Setting the Standard for Automation™

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

Graham Nasby
Co-chair ISA112 SCADA Systems standards committee
Guelph, Ontario, Canada

2023 Best Management Practices Summit
For Water & Wastewater Utilities – Feb 22-23, 2023

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

About the Speaker

Graham Nasby, P.Eng., FS Eng, PMP, CAP, CISM, CISSP

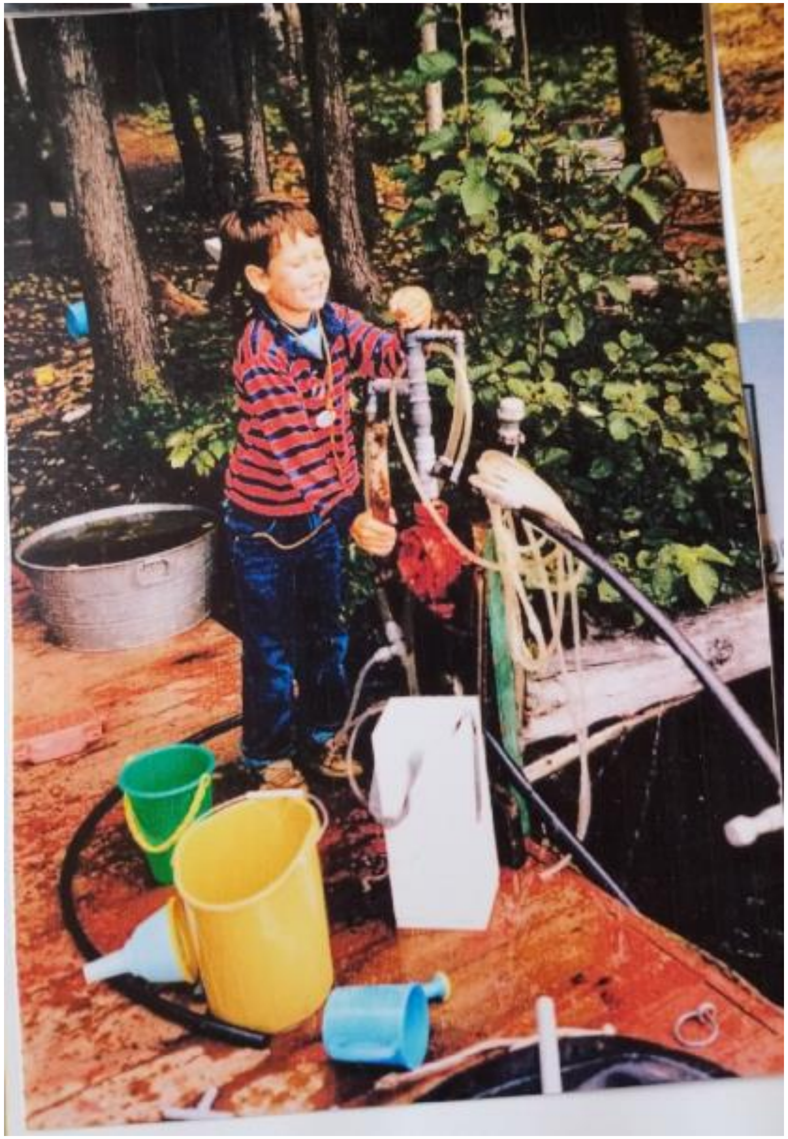
- 20+ years experience in operations, construction and automation sector
- 1998-2005 IT Consultant – University of Guelph
- 2005-2007 – controls specialist at various manufacturers
- 2007-2010 Process Engineer – Cheme Engineering
- 2010-2015 System Integrator & I/C Lead – Eramosa Engineering
- 2015-2022 Water SCADA & Security Specialist – Guelph Water
- 2022-present – Sr. Manager of OT Security Architecture – CN Rail

- Co-chair of ISA112 SCADA Systems standards committee
- Voting member of ISA101 HMI Design and ISA18 Alarm Management committees
- Member of IEC/SCC TC65A “Industrial process measurement, control and automation”
- Member of CSA P125 “Operational Technology: Functional Safety and Security”
- Member of the OWWA Automation Committee since 2015, active in AWWA & WEF 2010-2022

- Sessional instructor at McMaster University (Hamilton, ON) and Conestoga College (Cambridge, ON)
- Has published over 75 papers and articles on various OT, SCADA and industrial automation topics
- Received ISA’s technical division leader of the year award in 2013
- Received “Mid-Career Achievement Award” from his *alma mater* University of Guelph in 2014
- Recipient of the ISA’s society-level Standards Leader of the Year Award in 2021

- Contact: graham.nasby@grahamnasby.com

I wanna be a Water Guy when I grow up!



OK… Trains are cool too!

Presentation Outline

- SCADA Refresher
- Structure of SCADA Systems
- How SCADA Systems are Vulnerable
- Common SCADA Attack Vectors

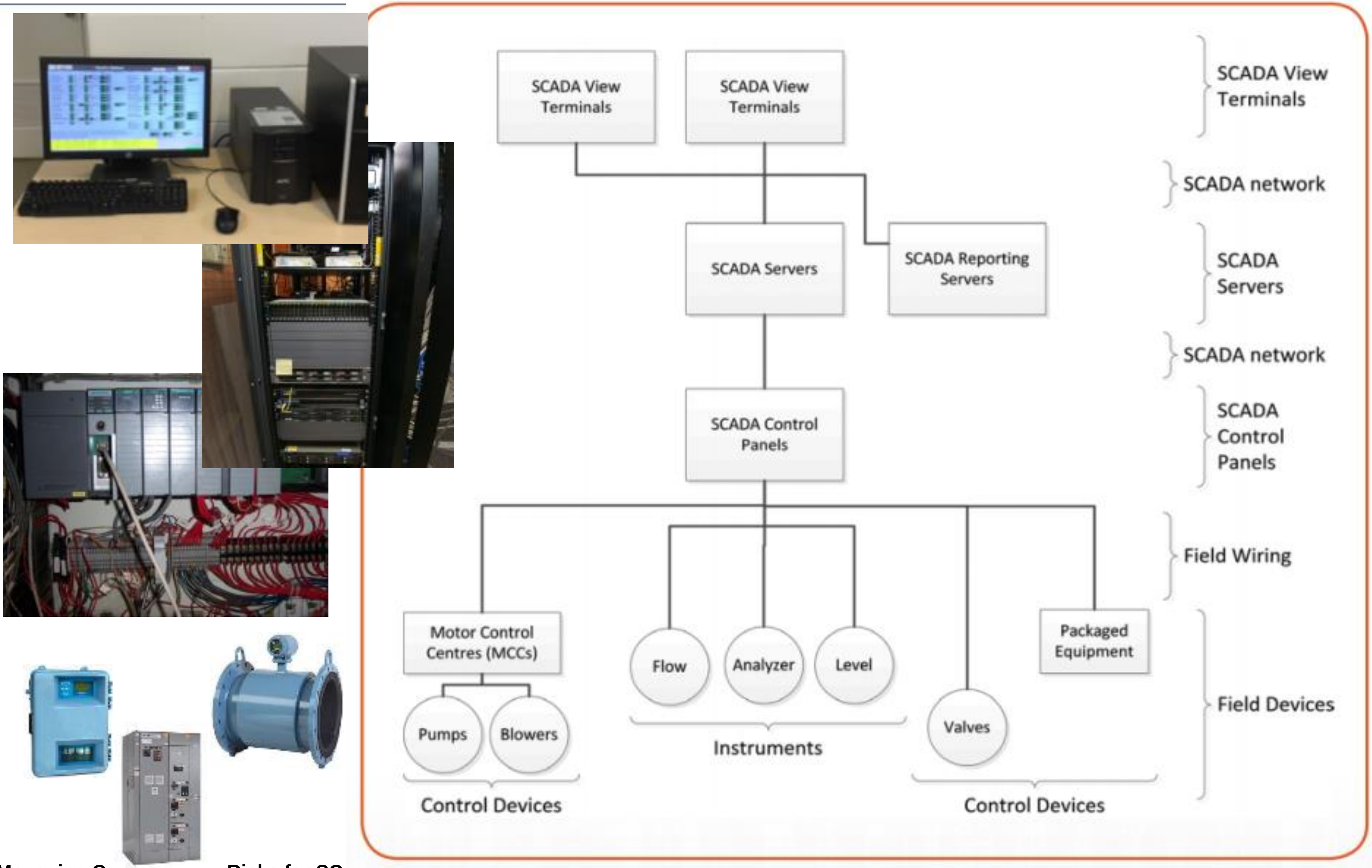
- Typical SCADA Risk Scenarios
- Establishing a SCADA Cybersecurity Program
- Published Technical Standards & Cybersecurity Frameworks

- Overview of the ISA/IEC-62443 Series of Standards
- Defence in Depth, Zones/Conduits, Maturity Level, Security Level
- Putting it All Together
- Challenges with Implementing Cyber Programs at Water Utilities

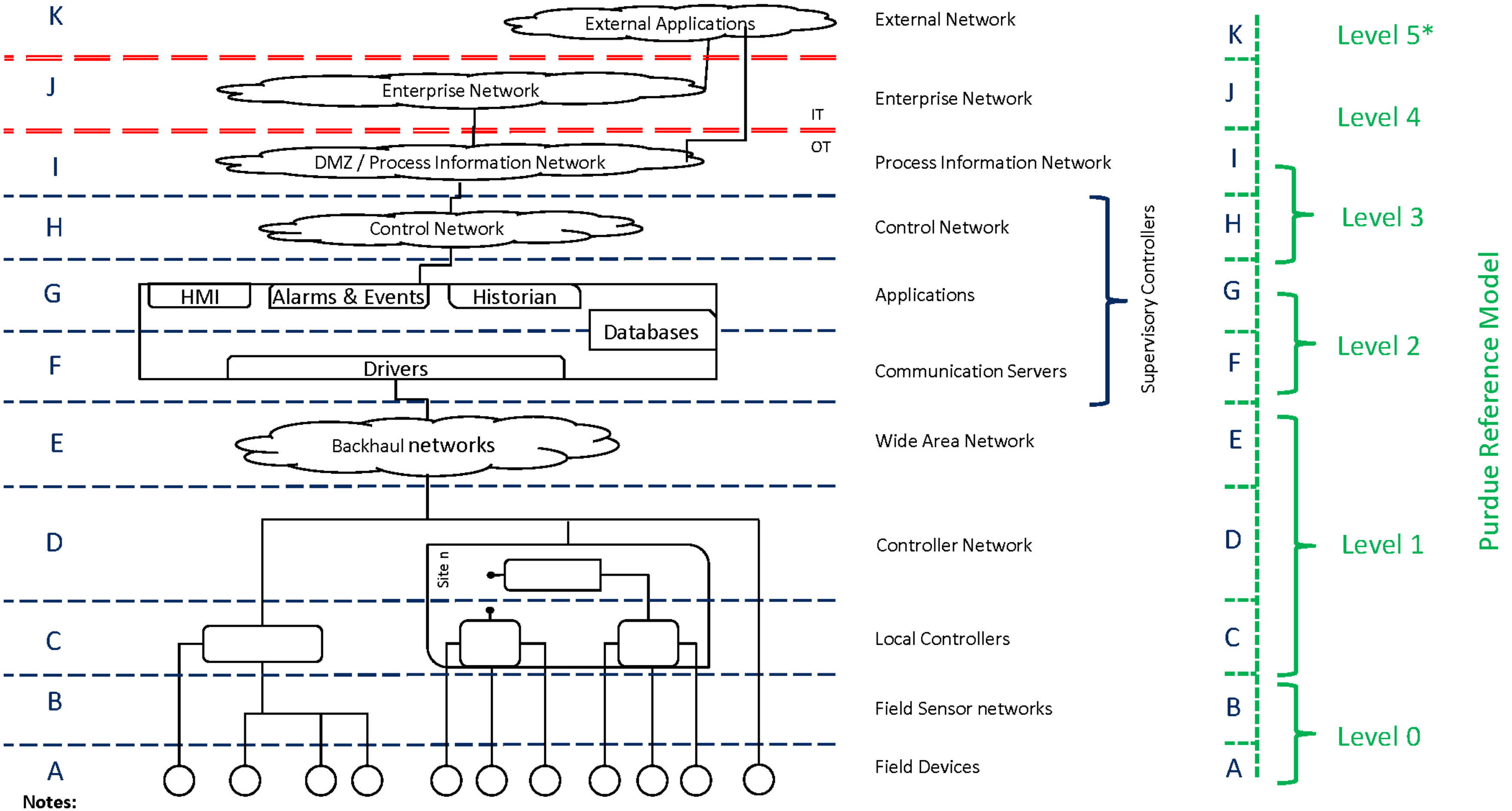
SCADA Refresher

SCADA = Supervisory Control and Data Acquisition

Typical SCADA Architecture



ISA112 SCADA System Architecture



Notes:

1 Letters are used to avoid potential conflict with ISA-95 and other "Layer" models.

2 Routers and Firewalls between layers as well as other system-specific servers, applications ,and workstations are not shown.

3 Individual architectures may vary from the above general model. For example, if only local systems are used Level E may not be required

4 Communications for any remote-hosted external applications (Cloud) with lower levels must be done using extreme care.

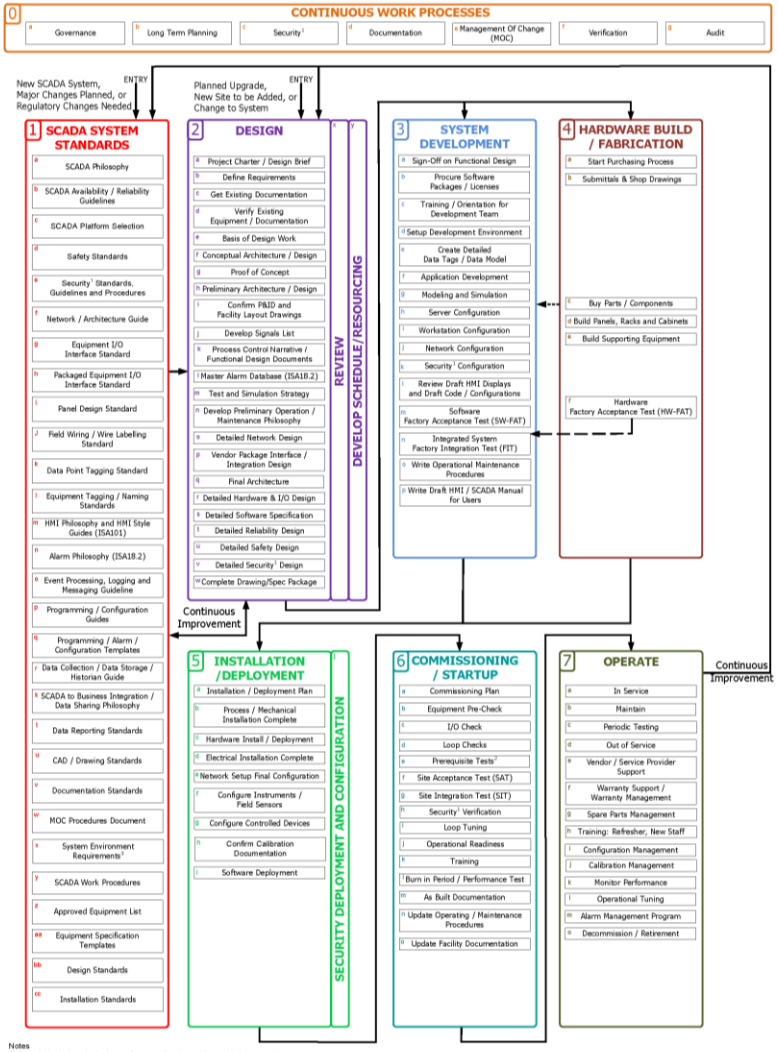
5 The use of direct-connections for remote applications is strongly discouraged. Refer to ISA/IEC-62443 for guidance on an appropriate zone/conduit implementation.

* We show a Purdue Level 5. The true Purdue Model only has levels 0-4 because it did not anticipate external applications.

IT = Information Technology

OT = Operational Technology

ISA112 SCADA Systems Lifecycle Diagram



0 CONTINUOUS WORK PROCESSES

- a Governance
- b Long Term Planning
- c Security[1]
- d Documentation
- e Management Of Change (MOC)
- f Verification
- g Audit

New SCADA System, Major Changes Planned, or Regulatory Changes Needed — ENTRY

Planned Upgrade, New Site to be Added, or Change to System — ENTRY

1 SCADA SYSTEM STANDARDS

- a SCADA Philosophy
- b SCADA Availability / Reliability Guidelines
- c SCADA Platform Selection
- d Safety Standards
- e Security[1] Standards, Guidelines and Procedures
- f Network / Architecture Guide
- g Equipment I/O Interface Standard
- h Packaged Equipment I/O Interface Standard
- i Panel Design Standard
- j Field Wiring / Wire Labelling Standard
- k Data Point Tagging Standard
- l Equipment Tagging / Naming Standards
- m HMI Philosophy and HMI Style Guides (ISA101)
- n Alarm Philosophy (ISA18.2)
- o Event Processing, Logging and Messaging Guideline
- p Programming / Configuration Guides
- q Programming / Alarm / Configuration Templates
- r Data Collection / Data Storage / Historian Guide
- s SCADA to Business Integration / Data Sharing Philosophy
- t Data Reporting Standards
- u CAD / Drawing Standards
- v Documentation Standards
- w MOC Procedures Document
- x System Environment Requirements[3]
- y SCADA Work Procedures
- z Approved Equipment List
- aa Equipment Specification Templates
- bb Design Standards
- cc Installation Standards

2 DESIGN

- a Project Charter / Design Brief
- b Define Requirements
- c Get Existing Documentation
- d Verify Existing Equipment / Documentation
- e Basis of Design Work
- f Conceptual Architecture / Design
- g Proof of Concept
- h Preliminary Architecture / Design
- i Confirm P&ID and Facility Layout Drawings
- j Develop Signals List
- k Process Control Narrative / Functional Design Documents
- l Master Alarm Database (ISA18.2)
- m Test and Simulation Strategy
- n Develop Preliminary Operation / Maintenance Philosophy
- o Detailed Network Design
- p Vendor Package Interface / Integration Design
- q Final Architecture
- r Detailed Hardware & I/O Design
- s Detailed Software Specification
- t Detailed Reliability Design
- u Detailed Safety Design
- v Detailed Security[1] Design
- w Complete Drawing/Spec Package

x REVIEW

y DEVELOP SCHEDULE/RESOURCING

Continuous Improvement

3 SYSTEM DEVELOPMENT

- a Sign-Off on Functional Design
- b Procure Software Packages / Licenses
- c Training / Orientation for Development Team
- d Setup Development Environment
- e Create Detailed Data Tags / Data Model
- f Application Development
- g Modeling and Simulation
- h Server Configuration
- i Workstation Configuration
- j Network Configuration
- k Security[1] Configuration
- l Review Draft HMI Displays and Draft Code / Configurations
- m Software Factory Acceptance Test (SW-FAT)
- n Integrated System Factory Integration Test (FIT)
- o Write Operational Maintenance Procedures
- p Write Draft HMI / SCADA Manual for Users

4 HARDWARE BUILD / FABRICATION

- a Start Purchasing Process
- b Submittals & Shop Drawings
- c Buy Parts / Components
- d Build Panels, Racks and Cabinets
- e Build Supporting Equipment
- f Hardware Factory Acceptance Test (HW-FAT)

5 INSTALLATION /DEPLOYMENT

- a Installation / Deployment Plan
- b Process / Mechanical Installation Complete
- c Hardware Install / Deployment
- d Electrical Installation Complete
- e Network Setup Final Configuration
- f Configure Instruments / Field Sensors
- g Configure Controlled Devices
- h Confirm Calibration Documentation
- i Software Deployment

j SECURITY DEPLOYMENT AND CONFIGURATION

6 COMMISSIONING / STARTUP

- a Commissioning Plan
- b Equipment Pre-Check
- c I/O Check
- d Loop Checks
- e Prerequisite Tests[2]
- f Site Acceptance Test (SAT)
- g Site Integration Test (SIT)
- h Security[1] Verification
- i Loop Tuning
- j Operational Readiness
- k Training
- l Burn in Period / Performance Test
- m As Built Documentation
- n Update Operating / Maintenance Procedures
- o Update Facility Documentation

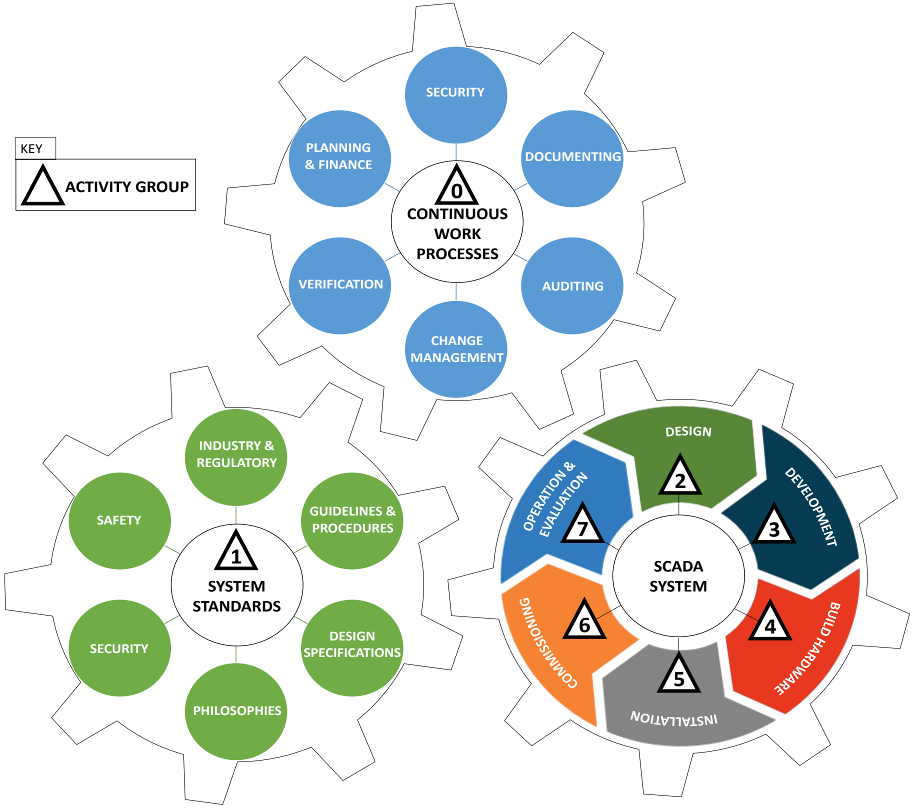
7 OPERATE

- a In Service
- b Maintain
- c Periodic Testing
- d Out of Service
- e Vendor / Service Provider Support
- f Warranty Support / Warranty Management
- g Spare Parts Management
- h Training: Refresher, New Staff
- i Configuration Management
- j Calibration Management
- k Monitor Performance
- l Operational Tuning
- m Alarm Management Program
- o Decommission / Retirement

Continuous Improvement

Notes
1) Security includes physical security, operational security, and cybersecurity.
2) Prerequisite tests typically include both cold and hot commissioning or dry / wet commissioning as applicable.
3) System Environment Requirements can include separate systems for development, testing, training, production, backup, disaster recovery, digital twins, and other uses, as part of development and Management Of Change (MOC) procedures

Note: This is an interim working draft from the ISA112 SCADA Systems standards committee, as of 2022-07-08. (A previous version was released on 2020-06-15.) This diagram is still subject to change.



Traditional SCADA Cyber Attack Types

- **Denial of Service**
  – an attacker actively blocks access or consumes system resources, so the system is not available for its intended use.
  – Loss of View and/or Loss of Control
- **Ransomware**
  – unauthorized encryption of data or servers, so that the system is not available for use and data is held hostage, until a ransom is paid.
- **Data Theft**
  – an attacker gains unauthorized access to they can copy data.
- **Unauthorized Access**
- – an attacker gains unauthorized access to a system so that they can copy data or make changes at will.
- **Unauthorized Modifications**
  – an attacker gains unauthorized access to system, usually a SCADA system, so they can issue commands or change setpoints with the intention of damaging property or impacting human health.
  – an attacker who can gain unauthorized access to a SCADA system's programming interfaces can do even more damage

Cyber Vulnerabilities

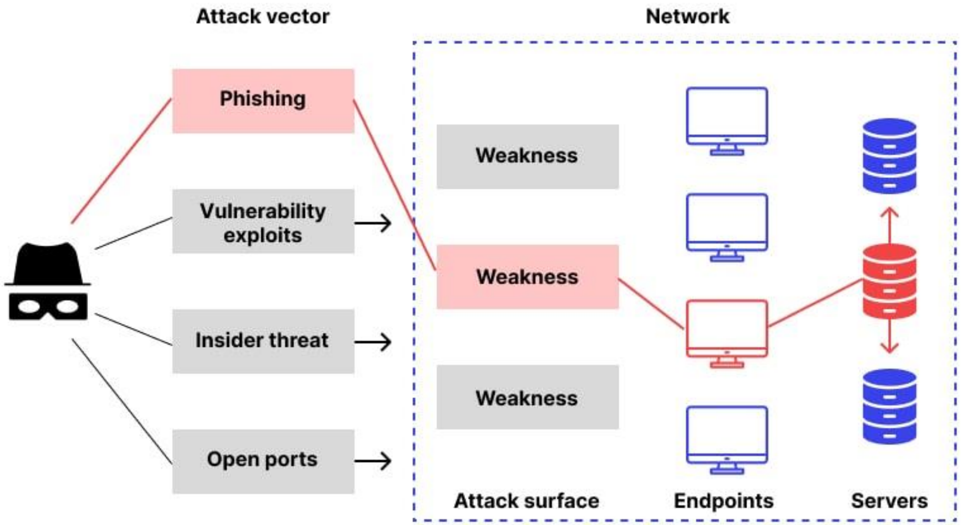
- Operator Workstations
- Engineering Workstations

- SCADA Network Jacks
- Servers and Server Rooms
- Network Closets

- Wide Area SCADA Network
- Network Panels / Hardware
- PLC Panels

- Connectivity with IT Systems

- Remote Access
  - Alarm Acknowledgement Systems
  - View-Only Remote HMI
  - Read/Write Remote HMI
  - Remote Programming Access



88% of cyber "attacks" are actually due to human error

2022 Study by Stanford University / Tessian

Major “Risk Scenarios” for W/WW SCADA

1. Loss of Operator View
   a) Not able to view status of facility – one site or multiple sites
   b) Loss of SCADA communications to one or more facilities
2. Loss of Operator Control
   a) Not able to view status & send commands to a facility
   b) Loss of SCADA communications to one or more facilities
3. Loss of Process Control
   a) Failure of PLC control of a facility – process shuts down / offline
   b) Compromised PLC control – erratic operation
   c) Compromised PLC control – auto-shutdown interlocks do not work
4. Alarm System Failure
   a) Screen-based alarms stop working – one site or multiple sites
   b) Alarm call-out systems don’t work – one site or multiple sites
5. Loss of Datalogging
   a) Loss of datalogging for one or more sites (e.g., logging chlorine values)
6. Unauthorized Access to Operator Workstation
   a) Unauthorized user is to view or make changes
   b) Compromise of an Operator Workstation – jump point into rest of system
7. Unauthorized Access to Engineering Workstation or Servers
   a) Unauthorized changes to the programming of the system
   b) Ability to change how data is collected, how commands are sent and programming
8. Unauthorized Access to SCADA Network
   1. Attack originating from the IT Network or IT Systems
9. Compromised Remote Access

Typically, 90% of cyber attacks of SCADA systems come in via the IT network or via Remote Access

Growing Risk of Cyber Incidents

In Past 5 years there have been more than 50 documented Water SCADA Systems in North America

Some Stats from 2021 (USA)

- January 2021, a hacker tried to poison a water treatment plant in San Francisco Bay area[iii].
- February 2021, a hacker attempted increase to caustic soda feed rates to dangerous levels at drinking water plant in Oldsmar Florida[iv].
- March 2021, a Nevada-based water/wastewater utility's SCADA systems were ransomwared[v].
- May 2021, the SCADA network for a Pennsylvania water utility was breached[vi].
- July 2021, a hacker was able to completely disable a Maine-based wastewater plant's SCADA system[vii], and the plant had to be run in manual while the SCADA computers replaced

