DELTAV™

Addressing the Foundational Requirements of IEC 62443 for Industrial Automation Control Systems

EMERSON

Prevention is Better than the Cure

- LockerGoga Ransomware
- 170 sites in 40 Countries
- 22,000 infected computers
- 4 months later, still not fully recovered
- Recovery cost expected to exceed $75M

BUSINESS / NEWS / EUROPE

Lower Prices And Cyber Attack Take Toll On Norsk Hydro's Q2 Financial Results

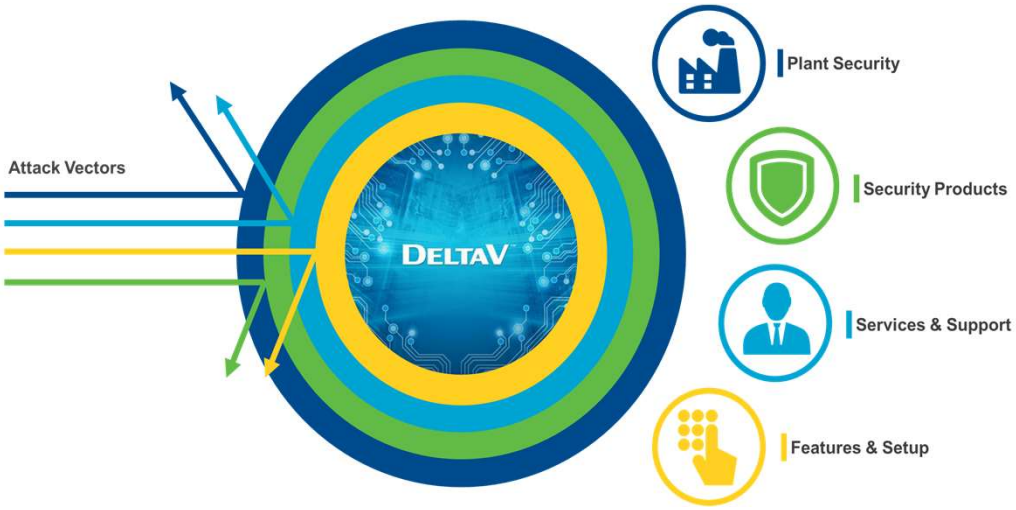
- Source: Norsk Hydro

BS EN61511 2017

…….. includes a mandatory requirement to risk assess any cybersecurity vulnerabilities of the Safety Instrumented System (Clause 8.2.4) and implement “mitigating” strategies to prevent or minimise their consequences

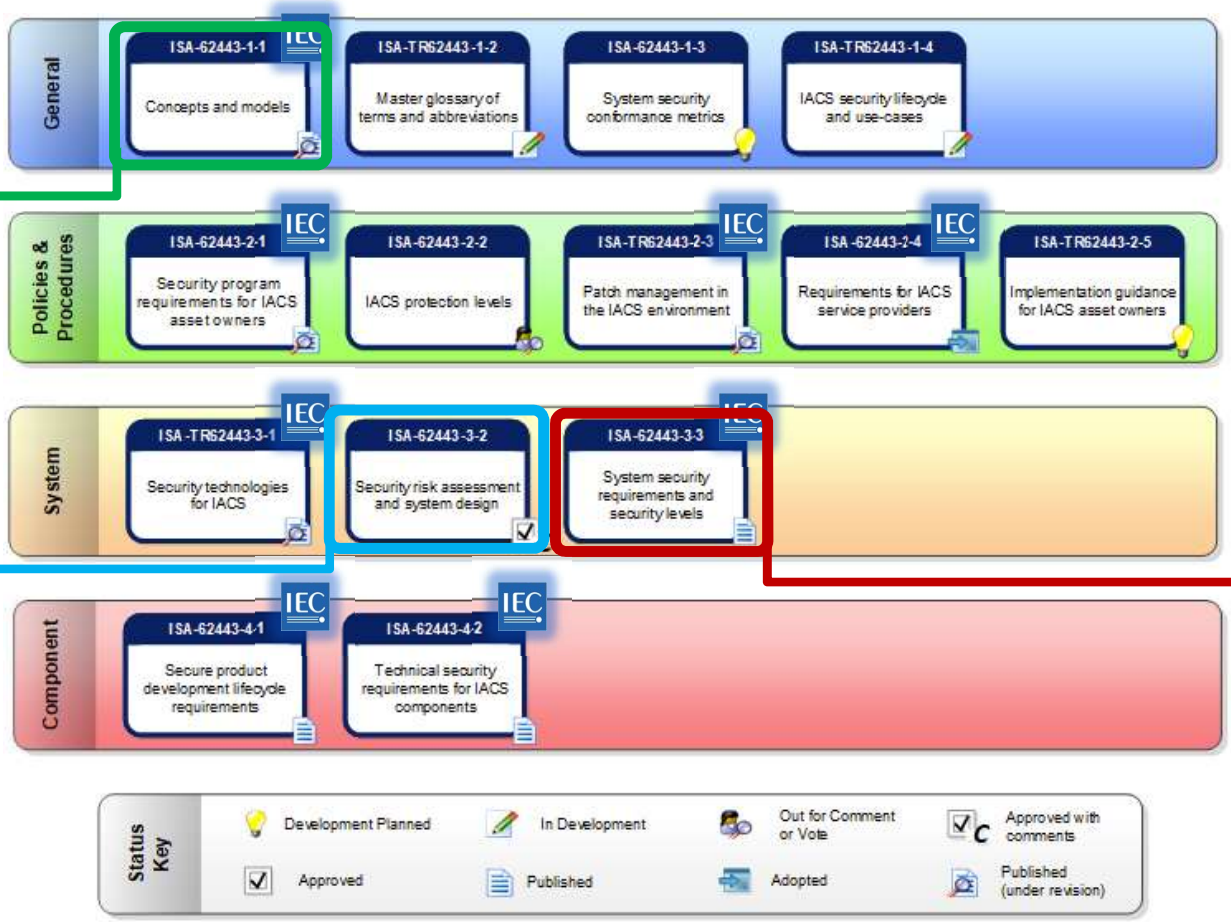
To comply ISA/IEC62443 is referenced as a means to be able to ASSESS, IMPLEMENT and MAINTAIN a suitable Defence in Depth Strategy for the Industrial Automation Control System (IACS) including the Safety Instrumented System (SIS).

(OG0086 Edition 2, regarded as Good Practice by the HSE, introduces concepts and models described and applied in more detail in the ISA/IEC62443 series of standards)



Overview of ISA / IEC 62443

Foundational requirements contain methods encompassing People, Processes and Technology to attain required IACS Security Levels (SL's)



Defines requirements for Risk Assessing both existing IACS and new designs

Defines technical requirements for IACS security

IEC 62443 Foundational Requirements

"Based on the target security level (SL-T) determined and using the processes defined in ISA62443-3-2 the IACS shall provide the necessary capabilities to…..

- FR 1- Access Control (AC)

…reliably identify and authenticate all users (humans, software processes and devices) attempting to access the ICS."

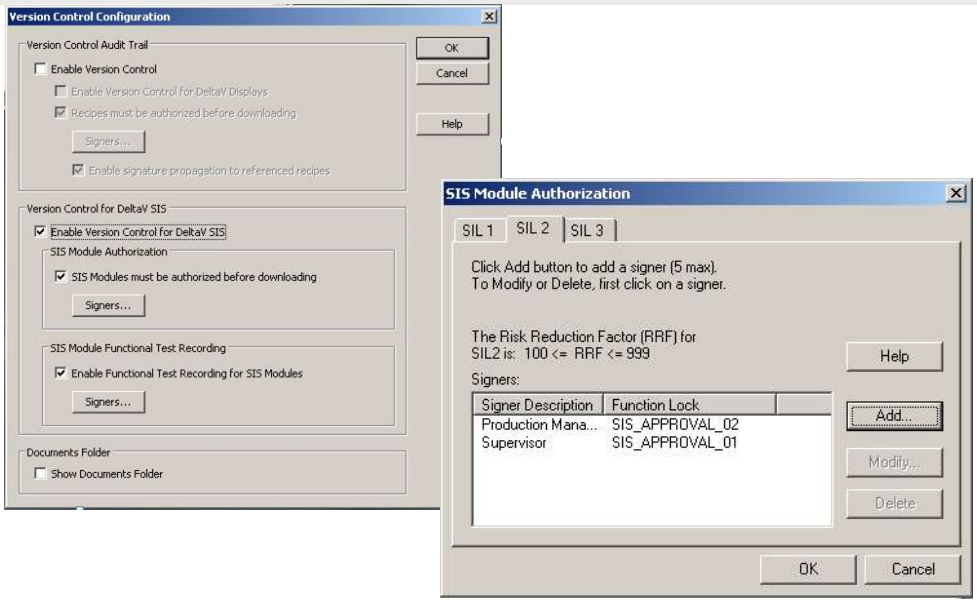
- FR 2- Use Control

…enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the system or assets and monitor the use of these privileges."

IEC 62443 Foundational Requirements

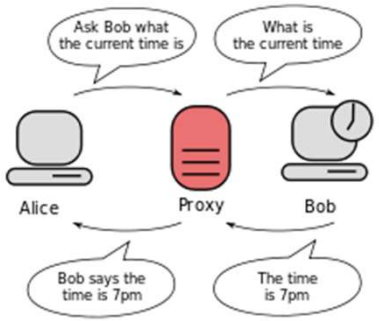
- FR 3- System Integrity

…ensure the integrity of the IACS to prevent unauthorised manipulation."



- FR 4 -Data Confidentiality (DC)

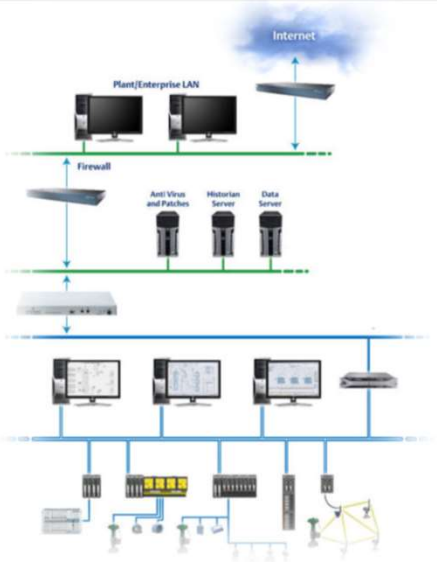
…ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorised disclosure."



IEC 62443 Foundational Requirements

- FR 5- Restrict Data Flow (RDF)

…segment the control system via zones and conduits to limit the unnecessary flow data.”



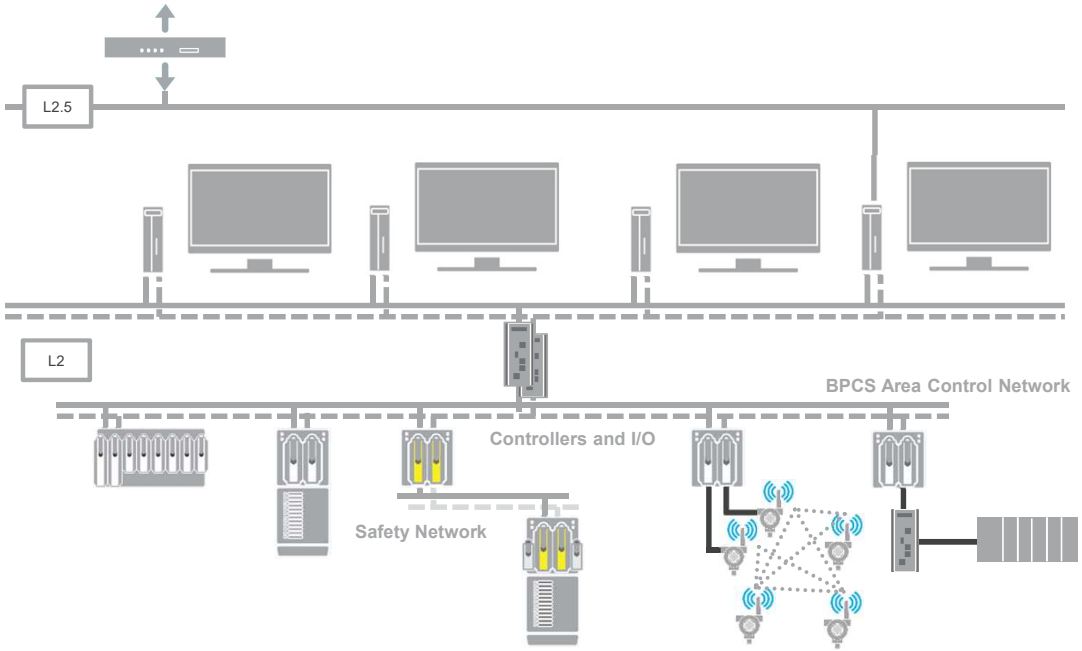
- FR 6- Timely Response to Events (TRE)

…respond to security violations by notifying the proper authority reporting needed evidence of the violation and taking timely corrective action when incidents occur.”

IEC 62443 Foundational Requirements

- FR 7- Resource Availability (RA)

…ensure the availability of the control system against the degradation or denial of essential services."



IEC 62443 Foundational Requirements

Foundational Requirements	SL-1	SL-2	SL-3	SL-4
FR 1 – Identification and Authentication Control	14	25	31	33
FR 2 – Use Control	15	19	28	31
FR 3 – System Integrity	6	10	16	19
FR 4 – Data Confidentiality	2	4	5	6
FR 5 – Restricted Data Flow	4	6	11	11
FR 6 – Timely Response to Event	1	2	3	3
FR 7 – Network Resource Availability	7	10	13	13

Security Level 0: No specific requirements or security protection necessary

Security Level 1: Protection against casual or coincidental violation

Security Level 2: Protection against intentional violation using simple means with low resources generic skills and low motivation

Security Level 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation

Security Level 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Determining How Best to Protect a System

- First understand the risk
  - Identify critical assets
  - Determine the realistic threats
  - Identify the existing vulnerabilities
  - Understand the consequence of compromise
  - Assess the effectiveness of current safeguards

- Develop a plan to address unacceptable risk
  - Evaluate any existing countermeasures
  - Recommend additional countermeasures
  - Recommend changes to current policies and procedures
  - Prioritise recommendations (Based on risk)
  - Evaluate cost. Complexity versus effectiveness

For more information go to: www.Emerson.com/Cybersecurity