Strategizing STPA implementation in a military aircraft Design Organization



MIT STAMP WORKSHOP

Max Chopart

Safety & Reliability Group

2026

Company introduction



Proprietary Platforms

L-39NG & L-159 aircraft



Customer Services

Maintenance, Repairs, Overhaul, Modernizations

MRO / CAMO



Aerostructures

Industrial Cooperation Programs

CONFIDENTIAL INFORMATION: PROPERTY OF AERO VODOCHODY AEROSPACE A.S.

CONTEXT

STAMP at AERO



STAMP at AERO – Internal to RAMS team

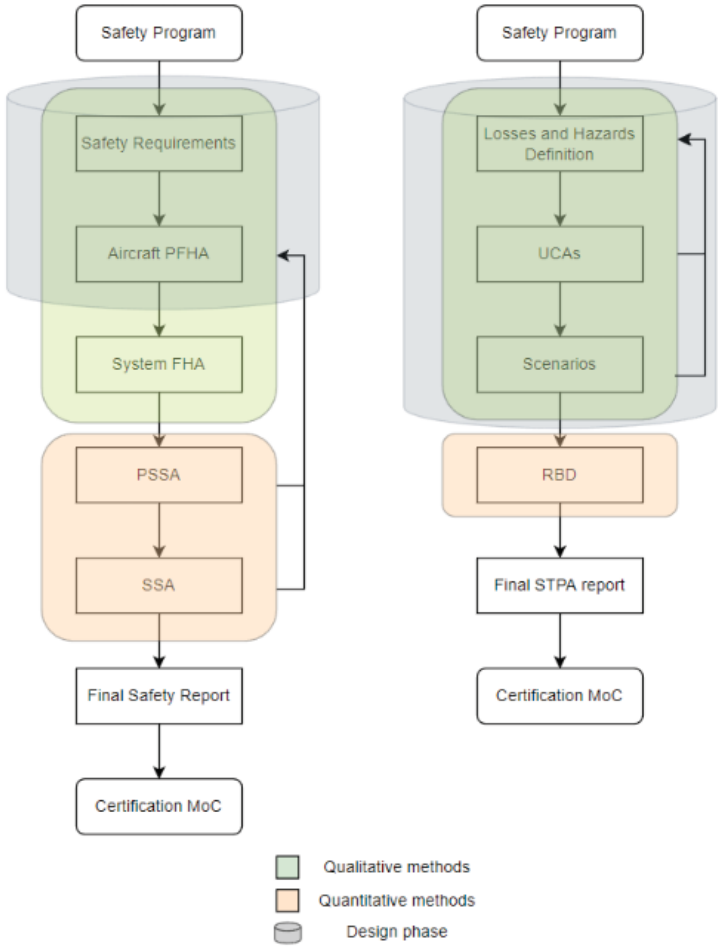
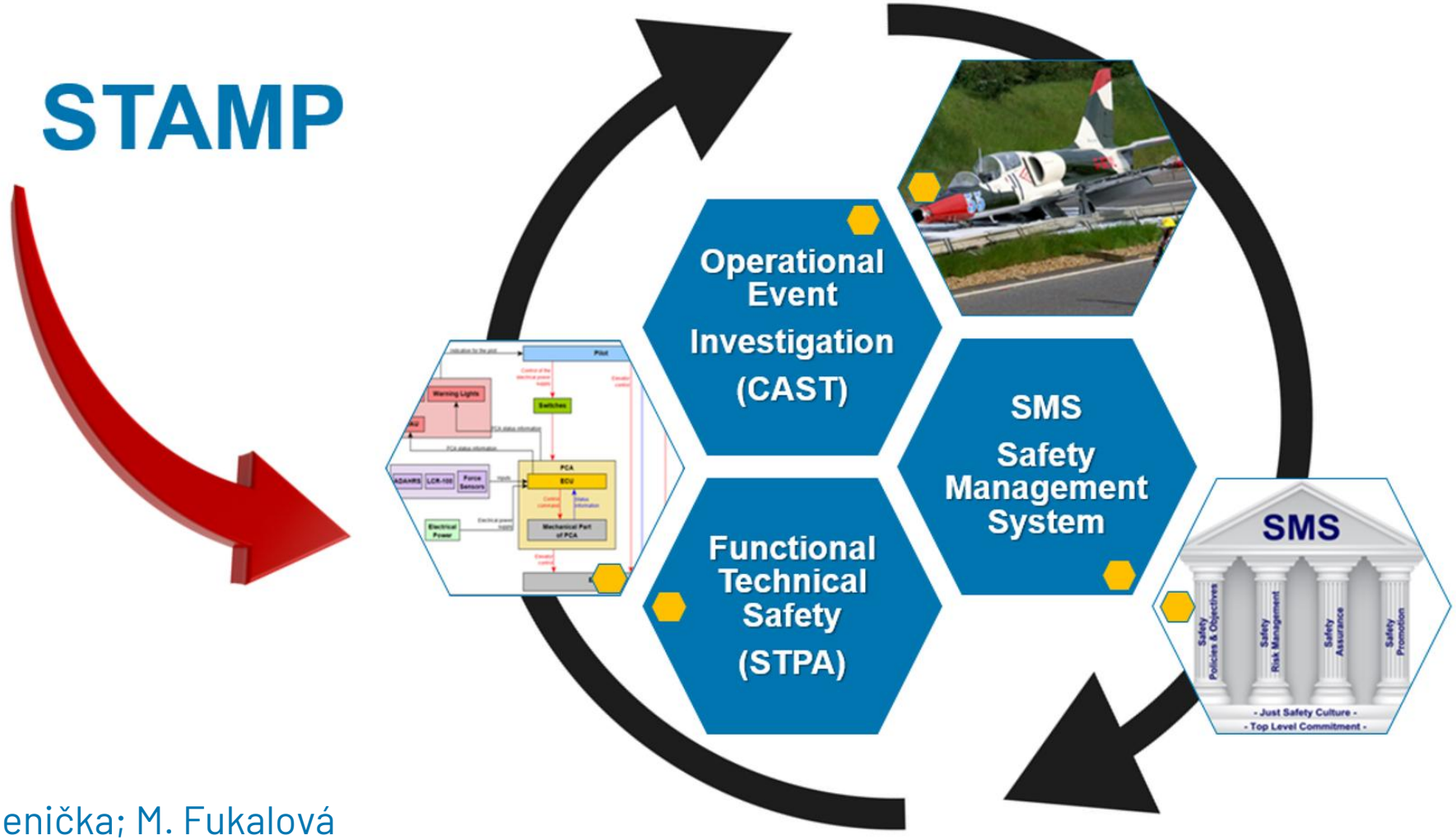


