CYBERSECURITY REQUIREMENTS ASSURANCE IN CRITICAL INFRASTRUCTURE SYSTEMS THROUGH THE APPLICATION OF FORMAL VERIFICATION AND ARTIFICIAL INTELLIGENCE-BASED METHODS

Daniel Daukševič[1]

[1]Vilnius University, Faculty of Mathematics and Informatics, Institute of Computer Science, Vilnius, Lithuania
daniel.dauksevic@mif.stud.vu.lt

Cybersecurity of critical infrastructure has become a major concern of modern society and a matter of national interest, with direct impacts on social life, the economy, and government operations. Formal verification, a mathematically rigorous method for proving the correctness of algorithms and system designs, has been widely and successfully applied to the design and certification of safety-critical and cyber-physical systems to guarantee correctness, reliability, and fault tolerance. However, its systematic application to cybersecurity at the architectural and topological levels of such infrastructures remains limited. With the rapidly increasing impact of Artificial Intelligence (AI) in various domains, including cybersecurity, the idea of combining AI with formal verification has emerged as a promising research direction. This hybrid approach has already shown promising results in several domains, such as the verification of cryptographic protocols, software vulnerability detection and automated code repair.

The main hypothesis of the doctoral thesis is that some of these formal techniques and methods, actively used in the verification of safety-critical systems, as well as their combination with AI methods, can be successfully adapted and applied to the verification of cybersecurity properties in complex critical infrastructure systems. The thesis aims to contribute to the systematic application of formal methods at the topological and architectural levels for cybersecurity, proposing a framework that integrates existing formal verification techniques from safety-critical domains and AI methods with modern security requirements.

In this thesis, computer networks that form the backbone of critical infrastructures are defined using mathematical notation. This representation enables automated examination of these systems against logical formulas that capture key cybersecurity requirements, including confidentiality, integrity, and availability. AI-based methods are incorporated to assist in identifying potential attack paths and vulnerabilities, as well as optimizing the process of verification.

The expected outcome is a methodological foundation for future research at the intersection of formal verification, AI, and cybersecurity. This foundation will support rigorous security analysis of critical infrastructure systems, including power networks and industrial control systems, and provide guidance for the application of formal methods in the design and evaluation of secure and resilient cyber-physical infrastructures.

Acknowledgements

This work has been supported by the Lithuanian Research Council under grant No. P-PAD-23-173.

Keywords: Formal Methods, Formal Verification, Cybersecurity, Critical Infrastructure Systems, Artificial Intelligence

[1] J. Rushby, "Formal methods and their role in the certification of critical systems," in Safety and Reliability of Software-Based Systems. London, U.K.: Springer, 1997, pp. 1–42. doi: 10.1007/978-1-4471-0921-1_1.

[2] L. Lamport, Specifying Systems. Boston, MA, USA: Addison-Wesley Professional, 2003.

[3] A. Remke and B. Steffen, Eds., FMICS 2025: Formal Methods for Industrial Critical Systems, Lecture Notes in Computer Science, vol. 16040. Cham, Switzerland: Springer, 2025.