Considerations for Cyber-Physical Design Teams Tasked with Engineering Safe and Secure Systems for a Notional Electrified Aircraft Concept

Martin "Trae" Span[1], Logan Mailloux[2], **Jeremy Daily**[1]

[1]Colorado State University, [2]Naval Postgraduate School

Fort Collins, CO, USA; Monterrey, CA, USA

Overview

Motivation

Background

Root Cause Analysis

Considerations for CPS Design Teams

Conclusion and Future Work

References

Motivation

https://www.google.com/url?sa=i&url=https%3A%2F%2Ftwitter.com%2Fjosephsteinberg%2Fstatus%2F1091363160446169092%3Flang%3Dhu&psig=AOvVaw0Mg37O-AIUgSDK7edFPACJ&ust=1666637222730000&source=images&cd=vfe&ved=0CA4QjhxqFwoTCIjlyM6B9_oCFQAAAAAdAAAAABAi

https://www.balbix.com/blog/top-10-cybersecurity-memes/

https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.lanworks.com%2Fcyber-attack-ransomware-emergency-response%2F&psig=AOvVaw3cyi5WY0kV6KRS9nE2FFBe&ust=1666637129764000&source=images&cd=vfe&ved=0CA4QjhxqFwoTCLjZpKKB9_oCFQAAAAAdAAAAABAE

Background

Systems Thinking Foundations:

- Peter Senge *Fifth Discipline* [13]
- Donnella Meadows *Thinking in Systems: A Primer* [9]

Content from Colorado State University Systems Thinking Course [14]

- Key Systems Thinking Principles
  - Emergent Properties of systems – Failure of reductionist approach to complex system design

Essential Terminology:

- **Safety** is freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. As adapted from MIL-STD-882E and the NASA Safety Handbook [14].

- **Security** is freedom from those conditions that can cause death, injury, or occupational illness; damage to or loss of equipment or property; damage to the environment; damage or loss of data or information; or damage to or loss of capability, function, or process. According to NIST SP 800-160, volume 1 [15].

