STPA Applied to Military Certification Process

1st Lt Diniz, Doc Eng Carlos Lahoz, Captain Silveira

Technological Institute of Aeronautics (ITA)

Brazilian Air Force - Industrial Fostering and Coordination Institute (IFI)

Objective

This research demonstrates the results of applied STPA in the systemic factors that influence safety and/or mission accomplishment in the context of Brazilian Military Aerospace Certification.

Headlines:

1) Motivation

2) Introduction – Military Type Certification Process

3) Losses

4) Hazards

5) Hierarchical Control Structure

6) Unsafe Control Actions

7) Loss Scenarios

8) Conclusions

Motivation

Statistics are based on all worldwide commercial (passenger) fatal accidents involving civil aircraft with a minimum capacity of 14 passengers, from the ASN Safety Database https://aviation-safety.net

AviationSafetyNetwork

Type Certification Process

AIRWORTHINESS REQUIREMENTS

FIT FOR FLIGHT

PERFORMANCE REQUIREMENTS

FIT FOR PURPOSE

Weapon System Specification

COMPLIANCE

INTEGRATION

Design Configuration

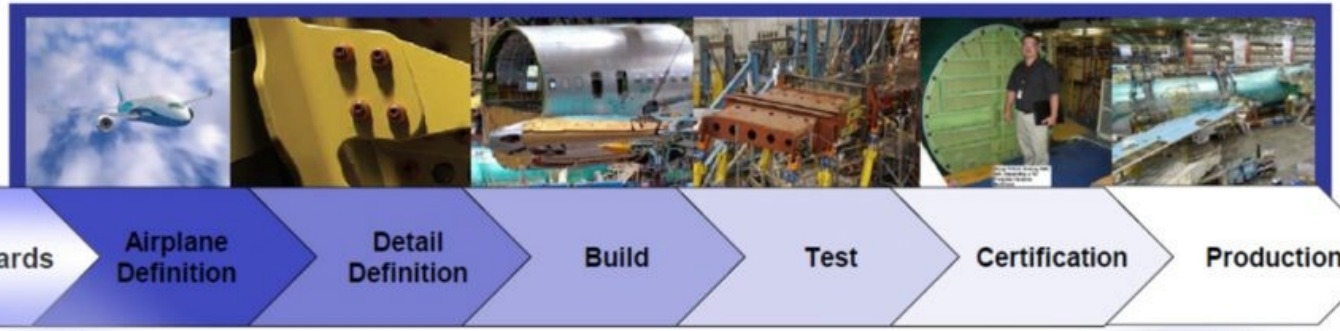
CERTIFICATION BASIS

Military Type Certification Process

Type Certificate

Type Certification Process

Design and Production Approval



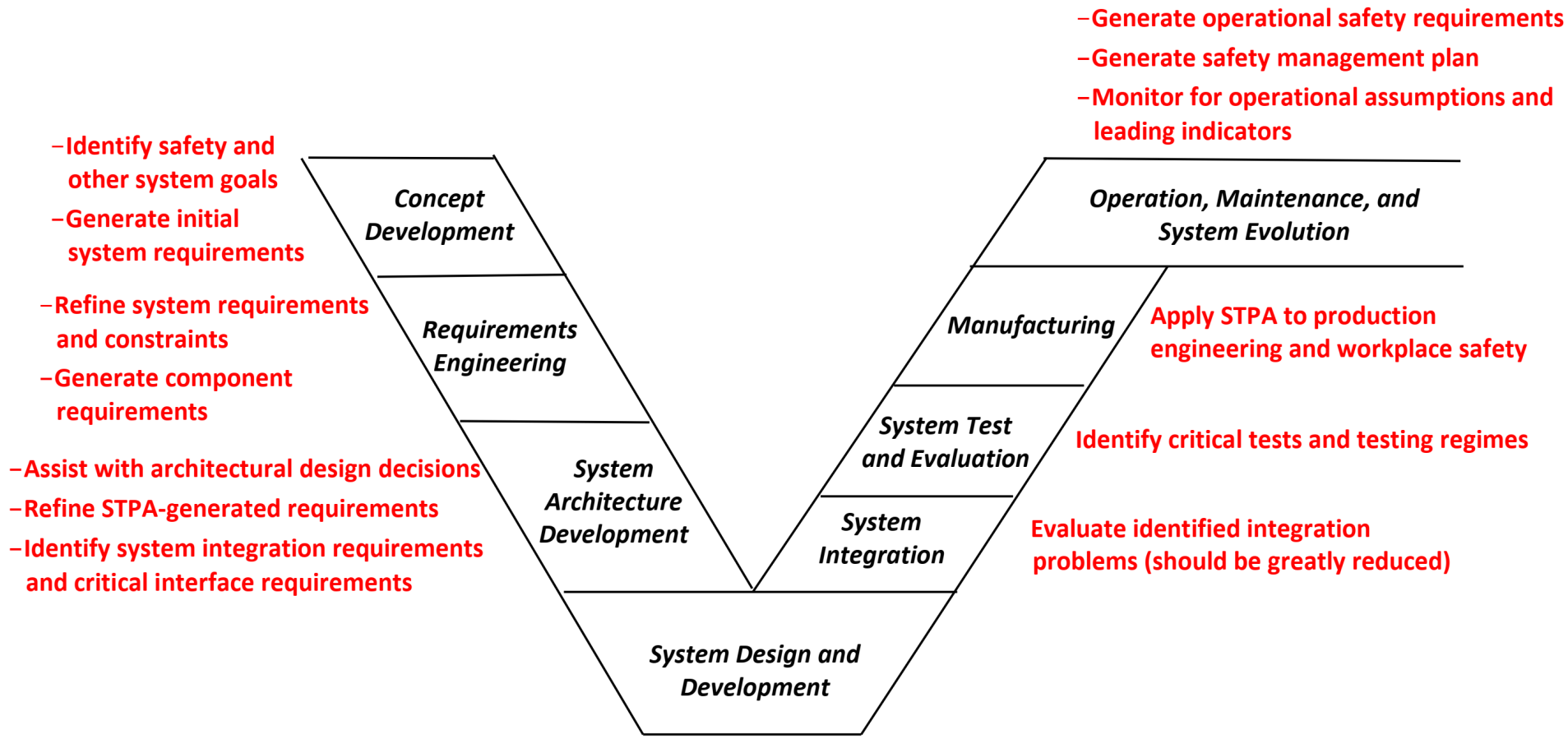
Standards | Airplane Definition | Detail Definition | Build | Test | Certification | Production

Familiarization Briefings
Application for TC/ATC/STC
Certification Project Notification
Application for Production Certificate
Preliminary Type Certification Board
Preliminary District Office Audit
Production Certification Board
Issue papers
Certification Basis
Equivalent Safety Findings
Special conditions
Exemptions
Certification plans

