ISASecure® Certification - An End User Perspective

Dennis Parker – Manager, Chevron Enterprise
PCN Cybersecurity Assurance

Kenny Mesker – ICS Cybersecurity Engineer
Chevron and
Board Chair – ISA Security Compliance Institute (ISCI)

Agenda

1 The Current Threat Landscape

2 IEC 62443 Standard

3 Value of Compliance Testing

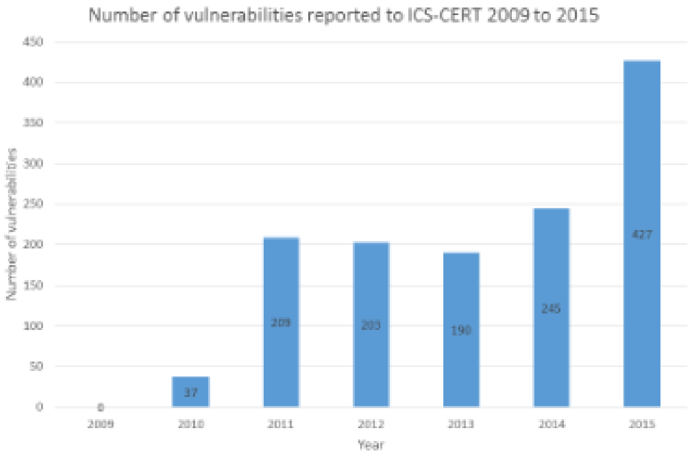
4 Conclusions

ICS Cyber Attacks Accelerating

“In this world nothing is certain except death, taxes, and cyber attacks”

“In this world nothing is certain except death, and taxes” - Ben Franklin, 1789

- Number of individuals with hacking skills increasing
- Tools that simplify hacking (Metasploit and others) readily available
  - Successful breach code is available on the internet
  - Much of NSA cybersecurity arsenal in the hands of adversaries
- Reported ICS Vulnerabilities on the rise[1]
- Ransomware is a billion dollar industry



Market data

- 54% of ICS companies suffered at least one cyberattack in the last 12 months[2]
- 69% of ICS security practitioners feel threat to ICS systems is severe/critical[3]
- US warns public about attacks on energy, industrial firms