Figure 4: Schematic comparison of the whole Safety Assessment process by traditional and STPA methods

Source: M. Pšenička; M. Fukalová; A. Lališ – "Implementation of STPA Methodology Into Military Jet Aircraft Certification Process According to EMAR Certification Criteria for Safety" – ESREL 2023

STAMP at AERO – Internal to RAMS team



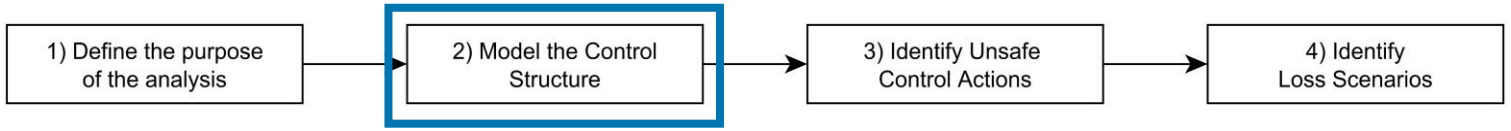
Source: M. Pšenička; M. Fukalová
"Application of STAMP in the Design Organization of Military Aircraft Manufacturer" – NTCA & ESWC 2026

CHALLENGE

Extending STPA beyond the RAMS team

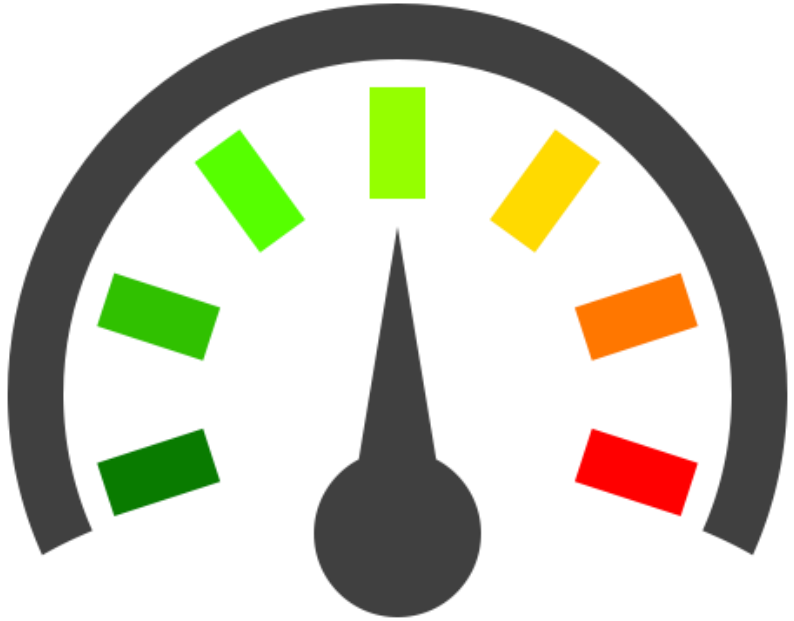


Extending STPA beyond the RAMS team



Environment context:

- Limited analysis resources.
- Document-centric requirements.
- **SMEs (avionics engineers) are unfamiliar with STPA and safety engineering.**