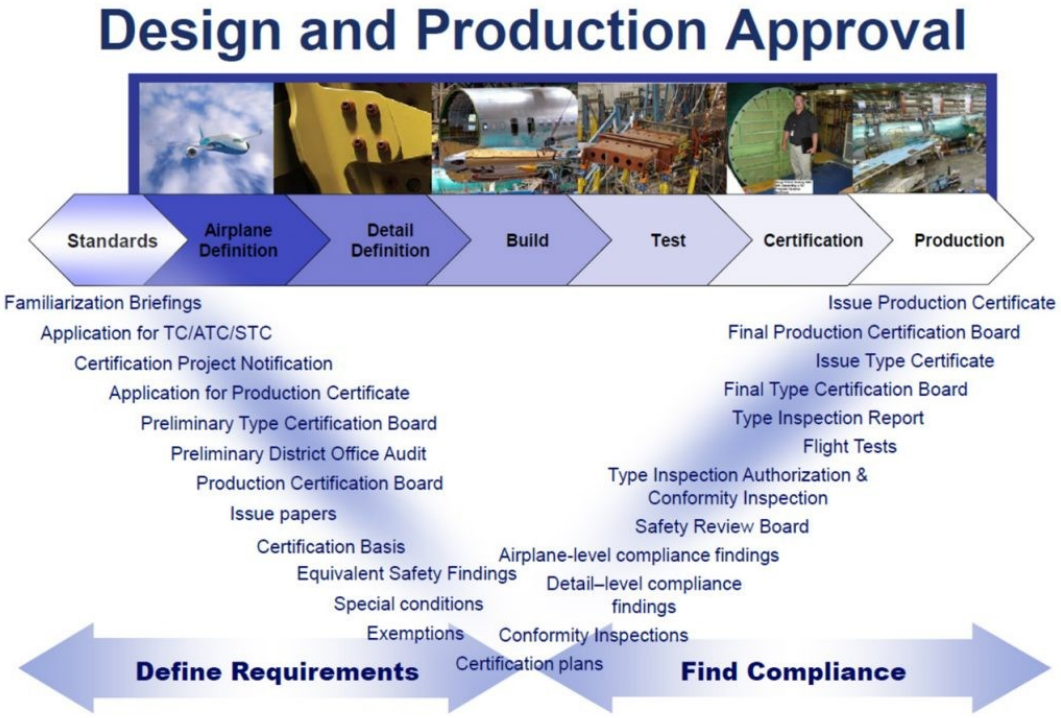
Issue Production Certificate
Final Production Certification Board
Issue Type Certificate
Final Type Certification Board
Type Inspection Report
Flight Tests
Type Inspection Authorization & Conformity Inspection
Safety Review Board
Airplane-level compliance findings
Detail–level compliance findings
Conformity Inspections

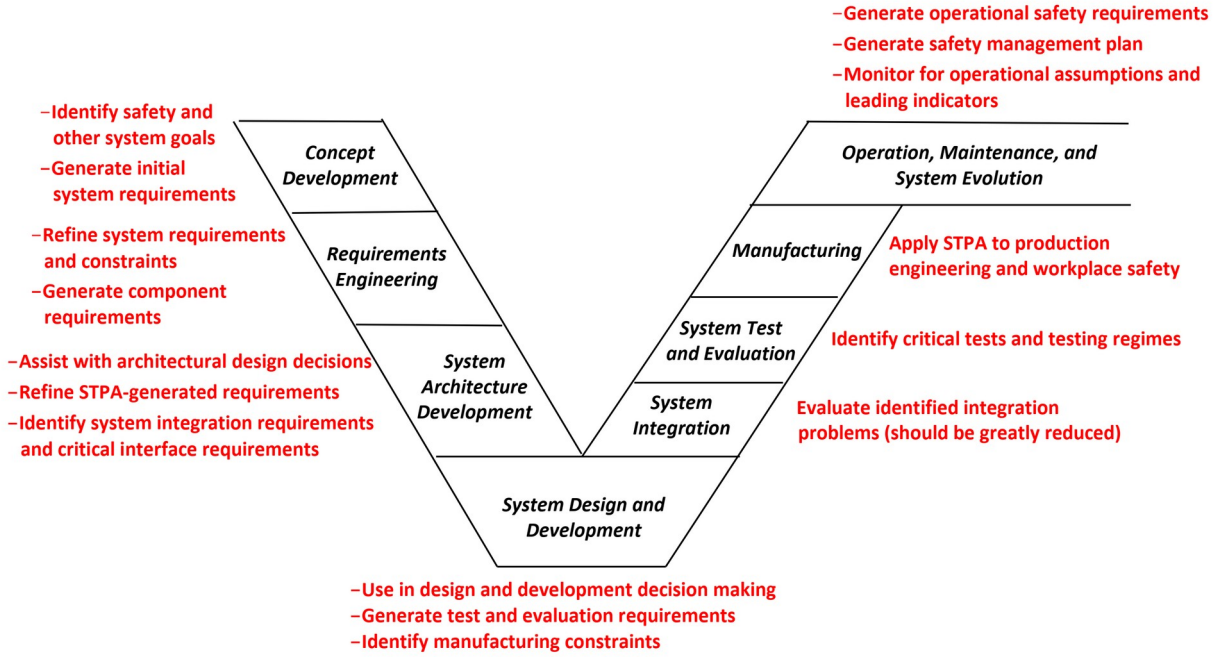
Define Requirements | **Find Compliance**

Type Certification Process



Type Certification Process





LOSSES

L-1: Loss or damage to test environments.

L-2: Loss of mission (or performance degradation).

L-3: Financial loss.

L-4: Loss due to rescheduling.

L-5: Loss of client satisfaction.

L-6: Loss of product certification.

L-7: Loss of classified information.

L-8: Loss of Human Life, Human Injury, Properties Damage or Environmental Losses.

HAZARDS

H-1: Company doesn't complete the certification processes. [L-1, L-3, L-5, L-6, L-8]

H-2: Products accepted in non-conformance with the specification. [L-1, L-2, L-3, L-5, L-6, L-8]

H-3: Certification Tests not performed as scheduled. [L-4, L-5, L-6]

H-4: Certification Process temporally interrupted due to budgetary constraints to the project. [L-4]

H-5: Leaking of project or production documentation. [L-5, L-7]

H-6: Product, Design or Quality Management System certificate expired by time or cancelled due to failures of the products in operational life. [L-3, L-4, L-5, L-6]

H-7: Design, Product, Quality Management System or Manufacturing Process certified with safety or mission related requirements not verified or not specified. [L-1, L-2, L-3, L-5, L-8]

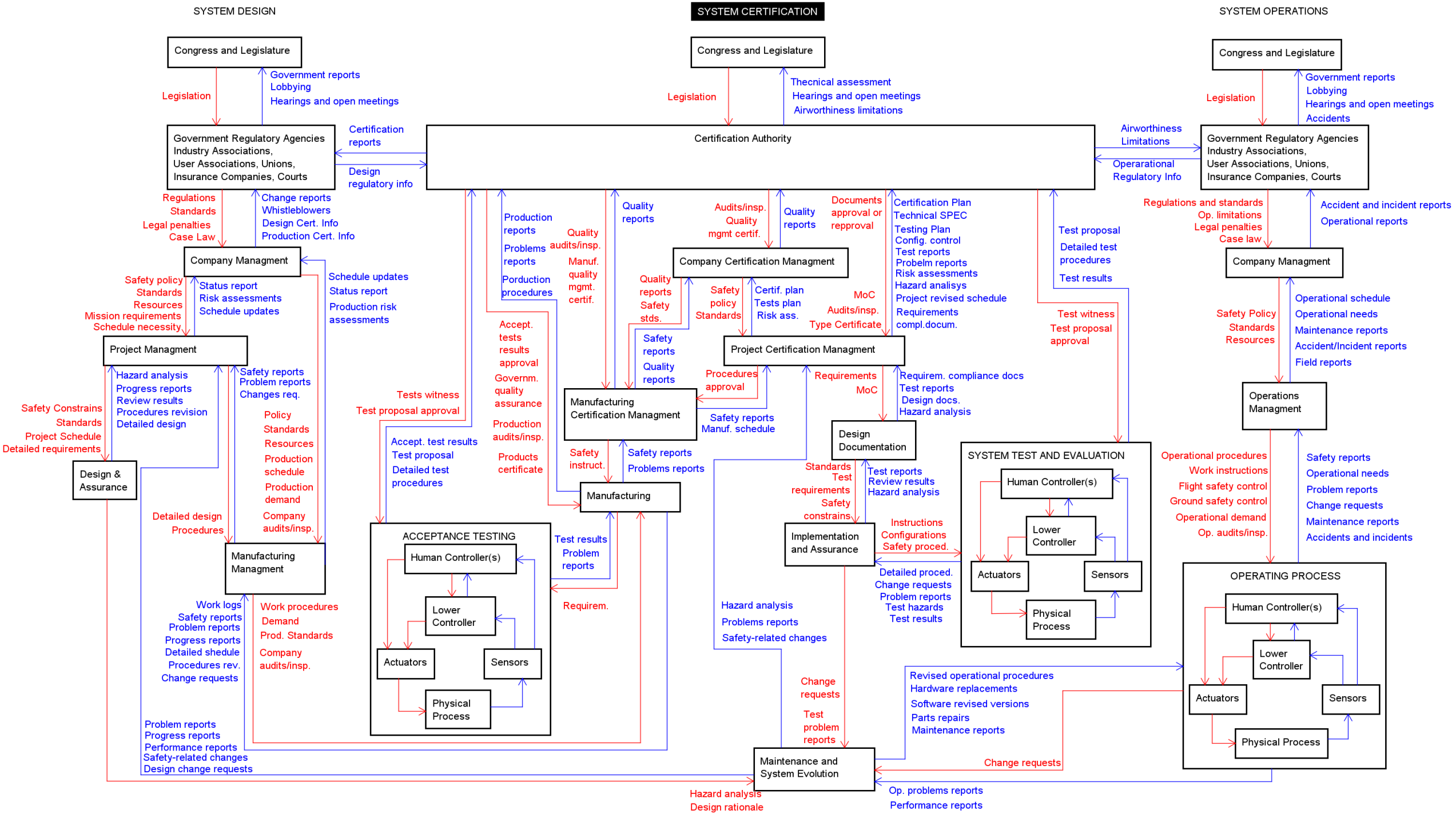
H-8: Reports, procedures, components, prototypes or design/production documents disapproved by Certification Authority. [L-3, L-4, L-5]

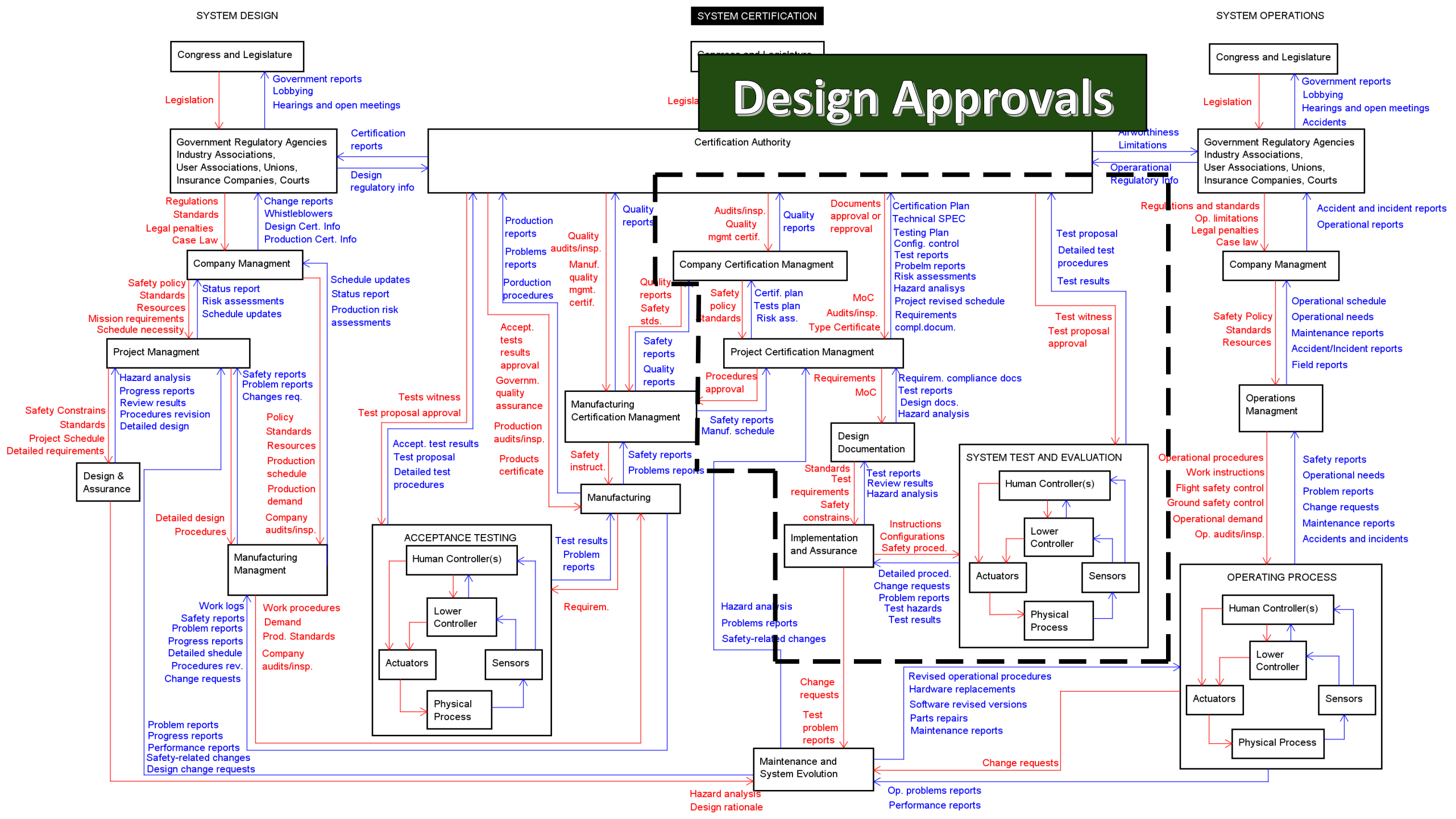
H-9: Certification Process implemented is not adequate to identify critical flaws or loss scenarios. [L-2, L-3, L-4, L-5, L-8]

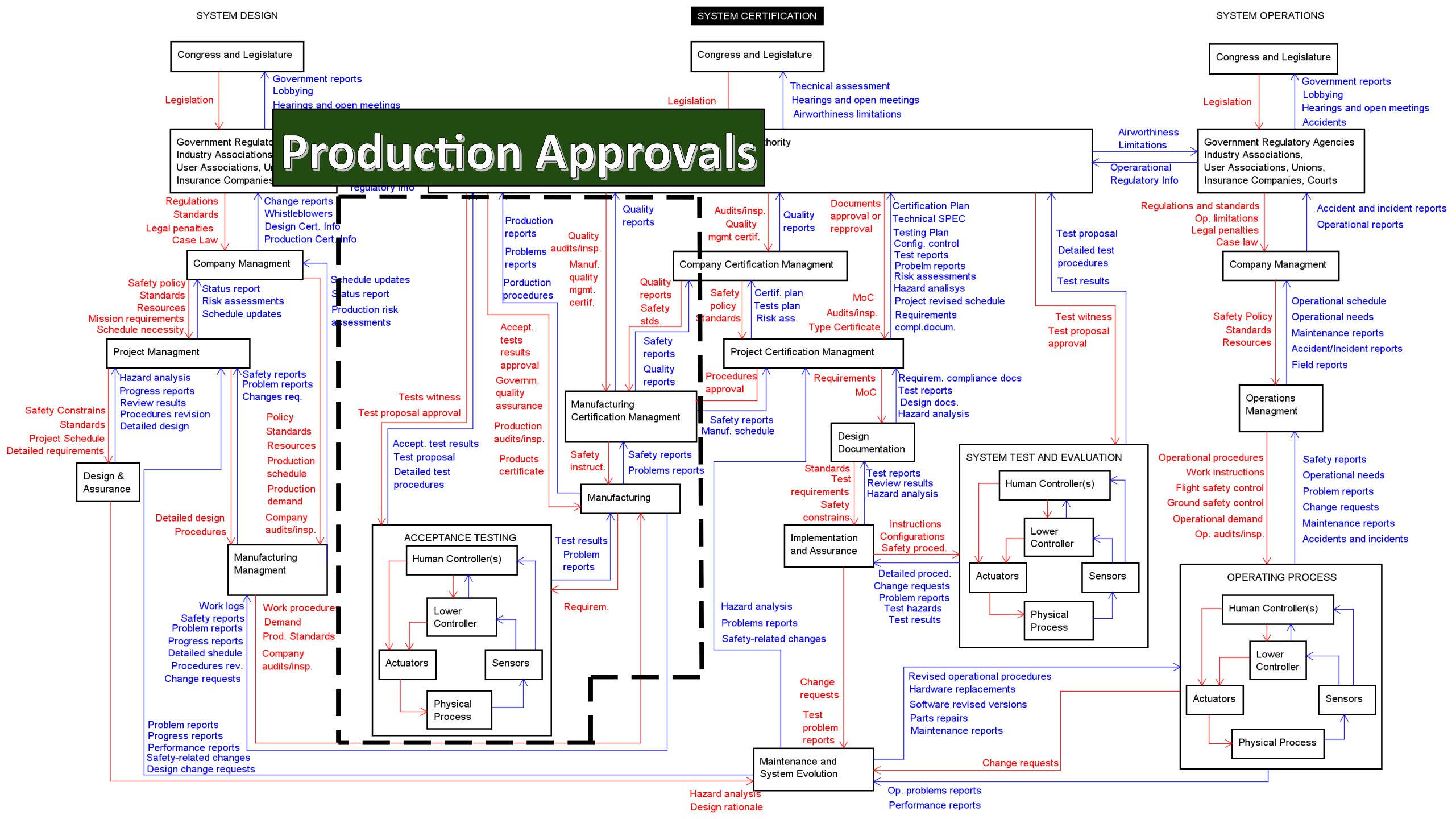
H-10: Certification Authority personal, including Organization Designation Authorization (ODA), unqualified to the product in analyse or at the certification process. [L-1, L-2, L-5, L-8]

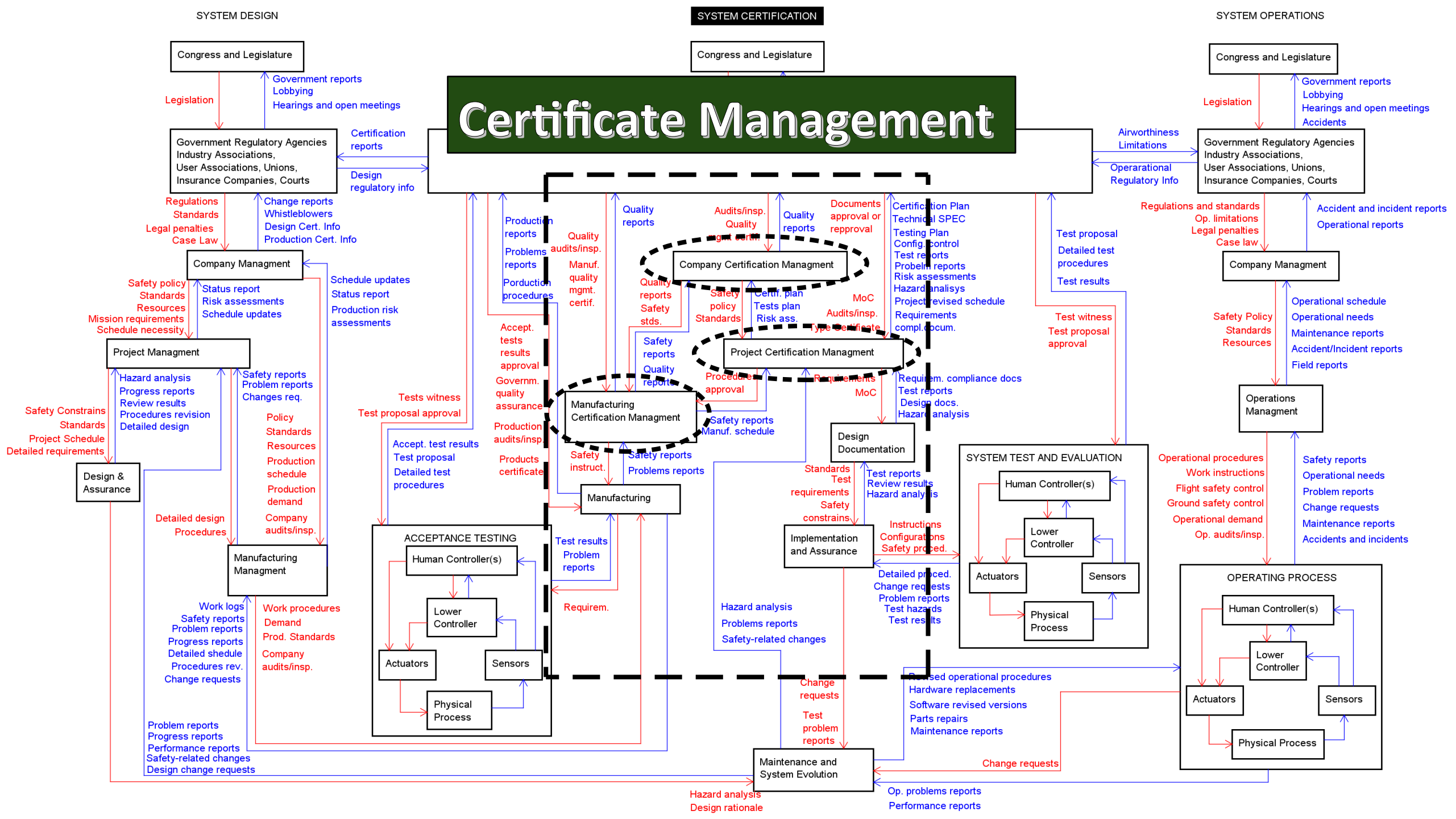
Hazard	Safety Constrains
H-1	SC-1.1: The Quality Management Systems and Manufacturing Processes of the Company's related to the Aeronautics and Space activities shall be certified. SC-1.2: All the safety/mission critical military aerospace designs and products shall be Certified to allow use or operation.
H-2	SC-2.1: Verify the conformity of the products to respective certified design. SC-2.2: The products shall be in conformity with the design. If it's not, it shall not be used or operated.
H-3	SC-3.1: The test planning shall consider the financial restrictions and the management risks of the project.
H-4	SC-4.1: The financial budget for the project development and production shall be allocated by the sponsors. SC-4.2: In case of budget restriction is unavoidable, the company management shall prioritize the activities without compromising safety or performance aspects.
H-5	SC-5.1: Sensitive information regarding the aircrafts, vehicles, payloads and ground support systems designs or procedures; personnel data; production process; material; organic or operational safety information, among others, shall be kept with the allocated restricted access.

