33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Presenter: Thomas Robert (Safran Landing Systems)
Kimberly Lai (University of Toronto), David Shindman (Safran Landing Systems), Alison Olechowski (University of Toronto)

MBFHA: A Framework for Model-Based Functional Hazard Assessment for Aircraft Systems

Table of Contents

Section 1

Background and Motivation

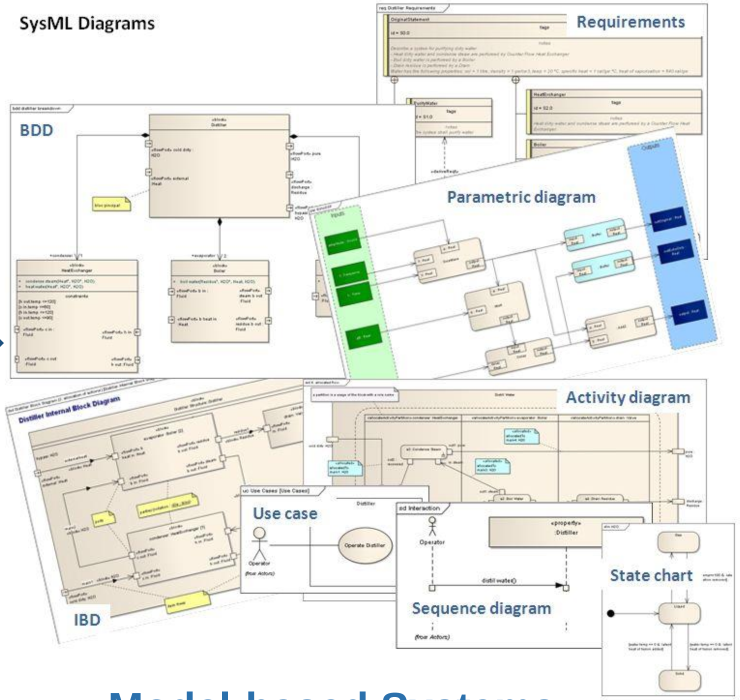
Background and Motivation

Increasing complexity of large integrated systems is driving a change in Systems Engineering practices

Traditional approach:

Document-based Systems Engineering

Current/future approach:



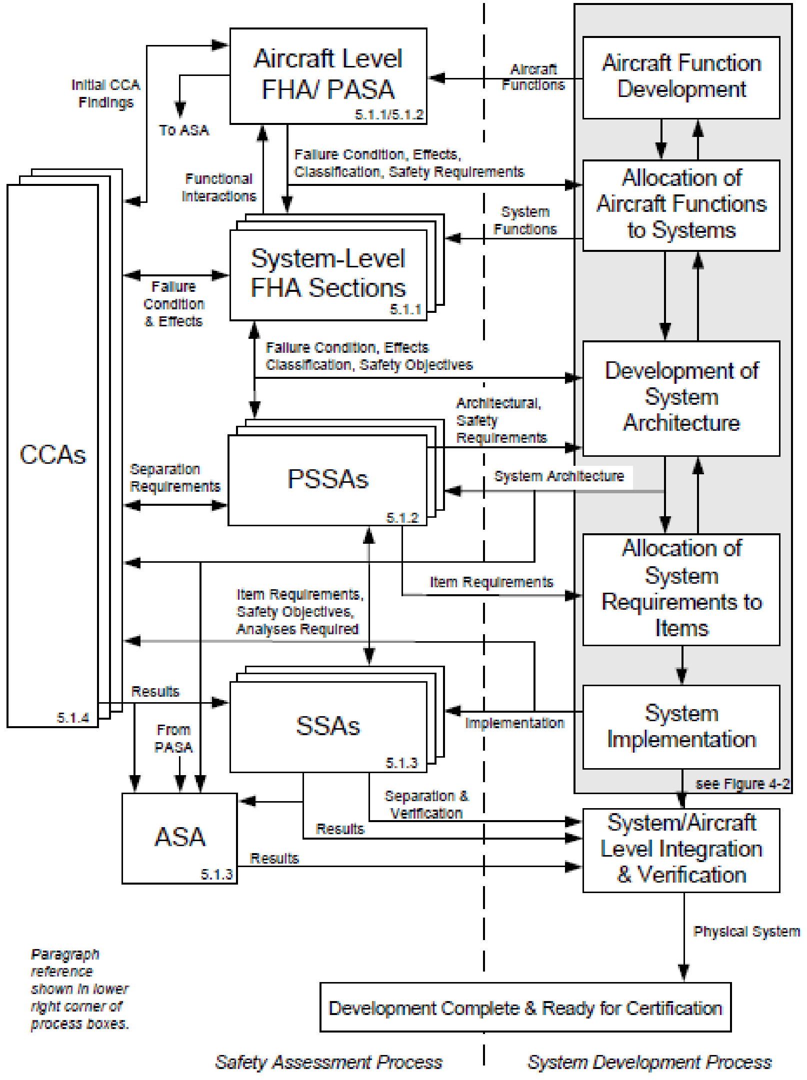
Model-based Systems Engineering (MBSE)

MBSE definition:

“Formalized **application of modeling** 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) -

Background and Motivation



For civil aircraft developments:
System development and safety assessment processes are highly dependent on one another

Safety assessment activities are performed in parallel to architecture and design activities (SAE ARP4761)

Safety Assessment ↔ **System Development**

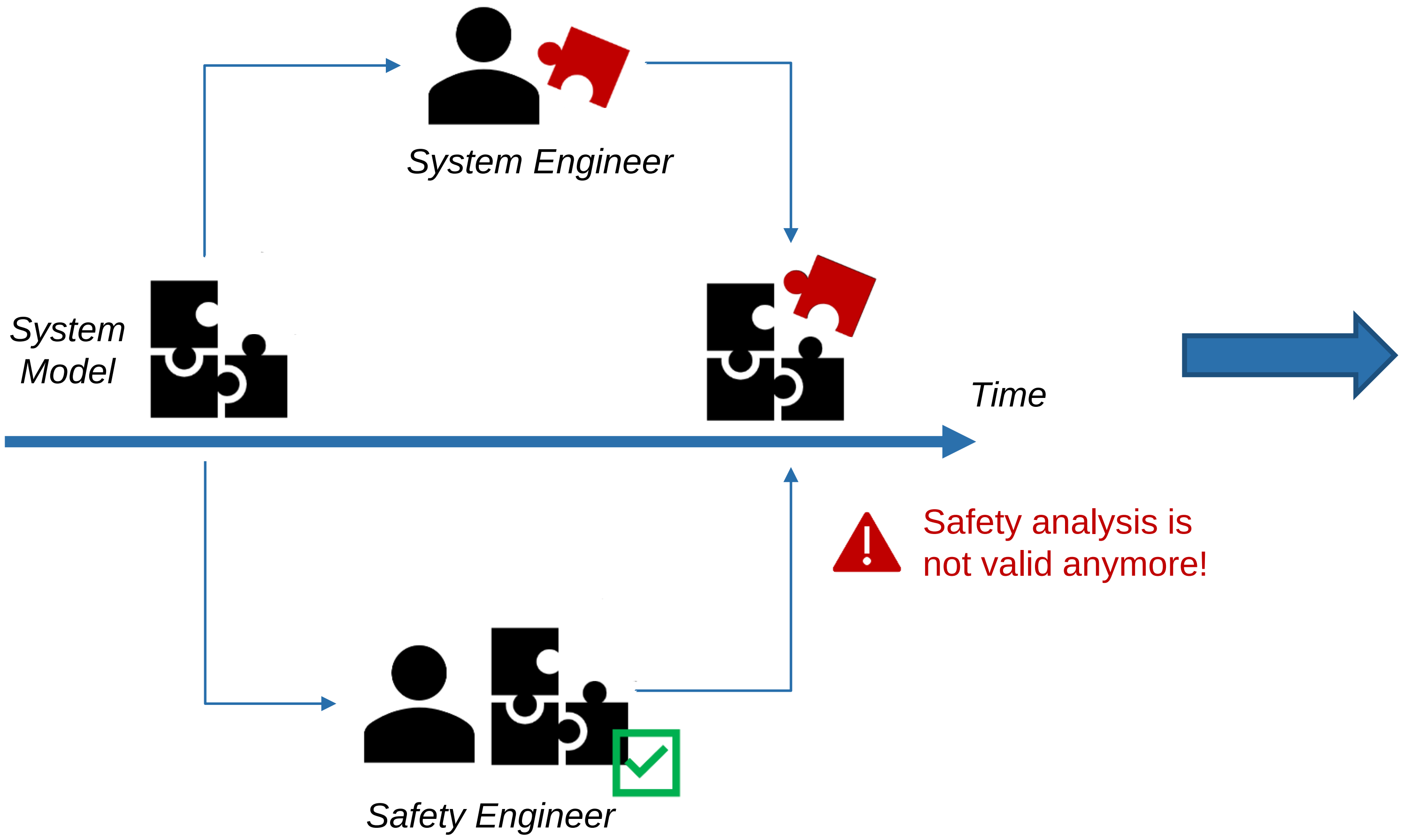
Document-based approach

Model-based approach (MBSE)

Not linked with MBSE methods and artefacts!

Background and Motivation

Document-based safety assessment activities are unable to keep up with architecture and design changes



Model-based approach to perform safety assessment is needed

- ✓ Increased efficiency
- ✓ Improved reliability
- ✓ Better traceability
- ✓ Decreased development time
- ✓ Introduction of automation

Background and Motivation

Existing approaches for Model-based Safety Assessment (MBSA)

Model-to-model transformation	Modeling language extension
• Transformation of the system model such that it can be analyzed by an existing safety tool • Example – MeDISIS methodology transforms a SysML model into AltaRica DataFlow and AADL	• Safety related concepts are introduced into the systems modeling profile (e.g. SysML) • Risk Analysis and Assessment Modeling Language (RAAML) Specification of the OMG

For our present work on **model-based FHA**, we chose to use a **modeling extension method**:

- To avoid transformation errors
- To encourage earlier integration between system and safety domains

Background and Motivation

Reference	Safety Assessment Artefact			Notes
	FHA	FMEA	FTA	
Clegg et al. (2019)	✕	✕	✓	
Biggs, Sakamoto & Kotoku (2016)	✕	✕	✕	Accounts for some hazard data but does not generate standardised artefacts.
David, Idasiak & Kratz (2010)	✕	✓	✕	
Douglass (2017)	✕	✓	✓	
Krishnan & Bhada (2020)	✕	✓	✓	
Mhenni, Nguyen & Choley (2018)	✕	✓	✓	
Muller, Roth & Lindemann (2016)	✕	✕	✕	Accounts for FHA & FMEA data but does not generate standardised artefacts.
Object Management Group (2021)	✕	✓	✓	

Works that propose modeling language extensions (UML/SysML)

Conclusion from literature review:

Focus is placed on facilitating FMEA and FTA only

→ Model-based approach for performing FHA is missing

Section 2

Definitions

Definitions

Functional Hazard Assessment (FHA)

Objective: identify potential **failure conditions** (functional failures), detail their **effects**, and **classify** the hazards associated with each one

- The **first step** of the safety assessment process performed on any new aircraft development programs
- A **qualitative assessment** that is performed at both the aircraft level and the system level
- A live document that is **updated iteratively** throughout the development as the aircraft and its systems become more defined

Standard FHA Table Example, Adapted from SAE ARP4761

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 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 overrun.	Catastrophic		S18 Aircraft Fault Tree

Definitions

Unified Modeling Language (UML)

A standardized **object-oriented modeling language** developed by the Object Management Group (OMG)

- "Provides system architects, software engineers, and software developers with tools for analysis, design, and implementation of software-based systems as well as for modeling business and similar processes"
- Is the basis from which the Systems Modeling Language (**SysML**) is created
- Enables the modeling of **structure diagrams** (e.g. class, component, structure) and **behavior diagrams** (e.g. state machine, activity, use case)
- **Profile extension** capability – enables creation of custom profiles to model **domain-specific information** (e.g. new stereotypes, properties and tagged values)
- UML model data can be **exchanged** among UML-compliant tools by using the **XML Metadata Interchange (XMI)** format

Section 3

MBFHA Framework

MBFHA Framework

To address the lack of model-based approach for performing FHA:

➡ We introduced a modeling profile to facilitate such model-based FHA

⚠ However, for a successful model-based implementation we need:

1. Language	2. Method	3. Tool
• Notations and elements for modeling	• How the tasks should be performed	• Modeling environment
Addressed by the modeling profile	FHA process flow defined by ARP4761 is high level, and not specific to MBSE	Wide range of tools, but limited guidance on their selection

MBFHA Framework

Objective: Introduce the **Model-based FHA (MBFHA) framework** for implementing model-based functional hazard assessment and integrating it into existing MBSE activities

1. Language

- FHA profile – UML profile extension

2. Method

- FHA report generation
- Requirements generation
- Overall workflow

3. Tool

- Constraints specification

MBFHA Framework

MBFHA Framework

To demonstrate the **real-life applicability** of the proposed MBFHA framework, we further created a **proof-of-concept** model using failure data for a **Landing Gear Extension and Retraction System** (LGERS) for a **generic business aircraft**.

Functions typically allocated to a LGERS:

- Provide landing gear extension
- Provide landing gear retraction
- Provide landing gear door opening
- Provide landing gear door closing
- Provide landing gear position indication
- Provide landing gear door position indication

Dassault Falcon 8X
(for illustration purposes only)

Section 4

MBFHA Framework – Language

MBFHA Framework – Language

Language: FHA profile metamodel

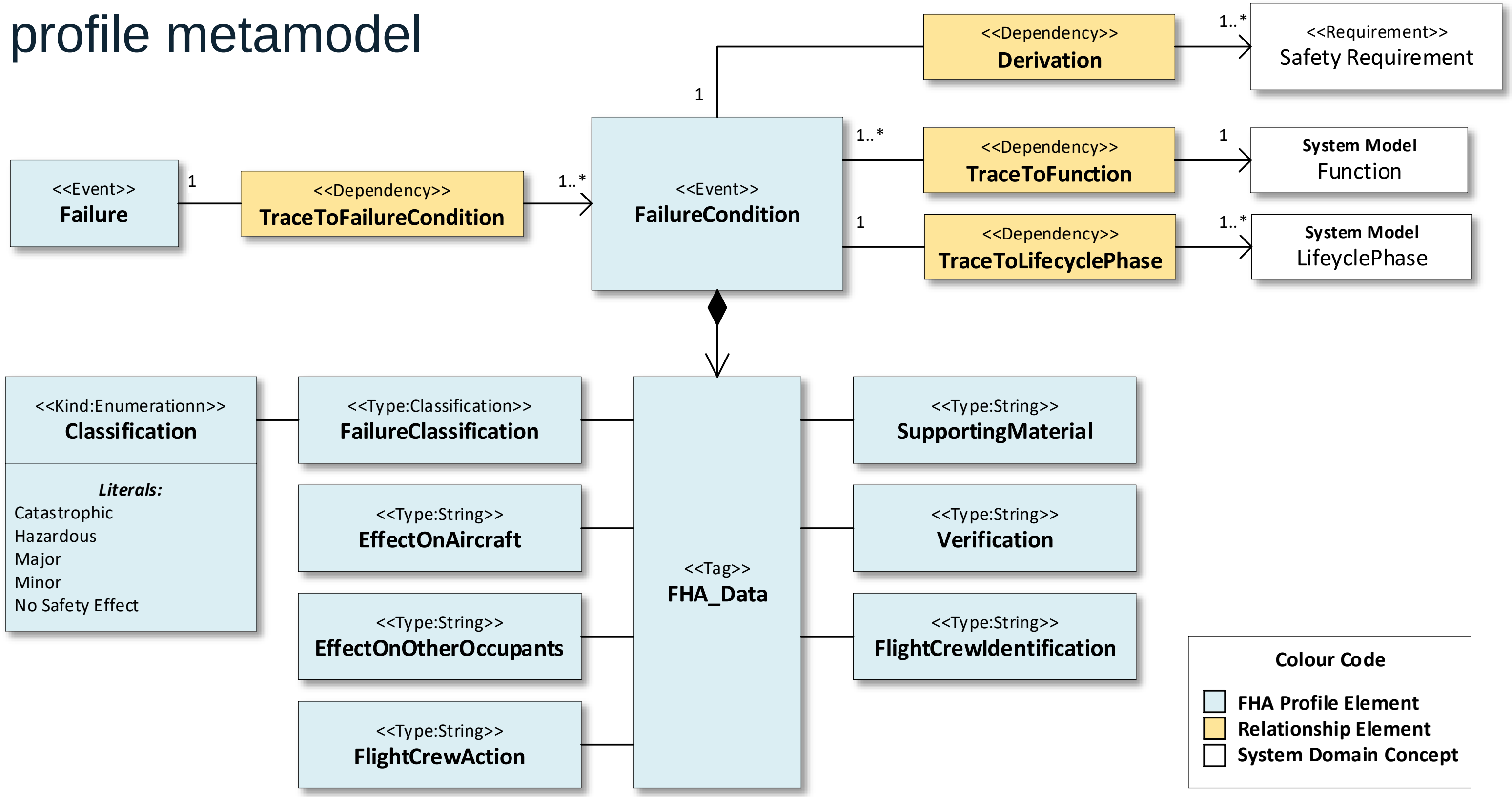
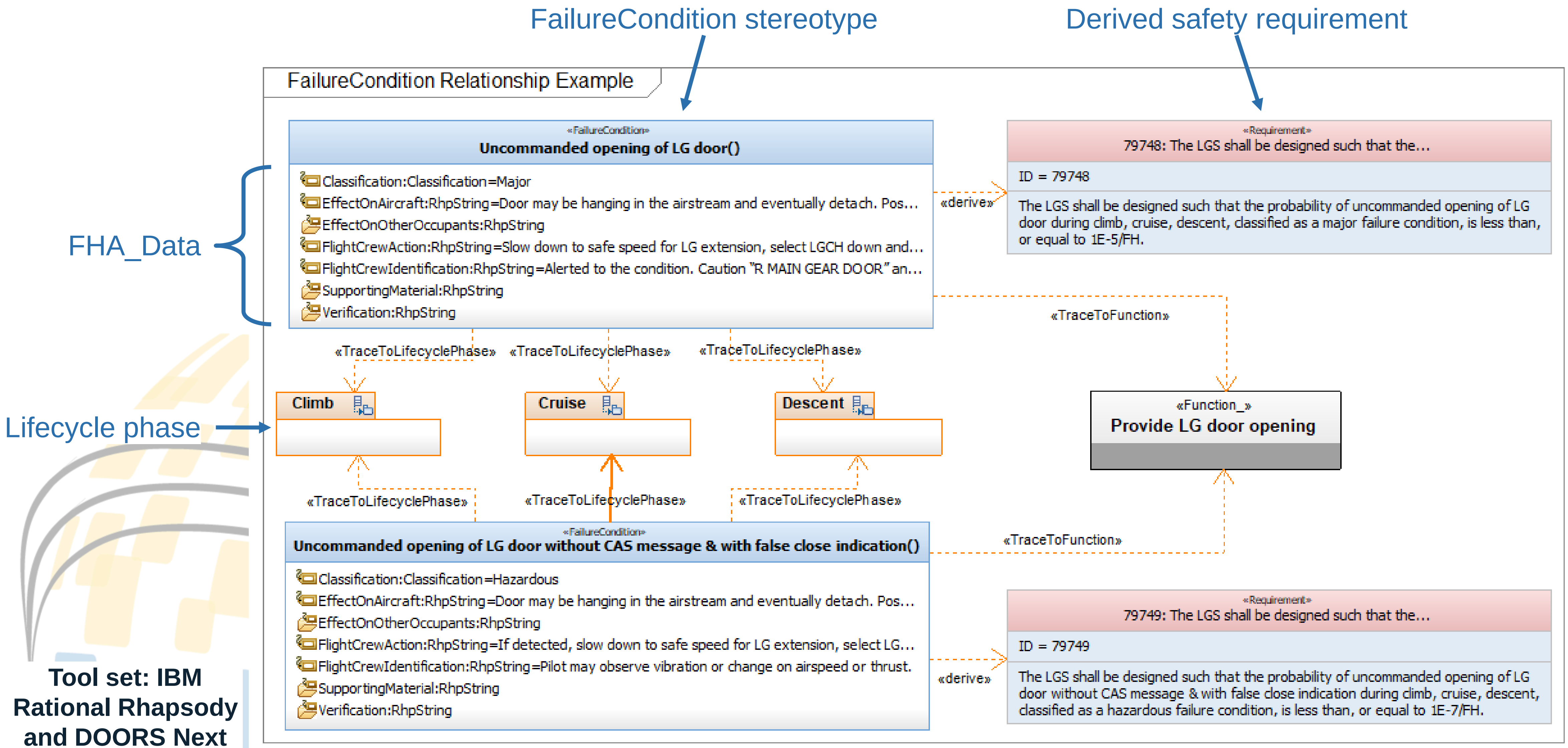


Table Layout	Description
FHA_Layout	FHA table – listing all failure conditions, the entries associated with each FHA_Data tag, and the function and lifecycle phase it is traced to.
FailuresToFC_Layout	Relating failures to failure conditions

Erratum:
Figure slightly modified from that found in the paper, correcting the cardinality between Function and FailureCondition on their TraceToFunction dependency.

MBFHA Framework – Language



Tool set: IBM Rational Rhapsody and DOORS Next

MBFHA Framework – Language

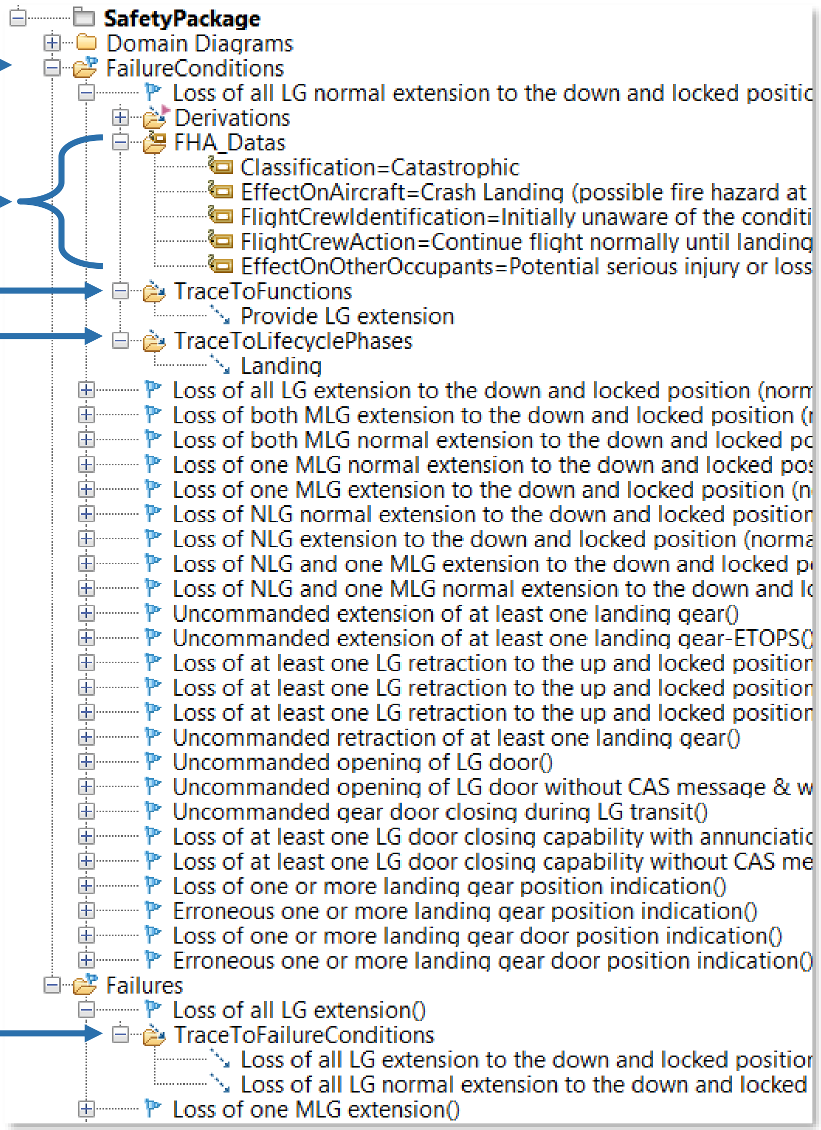
FailureCondition

FHA_Data

Dependency link to Function

Dependency link to Lifecycle Phase(s)

Dependency link from Failure to Failure Conditions



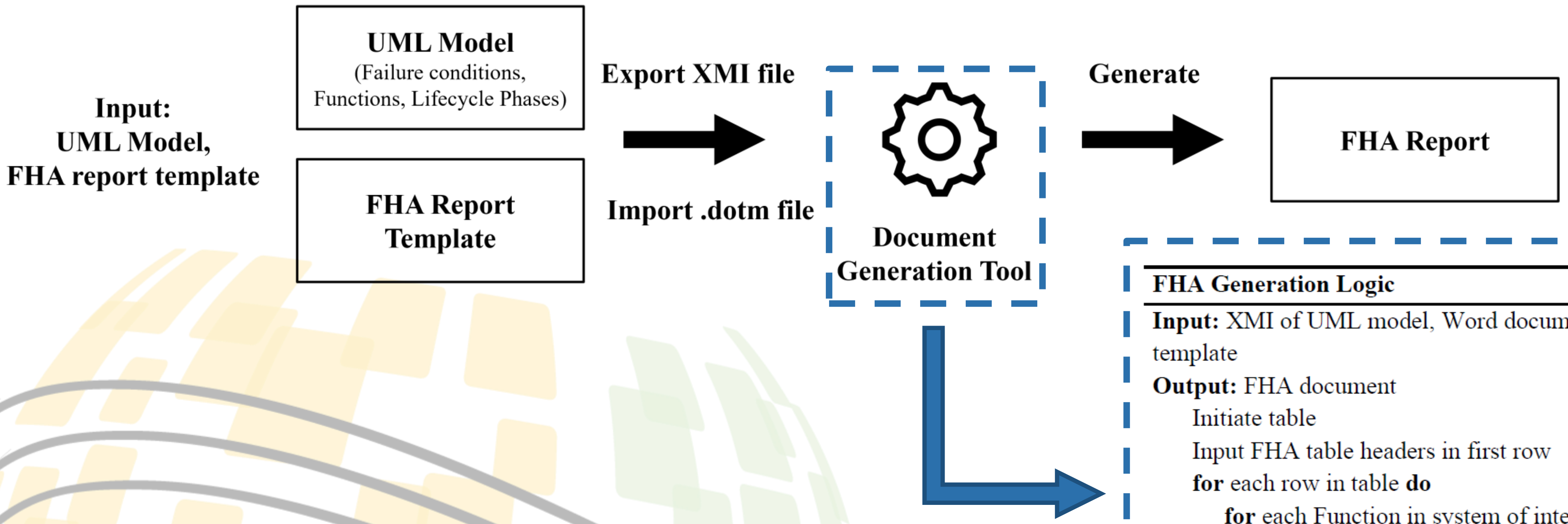
Section 5

MBFHA Framework – Method

MBFHA Framework – Method

Method: FHA report generation

Modelling environment	→	Document generation tool
IBM Rational Rhapsody	→	Rational Publishing Engine (RPE)
No Magic MagicDraw	→	Report Wizard




```
FHA Generation Logic
Input: XMI of UML model, Word document
template
Output: FHA document
    Initiate table
    Input FHA table headers in first row
    for each row in table do
        for each Function in system of interest do
            Find associated Failure Conditions
            for each Failure Condition do
                Get FHA Data information/details
            end for
        end for
    end for
```

MBFHA Framework – Method

Generated FHA report output (table)

