A Strategic Approach to SCADA Cyber Security – Water and Wastewater Network Architecture and Segmentation

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

[1]CH2M HILL, 3011 SW Williston Road, Gainesville, Florida, 32608, USA

(*norman.anderson@ch2m.com)

FORMAT

6-12 page paper plus 30-minute presentation

KEYWORDS

Cyber Security, Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Network Architecture, Network Segmentation

ABSTRACT

Network security for Water sector Process Control Systems (PCS) such as Supervisory Control and Data Acquisition (SCADA) systems continues to be increasingly important and ever evolving due to the need for secure and reliable control systems. Additionally, PCS systems continue to grow and the management of network connected devices and expansion of PCS networks can be difficult and cumbersome. To properly secure PCS networks, a multi-stage process is needed incorporating risk assessment, planning, design, implementation, and maintenance for a comprehensive defense in depth strategy. A critical aspect of defense in depth is the overall network system architecture and the network segmentation plan. A properly planned and executed network architecture and segmentation strategy lays the foundation for security and simplifies expansion and maintenance of the network.

This paper will discuss industry accepted methods for Industrial Control System network architecture and segmentation strategies as related to Water sector PCS and SCADA systems. Industry standard techniques, based on recently published standards and network design guides, will be discussed showing a layered network architecture approach to security and the use of logical subnets and VLANs for segmentation. The advantage of this approach is that it allows for simpler configuration of network security appliances and for simpler management and expansion of the network leading to increased network availability and a reduction in threat risk. A case study will be used to provide examples of actual methods implemented for a water sector utility.

About the Authors:

Norman Anderson, PE has over 6 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.

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.