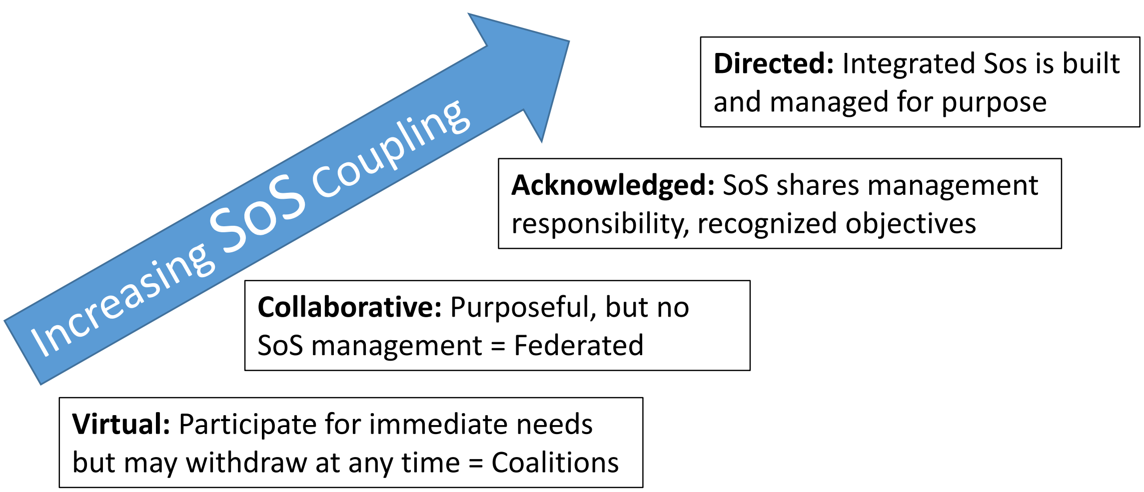

Figure 77. Categories of SoS per system engineering guide

intentional fleet management. Compliance period by FAA AD may be given (collaborative SoS) or compliance could be done at the next opportunity (Virtual). Also the fleet is becoming e-enabled SoS via AHMS. The following seven criteria are generally used for SoS determination [127].

(1) Operational independence of the individual system: Each airplane is a system independently operated by operators.

(2) Managerial independence of the individual system: Each airplane is managed independently by airliners.

(3) Geographical distribution: Airplanes are dispersed geographically.

(4) Emergent behavior: As a SoS, operators attend Fleet Team meetings, interact via Fleet Team exchanges, must incorporate AD related Service Bulletins (FAA requirements for safety related).

(5) Evolutionary development: Fleet is created, they grow and evolve, is modified and ceased.

(6) Self-organization: Fleet is organized loosely by fleet management teams (operators and manufacturers), and they respond to FAA directives.

(7) Adaptation: Fleet adapts to new regulatory requirements (external changes and perceptions of the environment).

Airplane fleet meet these seven categories of SoS determination as a loosely coupled type. Now that SoS characteristics of a fleet is explored, we wish to conduct a risk analysis for a fleet. Up to this point, we have explored risk analysis of at an individual level quite extensively. Now we would like to apply the risk concept at the fleet level. The steps to take for a fleet level risk starts with risk calculation of individual system for a lightning example. We start with the probability calculation for lightning strikes for an airplane and the lightning strike probability for zone 3 where fuel tanks are located. Then lightning probabilities for ascent flight path and for descent flight path are calculated. Then as we discussed earlier in this chapter, the probability for each segment of altitude is calculated. We have subdivided the altitude into nine ranges. This altitude consideration is also applied to the flammability calculation as well. Once the lightning strike probabilities and the flammability of fuel tanks are computed for each altitude segment, the two can be combined for each altitude range and combined to arrive at the top probability. These steps are summarized below.

