Using MBSE to Identify Safety Critical Functions in Airworthiness Certifications

Major Jeffery King
Instructor of Systems Engineering
AFIT, School of Systems and Logistics

Mr. Noah “Odie” Demerly
Process Automation Lead
DAF Digital Transformation Office

Controlled by: AFIT/LSS
CUI Category: Unclassified, No CUI
Distribution Statement A: Approved for public release, distribution unlimited
88th ABW PA Case Number 88ABW-2022-0809
POC: Jeffery King, 937-255-7777x3217

Objectives

- Discuss AFIT Research
- Highlight Results
- Review Lessons Learned
- Express Application of MBSE
- Taking a Step further
- Questions and Answers

Where it all Began

- AFIT Graduate Research
- Completed Feb 2021
- Sponsor: AFLCMC/EZI

Research Objective

- **Identify how a system model can aid and automate the execution of the airworthiness process**
  - What modeling aspects and/or program artifacts must be created to support the airworthiness certification process?
  - What airworthiness analyses can be done with a SysML domain-specific system model?
  - How could airworthiness analysis be automated or leaned to support parallel, continuous development operations?

Scope: Safety Critical Function analysis criteria found in MIL-HDBK-516C Section 15, *Computer Systems and Software* and Air Circular 17-01

Document Review

- **Sample of to-be modeled AC-17-01 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

1.3 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

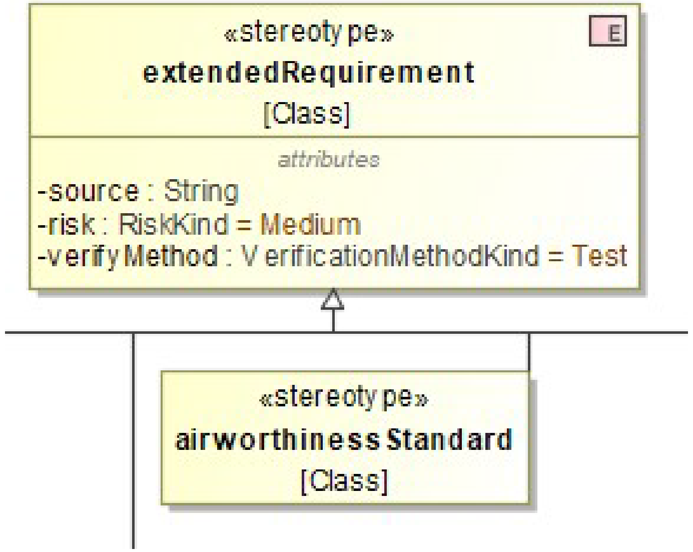
Document Translation

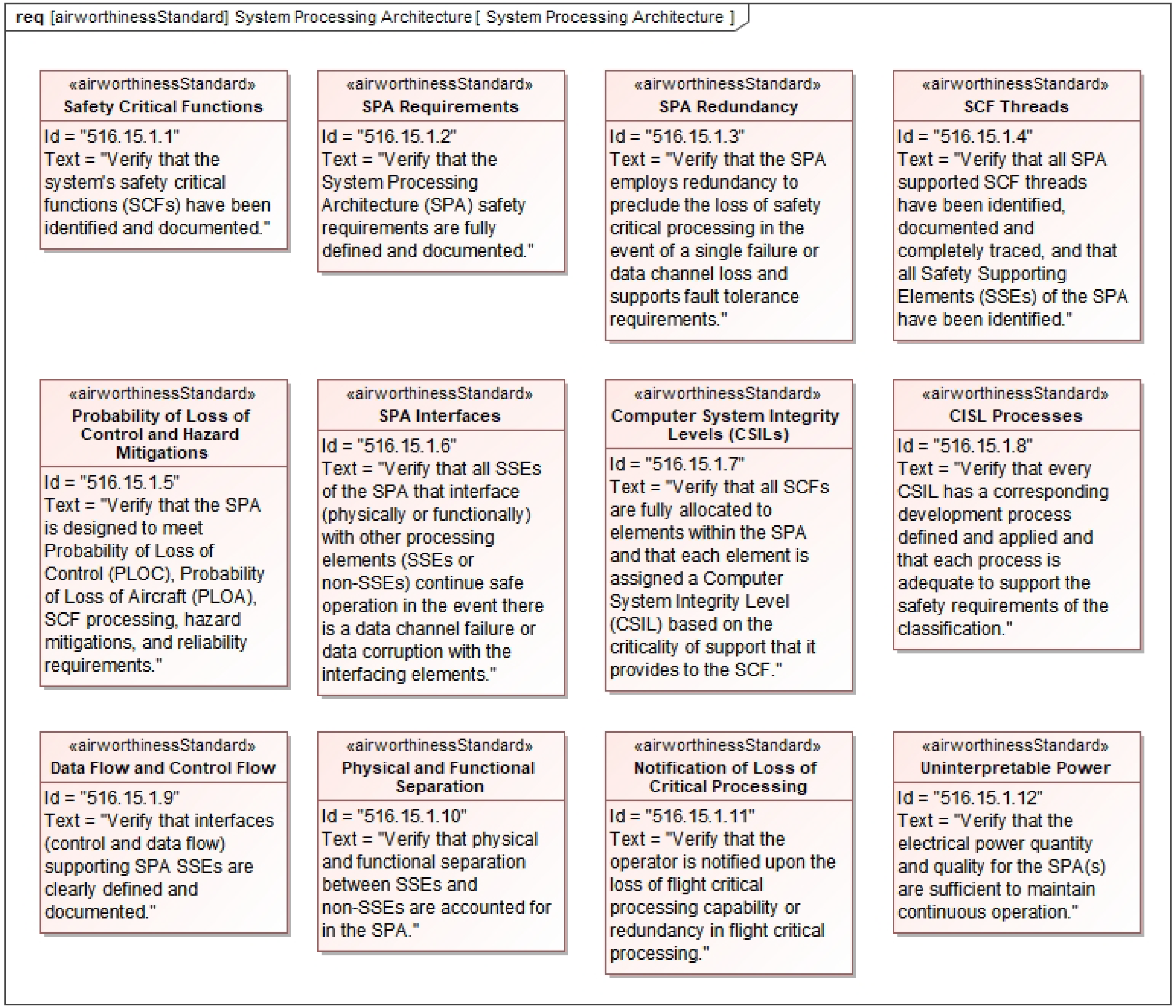
- **AC-17-01 Focus Areas**
  - SCF Identification
  - SCF Thread Analysis
  - Integration Methodology
  - Failure Mode and Effects Testing
  - Safety Interlock Design
  - SPA and Software Development
  - Full Qualification of Software

- **Model Focus Areas**
  - Certification Standards
  - SCF Identification
  - SCF Thread Analysis
    - Physical System
    - Computer System Integration Level (CSIL)
    - Validation and Verification
    - Failure Mode and Effects Testing (FMET)
    - Safety Interlock Design
    - Requirement Mapping

Document Modeling

- Certification Standards




req [airworthinessStandard] System Processing Architecture [System Processing Architecture]

«airworthinessStandard»
Safety Critical Functions
Id = "516.15.1.1"
Text = "Verify that the system's safety critical functions (SCFs) have been identified and documented."

«airworthinessStandard»
SPA Requirements
Id = "516.15.1.2"
Text = "Verify that the System Processing Architecture (SPA) safety requirements are fully defined and documented."

«airworthinessStandard»
SPA Redundancy
Id = "516.15.1.3"
Text = "Verify that the SPA employs redundancy to preclude the loss of safety critical processing in the event of a single failure or data channel loss and supports fault tolerance requirements."

«airworthinessStandard»
SCF Threads
Id = "516.15.1.4"
Text = "Verify that all SPA supported SCF threads have been identified, documented and completely traced, and that all Safety Supporting Elements (SSEs) of the SPA have been identified."

«airworthinessStandard»
Probability of Loss of Control and Hazard Mitigations
Id = "516.15.1.5"
Text = "Verify that the SPA is designed to meet Probability of Loss of Control (PLOC), Probability of Loss of Aircraft (PLOA), SCF processing, hazard mitigations, and reliability requirements."

«airworthinessStandard»
SPA Interfaces
Id = "516.15.1.6"
Text = "Verify that all SSEs of the SPA that interface (physically or functionally) with other processing elements (SSEs or non-SSEs) continue safe operation in the event there is a data channel failure or data corruption with the interfacing elements."

«airworthinessStandard»
Computer System Integrity Levels (CSILs)
Id = "516.15.1.7"
Text = "Verify that all SCFs are fully allocated to elements within the SPA and that each element is assigned a Computer System Integrity Level (CSIL) based on the criticality of support that it provides to the SCF."

