31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

Kimberly Lai

Thomas Robert, David Shindman, Dr. Alison Olechowski

Integrating Safety Analysis into Model-Based Systems Engineering for Aircraft Systems: A Literature Review and Methodology Proposal

Overview

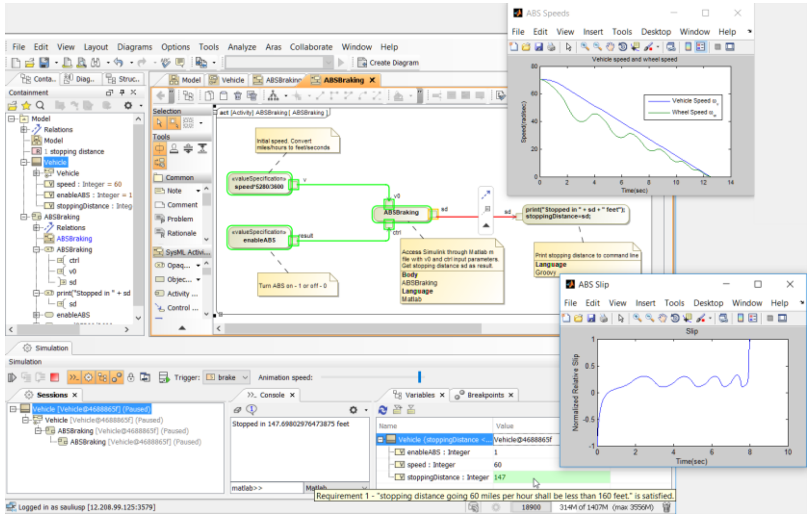
- Background
- Motivation
- Related Works
- Safety Profile
- Next steps

Innovation is Driving Change in SE Practices

Traditional approach:

Document-Based SE

Current/Future approach:



Initial speed. Convert miles/hours to feet/seconds

«valueSpecification» speed*5280/3600

«valueSpecification» enableABS

Turn ABS on - 1 or off - 0

Access Simulink through Matlab m file with v0 and ctrl input parameters. Get stopping distance sd as result.
Body
ABSBraking
Language
Matlab

print("Stopped in " + sd + " feet");
stoppingDistance=sd;

Print stopping distance to command line
Language
Groovy

Trigger: brake

```
Vehicle [Vehicle@4688865f] (Paused)
  Vehicle [Vehicle@4688865f] (Paused)
    ABSBraking [Vehicle@4688865f] (Paused)
      ABSBraking [Vehicle@4688865f] (Paused)
```

```
Stopped in 147.69802976473875 feet
matlab>>
```

Name	Value
Vehicle (stoppingDistance <...	Vehicle@4688865f
enableABS : Integer	1
speed : Integer	60
stoppingDistance : Integer	147

Requirement 1 - "stopping distance going 60 miles per hour shall be less than 160 feet." is satisfied.

Logged in as sauliusp [12.208.99.125:3579]

18900 314M of 1407M (max 3556M)

Model-Based SE (MBSE)

Innovation is Driving Change in SE Practices

Traditional approach:

Current/Future approach:

“Formalized **application of modelling** to support system **requirements, design, analysis, verification and validation** activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases”

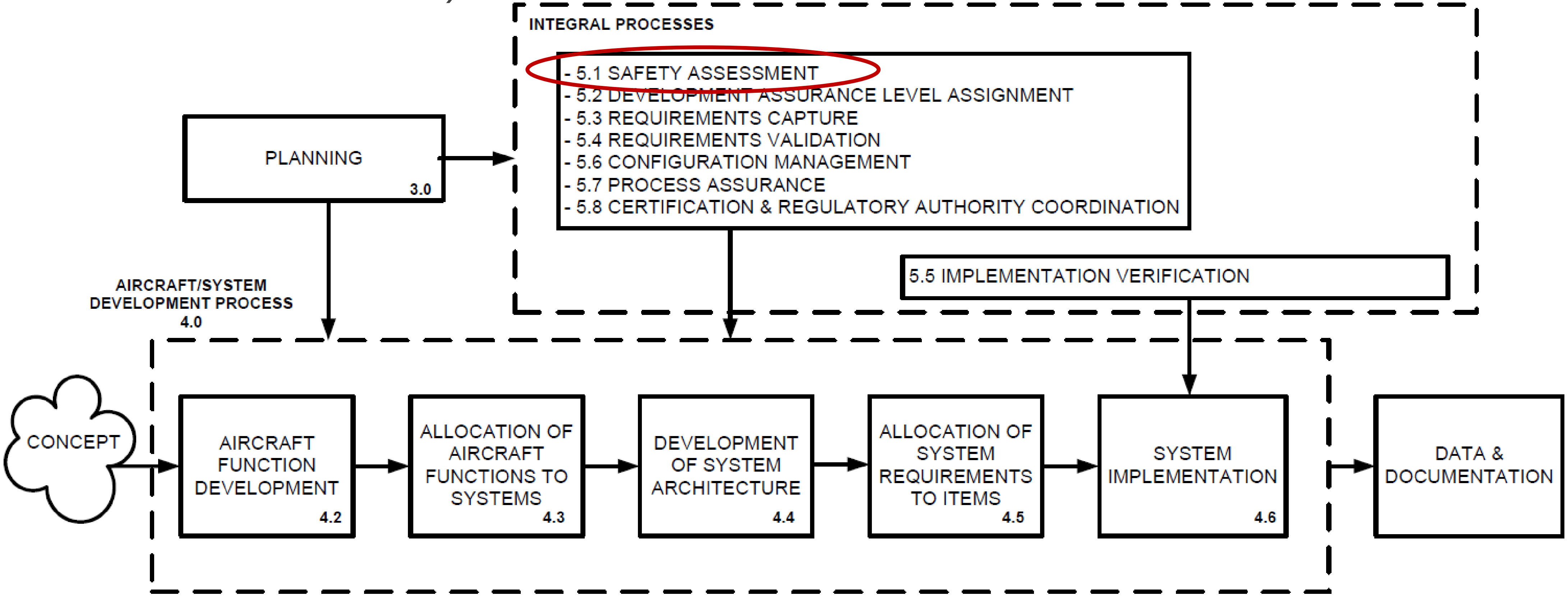
- International Council on Systems Engineering (INCOSE) -

Document-Based SE

Model-Based SE (MBSE)

Safety Analysis (SA) is Essential for Aircraft Systems

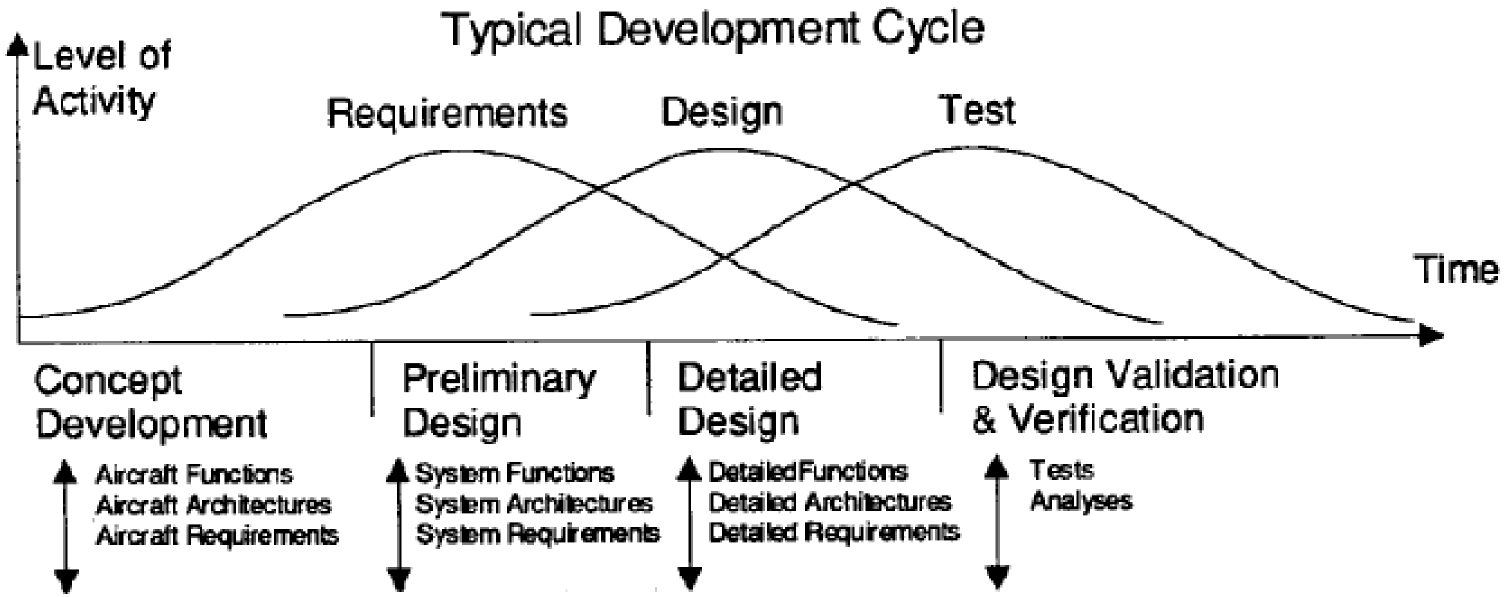
Aircraft & System Development Process Model:
(taken from SAE ARP4754A)


