3-2021

Utilizing Model Based Systems Engineering to Identify Safety Critical Functions in Airworthiness Certification

Jeffrey C. King

USING MODEL BASED SYSTEM ENGINEERING TO IDENTIFY SAFETY CRITICAL FUNCTIONS IN AIRWORTHINESS CERTIFICATIONS

THESIS

Jeffery C. King, Captain, USAF

AFIT-ENV-MS-21-M-241

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENV-MS-21-M-241

USING MODEL BASED SYSTEM ENGINEERING TO IDENTIFY SAFETY CRITICAL FUNCTIONS IN AIRWORTHINESS CERTIFICATIONS

THESIS

Presented to the Faculty

Department of Systems Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Systems Engineering

Jeffery C. King, BS

Captain, USAF

March 2021

AFIT-ENV-MS-21-M-241

USING MODEL BASED SYSTEM ENGINEERING TO IDENTIFY SAFETY CRITICAL FUNCTIONS FOR USE IN AIRWORTHINESS CERTIFICATIONS

Jeffery C. King, BS

Captain, USAF

Committee Membership:

Dr. John M. Colombi
Chair

Dr. Thomas C. Ford
Member

Dr. David R. Jacques
Member

AFIT-ENV-MS-21-M-241

Abstract

Modern aircraft are complex systems with numerous interacting hardware and software components. To minimize any safety mishaps during operations, new aircraft designs and modifications must go through an airworthiness certification. The current United States Air Force (USAF) airworthiness certification process, captured in MIL-HDBK-516C, is time-consuming and manpower intensive due to extensive documentation. To minimize inefficiencies of this document-based approach, this thesis examined model-based systems engineering (MBSE) to support Safety Critical Function (SCF) thread analysis against criteria found in Section 15 of MIL-HDBK-516C. Within this scope, the research identified an SCF domain-specific profile and style guide using the Systems Modeling Language (SysML) and domain specific extensions. The SCF profile was applied to an Unmanned Airborne System (UAS) designed and flight tested as a course sequence in AFIT's Graduate school. This research identified: 1) how a system model can support the execution of the airworthiness process, 2) how modeling can be minimally stereotyped to support various airworthiness analyses, and where airworthiness analysis could be automated and leaned. Using MBSE for SCF identification and thread analysis will not only improve airworthiness certification but support the digital transformation of the Defense acquisition system.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. John Colombi, for his guidance and support throughout the course of this thesis effort. The insight and experience were certainly appreciated. I would also like to thank my sponsor, Mr. Nicholas Shouse, from the Air Force Materiel Command for both the support and latitude provided to me in this endeavor.

Jeffery C. King

Table of Contents

Page

List of Figures

Page

List of Tables

Page

Acronyms

AC	Airworthiness Circular
AFLCMC	Air Force Life Cycle Management Center
AFMC	Air Force Material Command
AFOTEC	Air Force Operational Test and Evaluation Center
AFRL	Air Force Research Laboratory
BDD	Block Definition Diagram
DoD	Department of Defense
DOE	Department of Engineering
DRM	Design Research Methodology
EN	Engineering
FAA	Federal Aviation Administration
FHA	Functional Hazard Analysis
MFR	Military Flight Release
MTC	Military Type Certificate
PEO	Program Executive Officer
PO	Project Officer
SCF	Safety Critical Function
SCFTA	Safety Critical Function Thread Analysis
SME	Subject Matter Expert
SPA	System Processing Architecture
SPO	System Program Office
SysML	Systems Modeling Language
TAA	Technical Airworthiness Authority
UAS	Unmanned Aircraft System
V&V	Validation and Verification

USING MODEL BASED SYSTEM ENGINEERING TO IDENTIFY SAFETY CRITICAL FUNCTIONS FOR USE IN AIRWORTHINESS CERTIFICATIONS

I. Introduction

1.1 Background

Modern military aircraft are complex machines with numerous interacting systems all operating within diverse mission sets. Any improper design or operation on the myriad of components and functions of the aircraft poses a safety risk to all personnel who associate in and around the aircraft to include the general public. Given these potential risks, most aircraft are subject to government-mandated safety rules that apply to the airworthiness of the design, the production process used to make these machines, and the operation and maintenance of individual aircraft. In the United States, the Federal Aviation Administration (FAA) oversees most of these certifications for aircraft and aircraft operations. Additionally, the United States Military maintains additional airworthiness standards, policies, and procedures in conjunction with the FAA. Any new aircraft or new modifications on existing aircraft must be certified for airworthiness before it is placed in operation.

Department of Defense (DoD) handbook, MIL-HDBK-516C, is used for military aircraft airworthiness certification criteria. This document establishes the airworthiness certification criteria, standards, and methods of compliance to be used in the determination of the airworthiness of all manned and unmanned, fixed, and rotary wing air systems (Department of Defense, 2014). To address each portion of the airworthiness process, the handbook is divided into seventeen sections ranging from Systems

Engineering to System Safety to Computer Systems and Software etc. (Department of Defense, 2014). Each of these main sections provide further detailed criteria necessary for an air system to meet airworthiness certification.

MIL-HDBK-516C can be applied at any point throughout the life cycle of an air system whenever an airworthiness determination is necessary. The handbook should especially be used whenever there is a change to the functional or product baseline (Department of Defense, 2014). Additionally, not all airworthiness criteria apply to every type of air system, and platform-unique systems which contain previously undefined criteria may need to be added. Therefore, the handbook can be tailored to create a complete (necessary and sufficient) set of applicable airworthiness criteria, creating the system's certification basis (Department of Defense, 2014). From this, each aircraft platform system program office (SPO) has the responsibility to maintain individual records of their specific platform's airworthiness criteria.

The organizational focus for this thesis will be Air Force Materiel Command's (AFMC) Air Force Lifecycle Management Center (AFLCMC) Systems Design and Integration Branch (EZSI). AFLCMC/EZSI provides systems engineering, technical guidance, and support to program offices to design, develop, manufacture, integrate, test, and deploy systems to the warfighter. The branch organizes, trains, and equips AFLCMC professionals in the following technical disciplines: Early Systems Engineering, Development Systems Engineering, Sustainment Systems Engineering, Risk Management, and Aircraft Stores & Armament Integration. Products and support provided to programs offices include policy documents, implementation guides, tools, classroom and web-based training, implementation metrics, independent reviews and

special project assistance. Additionally, AFLCMC/EZSI provides technical counseling, competency and career management to engineers and security professionals across the Air Force Life Cycle Management Center (Shouse, 2021).

Airworthiness certification follows a logical data model of the key elements used within the airworthiness process as seen in Figure 1. Pre-contract, the process begins by developing an airworthiness plan followed by an airworthiness impact assessment to identify criteria that relate to or impact aircraft airworthiness. An audit is conducted on the aircraft equipment and functions followed by a reportability determination. During this time, requirements are developed, the modification is requested, and the certification basis is finalized. Moving into pre-flight testing, an analysis review is conducted. Here, airworthiness artifacts are gathered, engineering reviews are held, and criteria is checked against FAA and Air Force Regulation documents. Sub system and ground tests are then held, and the compliance data is collected. Upon review of the compliance data, the risks are assessed and accepted by proper authority. This allows for a test flight release and completion of flight test. Compliance data is once again gathered and reviewed prior to an updated risk assessment. Once the updated risk is accepted by the proper approval authority, the airworthiness documentation is updated, authentication is requested, and a flight approval, Military Flight Release (MFR) or Military Type Certificate (MTC) is awarded.

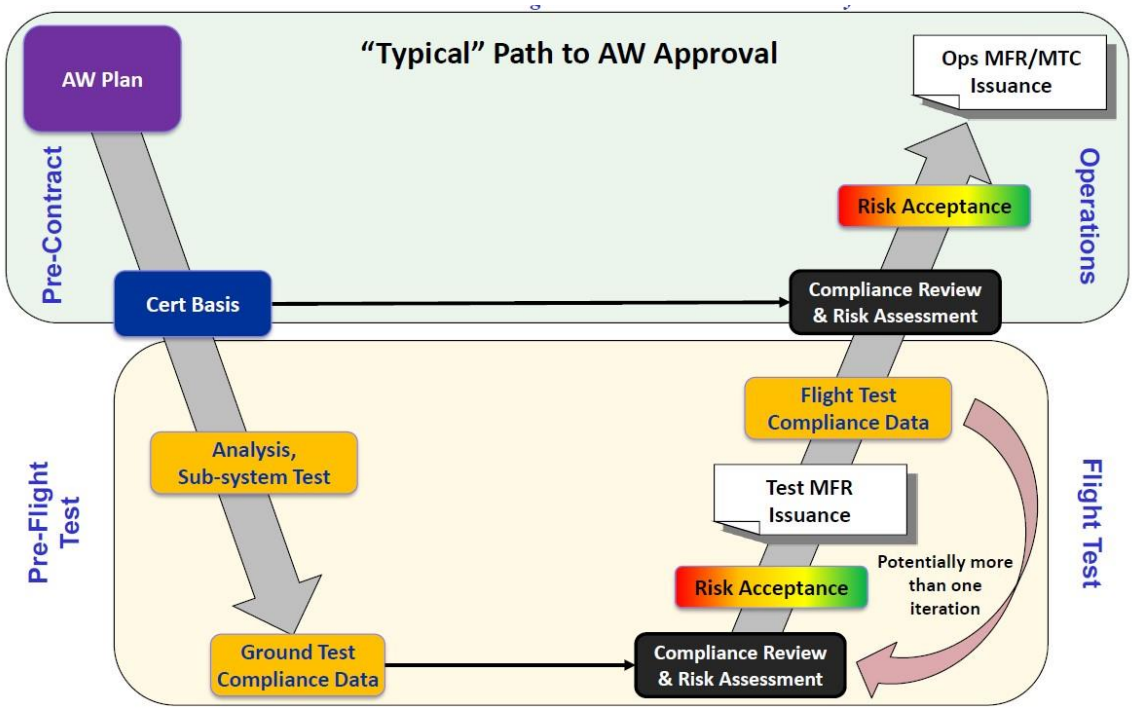

Figure 1. "Typical" Path to AW Approval (Airworthiness Office, 2020)

Throughout the logical data flow, the value producing operand is the airworthiness analysis and documentation. The documentation is what defines risk, criteria impacted, and ultimately an airworthiness certification. The process as it stands today impacts multiple organizations with the SPO being the central hub. As aircraft modifications come in from the operational unit, the SPO evaluates the requirement against artifacts from the FAA, Air Force Research Laboratory (AFRL), Air Force Operational and Test Command (AFOTEC), the platform contractor, and all other military regulation offices. Pending the level of the risk as defined by the SPO engineering team, the modification request is sent to the Chief Engineer or to AFLCMC engineering (EN) airworthiness home office. AFLCMC/EN then evaluates the requirements against regulations and confers with the independent technical

airworthiness authority (TAA) and department of engineering (DOE). When modification has been fully analyzed, the request with its associated risk is sent to the Program Executive Officer (PEO) for acceptance and signature of the MFR/MTC. The MFR/MTC is sent back to the SPO for program implementation and the modification is carried out for the customer.

1.2 Problem Statement

As represented in the logical data flow and As-Is Architecture – tracking risk and criteria is a several step complex process that impacts multiple organizations. This complexity constrains the airworthiness certification process to be labor intensive for all organizations involved. As it stands, to transfer information across organizations, spreadsheets are utilized to document changes, updates, requirements, etc. With the current document-based process, if something changes throughout the certification process, none of the previously accomplished tasks are updated automatically or easily. All system changes require an engineer at the SPO or home office to go back and update all the documents manually. Additionally, spreadsheet documentation does not easily allow for component to requirement tracing often used in the airworthiness process with risk and hazard impact studies. To minimize inefficiencies of a document-based approach to airworthiness certification, a different model-based process needs to be created that emphasizes three main goals: manage system functionality, manage airworthiness criteria, and manage airworthiness documentation.

1.3 Research Objective and Investigative Questions

Using Airworthiness Circular (AC) 17-01 as a guide, this thesis looked at using model-based systems engineering (MBSE) to create a Safety Critical Function (SCF) thread for software requirements against criteria found in Section 15 of MIL-HDBK-516C. Within this scope, the research objective was to identify how a system model can aid and automate the execution of the airworthiness process. Three specific questions were addressed in this thesis to provide a possible solution:

1. What modeling aspects and/or program artifacts must be created to support the airworthiness certification process?
2. What airworthiness analyses can be done with a SysML domain specific system model?
3. How could airworthiness analysis be automated or leaned to support parallel, continuous development operations.

1.4 Methodology Overview

Research for this thesis was completed using the Design Research Methodology (DRM) by Lucienne T.M. Blessing and Amaresh Chakrabarti. DRM consists of four stages: Research Clarification, Descriptive Study I, Prescriptive Study, and Descriptive Study II. Research Clarification helps clarify the current understanding and the overall research aim, develop a research plan, and provide focus for the subsequent stages. The Descriptive Study I target is increasing the understanding of design and the factors that influence its success by investigating the phenomenon of design, to inform the development support. Prescriptive Study aims at developing support in a systematic way,

considering the results of Descriptive Study I. Descriptive Study II focuses on evaluating the usability and applicability of the actual support and its usefulness through a success evaluation. Descriptive Study II was not addressed in this thesis. Although it is a part of DRM, where a comprehensive Descriptive Study I was completed with an Initial Prescriptive Study, a second Descriptive Study was not necessary.

1.5 Assumptions and Limitations

This thesis will be limited to MIL-HDBK-516C Section 15 Computer Systems and Software with emphasis on SCF identification. Further research into all other sections of MIL-HDBK-516C would be required to complete a full airworthiness certification process. The model evaluated throughout this thesis will be of a small unmanned aerial vehicle. This will allow for unrestricted data access and capability to model an airframe within the time allotted. The model used was developed by a team of students participating in the Systems Engineering Unmanned Aircraft Systems (UAS) courses provided by AFIT.

1.6 Expected Contributions

This thesis is expected to provide insight and understanding of the use of MBSE within the airworthiness process. Specifically, it will address the use of diagrams, relationship tracing, and coded analysis to ease and/or automate requirements within the computer and software portion of the airworthiness process. Work from this thesis is expected to assist in analyzing system safety, flight hazards, and risk elements of an aircraft system.

1.7 Summary

Chapter I gave a brief overview of the airworthiness certification process and the need to overcome inefficiencies of a document-based approach. A model-based process needs to be created that emphasizes three main goals: manage system functionality, manage airworthiness criteria, and manage airworthiness documentation. Using MBSE, an SCF thread for software requirements against criteria found in Section 15 of MIL-HDBK-516C was created for the Airworthiness Certification process.

Chapter II, Literature Review, provides benefits of MBSE over traditional spreadsheet tracking along with examples where MBSE is being used by other industry partners for airworthiness like certifications. Chapter III, Methodology, discusses in depth the guiding use of DRM for this thesis and how the SCF model was created. Chapter IV, Results and Analysis, presents a summary of the work completed to include MBSE models for SCF identification and the interaction of the identified SCF with the system. Finally, Chapter V will provide recommendations for future research.

II. Literature Review

2.1 Chapter Overview

The purpose of this chapter is to first define key terms within the airworthiness certification. This chapter will also address the use and benefits of model-based system engineering (MBSE) for airworthiness certification on military aircraft over traditional spreadsheet tracking. Finally, this chapter will address the ability of using MBSE for airworthiness certifications.

2.2 Key Terms within Airworthiness Certification

With the advent of integrated computer system architectures, reliable air system functionality is often dependent on information technology (IT), data and the reliable distribution of that data. Such systems include sensors, processors, software, and communication (data buses, backplanes, radios, switches, etc). This has led to an increased reliance on executing Safety Critical Functions (SCFs) with integrated computer system architectures. To provide the requisite safety assurance, the USAF airworthiness certification process has recognized that it is necessary to adhere to a rigorous standard of safety verification for these systems, referred to as System Processing Architectures (SPAs). The USAF airworthiness certification process utilizes MIL-HDBK-516 Section 15, Computer Systems and Software, to establish the airworthiness verification criteria for SPAs (Airworthiness, 2017).

An air system is an air vehicle plus the training and support systems for the air vehicle (e.g., communications, control, ground/surface/control station, launch and

recovery, and support elements), and any weapons to be employed on the air vehicle (Department of Defense, 2014).

An air vehicle includes the installed equipment (hardware and software) for airframe, propulsion, on-board vehicle and applications software, communications/identification, navigation/guidance, central computer, fire control, data display and controls, survivability, reconnaissance, automatic flight control, central integrated checkout, antisubmarine warfare, armament, weapons delivery, auxiliary equipment, and all other installed equipment (Department of Defense, 2014).

Airworthiness is the property of a particular air system configuration to safely attain, sustain, and terminate flight in accordance with the approved usage and limits (Department of Defense, 2014).

Airworthiness assessment is a technical evaluation of data against specific airworthiness criteria and determination of residual risk (Airworthiness Office, 2020)

The airworthiness certification is a repeatable process implemented to verify that a specific air system can be, or has been, safely maintained and operated within its described flight envelope. The two necessary conditions for issuance and maintenance of an airworthiness certification are: (1) the air system must conform to its type design; and (2) the air system must be in a condition for safe operation (Department of Defense, 2014).

A compliance report defines the approved certification basis with references to substantiating data that show compliance with the certification basis and lists risk levels for non-compliant criteria. The compliance report is used for final approval of a military type certificate (MTC) or military flight release (MFR) (Airworthiness Office, 2020).

The MTC provides the approval to fly a design configuration for the intended usage up to the Service Life Limit when a design is significantly compliant with its certification basis. This is typically only Low or Medium risks that may remain due to non-compliance (Airworthiness Office, 2020).

The MFR provides the approval to fly specific aircraft in a design configuration for a defined period. The MFR is awarded when a design may not meet the full standards and/or intent of an MTC (Airworthiness Office, 2020).

The term Safety Critical Function is defined in both MIL-STD-882 and MIL-HDBK-516C as: a function whose failure to operate or incorrect operation will directly result in a mishap of either Catastrophic or Critical severity. Per MIL-STD-882, SCFs are to be identified as part of the initial activity associated with the system safety process. Once identified, the SCFs are used in the Functional Hazard Analysis (FHA), which lays the foundation for identifying hazards within the system. The identification of SCFs is critical to understanding the focus area of airworthiness-oriented functionality (Airworthiness, 2017).

Safety Critical Functions (SCFs) are defined at the weapon system or air system level, so they are necessarily high-level functions. SCFs should be identified by the program's System Safety activity with support of engineers from relevant technical discipline areas. From an airworthiness perspective, identification of SCFs is essential to the process of verifying all functionality that contributes to airworthiness risk. The specific set of SCFs for a given system will be unique to each platform. All criteria in Section 15 indirectly rely on SCF identification since the criteria are only to be applied to equipment supporting SCFs; however, there is one criterion (15.1.1) that verifies that

SCFs have been identified for the system. In addition to 15.1.1, there are 32 criteria (including their associated standards) that directly reference or per definition (i.e., make reference to SSEs or flight critical functionality) rely on SCFs being identified in order to properly perform the verification (Airworthiness, 2017).