CPS Design Team Current State Systems Dynamics Model

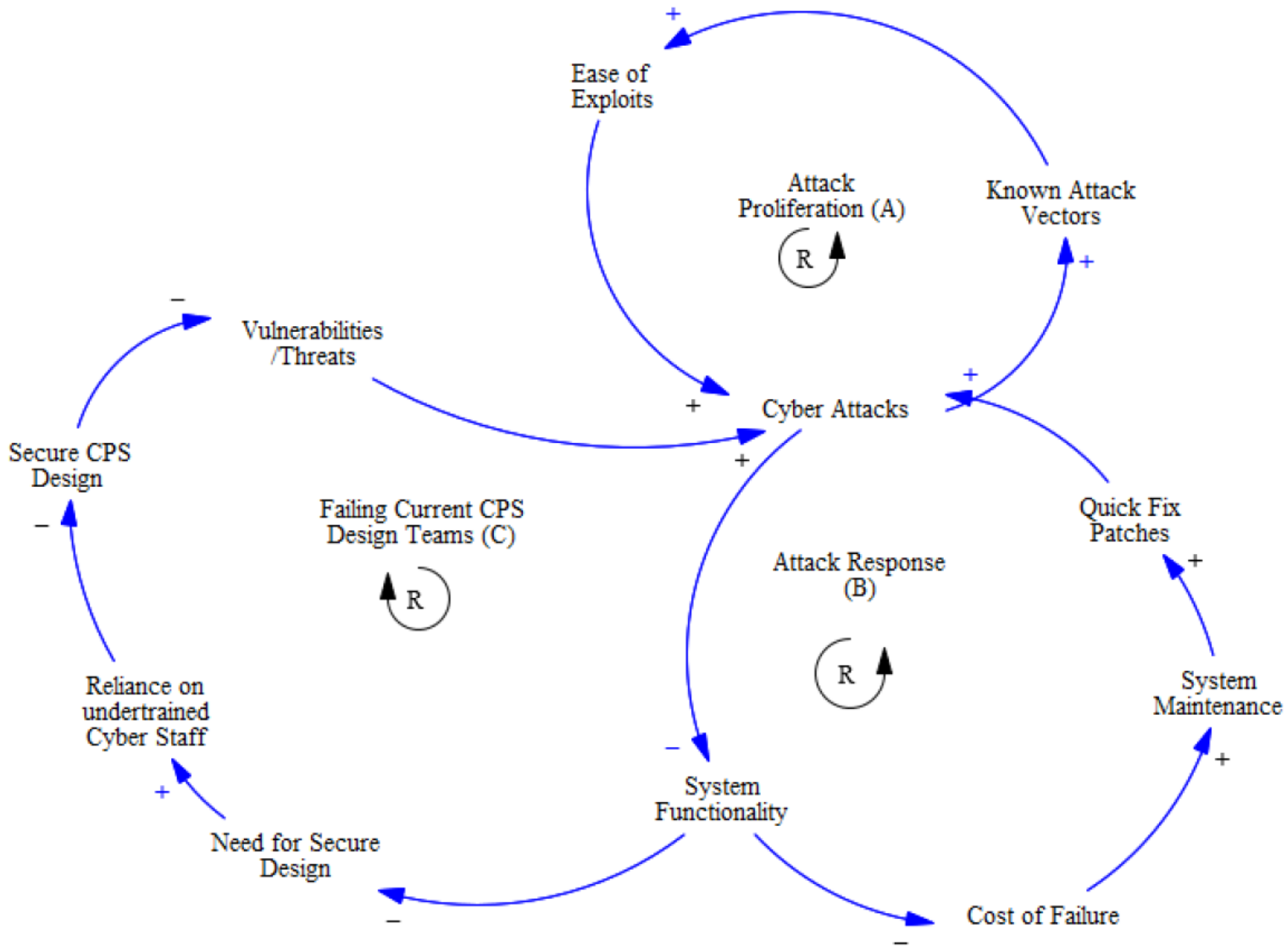
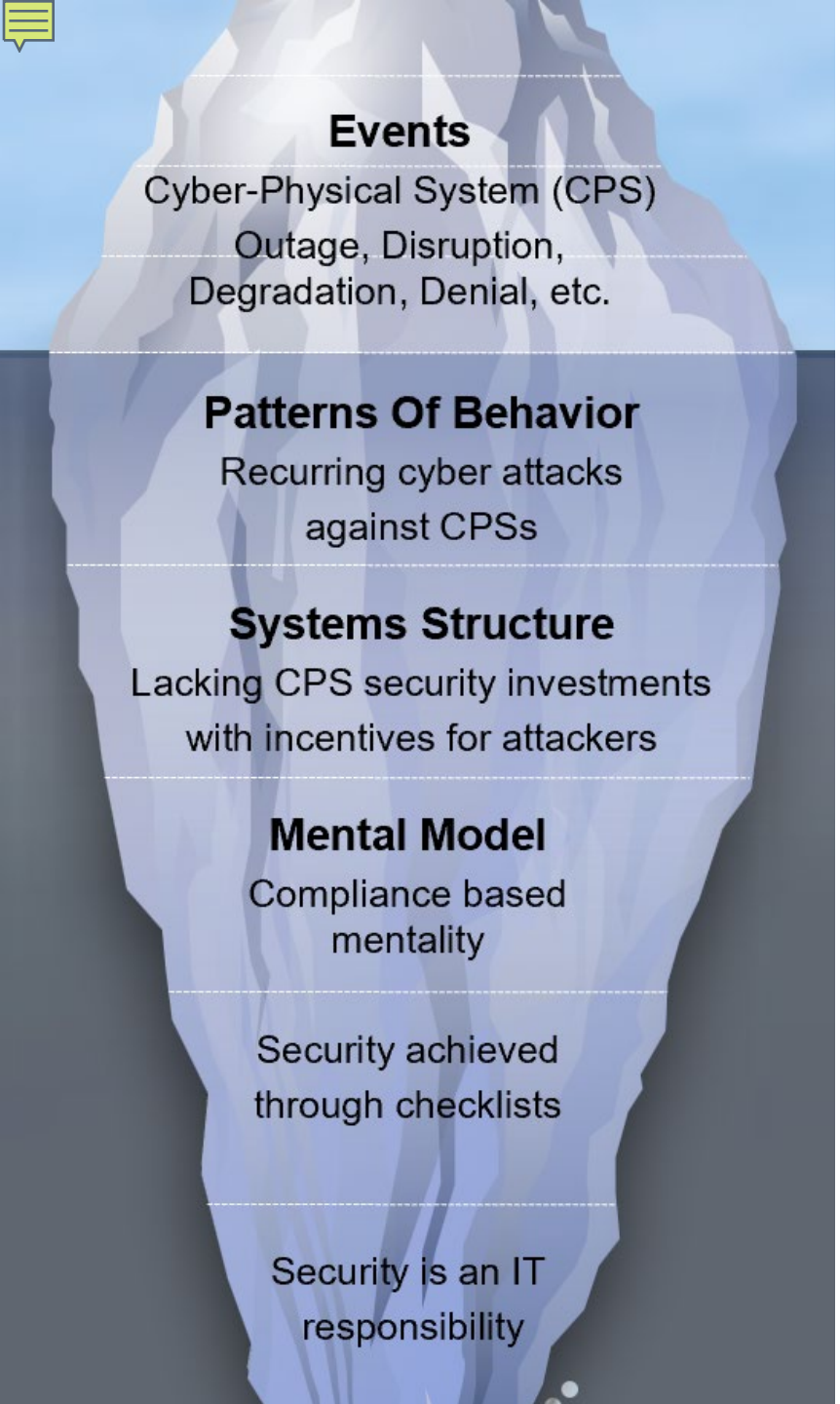


Diagram generated with VENSIM software

Fig. 2. A Causal Loop Diagram (CLD) is used to capture the complexity of CPS Design Teams and CPS Security Efforts from [6]



Characterization of the Problem Space

- Utility of Iceberg Model for Complex Problems
- Current problems with CPS Design Teams:
  - Lack of systems thinking mindset
  - Minimal adoption of systems thinking principles:
    - Holism: Lack of holistic view of a CPS
    - Evolution: Attackers evolve, but CPS does not
    - Emergence: Security is an emergent property, reductionist approach inadequate
    - Feedback: Vulnerabilities emerge from feedback loops and delays

Consideration for CPS Design Teams

- Structural Considerations
- Fundamentals – Security By Design
- Core Knowledge and Experiences
- Necessary Skills and Abilities
- Development Lifecycle

Structural Considerations

- Injection of cybersecurity and systems thinking conscious design engineers
- Healthier relationship between the corporation's enabling systems and CPS Team
- Employee training or new hires

