



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

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

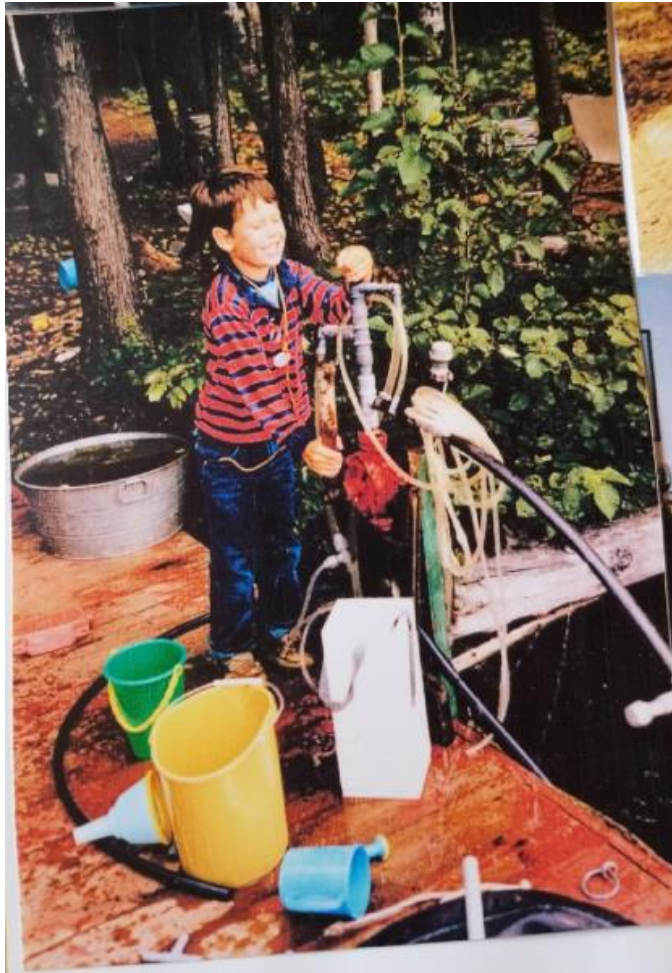
2022 National Water-Wastewater Conference
Canadian Water-Wastewater Association

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



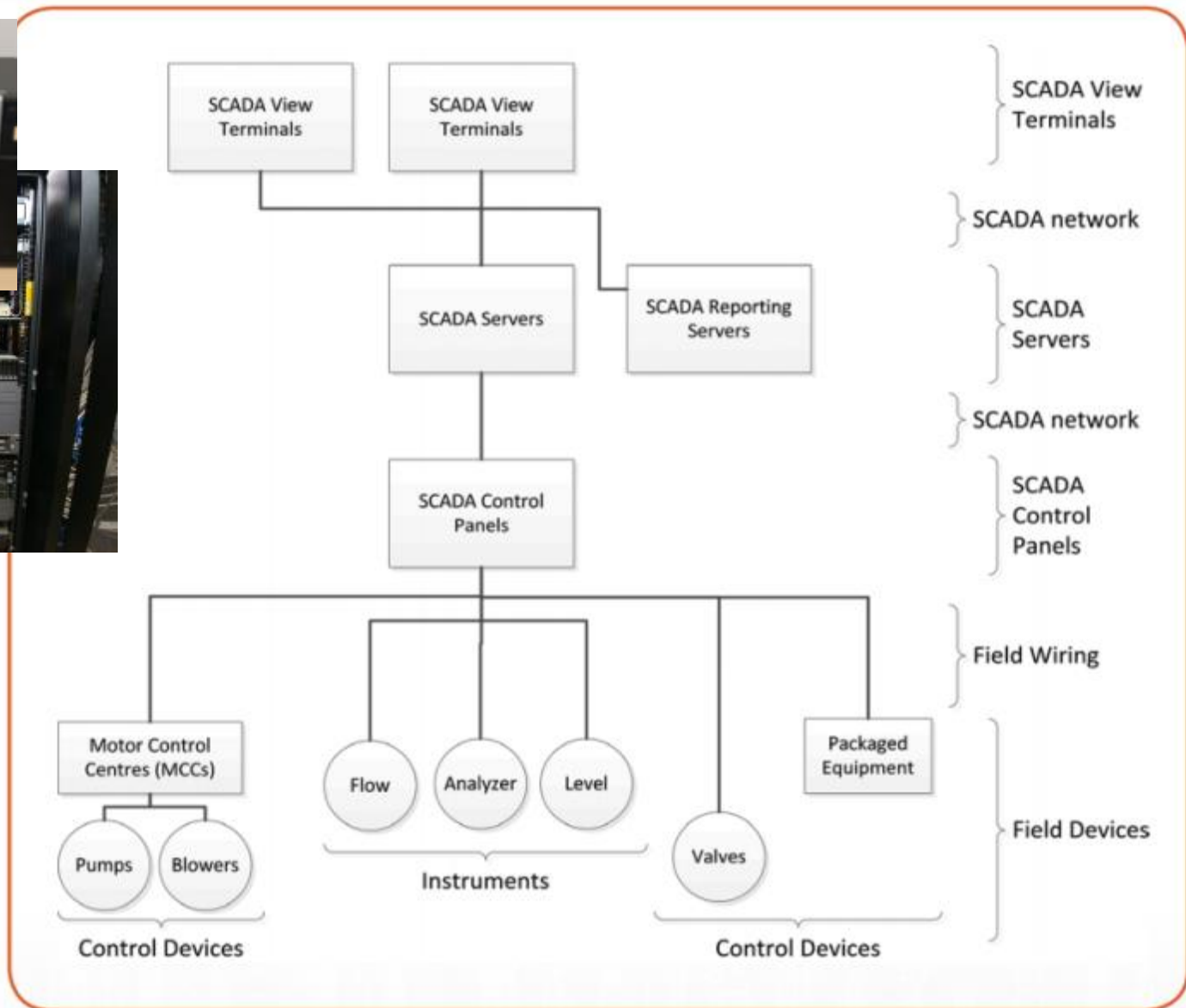
A Quick SCADA Refresher

What is SCADA?

