SeaPath Security Audit

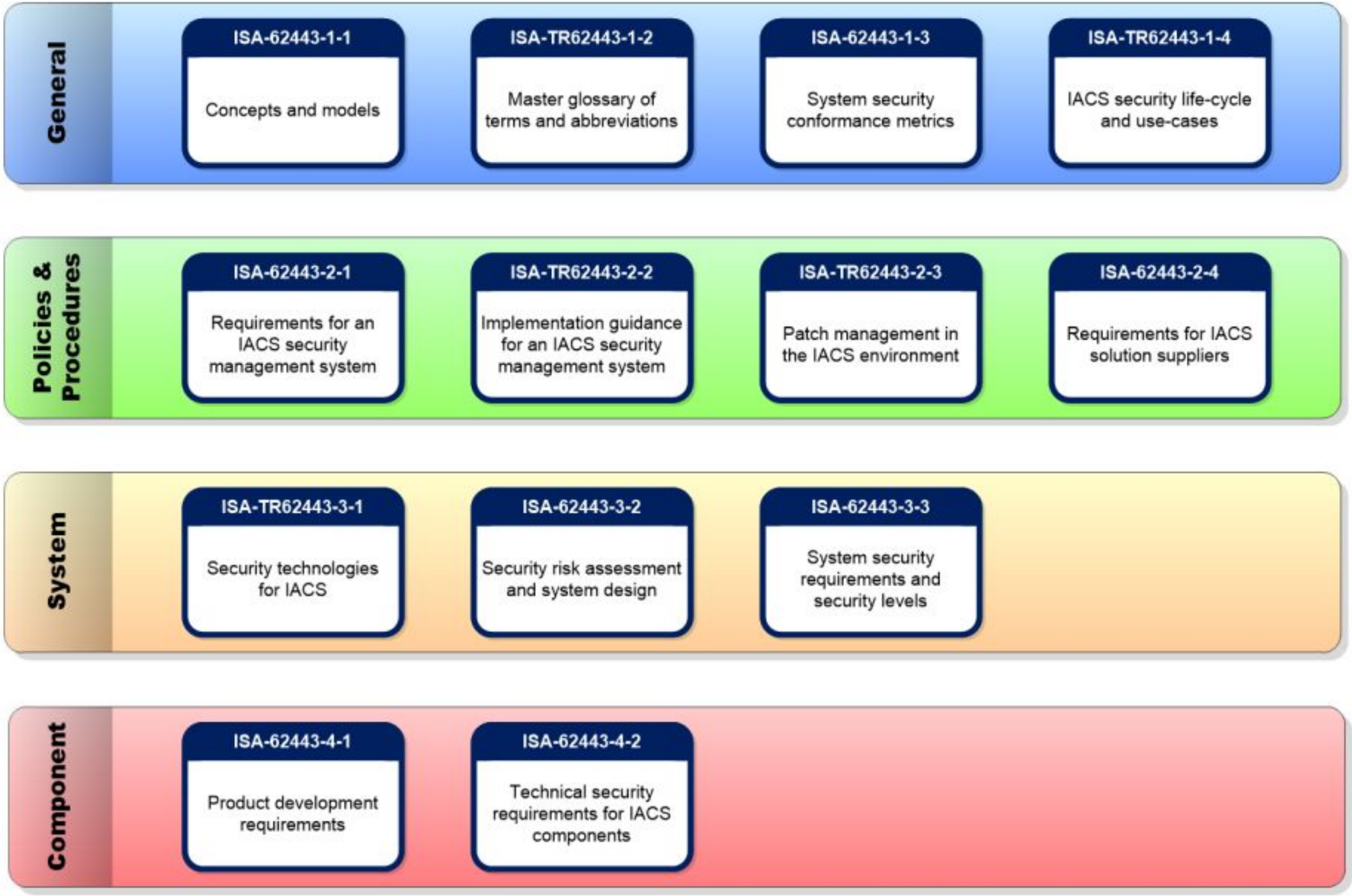
16 Feb 2024

Scope - ISA-62443

1. Audit based on ISA-62443
2. The goal is to investigate road to compliance and comply where possible
3. Improve the security posture of SeaPath

Scope - audit

1. 62443-1: Terminology, concepts, and models
2. 62443-2: Establishing an industrial automation and control systems security program
3. 62443-3: Security risk assessment for system design
4. 62443-4: Secure product development lifecycle requirements & Technical security requirements for IACS components



