A Systemic Approach to Aircraft System Supportability

2022 MIT STAMP Workshop

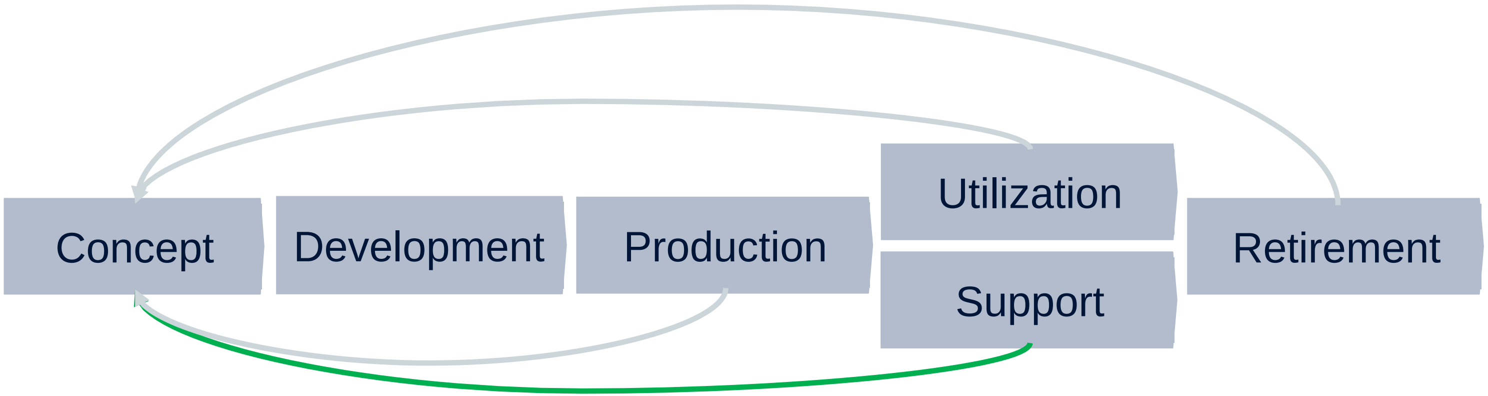
INTRODUCTION

SUMMARY

- **Supportability** concerns during concept definition of a system
- Applying **STAMP** approach

INTRODUCTION

LIFE CYCLE



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

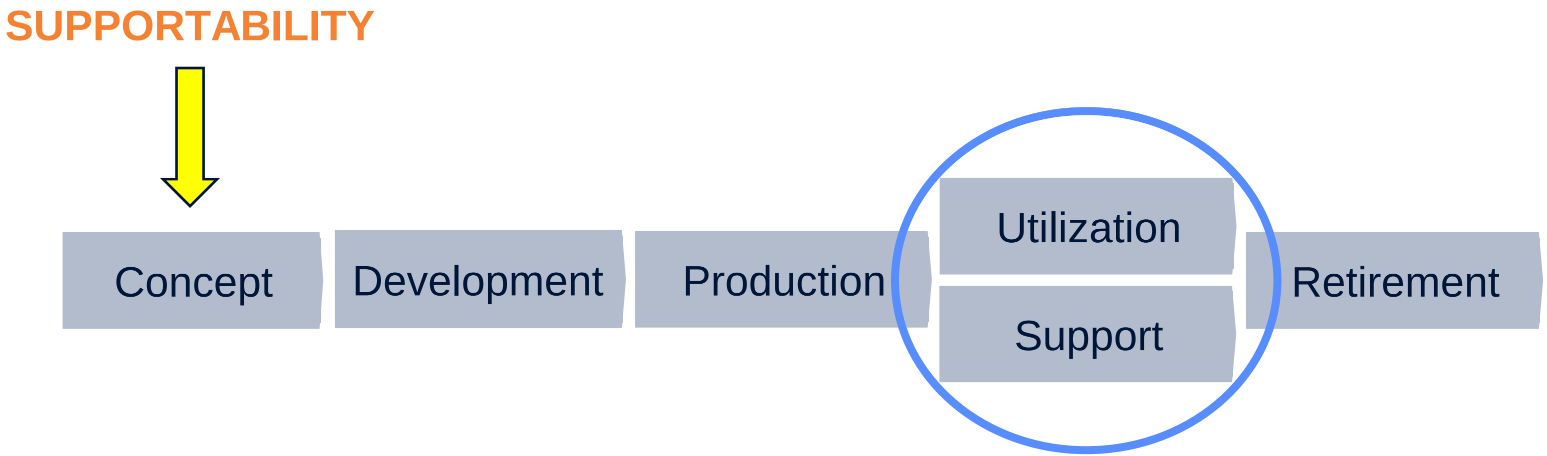
Test

Information

Equipment

INTRODUCTION

WHY IS SUPPORTABILITY IMPORTANT?