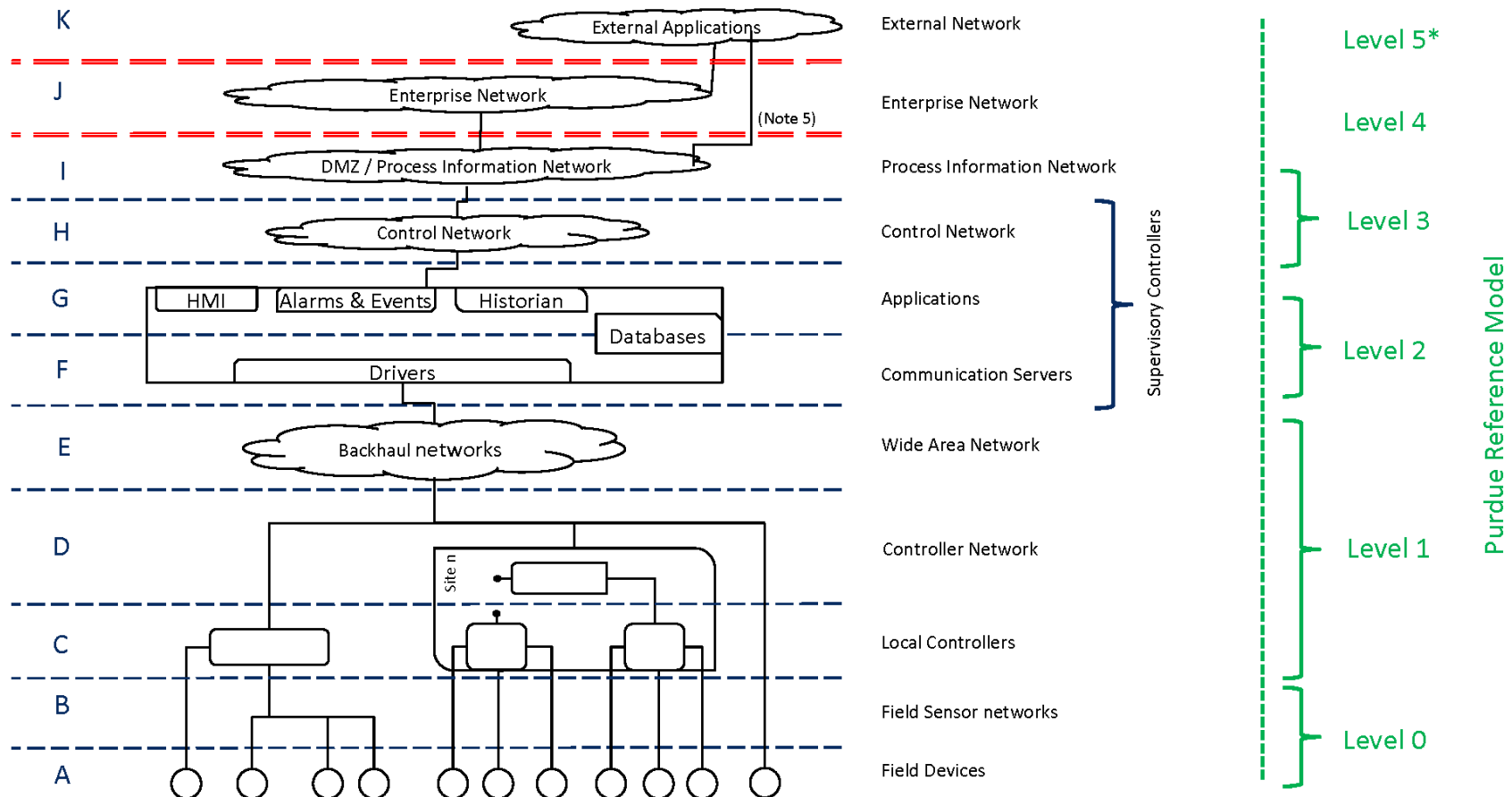


SCADA = Supervisory Control and Data Acquisition

Typical SCADA Architecture

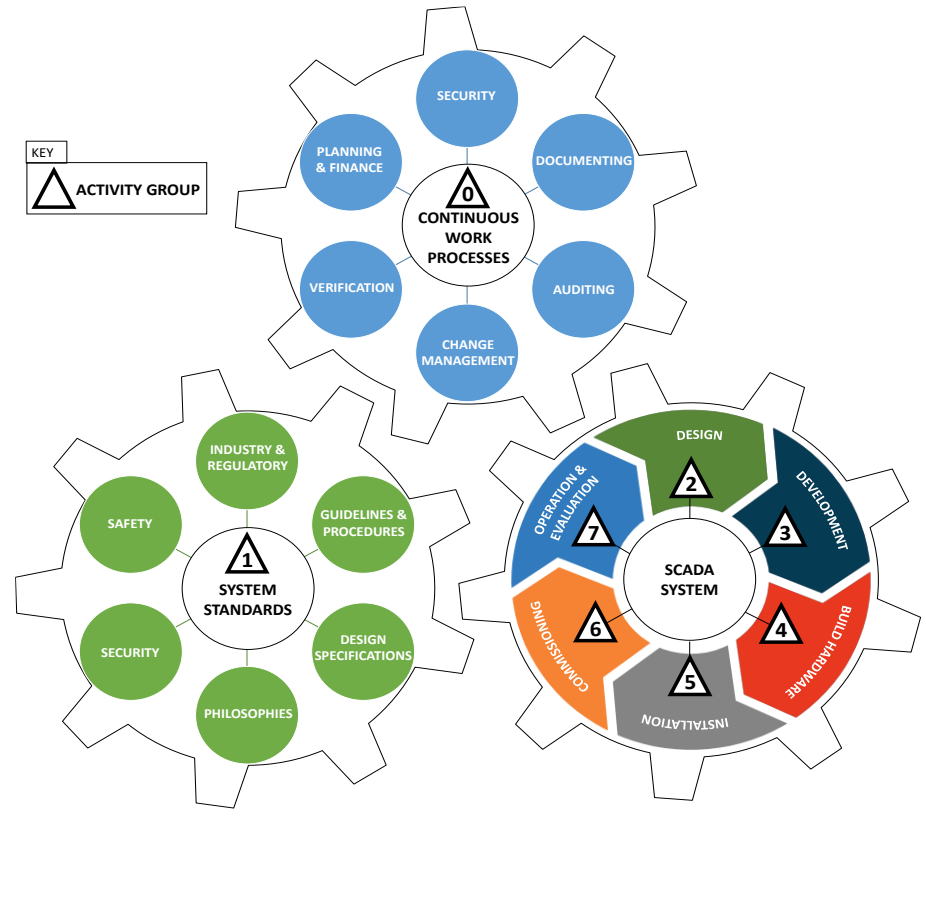
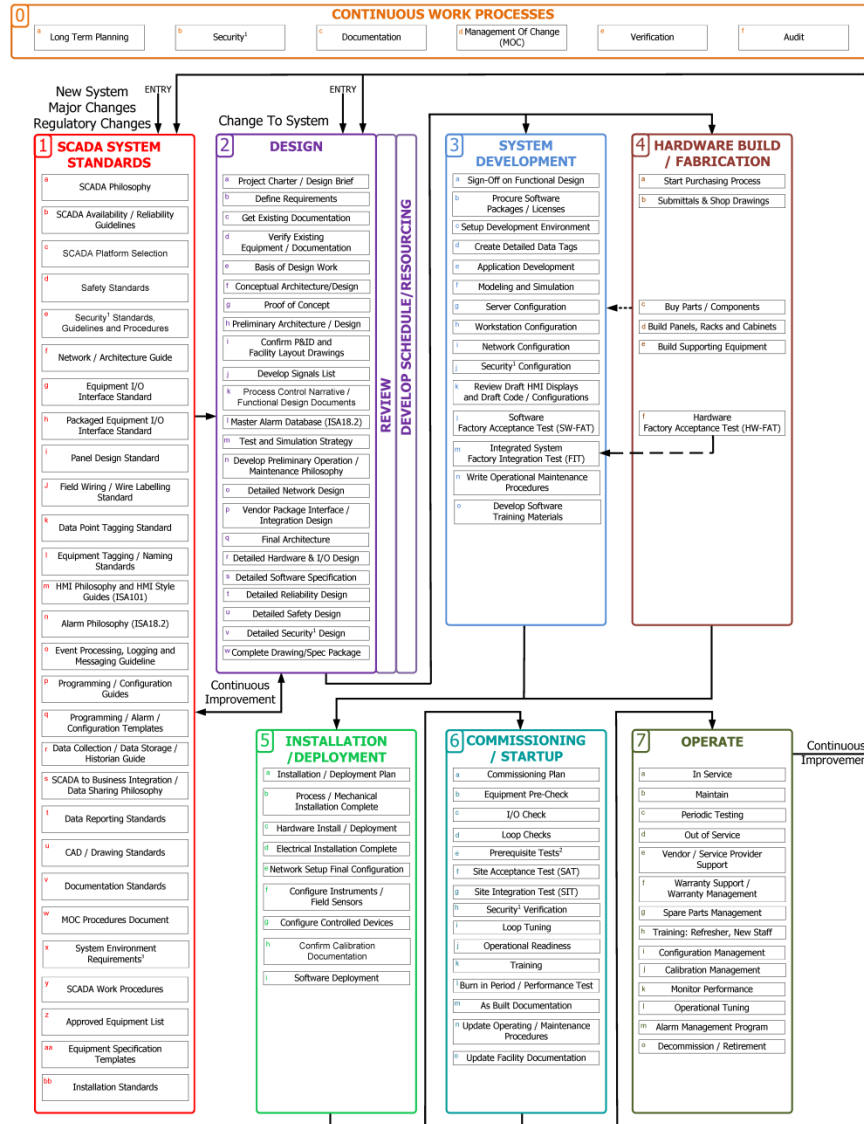


