Demystifying Cyber Attacks on ICS: How They Work and How to Use Engineered and Cyber Layer of Protections

Bryan Singer[1]*

[1]Kenexis, 3626 Timber Oak Circle, Helena, AL 35022
(*Email: bryan.singer@kenexis.com and Phone: 614-451-7031x121)

SUBMISSION TYPE

30 minute presentation – Guest Speaker

KEYWORDS

Cyber-attack, Industrial Control Systems (ICS), IT, Cyber-physical Integrity

ABSTRACT

Recent developments in ICS focused malware and documented attacked against ICS such as the Ukranian Power Grid incident show that successful attacks against ICS are growing in sophistication, and are often using complex multi-faceted techniques to manipulate physical processes. The traditional IT safeguards are shown to be insufficient in many cases. In most cases, the least cost and most effective solutions are to use engineered safeguards that are fundamentally resistant to cyber-attack. This presentation focuses on the concept of cyber-physical integrity, as an extension to mechanical integrity, and how to understand how to model and prevent cyber failure of an ICS through blending engineered layers of protection with IT security solutions.

ABOUT THE AUTHORS

Bryan Singer *is a Principal Investigator with Kenexis Security Corporation, based in Columbus, Ohio. In his over 25 years' experience, he continues as one of the primary catalysts in the field of industrial control systems and SCADA security. His primary professional responsibilities include cyber vulnerability assessment, penetration testing, security program design, incident response, forensics, and cyber threat research.*

Mr. Singer began his professional career with the US Army as an operator in Intelligence including disciplines in network and computer security. Professionally trained as a software developer and has written code in over 30 languages to date, and has extensive experience in Unix and Windows administration, network design, network performance analysis, intrusion detection, forensics, incident response, incident investigation, and security testing. He has worked for such great companies as Bellsouth, Rockwell Automation, and Tenet Healthcare Corporation before founding Kenexis Security in 2008. Kenexis Security was founded to focus on the intersection between safety and security, with the goal to create more cyber resilient facilities operating at the highest availability and efficiency possible

using the optimum blend of process engineering, automation system design, safety instrumented systems, physical safeguards, and IT security technologies. He has conducted cyber vulnerability assessments, penetration tests, and cyber security program design for over 3000 plants spanning 5 continents, and 49 of 50 states across nearly every industry sector.

Mr. Singer is a frequent speaker, trainer, and author on industrial cyber security including co-author of the book"Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS" and the soon to be published book "Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions." He also is a co-inventor on an industrial firewall patent, and holds various security certifications, and is a top rated instructor in ICS security for ISA including webinars and live courses. Contact: bryan.singer@kenexis.com