SCFs are grouped into five categories titled: Flight Critical, Operation Critical, Emergency Critical, Indication Critical, and Avoidance Critical. The only purpose for the five categories is to help convey the variety of functions that can be identified as SCFs. Below are descriptions for each of the categories (Airworthiness, 2017):

1. Flight Critical functions are functions used to achieve and control flight (loss or degradation could directly lead to loss of aircraft).
2. Operation Critical are SCFs that are used for supporting a non-Flight Critical function that has inherent safety functionality associated with its operation (loss/degradation could directly lead to a consequence of Catastrophic or Critical hazard severity).
3. Indication Critical are SCFs needed to provide indications to pilot/crew necessary for maintaining safe operation.
4. Emergency Critical are SCFs that exist purely for the purpose of mitigating risk associated with emergency conditions.
5. Avoidance Critical are SCFs needed purely to mitigate a potential safety risk.

An SCF thread is defined in MIL-HDBK-516C as: the combination of elements/components within a system and the required interfacing and interaction of those elements/components whose overall contribution is necessary for the operation of a given SCF. A Safety Critical Function Thread Analysis's (SCFTA) purpose is to:

1. Identify all the elements, hardware and software components, and interfaces that are necessary for the safe execution of all identified SCFs,
2. Ensure the identified elements and components are developed at Computer System Integrity Levels (CSILs) appropriate for SCF applications, and that safety critical interfaces are identified as such, and
3. Verify that end-to-end Validation and Verification (V&V) coverage is achieved by the tests used to verify the SCF functionality (includes: component level test and review; subsystem level test; through system integration test) (Airworthiness, 2017).

2.3 Benefits of MBSE over Spreadsheet Tracking

In May 2016, Tucson Embedded Systems presented a paper titled *Next-Generation Model-Based Systems Engineering Processes and Tools Supporting the Airworthiness efforts of Cyber Physical Systems (CPS)* in which they described how the Government and Industry Program Managers need improved end-to-end model-based (MB) tools to assist with the management of these complex development efforts, while airworthiness authorities need clarity of how MB tools and processes are available to support their airworthiness efforts. It is understood that airworthiness qualification practices are notoriously burdened, and existing tools used to develop and verify complex cyber physical systems do not provide insight into progress toward completion. These practices leave Program Managers without proper data to manage progress and efforts (Simi, Mulholland, & Merritt, 2016).

Utilizing a spreadsheet-based tool requires engineers at the SPO to manually input the data into each criterion identified by MIL-HDBK-516C. By keeping the requirements on Excel sheets, while it is informative, the spreadsheets do not provide staff with the effective connection between the requirement and its use in the system, or where the requirements stem from (Carros, 2019). Furthermore, issues are compounded by the document-centric nature of the certification process as the rules, requirements, and means of compliance are contained within documents that must be extracted by the reader and manually adapted into a document-based certification plan (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019). This manual update throughout the airworthiness process is what drives a very labor-intensive effort to transfer information across organizations.

To help with managing information across an organization, industries over the past few years have been turning to an MBSE approach to support Mission-based Analysis and Engineering. In interviews regarding the use of MBSE, the respondents were asked if they can compare their efficiency when they moved from document-based system engineering to model-based system engineering. Of respondents, 63% said that their productivity increased with the remaining saying that productivity did not change, or it decreased (Mazeika & Butleris, 2020). The respondents were also asked if their work quality improved when they moved from document-based system engineering to model-based system engineering. The majority of participants agreed that all the factors (Completeness; Consistency; Communication; Less defects) were improved (Mazeika & Butleris, 2020). State of the art MBSE tools provide an environment to evaluate the emerging system design through computer models, and demonstrate system compliance to user performance and design integrity requirements, all while managing airworthiness

risks (Blackburn, Cloutier, Witus, & Hole, 2014). The greatest advantage of MBSE is the relationship mapping between functions, components, requirements, and risk.

Systems modeling language (SysML), a language variant used in systems modeling, utilizes physical hierarchy models, functional mapping models, use cases, and activity diagrams to cross correlate each component to other parts and pieces of the aircraft. The model-based approach guarantees the completeness and consistency when tracking requirements from multiple sources (i.e. certification regulations, advisory circulars, pre-approved means of compliance) by providing formalized modeling techniques leading to a coherent system model incorporating up-to-date requirements and analysis (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019). MBSE tools not only capture and model the stakeholder's essential information, but also provides an approach to enable a program office to move through acquisition milestones in a more timely and efficient manner (Carros, 2019). In a document-based approach, as amendments are made to FAA regulations and/or standards, or if new modifications are requested on the aircraft, the amendments must be manually changed and updated in every single regulatory document. However, the model-based approach can automate the process of updating amendments and avoid the need to make manual changes in each document (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019). Therefore, using MBSE for airworthiness certification has the potential to allow the engineering team to identify not only what criteria is involved, but also recognize what exact components are affected.

2.4 Capability of using MBSE for Airworthiness certifications

In June of 2019, individuals from the Georgia Institute of Technology put out a paper titled *A Model-Based System Engineering Approach to Normal Category Airplane Airworthiness Certification* in which they demonstrated a model built for updating FAA regulations on commercial aircraft. Additionally, in Mar 2014, Stevens Institute of Technology and Wayne State University conducted research to assess the technical feasibility of creating and leveraging a more holistic MBSE approach and expected capabilities from such in their paper *Introducing Model Based Systems Engineering Transforming System Engineering through Model-Based Systems Engineering.* However, there are also challenges in cost and schedule associated with MBSE as pointed out by a Naval Postgraduate School Thesis on *MBSE Methodology and Analysis to Implement MBSE Post Milestone C.*

Bleu-Laine, et.al from Georgia Institute of Technology proposes an MBSE approach that is envisioned to parametrically transform the document-centric exercise of airworthiness to a model-based process. The approach helps collect the federal regulations and the associated means of compliance (MoC) in an integrated system model along with the relevant mappings between them (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019). Their first step towards solving the issue was to establish a complete representation of the federal regulations in a high level package structure that sections off the different parts of the regulations. By using a high level package structure in MBSE, they were able to separate the certification types. Then using a block definition diagram, they were able to create a hierarchical view of how the sections and subsections of the federal regulations are broken down. In one example, federal regulation Subpart B-Flight

was divided into Controllability, Trim, and Stability. Figure 2 shows the model view of the controllability portion of the regulation.

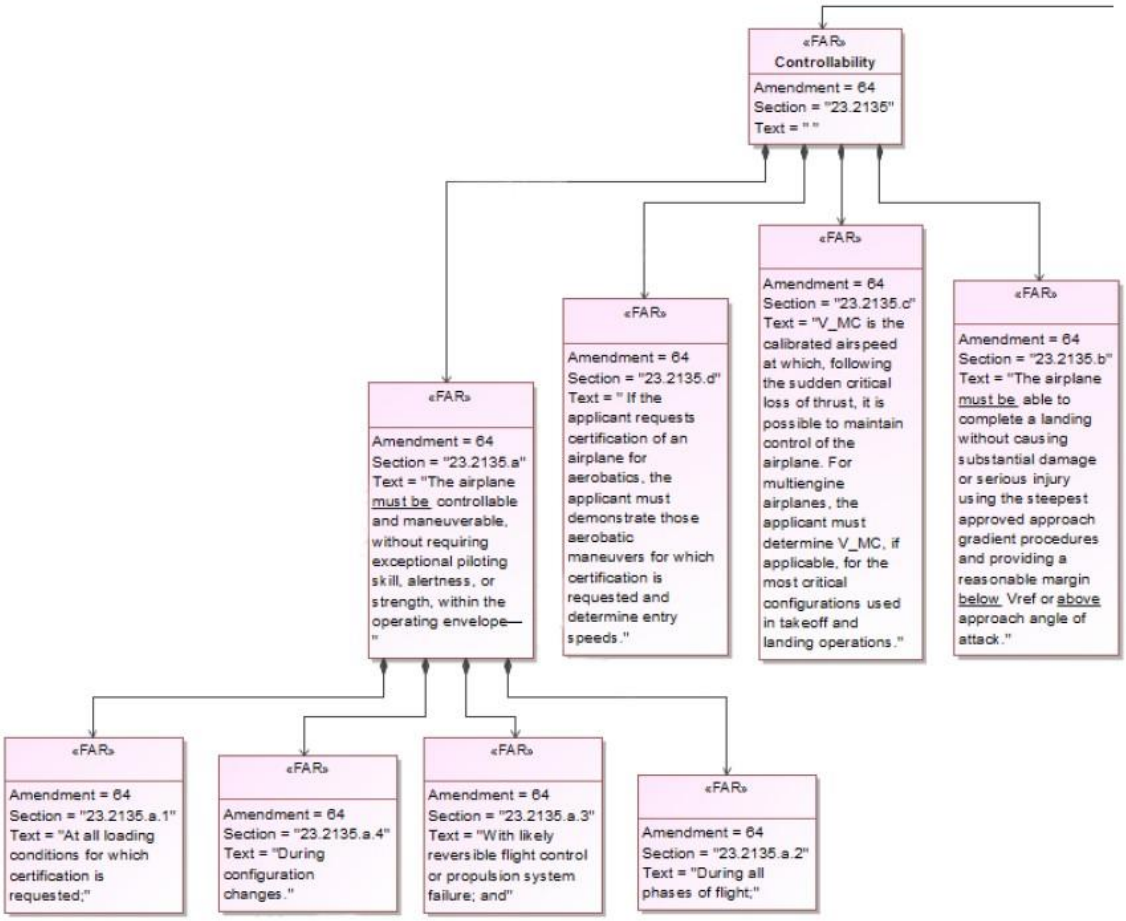

Figure 2. Controllability portion of Federal Regulation Subpart B-Flight hierarchical model (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019).

From there, standards files were mapped back to regulations and modeled using the mapping referential view in SysML. The stereotype Reference was used to distinguish that the structures are not shown anymore and that the relationships are the only important information presented (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019). In

the end, the model-based approach can automate the process of updating amendments and avoid the need to make manual changes in each document. This approach allows for changes in one part of the model to be propagated to others. Figure 3 shows an example in which a change was made to correct the section number of "Weight and Center of Gravity" in the federal regulations. Here, the wrong section number "23.201 - Weight and Center of Gravity" was corrected in the regulations hierarchical view to the right version of "23.21 - Weight and Center of Gravity". As shown in Figure 3, this change is conducted in a short time and the update is immediately propagated to other views and models as soon as the change is performed (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019).

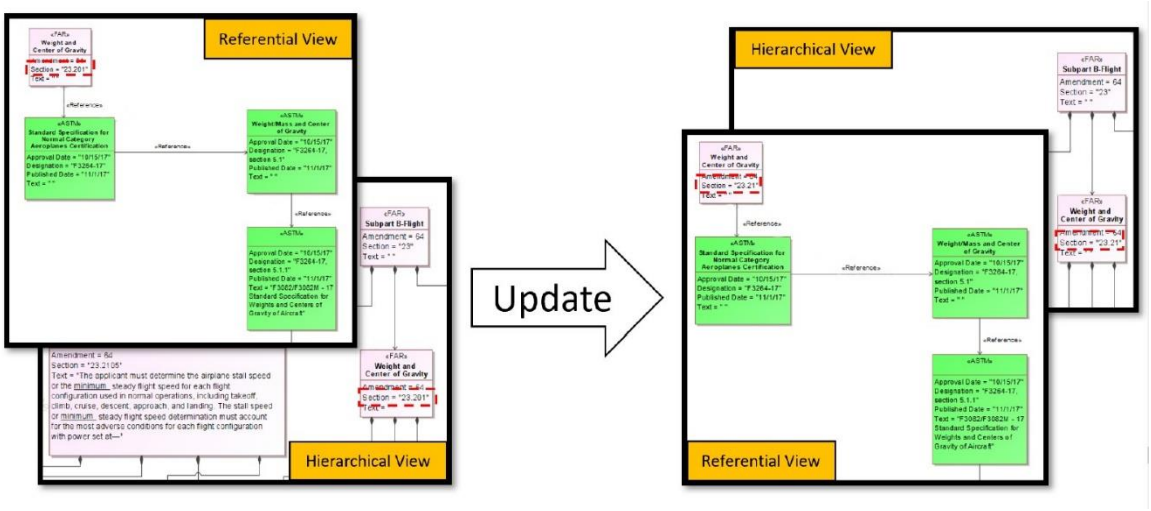

Figure 3. MBSE tools allow for updates in a model to be automatically propagated to other views and models as soon as the change is performed (Bleu-Laine, Bendarkar, Xie, & Mavris, 2019)

Airworthiness Certifications rely heavily on identification of SCFs and how they interact within in the system. Therefore, it is important for a model to capture the entire

system process. Multiple textbooks have been written for SysML that teach reliable methods of process modeling utilizing a model-based approach. One such book is *SysML for Systems Engineering* by Jon Holt and Simon Perry. Holt and Perry utilize the "seven views" approach to Process modelling that has been used successfully in both industry and academia for over two decades (Holt & Perry, 2018). Figure 4 shows a subset of the MBSE Ontology that has been identified as being relevant for Process modelling. Within in this model, the Process is associated to various areas of the system such as the Service in which it realizes, the Process Execution Group it is executed during, and the Use Case in which it satisfies. Furthermore, other views are also displayed to include the Stakeholder Role, Activities (to include what Resource those Activities consume), and Artefacts produced.

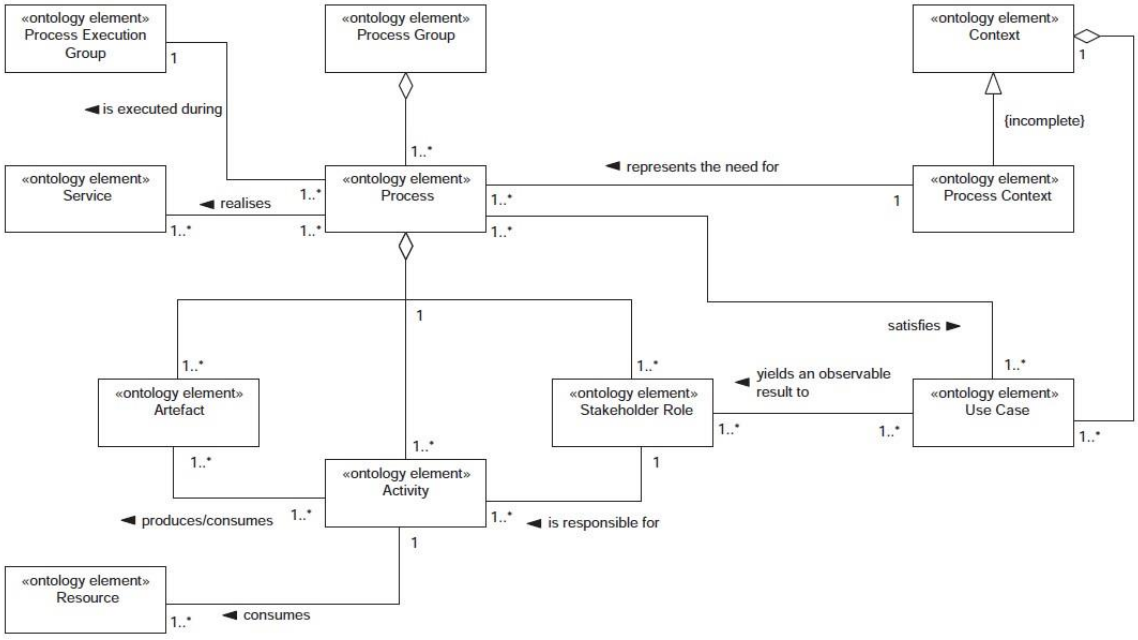

Figure 4. Subset of the MBSE Ontology focused on Process modelling (Holt & Perry, 2018)

The Process presented here may be used in a flexible way, pending the size and rigor of the Project. The Process may be used at any level of abstraction of the System and be used in several different ways. When using the Process for different levels of rigor or for different scale Projects, the fundamental Process stays the same, but it is the number of Views produced that changes and the way in which they are realized (Holt & Perry, 2018). The formal Process is executed on Projects that are critical in some way, such as safety-critical Systems and for mission-critical Systems (Holt & Perry, 2018). Figure 5 provides an example of a formal process model using SysML. The formal Process provides additional views to the Process model to include Source Elements, Rule Sets, Requirement Viewpoints, and Validation Viewpoints to name a few.

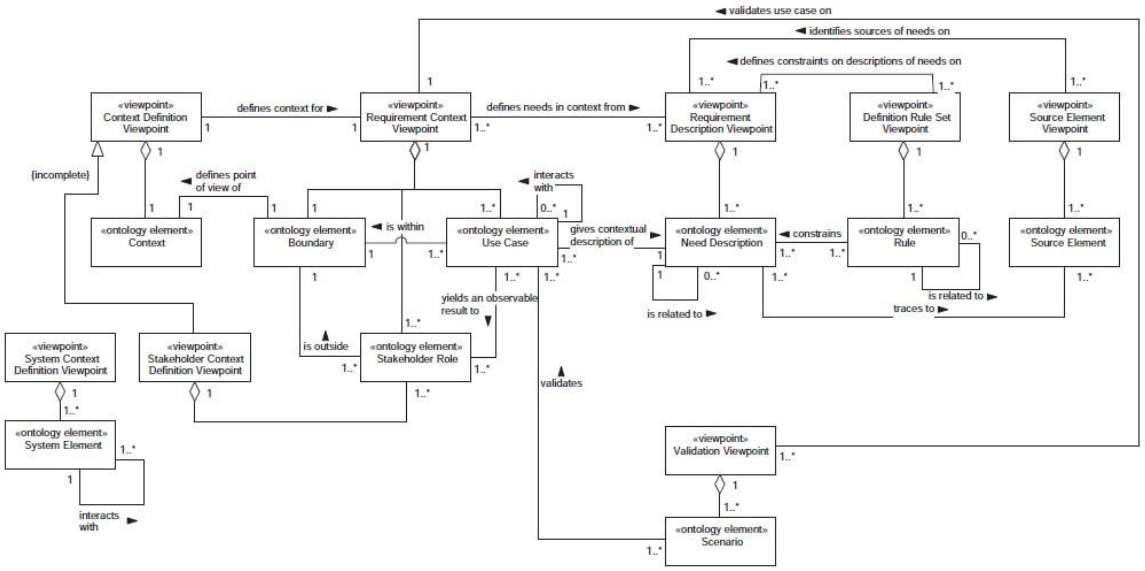

Figure 5. Example of a formal Process model executed on Projects that are safety-critical or mission-critical Systems (Holt & Perry, 2018).

Beyond System Views, MBSE can also be used for complex mathematical evaluations such as in the prediction of risk and in predictive analytic models to support

risk identification and management. More generally, models can be used to provide risk quantification for almost all types of decisions that are made by stakeholders. As an example, Stevens Institute of Technology and Wayne State University created a Bayesian model seen in Figure 6 using factors derived from MIL-HDBK-516 from a true story related to a C-130 Weapon Delivery system. The key characteristics of the approach is that the model ensures that all factors are considered in the decision-making process, and that all classes of stakeholders are adequately represented in the decision-making process. Each factor covers a specific aspect of airworthiness to ensure that all possible uncertainties and risk are considered in the quantification of risk. The risk index is a probability distribution where the mean can map to quantities in a risk matrix. With this systematic and comprehensive treatment of all relevant factors, it provides better risk identification (Blackburn, Cloutier, Witus, & Hole, 2014).