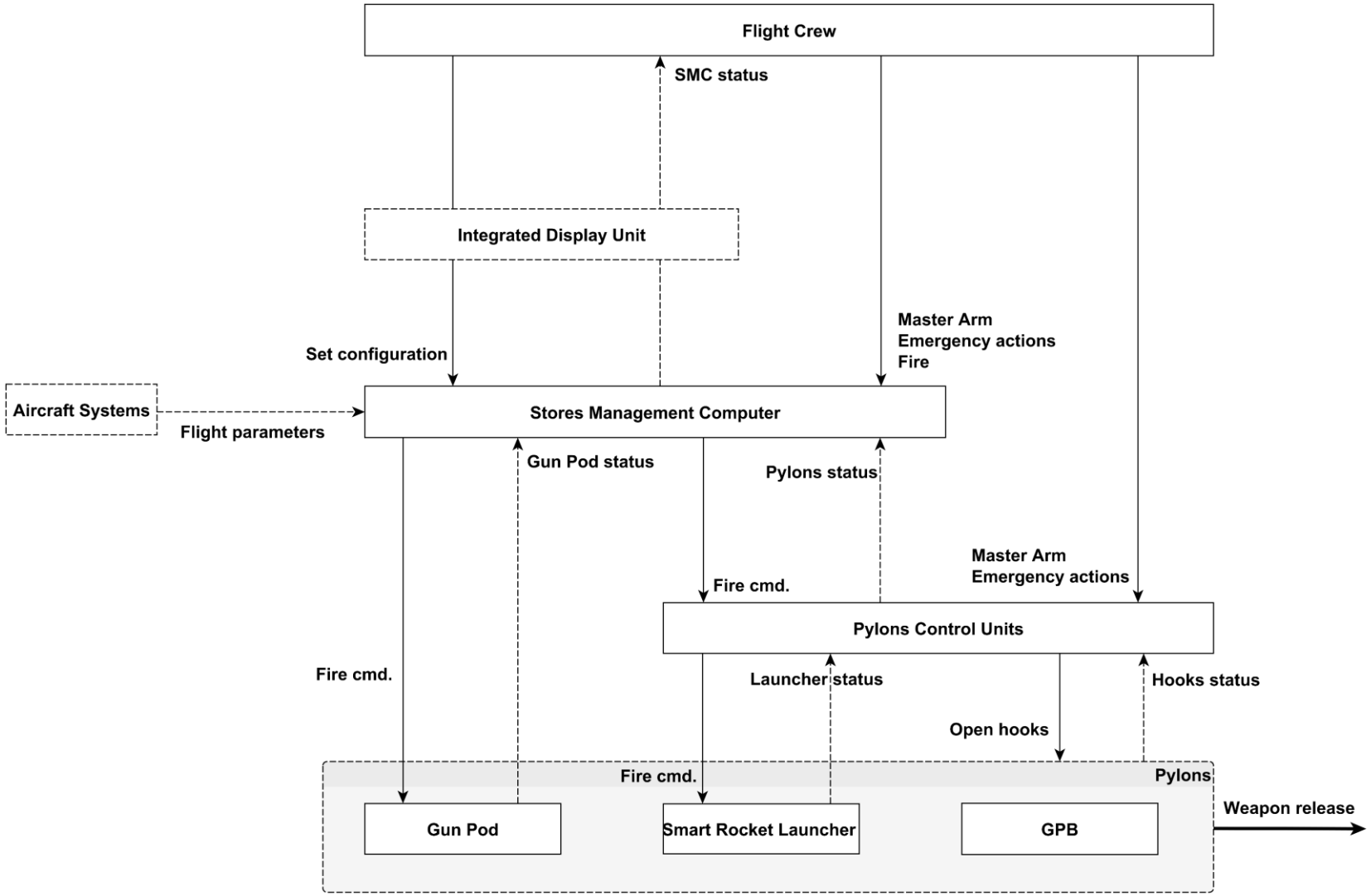


No relevant feedback

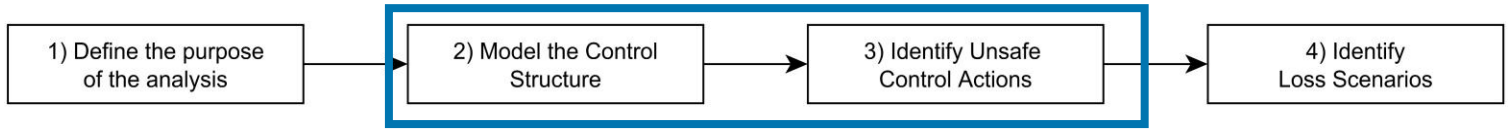
Overwhelming

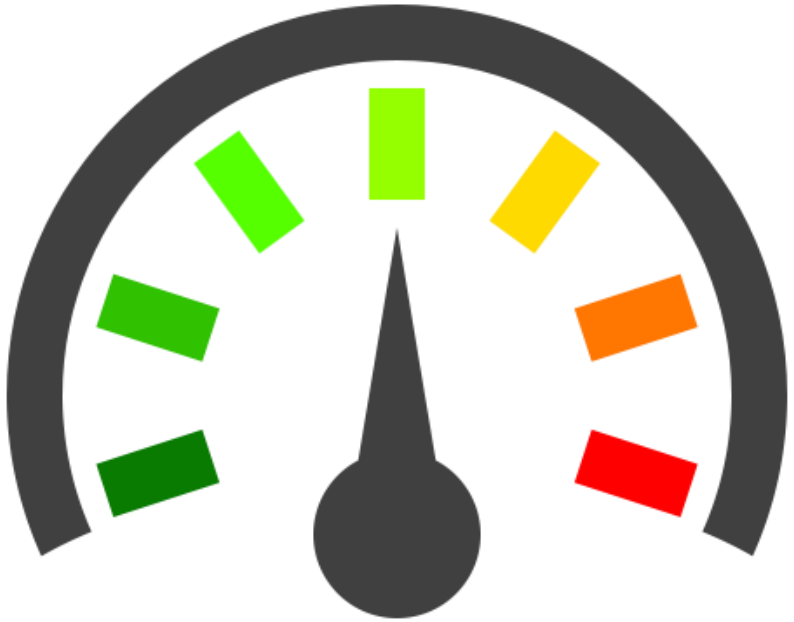
Use Case: Stores Management System

DISCLAIMER: Modified for public release



Extending STPA beyond the RAMS team – UCAs

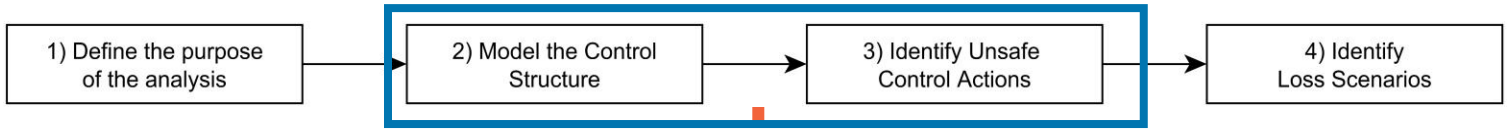




No relevant feedback

Overwhelming

Extending STPA beyond the RAMS team – UCAs

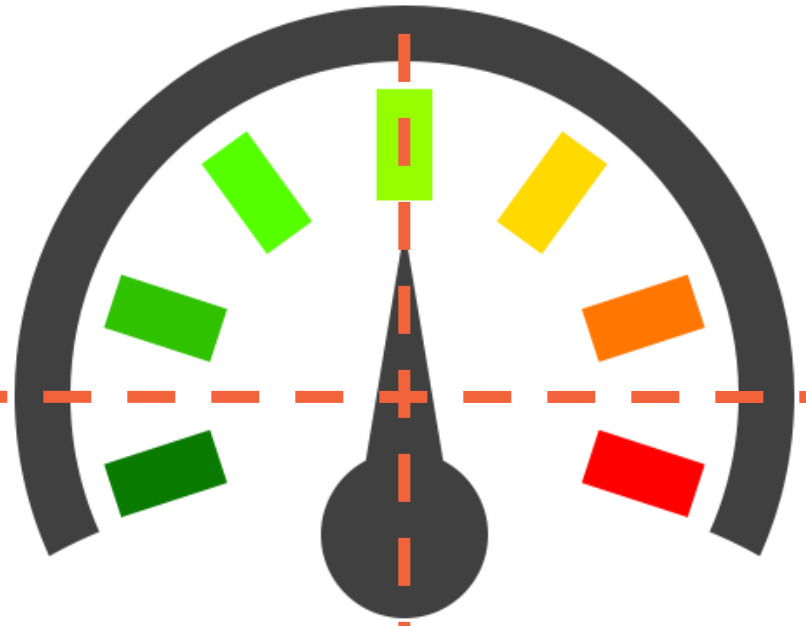


Review Controller Constraints using requirements-based format

181 UCAs identified

Ask the Avionics team to review a selected subset of UCAs

Develop the UCAs collaboratively with the Avionics team



No relevant feedback

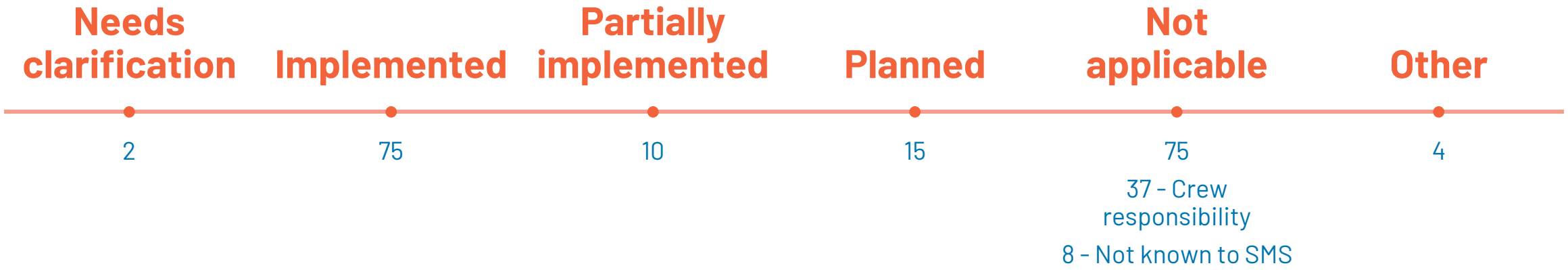
Overwhelming

STPA outputs as requirement review format

ID	Safety Requirement	UCA Ref.	Implementation status	Rationale
CC-X.Y	<Controller> shall (not) <Control Action> when <Context>	UCA-X.Y	• Implemented • Partially implemented • Not implemented • Planned • Not applicable • Needs clarification • Other	To be tested; Not known to SMS…

