MODEL-BASED STPA TUTORIAL

Combining System-Theoretic Development and Safety Approaches

30th November 2022

Alexander Ahlbrecht, German Aerospace Center (DLR)

Motivation and Research Questions
Current Trends

Automation Need

Novel Functionality

Software-Intensity

Reduced Development Time

- Emerging segments
- Novel vehicle concepts and functionality
- Changes in the resulting development requirements

Motivation and Research Questions
Research Questions

- How can we use model-based developments to tackle the recent challenges?
- How would a safety-guided architecture design process look like?
- How do we achieve a fast-paced, but still certifiable design process?

Tutorial Focus

What is the target	What is not targeted
Explanation of proof-of-concept STPA profile implementation in combination with MBSE	Not a perfect depiction of STPA execution • Resource: STPA Handbook
Demonstration focusses on profile application with Cameo Systems Modeler version 19.3	Does not focus on full in-depth explanation of every modelling step (modelling knowledge assumed) • Resource: MagicGrid Book of Knowledge
Demonstration of advanced implementation concepts that can support the analysis execution	Implementations might contain errors and should be viewed as proof-of-concept

Agenda

Background and Resulting Concept

STPA Profile

Basic Use Case Application

Demonstration of Advanced Concepts

Future Work, Discussion & Conclusion

Background
Model-Based Systems Engineering (MBSE)

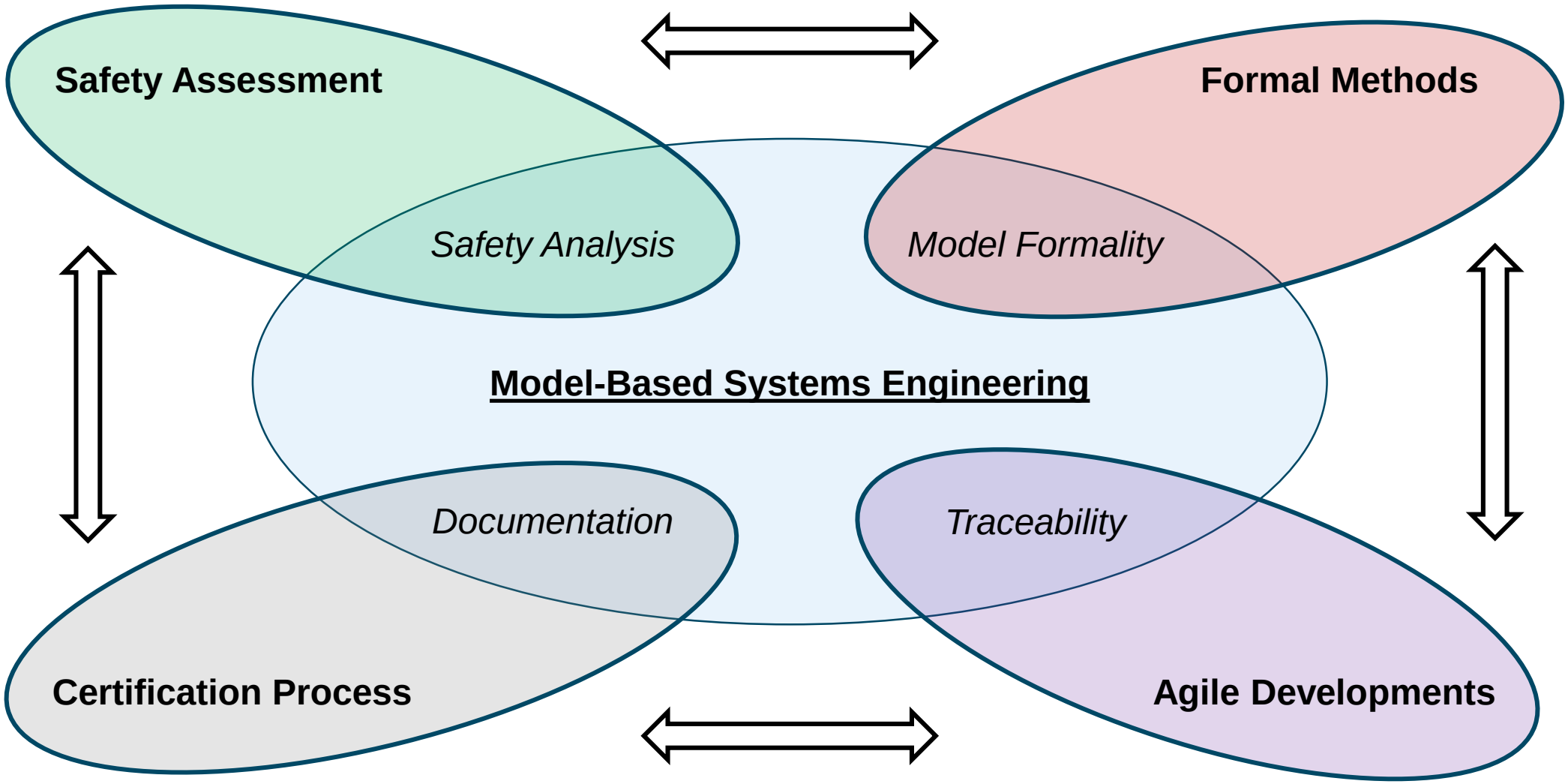
- **Definition: Systems Engineering (SE)**

is a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods. (INCOSE)

- **Definition: Model-Based Systems Engineering (MBSE)**

is the 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. (INCOSE)

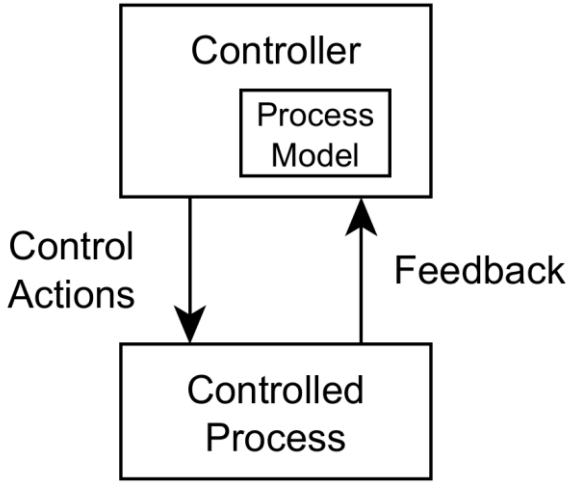
Background
MBSE Properties and Related Methods

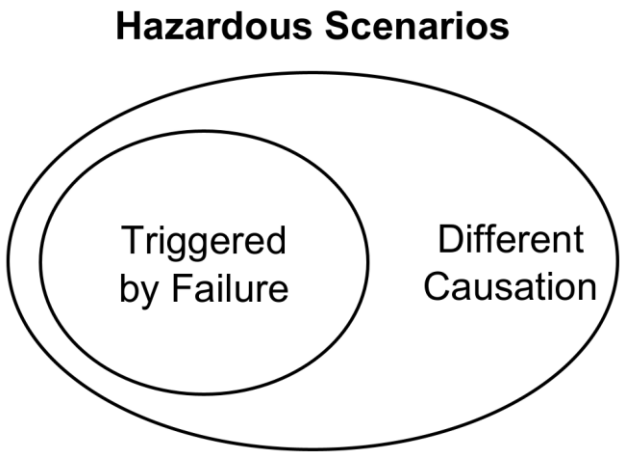


Background

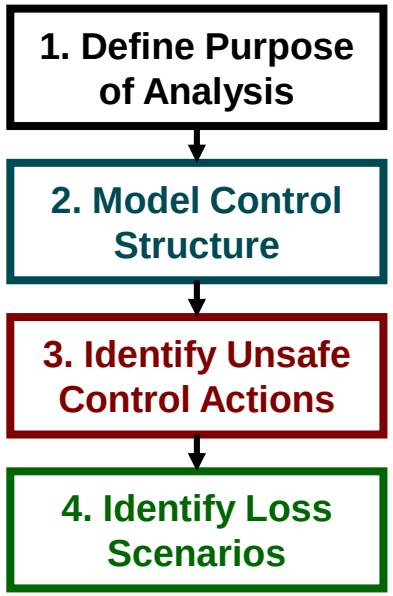
System-Theoretic Process Analysis (STPA)

- System-theoretic background
  - Safety treated as control problem
  - Control structure model as central artifact
- Extension over other safety-analyses
  - Analyses focused on component failures
  - Accidents: specification & interaction
  - Paradigm shift to control based analyses
  - Applied to analyse safety and security
- Formalization possible
  - Allows automation of analysis parts