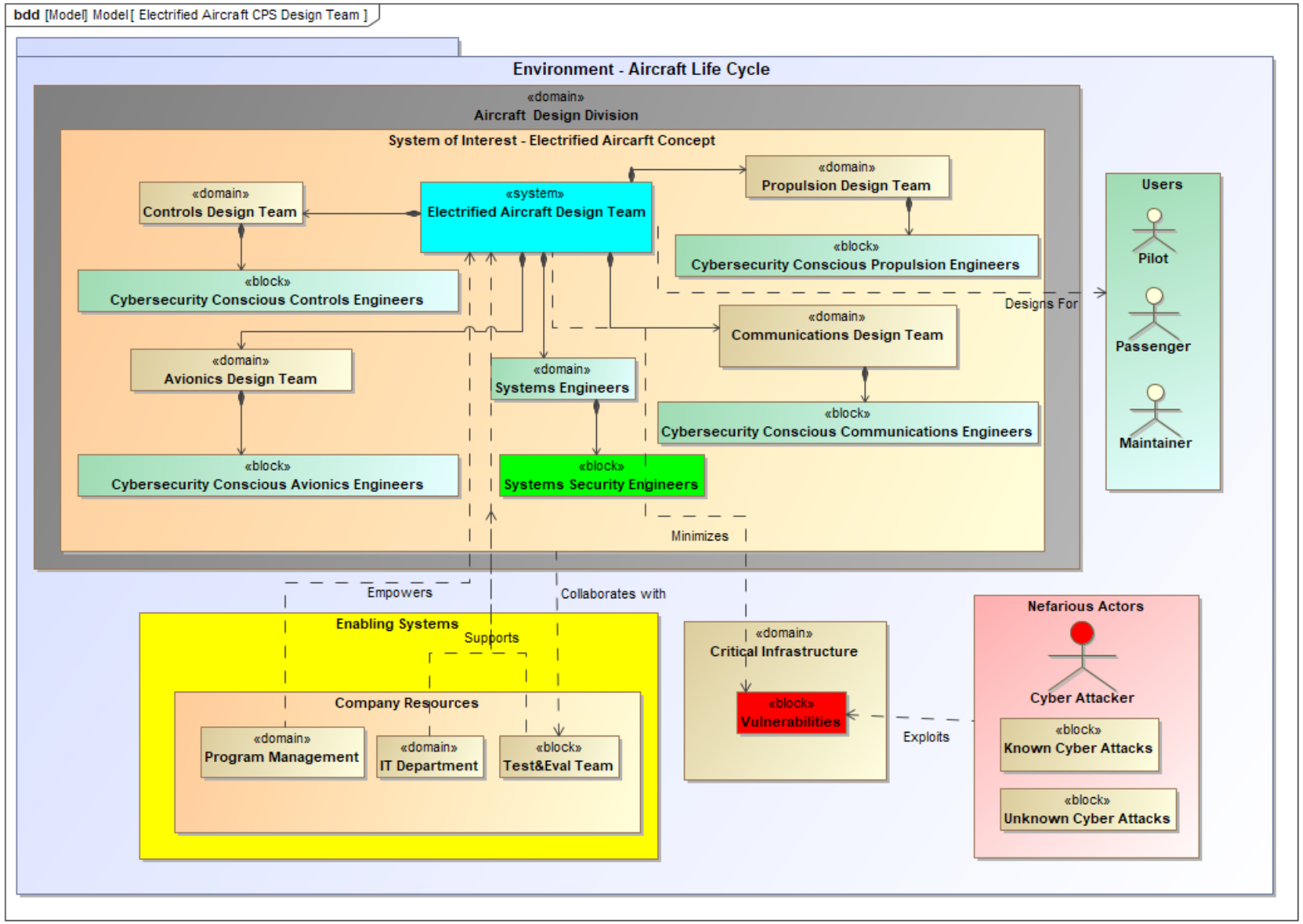


Fig. 4. Proposed Human Design Team Structure BDD for an Electrified Aircraft Concept.

Fundamentals

- Security By Design requires a Holistic Approach across the system development lifecycle
    - First must understand the system mission/purpose and its context.
- Early Focus on Stakeholder needs and Requirements – ID Critical Functionality
- Zero Trust Architecture
- Systems Thinking Principles–

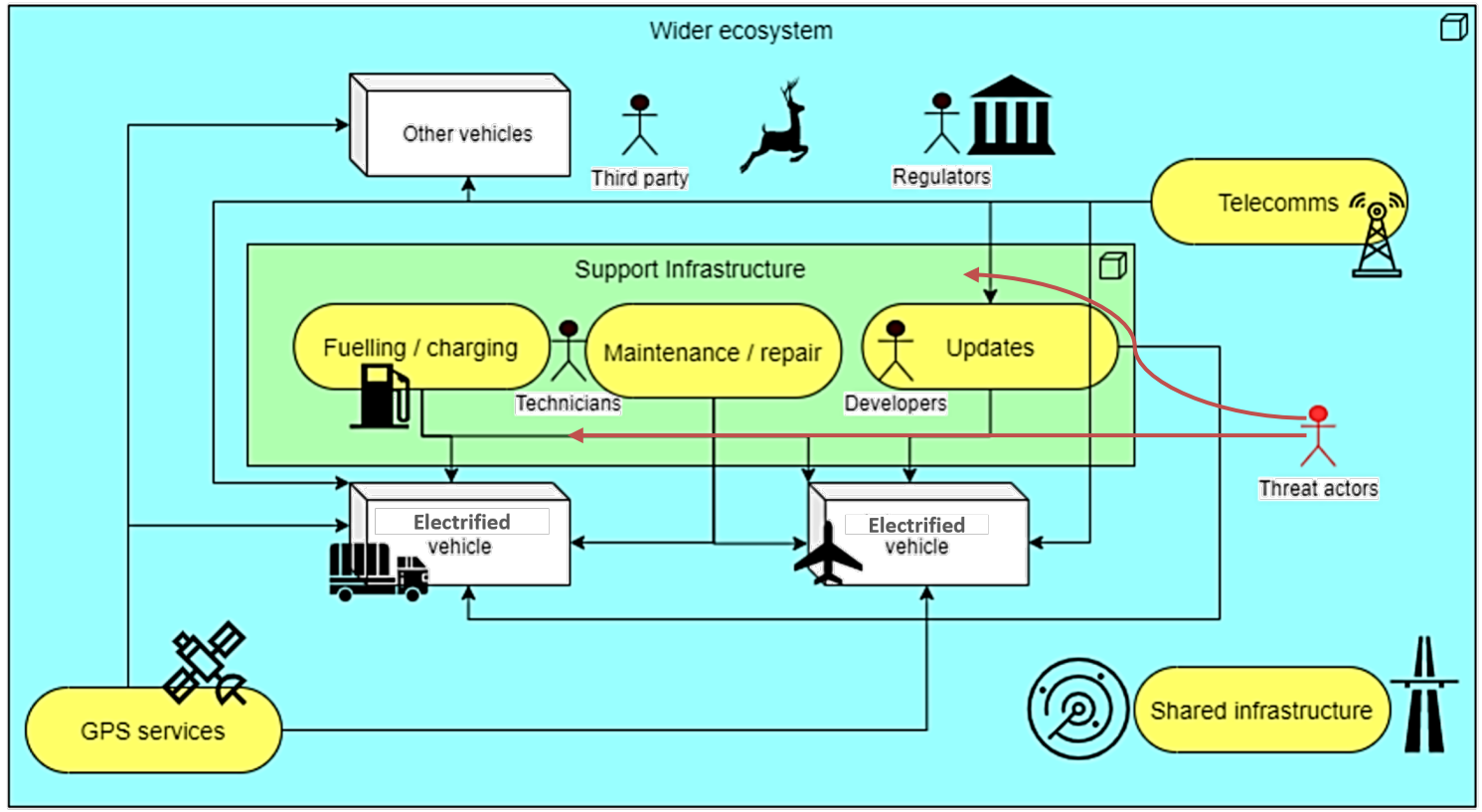
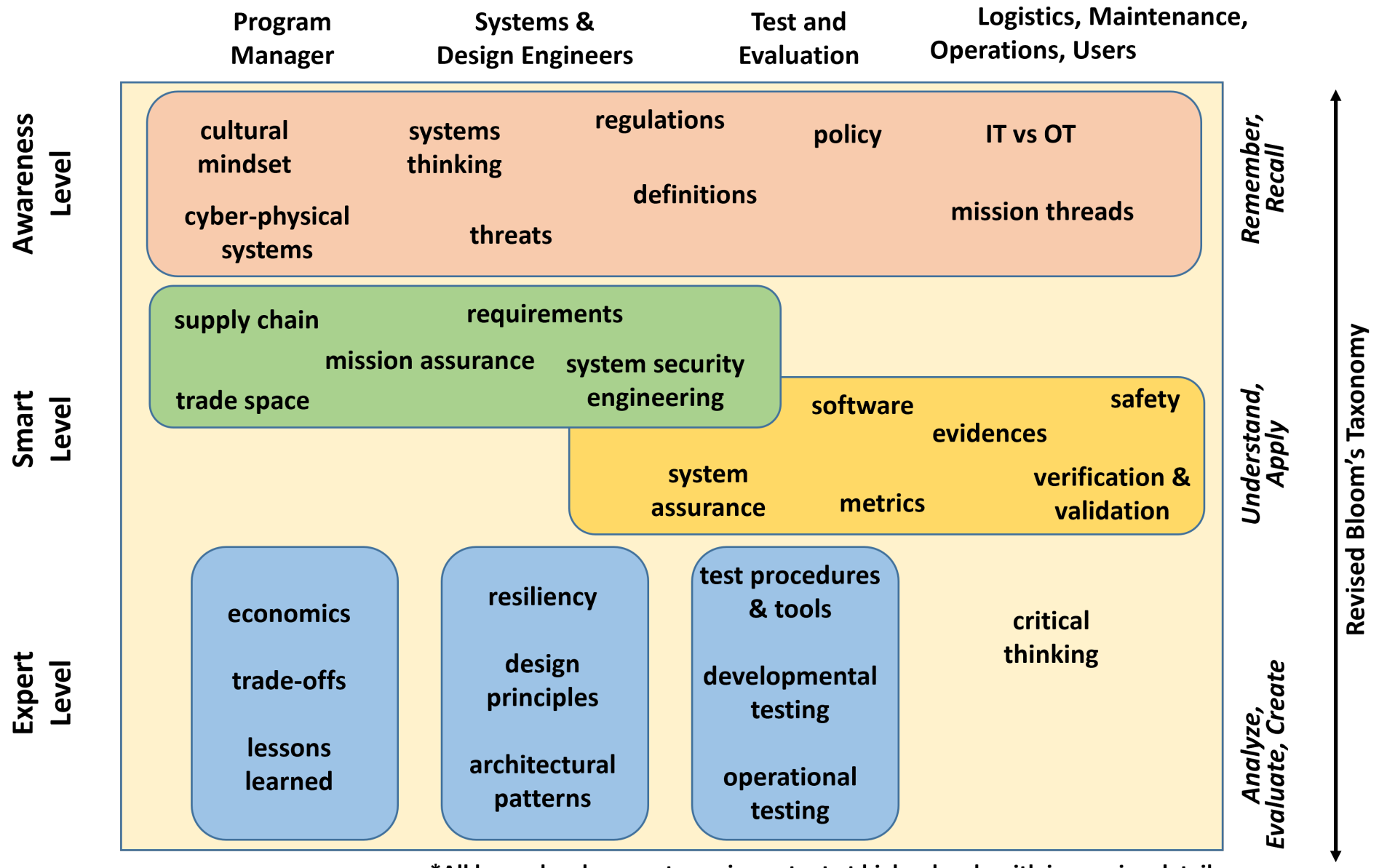


Fig. 5 Electrified Vehicle Operational Environment & Threat Diagram

Holism: A system is More than the sum of its parts: Elements, Interconnects (interdependence) and Purpose.
Emergence: The Complexity of Systems are often due to Emergent behavior
Evolution: Systems have a Life Cycle and they Evolve.
Feedback: Wanted or unwanted Emergent (non-linear) behavior is often determined by Feedback Loops (with delays) within and between the 3 systems

Core Knowledge and Experiences

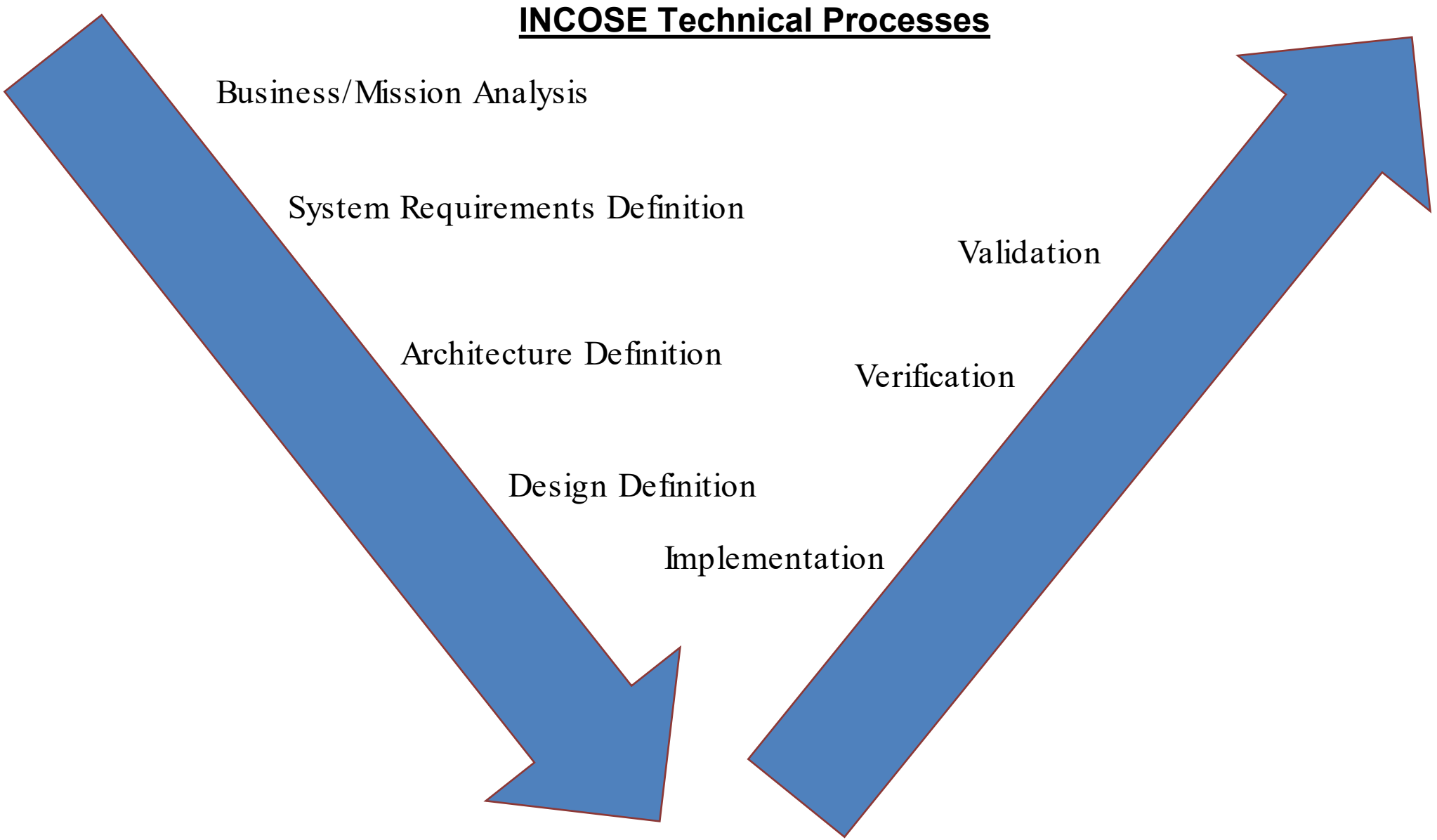
Taxonomy – desired skills and abilities for the CPS Design teams for secure design



*All lower-level concepts are important at higher levels with increasing detail

Fig. 6. Experience and Knowledge Required for Safe and Secure CPS Design Teams.

INCOSE Processes Illustration Specific to Secure Design

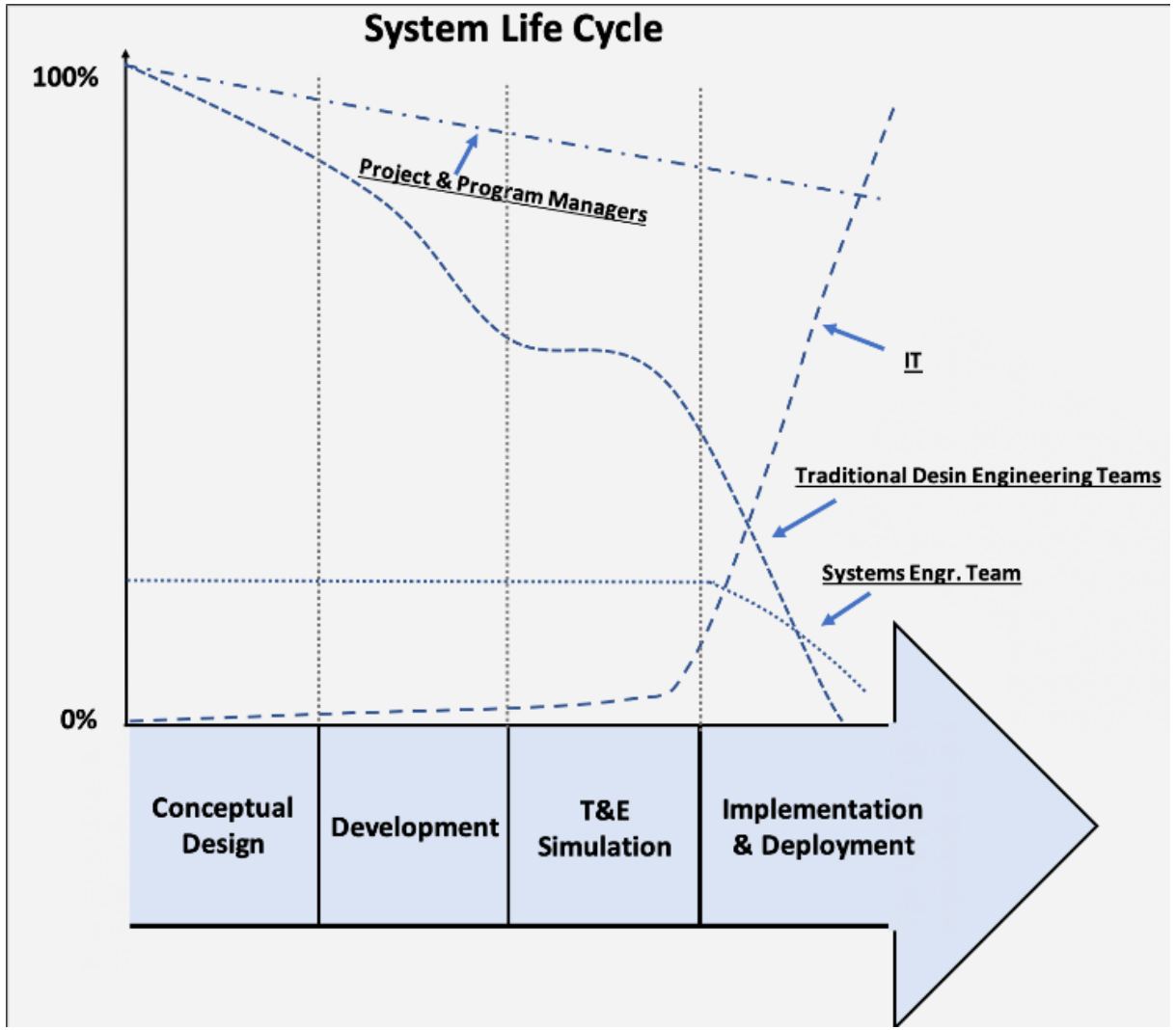


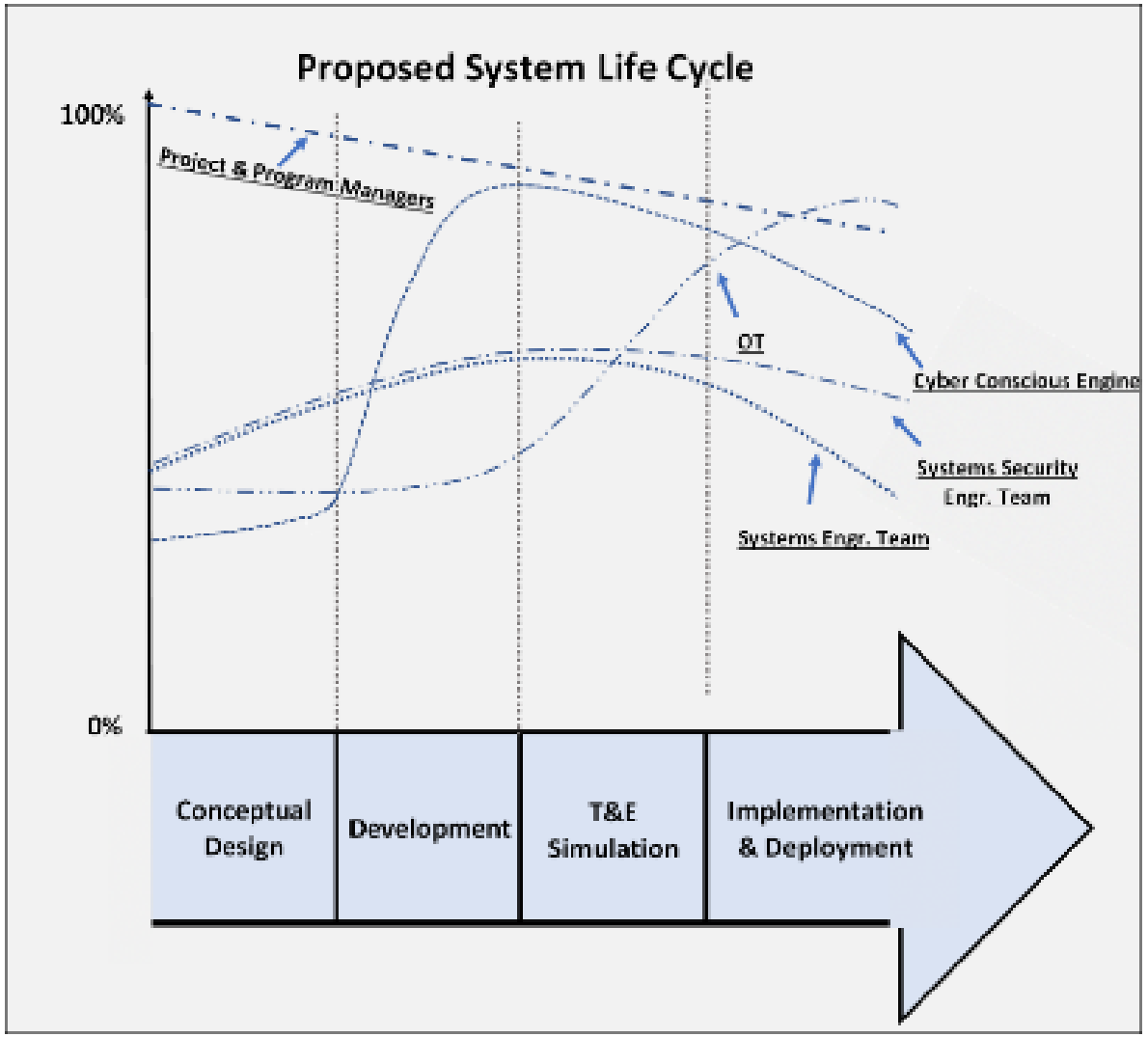
INCOSE Processes Illustration Specific to Secure Design

- **Business/Mission Analysis** - Consider the stakeholder's security needs across the system's set of operational concepts (transporting people or goods), operational environments (urban, suburban, or rural), operators (experienced or novice pilots).
- **System Requirements Definition** - Write "SMART" (Specific, Measurable, Achievable, Realistic, and Timely) security requirements like ensuring aircraft digital communications are encrypted and/or authenticated whenever feasible.
- **Architecture Definition** - Assess competing architectures (both functional and physical architectures) and prioritize potential solutions with consideration for long-term feasibility. This activity should be done not only for the internal SoI's architecture but with consideration for the existing infrastructure the aircraft must utilize and depends upon.
- **Design Definition** - While defining the SoI, it is important for CPS design teams to leverage best practices captured in applicable CPS cybersecurity frameworks to ensure 'Security by Design' for personnel, processes, and technological solutions are indeed designed in.
- **Implementation/Integration** - Historically, most security features are bypassed due to poor implementations rather than broken. Careful implementation and integration is necessary to deliver defensible systems.
- **Verification** - Performing low level test and evaluation of the Electrified Aircraft includes performing input fuzzing on each port and data input, hardware reliability analysis, and holistic cyber red-teaming to look for non-obvious vulnerabilities.
- **Validation** - Assessing the cybersecurity posture of the fielded system in a realistic operational environment includes performing and document cybersecurity activities in appropriate artifacts for inclusion in system security and risk management processes.

Notional Development Lifecycle

- Earlier and additional Systems Engineering, OT, and Systems Security involvement.





Conclusion and Future Work

Recommendations Summary:

- Improving the structure and composition of CPS Design Teams within an organization should encourage more secure system design
- Fundamentals of Systems Thinking and Systems Engineering should be incorporated in Secure System Design
- The Taxonomy of Core Knowledge and Experiences can be better understood per role within a design team – illustrations provided for executing INCOSE Technical Processes for System Design and Development.
- Earlier and Additional Systems Engineering, OT, and Systems Security involvement in the system lifecycle should enable more 'security by design'

Acknowledged Limitations:

- Impacting the design team composition alone is not the most effective or broadly applicable long-term solution:
- Training people is effective but not a universal solution:

  Degrees and formal education vary, often there is resistance to change and Employee turnover
- Hiring cybersecurity SME's is not a viable on every project: limited quantity of SME's and limited budget for project/system development

Future Work:

- Change and improve the design process by creating/specifying a better method for capturing cybersecurity requirements in initial system design

References

[1] Security Boulevard, “Cyber attacks on the power grid,” https: //securityboulevard.com/2022/05/cyber-attacks-on-the-power-grid/, 2022.
[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno,
“Comprehensive experimental analyses of automotive attack surfaces,” in Proceedings of the 20th USENIX Conference on Security, ser. SEC’11. USA: USENIX Association, 2011, p. 6.
[3] L. O. Mailloux, M. A. McEvilley, S. Khou, and J. M. Pecarina, “Putting the ”systems” in security engineering: An examination of NIST special publication 800-160,” IEEE Security & Privacy, vol. 14, no. 4, pp. 76–80, 2016.
[4] United States Government Accountability Office, “Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors,” Tech. Rep. GAO-21-179, Mar. 2021.
[Online]. Available: https://www.gao.gov/assets/gao-21-179.pdf
[5] J. Aviation, “JOBY Aviation,” 2022.
[6] M. T. Span et al., “Systems Thinking and Model Based Systems Engineering’s Utility to Solve Complex Organizational Problems - Cyber-Physical System Design Teams,” in 2022 IEEE International Symposium on Systems Engineering (ISSE), Oct. 2022, pp. 1–8.
[7] M. Winstead and M. McCevily, Trustworthy Secure System Design, 2022.
[8] J. P. Monat and T. F. Gannon, “What is systems thinking? A review of selected literature plus recommendations,” American Journal of
Systems Science, vol. 4, no. 1, pp. 11–26, 2015.
[9] A. Pyster, D. Olwell, N. Hutchison, S. Enck, J. Anthony, D. Henry, and A. Squires, Guide to the Systems Engineering Body of Knowledge (SEBoK) version 1.0. Hoboken, NJ: The Trustees of the Stevens Institute of Technology, 2012.
[10] P. Senge, Fifth Discipline: The Art and Practice of the Learning Organization. USA: Random House Books, 2006.
[11] D. H. Meadows, Thinking in systems: A primer. Chelsea Green Publishing, 2008.
[12] D. Gurdur and M. T¨orngren, “Design Thinking and Systems Thinking for Cyber-Physical Systems,” in DS 91: Proceedings of NordDesign
2018, Link¨oping, Sweden, 14th - 17th August 2018, 2018.
[13] INCOSE, “MBSE Initiative,” https://www.incose.org/incose-member-resources/working-groups/transformational/mbse-initiative, 2022.
[14] H. Dezfuli, A. Benjamin, C. Everett, M. Feather, P. Rutledge, D. Sen, and R. Youngblood, “NASA System Safety Handbook. Volume 2: System Safety Concepts, Guidelines, and Implementation Examples,” May 2015.
[Online]. Available: https://ntrs.nasa.gov/citations/20150015500
[15] R. Ross, M. Winstead, and M. McEvilley, “Engineering Trustworthy Secure Systems,” National Institute of Standards and Technology,
Tech. Rep. NIST Special Publication (SP) 800-160 Vol. 1 Rev. 1, Nov. 2022. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/final
[16] “Biannual ICS Risk & Vulnerability Report: 2H 2021.” [Online]. Available: https://claroty.com/resources/reports/2h-2021 [17] T. M. Chen and S. Abu-Nimeh, “Lessons from Stuxnet,” Computer, vol. 44, no. 4, pp. 91–93, 2011.
[18] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, “Ransomware: Recent advances, analysis, challenges and future research directions,” Computers & Security, vol. 111, p. 102490, Dec. 2021. [Online].
Available: https://www.sciencedirect.com/science/article/pii/S016740482100314X
[19] M. Span, L. O. Mailloux, and M. R. Grimaila, “Cybersecurity Architectural Analysis for Complex Cyber-Physical Systems,” The Cyber Defense Review, vol. 3, no. 2, pp. 115–134, 2018, publisher:
Army Cyber Institute. [Online]. Available: https://www.jstor.org/stable/26491226
[20] M. Span, L. O. Mailloux, R. F. Mills, and W. Young, “Conceptual systems security requirements analysis: Aerial refueling case study,” IEEE Access, vol. 6, pp. 46 668–46 682, 2018.
[21] L. O. Mailloux, M. Span, R. F. Mills, and W. Young, “A top down approach for eliciting systems security requirements for a notional autonomous space system,” in 2019 IEEE International Systems Conference (SysCon).
IEEE, 2019, pp. 1–7.
[22] J. M. Sayers, B. E. Feighery, and M. T. Span, “A STPA-Sec case study: Eliciting early security requirements for a small unmanned aerial system,” in 2020 IEEE Systems Security Symposium (SSS). IEEE, 2020, pp. 1–8.
[23] R. T. Reule, B. Feighery, M. W. Winstead, D. R. Hild, W. Barnum, and M. Span, “STPA-Sec analysis for DevSecOps reference design,” in INCOSE International Symposium, vol. 31, no. 1. Wiley Online Library, 2021, pp.
296–309.
[24] H. Sohier et al., “A tooled methodology for the system architect’s needs in simulation with autonomous driving application,” 2019, pp. 1–8.
[25] S. Khou, L. O. Mailloux, J. Pecarina, and M. Mcevilley, “A customizable framework for prioritizing systems security engineering processes, activities, and tasks,” IEEE Access, vol. 5, pp. 12 878–12 894, 05 2017.

Questions?

Contact:
Trae Span Trae.span@colostate.edu
Jeremy Daily Jeremy.daily@colostate.edu
Logan Mailloux logan.Mailloux@nps.edu