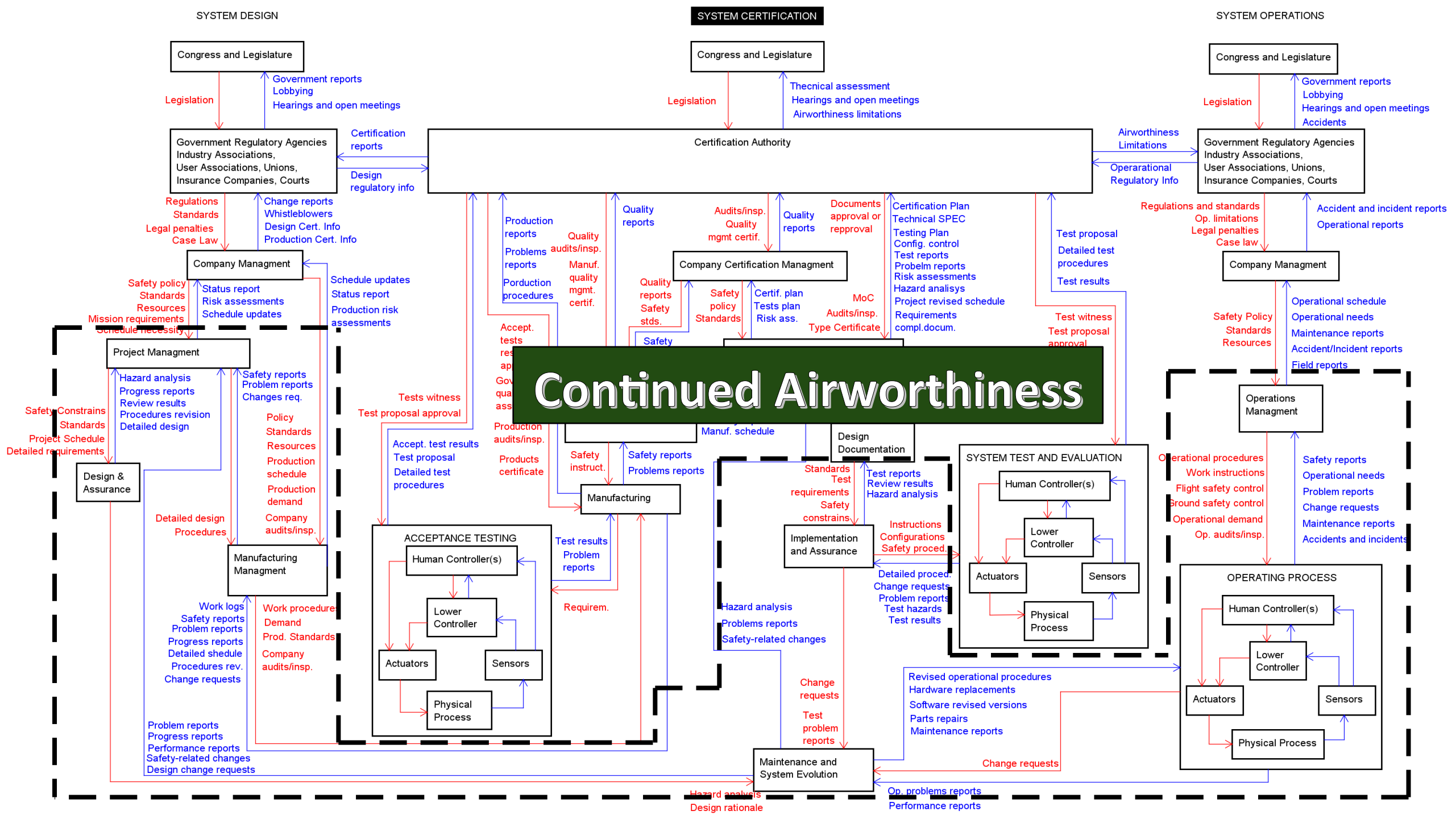
Hazard	Safety Constrains
H-6	SC-6.1: The owner of a certificate product shall be aware of the expiration date, if applicable, and provide the necessary documentation to avoid its expiration. SC-6.2: The owner of a certificate product shall maintain the system safety and the manufacturing according to the design approved to avoid the certificate to be cancelled.
H-7	SC-7.1: The certification process shall allow verification of all safety critical or performance requirements and also the system functions.
H-8	SC-8.1: The reports, procedures and documents not approved by Certification Authority shall be revised and the revisions shall be submitted to the Certification Authority for approval. It might be necessary to repeat test or simulations in order to verify design changes.
H-9	SC-9.1: The Certification Authority personnel shall be qualified at the certification process. SC-9.2: The Certification Authority personnel shall be qualified according to project/production area they are analysing.
H-10	SC-10.1: The certification process shall allow identification of critical flaws and loss scenarios. SC-10.2: The certification process shall be continuously updated, allowing improvement of the procedures and regulations.


SYSTEM DESIGN
SYSTEM CERTIFICATION
SYSTEM OPERATIONS
Congress and Legislature
Legislation
Government reports
Lobbying
Hearings and open meetings
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Certification reports
Design regulatory info
Certification Authority
Thecnical assessment
Hearings and open meetings
Airworthiness limitations
Airworthiness Limitations
Operarational Regulatory Info
Regulations
Standards
Legal penalties
Case Law
Change reports
Whistleblowers
Design Cert. Info
Production Cert. Info
Company Managment
Safety policy
Standards
Resources
Mission requirements
Schedule necessity
Status report
Risk assessments
Schedule updates
Schedule updates
Status report
Production risk assessments
Project Managment
Safety Constrains
Standards
Project Schedule
Detailed requirements
Hazard analysis
Progress reports
Review results
Procedures revision
Detailed design
Safety reports
Problem reports
Changes req.
Policy
Standards
Resources
Production schedule
Production demand
Company audits/insp.
Design & Assurance
Detailed design
Procedures
Manufacturing Managment
Work logs
Safety reports
Problem reports
Progress reports
Detailed shedule
Procedures rev.
Change requests
Work procedures
Demand
Prod. Standards
Company audits/insp.
Problem reports
Progress reports
Performance reports
Safety-related changes
Design change requests
Production reports
Problems reports
Porduction procedures
Quality audits/insp.
Manuf. quality mgmt. certif.
Quality reports
Tests witness
Test proposal approval
Accept. test results
Test proposal
Detailed test procedures
Accept. tests results approval
Governm. quality assurance
Production audits/insp.
Products certificate
ACCEPTANCE TESTING
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Test results
Problem reports
Requirem.
Manufacturing Certification Managment
Safety instruct.
Safety reports
Problems reports
Manufacturing
Audits/insp.
Quality mgmt certif.
Quality reports
Company Certification Managment
Quality reports
Safety stds.
Safety policy
Standards
Certif. plan
Tests plan
Risk ass.
Safety reports
Quality reports
Project Certification Managment
Procedures approval
Safety reports
Manuf. schedule
Documents approval or repproval
MoC
Audits/insp.
Type Certificate
Requirements
MoC
Design Documentation
Standards
Test requirements
Safety constrains
Implementation and Assurance
Certification Plan
Technical SPEC
Testing Plan
Config. control
Test reports
Probelm reports
Risk assessments
Hazard analisys
Project revised schedule
Requirements compl.docum.
Requirem. compliance docs
Test reports
Design docs.
Hazard analysis
Test reports
Review results
Hazard analysis
Instructions
Configurations
Safety proced.
Detailed proced.
Change requests
Problem reports
Test hazards
Test results
Hazard analysis
Problems reports
Safety-related changes
Change requests
Test problem reports
Maintenance and System Evolution
Hazard analysis
Design rationale
Test proposal
Detailed test procedures
Test results
Test witness
Test proposal approval
SYSTEM TEST AND EVALUATION
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Regulations and standards
Op. limitations
Legal penalties
Case law
Accident and incident reports
Operational reports
Company Managment
Safety Policy
Standards
Resources
Operational schedule
Operational needs
Maintenance reports
Accident/Incident reports
Field reports
Operations Managment
Operational procedures
Work instructions
Flight safety control
Ground safety control
Operational demand
Op. audits/insp.
Safety reports
Operational needs
Problem reports
Change requests
Maintenance reports
Accidents and incidents
OPERATING PROCESS
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Revised operational procedures
Hardware replacements
Software revised versions
Parts repairs
Maintenance reports
Change requests
Op. problems reports
Performance reports