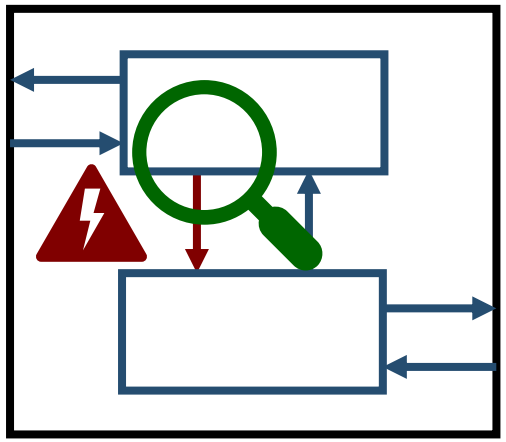




Engineering a Safer World & PhD John Thomas

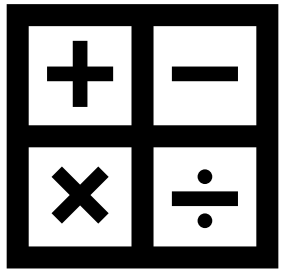


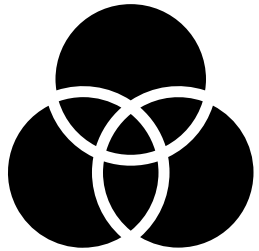
Define: Losses, Hazards, System Boundary, and Environment



Background
Formal Methods

Formal Methods are mathematic based techniques used to specify, design and verify hardware or software based systems





Stanford Lecture CS 357

- Advantages of formality
  - More precise specification
  - Machine readable and allow automation

Formality in a model-based context can be established by precisely defining relationships between model elements

OMG System Modeling Language™
(SysML®) v2 Release

SysML v2 Github

- SysML ≈ semi-formal (v2 tending upwards)

Resulting Concept
Process Baseline – Overall Concept

- MBSE as development foundation
  - Systematic development of systems
  - Provides semi-formal baseline
- Safety assessment integrated into MBSE
  - Model-based safety analysis
  - Safety-guided design possible
- Formal Methods
  - Allows automation of error-prone tasks
  - Provides time for creative tasks

Master's Thesis
DASC Paper 21
ISSE Paper 21

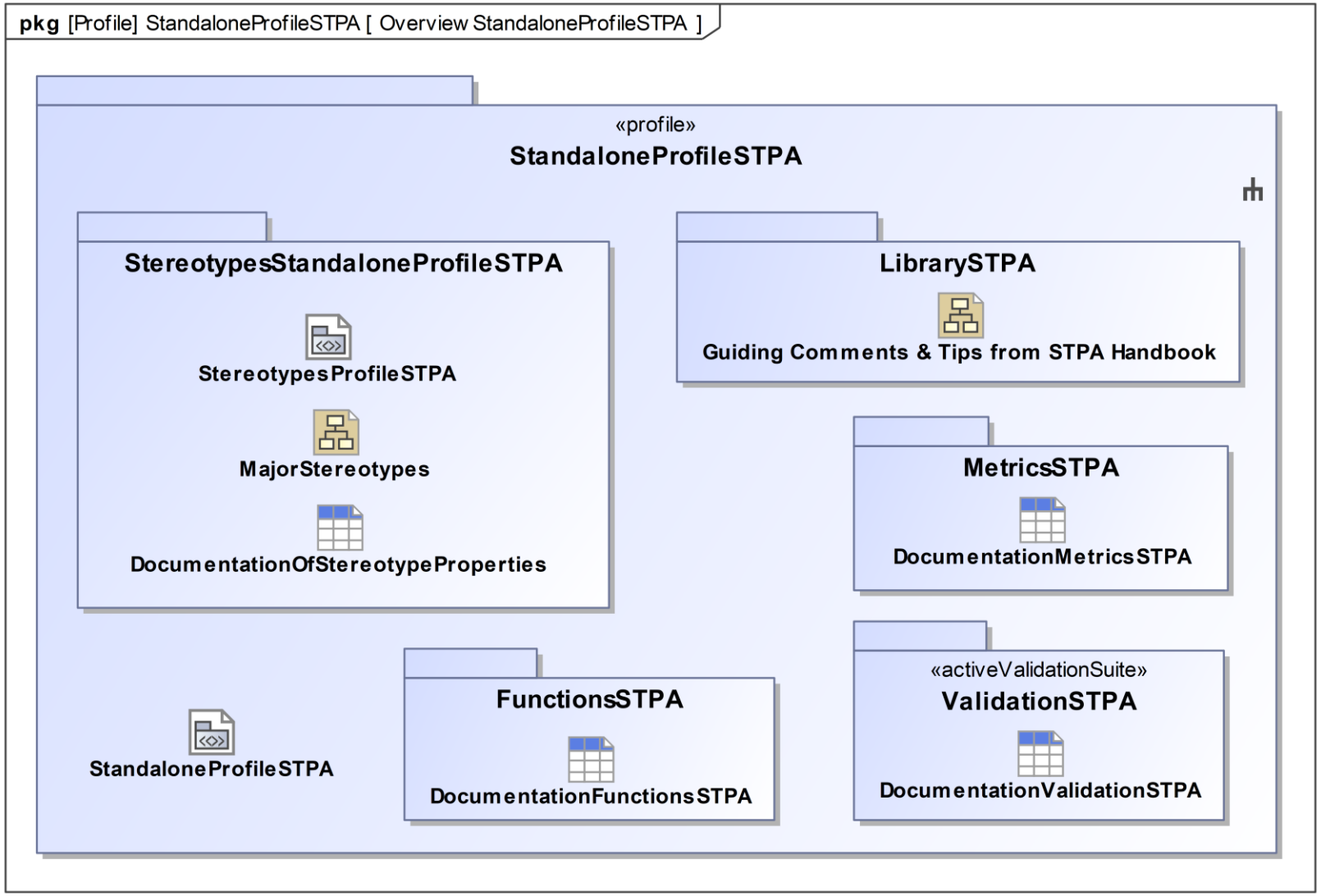
STPA Profile
Disclaimer

- Tutorial represents my own opinion and implementation which might contain inconsistencies with the original ideas of the STPA application

- Current profile implementation does not fully adhere to the STPA Profile of the Risk Analysis And Assessment Modeling Language (RAAML)

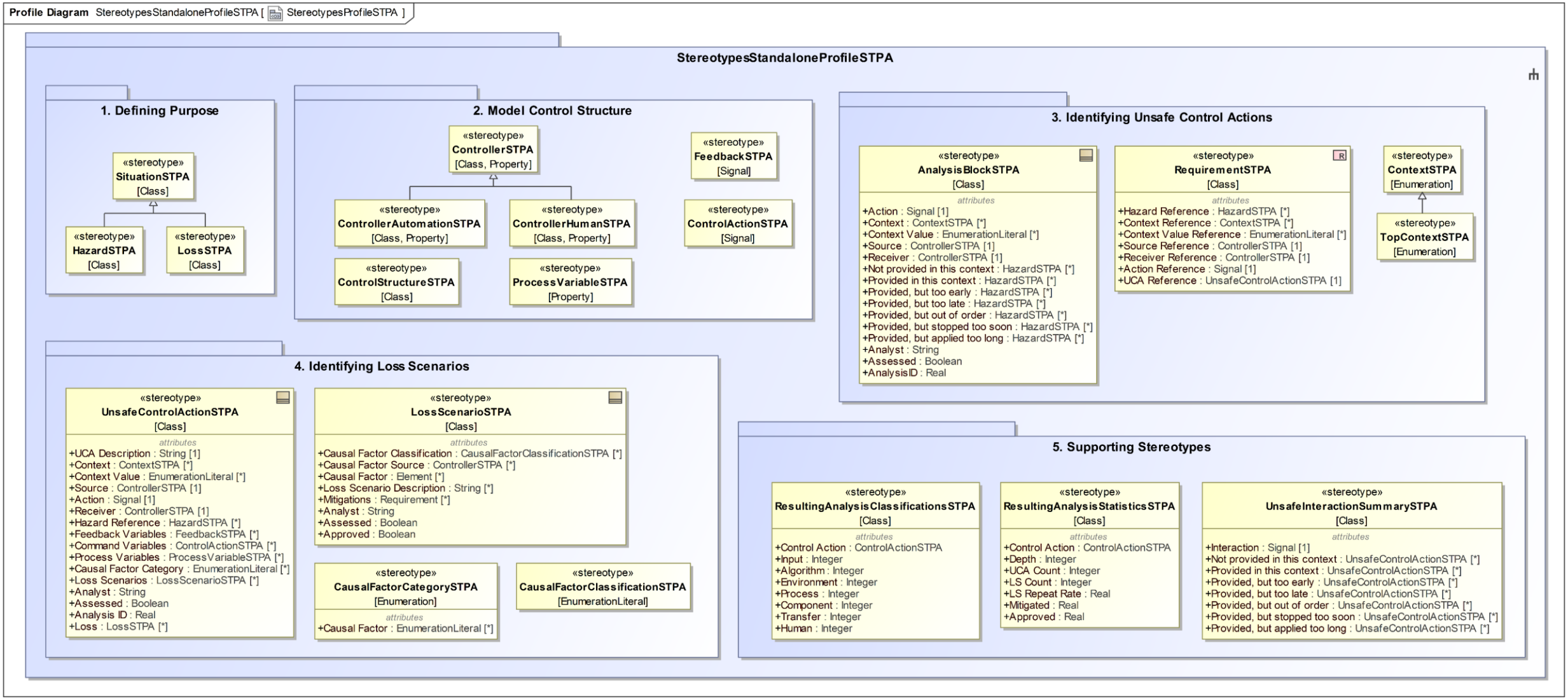
- I would recommend to consult sources with expert knowledge on the topic such as:
  - Engineering a Safer World (N. Leveson), STPA Handbook (N. Leveson, J. Thomas)
  - MIT Partnership for Systems Approaches to Safety and Security (PSASS)
  - SAE J3187 Guidance on STPA Application (SAE International)
  - RAAML Specification (Object Management Group)

STPA Profile
Profile Overview

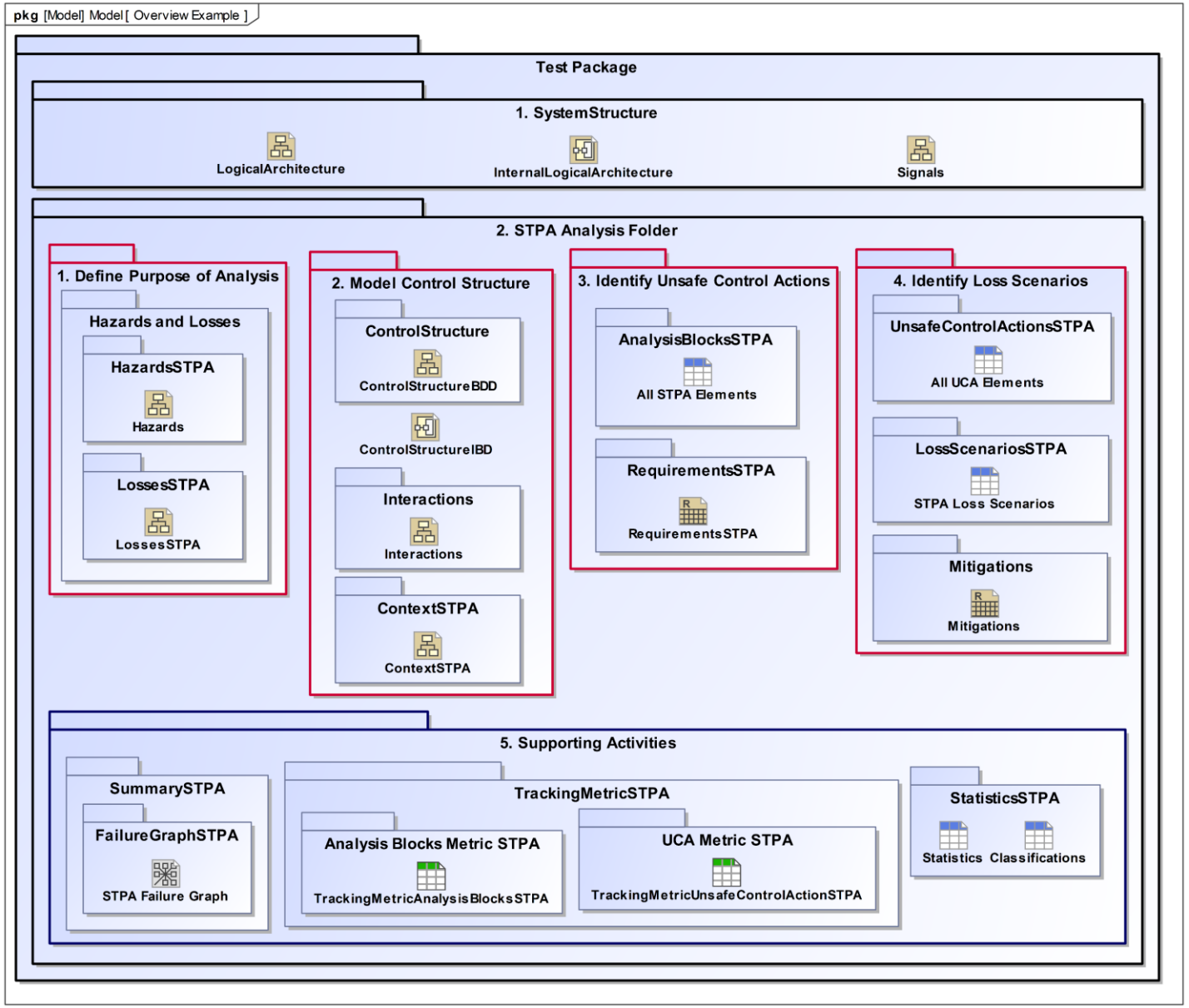


STPA Profile
STPA Stereotypes

1. Define Purpose of Analysis → 2. Model Control Structure → 3. Identify Unsafe Control Actions → 4. Identify Loss Scenarios

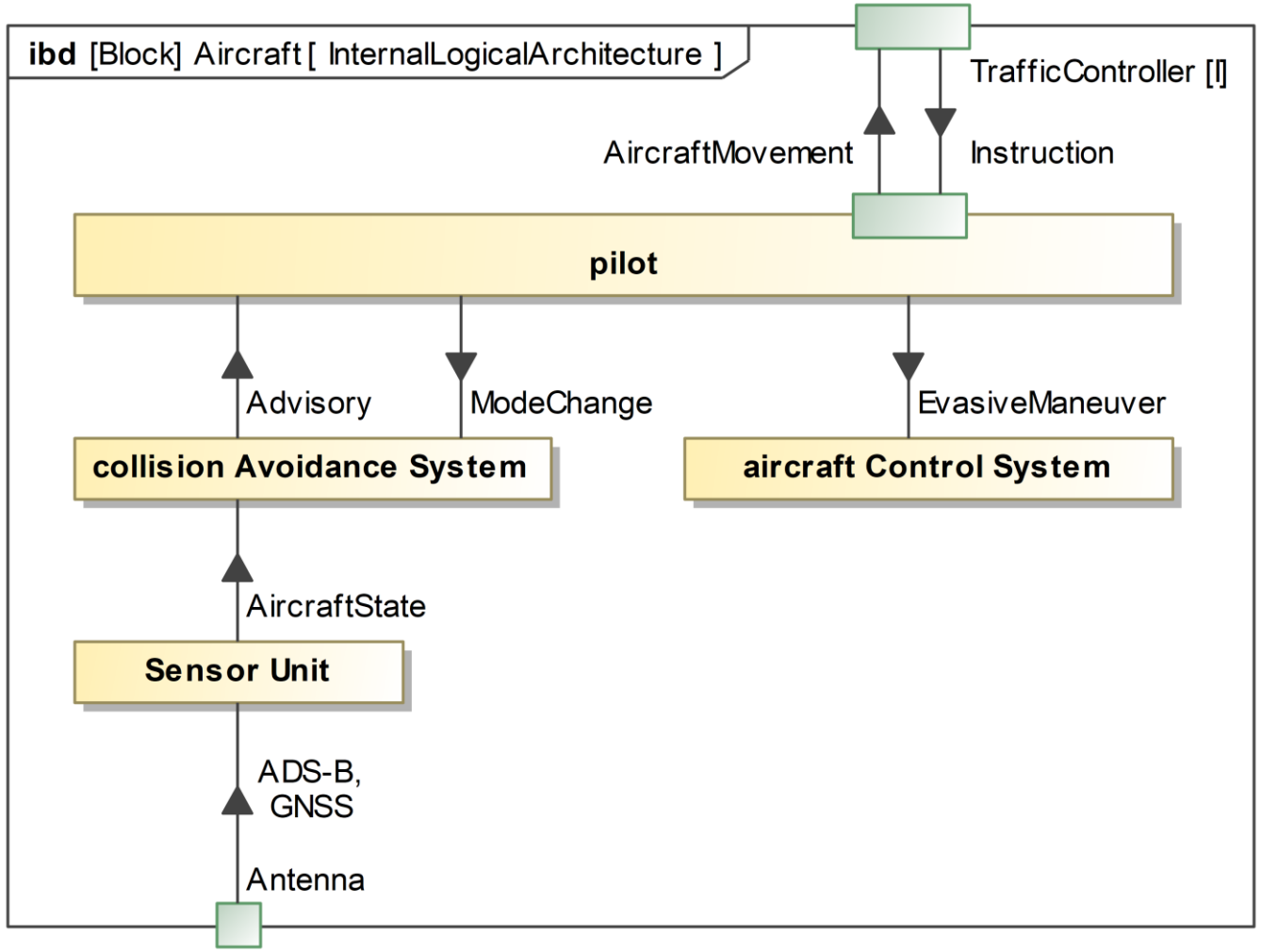


Profile Application
Example Overview

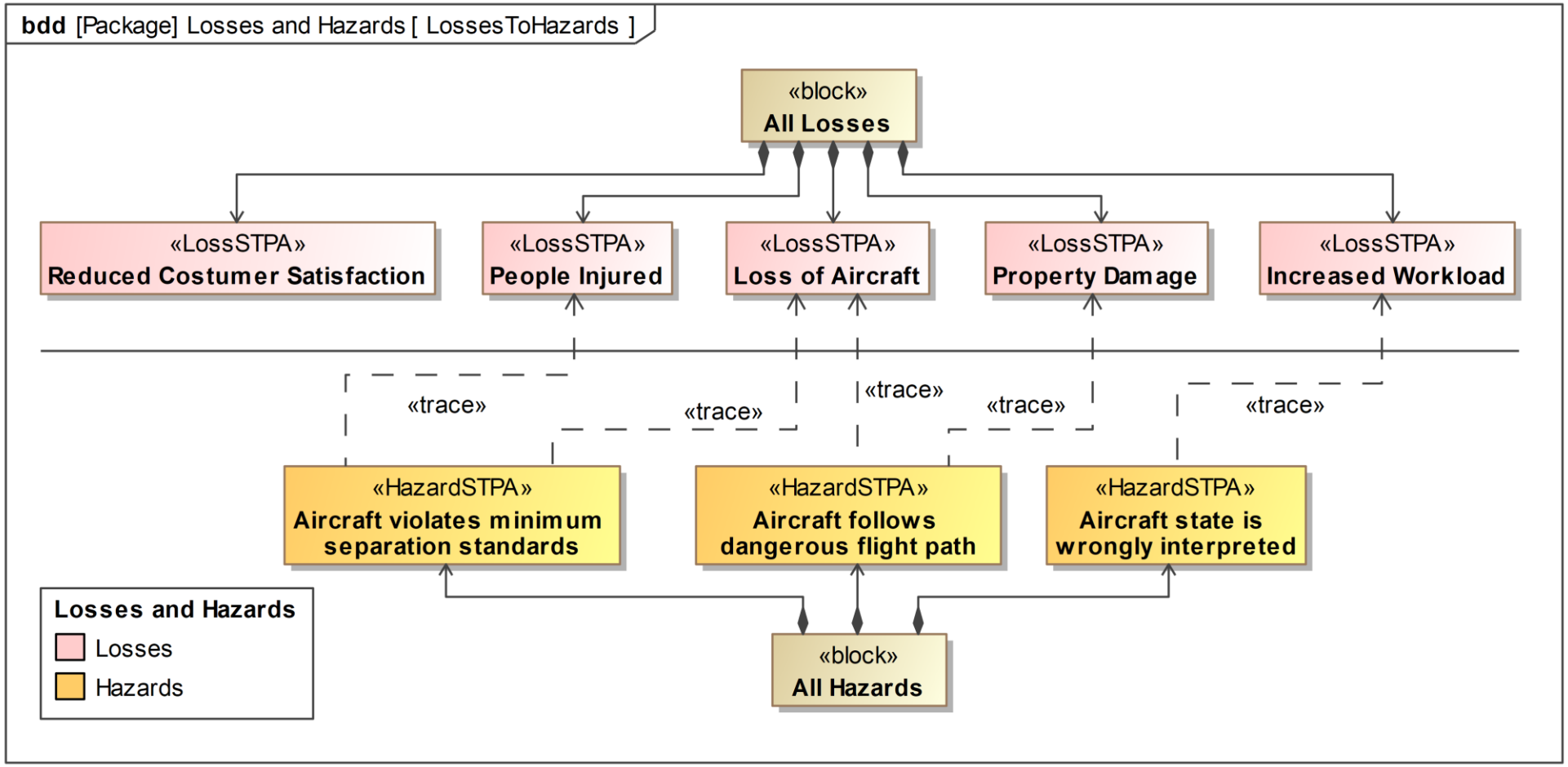


Profile Application
1. Architecture Baseline

DLR (CC BY-NC-ND 3.0)

