GridWise™ Interoperability

Joe Weiss PE
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com

Background

There are many reasons for integrating systems within the electric utility industry. Most are for productivity reasons, but there are also regulatory and business reasons. Some productivity improvements accrue from integrating non-control systems (e.g. corporate networks, GIS mapping systems, Enterprise Resource Planning-ERP systems, call management systems, etc.) to control systems. Examples of this approach include fleet asset management, substation automation, and Automated Metering Infrastructure (AMI) each with their own communication protocols. Additionally, "green" forms of generation including wind, solar, wave, micro turbines, etc. will also need to be connected electronically which also introduces potential cyber vulnerabilities.

These different systems utilize different communication protocols with differing degrees of security. Examples of multiple interfacing control system communication protocols include:

Generation:
- Profibus
- Modbus
- Fieldbus
- Hart
- IP

Transmission and Distribution:
- DNP3
- Modbus
- ICCP
- Conitel and other bit oriented protocols
- IEC 61850
- IP

Buildings:
- Bacnet
- IP
- others

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. Interoperability poses an interesting challenge: interoperability generally "opens" systems while security generally "closes" systems. The grand challenge is to have interoperability while maintaining adequate security.

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 (e.g. 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 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 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 communities are moving in the same direction.
- 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 control system communication protocols were developed for interoperability reasons with minimal to no security considerations.
- 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 (e.g. 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.

Summary

Security and interoperability often are attempting to meet mutually exclusive goals. Both need to be included in the design considerations for interoperable systems.