What can be certified with ISASecure

Mike Medoff
Director of Cybersecurity Certification
exida

Mike Medoff, CFSE, CACE

- Director of Cybersecurity Certification at exida
- Developer of many parts of ISASecure scheme
- Member of ISA 99 Committee
  - Leader of ISA99 task group which developed ISA/IEC 62443-4-1 standard (Security for industrial automation and control systems   Part 4-1: Product Development Requirements)
- Member ISA Security Institute Technical Steering Committee
- Lead assessor on exida ISASecure certifications
- Co-author of "Implementing IEC 62443: A Pragmatic Approach to Cybersecurity"

Acronyms Used in this Presentation

- IACS – Industrial Automation and Control System
- ISA – International Society of Automation
- ISCI – ISA Security Institute
- ISASecure – ISA Security Institute Certification Scheme
- IEC – International Electrotechnical Commission

Agenda:
1. ISA/IEC 62443 Standards
2. ISASecure Certification

Which standards apply

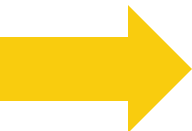Types of certifications

Types of components that can be certified

Types of systems that can be certified

Actual products and processes certified

3. Benefits of Certification

Agenda:

→ 1. ISA/IEC 62443 Standards

2. ISASecure Certification

      Which standards apply

      Types of certifications

      Types of components that can be certified

      Types of systems that can be certified

      Actual products and processes certified

3. Benefits of Certification
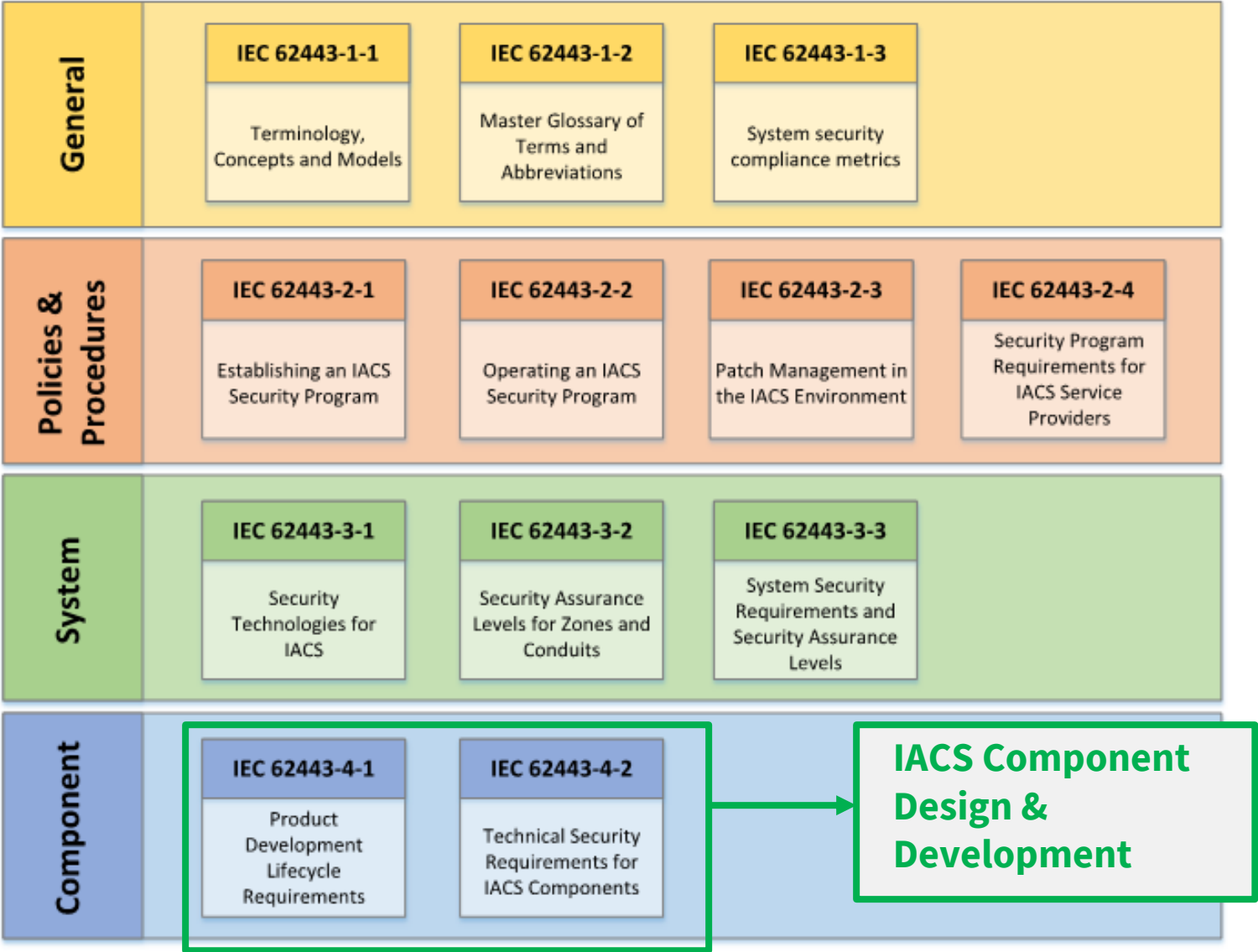
ISA/IEC 62443 Organization

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity.
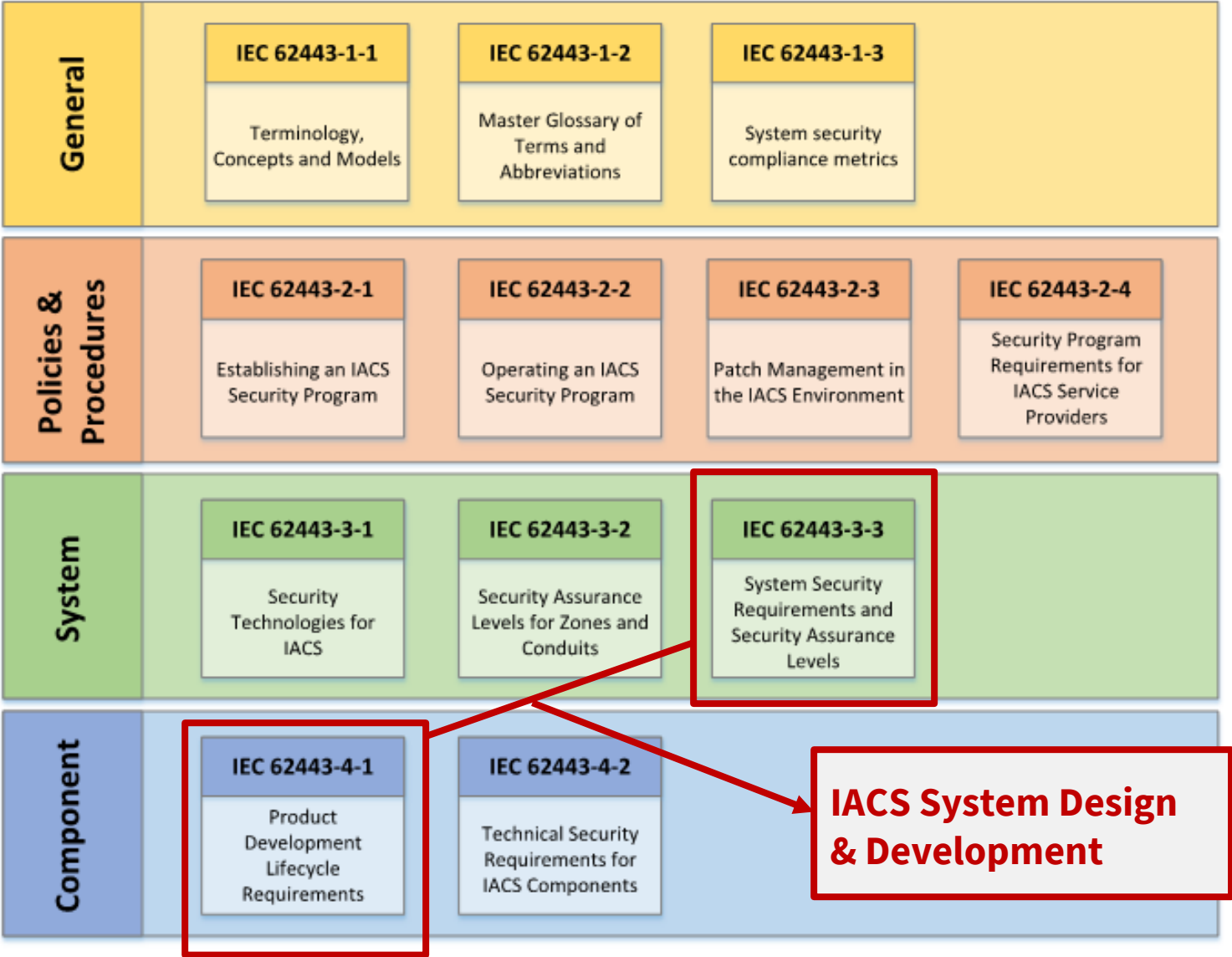
General			
IEC 62443-1-1 Terminology, Concepts and Models	**IEC 62443-1-2** Master Glossary of Terms and Abbreviations	**IEC 62443-1-3** System security compliance metrics	

Policies & Procedures			
IEC 62443-2-1 Establishing an IACS Security Program	**IEC 62443-2-2** Operating an IACS Security Program	**IEC 62443-2-3** Patch Management in the IACS Environment	**IEC 62443-2-4** Security Program Requirements for IACS Service Providers

System		
IEC 62443-3-1 Security Technologies for IACS	**IEC 62443-3-2** Security Assurance Levels for Zones and Conduits	**IEC 62443-3-3** System Security Requirements and Security Assurance Levels

