The bridge to possible

Securing Industrial Networks

A look at ISA/IEC 62443 and How Cisco Can Help Secure the Industrial Network

Flemming Andreasen, Distinguished Engineer
@FSAndreasen

BRKIOT-1527

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-1527

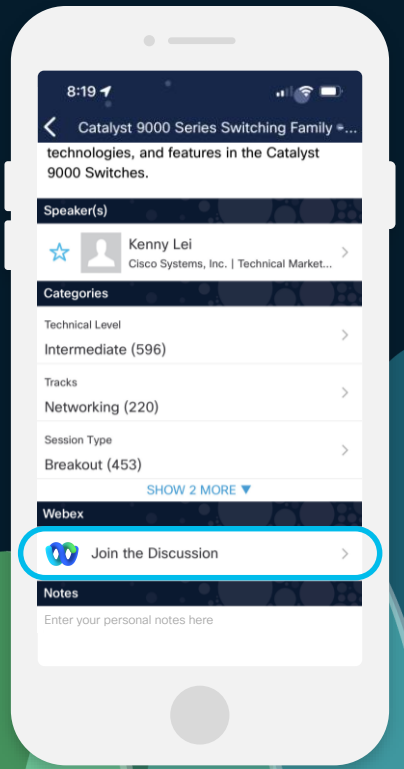
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.



Who Am I ?

Flemming Andreasen

- Cisco Distinguished Engineer
- Joined Cisco in 2000
- Worked in Voice over IP, Video and Mobility initially
- Spent the last 10+ years in Security and Industrial IoT
- Architecture, System Design, Protocols & Standards

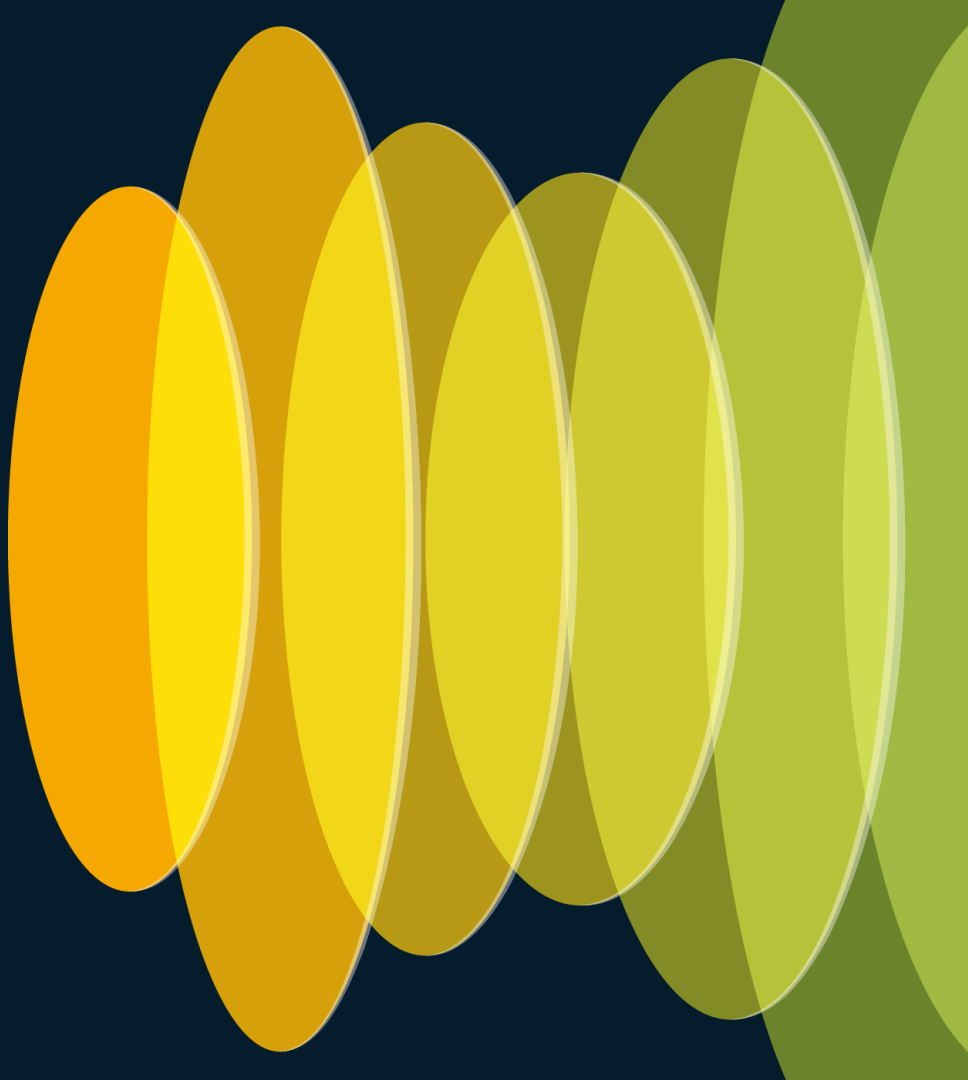
Goals of the Session

- Gain an understanding of the ISA/IEC 62443 set of standards for securing Industrial Networks and Critical Infrastructure, as follows
  - The overall Framework provided
  - The Key Concepts in the standards
- Understand how different Cisco technologies and products apply to ISA/IEC 62443 and can help secure your Industrial IoT Networks and Infrastructure

Agenda

- IEC-62443 Standards Overview
- IEC-62443 Key Concepts
- IEC-62443 and Cisco Security Technologies & Products
- Key Takeaways

IEC 62443 Standards Overview



cisco Live!

What is ISA/IEC 62443 ?

- A set of standards and technical reports addressing Security of Industrial Automation and Control Systems (IACS)
- ISA/IEC is developed by the ISA99 standards committee in conjunction with IEC Technical Committee 65, WG 10
  - International Society of Automation
  - International Electrotechnical Commission
- ISA/IEC 62443 (aka. IEC 62443) aim to
  - Improve the safety, integrity, availability and confidentiality of components or systems used for automation and control
  - Provide criteria for procuring, implementing and operating secure IACS

Where does ISA/IEC 62443 Apply ?

- Industrial Automation and Control Systems (IACS) whose compromise could result in
  - Endangerment of public or employee safety, or loss of public confidence
  - Violation of regulatory requirements
  - Economic loss, or loss of proprietary information
  - Impact on national security
- It is not limited to any specific industries or sectors – it applies to all types of plants, facilities and systems in all industries
  - For example, manufacturing, industrial process, building automation, transportation, etc.

Why is Cyber Security Important in IACS ?

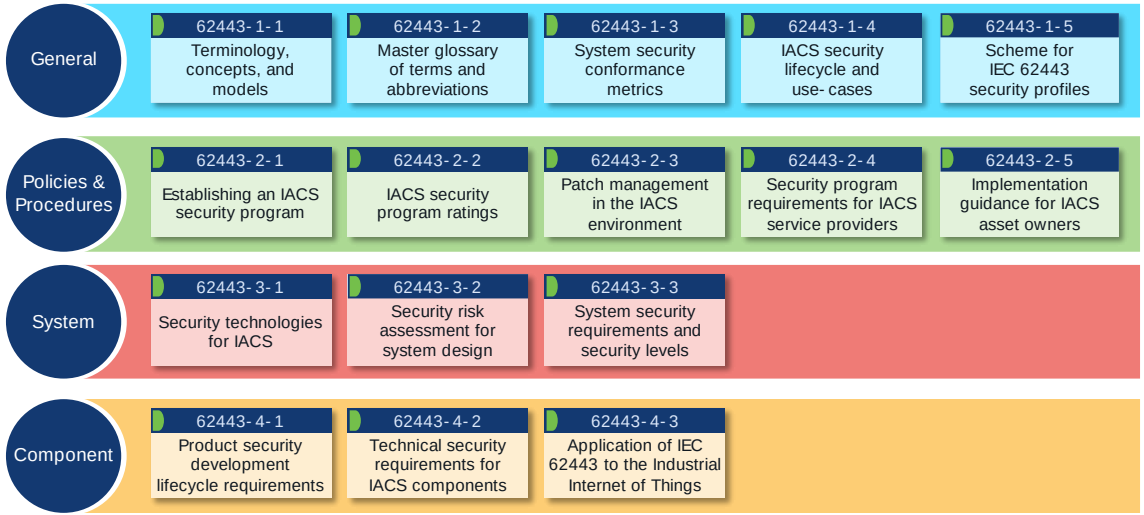
- Safety, Integrity and Reliability Concerns
  - Product integrity, loss of life, health, environmental damage, financial, etc.
- Regulatory requirements in some verticals
- Growing attack surface in Industrial IoT (IIoT) systems
  - Migration to commercial off-the-shelf technologies, e.g. Windows, Linux and TCP/IP
  - Increased connectivity of IACS assets, both internally and externally
  - Cloud and virtualization bring additional challenges
- Expanded means, resources, skills and motivation of cyber-attackers

Examples of Cyber Attacks in IACS

Year	Target	Method
2010	Iran Uranium Enrichment	Stuxnet
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2017	Global Shipping Company (Maersk)	NotPetya
2017	Health Care, Automotive & many others	WannaCry
2019	Norwegian Aluminum Company (Norsk Hydro)	LockerGaga
2020	Over 200 organizations around the world	Solarwinds breach
2022	Natural gas distributor (DESFA) - system outage	Ransomware
2023	Illinois Hospital – forced to close	Ransomware

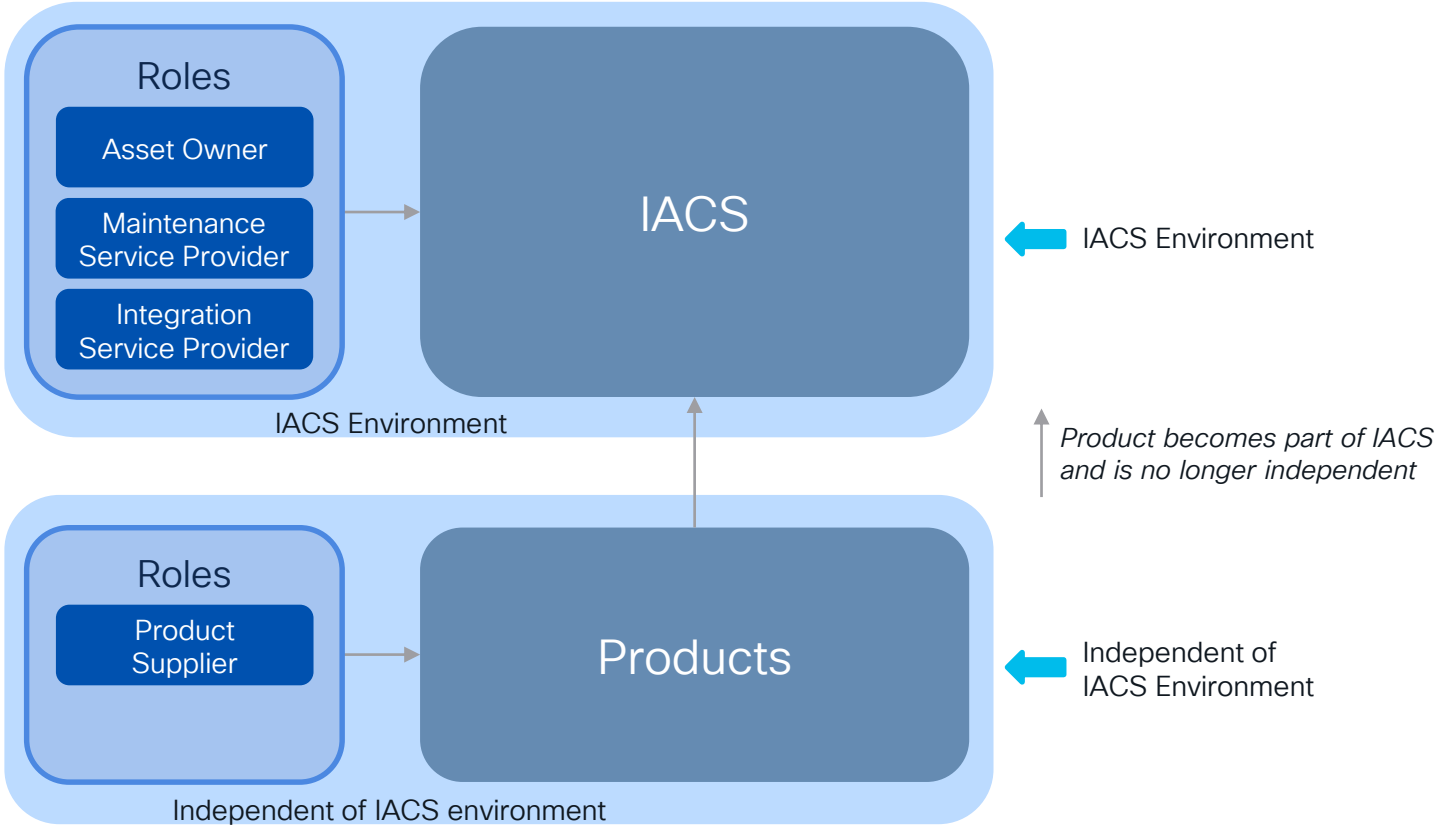
Source: ISA/IEC 62443 Quick Start Guide & https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