General

ISA-62443-1-1
Concepts and models

ISA-TR62443-1-2
Master glossary of terms and abbreviations

ISA-62443-1-3
System security conformance metrics

ISA-TR62443-1-4
IACS security life-cycle and use-cases

Policies & Procedures

ISA-62443-2-1
Requirements for an IACS security management system

ISA-TR62443-2-2
Implementation guidance for an IACS security management system

ISA-TR62443-2-3
Patch management in the IACS environment

ISA-62443-2-4
Requirements for IACS solution suppliers

System

ISA-TR62443-3-1
Security technologies for IACS

ISA-62443-3-2
Security risk assessment and system design

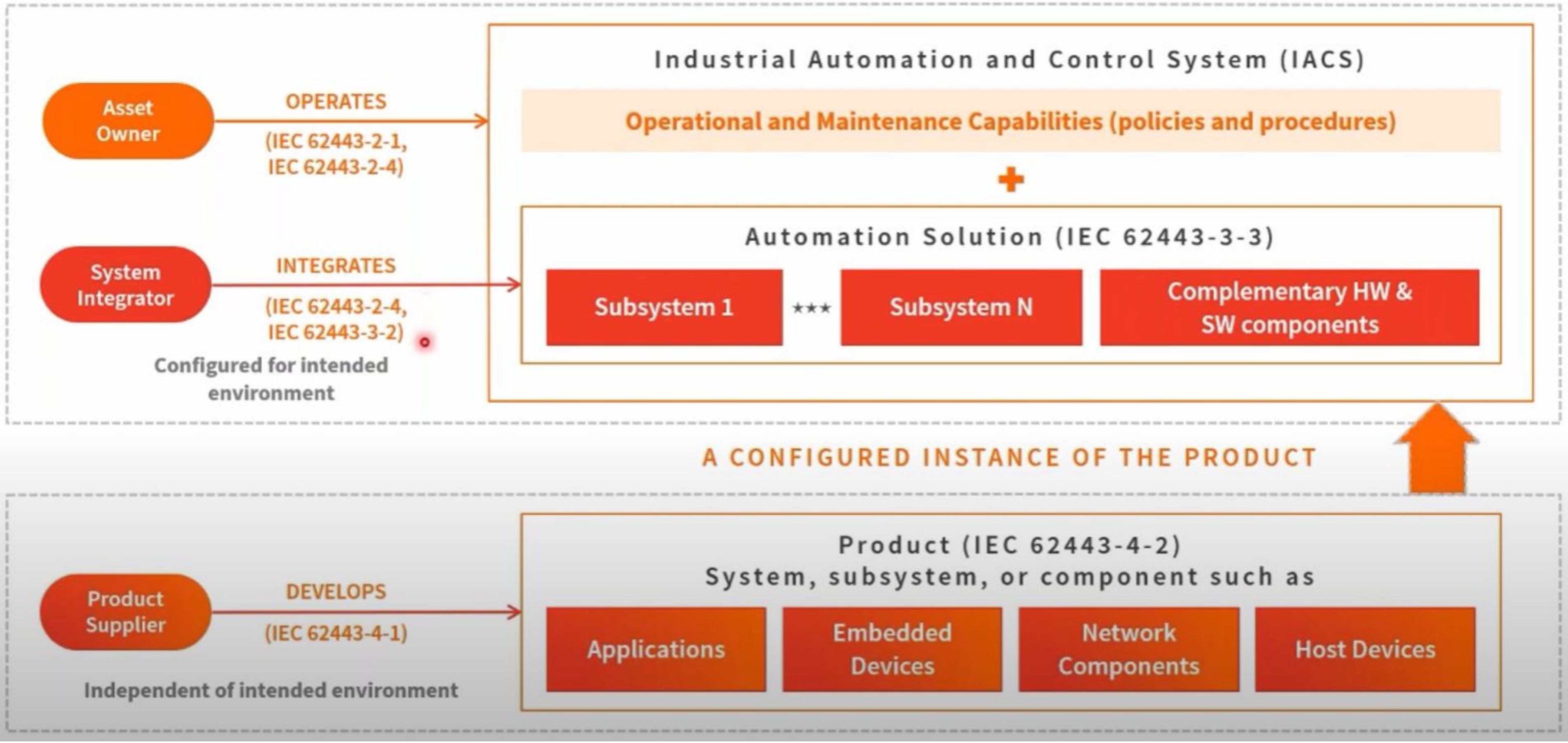
ISA-62443-3-3
System security requirements and security levels

Component

ISA-62443-4-1
Product development requirements

ISA-62443-4-2
Technical security requirements for IACS components

Logical view of IEC 62443 Standards



Asset Owner

OPERATES

(IEC 62443-2-1, IEC 62443-2-4)

System Integrator

INTEGRATES

(IEC 62443-2-4, IEC 62443-3-2)

Configured for intended environment

Industrial Automation and Control System (IACS)

Operational and Maintenance Capabilities (policies and procedures)

+

Automation Solution (IEC 62443-3-3)

Subsystem 1

***

Subsystem N

Complementary HW & SW components

A CONFIGURED INSTANCE OF THE PRODUCT

Product Supplier

DEVELOPS

(IEC 62443-4-1)

Independent of intended environment

Product (IEC 62443-4-2)
System, subsystem, or component such as

Applications

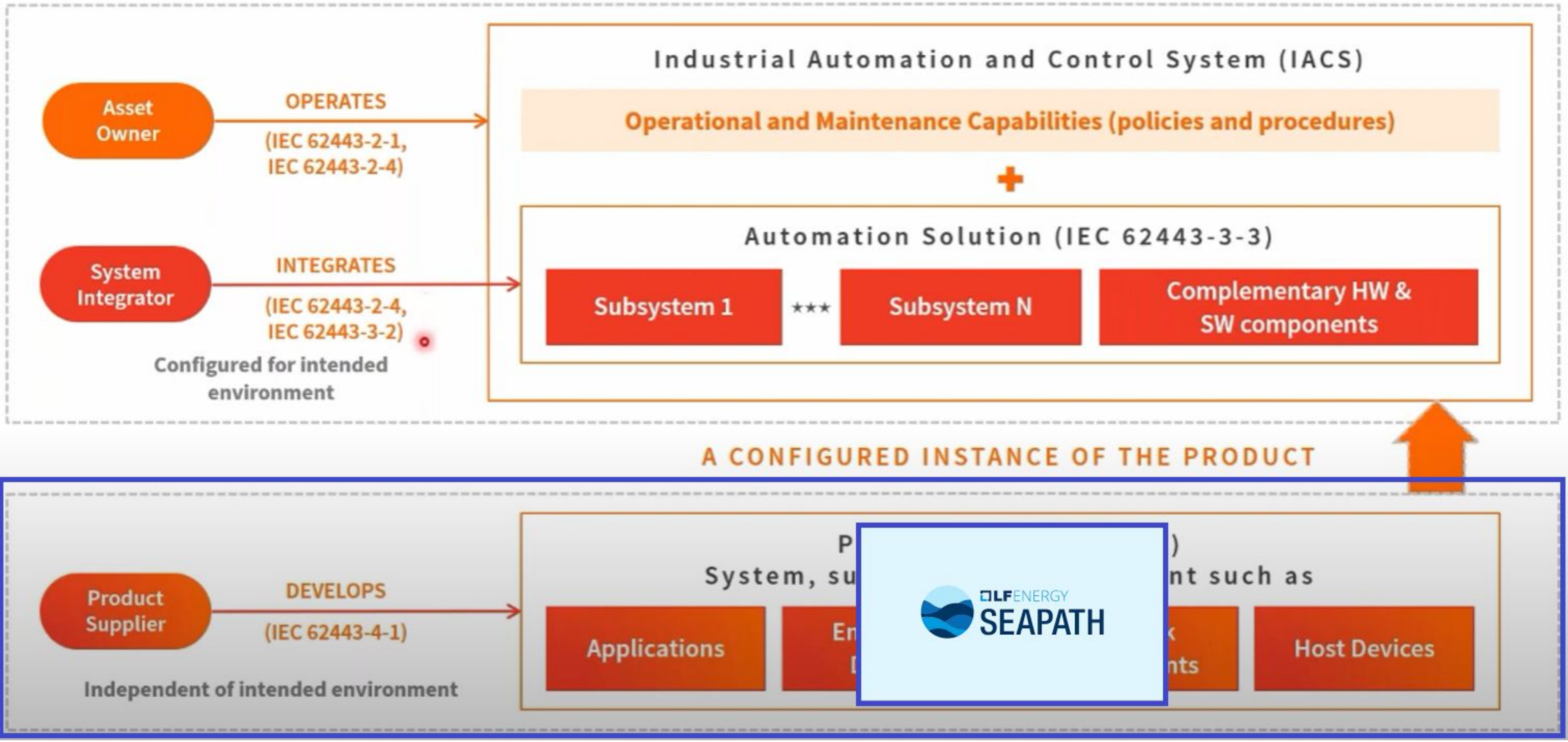
Embedded Devices

Network Components

Host Devices

https://youtu.be/cRIowkXRb2g?si=H4koSRAdIaxuMr-b&t=1031

Logical view of IEC 62443 Standards



Industrial Automation and Control System (IACS)

Operational and Maintenance Capabilities (policies and procedures)

+

Automation Solution (IEC 62443-3-3)

Subsystem 1 *** Subsystem N

Complementary HW & SW components

Asset Owner — OPERATES (IEC 62443-2-1, IEC 62443-2-4)

System Integrator — INTEGRATES (IEC 62443-2-4, IEC 62443-3-2)

Configured for intended environment

A CONFIGURED INSTANCE OF THE PRODUCT

Product Supplier — DEVELOPS (IEC 62443-4-1)

Independent of intended environment

P)

System, su nt such as

Applications

En

[

k

nts

Host Devices

LF ENERGY SEAPATH

https://youtu.be/cRIowkXRb2g?si=H4koSRAdIaxuMr-b&t=1031

Scope - ISA-62443

1. 62443-1: Terminology, concepts, and models
2. 62443-2: Establishing an industrial automation and control systems security program
3. 62443-3: Security risk assessment for system design
4. **62443-4: Secure product development lifecycle requirements & Technical security requirements for IACS components**

Scope - ISA-62443

1. 62443-1: Terminology, concepts, and models
2. 62443-2: Establishing an industrial automation and control systems security program
3. 62443-3: Security risk assessment for system design
4. **62443-4: Secure product development lifecycle requirements & Technical security requirements for IACS components**
   a. **62443-4-1: Secure product development lifecycle requirements**
   b. **62443-4-2: Technical security requirements for IACS components**

62443-4-1: Secure product development lifecycle requirements

1. **Development process**: How the maintainers and contributors work together securely.
2. **Product security context**: Threat model and the environment (context) SeaPath operates in.
3. **Secure design principles**: The design that SeaPath should follow.
4. **Security implementation review**: Documentation on evaluating whether SeaPath follows the design principles laid out in the “Secure design principles” section.
5. **Security verification and validation testing**: SeaPaths documentation and practices for automated and manual testing.
6. **Security disclosure**: Processes for receiving and handling security issues.
7. **Security update management**: How SeaPath handles, releases and notifies security patches.

62443-4-2: Technical security requirements for IACS components

A series of technical security requirements that SeaPaths products must adhere to.

62443-4-1: Secure product development lifecycle requirements

1. **Development process**: How the maintainers and contributors work together securely.
2. **Product security context**: Threat model and the environment (context) SeaPath operates in.
3. **Secure design principles**: The design that SeaPath should follow.
4. **Security implementation review**: Documentation on evaluating whether SeaPath follows the design principles laid out in the “Secure design principles” section.
5. **Security verification and validation testing**: SeaPaths documentation and practices for automated and manual testing.
6. **Security disclosure**: Processes for receiving and handling security issues.
7. **Security update management**: How SeaPath handles, releases and notifies security patches.

62443-4-1: Secure product development lifecycle requirements

1. **Development process**: How the maintainers and contributors work together securely.
2. **Product security context**: Threat model and the environment (context) SeaPath operates in.
3. **Secure design principles**: The design that SeaPath should follow.
4. **Security implementation review**: Documentation on evaluating whether SeaPath follows the design principles laid out in the “Secure design principles” section.
5. **Security verification and validation testing**: SeaPaths documentation and practices for automated and manual testing.
6. **Security disclosure**: Processes for receiving and handling security issues.
7. **Security update management**: How SeaPath handles, releases and notifies security patches.

62443-4-1: Secure product development lifecycle requirements

1. **Development process**: How the maintainers and contributors work together securely.
2. **Product security context**: Threat model and the environment (context) SeaPath operates in.
3. **Secure design principles**: The design that SeaPath should follow.
4. **Security implementation review**: Documentation on evaluating whether SeaPath follows the design principles laid out in the "Secure design principles" section.
5. **Security verification and validation testing**: SeaPaths documentation and practices for automated and manual testing.
6. **Security disclosure**: Processes for receiving and handling security issues.
7. **Security update management**: How SeaPath handles, releases and notifies security patches.

Next steps

1. **Development process**:
   a. Ada Logics sends requirements to SeaPath team.
   b. SeaPath team creates documentation.
   c. Ada Logics reviews.
2. **Product security context**: Threat model and the environment (context) SeaPath operates in.
   a. Ada Logics sends requirements to SeaPath team.
   b. SeaPath team and Ada Logics create different parts documentation and/or in collaboration.
3. **Secure design principles**: The design that SeaPath should follow.
   a. Ada Logics sends requirements to SeaPath team.
   b. SeaPath team and Ada Logics create different parts documentation and/or in collaboration.
4. **Security implementation review**: Documentation on evaluating whether SeaPath follows the design principles laid out in the “Secure design principles” section.
   a. SeaPath creates the processes for evaluating.
   b. Ada Logics evaluates.
5. **Security verification and validation testing**: SeaPaths documentation and practices for automated and manual testing.
   a. Same as 4
6. **Security disclosure**: Processes for receiving and handling security issues.
   a. Same as 1
7. **Security update management**: How SeaPath handles, releases and notifies security patches.
   a. Same as 1

Next steps - practice

1. Assign TODO’s in SeaPath team.
2. Schedule threat modelling exercise.
3. Draft process documentation is complete.
4. Ada Logics reviews documentation and audits code assets.
5. Ada Logics reports findings.
6. SeaPath reviews findings.
7. Security audit concludes.