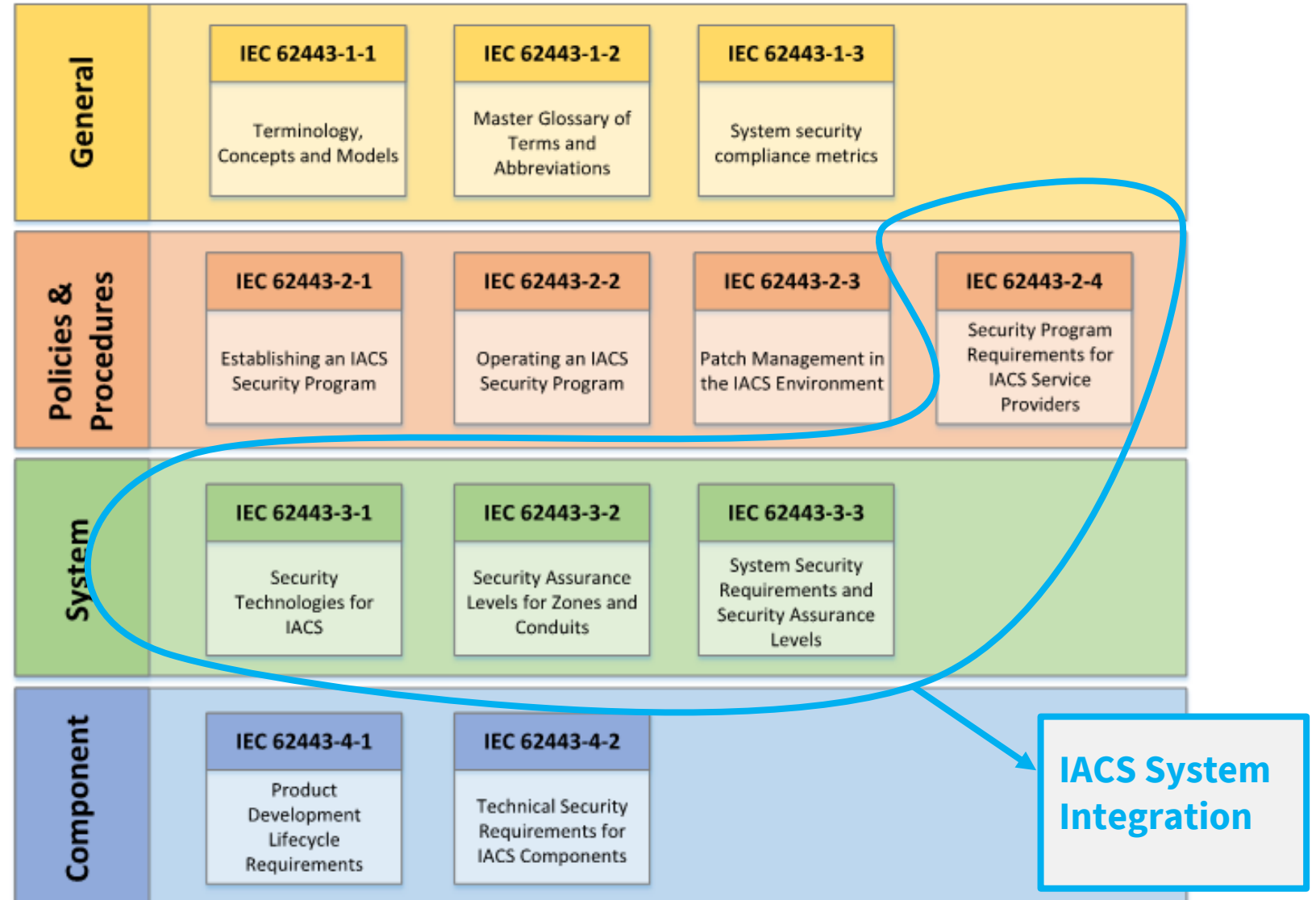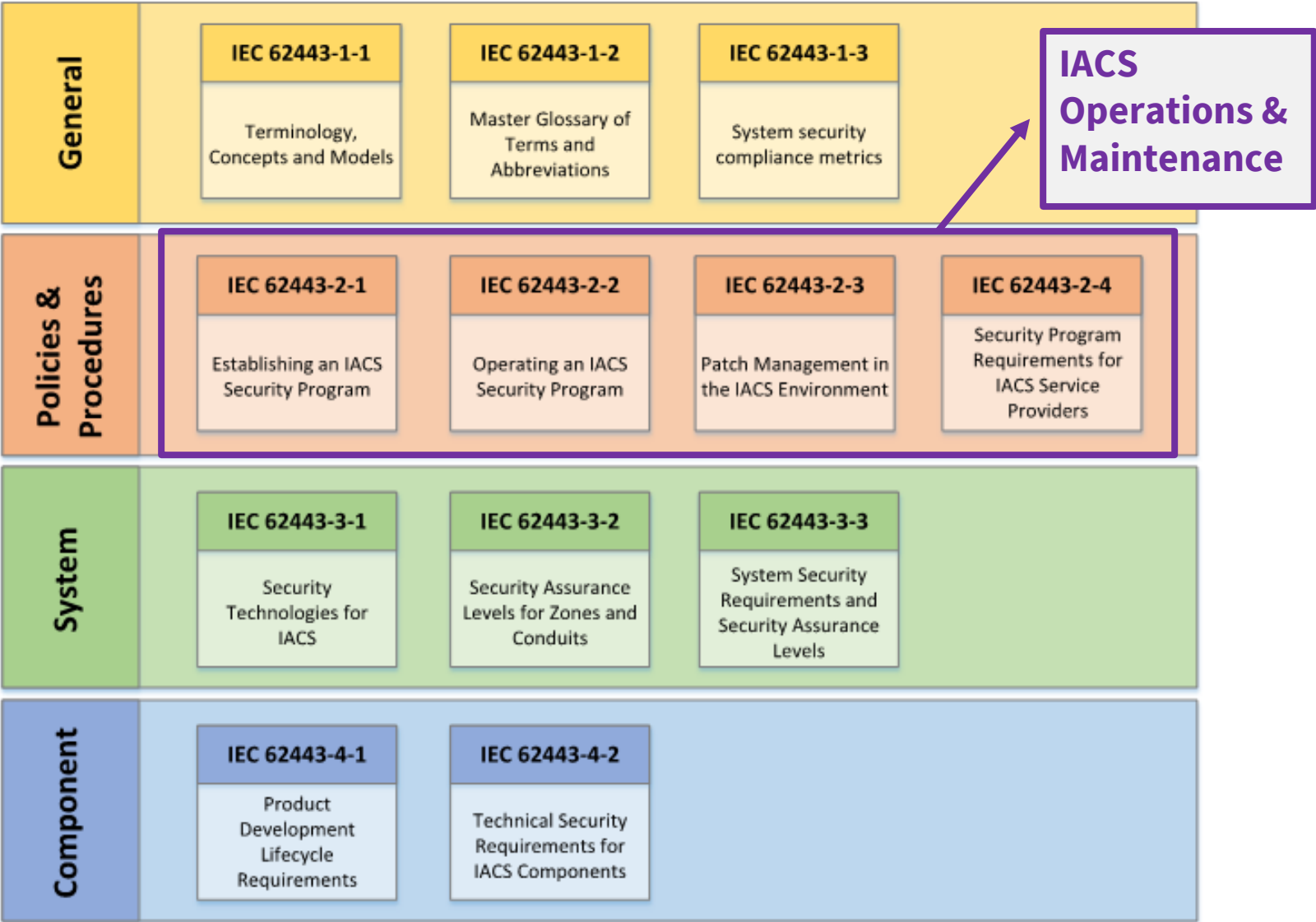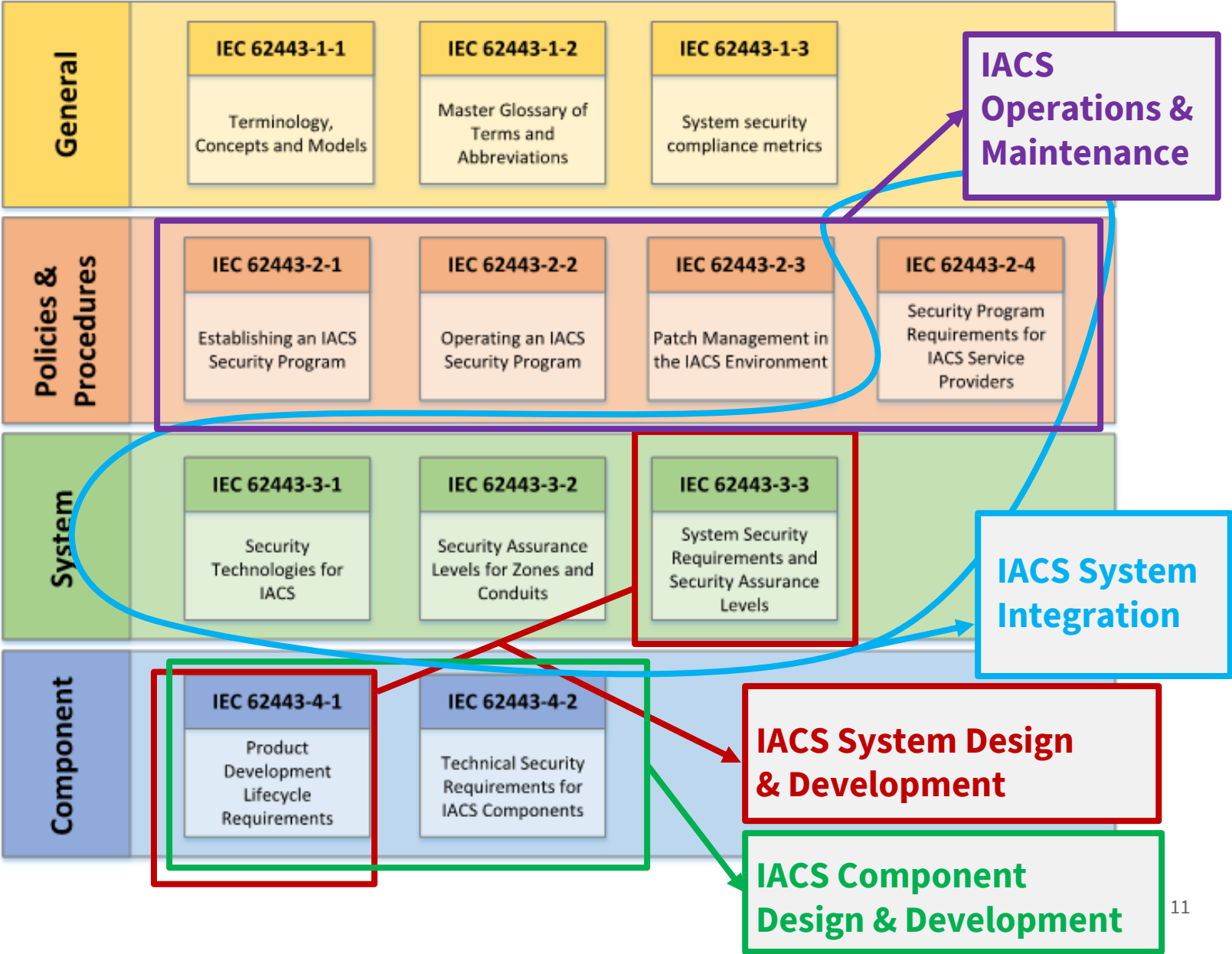| Component	
IEC 62443-4-1 Product Development Lifecycle Requirements	**IEC 62443-4-2** Technical Security Requirements for IACS Components

