

SCADA for the New World

Network Security – PLC – HMI Traffic Segregation– Maintainability, Scalability, and Up time

Marios Iacovou^{1*}

¹Brown and Caldwell, Columbus, Ohio, USA

(*Email: MIacovou@brwnncald.com and Phone: 614-923-5010)

FORMAT

30 minute presentation

KEYWORDS

Control System Redundancy, Robust Design, System Integration, HMI-PLC traffic segregation, Network Security

ABSTRACT

The recent technological advances in networking and the broad push and integration towards the Ethernet/IP and TCP/IP networking protocols from HMI, PLC, network infrastructure, and 3rd party system vendors surface the need of enforcing better design practices and procedures to mitigate the associated risks and challenges that many Water and Wastewater treatment municipalities face.

The practices and procedures outlined in this presentation come from personal experiences in SCADA design and programming jobs from the last couple years.

Sharing those experiences will help SCADA professionals digest the challenges and design approaches in preparation for a network infrastructure that is ready to support the integration of new devices and enable developers and integrators to achieve more secure networks by minimizing traffic congestion, reducing packet collisions that could result in traffic storms, and eliminating single points of failure.

Specifically my presentation explores and outlines lessons learned and procedures used in designing a more secure SCADA system. The presentation will touch the area of PLC redundancy and explain the benefits of utilizing and configuring DLR redundancy. In addition, it focuses in a PLC design that segregates HMI and PLC traffic by creating different paths and using appropriate IP addressing for the configuration of a more robust SCADA network.

The presentation material will demonstrate how to increase the uptime of SCADA systems and in general create a more secure SCADA infrastructure that can facilitate the integration of new devices and increase the security of network expansion through third party channels such as 3G/4G, ISP fiber lines and other techniques that are increasing in popularity for remote site expansion, and in general reduce the associated risks, internal and external to SCADA systems.

ABOUT THE AUTHOR

Marios Iacovou is an Electrical and Computer engineer focusing in SCADA systems. He has more than 5 years of experience in PLC, HMI, and network (virtual and non-virtual) configuration and programming with Brown and Caldwell where he has been supporting the SCADA needs of several water and wastewater treatment municipalities in the Mideast region.