

Towards Productive Cyber Resilience and Safety Analysis in Model-Based Systems Engineering

- Serdar Akar, ¹; Huseyin Dogan, ¹; Shamal Faily, ²; Duncan Ki-Aries, ¹
 - ¹Bournemouth University, ²Dstl

Summary

In the defense sector, cyber-physical systems (CPS) face escalating threats that compromise resilience—the ability to anticipate, withstand, recover from, and adapt to cyberattacks—while ensuring safety to mitigate hazards. Traditional document-based engineering struggles with the complexity of these systems, leading to fragmented analyses and inefficiencies. Model-Based Systems Engineering (MBSE) offers a paradigm shift by formalising models for automated verification, simulation, and trade-off analysis across lifecycle phases, as emphasised by INCOSE (2023). However, empirical evidence on scaling MBSE for integrated cyber resilience and safety analysis remains limited, with challenges including model scalability for thousands of components, manual bottlenecks in harmonising methods like STPA (Systems-Theoretic Process Analysis) and STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), tool interoperability issues, and over-reliance on specialists.

This poster presents ongoing PhD research aimed at enhancing productivity in MBSE-driven cyber resilience and safety analysis, aligned with the UK Ministry of Defence's PYRAMID programme for reusable architectures to reduce costs in air platforms (UK MoD, 2021). Key goals include identifying gaps in current workflows, developing prototypes to automate traceability (e.g., threat-to-safety links), and evaluating impacts on usability and efficiency in high-assurance environments.

The methodology employs a mixed-methods design: (1) A PRISMA-guided Systematic Literature Review (SLR) of peer-reviewed sources from 2014–2024 (e.g., IEEE Xplore, Scopus) synthesises challenges and opportunities, revealing fragmented methodologies and the need for standardised metrics like mean time to recovery (MTTR); (2) Stakeholder engagement via interviews and focus groups with defense engineers and integrators captures practical needs; (3) Gap, needs, and requirements analyses prioritise features like AI-driven optimisation; (4) Iterative prototype development integrates STPA, STRIDE, and model checking into SysML environments (e.g., Cameo Systems Modeler), incorporating MITRE ATT&CK for threat modeling; (5) Empirical evaluation through action research in exemplar defense cases measures outcomes using metrics such as time savings, error reduction, and Technology Readiness Level (TRL), with tools like UPPAAL for formal verification.

Preliminary results from the SLR and stakeholders highlight scalability limits and manual processes as primary barriers, with prototypes demonstrating potential 30% reductions in analysis time and improved traceability in defense architectures. The poster will visualise these via figures, including a cycle diagram of MBSE-driven resilience enhancement and a table of challenges/opportunities (e.g., automated checking with SysML and MITRE ATT&CK).

This work's impact on high-integrity software lies in bridging theoretical MBSE benefits with practical adoption, enabling general engineers to conduct analyses without specialist dependency. By fostering automated, co-engineered resilience-safety strategies, it supports cost-effective, resilient defense platforms and informs standards like ISO 26262. Future directions include AI-enhanced model checking and expansion to domains like aerospace, promoting broader industrial uptake and regulatory integration.