(1) Lightning strike probability for Transport airplane: typically 0.001

(2) Zone 3 lightning strike probability: typically 0.0033

(3) Lightning Probability during ascent: typically 0.35

(4) Lightning strike probability during descent: typically 0.65

(5) Probability for altitude segment 0 ft to 5000 ft: typically 0.17

(6) FTA produces fuel tank explosion probability: typically 4.72E-10

(7) Add all altitude segments: typically 1.08E-9/hr

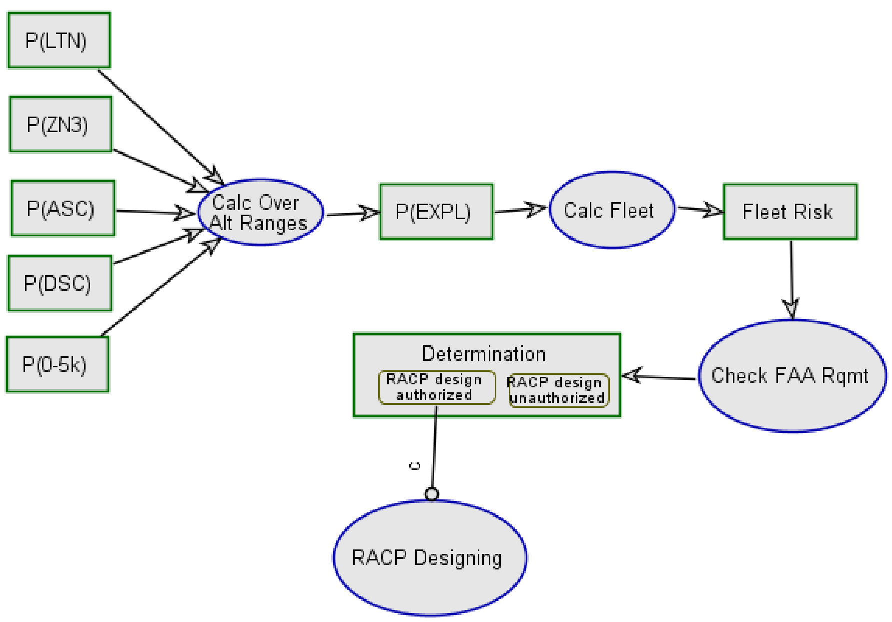

Figure 78. RACP generation flow modeled with OPM informational objects

The process up to this point generates individual risk probabilities. The following steps then generates the fleet level risk based on the individual risk probability.

(1) Obtain the fleet size: an example 143

(2) Obtain the estimated airplane life: an example 82,000 hours

(3) Calculate the fleet life: fleet size multiplied by airplane life

(4) Calculate the risk of accident over fleet life: individual airplane fuel tank explosion times fleet life: an example of the fleet risk 3%

(5) FAA publishes fleet level risk requirement: an example 10%

(6) Calculate the SACT (Service Action Compliance Time) if repair is required

As we noted, the first part of the calculation yields the individual risk. The second part of the calculation yields the fleet risk. By comparing the fleet risk to the requirement risk from FAA, a determination can be made as to the next action. This process is modeled with OPM in Fig. 78. We note that concept can also be an object in the OPM model. It is called informational object in OPM environment. Thus the probabilities can be considered as informational objects. These objects are shown on the left side of Fig. 78. These objects are processed to calculate the individual probabilities. This calculation is a process and shown as an ellipse in Fig. 78. Then the result is process once again by fleet risk calculation process. The fleet risk is evaluated against the FAA fleet requirement and a judgment is made whether we should proceed to RACP design or not. If the judgment is to design RACP, then the service action preparation time and the service action compliance time should be determined. These two time periods in combination are called managed exposure period. The details are shown in Fig. 79.