ISA/IEC 62443 Organization

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity.

General			
IEC 62443-1-1 Terminology, Concepts and Models	**IEC 62443-1-2** Master Glossary of Terms and Abbreviations	**IEC 62443-1-3** System security compliance metrics	

Policies & Procedures			
IEC 62443-2-1 Establishing an IACS Security Program	**IEC 62443-2-2** Operating an IACS Security Program	**IEC 62443-2-3** Patch Management in the IACS Environment	**IEC 62443-2-4** Security Program Requirements for IACS Service Providers

System		
IEC 62443-3-1 Security Technologies for IACS	**IEC 62443-3-2** Security Assurance Levels for Zones and Conduits	**IEC 62443-3-3** System Security Requirements and Security Assurance Levels

Component	
IEC 62443-4-1 Product Development Lifecycle Requirements	**IEC 62443-4-2** Technical Security Requirements for IACS Components

IACS Component Design & Development

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity.

General

IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3
Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics

Policies & Procedures

IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers

System

IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3
Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels

Component

IEC 62443-4-1	IEC 62443-4-2
Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components

IACS System Design & Development

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity.

General

IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3
Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics

Policies & Procedures

IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers

System

IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3
Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels

Component

IEC 62443-4-1	IEC 62443-4-2
Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components

IACS System Integration

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity.

General

IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3
Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics

Policies & Procedures

IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers

IACS Operations & Maintenance

System

IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3
Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels

Component

IEC 62443-4-1	IEC 62443-4-2
Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components

Unlike older standards (e.g. IEC 61508 functional safety) which covered everything in one document, ISA/IEC 62443 was broken up into multiple documents. This allows faster release and updating, something important for the fast moving field of cybersecurity.

General	IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	
	Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics	
Policies & Procedures	IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
	Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers
System	IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3	
	Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels	
Component	IEC 62443-4-1	IEC 62443-4-2		
	Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components		

