Paulo Oliveira

Functional Safety and Cybersecurity

Safe and Secure by design – the challenges and road ahead

Functional Safety and Cybersecurity

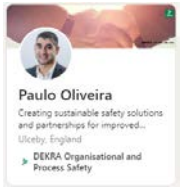
01 Safe + Secure by design - idealistic or achievable?

02 The real challenge…

03 What’s out there?

04 …the current work

05 What’s next?



www.linkedin.com/in/paulo-oliveira-9011a110

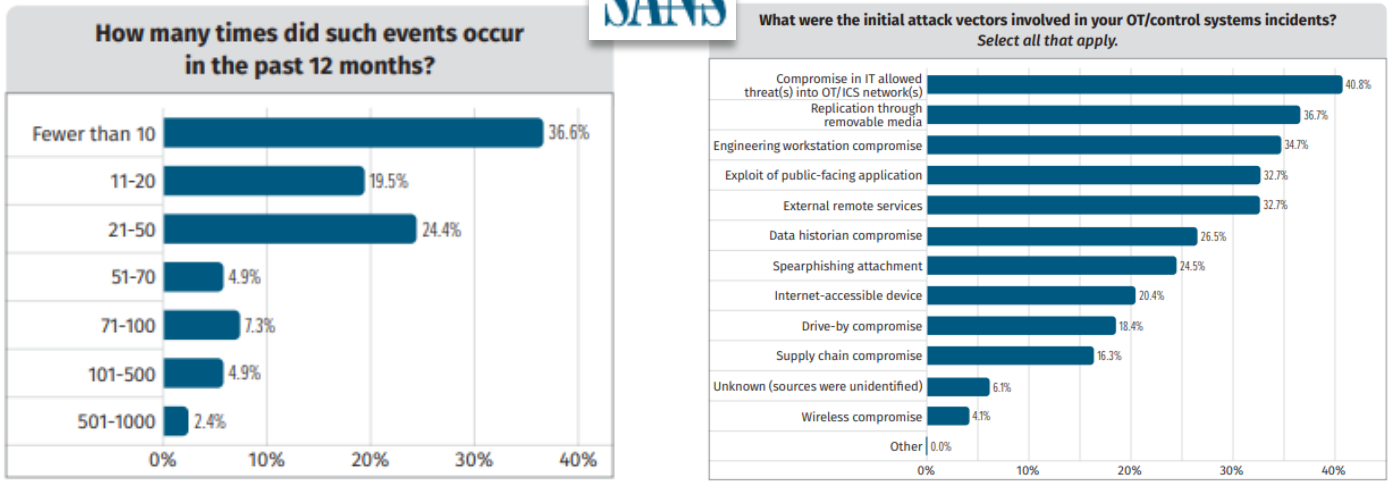
Safe + Secure - ideal or achievable output?

Functional Safety and Cybersecurity

- Functional Safety standards identifying the need to ensure that safety measures are supported by security (including cybersecurity) measures

  (IEC61508 clause 7.5.2.2 , IC61511 clause 8.2.4 & Clause 11.2.12)

- Cybersecurity is an increasing concern to Operational Technology (OT) and overall IT systems

