ABSTRACT for the 2012 ISA WWAC Symposium

Improving Water and Wastewater SCADA Cyber Security

Based on Work Performed for Large and Small Utilities

Bill Phillips[1]*, and Norman Anderson[2]

[1]Bill Phillips, CH2M HILL, 3011 SW Williston Road, Gainesville, Florida, USA, 32608
(*correspondence: Bill.Phillips@ch2m.com)
[2]Norman Anderson, CH2M HILL, 3011 SW Williston Road, Gainesville, Florida, USA, 32608

FORMAT: 30 minute PowerPoint presentation

KEYWORDS

Cyber Security, Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Vulnerability Mitigation, Large Utilities, Small Utilities

ABSTRACT

Water sector Process Control Systems (PCS) such as Supervisory Control and Data Acquisition (SCADA) systems are inherently vulnerable to various types of well documented cyber attacks such as denial of service, SQL injection attacks, and DCOM exploit attacks due to the use of standard computer hardware, software, and network connectivity. In addition, standard process control hardware is unable to determine the integrity of information or commands that are received and provides little, if any, inherent security features. When a PCS cyber attack occurs, the damage to a water or wastewater utility's reputation in the community, revenue stream, and ability to deliver clean water can be even more severe than the results from a physical attack. There is no one way to completely stop or prevent cyber attacks, but much can be done to reduce the risk of a cyber attack and to be prepared in the event that a cyber attack occurs while maintaining control system functionality and operation.

This presentation is based on work improving PCS and SCADA cyber security with both large and small water and wastewater utilities. Assessment, planning, designing, and implementation strategies for cyber security vulnerability mitigation will be addressed. Examples presented include new build/replacement projects and incremental addition projects. One advantage of incremental addition projects is that they significantly reduce operations disruption and annual cash flow for modifications to existing PCS. Implementation of cyber security solutions were performed using recently published PCS and SCADA specific cyber security standards and network design guides which will also be discussed.

About the Authors:

Bill Phillips, PE specializes in delivery of secure and reliable process control and SCADA network and communications systems, cyber security vulnerability assessment, and facility automation and information system planning and implementation. Bill has over 30 years of process control and SCADA system experience and has focused on control system network and communications cyber security for the last decade. Bill has a BSEE from Clemson University.

Norman Anderson, PE has over 5 years experience in the design and commissioning of Process Control Systems for the Water Sector. Norman has provided secure and reliable PLC, SCADA, and Network hardware and software architecture designs and provided control system automation solutions for a range of facilities. Norman has an M.S. in EE from Iowa State University and an M.S. in Physics from the University of Florida.