Design Approvals
SYSTEM DESIGN
SYSTEM CERTIFICATION
SYSTEM OPERATIONS
Congress and Legislature
Legislation
Government reports
Lobbying
Hearings and open meetings
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Certification reports
Design regulatory info
Certification Authority
Airworthiness Limitations
Operarational Regulatory Info
Regulations
Standards
Legal penalties
Case Law
Change reports
Whistleblowers
Design Cert. Info
Production Cert. Info
Company Managment
Safety policy
Standards
Resources
Mission requirements
Schedule necessity
Status report
Risk assessments
Schedule updates
Schedule updates
Status report
Production risk assessments
Project Managment
Hazard analysis
Progress reports
Review results
Procedures revision
Detailed design
Safety reports
Problem reports
Changes req.
Safety Constrains
Standards
Project Schedule
Detailed requirements
Design & Assurance
Policy
Standards
Resources
Production schedule
Production demand
Company audits/insp.
Detailed design
Procedures
Manufacturing Managment
Work logs
Safety reports
Problem reports
Progress reports
Detailed shedule
Procedures rev.
Change requests
Work procedures
Demand
Prod. Standards
Company audits/insp.
Problem reports
Progress reports
Performance reports
Safety-related changes
Design change requests
Production reports
Problems reports
Porduction procedures
Quality audits/insp.
Manuf. quality mgmt. certif.
Quality reports
Tests witness
Test proposal approval
Accept. test results
Test proposal
Detailed test procedures
Accept. tests results approval
Governm. quality assurance
Production audits/insp.
Products certificate
ACCEPTANCE TESTING
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Test results
Problem reports
Requirem.
Manufacturing
Safety instruct.
Safety reports
Problems reports
Manufacturing Certification Managment
Safety reports
Quality reports
Quality reports
Safety stds.
Audits/insp.
Quality mgmt certif.
Quality reports
Company Certification Managment
Safety policy standards
Certif. plan
Tests plan
Risk ass.
Documents approval or repproval
MoC
Audits/insp.
Type Certificate
Project Certification Managment
Procedures approval
Safety reports
Manuf. schedule
Requirements
MoC
Design Documentation
Certification Plan
Technical SPEC
Testing Plan
Config. control
Test reports
Probelm reports
Risk assessments
Hazard analisys
Project revised schedule
Requirements compl.docum.
Requirem. compliance docs
Test reports
Design docs.
Hazard analysis
Standards
Test requirements
Safety constrains
Test reports
Review results
Hazard analysis
Implementation and Assurance
Instructions
Configurations
Safety proced.
Detailed proced.
Change requests
Problem reports
Test hazards
Test results
Hazard analysis
Problems reports
Safety-related changes
Change requests
Test problem reports
Maintenance and System Evolution
Hazard analysis
Design rationale
Revised operational procedures
Hardware replacements
Software revised versions
Parts repairs
Maintenance reports
Change requests
Op. problems reports
Performance reports
Test proposal
Detailed test procedures
Test results
Test witness
Test proposal approval
SYSTEM TEST AND EVALUATION
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Regulations and standards
Op. limitations
Legal penalties
Case law
Accident and incident reports
Operational reports
Company Managment
Safety Policy
Standards
Resources
Operational schedule
Operational needs
Maintenance reports
Accident/Incident reports
Field reports
Operations Managment
Operational procedures
Work instructions
Flight safety control
Ground safety control
Operational demand
Op. audits/insp.
Safety reports
Operational needs
Problem reports
Change requests
Maintenance reports
Accidents and incidents
OPERATING PROCESS
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process


Production Approvals
SYSTEM DESIGN
SYSTEM CERTIFICATION
SYSTEM OPERATIONS
Congress and Legislature
Legislation
Government reports
Lobbying
Hearings and open meetings
Thecnical assessment
Airworthiness limitations
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Airworthiness Limitations
Operarational Regulatory Info
Regulations and standards
Op. limitations
Legal penalties
Case law
Accident and incident reports
Operational reports
Regulations
Standards
Legal penalties
Case Law
Change reports
Whistleblowers
Design Cert. Info
Production Cert.Info
Company Managment
Safety policy
Standards
Resources
Mission requirements
Schedule necessity
Status report
Risk assessments
Schedule updates
Production risk assessments
Project Managment
Hazard analysis
Progress reports
Review results
Procedures revision
Detailed design
Safety reports
Problem reports
Changes req.
Safety Constrains
Standards
Project Schedule
Detailed requirements
Design & Assurance
Policy
Standards
Resources
Production schedule
Production demand
Company audits/insp.
Detailed design
Procedures
Manufacturing Managment
Work logs
Safety reports
Problem reports
Progress reports
Detailed shedule
Procedures rev.
Change requests
Work procedures
Demand
Prod. Standards
Company audits/insp.
Problem reports
Progress reports
Performance reports
Safety-related changes
Design change requests
Production reports
Problems reports
Porduction procedures
Quality audits/insp.
Manuf. quality mgmt. certif.
Schedule updates
Status report
Production risk assessments
Quality reports
Tests witness
Test proposal approval
Accept. test results
Test proposal
Detailed test procedures
Accept. tests results approval
Governm. quality assurance
Production audits/insp.
Products certificate
ACCEPTANCE TESTING
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Test results
Problem reports
Requirem.
Manufacturing Certification Managment
Safety instruct.
Safety reports
Problems reports
Manufacturing
Work instructions
Safety reports
Problem reports
Progress reports
Detailed shedule
Procedures rev.
Change requests
Company audits/insp.
Hazard analysis
Design rationale
Audits/insp.
Quality mgmt certif.
Quality reports
Documents approval or repproval
Company Certification Managment
Quality reports
Safety stds.
Safety reports
Quality reports
Safety policy
Standards
Certif. plan
Tests plan
Risk ass.
MoC
Audits/insp.
Type Certificate
Project Certification Managment
Procedures approval
Safety reports
Manuf. schedule
Requirements
MoC
Requirem. compliance docs
Test reports
Design docs.
Hazard analysis
Design Documentation
Standards
Test requirements
Safety constrains
Test reports
Review results
Hazard analysis
Implementation and Assurance
Instructions
Configurations
Safety proced.
Detailed proced.
Change requests
Problem reports
Test hazards
Test results
Hazard analysis
Problems reports
Safety-related changes
Change requests
Test problem reports
Maintenance and System Evolution
Certification Plan
Technical SPEC
Testing Plan
Config. control
Test reports
Probelm reports
Risk assessments
Hazard analisys
Project revised schedule
Requirements compl.docum.
Test witness
Test proposal approval
Test proposal
Detailed test procedures
Test results
SYSTEM TEST AND EVALUATION
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Revised operational procedures
Hardware replacements
Software revised versions
Parts repairs
Maintenance reports
Change requests
Op. problems reports
Performance reports
Safety Policy
Standards
Resources
Operational schedule
Operational needs
Maintenance reports
Accident/Incident reports
Field reports
Operations Managment
Operational procedures
Work instructions
Flight safety control
Ground safety control
Operational demand
Op. audits/insp.
Safety reports
Operational needs
Problem reports
Change requests
Maintenance reports
Accidents and incidents
OPERATING PROCESS
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process