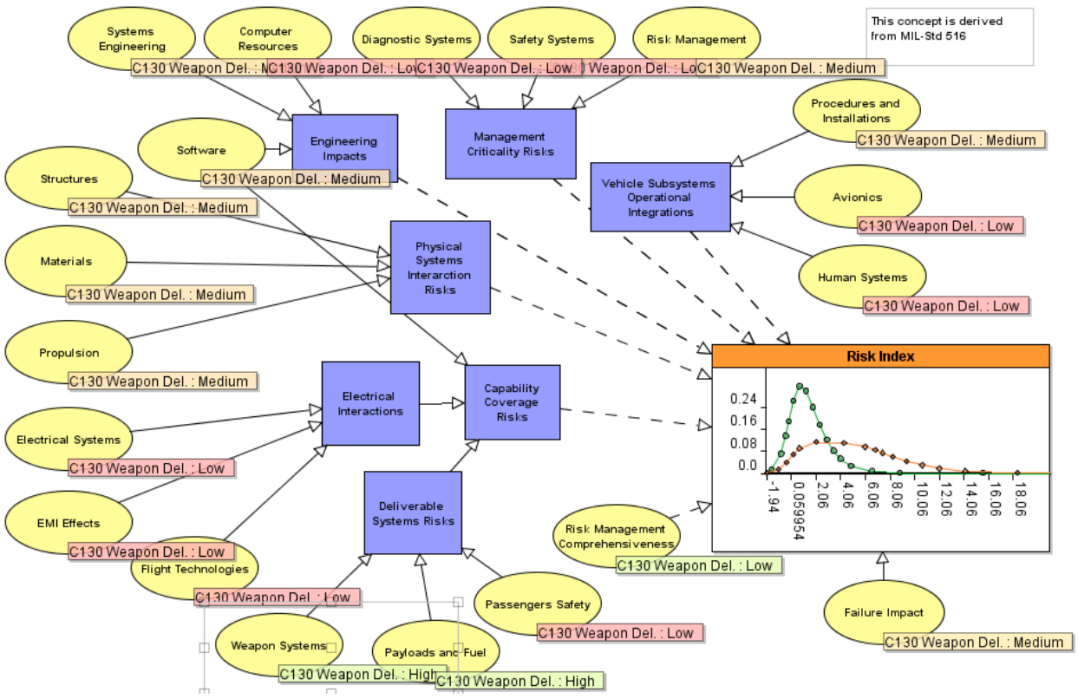

Figure 6. Example of how MBSE can be used to predict risk (Blackburn, Cloutier, Witus, & Hole, 2014).

With MBSE, there are challenges as well and it should be noted that it is not for every program or platform. The main challenge in implementing MBSE is the additional cost, which can be significant. The second major challenge in implementing MBSE is the schedule. It takes time to develop the models and implement the methodology. Combined, these efforts can take a year or more to implement. The last major challenge in implementing MBSE is the lack of understanding of what MBSE is and how it can be useful (Beaufait, 2018). However, with the combined relationship mapping, and the capability for automated updates across the entire system, there are significant benefits of using MBSE for continued airworthiness certification on those programs in which it makes sense to implement.

2.5 Summary

In this chapter, key terms within the airworthiness certification were first defined as per DoD guidelines. Secondly, this chapter addressed the benefit of MBSE over spreadsheet tracking. Spreadsheet tracking, although universally practiced, does not often allow an individual full insight into a System and the Process behind how that System operates without extensive piecemeal engineering of various documents. Third, this chapter addressed the use and benefits of MBSE for airworthiness certification on military aircraft over traditional spreadsheet tracking. This included the ability to update requirements and standards and have them immediately propagate across each view of the System as well as the ability to model an entire process view and perform complex mathematical calculations. Finally, this chapter addressed some of the challenges of using MBSE for airworthiness certifications such as cost and schedule. Next, Chapter III goes into the methodology used to characterize the scope of this thesis.

III. Methodology

3.1 Chapter Overview

The purpose of this chapter is to expound on the methodology used to identify and refine the scope against the use of MBSE in the airworthiness process. The methodology follows the Design Research Methodology (DRM) by Lucienne T.M. Blessing and Amaresh Chakrabarti. DRM consists of four stages: Research Clarification, Descriptive Study I, Prescriptive Study, and Descriptive Study II. Research Clarification helps clarify the current understanding and the overall research aim, develop a research plan, and provide focus for the subsequent stages. Descriptive Study I target is increasing the understanding of design and the factors that influence its success by investigating the phenomenon of design to inform the development support. Prescriptive Study aims at developing support in a systematic way, considering the results of Descriptive Study I. Descriptive Study II focuses on evaluating the usability and applicability of the actual support and its usefulness through a success evaluation (Blessing & Chakrabarti, 2009).

3.2 Research Clarification

The research clarification stage produced two main deliverables: a) current understanding and b) an overall research plan. To produce the deliverables discussed, the work was divided into six steps as suggested within DRM:

1. *Identify the topic* – The broad topic of MBSE and its use in the airworthiness process was introduced by AFLCMC. With review into the study, the topic was refined down to the main research objective identified as how can a

system model aid and automate the execution of the airworthiness process with particular focus on SCF identification as addressed in the introduction.

2. *Clarify the understanding* – To clarify the understanding of the Airworthiness Process, the USAF Airworthiness Policy and Implementation Course taught by AFLCMC's Engineering and Technical Management Services Directorate (AFLCMC/EZZ) was taken in-residence. This course provided an understanding of the current USAF airworthiness policy, implementation procedures, and individual/organizational responsibilities (Airworthiness Office, 2020). Further clarification on the possibility of utilizing a model-based environment for Airworthiness Certification scenarios was also researched through various articles and papers. Findings from this research were highlighted in Chapter II.
3. *Develop main questions and hypothesis* – To be able to judge the existing situation and suggest efficient and effective ways of improvement, one's understanding needs to involve a link to success (Blessing & Chakrabarti, 2009). For this link, three main questions were developed, each centering around how MBSE can be used to automate the airworthiness process. The questions are addressed in 1.3 Research Objective within in the introduction.
4. *Decide on a type of research* – To identify the type of research suitable to answer the chosen research questions and verify the hypothesis, the DRM framework presents seven main types of design research as seen in Figure 7. A review-based study is based on the review of the literature on design or on design support only and a comprehensive study is a study in which the results

are produced by the researcher, i.e. an empirical study, the development of support, or the evaluation of support (Blessing & Chakrabarti, 2009). A Type 2 – Comprehensive Study of the Existing Situation was chosen as the type of research. This type of study is undertaken when the criteria being studied can be established, but a better understanding of the existing situation is necessary to identify the factors that are most relevant to address to improve the situation (Blessing & Chakrabarti, 2009). Once sufficient understanding was gained, an Initial Prescriptive Study was accomplished to indicate how this understanding can be used to improve the intended design.

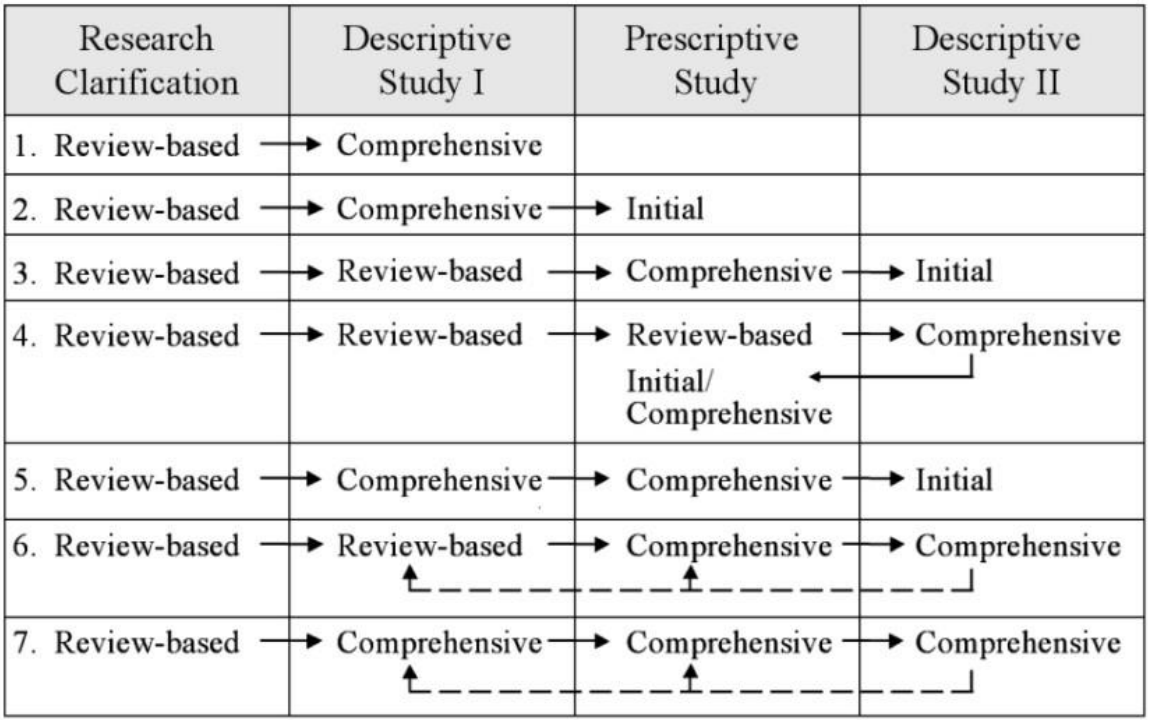

Figure 7. DRM breakdown of design research types (Blessing & Chakrabarti, 2009)

5. *Understand relevance and contribution* – The literature review focused a lot on traceability and capacity to update multiple views of the model with a

single change. The aim was to use this understanding to develop the initial reference model and impact models and how they would be affected by the ability to automate the airworthiness process. An Areas of Relevance and Contribution diagram (ARC diagram) as seen in Figure 8, was developed to understand the areas to which the research project will contribute. The blocks marked Essential indicate the areas to which the research project will contribute. This included the development of the model and what that model can inform leadership regarding risk, safety, and hazards. The blocks marked Influence indicate the areas to which this thesis will affect, but not be directly studied. This included the acquisition process between the Contractor, the SPO, and the Engineering Support. The blocks marked Other indicate the areas to which may or may not be impacted by the research. Items such as cost and product specifications were not regarded as a direct influence in the model.

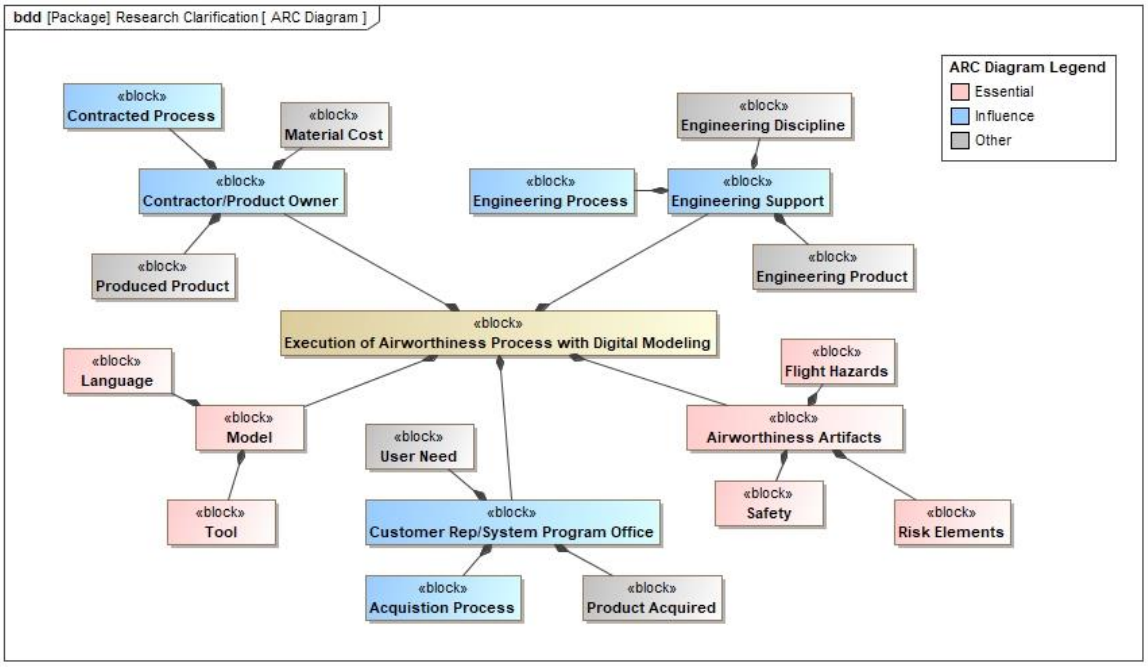

Figure 8. Areas of Relevance and Contribution (ARC) Diagram indicating how portions of the model developed in the research will contribute to the airworthiness process.

6. *Formulate a plan* – Taking each of the steps described above, and with the understanding of the timeframe available, an initial plan was developed. Using AC-17-01 as a guide, research was directed at creating an SCF thread using SysML for software requirements found against criteria identified in Section 15 of MIL-HDBK-516C. Emphasis was to be placed on criteria related to SCF identification and SCF interaction within the System. Overall, the plan would be completed by defining how the identified criteria could be automated, organized, or implemented into a digital model using SysML.

3.3 Descriptive Study I: Understanding Design

The Descriptive Study I produced two deliverables: a) a completed reference model and b) an updated initial impact model (Blessing & Chakrabarti, 2009). To achieve these deliverables, the work was divided into five steps as suggested by DRM:

1. *Review of the literature* – The aim of the literature review in Descriptive Study I was to extend the level of understanding gained thus far and update the expectations as represented in the Initial reference and Impact Models respectively (Blessing & Chakrabarti, 2009). Ebsco Discovery Service and IEEE Xplore research databases were used throughout the research. The use of MBSE in airworthiness processes was the primary search throughout the literature review. However, the search was also expanded into Process modeling and SysML techniques for safety critical systems to magnify opportunities within the model solution opportunities. In addition to MBSE research, literature was also conducted for airworthiness standards and practices regardless of model-based environments. This research included various SAE Aerospace Recommended Practice documents which were read to provide better understanding of aircraft design and development, aircraft operating environment and functions, hazard identification, and practices for showing compliance with regulations.
2. *Determination of the research focus* – From the Research Clarification, it was evident that focus of the research should be on reducing the workload required for airworthiness certification through digital automation in a model-based environment. This included determination of modeling aspects to support the

process, SysML domain specific system model analysis, and ability to support parallel and continuous development operations. This research focus coming directly from the research objective and questions being addressed with effort to create an SCF thread for the software requirements found in Section 15 of MIL-HDBK-516C. To aid in the execution of the SysML digital model, it was decided that data would also be necessary to ensure that the digital transformation of the airworthiness process being created could be executed in an aircraft model. The small Unmanned Aircraft System (UAS) Reference Architecture used by students at AFIT in the System Engineering department was chosen for the research focus due to familiarity with the system and ability to access the data.

3. *Development of a research plan* – The research plan was developed through the advice and experience of my thesis advisor, other AFIT faculty, and personnel from AFLCMC/EZI. Time was to be spent first in understanding the airworthiness process as it stands today. Then time would be spent in the model developing tools to automate and digitize the airworthiness process. To help answer the airworthiness process, the Fundamentals of Airworthiness course taught by AFLCMC/EZZ was completed to gain a better understanding of the process as it stands today. Academic courses were also taken at AFIT within the System Engineering department to understand SysML and its use within MBSE. Weekly progress checks were also set-up with AFIT faculty and personnel from AFLCMC/EZI to allow for clarification questions and, as needed, specific guidance could be provided regarding airworthiness scenarios

and SysML modeling techniques. Data collection was completed using notes from the weekly progress checks and SysML models were prepared for review prior to each meeting.

4. *Undertaking of an empirical study* – Where the nature of the study revolved around the capability of MBSE within the airworthiness process with data found through observation and formal lectures, a qualitative empirical study was chosen. Founding questions of what the problem with airworthiness is today, what needs to be captured in a model, and what goes into an SCF thread were addressed throughout. Each scenario discussed was then modeled with SysML and provided back to AFLCMC/EZI for acceptance. To further validate the use of the model, diagrams developed within the SysML Airworthiness Certification profile were re-constructed utilizing the UAS Reference Architecture. This allowed for cross-checking of the profile elements created in the profile against an aircraft system to ensure each diagram was both relevant and achievable.
5. *Deciding of overall conclusions* – From the study, it was decided that the key factor to be addressed within the digital model was the identification of the SCF and how that SCF interacted within the System. Therefore, it was decided that a SysML profile would be created that would guide the aircraft designer in how to construct each SCF within the model and connect the SCF with the various elements of the System. An Airworthiness Certification Profile package would be created to serve as the parent modeling aspect. The Profile could then be incorporated into any system model and provide that

system the necessary stereotypes and directions to create the diagrams necessary for the SCF relationship mapping used in the Airworthiness Certification Process.

3.4 Prescriptive Study: Developing Design Support

Two steps of the Systematic Prescriptive Study Processes were used as part of the initial Prescriptive Study format followed for this research: Task Clarification and Conceptualization. The initial Prescriptive Study format followed for this research was chosen as part of the Type 2 Research evaluated in the Research Clarification stage. Although MBSE is widely in use, and there is support for its capability, an initial Prescriptive Study was chosen to fully evaluate the potential of MBSE in airworthiness certification. The execution of the two steps is completed in Chapter IV, but an overview of the methodology can be seen here.

Task Clarification is to establish the problem to be solved by the support, to clarify its requirements, and to better define the desired situation (Blessing & Chakrabarti, 2009). From the results found in Descriptive Study I, the SysML model would plan to allow for each criterion established in Section 15 of MIL-HDBK-516C to be answered. However, focus of the model would be on airworthiness criteria within Section 15 experiencing repeated non-compliance as identified in AC-17-01. The guidance in the AC elaborates on particular airworthiness certification requirements that focus on design contributions that the hardware and software must provide to the system architecture in support of Safety/Flight Critical functionality, as well as key verification activities that are needed to evaluate the safety risk associated with the system design

(Airworthiness, 2017). Seven focus areas discussed in AC-17-01 were addressed for better understanding of the design, development, integration, and V&V expectations related to Section 15:

a) SCF Identification

b) SCF Thread Analysis

c) Integration Methodology: System, Software, and Levels of Testing

d) Failure Mode and Effects Testing (FMET)

e) Safety Interlock Design

f) SPA and Software Development Processes

g) Full Qualification of Software

The first task in Conceptualization is to identify and decide which functions the support needs to have to affect the Key Factors in the intended way (Blessing & Chakrabarti, 2009). From the results found in Descriptive Study I, the Key Factor that needed to be addressed was the identification of the SCF and how that SCF interacted within the System. Therefore, it was decided that a SysML profile would be created that would guide the aircraft designer in how to construct each SCF within the model and connect the SCF with the various elements of the System. To ensure that the model had merit against an established aircraft model, the UAS Reference Architecture was used as a proof of concept.

3.5 Descriptive Study II: Evaluating Design Support

Descriptive Study II was not addressed in this thesis. Descriptive Study II requires a completed design and is used to address the impact and evaluation of the design by

identifying whether the support indeed contributes to success (Blessing & Chakrabarti, 2009). Therefore, although it is a part of DRM, where only an initial design was completed through a comprehensive Descriptive Study I and an Initial Prescriptive Study, a second Descriptive Study was not necessary. Future research is recommended in this area to assess the impact and evaluation of the design in the Airworthiness Certification Process.