«airworthinessStandard»
CISL Processes
Id = "516.15.1.8"
Text = "Verify that every CSIL has a corresponding development process defined and applied and that each process is adequate to support the safety requirements of the classification."

«airworthinessStandard»
Data Flow and Control Flow
Id = "516.15.1.9"
Text = "Verify that interfaces (control and data flow) supporting SPA SSEs are clearly defined and documented."

«airworthinessStandard»
Physical and Functional Separation
Id = "516.15.1.10"
Text = "Verify that physical and functional separation between SSEs and non-SSEs are accounted for in the SPA."

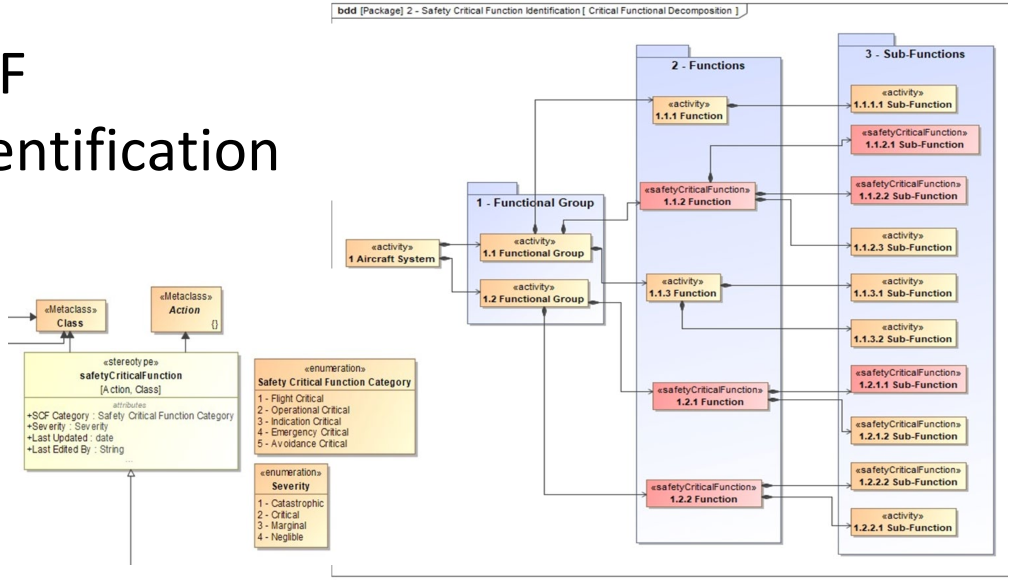
«airworthinessStandard»
Notification of Loss of Critical Processing
Id = "516.15.1.11"
Text = "Verify that the operator is notified upon the loss of flight critical processing capability or redundancy in flight critical processing."

«airworthinessStandard»
Uninterpretable Power
Id = "516.15.1.12"
Text = "Verify that the electrical power quantity and quality for the SPA(s) are sufficient to maintain continuous operation."

Document Modeling

AIR FORCE INSTITUTE OF TECHNOLOGY

SCF Identification



bdd [Package] 2 - Safety Critical Function Identification [Critical Functional Decomposition]

«Metaclass»
Class

«Metaclass»
Action
{}

«stereotype»
safetyCriticalFunction
[Action, Class]
attributes
+SCF Category : Safety Critical Function Category
+Severity : Severity
+Last Updated : date
+Last Edited By : String
...

«enumeration»
Safety Critical Function Category
1 - Flight Critical
2 - Operational Critical
3 - Indication Critical
4 - Emergency Critical
5 - Avoidance Critical

«enumeration»
Severity
1 - Catastrophic
2 - Critical
3 - Marginal
4 - Neglible

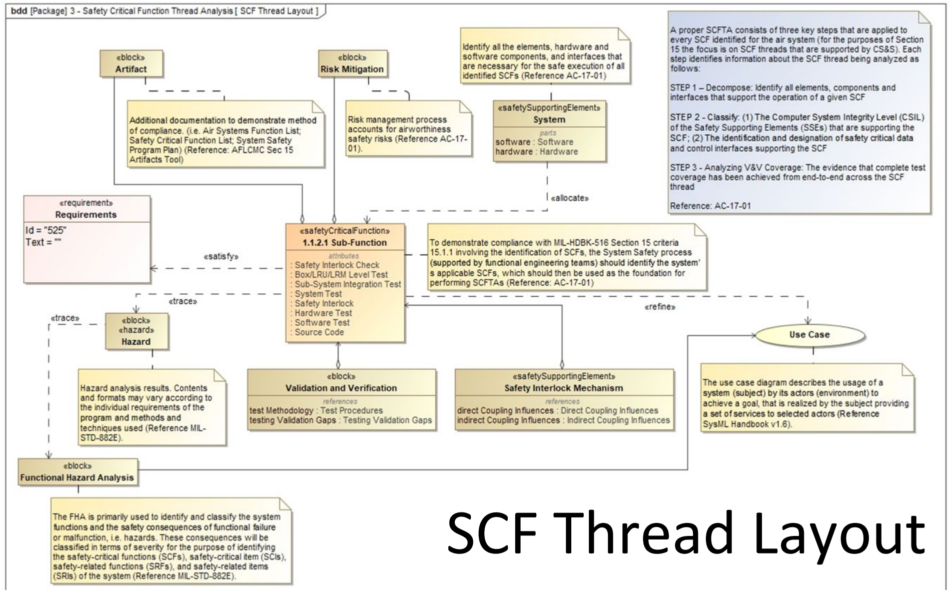
«activity»
1 Aircraft System

1 - Functional Group
«activity» **1.1 Functional Group**
«activity» **1.2 Functional Group**

2 - Functions
«activity» **1.1.1 Function**
«safetyCriticalFunction» **1.1.2 Function**
«activity» **1.1.3 Function**
«safetyCriticalFunction» **1.2.1 Function**
«safetyCriticalFunction» **1.2.2 Function**

3 - Sub-Functions
«activity» **1.1.1.1 Sub-Function**
«safetyCriticalFunction» **1.1.2.1 Sub-Function**
«safetyCriticalFunction» **1.1.2.2 Sub-Function**
«activity» **1.1.2.3 Sub-Function**
«activity» **1.1.3.1 Sub-Function**
«activity» **1.1.3.2 Sub-Function**
«safetyCriticalFunction» **1.2.1.1 Sub-Function**
«safetyCriticalFunction» **1.2.1.2 Sub-Function**
«safetyCriticalFunction» **1.2.2.2 Sub-Function**
«activity» **1.2.2.1 Sub-Function**

SCF Thread Layout



bdd [Package] 3 - Safety Critical Function Thread Analysis [SCF Thread Layout]

«block»
Artifact

Additional documentation to demonstrate method of compliance. (i.e. Air Systems Function List; Safety Critical Function List; System Safety Program Plan) (Reference: AFLCMC Sec 15 Artifacts Tool)

«block»
Risk Mitigation

Risk management process accounts for airworthiness safety risks (Reference AC-17-01).

Identify all the elements, hardware and software components, and interfaces that are necessary for the safe execution of all identified SCFs (Reference AC-17-01)

«safetySupportingElement»
System
parts
software : Software
hardware : Hardware

A proper SCFTA consists of three key steps that are applied to every SCF identified for the air system (for the purposes of Section 15 the focus is on SCF threads that are supported by CS&S). Each step identifies information about the SCF thread being analyzed as follows:

STEP 1 – Decompose: Identify all elements, components and interfaces that support the operation of a given SCF

STEP 2 - Classify: (1) The Computer System Integrity Level (CSIL) of the Safety Supporting Elements (SSEs) that are supporting the SCF; (2) The identification and designation of safety critical data and control interfaces supporting the SCF

STEP 3 - Analyzing V&V Coverage: The evidence that complete test coverage has been achieved from end-to-end across the SCF thread

Reference: AC-17-01

«requirement»
Requirements
Id = "525"
Text = ""

«safetyCriticalFunction»
1.1.2.1 Sub-Function
attributes
: Safety Interlock Check
: Box/LRU/LRM Level Test
: Sub-System Integration Test
: System Test
: Safety Interlock
: Hardware Test
: Software Test
: Source Code

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 (Reference: AC-17-01)

«block»
«hazard»
Hazard

Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used (Reference MIL-STD-882E).