SCADA System Architecture



Revision May 28, 2020

SCADA Systems Lifecycle Diagram



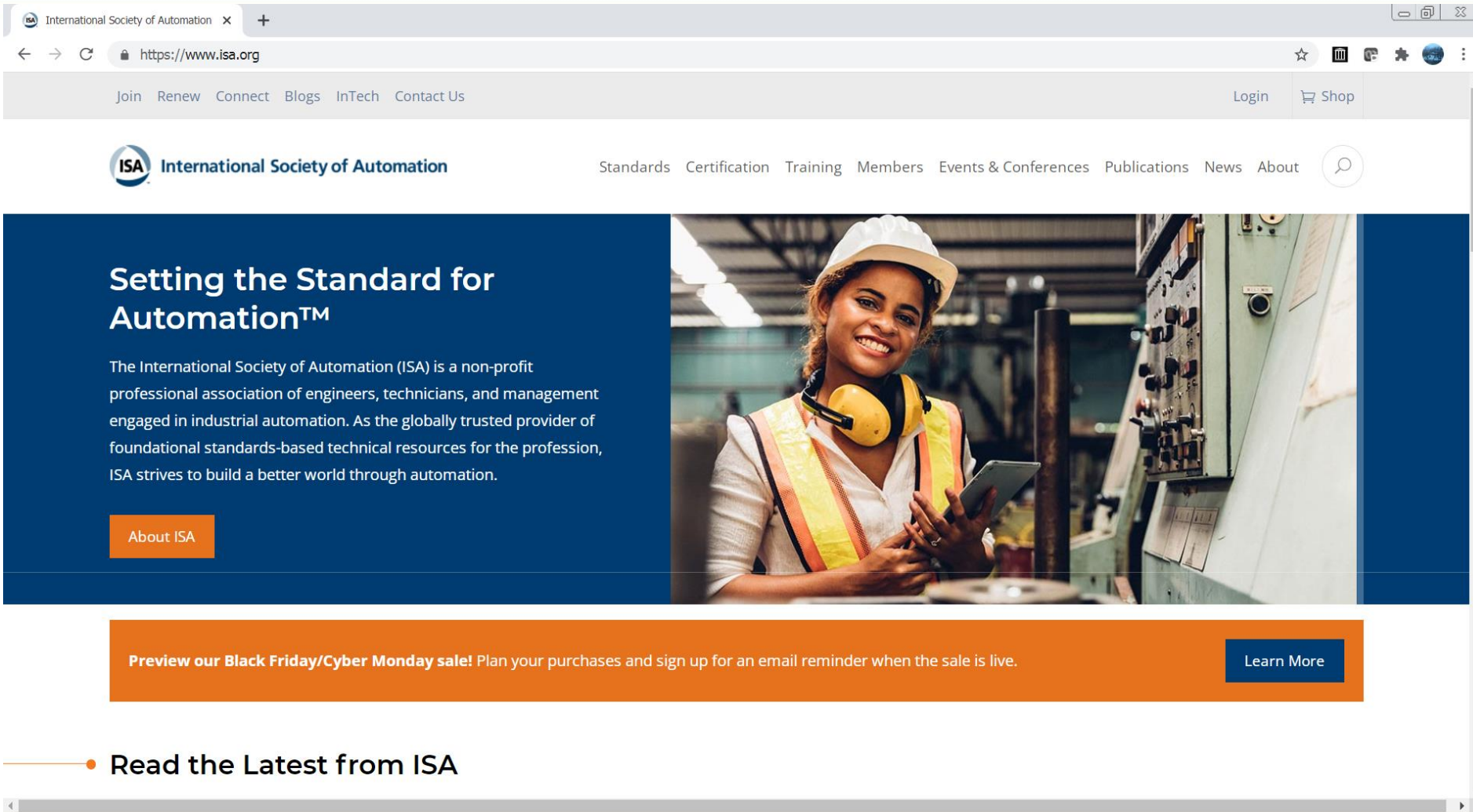
Notes
1) Security includes physical security, operational security, and cybersecurity.
2) Prerequisite tests typically include both cold and hot commissioning or dry / wet commissioning as applicable.
3) System Environment Requirements can include separate systems for development, testing, training,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

So how do we keep all this secure?

Answer:

ISA/IEC-62443 Series of Cybersecurity Standards

ISA – International Society of Automation



The screenshot shows the ISA website homepage. At the top, there's a navigation bar with links: Join, Renew, Connect, Blogs, InTech, Contact Us, Login, and Shop. Below this is the ISA logo and a search bar. The main content area features a large blue banner with the text "Setting the Standard for Automation™". To the right of this text is a photograph of a smiling female industrial worker wearing a white hard hat, a yellow safety vest, and a headset, holding a tablet. Below the banner is an orange promotional bar for a Black Friday/Cyber Monday sale, with a "Learn More" button. At the bottom, there's a section titled "Read the Latest from ISA" with a list of articles.

International Society of Automation x +

https://www.isa.org

Join Renew Connect Blogs InTech Contact Us Login Shop

ISA International Society of Automation

Standards Certification Training Members Events & Conferences Publications News About

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.

About ISA

Preview our Black Friday/Cyber Monday sale! Plan your purchases and sign up for an email reminder when the sale is live. [Learn More](#)

