Securing ICS Post-SolarWinds

Pauline Wu

CyberSecurity Service Provider Internship Program, ICS 296, 396 & 691C, Fall 2023

Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)

Problem Statement:

The 2020 SolarWinds hack highlighted serious vulnerabilities in the software supply chain, posing a major threat to the security of Industrial Control Systems (ICS). Urgent action is required to bolster security measures within ICS-operating organizations. Despite the acknowledged significance of securing ICS software, a lack of standardized practices and comprehensive solutions hinders effective prevention and mitigation of vulnerabilities in these environments.

Purpose:

The purpose of the research is to comprehensively investigate the current state of software security within Industrial Control Systems (ICS) and emphasize the critical role of securing ICS software. The study seeks to identify existing practices, assess their effectiveness, and propose recommendations to enhance the security and resilience of ICS environments.

Approach:

Our research employed a systematic literature search strategy, starting with foundational papers like "Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS)" for a broad understanding of ICS cybersecurity. We then expanded our exploration using references from these papers to include specialized and recent sources. Our search was guided by the specific domain and vulnerability types within ICS, aligning closely with our research problem. This targeted approach ensured a comprehensive view of both foundational and cutting-edge research. Important insights from each paper were synthesized to build a nuanced understanding of cybersecurity threats and vulnerabilities in Industrial Control Systems.

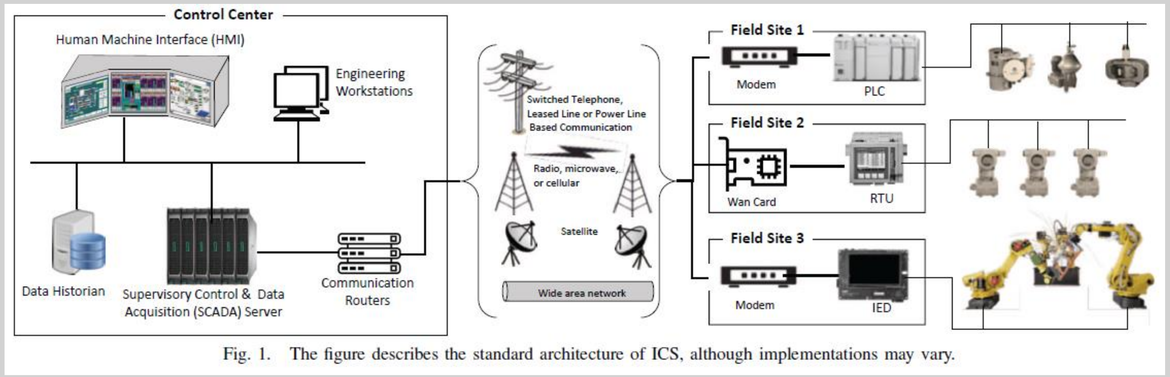

Fig. 1. The figure describes the standard architecture of ICS, although implementations may vary.

Discussion & Conclusion:

Our study on ICS software security post-SolarWinds, prompted by critical vulnerabilities, explored existing practices, their effectiveness, and recommendations for fortifying ICS security. Despite limitations like recruitment challenges and potential biases, our literature review provides valuable insights. Findings highlight the SolarWinds hack as a catalyst for urgent security practices (Lou, 2021), emphasizing weaknesses in ICS software (Gonzalez, 2019). Booth's framework (2016) offers a structured tool, and Karnouskos's (2011) insights broaden our understanding of cybersecurity impacts. Okutan's (2023) focus on automation aligns with contemporary trends, and Korkmaz's (2016) security testbeds provide practical implementations. Advocacy for integrating safety and security measures (Yang, 2014; Kriaa, 2015) underscores the interconnected nature of these domains, emphasizing the need for a coordinated effort to safeguard critical components within ICS, considering both physical and cyber aspects.

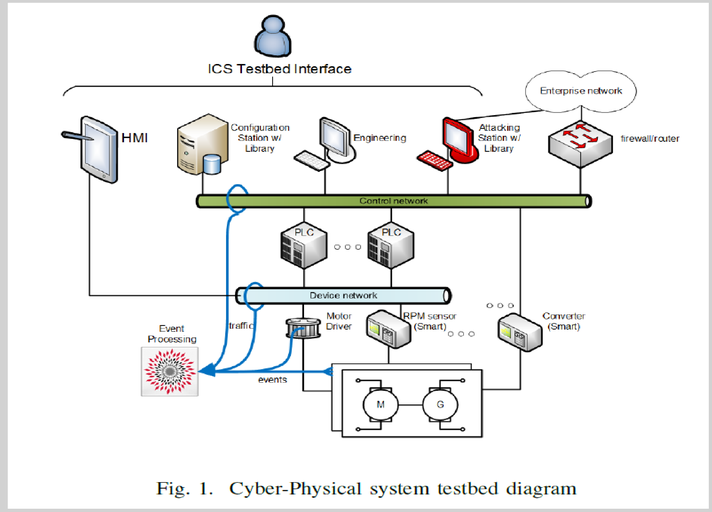

Fig. 1. Cyber-Physical system testbed diagram

Path Forward:

Future research should develop a comprehensive vulnerability analysis framework, explore resilience strategies, and integrate safety and security measures in ICS. Expanding real-world testing environments and conducting longitudinal studies will contribute to ongoing efforts in fortifying critical infrastructure.

References:

Korkmaz, E. (2016, June). Industrial Control Systems Security Testbed. ResearchGate.

Yang, W. (2014, August). Cybersecurity Issues of Critical Components for Industrial Control Systems. IEEE Xplore.