American Water Works Association

Dedicated to the World's Most Important Resource™

WEBINAR:

Practical Examples of Delivering Cybersecurity at a Water Utility

May 4, 2016

2016 Webinar Sponsors

Badger Meter

WOODARD & CURRAN

2

Webinar Moderator

Kevin Morley, Ph.D.

Security & Preparedness Program Manager
American Water Works Association

Kevin M. Morley, Ph.D. is the Security & Preparedness Program Manager for the American Water Works Association (AWWA). In this role he works closely with a variety of organizations tasked with advancing the security and preparedness of the Nation's critical infrastructure, including DHS/FEMA, EPA, USACE, CDC and the Water Sector Coordinating Council. This has included facilitating the expansion of mutual aid and assistance via the Water/Wastewater Agency Response Network (WARN) initiative. In addition, he has supported the development of water sector standards and guidance for security and preparedness, including ANSI/AWWA G430: Security Practices for Operations and Management, ANSI/AWWA G440: Emergency Preparedness and ANSI/AWWA J100: Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems. Most recently he led the development of a resource guide entitled Process Control System Security Guidance for the Water Sector and a supporting Use-Case Tool which provides a water sector-specific approach to the NIST Cybersecurity Framework. Dr. Morley received his Ph.D. from George Mason University for research assessing the resilience of the water sector through the development of the Utility Resilience Index (URI). He holds a M.S. from SUNY College of Environmental Science and Forestry and a B.A. from Syracuse University.

3

Enhance Your Webinar Experience

- Close
  - ✓Email Programs
  - ✓Instant messengers
  - ✓Other programs not in use
- GoToWebinar Support

  http://support.gotomeeting.com/ics/support/default.asp?deptID=5641

4

Webinar Survey

- Immediately upon closing the webinar
  - Survey window opens
  - Thank you

5

Products or Services

The mention of specific products or services in this webinar does not represent AWWA endorsement

AWWA does not endorse or approve products or services

6

Panel of Experts

Cheryl Santor
Information Security Manager
Metropolitan Water District of So. CA

Charles Aycock
EIM Systems Coordinator
City of Roseville

Brian Draper
IT Security Specialist
DHS, ICS-CERT

Graham Nasby
Water SCADA & Security Specialist
City of Guelph – Water Services

7

Agenda

I. NIST Cyber Security Framework to Improve Critical Infrastructure	Cheryl Santor
II. Working with the Department of Homeland Security ICS-CERT A Partnership for Success	Charles Aycock Brian Draper
III. SCADA Security at City of Guelph Water Services	Graham Nasby

8

Ask the Experts


Cheryl Santor


Charles Aycock


Brian Draper


Graham Nasby

Enter your **question** into the **question pane** at the lower right hand side of the screen.

Please include your name and specify to whom you are addressing the question.

9

NIST Cyber Security Framework to Improve Critical Infrastructure

Cheryl Santor, CGEIT, CISM, CISA, CISSP
Information Security Manager
Metropolitan Water District of So. CA

10

Rationale

- How to use the NIST Cybersecurity Framework? Use in conjunction with AWWA Guidance!
- Performance in cybersecurity enhanced by self assessment?

11

Learning Objectives

- Importance a cybersecurity review using the framework
- Identify gaps and future initiatives to enhance cybersecurity
- Assessment provides value
- Create a repetitive process

12

Agenda

- Governance and Risk Management
- Business Continuity and Disaster Recovery
- Server and Workstation Hardening
- Access Control
- Application Security
- Encryption
- Telecommunications; Network Security and Architecture
- Physical Security of ICS/SCADA
- Service Level Agreements
- Operations Security
- Education
- Personnel Security

13

Governance and Risk Management

- Management and Security controls of security systems
- Security polices, procedures and systems Confidentiality, Integrity and Availability (CIA)
- Reliability is what Operations requires
- Inventory – first task in Framework, how can you manage what you don't know?

14

Business Continuity & Disaster Recovery

- Business Continuity Plan(BCP)
  - Control Systems run even if failures occur – reliability
  - Fast recovery
- Disaster Recovery Plan (DRP)
  - Longer disruptions from more impactful events
- DRP and BCP
  - Managed processes
  - Identification of events
  - Estimates of impact
  - Development and monitoring mitigation strategies.