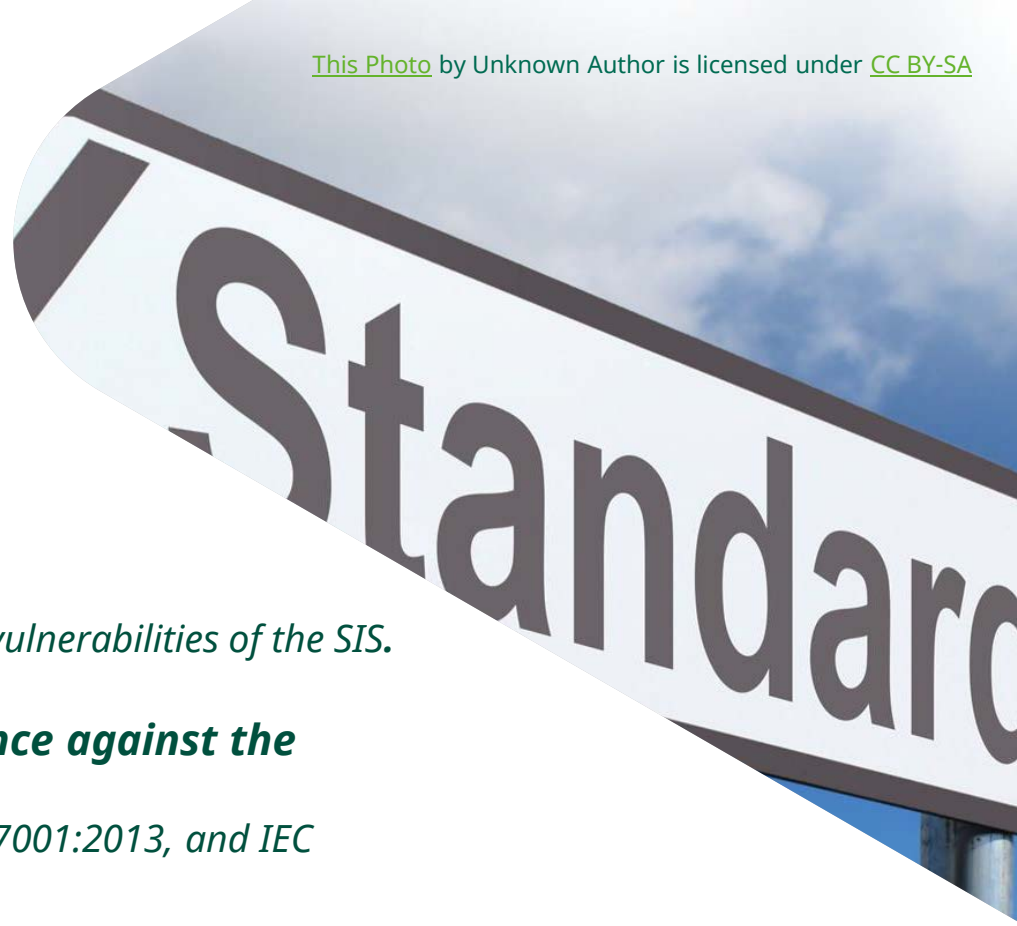


https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html

The need for safe and secure systems is now at the centre of integrity in operations (any sector)

But how do you bring these together?

Guidance Detail



IEC61508 clause 7.5.2.2

*If **security threats** have been **identified**, then a **vulnerability analysis** should be undertaken in order to **specify security requirements**.*
NOTE Guidance is given in IEC 62443 series.

IEC61511 clause 8.2.4

*A **security risk assessment shall be carried out** to identify the security vulnerabilities of the SIS.*

IEC61511 Clause 11.2.12

*The **design of the SIS** shall be such that it provides **the necessary resilience against the identified security risks** (see 8.2.4)*
NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.

Cybersecurity Act REGULATION (EU) 2019/881

*"(12) Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes **should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes** to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('**security-by-design**'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation."*

The real challenge…

"Tunnel vision" vs Holistic approach

I'm designing a new safety system or product… and I need the data to be available

Ok … what guidance do I use to achieve a **safe and secure** device

…and do they consider safety requirements?

If your product or system has connectivity and data exchange capability , you need to make it Cybersecure

Here's a list of Cysec standards you need to comply

No… just CySec

What’s out there…

Pick and mix?

- Cyber Resilience Act
- Machinery Safety Act
- **ISA/IEC62443 Series**
- **ISA TR84.00.09-2013 Security Countermeasures related to Safety Instrumented systems**
- **HSE OG 0086**
- NIST SSDF Security System Development Framework
- IEEE 1686 Intelligent Electronic Devices Cybersecurity Capabilities
- NER CIP – Critical infrastructure Protection Reliability Stds
- IPC 2591- Connected Factory Exchange
- RTCA DO-356/ED203 Airworthiness Security methods
- UL2900 Software Cybersecurity for Network- Connected prdt
- NIST SP800-82 Guide to Operational Technology Security
- **NIST CSF Cybersecurity Framework**
- **NSCS CAF**
- **IET code of practice – Cyber Security and Safety**
- **IEC TR 63069***
- **SAE JA7496 – Cyber Physical Systems Security***
- and more….

The real challenge…

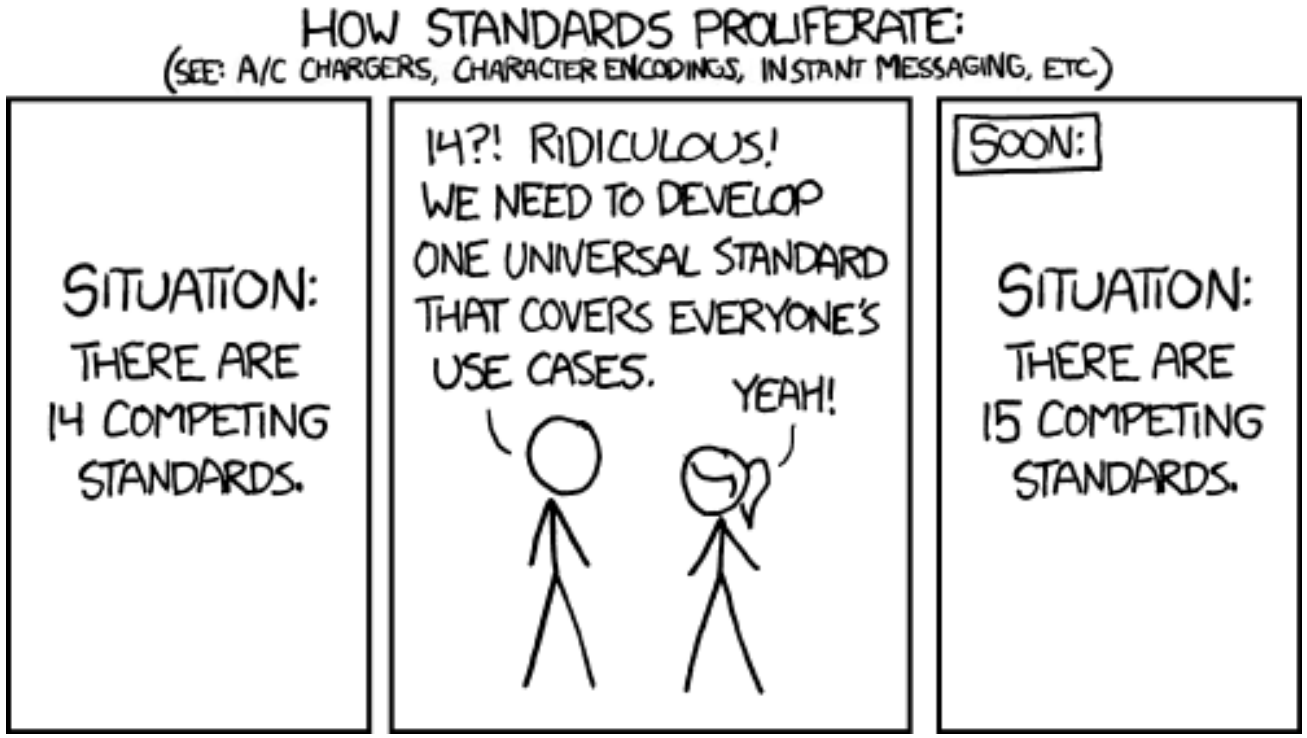
"Tunnel vision" vs Holistic approach

We need to a CySec approach that fits within FS needs… let's create some guidance

CySec applies to everything so just fit the FS needs to the CySec approach… let's create some guidance

This sounds familiar…

Rabbit Hole vs Competing standards



From https://imgs.xkcd.com/comics/standards.png

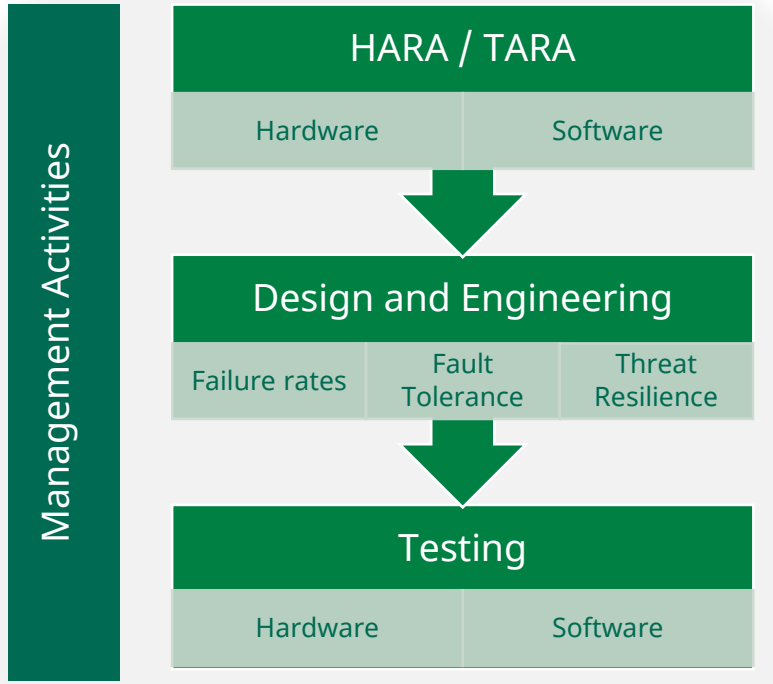
The real challenge…

"Tunnel vision" vs Holistic approach

Let's just **keep it together**!

How?…focus on system integrity overall…

- what safety and cyber capability do I need to implement?
- what activities need to happen together or separate?
- What conflicting requirements do we have?



Current Work

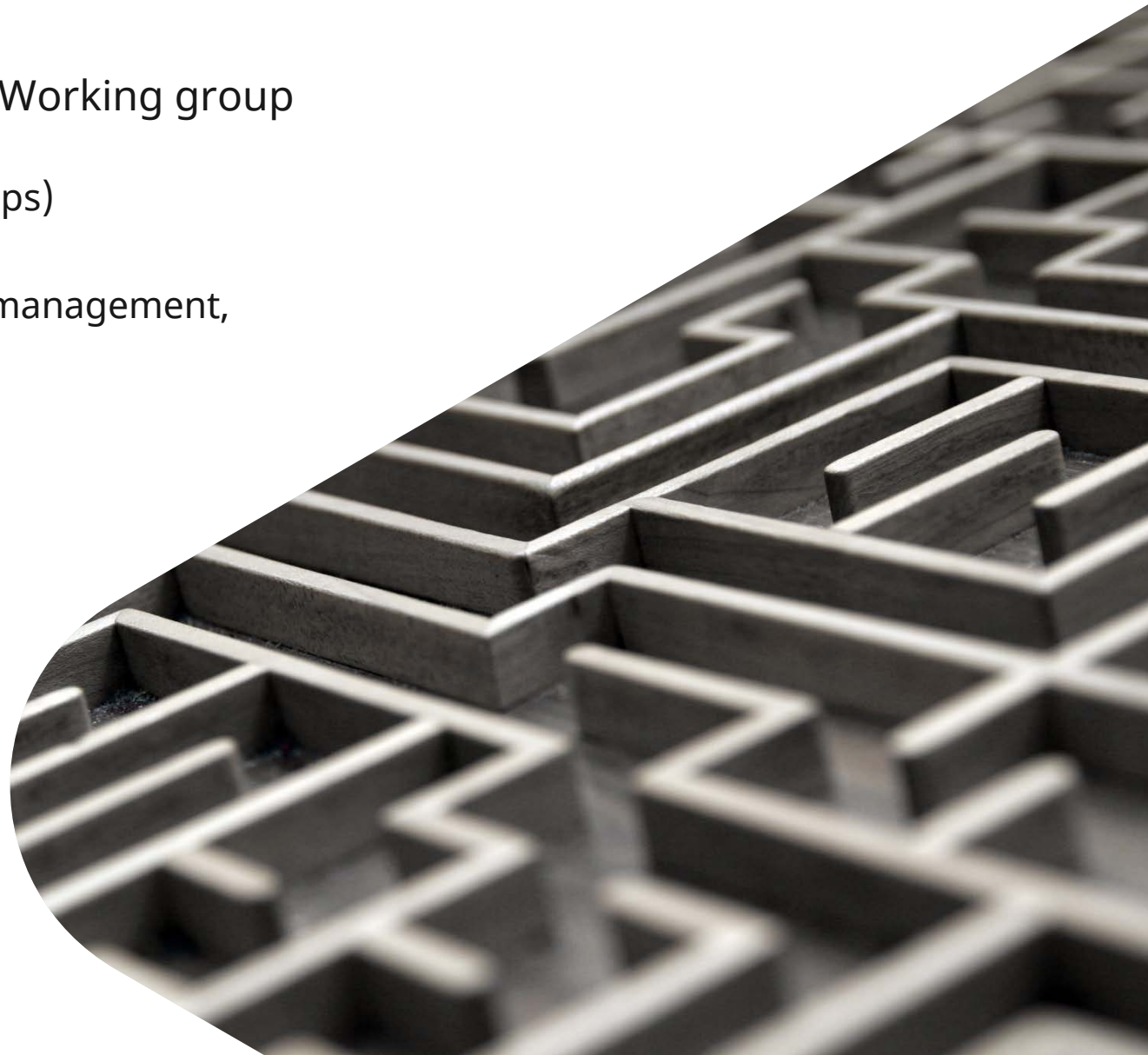
Overview

- BSI Functional Safety and Cybersecurity Ad Hoc Working group
- (inc. end-users, product manufacturers, technical experts, ISA/BSI)
  - Baseline assumptions causing the “division” (5 groups)
    - Properties
    - Ongoing maintenance/monitoring and change management,
    - Interfaces,
    - Supply chain
    - Configuration

- IEC62443 development and update (ongoing)

- Multiple iterations on peripheral guidance documents (e.g. IET Code of practice) to “catch up” with developments

- Many (too many?) groups trying to figure out what safe+secure means for their “silo” sector/application



What’s next?

(BSI AHWG perspective)

- Develop **useable whitepapers/technical position documents** to share with representative groups to develop “new paradigm” – integration from start

- Start with “assumptions”, then move to other areas such as (for example:
  - Risk Assessment
  - Testing
  - Management activities (systematic capability)

Not intending to create yet another standard!

Just help and interpretation on how to apply current guidance out there, in real life.

Safe +Secure

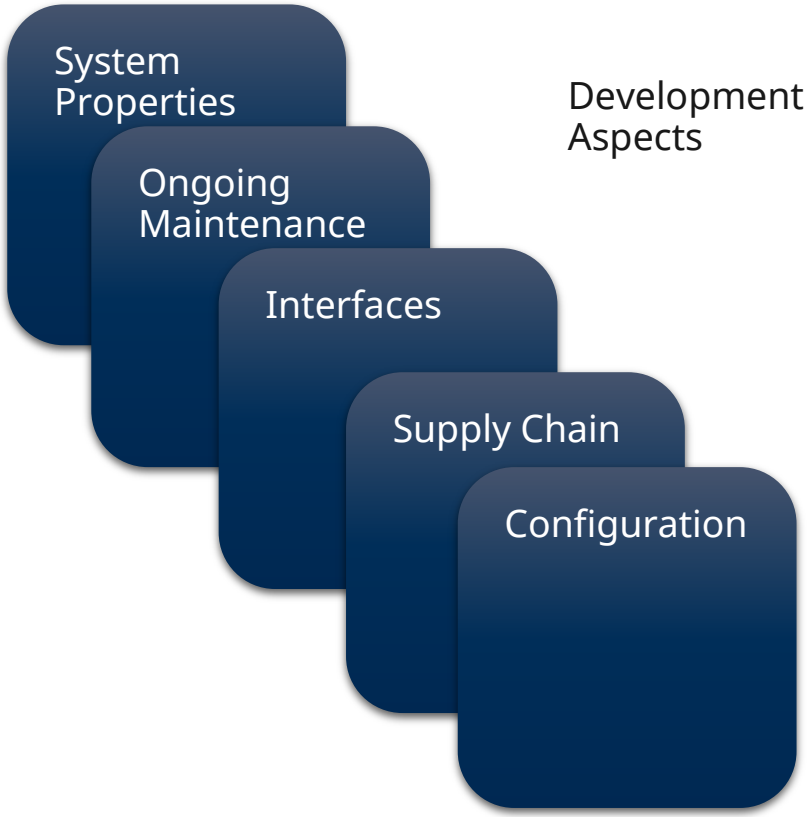
From idea to use

BSI GEL/065 ADWG

Current status

Objective: Safe and Secure by design

The "Assumption"	Starting Point
The Anti-thesis	
Origin of the Assumption	Context
Pitfalls if Assumption is adopted	What can go wrong?
Symptoms of need to improve	
"So What"?	What does the action to improve look like in real life?
Corrective Actions	



Development Aspects

Assumptions

Example (not finalised)

Objective: Safe and Secure by design

"If my system was secure enough yesterday it will be secure enough tomorrow as well"

security measures degrade
and **cannot be Static** ("for once and for all")

Starting Point

Security environment/consequent use cases are assumed to be **static**; provides a **fixed requirement** for contracts that's why attractive/ bounds contract risk

Context

system security becomes increasingly ineffective (degraded) and unable to cope with emergent threats

No periodic/scheduled review
No verifying audit outcomes
No updates to security approach/scheme

What can go wrong?

Symptoms

Security breaches may occur, which in turn could undermine safety. Security landscape changes much more quickly than functional safety.

"So What?"

Security measures updates;
Review latest developments / environment changes;
Design system for change

What does the action to improve look like in real life?

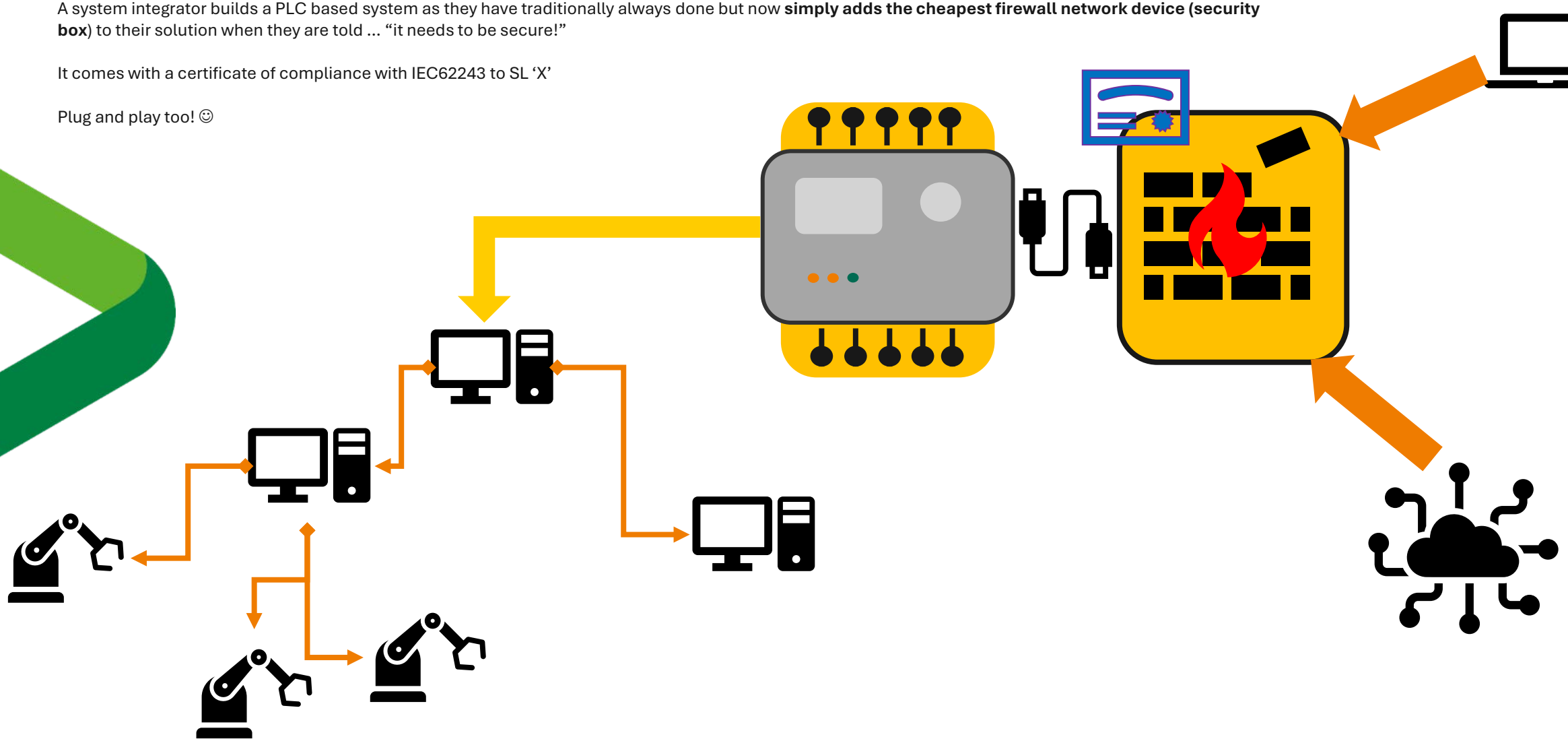
Study Case

The “security box” conundrum

A system integrator builds a PLC based system as they have traditionally always done but now **simply adds the cheapest firewall network device (security box**) to their solution when they are told … “it needs to be secure!”

It comes with a certificate of compliance with IEC62243 to SL ‘X’

Plug and play too! ☺

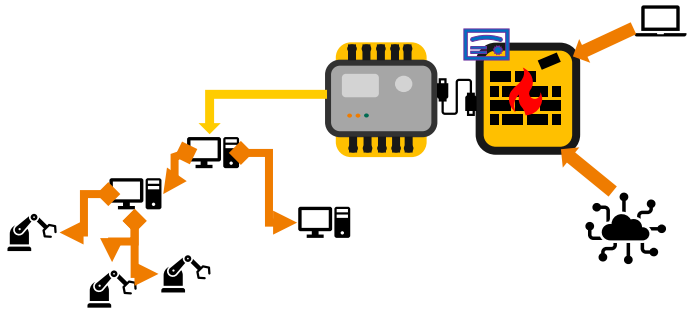


Study Case

The “security box” conundrum

A system integrator builds a PLC based system as they have traditionally always done but now **simply adds the cheapest firewall network device (security box**) to their solution when they are told … “it needs to be secure!”

1. Are the **necessary features** enabled?
2. Do we understand what security features are needed to achieve the **security objectives and outcomes**?
3. Who **verifies the achievement of Security Level ‘X’**? How is Achievement of SL ‘X’ verified/validated as part of the mandatory FS Assessment activities?
4. How and who **manages changes** to the protection scheme? i.e. How is the **security measure evolving in line with the threats**?
5. Are we **confident** that the “Security box” isn’t a “ghost barrier”, i.e. there but only in spirit?
    - Do we understand the impact of rework and redefinition of security measures/requirements at latter project stages? (It can impact **everything** in the proposed solution architecture)



Thank you

Slot	Start Time	Paper	Workshop	Finish Time
-	12:25	**LUNCH BREAK and NETWORKING** (Restaurant and Oak Room)		13:25
7	13:25	Slot 7A: Functional Safety and Artificial Intelligence	Slot 7B: **CASS 61508** & **62061** Workshop	13:55