Securing Control Systems using IEC 62443 Standards

Dan DesRuisseaux
Cybersecurity Program Director
Schneider Electric

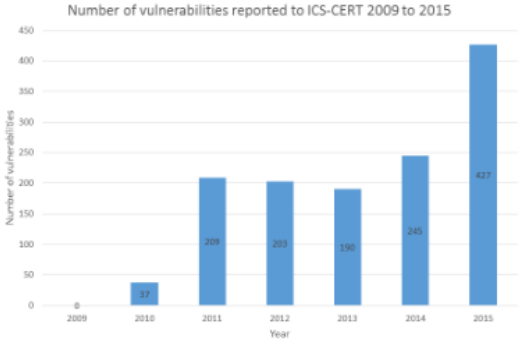
Agenda

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 and taxes" – Benjamin Franklin, 1789

- Number of individuals with hacking skills increasing
- Tools that simplify hacking (Metasploit) readily available
  - NSA hacking tools posted on the internet
- Reported ICS Vulnerabilities on the rise[2]
- Ransomware is a billion dollar industry
- ICS equipment in field for up to 20 years



Market data

- 54% of ICS companies suffered at least one cyberattack in the last 12 months[1]
- 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]Kaspersky Labs State of Industrial Cybersecurity Survey, 2017

[2]NCCIC/ICS-Cert Vulnerability Coordination Report - 2015

[3]Securing Industrial Control Systems, SANS 2017

Agenda

1. *The Current Threat Landscape*
2. *IEC 62443 Standard*
3. *Value of Compliance Testing*
4. *Conclusions*

Cybersecurity Standards Evolving

IEC 62443 leading the pack

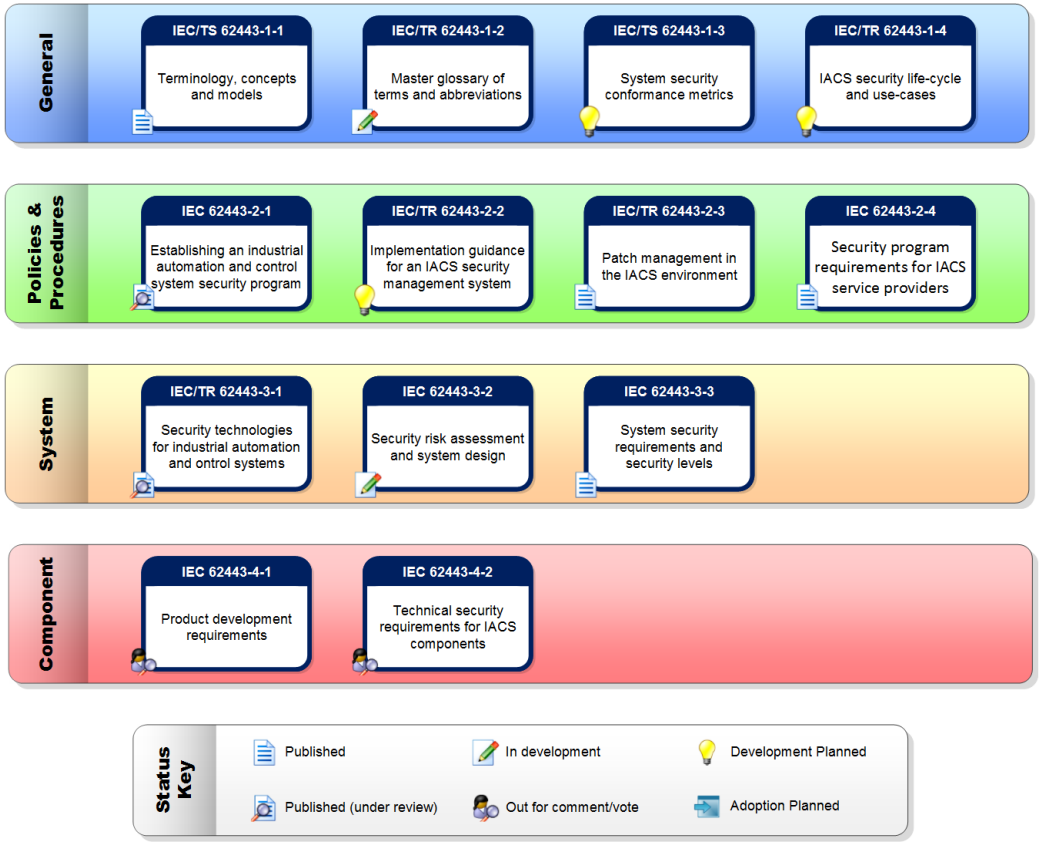
Industrial cybersecurity standards are emerging

- Segment based standards

Local regulations and certifications

- FSTEC Order No. 31 (Russia)
- CSPN (France)
- China

IEC 62443 Standards



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		○

Cybersecurity Foundational Requirements

Identification and Access Control – Passwords and user authentication

Use Control – Mapping to roles and authorization enforcement

System Integrity – Session handling, and cryptography to recognize changes

Data Confidentiality – Encryption

Restricted Data Flow – Network segmentation

Timely Response to Events – Logs

Resource Availability – System backup and recovery

IEC 62443 Security Assurance Levels

Security levels define the cybersecure functions embedded in our products, it increase the product robustness and make it resistant to the Cyber threats.

Groups/Nation-states, governmental organization member…	Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation	SL 4
Cybercrime player, Terrorists, Hacktivists, Professional thieves, Cyber-criminals, competitors	Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation	SL 3
Insider (Disgruntled employees or contractors…) or intruder (Thrill-seeking, hobbyist, malicious organization…)	Protection against intentional violation using simple means with low resources, generic skills and low motivation	SL 2
Insider (Well-intentioned, careless employees or contractors)	Protection against casual or coincidental violation	SL 1

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

SDL – Secure Development Lifecycle

Train	Require	Design	Develop	Verify	Release	Deploy	Respond
Deliver Security Training	***Security Requirements***	***Secure Design Reviews***	***Secure Code Practices***	***Security Testing***	***Secure Release Management***	***Secure Deployment***	***Incident Response***
On-demand training for each role	*Security requirements based on regulations*	*Conduct Threat Modeling and Architecture Review*	*Scan all code related to product*	*Secure white box and black box testing*	*Documentation and process details to securely deploy the offering*	*Full security lifecycle services for customers*	*Respond to incidents and vulnerabilities reported*

Agenda

1. *The Current Threat Landscape*
2. *IEC 62443 Standard*
3. *Value of Compliance Testing*
4. *Conclusions*

Which Car Should I Buy?

Certification….Why Assess and Certify?

Does the system perform as advertised?

Certification insures that standards have been properly adapted

Certification Value

End Users

- Simplifies specification process
- End users understand product capabilities
- Capabilities validated by external entity
- Reduced time in acceptance testing

Equipment Vendors

- Differentiate solutions
- Assurance products meet cybersecurity requirements
- Support cost reduction / customer satisfaction
- Reduce potential liabilities

IEC 62443 Certification Scheme

A not for profit organization created to facilitate IEC62443 standard certifications

- Comprised of representatives from end users, government agencies, suppliers, consultants, and certification labs

Certifying since 2010

Accredited certification labs

CSSC Certification Laboratory

exida

TÜVRheinland®

ISASecure® Supporters – Past & Present

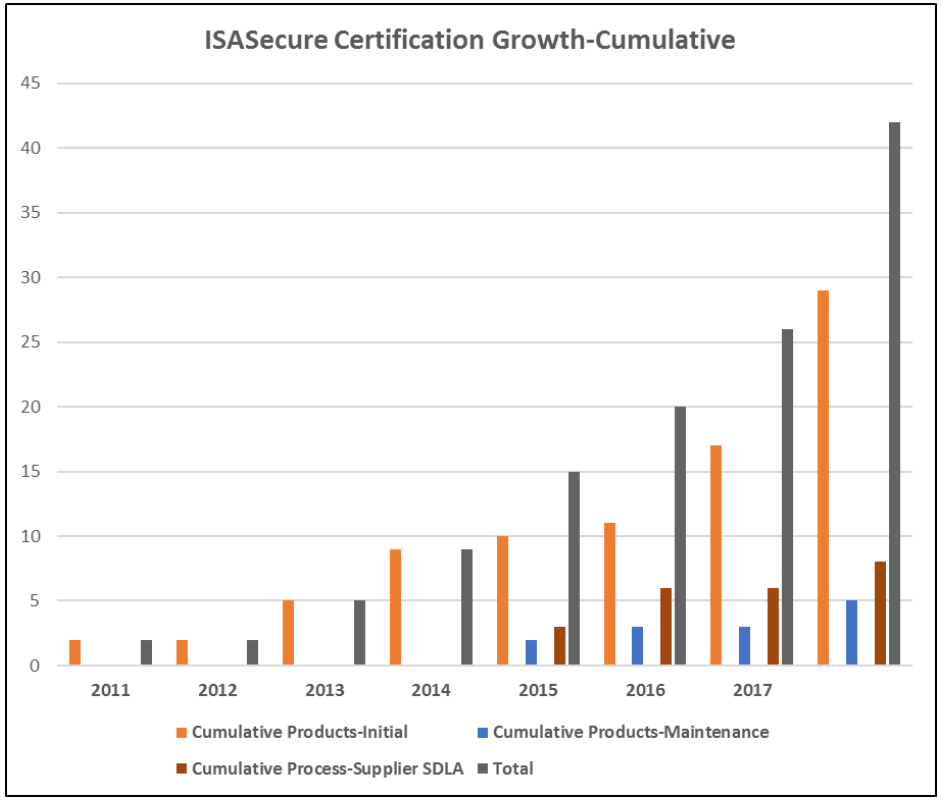
ISA Secure Certifications

Security Development Lifecycle Assurance (SDLA) – Process Certification
IEC-62443-4-1

Embedded Device Security Assurance (EDSA) – Product Certification
IEC 62443-4-2, IEC 62443-4-1

System Security Assurance (SSA) – System Certification
IEC-62443-3-3, IEC 62443-4-1

ISASecure Certification Growth



ISASecure Certified Development Organizations

Schneider Electric

5 Sites

Honeywell

1 Site

EMERSON

2 Sites

Cybersecurity Compliance Status

Slow but Gaining Momentum

Compliance driven by three 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 percentage of offer ranges

Potential outcomes

- Three forces accelerate change
- Major event(s) force change

Agenda

1. *The Current Threat Landscape*
2. *IEC 62443 Standard*
3. *Value of Compliance Testing*
4. *Conclusions*

Schneider Electric Utilizing ISA Secure

Defined certification scheme – security level certification enables differentiation

Mature certification scheme – most 62443 certifications,

Driven by non profit organization

- End user representation
- Supported by major suppliers

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

Thank You