15

Servers and Workstations

- Server and Workstation Hardening
  - Securing servers and workstations against cyber-attacks
  - Best practices to minimize probability of unauthorized access
  - Maintains CIA properties of servers/systems
    - Could include “whitelisting”, only approved applications and processes running

16

Access Control

- Access Control
  - Authorized personnel
  - Restricting resources and information access
  - Separate passwords
  - Rights management,
    - levels of access
    - further enhances controls
    - newer initiatives

17

Encryption

- Encryption –
  - Ensure appropriate encryption schemes
  - Cryptography used where needed/required
  - Weak encryption schemes dangerous
  - Avoid proprietary schemes
  - Standards in encryption technologies

18

Telecomm; Network Security and Architecture

- Telecommunications; Network Security and Architecture
  - Security of network infrastructure
- Layered defense architecture
  - Control Systems are at the core of the design
  - Adherence to new standards
  - Topology requirements
  - Network management

19

Physical Security

- Physical Security of ICS/SCADA equipment
  - Basic requirement for systems
  - Prevent, restrict physical access to authorized personnel
  - Access only when need to perform actions on hardware
  - Monitoring, detecting and responding to unauthorized physical access

20

Service Level Agreements

- Service Level Agreements
  - Definition and management of contracts
  - Define, negotiate, execute and monitor contracts to ensure appropriate service delivery
  - Requires minimum levels of performance, i.e., Committed Information Rate (CIR) for WAN services
  - Typically focus on QoS, SCADA/ICS do not require high bandwidth, but need reliability
  - SLAs with other teams, i.e., Information Technology services

21

Operations Security

- Operations Security
  - OPSEC - operational procedures and workflows to increase security properties (CIA)
  - May want to restrict employees social media re: organizational security procedures
  - Also includes; granting policies and procedures, security guard rotation schedules, backup/recovery, etc.

22

Education

- Education
  - Security awareness training
  - Include clients and service providers for organization
  - Identify best practices
  - Provide formal training on security policies and procedures
  - Training for incident response
  - Test key security processes to assure quick response

23

What is Your Organization Doing?

- What types of audits are conducted? Use NIST Cyber Security Framework and the AWWA Guidance.
- Integrated audits assist in understanding business needs and security.
- Audit/Security go hand in hand, how can you provide more service to the customer?

24

Personnel Security

- Personnel Security
  - Personal safety of employees, clients, contractors, and general public
  - Starts in part with hiring, background checks
  - Periodic recheck of employees and updates of policies and procedures
  - Purpose – personnel safety and integrity
  - Applies to external contractors and service personnel, ensure lower level privileged access

25

Summary

- Start using the NIST Cybersecurity Framework with the AWWA Guidance tool. The benefits are it is easy and provides a roadmap to follow.
- DHS and NIST are resources to assist with assessments, but the value of the knowledge by conducting an assessment will move your organizations forward.

26

Ask the Experts


Cheryl Santor


Charles Aycock


Brian Draper


Graham Nasby

Enter your **question** into the **question pane** at the lower right hand side of the screen.

Please include your name and specify to whom you are addressing the question.

27

Working with the Department of Homeland Security ICS-CERT

A Partnership for Success

Charles Aycock
EIM Systems Coordinator
City of Roseville

Brian Draper
IT Security Specialist
DHS, ICS-CERT

28

Rationale

- Legacy SCADA System
  - Obsolete VMS Platform
  - Don't touch unless it's broken
  - "Isolated" from outside world
- New SCADA System
  - Virtualized Server System
  - Remote Deployment and Access
  - Significantly more complex network
  - Two SCADA System Technicians

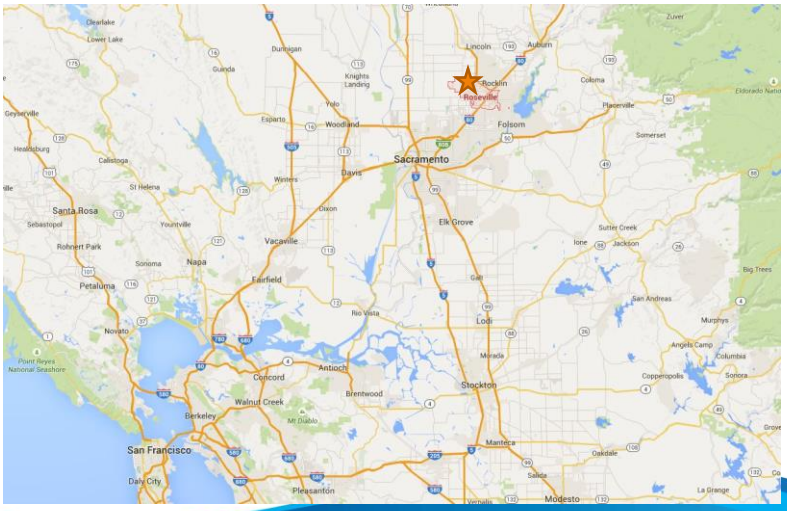
29

Learning Objectives

- Offerings provided by DHS
  - Cybersecurity Evaluation Tool
  - Design Architecture Review
  - Network Architecture Verification and Validation
  - Training