The ISA/IEC 62443 Family of Standards

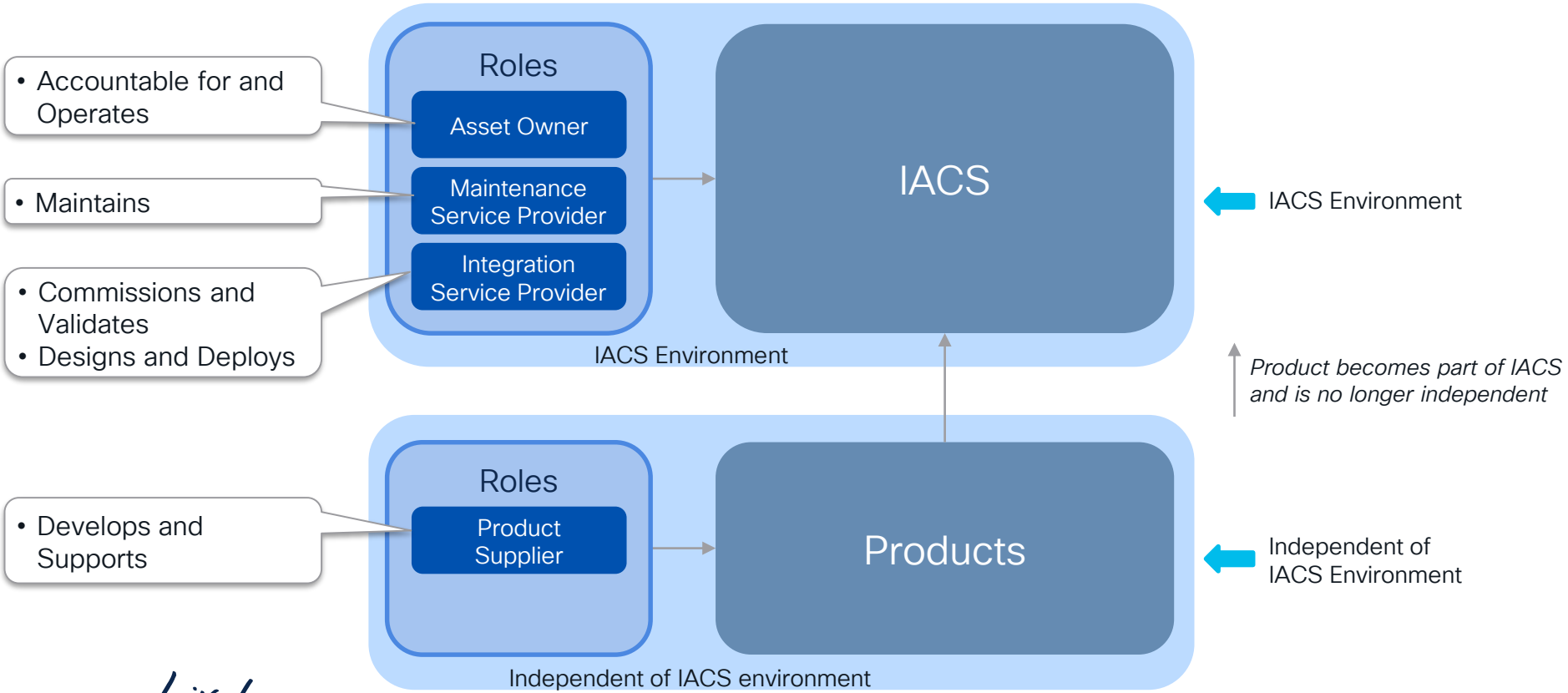


Principal Roles – High Level

Principal Roles – High Level

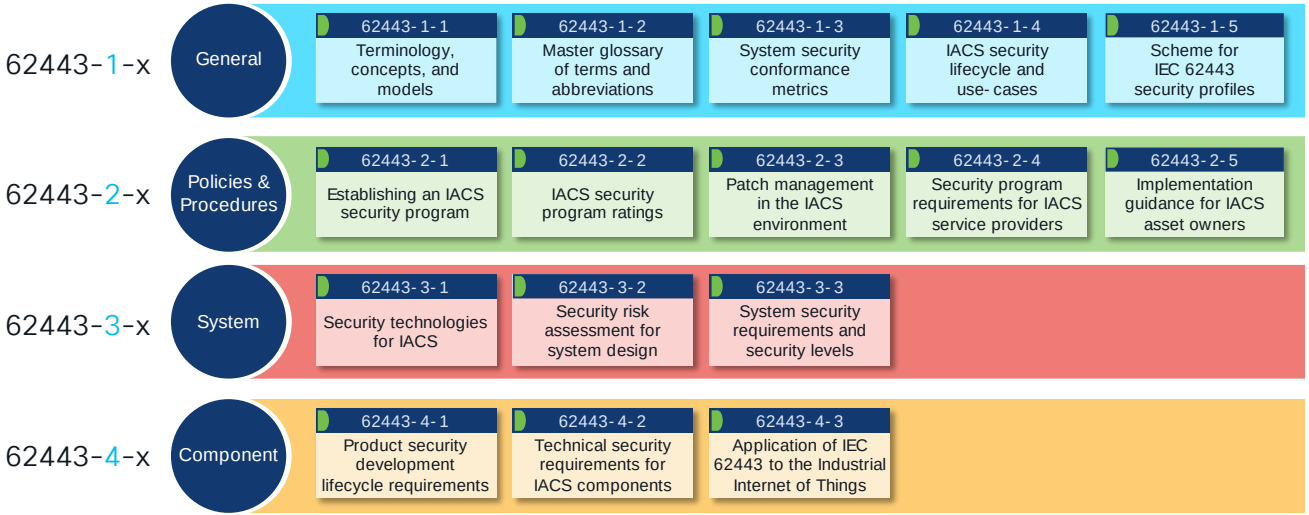


Principal Roles – High Level



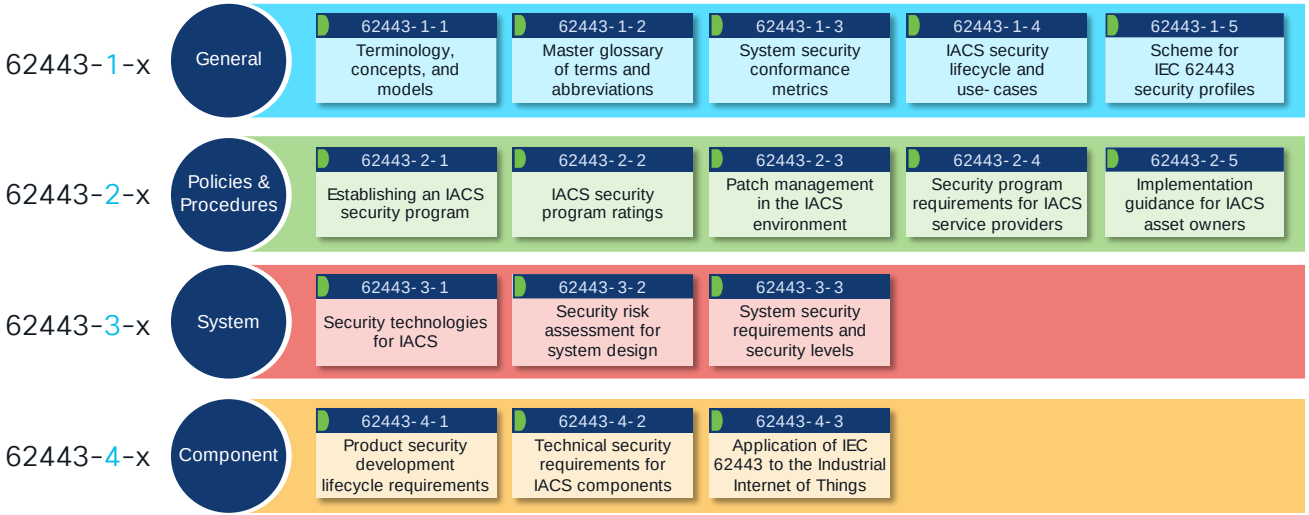
The ISA/IEC 62443 Family of Standards

4 different groups corresponding to the primary focus and intended audience



The ISA/IEC 62443 Family of Standards

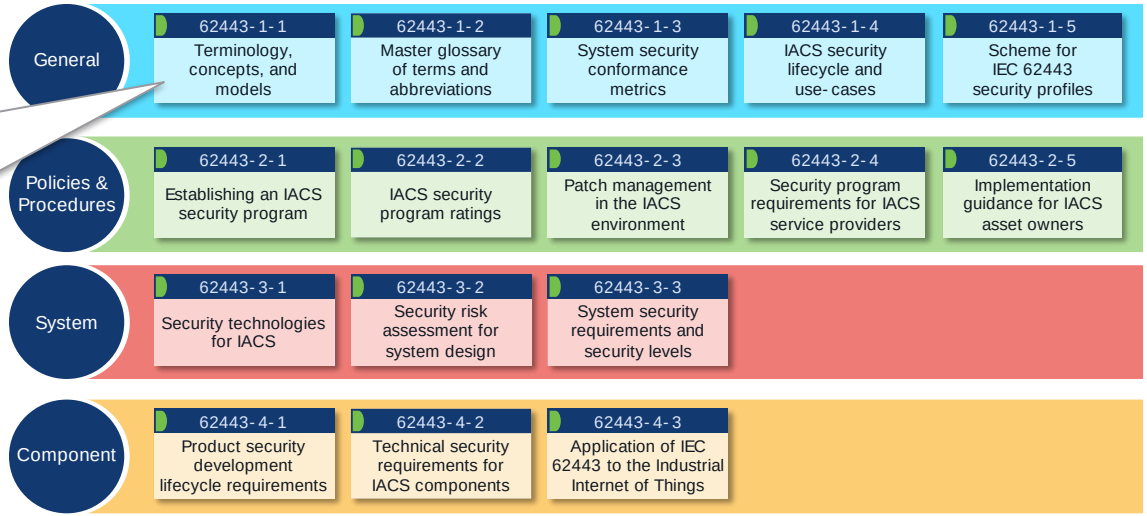
4 different groups corresponding to the primary focus and intended audience



The ISA/IEC 62443 Family of Standards

62443-1-1

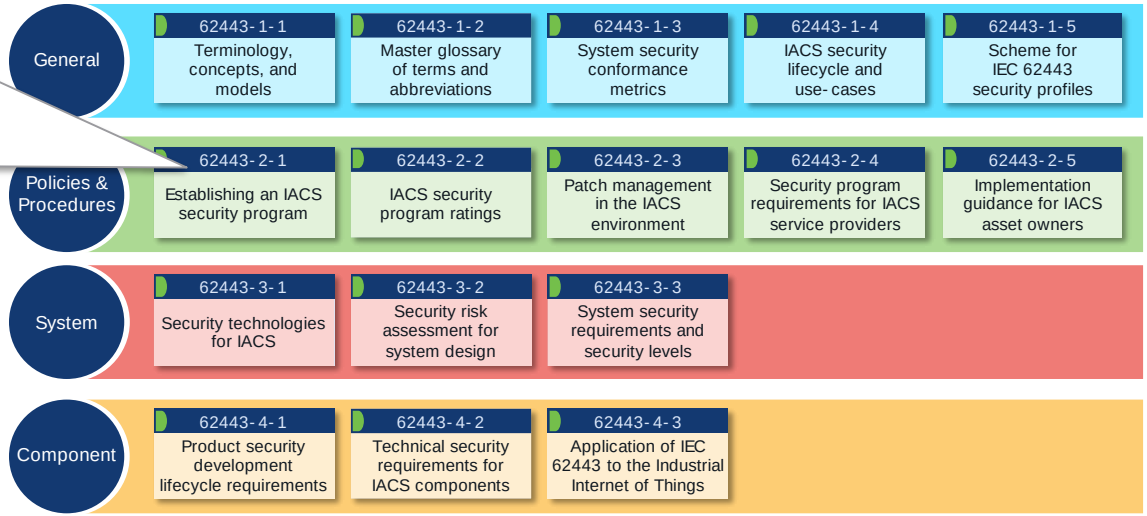
- Introduces the concepts and models used throughout the series, incl. seven Foundational Requirements (FR)
- Intended audience:
  - Anyone wishing to become familiar with the fundamental concepts that form the basis for the series



