ABSTRACT for the 2016 ISA WWAC Symposium

Designing ISA 62443 Cybersecurity compliant Virtual Machine (VM) architectures

Kenneth Frische*

AE Solutions, 9129 Rocky Point Road, Lakesite, TN 37279-3044
(*Email: Kenneth.Frische@aesolns.com and Phone: 423-413-3520)

SUBMISSION TYPE

30 minute presentation

KEYWORDS

Cybersecurity, Virtual Machine, IT, OT, Networks

ABSTRACT

Virtual machines offer great advantages in cost, resource utilization, performance, backup/recovery, redundancy, and testing, but they also come with their own unique architectural vulnerabilities very similar to those encountered with physical networks and systems. If these vulnerabilities are not recognized and addressed there could be pathways into your process control network(s) that you did not know existed.

Cyber Security Architects focus on designing system and network architectures that segment and protect their IT and OT systems (Process Control Networks and Assets). They include security considerations for hardware and the software that runs on that hardware. There is however a category of software that often gets little or no attention; that of VM host software and the actual VMs. This omission usually happens because network standards don't often exist for virtual network configurations. In addition, the physical system and network architectural design effort is usually finished prior to the VM installation and configuration; often implemented by an installation focused group over an extended period of time. It is effectively assumed that if the network architecture is already deemed cyber safe then the VM installations and configurations could not significantly affect that rating. We will make the case that this is not true.

VMs are now found in "virtually" every IT architecture; and now, commonly found in Process Control Networks. Unfortunately, the knowledge domain for virtualized network interface cards (NICs) and networks is somewhat specialized so the topic is often unaddressed by cyber standards organizations, committees, and certification programs.

The ISA 62443 standard as well does not directly address virtual machines and networks, but it does offer a Zone and Conduit model that can be applied to effectively secure both physical and virtual architectures.

This session will step through the relevant ISA 62443 cybersecurity standards and apply them to the typical network architectures we see in various industries. We will then layer virtual machines and

networks over this structure and highlight the vulnerabilities. Finally, we will correct these architectures in step-by-step manner using the guidance provided by the ISA 62443 standard.

Expected Audience Benefits

- General understanding of the capabilities, concerns, and vulnerabilities inherent in virtual technologies
- General understanding of how to apply the Zones and Conduits approach to virtual technologies
- General understanding of changes needed to IT and OT standards, policies, and procedures so as to maintain security when VM configurations are modified or VMs are copied.

ABOUT THE AUTHORS

Kenneth Frische *has over 28 years' experience in providing IT & OT solutions and services for Military, Oil & Gas, Pharma, Food & Beverage, Packaging, Chemical, Water/Wastewater, Discrete Manufacturing, and Correctional Facilities.*

From hands-on coding to management and consulting, Kenneth Frische has worn many hats to include: IT Director, Solutions Architect, Enterprise Architect, Project Manager, Req/Tech Spec Writer, and Programmer Lead.

His domain expertise includes Process Control and HMI Systems Design and Development, MES integration, Database Management and Design, Business Intelligence / Data Analytics, Business Process Improvement, and Data Warehousing.

Kenneth Frische currently provides risk assessment and secure network design services, cyber security consulting, and ISA 62443 IC32 training as a member of the Cyber Security Services department at aeSolutions. Contact: Kenneth.Frische@aesolns.com