Operational Resiliency Quantification in Cyber-Physical Systems: Method, Implementation and Validation

Tarmo Korõtko, Shaymaa Mamdouh Khalil, Alvaró Schuller, Vahur Kotkas, Jaakob Lambot and Karl Pappel

Dept. of Electrical Power Engineering and Mechatronics and Dept. of Software Science, Tallinn University of Technology

Objectives

This research explores the practical and operational implementation of the MITRE CRUC method in Cyber-Physical Systems (CPS).

The study addresses the following research questions:

- How is the MITRE CRUC method applied in CPSs?
- Which implementation activities and artefacts influence the resulting resilience assessment?
- Is the MITRE CRUC method suitable for operational resiliency assessment (automated and telemetry-driven in contrast to manual, analytical evaluation)?

Introduction

Adversary behaviours in cyber-physical systems (CPS) must be exercised on real systems or high-fidelity testbeds to obtain decision-quality evidence about mission impact and the effectiveness of mitigation [1]. CPS Taxonomies, threat-modelling studies, and in-depth studies linking threats, assets, and consequences [2, 3] underscore the need to validate defence and mitigation measures empirically, rather than theoretically.

Empirical validation requires the quantification of system resiliency, which is used for informed governance and investment decisions. Comparable measures enable the evaluation of system design and alternatives to select the optimal mission continuity improvement per unit of cost, burden, or risk [4, 5]. We select the MITRE Cyber-Resiliency Use-Case (CRUC) method due to (a) its explicit mission-centricity and consistency with the National Institute of Standards and Technology (NIST) cyber-resiliency engineering framework [6]; (b) its traceability from adversary tactics to design techniques and testable hypotheses; (c) it can be used with pre-existing prioritisation schemes (e.g., ATT&CK) and multi-criteria decision methods [7]. CPS case studies reveal the lack of public, step-by-step implementation guidance for operationalising quantification methods in actual CPSs [8, 9].

Employed Method

- A case study describing a fictitious manufacturing company and its operations and procedures.
- Determining the mission goal and primary mission objective, followed by the identification of supporting goals, objectives, and sub-objectives (MITRE CREF Navigator [10]).
- Weighing of mission objectives and sub-objectives through contextual risk analysis and threat modelling.
- Defining quantification methods for measurable actions of sub-objectives.
- An experimental testbed to emulate the manufacturing operations and relevant ICT and power systems.
- Automated data collection of measured parameters for the quantification of individual actions.

Resiliency Quantification

Resiliency quantification through the Cyber Resiliency Score R [11] (Equations 1 to 3), where PE^O is the objective component, PR^O is the objective weight, PE^{SO} is the sub-objective component, PR^{SO} is the sub-objective weight, PE^A is the action component, and PR^A is the action weight.

$$PE^{SO} = \frac{100 \cdot \sum (PR^A \cdot PE^A)}{\sum (PR^A \cdot 5)} \quad (1)$$

$$PE^{O} = \frac{100 \cdot \sum (PR^{SO} \cdot PE^{SO})}{\sum (PR^{SO} \cdot 100)} \quad (2)$$

$$R = \frac{100 \cdot \sum (PR^{O} \cdot PE^{O})}{\sum (PR^{O} \cdot 100)} \quad (3)$$

R values are used for calculating the Cyber Resiliency Quantification Index (CRQI) Γ using 4, where n is the number of values, i the index of cyber resiliency value $0, 1, \ldots, n-1$, R_i the cyber resiliency value at index i, and T_i the timestamp of cyber resiliency value.

$$\Gamma = \sum_{i=1}^{n} \frac{(200 - R_{i-1} - R_i)}{2} \cdot (T_i - T_{i-1}) \quad (4)$$

CPS testbed

An experimental CPS setup is built for the case study to emulate relevant ICT resources (Fig. 1).

