

Cybersecurity Strategies for Protecting Industrial Control Systems

Riley Martin
PhD
Technion - Israel Institute of Technology
Technion City, Haifa 3200003, Israel

Kim Allen
PhD
Khalifa University
P.O. Box 127788, Abu Dhabi, UAE

Taylor Wilson
PhD
Norwegian University of Science and Technology
Høgskoleringen 1, 7491 Trondheim, Norway

Abstract. This study addresses cybersecurity challenges in industrial control systems (ICS), proposing strategies to mitigate risks and enhance system integrity. By analyzing common vulnerabilities and attack vectors, the research offers a comprehensive framework for safeguarding ICS environments. The findings emphasize the importance of robust security measures to protect critical infrastructure and ensure operational continuity.

Keywords: cybersecurity, industrial control systems, risk mitigation, system integrity, critical infrastructure

Introduction

Industrial control systems (ICS) are integral to the operation of critical infrastructure across various sectors. As these systems become increasingly networked, they are exposed to a growing array of cybersecurity threats. This paper explores the strategies necessary to protect ICS from cyber attacks, focusing on identifying vulnerabilities and implementing robust security protocols. By examining past incidents and analyzing current threats, the research provides a framework for enhancing ICS security. The study highlights the need for continuous monitoring and adaptive defense mechanisms to safeguard these vital systems, ensuring both operational continuity and the protection of sensitive data.

This is a preliminary version. To read the full version of the article, please purchase a subscription.

References

1. Рагимов, Э. (2011). КВАЛИМЕТРИЧЕСКИЕ ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ ПРОГРАММНЫХ КОМПЛЕКСОВ, РЕАЛИЗУЮЩИХ СИСТЕМУ УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕТЯМИ. Problems of information technology, 2(1), 18-23.