Best Management Practices Summit – For Water & Wastewater Utilities
February 22 & 23, 2023 – Online Format – www.bmpsummit.ca

Using a Risk-based Approach for Protecting Against SCADA System Cyber Threats to Municipal Drinking Water Facilities

Graham Nasby, P.Eng, FS Eng, PMP, CAP, CISSP, CISM[1]*
[1] Co-Chair, ISA112 SCADA Systems Management Committee, International Society of Automation
(*correspondence: graham.nasby@grahamnasby.com)

Keywords:
SCADA, Automation, OT/IT, Operational Technology, Security, Cybersecurity, Municipal Water, ICS, Critical Utilities, High Availability, Cybersecurity Management, ISA/IEC-62443, AWWA-GW430, NIST-800

Format: 30 min. presentation

Abstract:

Cyber threats, both malicious and unintentional, represent a significant and growing threat to our collective critical water/wastewater infrastructure. This is particularly the case with OT (operational technology systems), such as SCADA, which are responsible for not only controlling and monitoring water systems, but also ensuring regulatory compliance by way of 24/7 data logging, automated control, operator alarms, and protective shutdown interlocks.   Cyber threats can take many forms. These include ransomware, denial of service, data theft, unauthorized changes, data falsification, and interruption to core functionality such as process control, data logging, alarms, operator screens, reporting systems, communications, and protective interlocks. Cyber threats can also come from many sources, including not only a malicious attacker but also unintentionally when internal staff or vendors inadvertently cause cyber incidents.

The frequency and breath of cyber incidents continue to rise. In the last 5 years there have been more than 50 documented cases of cyber incidents involving water/wastewater SCADA systems. This includes several in Ontario. In addition, there also have been a growing number of cyber incidents affecting municipal IT systems and other public infrastructure. In other critical sectors, cyber incidents and ransomware are now considered to be one of the top risks to business operations and regulatory compliance. Cyber threats are not going to go away – instead they continue to increase in both frequency and sophistication. For water/wastewater utilities, it is imperative that cyber risks be proactively identified, and programs be implemented to control and mitigate the associated risks.

In this talk, the presenter will provide an overview of what the most common types of cyber incidents are and various scenarios of how they can impact water a water utility, ranging from the relatively benign to those severely impacting operations. The talk will then outline the essential components of an effective cybersecurity program, including outlining several ways in which a cyber program can be implemented. Lastly, the talk will provide an overview of the ISA/IEC-62443 series of industrial control system cybersecurity standards and how they can be leveraged, along with the NIST 800 series and AWWA GW430 standards, to develop a comprehensive strategy to counter the ever-growing risk of cyberattacks.

About the Speaker

Graham Nasby, P.Eng, FS Eng, PMP, CAP, CISSP, CISM an industry-recognized leader in the OT (operational technology), SCADA, and industrial automation sector for his efforts in cyber security best practices, standards development, alarm management, and operational efficiency.

Through his work with ISA, CSA, ANSI and the IEC, he has co-authored international standards on systems design, cyber security, industrial automation, alarm management, and HMI systems.

Graham has multi-industry experience, ranging from technical to project/program management, in the pharmaceutical, water/wastewater, nanotechnology, process, and rail transport industries.

His background includes operations, capital projects, construction, program development, and developing long term technology roadmaps. As a technical and thought leader, Graham is a frequent author of industry articles and invited speaker at industry events.

Graham currently holds the position of senior manager of OT security architecture for CN, one of the largest Class 1 railroad and logistics companies in North America. Graham also teaches a night course in engineering law and ethics at McMaster University's faculty of engineering.

Graham has been the co-chair of the ISA112 SCADA Systems Management Standards Committee since 2015.