Read the Latest from ISA

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



Principal Roles

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

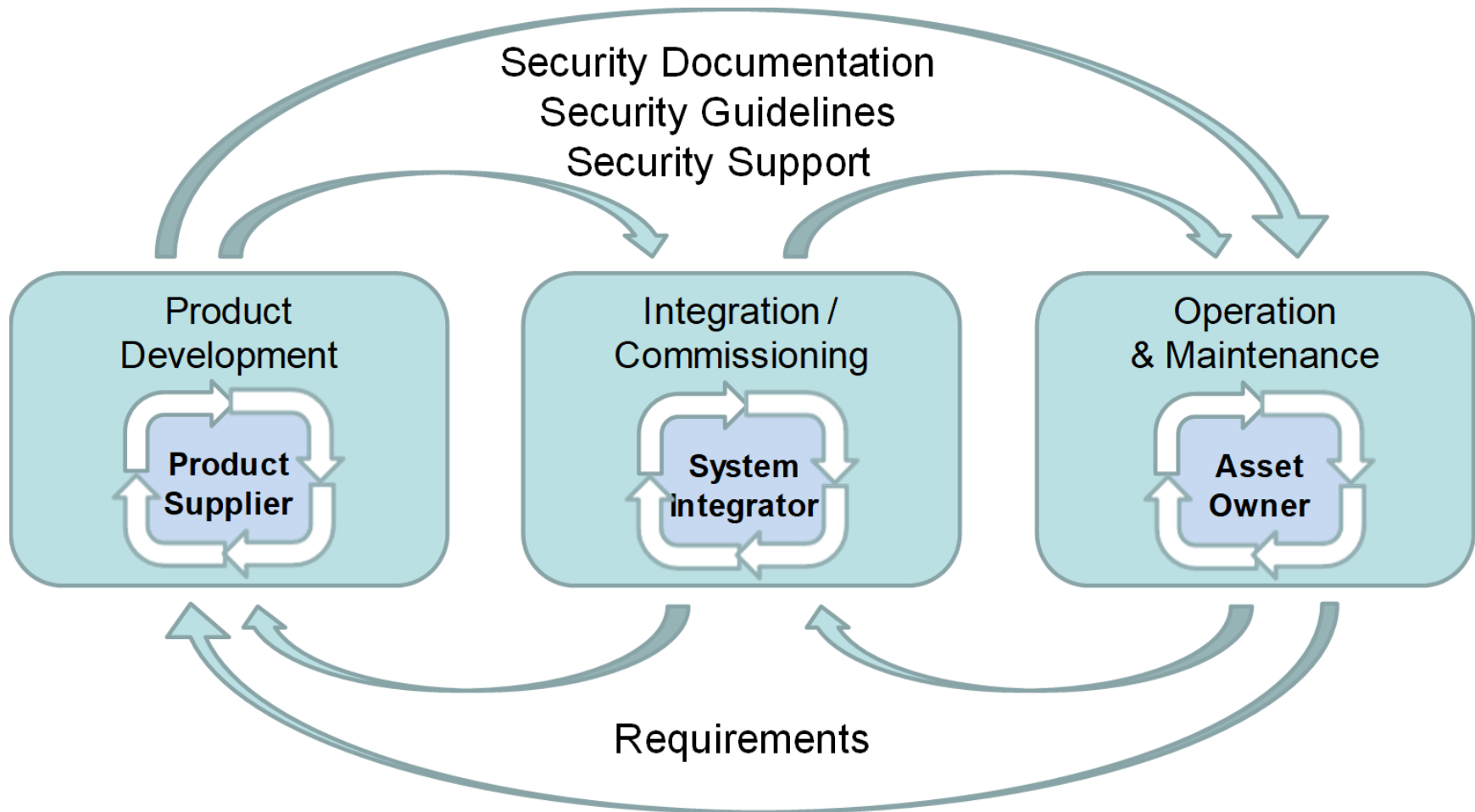


Associated Roles

- 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...



- [illegible]