30

Project Location – Roseville CA



Roseville, CA

- Major SCADA Systems Replacement Project affecting:
  - Water Treatment Plant (100MGD)
    - 21 Water Distribution facilities
    - 6 Storm Water facilities
  - 2 Wastewater Treatment Plants (18 and 12MGD)
    - 14 Wastewater Collection Facilities
    - 2 Recycled Water Pumping Stations

Before You Begin

- Educate Management about DHS's 'FREE' Offered Services
  - DHS is there to lend their knowledge and experience to help you understand where you stand relative to your peers.
  - DHS Staff are not there to impose policies or procedures on your organization.
  - The outcome of their assessments result in "Options for Consideration".

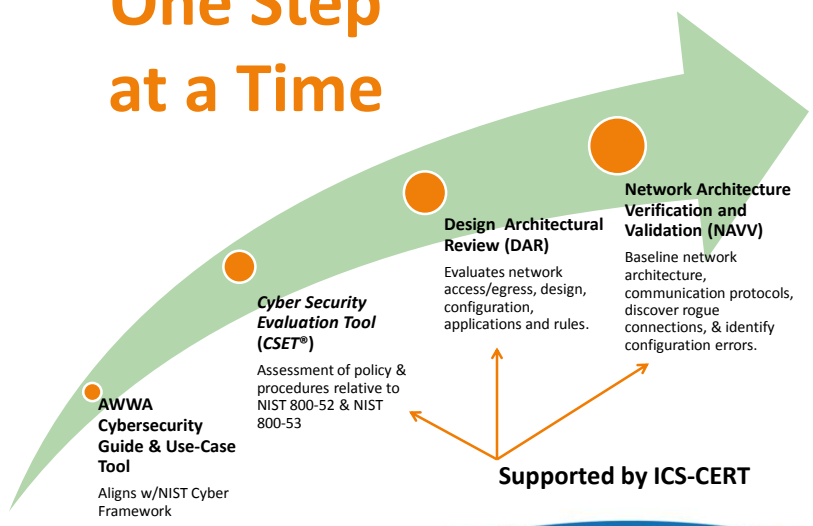
33

When to Contact DHS

- If possible, plan to collaborate with DHS during design and implementation
  - We were fortunate to have DHS input during our architecture design phase
  - Worked with our implementation team directly
- If an existing system, plan to work with them when schedule permits.
  - You don't have to do all of the steps, but I would highly encourage it.

34

One Step at a Time



35

Cyber Security Evaluation Tool (CSET)

- Self-Assessment and Facilitated Assessments available
  - Questionnaire format
    - Garbage in = Garbage out
      - Need to be honest with responses
      - If not currently implemented, then recommend responding as not existing
    - Compare
    - Output is a prioritized list of recommendations for improving cybersecurity posture based on recognized industry standards

36

CSET Reporting

Design Architecture Review (DAR)

- ICS Network Architecture
  - Perimeter Defenses (Ingress and Egress)
  - Remote Access methods
  - Field and Device-Device Communications
  - Trust Relationships and Connectivity to Enterprise Networks
  - Wired and Wireless Communications

Design Architecture Review (DAR)

- Asset Inventory
  - Configuration Guidelines relative to Best Practices
  - Backup and Recovery Methods
  - Physical Security of Assets
  - Data Integrity

39

Design Architecture Review (DAR)

- Protective and Detective Controls
  - Means of detecting Intrusions
  - Review of device configurations
  - Threat detection and alerting methods
  - Threat and intelligence sources
    - DHS ICS Alerts and Notifications

40

Network Architecture Verification and Validation (NAVV)

- Evaluate network traffic on ICS network
  - Protocol hierarchy and organization of network traffic
  - Device to Device communications – What are the top 'talkers'
  - Communications traversing (or attempting to traverse) the ICS network boundary
  - Potentially misconfigured devices – or those exhibiting suspicious or anomalous behavior
  - Establishes baseline for your ICS

41

Assessments and Reviews Results

- Regardless of whether it is an assessment or review, DHS will provide:
  - "**Options for Consideration**"
    - Reduces liability for both DHS and Owner
    - Select options within available budget and as appropriate for your needs
    - Results can be compared to related facilities
  - **At no cost to the asset owner**

42

Common Observations

- FY-2015 Top Weakness Categories
  - Boundary Protection
  - Least Functionality
  - Authenticator Management
  - Identification and Authentication (Organizational Users)
  - Least Privilege

43

How Do I Start the Process??

