Integrating ICS Safety and Security

Anna Ellis, Indigon Consulting

Aim

- An upbeat session which looks for positives; what can be done to try to address (sometimes competing) safety and security drivers, whilst retaining a solution which meets operational needs?
- But what are the implications of doing this?
- Elicit discussion and debate

Agenda

indigon consulting

- Aim, Agenda
- Introduction
- Background
- Overview of System Design Approaches for Safety, Security, Operation
- Commonalities between these Approaches - Overview
- Commonalities between these Approaches – Detail
- Summary – What do we end up with if we maximise the commonalities?
- Conclusion / Discussion – How applicable are the ideas to other industries?

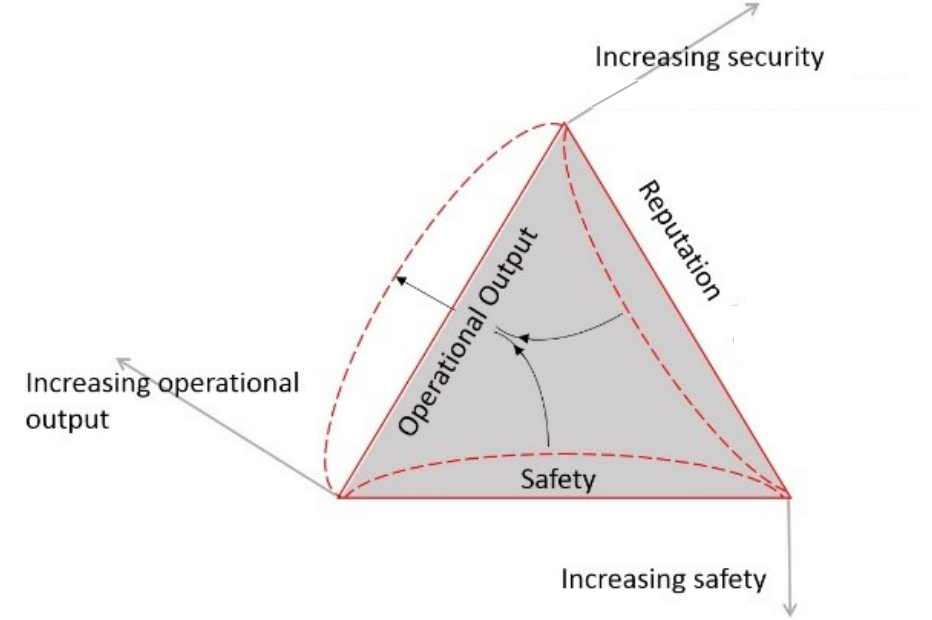
Introduction

- Anna Ellis, ICS Safety specialist
- Background in Consultancy within the UK civil Nuclear Industry
- Detailed understanding of ICS safety, some understanding of ICS security, but also an understanding of operational context and drivers
- I am less siloed than some people …

Background

- Siloes
- What do I mean by “meeting operational needs”?
- What drives Safety design?
- What drives Security design?
- How does Operability and Maintainability fit in?
- Other Drivers?
- An example of a potential conflict …

Background



- A thought …
- Is there a balance point which achieves the optimum position depending on the organisation's priorities? From this point, further positive improvements in one direction would negatively impact one or both of the other two.

Background

- Problem Statement:
  - Lack of a common understanding between siloed teams, lack of a framework to decide whose priority takes precedence when they conflict
  - Difficulties communicating risks to decision makers
  - No single framework for deciding whether a given solution is “good enough”.

System Design Approaches for Safety, Security, Operability

Safety	Security	Operation
Identify plant safety functions, define ICS functions required to deliver these, identify applicable ICS design guidance		Identify required functionality
Define architecture to deliver these safety functions	Assess architecture, apply design guidance	
Allocate functions to systems	Carry out risk assessment	
Capture requirements (from safety functions and from design guidance) in a specification	Capture requirements for security controls	Capture additional requirements for Operation and Maintenance (O&M)
Design systems		
Justify / test against requirements	Penetration Testing	Operability testing
On-going review and modification ….		

Commonalities

indigon consulting

- Identifying "functions" based on what the system needs to achieve
- Design an architecture to best fulfil the required functions
- Incorporate design guidelines / good practice when designing architecture and when allocating functions
- Assess initial system for risks and identify further controls
- Put all of the above into a requirements specification
- Trace requirements through the development lifecycle, demonstrate that they are implemented through documentation and test
- Re-assess the system on an on-going basis, for degradation, weaknesses or new threats

Commonalities - Functions

- Definition of Safety, Security and Operability functions up-front
- Method to prioritise in line with Company goals
- An example …

