34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Elizabeth Pennington, Kip Johnson, PhD, John Colombi, PhD, Kerianne Hobbs, PhD

Integrating STPA-Coordination Into SysML Using RAAML

Acknowledgements

AFIT
AIR FORCE INSTITUTE OF TECHNOLOGY

DIGITAL INNOVATION & INTEGRATION CENTER OF EXCELLENCE (DIICE)

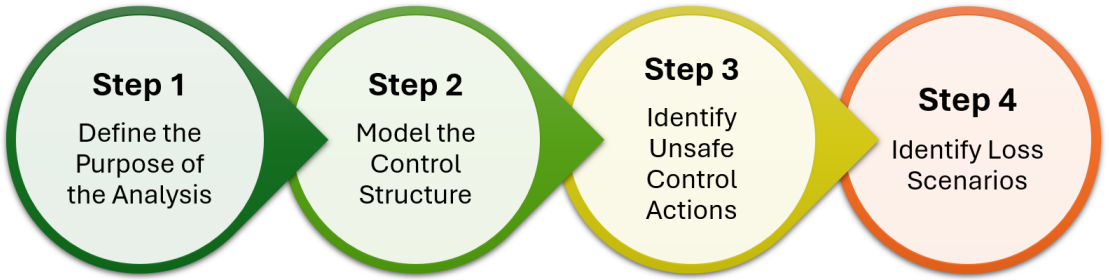
Acknowledgements

The views expressed in this presentation are those of the presenter and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

Background

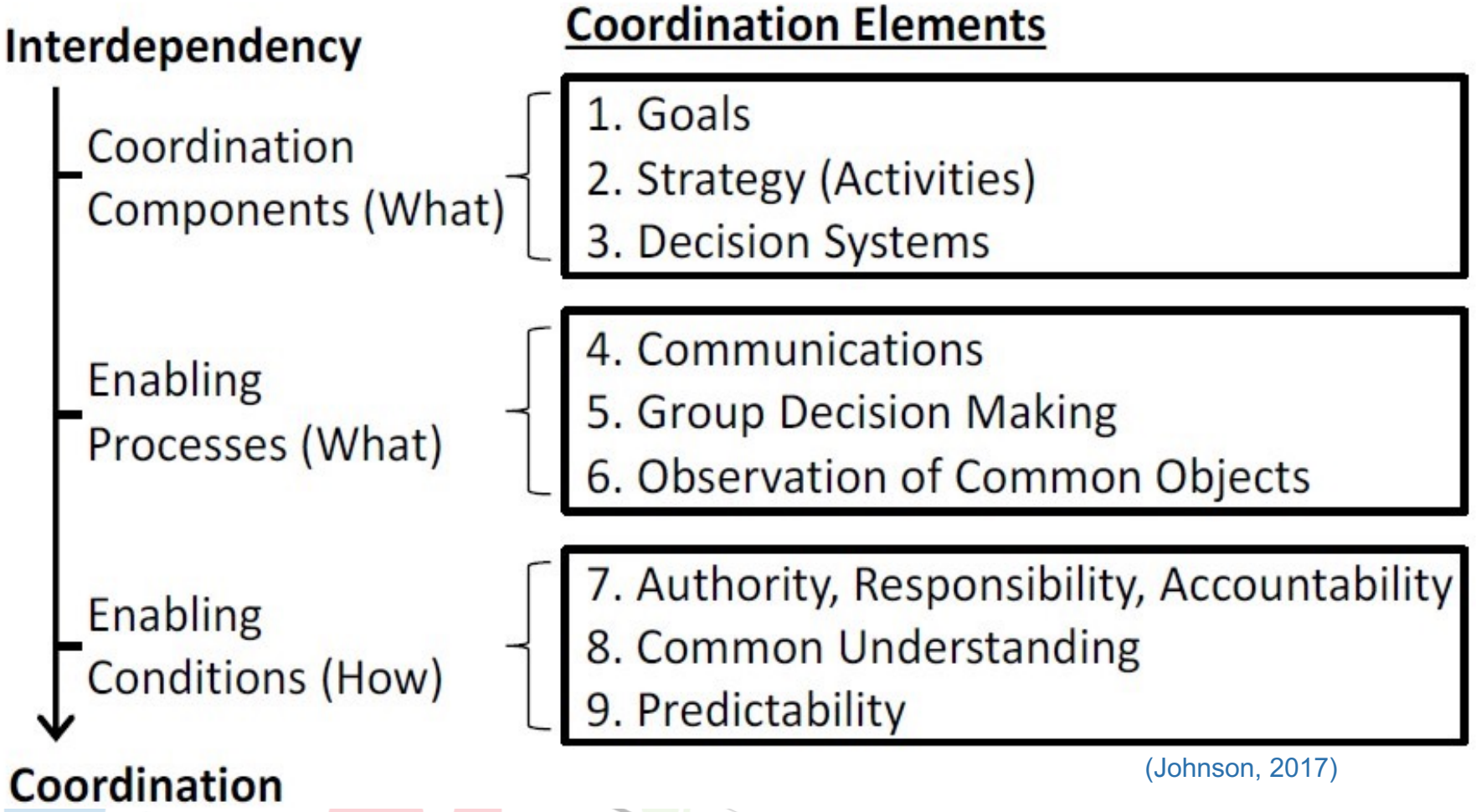
STPA Extended for Coordination (STPA-Coord)

- Safety and hazard analysis method using Systems Theory and model abstraction to analyze coordination between decision-makers for system-of-systems architectures
  - (Johnson, 2017; Leveson, 2012)
- Based on parent method, Systems Theoretic Process Analysis (STPA)
  - (Leveson, 2012)
- Coordination ≠ communication
  - (Johnson, 2017)



(Adapted from Leveson & Thomas, 2018)

STPA-Coord Coordination Elements



(Johnson, 2017)

MBSE for STPA-Coord

2019

- Various analysts used Systems Modeling Language (SysML) to supplement STPA analyses through behavioral diagrams
  - (Hurley &Wankel, 2019; de Souza et al. 2020; Zhong et. al., 2022)

~2021

- SysML co-creators began beta testing a SysML extension for safety analyses called **Risk Analysis and Assessment Modeling Language (RAAML)**
  - (Object Management Group, 2021)

2021-2022

- Ahlbrecht et al. used RAAML as a baseline to formalize requirement generation, validation, verification
  - (Ahlbrecht et al., 2022; Ahlbrecht & Bertram, 2021; Ahlbrecht & Durak, 2021, 2022)