Results: Stores Management System

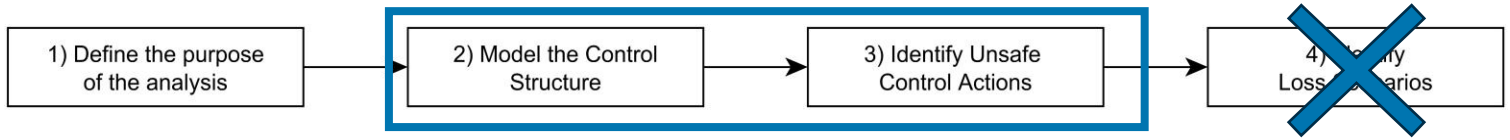
181 UCAs

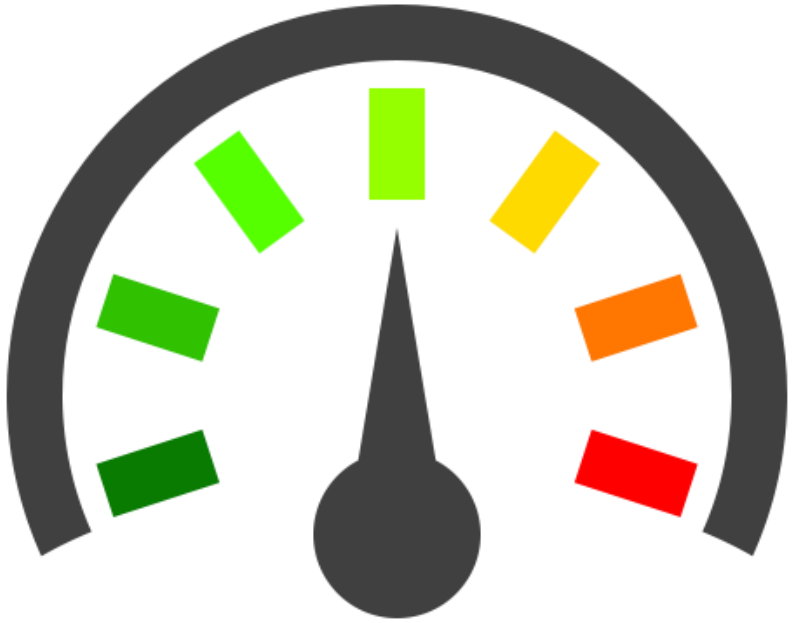


ID	Safety requirement	Status	Rationale
CC-3.1	Flight Crew shall jettison a store only after an already started firing sequence is ended or interrupted properly.	Planned	To be tested what it does in the SW
CC-6	Flight Crew shall not provide the Master Arm while a release sequence was already initiated.	Other	To be tested when Master Arm is switched OFF during sequence

