Abstract Submission: WWAC Symposium 2018 Call for Papers
Submitted January 31, 2018, via email to: abstracts2018@isawwsymposium.com, provenzano2@comcast.net

Track 2: SCADA Security
Format: 30-Minute Presentation | No Paper
Speaker: Ken Frische
Abstract Narrative:

Why Operational Technology (OT) Deep Packet Inspection is Necessary for Comprehensive SCADA Security

The emergence of new malware such as Triton (also called Trisis/HatMan) is shaping technologies for cyber-securing critical infrastructure worldwide. Triton recently impacted a facilities industrial control system (ICS) known as the Triconex safety instrumented system (SIS), threatening to cause major operational and safety consequences. The attack illustrated the necessity of anomaly detection in the forms of deep packet inspection (DPI) and applications whitelisting to combat today's escalating threat to automated and SCADA systems.

DPI technology extends beyond basic firewall, perimeter and signature-based defense. It enables enhanced visibility and control by accessing the detail of critical commands and values shared by devices, networks and machines that define how the overall operation behaves. DPI supports this ability by providing a clearer view of the critical commands and values shared by devices, networks and machines that direct overall operational behavior. DPI technology fully parses the protocols used for this communication with no impact on operations.

This session will explore how DPI functionality delivers enhanced control and visibility to fill the voids left by legacy ICS devices and technology in SCADA networks. It also will consider network segmentation with DPI as a best practice, to and from remote stations. Attendees will learn how this technology can be used to enforce an application whitelisting policy with relative ease to afford protection at the network layer.

Takeaways will include:

- How to fully parse the protocols used for communications without impacting the operation
- Enhance visibility and controls to fill the voids left by existing ICS devices and technology
- How to enforce an application whitelisting policy to protect embedded devices at the network layer
- Methods for increasing network visibility for external software-based anomaly detection tools

About Kenneth Frische
Email: kenneth.frische@ultra-3eti.com
Phone: 301.670.6779

Ken Frische is Director of Cybersecurity for Ultra Electronics, 3eTI. He brings the company 30 years of experience providing IT and OT solutions, services and consulting for the defense, energy, chemical and other industries. For 3eTI, Ken specializes in product design and marketing for the company's award-winning cyber product suite. He provides customers cyber consulting services, partner relationship management, and ISA 62443 series training.

Prior to joining 3eTI, Ken held senior-level technical positions, specifically in IT and cybersecurity/solutions architecture, for organizations including aeSolutions, InSource Solutions, First Union Bank and CC Dickson Co. Ken holds an MBA from the University of Oklahoma and a bachelor's degree in computer science from Purdue University.