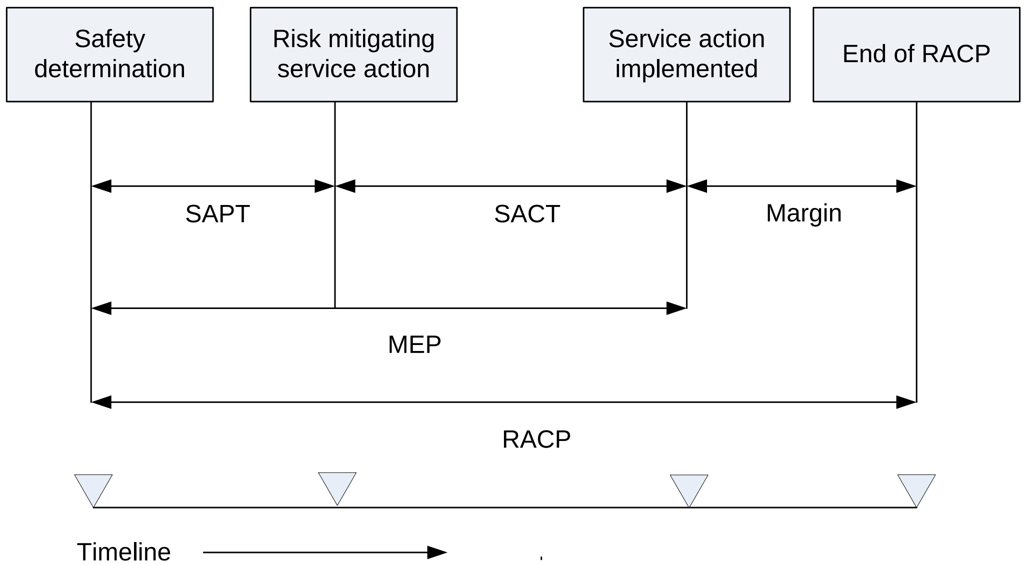

Figure 79. RACP example of airplane fleet as a system of systems

SAPT: Service Action Preparation Time
SACT: Service Action Compliance Time
MEP: Managed Exposure Period
RACP: Risk Associated Compliance Period

7.9 Chapter Conclusions

In order to validate the developed model, several case studies have been conducted in the areas of risk analysis, risk acceptance and risk mitigation. As an example of risk analysis, procedural probability calculation with CAFTA was shown. The features noteworthy was inclusion of altitude factors in the calculation. The lightning probabilities were calculated for each range of altitude and later they were summed to get the final probabilities.

For risk acceptance case study, lightning strike damage inspection was considered. Although a pilot may report lightning strike incidents, if preliminary inspections show there are no noticeable damages, the airplane may be dispatched until the airplane flies to a major repair facility. In other words, we accept calculated risks.

For risk mitigation case study, grounding cable design was considered. The voltage development factor due to lightning current flow and the temperature rise factor should be considered to arrive an optimum number of grounding cables. If the temperature rise does not exceed the melting point of materials for cables including outer jacket and the voltage development does not exceed estimated maximum level of voltage due to lightning, it will be acceptable. As the number of cables increases, the total inductance decreases and the voltage developed will decrease. The same logic applies to resistance as well, which contributes to the voltage development and the temperature rise.

Another example of risk mitigation was for the fleet level risk. Fleet may be considered to be a system of systems of loose coupling. Once the individual risk was calculated, the fleet level risk can be calculated by multiplying the individual probability and the total fleet flight hours. Typically FAA requires a fixed number for the fleet risk such as 10%, so the question whether risk mitigation should occur in the form of repair may be determined with the fleet risk calculation. If it is determined that repair is necessary, a risk associated compliance period should be designed. This enables engineers to practically address the fleet level risk. The risk associated compliance period is consisted of service action preparation time (SAPT), service action compliance time (SACT), and a period for margin. When the safety determination is made the service action preparation time (SAPT) starts. When the fully mitigating service action is issued, the service action preparation time ends and the service action compliance time starts. The service action preparation time and service action compliance time together are called managed exposure period (MEP). The managed exposure period and the margin together are called the risk associated compliance period, which is shows diagrammatically in Fig. 79.