Extending STPA beyond the RAMS team

> 700 high-level scenarios





No relevant feedback

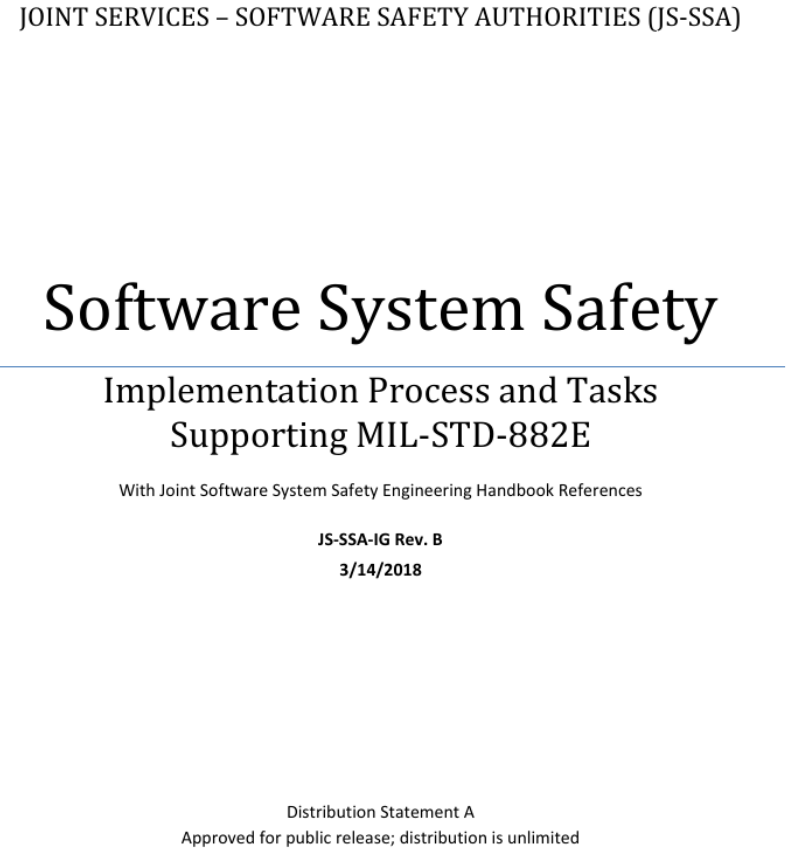
Overwhelming

Embedding and scaling STPA

STPA mapping to current safety activities



STPA mapping to current safety activities



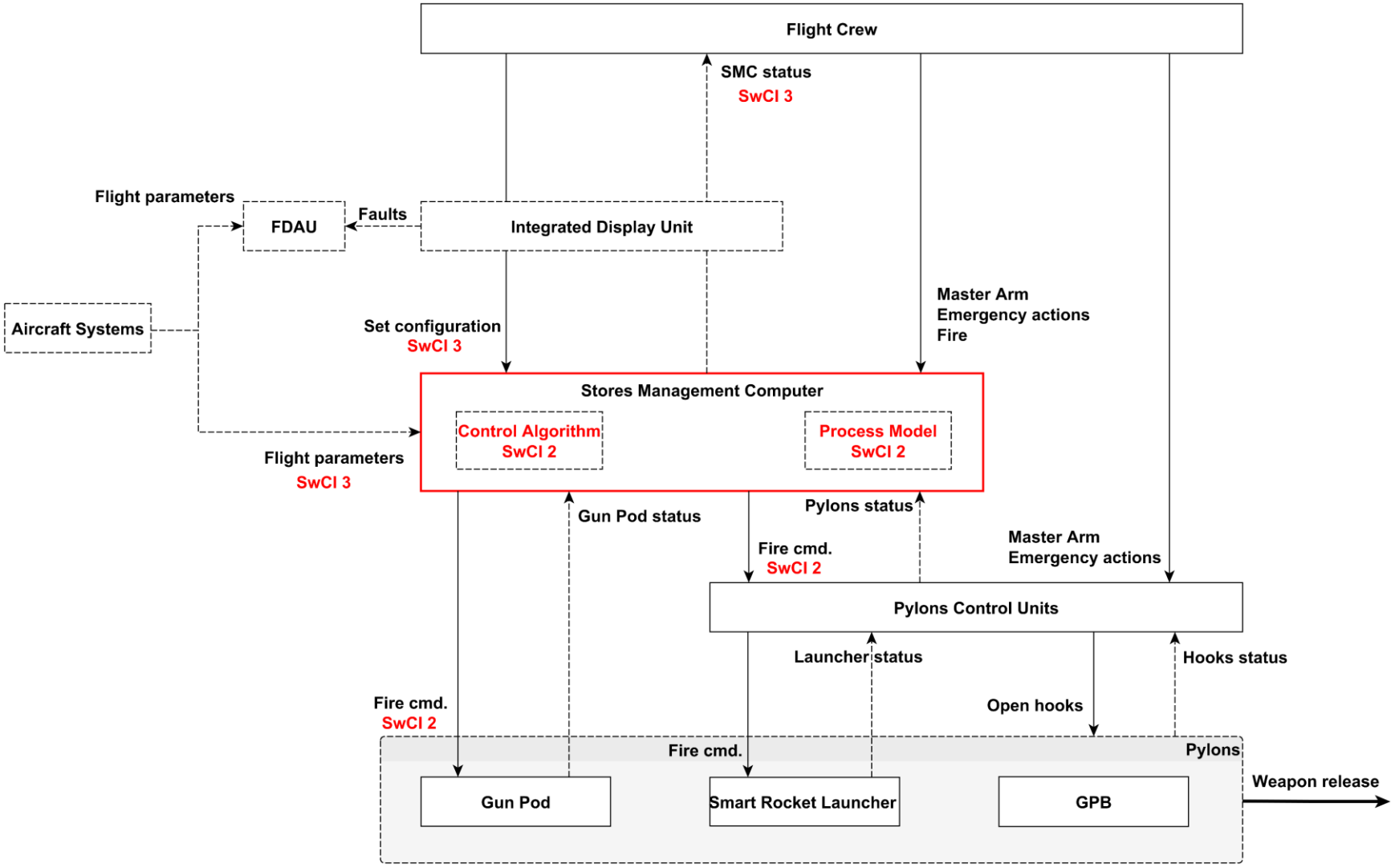
Appendix A: Preferred Level of Rigor Activities Table:

- 102 tasks - 40 tasks (out of scope for system/ software safety) = 62 tasks
- STPA can support about **30 (requirement-based)**

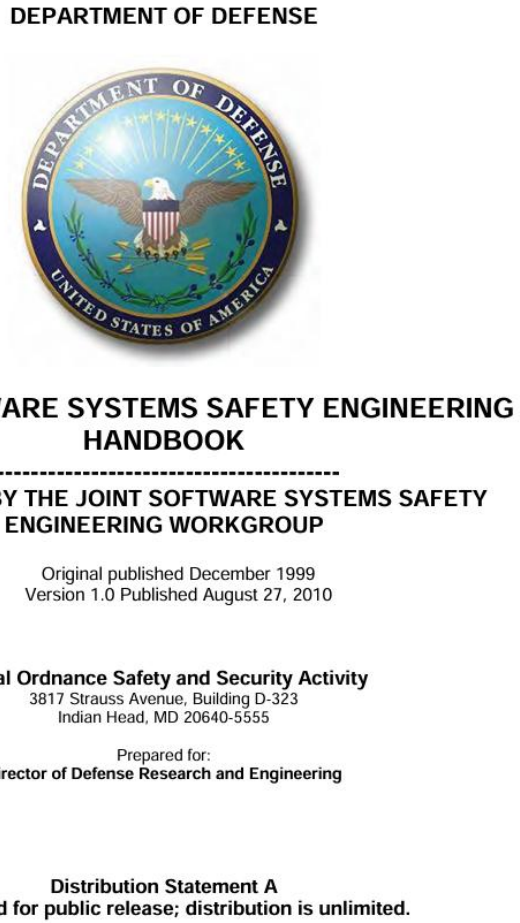
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

STPA mapping to current safety activities

DISCLAIMER: Modified for public release



STPA mapping to current safety activities



DEPARTMENT OF DEFENSE

JOINT SOFTWARE SYSTEMS SAFETY ENGINEERING HANDBOOK

DEVELOPED BY THE JOINT SOFTWARE SYSTEMS SAFETY ENGINEERING WORKGROUP

Original published December 1999
Version 1.0 Published August 27, 2010

Naval Ordnance Safety and Security Activity
3817 Strauss Avenue, Building D-323
Indian Head, MD 20640-5555

Prepared for:
Director of Defense Research and Engineering

Distribution Statement A
Approved for public release; distribution is unlimited.

"Software does not wear out, break, or have increasing tolerances that result in failures. Software errors are generally **errors in the requirements**."

"Once all known functionality of the system is identified and documented, each function must be assessed against the **following scenarios**:

- The function is unavailable (**does not occur when expected to occur**).
- The function malfunctions (degraded, partial, or **unexpected results of the function**).
- The function performs its intended activity but is **out of sequence**.
- The function performs its intended activity, but at the **incorrect time (too early, too late, outside defined window)**."

STPA mapping to current safety activities

DEPARTMENT OF DEFENSE

JOINT SOFTWARE SYSTEMS SAFETY ENGINEERING HANDBOOK

DEVELOPED BY THE JOINT SOFTWARE SYSTEMS SAFETY ENGINEERING WORKGROUP

Original published December 1999
Version 1.0 Published August 27, 2010

Naval Ordnance Safety and Security Activity
3817 Strauss Avenue, Building D-323
Indian Head, MD 20640-5555

Prepared for:
Director of Defense Research and Engineering

Distribution Statement A
Approved for public release; distribution is unlimited.

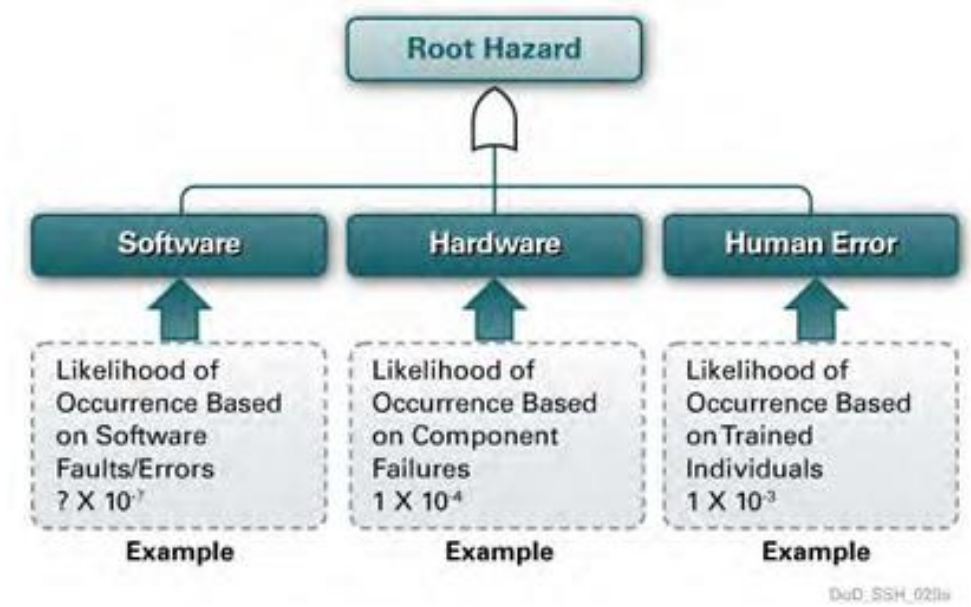


Figure 4-17: Likelihood of Occurrence Example

STPA mapping to current safety activities

NOT MEASUREMENT SENSITIVE

National Aeronautics and Space Administration

NASA-GB-8719.13
March 31, 2004

NASA Software Safety Guidebook

Chapter 6 Software Requirements



The cost of correcting software faults and errors escalates dramatically as the development life cycle progresses, making it important to correct errors and implement correct software requirements from the very beginning. Unfortunately, it is generally impossible to eliminate all errors.

Software developers must therefore work toward two goals:

1. To develop complete and correct requirements and correct code.
2. To develop fault-tolerant designs, which will detect and compensate for software faults.

Note that (2) is required because (1) is usually impossible.

STPA mapping to current safety activities

DISCLAIMER: Modified for public release

Source component	Target component	Link type	Control action / feedback	**STPA-informed function**
SMC	Gun Pod	Control Action	- Fire cmd. - Master Arm - Power	**Fire gunpod**
Aircraft Systems	Stores Management Computer	Input	- Air speed - Altitude - AoA - ...	**Acquire flight data**

LESSONS LEARNT



Lessons learnt

System familiarization

- No prior knowledge of SMS
- Approx. 1 month

Review of Controller Constraints (181)

- 3 Avionics engineers
- Approx. 2 hours (some intensively discussed points)

STPA analysis (without scenarios)

- 1 analyst, experienced with STPA
- Approx. 1 month

Additional coordination

- Introductory meetings and iteration over Control Structure

Most of the effort remained with the STPA analyst

Lessons learnt

A basic control structure is sufficient to begin

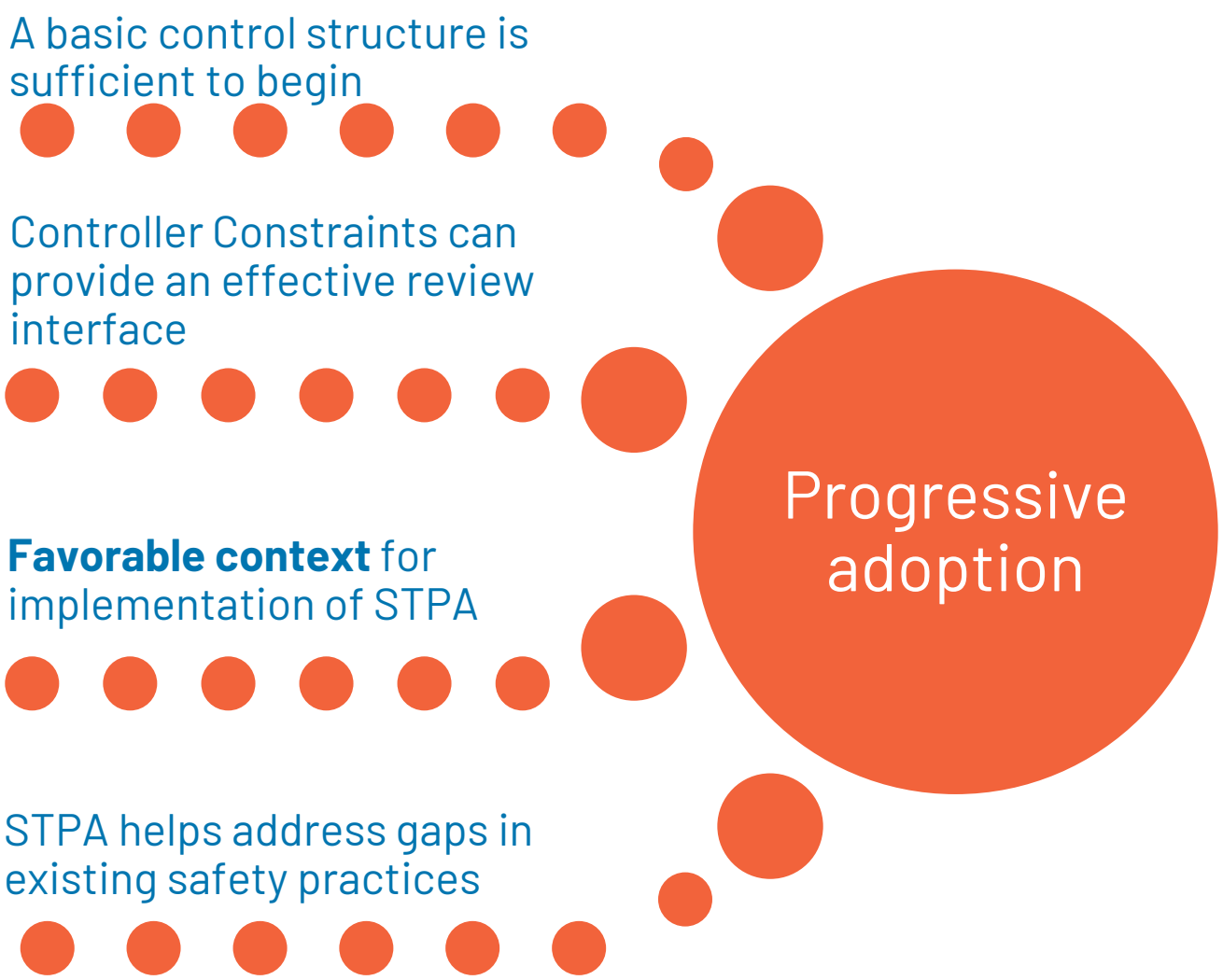
Controller Constraints can provide an effective review interface

Favorable context for implementation of STPA

STPA helps address gaps in existing safety practices



Lessons learnt



"It yields nicely packed set of questions to ask, […] some points sparked interesting debates.

This approach would be better introduced earlier in the development process.

The Flight Crew requirements and processes will be in my opinion very valuable for flight operations documentation phase later."

What's next

Integrate

- Formalize how STPA outputs enter existing processes.
- Continue development of high-level and refined scenarios.

Test

- New STPA study underway on a smaller system (23 UCAs).

Enhance

- Helps to address aspects of software safety that are not comprehensively covered by current practices.

Expand

- Evaluate STPA applications in organizational safety and Safety Management System processes.

CONFIDENTIAL INFORMATION: PROPERTY OF AERO VODOCHODY AEROSPACE A.S.

STPA adoption is an organizational problem, not a technical one



I would welcome your perspectives on:

- Alternative integration strategies
- Lessons learned from your own implementations
- Opportunities for improving the approach presented here

max.chopart@aero.cz

linkedin.com/in/max-chopart

CONFIDENTIAL INFORMATION: PROPERTY OF AERO VODOCHODY AEROSPACE A.S.