INTEGRAL PROCESSES
- 5.1 SAFETY ASSESSMENT
- 5.2 DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT
- 5.3 REQUIREMENTS CAPTURE
- 5.4 REQUIREMENTS VALIDATION
- 5.6 CONFIGURATION MANAGEMENT
- 5.7 PROCESS ASSURANCE
- 5.8 CERTIFICATION & REGULATORY AUTHORITY COORDINATION
5.5 IMPLEMENTATION VERIFICATION
PLANNING
3.0
AIRCRAFT/SYSTEM DEVELOPMENT PROCESS
4.0
CONCEPT
AIRCRAFT FUNCTION DEVELOPMENT
4.2
ALLOCATION OF AIRCRAFT FUNCTIONS TO SYSTEMS
4.3
DEVELOPMENT OF SYSTEM ARCHITECTURE
4.4
ALLOCATION OF SYSTEM REQUIREMENTS TO ITEMS
4.5
SYSTEM IMPLEMENTATION
4.6
DATA & DOCUMENTATION

Guidelines for Development of Civil Aircraft Systems, “SAE ARP4754A,” Society of Automotive Engineers SAE International Standard, 2010.

Safety Analysis (SA) is Essential for Aircraft Systems

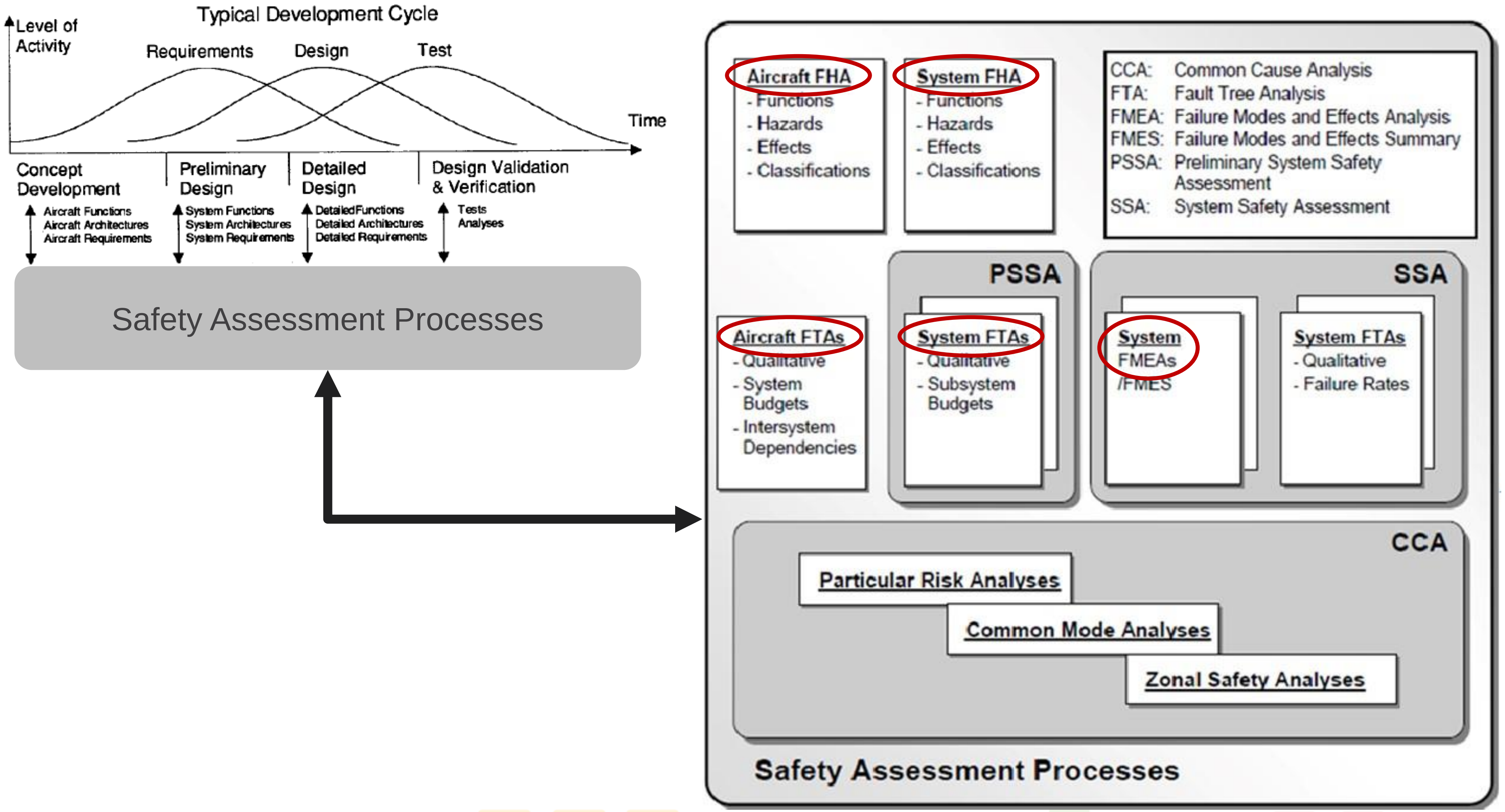
Typical Development Cycle: (taken from SAE ARP4761)



Safety Assessment Processes

Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airbone Systems and Equipment, “SAE ARP4761,” Society of Automotive Engineers SAE International Standard, 1996.

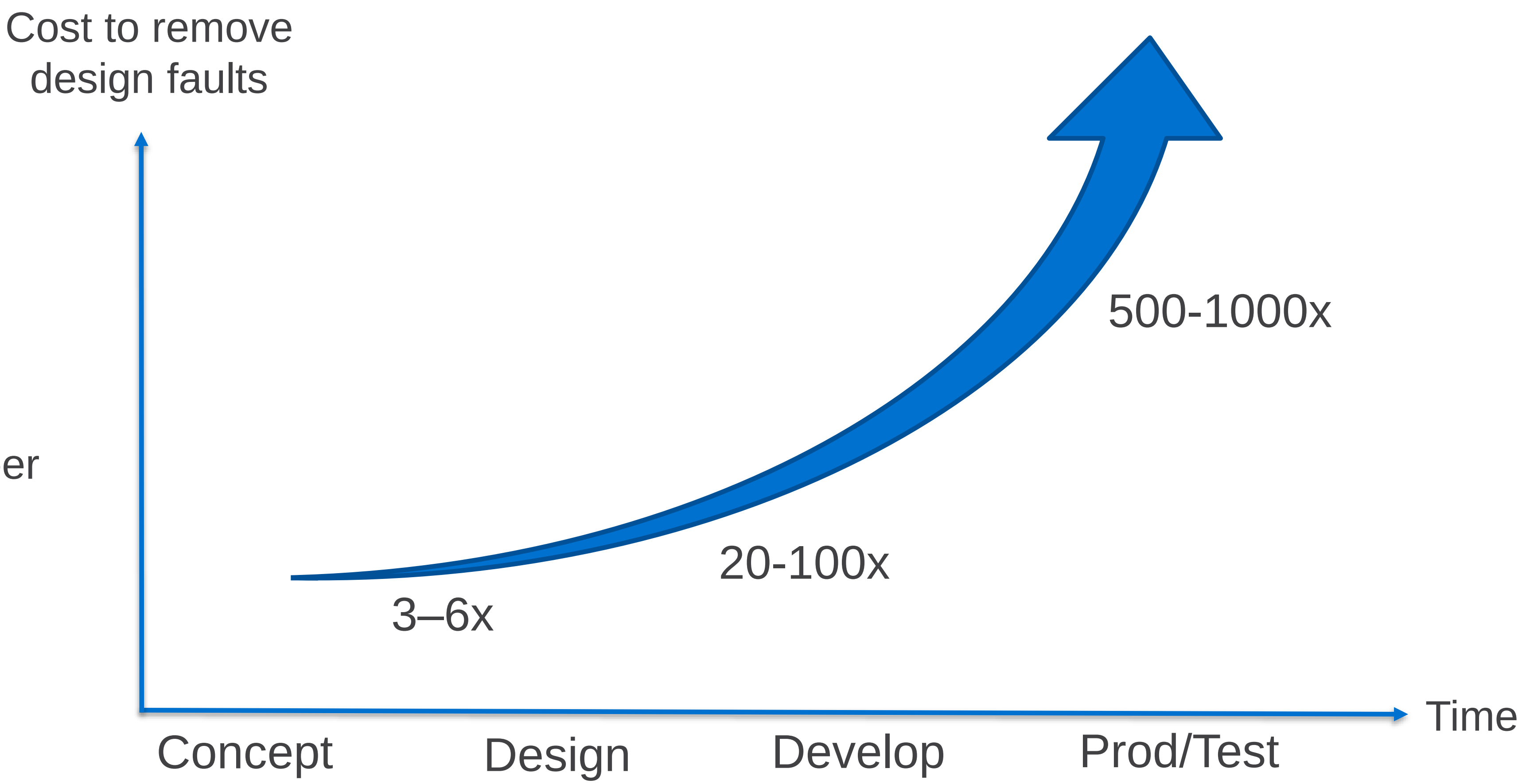
Safety Analysis (SA) is Essential for Aircraft Systems



Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airbone Systems and Equipment, “SAE ARP4761,” Society of Automotive Engineers SAE International Standard, 1996.

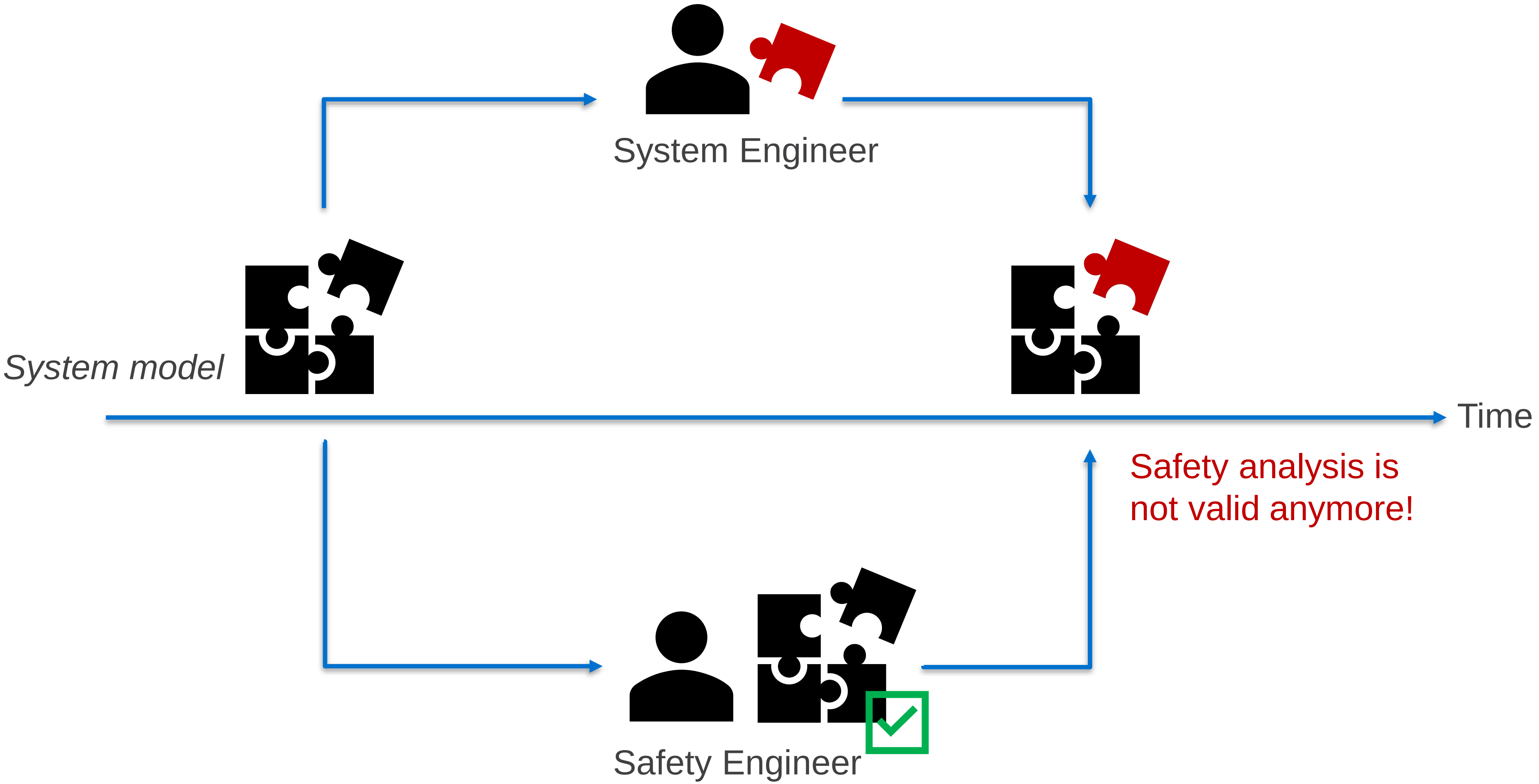
Safety Analysis is Performed Independently, Missed Opportunities are Costly

System Engineer ≠ Safety Engineer



International Council on Systems Engineering (INCOSE), “Systems Engineering Handbook, Version 3,” 2006.

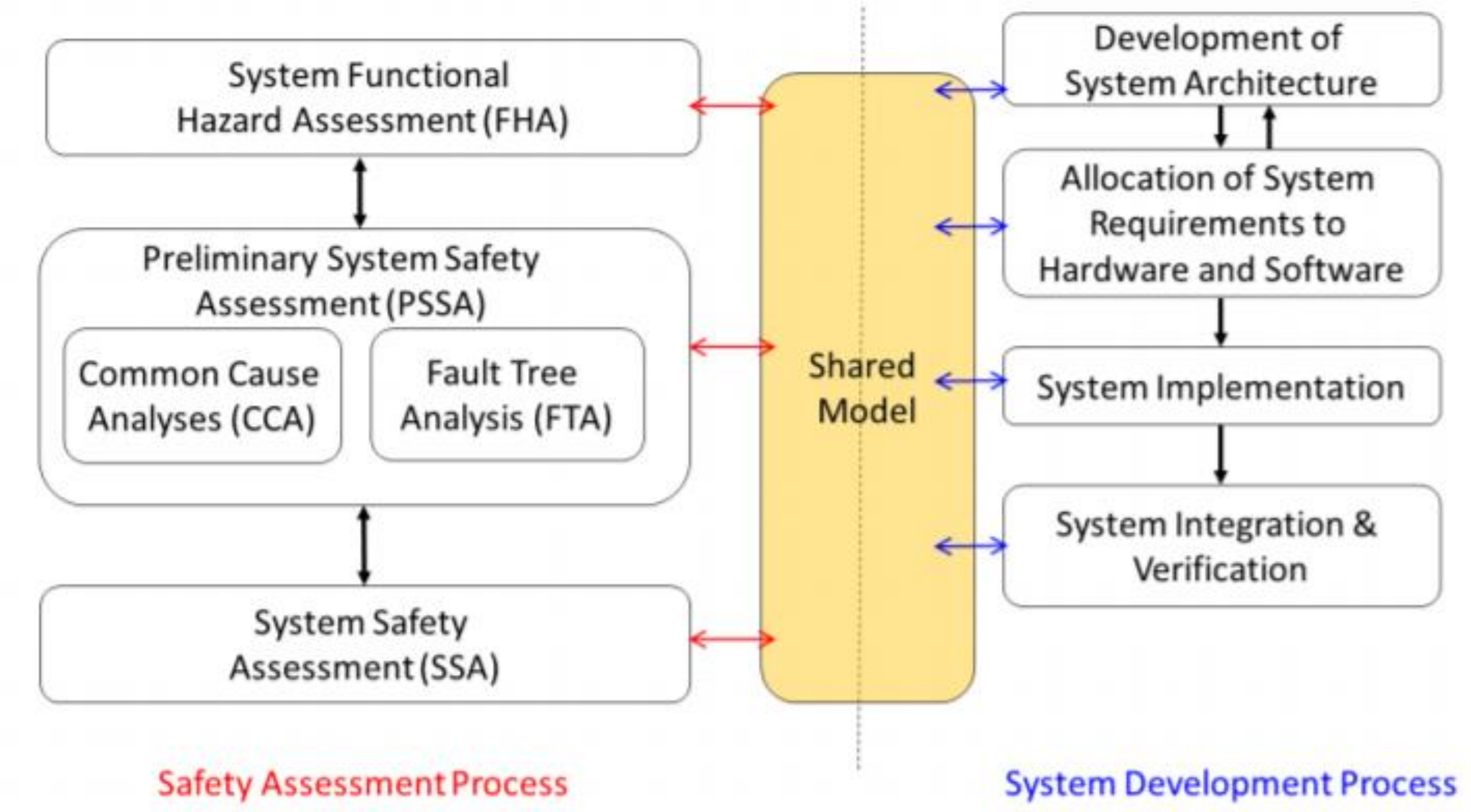
Traditional SA Practices Cannot Keep Up



Safety analysis is not valid anymore!

