

Position Paper on Research Needs for Secure Control Systems
Beyond SCADA: Network Embedded Control for Physical Systems

Joe Weiss, PE, CISM
KEMA, Inc.

What are the most important challenges:

Industrial control systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), intelligent field devices, smart meters, and smart equipment diagnostic systems. These systems are common across the industrial infrastructure (eg, electric, water, oil/gas, chemicals, etc.). From a cyber security perspective, there are two classes of control systems: existing systems that have been installed or are being sold now which did not consider security as a design objective; and new, undersigned systems where security can be incorporated as part of the initial design. The primary challenge is to secure these existing systems without impacting their performance, reliability, or flexibility in a cost-effective manner. Subtasks to this over-arching challenge include:

- Advanced control systems are moving in such a direction (moving measurement and control to the field devices from a centralized control system such as a SCADA or DCS) that some the security technologies being applied to today's control systems may not be relevant to these new "truly distributed" systems. There is a need to assure that the IT security community and the control system community are moving in the same direction.
- Certification does not exist for control systems or people. Certifying individual components does not address the cyber vulnerabilities of systems talking to other systems. There are VERY FEW individuals world-wide who truly understand control system cyber security as the technologies and security policies and procedures are different than for traditional IT cyber security. Consequently certification for IT security such as the CISSP and CISM examinations may not be relevant, or in some cases, include tasks that could impact control system operations.
- Currently, most industrial control systems software has been developed to good engineering principles with the level of verification and validation (V&V) commensurate with the level of risk. That means that nuclear plant software would have a more rigorous V&V than software for fossil plants or SCADA systems. However, I am not aware of any industrial control systems that have included information assurance requirements.
- Many legacy control systems have neither the computing resources nor the secure operating systems to utilize the security technologies being developed for the non-control system community.
- Many legacy control systems do not have traditional IP stacks. Conventional IT scanning software such as NESSUS can, and has, led to control system impacts. Consequently, appropriate security testing methodologies for control systems are needed that will not affect control system performance.
- Arguably, the most common cyber challenge is the use of commercial off-the-shelf operating systems (eg, Windows) with all of the insecure and unneeded

- applications. The challenge is to understand what services and applications are needed for control system applications and to eliminate the rest without affecting system operation.
- Productivity improvements are accruing from integrating systems, including non-control systems (eg, corporate networks, GIS mapping systems, Enterprise Resource Planning-ERP systems, call management systems, etc.) to control systems. The challenge is to develop methodologies for allowing systems with differing degrees of security (from no security to fully-secured) to communicate with each other.

What are the most important information technology research needs?

- Development of an information assurance program for industrial control systems
- Development of secure Real Time Operating Systems (RTOS) for industrial control systems
- Identification of the minimal amount of resources for security applications – authentication and integrity
- Development of forensics for control systems
- Development of appropriate risk methodologies for non-deterministic control systems where frequencies are not available and consequences can vary significantly depending on the assumptions
- Development of certification for people and processes for control system cyber security
- Development of control system security metrics – how much security is enough?
- How to determine that new adaptive non-deterministic systems and human/software interactions do not introduce new cyber vulnerabilities
- Software development guidelines that include appropriate cyber security recommendations including warnings of buffer overflows and in-secure Application-Programming Interfaces (APIs)
- Development of “skinny” versions of commercial operating systems and web services specifically for control system applications
- Development of specifications for integrating systems with various degrees of security.
- Development of specifications and demonstrations of control system technology with security, performance, and reliability as trade-offs in the design process.
- Development of technologies to securer wireless sensors and wireless communication networks