«block»
Validation and Verification
references
test Methodology : Test Procedures
testing Validation Gaps : Testing Validation Gaps

«safetySupportingElement»
Safety Interlock Mechanism
references
direct Coupling Influences : Direct Coupling Influences
indirect Coupling Influences : Indirect Coupling Influences

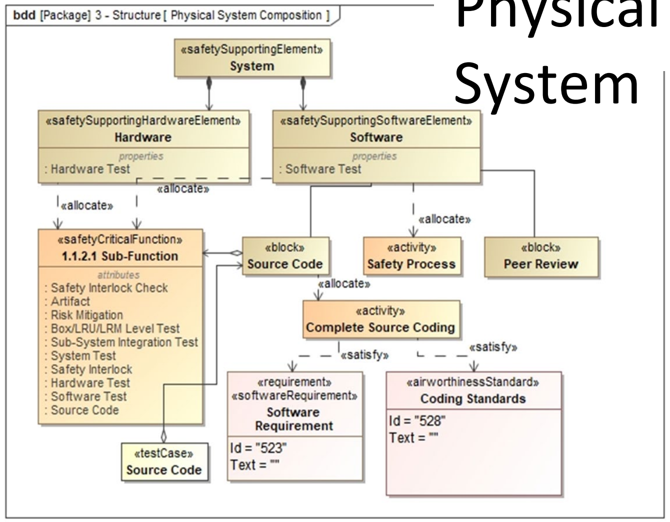
Use Case

The use case diagram 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 (Reference SysML Handbook v1.6).

«block»
Functional Hazard Analysis

The FHA is primarily used to identify and classify the system functions and the safety consequences of functional failure or malfunction, i.e. hazards. These consequences will be classified in terms of severity for the purpose of identifying the safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs) of the system (Reference MIL-STD-882E).

Physical System



bdd [Package] 3 - Structure [Physical System Composition]

«safetySupportingElement»
System

«safetySupportingHardwareElement»
Hardware
properties
: Hardware Test

«safetySupportingSoftwareElement»
Software
properties
: Software Test

«safetyCriticalFunction»
1.1.2.1 Sub-Function
attributes
: Safety Interlock Check
: Artifact
: Risk Mitigation
: Box/LRU/LRM Level Test
: Sub-System Integration Test
: System Test
: Safety Interlock
: Hardware Test
: Software Test
: Source Code

«block» **Source Code**

«activity» **Safety Process**

«block» **Peer Review**

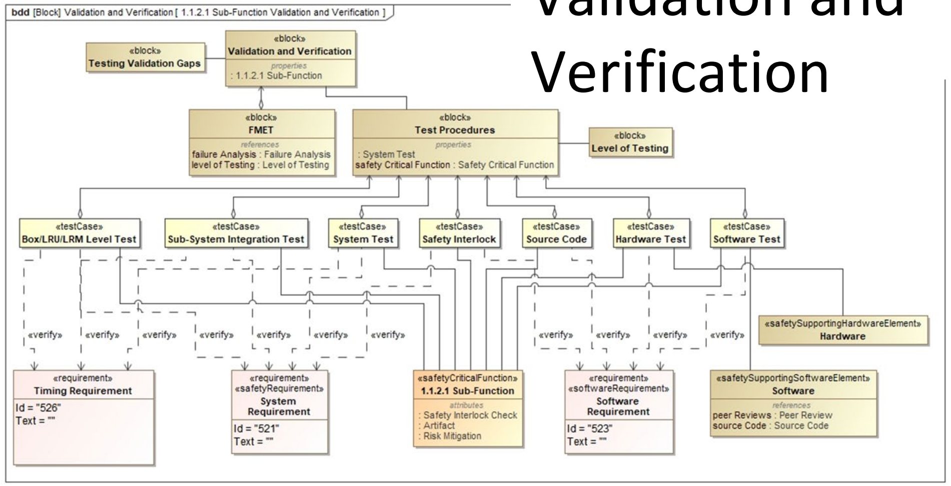
«activity» **Complete Source Coding**

«testCase» **Source Code**

«requirement»
«softwareRequirement»
Software Requirement
Id = "523"
Text = ""

«airworthinessStandard»
Coding Standards
Id = "528"
Text = ""

Validation and Verification



bdd [Block] Validation and Verification [1.1.2.1 Sub-Function Validation and Verification]

«block» **Testing Validation Gaps**

«block»
Validation and Verification
properties
: 1.1.2.1 Sub-Function

«block»
FMET
references
failure Analysis : Failure Analysis
level of Testing : Level of Testing

«block»
Test Procedures
properties
: System Test
safety Critical Function : Safety Critical Function

«block» **Level of Testing**

«testCase» **Box/LRU/LRM Level Test**
«testCase» **Sub-System Integration Test**
«testCase» **System Test**
«testCase» **Safety Interlock**
«testCase» **Source Code**
«testCase» **Hardware Test**
«testCase» **Software Test**

«safetySupportingHardwareElement»
Hardware

«requirement»
Timing Requirement
Id = "526"
Text = ""

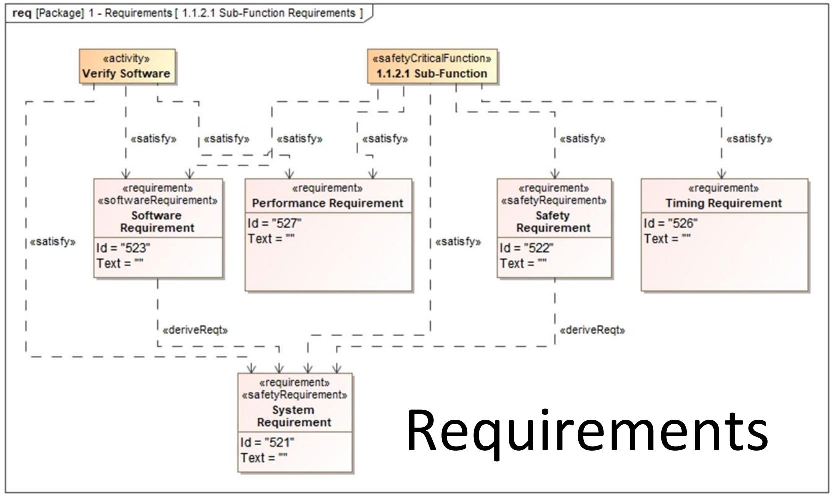
«requirement»
«safetyRequirement»
System Requirement
Id = "521"
Text = ""

«safetyCriticalFunction»
1.1.2.1 Sub-Function
attributes
: Safety Interlock Check
: Artifact
: Risk Mitigation

«requirement»
«softwareRequirement»
Software Requirement
Id = "523"
Text = ""

«safetySupportingSoftwareElement»
Software
references
peer Reviews : Peer Review
source Code : Source Code

Requirements



req [Package] 1 - Requirements [1.1.2.1 Sub-Function Requirements]

«activity»
Verify Software

«safetyCriticalFunction»
1.1.2.1 Sub-Function

«requirement»
«softwareRequirement»
Software Requirement
Id = "523"
Text = ""

«requirement»
Performance Requirement
Id = "527"
Text = ""

«requirement»
«safetyRequirement»
Safety Requirement
Id = "522"
Text = ""

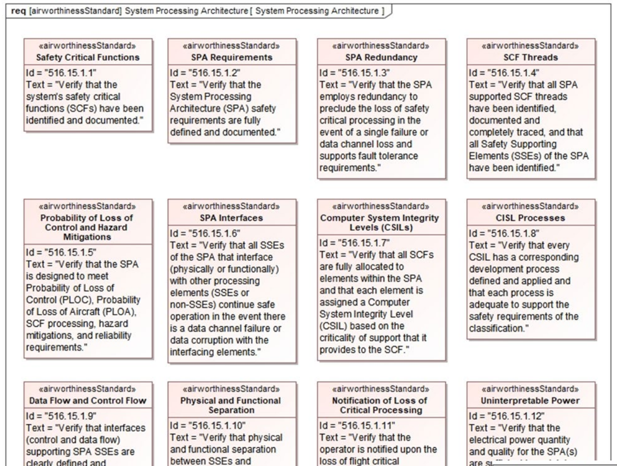
«requirement»
Timing Requirement
Id = "526"
Text = ""

«requirement»
«safetyRequirement»
System Requirement
Id = "521"
Text = ""

