Standards: key for digital security of critical infrastructure

Richard Schomberg
IEC Ambassador & Chair IEC Systems Committee for Smart Energy
Past Chair IEC Nuclear Instrumentation

OECD Workshop
Digital Security
15-16 February, 2018
Paris, France
Questions to be addressed

• What are the greatest digital risks to energy systems
• What can be done to enhance digital resilience
• Who is responsible for what
• How to verify proper implementation of regulations
Energy: complexity is increasing

+ More interconnection
+ More information exchange
+ Higher reliability, increased control
+ Better interoperability

- Increased cyber vulnerabilities
Roles and challenges

Regulators:

• Raise cyber security awareness, assign accountability, provide clear requirements

Utilities:

• Accept responsibility, update infrastructure, commit necessary investment
Energy security: ICT and OT

Virtual world
Data
Identify, correct, protect from constant attacks
Large surface for attacks

Physical world
Ensure physical function - reliability, time and time again - either/or
Narrow surface for attacks
Global risks, global approach

Prefer common platforms that encourage cooperation and avoid island solutions.

IEC Standards:
• Global reach – 171 countries
• Members = countries not companies
• Built-in high consensus value
• Neutral, independent

Provide input to standardization.
Three axes of cyber security

- **Organisation**
  - Patch Management
  - Security Awareness
  - Security Training
  - Secure Operations
  - Audit Capability
  - Secure Configuration

- **Process**
  - Patch Management
  - Incidence Response
  - Secure Dev. And Test
  - Risk Assessment
  - Secure Configuration
  - Access Protection

- **Technical**
  - Hardening
  - Access Protection
  - User Authentication
  - Security Logs
  - Secure Communications

Credit: Schneider Electric
IEC 27001/2 key clauses

- Foreword
- Introduction
- Scope
- Normative references
- Terms and definitions
- Structure of this standard
- Bibliography

- Asset management
- Access control

- Operations security

- Information security policies

- Cryptography
- Physical and environmental security

- Communications security
- Systems acquisition, development and maintenance

- Compliance
- Supplier relationships
- Incident management
- Information security aspects of business continuity management

★ = Unique Domains
Build to International Standards

IEC: 235 OT and ICT security related publications
IEC CA Systems also active in cyber security – helps regulators verify implementation

Credit: Schneider Electric
Real-time visibility of threats

Organisation
- Patch Management
- Security Awareness
- Security Training
- Secure Operations
- Audit Capability
- Secure Configuration

Process
- Patch Management
- Incidence Response
- Secure Dev. And Test
- Risk Assessment
- Secure Configuration
- Access Protection

Technical
- Hardening
- Access Protection
- User Authentication
- Security Logs
- Secure Communications

Energy Industry Standards and Guidelines
- IEC 62351
- IEC 62443/ISA 99
- IEEE 1686
- IEEE C37 240
- NISTIR 7628
- NIST SP800-53
- ISO/IEC 27002/19

Credit: Schneider Electric
IEC 62645 for nuclear: from generic to specialized

ISO/IEC 27000 → IAEA