ABSTRACT for the 2017 ISA WWAC Symposium

Defending Against Cyber Attacks

Best Practices for Securing your Industrial Control System

Witucki, Richard [1]*, DesRuisseaux, Daniel[2]

[1]Schneider Electric, 30000 Mill Creek Ave, Alpharetta GA, 30022
(*correspondence: richard.witucki@schneider-electfric.com)
[2] Schneider Electric, 1 High St # 5, North Andover, MA 01845

SUBMISSION TYPE

30 minute presentation

KEYWORDS

Cyber, Cybersecurity, Security, ICS, Automation, Defense in Depth, DiD, Risk, Malware, SCADA, DCS, SIS

ABSTRACT

In this session, we will discuss practical techniques to strengthen industrial control systems against cyber-attacks. The session will begin with a brief overview of the current threat landscape, and actions taken by customers, the industry, and vendors to improve cybersecurity. The session will then transition to an overview of cybersecurity features that are being added to industrial control equipment. The session will review potential attack vectors (web access, rogue Modbus client, IP spoofing, stolen password, malware via USB, and malware via URL) and provide a hands on demonstration of how new security features in industrial control systems can be configured to counter attack vectors to mitigate risk. The session will couple practical demonstrations with instruction to maximize the understanding of concepts.

ABOUT THE AUTHORS

Rich Witucki *is a Cybersecurity Architect for Schneider Electric in the U.S. He works closely with sales, professional services and the end customer to provide best in class solutions. Rich's experience includes design, build and program of custom test and control systems on a variety of hardware and software platforms and the integration of these systems at all levels of the organization. Contact: richard.witucki@schneider-electfric.com*

Dan DesRuisseaux *is a Cybersecurity Offer Manager within Schneider Electric's industry business unit. Dan has over 25 years of experience in defining, marketing, and selling technical products and solutions. Core responsibilities include creating cybersecurity strategy, driving cybersecurity features in product line roadmaps, and working with best in class partners to improve solution security.*