Review

- Translate -> Define -> Build

1	SCF Identification	2.1.4	Identify Safety Supporting Software Elements (SSSE)
1.1	SCFs in a system need to be identified and set apart from other functions	2.2	Classify SSE
1.2	SCFs are identified by the program's System Safety process	2.2.1	Mark CSIL Classification for SSE, SSHE, SSSE
1.3	SCFs need to trace back to their origin in the System Safety process	2.2.2	Identify interfaces supporting an SCF
1.4	SCF analysis is to be supported by engineers from various technical disciplines	2.3	Analyzing V&V Coverage: The evidence that complete test coverage has been achieved from end-to-end across the SCF thread
1.5	SCFs for a given system will be unique to each platform	2.3.1	Trace testing to supporting sub-function
1.6	SCFs are often put in a list format	2.3.2	Trace testing of SSE, SSHE, SSSE
1.7	SCFs can be categorized: Flight Critical, Operation Critical, Emergency Critical, Indication Critical, and Avoidance Critical.	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	SCFTA	2.3.5	Requirements implemented through components that support and SCF are traced to the SCF
2.1	Decompose: Identify all elements, components and interfaces that support the operation of a given SCF	2.3.6	Traceability of SCF to supporting components
2.1.1	Break down into sub-functions	2.3.7	Traceability exists from Software to testing performed
2.1.2	Identify Safety Supporting Elements (SSEs)	2.3.8	Safety interlocks are identified, analyzed, and tested
2.1.3	Identify Safety Supporting Hardware Elements (SSHE)	2.3.9	Identified testing gaps noted


req [airworthinessStandard] System Processing Architecture [System Processing Architecture]

«airworthinessStandard» Safety Critical Functions
Id = "516.15.1.1"
Text = "Verify that the system's safety critical functions (SCFs) have been identified and documented."

«airworthinessStandard» SPA Requirements
Id = "516.15.1.2"
Text = "Verify that the System Processing Architecture (SPA) safety requirements are fully defined and documented."

«airworthinessStandard» SPA Redundancy
Id = "516.15.1.3"
Text = "Verify that the SPA employs redundancy to preclude the loss of safety critical processing in the event of a single failure or data channel loss and supports fault tolerance requirements."

«airworthinessStandard» SCF Threads
Id = "516.15.1.4"
Text = "Verify that all SPA supported SCF threads have been identified, documented and completely traced, and that all Safety Supporting Elements (SSEs) of the SPA have been identified."

«airworthinessStandard» Probability of Loss of Control and Hazard Mitigations
Id = "516.15.1.5"
Text = "Verify that the SPA is designed to meet Probability of Loss of Control (PLOC), Probability of Loss of Aircraft (PLOA), SCF processing, hazard mitigations, and reliability requirements."

«airworthinessStandard» SPA Interfaces
Id = "516.15.1.6"
Text = "Verify that all SSEs of the SPA that interface (physically or functionally) with other processing elements (SSEs or non-SSEs) continue safe operation in the event there is a data channel failure or data corruption with the interfacing elements."

«airworthinessStandard» Computer System Integrity Levels (CSILs)
Id = "516.15.1.7"
Text = "Verify that all SCFs are fully allocated to elements within the SPA and that each element is assigned a Computer System Integrity Level (CSIL) based on the criticality of support that it provides to the SCF."

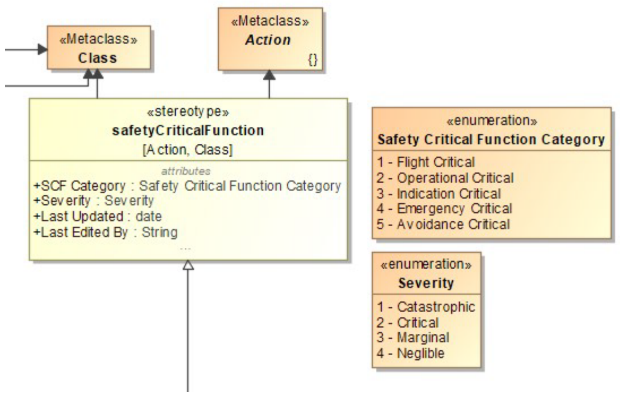
«airworthinessStandard» CISL Processes
Id = "516.15.1.8"
Text = "Verify that every CSIL has a corresponding development process defined and applied and that each process is adequate to support the safety requirements of the classification."

«airworthinessStandard» Data Flow and Control Flow
Id = "516.15.1.9"
Text = "Verify that interfaces (control and data flow) supporting SPA SSEs are clearly defined and documented."

«airworthinessStandard» Physical and Functional Separation
Id = "516.15.1.10"
Text = "Verify that physical and functional separation between SSEs and non-SSEs are accounted for in the SPA."

«airworthinessStandard» Notification of Loss of Critical Processing
Id = "516.15.1.11"
Text = "Verify that the operator is notified upon the loss of flight critical processing capability or redundancy in flight critical processing."

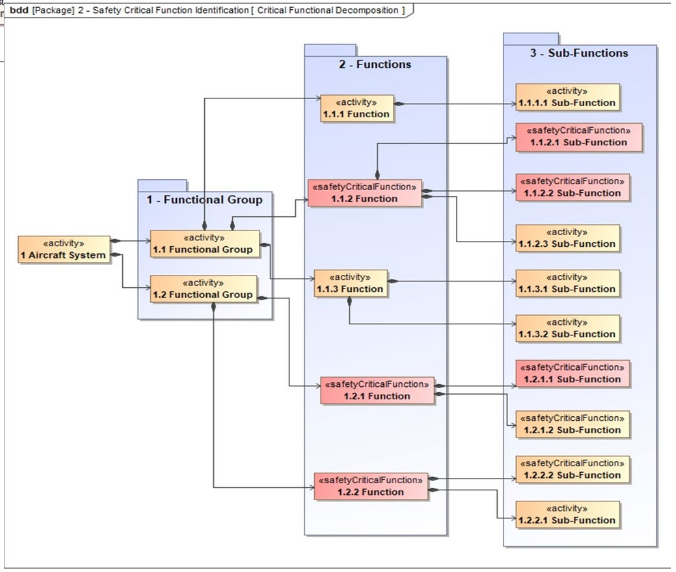
«airworthinessStandard» Uninterpretable Power
Id = "516.15.1.12"
Text = "Verify that the electrical power quantity and quality for the SPA(s) are su
contin

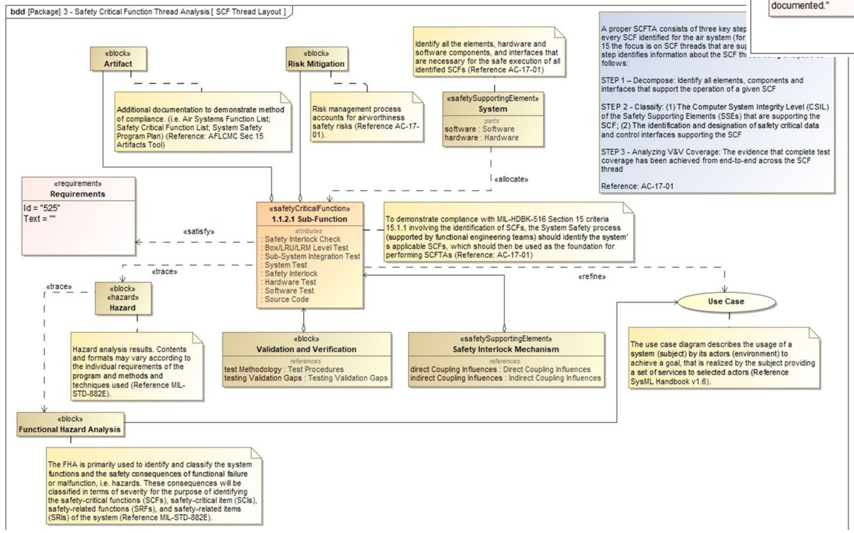


+SCF Category : Safety Critical Function Category
+Severity : Severity
+Last Updated : date
+Last Edited By : String

«enumeration» Safety Critical Function Category
1 - Flight Critical
2 - Operational Critical
3 - Indication Critical
4 - Emergency Critical
5 - Avoidance Critical

«enumeration» Severity
1 - Catastrophic
2 - Critical
3 - Marginal
4 - Neglible




bdd [Package] 3 - Safety Critical Function Thread Analysis [SCF Thread Layout]
«block»
Artifact
«block»
Risk Mitigation
«safetySupportingElement»
System
parts
software : Software
hardware : Hardware
«allocate»
«requirement»
Requirements
Id = "525"
Text = ""
«satisfy»
«safetyCriticalFunction»
1.1.2.1 Sub-Function
attributes
: Safety Interlock Check
: Box/LRU/LRM Level Test
: Sub-System Integration Test
: System Test
: Safety Interlock
: Hardware Test
: Software Test
: Source Code
«trace»
«trace»
«block»
«hazard»
Hazard
«refine»
Use Case
«block»
Validation and Verification
references
test Methodology : Test Procedures
testing Validation Gaps : Testing Validation Gaps
«safetySupportingElement»
Safety Interlock Mechanism
references
direct Coupling Influences : Direct Coupling Influences
indirect Coupling Influences : Indirect Coupling Influences
«block»
Functional Hazard Analysis

Identify all the elements, hardware and software components, and interfaces that are necessary for the safe execution of all identified SCFs (Reference AC-17-01)

Additional documentation to demonstrate method of compliance. (i.e. Air Systems Function List; Safety Critical Function List; System Safety Program Plan) (Reference: AFLCMC Sec 15 Artifacts Tool)

Risk management process accounts for airworthiness safety risks (Reference AC-17-01).