Sources

[1] NCCIC/ICS-Cert Vulnerability Coordination Report – 2015

[2] Kaspersky Labs State of Industrial Cybersecurity Survey, 2017

[3] Securing Industrial Control Systems, SANS 2017

Agenda

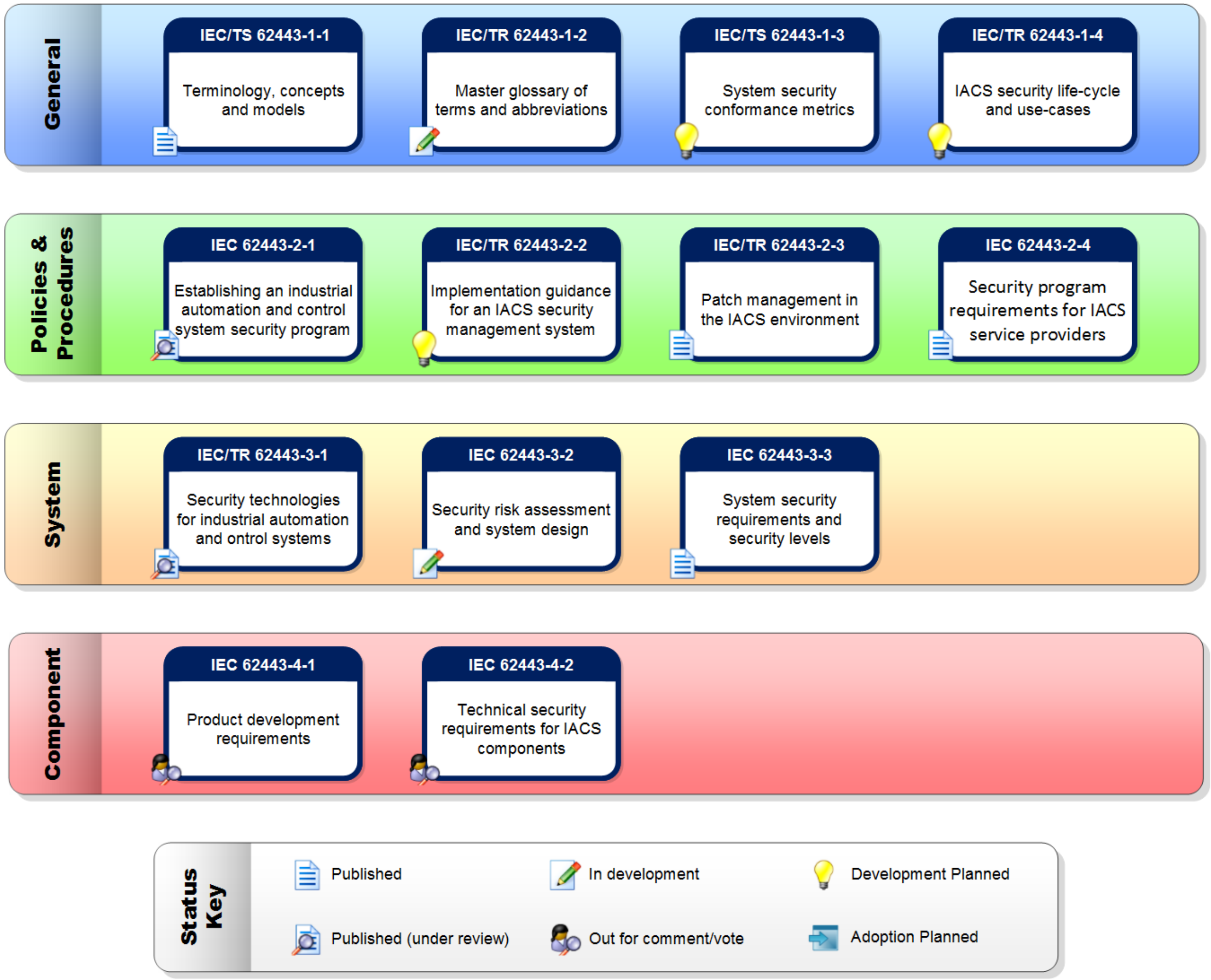
1 The Current Threat Landscape

2 IEC 62443 Standard

3 Value of Compliance Testing

4 Conclusions

IEC 62443 Standards Address Industrial Security



General

- 📄 **IEC/TS 62443-1-1** Terminology, concepts and models
- ✏ **IEC/TR 62443-1-2** Master glossary of terms and abbreviations
- 💡 **IEC/TS 62443-1-3** System security conformance metrics
- 💡 **IEC/TR 62443-1-4** IACS security life-cycle and use-cases

Policies & Procedures

- 🔍 **IEC 62443-2-1** Establishing an industrial automation and control system security program
- 💡 **IEC/TR 62443-2-2** Implementation guidance for an IACS security management system
- 📄 **IEC/TR 62443-2-3** Patch management in the IACS environment
- 📄 **IEC 62443-2-4** Security program requirements for IACS service providers

System

- 🔍 **IEC/TR 62443-3-1** Security technologies for industrial automation and ontrol systems
- ✏ **IEC 62443-3-2** Security risk assessment and system design
- 📄 **IEC 62443-3-3** System security requirements and security levels

Component

- 👥 **IEC 62443-4-1** Product development requirements
- 👥 **IEC 62443-4-2** Technical security requirements for IACS components

Status Key

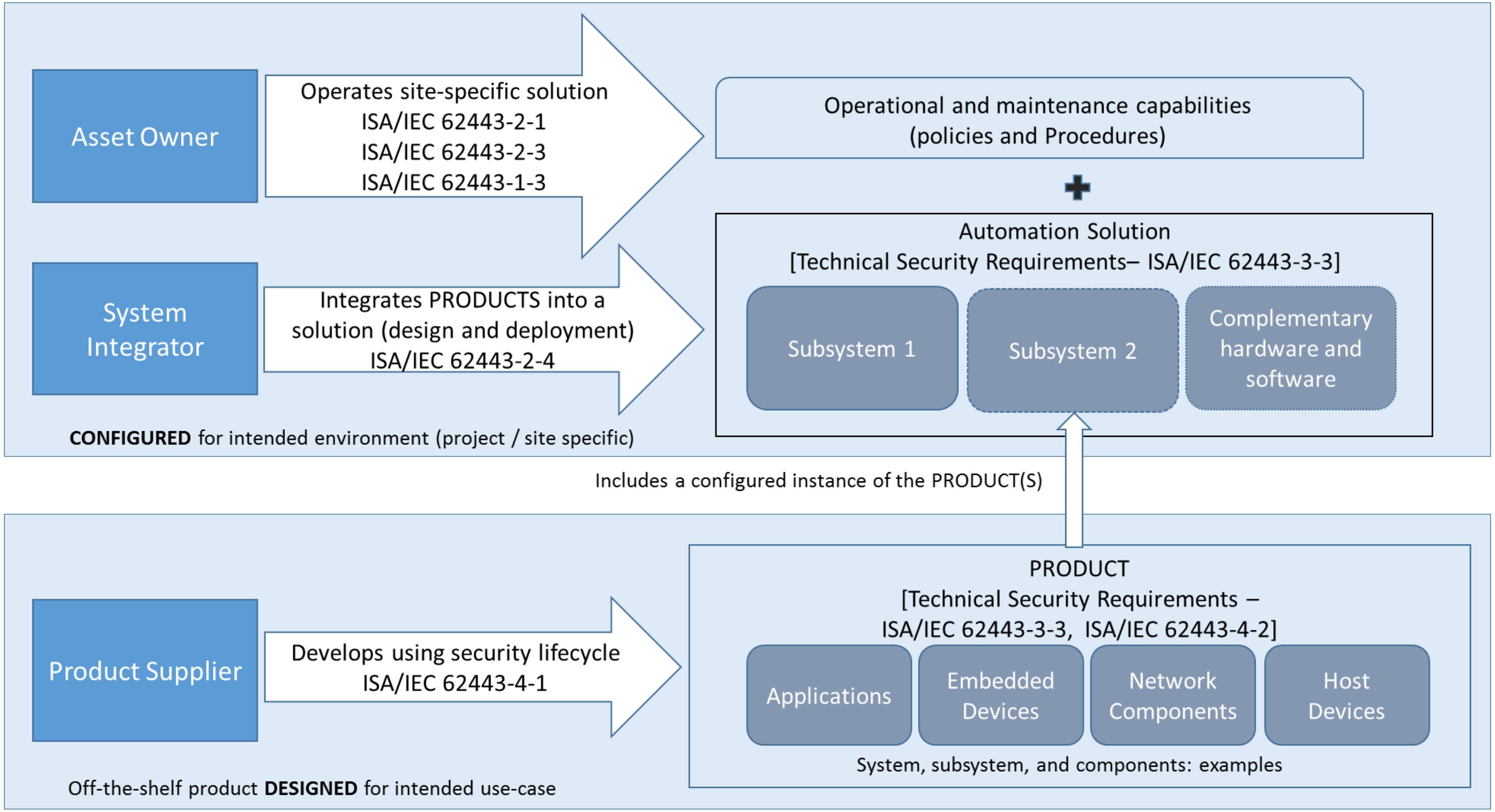
📄 Published	✏ In development	💡 Development Planned
🔍 Published (under review)	👥 Out for comment/vote	➡ Adoption Planned

Key Standards

IEC Standard	Overview	Equipment Vendor	Systems Integrator
IEC 62443-2-4	System integrator - Policies and process		●
IEC 62443-4-1	Vendor - Secure development lifecycle	●	
IEC 62443-4-2	Vendor – Component specification	●	
IEC 62443-3-3	Vendor/Integrator – System specification		●

IEC 62443 Standards Family

Industrial Automation and Control System (IACS) (from ISA 62443-2-4)



Asset Owner

Operates site-specific solution
ISA/IEC 62443-2-1
ISA/IEC 62443-2-3
ISA/IEC 62443-1-3

Operational and maintenance capabilities
(policies and Procedures)

✚

System Integrator

Integrates PRODUCTS into a solution (design and deployment)
ISA/IEC 62443-2-4

Automation Solution
[Technical Security Requirements– ISA/IEC 62443-3-3]

CONFIGURED for intended environment (project / site specific)

Includes a configured instance of the PRODUCT(S)

Product Supplier

Develops using security lifecycle
ISA/IEC 62443-4-1

PRODUCT
[Technical Security Requirements –
ISA/IEC 62443-3-3, ISA/IEC 62443-4-2]

System, subsystem, and components: examples

Off-the-shelf product **DESIGNED** for intended use-case

IEC 62443 Security Assurance Levels

Security Level	Skills	Motivation	Means	Resources
SL1 Employee, Contractor	No Attack Skills	Mistakes	Non-intentional	Individual
SL2 Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individuals)
SL3 Hacktivist, Terrorist	ICS Specific	Moderate	Sophisticated (attack)	Moderate (Hacker Groups)
SL4 Nation State	ICS Specific	High	Sophisticated (campaign)	Extended (Multi-disciplinary Teams)

Sample Requirements

IEC 62443-4-2 Component Identification and Authentication Control

Feature	SL1	SL2	SL3	SL4
Identify and authenticate human users	X	X	X	X
Component shall enable the management of accounts	X	X	X	X
Component shall support the management of identifiers	X	X	X	X
Component shall support authenticator management	X	X	X	X
Password based authentication with defined password strength	X	X	X	X
Obscure authentication feedback during authentication process	X	X	X	X
Enforce unsuccessful login attempt limit, lock account	X	X	X	X
Provide warning message to individuals attempting to access the system	X	X	X	X
Uniquely identify and authenticate all human users		X	X	X
Software process and device identification and authentication		X	X	X
When PKI is used, the component shall integrate with PKI infrastructure		X	X	X
When PKI is used, the component shall check validity of certificates		X	X	X
Support for symmetric key based authentication		X	X	X
Unique software process and device identification and authentication			X	X
Authenticators shall be protected by hardware mechanisms			X	X
Prevent password reuse for configurable number of generations human users			X	X
Protection of public key via hardware			X	X
Protection of symmetric key data via hardware			X	X
Multifactor authentication for all interfaces				X
Prevent password reuse for configurable number of generations software process or device				X

Agenda

1 The Current Threat Landscape

2 IEC 62443 Standard

3 Value of Compliance Testing

4 Conclusions

ISASecure® Certification Scheme

ISASecure

A not for profit organization created to facilitate IEC62443 standard certifications

- Comprised of representatives from end users, government agencies, suppliers, consultants, and certification labs
- Chevron is a founding member

Certifying since 2010

Accredited certification labs

CSSC Certification Laboratory

exida

TÜVRheinland®

EDSA Certifications – 22+ Products from 11+ different companies

Why Certify COTS Products?

1. Security capabilities are independently assessed and certified by experts at accredited ISASecure labs
2. Reduces effort for end user to validate and verify security capabilities. (scarcity of talented cybersecurity expertise)
3. Objective metric for security capabilities based on industry standards. (hundreds of years of SME and knowledge codified into IEC 62443-x-x from hundreds of committee participants.)

One specification, one service mark, one assessment

Three ISASecure® certifications available

1. Embedded Device Security Assurance (EDSA) product certification
   - **IEC 62443-4-2**
   - **IEC 62443-4-1**
   - **Vulnerability Identification Test**
   - **+ Communication Robustness Test**
2. System Security Assurance (SSA) product certification
   - **IEC-62443-3-3**
   - **IEC 62443-4-1**
   - **IEC 62443-4-2**
   - **Vulnerability Identification Test**
   - **+ Communication Robustness Test**
3. Security Development Lifecycle Assurance (SDLA) process certification
   - **IEC-62443-4-1**

Cybersecurity Compliance Status

Slow, Gaining Momentum

Compliance in the industry driven by four forces

- End users demand compliance for new orders – Limited requirements at present
- Regulations demand compliance testing – Some countries proposing standards
- Vendors certify solutions for differentiation – Vendors certify small percentage of offer ranges
- Major event(s) force change

End User Perspective

Chevron realizes the importance of integrating cybersecurity in the beginning of the procurement process

Standards based certification enables:

- Efficient alternative analysis during project planning
- Use of common compliance language with internal staff, vendors, and ONG partners

ISA/IEC 62443 security level concept gives end users the ability to select solutions to close security gaps

Certification provides assurance that cybersecurity features are available and lowers the burden of post project deployment compliance

Chevron is a committed member of the ISA Security Compliance Institute (ISCI) – the organization behind ISASecure. ISCI provides a forum where end-users can:

- ensure that ISA/IEC 62443 standards are implemented as intended, and
- include their company specific requirements in certification specifications

End-user Benefits and Value

- Simplifies procurement specification process
- End users understand standards-based product cybersecurity capabilities
- Capabilities independently validated by external entity
- Confidence that security features will evolve over time
- ISCI provides a forum where end-users can ensure that
- ISA/IEC 62443 standards are implemented as intended
- Forum where an end-user can include their company specific requirements in certification specifications

Agenda

1 The Current Threat Landscape

2 IEC 62443 Standard

3 Value of Compliance Testing

4 Conclusions

Conclusions

The rate of cyber attacks has been steadily increasing – rate expected to increase for the foreseeable future

IEC 62443 specification generally accepted standard for industrial security

Third party certification of standards compliance provides value to end users and vendors – Compliance certification solutions in place today