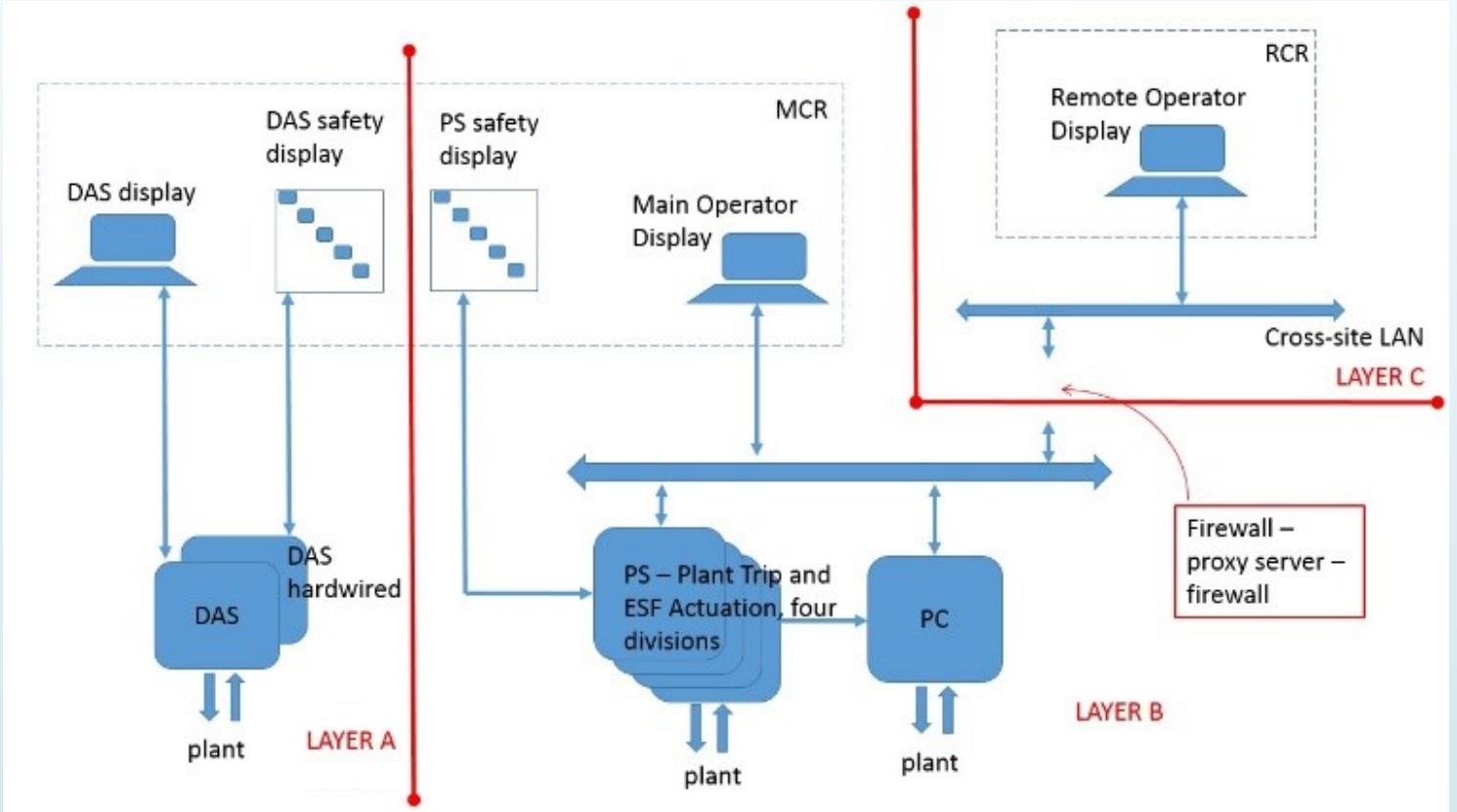
Commonalities – Architecture

(Barriers: Architecture, Technology, Human)

- Can we identify architectural constraints or guidance which responds to both safety and security drivers?
- In Safety; "the Barrier Model"
- In Security; think of barriers between the system and threat actors
  - Barriers between the system and the internet
  - Barriers between the system and open ports, open connectivity
  - Barriers by limiting intentional connectivity, and by constraining comms
  - Greatest number of barriers for the parts of the system we are most concerned about
- What does this look like? …

Commonalities – Architecture

(Barriers: Architecture, Technology, Human)



Commonalities – Architecture

(Barriers: Architecture, Technology, Human)

indigon consulting

- For parts of the system we are most concerned about, increase barriers:
  - Hard-to-access technology. Hardwired / FPGA technology?
  - Greater constraints on comms, ports, etc.
  - Greater constraints on humans; clearance, diversity of staff, access restrictions, etc.
- What are the parts of the system we are most concerned about?
  - Safety analysis identifies functions that need to go in a backup protection system (additional risk reduction for events that have a particularly unpalatable combination of likelihood and consequence)
  - Safety analysis can identify functions that protect in cases when software based systems are all compromised, or operate spuriously
  - Can we also include anything we consider to be a high security risk?
  - Can we design an "ultimate backstop" protection system and highly isolate from threats using barriers?
- Can we design an "ultimate backstop" protection system and highly isolate it from threats using barriers?