SYSTEM DESIGN
SYSTEM CERTIFICATION
SYSTEM OPERATIONS
Certificate Management
Congress and Legislature
Legislation
Government reports
Lobbying
Hearings and open meetings
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Certification reports
Design regulatory info
Airworthiness Limitations
Operarational Regulatory Info
Regulations
Standards
Legal penalties
Case Law
Change reports
Whistleblowers
Design Cert. Info
Production Cert. Info
Company Managment
Safety policy
Standards
Resources
Mission requirements
Schedule necessity
Status report
Risk assessments
Schedule updates
Schedule updates
Status report
Production risk assessments
Project Managment
Hazard analysis
Progress reports
Review results
Procedures revision
Detailed design
Safety reports
Problem reports
Changes req.
Safety Constrains
Standards
Project Schedule
Detailed requirements
Design & Assurance
Policy
Standards
Resources
Production schedule
Production demand
Company audits/insp.
Detailed design
Procedures
Manufacturing Managment
Work logs
Safety reports
Problem reports
Progress reports
Detailed shedule
Procedures rev.
Change requests
Work procedures
Demand
Prod. Standards
Company audits/insp.
Problem reports
Progress reports
Performance reports
Safety-related changes
Design change requests
Production reports
Problems reports
Porduction procedures
Quality audits/insp.
Manuf. quality mgmt. certif.
Quality reports
Audits/insp.
Quality mgmt. certif.
Quality reports
Documents approval or repproval
Company Certification Managment
Quality reports
Safety stds.
Safety policy
Standards
Certif. plan
Tests plan
Risk ass.
MoC
Audits/insp.
Type Certificate
Project Certification Managment
Procedures approval
Requirements
MoC
Certification Plan
Technical SPEC
Testing Plan
Config. control
Test reports
Probelm reports
Risk assessments
Hazard analisys
Project revised schedule
Requirements compl.docum.
Requirem. compliance docs
Test reports
Design docs.
Hazard analysis
Test proposal
Detailed test procedures
Test results
Test witness
Test proposal approval
Accept. tests results approval
Governm. quality assurance
Production audits/insp.
Products certificate
Manufacturing Certification Managment
Safety reports
Manuf. schedule
Safety reports
Quality reports
Tests witness
Test proposal approval
Accept. test results
Test proposal
Detailed test procedures
Safety instruct.
Safety reports
Problems reports
Manufacturing
Design Documentation
Standards
Test requirements
Safety constrains
Test reports
Review results
Hazard analysis
Implementation and Assurance
Instructions
Configurations
Safety proced.
Detailed proced.
Change requests
Problem reports
Test hazards
Test results
Hazard analysis
Problems reports
Safety-related changes
ACCEPTANCE TESTING
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Test results
Problem reports
Requirem.
SYSTEM TEST AND EVALUATION
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Change requests
Test problem reports
Maintenance and System Evolution
Revised operational procedures
Hardware replacements
Software revised versions
Parts repairs
Maintenance reports
Change requests
Hazard analysis
Design rationale
Op. problems reports
Performance reports
Regulations and standards
Op. limitations
Legal penalties
Case law
Accident and incident reports
Operational reports
Company Managment
Safety Policy
Standards
Resources
Operational schedule
Operational needs
Maintenance reports
Accident/Incident reports
Field reports
Operations Managment
Operational procedures
Work instructions
Flight safety control
Ground safety control
Operational demand
Op. audits/insp.
Safety reports
Operational needs
Problem reports
Change requests
Maintenance reports
Accidents and incidents
OPERATING PROCESS
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process


SYSTEM DESIGN
SYSTEM CERTIFICATION
SYSTEM OPERATIONS
Congress and Legislature
Legislation
Government reports
Lobbying
Hearings and open meetings
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Certification reports
Design regulatory info
Certification Authority
Thecnical assessment
Hearings and open meetings
Airworthiness limitations
Airworthiness Limitations
Operarational Regulatory Info
Accidents
Regulations
Standards
Legal penalties
Case Law
Change reports
Whistleblowers
Design Cert. Info
Production Cert. Info
Company Managment
Safety policy
Standards
Resources
Mission requirements
Schedule necessity
Status report
Risk assessments
Schedule updates
Production risk assessments
Production reports
Problems reports
Porduction procedures
Quality audits/insp.
Manuf. quality mgmt. certif.
Quality reports
Company Certification Managment
Audits/insp.
Quality mgmt certif.
Quality reports
Safety policy
Standards
Certif. plan
Tests plan
Risk ass.
Documents approval or repproval
MoC
Audits/insp.
Type Certificate
Certification Plan
Technical SPEC
Testing Plan
Config. control
Test reports
Probelm reports
Risk assessments
Hazard analisys
Project revised schedule
Requirements compl.docum.
Test proposal
Detailed test procedures
Test results
Test witness
Test proposal approval
Regulations and standards
Op. limitations
Legal penalties
Case law
Accident and incident reports
Operational reports
Safety Policy
Standards
Resources
Operational schedule
Operational needs
Maintenance reports
Accident/Incident reports
Field reports
Continued Airworthiness
Project Managment
Hazard analysis
Progress reports
Review results
Procedures revision
Detailed design
Safety reports
Problem reports
Changes req.
Safety Constrains
Standards
Project Schedule
Detailed requirements
Policy
Standards
Resources
Production schedule
Production demand
Company audits/insp.
Design & Assurance
Detailed design
Procedures
Manufacturing Managment
Work logs
Safety reports
Problem reports
Progress reports
Detailed shedule
Procedures rev.
Change requests
Work procedures
Demand
Prod. Standards
Company audits/insp.
Problem reports
Progress reports
Performance reports
Safety-related changes
Design change requests
Tests witness
Test proposal approval
Accept. test results
Test proposal
Detailed test procedures
Accept. tests
Production audits/insp.
Products certificate
Safety instruct.
Safety reports
Problems reports
Manufacturing
Manuf. schedule
Test results
Problem reports
Requirem.
ACCEPTANCE TESTING
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Design Documentation
Standards
Test requirements
Safety constrains
Test reports
Review results
Hazard analysis
Implementation and Assurance
Instructions
Configurations
Safety proced.
Detailed proced.
Change requests
Problem reports
Test hazards
Test results
Hazard analysis
Problems reports
Safety-related changes
SYSTEM TEST AND EVALUATION
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Operations Managment
Operational procedures
Work instructions
Flight safety control
Ground safety control
Operational demand
Op. audits/insp.
Safety reports
Operational needs
Problem reports
Change requests
Maintenance reports
Accidents and incidents
OPERATING PROCESS
Human Controller(s)
Lower Controller
Actuators
Sensors
Physical Process
Change requests
Test problem reports
Revised operational procedures
Hardware replacements
Software revised versions
Parts repairs
Maintenance reports
Change requests
Maintenance and System Evolution
Hazard analysis
Design rationale
Op. problems reports
Performance reports

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Government Quality Assurance (GQA) (Certification Authority → Manufacturing) Production Approvals	**UCA-1.1:** Certification Authority does not provides Government Quality Assurance (GQA) at Manufacturer while critical safety/mission related components are being produced. [H-2][H-6][H-7][H-8][H-9][H-10]	**UCA-1.2:** Certification Authority provides Government Quality Assurance (GQA) at the production of all components, even those not safety or mission related. [H-1][H-4][H-9][H-10]	**UCA-1.3:** Certification Authority provides Government Quality Assurance (GQA) at the production too late, after many parts are already produced. [H-1][H-2] [H-6][H-7][H-8][H-9][H-10] **UCA-1.4:** Certification Authority provides Government Quality Assurance (GQA) at the production too early, before assembly of the production line. [H-1] [H-4] [H-9][H-10]	**UCA-1.5:** Certification Authority stopped too soon to provide the Government Quality Assurance (GQA) at the production, do not accompanying the production of some critical parts for the mission/safety. [H-1][H-2][H-6][H-7][H-8] [H-9][H-10]

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Means of Compliance (MoC) (Certification Authority → Project Certification Management) Design Approvals	**UCA-2.1:** Certification Authority does not provide or evaluate the MoC of the requirements until the end of the certification process. [H-6][H-7][H-8][H-9]	**UCA-2.2:** Certification Authority provides MoC of the requirements without interaction with the company. [H-1] [H-3] [H-4] [H-6] [H-7] [H-9] [H-10] **UCA-2.3:** Certification Authority provides MoC of the requirements according to the proposal of the company without a third-part evaluation of a certification personnel. [H-6] [H-7] [H-8] [H-9]	**UCA-2.4:** Certification Authority provides MoC of the requirements too early, before receiving any design documentation or Technical specifications. [H-1] [H-6] [H-7] [H-9] [H-10] **UCA-2.5:** Certification Authority provides MoC of the requirements too late, after the tests, simulations or system analyses had begun. [H-6] [H-7] [H-8] [H-9]	**UCA-2.6:** Certification Authority stopped too soon the determination/ evaluation of the MoC, without analysing of proposed MoC of all requirements. [H-6] [H-7] [H-8] [H-9] [H-10]

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Quality Inspections and Audits (Certification Authority → Manufacturing Certification Managment) Certificate Managment	**UCA-3.1:** Certification Authority does not provide inspections and audits in production to check the Manufacturing Process, including acceptance of critical parts to be used at the aerospace system. [H-2] [H-6] [H-7] [H-9] [H-10]	**UCA-3.2:** Certification Authority provides quality inspections and audits in production of all components, even those not related to safety or mission. [H-1] [H-4] [H-9]	**UCA-3.3:** Certification Authority provides quality inspections and audits in production too late, after critical parts are already produced. [H-2] [H-6] [H-7] [H-9] [H-10] **UCA-3.4:** Certification Authority provides quality inspections and audits in Manufactures too early, before initiate production of critical parts. [H-2] [H-6] [H-7] [H-9]	**UCA-3.5:** Certification Authority stopped too soon the quality inspections and audits, not verifying some safety critical equipment or process. [H-2] [H-6] [H-7] [H-9] [H-10] **UCA-3.6:** Certification Authority applied too long the quality inspections and audits, causing delays in the production line. [H-1] [H-3] [H-4]

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Change Requests (Implementation and Assurance → Maintenance and System Evolution) Continued Airworthiness	**UCA-4.1:** Implementation and Assurance does not provide identified change requests, while the system is being operated with unsafe procedures/ characteristics. [H-6] [H-9]	N/A	**UCA-4.2:** Implementation and Assurance provides change requests too late, after critical events already happened. [H-6] **UCA-4.3:** Implementation and Assurance provides change requests out of order, at a way the Maintenance and System Evolution are not able to implement the requested changes at the product. [H-6] [H-9]	**UCA-4.4:** Implementation and Assurance stopped too soon to provide change requests, even knowing the Airworthiness may be compromised due to system obsolescence. [H-6] [H-9]

Loss Scenarios

a) Identifying scenarios that lead to Unsafe Control Actions

Suppose that the following **unsafe control action was provided** by the controller:

UCA-2.3: Certification Authority provides MoC of the requirements according to the proposal of the company, without a third-part evaluation by a certification personnel.

The question that should be used to this case is:
“What are the causal factors that make the MoC of the requirements to be provided or approved by the Certification Authority without a third-part evaluation by a certification personnel?”

Loss Scenarios

Type a – Unsafe control action was provided by the controller

UCA-2.3: “Certification Authority provides MoC of the requirements according to the proposal of the company, without a third-part evaluation by a certification personnel.”

Scenario	Associated Causal Factor	Requirement	Allocated To	Rationale
[Incorrect or no information provided] The Company sent the Certification Plan with proposed MoC of requirements to a certification personnel, but the product was not evaluated on specified time.	Lack of Human Resource. Small amount of time to accomplish the task.	The certification personnel allocated and the analyses time provided shall be proportional to the task.	Certification Process Coordinators	Personal and time allocated may not be applicable for the task.
[Process model inconsistent, incomplete or incorrect] Current state of the process model is inconsistent, incorrect or incomplete.	Trust in the company work. MoC proposed is a copy of a similar system.	MoC of the requirements shall not be approved without a third-part evaluation by a certification personnel	System’s designers	(N/A)
[Control Input or external information wrong or missing] Certification Authority receive the MoC of the requirements or the Certification Plan as it is already approved by the Authority, not proceeding with evaluations. (Incorrect information)	Failure in the communication between Certification Authority and the Project Management.	The communication between Certification Authority and Project Management must be improved.	Certification Authority and Company Management	Simulations and tests can help to validate the system, MoC need to be properly defined

Loss Scenarios

b) Identifying scenarios in which control actions are improperly executed or not executed.

Suppose that the following **control action was provided** by the controller **but was not followed, or was executed inadequately,** by other components/operators:

SCA: “Certification Authority provides the MoC of the requirements after a third-part evaluation by a certification personnel.”

One of the questions that could be used for this case is:
“What are the causal factors that make other operators not follow or execute inadequately the Means of Compliance of the requirements approved by the Certification Authority?

Loss Scenarios

Type b – Control action was **provided** by the controller but **was not followed, or was execute inadequately**, by other components/operators:

Scenario	Associated Causal Factor	Requirement	Allocated To	Rationale
[Inadequate Operation] System Test and Evaluation cannot act (accomplishing all the tests, simulations and analyses) in order execute the MoC's defined.	Limitations of Tests Platforms. Budgetary constrains. Software not available for required simulations.	"Project Management" shall align information with the "System Test and Evaluation" and with the "Certification Authority".	Certification Personnel	Knowledge of the company and experience at previous certifications process can minimize the occurrence of this scenario.
[Inadequate Operation] Test Procedure do not allow entire verification of the accomplishment of the requirement.	Failure in the elaboration of Test Procedure	Tests Procedures shall be proposed and approved according to the requirements seeking compliance.	Designers and Testers	Simulations and tests can help to validate the system
[Inadequate Operation] Test execution not according to test proposal approved by the Certification Authority	Failure in the execution of the procedures of the Test Proposal.	Test Procedures shall be followed. For safety/mission critical related requirements, certification personnel shall be present during test execution.	Designers, Testers Certification Personnel	Simulations and tests can help to validate the system

Conclusions

The HCS of this study produced Control Actions and Feedbacks used to identify Constraints in order to propose useful Safety Recommendations to apply in the Brazilian Military Certification Authority.

Besides the Safety Constraints focused on compliance with defined certification process, were also identified gaps in this process.

These Safety Recommendations is the starting point to propose modification in the Certification Processes, minimizing the approval of unsafe systems and avoiding the occurrences of loss scenarios.

STPA - References

[1] Leveson, N. G. A new accident model for engineering safer systems. Safety Science, v. 42, n. 4, 2004, p. 1-2.

[2] Leveson, N. G. STPA-Handbook. USA, 2018.

[3] Brazilian Air Force, ICA 60-2: Procedures for certification of products and quality management systems at space sector, 2019.

[4] Leveson, N. G.; Thomas, J. STPA Primer. USA, 2013.

[5] Aviation Safety Network Graphs – www.aviation-safety.net.

[6] Leveson, N. G.; Stephanopoulos, G. A system-theoretic, control-inspired view and approach to process safety. AIChE Journal, v. 60, n. 1, 2014, p 13.

[7] FAA, The FAA and Industry Guide to Product Certification, Third Edition, 2017.

[8] Brazilian Air Force, DCA 400-6: Life Cycle of Aeronautical Systems and Materials, 2007.

[9] Brazilian Air Force, ICA 57-21: Procedures for certification of aeronautical products, 2018.

[10] Leveson, N. G. Engineering a Safer World: Systems Thinking Applied to Safety,,Cambridge, Mass.: The MIT Press, 2012.

[11] Young, W. & Leveson, N. Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory. Proceedings of the ACM, 2014, Vol 57 no 2, p. 35.

[12] Walls, L., Revie, M., Bedford, T. Risk, Reliability and Safety: Innovating Theory and Practice. 26th ESREL. Glasgow, Scotland, 2016, p. 129.

[13] STAMP Workbench 1.0.1/bcc4c6, developed by Apache Software Foundation. Copyright (C) 2018 Information-technology Promotion Agency, Japan (IPA).

[14] Brazilian Air Force, DCA 800-2: Quality and Safety of Systems and Products at COMAER, 2019.

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

Objective

This research demonstrates the results of applied STPA in the systemic factors that influence safety and/or mission accomplishment in the context of Brazilian Military Aerospace Certification.