Setting the Standard for Automation™

Introducing the ISA / IEC-62443 Series of Cybersecurity Standards
&
Applying them to the Municipal Water Systems

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

2022 National Water-Wastewater Conference
Canadian Water-Wastewater Association

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

About the Speaker

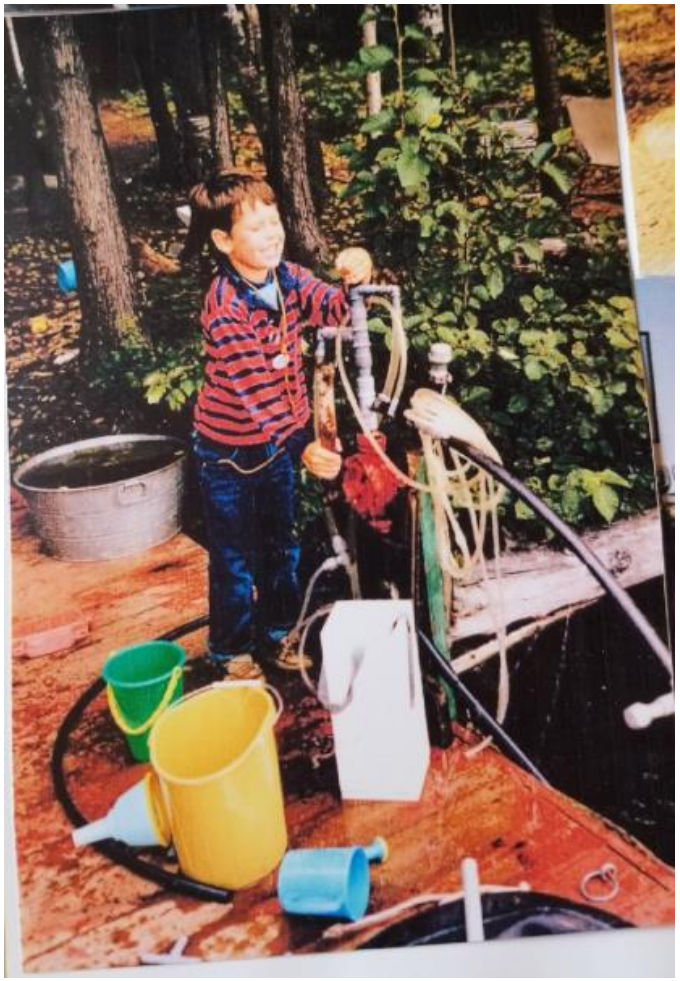
Graham Nasby, P.Eng., PMP, CAP
Water SCADA & Security Specialist
City of Guelph Environmental Services (Water Services)

- 10 years in the consulting sector
- Joined Guelph Water Services in 2015

- OWWA and WEAO Member, Member of OWWA Automation Committee
- Co-chair of ISA112 SCADA Systems standards committee
- Voting member of ISA101 HMI Design standards committee
- Voting member of ISA18 Alarm Management standards committee
- Named Canadian Expert on IEC/SCC-TC65 with Standards Council of Canada

- Guest instructor at McMaster University and Conestoga College
- Has published over 40 papers and articles on automation topics
- Received University of Guelph “Mid Career Achievement Award” in 2014
- Received ISA’s Standards Committee Leader of the year award in 2021.

- Contact: graham.nasby@guelph.ca



I wanna be a Water Guy when I grow up!

Presentation Outline

- SCADA Refresher
- What are the ISA/IEC-62443 Standards
- Who develops the 62443 standards
- 62443 Standards Structure & Documents

- Common Themes of ISA/IEC-62443 Standards
- Structure of the Standards
- Maturity, Security Level, Zones/Conduits
- Key ISA/IEC-62443 Concepts

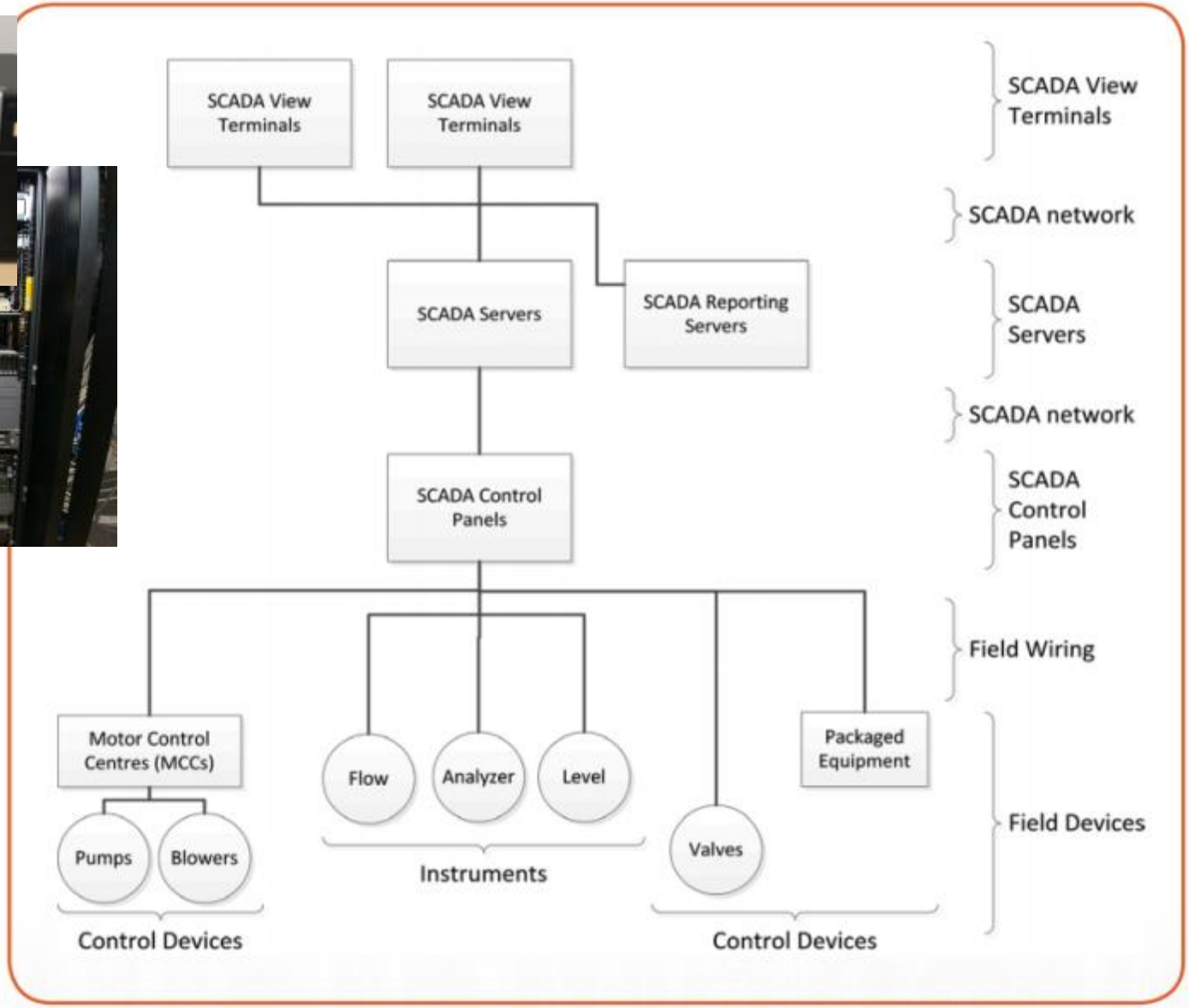
- How to Apply 62443 Standards to SCADA Systems
- Working with other Cybersecurity Standards
- Best Practices & Take-Aways