Closer to Home

- Wasaga Beach (2018)[viii],
- Midland (2018)[ix],
- Stratford (2019)[x],
- Woodstock (2019)[xi],
- Metro Vancouver Transit (2020)[xii],
- Toronto Transit Commission (2021)[xiii],

Components of a SCADA Cybersecurity Program

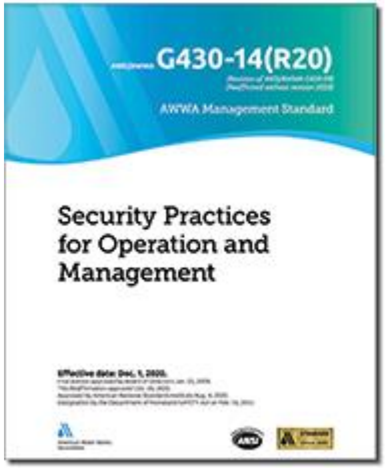
- Education Program, including annual training for users
- Keeping hardware/software up to date, avoiding obsolesce
- Removing obsolete equipment that is no longer needed
- Maintain separation between IT and SCADA systems
- Network Segmentation & Firewalls

- Documentation – process control narratives, configurations, setpoints, P&IDs, wiring, etc.
- Asset Inventory, ideally automated with help of software
- Status monitoring of SCADA components, including SCADA network
- Vulnerability scanning, logging and visibility – and staffing to investigate and resolve issues!
- Patching Program (with mitigations for difficult to patch systems)
- Backup & Disaster Recovery System – and test it regularly
- Change Management and Tracking Revisions

- SCADA User Accounts, Separation of Duties, and MFA (multi-factor authentication)
- Operator Workstation hardening
- Restricting access to physical SCADA network, servers and server rooms
- Thinking carefully about remote access – if it is needed and if so, how & how it is designed

SCADA Cyber Security – Published Standards

- ISA/IEC-62443
- NIST 800 series
- AWWA GW430



G430-14(R20)

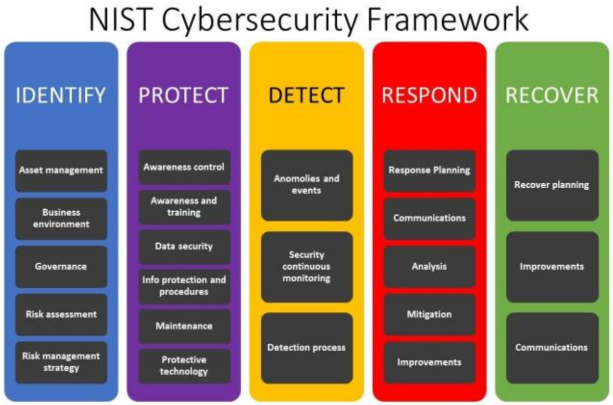
AWWA Management Standard

Security Practices for Operation and Management

Effective date: Dec. 1, 2020.

ISA/IEC-62443 Cyber Security Framework

General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Product security development life-cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 Security protection scheme and security protection ratings	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 Security life cycle and use cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		



NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset management	Awareness control	Anomolies and events	Response Planning	Recover planning
Business environment	Awareness and training	Security continuous monitoring	Communications	Improvements
Governance	Data security	Detection process	Analysis	Communications
Risk assessment	Info protection and procedures		Mitigation	
Risk management strategy	Maintenance		Improvements	
	Protective technology			

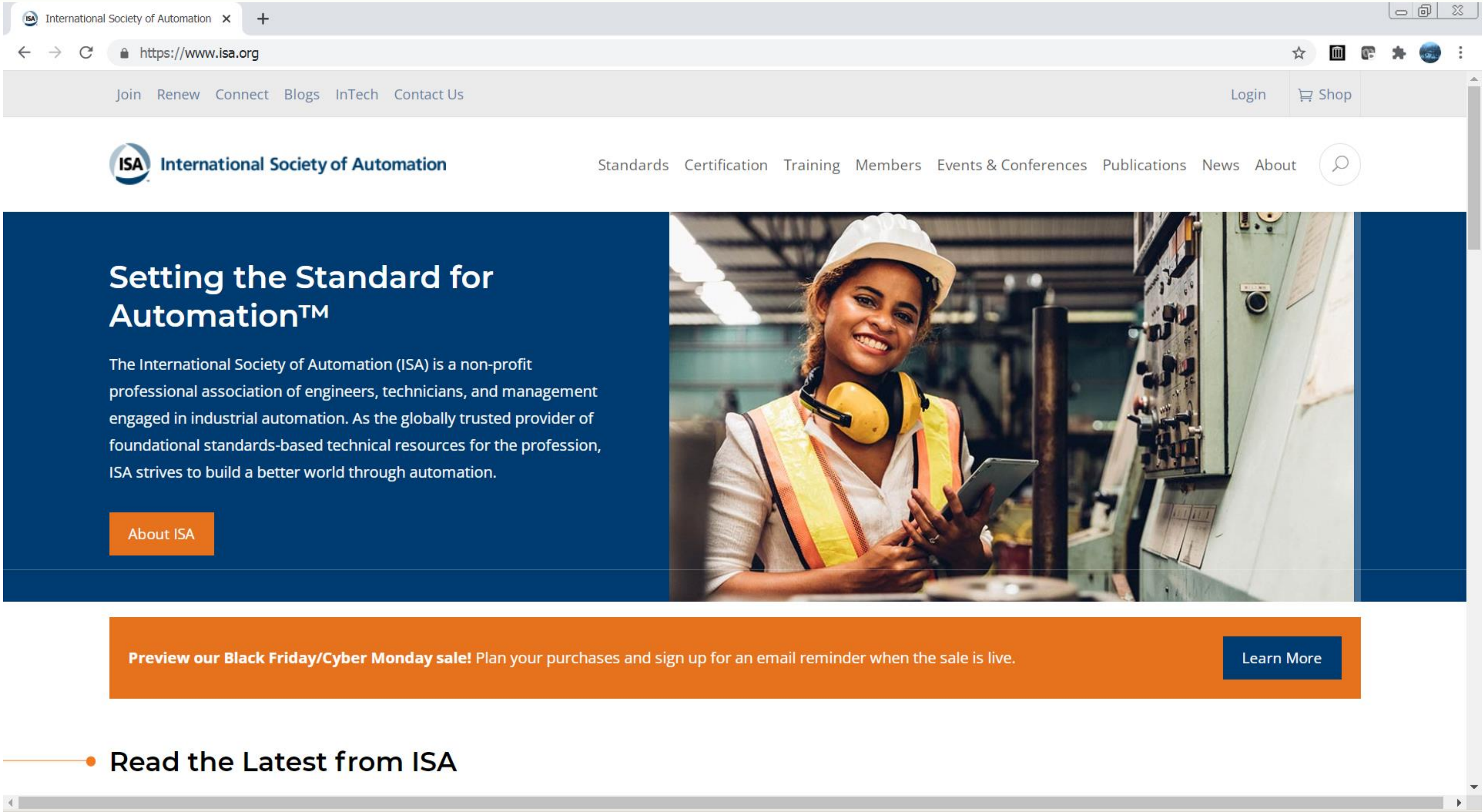
Introducing the ISA/IEC-62443 Standards

General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Product security development life-cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 Security protection scheme and security protection ratings	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 Security life cycle and use cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

In ISA / IEC-62443 terminology:

IACS = Industrial Automation Control System
also known as "OT" or "SCADA"

ISA – International Society of Automation



Setting the Standard for Automation™

The International Society of Automation (ISA) is a non-profit professional association of engineers, technicians, and management engaged in industrial automation. As the globally trusted provider of foundational standards-based technical resources for the profession, ISA strives to build a better world through automation.

Preview our Black Friday/Cyber Monday sale! Plan your purchases and sign up for an email reminder when the sale is live.

Read the Latest from ISA

ISA99 Standards Committee

The International Society of Automation (ISA) committee ISA99 Security for Industrial Automation & Control Systems

- Members from around the world
- Multiple sectors and stakeholders
- Working in collaboration with IEC TC65 WG10
- Consistent leadership since c. 2002

ISA99 Committee Scope(*)

"… automation and control systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee safety
- environmental protection
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on entity, local, state, or national security"

(*) Taken from the original committee scope description

ISA99 Committee Membership

Reflects expertise from many sectors, including:

- Chemicals, Oil and Gas
- Food and Beverage
- Energy
- Pharmaceuticals
- **Water/Wastewater**
- Manufacturing
- Transportation
- ICS suppliers
- Government

ISA/IEC-62443 Standards Documents

General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Product security development life-cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 Security protection scheme and security protection ratings	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 Security life cycle and use cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

In ISA / IEC-62443 terminology:

IACS = Industrial Automation Control System
also known as “OT” or “SCADA”

Why SCADA is different than IT

- Safety, Integrity, Availability, Confidentiality
  - Addition of safety
  - Availability has the highest priority after safety
  - *IT focus is: Confidentiality, Integrity and Availability*
- Functional Safety and Security
  - Coordinated approach to risk assessment

Foundational Requirements

- FR 1 – Identification & authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

ISA/IEC-62443 Common Themes

Defense In Depth

- Defense in Depth is a concept in which several levels of security (defense) are distributed throughout the system. The goal is to provide redundancy in case a security measure fails or a vulnerability is exploited.

Zones and Conduits

- **Zones divide a system into homogeneous zones** by grouping the (logical or physical) assets with common security requirements. The security requirements are defined by Security Level (SL). The level required for a zone is determined by the risk analysis.
- **Zones have boundaries that separate the elements inside the zone from those outside.** Information moves within and between zones. Zones can be divided into sub-zones that define different security levels (Security Level) and thus enable defense-in-depth.
- **Conduits group the elements that allow communication between two zones**. They provide security functions that enable secure communication and allow the coexistence of zones with different security levels.

General Security Principals

- Security Elements
- Risk-Based Approach
- Compensating Measures
- Least Privilege
- Least Function
- Essential Function
- Defense in Depth
- Supply Chain Security

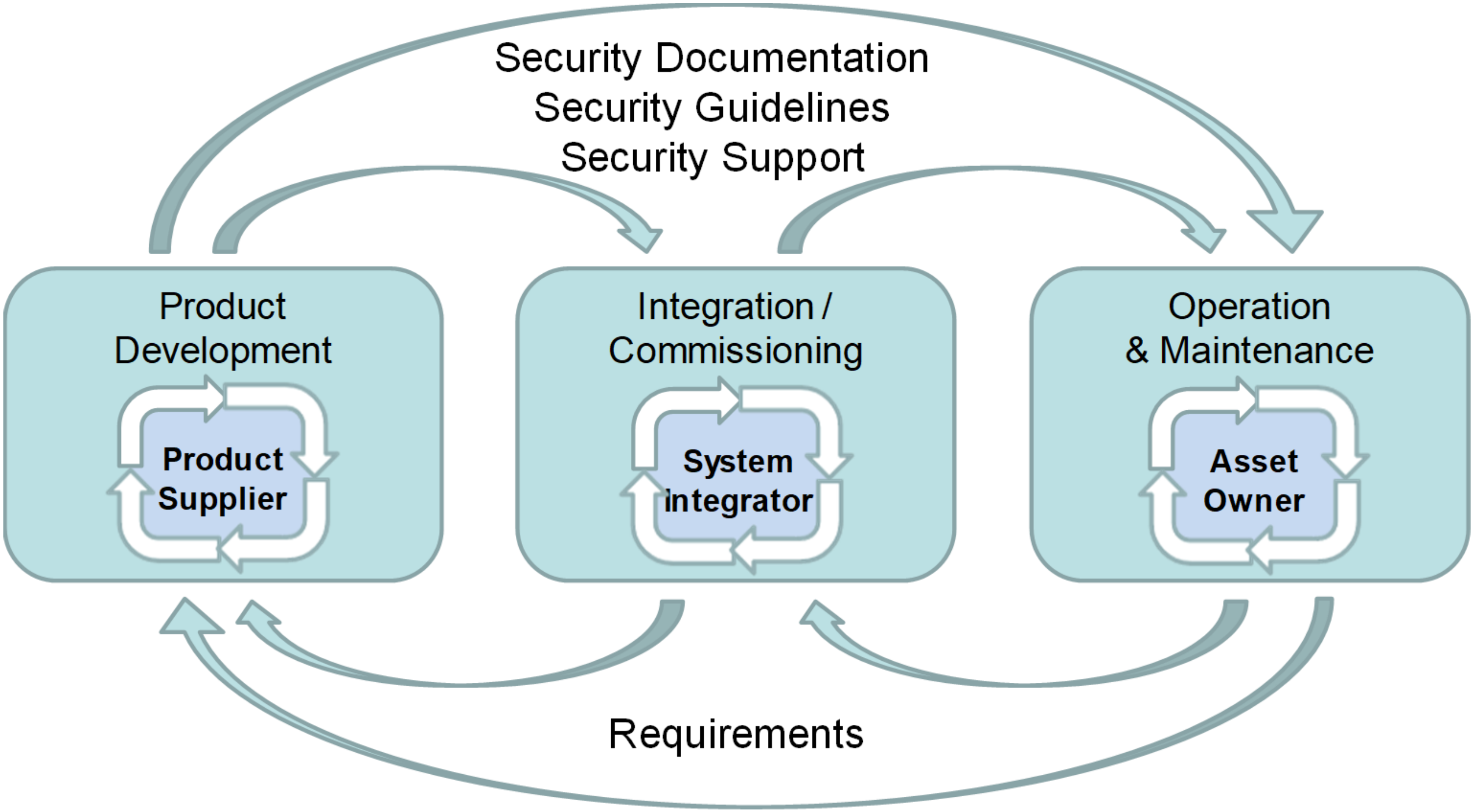
Source: ISA-62443-1-1

Operations Security Principals

- How Different Parts of the System are Used
- Defining System Access Points
- Safety, Integrity, Availability, Confidentiality (OT vs IT)
- Zones and Conduits
- Security Levels
- Maturity Levels
- Security Protection Scheme
- Security Protection Rating
- Security and Functional Safety

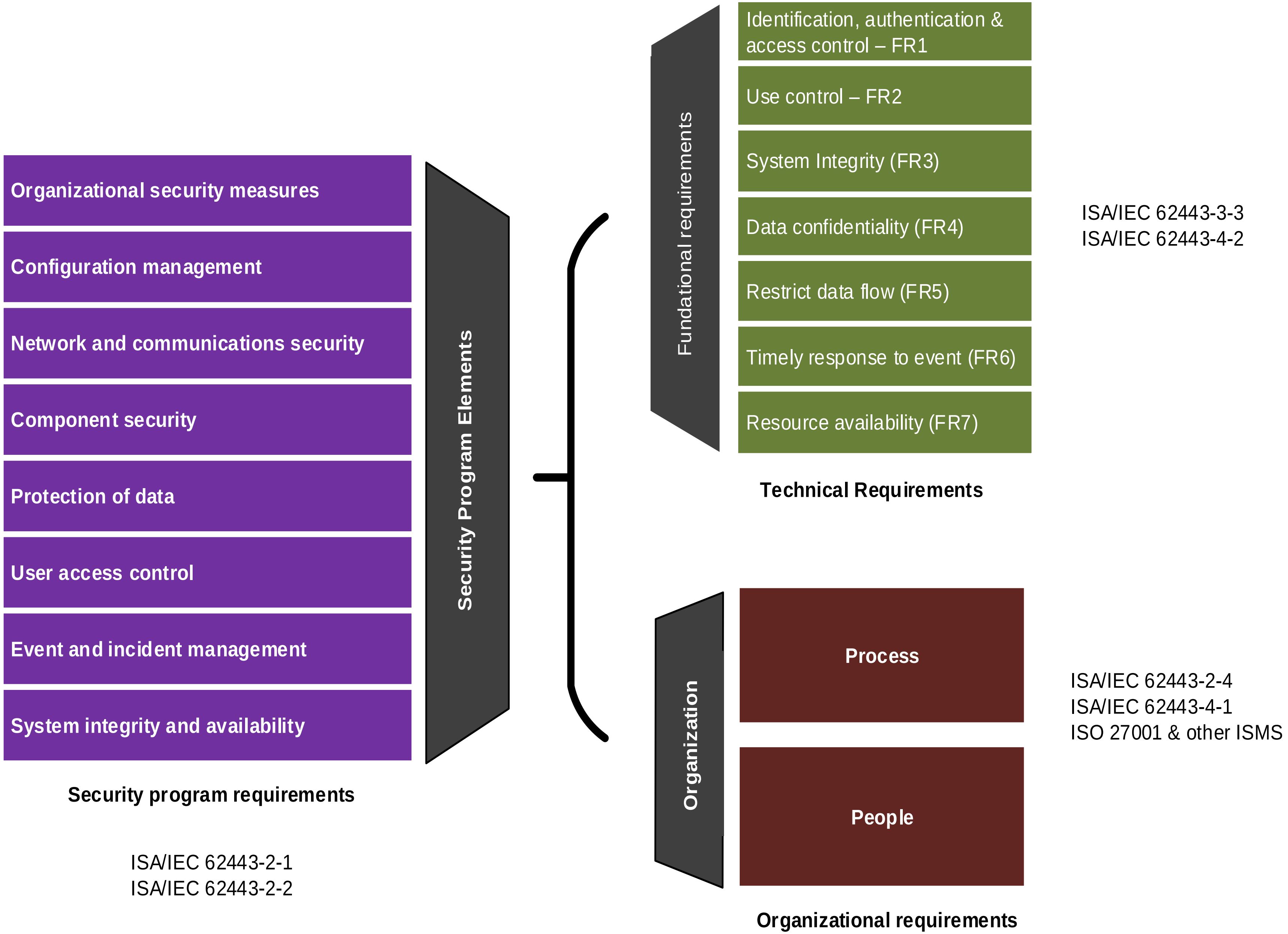
Source: ISA-62443-1-1

Related Lifecycles



Based on VDI 2182

Security Element Grouping



Organizational security measures

Configuration management

Network and communications security

Component security

Protection of data

User access control

Event and incident management

System integrity and availability

Security Program Elements

Security program requirements

ISA/IEC 62443-2-1
ISA/IEC 62443-2-2

Fundational requirements

Identification, authentication & access control – FR1

Use control – FR2

System Integrity (FR3)

Data confidentiality (FR4)

Restrict data flow (FR5)

Timely response to event (FR6)

Resource availability (FR7)

Technical Requirements

ISA/IEC 62443-3-3
ISA/IEC 62443-4-2

Organization

Process

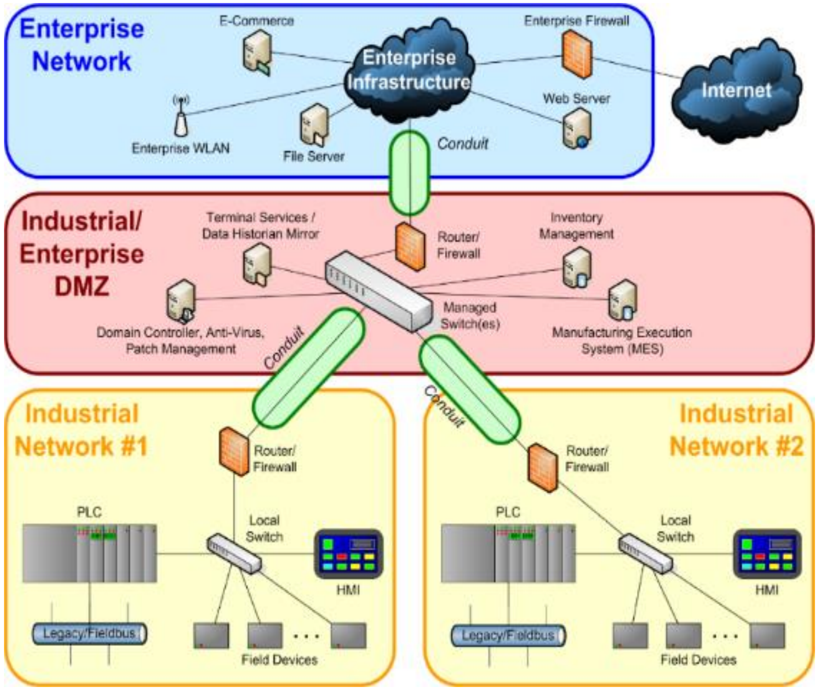
People

Organizational requirements

ISA/IEC 62443-2-4
ISA/IEC 62443-4-1
ISO 27001 & other ISMS

Zones & Conduits

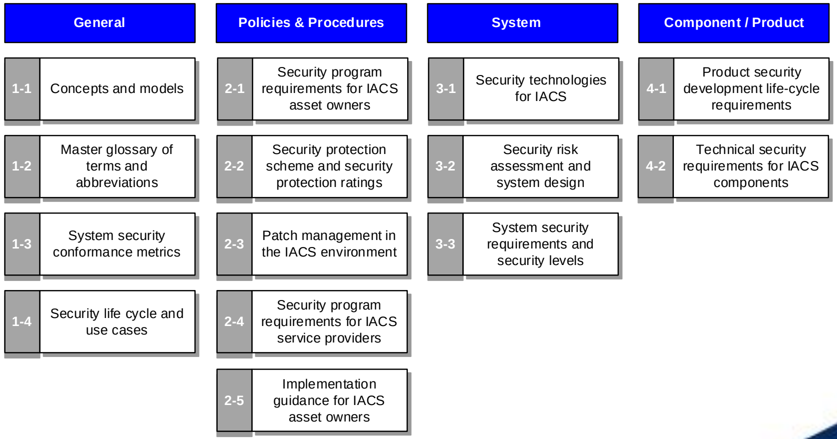
- A means for defining…
  - How different systems interact
  - Where information flows between systems
  - What form that information takes
  - What devices communicate
  - How those devices communicate
  - The security differences between system components



- Technology helps, but architecture is more important
- SCADA systems must be separated from IT Systems

Applying ISA/IEC-62443 to the Water Sector

- Use Zones & Conduits Architecture – Segment & Protect
- Design Security into the System instead of afterwards
- Use a Risk-Based Approach to Design, Testing & Ops
- Design a system around: Least Privilege, Least Function
- Defense in Depth
- Supply Chain Security
- Documented Procedures
- Review Security Frequently
- Active Monitoring
- Treat it as a Lifecycle



General	Policies & Procedures	System	Component / Product
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Product security development life-cycle requirements
1-2 Master glossary of terms and abbreviations	2-2 Security protection scheme and security protection ratings	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 Security life cycle and use cases	2-4 Security program requirements for IACS service providers		
	2-5 Implementation guidance for IACS asset owners		

Cybersecurity Challenges At Water Utilities

- **Managing Technical Debt**
  - Obsolete PLC/PAC hardware
    - Older PLC hardware cannot be secured
    - If spare spares are not commercially available, it needs to be replaced!
  - SCADA networks that cannot be segmented
    - Many existing wire area networks can't provide separate logical VLANs
    - Unmanaged network hardware
  - IT controlled networking equipment
  - Unknown programming that is not documented
  - No up-to-date process control narratives
  - No up-to-date P&IDs or wiring diagrams

- **Funding for cybersecurity programs**
  - Cybersecurity funding needs to be "new" funding
  - Requires specialist practitioners, traditional IT or system integrators may have skills

- **Finding and training SCADA cybersecurity staff**
  - Cybersecurity is newer profession = shortage of cybersecurity professionals
  - Even fewer have OT/SCADA cybersecurity training: CISSP, GICSP, ISA-Cyber-Expert

- **Will require new ongoing funding**

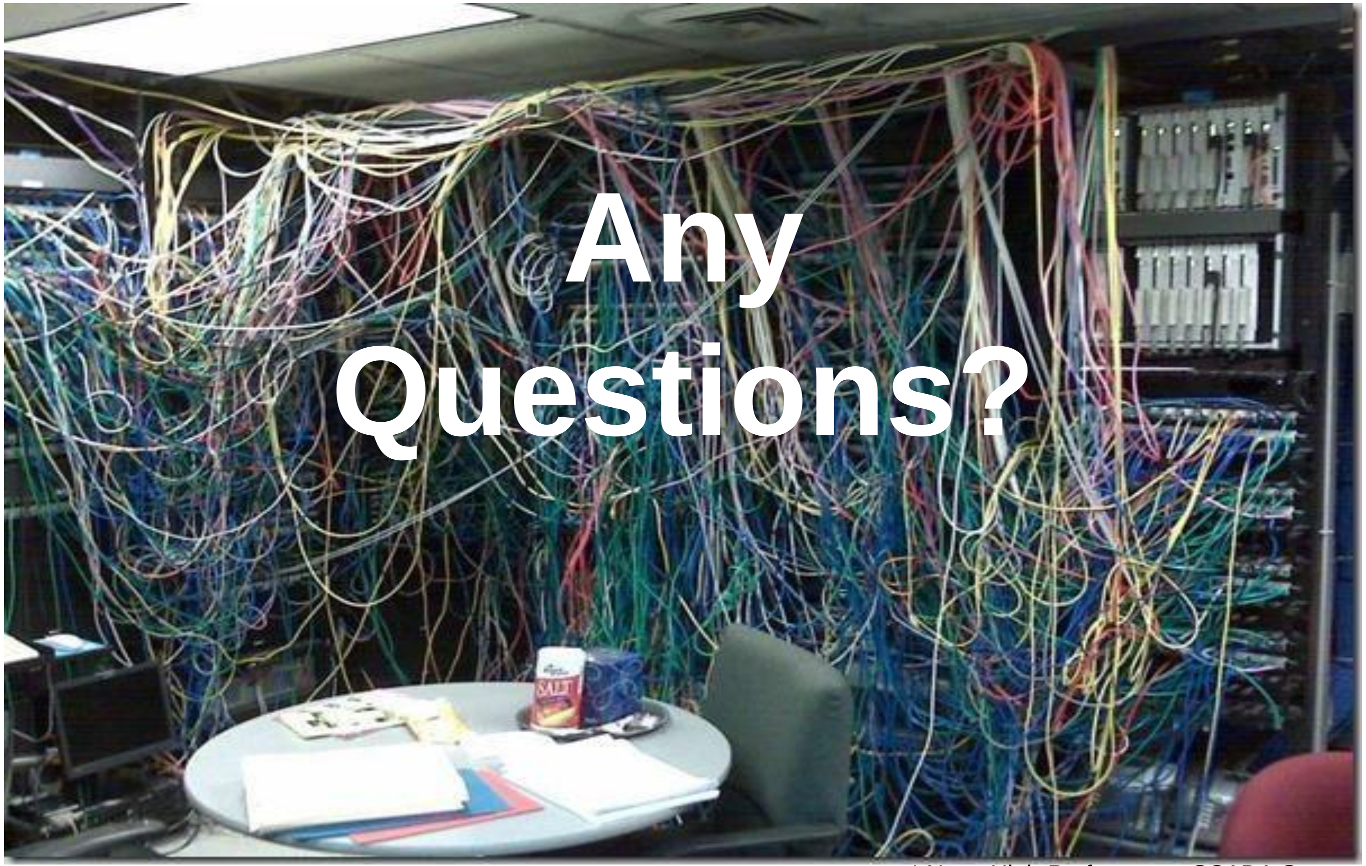
SCADA Cybersecurity Program – Getting Started

- Asset Inventory – what do you have
- Assess SCADA assets
  - How old is it, Does it work properly, Is it documented, Is it maintainable, Is it obsolete
- Lifecycle upgrade program: SCADA hardware, software and programming
  - SCADA hardware, software and programming needs more frequent updates that Capital Works
- Document your System – so you have a record of how it *actually* works

- User Account Clean-Up, Procedures around issuing/removal of user accounts
- Back up and Disaster Recovery Systems – test them frequently

- Secure and Harden operator workstations
- Segment the SCADA network form other networks, and sub-segment network
- User Accounts – Separating Account by Duty, Multi-Factor Authentication, Logging
- Physically secure SCADA assets and access to SCADA network
- Control access to SCADA servers and engineering workstations

- Automated SCADA asset collection and vulnerability scanning (passive)
- SCADA system component monitoring and automated
- Change Management, Revision control and backup systems for changes
- Periodic Testing of functionality



* Not a High-Performance SCADA System

Graham Nasby
Co-Chair, ISA112 SCADA Systems Management Committee
graham.nasby@grahamnasby.com