University of Nebraska Lincoln | NEBRASKA CENTER FOR ENERGY SCIENCES RESEARCH

Cycle 16
January 2022

Investigator: Hamid Sharif
Position Title: Professor
Department: Electrical and Computer Engineering

Email: hsharif@unl.edu

Phone: (402) 554-3628
Webpage: https://engineering.unl.edu/ece/faculty/hamid-sharif/

A Novel Framework for Cybersecurity Vulnerability Analysis of Energy Sector OT Communications Technologies

Abstract: Historically, the focus of Operational Technology (OT), such as building control systems, networked occupancy sensors, valve controllers, phasor measurement units (PMUs), etc. in Industrial Automation and Control processes was never on cybersecurity. Energy Sector OT benefited from inherent system isolation. But the trend in IT-OT Convergence means that previously isolated systems are now connected to IT systems and the internet, which poses a significant cybersecurity challenge.
This proposal seeks funding to conduct a pilot study for a modeling and simulation framework to evaluate cybersecurity capabilities, flaws and risks in Energy Sector OT communications protocols. This builds upon this team's proposed OT Protocol Specification Language (OTPSL) – an intermediate descriptor language that makes a human-readable protocol specification machine-understandable to automate the analysis and verification process, with emphasis on:
- **Confidentiality**: Can attackers intercept and observe the OT system data?
- **Integrity**: Can attackers modify the transmitted data to elicit a malicious response?
- **Availability**: Can attackers exploit this protocol to cause the OT system to stop operating?
- **Safety**: Can attackers use the above three to impair the OT system's operation and cause physical harm to people?

In parallel to OTPSL's formal verification methodology, this team will develop Hardware-in-the-Loop (HWIL) simulation capabilities for OT protocol implementation analysis. This utilizes network simulations paired with the OPAL-RT realtime simulator facility established jointly between UNL's Advanced Telecommunications Engineering Laboratory (TEL) and UNMC. Throughout this project we will utilize UNMC's power infrastructure as a case study highly representative of deployed energy sector OT technologies and relevant to the energy sector stakeholders. Our plan is to use this pilot study to complement our current cybersecurity work with Oak Ridge National Lab to secure extramural funding from the Department of Energy and other agencies for conducting a systematic and comprehensive cybersecurity analysis of energy sector OT technologies.