Towards Productive Cyber Resilience and Safety Analysis in MBSE

- Serdar Akar, PhD Researcher[1]; Supervisor:Huseyin Dogan, PhD[1]; Supervisor: Shamal Faily, PhD[2]; Supervisor:Duncan Ki-Aries , PhD[1]
- [1]Bournemouth University, [2]Dstl

Introduction

Background

Cyber resilience enables systems to resist and recover from attacks, restoring functionality, while safety analysis identifies hazards and mitigates risks. In defense, design trades (e.g., architectural dissimilarity) affect these alongside cost and schedule. Traditional document-based engineering struggles with complexity, leading to MBSE adoption—a model-centric approach for automated analysis across lifecycle phases. Programmes like PYRAMID envision reusable architectures to cut costs (UK MoD, 2021). However, empirical evidence on scaling MBSE for cyber resilience and safety is limited, with challenges in automation and specialist reliance (Estefan, 2008; Holt & Perry, 2013). This project aims to improve productivity by integrating these analyses into MBSE workflows.

Objectives

01 Challenge and Opportunity Identification

02 Gap, Needs, and Requirements Analyses

03 Prototype Development

04 Empirical Evaluation

Category	Challenges	Opportunities
Scalability	Handling large models (Estefan, 2008)	Automated model checking (Holt & Perry, 2013)
Workflow Efficiency	Manual processes (Altaf et al., 2022)	STPA + STRIDE integration (Friedberg et al., 2017; Mika et al., 2023)
Tool Interoperability	Integration barriers (Naseir et al., 2021)	SysML with MITRE ATT&CK
Usability	Specialist dependency	Guidelines for general engineers

Table 1: Key Challenges and Opportunities in MBSE Integration

Research

Methodology

A mixed-methods research design is adopted, combining qualitative and quantitative approaches for comprehensive insights (Page et al., 2021):

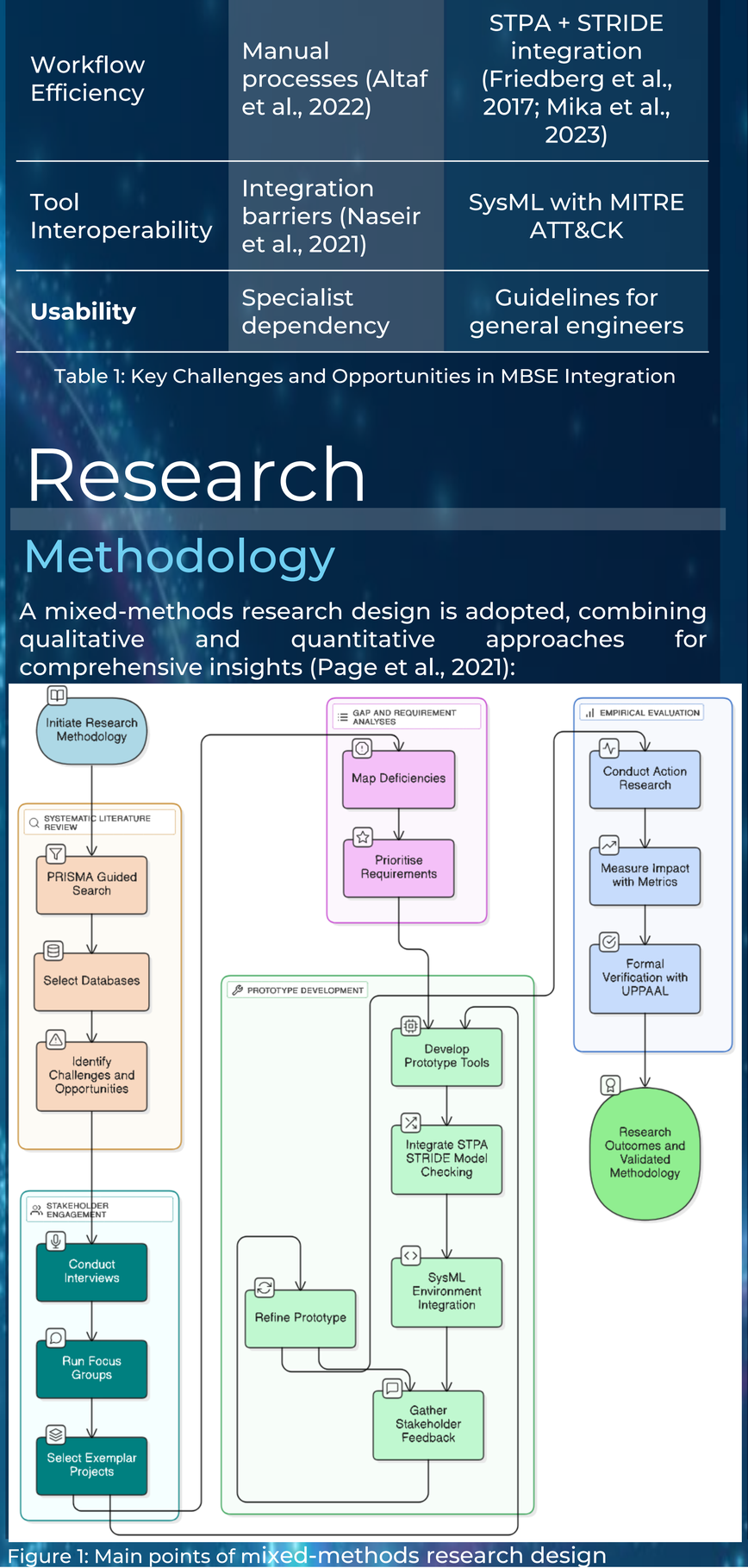

Figure 1: Main points of mixed-methods research design

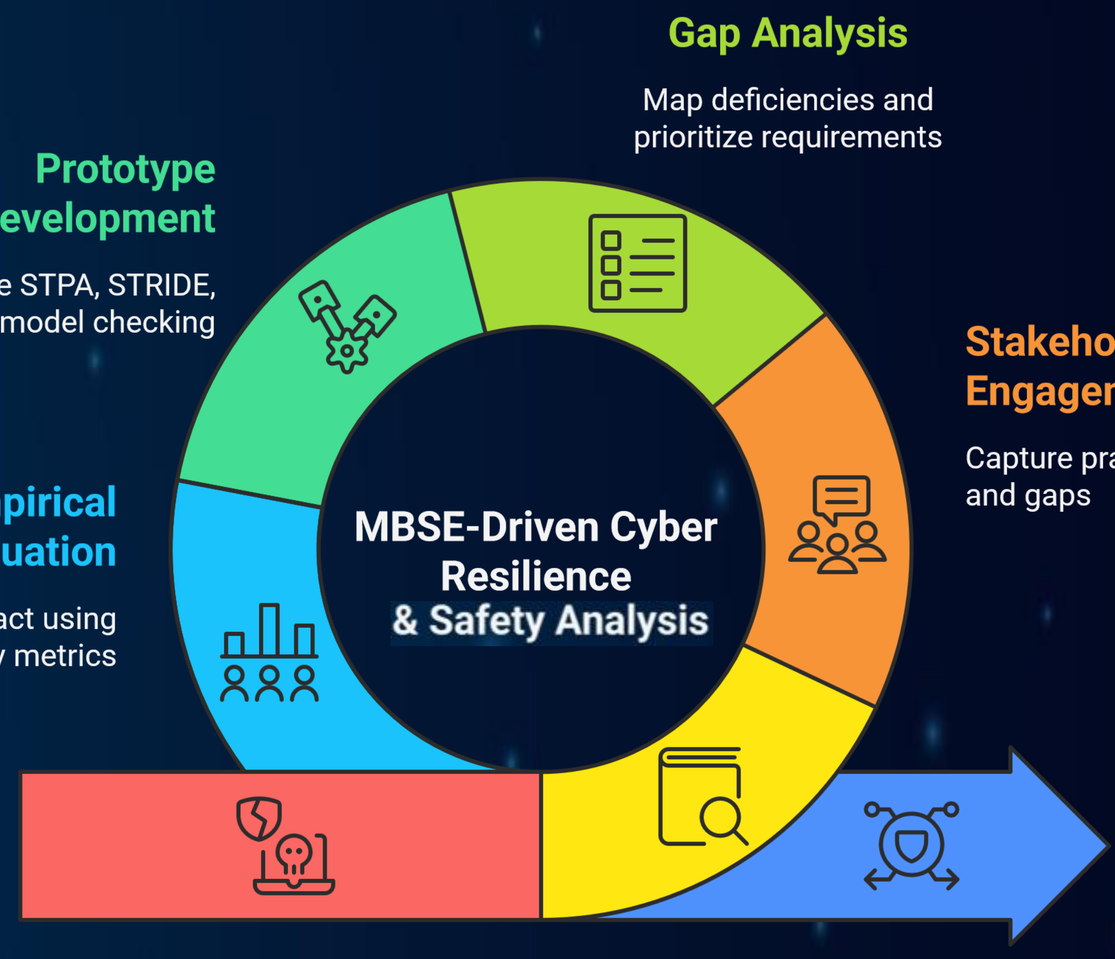

Figure 2: Key Steps of Enhancing Cyber Resilience & Safety Analysis with MBSE

Results

Preliminary findings from literature and stakeholder inputs:

Gaps: Scalability limits in models with thousands of components; manual bottlenecks in harmonizing STPA and STRIDE ; tool interoperability issues (Naseir et al., 2021; Altaf et al., 2022).

Needs: Automated traceability (threat-to-safety), risk prioritization, and reduced specialist dependency.

Requirements: AI-driven optimization, integrated frameworks ranked by impact vs. complexity. Prototypes show potential 30% time reductions in analysis; exemplar cases validate scalability in defense architectures. Metrics: Error reduction, consistency in trade-offs.

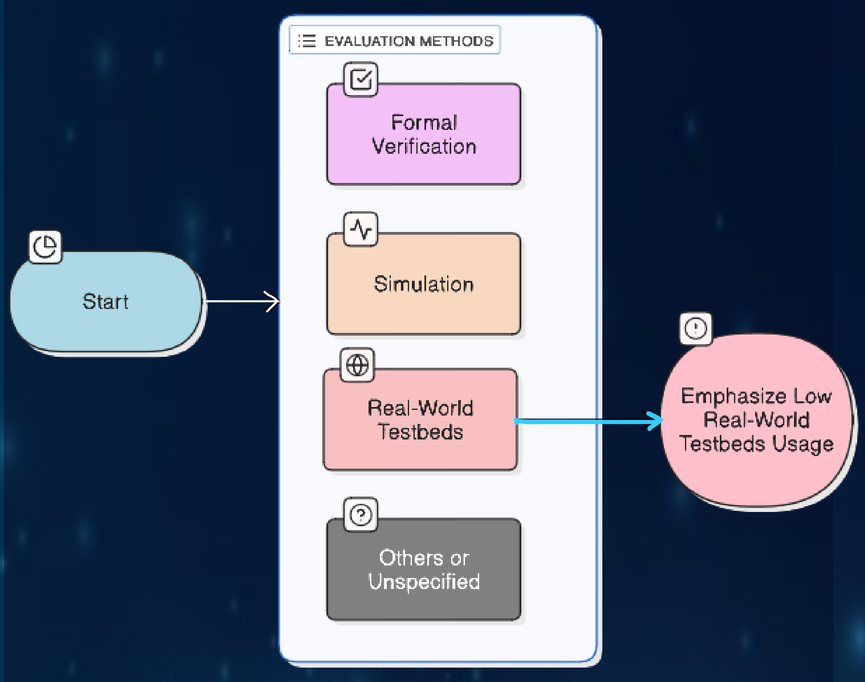

Figure 3: Key Challenges and Opportunities in MBSE Integration

Discussion

Integrating cyber resilience and safety into MBSE addresses defense challenges but requires overcoming manual efforts and expertise barriers. Prototypes enable general engineers to perform analyses, aligning with PYRAMID goals. Empirical evidence supports scalability, though adoption needs promotion via guidelines. Limitations: Defense-specific contexts may limit generalizability; future iterations could incorporate AI for adaptive modeling.

Conclusion

This project provides empirical evidence that integrating cyber resilience and safety analysis into MBSE enhances productivity, scalability, and usability in defence systems engineering. It bridges theoretical MBSE benefits with practical applications, offering validated prototypes, structured guidelines, and a framework for automated co-analysis of resilience and safety (Japs, 2020; Larsen et al., 2024). By reducing manual effort, improving traceability, and supporting informed trade-offs, the research contributes to more resilient, safe, and cost-effective defence platforms. The outcomes support the UK MoD's strategic goals and provide a foundation for broader industrial adoption.

Future Directions

Expand prototypes to include AI-enhanced model checking; test in additional domains (e.g., automotive); develop training modules for adoption; update defense standards based on findings. Long-term: Full integration into regulatory frameworks for broader impact.

sakar@bournemouth.ac.uk
School of Computing and Engineering
Faculty of Media, Science and Technology
Bournemouth University

References

- Altaf, A., et al. (2022). Challenges in MBSE workflows.
- Estefan, J. A. (2008). Survey of model-based systems engineering methodologies.
- Friedberg, I., et al. (2017). STPA-Sec: Security considerations in STPA.
- Gudla, S., & Jamalpur, B. (2024). Cyber resilience frameworks.
- Hassan, A., et al. (2024). MBSE for complex systems.
- Holt, J., & Perry, S. (2013). SysML for systems engineering.
- INCOSE. (2023). Systems engineering handbook.
- Linkov, I., et al. (2013). Resilience and stability of ecological systems.
- Mika, D., et al. (2023). STRIDE methodology for cybersecurity.
- Naseir, M., et al. (2021). Tool integration in MBSE.
- Page, M., et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews BMJ 2021
- Teper, D., et al. (2025). MBSE in aerospace and defense.
- UK MoD. (2021). PYRAMID programme overview.
- Wei, R., et al. (2022). Safety analysis in SCSE.
- Weisman, D., et al. (2024). Cyber resilience in digital environments.