VINÇOTTE

a kiwa company

Bridging IT & OT Security Frameworks: Ensuring Compliance in Industrial Environments

Academic Insights, Industrial Impact

The Future of IoT Security Testing

Sam Van Hauwaert

https://www.linkedin.com/in/svanhauwaert/

VINÇOTTE

a kiwa company

Case Study 1:
Complying with the NIS2 in the Industry

Academic Insights, Industrial Impact

The Future of IoT Security Testing

Sam Van Hauwaert

https://www.linkedin.com/in/svanhauwaert/

Industry Testimonial Introduction

- This case is in the course of implementation in a pan-European Waste Management Company
  - Their core business is Industrial Waste Management
  - As a byproduct of burning waste,
    - they operate district-heating systems
    - they produce electricity

- This organization has over 30 entities in Europe
- They must comply with NIS2 as an essential entity

Industry Testimonial
Problem Definition

- The common denominator across Europe for complying with NIS2 will probably be ISO27001
  - Confirmed: Belgium, Hungary, Croatia, Romania, Finland
  - Unclear: The Netherlands, Germany

- They currently operate OT installation loosely based on ISA/IEC62443, but without formal definition of Risk, Risk Tolerance or Security Level

- The combination of ISO27001/27002 does not fully support typical Industrial realities: Long Life-Cycle (+15y), the 24x7 uptime requirements, the use of legacy technology, the concept of ‘Safety’

Industry Testimonial Approach

The organization has decided to create a unified IT/OT management system using ISO27001 as primary ISMS, as instructed in ISA/IEC 62443-2-1:2024

'ORG 1.1 If the asset owner has an ISMS, the asset owner **shall** coordinate the IACS Security Program (SPM) with the ISMS. If the Asset owner does not have an ISMS, the asset owner shall incorporate the appropriate management process into the IACS Security Program (SP).
The ISMS and the IACS Security Program (SP) should be coordinated to provide an integrated defense-in-dept strategy, avoiding duplication of effort and increasing security between IT and IACS Systems'

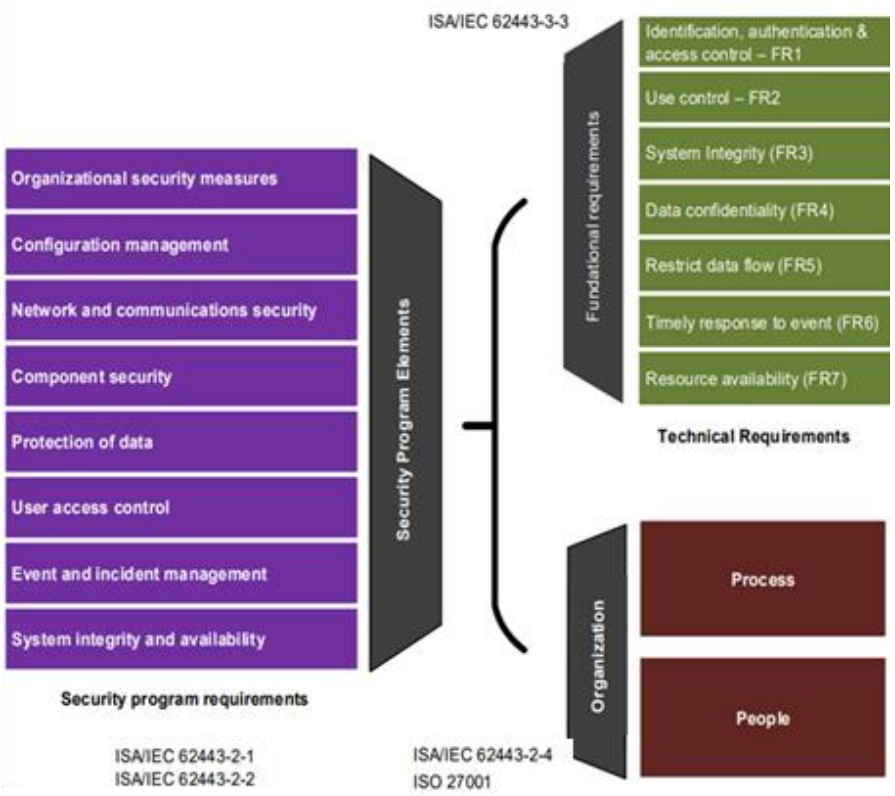
- Where practical, the IACS SP(s) should be compatible with the organizations ISMS
- Complete consistency might not be possible due to conflicting objectives
- Alignment should be improved by aligning security goals and objective