The ISA/IEC 62443 Family of Standards

62443-2-1

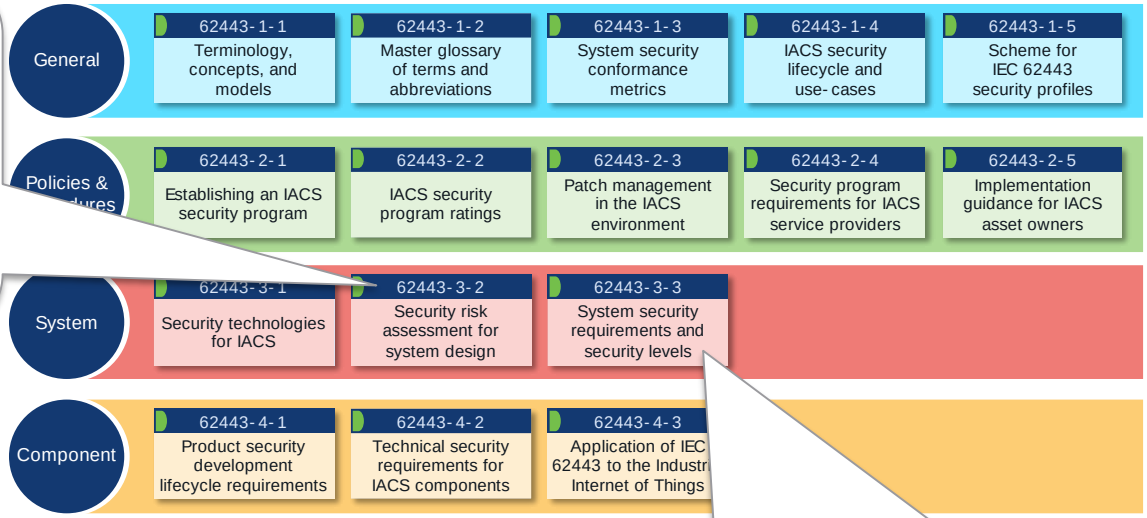
- Describes what is required to define and implement an effective IACS cyber security management system (CSMS)
  - Risk analysis, addressing risk, monitoring and improving CSMS, etc.
- Intended audience:
  - Asset Owners who have responsibility for the design and implementation of such a program



The ISA/IEC 62443 Family of Standards

62443-3-2

- Addresses cybersecurity risk assessment and system design for IACS. The outputs of this process are a Zone and Conduit model, associated Risk Assessments and Target Security Levels
- Intended audience:
  - Primarily Asset Owners and Integration Service Providers

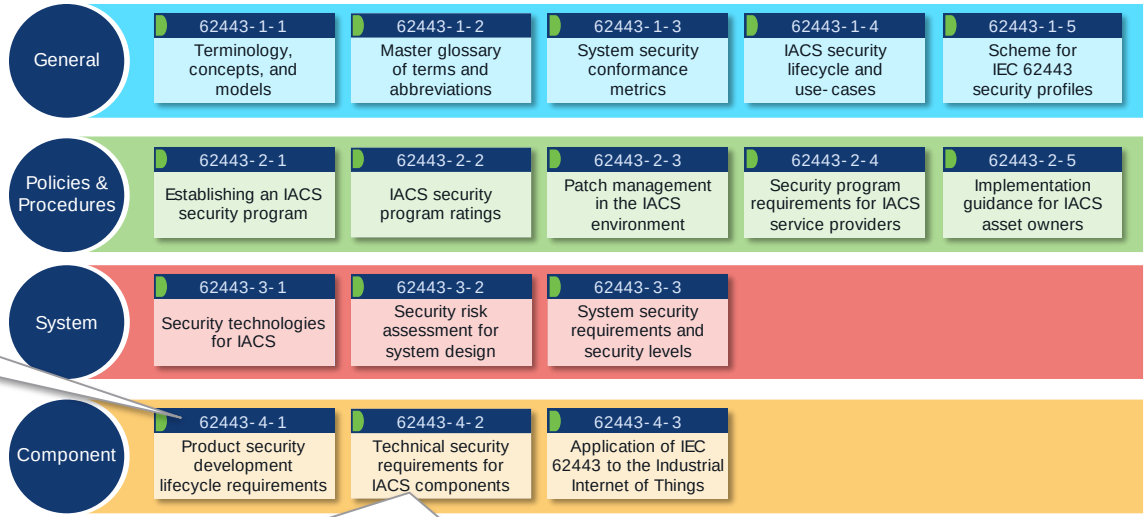


62443-3-3

- Describes the System Requirements (expanded FRs) for an IACS System based on 4 Security Levels
- Intended Audience:
  - Product Suppliers of IACS System products, Integration Service Providers and Asset Owners

The ISA/IEC 62443 Family of Standards

62443-4-1
- Describes the requirements for a Product Supplier's security development lifecycle
- Intended audience:
  - Suppliers of IACS System and IACS Component products

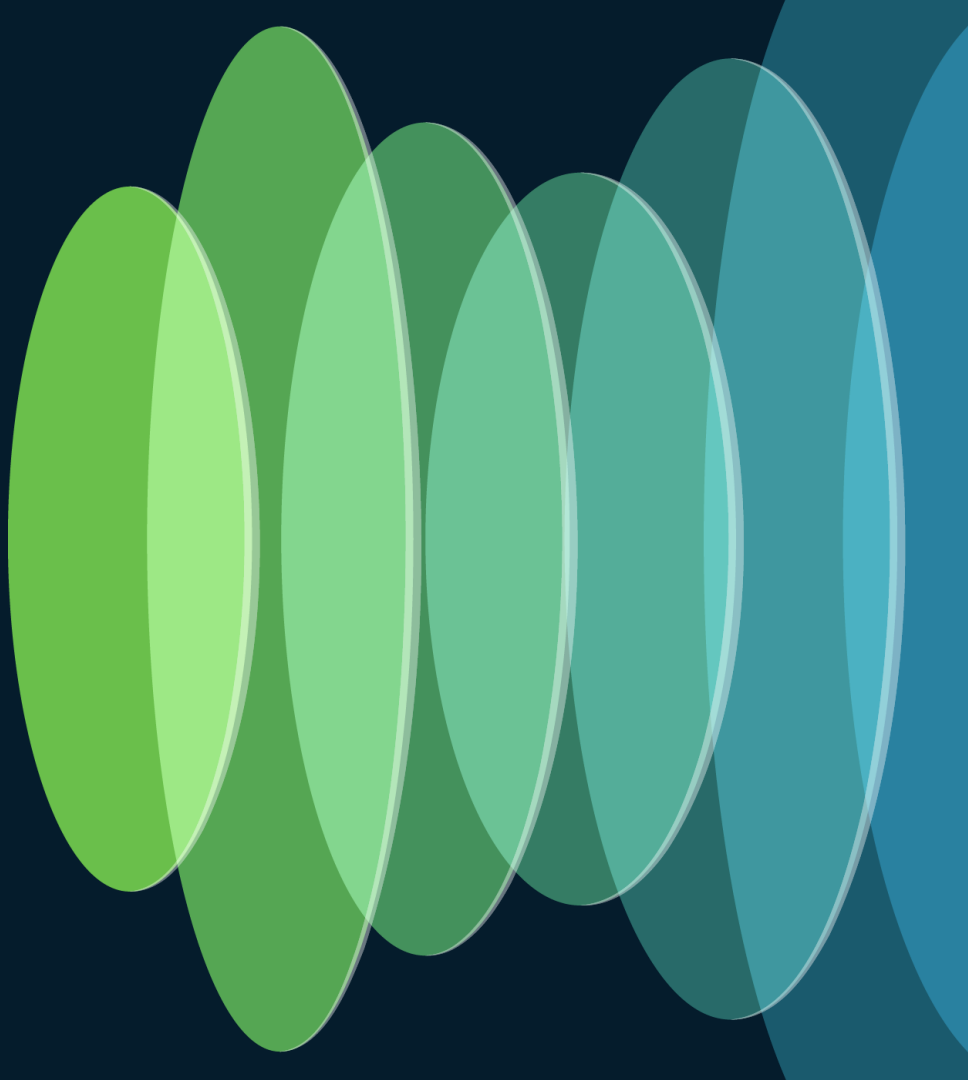


62443-4-2
- Describes the requirements for IACS Components based on Security Level. IACS Components include embedded devices, host devices, network devices and software applications
- Intended audience:
  - Product Suppliers of IACS Component products

Section Recap

- Cyber Security is important in Industrial Automation and Control Systems (IACS)
  - Safety, Integrity, Reliability & Regulatory concerns
  - Many examples of high-profile and costly cyber attacks
- IEC 62443 addresses security of IACSs across many sectors
- IEC 62433 specifications are divided into 4 major groups covering
  - Functional and Procedural requirements
  - Components, Systems and Organizations
- Each specification caters to one or more principal roles
  - Asset Owner, Integration Service Provider, Maintenance Service Provider
  - Product Supplier

IEC 62443
Key Concepts



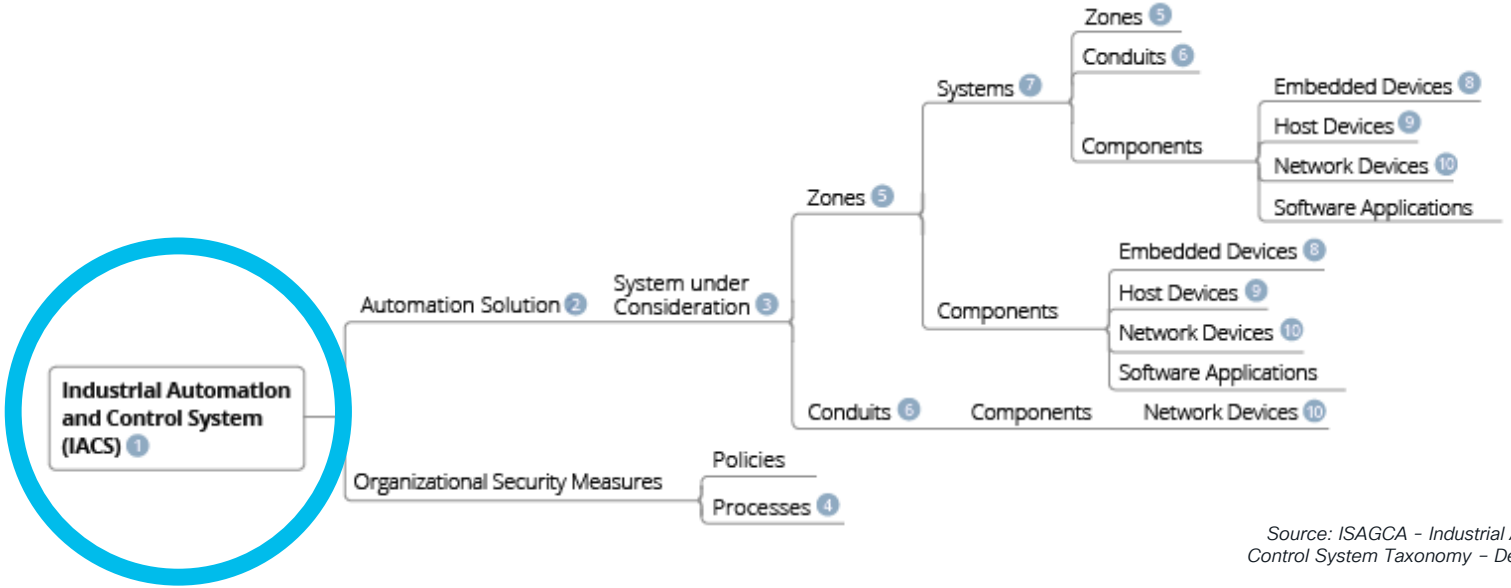
cisco Live!