A Quick SCADA Refresher

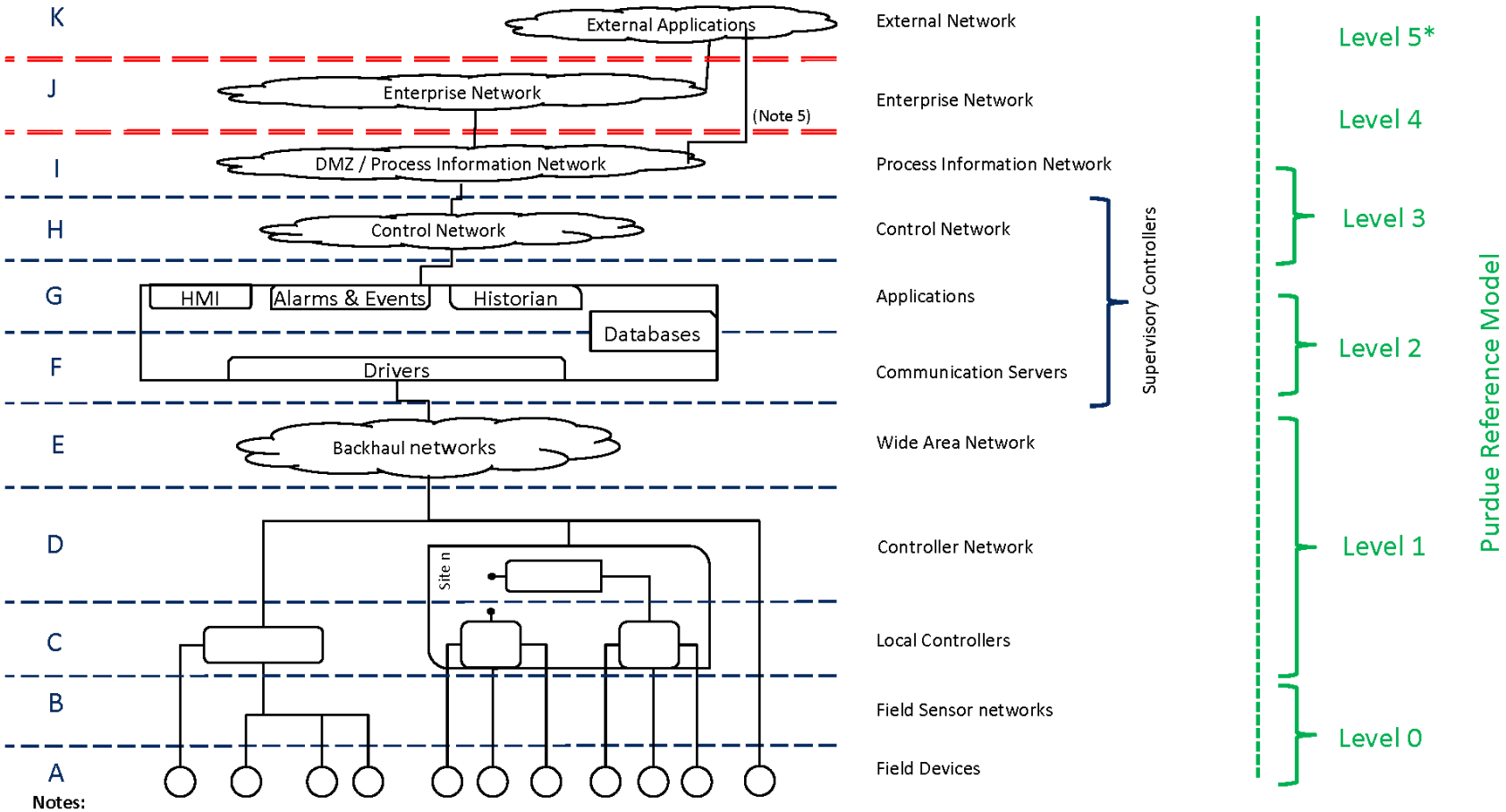
What is SCADA?