3.6 Summary

This chapter went over the methodology used to identify and refine the scope for MBSE in the airworthiness process. The methodology follows the DRM by Lucienne T.M. Blessing and Amaresh Chakrabarti. This chapter discussed the four stages of DRM: Research Clarification, Descriptive Study I, Prescriptive Study, and Descriptive Study II. Within Research Clarification, the understanding of the topic was clarified, and an initial impact model and an Initial reference model were created to capture how the research applies to each stakeholder and how various portions of the airworthiness process relate in generating an MFR. For Descriptive Study I, literature was reviewed to identify what industry and academia has already explored for MBSE in airworthiness processes and development of a research plan was created. The Prescriptive Study was used to provide final Task Clarification and Conceptualization to the project. Finally, Descriptive Study II was not addressed in this thesis. Chapter IV next will provide the results from the Prescriptive Study portion.

IV. Analysis and Results

4.1 Chapter Overview

This chapter provides details on the completion of the Prescriptive Study which includes the task clarification and conceptualization portions of the study. Additionally, application of the study against an established UAS Reference Architecture model will also be addressed. The task clarification segment concentrates on the seven focus areas discussed in AC-17-01 that were addressed for better understanding of the design, development, integration, and V&V expectations related to Section 15. The conceptualization piece will focus on the construction of the SysML Airworthiness Certification Profile. Finally, application of the Profile against the UAS Reference Architecture as a proof of concept will then be discussed.

4.2 Prescriptive Study: Task Clarification

For the Task Clarification, a review of AC-17-01 was conducted in whole and against the seven focus areas contained within. The first focus area being the identification of SCFs. Identification of SCFs is critical to understanding the focus area of airworthiness-oriented functionality (Airworthiness, 2017). The SCF Identification is used to demonstrate compliance with MIL-HDBK-516 Section 15 criteria 15.1.1 involving the identification of SCFs. The System Safety process (supported by functional engineering teams) should identify the system's applicable SCFs, which should then be used as the foundation for performing SCFTAs (Airworthiness, 2017).

The next focus area is the SCFTA. Where a key purpose of the airworthiness process is to ensure the design is safe to operate within its intended envelope of

operation, the SCFTA is a foundational tool for providing evidence that the end-to-end SCF functionality has been verified (Airworthiness, 2017). An SCFTA is considered to be satisfactorily completed when all the SCF threads have been fully identified (i.e., all supporting elements, components, and interfaces identified with associated CSIL) and complete test coverage of all SCF threads is verified and documented (Airworthiness, 2017). As the SCFTA is a large portion of the analysis, a significant focus was put on this aspect within the model.

Next in AC-17-01 is the System and Software Integration Methodology. The system integration methodology is the systematic process that is employed to bring the subsystem elements of a system together as a functional system (Airworthiness, 2017). AC-17-01 includes various recommendations to demonstrate compliance with MIL-HDBK-516 Section 15 criteria involving the system and software integration methodologies within the integration and test plans. The SCF Thread Layout model incorporates each of these in the following ways:

a) The complete V&V coverage of requirements, functions, and failure conditions could be addressed within each respective SCFTA model layout by embedding diagrams from the system into the Test Methodology block and System Test testCase elements.

b) End-to-End functional test coverage of SCF threads over all levels of testing could be addressed in the System Test testCase elements for the respective SCF.

c) Test methodologies that include proper levels of testing and that the testing focus is appropriate at each level could be addressed in the Test Methodology block of the SCFTA model.

d) All essential functionality for intended flight operations could be addressed with the System Service block.

AC-17-01 then goes into FMET. Understanding the system's susceptibility to errors and faults is essential in determining that a system is safe. To demonstrate compliance with the various MIL-HDBK-516 Section 15 criteria involving FMET, a comprehensive suite of failure mode tests should be developed and executed at each integration level of the design (Airworthiness, 2017). The SCF Thread Layout model addresses this through the Test Methodology and Mitigation Test testCase. FMET test case results and methodology from the system model are to be embedded into the FMET block to establish compliance.

Following FMET is Safety Interlock Design. Interlocks are defined in MIL-HDBK-516C as system design mechanization to enable or disable systems, functions, subsystems, or modes at given times and conditions. A safety interlock is defined in MIL-HDBK-516C as an interlock that is necessary for the operation of one or more SCFs. For Airworthiness purposes, safety interlocks provide control over the functional operation of an SCF to ensure safe operation is maintained with proper mode engagement (or enabling of functionality) and disengagement (or disabling of functionality) (Airworthiness, 2017). To demonstrate compliance with MIL-HDBK-516 Section 15 criteria 15.2.6 and 15.5.4 involving safety interlocks, all safety interlocks associated with an SCF thread should be identified (Airworthiness, 2017).

AC-17-01 then goes into SPA and Software Development Processes. Numerous criteria in Section 15 evaluate the suitability of the development and V&V processes used for producing a system's SPA and software (Airworthiness, 2017). Numerous attributes

were identified in this stage of the process as it constitutes the bringing together of each of the above steps along with providing traceability between such.

The last focus area addressed in AC-17-01 is Full Qualification of Software. Full qualification of software is achieved when 100 percent of the software-level requirements are tested before the software is released for flight (Airworthiness, 2017). A lot of the attributes found in this area dealt with the verification of software to the requirements.

The attributes listed below were identified as an area to be applied to a digital environment found from the various focus areas just discussed. Each attribute has been either directly copied from the AC or interpreted from the AC and re-written. The list in this research does not cover all process and product attributes identified within the AC. Any missing attributes from those listed in the AC were either seen as a duplication from a previous section, or that the task would be completed within a step already portrayed in the profile. For further clarification of any of the attributes, it is recommended to review the appropriate section within the AC. The attributes in Table 1 have been grouped together under the seven focus areas for readability.

Table 1. AC-17-01 To-Be Modeled SCF Attributes from Task Clarification

1	SCF Identification
1.1	SCFs in a system need to be identified and set apart from other functions
1.2	SCFs are identified by the program's System Safety process
1.3	SCFs need to trace back to their origin in the System Safety process
1.4	SCF analysis is to be supported by engineers from various technical disciplines
1.5	SCFs for a given system will be unique to each platform
1.6	SCFs are often put in a list format

1.7	SCFs can be categorized: Flight Critical, Operation Critical, Emergency Critical, Indication Critical, and Avoidance Critical.
2	SCFTA
2.1	Decompose: Identify all elements, components and interfaces that support the operation of a given SCF
2.1.1	Break down into sub-functions
2.1.2	Identify Safety Supporting Elements (SSEs)
2.1.3	Identify Safety Supporting Hardware Elements (SSHE)
2.1.4	Identify Safety Supporting Software Elements (SSSE)
2.2	Classify SSE
2.2.1	Mark CSIL Classification for SSE, SSHE, SSSE
2.2.2	Identify interfaces supporting an SCF
2.3	Analyzing V&V Coverage: The evidence that complete test coverage has been achieved from end-to-end across the SCF thread
2.3.1	Trace testing to supporting sub-function
2.3.2	Trace testing of SSE, SSHE, SSSE
2.3.3	Testing needs to be at system integration level, subsystem integration level, and box/LRU/LRM level
2.3.4	Requirements implemented through components that support an SCF are tagged as such
2.3.5	Requirements implemented through components that support and SCF are traced to the SCF
2.3.6	Traceability of SCF to supporting components
2.3.7	Traceability exists from Software to testing performed
2.3.8	Safety interlocks are identified, analyzed, and tested
2.3.9	Identified testing gaps noted
3	System and Software Integration
3.1	Identify the level of testing on software and hardware
3.2	Perform an impact analysis
4	FMET
4.1	Complete FMET Process
4.1.1	Identify FMET test case driver
4.1.1.1	System/sub-system requirements
4.1.1.2	Failure analyses
4.1.2	Determine level of testing

4.1.3	Develop test case for each level
4.2	Trace FMET test results to SCF
5	Safety Interlock
5.1	Identify the SI
5.1.1	Use SCFTA to scope where SI resides in design
5.1.2	Ensure traceability from SCF to SI
5.2	Analyze the SI
5.2.1	Provide SI condition table/state diagram
5.2.2	Perform coupling analysis
5.2.2.1	Indicate direct coupling influences from utilized signals
5.2.2.2	Indicate indirect coupling influences from functional dependencies
5.2.3	Ensure data is traceable to the specific interlock design mechanism
5.3	Test the SI
5.3.1	Test case needs to be traceable to the specific interlock design mechanism
6	SPA and Software Development
6.1	Identify key attributes about the software
6.1.1	Note development pedigree: developmental or non-developmental
6.1.2	Note CSIL
6.1.2.1	FOR FLIGHT CRITICAL SSSEs: software is given a CSIL assignment that establishes processes that include all unique Flight Critical process and product attributes identified in this attachment
6.1.3	Software supporting SCFs need to be identified as SSSEs
6.1.3.1	Number of SCFs supported by given SSSE is documented
6.2	Requirements are robust
6.2.1	Performance requirements identified and documented
6.2.2	Software requirements are established from a clear allocation of system/subsystem requirements
6.2.3	Software requirements trace to no more than, and no less than, one parent requirement
6.2.4	Requirements are clearly identified and delineated from design
6.2.5	Design timing requirements are defined and documented
6.3	Software is integrated and tested in multi-level approach with a minimum of three levels utilized: unit level, software integration level (including hardware-software integration), and CSCI/requirements qualification level testing
6.4	Coding standards supporting safety are utilized

6.5	Software safety process performed
6.6	Peer reviews conducted
6.7	Traceability database is utilized that facilitates linking of traceable objects
6.7.1	All traceable items (e.g., requirements, design, SCFs) can be captured in the database as a unique object that can be traced to multiple objects
6.7.2	Bidirectional traceability established from software requirements to parent requirements up through system requirements
6.7.3	Bidirectional traceability established from software requirements to design
6.7.4	Bidirectional traceability established from design to source code
6.7.5	Bidirectional traceability established from source code to test cases
6.7.6	Bidirectional traceability established from software requirements to test cases
6.7.7	Bidirectional traceability established from test cases to test procedures
6.7.8	Bidirectional traceability established from software requirements to supported SCFs
6.7.9	Bidirectional traceability established from test cases to supported SCFs
6.7.10	Bidirectional traceability established from source code to SCF threads
6.7.11	The trace to source code will support the SCFTA verification activity
6.7.12	All source code in a software flight release traces to a software requirement
6.8	System and Software V&V is conducted
6.8.1	Unit level testing performed when created (or modified) and results documented
6.8.2	Software design requirements are fully verified
6.8.3	System/subsystem performance requirements supported by software are verified
6.8.4	System/subsystem safety requirements supported by software are verified
7	Full Qualification of Software
7.1	Demonstrate that all changed software meets requirements
7.2	Demonstrate that all unchanged software continues to meet requirements
7.3	Perform a systematic verification of every software requirement on the target processing hardware configuration

4.3 Prescriptive Study: Conceptualization

As discussed in the methodology, the key factor to be addressed within the digital model was the identification of the SCF and how that SCF interacted within the System. Therefore, it was decided that a SysML profile would be created that would guide the aircraft designer in how to construct each SCF within the model and connect the SCF with the various elements of the System. An Airworthiness Certification Profile package was created to serve as the parent modeling aspect. The Profile package contains mechanisms that allow metaclasses from existing metamodels to be extended to adapt them for different purposes (Object Management Group, 2019). Each of the modeling aspects created for purposes within the airworthiness certification process are contained in this profile. The Profile package can be shared and loaded within a system model providing a system with the necessary stereotypes and formats to guide the system modeler how to meet various standards within the airworthiness process. As seen in Figure 9, the Airworthiness Certification Profile package is sub-divided into four packages: 1) System Model Example, 2) System Safety, 3) MIL-HDBK-516C, and 4) Custom Stereotypes.

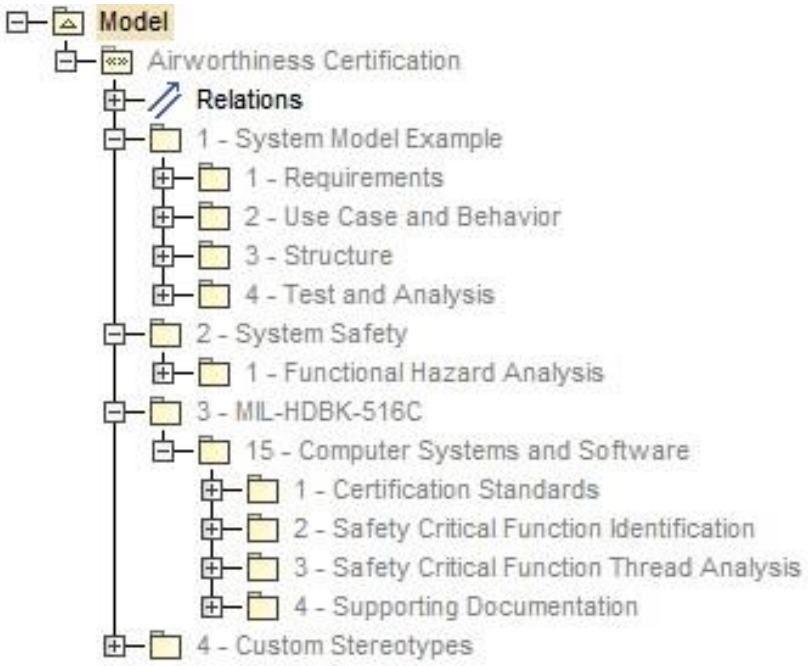

Figure 9. Airworthiness Certification Profile Containment Tree

The System Model Example is utilized in the profile simply as an example and does not direct how the System Engineering team should model their system. The intent of this portion of the Airworthiness Certification Profile is to show how the Profile can be used with a new aircraft model or incorporated into an existing model. The Profile is not set up to change or replace an existing model, but instead use of the example in the Airworthiness Certification Profile is to demonstrate how various elements from the model are utilized in the SCF thread. For the example, the package is further divided into four sub-packages: 1) Requirements, 2) Use Case and Behavior, 3) Structure, and 4) Test and Analysis. The Requirements represent all the requirements placed on the program. This includes, but is not limited to, the System Requirements, Safety Requirements, and Software Requirements. Use Case and Behavior represents the location of the use case diagram that describes the usage of a system (subject) by its actors (environment) to

achieve a goal, that is realized by the subject providing a set of services to selected actors (Object Management Group, 2019). The Structure represents the physical hardware and software components of the system and identifies how each interact within the system itself. Finally, Test and Analysis represents the Verification and Validation portions of the system. This includes, but is not limited to, test methodology, failure testing, mitigation testing, system testing, and software testing.

The System Safety package is also used as an example in the profile and does not direct how the System Engineering team should model their system. The System Safety was placed in the profile to represent an area for hazard identification and placement of the Functional Hazard Analysis (FHA). All other safety documentation and/or analysis can also be placed in this package as needed to allow for proper tracing between the system and its safety and development process.

The MIL-HDBK-516C package serves as the focal point of the Airworthiness Certification Profile. The current profile is set with only the elements from Section 15 – Computer Systems and Software per scope of the research. However, the package is designed to be expanded for each section. The Section 15 package contains four additional packages: 1) Certification Standards, 2) Safety Critical Function Identification, 3) Safety Critical Function Thread Analysis, and 4) Supporting Documentation.

Although not explicitly mentioned in AC-17-01, the Certification Standards package was one of the first portions of the model to be added. This was done by breaking down the standards and methods of certification identified in MIL-HDBK-516C Section 15 with the use of a requirements diagram. To separate a system requirement from a method of compliance, an Airworthiness Standard custom stereotype was created

with a stereotype extendedRequirement Generalization, see Figure 10. Then a Requirement Diagram was created that encompasses each respective standard and evaluation criterion, see Figure 11 for a snapshot portion of the requirement diagram.

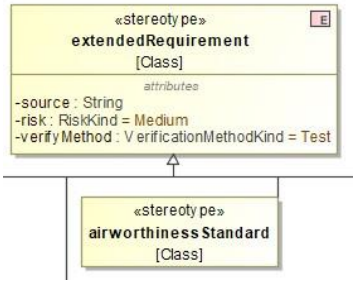

Figure 10. Airworthiness Standard Custom Stereotype

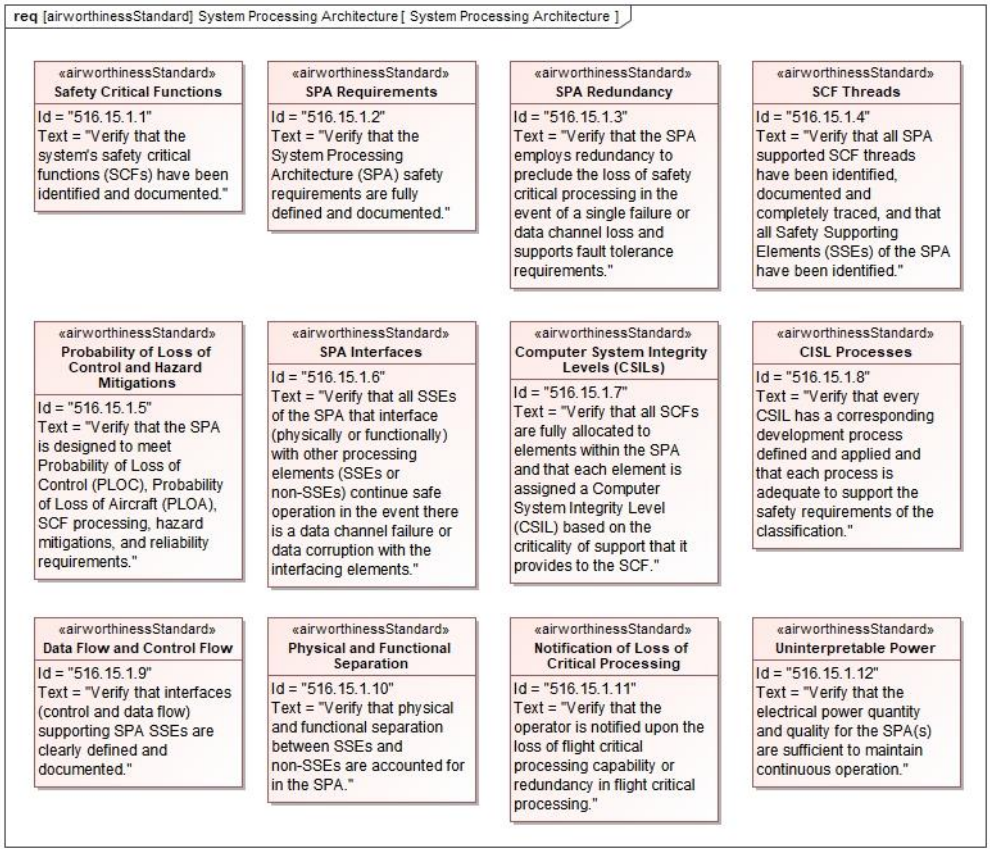

Figure 11. Portion of the MIL-HDBK-516C Section 15 Airworthiness Standard Requirement Diagram

Once the Airworthiness Standards were in place, the rest of the Profile was constructed against the To-Be Modeled Attributes from AC-17-01 listed in Table 1. As the model progressed, it was found that there was overlap between the focus areas discussed in the Task Clarification. Therefore, each portion of the model discussed below takes from Table 1 as a whole and combines those attributes that correlate with each other in the model design. Therefore, each diagram modeled answers multiple of the attributes found in AC-17-01. Individual Tables are provided for each section that identify what attributes were included in a particular design. Table 2 below shows the comparison of the AC-17-01 Focus Areas to the Profile model diagrams that are addressed throughout this research.