Industrial Automation and Control Systems (IACS)

- “Collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation”

Industrial Automation and Control Systems (IACS)

- "Collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation"



Source: ISAGCA – Industrial Automation and Control System Taxonomy – Definitions of Terms

Foundational Requirements

- Seven Foundational Requirements (FRs) provided in 62443-1-1 form the basis for the technical requirements
  1. Identification and Authentication Control (IAC)
  2. Use Control (UC)
  3. System Integrity (SI)
  4. Data Confidentiality (DC)
  5. Restricted Data Flow (RDF)
  6. Timely Response to Events (TRE)
  7. Resource Availability (RA)
- System Requirements (SR) for each FR are provided in 62443-3-3
  - Different versions of each SR based on 4 different Security Levels (SL)

Example Foundational Requirement

- FR 1 – Identification and Authentication Control (IAC) [ISA/IEC 62443-3-3]:
  - “Based on the target security level (SL-T) determined, and using the processes defined in ISA-62443-3-2, the IACS shall provide the necessary capabilities to reliably identify and authenticate all users (humans, software processes, and devices) attempting to access the ICS”

Example System Requirement

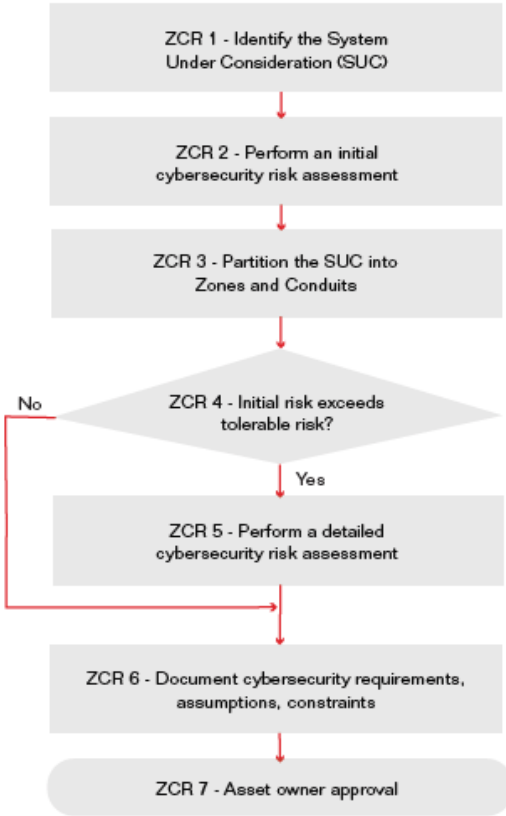
- SR 1-1 – Human User Identification and Authentication [ISA/IEC 62443-3-3]
  - **Requirement**
    - The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.
  - **Requirement Enhancements**
    - (1) Unique identification and authentication
      - The control system shall provide the capability to uniquely identify and authenticate all human users.
    - (2) Multifactor authentication for untrusted networks
      - The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).
    - (3) Multifactor authentication for all networks
      - The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.
  - **Security Levels**
    - SL-C(IAC, control system) 1: SR 1.1
    - SL-C(IAC, control system) 2: SR 1.1 (1)
    - SL-C(IAC, control system) 3: SR 1.1 (1) (2)
    - SL-C(IAC, control system) 4: SR 1.1 (1) (2) (3)

Example System Requirement

- SR 1-1 – Human User Identification and Authentication [ISA/IEC 62443-3-3]
  - Requirement
    - The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.
  - Requirement Enhancements
    - (1) Unique identification and authentication
      - The control system shall provide the capability to uniquely identify and authenticate all human users.
    - (2) Multifactor authentication for untrusted networks
      - The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).
    - (3) Multifactor authentication for all networks
      - The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.
  - Security Levels
    - SL-C(IAC, control system) 1: SR 1.1
    - SL-C(IAC, control system) 2: SR 1.1 (1)
    - SL-C(IAC, control system) 3: SR 1.1 (1) (2)
    - SL-C(IAC, control system) 4: SR 1.1 (1) (2) (3)

Risk Assessment for System Design

[62443-3-2]



Source: ISASecure: An Overview of ISASecure Certification

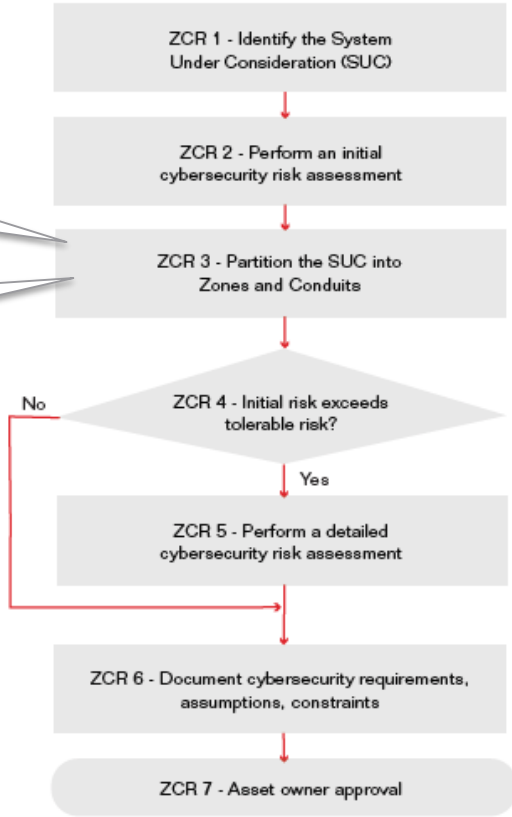
Risk Assessment for System Design [62443-3-2]

A key step is to partition the System under Consideration into Zones and Conduits

Intent is to identify assets with common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk

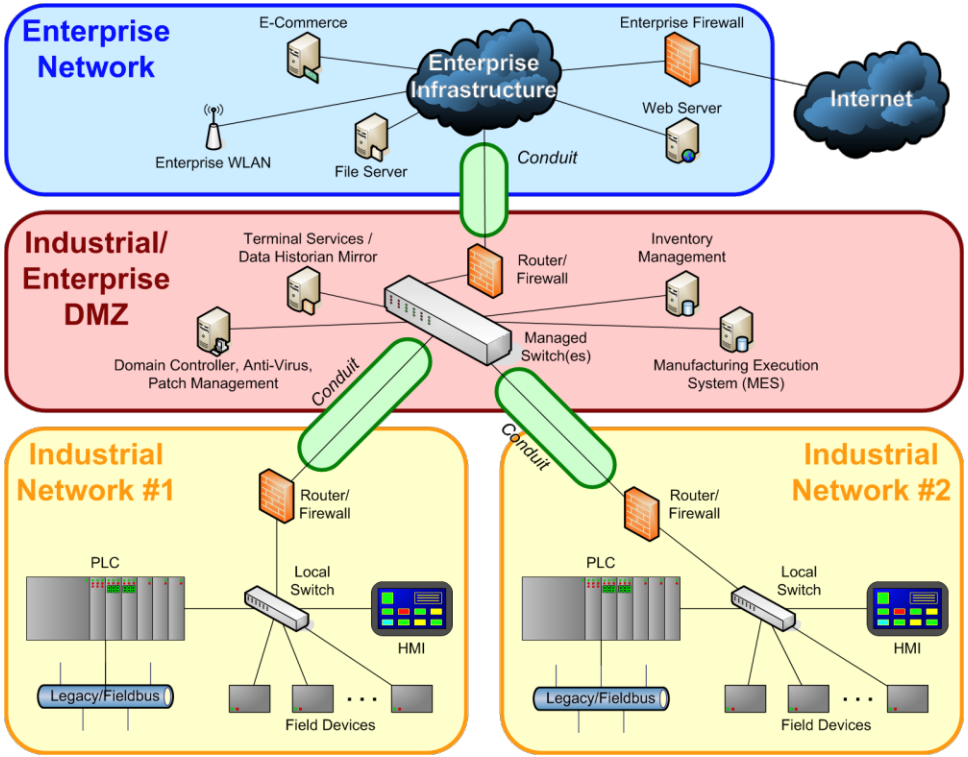
62443-3-2 defines various requirements for the partitioning, e.g.

- Group based on risk criteria
- Separate business and IACS assets
- Separate safety related assets
- Etc.



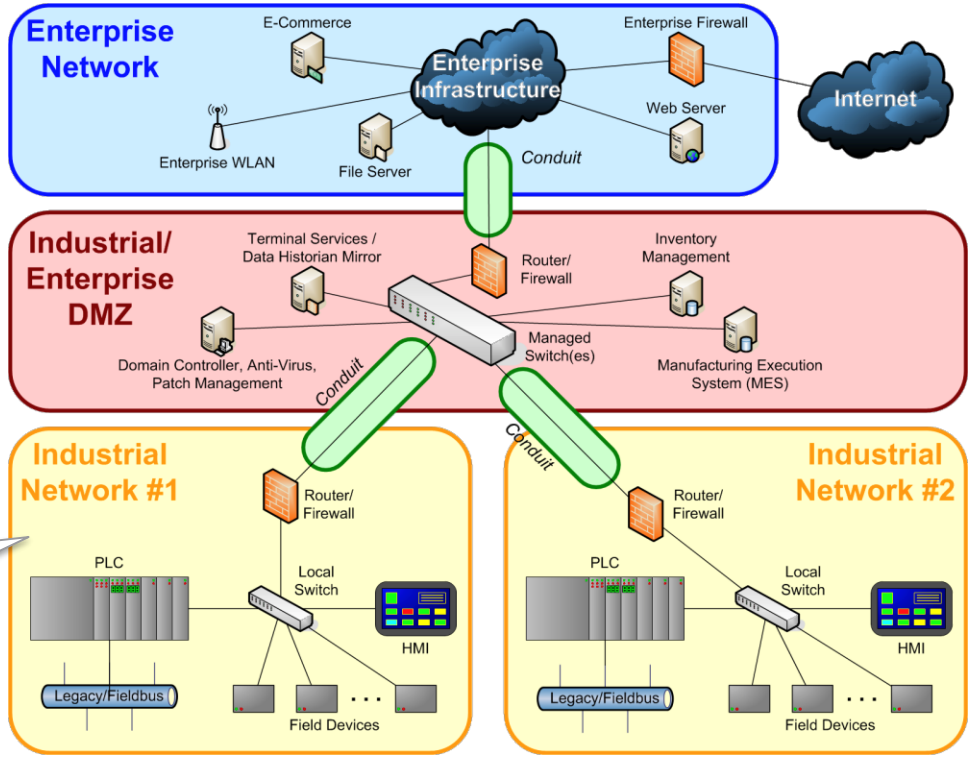
Source: ISASecure: An Overview of ISASecure Certification

Zones and Conduits



Source: IEC 62443-3-3

Zones and Conduits



Source: IEC 62443-3-3

Zone

- Collection of entities that represent a partitioning of a System under Consideration (SUC) based on their functional, logical and physical (including location) relationship that share common security requirements

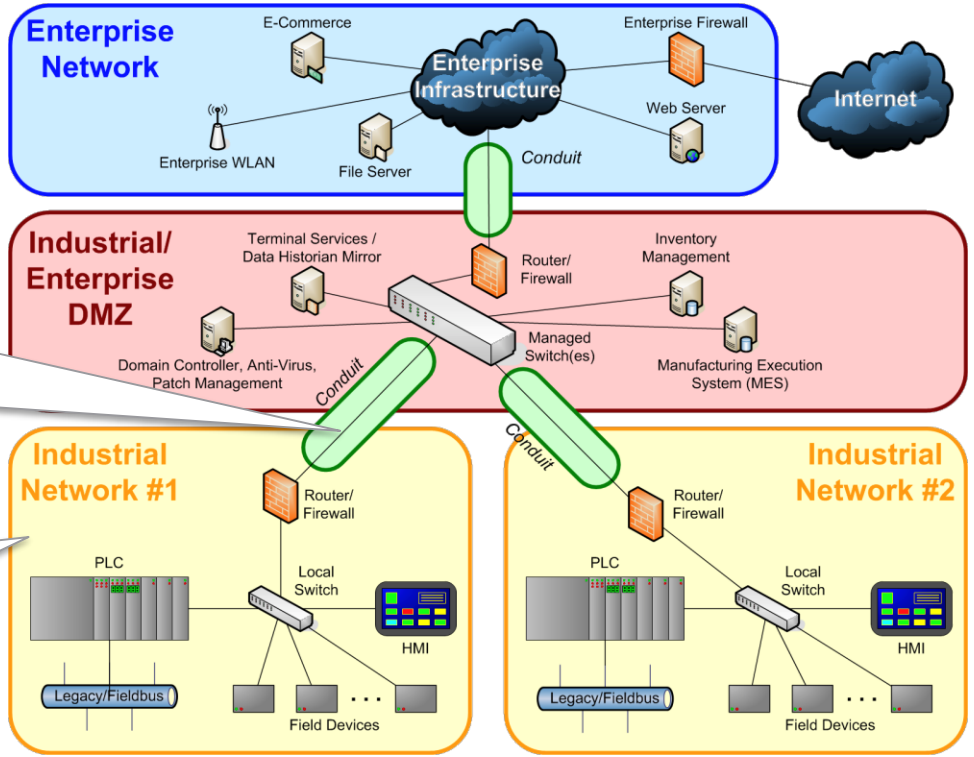
Zones and Conduits

Conduit

- Physical or logical grouping of communication channels, intermittent or permanent, between connecting a zone with another zone or with the outside that share common security requirements

Zone

- Collection of entities that represent a partitioning of a System under Consideration (SUC) based on their functional, logical and physical (including location) relationship that share common security requirements



Source: IEC 62443-3-3

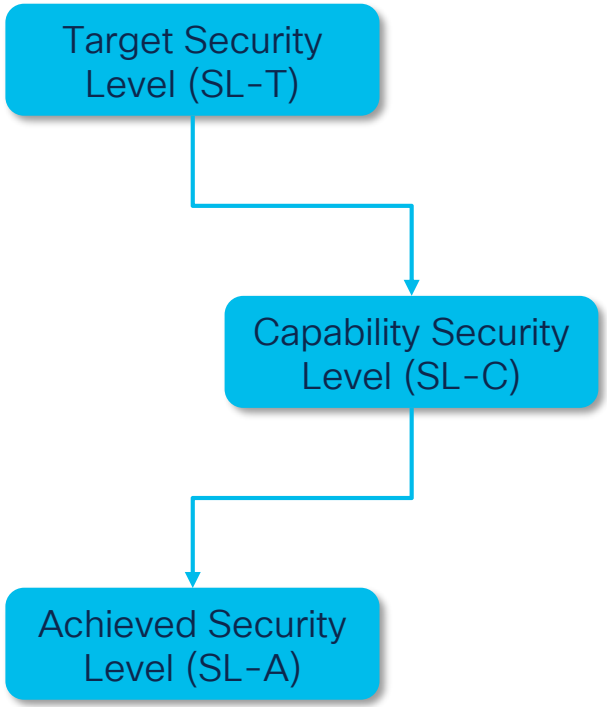
Security Levels

Higher Security Level => Protect Against More Capable Adversary

- Security Level: Measure of confidence that the System under Consideration (SuC), Zone or Conduit is free from vulnerabilities and functions in the intended manner
- ISA/IEC 62443-3-3 further defines the Security Level in terms of the Means, Resources, Skills and Motivation of the threat actor as follows:

