ABSTRACT for the 2013 ISA WWAC Symposium

Invited Speaker

The Current State of Cyber Security in Municipal Water Plants

John Cusimano[1]*

[1]exida, 64 North Main Street, Sellersville, Pennsylvania, 18960, USA

(*correspondence: jcusimano@exida.com, Tel: 1-215-453-172)

FORMAT

30 minute presentation

KEYWORDS

ICS cyber security, control system cyber security, SCADA cyber security

ABSTRACT

The Water/Wastewater Sector relies extensively on SCADA, DCS, and other control systems that enable automated control of water/wastewater treatment. These systems integrate a variety of distributed electronic devices and networks to help monitor and control purification and distribution of clean water infrastructure. Control systems have helped to improve the productivity, flexibility, and reliability of water/wastewater treatment. However, these same control systems communicate with a multitude of physically dispersed devices and various information systems that can expose these systems to malicious cyber attacks. A successful cyber attack could compromise control systems and disrupt the availability of clean water or result in sanitary sewer overflows (SSO).

In the past few years, the landscape has changed dramatically as the external and internal threats to Information Systems have migrated from their traditional turf in the business systems area to begin attacking industrial systems as well. In addition, recent attacks like Stuxnet and Flame have awakened us to the concept that not only are the control and safety assets targets themselves, but that the threat profiles have expanded to include direct access to those assets.

This presentation will study several actual control system security incidents in the water industry and other related critical infrastructure industries and review the common vulnerabilities that were exploited, the impact of the incidents, the actions taken to prevent future incidents and the lessons learned.

The presentation will also review the findings from several preemptive control system security assessments and discuss how numerous facilities have reduced their risk of unplanned downtime and safety incidents by improving the cyber security of their control and SCADA systems.

About the Author:

John Cusimano, CFSE, CISSP is director of exida's security services division. A process automation safety, security and reliability expert with more than twenty years of experience, John leads a team devoted to improving the security of control systems for companies worldwide. He has conducted or supervised numerous cyber security assessments of industrial control and SCADA systems in a variety of industries including chemical, water/wastewater, oil & gas, and electric power. John is chairman of ISA 99 WG4 TG2 Zones & Conduits committee and co-chair of ISA 99 WG4 TG6 Product Development committee. John is a voting member on the ISA-99 standards committee on control

system security and the ISA Security Compliance Institute's Technical Steering Committee. John is also active in a variety of other ISA99, ISA84, and ICSJWG working groups. John is also a qualified Achilles™ communication robustness test engineer. Prior to joining exida, John led market development for Siemens' process automation and safety products and held various product management positions at Moore Products Co. John started his career at Eastman Kodak Company, where he implemented and managed automation projects. John has a B.S. degree in Electrical & Computer Engineering from Clarkson University and holds a CFSE and CISSP certification.