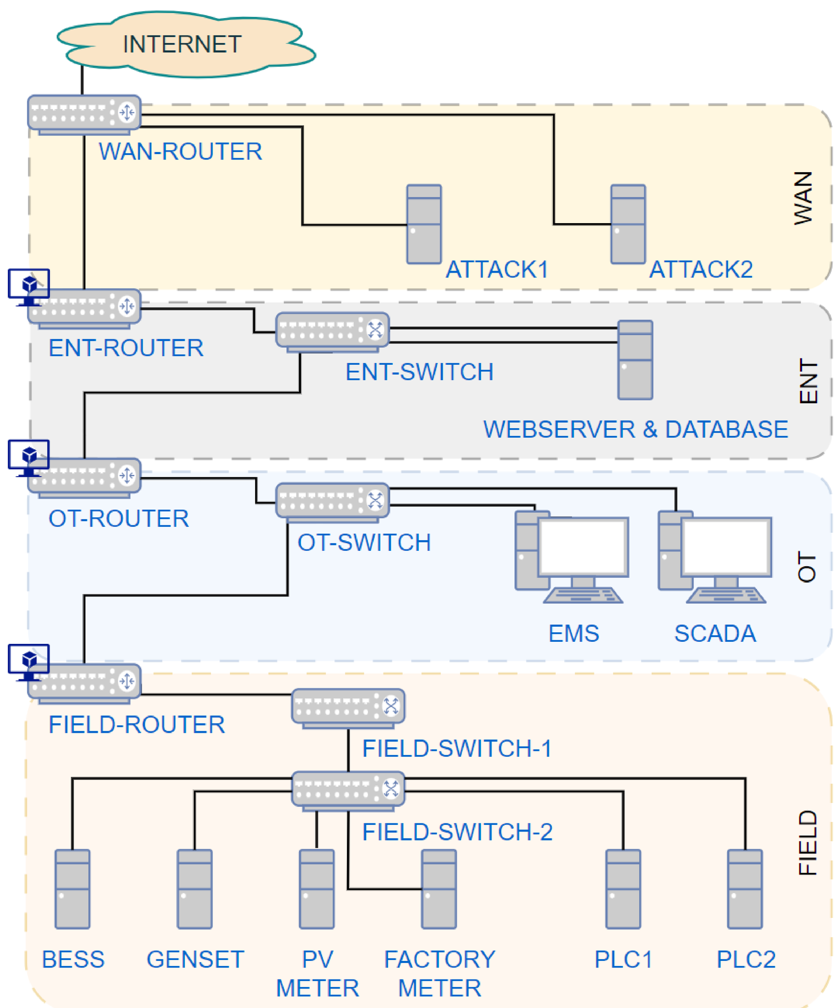

Figure 1: ICT hardware used in case-study.

Experiment Results

Cyber resiliency values for both Experiment Scenarios (Figures 2 and 3, and Table 1).

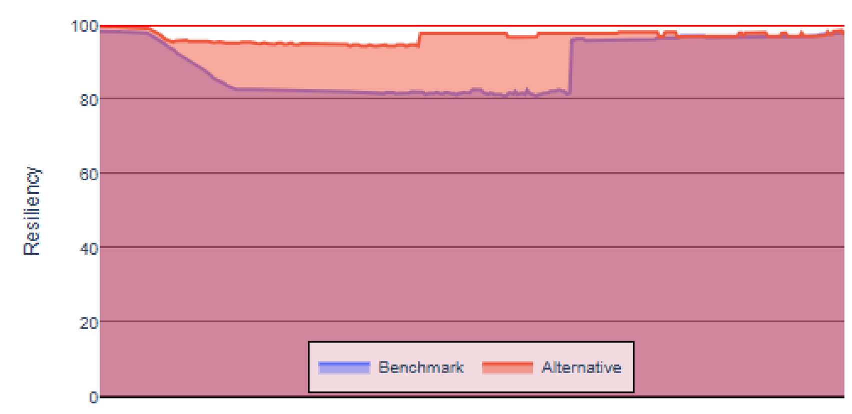

Figure 2: Cyber resiliency values for Experiment Scenario #1.

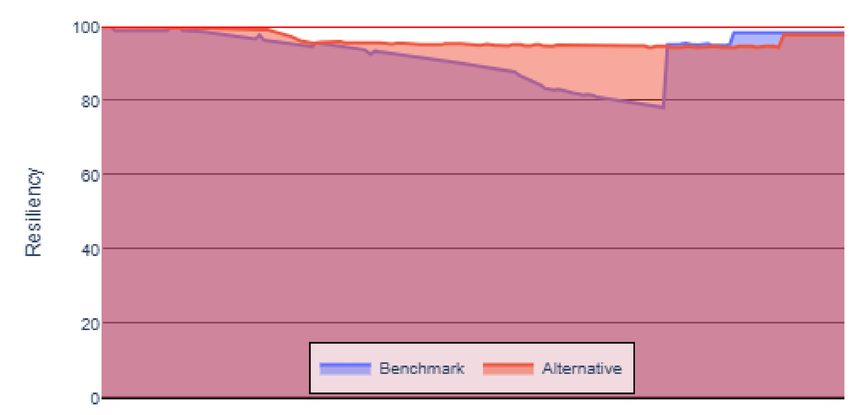

Figure 3: Cyber resiliency values for Experiment Scenario #2.

Table 1: Experiment Results of Scenarios #1 and #2

	Experiment Scenario #1		Experiment Scenario #2	
	Benchmark Scenario	Alternative Scenario	Benchmark Scenario	Alternative Scenario
CRQI	42 256	13 836	41 242	17 398
Lowest Cyber Resiliency Value	80.8	94.3	58.6	78.9
Cyber Resiliency Improvement	–	67%	–	58%
No Internet or manufacturing stopped	16m 00s	11m 30s	27m 15s	20m 55s

Conclusion

We demonstrate an operational application of the MITRE CRUC method in CPSs. The conducted case study allowed for quantified comparisons between baseline and segmented designs, revealing sizable and comparative gains in operational resilience (CRQI improvements of 67 % and 58 %) and increases in minimum resiliency with reduced downtime.

We demonstrate that the MITRE CRUC method is suitable for operational assessment when supported by sophisticated system analysis and robust telemetry; however, outcomes remain contingent on context-specific weighting, the completeness of metrics, and monitoring fidelity.

Acknowledgements

This research was funded through the NATO DIANA program, under which Goldilock Secure Ltd. contracted TalTech to perform the testing (according to Tender nr 3-30/37-1 of 31.05.2024). This research was supported by the project „Increasing the knowledge intensity of Ida-Viru entrepreneurship“ co-funded by the European Union (2021-2027.6.01.23-0034).

References

[1] Michael J. Weisman, Alexander Kott, Jason E. Ellis, Brian J. Murphy, Travis W. Parker, Sidney Smith, and Joachim Vandekerckhove. Quantitative measurement of cyber resilience: Modeling and experimentation. *arXiv preprint*, 2023.

[2] Shaymaa Mamdouh Khalil, Hayretdin Bahsi, Henry Ochieng' Dola, Tarmo Korõtko, Kieran McLaughlin, and Vahur Kotkas. Threat modeling of cyber-physical systems—a case study of a microgrid system. *Computers & Security*, 124:102950, 2023.

[3] Hayretdin Bahsi, Henry Ochieng' Dola, Shaymaa Mamdouh Khalil, and Tarmo Korõtko. A cyber attack taxonomy for microgrid systems. In *IEEE System of Systems Engineering Conference (SoSE)*, 2022.

[4] Seyedmohsen Hosseini, Kash Barker, and Jose E. Ramirez-Marquez. A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145:47–61, 2016.

[5] DJ Bodeau, RD Graubart, RM McQuaid, and J Woodill. Cyber resiliency metrics, measures of effectiveness, and scoring (mitre technical report no. mtr180314). the mitre corporation, 2018.

[6] Ronald Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. Developing cyber-resilient systems: A systems security engineering approach. Special Publication 800-160, Volume 2, Revision 1, National Institute of Standards and Technology, 2021.

[7] Ihab Mohamed, Hesham A. Hefny, and Nagy R. Darwish. Enhancing cybersecurity defenses: A multicriteria decision-making approach to mitre att&ck mitigation strategy. *International Journal of Computer Networks & Communications*, 16(4), 2024.

[8] Shaymaa Mamdouh Khalil, Hayretdin Bahsi, and Tarmo Korõtko. Threat modeling of industrial control systems: A systematic literature review. *Computers & Security*, 136:103543, 2024.

[9] Mariana Segovia-Ferreira, Jose Rubio-Hernan, Ana Rosa Cavalli, and Joaquin Garcia-Alfaro. A survey on cyber-resilience approaches for cyber-physical systems. *arXiv preprint*, 2024.

[10] MITRE. CREF navigator. Online resource.

[11] Richard D. Graubart, Robert McQuaid, and Jay Woodill. Cyber resiliency metrics and scoring in practice, 2018.

Contact

E-mail: tarmo.korotko@taltech.ee