Table 2. Comparison of AC-17-01 Focus Areas to the Model Focus Areas

AC-17-01 Focus Areas	**Model Focus Areas**
SCF Identification	Certification Standards
SCF Thread Analysis	SCF Identification
Integration Methodology	SCF Thread Analysis
Failure Mode and Effects Testing	Physical System
Safety Interlock Design	Computer System Integration Level
SPA and Software Development	Validation and Verification
Full Qualification of Software	Failure and Effects Testing
	Safety Interlock Design
	Requirement Mapping

The first task to be modeled was SCF Identification. The identification of SCFs is critical to understanding the focus area of airworthiness-oriented functionality. All criteria in Section 15 indirectly rely on SCF identification since the criteria are to be applied to equipment supporting SCFs (Airworthiness, 2017). AC-17-01 Attachment 1

contains detailed guidance regarding SCF identification. The SCF Identification package was created and a Critical Functional Decomposition Block Definition Diagram (BDD) was generated. The attributes listed in Table 1 were evaluated against SCF Identification and those listed below in Table 3 were the decided attributes to model in the Critical Function Decomposition BDD.

Table 3. AC-17-01 Critical Functional Decomposition Block Definition Diagram Attributes

1	SCF Identification
1.1	SCFs in a system need to be identified and set apart from other functions
1.2	SCFs are identified by the program's System Safety process
1.4	SCF analysis is to be supported by engineers from various technical disciplines
1.5	SCFs for a given system will be unique to each platform
1.6	SCFs are often put in a list format
1.7	SCFs can be categorized: Flight Critical, Operation Critical, Emergency Critical, Indication Critical, and Avoidance Critical.

The SCFs are identified by the program's System Safety process (Attribute 1.2) and are originated in the Functional Hazard Analysis (FHA), which lays the foundation for identifying hazards within the system. Once the SCF's are identified within the system, the Profile models the SCF's by breaking them down into a functional decomposition BDD separated into hierarchical columns composed of the aircraft system, functional group, function, and sub-function (Attribute 1.1, 1.5, 1.6). Each function is displayed as blocks refactored and converted to activities. Each activity block is linked through a directed composition flowing from the aircraft system down to the lowest sub-function. Folders were used to group each portion of the model and any further comments

and/or notes may be added for clarification. See Figure 12 for the BDD utilized in the Profile. SCF's are then identified using a custom stereotype and can be highlighted a separate color for ease of recognition (Attribute 1.1). To model the SCF Decomposition diagram, the Profile uses a Safety Critical Function custom stereotype that Extends to Metaclass Action and Metaclass Class with appropriate attributes. Enumerations for Safety Critical Function Category (Attribute 1.7) and Severity (Attribute 1.1) are also used to provide tags to further classify the SCF. See Figure 13 for the custom stereotype used within the Profile. With the use of the Profile, engineers from various technical disciplines have ready access and ease of SCF identification (Attribute 1.4).

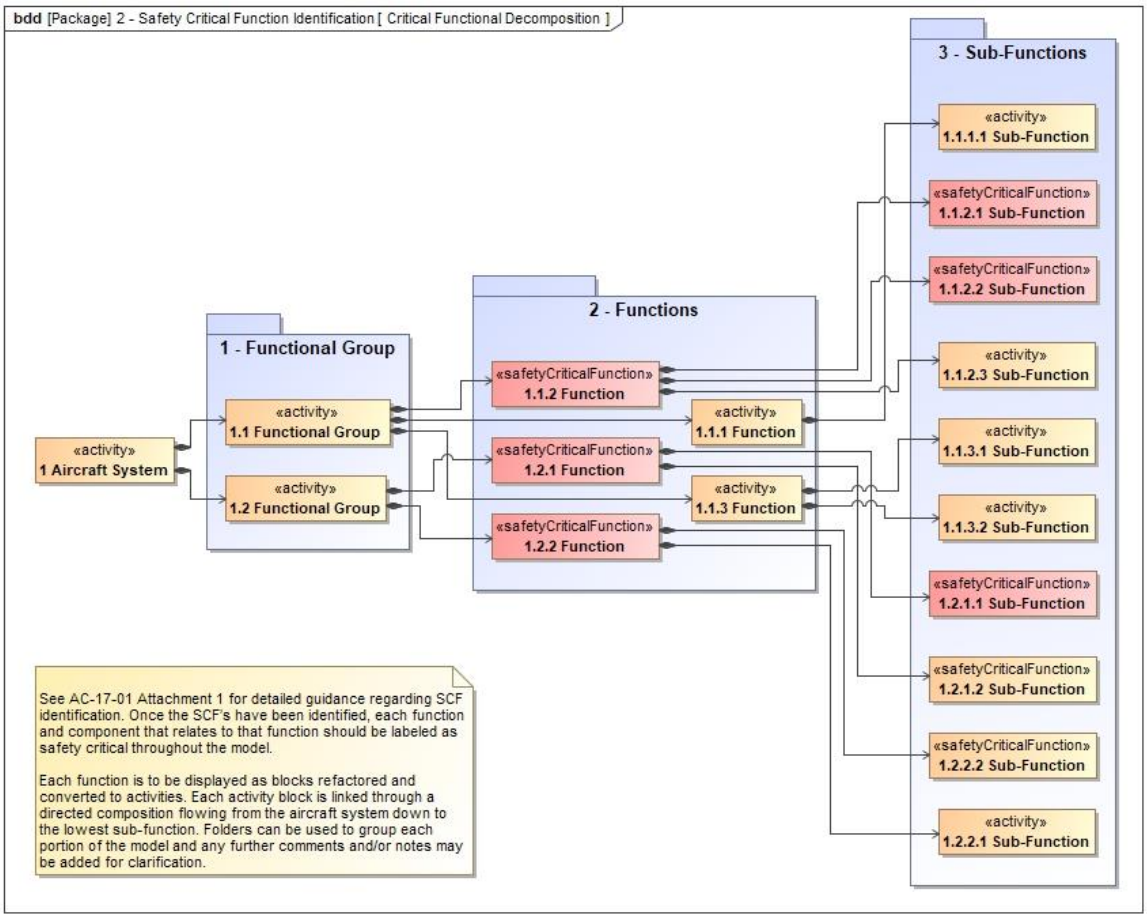

Figure 12. Safety Critical Functional Decomposition with SCF identified using a custom stereotype and highlighted in red.

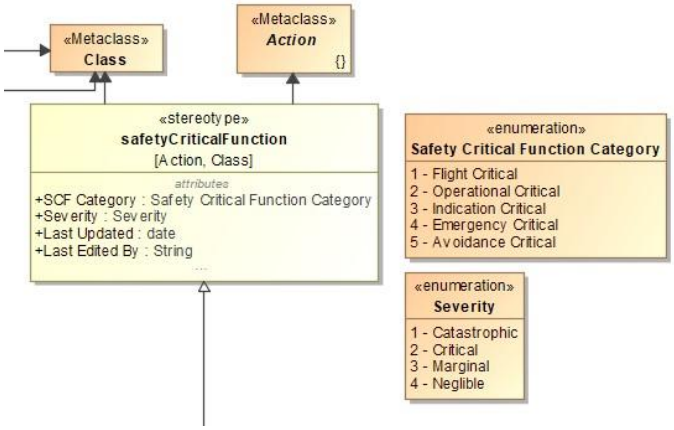

Figure 13. SCF custom stereotype used to classify the critical functions identified.

The Safety Critical Functional Thread Analysis package was next created to contain an SCF Thread Layout diagram that links each of the segments that the SCF interacts with within the system. An SCF thread is defined in MIL-HDBK-516C as: the combination of elements/components within a system and the required interfacing and interaction of those elements/components whose overall contribution is necessary for the operation of a given SCF (Airworthiness, 2017). The guidance given in AC-17-01 elaborates on particular airworthiness certification requirements that focus on design contributions that the hardware and software must provide to the system architecture in support of Safety/Flight Critical functionality, as well as key verification activities that are needed to evaluate the safety risk associated with the system design (Airworthiness, 2017). See AC-17-01 Attachment 2 for further clarification on SCF thread analysis.

For the SCFTA, Table 4 was constructed with the various attributes that were discovered to provide the details required for the thread analysis. To generate an SCF thread, the Airworthiness Certification Profile utilizes a second BDD called SCF Thread Layout embedded within the activity block of the respective SCF sub-function identified and displayed in the functional decomposition described above. A BDD was used to capture the SCF Thread as a combination of elements/components within a system and the required interfacing and interaction of those elements/components as defined in AC-17-01 (Airworthiness, 2017). The BDD intent was to focus not only on the physical hierarchy, but on all aspects of the function to include the requirements, use case, hazards, and artifacts generated. The thread layout does allow for hyperlinks to Internal Block Diagrams, Activity Diagrams, State Machine Diagrams, etc. needed to fully define the functional thread. Therefore, in meeting typical behavioral modeling, an Activity

Diagram could be used in addition to the BDD for the SCF Thread interaction with the system. For the Activity Diagram, SysML partitions, known as swim lanes, could be used to allocate hardware and software elements to the function. The SysML partitions display the functions/activity being modeled using the physical system blocks which accomplishes the same allocate relationship as if using a BDD. The full SCF Thread Layout for the given SCF 1.1.2.1 Sub-Function can be seen in Figure 14.

Table 4. AC-17-01 To-Be Modeled Attributes for SCF Thread.

1	SCF Identification
1.3	SCFs need to trace back to their origin in the System Safety process
2	SCFTA
2.1	Decompose: Identify all elements, components and interfaces that support the operation of a given SCF
2.1.1	Break down into sub-functions
2.3	Analyzing V&V Coverage: The evidence that complete test coverage has been achieved from end-to-end across the SCF thread
5	Safety Interlock
5.1	Identify the SI
5.1.1	Use SCFTA to scope where SI resides in design
5.1.2	Ensure traceability from SCF to SI
6.7.8	Bidirectional traceability established from software requirements to supported SCFs

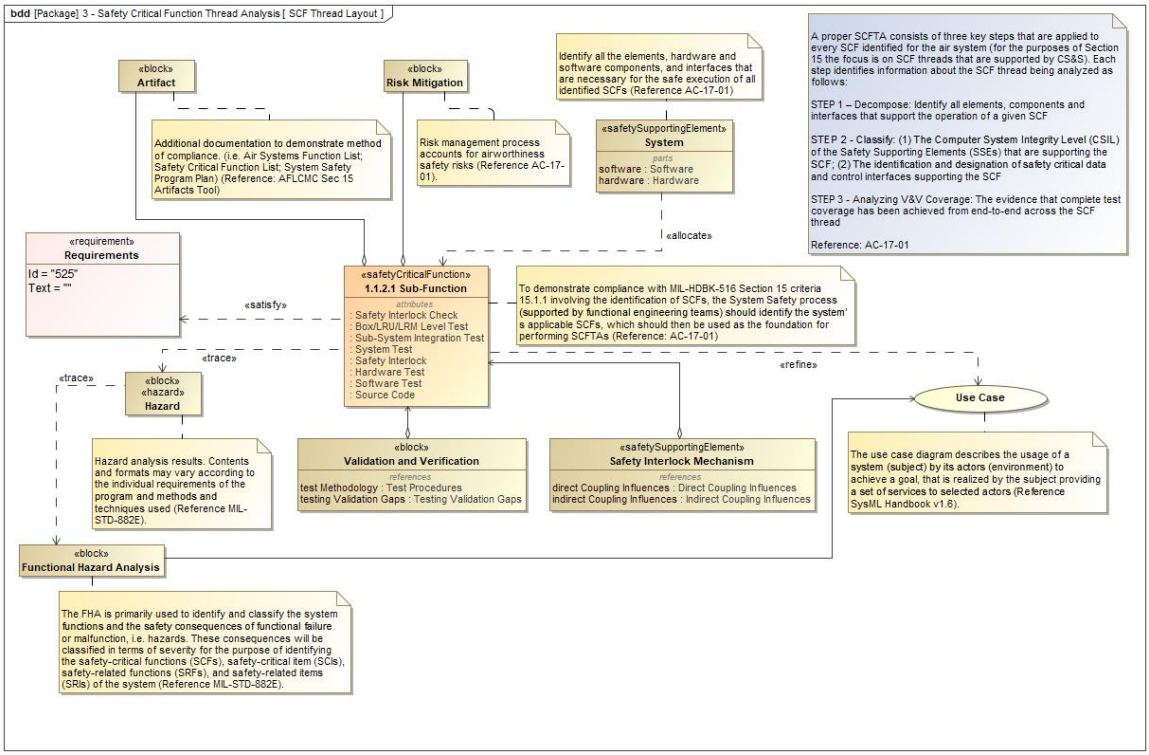

Figure 14. SCF Thread Layout from Airworthiness Certification Profile that Displays the Full SCF Thread of an SCF.

To provide full understanding of how the SCF operates within the system, the SCF Thread Layout centers around a single SCF Sub-Function displayed as an activity block (Attribute 2.1.1). To accomplish this understanding, a trace relationship is generated from the SCF Sub-Function back to the originating Hazard block (Attribute 1.3). The Hazard block can be used to characterize the hazard identified in the FHA, or the functional flow of the hazard with a hyperlinked Activity Diagram. The Hazard is then traced back to the Functional Hazard Analysis block to provide insight into the origination of the SCF from the System Safety review (Attribute 1.3). To provide understanding of where the SCF Sub-Function is within the design, the SCF is also tied to

the respective Use Case through a refine relationship. The physical architecture, represented by a System block, is utilized to identify all elements, components and interfaces that support the operation of a given SCF System (Attribute 2.1). Where the SCF Sub-Function must pass multiple testing procedures, the results of each Validation and Verification exercise are displayed as a block with an aggregation back to the SCF Sub-Function (Attribute 2.3). Any Safety Interlock Mechanisms are also displayed on the SCFTA through an aggregation back to the SCF Sub-Function (Attribute 5.1, 5.1.1). Requirements being met by the SCF are displayed through a satisfy relationship between the SCF and the various requirements being met (Attribute 6.7.8). Beyond AC-17-01, both an Artifact and Risk Mitigation block were placed on the diagram to link documentation created through the analysis of the SCF.

Furthermore, the SCF is also related through a satisfy relationship to requirements utilized to mitigate the identified system hazards and meet environmental and occupational hazards. The Safety Requirements can be either derived from the System Requirements or stand alone. Then where the SCF is utilized to satisfy either a safety requirement or a System Requirement, these requirements are given a safety requirement stereotype to indicate their relationship to an SCF. Finally, SCF Sub-Functions are displayed through an aggregation to the SCF to allow further relationship mapping between each.

Going beyond the initial identification of the SCF for the System, it is also important to show how it operates in the system. The first is to identify all the elements, hardware and software components, and interfaces that are necessary for the safe execution of all identified SCFs (Airworthiness, 2017). In the Profile, a hyperlink is

attached to the System block of the respective SCF Sub-Function that links to a Physical System Decomposition BDD. This Physical System Composition is then utilized to further answer various AC-17-01 attributes listed in Table 5. Figure 15 shows the Physical System Composition BDD as depicted in the Profile.

Table 5. AC-17-01 To-Be Modeled Attributes for Physical System Composition

2	SCFTA
2.1	Decompose: Identify all elements, components and interfaces that support the operation of a given SCF
2.1.1	Break down into sub-functions
2.1.2	Identify Safety Supporting Elements (SSEs)
2.1.3	Identify Safety Supporting Hardware Elements (SSHE)
2.1.4	Identify Safety Supporting Software Elements (SSSE)
2.2	Classify SSE
2.2.1	Mark CSIL Classification for SSE, SSHE, SSSE
2.2.2	Identify interfaces supporting an SCF
2.3.6	Traceability of SCF to supporting components
6	SPA and Software Development
6.1	Identify key attributes about the software
6.1.1	Note development pedigree: developmental or non-developmental
6.1.2	Note CSIL
6.1.2.1	FOR FLIGHT CRITICAL SSSEs: software is given a CSIL assignment that establishes processes that include all unique Flight Critical process and product attributes identified in this attachment
6.1.3	Software supporting SCFs need to be identified as SSSEs
6.1.3.1	Number of SCFs supported by given SSSE is documented
6.4	Coding standards supporting safety are utilized
6.5	Software safety process performed
6.6	Peer reviews conducted
6.7.4	Bidirectional traceability established from design to source code
6.7.5	Bidirectional traceability established from source code to test cases
6.7.10	Bidirectional traceability established from source code to SCF threads
6.7.11	The trace to source code will support the SCFTA verification activity
6.7.12	All source code in a software flight release traces to a software requirement

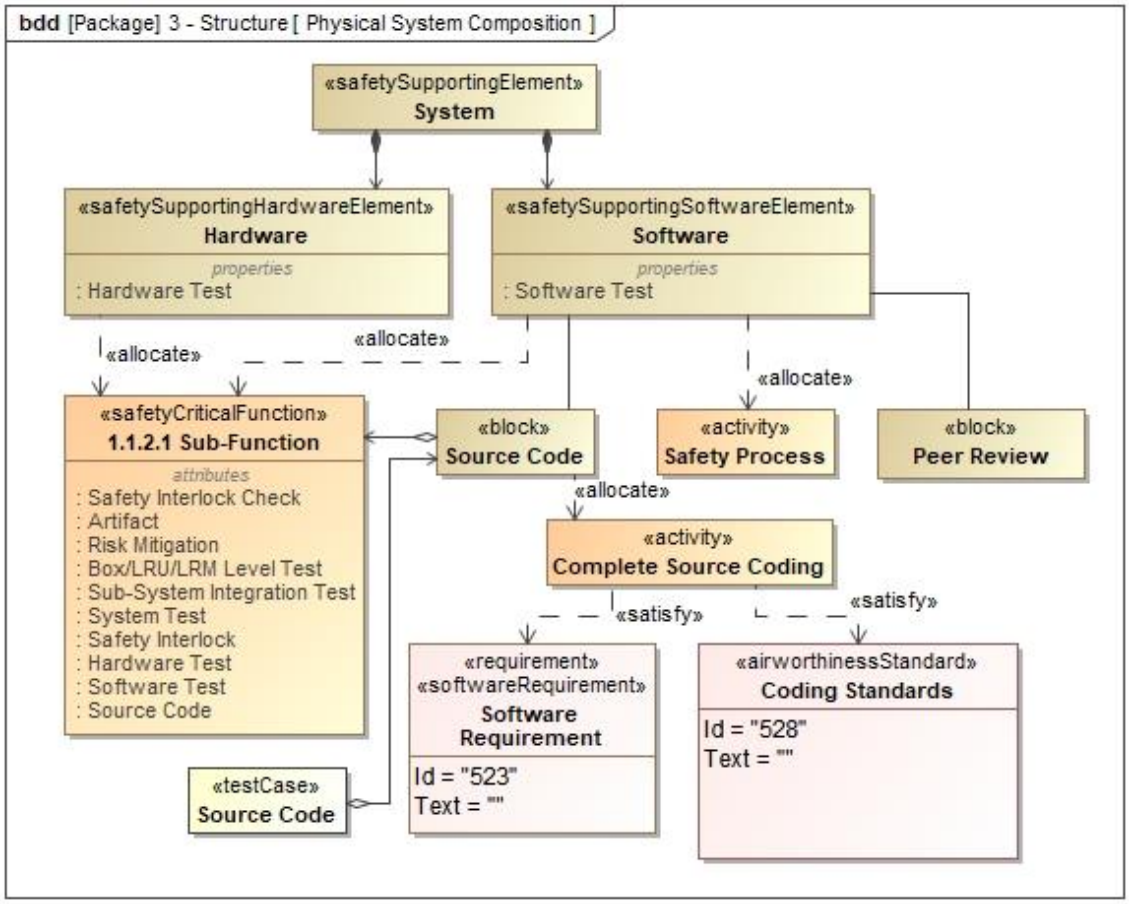

Figure 15. Physical System Composition BDD portion of the SCF Thread Layout model that shows the relationship between the physical system and the function.

For the Physical System Composition BDD, the Safety Supporting Elements (SSE), Safety Supporting Hardware Elements (SSHE), and Safety Supporting Software Elements (SSSE) that enable the operation of the SCF Sub-Function (Attribute 2.1) are identified within the system(Attribute 2.1.2, 2.1.3, 2.1.4), given the appropriate stereotype seen in Figure 16, and allocated to the SCF Sub-Functions (Attribute 2.1.1, 2.3.6). The SSE, SSHE, and SSSE are brought into the Profile from the System Design Model. The Hardware block can each be further embedded with an Internal Block Diagram (IBD) to display the interfaces that support the given SCF Sub-Function

(Attribute 2.2.2). Additionally, the Software block can be further embedded with an IBD or Activity Diagram to display the innerworkings of the software (Attribute 6.1).

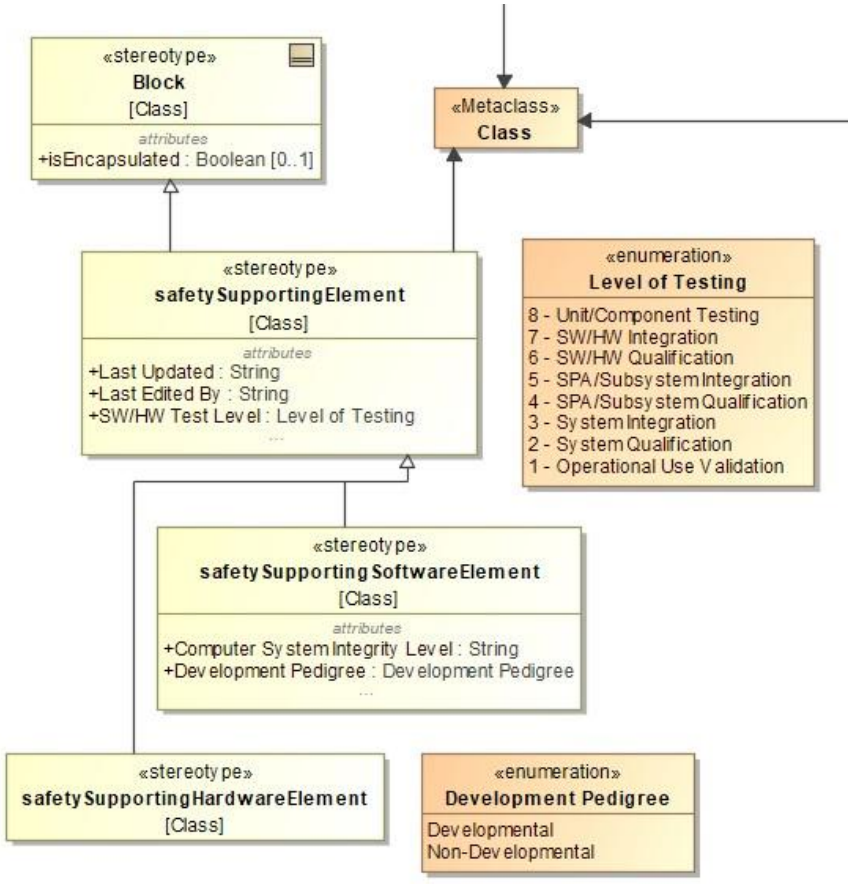

Figure 16. Safety Supporting Element Stereotype for Physical Hardware and Software Components Supporting an SCF

The second purpose of the SCFTA is ensure the identified elements and components are developed at Computer System Integrity Levels (CSILs) appropriate for SCF applications, and that safety critical interfaces are identified as such (Airworthiness, 2017). To accomplish this in the SCF Thread Layout model, each portion of the physical architectural system that interacts with the SCF is given the appropriate safety critical

stereotype (Attribute 2.2.1). As depicted in Figure 15 above, the portion of the system that interacts with the SCF is given a safety supporting element stereotype. The Software and Hardware that enable the SCF are also given a custom stereotype of safety supporting software element and safety supporting hardware element respectively to differentiate the components from other portions of the design (Attribute 2.1.2, 2.1.3, 2.1.4, 6.1.3). Additionally, tags for the level of testing, software development pedigree, and the CSIL can be inputted into the stereotype to ensure the identified elements and components are developed at the appropriate levels (Attribute 6.1.1, 6.1.2, 6.1.2.1).

Staying within the Physical System Composition, the software portion of the architecture traces to the source code and safety standards are utilized with the coding in addition to all Safety Processes (Attribute 6.4, 6.5). Any Peer Reviews conducted on the coding are also associated with the software (Attribute 6.6). For the source code, bidirectional traceability is established from the design to the source code through association (Attribute 6.7.4). Bidirectional traceability is also established from the source code to source code test cases and SCF with aggregation (Attribute 6.7.5, 6.7.10). These traces with the source code will support the SCFTA verification activity (Attribute 6.7.11). Furthermore, all source code for the software allocates to the coding activity that in turn satisfies the appropriate Software Requirement (Attribute 6.7.12).

The third purpose of the SCFTA is to verify that end-to-end V&V coverage is achieved by the tests used to verify the SCF functionality (Airworthiness, 2017). To accomplish this in the SCF Thread Layout model, the testing event(s) that have occurred for the SCF functionality are displayed within the Validation and Verification block on

the SCF Thread Layout. The Validation and Verification block contains a hyperlink to a Validation and Verification BDD specific to the SCF Sub-Function as seen in Figure 17.

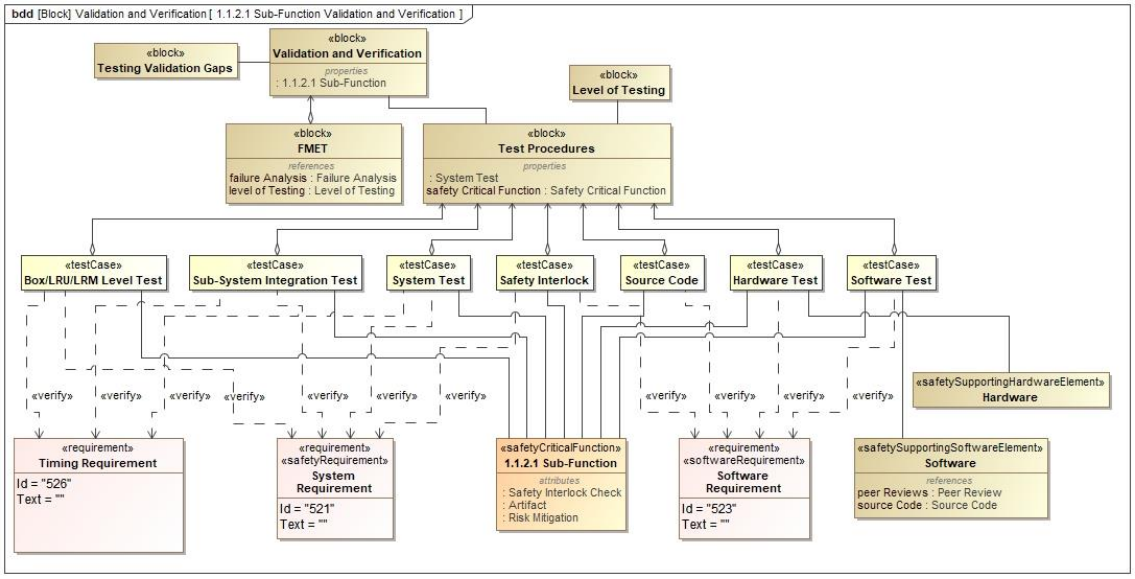

Figure 17. SCF Test Methodology and System Test portion of the SCF Thread Layout model.

In verifying the end-to-end V&V portion of the model, the Validation and Verification BDD helps answer additional attributes from AC-17-01 listed in Table 6. This BDD allows for systematic testing of every software requirement on the associated hardware for the intended SCF Sub-Function (Attribute 6.8, 7.3). Then the testing can be traced to the supporting SCF sub-function, SSHE, and SSSE through an association between the SCF or component and the respective test cases (Attribute 2.3.1, 2.3.2, 2.3.7, 6.7.9). The Validation and Verification BDD also utilizes a block for Test Procedures to be embedded in which each test case is aggregated to. The Test Procedures establish the Level of Testing to be completed (Attribute 2.3.3, 3.1, 6.7.7, 6.8.1). Additionally, test cases are established for system integration level, subsystem integration level, and

box/LRU/LRM level (Attribute 2.3.3). The respective requirement that each test case verifies is also displayed in this BDD (Attribute 6.7.6). Finally, the Validation and Verification BDD tests safety interlocks identified for the SCF and any testing gaps throughout the process can be noted (Attribute 2.38, 2.3.9). Overall, by linking the test events into the SCF Thread Layout model it allows airworthiness review personnel the ability to easily verify that end-to-end V&V coverage is achieved by the tests used to verify the SCF functionality.

Table 6. AC-17-01 To-Be Modeled Attributes for Validation and Verification

2.3	Analyzing V&V Coverage: The evidence that complete test coverage has been achieved from end-to-end across the SCF thread
2.3.1	Trace testing to supporting sub-function
2.3.2	Trace testing of SSE, SSHE, SSSE
2.3.3	Testing needs to be at system integration level, subsystem integration level, and box/LRU/LRM level
2.3.7	Traceability exists from Software to testing performed
2.3.8	Safety interlocks are identified, analyzed, and tested
2.3.9	Identified testing gaps noted
3	System and Software Integration
3.1	Identify the level of testing on software and hardware
6.7.6	Bidirectional traceability established from software requirements to test cases
6.7.7	Bidirectional traceability established from test cases to test procedures
6.7.9	Bidirectional traceability established from test cases to supported SCFs
6.8	System and Software V&V is conducted
6.8.1	Unit level testing performed when created (or modified) and results documented
7.3	Perform a systematic verification of every software requirement on the target processing hardware configuration

Another portion of the Validation and Verification BDD is the FMET. Understanding the system's susceptibility to errors and faults is essential in determining

that a system is safe. The Validation and Verification BDD contains a FMET block with a hyperlink to a FMET BDD seen in Figure 18 in which the FMET analysis for the specific SCF Sub-Function can be conducted.

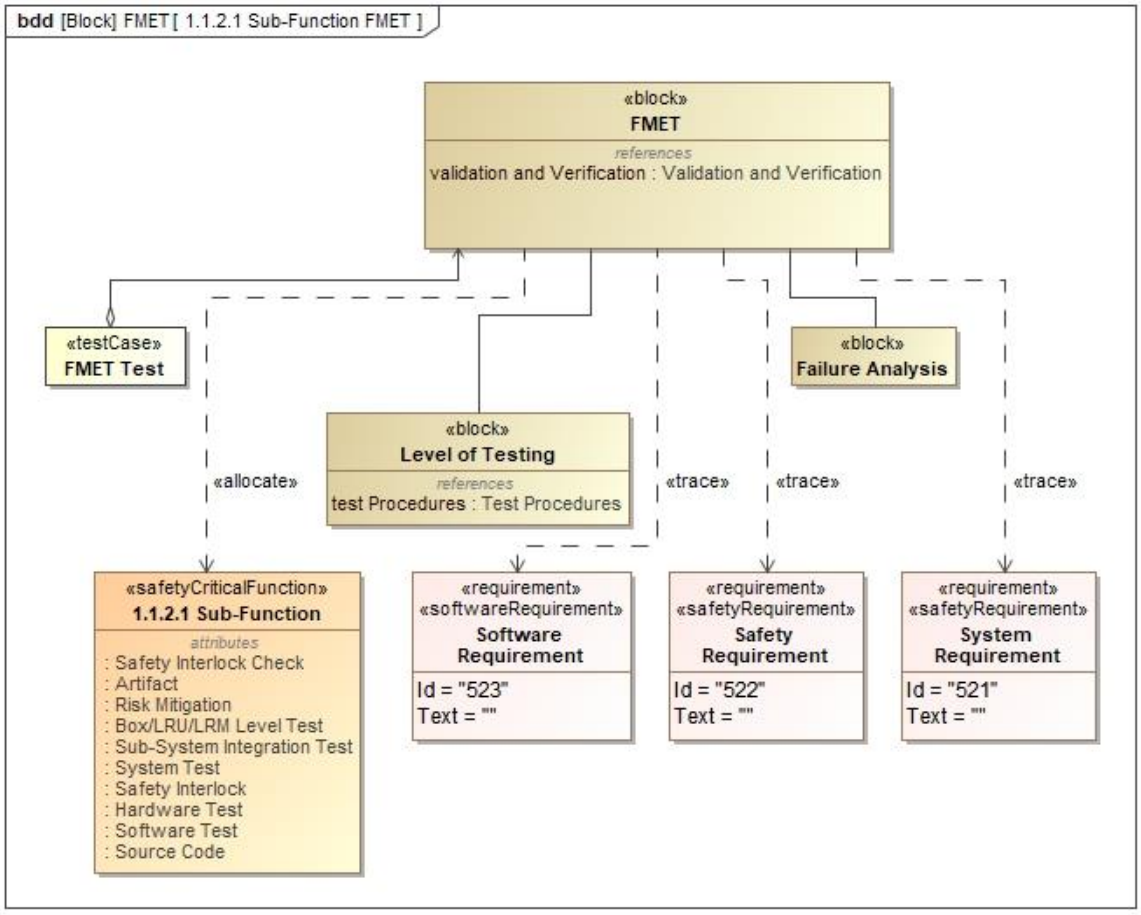

Figure 18. FMET BDD embedded in the FMET block which is contained within the Validation and Verification BDD

The FMET BDD addresses AC-17-01 attributes listed in Table 7. The FMET Process begins with identification of the level of testing, a trace to the respective requirements, and an association to the failure analysis (Attribute 4.1, 4.1.1, 4.1.1.1, 4.1.1.2). Then test cases are developed for each level and FMET cases are to be run at

every level (Attribute 4.1.2, 4.1.3). Each test result is traced back to the SCF through an allocation with the FMET block (Attribute 4.2).

Table 7. AC-17-01 To-Be Modeled Attributes for FMET.

4	FMET
4.1	Complete FMET Process
4.1.1	Identify FMET test case driver
4.1.1.1	System/sub-system requirements
4.1.1.2	Failure analyses
4.1.2	Determine level of testing
4.1.3	Develop test case for each level
4.2	Trace FMET test results to SCF

Another aspect of the SCF Thread Layout Model is the identification of a Safety Interlock Mechanism with the SCF Sub-Function. For Airworthiness purposes, safety interlocks provide control over the functional operation of an SCF to ensure safe operation is maintained with proper mode engagement (or enabling of functionality) and disengagement (or disabling of functionality) (Airworthiness, 2017). As seen in Table 8, various aspects of the safety interlock mechanism need to be modeled. This is done by first connecting the Safety Interlock Mechanism with the SCF Sub-Function through an aggregation on the SCF Thread Layout model (Attribute 5.1.1, 5.1.2). The Safety Interlock Mechanism is given the safety supporting element with a hyperlink to the Safety Interlock Mechanism BDD for the respective SCF seen in Figure 19.

Table 8. AC-17-01 To-Be Modeled Attributes for Safety Interlock.

5	Safety Interlock
5.1	Identify the SI
5.1.1	Use SCFTA to scope where SI resides in design
5.1.2	Ensure traceability from SCF to SI
5.2	Analyze the SI
5.2.1	Provide SI condition table/state diagram
5.2.2	Perform coupling analysis
5.2.2.1	Indicate direct coupling influences from utilized signals
5.2.2.2	Indicate indirect coupling influences from functional dependencies
5.2.3	Ensure data is traceable to the specific interlock design mechanism
5.3	Test the SI
5.3.1	Test case needs to be traceable to the specific interlock design mechanism

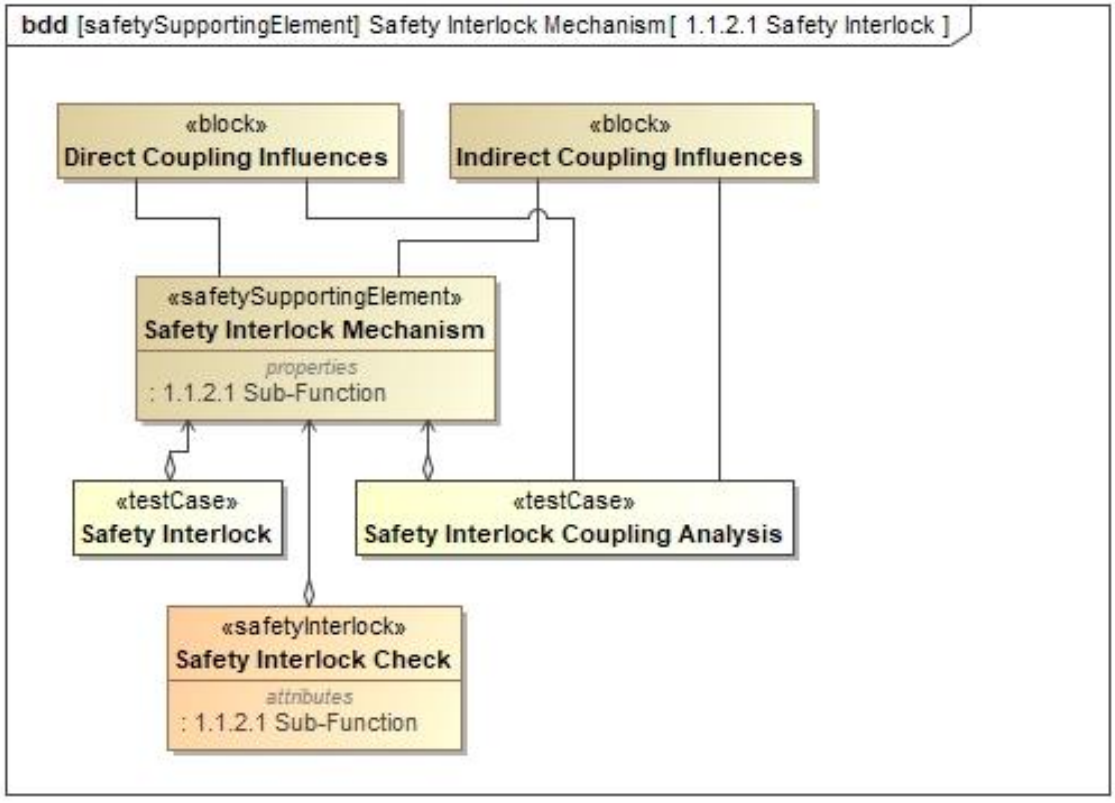

Figure 19. Safety Interlock Mechanism BDD for the specific SCF Sub-Function embedded in the Safety Interlock Mechanism block of the SCF Thread Layout.

The Safety Interlock Mechanism BDD connects the safety supporting element to its individual test cases and coupling analysis for direct and indirect influences (Attribute 5.2.2, 5.2.2.1, 5.2.2.2, 5.3.1). A table or state diagram can also be hyperlinked to the Safety Interlock Mechanism block as needed (Attribute 5.2.1). Finally, the BDD allows for the data surrounding the mechanism be traced back to the specific mechanism (Attribute 5.2.3).

The final piece of the SCF Thread Layout model was to incorporate each of the various requirements that connect with the individual SCF. To accomplish this, the SCF Thread Layout model uses a satisfy relationship between the SCF and the Requirements. To maintain simplicity of the model, a Requirement element is used on the SCF Thread Layout model that hyperlinks to a Requirement Diagram seen in Figure 20 that contains each of the Requirements associated with the SCF. The Requirement Diagram also helps to complete various attributes from AC-17-01. As seen in Table 9, multiple portions of the overall process stem back to the requirements.

One of the first steps was to identify each Requirement that supports an SCF (Attribute 2.3.4). This was done using a safety requirement stereotype that behaves as an extendedRequirement through a generalization link. The SCF Sub-Function then connects to each requirement through a satisfy link (Attribute 2.3.5). This satisfy link includes, but is not limited to Performance, Design, Timing, Software, Safety, and System requirements that have been identified and documented (Attribute 6.2.1, 6.2.4, 6.2.5). The diagram is also used to establish clear allocation of software requirements from system/subsystem requirements and where those software requirements trace back to (Attribute 6.2.2, 6.2.3). The diagram is also used to provide opportunity to showcase

software design requirement verification and traceability (Attributes 6.7.1, 6.7.2, 6.7.3, 6.8.2, 6.8.3, 6.8.4, 7.1, and 7.2).

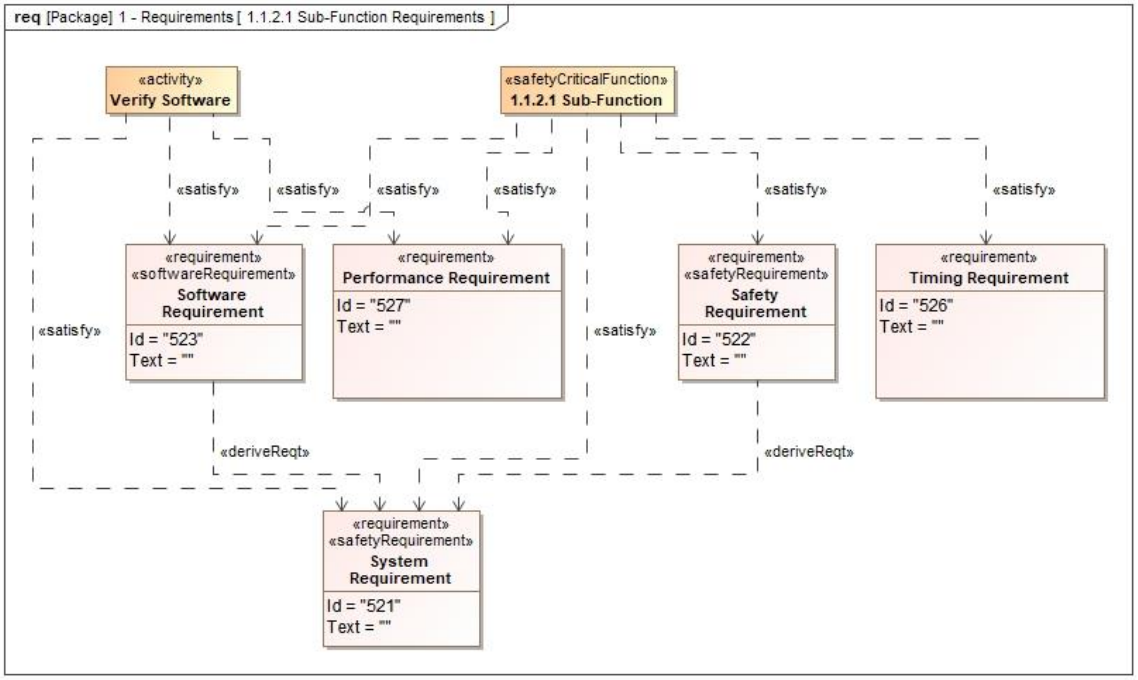

Figure 20. Requirement Diagram that shows which requirements the individual Sub-Function satisfy.

Table 9. AC-17-01 To-Be Modeled Attributes for Requirements.

2.3.4	Requirements implemented through components that support an SCF are tagged as such
2.3.5	Requirements implemented through components that support and SCF are traced to the SCF
6.2	Requirements are robust
6.2.1	Performance requirements identified and documented
6.2.2	Software requirements are established from a clear allocation of system/subsystem requirements
6.2.3	Software requirements trace to no more than, and no less than, one parent requirement
6.2.4	Requirements are clearly identified and delineated from design
6.2.5	Design timing requirements are defined and documented

6.7	Traceability database is utilized that facilitates linking of traceable objects
6.7.1	All traceable items (e.g., requirements, design, SCFs) can be captured in the database as a unique object that can be traced to multiple objects
6.7.2	Bidirectional traceability established from software requirements to parent requirements up through system requirements
6.7.3	Bidirectional traceability established from software requirements to design
6.8.2	Software design requirements are fully verified
6.8.3	System/subsystem performance requirements supported by software are verified
6.8.4	System/subsystem safety requirements supported by software are verified
7	Full Qualification of Software
7.1	Demonstrate that all changed software meets requirements
7.2	Demonstrate that all unchanged software continues to meet requirements

4.4 Application of Profile Against UAS Reference Architecture

The MBSE UAS Reference Architecture used in this study was originally created for a three-part course series taught within the Systems Engineering Department at AFIT. Throughout each UAS course, students address systems engineering concepts such as mission analysis, requirements refinement, system design, and validation and verification. The final culminating event leads to a product build and flight test of the designed UAV.

The mission of the small UAS seen in Figure 21 was to provide forward deployed ground-based units the capability to conduct low altitude, intelligence, surveillance, and reconnaissance (ISR), and small payload deployment operations from a safe standoff distance. The UAS was constructed to operate using both auto-pilot and manual operations. Students would utilize the MBSE Reference Architecture throughout the course to identify the system components necessary to complete the mission. As the

physical UAV is being developed, a digital model of the system and its interactions was evaluated for pre-built analysis and study.

Figure 21. Small UAS Used for AFIT UAS Instructional Course Series.

To begin, the Airworthiness Certification Profile was loaded into the UAS Reference Architecture. Then, in utilizing the UAS Reference Architecture, and in following the design of the Airworthiness Certification Profile, the UAS was broken down into its mission functions grouped by Functional Group, Function, and Sub-Function. Those functions determined as Safety Critical were given the safety critical function stereotype from the custom stereotypes in the Profile and were highlighted in red as seen in Figure 22.

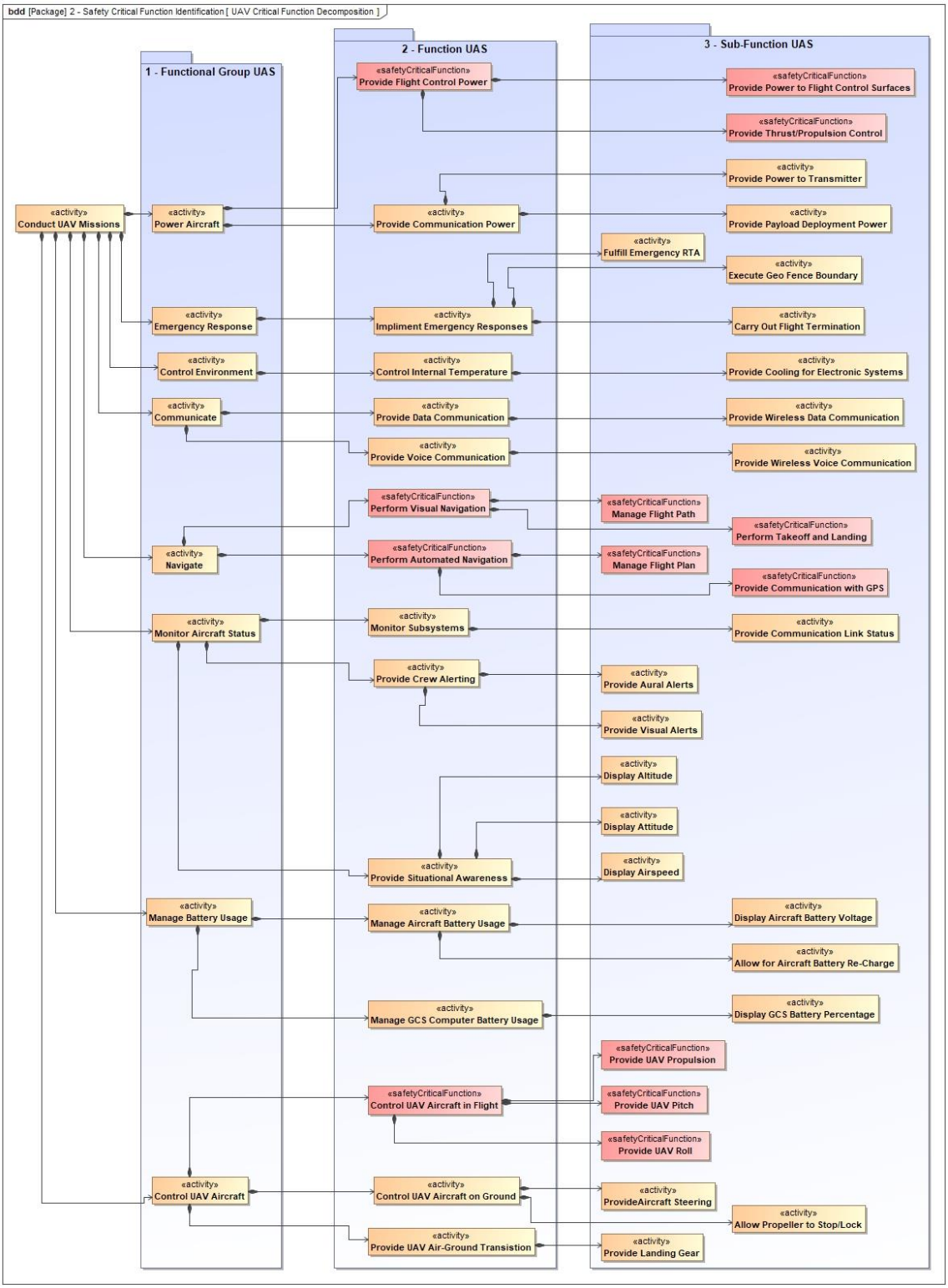

Figure 22. UAS Safety Critical Function Decomposition utilizing the Custom Stereotypes from the Airworthiness Certification Profile.

In maintaining the format of the Airworthiness Certification Profile, following the identification of each SCF, an SCF Thread Analysis was conducted on the SCF Sub-Functions. For this research, the *Provide UAV Propulsion* Sub-Function of the *Control UAV Aircraft in Flight* Function was chosen. The *Provide UAV Propulsion* Sub-Function seen in Figure 23 was brought into an SCF Thread Layout BDD as depicted in the Profile and further broken down into the various elements that define and support the function.

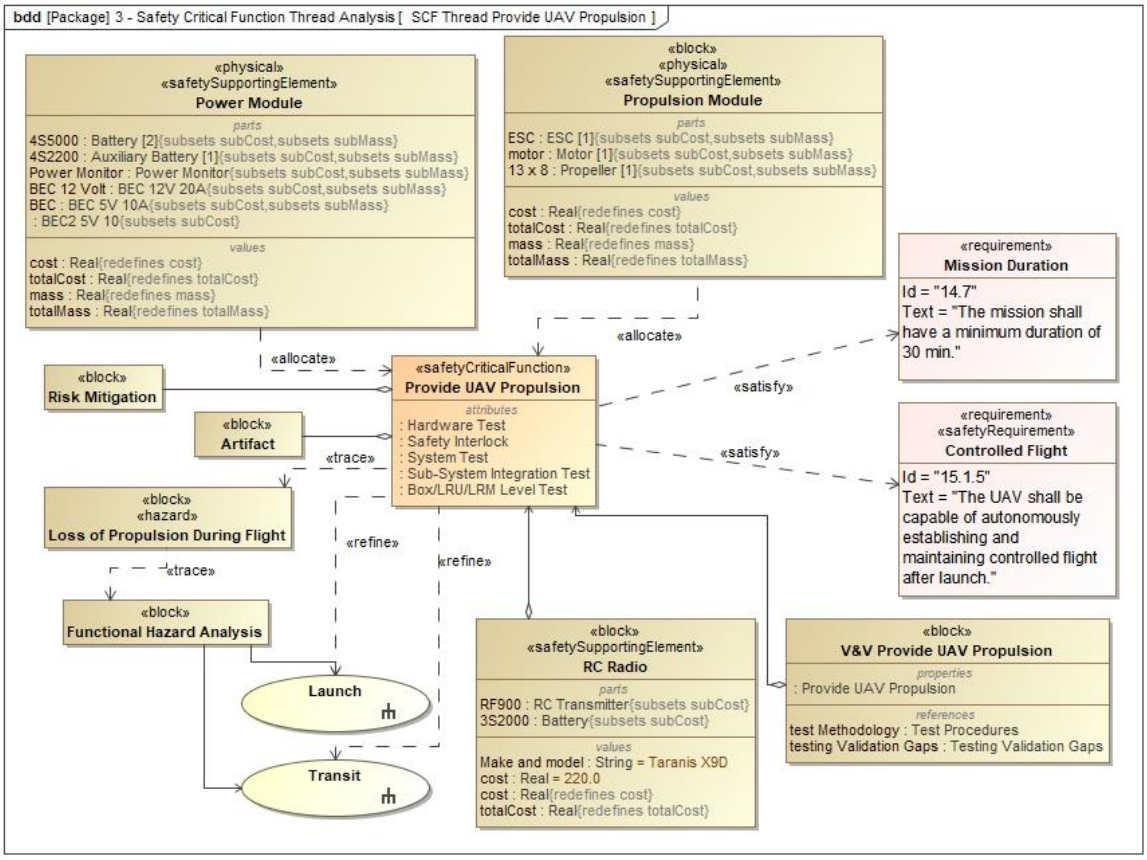

Figure 23. SCF Thread for Provide UAV Propulsion SCF Sub-Function.

In following the criteria laid out in AC-17-01, the first goal of the SCF Thread is to identify the components that enable the function to occur. For the Provide UAV Propulsion SCF Sub-Function, the Propulsion Module elements from the Physical

Architecture portion of the System Model were added to the thread. Then, where the Propulsion Module is designated as supporting an SCF, the Propulsion Module was stereotyped as a safety supporting element. A hyperlink was then added to the Propulsion Module block to a Propulsion Model BDD that further identified the components that make up the Propulsion Module as seen in Figure 24. This included the Electronic Speed Controller (ESC), Motor, and Propeller. Each of these individual components were then designated as safety supporting hardware elements and were allocated back to the Provide UAV Propulsion SCF Sub-Function for relationship continuity.

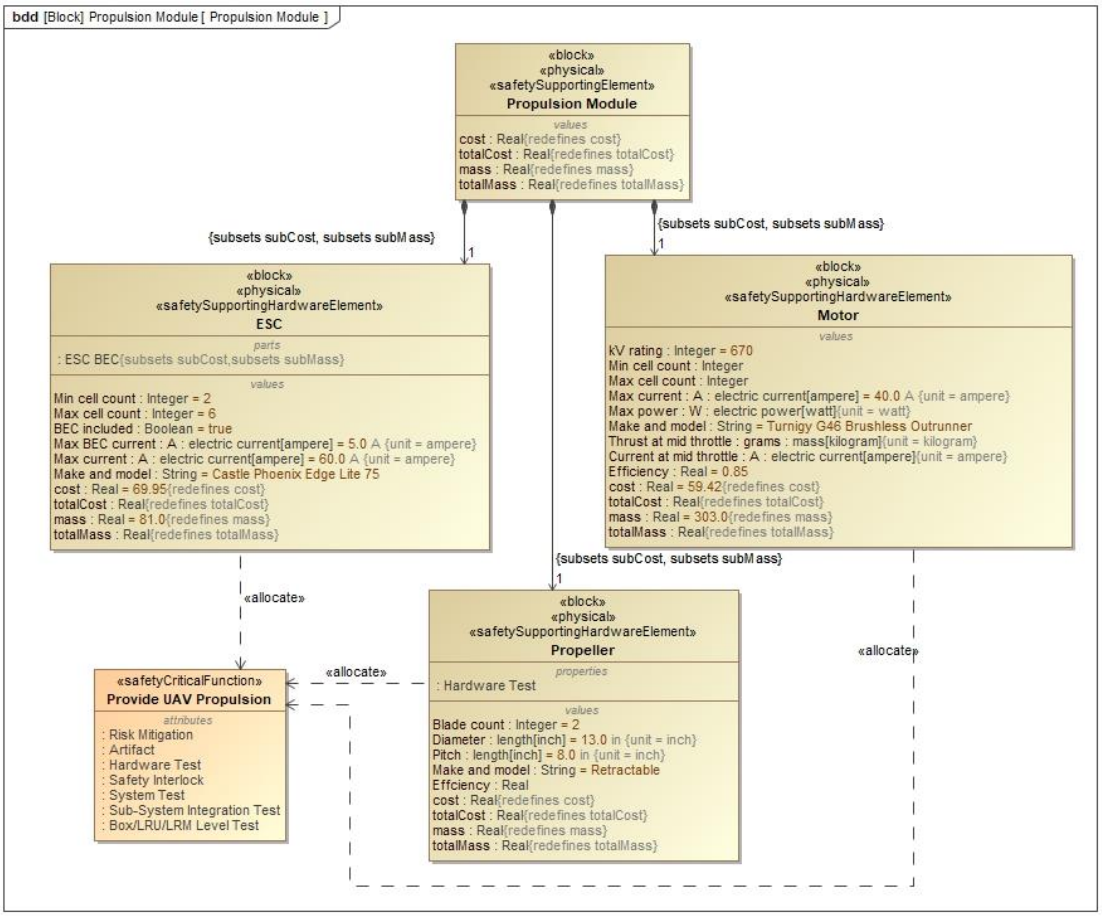

Figure 24. Physical Structure Portion of the Safety Critical Thread that shows the Allocation of the SSHE to the SCF.

Another step in the SCF Thread is the identification and linking of the SCF Sub-Function to the Validation and Verification efforts completed. From Figure 23, the Validation and Verification is represented as a block to match with the SCF Thread Layout in the Profile. That Validation and Verification block then hyperlinks to a separate Provide UAV Propulsion Sub-Function Validation and Verification BDD seen in Figure 25. Here the various testCase events conducted on the propulsion portion of the physical architecture are linked to the Provide UAV Propulsion Sub-Function. The Validation and Verification BDD also shows how each testCase is conducted to verify the Controlled Flight requirement.

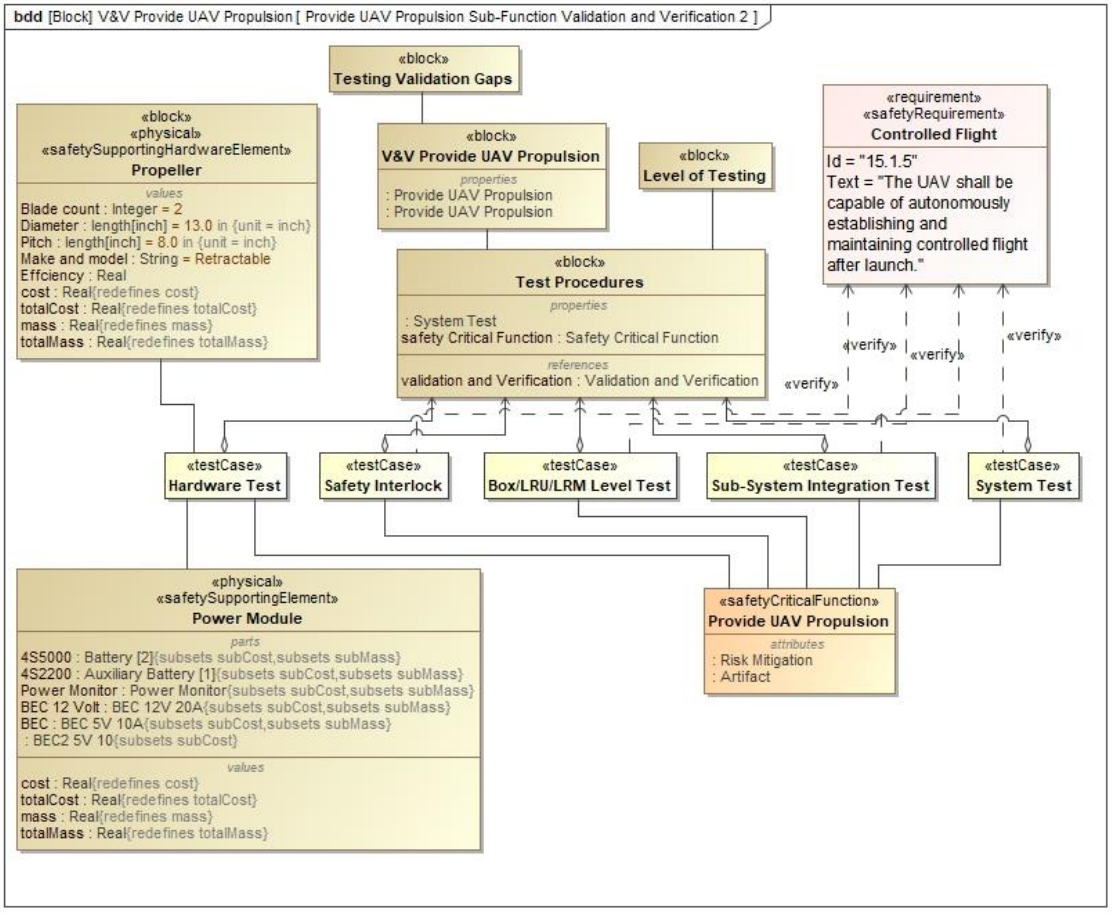

Figure 25. UAV Propulsion Validation and Verification Portion of the SCF Thread

4.5 Summary

This chapter provided details on the completion of the Prescriptive Study which included the task clarification and conceptualization portions of the study. Additionally, application of the study was completed against an established UAS Reference Architecture model. The task clarification segment concentrated on the seven focus areas discussed in AC-17-01 and each were addressed for better understanding of the design, development, integration, and V&V expectations related to Section 15. The conceptualization piece focused on the construction of the SysML Airworthiness Certification Profile. Finally, an application of the Profile against the UAS Reference Architecture as a proof of concept was conducted.

V. Conclusions and Recommendations

5.1 Chapter Overview

The preceding thesis outlines a tailored model-based system engineering (MBSE) solution to support Safety Critical Function (SCF) thread analysis against airworthiness criteria found in Section 15 of MIL-HDBK-516C. Within this scope, the research identified an SCF domain-specific profile and style guide using the Systems Modeling Language (SysML) and domain-specific extensions. The SCF profile was applied to an Unmanned Airborne System (UAS) designed and flight tested as a course sequence in AFIT's Graduate school. The contributions of this research identified: 1) how a system model can support the execution of the airworthiness process, 2) how modeling can be minimally stereotyped to support various airworthiness analyses, and where airworthiness analysis could be automated and leaned.

This chapter discusses how the three investigative questions from Chapter I were addressed using the SCF Profile design model completed in Chapter IV. Following the answers to the investigative questions, recommendations for action to be completed by the Air Force as it applies the SCF Profile model are provided. Finally, recommendations for future research for expanding and refining the SCF Profile model are provided.

5.2 Research Questions

The first question addressed throughout this research was what modeling aspects and/or program artifacts must be created to support the airworthiness certification process. In working with a SysML domain specific model, the digital tool provides a lot of built-in features that enable system design, system decomposition, and system

relationship traceability. However, one of the great powers of SysML is the ease in which a user can tailor the given language to meet the needs of an individual system model. For the Airworthiness Certification Profile created for this research, both built in and tailored domain specific extensions were utilized.

For the tailored domain specific extensions, there were multiple different modeling aspects created. The first was the creation of custom stereotypes to identify and define various aspects of the System. This included safety critical function, hazard, safety supporting element, safety supporting hardware element, safety supporting software element, airworthiness standard, safety requirement, and safety interlock. For the custom stereotypes, enumerations were also created and applied to tag and refine the stereotypes with various categories and specifications. Second, the safety and airworthiness standards and methods of compliance from DoD references were integrated into the system model utilizing a requirement diagram and distinguished with the airworthiness standard custom stereotype contained in the Profile. Third, each SCF identified in the System Safety Process was categorized through a decomposition of the system by way of Functional Group, Function, and Sub-Function. Fourth, a thread for each identified SCF was created to provide relationship mapping between the various elements and events that support the operation of a given SCF. Finally, SysML Analysis Diagrams are to be used with the System Model relationships to create reports necessary to show completion of the standards and methods of compliance required for the airworthiness certification.

The second question addressed through this research is what airworthiness analyses can be done with a SysML domain specific system model. The incorporation of a SysML domain specific digital model into the Airworthiness Certification Process

provides significant impact into various stages of the overall airworthiness analysis. The first is the opportunity for the Airworthiness Home Office to transfer use of the Artifacts Tool from a document-based environment into a model-based asset. With a model-based Artifacts Tool, Airworthiness Certification Officials can conduct their review using the very system model utilized by the developer of the aircraft. This analysis is completed using a Requirement Table that lists the Standards and Methods of Compliance along with a trace to various model relationships, how the standard is being verified, any risk associated with the standard, and how that standard is being verified in model. The Requirement Table works similar to the Excel version of the Artifacts Tool in use and would require minimal adjustment on the Certification Official.

The second analyses that can be done with a SysML domain specific system model is that of an Allocation Matrix. This matrix shows the allocated relationship between various pieces of the model. Commonly, it shows the allocation between the functions, or activities and the corresponding block in the model. This is important for quick and easy analysis to ensure that each function has a corresponding component that enables that function.

Finally, and probably most important, a SysML domain specific model allows the Airworthiness Certification Official to thoroughly analyze the SCF Thread. The digital model, when done correctly, establishes a relation map between each of the elements that creates the desired thread between the various portions of the model. With the SCF Thread, Airworthiness Certification Officials can identify the combination of elements/components within a system and the required interfacing and interaction of

those elements/components whose overall contribution is necessary for the operation of a given SCF as defined by MIL-HDBK-516C.

Finally, the third question addressed throughout this research was how could airworthiness analysis be automated or leaned to support parallel, continuous development operations. The intent of this question was to discover ways in which the model could generate an SCF analysis in a black box like environment without continuous user input. However, throughout this research, it was quickly discovered that to automate the process, a Profile first needs to be established that can contain the data and relationships necessary for automatic analysis. Therefore, there is not a direct answer for how the question was first intended and future work in this area is recommended.

On the other hand, from the perspective of an Airworthiness Certification Official, the generous capabilities of MBSE provide a more automated like insight into the Airworthiness Analysis than the documented approach in use. Throughout this research, MBSE has really become a positive approach to airworthiness certification through use of a model that comprises a coherent and consistent set of interlinked views that reflect multiple viewpoints of the system. By generating links between the elements, as a system is updated in a particular area, that update will be automatically reflected across each view in which that element is included. Furthermore, if a component or piece of software needs to be updated, the model can generate the impacted portions of the system through relation mapping that instantly informs users of the affected functions.

5.3 Recommendations for Action

With the creation of the Airworthiness Certification Profile, it is recommended that the Air Force take action to begin the implementation of the Profile into the Airworthiness Certification Process. To begin this transformation, it is recommended that the Profile be reviewed by the MIL-HDBK-516C Section 15 Airworthiness Certification Officials and Subject Matter Experts to ensure that each essential portion of the certification analysis is covered within the profile. Upon acceptance of the Profile, the Profile will need to be expanded to other Sections of MIL-HDBK-516C. Once each section of MIL-HDBK-516C is represented and the Profile is standardized, it is recommended that the Air Force utilize the Profile as an Airworthiness Certification Document to be issued to all contracted aircraft developers.

5.4 Recommendations for Future Research

Incorporate Rule Verification Coding into the SCF Thread Portion of the Airworthiness Certification Profile. With the myriad of attributes required for certification just coming out of Section 15, research could be conducted into a rule verification tool. This tool would run in the background but provide visual warnings and recommendations for any portions of the Profile properties that are not being followed. For example, one major portion of the SCF Thread is the allocation of the Hardware and Software to the SCF. Although it is common practice in SysML to allocate components to functions, it may not be known that those components that support an SCF need to be marked as an SSE. Right now, SysML does not give a confirmation or warning if an SCF supporting component is marked with this stereotype or not.

Develop Automation Capabilities within the Airworthiness Certification Profile. Although MBSE provides continuity between elements and diagrams through relationship mapping, there is potential for various Airworthiness Analysis that could be automated through a script generation. One such aspect is with a Report Generator. Although the model assists in SCF Identification within the system, there are still a lot of reports needed for the Airworthiness evaluation to include a risk estimate, function severity, and Compliance Report. As FMET events for software are conducted and hardware failure rates are identified, risk calculations against the safety of the system could be generated. Another automation feature within the Profile would be calculating the severity of a function. Where the identification of an SCF is so important to the safety of a System, it would be a valuable to have a more automated calculation of the severity of a function that fails to operate. Finally, the model could provide a way to capture the information mentioned and all additional evaluation material in a report that is acceptable by decision makers.

Review of Airworthiness Policy to Identify Redundancy when using MBSE. The approach of this research was to take pedigreed policy and convert it to a model-based environment. However, future research could look at the policy itself and pinpoint redundant information already captured in the model that could simplify the process or policy being examined. This could include removal of documents, redundant steps, or unnecessary artifact generation.

Incorporate Other Sections of MIL-HDBK-516C into the Airworthiness Certification Profile. For an airworthiness certification to be fully completed, each Section of MIL-HDBK-516C must be reviewed and signed off. This means that each

Section would need to be researched and the respective analysis and diagrams required to fulfill the Section Standards would need to be brought into the Profile.

Use of the Airworthiness Certification Profile in other Military and Commercial Sectors. Research could be conducted into the use of the Airworthiness Certification Profile for digital models outside of the Air Force Airworthiness Home Office. The Profile could easily be adapted for commercial aircraft and the incorporation of Federal Aviation Administration (FAA) documents. Additionally, the Profile could be adapted for the Airworthiness Certifications of Army, Navy, and Marine aircraft as well.

Is using model-based format better than using a document-based format? Research is needed to determine if replicating a document-based policy by using system models does make the process better. Perhaps there is something else that needs to change, whether in the process or automation, to achieve an improved course of action. Lessons could be learned from application of this model in Airworthiness Certification pilot projects.

5.5 Summary of Research

The current United States Air Force (USAF) airworthiness certification process, captured in MIL-HDBK-516C, is time-consuming and manpower intensive due to extensive documentation. To minimize inefficiencies of this document-based approach, this thesis examined MBSE to support SCF thread analysis against criteria found in Section 15 of MIL-HDBK-516C. Within this scope, the research identified an SCF domain-specific profile and style guide using the SysML and domain specific extensions.

The Airworthiness Certification Profile is a groundbreaking step forward for Airworthiness Certification. The Profile created for this research utilized both built in and tailored domain specific extensions to create modeling aspects and/or program artifacts within the certification process. The incorporation of a SysML domain specific digital model into the Airworthiness Certification Process provides significant impact into various stages of the overall airworthiness analysis. This includes the opportunity for the Airworthiness Home Office to transfer use of the Artifacts Tool from a document-based environment into a model-based asset with each portion of the model answering multiple attributes found in AC-17-01.

Using the Airworthiness Certification Profile has substantial potential in reducing workloads in the digital transfer of airworthiness certification reporting documentation between organizations. No longer will there be a need to have a system designer generate the data to the SPO, have the SPO interpret that data, and then have the SPO translate the data to a document-based format for airworthiness evaluation. With a digital model, the system design, with an applied Airworthiness Certification Profile, can directly pass between the system designer, SPO, and Airworthiness Home Office. Additionally, by using a Profile, any aircraft developer can incorporate it directly into their MBSE System Model. This allows the use of the Profile to be placed against any Aircraft Platform and used with any SPO.

Another aspect of the Airworthiness Certification Profile is its ability to be used with a new aircraft model or incorporated into an existing model. The Profile is not set up to change or replace an existing aircraft system model, but instead the relationship mapping shows the system modeler how to take the elements from the system model and

place them in separate diagrams used for the Airworthiness Certification process. The Airworthiness Certification Profile is only built to provide stereotypes and demonstrate relationship mapping of existing aircraft modeled functions that will then be used as part of the certification process.

Finally, workload reduction and System clarity occurs in the use of the verification of compliance to each of the Airworthiness Standards. Digital tables generated in the Profile are set to match the current airworthiness certification artifacts tool. This method of compliance requirement diagram is to be used to label each standard and provide the appropriate diagram and/or artifacts that satisfy the standard. This way, an Airworthiness Certification Official can not only verify the compliance, but also review the direct use of the analyzed element throughout the system.

Throughout this research, MBSE has really become a positive approach to airworthiness certification. With the Airworthiness Certification Profile, a System model can become undergo various aspects of the safety analysis using a coherent and consistent set of interlinked views that reflect multiple viewpoints of the system. The use of this Profile is a true beginning to accomplishing the Office of the Secretary of Defense (OSD) digital engineering strategy. Ultimately, using MBSE for SCF identification and thread analysis will not only improve airworthiness certification but support the digital transformation of the Defense acquisition system.

Bibliography

AFLCMC. (2018, November). *Air Force Life Cycle Management Center*. Retrieved from Welcome - About Us: https://www.aflcmc.af.mil/WELCOME/About-Us/

Airworthiness Office, U. (2020, August 10). USAF Airworthiness Policy and Implementation Course. Wright Patterson, OH, United States of America: USAF Airworthiness Office.

Airworthiness, U. C. (2017, March 23). AC-17-01. *AIRWORTHINESS CIRCULAR Verification Expectations for Select Section 15 Criteria*. Wright-Patterson AFB, Ohio, United States of America: Department of the Air Force.

Beaufait, J. (2018). *MBSE Methodology and Analysis Tool to Implement MBSE Post Milestone C.* Monterey: Naval Postgraduate School.

Blackburn, M., Cloutier, R., Witus, G., & Hole, E. (2014). Introducing Model Based Systems Engineering Transforming System Engineering through Model-Based Systems Engineering. *Systems Engineering Research Center*, 8.

Blessing, L. T., & Chakrabarti, A. (2009). *DRM, a Design Research Methodology*. London: Springer-Verlag.

Bleu-Laine, M.-H., Bendarkar, M. V., Xie, S. B., & Mavris, D. N. (2019). A Model-Based System Engineering Approach to Normal Category Airplane Airworthiness Certification. *AIAA Aviation Forum* (p. np). Dallas: American Institute of Aeronautics and Astronautics, Inc.

Carros, P. J. (2019, December 9). Implementing Model Based Systems Engineering into the T-7A SPO. Wright Patterson AFB, OH, United States of America: Self.

Colombi, J., Miller, M. E., Schneider, M., McGrogan, J., Long, D. S., & Plaga, J. (2012). Predictive mental workload modeling: implications for system design. *Journal of Systems Engineering, 15*(4), 448-460.

Department of Defense. (2014). *MIL-HDBK-516C, AIRWORTHINESS CERTIFICATION CRITERIA.* Washington DC: Department of Defense. Retrieved from http://everyspec.com/MIL-HDBK/MIL-HDBK-0500-0599/MIL-HDBK-516C_52120/

Holt, J., & Perry, S. (2018). *SysML for Systems Engineering, A Model-Based Approach, 3rd Edition.* London: The Institution of Engineering and Technology.

Mazeika, D., & Butleris, R. (2020, April). MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems. *Applied Sciences*, p. 10(7):2574.

Object Management Group. (2019, November). *OMG Systems Modeling Language Specification Version 1.6.* Retrieved from OMG.org: https://www.omg.org/spec/SysML/1.6/

Shouse, N. J. (2021, January 8). AFLCMC/EZSI System Engineering Integration Technical Advisor. (J. C. King, Interviewer)

Simi, S. M., Mulholland, S. P., & Merritt, L. B. (2016). Next-Generation Model-Based Systems Engineering Processes and Tools Supporting the Airworthiness efforts of Cyber Physical Systems (CPS). *Annual Forum Proceedings - AHS International*, 3068-3075.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	
08-03-2021	Master's Thesis	October 2019 – March 2021

TITLE AND SUBTITLE

Using Model Based System Engineering to Identify Safety Critical Functions in Airworthiness Certifications

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

King, Jeffery C, Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENV-MS-21-M-241

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Lifecycle Management Center Engineering and Technical Management Services Directorate
1970 Monohan Way
WPAFB OH, 45433
(937) 656-9603
nicholas.shouse@us.af.mil
ATTN: Mr. Nick Shouse, NH-04

10. SPONSOR/MONITOR'S ACRONYM(S)

AFLCMC/EZSI

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
Modern aircraft are complex systems with numerous interacting hardware and software components. To minimize any safety mishaps during operations, new aircraft designs and modifications must go through an airworthiness certification. The current United States Air Force (USAF) airworthiness certification process, captured in MIL-HDBK-516C, is time-consuming and manpower intensive due to extensive documentation. To minimize inefficiencies of this document-based approach, this thesis examined model-based systems engineering (MBSE) to support Safety Critical Function (SCF) thread analysis against criteria found in Section 15 of MIL-HDBK-516C. Within this scope, the research identified an SCF domain-specific profile and style guide using the Systems Modeling Language (SysML) and domain specific extensions. The SCF profile was applied to an Unmanned Airborne System (UAS) designed and flight tested as a course sequence in AFIT's Graduate school. This research identified: 1) how a system model can support the execution of the airworthiness process, 2) how modeling can be minimally stereotyped to support various airworthiness analyses, and where airworthiness analysis could be automated and leaned. Using MBSE for SCF identification and thread analysis will not only improve airworthiness certification but support the digital transformation of the Defense acquisition system.

15. SUBJECT TERMS
MBSE, SysML, Airworthiness, Safety Critical Function, Digital Engineering

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. John Colombi, AFIT/ENV
U	**U**	**U**	**UU**	95	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 3347 (john.colombi@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18