IACS Operations & Maintenance

IACS System Integration

IACS System Design & Development

IACS Component Design & Development

11

Agenda:
1. ISA/IEC 62443 Standards
→ **2. ISASecure Certification**

Which standards apply

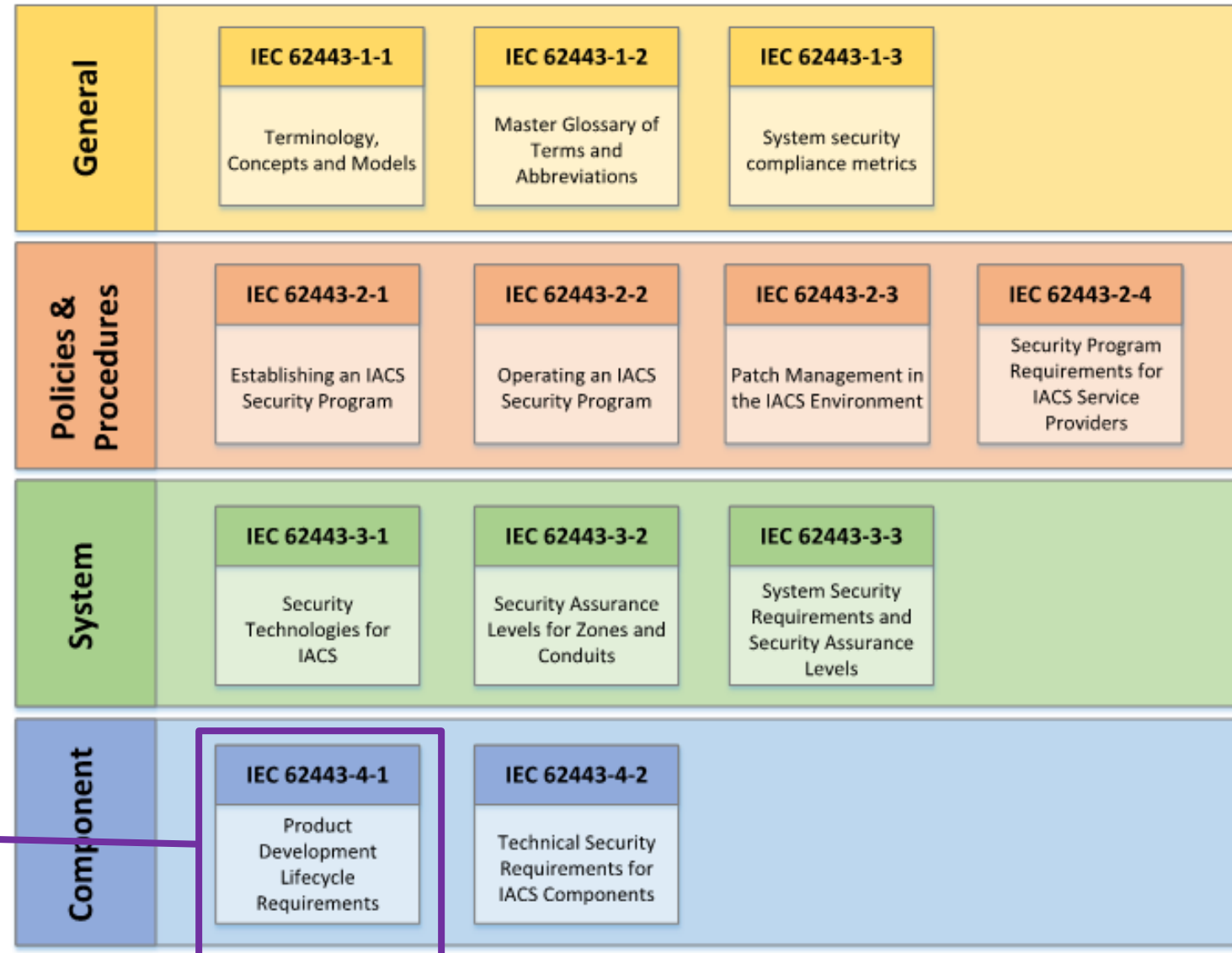Types of certifications