8. Summary and Conclusions

This work is concerned with the system level risk analysis of electromagnetic and lightning effects in aircraft systems. The purpose is to add rigor to the risk analysis methodology and to provide details of how system level risk analysis may be done. In order to achieve the goal, following measures have been taken:

1. Discussed the general emergence theory and the engineering emergence theory
2. Viewed the system level risk as an emergent property of a system
3. Developed extended SAI method for ilities translation to subsystem level
4. Developed additional system architecture principles for more effective systems thinking
5. Utilized the systems engineering approach for the E^3 and lightning effects via risk analysis
6. Applied Object Process Methodology to E^3 and lighting risk analysis and resolution
7. Examined the fleet level risk and presented risk associated compliance period estimation method

The result was the development of a risk management approach which may be streamlined and used for engineering product development and service engineering over lifecycle.

Integrated approach developed in this work would benefit aerospace organizations in terms of reducing cost and schedule and enhancing the quality and safety of aircraft.

This research focused primarily on electromagnetic risk management in aircraft. Additional work is required to apply this approach to other areas such as communications and navigation avionics, power systems, and electrical wiring interconnect systems.

9. References

[1] F. A. Fisher, J. A. Plumer and R. A. Perala, *Lightning Protection of Aircraft*, 2nd ed., Lightning Technologies Inc., 2001.

[2] E. Genender, H. Garbe and F. Sabath, "Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level," IEEE Transactions on Electromagnetic Compatibility, vol. 56, no. 1, pp. 200-207, February 2014.

[3] F. Sabath, Ultra-Wideband, Short-Pulse Electromagnetics, vol. 10, F. Sabath and E. L. Mokole, Eds., New York: Springer Science, 2014, pp. 265-278.

[4] K. Armstrong, "EMI Risk Analysis," IEEE In Compliance, 1 August 2011.

[5] K. Armstrong, "Opportunities in the Risk Management of EMC," in IEEE International Symposium on Electromagnetic Compatibility (EMC), 2011.

[6] I. Moir and A. Seabridge, *Aircraft Systems Mechanical, Electrical and Avionics Subsystems Integration*, 3rd ed., Wiley, 2008.

[7] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed., Prentice Hall, 2011.

[8] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, 2nd ed., Wiley, 2011.

[9] N. P. Whitehead, W. T. Scherer and M. C. Smith, "Systems Thinking about Systems Thinking," IEEE Systems Journal, vol. 9, no. 4, pp. 1117-1128, December 2015.

[10] Aristotle, *Metaphysics*, New edition, Penguin Classics, 1999.

[11] C. W. Johnson, “What are emergent properties and how do they affect the engineering of complex systems?” Department of Computing Science, University of Glasgow, Scotland, UK, web address: http://www.dcs.gla.ac.uk/~johnson

[12] M. Bedau, “Downward causation and the autonomy of weak emergence,” *Principia*, Vol. 6, No. 1, 2002, pp. 5-50.

[13] C.W. Johnson, “What are emergent properties and how do they affect the engineering of complex systems?” Reliability Engineering and Systems Safety, vol. 91, no. 12, pp. 1475-1481, Dec. 2006.

[14] Deguet, Y. Demazeau, L. Magnin, “Elements about the emergence issue: A survey of emergence definitions,” Complexus, 2006, Vol. 3, pp. 24-31.

[15] R. Gore, P.F. Reynolds, Jr., “An exploration-based taxonomy for emergent behavior analysis in simulations,” Proceedings of the Winter Simulation Conference, Washington DC, Dec. 2007, pp. 1232-1240.

[16] C. Szabo, Y.M. Teo, G.K. Chengleput, “Understanding complex systems: Using interaction as a measure of emergence,” Proceedings of the Winter Simulation Conference, Savanah, GA, Dec. 2014, pp. 207-218.