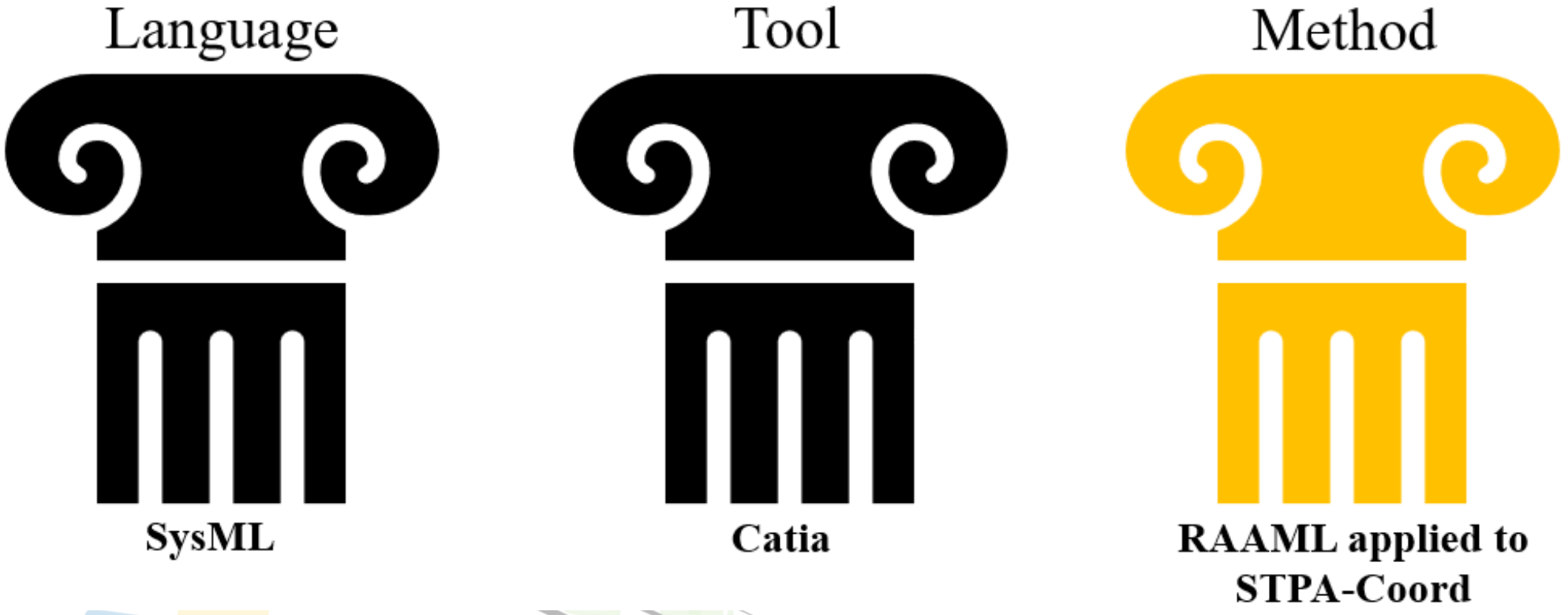
2023

- Object Management Group (OMG) published RAAML for use
  - (Object Management Group, 2023)

RAAML for STPA

a. Set of SysML packages providing elements for safety analyses
    a. STPA, FTA, FTEA, GSN
b. Supplemental guidance for STPA elements
    a. Brief guidance for how to use elements
    b. 6 pages, 10 images
        a. “Risk Analysis and Assessment Modeling Language (RAAML) Examples (Informative)” (OMG, 2021)

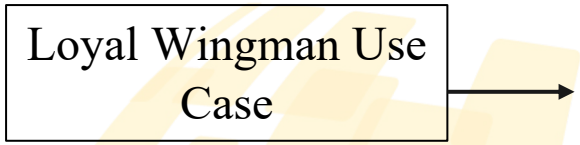
Research Objective



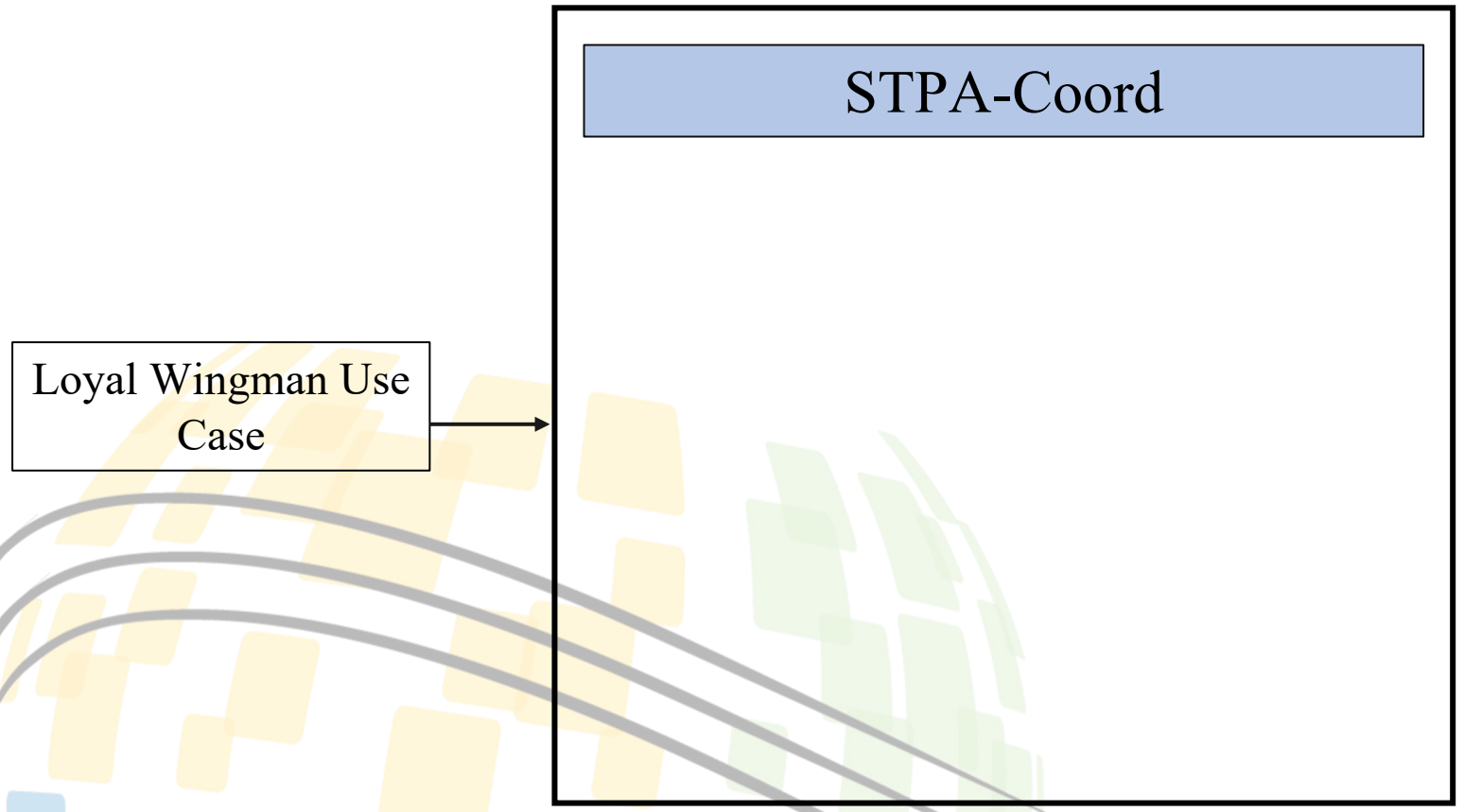
(Inspired by Delligati (2014))

Methodology

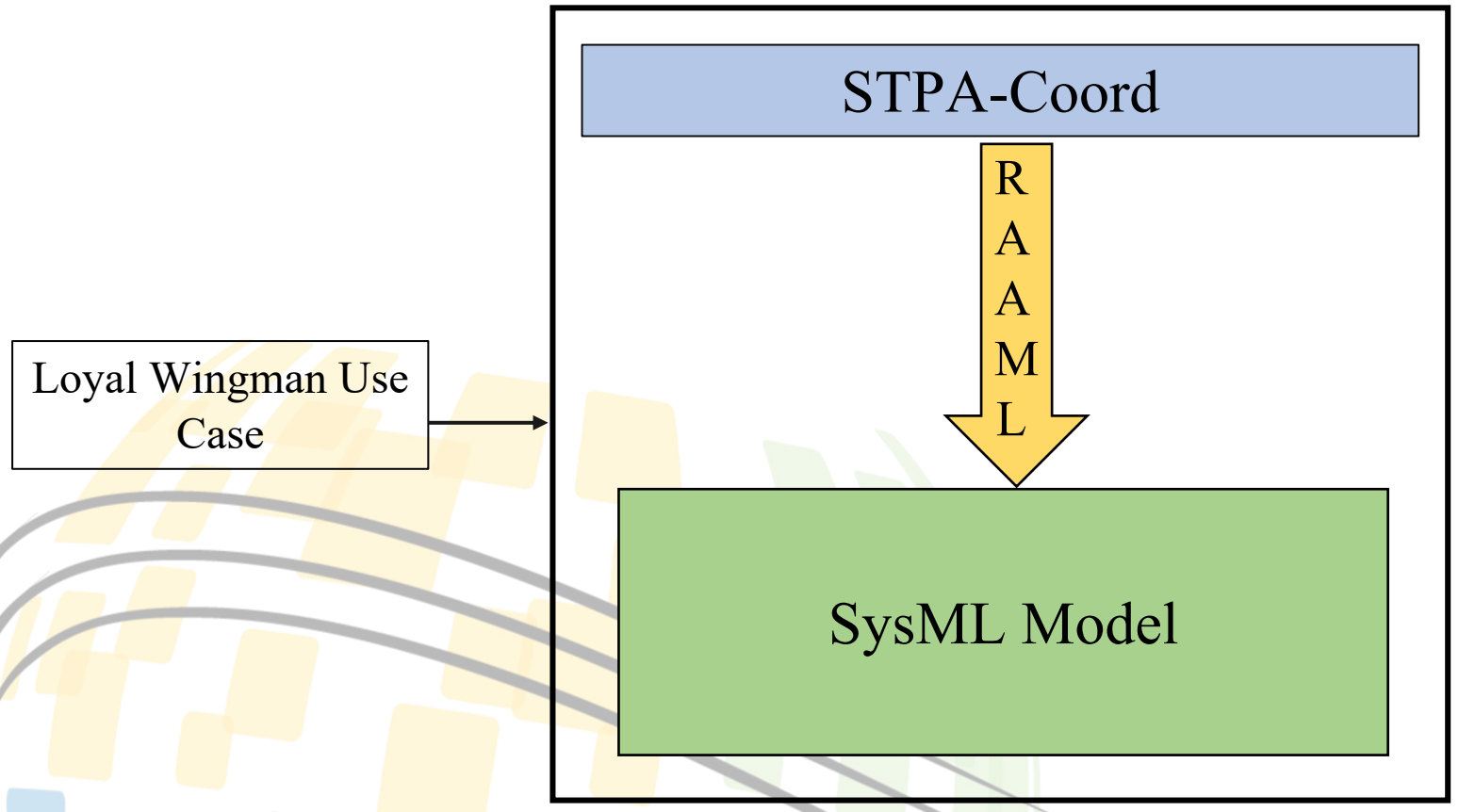
Methodology



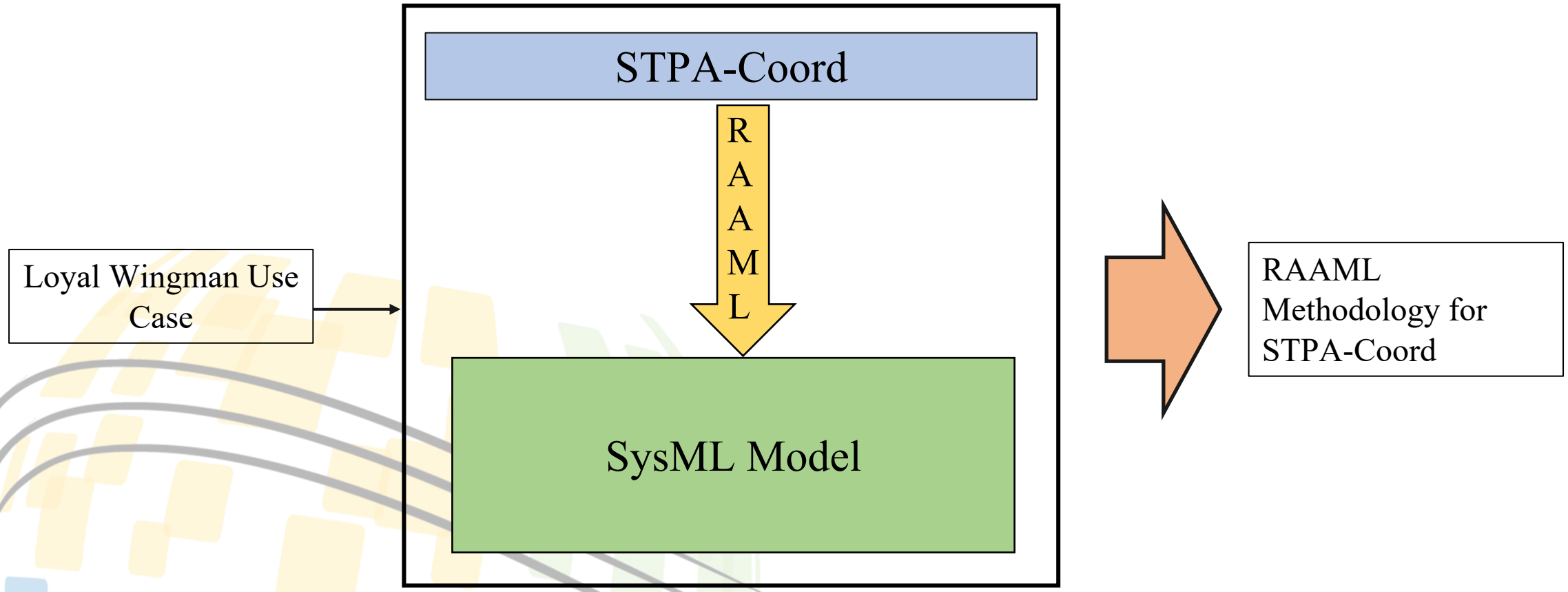
Methodology



Methodology



Methodology

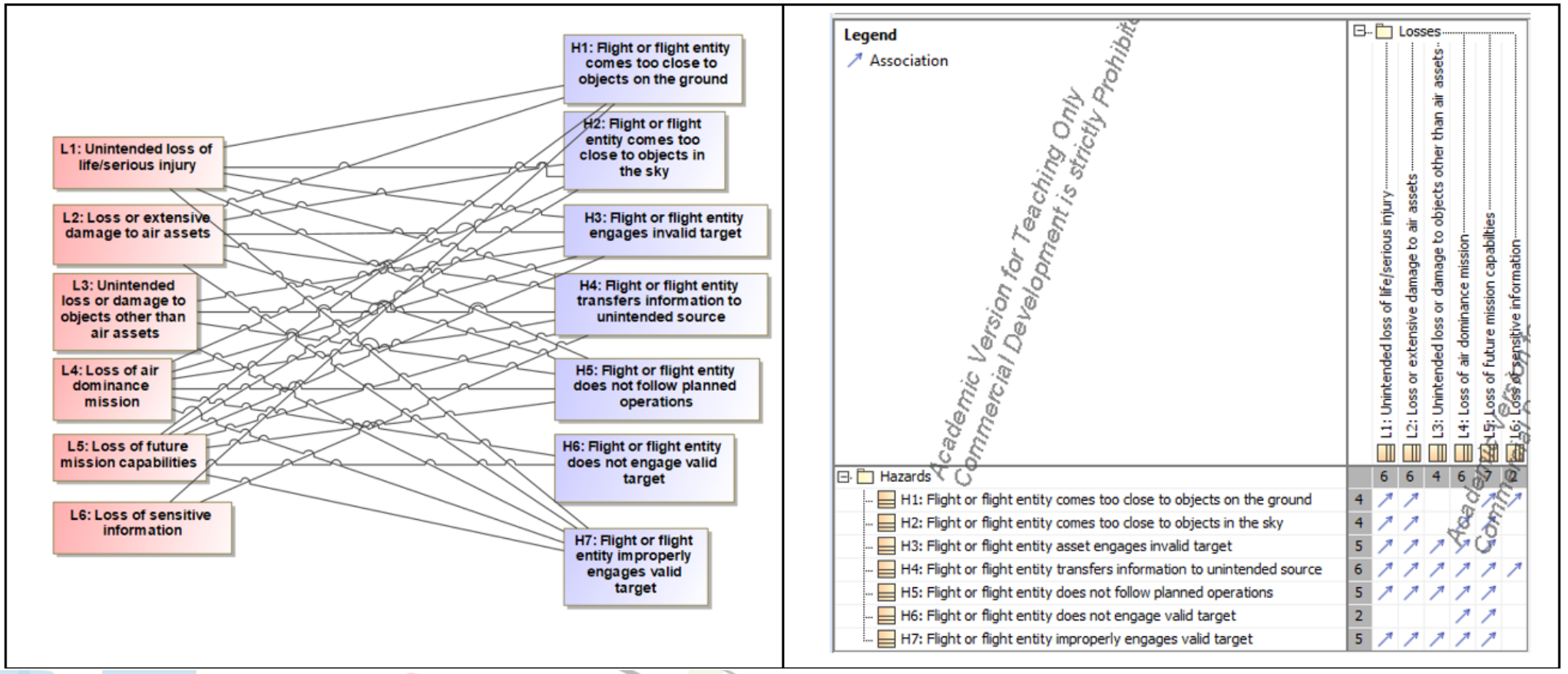


Results

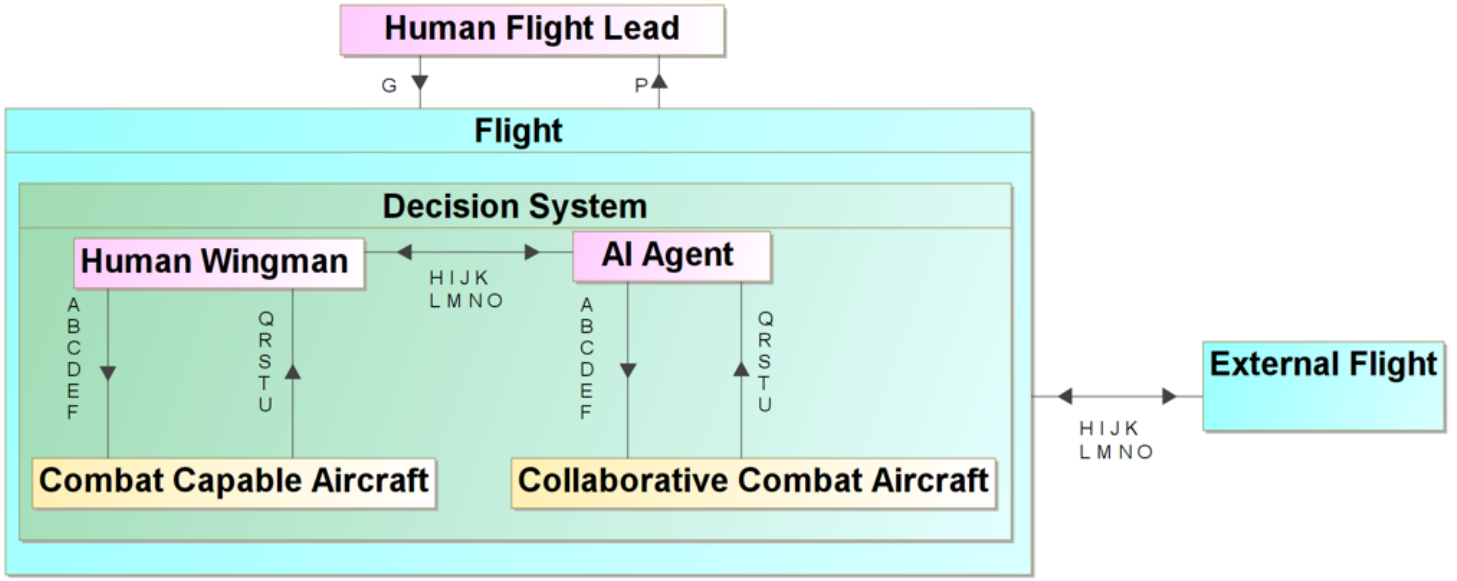
Results

STPA Element	Associated STPA Step	SysML Diagram (RAAML)	SysML Diagram (Proposed)
Losses and Hazards	Step 1	Block Definition Diagram	Block Definition Diagram
Loss/Hazard Relations	Step 1	Internal Block Diagram	Dependency Matrix
Control Structure	Step 2	Internal Block Diagram	Internal Block Diagram
Unsafe Control Actions	Step 3	Block Definition Diagram/Generic Table	Generic Table
Unsafe Control Action/Hazard Relations	Step 3	Internal Block Diagram	Generic Table
Loss Scenarios	Step 4	Block Definition Diagram	Generic Table

Step 1: Define the Purpose of the Analysis

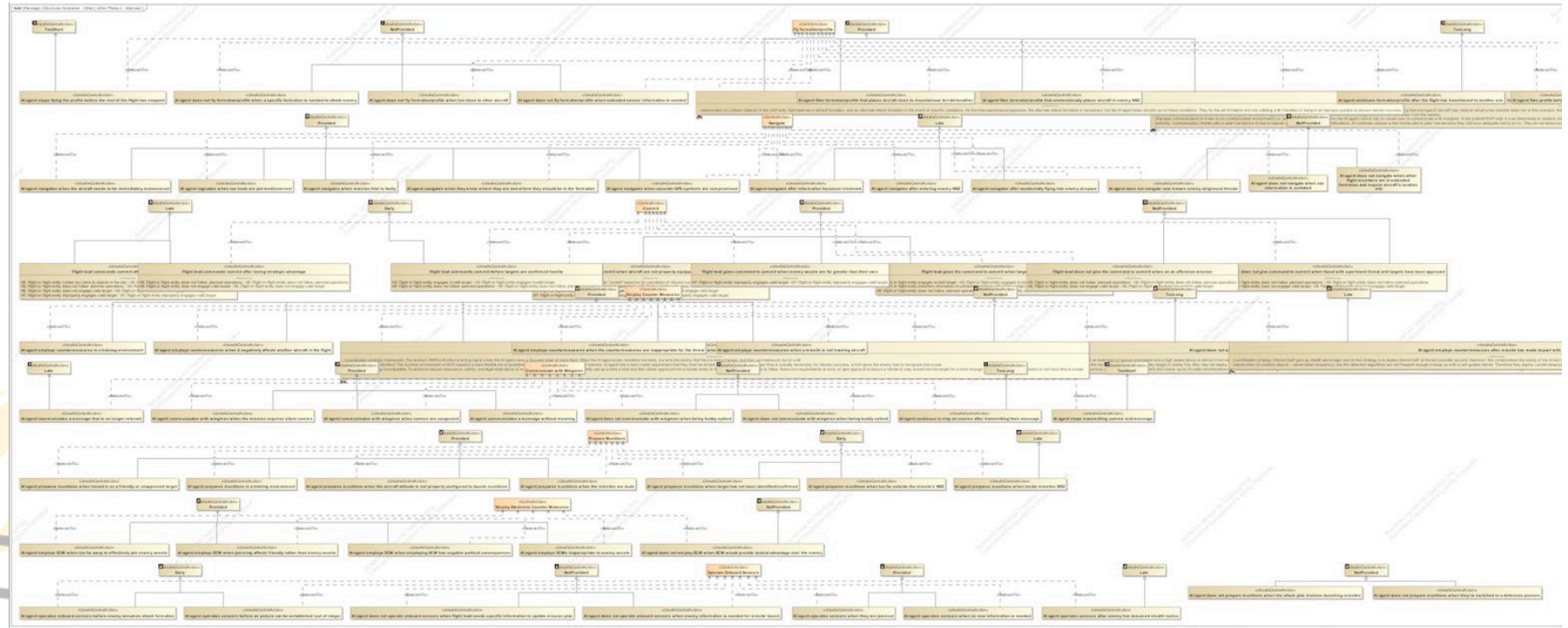


Step 2: Model the Control Structure



Control Actions	Coordination Details	Feedback
A: Communicate with Wingmen	H: Current/Adjusted Attack Plan	P: Compliance
B: Fly Formation/Profile	I: Select Targets	Q: Enemy Location/Status
C: Navigate	J: Abort? Y/N	R: Munition Status
D: Operate Sensors	K: Reattack? Y/N	S: A/C Health
E: Employ Countermeasures	L: Launch Timing	T: Location
F: Launch Missile	M: Communicate? Y/N	U: A/C Attitude
G: Commit	N: Determine Formation/Profile	
	O: Buddy Spike	