Types of components that can be certified

Types of systems that can be certified

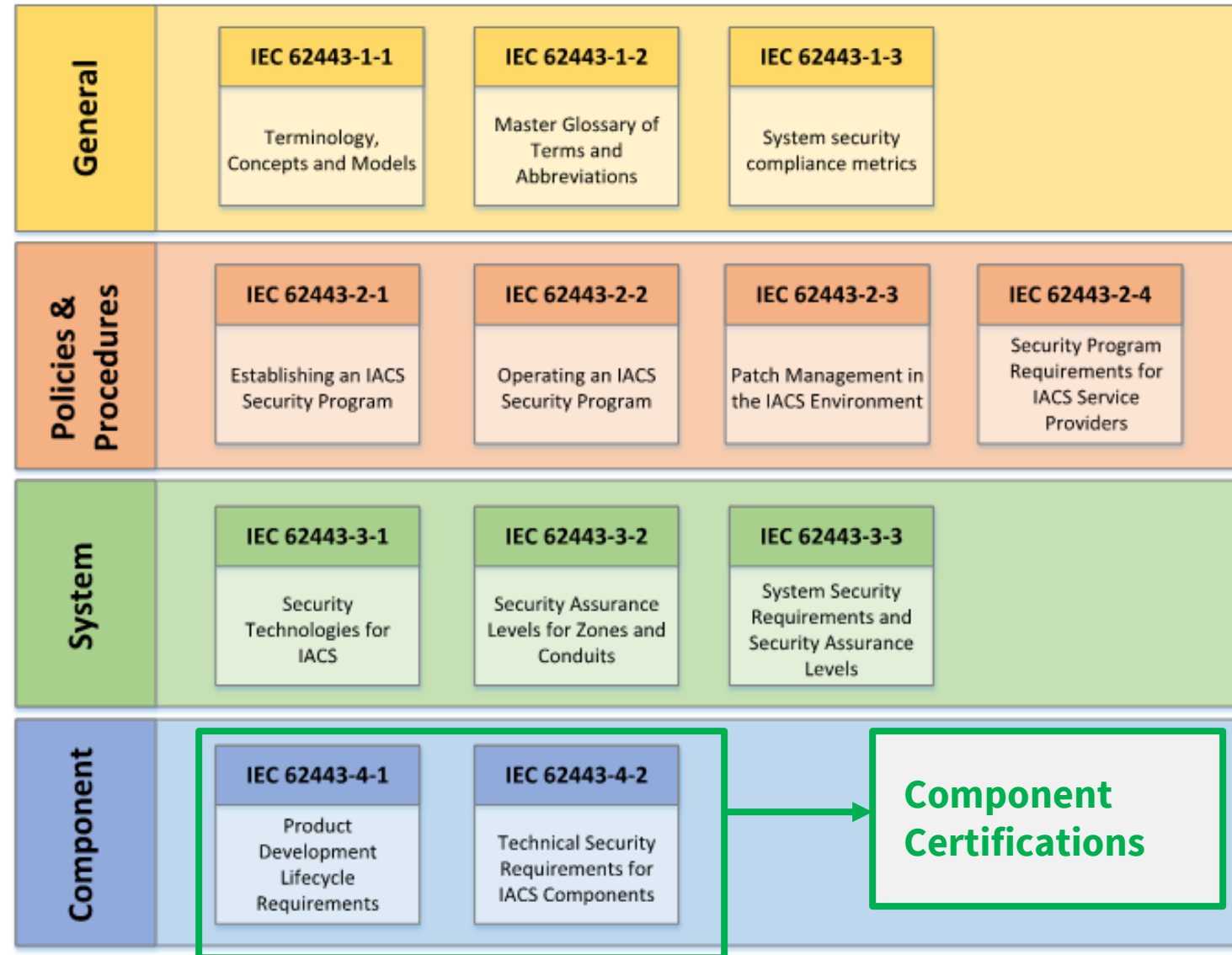Actual products and processes certified
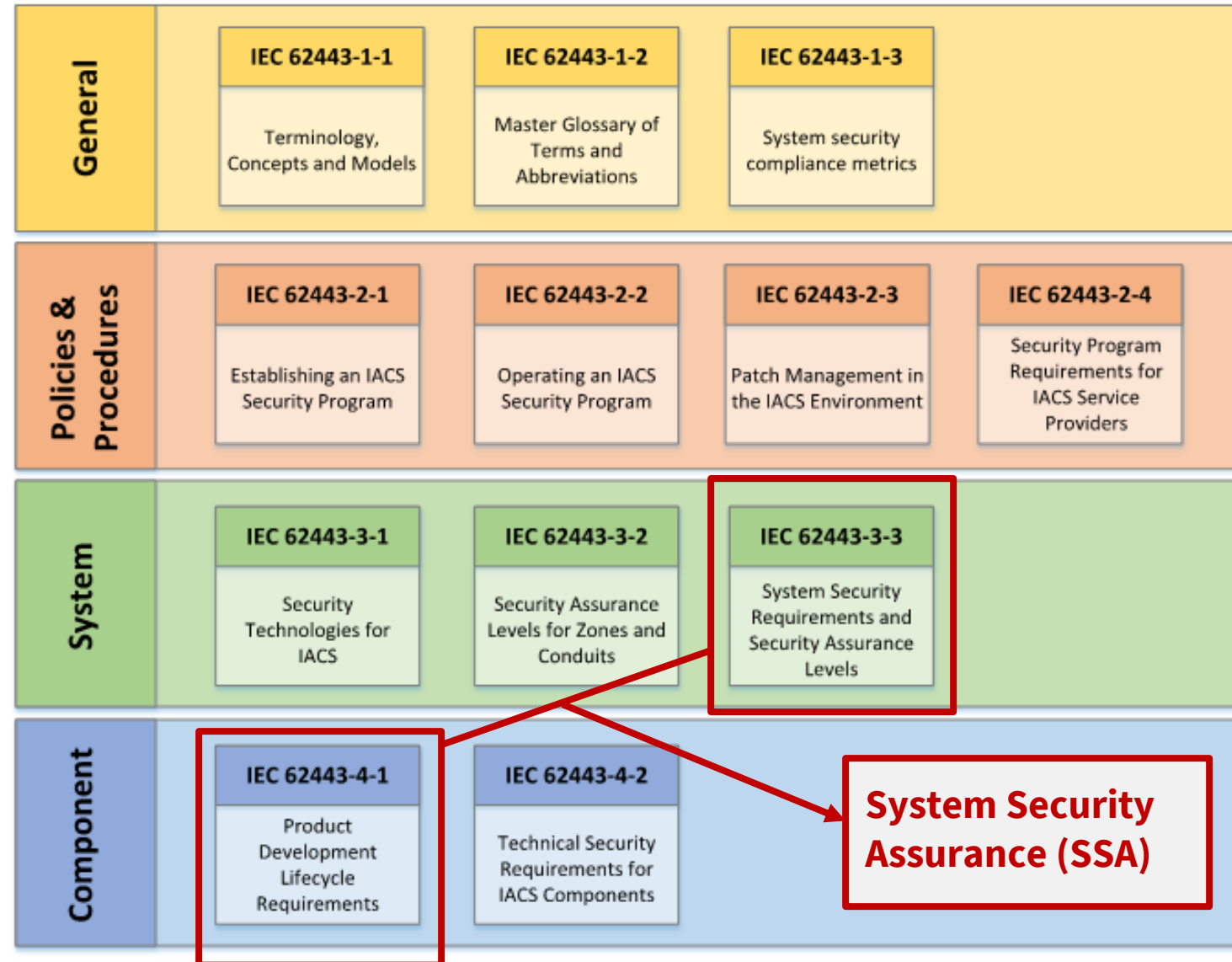
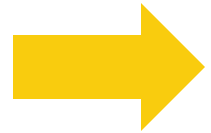**3. Benefits of Certification**