[17] J. Crutchfield, “Is anything ever new? Considering emergence,” Santa Fe Institute Working Paper #94-03-011, 1994

[18] P. A. Corning, “The re-Emergence of Emergence. A Venerable Concept in Search of a Theory,” Complexity, 7 (6): 18-30, 2002.

[19] G. Galilei, *Dialogues Concerning Two New Sciences*, 1638, Dover Books on Physics, 1954.

[20] H. Petroski, *Design Paradigms*, 1994.

[21] S. Ferreira, M. Faezipour, H. W. Corley, "Defining and addressing the risk of undesirable emergent properties" IEEE International Systems Conference (SysCon), 2013.

[22] J. Black, P. Koopman, "System Safety as an Emergent Property in Composite System," International Conference on Dependable Systems and Networks, 2009

[23] A. Vinerbi, A. Bondavallli, P. Liollini, "Emergence: A New Source of Failures in Complex Systems," IEEE The Third International Conference on Dependability (DEPEND), 2010.

[24] S. Ferreira, M. Faezipour, H. W. Corley, "Defining and addressing the risk of undesirable emergent properties" IEEE International Systems Conference (SysCon), 2013.

[25] INCOSE, *Systems Engineering Handbook*, 2015.

[26] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Chapter 3, Unpublished.

[27] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Unpublished.

[28] IEEE Std 61-12-1990 (R2002) *IEEE Standard Glossary of Software Engineering Terminology*.

[29] ISO/IEC/IEEE, *International Standard, Systems and Software Engineering Vocabulary*, 1st ed., 12-15-2010.

[30] C.H. Dagli, N.Kilicay-Ergin, "Systems of Systems Architecting," Chapter 4 in System of Systems Engineering, ed. M. Jamshidi (Hoboken, NJ: John Wiley & Sons: 2009), p. 77.

[31] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Unpublished, p. 1-13.

[32] E. Crawley, B. Cameron and D. Selva, *System Architecture: Strategy and Product Development for Complex Systems*, Pearson, 2015, front cover.

[33] E. Crawley, B. Cameron and D. Selva, *System Architecture: Strategy and Product Development for Complex Systems*, Pearson, 2015, p. 22.

[34] ISO/IEC/IEEE 15288

[35] INCOSE, *Systems Engineering Handbook*, 2015, p. 5.

[36] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed., Prentice Hall, 2011, pp. 6-7.

[37] E. Crawley, B. Cameron and D. Selva, *System Architecture: Strategy and Product Development for Complex Systems*, Pearson, 2015, p. 78.

[38] D. Bohm, *Thought as a System*, Routledge, 1992

[39] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, 2nd ed., Wiley, 2011, pp. 69-82.

[40] E. Crawley, B. Cameron and D. Selva, *System Architecture: Strategy and Product Development for Complex Systems*, Pearson, 2015, p. 77-82.

[41] Rene Descartes, *Discourse on Method and Meditations on First Philosophy*, Translated by D. A. Cress, 4th Ed. Hackett Publishing Company, 1999.

[42] *Stanford Encyclopedia of Philosophy*, 2006.

[43] D. Dori, *Model-Based Systems Engineering with OPM and SysML*, Springer, 2016.

[44] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed., Prentice Hall, 2011, p. 690.

[45] P. G. Smith and G. M. Merritt, *Proactive Risk Management*, CRC Press, 2002, pp. 2-3.

[46] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Unpublished, Ch. 3.

[47] K. Armstrong, “Opportunities in the Risk Management of EMC,” IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 988 – 993, 2011.

[48] K. Armstrong, “Including EMC in Risk Assessments,” IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 796 – 801, 2010.

[49] FAA 2015. “Mission.” FAA.gov, https://www.faa.gov/about/mission/

[50] INCOSE, *Systems Engineering Handbook*, 2015, pp. 211-245.

[51] O. L. de Weck, D. Roos, C. L. Magee, *Engineering Systems,* Cambridge, MA: The MIT Press, 2011, p. 66.

[52] S. Corpino, F. Nichele, "An ilities-driven methodology for the analysis of gaps of stakeholders needs in space systems conceptual design," IEEE Systems Journal (not published yet).

[53] J. Wilmot, L. Fesq, D. Dvorak, "Quality attributes for mission flight software: A reference for architects," IEEE Aerospace Conference, March 5-12, 2016, pp. 1-7.

[54] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Unpublished, Ch. 1, p. 13.

[55] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed., Prentice Hall, 2011, pp. 6-7.

[56] D. Bohm, *Thought as a System*, Routledge, 1994.

[57] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, 2nd ed., Wiley, 2011

[58] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Unpublished, Ch. 3,

[59] E. Crawley, B. Cameron and D. Selva, *System Architecture: Strategy and Product Development for Complex Systems*, Pearson, 2015, p. 78.

[60] J. Y. Lee and G. J. Collins, "Risk Analysis of Electromagnetic Effects in Aircraft," IEEE Aerospace Conference Proceedings, March 2017

[61] J. Y. Lee and G. J. Collins, "Risk Analysis of Lightning effects in Aircraft System," IEEE Aerospace Conference Proceedings, March 2017.

[62] FAA 2015. "Mission." FAA.gov, https://www.faa.gov/about/mission/

[63] Boeing 2015, "A Foundation of Innovations," http://www.boeing.com/principles/vision.page

[64] I. Moir and A. Seabridge, *Aircraft Systems Mechanical, Electrical and Avionics Subsystems Integration*, Third Edition, Wiley, 2008.

[65] J. Y. Lee and G. J. Collins, "Risk Analysis of Electromagnetic Effects in Aircraft," IEEE Aerospace Conference Proceedings, March 2017.

[66] F. A. Fisher, J. A. Plumer and R. A. Perala, *Lightning Protection of Aircraft*, 2nd ed., Lightning Technologies Inc., 2001.

[67] C. R. Paul, *Introduction to Electromagnetic Compatibility*, John Wiley & Sons, 2006.

[68] H. W. Ott, *Electromagnetic Compatibility Engineering*, John Wiley & Sons, 2009.

[69] J. J. Ely, "Electromagnetic Interference to Flight Navigation and Communication Systems: New Strategies in the Age of Wireless," AIAA Guidance, Navigation, and Control Conference and Exhibit, 15 – 18 August 2005, San Francisco, CA, 2005.

[70] Federal Aviation Administration (FAA) Advisory Circular (AV) 91.21-1C, "Use of Portable Electronic Devises Aboard Aircraft," dated 7 May 2015.

[71] F. A. Fisher, J. A. Plumer and R. A. Perala, *Lightning Protection of Aircraft*, 2nd ed., Lightning Technologies Inc., 2001, pp. 147 – 214.

[72] G. Sweers, B. Birch, J. Gokcen, "Lightning Strikes: Protection, Inspection, and Repair," AERO, Published by Boeing Commercial Airplanes, QTR 4, 2012.

[73] L.M. Cysneiros, J.C.S. do Prado Leite, "Nonfunctional requirements: From elicitation to conceptual models," IEEE Trans. Software Engineering, Vol. 30, No. 5, May 2004, pp. 328-350.

[74] N. Ricci, M.E. Fitzgerald, A.M. Ross, D.H. Rhodes, "Architecting systems of systems with ilities: an overview of the SAI method," Procedia Computer Science, Vol. 28, 2014, pp. 322-331.

[75] S. Corpino, F. Nichele, "An ilities-driven methodology for the analysis of gaps of stakeholders needs in space systems conceptual design," IEEESystems Journal (not published yet)

[76] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, Second Edition, Wiley, 2011, p. 94.

[77] J. K. Pinto, *Project Management Achieving Competitive Advantage*, 4th edition, Pearson Education Limited, 2016

[78] E. Genender, H. Garbe, F. Sabath, "Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level," IEEE Transactions on Electromagnetic Compatibility, vol. 56, No. 1, February 2014, pp. 200-207.

[79] P. G. Smith, G. M. Merritt, *Proactive Risk Management*, CRC Press, 2002, p. 30.

[80] H. W. Ott, *Electromagnetic Compatibility Engineering*, Wiley, 2009.

[81] C. R. Paul, *Introduction to Electromagnetic Compatibility*, John Wiley & Sons, 2006, p. 3.

[82] A. Ruehli, G. Antonini, L. Jiang, *Circuit Oriented Electromagnetic Modeling Using the PEEC Techniques*, First Edition, Wiley-IEEE, 2017.

[83] C. R. Paul, *Introduction to Electromagnetic Compatibility*, John Wiley & Sons, 2006, pp. 7-9.

[84] T. X. Nguyen, "Cumulative interference to aircraft radios from multiple portable electronics devices," 24th Digital Avionics Systems Conference, October 30, 2005.

[85] J. J. Ely, "Electromagnetic Interference to Flight Navigation and Communication Systems: New Strategies in the Age of Wireless," AIAA Guidance, Navigation, and Control Conference and Exhibit, 15 – 18 August 2005, San Francisco, CA, 2005.

[86] I. Moir and A. Seabridge, *Aircraft Systems Mechanical, Electrical and Avionics Subsystems Integration*, Third Edition, Wiley, 2008.

[87] S. Jackson, *Systems Engineering for Commercial Aircraft*, Ashgate Publishing Company, 2015, p. 16.

[88] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, Fifth Edition, Prentice Hall, 2011.

[89] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, Second Edition, Wiley, 2011.

[90] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, Second Edition, Wiley, 2011, pp. 120-128.

[91] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, Second Edition, Wiley, 2011, p. 7.

[92] K. Armstrong, "Opportunities in the Risk Management of EMC," IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 988 – 993, 2011.

[93] D. Pissoort, A. Degraeve, and K. Armstrong, "EMI Risk Management: a Necessity for Safe and Reliable Electronic Systems!," IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin) pp. 208–210, 2015.

[94] K. Armstrong, "EMI Risk Analysis," IEEE In Compliance Magazine, August 1, 2011.

[95] K. Armstrong, "Including EMC in Risk Assessments," IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 796 – 801, 2010

[96] F. Sabath, "EMI Risk Management with the Threat Scenario, Effect, and Criticality Analysis," Ultra-Wideband, Short-Pulse Electromagnetics 10, F. Sabath and E. L. Mokole Eds. New York: Springer Science, pp. 265–278, 2014.

[97] K. Armstrong, "Why few (if any) medical devices comply with their EMC standard, and what can be done about it," IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 929 – 934, 2014.

[98] N. K. Agarwal, "EMI Control in High Reliability Space Systems," Proceedings of the International Conference on Electromagnetic Interference and Compatibility (INCEMIC), pp. 1 – 6, 1999.

[99] G. Smith and G. M. Merritt, *Proactive Risk Management*, CRC Press, 2002.

[100] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, Fifth Edition, Prentice Hall, 2011, p. 3.

[101] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice,* Second Edition, Wiley, 2011, pp. 30-34.

[102] N. P. Whitehead, W. T. Scherer, M. C. Smith, "Systems Thinking about Systems Thinking," IEEE Systems Journal, Vol. 9, No. 4, pp. 1117-1128, December 2015.

[103] M. Tooley, D. Wyatt, *Aircraft Electrical and Electronic Systems Principles, Maintenance and Operation*, Routledge Taylor & Francis Group, 2009.

[104] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, Fifth Edition, Prentice Hall, 2011, p. 690.

[105] P. G. Smith, G. M. Merritt, *Proactive Risk Management*, CRC Press, 2002, p. 19-21.

[106] ISO 31000, *Risk Management*, 2009

[107] M. W. Maier; E. Rechtin, *The Art of Systems Architecting*, CRC Press, 3rd ed. 2009.

[108] F. A. Fisher, J. A. Plumer and R. A. Perala, *Lightning Protection of Aircraft*, 2nd ed., Lightning Technologies Inc., 2001, p. 62.

[109] C. R. Paul, *Introduction to Electromagnetic Compatibility*, 2nd ed., John Wiley & Sons, Inc., 2006, pp. 3-10.

[110] E. T. Pierce, "Triggered Lightning and Some Unsuspected Lightning hazards," American Association for the Advancement of Science, 138th Annual Meeting, 1971, Stanford Research Institute, Menro Park, California, January 1972.

[111] B. D. Sherman, T. He, B. Nozari, T. Rudolph, "MD-90 Transport Aircraft Lightning Induced Transient Level Evaluation by Time Domain Three Dimensional Finite Difference Modeling," Proceedings of the International Aerospace and Ground Conference on Lightning and Static Electricity, Williamsburg, VA, pp. 69-1 – 69-15, 1995.

[112] B. D. Sherman, T. He, B. Nozari, T. Rudolph, "MD-90 Transport Aircraft Lightning Induced Transient Level Evaluation by Time Domain Three Dimensional Finite Difference Modeling," Proceedings of the International Aerospace and Ground Conference on Lightning and Static Electricity, Williamsburg, VA, pp. 69-1 – 69-15, 1995.

[113] G. Sweers, B. Birch, J. Gokcen, "Lightning Strikes: Protection, Inspection, and Repair," AERO, Published by Boeing Commercial Airplanes, QTR 4, 2012.

[114] "Aircraft Lightning Zoning," Aerospace Recommended Practice (ARP) 5414A, SAE International, Warrendale, PA, 2005.

[115] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, Fifth Edition, Prentice Hall, 2011.

[116] A. Kossiakoff, W. N. Sweet, S. J. Seymour and S. M. Biemer, *Systems Engineering Principles and Practice*, Second Edition, Wiley, 2011.

[117] N. P. Whitehead, W. T. Scherer, M. C. Smith, "Systems Thinking about Systems Thinking," IEEE Systems Journal, Vol. 9, No. 4, pp. 1117-1128, December 2015.

[118] G. Smith and G. M. Merritt, *Proactive Risk Management*, CRC Press, 2002.

[119] E. Genender, H. Garbe, F. Sabath, "Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level," IEEE Transactions on Electromagnetic Compatibility, Vol. 56, No. 1, pp. 200 – 207, February 2014.

[120] G. Sweers, B. Birch, J. Gokcen, "Lightning Strikes: Protection, Inspection, and Repair," AERO, Published by Boeing Commercial Airplanes, QTR 4, 2012.

[121] F. A. Fisher, J. A. Plumer and R. A. Perala, *Lightning Protection of Aircraft*, 2nd ed., Lightning Technologies Inc., 2001.

[122] J. M. Borky, *Architecting Information-Intensive Aerospace Systems*, Unpublished.

[123] F. A. Fisher, J. A. Plumer and R. A. Perala, *Lightning Protection of Aircraft*, 2nd ed., Lightning Technologies Inc., 2001, pp. 585-586.

[124] ARP5416A Aircraft Lightning Test Methods, SAE International, January 7, 2013.

[125] ARP 5412B Aircraft Lightning Environment and Related Test Waveforms, SAE International, January 11, 2013.

[126] K. E. Boulding, "General Systems Theory — The Skeleton of Science," Management Science, vol. 2, no. 3, p. 197, 1956.

[127] A. Sage and C. Cuppan, "On Systems Engineering and Management of Systems of Systems and Federation of Systems," Information Knowledge System Management, 2(4), 325 – 345, 2001.