26
26

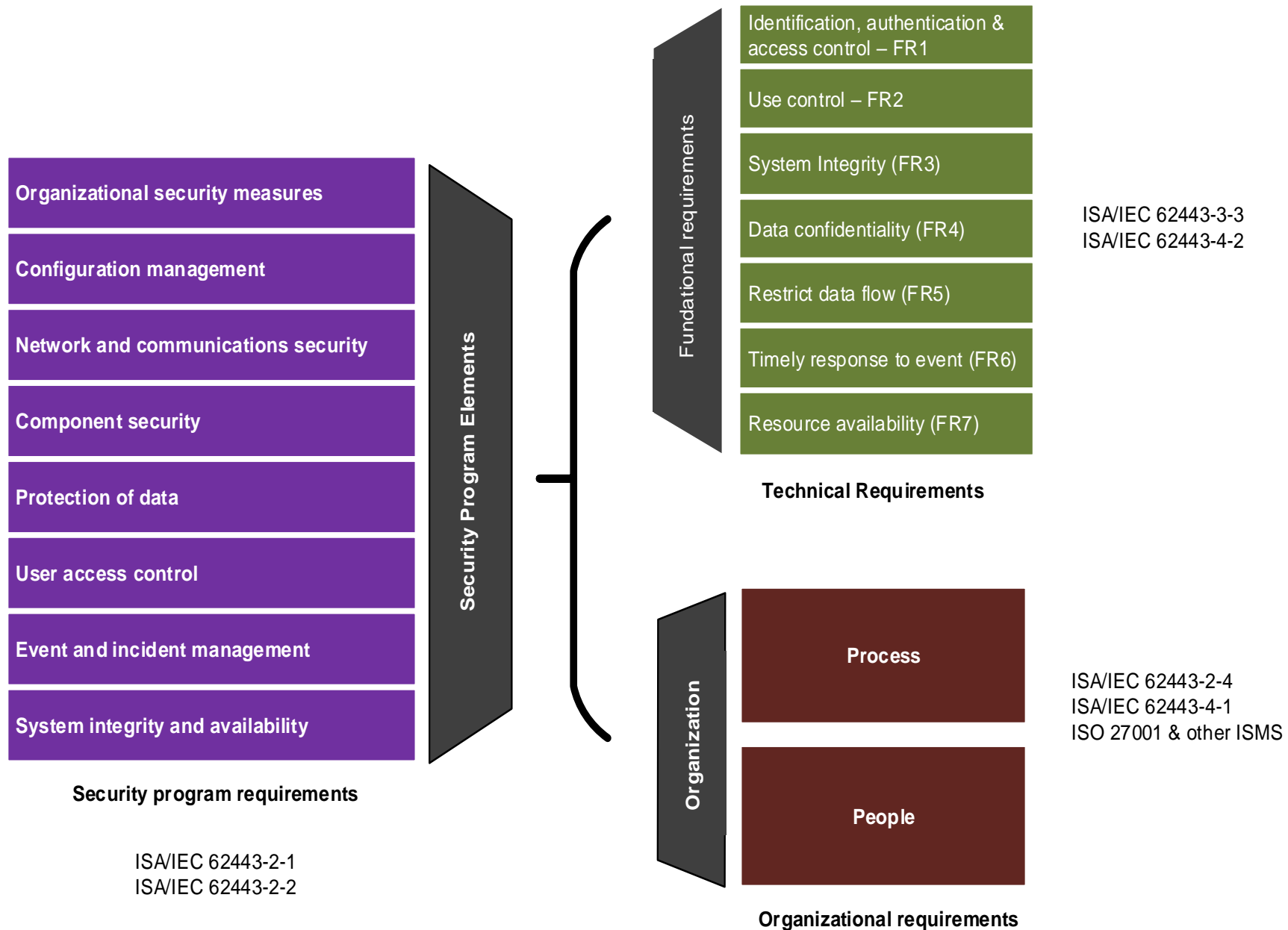
Operations Security Principals

- 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

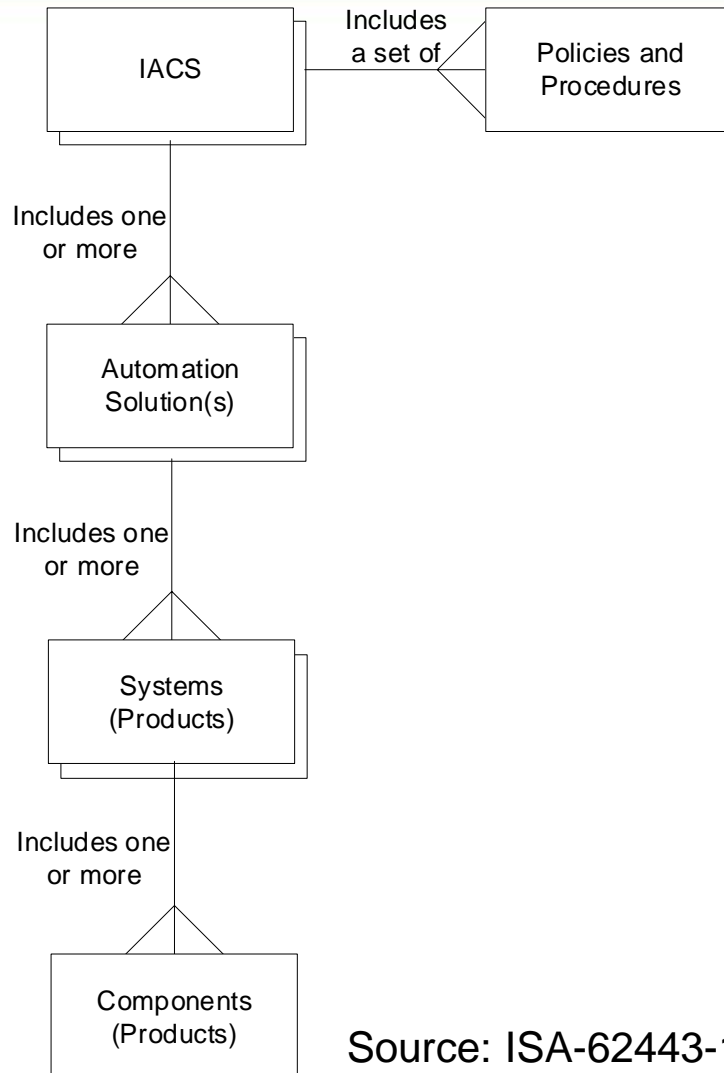


Source: ISA-62443-1-1

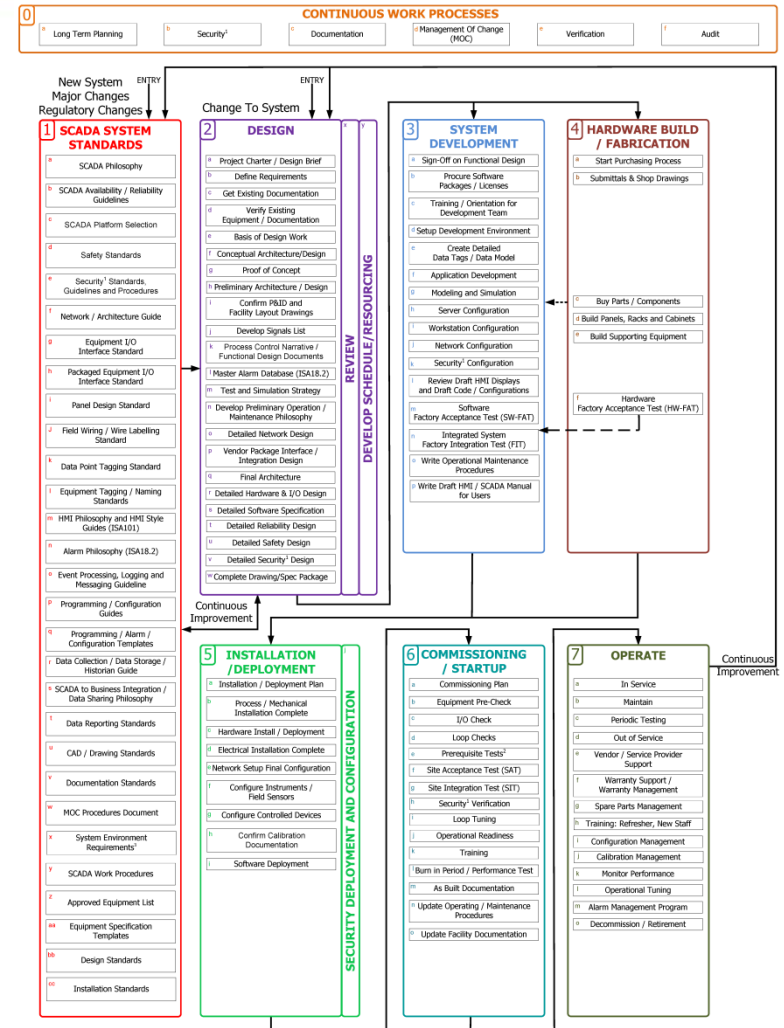
Security Element Grouping



Typical Structure of IACS System (SCADA)



Source: ISA-62443-1-1



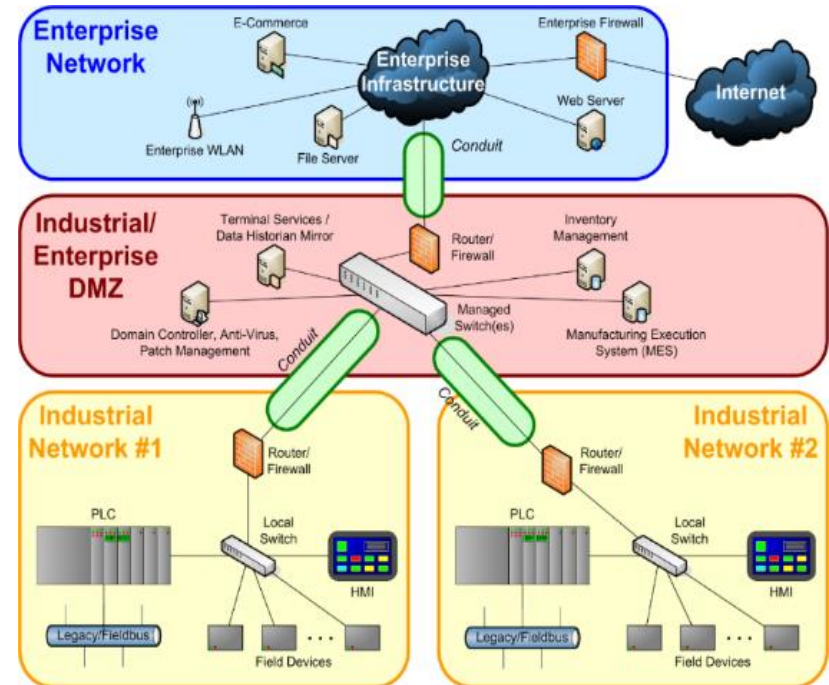
Notes
 1) Security includes physical security, operational security, and cybersecurity.
 2) Pre-mise tests typically include cold and hot commissioning or dry / wet commissioning as applicable.
 3) System Environment Requirements can include separate systems for development, testing, training, production,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

