A Systemic Approach to Aircraft System Supportability

2022 MIT STAMP Workshop
INTRODUCTION

SUMMARY

• **Supportability** concerns during concept definition of a system

• Applying **STAMP** approach
INTRODUCTION

LIFE CYCLE

- Concept
- Development
- Production
- Utilization
- Support
- Retirement

A Systemic Approach to Aircraft System Supportability
INTRODUCTION

SUPPORTABILITY

Concept

- logistics
- maintenance
- recovery

SUPPORTABILITY
INTRODUCTION

SUPPORTABILITY ELEMENTS

SUPPORTABILITY

SYSTEMS PERSPECTIVE

Planning

Supply support

Training

Personnel

Computer resources

Technical data

Facilities and utilities

Packaging, handling, storage, and transportation

Test

Information

Equipment
INTRODUCTION

WHY IS SUPPORTABILITY IMPORTANT?

SUPPORTABILITY

- Concept
- Development
- Production
- Utilization
- Support
- Retirement

60% OF THE TOTAL SYSTEM LIFE CYCLE COST
INTRODUCTION

TOPICS

SUPPORTABILITY from a systems perspective
SUPPORTABILITY from system concept
STAMP (System-Theoretic Accident Model and Process)

modelling causality of value losses related to emergent properties of systems
METHODOLOGY AND RESULTS

PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

- Analysis purpose and scope definition
- Context analysis
- Causal scenarios identification
- Recommendations proposal
A Systemic Approach to Aircraft System Supportability

METHODOLOGY AND RESULTS
PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

TABLE I. VALUE LOSSES

<table>
<thead>
<tr>
<th>ID</th>
<th>Loss</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>Loss of mission</td>
<td>Impacts on operational objectives</td>
</tr>
<tr>
<td>L2</td>
<td>Loss of life of injury to people</td>
<td>Impacts on human life</td>
</tr>
<tr>
<td>33</td>
<td>Environmental losses</td>
<td>Impacts on environment</td>
</tr>
<tr>
<td>L4</td>
<td>Monetary Losses</td>
<td>Impacts on business that could lead to financial losses, including reputation, sensitive information leak</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Hazard</th>
<th>Example of contributions from support actions</th>
<th>Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Mission preparation time is exceeded</td>
<td>For time critical missions, long logistics actions can contribute to increase required preparation time</td>
<td>L1-L4</td>
</tr>
<tr>
<td>H2</td>
<td>System operational limits are exceeded</td>
<td>Support actions may lead to repair task not being performed or to the inclusion of additional problems, compromising system operational performance</td>
<td>L1-L4</td>
</tr>
<tr>
<td>H3</td>
<td>System is not ready to fulfill designated mission</td>
<td>System is not configured properly to perform a specific mission</td>
<td>L1-L4</td>
</tr>
<tr>
<td>H4</td>
<td>Mission efficiency is compromised by interference</td>
<td>Downtime can be increased by frequent and long maintenance actions, penalizing system availability and operational efficiency</td>
<td>L1-L4</td>
</tr>
<tr>
<td>H5</td>
<td>Mission critical information is exposed to unauthorized access</td>
<td>Support actions are also related to exploitation of system vulnerability</td>
<td>L1-L4</td>
</tr>
</tbody>
</table>
A Systemic Approach to Aircraft System Supportability

METHODOLOGY AND RESULTS

PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

Analysis purpose and scope definition

Context analysis

Causal scenarios identification

Recommendations proposal

OEM operator responsibilities:
- Reconfigure system depending on the expected mission [H3, H4];
- Maintain system up-to-date [H2, H3, H5];
- In-company logistics [H2];

Field team responsibilities:
- Restore aircraft system functionality on field [H2, H4; H5];
- On field logistics [H1, H2, H3];
- Assist in system recovery from accidents [H4];
- Prepare system for mission execution [H1, H2, H3]
METHODOLOGY AND RESULTS
PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

Analysis purpose and scope definition

Context analysis

Causal scenarios identification

Recommendations proposal

Examples (Hazardous Control Actions):

- OEM operator provides inadequate system update during support resulting in unexpected system behavior during operation. [H2, H3, H5]
- Field Team provides inadequate mooring in strong wind conditions, resulting in damage to Sol. [H2]
- Towing provided during preparation when system is parked causing material damage. [H2]
- Field Team does not provide maintenance action when system is not functional, resulting in unexpected system behavior during operation. [H2, H3]
- Field Team performs unload too late during mission preparation resulting in mission delay and economical losses regarding airport facilities. [H1, H4]
METHODOLOGY AND RESULTS

PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

Examples:
- a. lifting points do not support system load resulting in rupture in system attachment;
- b. access to pain point by the field team is difficult, leading the operator to take long to perform action;
- c. system incorrectly returns that the issue has been fixed leading the field team to believe that the action was completed;
- d. system diagnostic did not inform that repair task is needed leading to problem being hidden and the field team believed the system was ready for mission execution;
- e. the procedure does not inform how to perform unloading and the field team struggles to remove cargo;
- f. system provides inaccurate fault diagnosis leading the field team to perform actions that do not address the problem, delaying system availability;
- g. during logistic transport, field team towed system, but towing interface did not support traction;
- h. OEM operator updates system with compromised resource: integrity of a software update is compromised due to a successful tampering attack, then the system behavior is compromised during operation.

METHODOLOGY AND RESULTS

PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

- Analysis purpose and scope definition
- Context analysis
- Causal scenarios identification
- Recommendations proposal

Requirements Analysis
CONCLUSION

• The analysis provided the reasoning to avoid supportability related value losses (traceability);
• Important life cycle considerations addressed together during concept stage;
• STAMP/STPA structured the process and made the problem easier to study;
• Requirements definition process improved.
A Systemic Approach to Aircraft System Supportability

Carina Carla Silva  
Chief Engineer Office  
EMBRAER  
São José dos Campos, Brazil  
carina.silva@embraer.com.br

Claudio Medrado Filho  
Chief Engineer Office  
EMBRAER  
São José dos Campos, Brazil  
claudio.medrado@embraer.com.br

Alexandre Magno Pinto  
Chief Engineer Office  
EMBRAER  
São José dos Campos, Brazil  
ampinto@embraer.com.br
A Systemic Approach to Aircraft System Supportability

Carina Carla Silva  
Chief Engineer Office  
EMBRAER  
São José dos Campos, Brazil  
carina.silva@embraer.com.br

Claudio Medrado Filho  
Chief Engineer Office  
EMBRAER  
São José dos Campos, Brazil  
claudio.medrado@embraer.com.br

Alexandre Magno Pinto  
Chief Engineer Office  
EMBRAER  
São José dos Campos, Brazil  
ampinto@embraer.com.br