Cyber Security for Process Control Systems Used in Critical Infrastructure (Secure ICS)

Protecting Our Nation's Water Supply

Cyber threats to industrial control systems (ICS) that operate the US water infrastructure are increasing. Any interruption of a safe water supply would erode public confidence and produce significant health and economic consequences. To insure that the nation's water supply continues to operate with no loss of critical function during or after a cyber incident, secure industrial control systems are necessary.

Targeting Cyber Threats

Industrial control systems are an integral part of critical infrastructures, including that found in the water sector. Concern about cyber security issues and their link to industrial control systems has expanded. Concern for the cyber security of industrial control systems results from many factors including the lack of security in legacy systems, increased use of off the shelf hardware and software components, and a growing trend to connect control networks to other networks. Because ICSs connect to, and control, real physical systems, they have unique cyber security requirements. This is highlighted by the fact that cyber-attacks on such systems can lead to serious environmental damage or to loss of life.

Traditional Information Technology (IT) cyber security solutions play a role in cyber security for ICS, but research and development is needed to identify and address the unique cyber security challenges facing ICS.

Developing Technology

The University of Louisville is assessing and developing technology, methods and educational support to mitigate the vulnerabilities of systems that control much of the nation's critical infrastructure, specifically in the Water Sector. This work features a detailed review and analysis of the ongoing research in the area, with particular attention to water system industrial control systems (ICS). Based on this analysis, threats and vulnerabilities to these systems have been identified. A mapping of the vulnerabilities to possible technology solutions has been developed, and solutions addressing high-priority threat areas has been investigated in detail through prototype development, testing and evaluation.

An ICS Cyber Security Landscape Assessment has been completed and reviewed by an advisory board. This comprehensive review includes work at DOE National SCADA Test Bed (NSTB), DHS, CSSP, DHS S&T, industry and universities. Mapping of Water Sector vulnerabilities has also been completed. A patent has also been filed and granted on technology for creating a security hardened remote terminal unit for industrial control systems. This patent may also have application in many cyber infrastructures including power, chemical, water and dam sectors.

To learn more about this project, contact: Jay Robinson, Program Manager, at jay.robinson@hq.dhs.gov or Ewell Balltrip, NIHS, CEO at eballtrip@thenihs.org

2015-01.1pager