Function	Failure Condition	Flight Phase	Effect on Aircraft	Flight Crew Identification	Flight Crew Action	Effect on Other Occupants	Classification	Verification	Supporting Material
Provide LG retraction	Loss of at least one LG retraction to the up and locked position combined with loss of 1 engine	Climb Second approach Takeoff	Significant increase in drag. Cannot establish climb gradient. Possible collision with objects.	Noticeable drag. Alerted to the condition. Caution “GEAR DISAGREE” and Landing Gear Status indication(s).	Forced landing or ditching	Potential serious injury or loss of life.	Catastrophic		
Provide LG retraction	Loss of at least one LG retraction to the up and locked position without CAS message & with false uplock indication	Climb	Significant increase in aircraft drag.	Noticeable drag.	Change of flight plan with subsequent landing gear extended flight. Land at nearest airfield.	None	Major		
Provide LG retraction	Loss of at least one LG retraction to the up and locked position	Climb Second approach Takeoff	Significant increase in drag.	Noticeable drag. Alerted to the condition. Caution “GEAR DISAGREE” and Landing Gear Status indication(s).	Change of flight plan with subsequent landing gear extended flight. Land at nearest airfield.	None.	Minor		
Provide LG retraction	Uncommanded retraction of at least one landing gear	Takeoff Landing Taxi	Induced directional moment on aircraft. Possible aircraft ground loop. Possible runway excursion. Potential structural damage to fuselage, wing high lift surfaces.	Self evident. Sudden change in aircraft attitude on the ground. Alerted to the condition. Caution “GEAR DISAGREE” and Landing Gear Status indication(s).	Below V1: Stop aircraft. Abort takeoff. Above V1: Continue takeoff. After takeoff return to land. Emergency extension of landing gear prior to landing.	Potential serious injury or loss of life.	Catastrophic		

MBFHA Framework – Method

Method: Safety requirements generation

Requirement generation pattern:

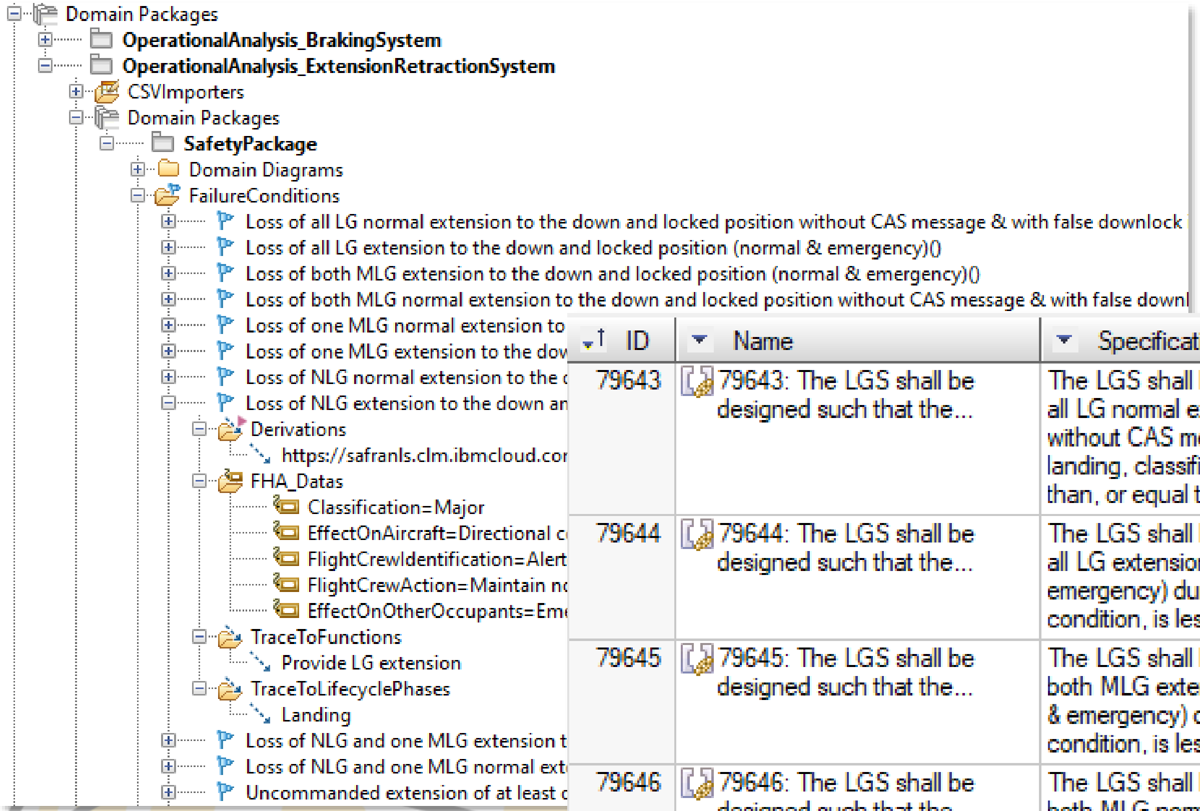
"The **'System of Interest'** shall be designed such that the probability of **[*failure condition*]**, during **[*flight phase*]**, classified as a **[*classification*]** failure condition, is less than, or equal to **[*probability*]**."

As defined in SAE ARP4761:

Failure classification	Probability (per flight hour)
Catastrophic	1×10^{-9}
Hazardous	1×10^{-7}
Major	1×10^{-5}
Minor	1×10^{-3}

Failure Condition	Lifecycle Phase	Classification	Probability
Loss of all LG extension to the down and locked position (normal & emergency)	Landing	Major	1E-5/FH
Safety Requirement			
The LGS shall be designed such that the probability of loss of all LG extension to the down and locked position (normal & emergency) during landing, classified as a major failure condition, is less than, or equal to 1E-5/FH.			

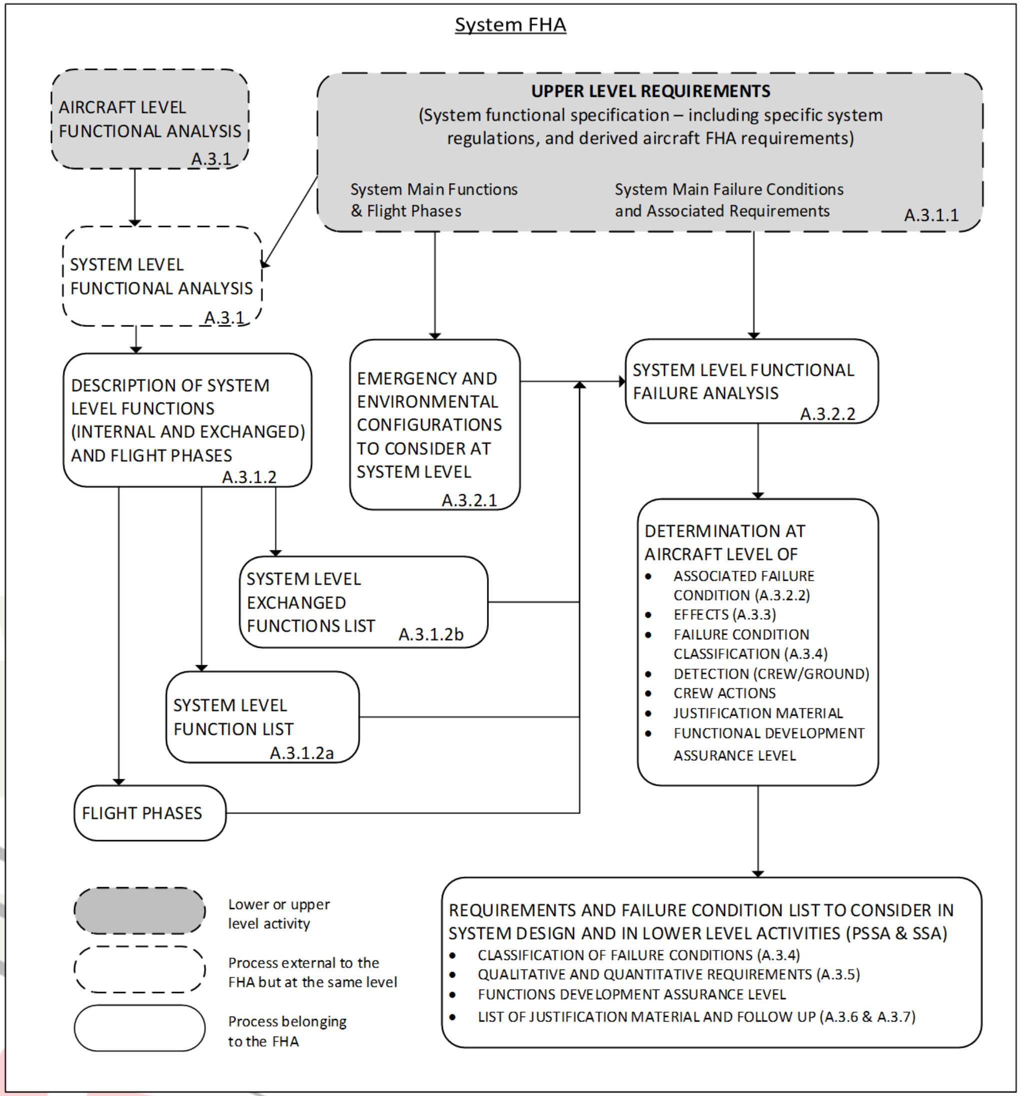
MBFHA Framework – Method



ID	Name	Specification	Link Type	Link From
79643	79643: The LGS shall be designed such that the...	The LGS shall be designed such that the probability of loss of all LG normal extension to the down and locked position without CAS message & with false downlock indication during landing, classified as a catastrophic failure condition, is less than, or equal to 1E-9/FH.	Derivation	Loss of all LG normal extension to the down and locked position without CAS message & with false downlock indication
79644	79644: The LGS shall be designed such that the...	The LGS shall be designed such that the probability of loss of all LG extension to the down and locked position (normal & emergency) during landing, classified as a major failure condition, is less than, or equal to 1E-5/FH.	Derivation	Loss of all LG extension to the down and locked position (normal & emergency)
79645	79645: The LGS shall be designed such that the...	The LGS shall be designed such that the probability of loss of both MLG extension to the down and locked position (normal & emergency) during landing, classified as a hazardous failure condition, is less than, or equal to 1E-7/FH.	Derivation	Loss of both MLG extension to the down and locked position (normal & emergency)
79646	79646: The LGS shall be designed such that the...	The LGS shall be designed such that the probability of loss of both MLG normal extension to the down and locked position without CAS message & with false downlock indication during landing, classified as a catastrophic failure condition, is less than, or equal to 1E-9/FH.	Derivation	Loss of both MLG normal extension to the down and locked position without CAS message & with false downlock indication
79647	79647: The LGS shall be designed such that the...	The LGS shall be designed such that the probability of loss of one MLG normal extension to the down and locked position without CAS message & with false downlock indication during landing, classified as a catastrophic failure condition, is less than, or equal to 1E-9/FH.	Derivation	Loss of one MLG normal extension to the down and locked position without CAS message & with false downlock indication

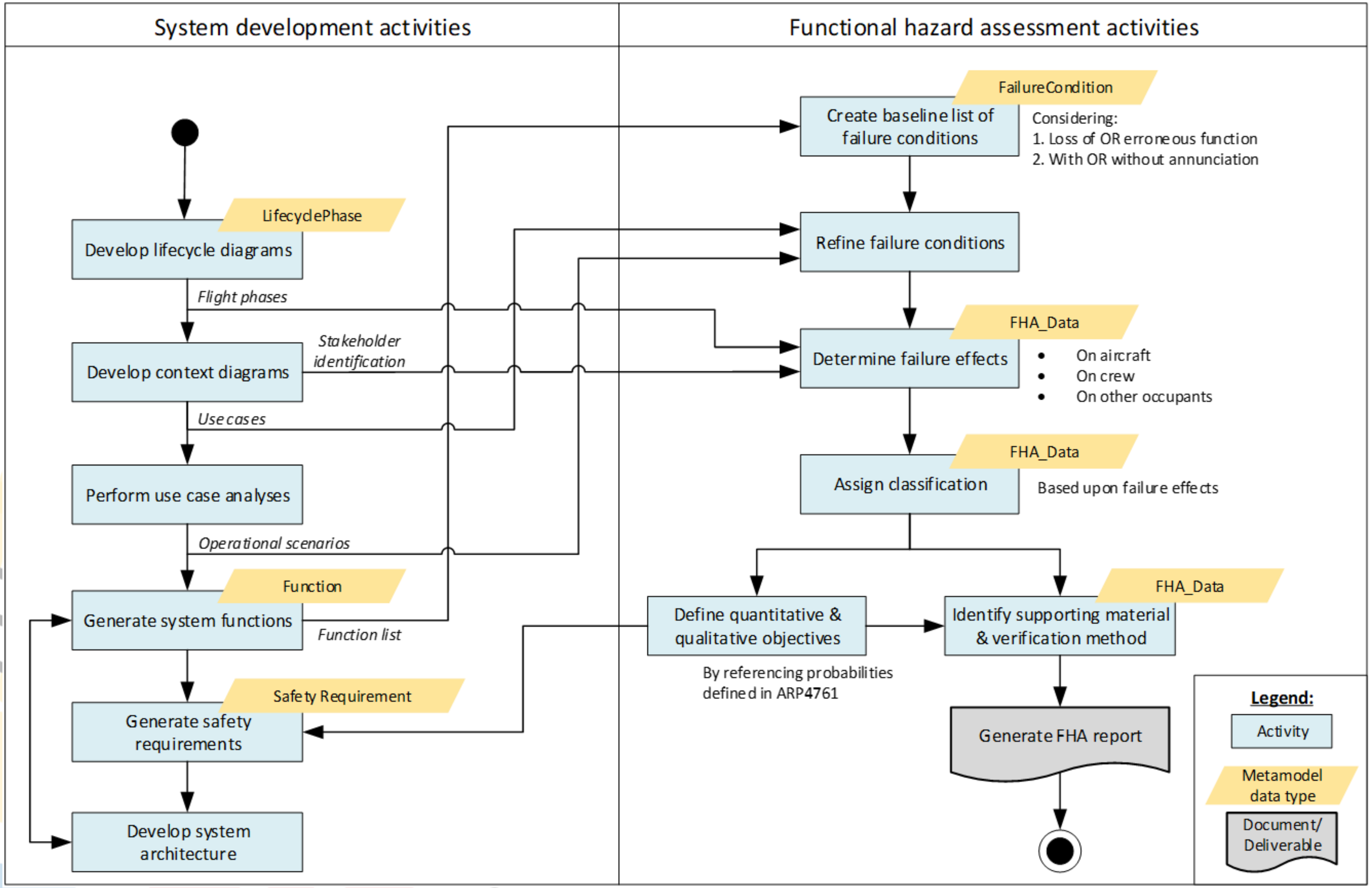
MBFHA Framework – Method

Method: Standard FHA process flow (SAE ARP4761)



MBFHA Framework – Method

Method: Overall MBFHA workflow



Section 6

MBFHA Framework – Tool

MBFHA Framework – Tool

Tool: Constraints specification

Six key capabilities a tool should have to implement the MBFHA framework effectively:

UML & SysML compatibility	• Standard/fundamental modeling languages
UML profile extension	• To enable creation of FHA profile
Document generation capability	• To export model data into documents through a custom template
Requirements integration	• To import requirements into the modeling environment
Requirements traceability	• To trace which safety requirements are derived from which model elements
XML export	• To convert to XML according to XML Metadata Interchange (XMI) standard

Section 7

Conclusions

Conclusions

Key contributions of the MBFHA framework

- Modeling of failure conditions, and tracing them to functions in the system model
- Automatic generation of FHA report, and storing FHA tables in the system model
- Generation of safety requirements using failure condition data, and creating a traceability link between the two elements
- Providing a systematic workflow for performing model-based FHA, in line with the ARP4761 guidelines

Conclusions

Benefits of the MBFHA framework

- Prevents safety analysis from being performed on outdated system design
- Enhances consistency between system and safety domains
- Provides better traceability between inputs and outputs of FHA
- Provides a more complete identification of possible failure conditions
- Ensures consistency between FHA and safety requirements
- Increases efficiency by using automation (i.e. FHA report generation)
- Provides an opportunity for re-use (i.e. FHA building blocks)

Conclusions

Criticism and drawbacks

Currently limited to IBM tools for implementation

Certification concerns with model-based safety analyses

Section 8

Next steps

Next steps

Integrate proposed FHA profile
with OMG RAAML profile

Link MBFHA (FHA) and MBSA
(FMEA, FTA) activities

Develop a library of reusable
MBFHA building blocks

Explore Model-based Safety
Analysis for other industries

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS