Setting the Standard for Automation™

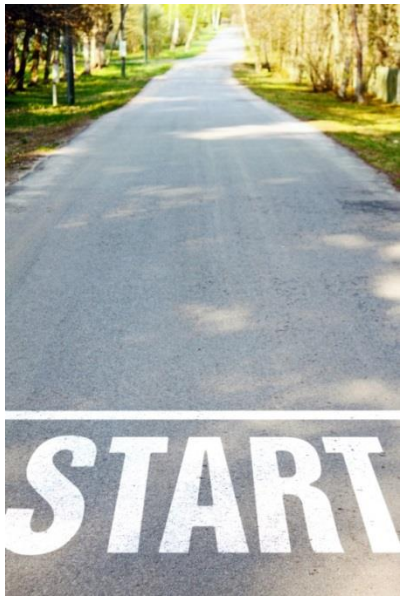
Securing your IP in the OT environment

ARJAN MEIJER
Technical lead
Hudson Cybertec
+31 70 2500717
info@hudsoncybertec.com
www.hudsoncybertec.com

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Agenda

- Introduction
- What is Intellectual property?
- Is it a real problem?
- Why technology alone will fail
- How IEC 62443 standard helps
- Countermeasures, theory to practice
- Conclusions



Introduction (1/2)

- Arjan Meijer
  - Technology lead @ Hudson Cybertec
  - B.eng. Electrical engineering
  - Experience in various security domains
  - Certified ISA/IEC 62443 trainer

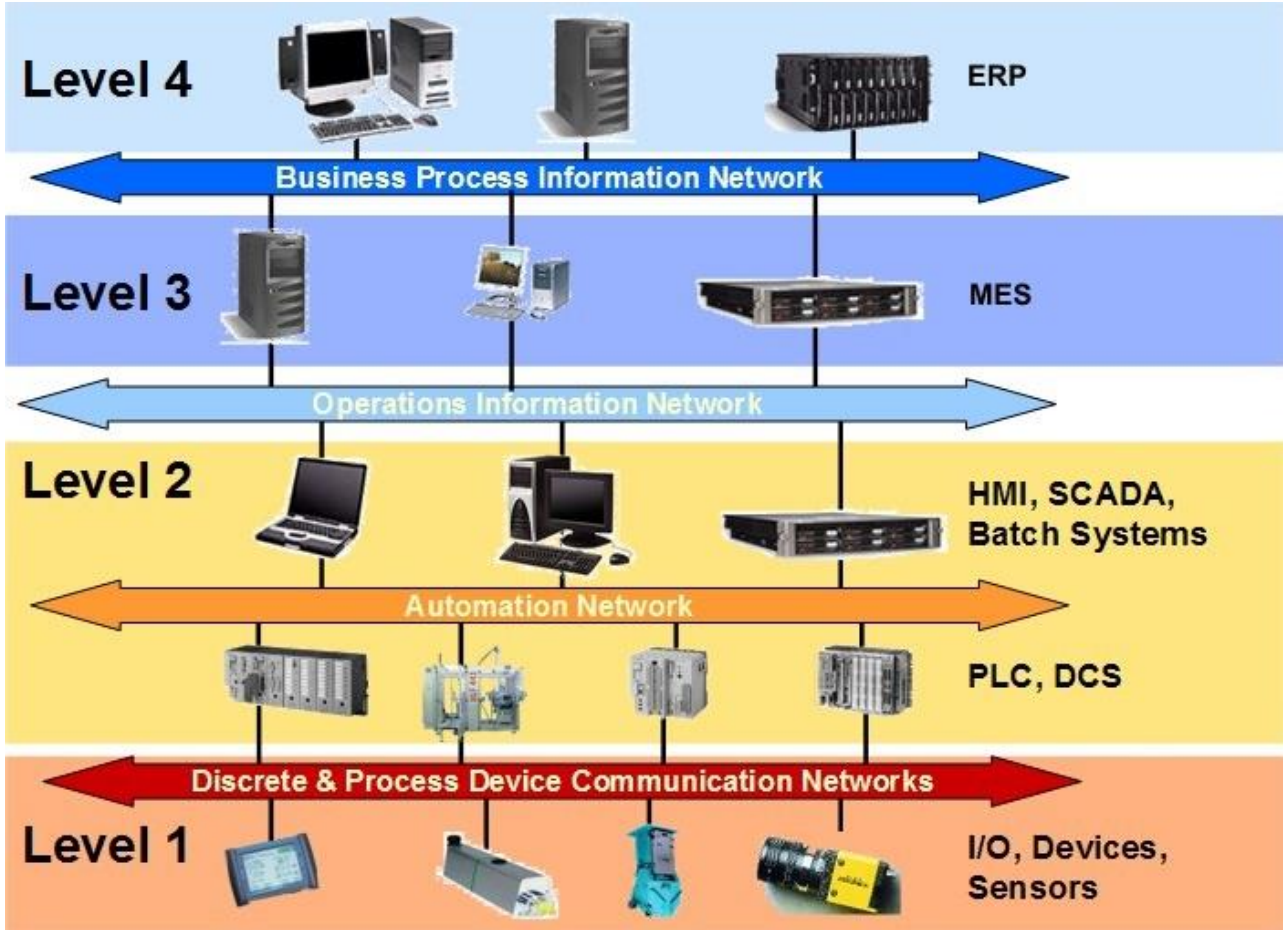
Introduction (2/2)

- Hudson Cybertec
  - Solution Provider for Cyber Security in the OT domain
  - Full focus at Cyber Security and networks in technical environments
    - Specialized knowledge & resources for all companies;
      - In industry
      - Where technical installations are essential for your business
  - Distinctive capacity:
    - Domain knowledge
    - Broad experience with OT & IT Security
    - Subject Matter Expert (SME) for ISA/IEC 62443
    - Extensive expertise in Industrial & Technical Automation
    - Certified ISA/IEC 62443 Training Partner EMEA

What is IP

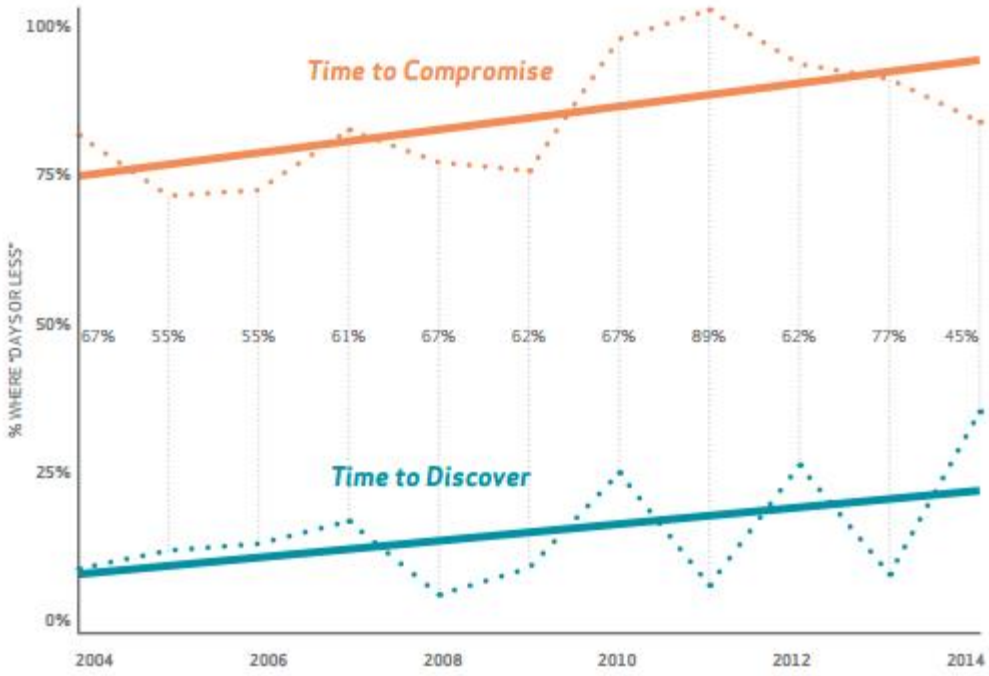
- **Intellectual property** (**IP**) is a term referring to creations of the intellect for which a monopoly is assigned to designated owners by law.

Where does it exists

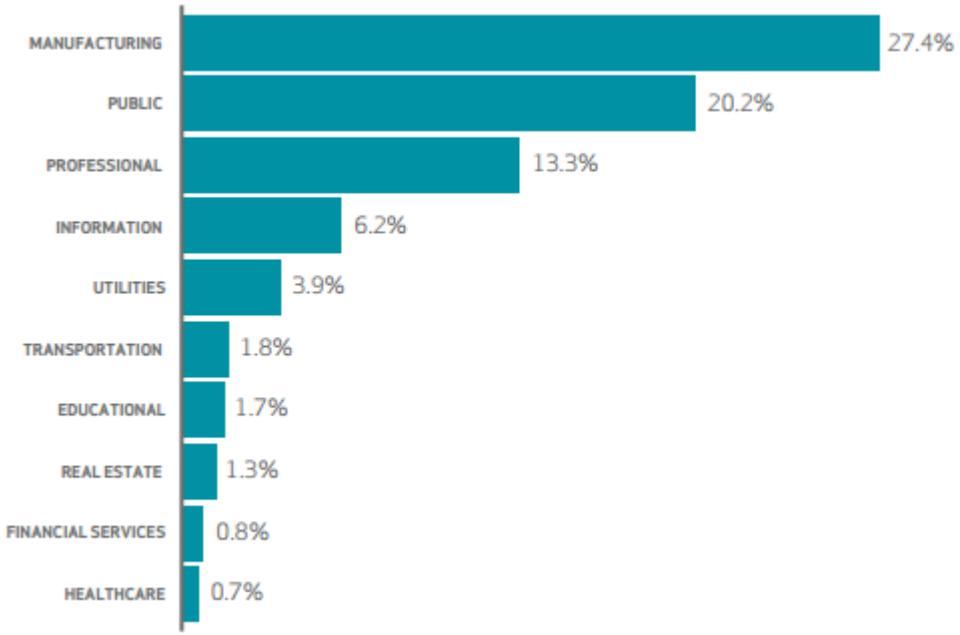


Is it a real problem?

- 2014:
  - Healthcare and pharmaceutical companies have the worst cyber security among Standard & Poor's (S&P) 500;



Talking about cyber espionage

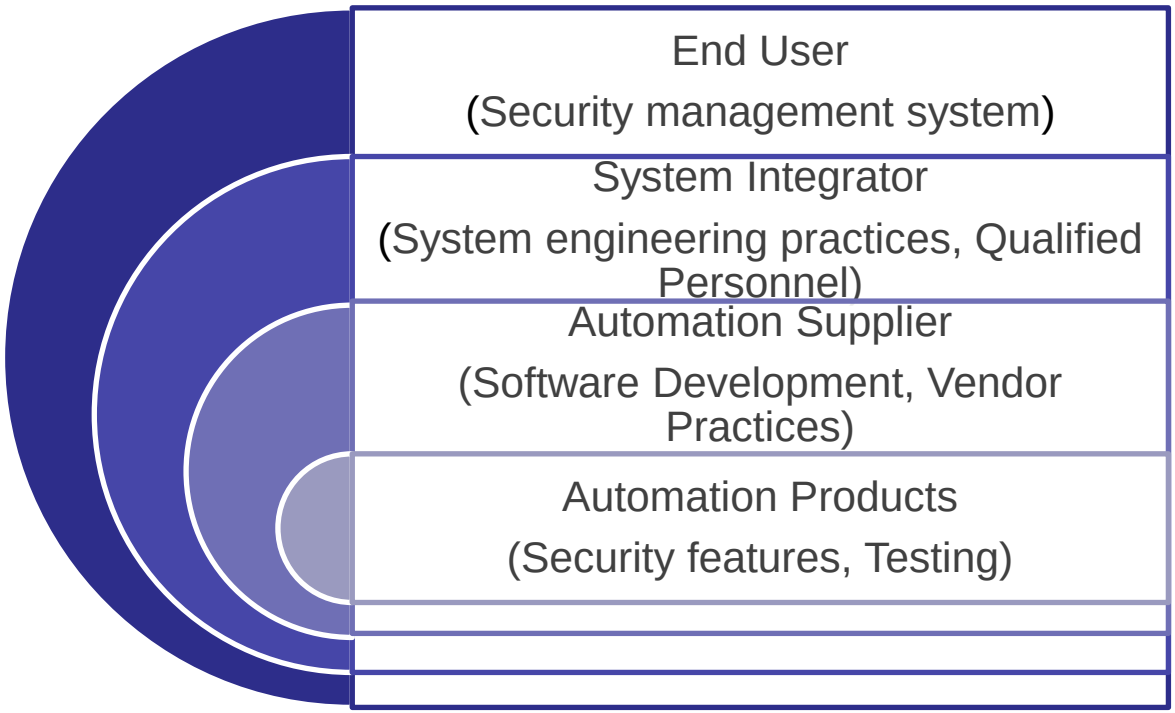


Setting the Standard for Automation™

IEC 62443

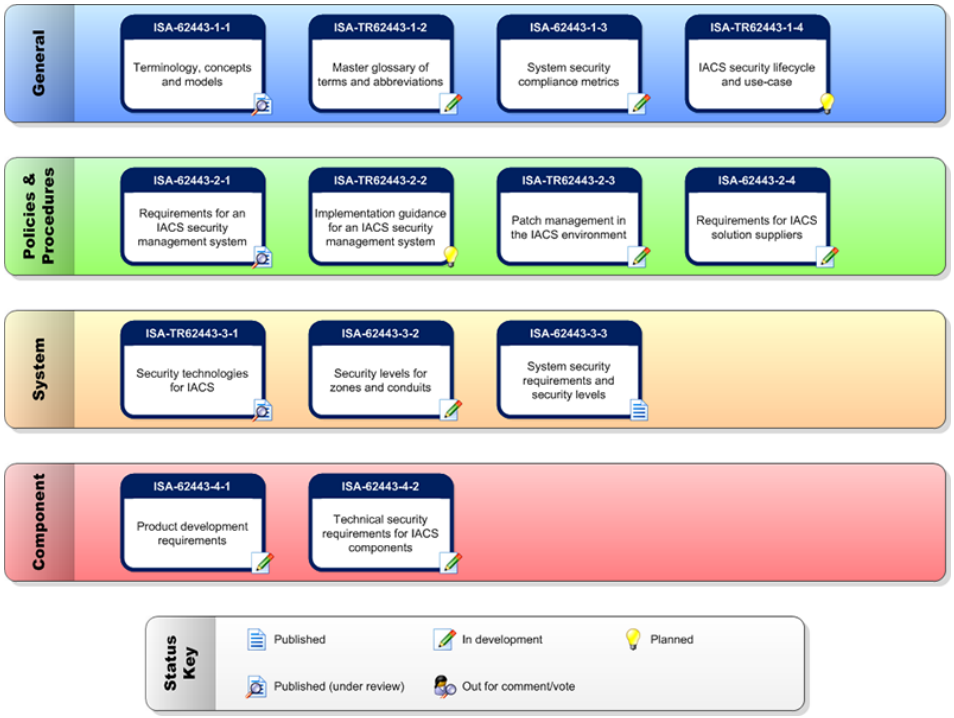
Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Control System Security: Layers of Responsibility



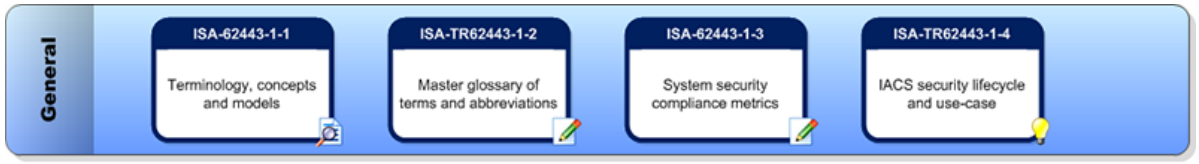
IEC 62443

IEC 62443 Cyber Security standard



IEC 62443: General

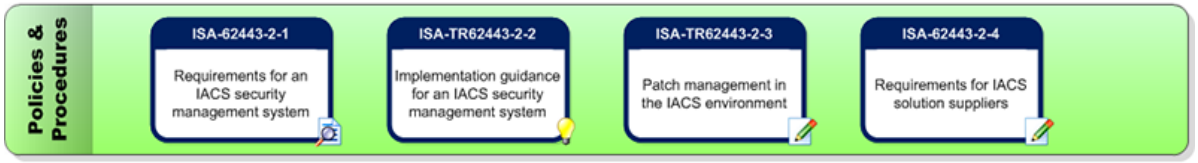
- Everyone needs to speak the same language
  - Vendor, System Integrator & End-user



- IEC 62443 1-1 “Terminology, Concepts and Models”

IEC 62443: Policies and Procedures

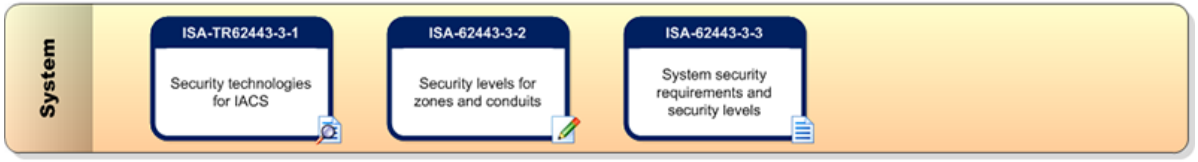
- End-users need to manage the security of their OT



- ISA99/IEC 62443 2-1 “Requirements for an IACS Security Management System
- ISA99/IEC 62443 2-2 “Implementation Guidance for an IACS Security Management System”
- ISA99/IEC 62443 2-4 “Installation and Maintenance Requirements for IACS Suppliers”

IEC 62443: System

- System Integrators need to make a Security Architecture Design



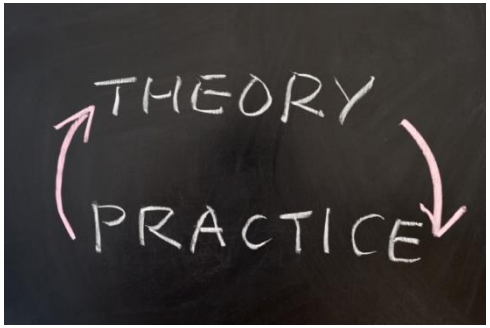
- ISA99/IEC 62443 3-2 “Security Levels for Zones and Conduits”
- ISA99/IEC 62443 3-3 “System Security Requirements and Security Levels”

IEC 62443: Component

- Vendors need to develop secure products

- ISA99/IEC 62443 4.1 “Product Development Requirements”
- ISA99/IEC 62443 4.2 “Technical Security Requirements for IACS Components”
- ISA Secure™ Program

Defending against attacks like Dragonfly



Dragonfly

- Modus operandi
- Some countermeasures

Dragonfly: Spear-Phising

- Email with malicious attachment sent to selected employees in targeted companies
- Exploit of PDF-vuln
- Installing Remote Access Trojan

Dragonfly: Watering Hole-Attack

- Websites likely visited by targeted group were hacked (vulns in open source CMS)
- Redirect to malicious site
- Exploiting JAVA or IE vulns (LightsOutExploitKit)
- Installing Remote Access Trojan

Dragonfly: Trojanized Drivers

- Websites of three ICS-related vendors compromised
- Driver software, which customers could download for ICS-related products, was trojanized and placed on the vendor's sites
- Customers who downloaded (and executed) this driver software also installed Remote Access Trojan functionality

Dragonfly: Payloads

- Disclosing outlook contacts from victim
- Getting system information
- OPC scanner
- ??

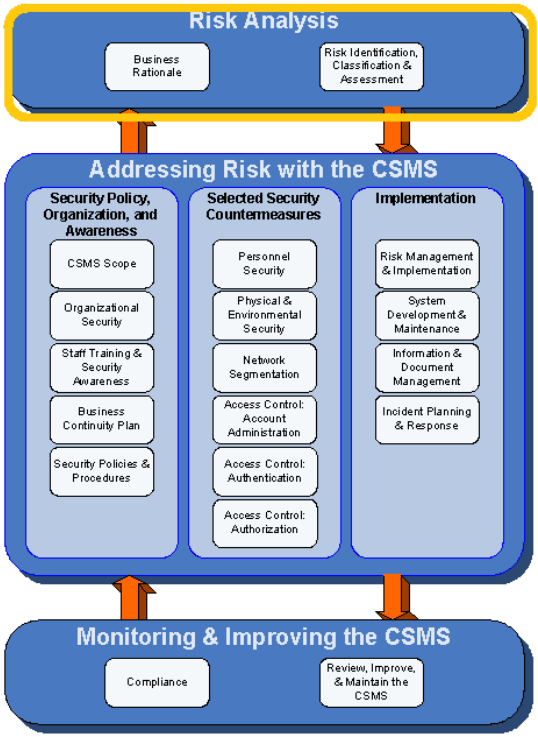
Dragonfly: Goals

- First thought
  - Energysector
- Second thought
  - Dragonfly Malware Could Lead To Drug Counterfeiting

How will IEC 62443 help me

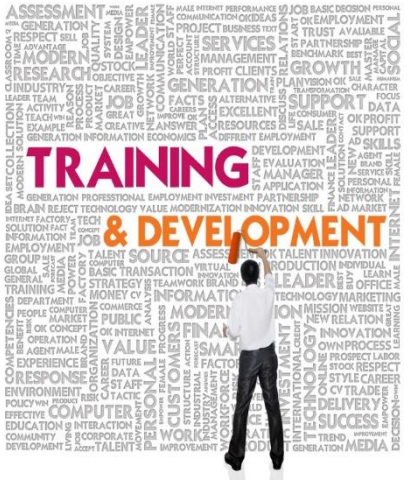
- General:
  - Risk Analysis
  - Identify appropriate countermeasures

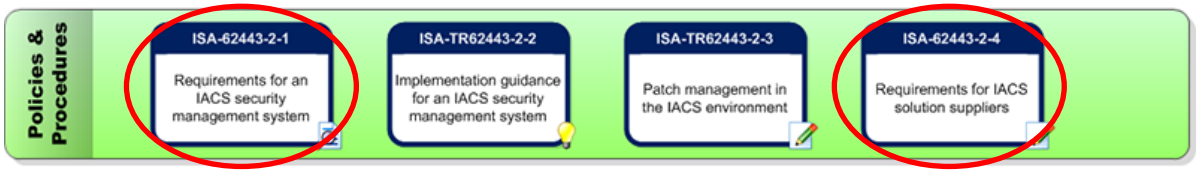
- Addressing the risk with countermeasures



Staff Training and Awareness

- 62443 2-1 : setting objectives and requirements for end-user organization
- 62443 2-4 : contains requirements for your vendor(s)

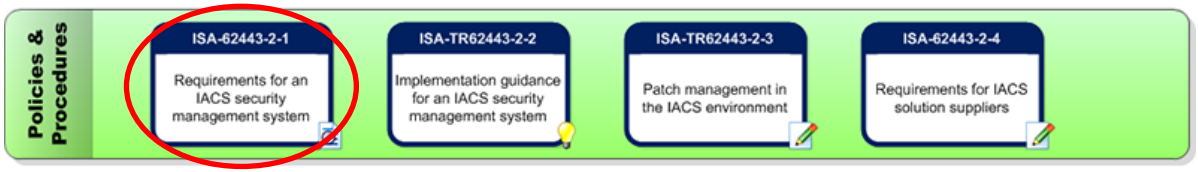


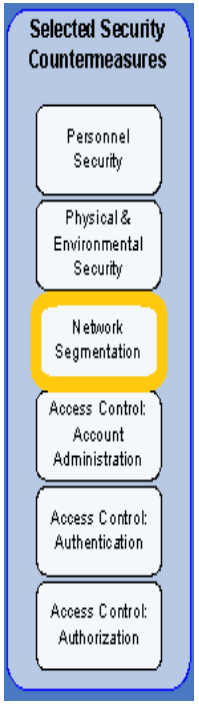


Zones and Conduits (1/4)

- 62443 2-1; countermeasure Network segmentation

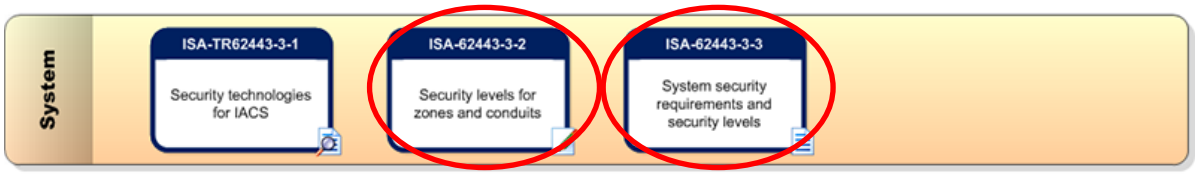
Description	Requirement
Develop the network segmentation architecture	A network segmentation countermeasure strategy employing security zones **shall** be developed for IACS devices based upon the risk level of the IACS.
Employ isolation	High risk IACS **shall** be isolated from the



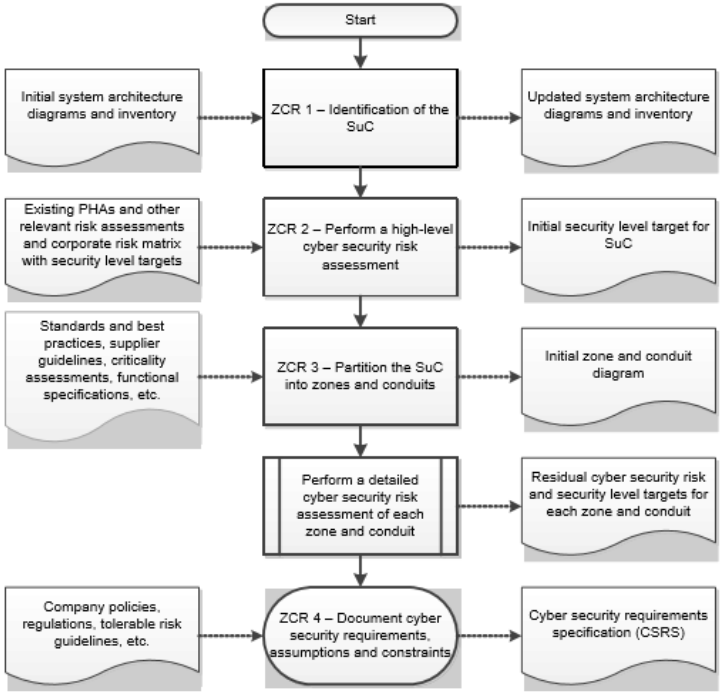


Zones and Conduits (2/4)

- Requirements for defining zones and conduits are provided in ISA-62443 3-2 “Security Levels for Zones and Conduits”
- And the next step: System security requirements & security levels” are provided in ISA-62443 3-3



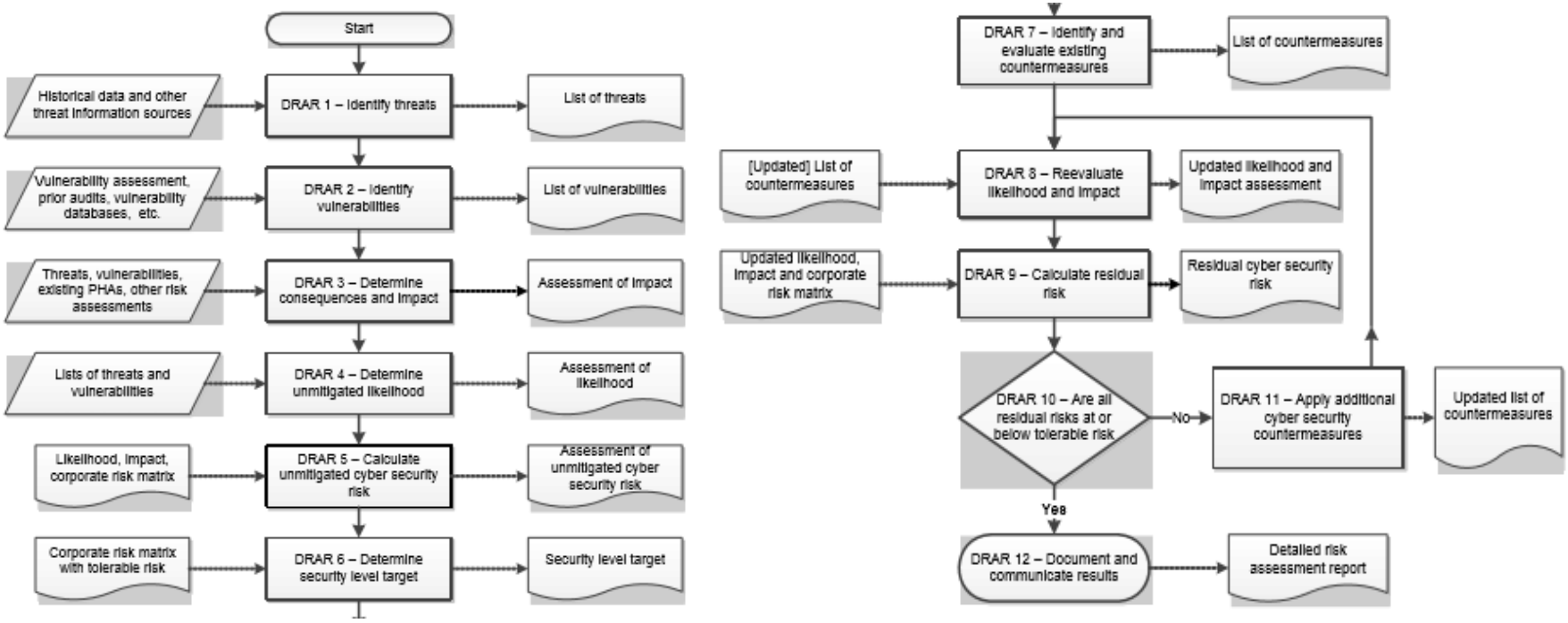
IEC 62443 3-2 Risk assessment process



Zones and Conduits (3/4)

- Zone definition requirements
  - describe the steps you have to take to get a zones & conduits definition
  - describe how to document your zones
  - describe separation criteria for zones
- Security level definition
  - ISA-62443 series define SLs in terms of five different levels (0, 1, 2, 3 and 4), each with an increasing level of security.
  -assign appropriate security level to a zone

IEC 62443 3-2 Risk assessment process

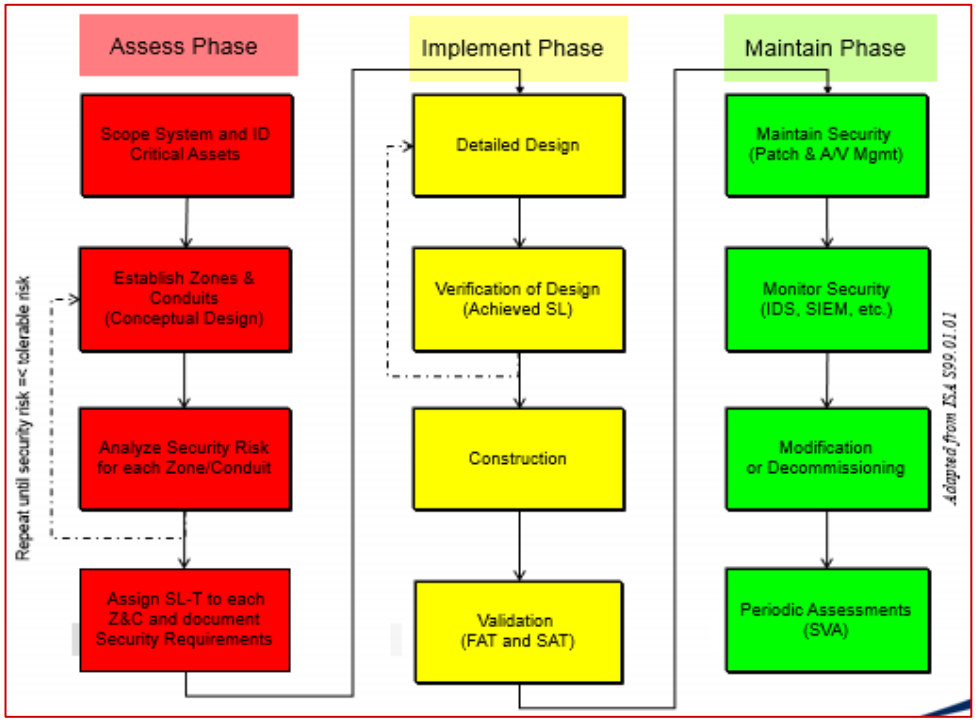


Zones and Conduits (4/4)

- Example: Restrict Data Flow

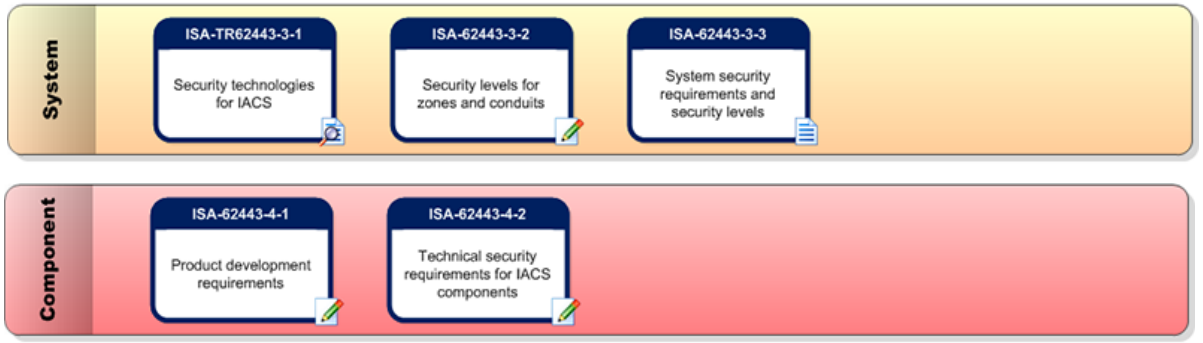
Security Requirements and Requirement Enhancements (RE)	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
SR 5.1 – Network segmentation	✓	✓	✓	✓
RE (1) Physical network segmentation		✓	✓	✓
RE (2) Independence from non-control system networks			✓	✓
RE (3) Logical and physical isolation of critical networks				✓
SR 5.2 – Zone boundary protection	✓	✓	✓	✓
RE (1) Deny by default, allow by exception		✓	✓	✓

ISA/IEC 62443 Security Lifecycle



ISA Secure (1/2)

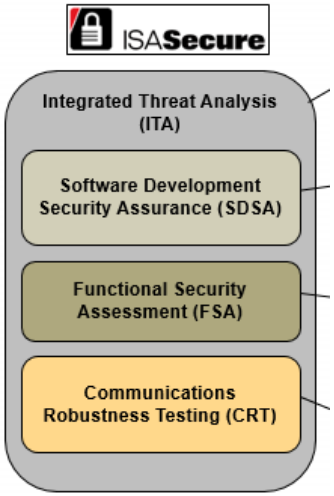
- Structured, auditable, repeatable, approach to evaluating security of an ICS product
- Assurance that automation products, systems and suppliers meet baseline

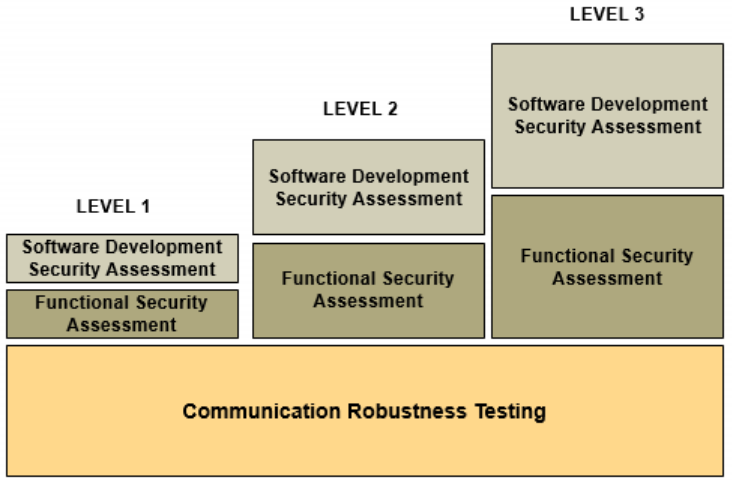


ISASecure

ISASecure

ISA Secure (2/2)





- See www.isasecure.org for more information and list of certified products etc.

Finding the balance

- Or else…

Taking countermeasures (1/3)

- Create security awareness / knowledge at all levels of the organization
  - Gives a state of mind encompassing (cyber) security
  - Provide training

- Assess/audit the status of your process control network
  - Starting point to improve the cyber security
  - Assessment gives insight in the current security status, including
    - Technique
    - Organization
    - Physical security
    - Available knowledge

Taking countermeasures (2/3)

- Implement Cyber Security Management
  - Risk analysis
    - Inventorize actual threat level & potential business impact of incidents
  - Cyber Security Management System
    - Encompass Process Control Security as integral part of operational management
  - Risk Management
    - Make ICS / TA security part of new project requirements
    - Link cyber risks to business processes

Taking countermeasures (3/3)

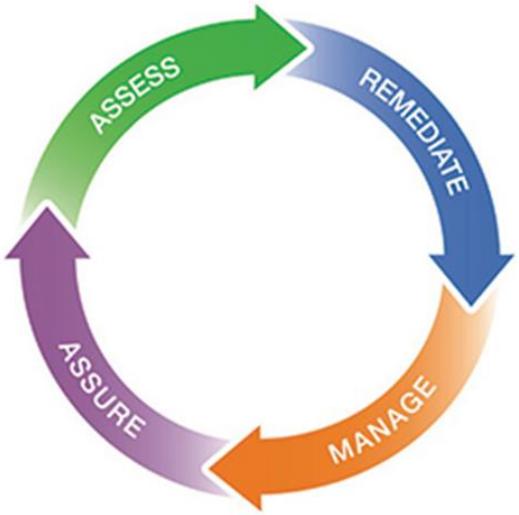
- Embrace ISA99/IEC 62443 standard
  - for Industrial Automation and Control Systems Security

- Know your network!
  - Know what is used (assets, protocols, …)
  - Update “as-built” documentation

Conclusions

- ISA99/IEC 62443 gives direction
- ISA99/IEC 62443 anchors security within organization
- ISA99/IEC 62443 gives guidance for Security by Design

- Security is a process



Standards improve your cyber security level!

Setting the Standard for Automation™

Fighting cyber espionage with industry standards

HUDSON CYBERTEC
Cyber Security - Technical Automation

ARJAN MEIJER
Security Consultant
Hudson Cybertec

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits