ABSTRACT for the 2015 ISA WWAC Symposium

# Looking for Trouble on OT Networks

Tools and Techniques to Identify Threats to ICS Communications

Bryan L Singer, CISSP, CAP[1]*

[1]Kenexis, 3366 Riverside Drive, Suite 200, Columbus, OH 43221
(*Email: bryan.singer@kenexis.com and Phone: 614-643-2451)

## SUBMISSION TYPE

30 minute presentation

## KEYWORDS

OT Network, Threat, Security, Intrusion Detection, Wireshark

## ABSTRACT

In today's OT networks, Industrial Control Systems such as SCADA use information to drive the physics of process control. Maintaining mechanical integrity of the connected process requires thorough understanding of the communications between these components in order to maintain safe and efficient operations. In this cyber-physical world, is often difficult to spot communications errors, cyber security threats, and poor network health problems. The symptoms, however, are obvious: slow HMI updates, unexplained shutdowns, and in the worst cases, dangerous failures of ICS components. A robust and healthy OT network is key to preventing these failures. This talk focuses on the tools and techniques used by professional cyber security including Network Security Monitoring (NSM), Intrusion Detection Systems (IDS), and manual analysis techniques with Wireshark that investigators use to find and isolate problems on OT networks before they cause harmful impacts, or worse found by our adversaries.

## ABOUT THE AUTHORS

**Bryan Singer, CISM, CAP** *is a principal investigator with Kenexis Security Corporation. He has over 23 years of experience in information technology security including 16 years specializing in industrial automation and control systems security, critical infrastructure protection, computer and ICS forensics, counter-terrorism, network design, and software development. He was the founding chairman and co-chairman of ISA/IEC 62443 (ISA-99) Industrial Automation and Control Systems Security Standards Committee from 2002 until 2012, past board member of DHS's Process Control Systems Forum (PCSF), member of the NERC CIP SAR Drafting Team, and current Director Elect of the ISA Safety and Security Division. He is co-inventor on a patent (2006015586) for firewall methods and apparatus for industrial protocols, and is a co-author on the highly rated book, "Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS". Contact: bryan.singer@kenexis.com.*