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

Airliner Accidents Per 1 Million Flights 1977-2017

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
Type Certification Process

- AIRWORTHINESS REQUIREMENTS
  - FIT FOR FLIGHT
- PERFORMANCE REQUIREMENTS
  - FIT FOR PURPOSE
- Weapon System Specification
- COMPLIANCE
- INTEGRATION
- CERTIFICATION BASIS
- Military Type Certification Process
- Design Configuration
- Type Certificate

Copyright © IFI 2020 – Todos os direitos reservados.
Type Certification Process

Design and Production Approval

Define Requirements

Find Compliance

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

Airplane-level compliance findings
Detail-level compliance findings
Conformity Inspections
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

Copyright © IFI 2020 – Todos os direitos reservados.
Type Certification Process

- Identify safety and other system goals
- Generate initial system requirements
- Refine system requirements and constraints
- Generate component requirements
- Assist with architectural design decisions
- Refine STPA-generated requirements
- Identify system integration requirements and critical interface requirements

- Use in design and development decision making
- Generate test and evaluation requirements
- Identify manufacturing constraints

- Generate operational safety requirements
- Generate safety management plan
- Monitor for operational assumptions and leading indicators

Operation, Maintenance, and System Evolution

- Apply STPA to production engineering and workplace safety
- Identify critical tests and testing regimes
- Evaluate identified integration problems (should be greatly reduced)
Type Certification Process

Design and Production Approval

- Identify safety and other system goals
- Generate initial system requirements
- Refine system requirements and constraints
- Generate component requirements
- Assist with architectural design decisions
- Refine STPA-generated requirements
- Identify system integration requirements and critical interface requirements

- Use in design and development decision making
- Generate test and evaluation requirements
- Identify manufacturing constraints

Copyright © IFI 2020 – Todos os direitos reservados.
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]
<table>
<thead>
<tr>
<th>Hazard</th>
<th>Safety Constrains</th>
</tr>
</thead>
</table>
| **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. |
<p>| <strong>H-5</strong> | 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. |</p>
<table>
<thead>
<tr>
<th>Hazard</th>
<th>Safety Constrains</th>
</tr>
</thead>
</table>
| 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. |
Continued Airworthiness
<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, too late, out of order</th>
<th>Stopped too soon, applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government Quality Assurance (GQA)</strong></td>
<td><strong>UCA-1.1:</strong> 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]</td>
<td><strong>UCA-1.2:</strong> 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]</td>
<td><strong>UCA-1.3:</strong> 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]</td>
<td><strong>UCA-1.5:</strong> 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]</td>
</tr>
<tr>
<td><strong>Production Approvals</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, too late, out of order</th>
<th>Stopped too soon, applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Means of Compliance (MoC)</strong></td>
<td>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]</td>
<td>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]</td>
<td>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]</td>
<td>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]</td>
</tr>
<tr>
<td>(Certification Authority → Project Certification Management)</td>
<td>Design Approvals</td>
<td>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]</td>
<td>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]</td>
<td></td>
</tr>
<tr>
<td>Control Action</td>
<td>Not providing causes hazard</td>
<td>Providing causes hazard</td>
<td>Too early, too late, out of order</td>
<td>Stopped too soon, applied too long</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------</td>
<td>------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Quality Inspections and Audits (Certification Authority → Manufacturing Certification Management)</td>
<td>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]</td>
<td>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]</td>
<td>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]</td>
<td>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]</td>
</tr>
<tr>
<td>Certificate Management</td>
<td></td>
<td>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]</td>
<td></td>
<td>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]</td>
</tr>
<tr>
<td>Control Action</td>
<td>Not providing causes hazard</td>
<td>Providing causes hazard</td>
<td>Too early, too late, out of order</td>
<td>Stopped too soon, applied too long</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------</td>
<td>------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Change Requests (Implementation and Assurance → Maintenance and System Evolution)</td>
<td><strong>UCA-4.1:</strong> Implementation and Assurance does not provide identified change requests, while the system is being operated with unsafe procedures/characteristics. [H-6] [H-9]</td>
<td></td>
<td><strong>UCA-4.2:</strong> Implementation and Assurance provides change requests too late, after critical events already happened. [H-6]</td>
<td><strong>UCA-4.4:</strong> 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]</td>
</tr>
<tr>
<td>Continued Airworthiness</td>
<td><strong>N/A</strong></td>
<td></td>
<td><strong>UCA-4.3:</strong> 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]</td>
<td></td>
</tr>
</tbody>
</table>
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.”**

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

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

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