A proper SCFTA consists of three key step every SCF identified for the air system (for 15 the focus is on SCF threads that are su step identifies information about the SCF th follows:

STEP 1 – Decompose: Identify all elements, components and interfaces that support the operation of a given SCF

STEP 2 - Classify: (1) The Computer System Integrity Level (CSIL) of the Safety Supporting Elements (SSEs) that are supporting the SCF; (2) The identification and designation of safety critical data and control interfaces supporting the SCF

STEP 3 - Analyzing V&V Coverage: The evidence that complete test coverage has been achieved from end-to-end across the SCF thread

Reference: AC-17-01

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 (Reference: AC-17-01)

Hazard analysis results. Contents and formats may vary according to the individual requirements of the program and methods and techniques used (Reference MIL-STD-882E).

The use case diagram 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 (Reference SysML Handbook v1.6).

The FHA is primarily used to identify and classify the system functions and the safety consequences of functional failure or malfunction, i.e. hazards. These consequences will be classified in terms of severity for the purpose of identifying the safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs) of the system (Reference MIL-STD-882E).

Lessons Learned

- **Apply technique to other (document) processes**
  - Unified Test Profile for DoD (UTP-D)
  - Test cards, test points, test Reqt, test config,…
- **Test/Apply the profile on data iteratively**
  - Socialize results. Codify in CDRL/DID/ contract language
- **Keep it simple**
  - Balance new <<stereotypes>> , extensions of existing stereotypes
  - new tags (attributes), appropriate relationships

Jeffery King
Major, USAF
AFIT/LSS
jeffery.king.1@us.af.mil

WKSP0696 – Applied MBSE using SysML

Visit the Air University Portal
(CAC-Access Required)
https://aueems.cce.af.mil/

AVOLVE

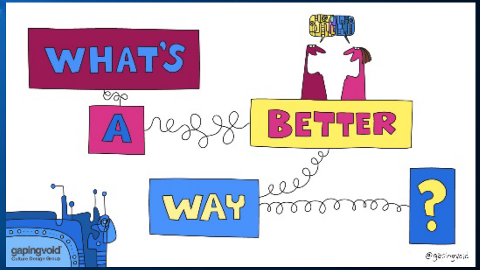
For those with CAC-access:
https://avolve.apps.dso.mil
(Note: 1st-time login requires setting up a Platform One account)

Air Force Institute of Technology
School of Systems & Logistics
https://www.afit.edu/LS/

the future of humanity is digital
are you sure you want to wait this one out?

DTO

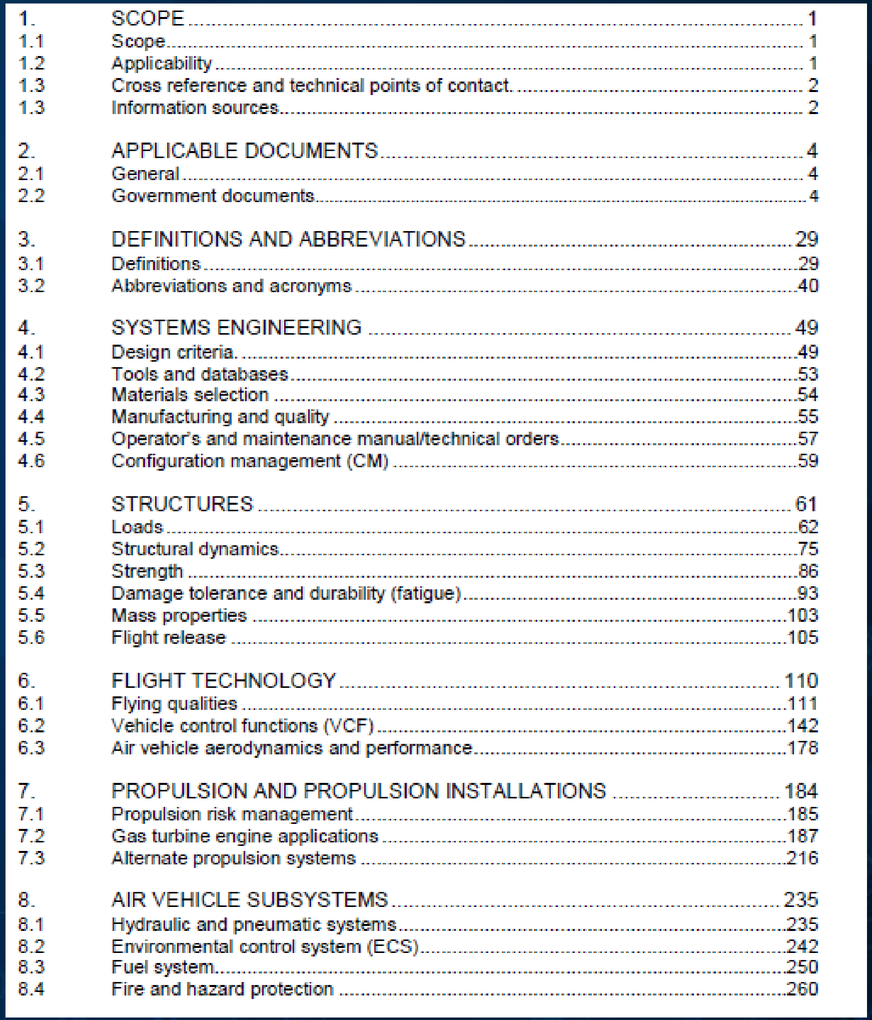
DIGITAL TRANSFORMATION OFFICE



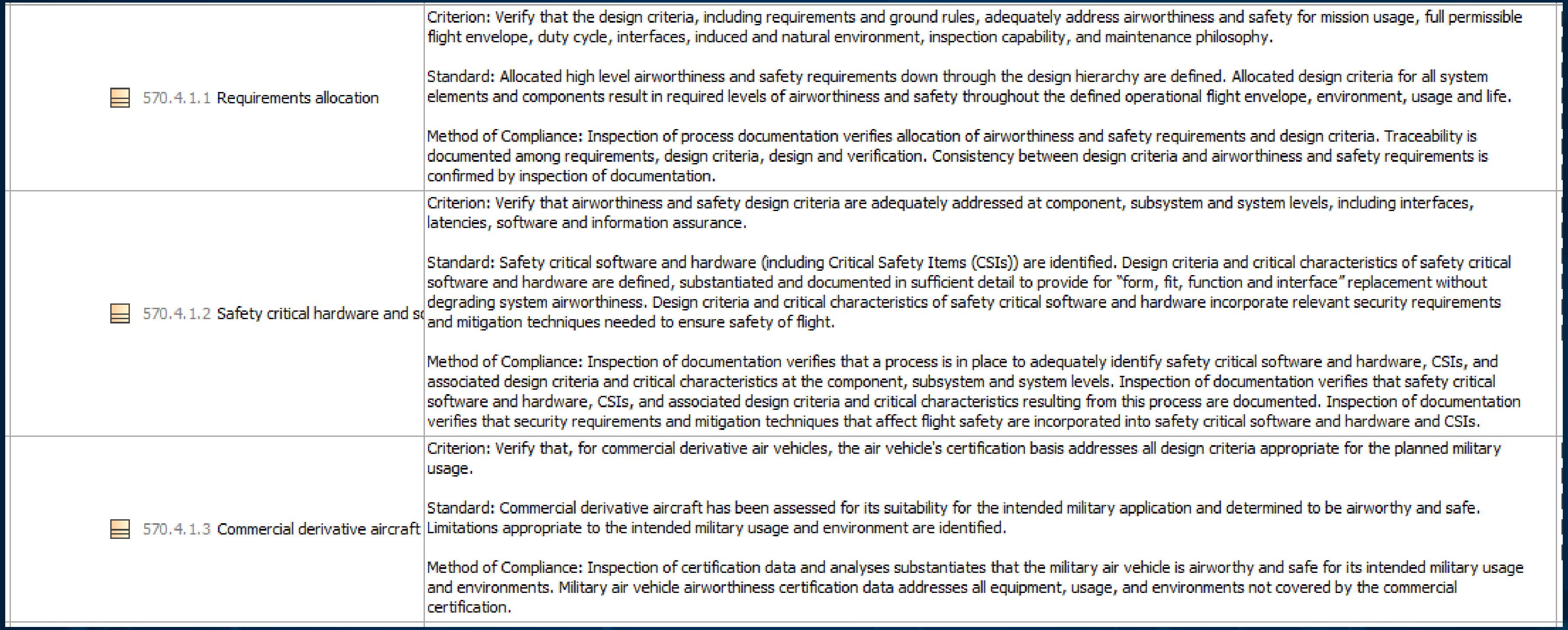
Taking a Step Further – Noah "Odie" Demerly

MIL-HDBK-516

- Airworthiness handbook produced by the DoD for Military Airworthiness Certification Criteria
  - Used widely in USAF/USA/USN as the document to follow for guidance during certification of military aircraft
  - NOT a requirements document; this is a handbook
  - Each sub section has a Criteria, Standard, Method of Compliance, and References (JSSG's, MIL-STD, etc.)
  - Currently on Revision C, move to revision D in process
- Certification Basis (CB) / Compliance Report (CR)
  - CB is "baseline", CR assesses compliance / risk



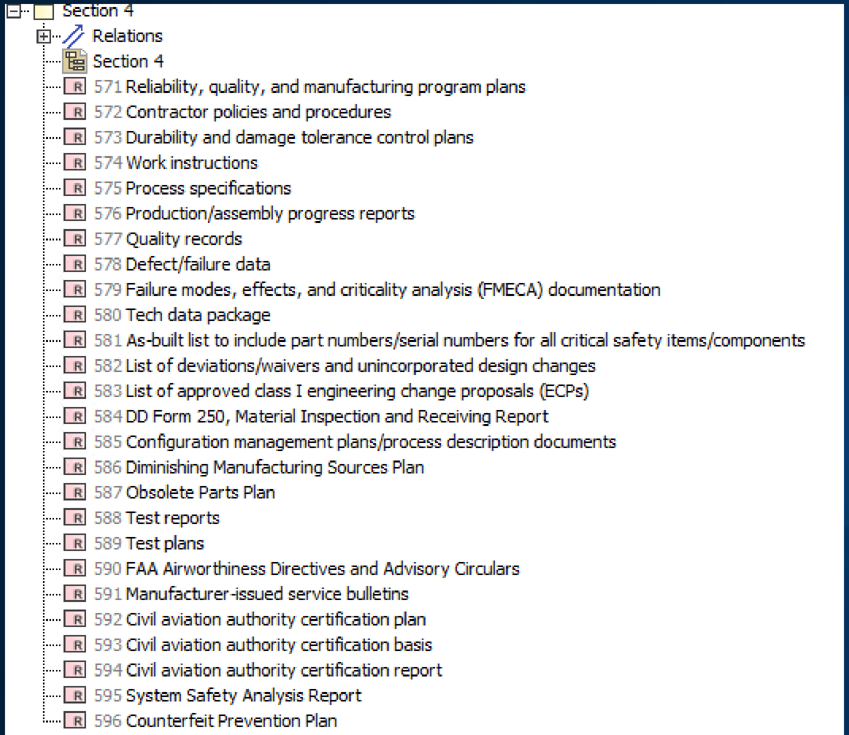
MIL-HDBK-516C – Creating a Digital "Copy"



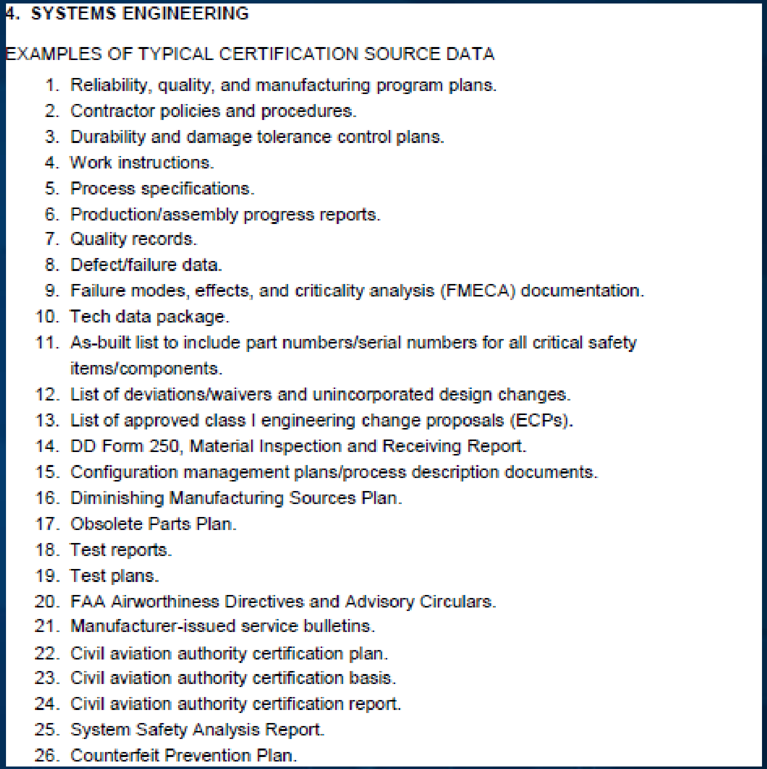
570.4.1.1 Requirements allocation	Criterion: Verify that the design criteria, including requirements and ground rules, adequately address airworthiness and safety for mission usage, full permissible flight envelope, duty cycle, interfaces, induced and natural environment, inspection capability, and maintenance philosophy. Standard: Allocated high level airworthiness and safety requirements down through the design hierarchy are defined. Allocated design criteria for all system elements and components result in required levels of airworthiness and safety throughout the defined operational flight envelope, environment, usage and life. Method of Compliance: Inspection of process documentation verifies allocation of airworthiness and safety requirements and design criteria. Traceability is documented among requirements, design criteria, design and verification. Consistency between design criteria and airworthiness and safety requirements is confirmed by inspection of documentation.
570.4.1.2 Safety critical hardware and s	Criterion: Verify that airworthiness and safety design criteria are adequately addressed at component, subsystem and system levels, including interfaces, latencies, software and information assurance. Standard: Safety critical software and hardware (including Critical Safety Items (CSIs)) are identified. Design criteria and critical characteristics of safety critical software and hardware are defined, substantiated and documented in sufficient detail to provide for "form, fit, function and interface" replacement without degrading system airworthiness. Design criteria and critical characteristics of safety critical software and hardware incorporate relevant security requirements and mitigation techniques needed to ensure safety of flight. Method of Compliance: Inspection of documentation verifies that a process is in place to adequately identify safety critical software and hardware, CSIs, and associated design criteria and critical characteristics at the component, subsystem and system levels. Inspection of documentation verifies that safety critical software and hardware, CSIs, and associated design criteria and critical characteristics resulting from this process are documented. Inspection of documentation verifies that security requirements and mitigation techniques that affect flight safety are incorporated into safety critical software and hardware and CSIs.
570.4.1.3 Commercial derivative aircraft	Criterion: Verify that, for commercial derivative air vehicles, the air vehicle's certification basis addresses all design criteria appropriate for the planned military usage. Standard: Commercial derivative aircraft has been assessed for its suitability for the intended military application and determined to be airworthy and safe. Limitations appropriate to the intended military usage and environment are identified. Method of Compliance: Inspection of certification data and analyses substantiates that the military air vehicle is airworthy and safe for its intended military usage and environments. Military air vehicle airworthiness certification data addresses all equipment, usage, and environments not covered by the commercial certification.

Directly copied Criteria/Standard/MOC into <<airworthinessStandard>> Stereotype so that relevant information is displayed in each view of the model for Section 4, Systems Engineering

Tracing source Data to “requirements”



- Section 4
  - Relations
  - Section 4
  - 571 Reliability, quality, and manufacturing program plans
  - 572 Contractor policies and procedures
  - 573 Durability and damage tolerance control plans
  - 574 Work instructions
  - 575 Process specifications
  - 576 Production/assembly progress reports
  - 577 Quality records
  - 578 Defect/failure data
  - 579 Failure modes, effects, and criticality analysis (FMECA) documentation
  - 580 Tech data package
  - 581 As-built list to include part numbers/serial numbers for all critical safety items/components
  - 582 List of deviations/waivers and unincorporated design changes
  - 583 List of approved class I engineering change proposals (ECPs)
  - 584 DD Form 250, Material Inspection and Receiving Report
  - 585 Configuration management plans/process description documents
  - 586 Diminishing Manufacturing Sources Plan
  - 587 Obsolete Parts Plan
  - 588 Test reports
  - 589 Test plans
  - 590 FAA Airworthiness Directives and Advisory Circulars
  - 591 Manufacturer-issued service bulletins
  - 592 Civil aviation authority certification plan
  - 593 Civil aviation authority certification basis
  - 594 Civil aviation authority certification report
  - 595 System Safety Analysis Report
  - 596 Counterfeit Prevention Plan



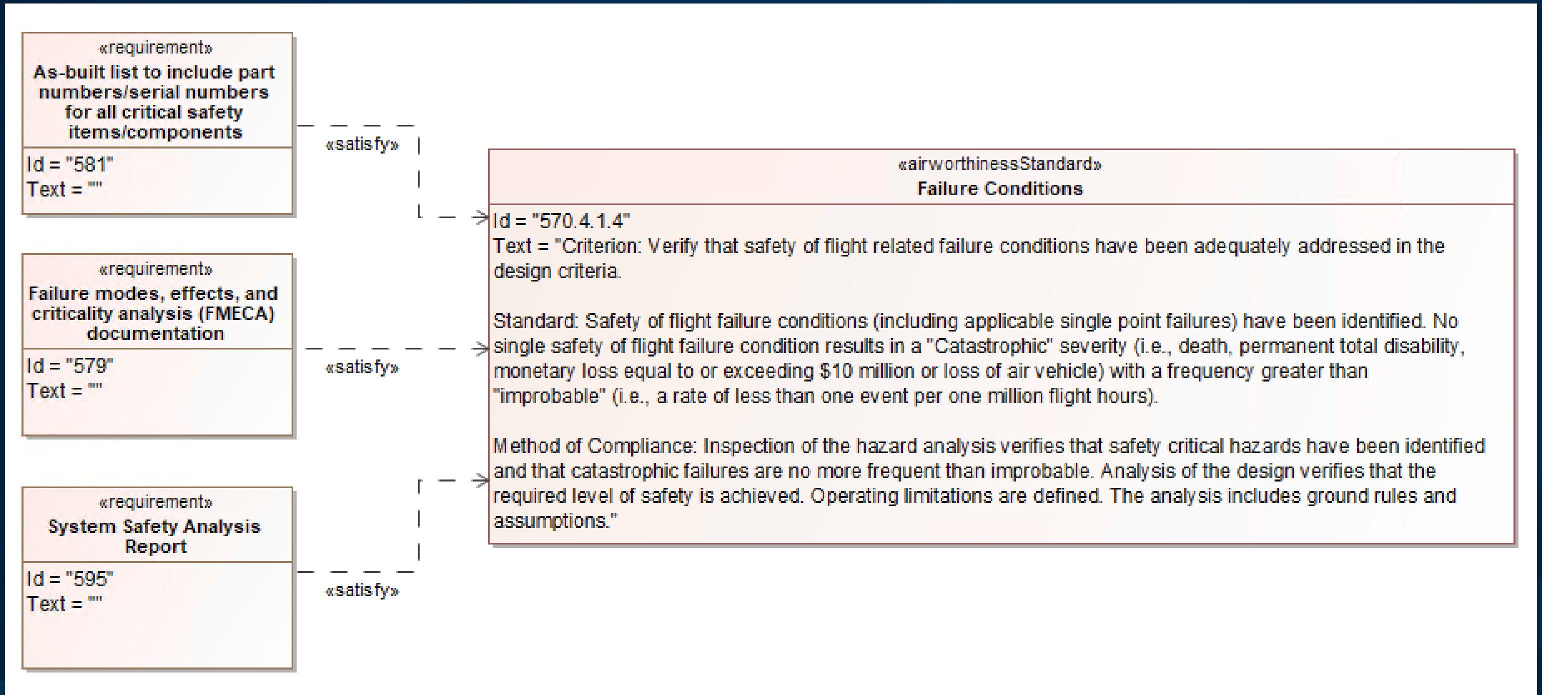
4. SYSTEMS ENGINEERING

EXAMPLES OF TYPICAL CERTIFICATION SOURCE DATA

1. Reliability, quality, and manufacturing program plans.
2. Contractor policies and procedures.
3. Durability and damage tolerance control plans.
4. Work instructions.
5. Process specifications.
6. Production/assembly progress reports.
7. Quality records.
8. Defect/failure data.
9. Failure modes, effects, and criticality analysis (FMECA) documentation.
10. Tech data package.
11. As-built list to include part numbers/serial numbers for all critical safety items/components.
12. List of deviations/waivers and unincorporated design changes.
13. List of approved class I engineering change proposals (ECPs).
14. DD Form 250, Material Inspection and Receiving Report.
15. Configuration management plans/process description documents.
16. Diminishing Manufacturing Sources Plan.
17. Obsolete Parts Plan.
18. Test reports.
19. Test plans.
20. FAA Airworthiness Directives and Advisory Circulars.
21. Manufacturer-issued service bulletins.
22. Civil aviation authority certification plan.
23. Civil aviation authority certification basis.
24. Civil aviation authority certification report.
25. System Safety Analysis Report.
26. Counterfeit Prevention Plan.

Used Section 4 front matter to trace a “requirement” to each expected artifact / data to meet the criteria in Section 4 – Systems Engineering

Tracing Artifact “requirements” to Criteria



«requirement»
As-built list to include part numbers/serial numbers for all critical safety items/components
Id = "581"
Text = ""

«requirement»
Failure modes, effects, and criticality analysis (FMECA) documentation
Id = "579"
Text = ""

«requirement»
System Safety Analysis Report
Id = "595"
Text = ""

«airworthinessStandard»
Failure Conditions
Id = "570.4.1.4"
Text = "Criterion: Verify that safety of flight related failure conditions have been adequately addressed in the design criteria.

Standard: Safety of flight failure conditions (including applicable single point failures) have been identified. No single safety of flight failure condition results in a "Catastrophic" severity (i.e., death, permanent total disability, monetary loss equal to or exceeding $10 million or loss of air vehicle) with a frequency greater than "improbable" (i.e., a rate of less than one event per one million flight hours).

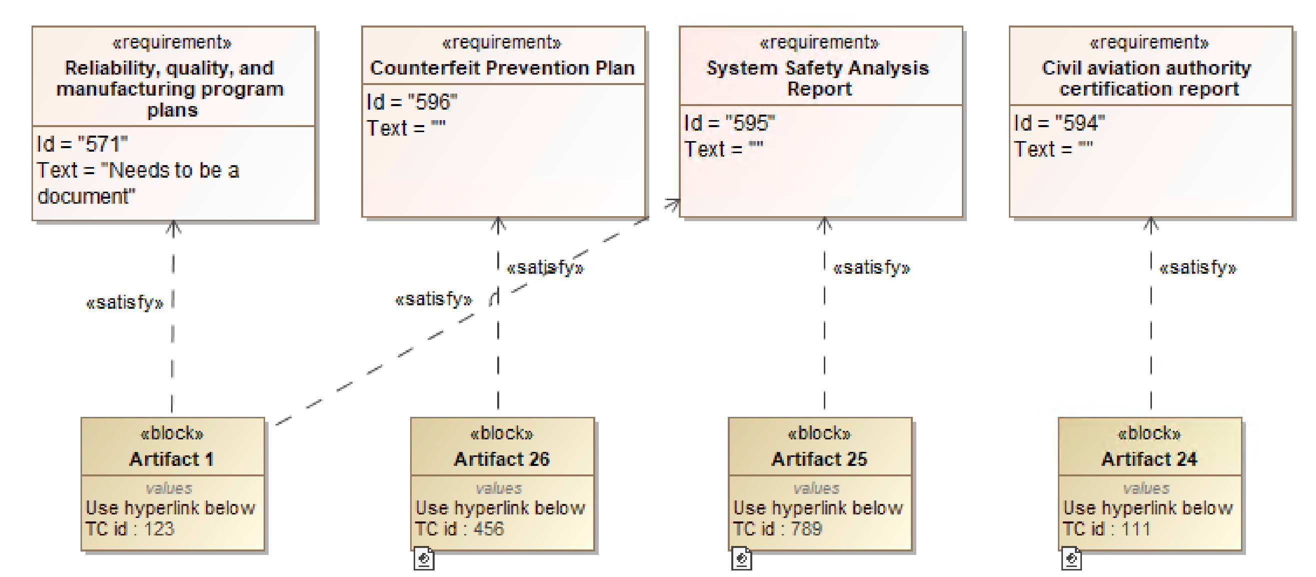
Method of Compliance: Inspection of the hazard analysis verifies that safety critical hazards have been identified and that catastrophic failures are no more frequent than improbable. Analysis of the design verifies that the required level of safety is achieved. Operating limitations are defined. The analysis includes ground rules and assumptions."

Example: Criteria 4.1.4 – Failure Conditions

SC components, FMECA and SSAR map to Criteria/Standard/MoC

Currently working with Section 4 Tech Experts to refine/validate mapping

Tracing Source Data (Artifacts) to Artifact “requirements”



«requirement»
Reliability, quality, and manufacturing program plans
Id = "571"
Text = "Needs to be a document"

«requirement»
Counterfeit Prevention Plan
Id = "596"
Text = ""

«requirement»
System Safety Analysis Report
Id = "595"
Text = ""

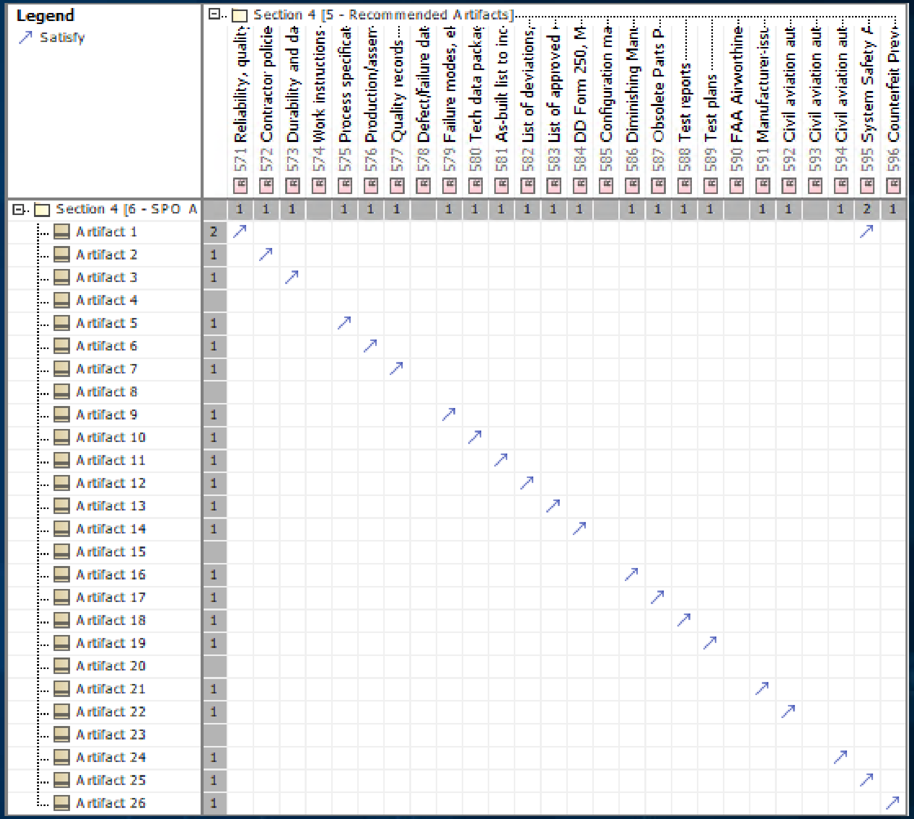
«requirement»
Civil aviation authority certification report
Id = "594"
Text = ""

«block»
Artifact 1
values
Use hyperlink below
TC id : 123

«block»
Artifact 26
values
Use hyperlink below
TC id : 456

«block»
Artifact 25
values
Use hyperlink below
TC id : 789

«block»
Artifact 24
values
Use hyperlink below
TC id : 111



Legend
↗ Satisfy

Section 4 [5 - Recommended Artifacts]

Section 4 [6 - SPO A		571 Reliability, quality	572 Contractor policie	573 Durability and da	574 Work instructions	575 Process specificat	576 Production/assem	577 Quality records	578 Defect/failure dat	579 Failure modes, ef	580 Tech data packag	581 As-built list to inc	582 List of deviations,	583 List of approved	584 DD Form 250, M	585 Configuration ma	586 Diminishing Manu	587 Obsolete Parts P	588 Test reports	589 Test plans	590 FAA Airworthine	591 Manufacturer-issu	592 Civil aviation aut	593 Civil aviation aut	594 Civil aviation aut	595 System Safety A	596 Counterfeit Prev
		1	1	1		1	1	1		1	1	1	1	1	1		1	1	1	1		1	1		1	2	1
Artifact 1	2	↗																								↗	
Artifact 2	1		↗																								
Artifact 3	1			↗																							
Artifact 4																											
Artifact 5	1					↗																					
Artifact 6	1						↗																				
Artifact 7	1							↗																			
Artifact 8																											
Artifact 9	1									↗																	
Artifact 10	1										↗																
Artifact 11	1											↗															
Artifact 12	1												↗														
Artifact 13	1													↗													
Artifact 14	1														↗												
Artifact 15																											
Artifact 16	1																↗										
Artifact 17	1																	↗									
Artifact 18	1																		↗								
Artifact 19	1																			↗							
Artifact 20																											
Artifact 21	1																					↗					
Artifact 22	1																						↗				
Artifact 23																											
Artifact 24	1																								↗		
Artifact 25	1																									↗	
Artifact 26	1																										↗

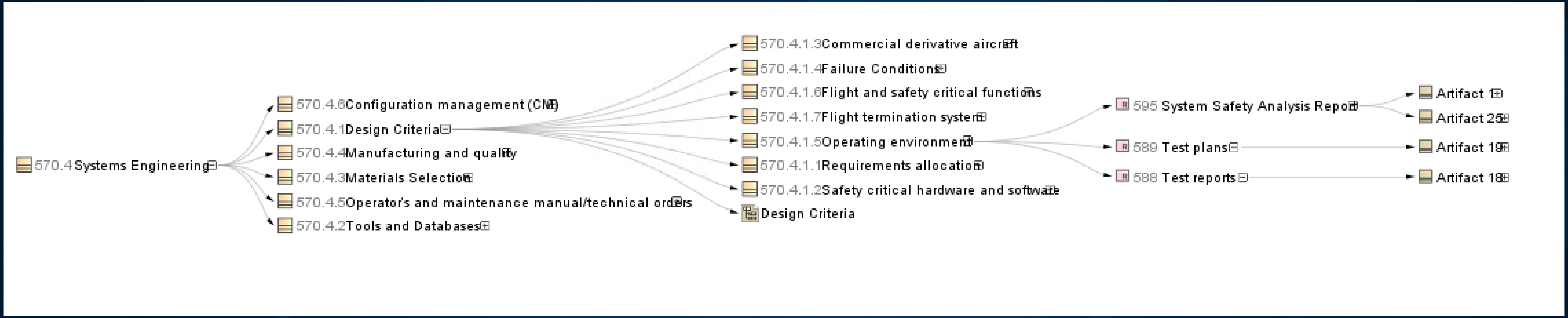
Each artifact/source data can be linked to one or many artifact “requirements”

Hyperlinked in a SharePoint library – linked to other sources (Teamcenter, etc.) via value properties

Could be data/test cases/documents, just needs linked

Also created a RVM to show relationships between artifacts and artifact “requirements”

Relational Mapping – showing the linkages


570.4 Systems Engineering
570.4.6 Configuration management (CM)
570.4.1 Design Criteria
570.4.4 Manufacturing and quality
570.4.3 Materials Selection
570.4.5 Operator's and maintenance manual/technical orders
570.4.2 Tools and Databases
570.4.1.3 Commercial derivative aircraft
570.4.1.4 Failure Conditions
570.4.1.6 Flight and safety critical functions
570.4.1.7 Flight termination system
570.4.1.5 Operating environment
570.4.1.1 Requirements allocation
570.4.1.2 Safety critical hardware and software
Design Criteria
595 System Safety Analysis Report
589 Test plans
588 Test reports
Artifact 1
Artifact 25
Artifact 19
Artifact 18

- Created a relational map – Section -> Subsection -> Criteria -> “requirement” -> Data/Artifact
- Could interface with Requirements tool (DOORS, etc.) and PLM (Teamcenter, etc) to do revisional control of Cert Basis, Compliance Report and Artifacts / Source Data
- Mapping gives the capability to create “standard work” when putting source data on contract or during the airworthiness process

Contact Information:

Noah “Odie” Demerly

noah.demerly.3@us.af.mil

dafdto.com

USAF Digital Guide:

https://wss.apan.org/af/aflcmc/default.aspx

(must create an account)

Questions?

DTO