ISA112 Lifecycle Diagram
 Working Draft
 Revised July 20th, 2023

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

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

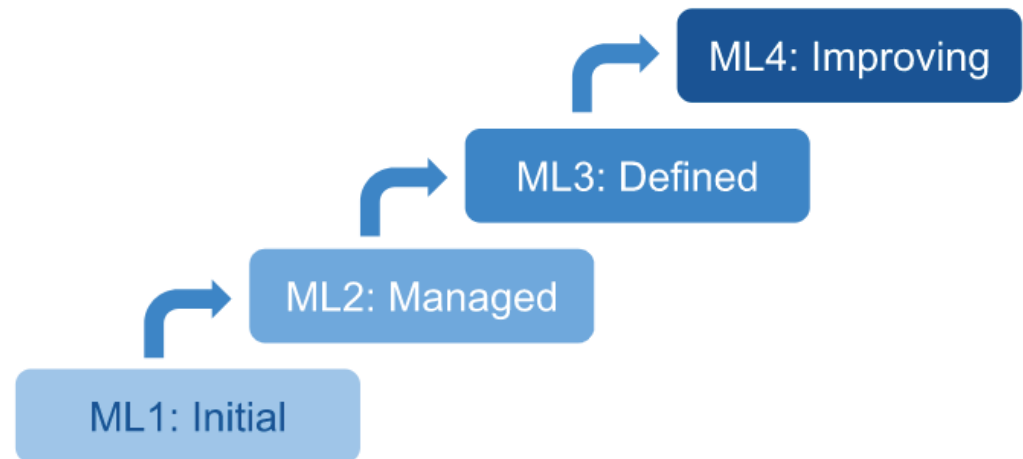
Intentional Violation Using Simple Means with Low Resources, Generic Skills & Low Motivation

1

Casual or Coincidental Violation

(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”

Looking in some ISA/IEC-62443 Documents

– 7 –

ANSI/ISA-62443-1-1 (99.01.01)–2007

Table of Contents

Foreword.....	11
Introduction	13
1 Scope	
2 Normative References	
3 Definitions.....	
3.1 Introduction	
3.2 Terms	
3.3 Abbreviations	
4 The Situation	
4.1 General	
4.2 Current Systems	
4.3 Current Trends	
4.4 Potential Impact.....	
5 Concepts.....	
5.1 General.....	36
5.2 Security Objectives	37
5.3 Defense in Depth	37
5.4 Security Context	39
5.5 Threat-Risk Assessment	46
5.6 Security Program Maturity	52
5.7 Policies	57
5.8 Security Zones	58
5.9 Conduits	60
5.10 Security Levels	

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

- 7 -

ANSI/ISA-62443-3-2-2020

CONTENTS

FOREWORD	9
INTRODUCTION	
1 Scope	
2 Normative references	
3 Terms, definitions, abbreviated terms, acronyms and conventions	
3.1 Terms and definitions	
3.2 Abbreviated terms and acronyms	
3.3 Conventions	
4 Zone, conduit and risk assessment requirements	
4.1 Overview	
4.2 ZCR 1: Identify the SUC	
4.2.1 ZCR 1.1: Identify the SUC perimeter and access points	
4.3 ZCR 2: Initial cyber security risk assessment	
4.3.1 ZCR 2.1: Perform initial cyber security risk assessment	
4.4 ZCR 3: Partition the SUC into zones and conduits	
4.4.1 Overview	
4.4.2 ZCR 3.1: Establish zones and conduits	
4.4.3 ZCR 3.2: Separate business and IACS assets	
4.4.4 ZCR 3.3: Separate safety related assets	
4.4.5 ZCR 3.4: Separate temporarily connected devices	
4.4.6 ZCR 3.5: Separate wireless devices	
4.4.7 ZCR 3.6: Separate devices connected via external networks	
4.5 ZCR 4: Risk comparison	
4.5.1 Overview	
4.5.2 ZCR 4.1: Compare initial risk to tolerable risk	
4.6 ZCR 5: Perform a detailed cyber security risk assessment	
4.6.1 Overview	22
4.6.2 ZCR 5.1: Identify threats	23
4.6.3 ZCR 5.2: Identify vulnerabilities	24
4.6.4 ZCR 5.3: Determine consequence and impact	24
4.6.5 ZCR 5.4: Determine unmitigated likelihood	25
4.6.6 ZCR 5.5: Determine unmitigated cyber security risk	25



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

12 August 2013

– 7 –

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

CONTENTS

PREFACE	3
FOREWORD	10
0 Introduction	11
0.1 Overview	11
0.2 Purpose and intended audience	12
0.3 Usage within other parts of the ISA-62443 series	12
1 Scope	15
2 Normative references	15
3 Terms, definitions, abbreviated terms, acronyms, and conventions	15
3.1 Terms and definitions	15
3.2 Abbreviated terms and acronyms	21
3.3 Conventions	23
4 Common control system security constraints	24
4.1 Overview	24
4.2 Support of essential functions	24
4.3 Compensating countermeasures	24
4.4 Least privilege	25
5 FR 1 – Identification and authentication control	25
5.1 Purpose and SL-C(IAC) descriptions	25
5.2 Rationale	25
5.3 SR 1.1 – Human user identification and authentication	25
5.4 SR 1.2 – Software process and device identification and authentication	27
5.5 SR 1.3 – Account management	28
5.6 SR 1.4 – Identifier management	28
5.7 SR 1.5 – Authenticator management	29
5.8 SR 1.6 – Wireless access management	30
5.9 SR 1.7 – Strength of password-based authentication	31
5.10 SR 1.8 – Public key infrastructure (PKI) certificates	32
5.11 SR 1.9 – Strength of public key authentication	33
5.12 SR 1.10 – Authenticator feedback	34
5.13 SR 1.11 – Unsuccessful login attempts	34
5.14 SR 1.12 – System use notification	35
5.15 SR 1.13 – Access via untrusted networks	35
6 FR 2 – Use control	36
6.1 Purpose and SL-C(UC) descriptions	36
6.2 Rationale	36
6.3 SR 2.1 – Authorization enforcement	37

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

0	Introduction	
0.1	Overview	
0.2	Purpose and intended audience	
1	Scope	
2	Normative references	
3	Terms, definitions, abbreviated terms, acronyms, and conventions	
3.1	Terms and definitions	
3.2	Abbreviated terms and acronyms	
3.3	Conventions	
4	Common Component Security Constraints	
4.1	Overview	
4.2	CCSC 1 Support of essential functions	
4.3	CCSC 2 Compensating countermeasures	
4.4	CCSC 3 Least privilege	
4.5	CCSC 4 Software development process	
5	FR 1 – Identification and authentication control	
5.1	Purpose and SL-C(IAC) descriptions	
5.2	Rationale	
5.3	CR 1.1 – Human user identification and authentication	
5.4	CR 1.2 – Software process and device identification and authentication	
5.5	CR 1.3 – Account management	
5.6	CR 1.4 – Identifier management	
5.7	CR 1.5 – Authenticator management	
5.8	CR 1.6 – Wireless access management	
5.9	CR 1.7 – Strength of password-based authentication	
5.10	CR 1.8 – Public key infrastructure certificates	
5.11	CR 1.9 – Strength of public key-based authentication	33
5.12	CR 1.10 – Authenticator feedback	34
5.13	CR 1.11 – Unsuccessful login attempts	35
5.14	CR 1.12 – System use notification	36
5.15	CR 1.13 – Access via untrusted networks	36
5.16	CR 1.14 – Strength of symmetric key-based authentication	36
6	FR 2 – Use control	37
6.1	Purpose and SL-C(UC) descriptions	37



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

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				

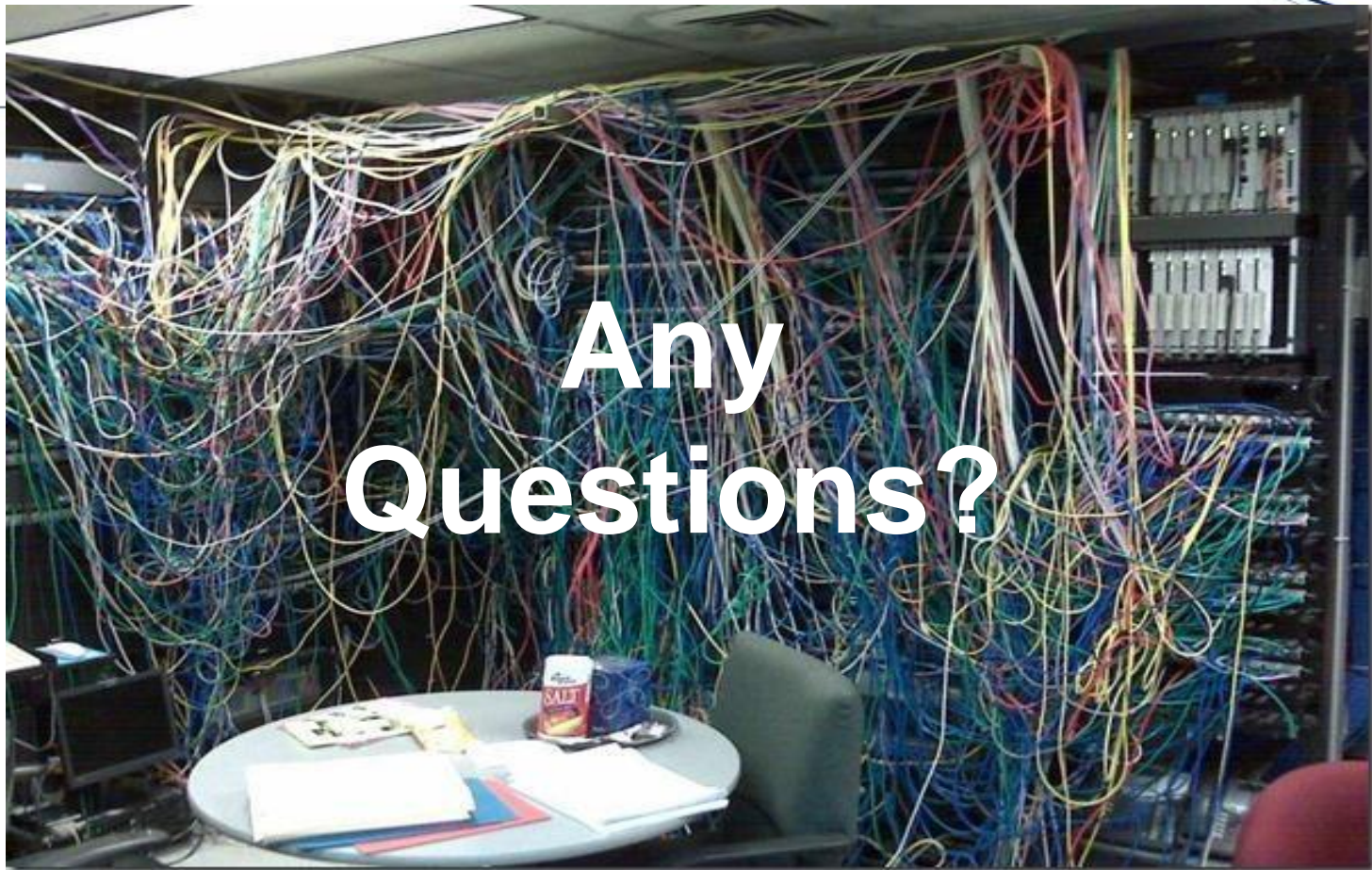
In ISA / IEC-62443 terminology:

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

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				



* Not a High Performance SCADA System

Graham Nasby, Water SCADA & Security Specialist

graham.nasby@guelph.ca