60% OF THE TOTAL
SYSTEM LIFE CYCLE COST

INTRODUCTION

TOPICS

SUPPORTABILITY from a systems perspective

SUPPORTABILITY from system concept

STAMP

INTRODUCTION

STAMP

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

METHODOLOGY AND RESULTS

PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

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

TABLE I. VALUE LOSSES

ID	Loss	Description
L1	Loss of mission	Impacts on operational objectives
L2	Loss of life of injury to people	Impacts on human life
33	Environmental losses	Impacts on environment
L4	Monetary Losses	Impacts on business that could lead to financial losses, including reputation, sensitive information leak

TABLE II. HAZARDS

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

METHODOLOGY AND RESULTS

PURPOSE: AVOID SUPPORTABILITY RELATED VALUE LOSSES FROM CONCEPT

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

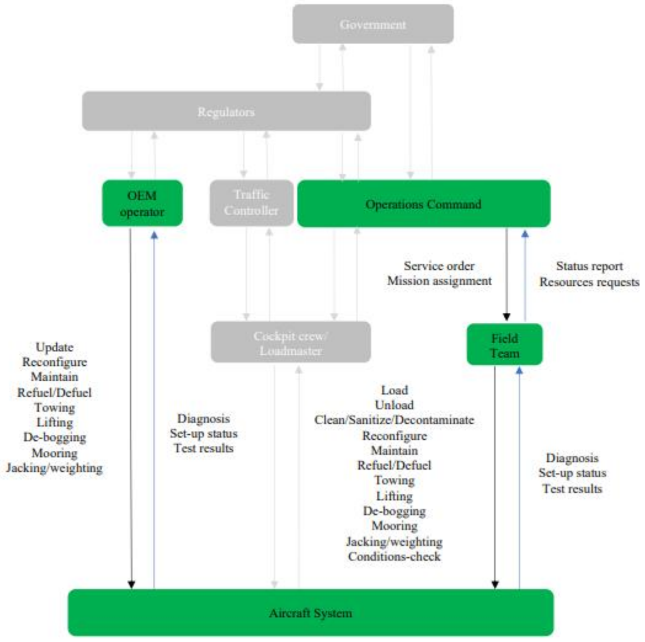


Figure 2 – Control Diagram evaluated

OEM operator responsibilities:

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

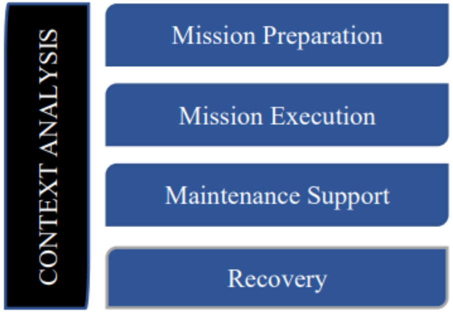
Field team responsibilities:

- 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



i. Control action provided;

ii. Control action not provided;

iii. Control action provided too late;

iv. Control action provided too early;

v. Control action provided out of order;

vi. Control action applied for too long;

vii. Control action stopped too soon.

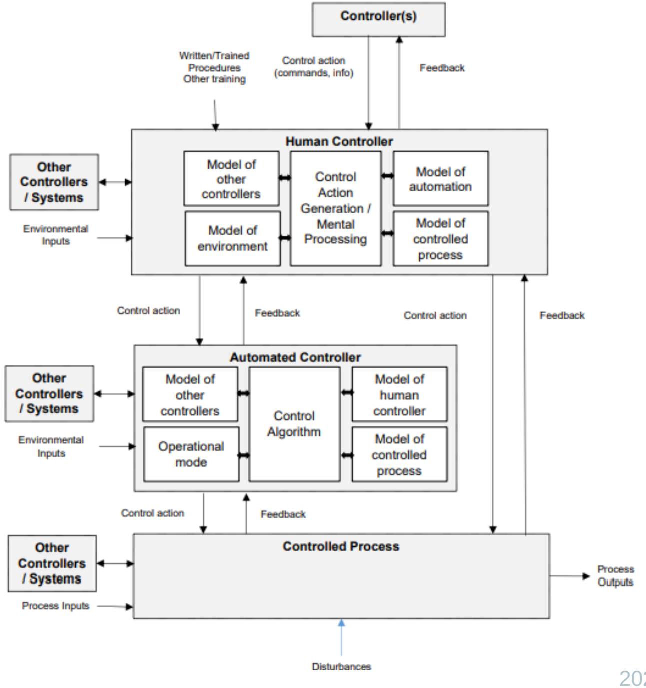
Examples (**Hazardous Control Actions**):

- 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 SoI. [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

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



Generic control loop as proposed in Leveson, N. (2020). An Improved Design Process for Complex, Control-Based Systems Using STPA and a Conceptual Architecture.

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

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

- ISO/IEC/IEEE 15288. (2015). Systems and Software Engineering – System Life Cycle Processes. Geneva, Switzerland: international Organization for Standardization.
- Blanchard, B. S., & Fabrycky, W. J. (2006). Systems engineering and analysis. Upper Saddle River, N.J: Pearson Prentice Hall. Chicago (Author-Date, 15th ed.).
- Department of Defense – Defense System Management College (1986). Integrated Logistics Support Guide. Fort Belvoir, Virginia. 1st ed.
- Leveson, N. G. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.
- Kohnfelder, Loren; Garg, Praerit (April 1, 1999). "The threats to our products". Microsoft Interface. Retrieved 18 August 2018.
- Leveson, N. (2020). An Improved Design Process for Complex, Control-Based Systems Using STPA and a Conceptual Architecture.