Integration of SA into MBSE → MBSA

The concept of Model-Based Safety Analysis:


System Functional Hazard Assessment (FHA)
Preliminary System Safety Assessment (PSSA)
Common Cause Analyses (CCA)
Fault Tree Analysis (FTA)
System Safety Assessment (SSA)
Shared Model
Development of System Architecture
Allocation of System Requirements to Hardware and Software
System Implementation
System Integration & Verification
Safety Assessment Process
System Development Process

- ✓ Automation
- ✓ Traceability
- ✓ Decrease development time
- ✓ Increase efficiency

D. Stewart, J. Liu, D. Cofer, M. Heimdahl, M. W. Whalen, and M. Peterson, “Architectural Modeling and Analysis for Safety Engineering (AMASE) Final Report, 2019.

Existing Methodologies

Model-to-model transformation

- Transformation via an external tool
- Safety model uses a different modelling language (e.g. AltaRica)

✓ Simpler to implement

Extension of modelling language

- System modelling language (e.g. SysML) is modified
- Preliminary safety model can be derived directly from the system development model

✓ Use of a single tool

Related Works

	SMF-FTA Yakmets, Jaber & Lanusse (2013)	**MéDISIS** David, Idasiak & Kratz (2010)	**Helle's method** Helle (2012)	**SafeSysE** Mhenni, Nguyen & Choley (2018)
Requirements capture	✗	✓	✓	✗
Identifying failure probability of designs	✗	✓	✓	✗
FHA generation	✗	✗	✗	✗
FMEA generation	✗	✓	✗	✓
FTA generation	✓	✗	✗	✓
Flexibility with other modelling tools	✓	✓	✗	✓
Propagation of manual edits into the model	✗	✓	✗	✓

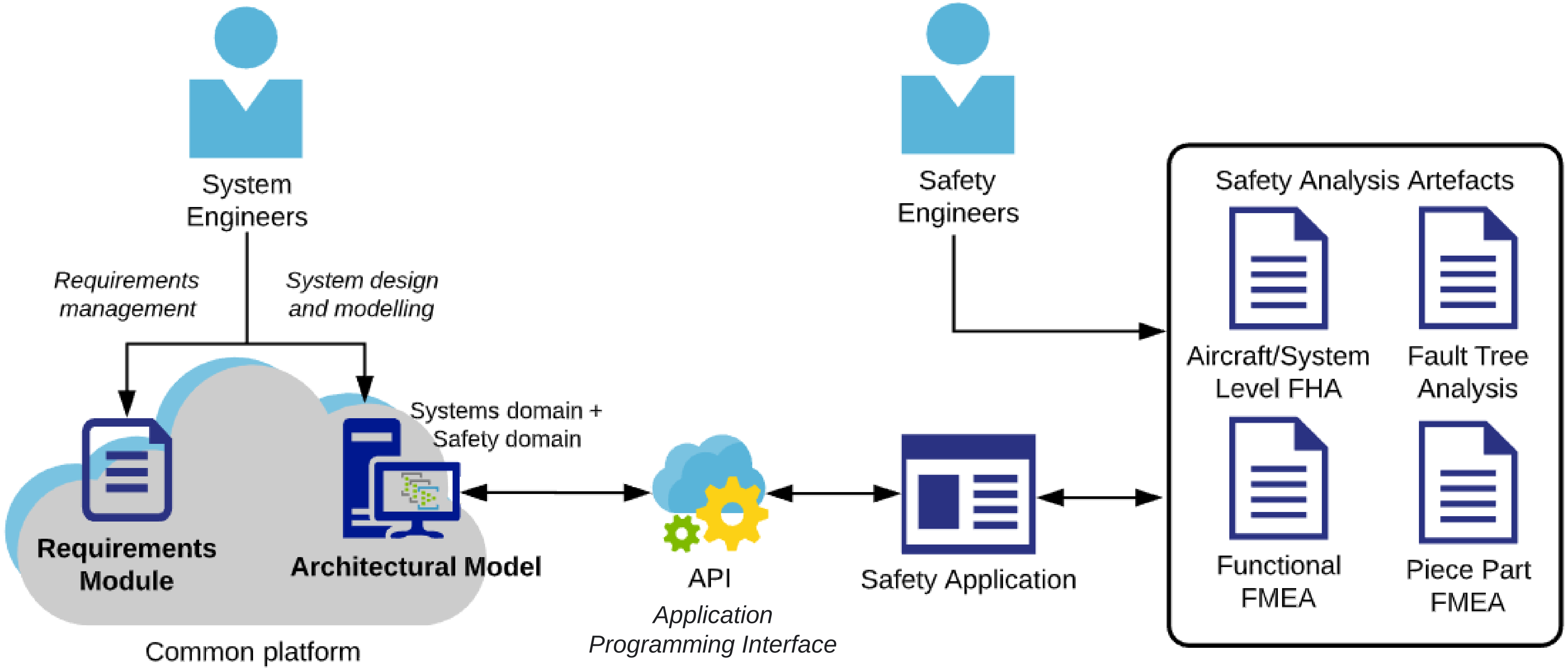
Objectives of Proposed Methodology

1 Automatic generation of FHA, FMEA and FTA

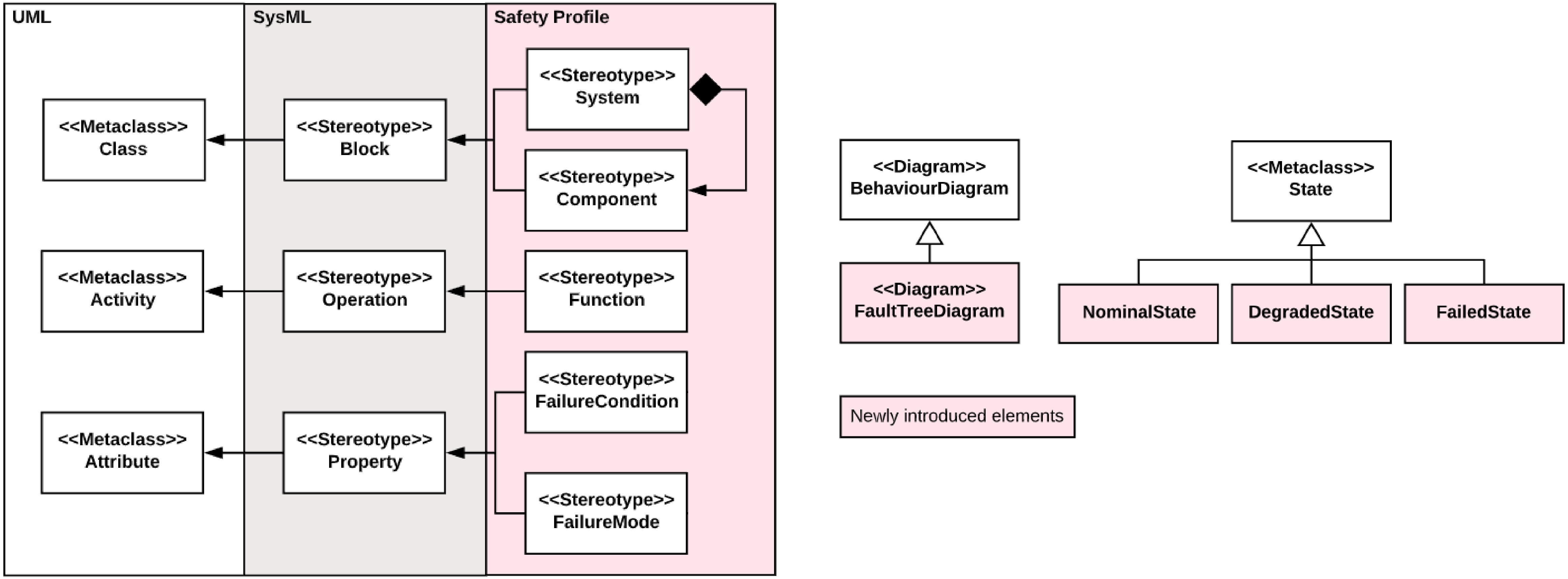
2 Propagation of manual edits in the generated SA artefacts back into the shared model

3 Traceability of safety model elements to requirements

Safety Profile: Overall Process



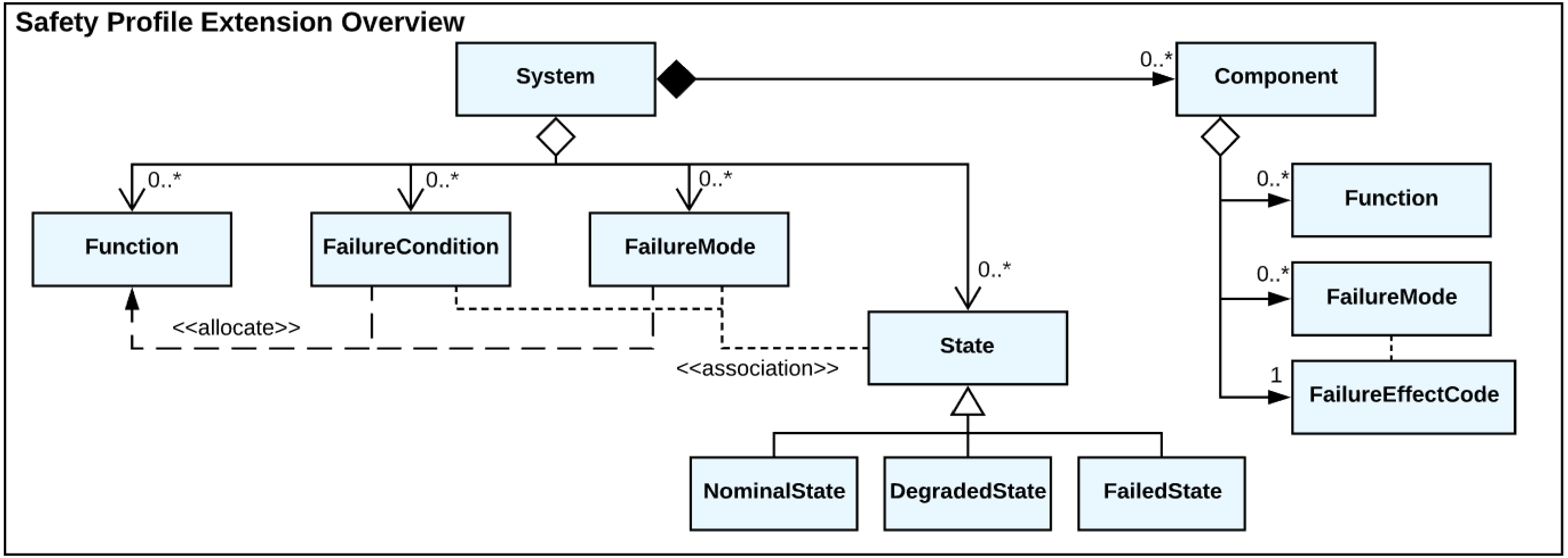
Safety Profile: Meta-class Extension



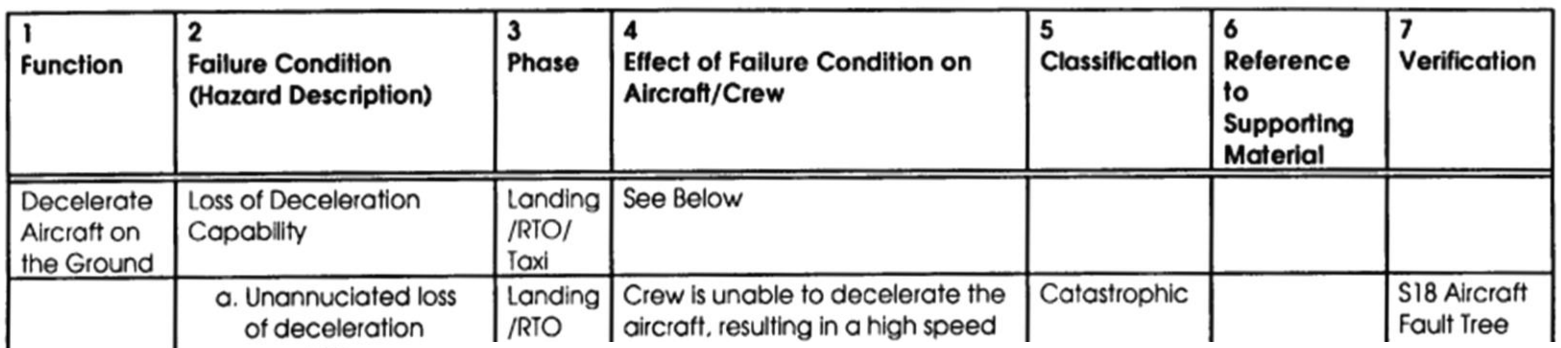
Newly introduced elements

Safety Profile: Overview

- Capture safety data
- Automatic generation of FHA, FMEA & FTA
- Safety certification still carried out independently

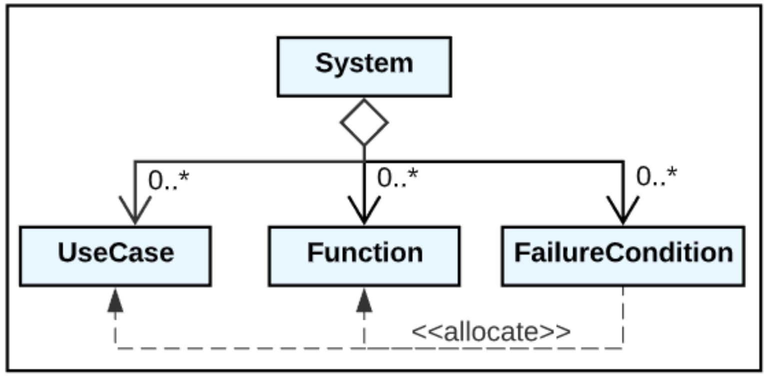


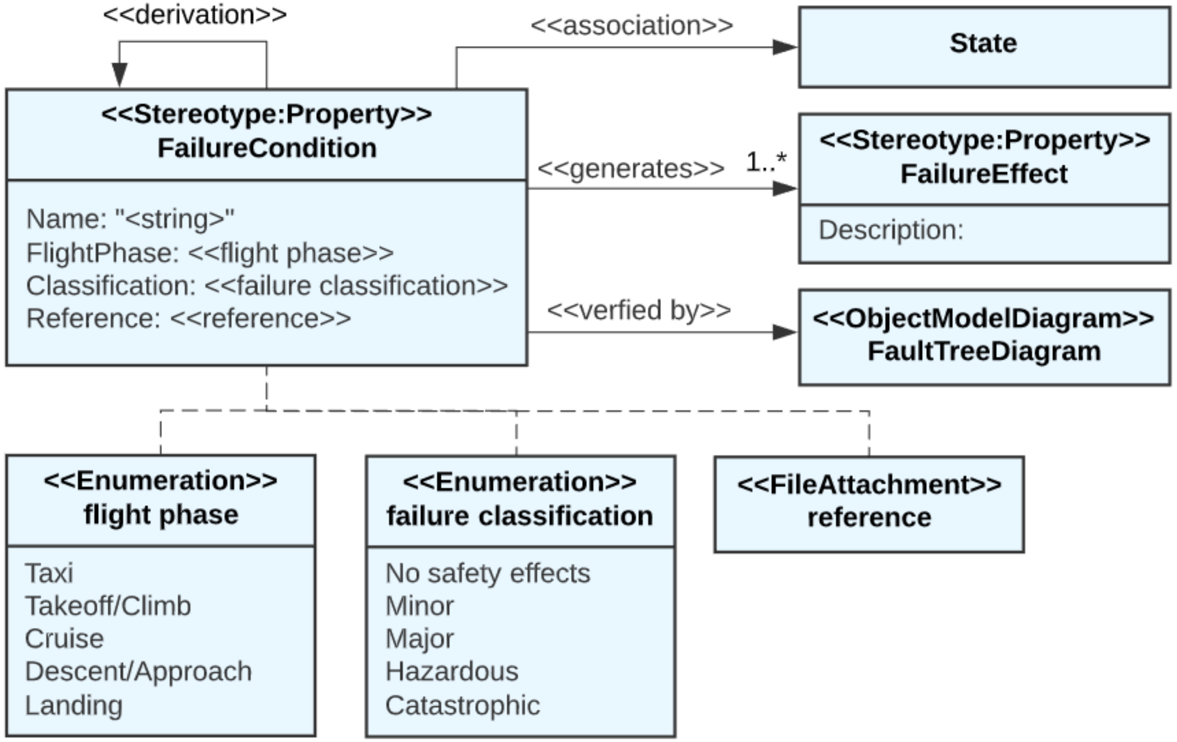
Safety Profile: FHA Generation



1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
Decelerate Aircraft on the Ground	Loss of Deceleration Capability	Landing /RTO/ Taxi	See Below			
	a. Unannunciated loss of deceleration capability	Landing /RTO	Crew is unable to decelerate the aircraft, resulting in a high speed	Catastrophic		S18 Aircraft Fault Tree
	b. Annunciated lo					

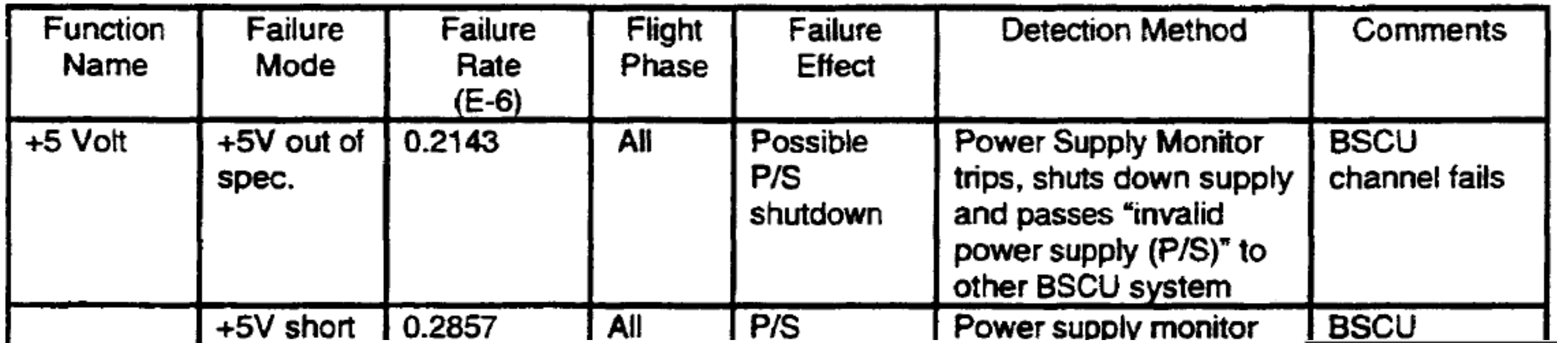
Typical FHA table (taken from ARP4761)





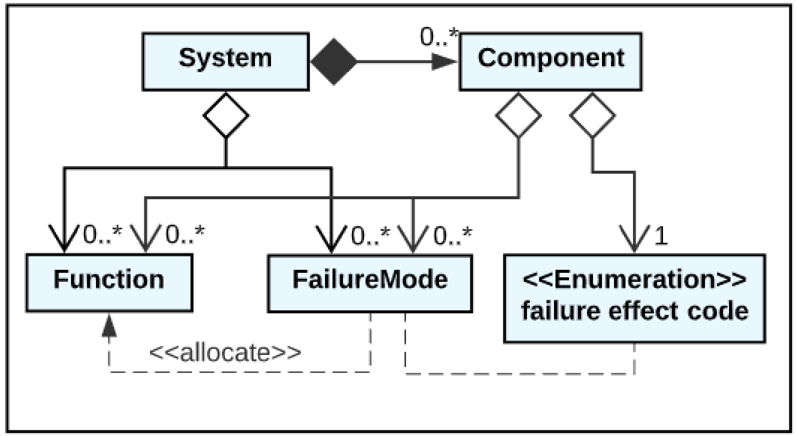
Metamodel for FHA generation

Safety Profile: FMEA Generation

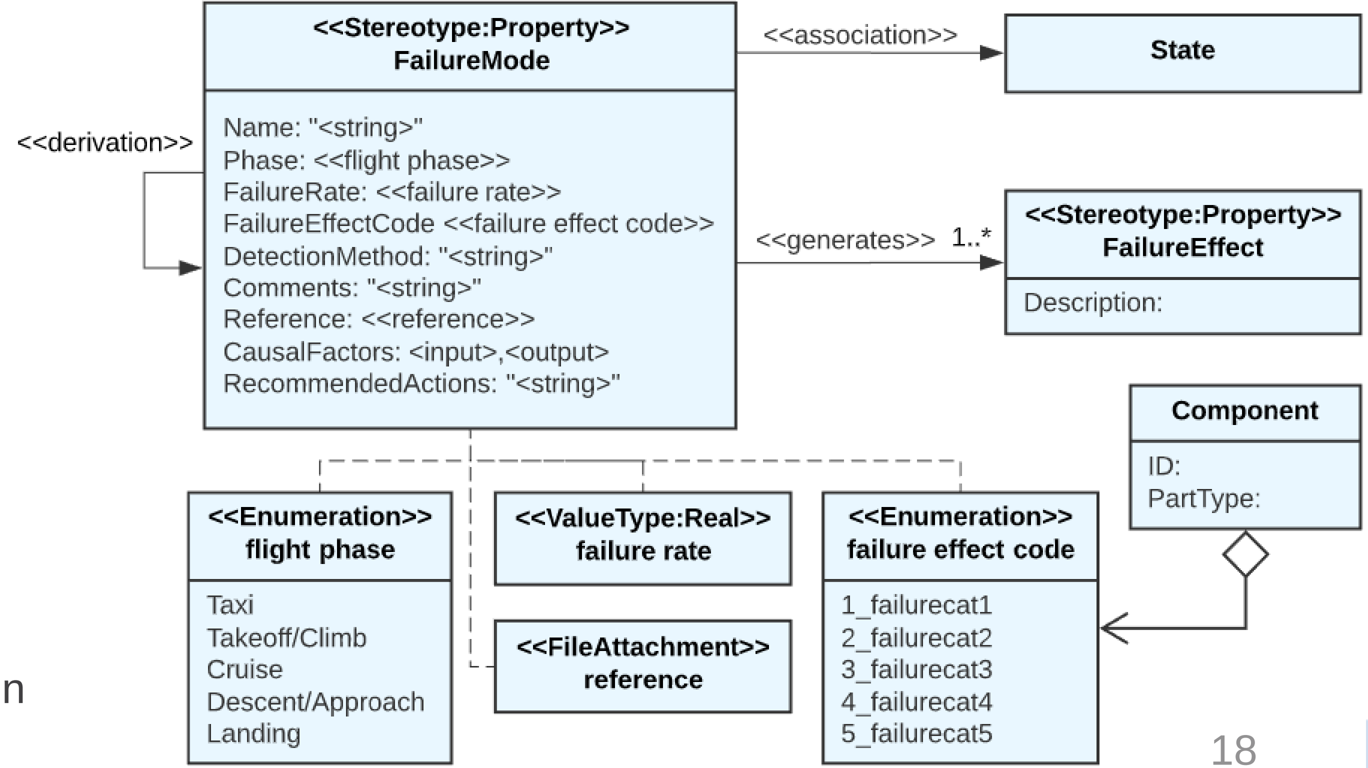


Function Name	Failure Mode	Failure Rate (E-6)	Flight Phase	Failure Effect	Detection Method	Comments
+5 Volt	+5V out of spec.	0.2143	All	Possible P/S shutdown	Power Supply Monitor trips, shuts down supply and passes "invalid power supply (P/S)" to other BSCU system	BSCU channel fails
	+5V short to gro	0.2857	All	P/S	Power supply monitor	BSCU
	Loss reduc filterir					

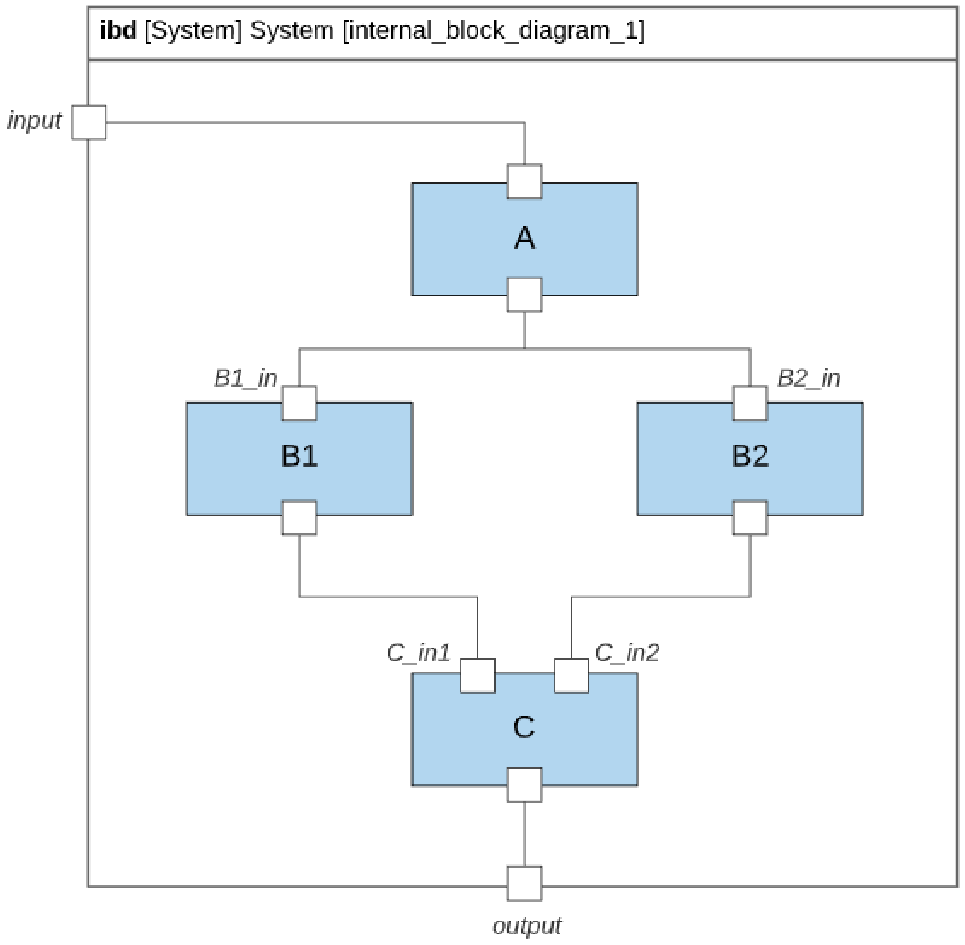
Typical Functional FMEA table (taken from ARP4761)



Metamodel for FMEA generation



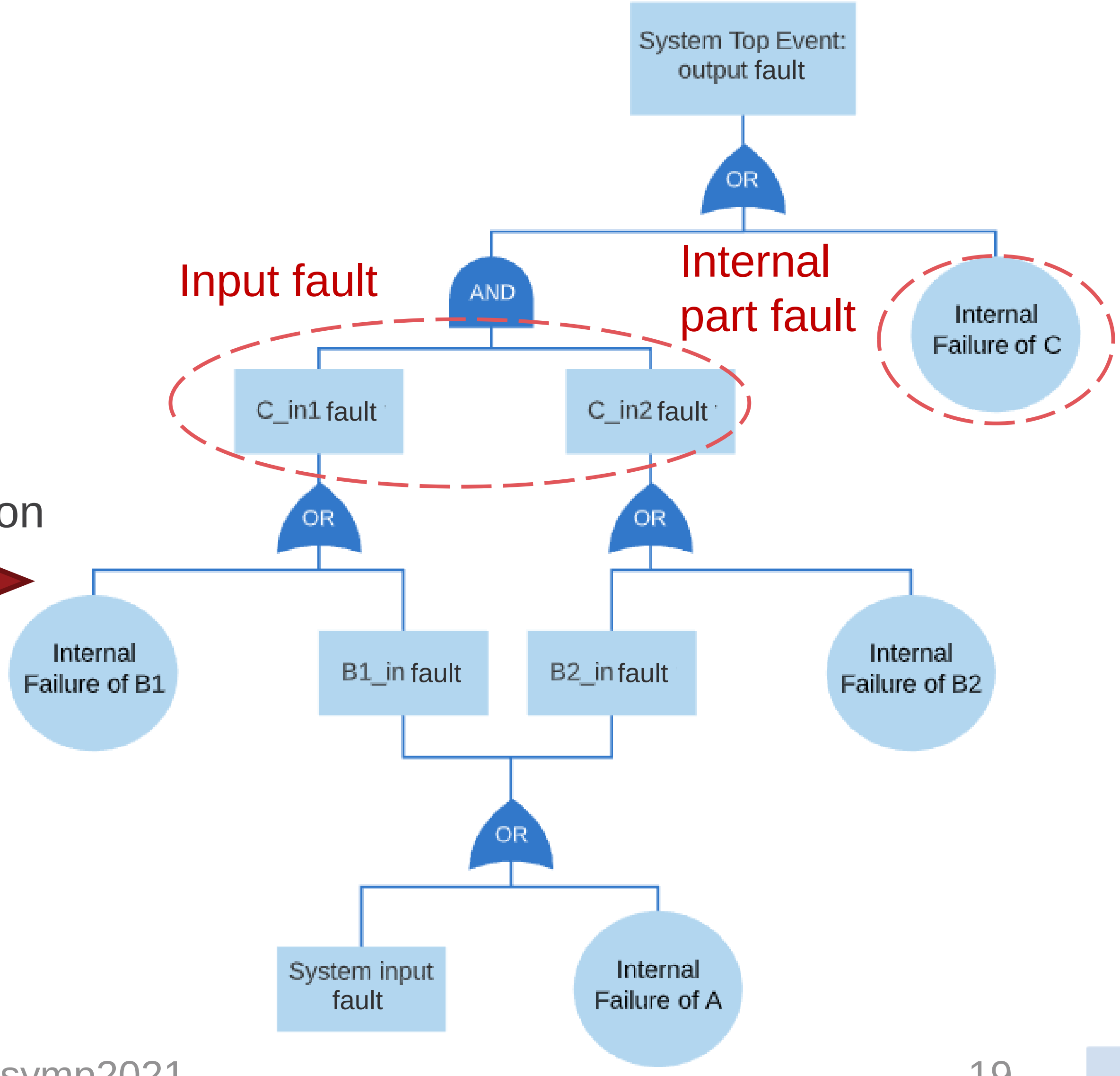
Safety Profile: FTA Generation



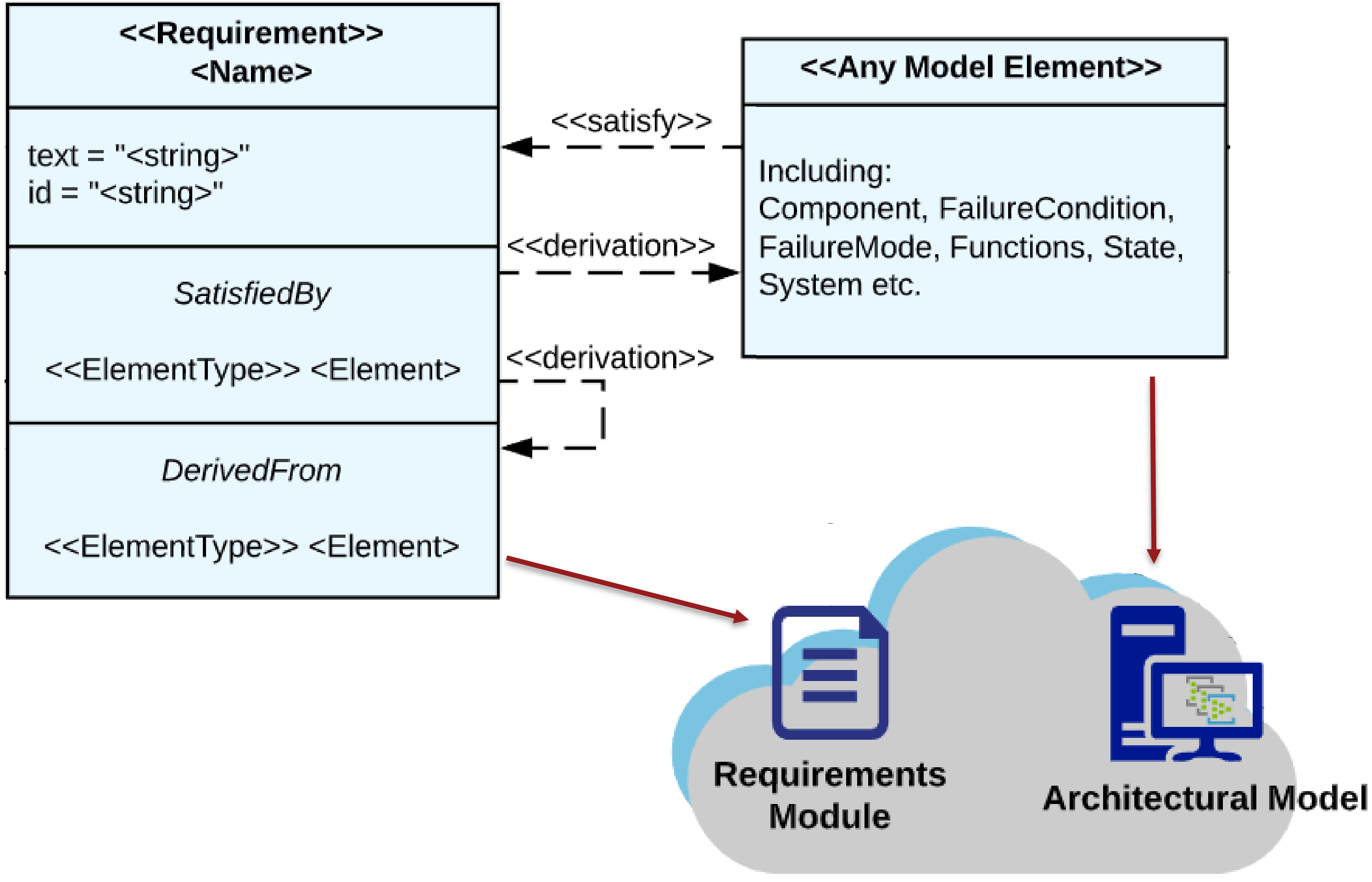
Access, extract and manipulate model elements

Safety Application

written using an API

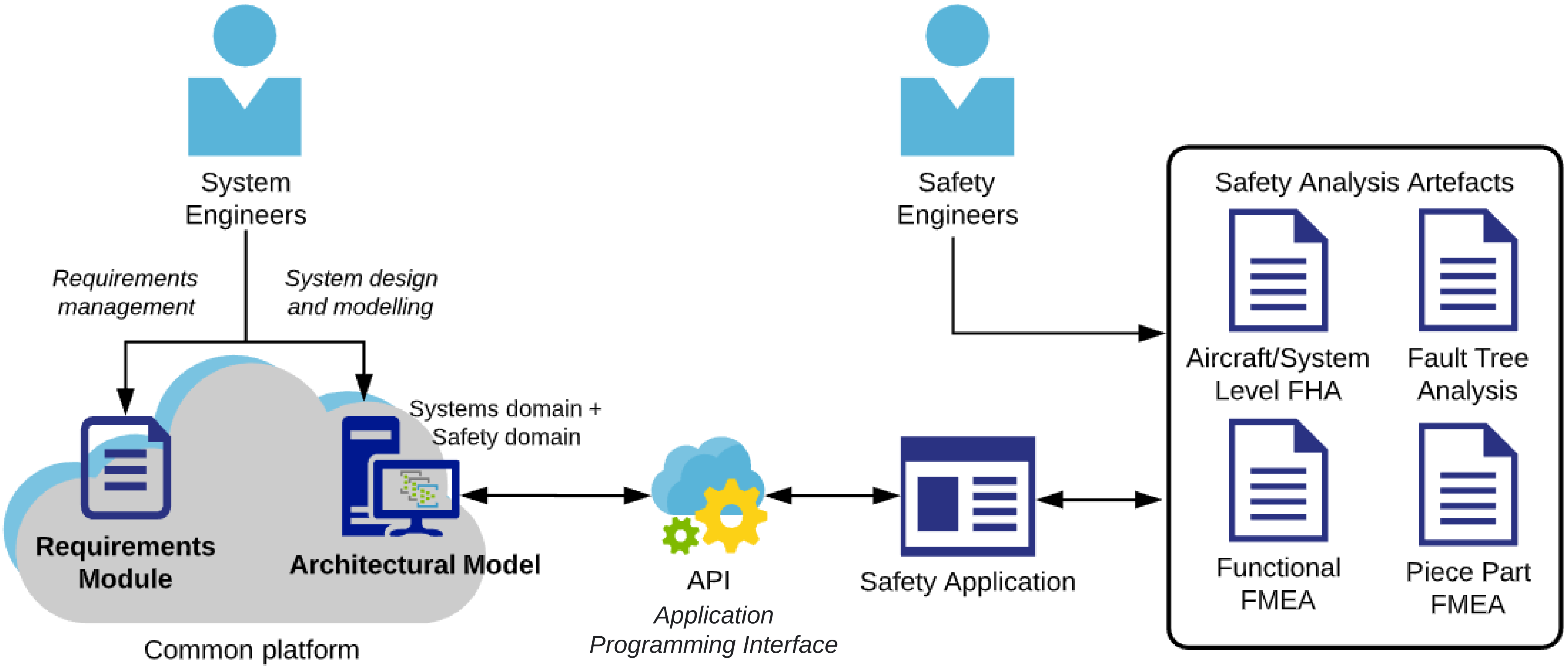


Safety Profile: Requirements Integration



Common platform

Safety Profile: Overall Process



Areas for Future Work

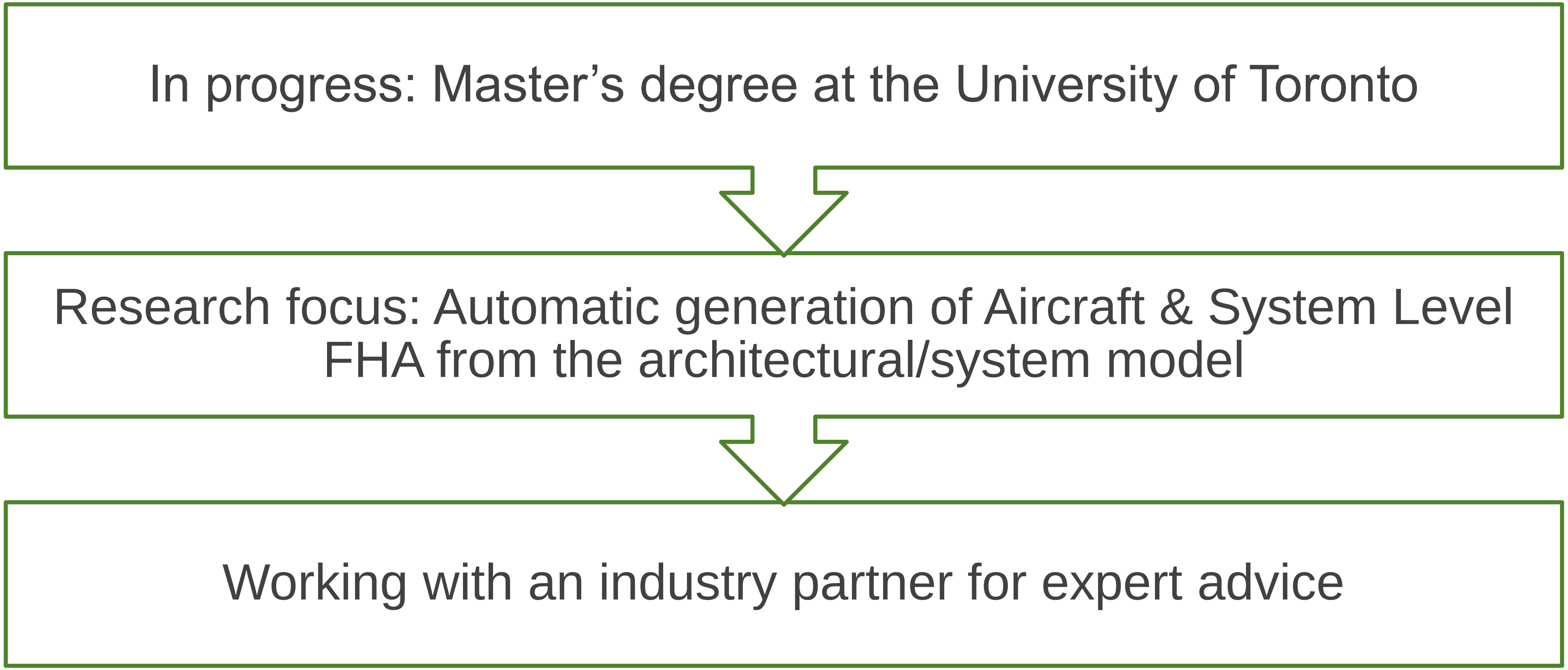
Detailed implementation method

Case study/proof of concept

Improve fault tree generation capabilities

Feedback from stakeholders or industry experts

Current Status



In progress: Master’s degree at the University of Toronto

Research focus: Automatic generation of Aircraft & System Level FHA from the architectural/system model

Working with an industry partner for expert advice

Thank you!

✉ kimberly.lai@mail.utoronto.ca

31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

www.incose.org/symp2021