If you're interested in having us come out; the process is easy to start….

- Call us
- Send us an email

44

DHS Offered Training

- https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT
  - Web Based
    - Operational Security for Control Systems (101W) – 1 Hour
    - Cybersecurity for Industrial Control Systems (210W) – 15 hours
  - Instructor Led:
    - ICS Cybersecurity (301) – 5 Days in Idaho Falls, ID – Red/Blue Team

45

DHS Contact Information

- ICS-CERT https://ics-cert.us-cert.gov/
- (877) 776-7585
- (208) 526-0900 (International)
- ics-cert@hq.dhs.gov

Charles Aycock: caycock@roseville.ca.us
Brian Draper: brian.draper@hq.dhs.gov

46

Ask the Experts


Cheryl Santor


Charles Aycock


Brian Draper


Graham Nasby

Enter your **question** into the **question pane** at the lower right hand side of the screen.

Please include your name and specify to whom you are addressing the question.

47

SCADA Security at City of Guelph Water Services

Graham Nasby, P.Eng., PMP, CAP
Water SCADA & Security Specialist
City of Guelph – Water Services

SCADA Security at Guelph Water Services

48

Rationale

- Our Reliance on SCADA for Operations & Compliance
- Uptime and Data Integrity is Key
- Managing Risks
  - External Threats
  - Internal Threats
  - Human Error
  - Equipment Failures

- Safeguarding your SCADA system
- Applying Best Practices from Industry Standards

SCADA Security at Guelph Water Services 49

Learning Objectives

- Common Techniques to Safeguard a SCADA System
- SCADA Network Design Best Practices
- Tips to Safeguard SCADA Servers
- Strength in Redundancy

- Overview of ISA/IEC-62443 “Zones & Conduits” security model
- IT: Information Technology vs. OT: Operational Technology
- Relating back to AWWA Cyber Security Guidance Document

SCADA Security at Guelph Water Services 50

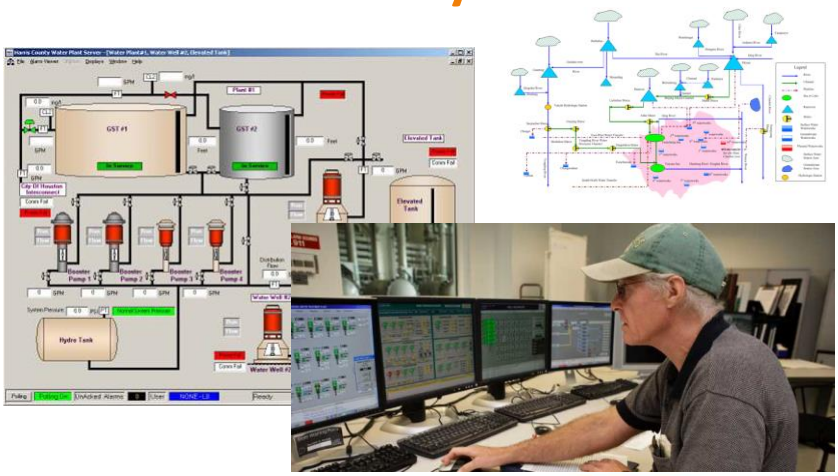
Agenda

- About Guelph Water Services
- Risks to SCADA Systems
- IT vs. Operational Technology
- Leveraging Industry Standards for Cyber Security
- Remote Access Question
- How Guelph Implemented its SCADA System
- Items to Consider when Implementing Remote Access
- Summary and Takeaways

City of Guelph Water Services

- Guelph, Ontario, Canada
- 130,000 residents
- 21 groundwater wells
- 3 water towers
- 549 km of water mains
- 45,000 service connections
- 2,750 fire hydrants
- 46,000 m3/day [12 MGD]

SCADA Systems



Risks to SCADA Systems

- Loss of Process Visibility
- Interruption of Data Logging
- Inability to Remotely Control
- Loss of Automatic Control Schemes
- Other systems not able to access data

Common Threats

- External Hacker
- Equipment Failure
- Network Connectivity
- System Upgrades/Changes
- IT Department Miscommunication

Other Threats

- Human Error
- Naïve Users
- Contractors & Consultants
- After Hours Work
- Bad Luck

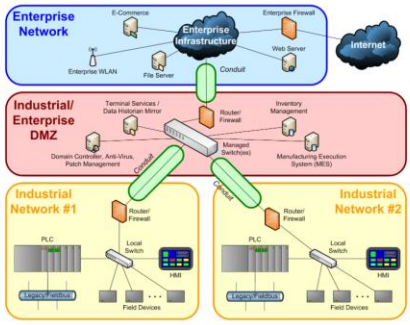
IT vs. OT

- Information Technology: Your IT Department
- Operational Technology: Your SCADA System
- Different Expectations
  - Critical Applications
  - Uptime & Outage Tolerance
  - Allowable Latency
  - Taking Systems Offline for Maintenance or Upgrades
  - Edge Devices vs. Servers

SCADA Security at Guelph Water Services 57

Use Industry Standards as Tools

- ISA/IEC-62443 (formerly ISA-99)
- ISO 27000
- NIST Cyber Security Framework
- AWWA Cyber Security Guidance Document



SCADA Security at Guelph Water Services 58

A look at ISA/IEC-62443

- Zones and Conduits

- Part 1: Definitions & Metrics, Lifecycle
- Part 2: Cyber Security Risk Management Program
- Part 3: Zones and Conduits (Firewall Rules)
- Part 4: Secure Hardware/Firmware Standards

SCADA Security at Guelph Water Services 59

Remote Access – Do You Need It?

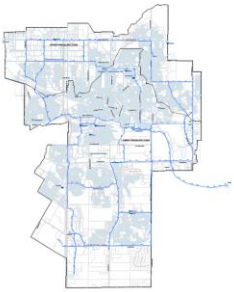
- Who would use it?
- Operational Pros & Cons
- Staffing of Central Control Room
- After Hours Access

- Risks Associated with Remote Access
- Selecting & Maintaining Appropriate Technology

SCADA Security at Guelph Water Services 60

Guelph Water SCADA Architecture

- View Terminals
- SCADA I/O Servers & Historian Servers
- SCADA Network
- PLC Controllers
- Hardwired Backup Control



SCADA Security at Guelph Water Services

61

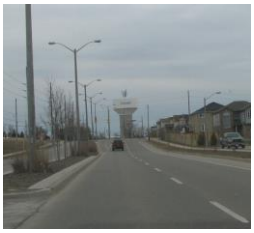
Redundancy: View Terminals

- All have their own HMI code on them
- Located at facilities across the City
- Not Dependant on a Single Server
- Can be re-pointed to backup SCADA Servers

SCADA Security at Guelph Water Services

62

Redundancy: SCADA Servers



- Multiple Server Groups
  - Main Servers
  - Online Backup Servers ("hot backup")
  - Near-Line Backup Servers
  - Multiple data centres
- Using "Virtual Servers" on server hosts
- Servers are backed up 4X per day
- Separate servers by function

Redundancy: SCADA Network

- Guelph chose to have no remote access to SCADA
- Staffed control room and cellular call-out alarms

- Completely separate from Corporate Network
- Privately-Routed SCADA Fibre-optic Network
- Backup Privately-Routed SCADA DSL Network
- We use non-routable IP block addressing for SCADA (172.xx.xx.xx)

Redundancy: PLCs & Data-Loggers

- Multiple Well Sites: 21 groundwater wells
- Site backup Data-Loggers, integrated with historian
- Backup hardwired control for critical interlocks

- Hand-Off-Auto switches on equipment
- Physical Security at sites
- System designed so redundant PLCs not needed

SCADA Security at Guelph Water Services 65

Remote Access: Items to Consider

- Do you need it? Who will use it?
- Internet Connection or Private Network
- Firewalls and Authentication Methods
- Traffic Encryption, NAT, IP Address Ranges
- Segmenting your Network in Zones

- Think Big Picture: System Uptime, Availability, & Data
- Managing Risks & Monitoring System

SCADA Security at Guelph Water Services 66

Summary & Takeaways

- Uptime and Availability are key for SCADA Systems
- Focus should be on resiliency of the SCADA system
- If remote access required, look to ISA/IEC-62443
- Consider other threats to SCADA uptime

- Resources:
  - AWWA Cyber Security Guidance Document
  - NIST Cyber Security Guidance Document
  - ISA/IEC-62443 (formerly ISA-99)

SCADA Security at Guelph Water Services

67

Ask the Experts


Cheryl Santor


Charles Aycock


Brian Draper


Graham Nasby

Enter your **question** into the **question pane** at the lower right hand side of the screen.

Please include your name and specify to whom you are addressing the question.

68

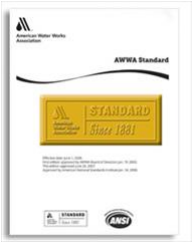
Resources

Process Control System Security Guidance for the Water Sector and Use-Case Tool

www.awwa.org/cybersecurity

Business Continuity Plans for Water Utilities

http://www.waterrf.org/Pages/Projects.aspx?PID=4319



AWWA G430-14
Security Practices for Operation and Management
Catalog No. 47430-2014

AWWA G440-11
Emergency Preparedness Practices
Catalog No. 47440

69

Upcoming Webinars

May 11 – Preparing for Cyanotoxin Events: Learning from Recent Utility and State Experiences

May 18 – Advancing the Capital Improvement Planning Strategy for Your Utility

May 25 – Lead and Copper Rule: Potential Revisions and Steps Utilities Can Take to Prepare

Register for a 2016 Webinar Bundle

- Individual Full Year
- Group Full Year

www.awwa.org/webinars

70

Upcoming Conferences

Register Online at:

www.awwa.org/conferences

71

Thank You for Joining AWWA's Webinar

- As part of your registration, you are entitled to an additional 30-day archive access of today's program.
- Until next time, keep the water safe and secure.

72

Presenter Biography Information

Cheryl Santor has a strong history of banking system security, which she brought to Metropolitan in 1995. She is a certified member of multiple security organizations [list], and works closely with State and Federal Security Agencies to address water industry challenges. She has significant practical experience in addressing Metropolitan's security challenges.

Charles Aycock has been with the City of Roseville over 20 years; in the Environmental Utilities Department. Charles administers electrical, instrumentation and mechanical standards on all capital improvement projects relating to the City of Roseville's water and wastewater treatment facilities, RW, waste collection, water distribution and storm water systems. Charles was a contributing author of WEF's MOP-21, Automation of Water Resource Recovery Facilities, 3rd and the 2014 released 4th edition.

73

Presenter Biography Information

Brian Draper joined the Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) team in November of last year. Prior to joining DHS, Brian spent the past 10 years with the Florida Department of Law Enforcement and was assigned to the Cyber High Tech Crime Sqyad. Brian is an experienced IT security professional with over 25 years of experience in the IT industry. During his career Brian has held positions in desktop support, server security administration, incident response and digital forensics. In addition to Brian's years of experience, he also holds a number of industry certifications.

Graham Nasby, P.Eng, PMP, CAP holds the position of Water SCADA & Security Specialist at City of Guelph Water Services, a publicly-owned water utility located in Guelph, Ontario, Canada. He is senior member of the International Society of Automation (ISA) and past director of the ISA's water/wastewater technical division. As an AWWA and WEF member, he continues to promote the importance of automation and cyber security in the municipal water sector. Graham sits on several international standards committees, including the ISA-99 cybersecurity committee, the IEC TC65 industrial automation committee, and the ISA-18 alarm management committee. In 2013, Graham received the ISA's Technical Division Leader of the Year his contributions to the municipal water/wastewater sector. In 2014, he was recognized with a 'Mid-Career Achievement' award from his alma mater, the University of Guelph's School of Engineering.

74

CE Credits (CEUs) and Professional Development Hours (PDHs)

AWWA awards webinar attendees CEUs. If you wish to take advantage of the opportunity to earn CEUs, visit **www.awwa.org/credits**

Certificates will be available within 30 days of the webinar

75

How To Print Your CEU Certificate of Completion

Within 30 days of the webinar, login to www.awwa.org or register on the website. If you are having problems, please email educationservices@awwa.org.

Once logged in, go to:

- My Account
- My Transcript Information

To print your official transcript, click **Print list**
To print certificates, click **Download certificate**

76

2016 Webinar Sponsors

Badger Meter

WOODARD & CURRAN

77