Course Overview

Course number: MOPC-0009-WS
Course length: 1 day

In a world where unauthorized access to systems and cyber-terrorism have led to compromise of vital information and actual physical damage to control system components, security has assumed a much higher priority. Building on the material covered in MOPC-0007-WS, and using the same tools and mechanisms, this workshop will teach participants the basics of applying tighter access control to OPC architectures and components.

During this workshop, participants will:

- Learn about the current threat environment
- Discuss best practices for implementing and configuring security in modern process control and automation systems
- Configure Windows security to restrict access to OPC servers
- Use OPC applications to enhance Windows security
- Learn how the OPC Security specification can be implemented to provide server-level access control

Course Benefits

Participants will gain hands-on experience in assessing the current security posture of their system, and implementing and configuring additional security mechanisms, in accordance with their site-specific Security Policy.

Completion of MOPC-0007-WS, MOPC-0008-WS, and MOPC-0009-WS will grant the student MatrikonOPC Systems Integrator certification. To learn more about MatrikonOPC Systems Integrator certification and how the completion of this course can be used for Educational and Professional Credits visit:
http://matrikonopc.com/training/workshops/opc-workshops-opcsi-certification.aspx

Course Delivery Options

- In-Center Instructor-Led Training
- On-Site Instructor-Led Training
- Virtual Instructor-Led Training
- Hybrid Instructor-Led Training

Who Should Take This Course?

The Industrial Cyber Security for OPC Workshop is principally targeted at Process Control Engineers, Technologists, Technicians and managers responsible for the commissioning and day-to-day operation of automation and process control systems. It also contains information relevant to security audits, managers and administrators responsible for the design of process control architectures, selection of technologies and software and the purchase of both hardware and software for these systems.

Prerequisite/Skill Requirements

Prerequisite Course(s)
- None

Required Skills and/or Experience
- Microsoft Windows and basic computer use
- An understanding of automation requirements

Desirable Skills and/or Experience
- It is recommended that participants in this workshop have completed the OPC Classic Fundamentals workshop

Course Topics

ICS Threats, Vulnerabilities, and Risks: This module discusses the current issues faced by organizations in securing their industrial control system environments. Known threats such as the Stuxnet virus and other malware, social engineering and other vectors or sources of attack as well as vulnerabilities inherent to control network equipment and configurations that can be exploited by those threats are discussed.

Best Practices for Secure Industrial Network Architecture: Recommended approaches for securing process control networks including policies, procedures and technologies that should be developed or implemented within a comprehensive cyber security framework will be discussed throughout the workshop.

Operating System Security: This module discusses carrying out all of the necessary configuration items to allow OPC communication to take place both locally and remotely. The Windows Operating System Security topic provides the basic structure to explain these settings and the Windows security framework that supports them.
Course Topics cont’d

**Securing OPC Communication:** This module discusses how to ensure the security of OPC communications within the secure network architecture framework addressed earlier in the workshop. It covers technologies and procedures recommended in order to achieve secure and reliable OPC communications.

**The OPC Security Specification:** This module looks at the Security specification, and how it affords vendors the opportunity to implement an additional level of authorization on the OPC server itself. The MatrikonOPC implementation of this specification will be discussed in detail, along with mechanisms for implementing a consistent security implementation across multiple OPC applications.

**Troubleshooting and Mitigating Security Issues:** This module discusses methods for addressing security issues discovered on OPC systems in process control networks. This topic provides procedures and tools for troubleshooting issues, repairing problems and mitigating future potential issues from occurring again or in other areas of the network.

**Workshop Schedule**

http://matrikonopc.com/training/workshops/course-schedule.aspx

**Additional Training**

To increase your knowledge and skills, there are additional courses available from Automation College.

For more information and registration, visit www.honeywellprocess.com/en-US/training.