What is ISASecure Certification?

- **Third party technical expert attestation of compliance against ISA/IEC 62443 requirements from three categories:**

  - Detailed Analysis of engineering processes to determine Systematic Capability and Cybersecurity Strength

  - Detailed Analysis of product design and validation testing to show cybersecurity protection mechanisms in the product.

  - Network Testing to show safe, correct operation and Cybersecurity Susceptibility

ISA Security Institute Role

- **Owns ISASecure Certification Scheme which means:**
  - Defines scheme which defines how certification will be done
  - Maintains scheme – Updates occur when standard is updated or improvements needed
  - Approves certification bodies to perform the certification
    - *exida* was the first Accredited ISASecure Certification Body

Agenda:
1. ISA/IEC 62443 Standards
2. ISASecure Certification
→ **Which standards apply**
Types of certifications
Types of components that can be certified
Types of systems that can be certified
Actual products and processes certified
3. Benefits of Certification

ISA/IEC 62443 Organization

General			
IEC 62443-1-1	**IEC 62443-1-2**	**IEC 62443-1-3**	
Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics	

Policies & Procedures

IEC 62443-2-1	**IEC 62443-2-2**	**IEC 62443-2-3**	**IEC 62443-2-4**
Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers

System

IEC 62443-3-1	**IEC 62443-3-2**	**IEC 62443-3-3**
Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels

Component

IEC 62443-4-1	**IEC 62443-4-2**
Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components

Security Development Lifecycle Assessment (SDLA)

ISA/IEC 62443 Organization

General	IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	
	Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics	

Policies & Procedures	IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
	Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers

System	IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3	
	Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels	

Component	IEC 62443-4-1	IEC 62443-4-2	Component Certifications
	Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components	

ISA/IEC 62443 Organization

General	IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	
	Terminology, Concepts and Models	Master Glossary of Terms and Abbreviations	System security compliance metrics	

Policies & Procedures	IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
	Establishing an IACS Security Program	Operating an IACS Security Program	Patch Management in the IACS Environment	Security Program Requirements for IACS Service Providers

System	IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3	
	Security Technologies for IACS	Security Assurance Levels for Zones and Conduits	System Security Requirements and Security Assurance Levels	

Component	IEC 62443-4-1	IEC 62443-4-2	
	Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components	

System Security Assurance (SSA)

ISA/IEC 62443 Organization

Agenda:
1. ISA/IEC 62443 Standards
2. ISASecure Certification

Which standards apply

→ Types of certifications

Types of components that can be certified

Types of systems that can be certified

Actual products and processes certified

3. Benefits of Certification

Types of certifications

- Process Certifications
  - Shows that a company has a documented process that complies with the requirements of a standard
  - Shows that this process is being followed by that company for a sampling of products
- Product (Component) Certifications
  - Shows that a particular product is compliant with the requirements of one or more standards
- System Certifications
  - Shows that a system (collection of components) is compliant with the requirements of one or more standards

Types of certifications

- Process Certifications
  - Security Development Lifecycle Assurance (SDLA)
  - Shows that a company has a documented process that complies ISA/IEC 62443-4-1 (Product Development Lifecycle Requirements)
  - Shows that this process is being followed by that company for a sampling of products
- Product (Component) Certifications
  - ISASecure has 4 types of these certifications (EDSA, NDSA, SASA, and HDSA)
  - Shows that a particular product is compliant with the requirements of ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 (Technical Security Requirements for IACS Components)
- System Certifications
  - System Security Assurance (SSA)
  - Shows that a system (collection of components) is compliant with the requirements ISA/IEC 62443-4-1 and ISA/IEC 62443-3-3 (System Security Requirements and Security Levels)

Component Types

- ISA/IEC 62443-4-2 defines 4 types of components
  - **Embedded Device** - special purpose device designed to directly monitor or control an industrial process
  - **Network Device** - device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process
  - **Host Device** - general purpose device running an operating system capable of hosting one or more software applications, data stores or functions from one or more suppliers
  - **Software Application** - one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

Component Certifications

- ISASecure defines 4 types of component certifications for compliance with ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2:
  - **Embedded Device Security Assurance (EDSA)** – certification of embedded devices
  - **Network Device Security Assurance (NDSA)** – certification of network devices
  - **Host Device Security Assurance (HDSA)** – certification of host devices
  - **Software Application Security Assurance (SASA)** – certification of software applications

Agenda:
1. ISA/IEC 62443 Standards
2. ISASecure Certification

      Which standards apply

      Types of certifications

➡️ Types of components that can be certified

      Types of systems that can be certified

      Actual products and processes certified

3. Benefits of Certification

Types of Components that can be certified

- Types of Embedded Devices that can be certified
  - Programable Logic Solvers (PLCs)
  - Distributed Control Systems (DCSs)
  - Remote Terminal Units (RTUs)
  - Remote I/O
  - Smart Transmitters
  - Single Loop Controllers
  - Logic Solvers
  - Safety Related Programmable Electronic Systems
  - Controllers
  - Protection Relays
  - Motor Drives

Types of Components that can be certified

- More Types of Embedded Device that can be certified
  - Safety Control System
  - Sensors
  - Actuators
  - Robotics
  - IP Cameras
  - Building Control Systems
  - Sensors and Controllers used for mechanical rooms, HVAC zones and for chillers and boilers
  - Any device that directly monitors and/or controls an industrial process

  Note: Not a complete list

Types of Components that can be certified

- Types of Network Devices that can be certified
  - Gateways
  - Routers
  - Switches
  - Firewalls
  - Wireless Controllers
  - Security Appliances
  - Intrusion Prevention Systems
  - Data Diodes
  - Edge Nodes
  - And more (not a complete list)

Types of Components that can be certified

- Types of Host Device that can be certified – not complete list
    - Industrial Computing Platforms
    - Blade Servers
    - Embedded PCs
    - Ruggedized Computers
    - Rack-mounted Servers
    - Industrial Laptops
    - HMI Panels
    - Industrial Tablets
    - Terminals

    Note: Not a complete list

Types of Components that can be certified

- Types of Software Applications that can be certified
  - Data Historians
  - Human Machine Interfaces (HMI)
  - Operator Consoles
  - System Configuration Software
  - Batch Control Software
  - Intrusion Detection Systems
  - Asset Management Systems
  - Engineering and Design Tools

  Note: Not a complete list

Agenda:

1. ISA/IEC 62443 Standards

2. ISASecure Certification

Which standards apply

Types of certifications

Types of components that can be certified

→ Types of systems that can be certified

Actual products and processes certified

3. Benefits of Certification

System Certification Examples

- An Industrial Control System (ICS) or SCADA system that is available from a single system supplier
- It may be comprised of hardware and software components from several manufacturers but must be integrated into a single system and supported, as a whole, by a single supplier
- Examples:
  - Control System Platform
  - SCADA System Platform
  - Packaged Control System
    - Boiler Control System
    - Burner Management System
    - Drilling Control System
    - Wellhhead Control System
    - Packaging Machines
    - Reactors
    - Distillation
  - Robotic Control System
  - Power Generation System
  - HMI/PLC Combination System
  - Distributed Control System (DCS)
  - Safety Instrumented System (SIS)

Agenda:
1. ISA/IEC 62443 Standards
2. ISASecure Certification

Which standards apply

Types of certifications

Types of components that can be certified

Types of systems that can be certified

➡ Actual products and processes certified

3. Benefits of Certification

SDLA Certifications

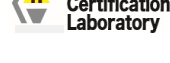| Company Logo	Company Name ▲	Certified Location	Supplier's SDL Methodology Name/Version	ISASecure SDLA Version/Level (click to see certificate)	Certification Date
EMERSON	Emerson Automation Solutions	Austin, TX, USA	DeltaV and DeltaV SIS Development Process	SDLA Version 1 Level 1	7/18/2018
EMERSON	Emerson Automation Solutions	Manila, Philippines	DeltaV and DeltaV SIS Development Process	SDLA Version 1 Level 1	7/18/2018
Honeywell	Honeywell Process Solutions	Phoenix, AZ, USA	Standard HPS Iterative Process (HIP)	SDLA Version 1 Level 1	11/15/2016
Schneider Electric	Schneider Electric	Foxboro, MA, USA	SDL	SDLA Version 1 Level 1	8/10/2015
Schneider Electric	Schneider Electric	Worthing, UK	SDL	SDLA Version 1 Level 1	8/10/2015
Schneider Electric	Schneider Electric	Hyderabad, India	SDL	SDLA Version 1 Level 1	8/10/2015
Schneider Electric	Schneider Electric	Lake Forest, CA	SDL	SDLA Version 1 Level 1	10/1/2016
Schneider Electric	Schneider Electric	Calgary, AB Canada	SDL	SDLA Version 1 Level 2	11/1/2016

Embedded Device Certifications

| Picture	Supplier	Type	Model	Version	Level	Certification Date
	Honeywell Process Solutions	Safety Manager	HPS 1009077 C001	R145.1	EDSA 2010.1 Level 1	6/6/2011
	RTP Corporation	Safety manager	RTP 3000	A4.36	EDSA 2010.1 Level 2	8/12/2011
	Honeywell Process Solutions	DCS Controller	Experion C300	R400	EDSA 2010.1 Level 1	8/21/2013
	Honeywell Process Solutions	Fieldbus Controller	Experion FIM	R400	EDSA 2010.1 Level 1	8/21/2013
	Yokogawa Electric Corporation	Safety Control System	ProSafe-RS	R3.02.10	EDSA 2010.1 Level 1	12/24/2013
	Yokogawa Electric Corporation	DCS Controller	CENTUM VP	R5.03.00	EDSA 2010.1 Level 1	7/14/2014
	Hitachi, Ltd.	DCS Controller	HISEC 04/R900E	01-08-A1	EDSA 2010.1 Level 1	7/14/2014
	Azbil Corporation	DCS Controller	Harmonas/Industrial-DEO/Harmonas-DEO system Process Controller DOPCIV (Redundant type)	R4.1	EDSA 2010.1 Level 1	12/17/2014
	Schneider Electric	Field Control Processor	Field Control Processor 280 (FCP280)	S91061	EDSA 2010.1 Level 1	12/23/2014
	Honeywell Process Solutions	DCS Controller	Experion C300	R410	EDSA 2010.1 Level 1	4/13/2015

Embedded Device Certifications

Picture	Supplier	Type	Model	Version	Level	Certification Date
	Yokogawa Electric Corporation	DCS Controller	CENTUM VP	R6.01.00	EDSA 2010.1 Level 1	8/7/2015
	Yokogawa Electric Corporation	Safety Control System	ProSafe-RS	R4.01.00	EDSA 2010.1 Level 1	7/26/2016
	Honeywell Process Solutions	DCS Controller	Experion C300	R430	EDSA 2010.1 Level 1	10/27/2016
	Schneider Electric	Field Device Controller	Field Device Controller FDC280	0900009000	EDSA 2.0.0 Level 1	11/1/2016
	TOSHIBA INFRASTRUCTURE SYSTEMS & SOLUTIONS CORPORATION	DCS Controller	CIEMAC-DS/nv (TOSDIC-CIE DS/nv) Unified Controller nv Series type2	FN812S:V01.01, PU821S:V01.CF, SA911:V01.34	EDSA 2010.1 Level 1	2/8/2017
	Schneider Electric	Safety Related Programmable Electronic System	TRICONEX Communication Module TCM	4351 A/B/AB & 4352 A/B/AB	EDSA 2010.1 Level 1	6/9/2017
	Honeywell Process Solutions	PLC	ControlEdge PLC	R140	EDSA 2.0.0 Level 2	7/3/2017
	HIMA Paul Hildebrandt GmbH	Safety Related Programmable Electronic System	HIMAX X	CPU 01 FW Version 8.8 & COM 01 FW Version 9.2	EDSA 2.0.0 Level 1	7/6/2017
	Beijing Consen Technologies	Safety Related Programmable Electronic System	TSxPlus V1.0	CM01-A-V001	EDSA 2.0.0 Level 1	7/7/2017
	Tri-Sen Systems Corporation	Safety Related Programmable Electronic System	TSxPlus V1.0	CM01-A-V001	EDSA 2.0.0 Level 1	10/20/2017

Embedded Device Certifications

Picture	Supplier	Type	Model	Version	Level	Certification Date	
	ABB	Controller	HPC800 Controller	HCA800B1	EDSA 2010.1 Level 1	1/22/2018	exida
	Schneider Electric	Safety Related Programmable Electronic System	TRICONEX Communication Module TCM	4355X, Firmware Revision Build 290 (TCM2) 288	EDSA 2.0.0 Level 1	1/31/2018	TÜVRheinland
	Honeywell Process Solutions	Remote Terminal Unit	ControlEdge RTU	R150	EDSA 2.0.0 Level 2	4/2/2018	exida
	Honeywell Process Solutions	Unit Operations Controller	ControlEdge UOC	R505.1	EDSA 2.0.0 Level 2	5/31/2018	exida
	Honeywell Process Solutions	Safety Manager	Safety Manager SC with FC-SCNT01 S300 Control Module	R200	EDSA 2.0.0 Level 2	8/21/2018	exida
	Honeywell Process Solutions	DCS Controller	Experion C300 with CF9	R500	EDSA 2.0.0 Level 1	8/23/2018	exida
	Schneider Electric	Safety Related Programmable Electronic System	TRICONEX Communication Module TCM	4355X, Firmware Revision Build 313 (TCM2TCOM2) 311	EDSA 2.0.0 Level 1	9/21/2018	TÜVRheinland
	Honeywell Process Solutions	DCS Controller	Experion C300 with CF9	R501	EDSA 2.0.0 Level 1	10/1/2018	exida
	Honeywell Process Solutions	DCS Controller	Experion C300 with CF9	R510	EDSA 2.0.0 Level 1	11/2/2018	exida
	Honeywell Process Solutions	Wireless Device Manager	WDMY	R320	EDSA 2.0.0 Level 1	11/2/2018	exida
	Schneider Electric	Safety Related Programmable Electronic System	TRICONEX Communication Module TCM	4351 A/AC/AC1, 4351 B/BC/BC1, 4352 A/AC/AC1, 4352 B/BC/BC1 - (Firmware Revision 6430 Build 344)	EDSA 2.0.0 Level 1	12/10/2018	exida

ISA Secure EDSA Certifications by Year
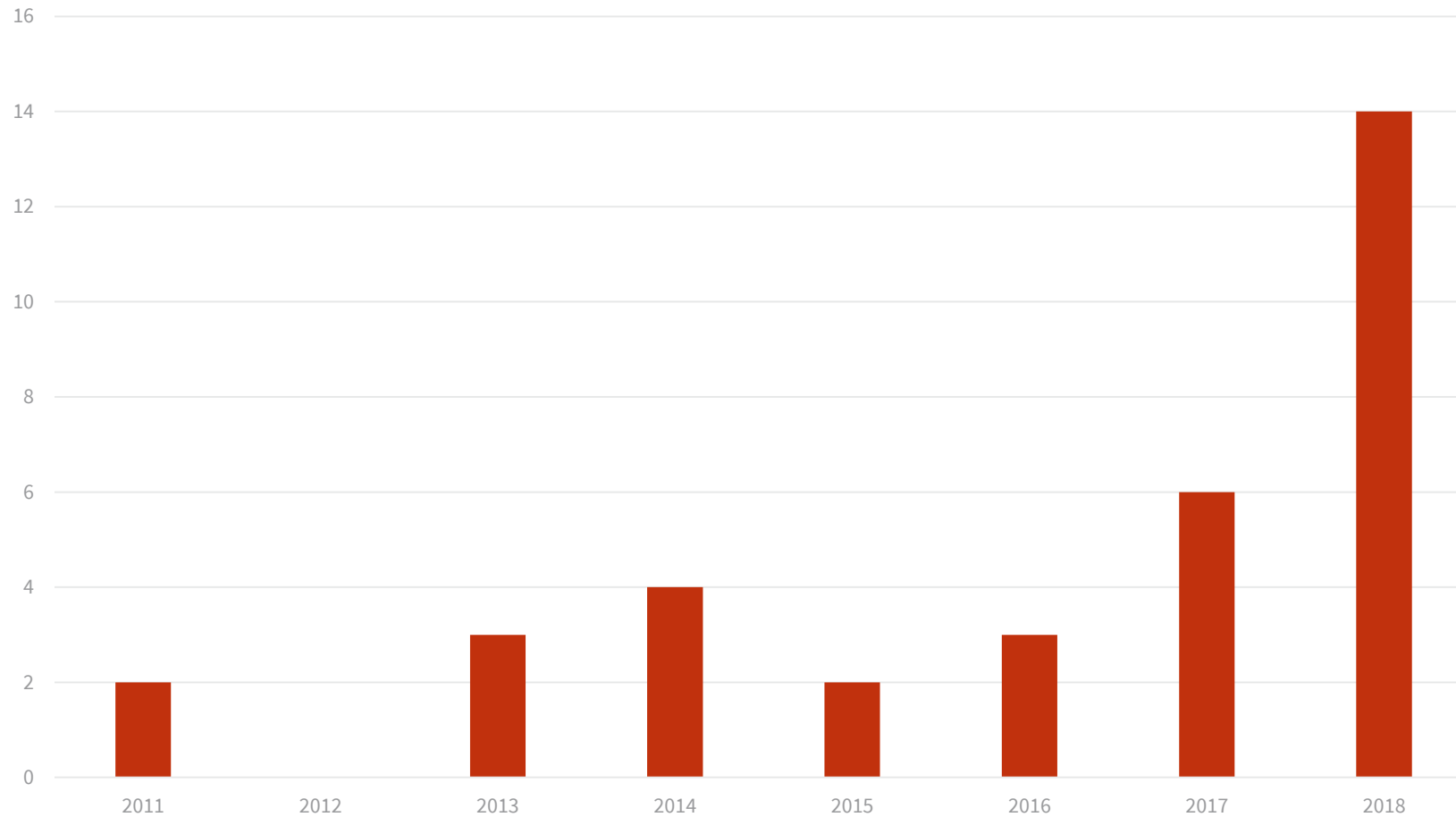
Agenda:
1. ISA/IEC 62443 Standards
2. ISASecure Certification

Which standards apply

Types of certifications

Types of components that can be certified

Types of systems that can be certified

Actual products and processes certified

➡ ## 3. Benefits of Certification

Benefits of IEC 62443 Cybersecurity Certification

Structured, auditable, repeatable approach to evaluating the security of an IACS product and the development practices of the manufacturer/integrator against an established benchmark.

End-user

- Easy to specify security needs – security level
- Build security requirement into RFP
- Reduced time in FAT/SAT
- Know security level out of the box
- Better cybersecurity strength
- Provides confidence from independent expert technical assessment

Supplier

- Evaluated once
  - Does not have to be re-evaluated by each customer
- Recognition for effort
- Build in security
- Product differentiator
- Reduce support costs
- Enhance credibility
- Break the pen/patch cycle
- Can be applied globally

Questions?