Security Level	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation	Eavesdropping, no authentication, no access control, etc.			
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation	Simple	Low	Generic	Low
3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and moderate motivation	Sophisticated	Moderate	IACS-specific	Moderate
4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation	Sophisticated	Extended	IACS-specific	High

Three Types of Security Levels in ISA/IEC 62443



Three Types of Security Levels in ISA/IEC 62443

- Desired Level of security for Zones and Conduits in a given Automation Solution, as determined by the Risk Assessment process

Target Security Level (SL-T)

- Level of security that IACS Systems or Components can provide
- Native security level provided without additional compensating security measures (e.g. a Firewall)

Capability Security Level (SL-C)

- The actual levels of security for Zones and Conduits in a particular Automation Solution
- Includes operational and maintenance policies and processes

Achieved Security Level (SL-A)

Three Types of Security Levels in ISA/IEC 62443

- Desired Level of security for Zones and Conduits in a given Automation Solution, as determined by the Risk Assessment process

Target Security Level (SL-T)

- Level of security that IACS Systems or Components can provide
- Native security level provided without additional compensating security measures (e.g. a Firewall)

Capability Security Level (SL-C)

- The actual levels of security for Zones and Conduits in a particular Automation Solution
- Includes operational and maintenance policies and processes

Achieved Security Level (SL-A)

Goal: SL-A = SL-T

Three Types of Security Levels in ISA/IEC 62443

- Desired Level of security for Zones and Conduits in a given Automation Solution, as determined by the Risk Assessment process

Target Security Level (SL-T)

- Level of security that IACS Systems or Components can provide
- Native security level provided without additional compensating security measures (e.g. a Firewall)

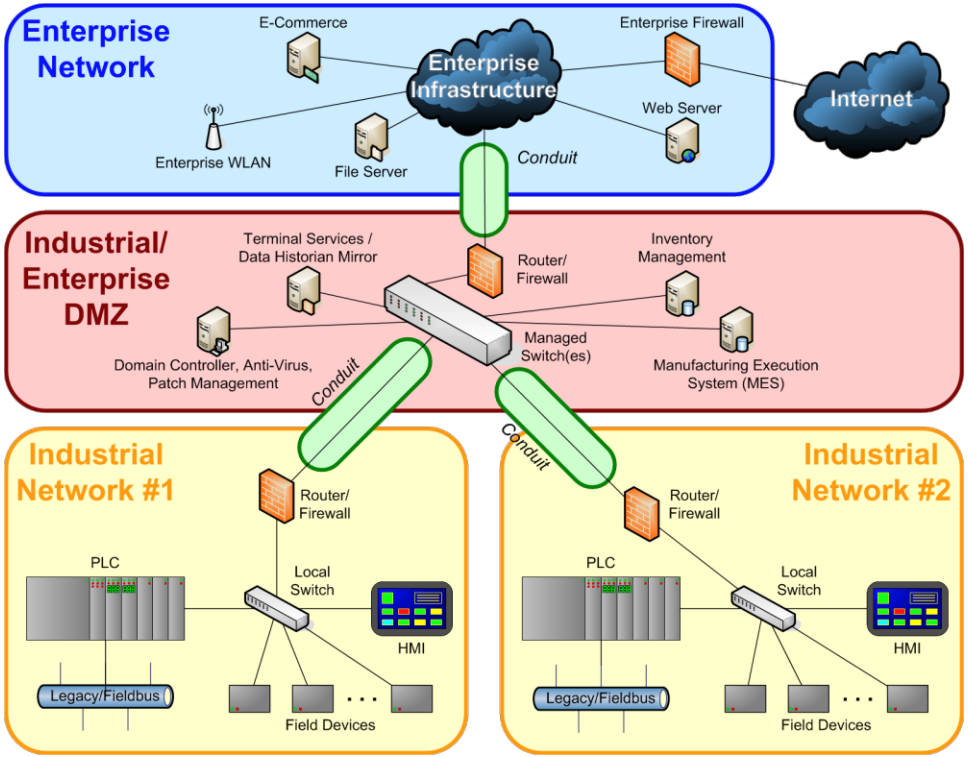
Capability Security Level (SL-C)

- The actual levels of security for Zones and Conduits in a particular Automation Solution
- Includes operational and maintenance policies and processes

Achieved Security Level (SL-A)

Goal:	SL-A = SL-T
Problem:	SL-C < SL-T

Zones and Conduits Revisited



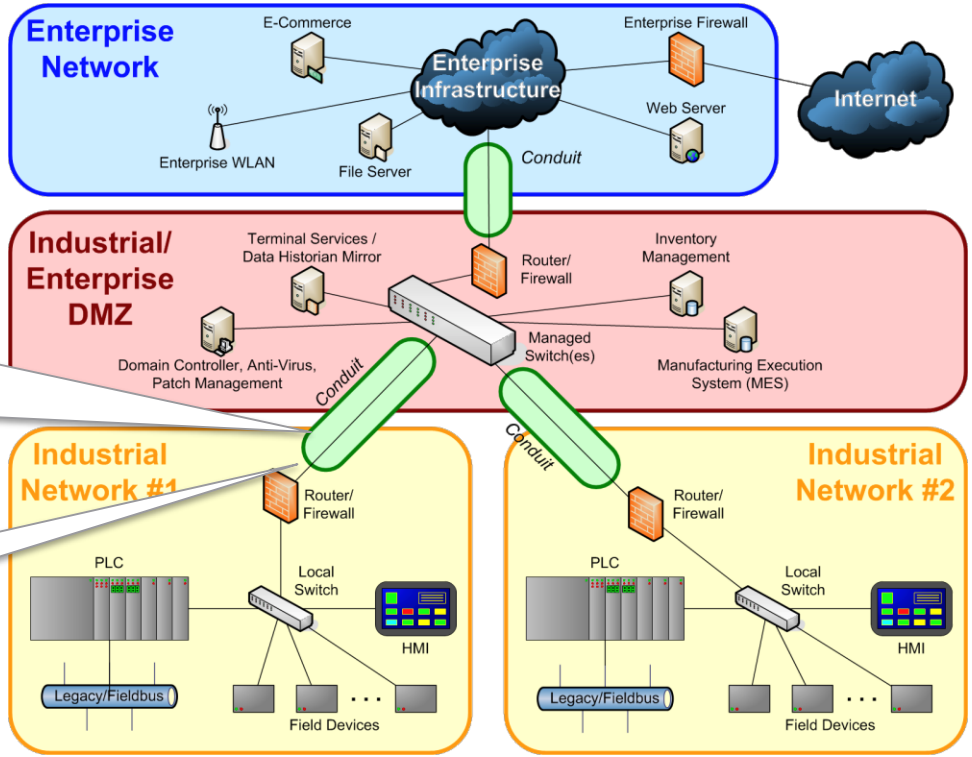
Source: IEC 62443-3-3

Zones and Conduits Revisited

The Conduit controls access to the Zone and may implement a variety of security features

- Segmentation, Proxying, Firewalling, Malware Detection, Intrusion Detection, etc.

When SL-C < SL-T for a given zone, the Conduit implements additional security features to support SL-A = SL-T



Source: IEC 62443-3-3

Maturity Levels

Higher Maturity Level => Higher Confidence in Security Level

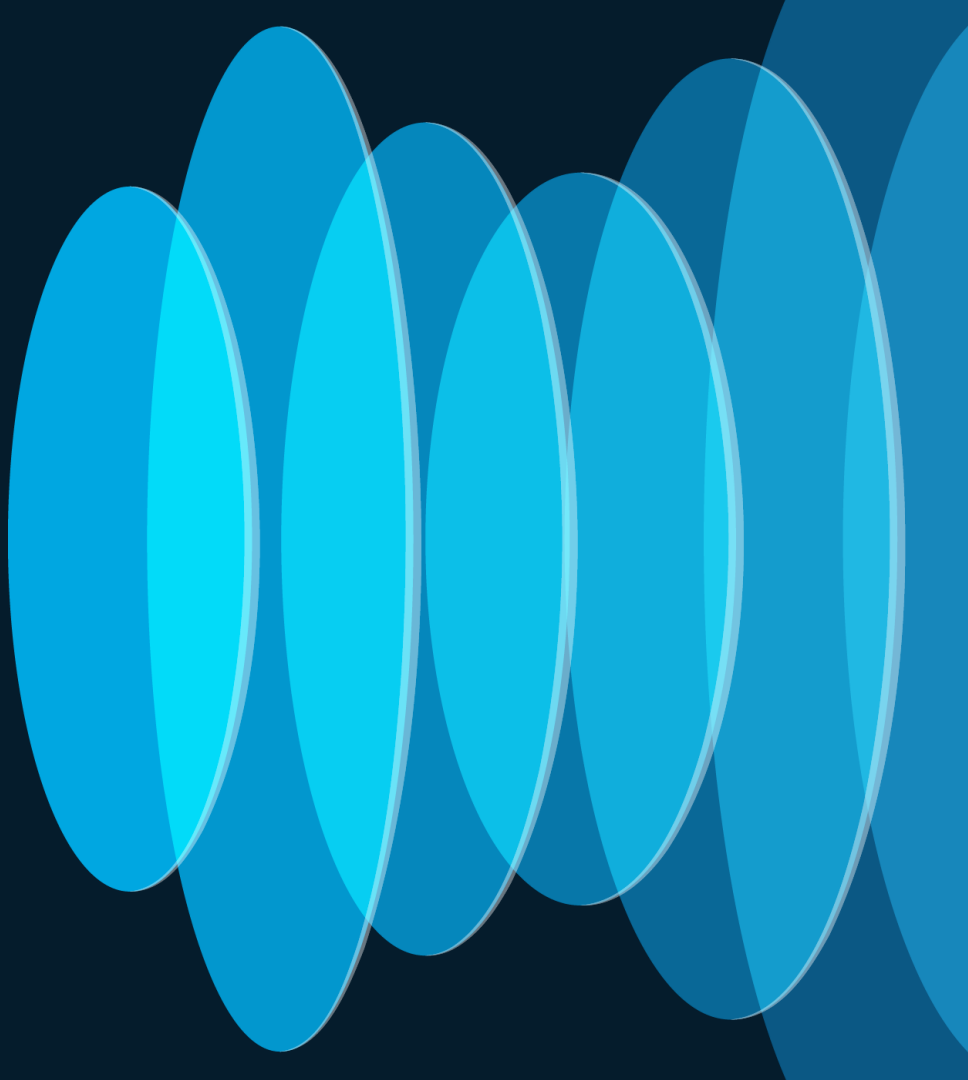
- A measure of processes (people, policies and procedures)
- Applies to organizations as well as suppliers
- ISA/IEC 62443-4-1 provides requirements to address a secure by design, defense in depth approach to designing, building, maintaining and retiring products used in IACS (like Cisco Secure Development Lifecycle – CSDL)
- Maturity Levels for Suppliers:
  - Provides more details on how thoroughly a supplier has met a requirement
  - System Integrators and Asset Owners can use them to assess the rigor used to develop products
  - Maturity Levels are based on the Capability Maturity Model Integration (CMMI) for Development (CMMI-DEV)

Level	CMMI	62443	Description
1	Initial	Initial	• Product development typically ad-hoc and often undocumented • Consistency and repeatability may not be possible
2	Managed	Managed	• Product development managed using written policies • Personnel have expertise and are trained to follow procedures • Processes are defined but some may not be in practice
3	Defined	Defined (Practiced)	• All processes are repeatable across the organization • All processes are in practice with documented evidence
4	Quanti-tatively Managed	Improving	• CMMI Levels 4 and 5 are combined • Process metrics are used to control effectiveness and performance • Continuous improvement
5	Optimi-zing		

Section Recap

- IEC 62443 Industrial Automation and Control Systems (IACS) cover personnel, hardware, software and policies
- 7 Foundational Requirements (FR) are defined
  - Each FR has more detailed System Requirements (SR)
  - Each SR has different versions based on 4 different Security Levels
- A key step in Risk Assessment is to partition the system into Zones and Conduits
  - Entities in a zone share common security requirements
  - Communication between entities in different zones is via a conduit
  - A conduit can implement a variety of security features
  - Conduits can help achieve a target security level (SL-T, SL-C, SL-A)
- 4 Maturity Levels are defined for organizations' and suppliers' processes

IEC 62443 and Cisco Security Technologies & Products



cisco Live!