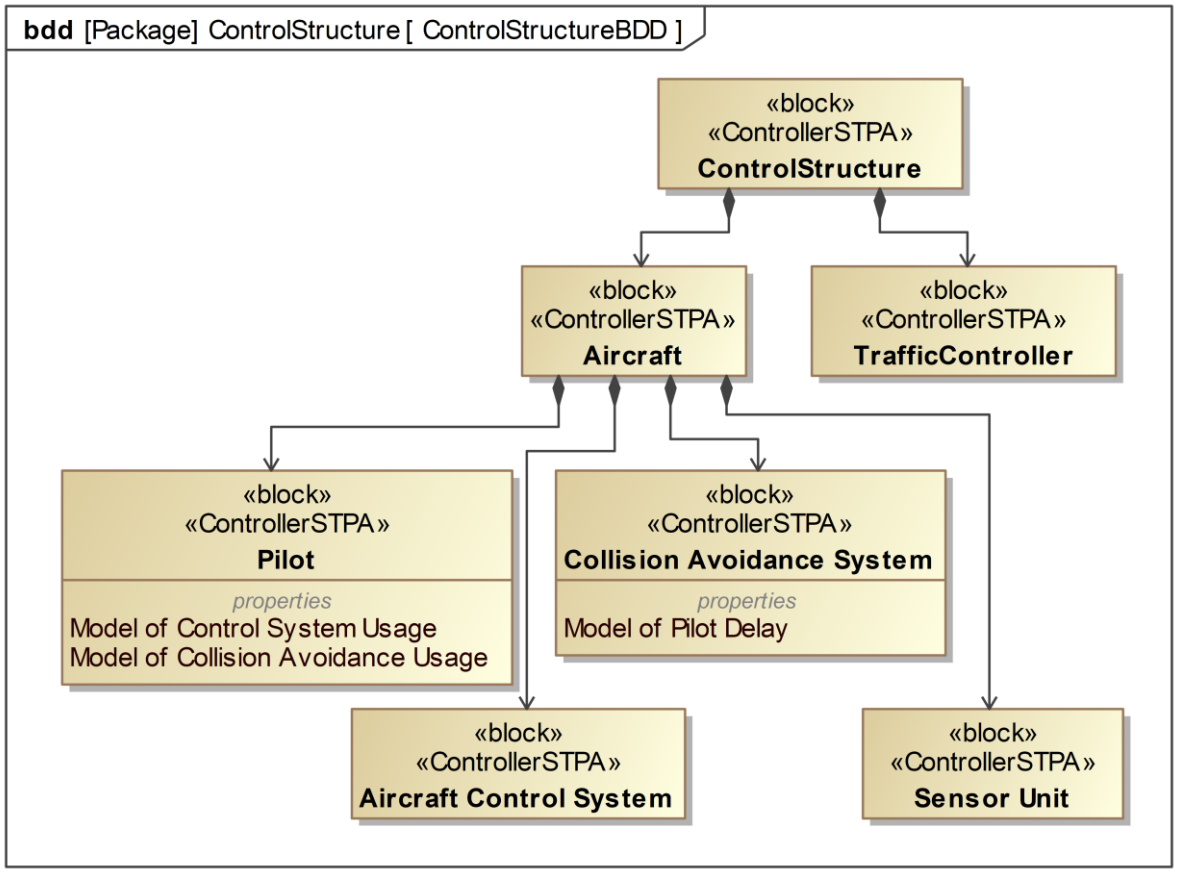


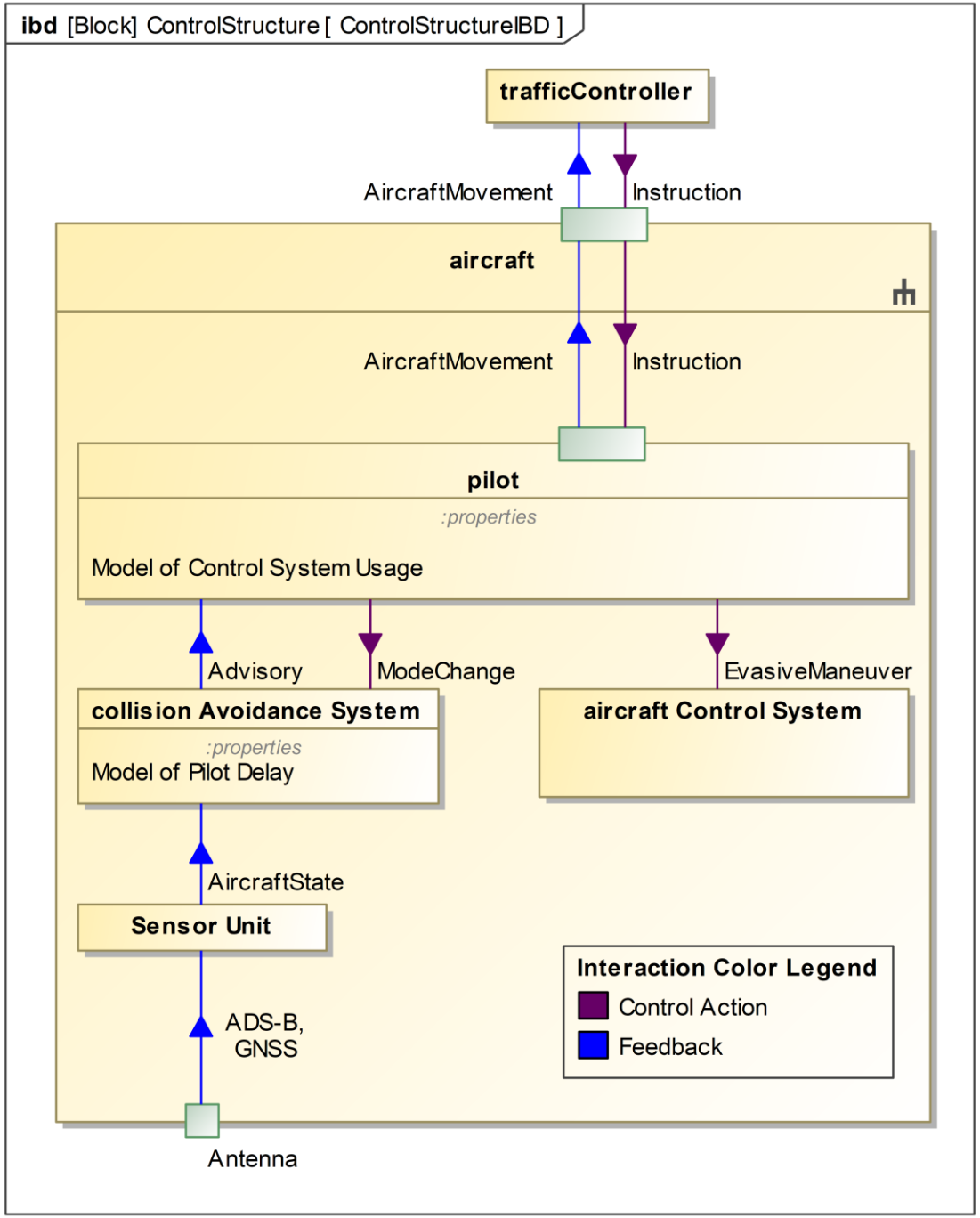
Profile Application
2.1 Defining the Purpose



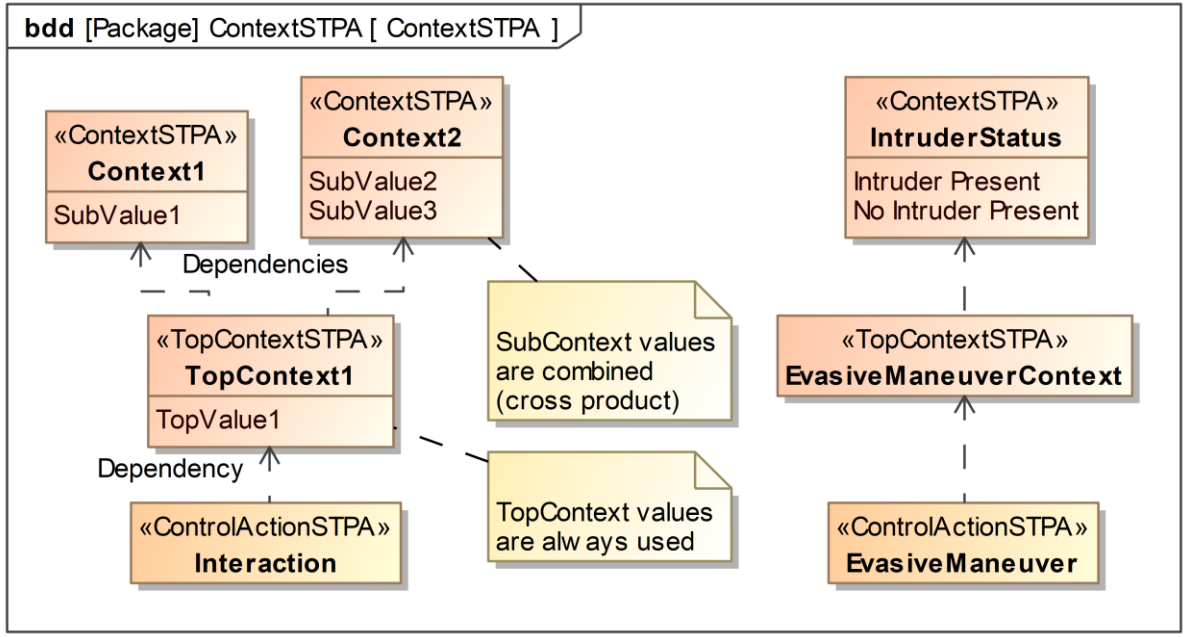
Profile Application

2.2 Modeling the Control Structure





Profile Application
2.3 Identifying Unsafe Control Actions



#	Name	Context	Context Value	Source	Action	Receiver	Not provided in this context	Provided in this context	Assessed	Analyst
1	STPA Element 10	TopContext1 Context1 Context2	TopValue1 SubValue1 SubValue2	Aircraft	Interaction	Sensor Unit			<undefined>	
2	STPA Element 11	TopContext1 Context1 Context2	TopValue1 SubValue1 SubValue3	Aircraft	Interaction	Sensor Unit			<undefined>	
3	STPA Element 8	IntruderStatus	Intruder Present	Pilot	EvasiveManeuver	Aircraft Control System	Aircraft violates minimum separation standards		true	A. Ahlbrecht
4	STPA Element 9	IntruderStatus	No Intruder Present	Pilot	EvasiveManeuver	Aircraft Control System		Aircraft violates minimum separation standards	true	A. Ahlbrecht

Profile Application
2.4 Identifying Loss Scenarios

#	Name	UCA Description	Action	Command Variables	Feedback Variables	Process Variables	Loss	Loss Scenarios	Assessed	Analyst
1	NoEvasiveManeuverWhenIntruderPresentLeadsToSeparationViolation	The [Pilot] does not apply [EvasiveManeuver] to the [Aircraft Control System] when [IntruderStatus] is in state [Intruder Present].	EvasiveManeuver	Instruction	Advisory	Model of Control System Usage Model of Collision Avoidance Usage	Loss of Aircraft	NoEvasiveManeuverDueToUncertainInstructionPriority	true	A. Ahlbrecht
2	EvasiveManeuverWhenNoIntruderPresentLeadsToSeparationViolation	The [Pilot] applies [EvasiveManeuver] to the [Aircraft Control System] when [IntruderStatus] is in state [No Intruder Present].	EvasiveManeuver	Instruction	Advisory	Model of Control System Usage Model of Collision Avoidance Usage	Loss of Aircraft		<undefined>	

#	Name	Causal Factor Source	Causal Factor	Causal Factor Classification	Loss Scenario Description	Mitigations	Assessed	Analyst	Approved
1	NoEvasiveManeuverDueToUncertainInstructionPriority	Pilot TrafficController Collision Avoidance System	Model of Collision Avoidance Usage Instruction Advisory	Process Model	Simultaneous instructions from the collision avoidance system and the traffic controller lead to a pilot confusion and a missing evasive maneuver.	48.3.3 Clear Instruction Priority	true	A. Ahlbrecht	false
2	EvasiveManeuverDueToUncessaryAdvisory	Collision Avoidance System	Advisory	Algorithm	An inadequate avoidance advsisory leads to an unnecessary evasive maneuver advisory.	48.4.2 Ensure Collision Avoidance Correctness	true	A. Ahlbrecht	false

#	△ Name	Text	Documentation
1	48.3.3 Clear Instruction Priority	The instruction priority between the collision avoidance system and the traffic controller shall be clearly defined.	e.g. through training
2	48.4.2 Ensure Collision Avoidance Correctness	The collision avoidance algorithm correctness shall be ensured with verification and validation activities.	e.g. test cases, etc.

Advanced Application
Process Improvement – Assistance Functionality

- Automating error-prone tasks such as:
  - Creation of table elements, automatic V&V, and progress tracking through metrics

#	Name	Context	Context Value	Source	Control Action	Receiver	Not provided in this context	Provided in this context	Assessed	Analyst
1	STPA Element 0	*ModeChange*	No mode change wanted	Pilot	Mode Change	CAS		*Pilot is not aware of CAS state*	true	A. Ahlbrecht
2	STPA Element 1	*ModeChange*	Mode change wanted	Pilot	Mode Change	CAS	*Pilot is not aware of CAS state*		true	
3	STPA Element 2	*AdvisoryRequest* *IntruderPresent*	No advisory needed No intruder present	CAS	Advisory	Pilot		*Aircraft violates minimum seperation standards*	true	A. Ahlbrecht
4	STPA Element 3	*AdvisoryRequest* *IntruderPresent*	No advisory needed Intruder present	CAS	Advisory	Pilot		*Aircraft violates minimum seperation standards*	true	A. Ahlbrecht
5	STPA Element 4	*AdvisoryRequest* *IntruderPresent*	Advisory needed No intruder present	CAS	Advisory	Pilot	*Aircraft violates minimum seperation standards*	*Aircraft violates minimum seperation standards*	true	A. Ahlbrecht
6	STPA Element 5	*AdvisoryRequest* *IntruderPresent*	Advisory needed Intruder present	CAS	Advisory	Pilot	*Aircraft violates minimum seperation standards*		true	A. Ahlbrecht

#	Date	Scope	Amount of Analysis Elements	Amount of Assessed Analysis Elements	Percentage of Assessed Analysis Elements
1	2021.07.07 17.42	STPA Elements	6	6	100

Advanced Application
Process Improvement – Enabling Agility

ISSE Paper 22, © 2023 IEEE

Proactive application of analyses within agile model-based developments

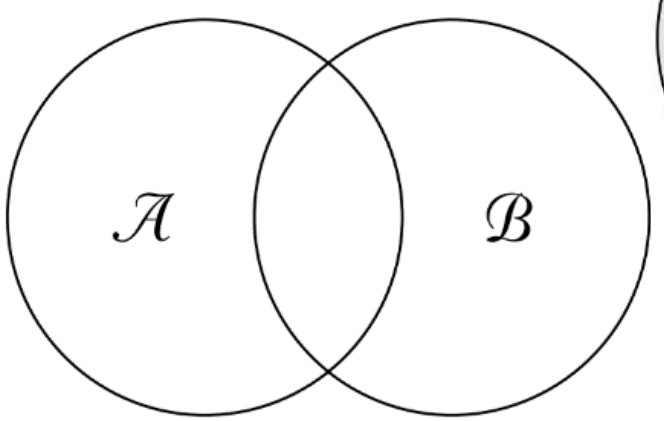
↳ **MBSE and STPA Integration**

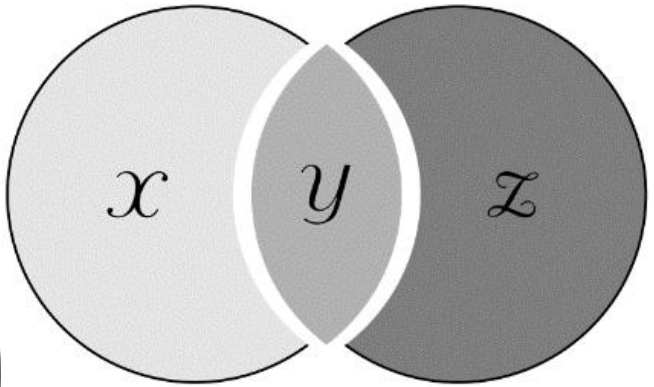
Traceability of design change impact towards safety artifacts

↳ **Safety Traceability**

	Requirements	Behavior	Structure	Parametrics	Safety
Problem	Stakeholder Needs	Use Cases Functional Analysis	System Context Logical Systems	Measure-ments of Effectiveness	Concept STPA
Solution	Solution Requirements	Solution Behavior	Solution Assembly	Solution Parameters	Solution STPA

$\mathcal{A}$ - RequiredElements
$\mathcal{B}$ - CurrentElements





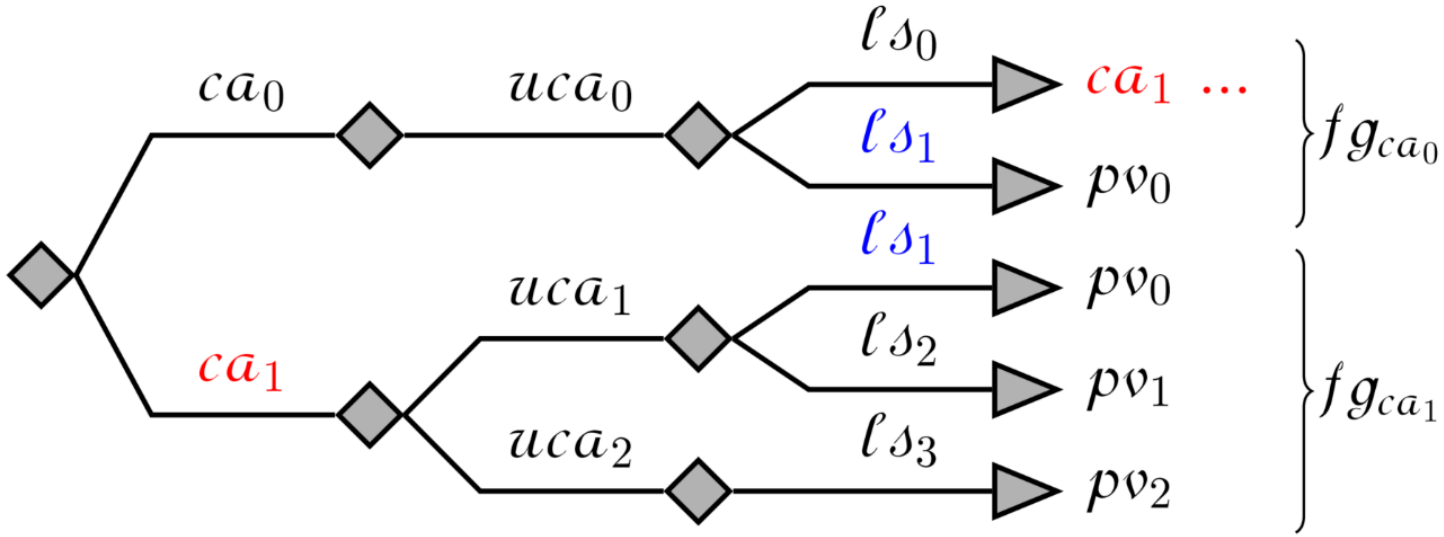
$\mathcal{X}$ - NewAndChangedElements
$\mathcal{Y}$ - StableElements
$\mathcal{Z}$ - OutdatedElements

Advanced Application

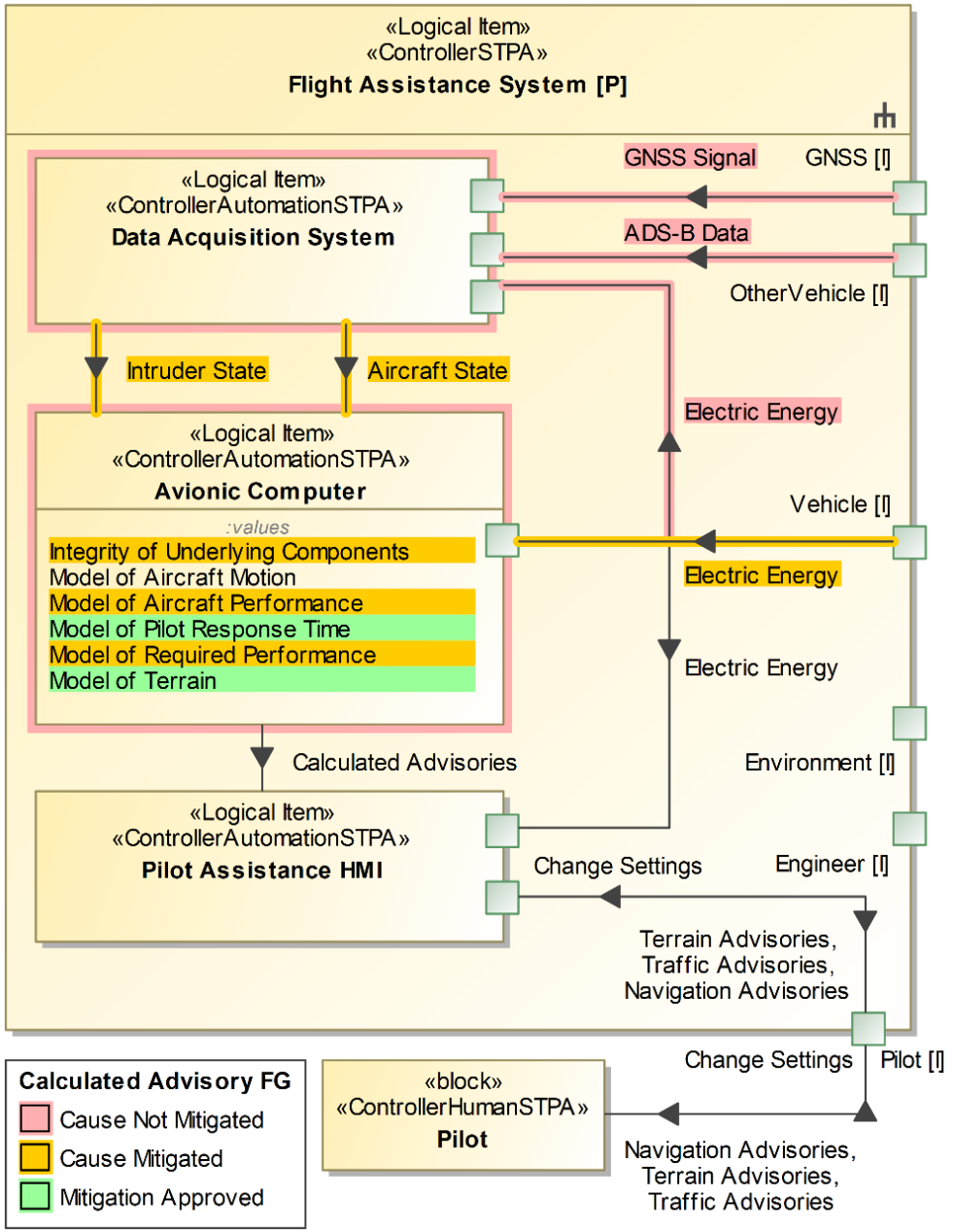
Process Improvement – Supporting Coverage

Supporting functionality to indicate sufficiency of the applied analyses

Coverage Assessment

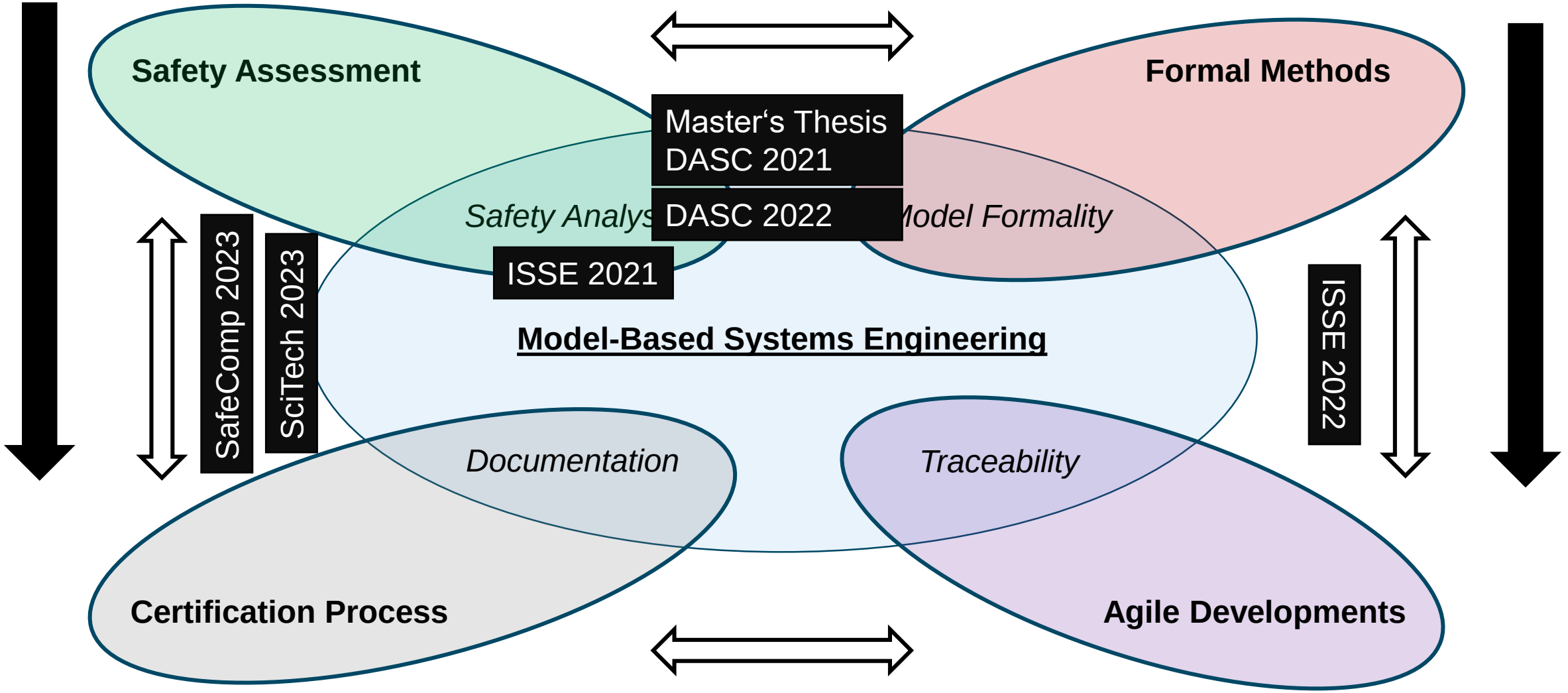


Control Action (CA) | Unsafe Control Action (UCA) | Loss Scenario (LS) | Causal Factor (CF)



Future Work, Discussion & Conclusion

Future Work



Future Work, Discussion & Conclusion

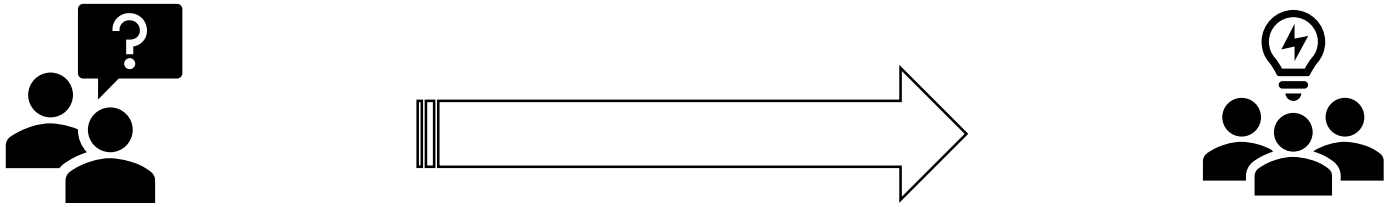
Discussing Limitations

Limitations

- Analysis only as good as the corresponding model
  - Thoughtful modeling required
- Automation inserts potential for failures
  - Failures in automation algorithm
  - Automation requires formal structure
  - Too much reliance on automation

Managing Limitations

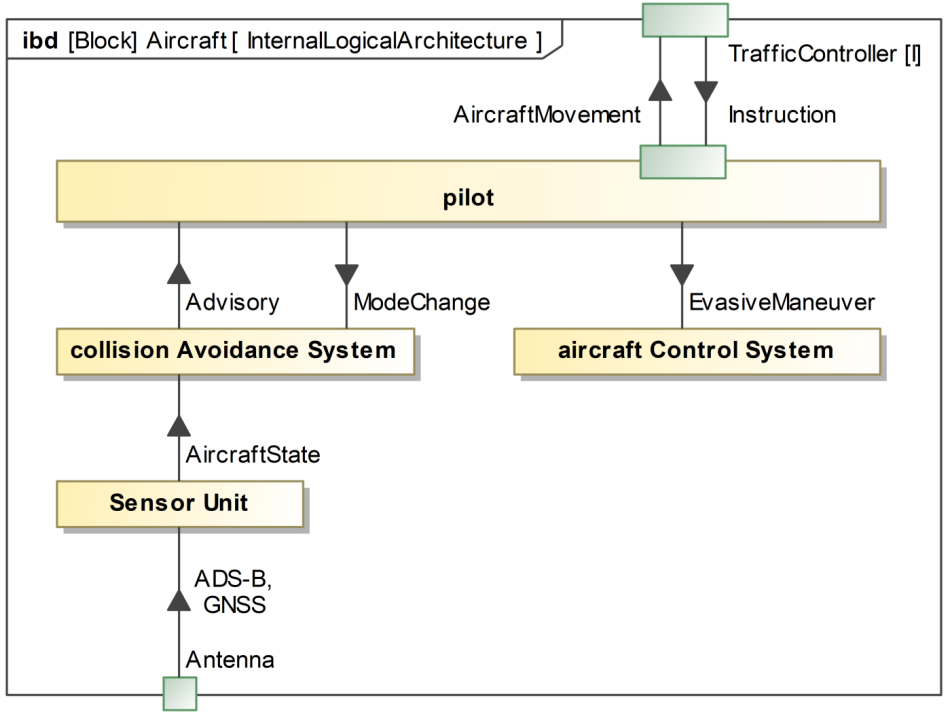
- Follow systematic MBSE framework
- Explicit analysis of underlying model
- Implementing a qualified profile
- Clear training of automation usage
- Explicit analysis of provided information



Future Work, Discussion & Conclusion

Discussing Limitations

- Reuse of development model for model-based STPA?
  - Potential Issues due to control-structure paradigm of STPA:
    - Object-oriented vs. control-oriented view
    - Leverages detailed process models
    - Abstraction with a purpose
- Learnings:
  - Experience is required to model the control-structure in the right form
  - Process model needs to be described
  - Abstraction needs to be monitored



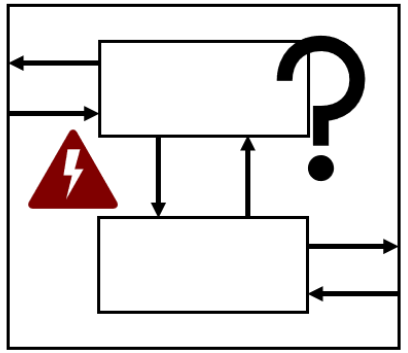
PSASS Materials

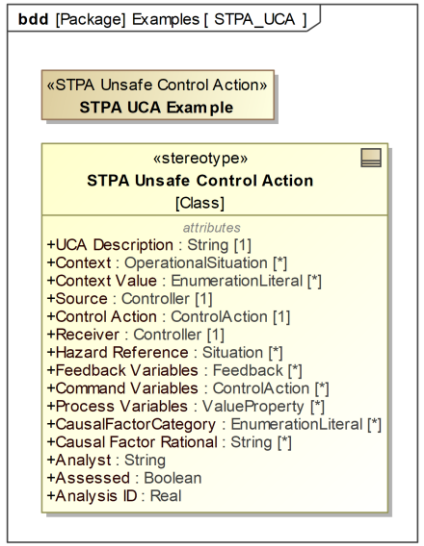
Discussion and Conclusion

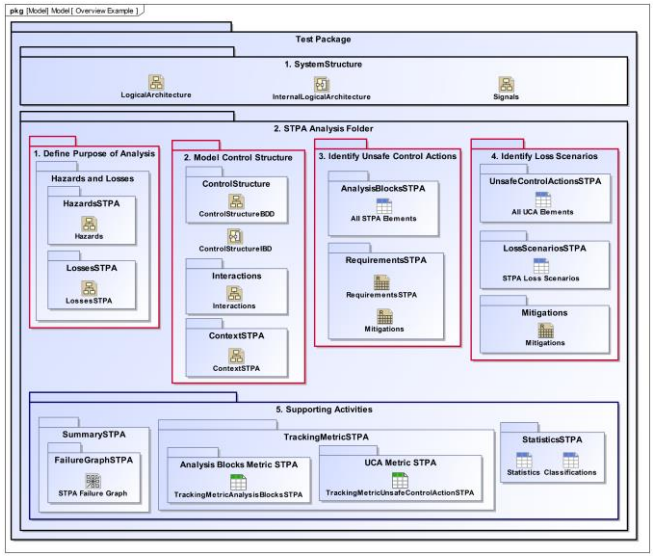
Conclusion

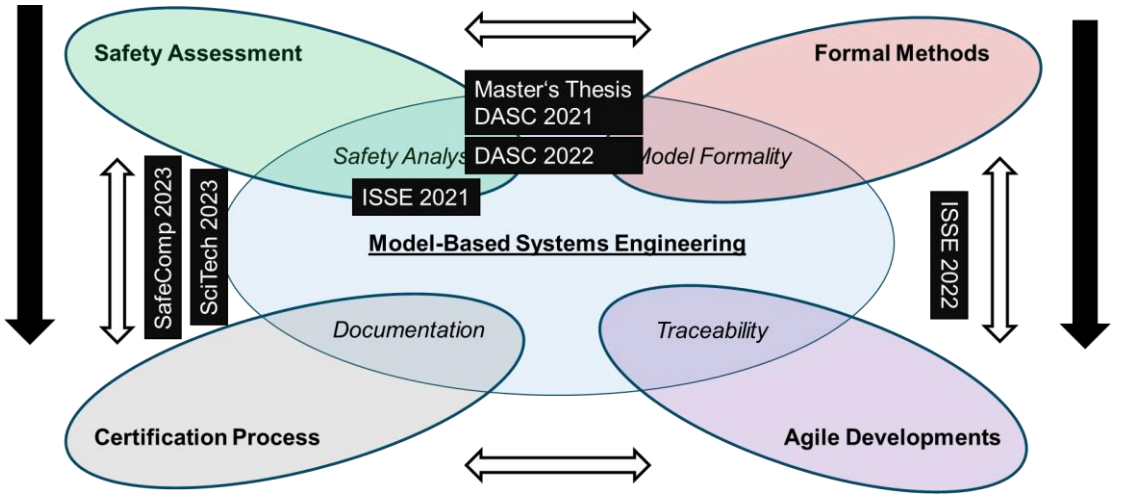
1. Define Purpose of Analysis
2. Model Control Structure
3. Identify Unsafe Control Actions
4. Identify Loss Scenarios

Define: Losses, Hazards, System Boundary, and Environment









References

Used Tag	Corresponding Source Link
MagicGrid Book	https://discover.3ds.com/magicgrid-book-of-knowledge
STPA Introduction	http://psas.scripts.mit.edu/home/wp-content/uploads/2019/03/JThomas-STPA-Intro.pdf
Economic Analysis of MBSE	https://www.mdpi.com/2079-8954/7/1/12
Engineering A Safer World	https://mitpress.mit.edu/books/engineering-safer-world
STPA Handbook	http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
PhD Thesis John Thomas	http://sunnyday.mit.edu/JThomas-Thesis.pdf
Stanford Lecture CS 357	https://stanford.edu/class/cs357/
SysML v2 Github	https://github.com/Systems-Modeling/SysML-v2-Release
RAAML Spec	https://www.omg.org/spec/RAAML/1.0/Beta1/About-RAAML/
PSASS	http://psas.scripts.mit.edu/home/materials/

*hyperlinks are attached

Own References

[Integrating Safety into MBSE]

[Master‘s Thesis] (German)

[Early Architecture Safety Evaluation]

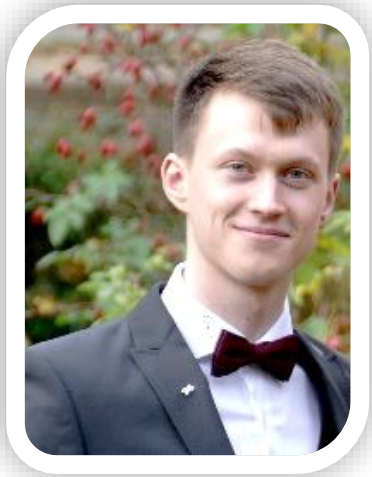
[Towards Safety Coverage]

[Agile Safety-Guided Design]

Copyright Information

DASC Paper 21, Slides: 20, 26	© 2023 IEEE. Reprinted, with permission, from Integrating Safety into MBSE Processes with Formal Methods.
ISSE Paper 22 , Slides: 21	© 2023 IEEE. Reprinted, with permission, from Model-Based STPA: Towards Agile Safety-Guided Design with Formalization.
DASC Paper 22 , Slides: 22	© 2023 IEEE. Reprinted, with permission, from Model-Based STPA: Enabling Safety Analysis Coverage Assessment with Formalization.
DLR Images, Slides: 2, 15, 26	© DLR, CC BY-NC-ND 3.0
DLR Logo	© DLR, CC BY-NC-ND 3.0

Any Questions, Comments, or Suggestion?



LinkedIn GoogleScholar Researchgate

Alexander Ahlbrecht, Scientific Associate,
German Aerospace Center (DLR)
Alexander.Ahlbrecht@dlr.de