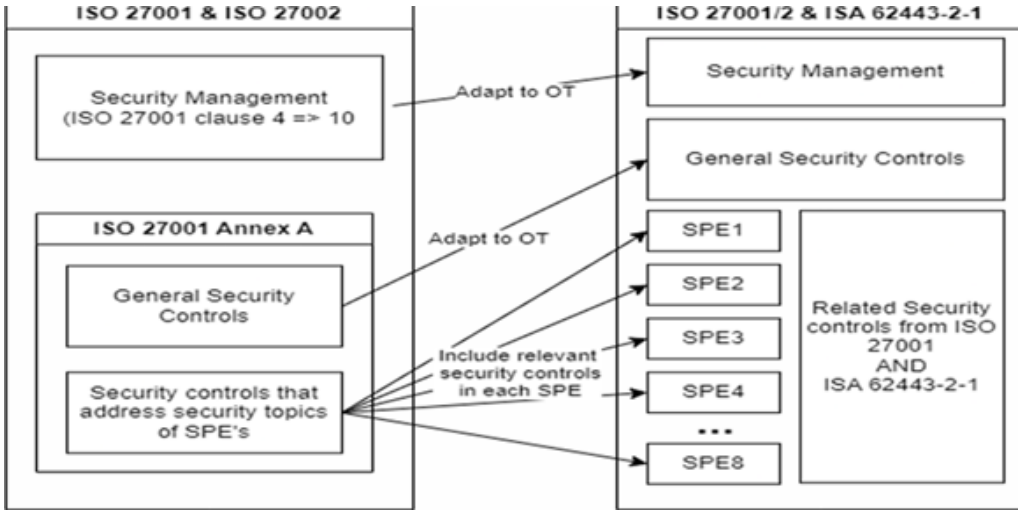
Industry Testimonial Approach

The use ISO27001 is their single management system, ensuring that certification against ISO27001 can be obtained for the entire organization, while still maintaining best-practice controls from ISA/IEC 62443-3-2 and 62443-3-3

- They create a very generic, high-level set of policies that can apply to both IT and OT
- They detail IT Specifics in an IT-Standard and OT-Specific in an OT-Standard, that both comply with the high-level policy
- They decided to use a single 'initial' Risk-Analyses qualitative risk assessment methodology that uses the same methodology for both IT and OT. When 'Detailed Risk Analyses' is required, they revert to the ISA/IEC 62443-3-2 process.
- They created a Statement of applicability that contains both 27002 Controls as 62443-3-3 Controls as applicable

Industry Testimonial
ISMS Structure





Industry Testimonial
Risk Management

- The client established a qualitative risk matrix of 3x4
- Management set the Tolerable Risk to 6
- All Initial Risk-Assessments are done according to ISO27005, but the Detailed Risk Analyses for OT is done according to ISA/IEC62443,
- OT Risks are assigned to a Foundational Requirement
- Security-Level Target per foundational Requirement is calculated:

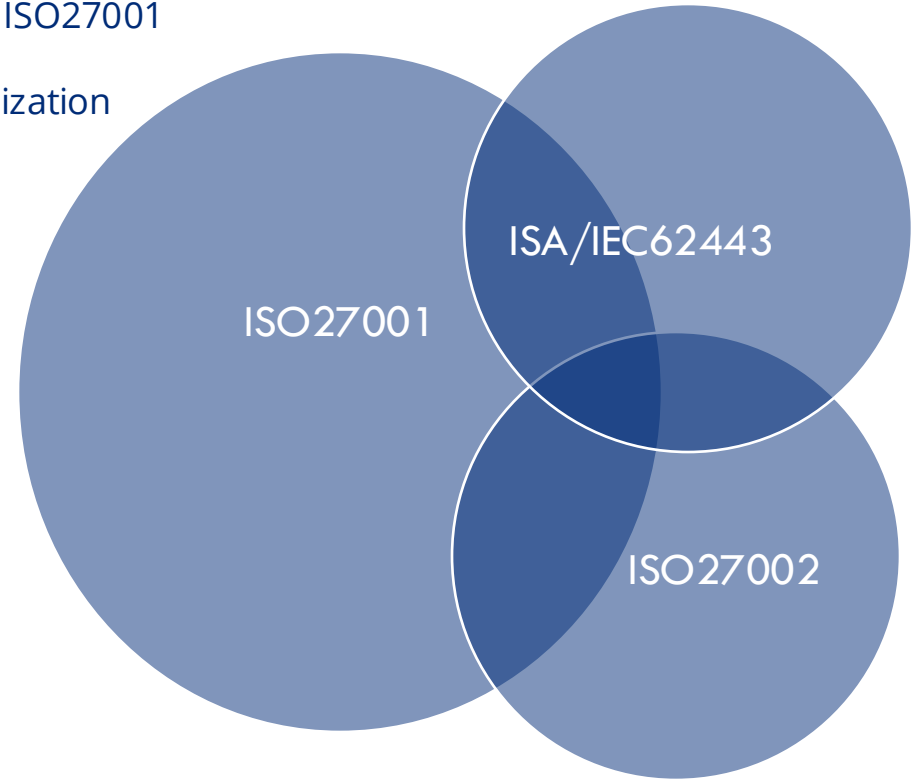
$$CRRF = \frac{\text{Unmitigated Risk}}{\text{Tolerable Risk}}$$

		Consequence			
Likelihood		1	2	3	4
	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12

Industry Testimonial Result

The client will certify its management system according to ISO27001

- Using a SoA based on ISO27002 and ISA/IEC62443
- Using the required scope of the entirety of the organization
- Maintaining specific different needs for IT and OT

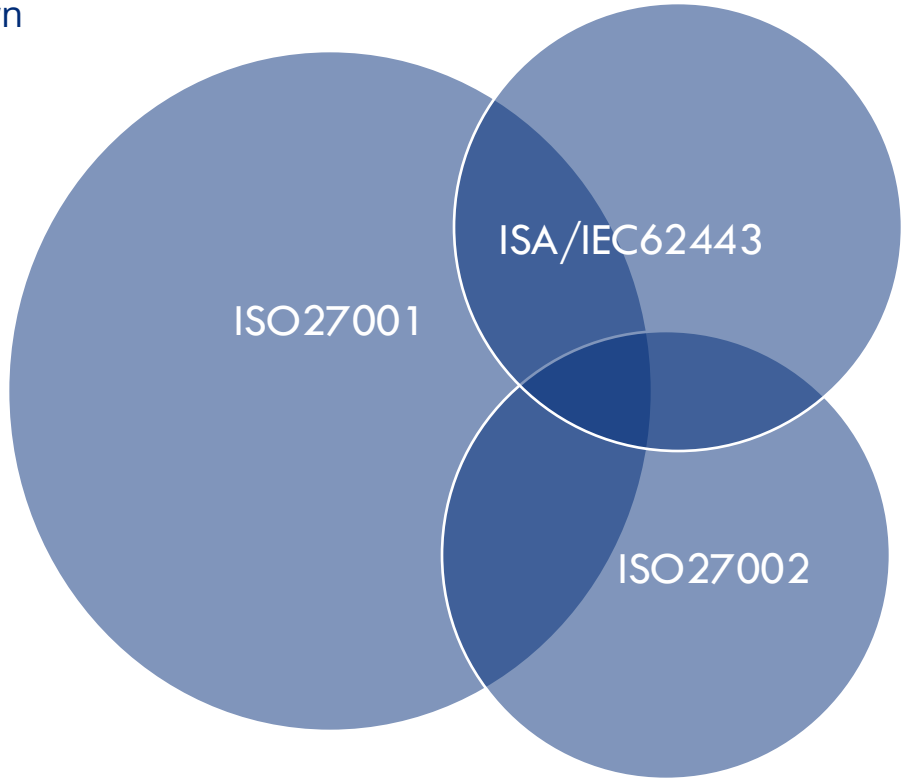


Industry Testimonial
Opportunities for collaboration

- The proposed ISMS approach can be verified by our own Auditors
- We currently don't know if the CCB will accept the SoA
- The CCB-mapping to the ISA/IEC 62443 is outdated

Academics could collaborate with the government to:

- Update the references in the CyFun framework
- Collaborate on acceptable modifications to the ISO27001/27002 Statement of applicability



VINÇOTTE

a kiwa company

Case Study:
Complying with the EU-RED, CRA and the Machinery Directive

Academic Insights, Industrial Impact

The Future of IoT Security Testing

Sam Van Hauwaert

https://www.linkedin.com/in/svanhauwaert/

Industry Testimonial Introduction

- An international system integrator has won a public tender to install (parts of) a public infrastructure on water.
- The tender states that the system must be certified against IEC 62443-3-3 at Security Level 3.
- The tender also states that the system must obtain a CE-Certification.
- The date of delivery of the system is Q1 2028, so the machinery regulation and CRA both apply at full force.

Industry Testimonial
Setting the Scene

- OT and IIoT manufacturers have traditionally been using the combination of ISA/IEC62443-4-1 (SDLC) and ISA/IEC 62443-4-2 (Product Security) against a Security Level

- New European Legislation such as RED-DA (2014/53/EU), The Cyber Resilience Act (2024/2847/EC) and even the new Machinery Regulation (2006/42/EC) enforce Security By Design and Security By Default principles

- ISA/IEC 62443-4-x is a very broad standard, designed to provide a horizontal umbrella for OT, IIoT and Building Automation

- The EU is promoting the creation of a number of Harmonized Standards. For the machinery directive we have +800 Harmonized Standards, For CRA 41 were requested, for RED-DA 1 Harmonized Standard has been published

Industry Testimonial
EN 18031

- EN 18031-1
  - common security requirements for all internet-connected radio equipment, focusing on network protection and service integrity.

- EN 18031-2
  - technical requirements for radio equipment that processes personal, traffic, or location data, including devices like internet-connected radio equipment, childcare devices, toy radio equipment, and wearable radio equipment.

- EN 18031-3
  - radio equipment that processes virtual money or monetary value and is capable of internet communication, focusing on preventing fraud.

Industry Testimonial
Core Principles

- Security By Design, Security Default Configuration
- EN 18031 has 33 requirements, divided in 11 groups

EN 18031 Element Groups	62443-4-1	62443-4-2
Access Control		FR2 - Use Control
Authentication		FR1 - Identification and Authentication
Secure Updates	Secure Update Management (SUM)	
Secure Storage	Security Manageent: SM-6: File Integrity	FR3 - System Integrity
Secure Communications		FR3 - System Integrity
Resilience	SR-2 Threat Model SD-X Security By Design SG-1 Security Guidelines	FR7 - Resource Availibility
Network Monitoring		FR8 - Timely Response to Events
Traffic Control		FR5 - Restricted Data Flow
Confidentiality of Cryptographic Keys	Security Management: SM-8: Control for private keys	FR4 - Data Confidentiality
General Device Capabilities	Security Guidelines (SG) & Secure By Design (partial)	
Cryptography		FR3 - System Integrity

Industry Testimonial
Core Principles

- Let's Zoom in on AUM: Authentication Mechanisms

Industry Testimonial
Opportunities for collaboration

The Academic world could support the Industry by:

- Providing reliable mappings between Industry Standards and Harmonized Standards as they arise.
- Work on tooling for systematic gap-analyses against these legislations and standards

Industry Testimonial Conclusions

- CRA is designed to cover a broad spectrum of devices, not only OT or IIoT
- We don’t know fully know how the requirements for CRA or Machinery Directive will be translated into harmonized standards
- Assuming EN18031-X will be a good comparison, most OT and IIoT products mostly already comply with the vast majority of these requirements.

- The existing ISA/IEC 62443-4-X Standard is a good bases to start developing IoT and IIot. It seems to be covering the vast majority of controls in Security Level 2/3, with some specific requirements that can be included from EN18031-X.

- Vinçotte and KIWA are unable to give 100% correct advise for the best approach to comply with the legal requirements and standard utilization