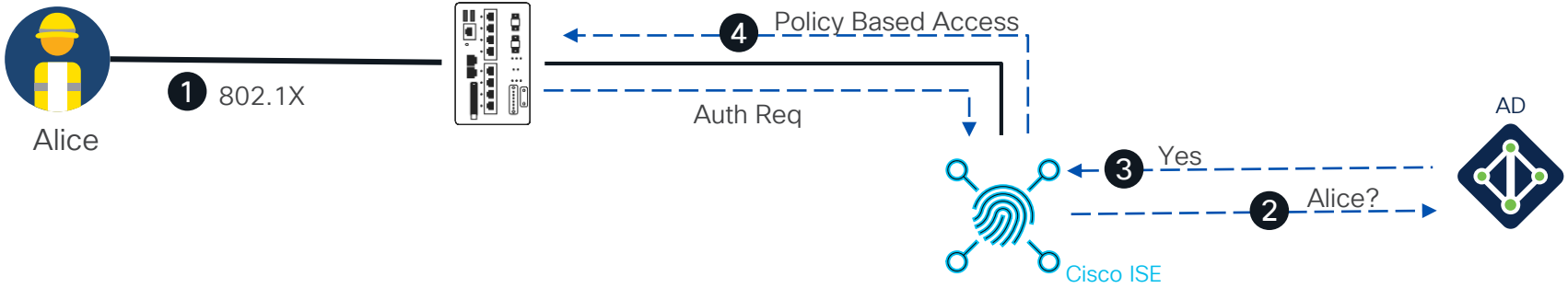
Cisco and IEC 62443

- Cisco is an active participant in ISA/IEC 62443
  - Technical contributor
  - Voting member in ISA99 and voting rights in IEC
- Cisco IoT is IEC 62443-4-1 certified
  - Cisco Secure Development Lifecycle (CSDL)
  - Certification requires not only initial secure development practices, but also ongoing security support for the supplier's products
- Cisco IoT has products that are 62443-4-2 certified
  - Catalyst IE3x00 / Stratix 5800
  - Catalyst IE9300 (expected in June 2024)

FR 1: Identification and Access Control (IAC)

Purpose	
Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system	
Use Cases based on System Requirements (SR)	**Technologies & Products**
Network Access Control for users and devices	• Cisco Identity Services Engine (ISE) • Cisco switches, access points and routers • Cisco Cyber Vision • Cisco Duo • Cisco Secure Firewall (VPN) • Cisco Secure Client (AnyConnect) • Cisco Secure Equipment Access (SEA)
Device Identification & Inventory	
Multi-Factor Authentication (MFA)	
Log failed OT device logins	
Remote network access	
Remote OT device access	

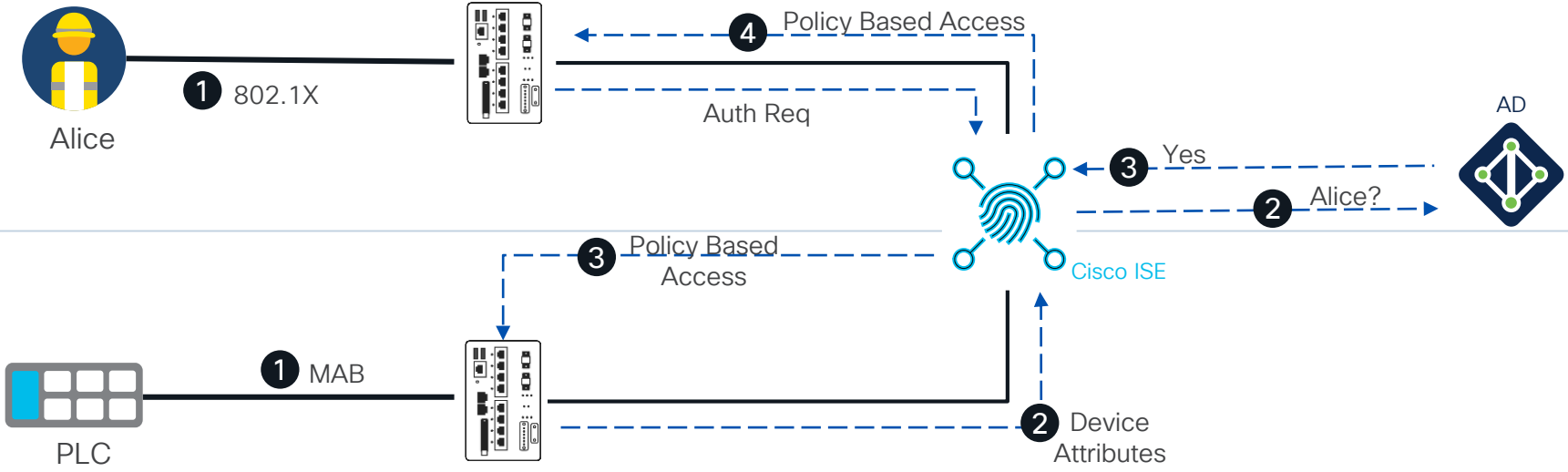
Authentication of users and devices with ISE



User Identity

IP to User mapping using active interaction between ISE and the client via **802.1X**, **Web authentication**, **Remote access VPN**, etc.

Authentication of users and devices with ISE



User Identity

IP to User mapping using active interaction between ISE and the client via **802.1X**, **Web authentication**, **Remote access VPN**, etc.

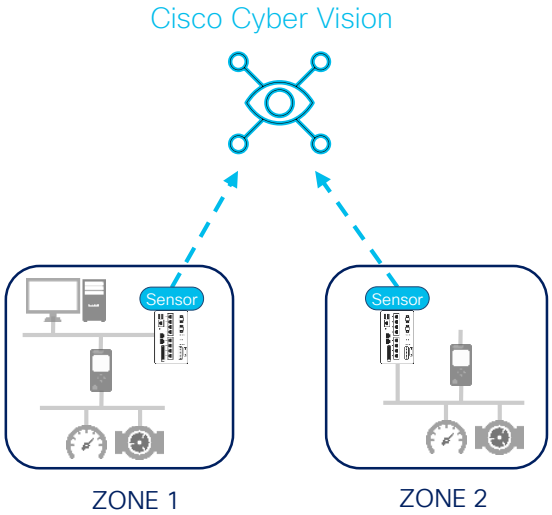
Device Identity

Devices authenticate to the network via **MAC Authentication Bypass (MAB)**, and policy is applied through host profiling.

FR 2: Use Control (UC)

Purpose	
Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the IACS and monitor the use of these privileges	
Use Cases based on System Requirements (SR)	**Technologies & Products**
Access Control Lists for wired and wireless devices	• Cisco ISE • Cisco switches, access points and routers • Cisco Secure Firewall • Cisco Cyber Vision • Cisco Secure Equipment Access (SEA) • Cisco Secure Network Analytics (SNA) • Cisco Duo
OT protocol granular access control (e.g. read/write)	
Log and monitor IACS use	
Restrict portable and mobile devices	
Session Termination	

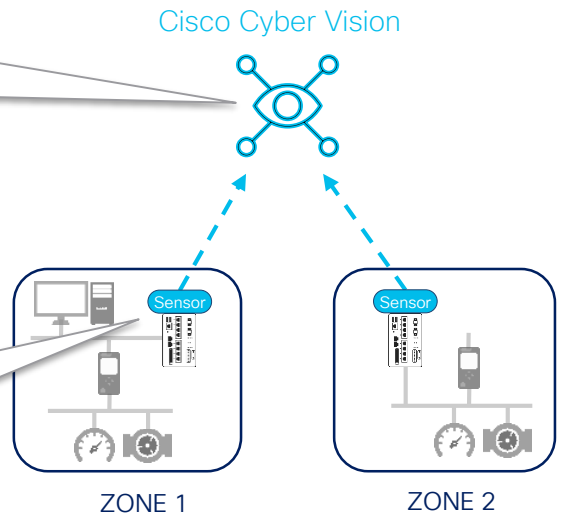
Log and Monitor IACS Use



Log and Monitor IACS Use

- Cyber Vision Center provides
  - Asset inventory, incl. vulnerabilities and risk scoring
  - IACS traffic insights (protocol level), communication patterns, anomaly detection, etc.

- Cyber Vision sensors in switches and routers
  - Discover assets and observe IACS traffic (protocol level) in each zone
  - Report discovered asset information and traffic metadata to Cyber Vision Center



FR 3: System Integrity (SI)

Purpose	
Ensure the integrity of the IACS to prevent unauthorized manipulation	
Use Cases based on System Requirements (SR)	**Technologies & Products**
General	• Hardware trust anchors, secure boot • MACsec, Secure tunnels (VPN, SD-WAN, etc.) with Cisco Secure Firewall, routers, switches and access points • Cisco Secure Firewall • Cisco Secure Endpoint (AMP) • Cisco Cyber Vision • Cisco Kenna • Cisco ISE • Cisco Duo • Cisco Secure Client
Communication integrity	
Malware protection	
Software Vulnerability Management	
Software change detection	
Endpoint posture	

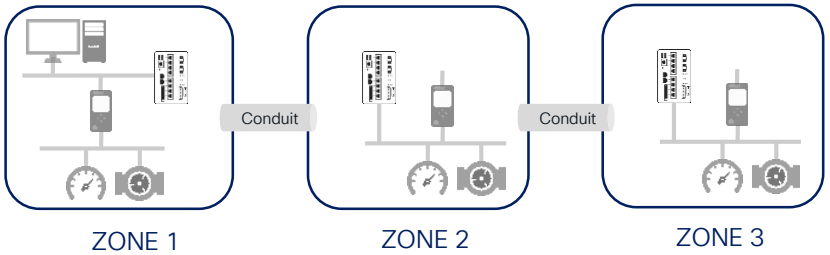
FR 4: Data Confidentiality (DC)

Purpose	
Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	
Use Cases based on System Requirements (SR)	**Technologies & Products**
Communication Confidentiality	• MACsec and Secure tunnels (VPN, SD-WAN, etc.) with Cisco Secure Firewall, routers, switches and access points • Cisco Secure Firewall • Cisco Secure E-mail • Cisco Secure Access (Security Service Edge/SSE)
Data Loss Prevention (DLP)	

FR 5: Restricted Data Flow (RDF)

Purpose	
Segment the control system via zones and conduits to limit the unnecessary flow of data	
Use Cases based on System Requirements (SR)	**Technologies & Products**
Zone Determination	• Cisco Cyber Vision • Cisco Secure Network Analytics • Cisco switches, access points and routers • Cisco Secure Firewall • Cisco ISE • Cisco TrustSec (Cisco ISE, Cisco Secure Firewall, Cisco switches, access points and routers)
Network Segmentation	
Group-Based Policies	
Conduit Monitoring	
Conduit Security	

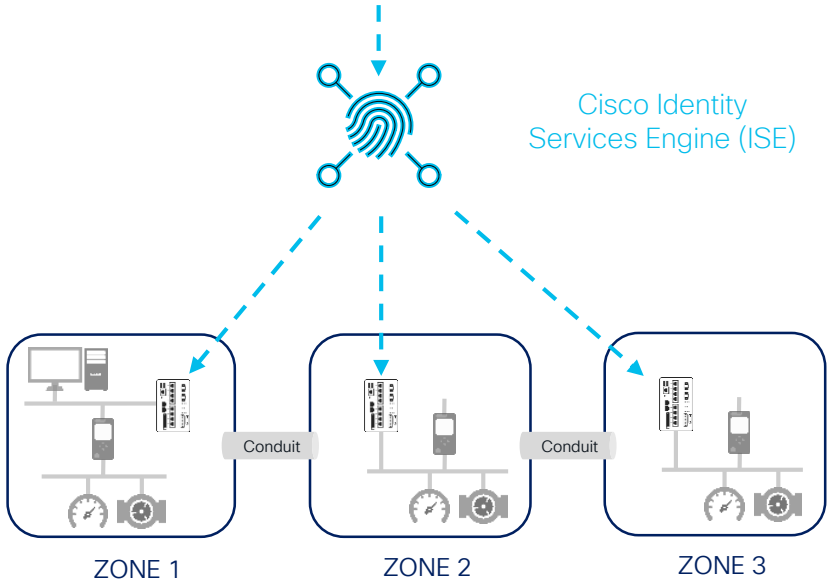
Network Segmentation



Network Segmentation

SGT-Based Access Control Policy

	Zone 1	Zone 2	Zone 3
Zone 1	Yes	Yes	No
Zone 2	Yes	Yes	Yes
Zone 3	No	Yes	Yes

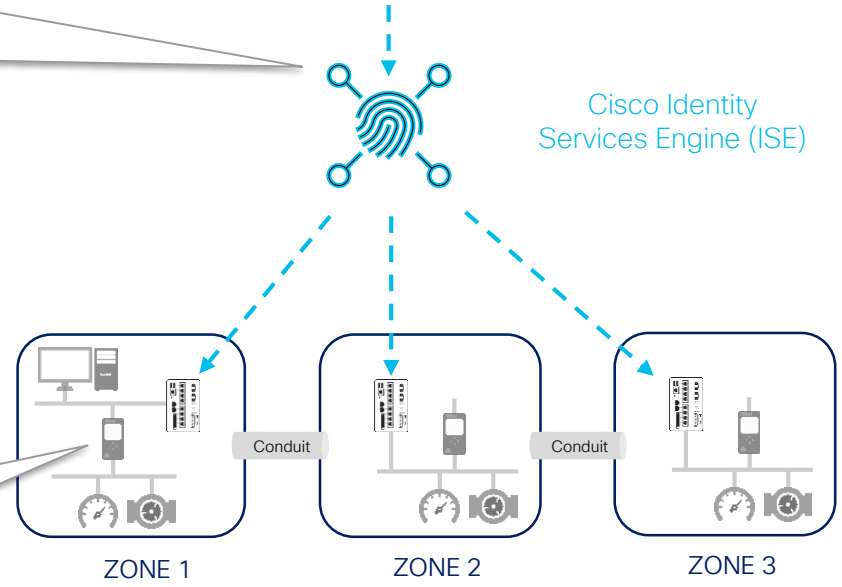


Network Segmentation

- Simple to use Matrix for access control based on Security Group Tags (SGT)
- ISE installs SGT-based access control policies in network
- Hybrid Macro and Micro-segmentation technology

SGT-Based Access Control Policy

	Zone 1	Zone 2	Zone 3
Zone 1	Yes	Yes	No
Zone 2	Yes	Yes	Yes
Zone 3	No	Yes	Yes



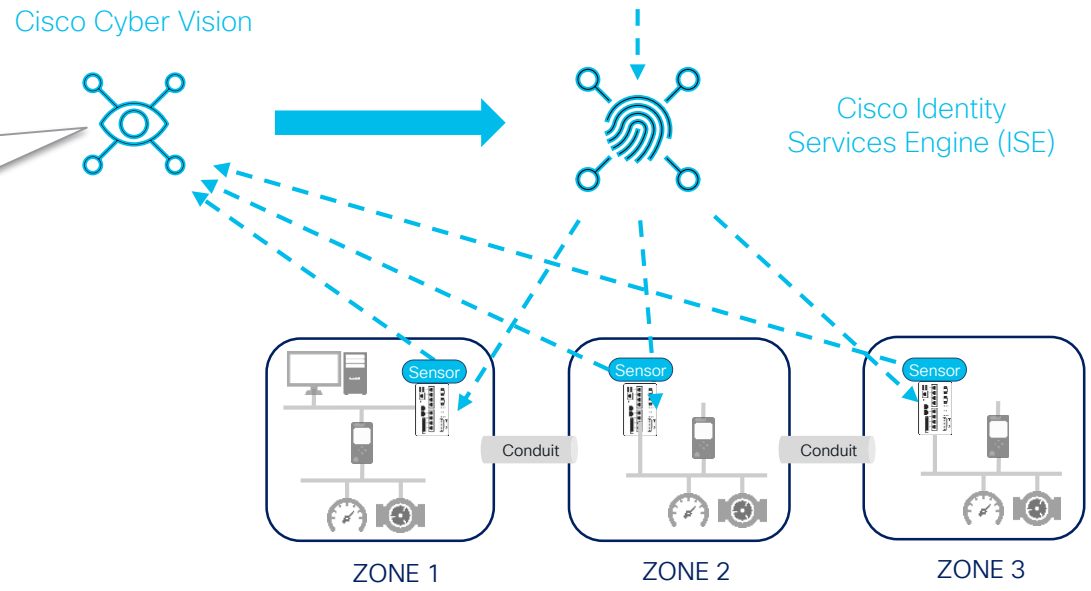
- Users and Devices are assigned a Security Group Tag (SGT) upon connecting to the network
- SGT-based access control enforced by the network

Network Segmentation & Zone Determination

SGT-Based Access Control Policy

	Zone 1	Zone 2	Zone 3
Zone 1	Yes	Yes	No
Zone 2	Yes	Yes	Yes
Zone 3	No	Yes	Yes

- Cyber Vision Center gets device inventory and communication patterns
- Add devices to ISE and assist with zone determination



Network Segmentation & Zone Determination

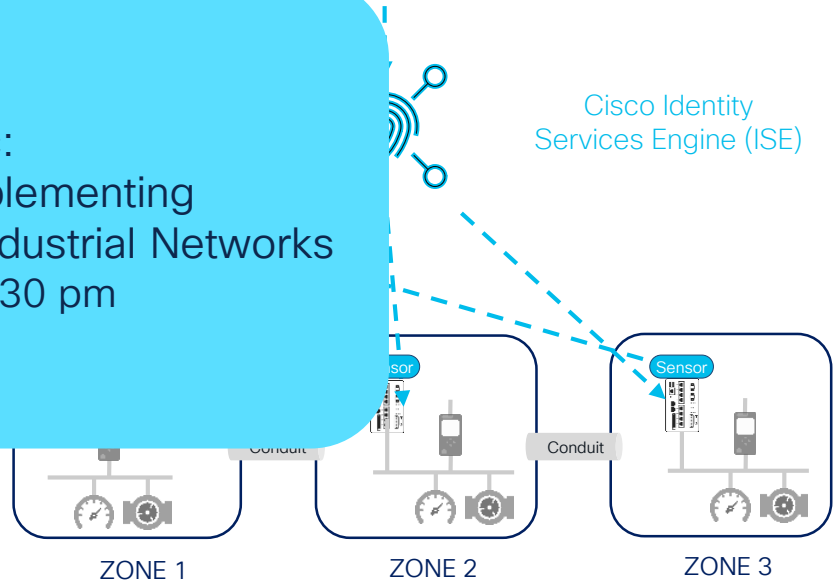
SGT-Based Access Control Policy

	Zone 1	Zone 2	Zone 3
Zone 1	Yes	Yes	No
Zone 2	Yes	Yes	Yes
Zone 3	No	Yes	Yes

- Cyber Vision Center gets devi
  inventory and communication
- Add devices to ISE and assist
  determination

For more on this topic:

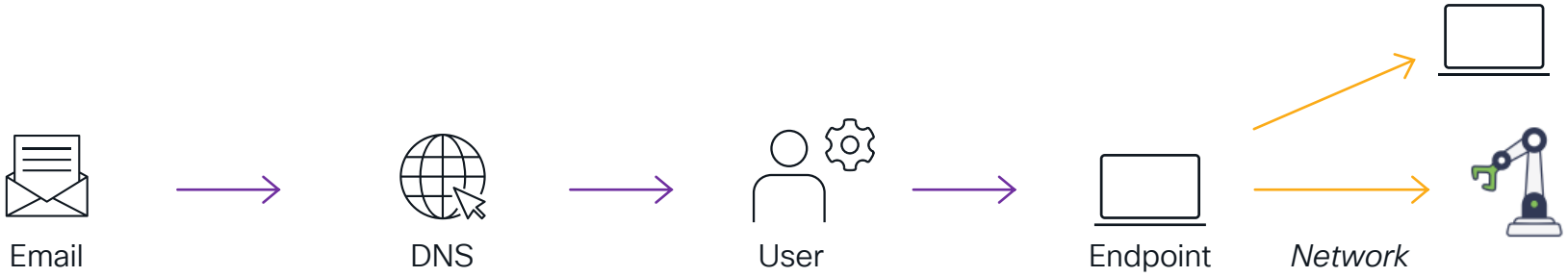
- BRKIOT-2882: Implementing Segmentation in Industrial Networks
  - Wed, June 5th, 2:30 pm



FR 6: Timely Response to Events (TRE)

Purpose	
Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered	
Use Cases based on System Requirements (SR)	**Technologies & Products**
Audit Logs	• Cisco Cyber Vision • Cisco ISE • Cisco Secure Network Analytics • Cisco Secure Firewall • Cisco switches, access points and routers • Cisco Duo • Cisco Secure Endpoint • Cisco Talos (threat intelligence) • Cisco XDR (eXtended Detection and Response)
Continuous Monitoring	

Many attacks use a sequence like this...



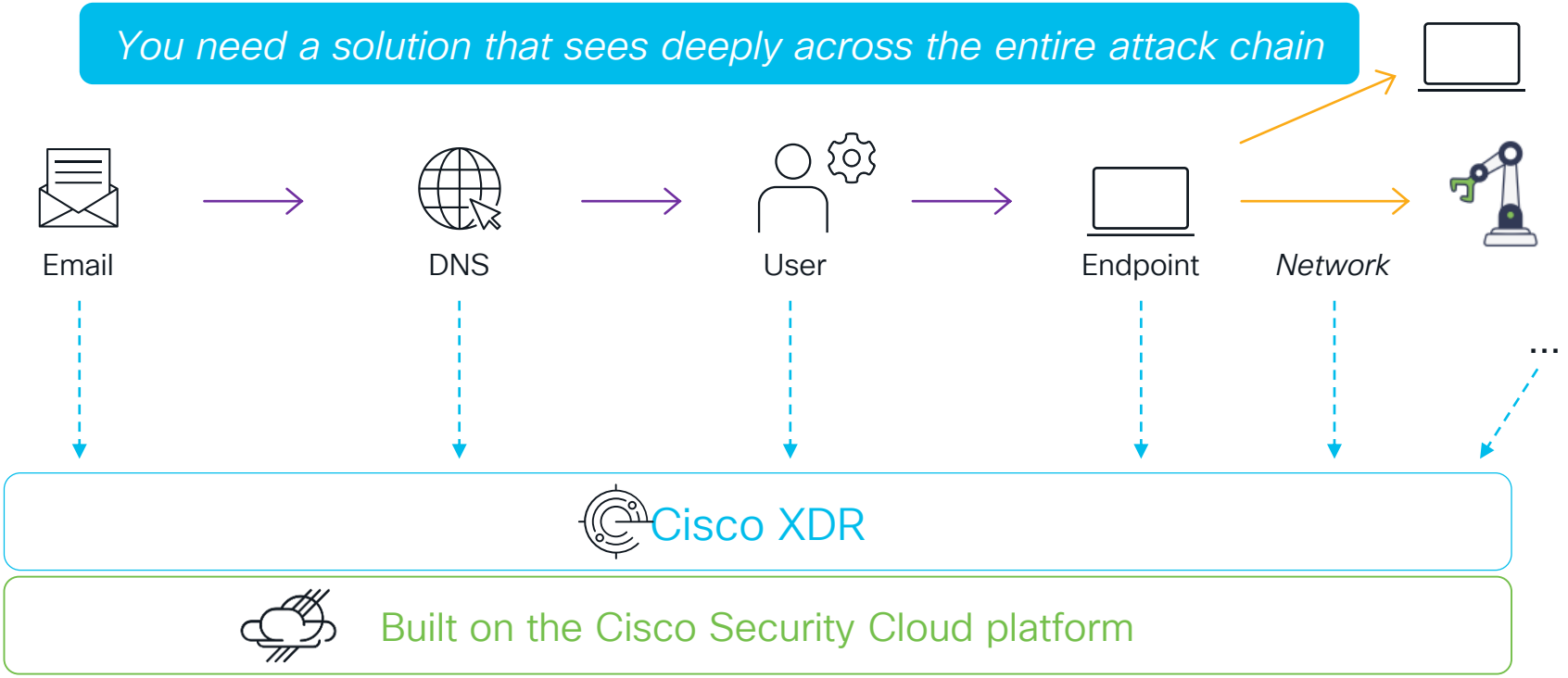
A well-tailored and personalized email causes a user to click...

Which goes to a questionable web site...

Which leads to a strange process being created locally on the user's device...

That process will connect to another machine or directly to their data

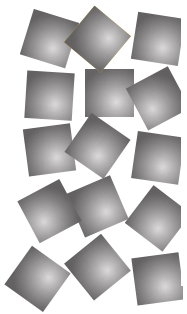
Most attacks use a sequence like this...