Commonalities – Architecture

(Barriers: Architecture, Technology, Human)

- Aim for an "ultimate backstop" protection system to guard against safety, security threats and – possibly - provide a minimal set of indications to an operator to guide decision-making
- Use architecture, technology and human defences to protect the ultimate backstop to the greatest extent feasible
- We need to continually re-assess the scope and resilience of this "ultimate backstop" system. Therefore we need to engineer a process and tools to review, modify and test the system. This might be due to:
  - Safety: Degradation
  - Security: Evolving threats
  - Operability: New requirements … amongst others …

Commonalities – Architecture

(Barriers: Architecture, Technology, Human)

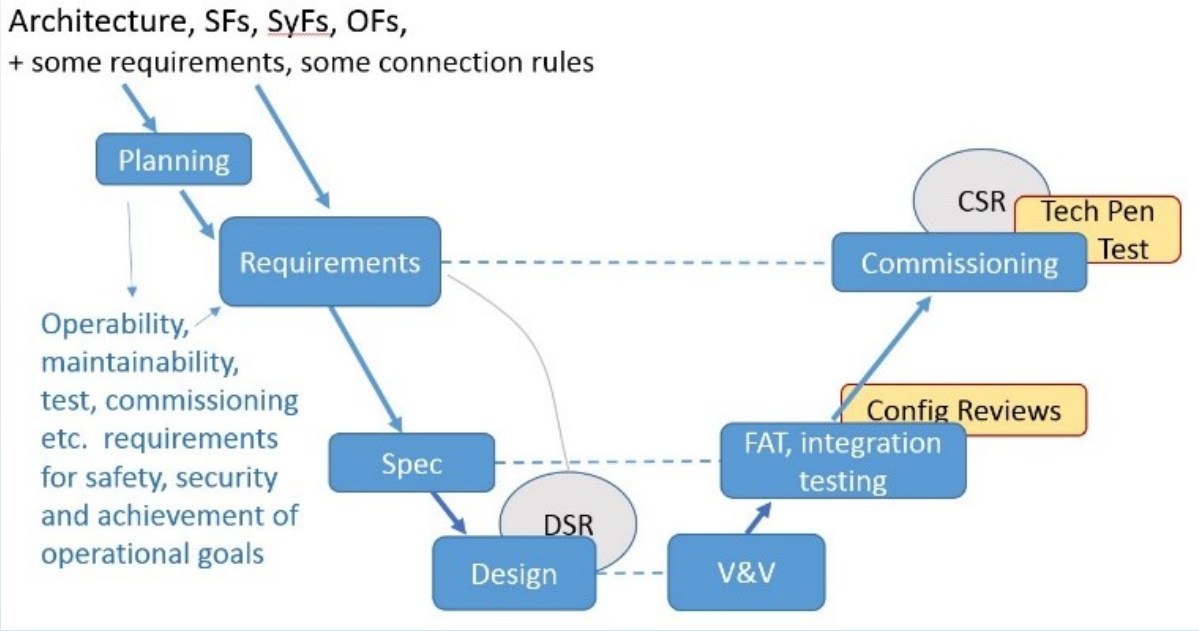
- A single, agreed document providing design guidance and good practices across ICS safety and security (but with a focus on preserving operational functionality) would be useful.
- What would go in it?
- The next commonality is "Assess risks and implement further barriers". This document could list useful barriers

Commonalities – Assess Risks and Implement Further Barriers

- What are the risks that the system we have designed so far does not fulfil its safety, security or operability functions?
- What are the most likely causes for these to be compromised?
  - Some threats might be technical (what are the failure modes? What happens if these occur?) Existing safety techniques consider this.
  - Some threats might be human. Existing security techniques consider this.
  - Some threats might be operational; to do with plant states and transients. Existing safety techniques cover this.
- If there's not a case to do a detailed analysis, at least look for the big-hitters.
- The "further barriers" to implement against specific risks could be identified in our design guidance and good practices document (proposed in the last slide).

Commonalities - Lifecycle

- Requirements Specification to capture all requirements
- Justification of implementation against requirements using substantiation reports at design stage and test reports at commissioning stage.



Re-assess the system on an on-going basis

- E.g. for degradation, weaknesses or new threats
- Permanent team?
- Proceduralise / Set KPIs?
- Incorporate operational experience from safety, security, even operability events / concerns
- A single entity to collect and interpret ICS security event data across all industries would be useful. What would the output from such an entity be?

Summary

- This is what we end up with …
- Is it acceptable?
- What are the implications of this?

indigon consulting

Conclusion

- Aim:
- An upbeat session which looks for positives; what can be done to try to address (sometimes competing) safety and security drivers, whilst retaining a solution which meets operational needs?
- But what are the implications of doing this?
- Elicit discussion and debate …

Discussion

- How applicable are these ideas to your industry?
- Discuss!

Anna Ellis, Indigon Consulting
www.indigonconsulting.com