SCADA = Supervisory Control and Data Acquisition

Typical SCADA Architecture



SCADA System Architecture

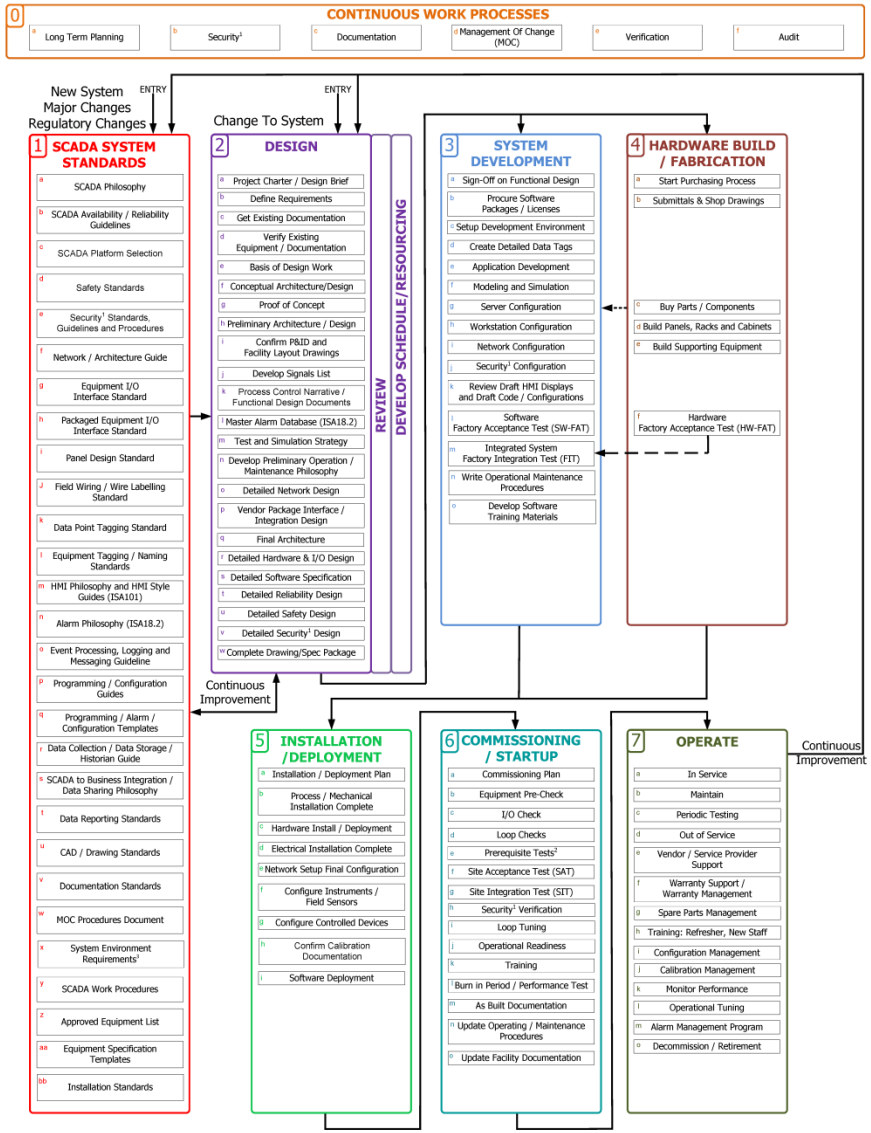


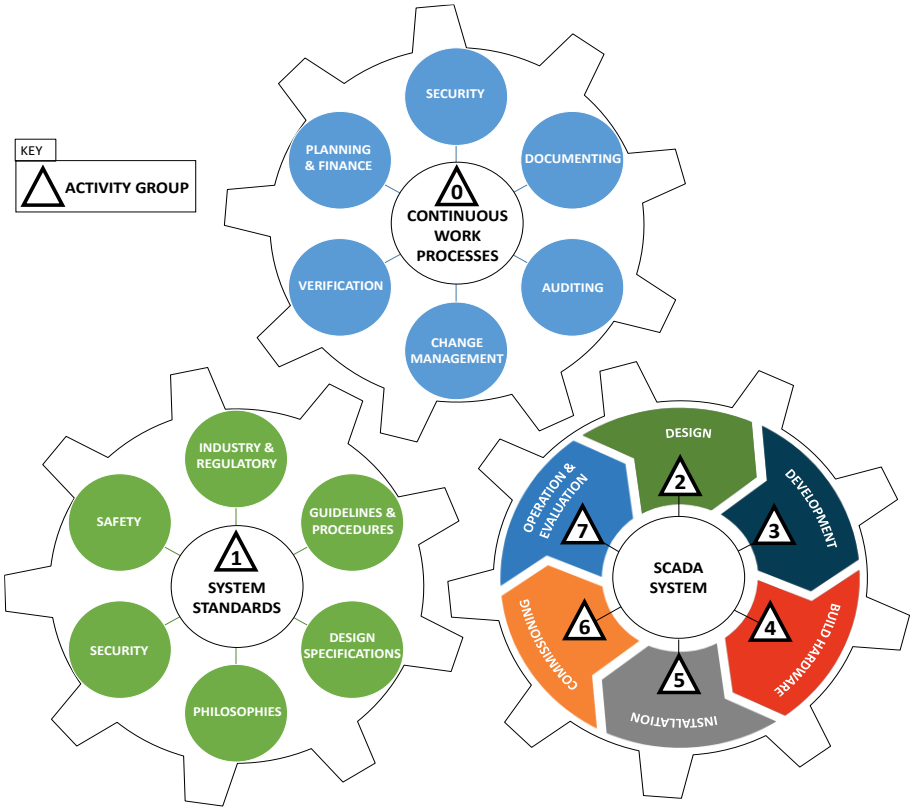
Notes:

1 Letters are used to avoid potential conflict with ISA-95 and other "Layer" models.
2 Routers and Firewalls between layers are not shown.
3 Other system-specific servers, applications ,and workstations are not shown.
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.

Revision May 28, 2020

SCADA Systems Lifecycle Diagram

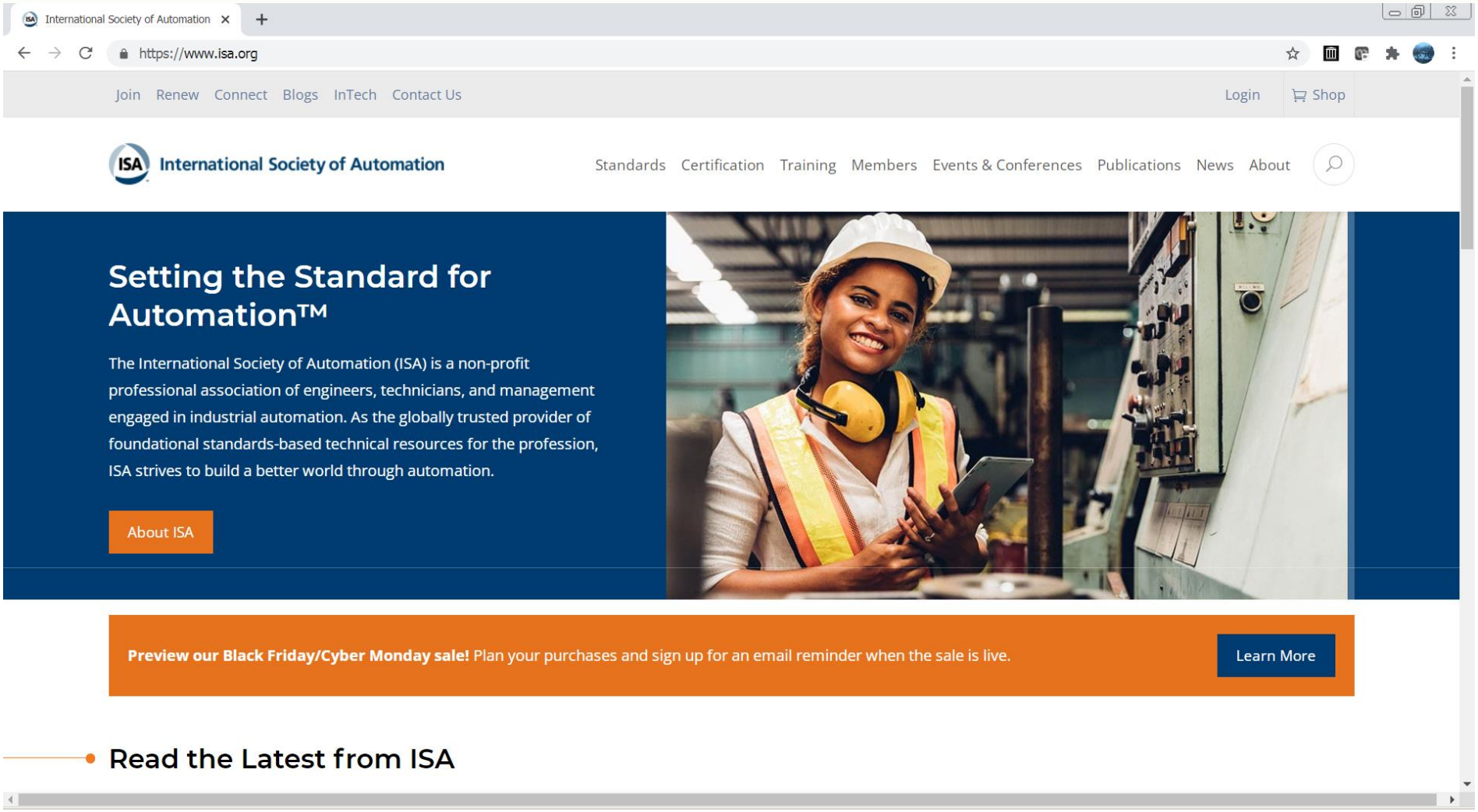




So how do we keep all this secure?

Answer:
ISA/IEC-62443 Series of Cybersecurity Standards

ISA – International Society of Automation



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”

Who Develops the 62443 Standards

- ISA-62443 (and IEC 62443); a series of standards developed primarily by ISA and published by two groups:
  - ISA99 → ISA-62443
  - IEC TC65/WG10 → IEC 62443

- In consultation with:
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x

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”

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.

ISA/IEC-62443 Common Themes

Maturity Level

- **Maturity Level 1** - Initial: Product supplier/implementers usually carry out product development ad hoc and often undocumented process
- **Maturity Level 2** - Managed: The product supplier/implementer is able to manage the development of a product according to written guidelines. It must be demonstrated that the personnel who carry out the process have the appropriate expertise, are trained and/or follow written procedures. The processes are repeatable.
- **Maturity Level 3** - Defined (practiced): The process is repeatable throughout the supplier's organization. The processes have been practiced and there is evidence that this has been done.
- **Maturity Level 4** - Improving: Product suppliers use appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.
- **Maturity Level 5** – Same as 4, but has been improved/optimized over time, and continues to be optimized to meet both security and repeatability goals

ISA/IEC-62443 Common Themes

Security Level

- Technical requirements for systems (IEC 62443-3-3) and products (IEC 62443-4-2) are evaluated in the standard by four so-called Security Levels (SL). The different levels indicate the resistance against different classes of attackers. The standard emphasizes that the levels should be evaluated per technical requirement (see IEC 62443-1-1) and are not suitable for the general classification of products.

- **Security Level 0:** No special requirement or protection required.
- **Security Level 1:** Protection against unintentional or accidental misuse.
- **Security Level 2:** Protection against intentional misuse by simple means with few resources, general skills and low motivation.
- **Security Level 3:** Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation.
- **Security Level 4:** Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation.

ISA/IEC-62443 Components

- Principal Roles
- Life Cycles and Processes
- System Under Consideration
- General Security Concepts
- Operations Security Concepts
- Foundational Requirements

21

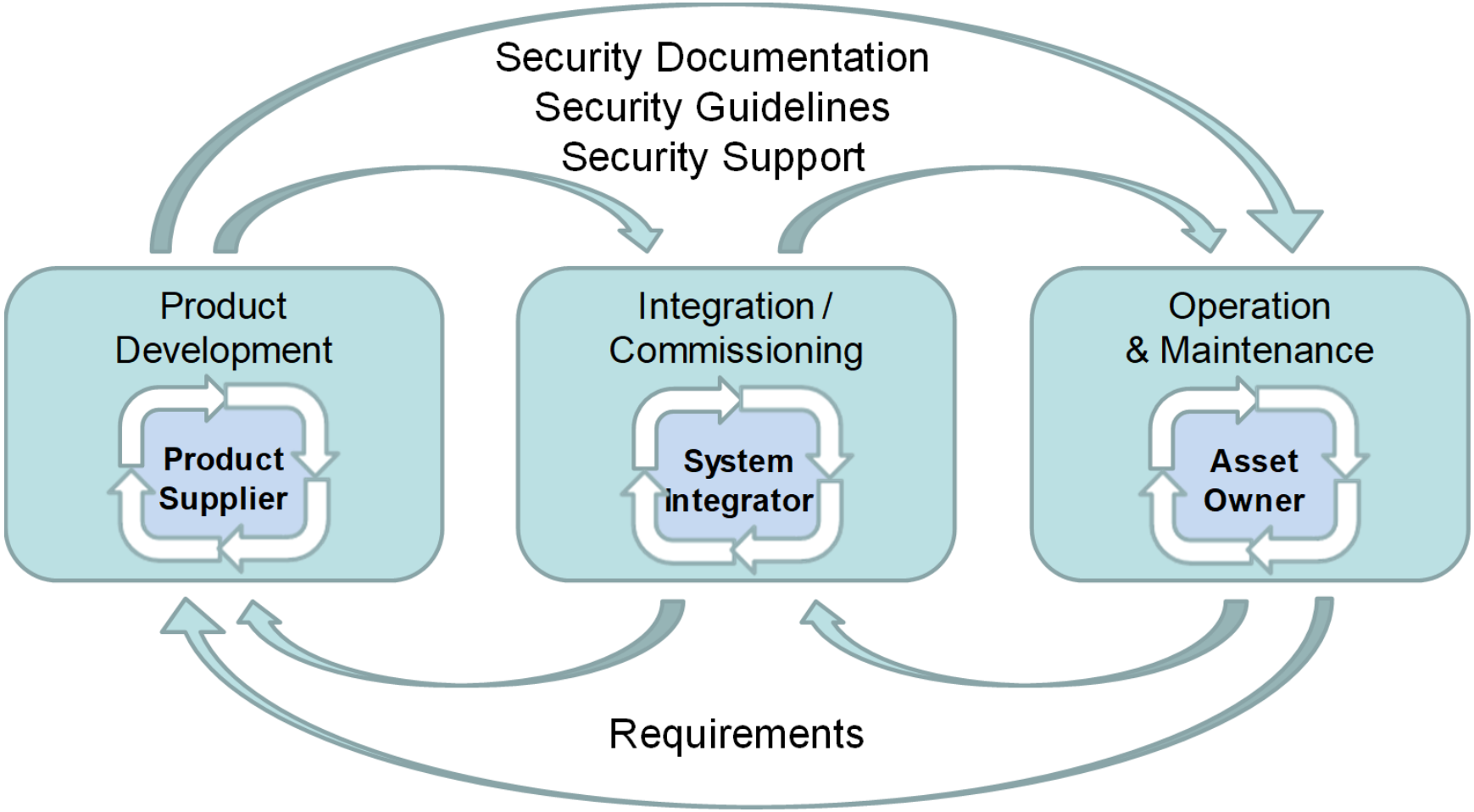
Principal Roles

- Asset Owner
- Product Supplier
- Maintenance Service Provider
- Integration Service Provider

Associated Roles

- Asset Operator
- Regulatory Authority
- Compliance Authority

Related Lifecycles



Based on VDI 2182

System to be Protected

- Describes the scope of the system being addressed by the security response
- Must be defined by the asset owner for the specific situation

- What is being protected?
- What do you want to protect it from?
- What level of risk is acceptable?
- How many resources to invest…

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

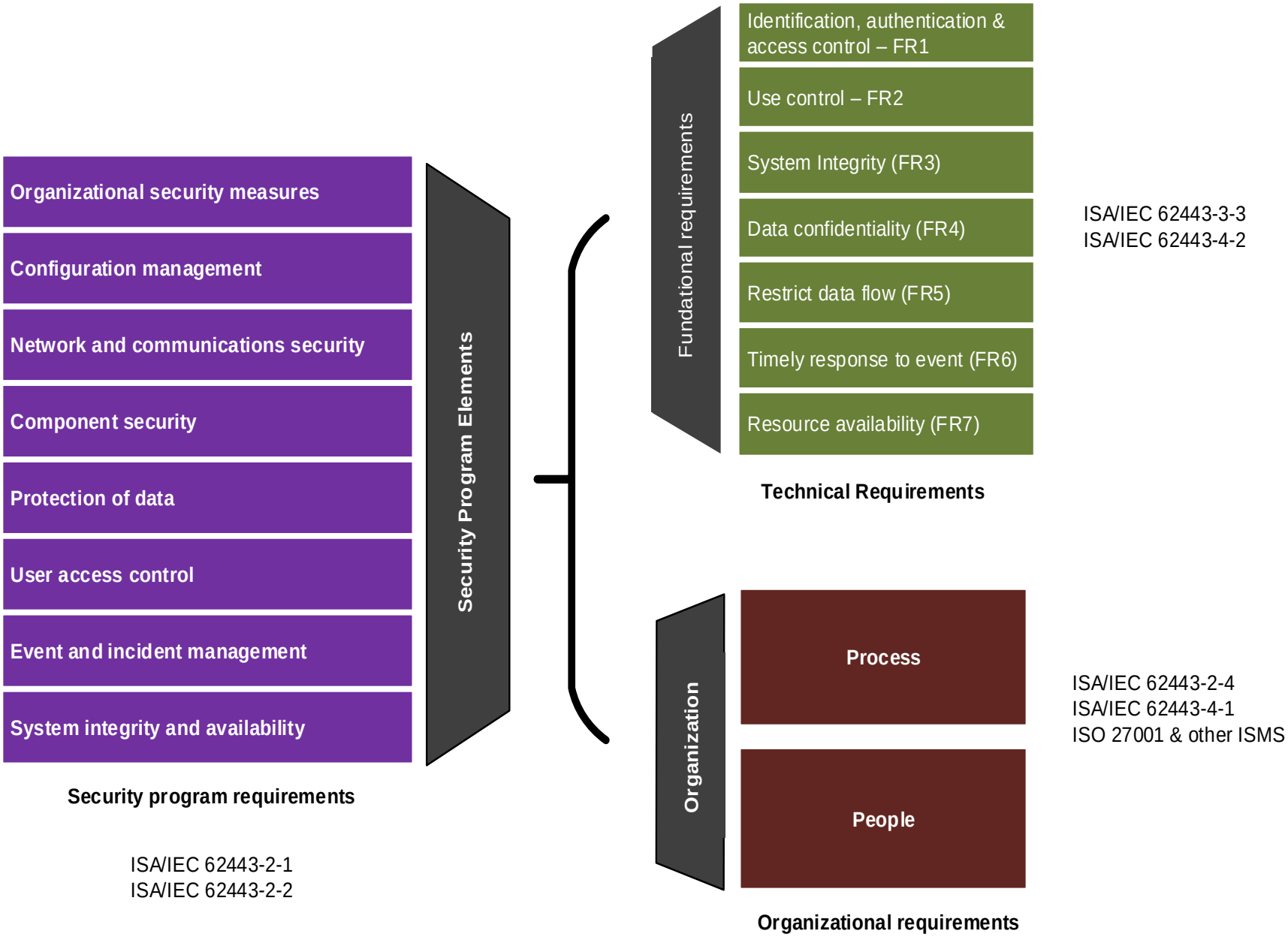
Operations Security Principals

- 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

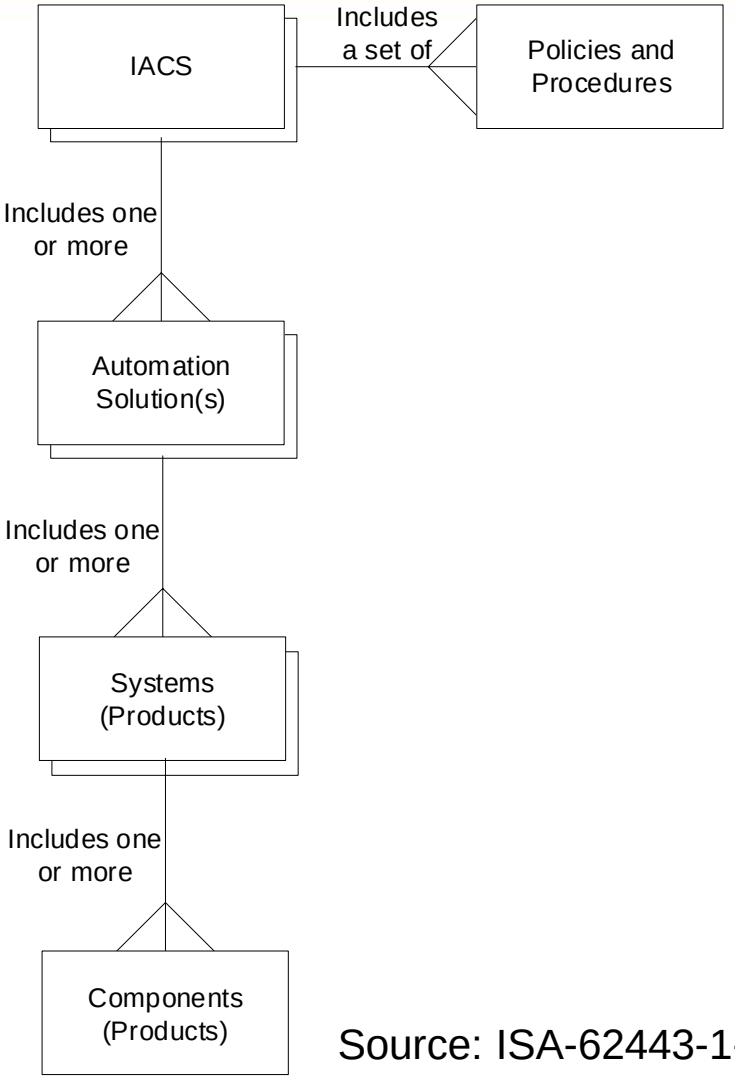
Source: ISA-62443-1-1

27

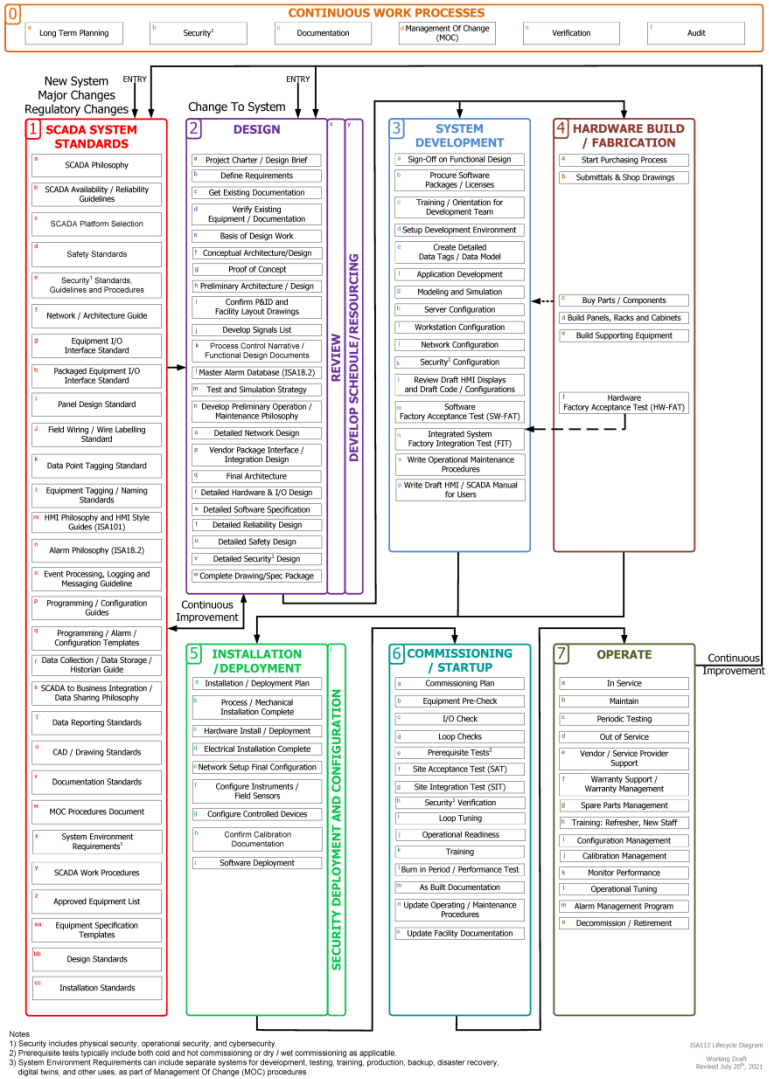
Security Element Grouping



Typical Structure of IACS System (SCADA)



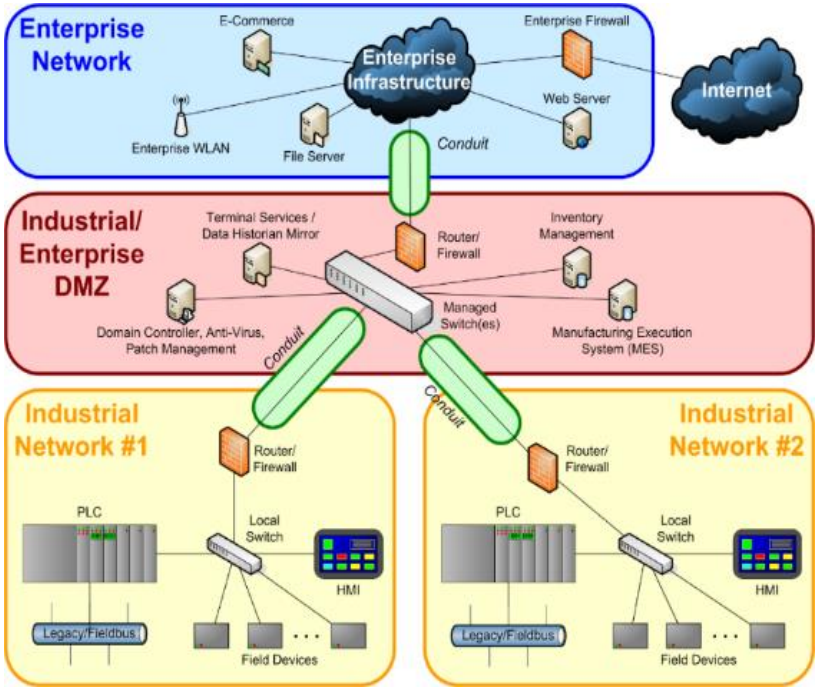
Source: ISA-62443-1-1



Source: ISA112

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

Source: ISA112

Security (Protection) Levels

Protection against…

4 Intentional Violation Using Sophisticated Means with Extended Resources, IACS Specific Skills & High Motivation

3 Intentional Violation Using Sophisticated Means with Moderate Resources, IACS Specific Skills & Moderate Motivation

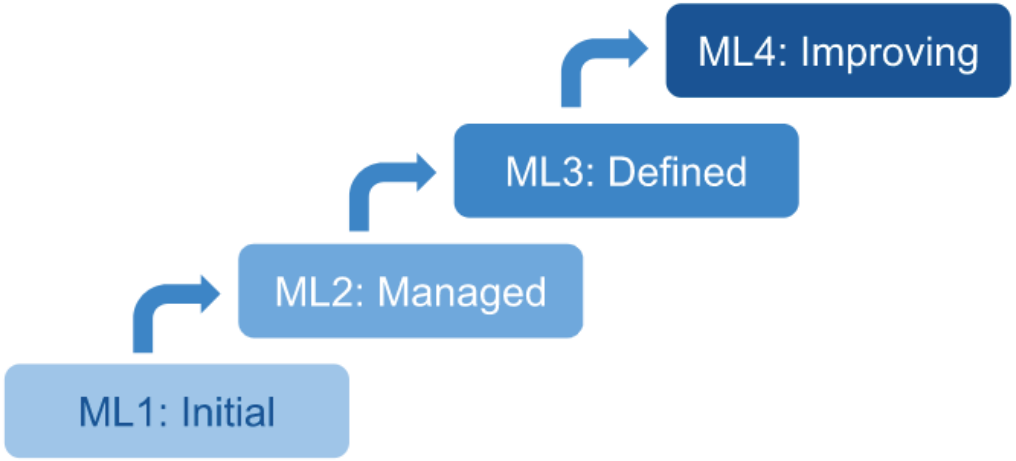
2 Intentional Violation Using Simple Means with Low Resources, Generic Skills & Low Motivation

1 Casual or Coincidental Violation

Source: ISA112

(Security) Maturity Levels

- A means of assessing capability
- An evolving concept in the standards
- Progressive levels of achievement
  - Initial
  - Managed
  - Defined
  - Improving



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

Other Important Requirements

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

Other Important Requirements

- **Security Protection Scheme (SPS)**
  - a set of technical and organizational security measures for protecting the system against cyber threats during operation
- **Security Protection Rating (SPR)**
  - used when assessing the fulfillment by the SPS of the security requirements

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”

36

Looking in some ISA/IEC-62443 Documents

Table of Contents

AMERICAN NATIONAL STANDARD

ANSI/ISA–62443-1-1 (99.01.01)–2007
(formerly designated as ANSI/ISA-99.00.01-2007)

Security for Industrial Automation
and Control Systems
Part 1-1: Terminology, Concepts, and Models

Approved 29 October 2007

Looking in some ISA/IEC-62443 Documents

CONTENTS

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

AMERICAN NATIONAL STANDARD

ANSI/ISA-62443-3-2-2020

Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design

Approved August 11, 2020

Looking in some ISA/IEC-62443 Documents

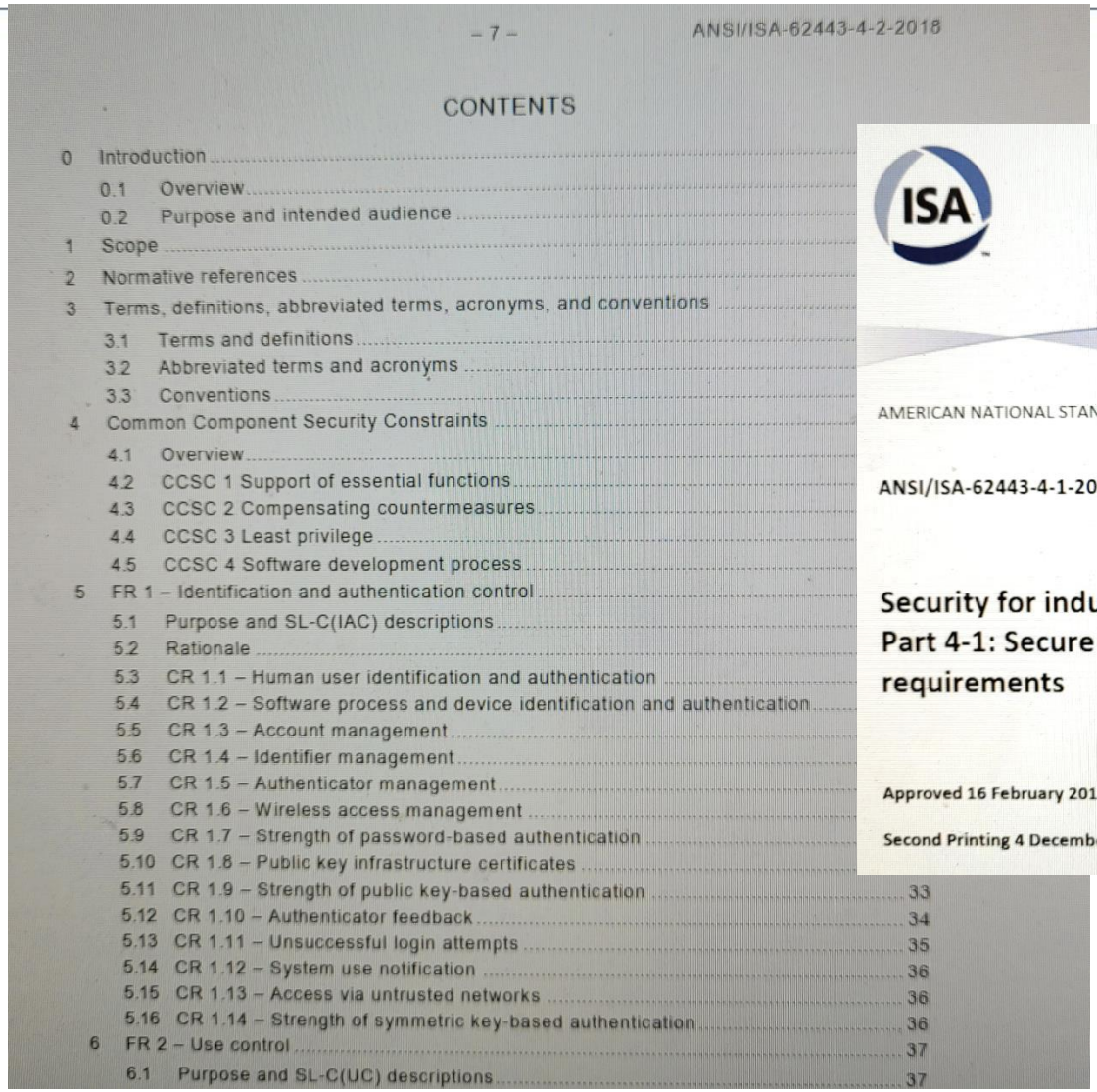
CONTENTS

ANSI/ISA-62443-3-3 (99.03.03)-2013

Security for industrial automation and control systems
Part 3-3: System security requirements and security levels

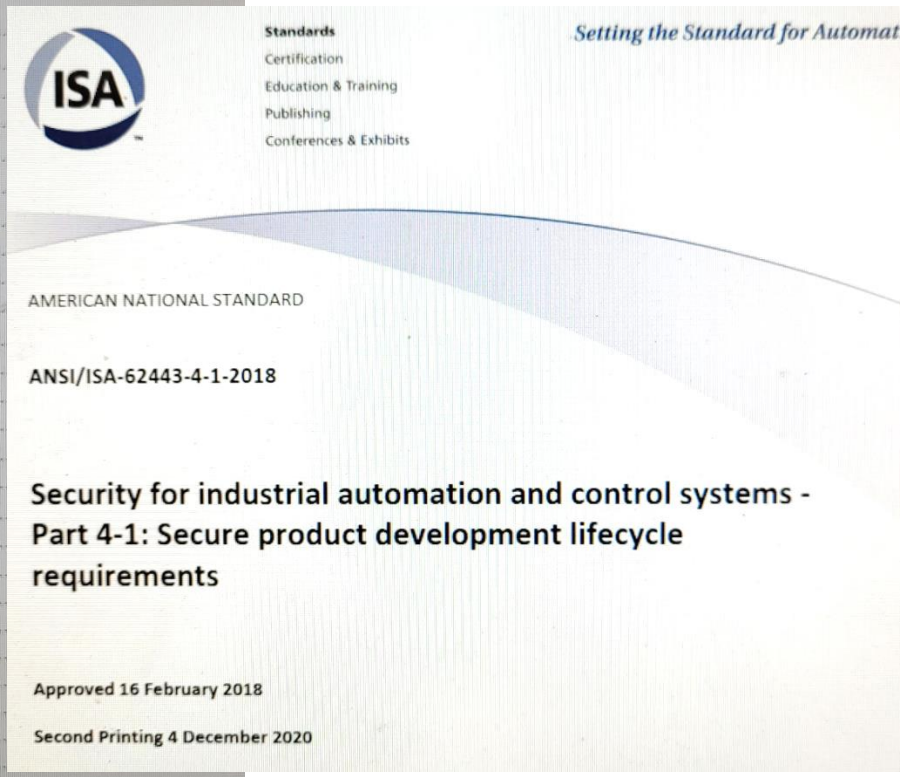
Approved 12 August 2013

Looking in some ISA/IEC-62443 Documents



– 7 – ANSI/ISA-62443-4-2-2018

CONTENTS



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automat

AMERICAN NATIONAL STANDARD

ANSI/ISA-62443-4-1-2018

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

Approved 16 February 2018

Second Printing 4 December 2020

40

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				

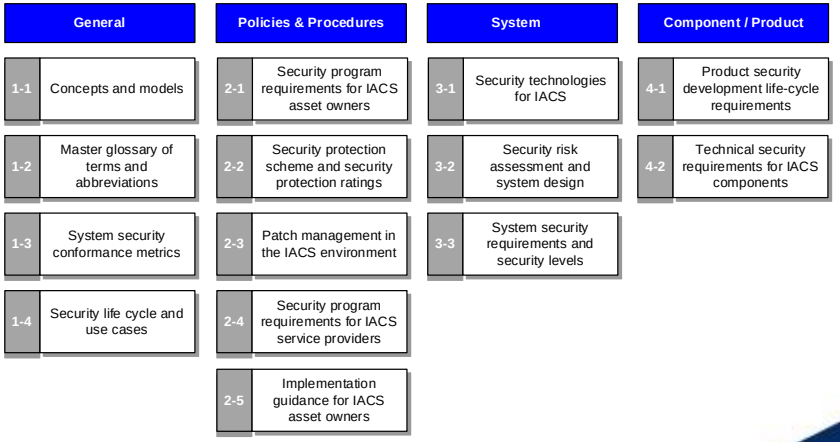
In ISA / IEC-62443 terminology:

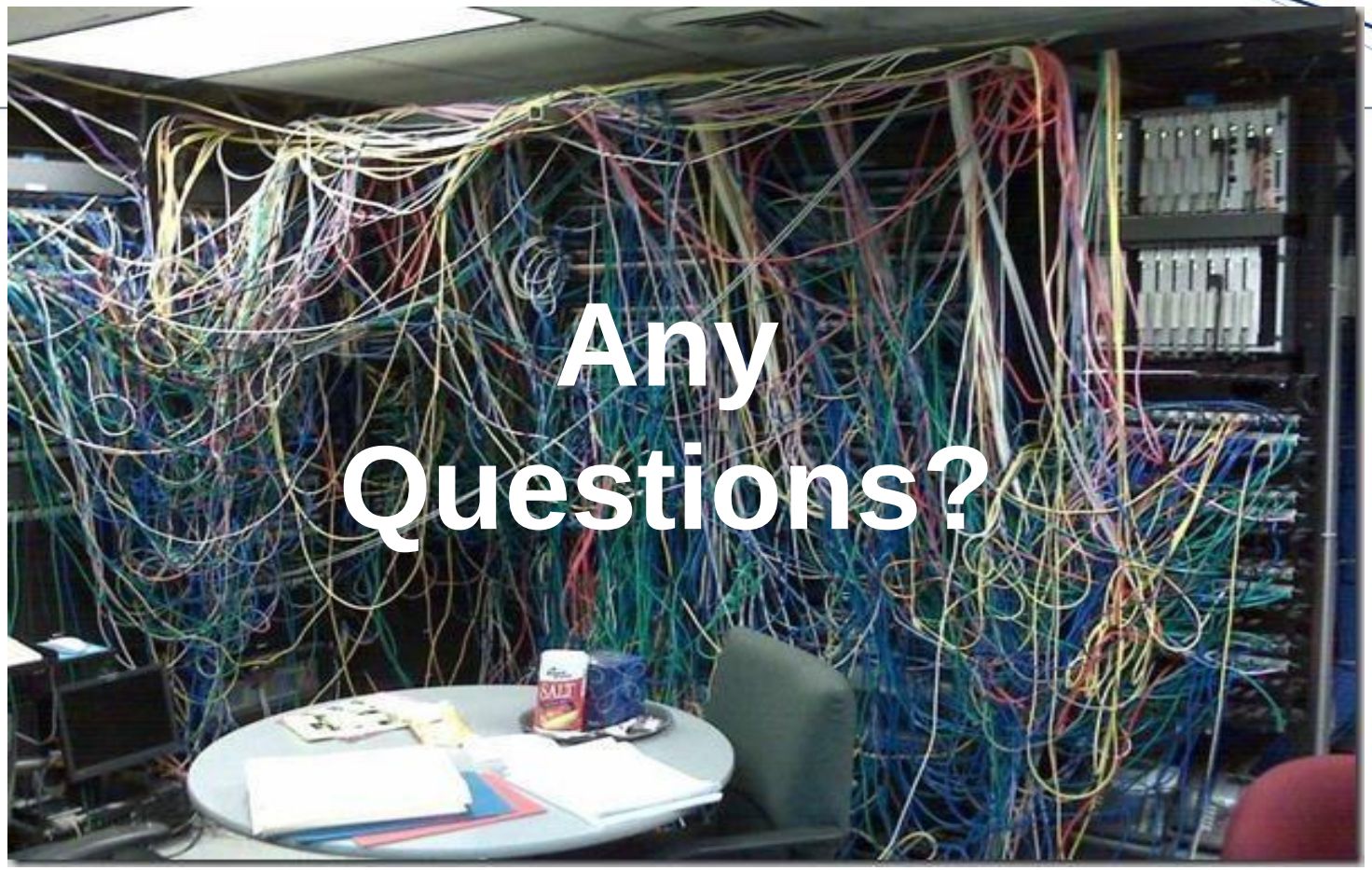
IACS = Industrial Automation Control System
also known as “OT” or “SCADA”

41

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





* Not a High Performance SCADA System

Graham Nasby, Water SCADA & Security Specialist
graham.nasby@guelph.ca