FR 7: Resource Availability (RA)

Purpose	
Ensure the availability of the control system against the degradation or denial of essential services	
Use Cases based on System Requirements (SR)	**Technologies & Products**
Denial of Service (DoS) Protection	• Cisco Secure Firewall • Cisco routers, switches and access points • Cisco Cyber Vision • Cisco ISE • Cisco Secure Firewall • Cisco DNA-C (network management) • Cisco Secure Network Analytics • Cisco XDR • See also FR 5 (“Restricted Data Flow”)
Configuration Management	
Restrict access to what is required	
Device Inventory (Control System Components)	

Quality of Service (QoS) as a Security Measure



IDENTIFY & PRIORITIZE

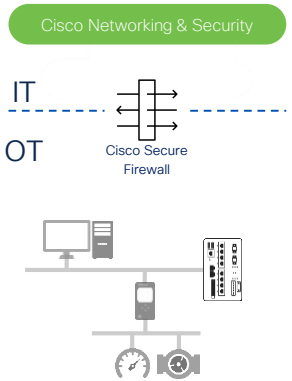
MANAGE & SORT

PROCESS & SEND

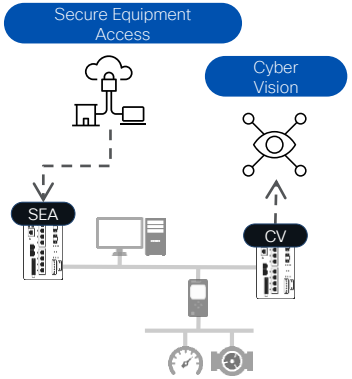
- QoS Integrated into switch configurations
- Rate limiting to protect assets
- Ensure critical operations are given priority
- DoS attack from non-critical network will NOT impact critical operations

Cisco Industrial Security Framework

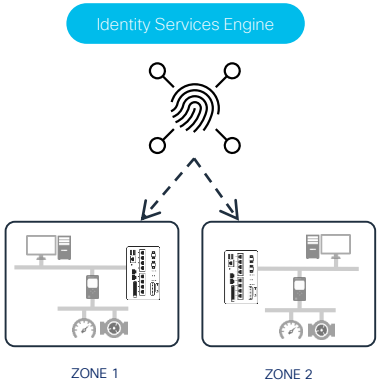
Build a Security Foundation



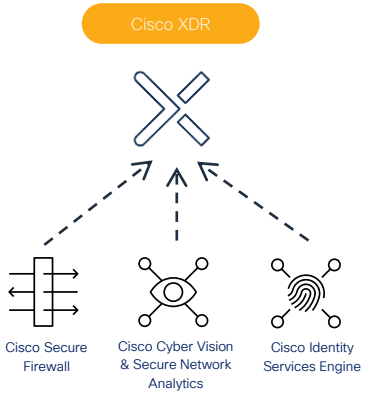
Security Posture & ZTNA of OT Assets



Segment Network into Smaller Trust Zones

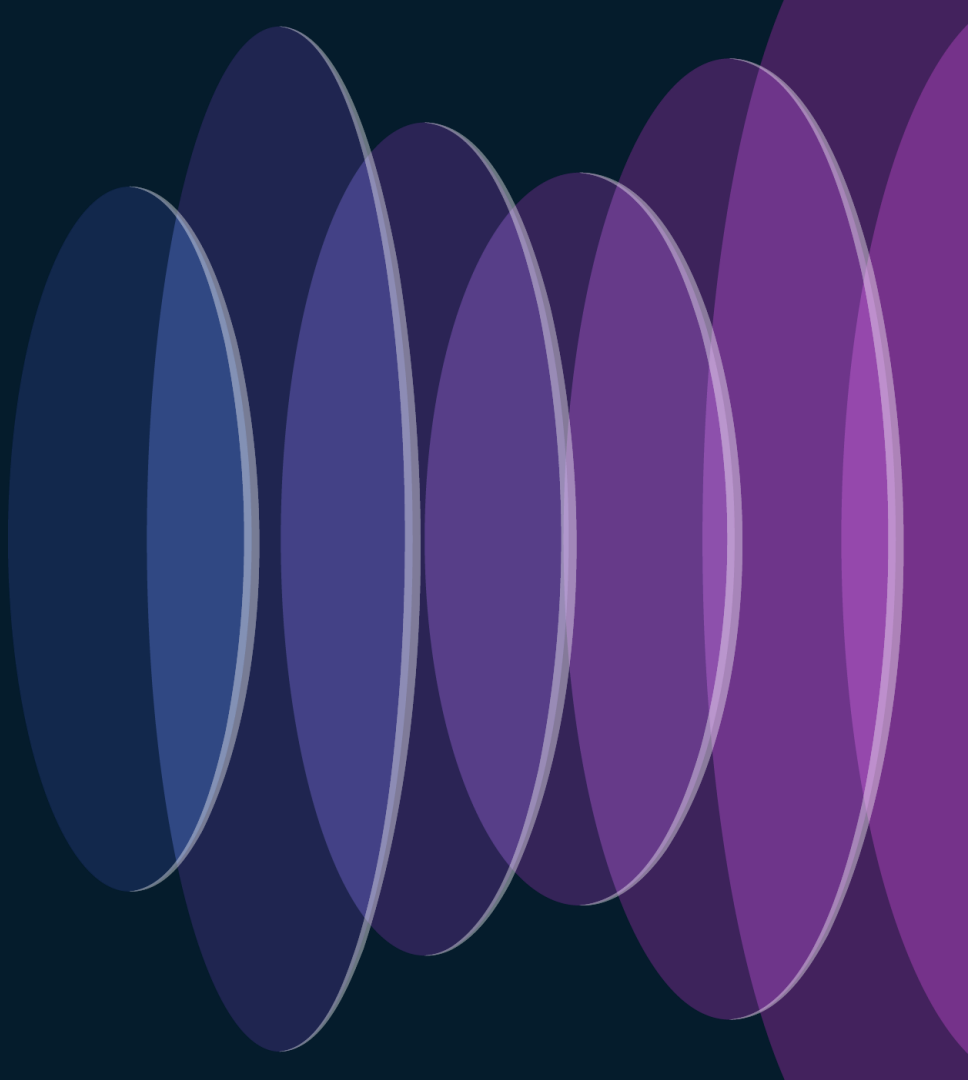


Develop Incident Investigation & Response



Talos Threat Intelligence + Talos Incident Response

Key Takeaways



Key Takeaways

- The ISA/IEC 62443 standards provide an overall framework for securing Industrial Automation and Control Systems, incl. products and procedures
- Key Concepts include
  - Seven Foundational Requirements (FRs) further detailed by System Requirements (SRs)
  - Security Levels (1-4), Security Level Types (SL-T, SL-C & SL-A) and Maturity Levels
  - Devices are organized in Zones with communication controlled by Conduits
- Technologies to adhere to ISA/IEC 62443 include
  - Device Inventory, Network Access Control, Network Segmentation, Firewall (incl. IDS/IPS), Malware Detection, Visibility, Analytics, Device Posture, Vulnerability Management, MFA, XDR
- Cisco Products providing the above include
  - Cisco ISE, Secure Firewall, Routers, Switches, Access Points, Secure Equipment Access
  - Cyber Vision, Secure Network Analytics, XDR, Duo, Secure Endpoint, Secure Client

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: fandreas@cisco.com

Monday, June 3

- **8:00-9:00 - BRKIOT-2601** – Palm D
  8 Tips for Deploying Indoor Wireless Mobility with Cisco Industrial Wireless

  DJ Cole
- **10:30-Noon - BRKIOT-2018** – Mariners AB
  Journey to Innovation: Paving the Way with Smart Architectures and Insights from the Department of Transportation's Pioneers

  Andrew Nolan, Pete Kavanagh, Jeremy Sanders
- **1:00-2:30 - BRKIOT-2720** – Surf EF
  Revolutionizing Manufacturing: The Dawn of Industry 4.0 and Smart Factory Integration

  Arun Siddeswaran, Paul Didier, Kevin Wood
- **2:30-3:30 - BRKIOT-2016** – Palm D
  Streamline Your Success: Automating OT Services with Cisco Catalyst Center Best Practices

  Hailu Meng

Tuesday, June 4

- **10:30-Noon - BRKIOT-1006** – Mariners AB
  Unlocking the Future: Introducing Cisco's Industrial Networking and IoT Essentials

  Rob Barton
- **1:00-2:00 - BRKIOT-1527** – South Seas A
  Securing Industrial Networks - A look at ISA/IEC-62443 and How Cisco Can Help Secure the IIoT Network

  Flemming Andreasen
- **3:00-4:30 - BRKIOT-2265** – Surf EF

  Let's Get Physical with IIoT Wireless

  Igor Moiseev

Wednesday, June 5

- **10:30-11:30 - BRKIOT-2116** – South Seas A
  Using Cyber Vision for OT Asset Visibility and Securing the Industrial Network

  Kevin Holcomb
- **1:00-2:00 - IBOIOT-2101** – Lagoon C
  Revolutionizing Industrial Operations: Unveiling the Power of AI in IIoT with Cisco Solutions and Emerging Industry Trends

  Casca Kwok, Kevin Wood
- **2:30-4:00 - BRKIOT-2882** – Mariners AB
  Implementing Segmentation in Industrial Networks

  Erika Franco, Andrew McPhee
- **4:00-5:00 - BRKIOT-1126** – South Seas A
  Connecting Moving Assets with Cisco IoT Solutions

  Emmanuel Tychon

Thursday, June 6

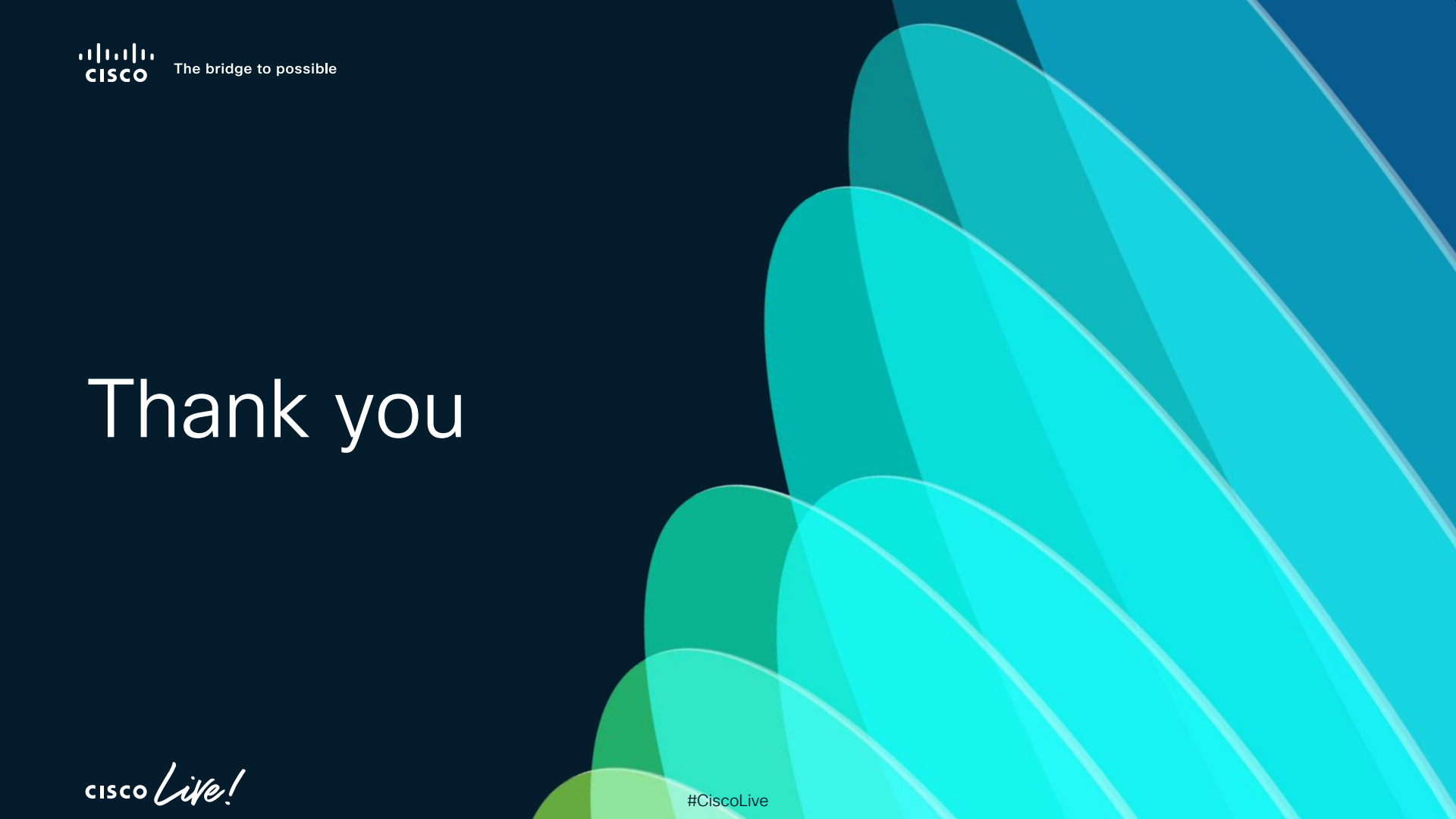
- **8:00-9:00 - BRKIOT-1005** – South Seas A
  Enable Zero Trust Network Access for Industrial Networks with Cisco Secure Equipment Access

  Andrew McPhee, Emmanuel Tychon
- **10:30-12:00 - BRKIOT-2017** – Mariners AB
  Streamline Your Industry: Dynamic SD-WAN Use Cases for Enhanced Industrial Performance

  Pete Kavanaugh, Dan Madey,
- **11:00-12:00 -BRKIOT-2015** – Lagoon EF
  The New Digital Substation: More Efficient, More Secure, and Ready for Demanding Modern Grid Applications

  Marcus Smith
- **1:00-2:00 - IBOIOT-2100** – Lagoon C
  Cut Through the Complexity: Navigating LAN Redundancy Options with Ease

  Albert Mitchell, Erika Franco


The bridge to possible
Thank you
cisco Live!
#CiscoLive