Step 3: Identify Unsafe Control Actions

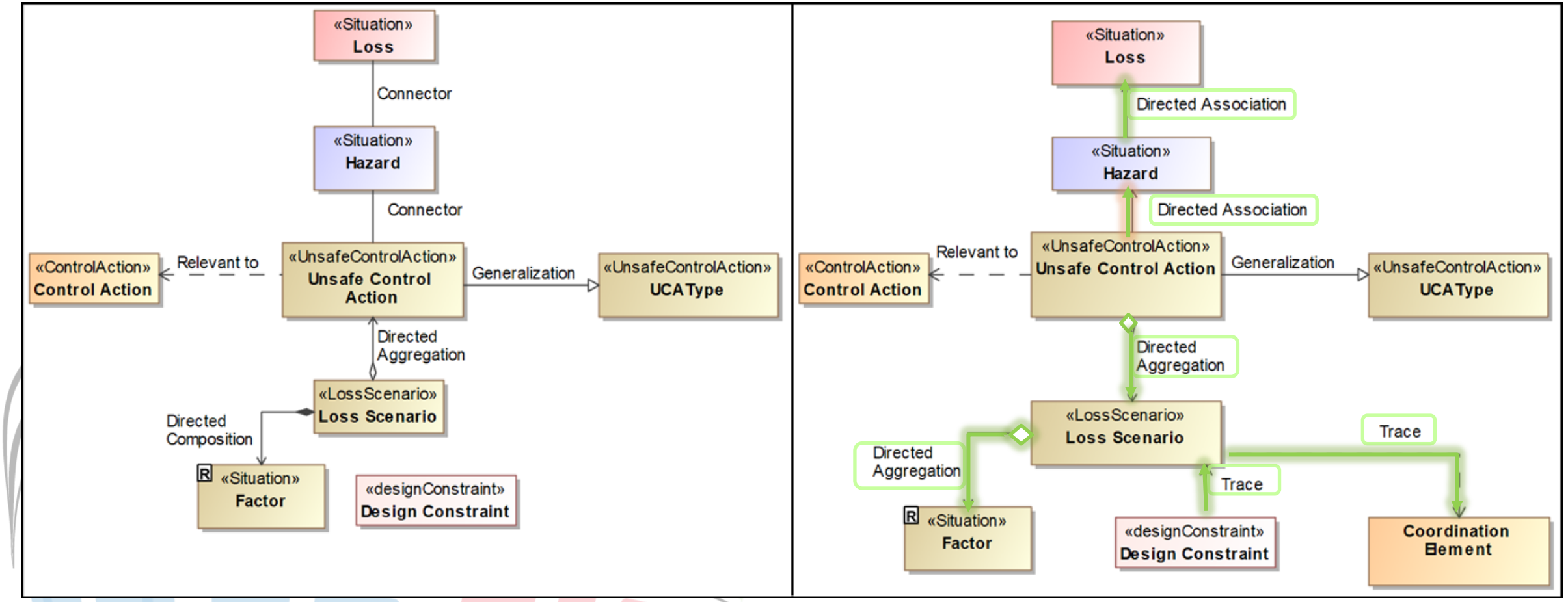


#	Control Action	Type	Name	Related Hazards
1	Launch Missile	NotProvided	AI agent does not launch missile when ordered to hit a target	H6: Flight or flight entity does not engage valid target H5: Flight or flight entity does not follow planned operations
2	Launch Missile	NotProvided	AI agent does not launch missile when they decide to hit a target	H5: Flight or flight entity does not follow planned operations H6: Flight or flight entity does not engage valid target
3	Launch Missile	NotProvided	AI agent does not launch missile when they need to defend themselves, their team, or other assets	H5: Flight or flight entity does not follow planned operations H6: Flight or flight entity does not engage valid target H2: Flight or flight entity comes too close to objects in the sky
4	Launch Missile	Late	AI agent launches missile after strike window passes	H3: Flight or flight entity engages invalid target H5: Flight or flight entity does not follow planned operations H6: Flight or flight entity does not engage valid target
5	Launch Missile	Early	AI agent launches missile before approved to strike target	H5: Flight or flight entity does not follow planned operations H3: Flight or flight entity engages invalid target

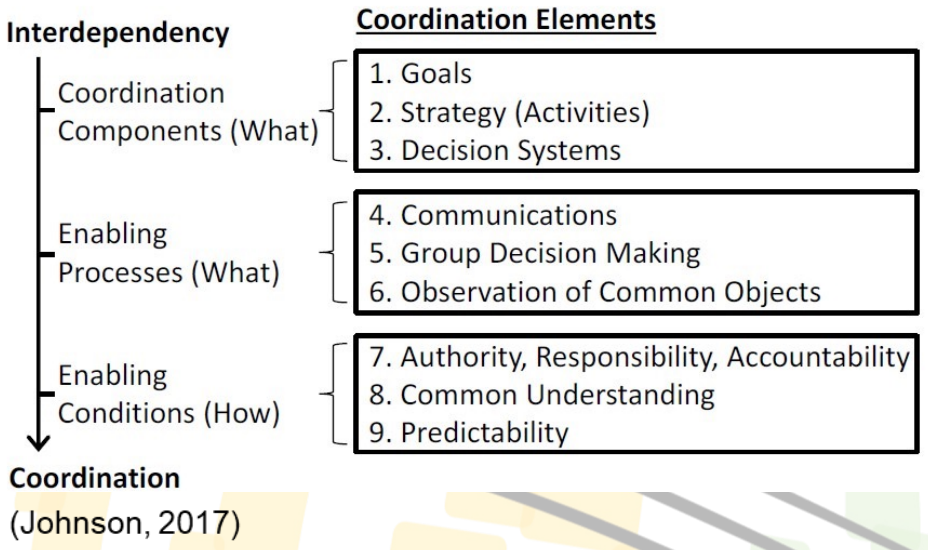
Step 4: Identify Loss Scenarios

#	Associated UCA	Name	Potential Factors	Design Considerations	△ Related Coordination Elements
1	AI agent does not launch missile when ordered to hit a target	AI prioritizes their sight picture more than the flight lead's authority.	Flight lead has an "authoritatve" and "peer" role given the nature of BVR. AI believes "launch" command is coming from their wingman as a peer AI doesn't have a framework to determine which commands are "mandatory" and which the AI has autonomy to accept or reject Gaining an accurate picture of the airspace takes too much of the AI's bandwidth to receive other information	R 1 Missile Launch Protocol R 52 Flight Lead Authority R 53 Authority Communication	Authority, Responsibility, Accountability

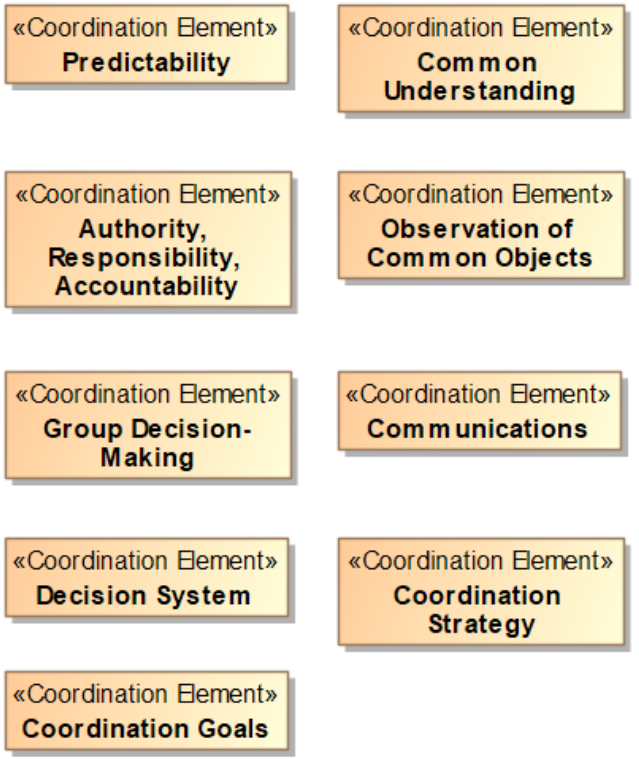
Relationship Mapping



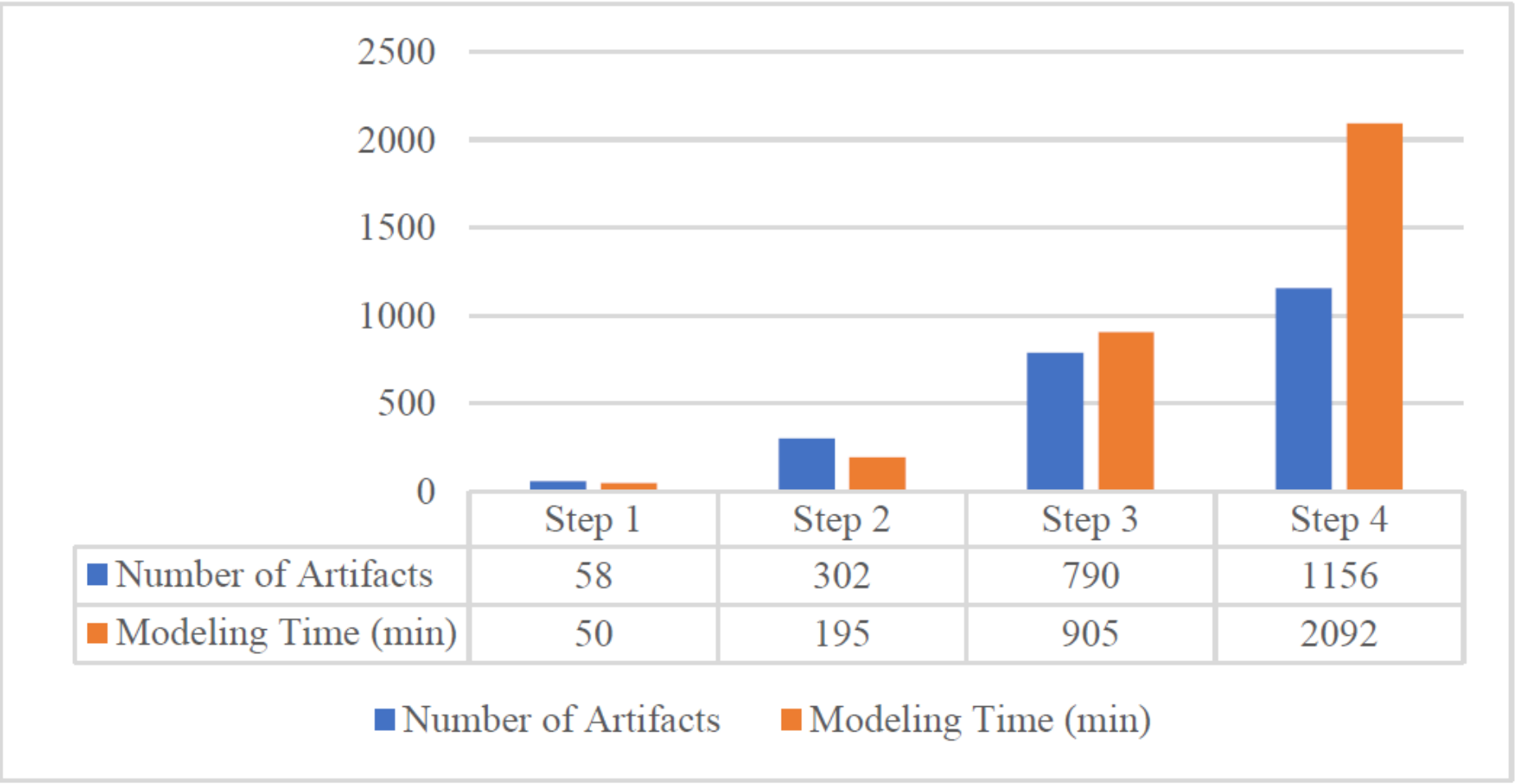
Coordination Elements in SysML



(Johnson, 2017)

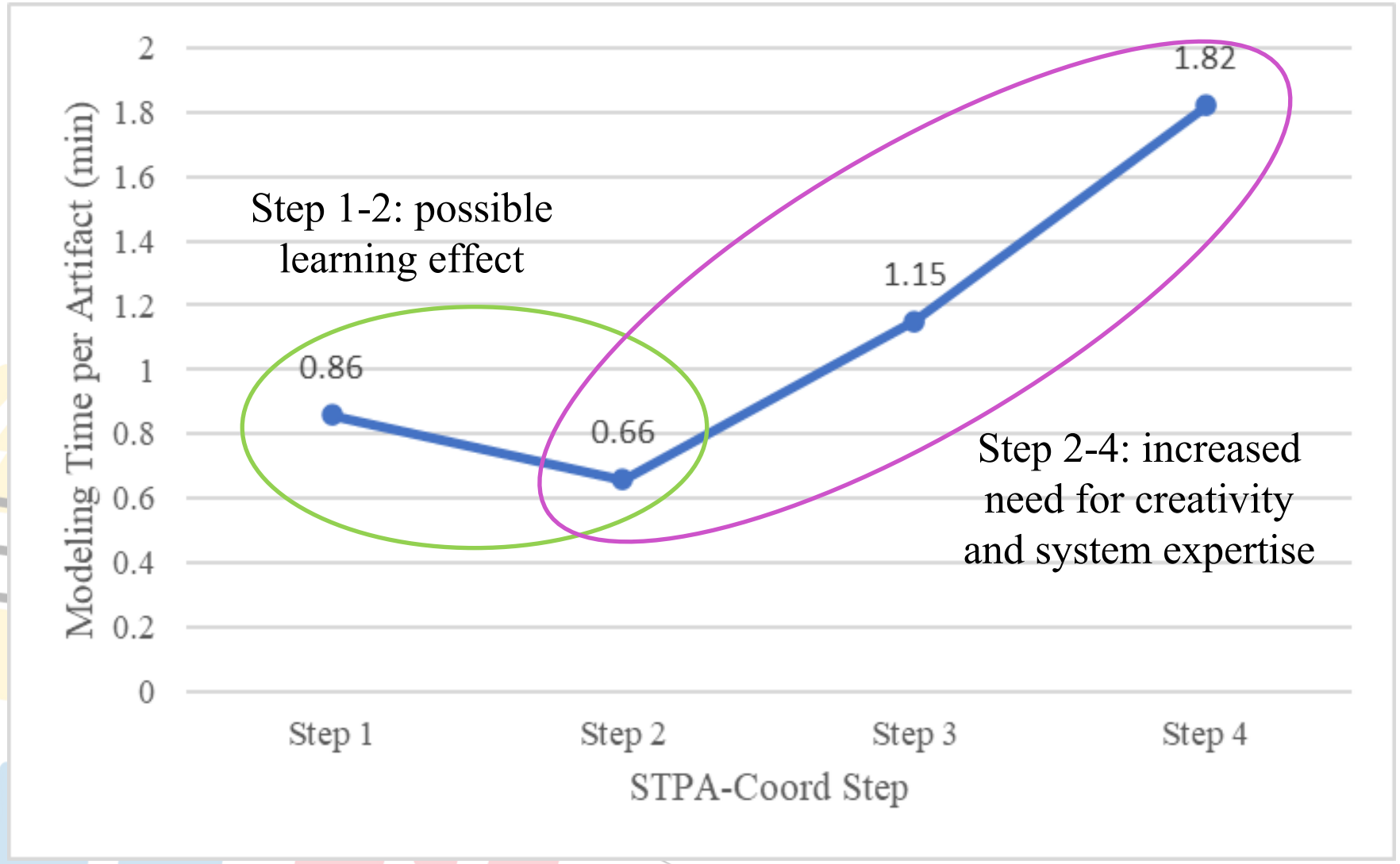


Time Required to Model



Total:
54 hours

Modeling Time per Artifact



Observed Benefits of MBSE for STPA-Coord

Analysis Verification	Authoritative Source of Truth	Display Flexibility
Traceability	Multi-capable Tool	Element Modularity
	Ease of Iteration	
	*Cloud Capabilities	

*Perceived Capability

Future Work

- More STPA-Coord analyses in SysML
- Extend RAAML for other STPA extensions
- Merge STPA-Coord analysis into existing MBSE model for the same system

Questions?

References

- N. Leveson and J. Thomas, “STPA Handbook,” https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. pp. 1–188, 2018.
- K. E. Johnson, “Systems-Theoretic Safety Analyses Extended for Coordination,” S.M. Aeronauts and Astronautics, 2017.
- Department of Defense, “DoD Instruction 5000.97 Digital Engineering,” 2023. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500097p.PDF?ver=bePIqKXaLUTK_Iu5iTNREw%3D%3D
- N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press, 2012.
- F. G. R. de Souza, J. de Melo Bezerra, C. M. Hirata, P. de Saqui-Sannes, and L. Apvrille, “Combining STPA with SysML modeling,” in SYSCON 2020 - 14th Annual IEEE International Systems Conference, Proceedings, 2020. doi: 10.1109/SysCon47679.2020.9275867.
- A. Ahlbrecht and O. Bertram, “Evaluating System Architecture Safety in Early Phases of Development with MBSE and STPA,” in ISSE 2021 - 7th IEEE International Symposium on Systems Engineering, Proceedings, Institute of Electrical and Electronics Engineers Inc., Sep. 2021. doi: 10.1109/ISSE51541.2021.9582542.
- A. Ahlbrecht, W. Zaeske, and U. Durak, “Model-Based STPA: Towards Agile Safety-Guided Design with Formalization,” in ISSE 2022 - 2022 8th IEEE International Symposium on Systems Engineering, Conference Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ISSE54508.2022.10005396.
- A. Ahlbrecht and U. Durak, “Model-Based STPA: Enabling Safety Analysis Coverage Assessment with Formalization,” in AIAA/IEEE Digital Avionics Systems Conference - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/DASC55683.2022.9925883.
- M. Hurley and J. Wankel, “Safety Guided Design Using STPA and Model Based System Engineering (MBSTPA),” 2019.
- “Risk Analysis and Assessment Modeling Language Examples (Informative).” Object Management Group, pp. 10–16, Nov. 03, 2021.
- A. Ahlbrecht and U. Durak, “Integrating Safety into MBSE Processes with Formal Methods,” in AIAA/IEEE Digital Avionics Systems Conference - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/DASC52595.2021.9594315.
- “ABOUT THE RISK ANALYSIS AND ASSESSMENT MODELING LANGUAGE SPECIFICATION VERSION 1.0,” OMG Standards Development Organization, Apr. 2023. https://www.omg.org/spec/RAAML/1.0/About-RAAML (accessed Apr. 19, 2023).
- K. X. Campo, T. Teper, C. E. Eaton, A. M. Shipman, G. Bhatia, and B. Mesmer, “Model-based systems engineering: Evaluating perceived value, metrics, and evidence through literature,” *Systems Engineering*, vol. 26, no. 1. John Wiley and Sons Inc, pp. 104–129, Jan. 01, 2023. doi: 10.1002/sys.21644.
- K. Henderson and A. Salado, “Value and benefits of model-based systems engineering (MBSE): Evidence from the literature,” *Systems Engineering*, vol. 24, no. 1. John Wiley and Sons Inc, pp. 51–66, Jan. 01, 2021. doi: 10.1002/sys.21566.
- A. M. Madni and S. Purohit, “Economic analysis of model-based systems engineering,” *Systems*, vol. 7, no. 1, Mar. 2019, doi: 10.3390/systems7010012.
- “MBSE Initiative,” *INCOSE*. https://www.incose.org/incose-member-resources/working-groups/transformational/mbse-initiative#:~:text=MBSE%20is%20the%20formalized%20application,and%20later%20life%20cycle%20phases. (accessed May 22, 2023).

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS