SKADI SOLUTIONS
RESILIENCE READY

Designing Defensible Architecture for Critical Infrastructure

Architecting for Innovation

Date:
30/04/2026

Presented By:
Daniel Castillo

+61 404 630 324

www.skadisolutions.com.au

Your Presenter

Daniel Castillo is the founder & director of Skadi Solutions, Australia's first independent enterprise-focused cyber security firm dedicated to Critical Infrastructure.

Break into industry was as Systems Engineer, and field services OT specialist at Honeywell Building Technologies.

Daniel was the OT cyber security specialist for the ASD's Critical Infrastructure Uplift Program (CI-UP), a resilience uplift capability formed under the REDSPICE initiative. Since then, it has been his mission to make cyber resilience uplift **actionable** and **accessible** for CI providers big and small.

- Bachelor Mechatronics Engineering (UNSW)
- 8 Years experience across IT & OT Cybersecurity
- Experience in water, waste, electricity generation & transmission, corrections, healthcare, defence, commercial buildings, and IT / OT Consulting Industries.
- ISA Board member for ISA AU / NZ chapter

SKADI SOLUTIONS
RESILIENCE READY

Skadi Solutions

Tailor-Made Services for Critical Infrastructure Asset Owners

Cyber Security Resiliency Uplift Program

Our comprehensive engagement blueprint for cyber resilience uplift, we leverage various modes of technical validation to deliver a prioritised plan that is both pragmatic and actionable.

OT Attack Surface Management Service

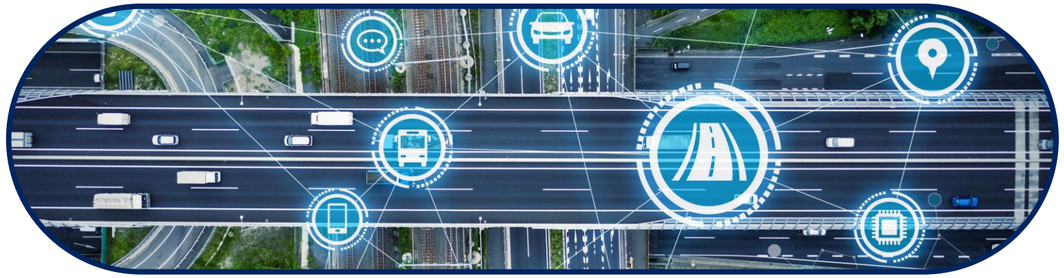
Our evergreen service for attack surface management and contextualised asset inventory, supported by expert insights which drive systematic improvements to your cyber security posture.

Secure-by-Design Enablement Service

Our secure-by-design service leverages our principled design methodology to accelerate the delivery of complex engineering projects and ensures security-focused engineering design.

Skadi Solutions maintain a highly focused service suite centered around the specific needs of Critical Infrastructure asset owners and the mission for enterprise-wide resilience. While our approach is more pragmatic and less compliance focused, our services support providers with compliance obligations and maturity goals regarding:

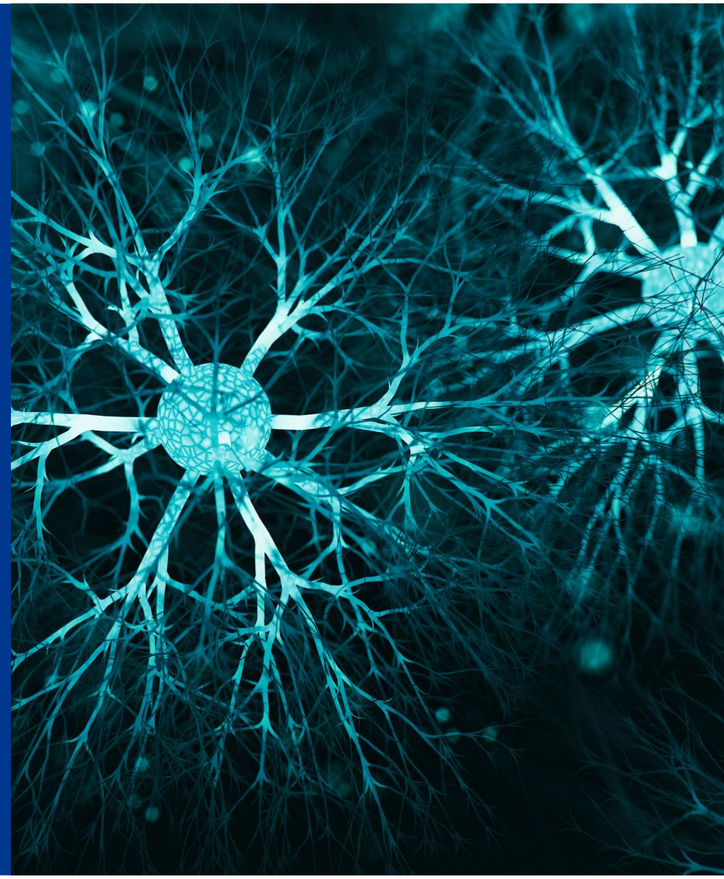
- SOCI Act Obligations & CIRMP
- SANS Top 5 CC for ICS
- ASD ACSC's CI-Fortify
- AEMO AESCSF (Energy)
- IEC/ISA 62443
- CLC/TS 50701 (Rail)



Today’s Agenda

SKADI SOLUTIONS
RESILIENCE READY

- Overview on Critical Infrastructure (CI)
- Threats & Cyber Resilience in CI
- 5 Principles for Defensible Architecture in CI
- Common Pitfalls
- Worked Example
- Key Takeaways
- Questions & Answers



Cyber in Critical Infrastructure Sectors

SKADI SOLUTIONS
RESILIENCE READY

The essential services fundamental to a nation's function

What is it?

- "The systems which are responsible for supply us the essential services required for everyday life"
- Fundamental to a nations function – less all hell breaks loose

Cyber in Critical Infrastructure Sectors

SKADI SOLUTIONS
RESILIENCE READY

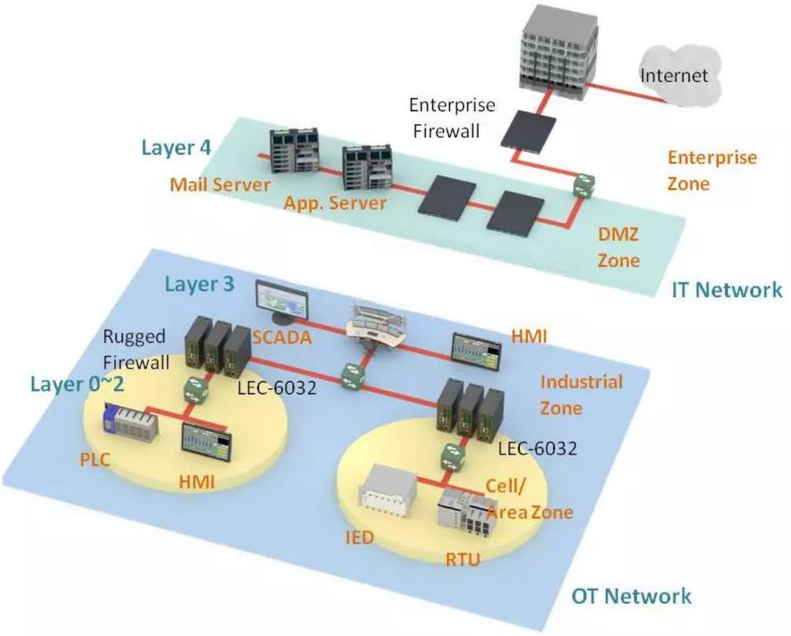
The essential services fundamental to a nation's function

What is it?

- "The systems which are responsible for supply us the essential services required for everyday life"
- Fundamental to a nations function – less all hell breaks loose

Key Characteristics:

- Typically contains a combination of Information Technology (IT) and Operational Technology (OT) systems (and even IoT)
- Traditional architectures include Air-Gap networks & limited use-cases for external integration



Sources:

[1] SCADA System | www.lanner-america.com

Cyber in Critical Infrastructure Sectors

SKADI SOLUTIONS
RESILIENCE READY

The essential services fundamental to a nation's function

What is it?

- "The systems which are responsible for supply us the essential services required for everyday life"
- Fundamental to a nations function – less all hell breaks loose

Key Characteristics:

- Typically contains a combination of Information Technology (IT) and Operational Technology (OT) systems (and even IoT)
- Traditional architectures include Air-Gap networks & limited use-cases for external integration
- Modern requirements demand more interconnectivity and multiple use-cases for external integration

Use cases driving increased interconnectivity

- Predictive Maintenance & AI Analytics
- Data Aggregation & Insights (Data Lake)
- AI / Machine Learning Optimisation
- Remote Operations & Centralised Control
- Vendor Remote Support & Managed Services

Cyber in Critical Infrastructure Sectors

SKADI SOLUTIONS
RESILIENCE READY

The essential services fundamental to a nation's function

What is it?

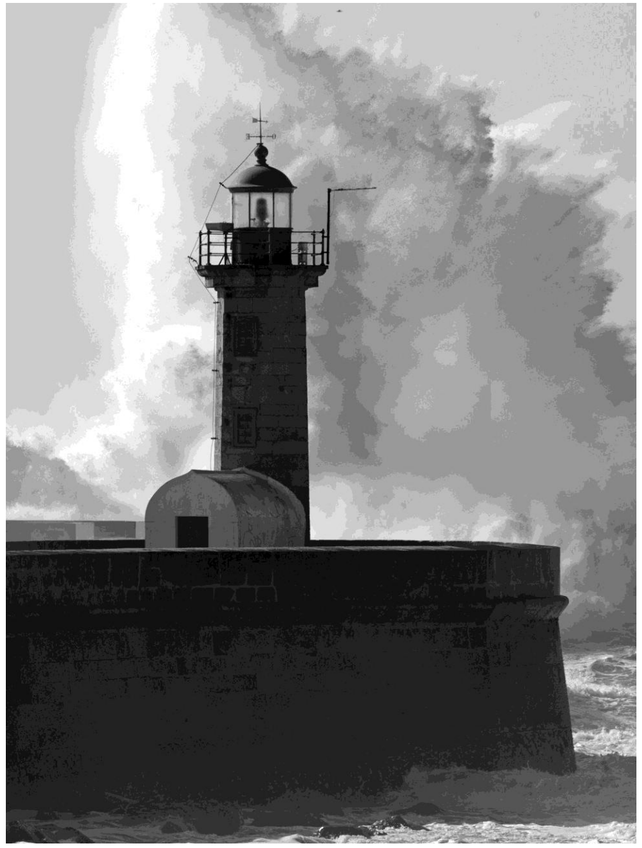
- "The systems which are responsible for supply us the essential services required for everyday life"
- Fundamental to a nations function – less all hell breaks loose

Key Characteristics:

- Typically contains a combination of Information Technology (IT) and Operational Technology (OT) systems (and even IoT)
- Traditional architectures include Air-Gap networks & limited use-cases for external integration
- Modern requirements demand more interconnectivity and multiple use-cases for external integration

Our topic for today:

- Designing Defensible Architecture for Critical Infrastructure
- 5 Architectural principles for installing resilience into Critical Infrastructure environments
- Common pitfalls which compromise defensibility and resilience
- Worked example demonstrating defensible architecture in action



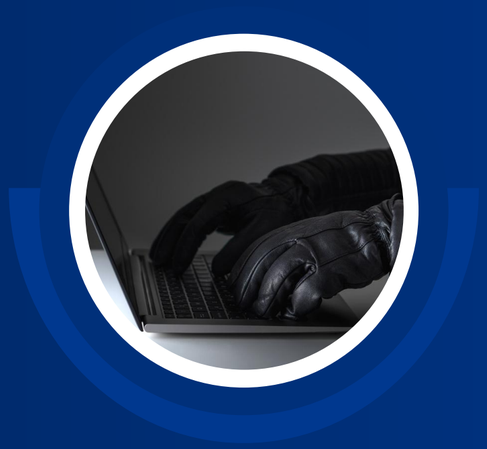
Cyber Resilience in CI

SKADI SOLUTIONS
RESILIENCE READY

Resilience is not the absence of threats — it is the ability to keep operating while threats are present.

Active Threat Landscape

- Tense geopolitical climate
- Cyber as a military capability
- PRC State-Sponsored Cyber Actors[1]
- GRU Unit 29155 Cyber Actors[2]
- Living-off-the-land (LOTL) techniques
- Pre-positioning for impact



Commoditised Malware & TTPs

- Major focus on IT-orientated attacks
- Use of open-source tools like Shodan, & Censys by opportunistic criminals
- Trade craft against CI (Impacket, Mimikatz, extraction of NTDS.dit)
- Advances in ICS specific malware

Sources:

[1] PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | Cyber.gov.au

[2] Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure | Cyber.gov.au

Cyber Resilience in CI

SKADI SOLUTIONS
RESILIENCE READY

Resilience is not the absence of threats — it is the ability to keep operating while threats are present.

Clear shift in the Approach:

- Assume breach, protect operating priorities

Cyber Threats to OT CI

- **Manipulation of View or Control**
- **Theft of Operational Information**
- **Loss of Safety or Protection**
- **Damage to property**

Priorities

Cyber Resilience in CI

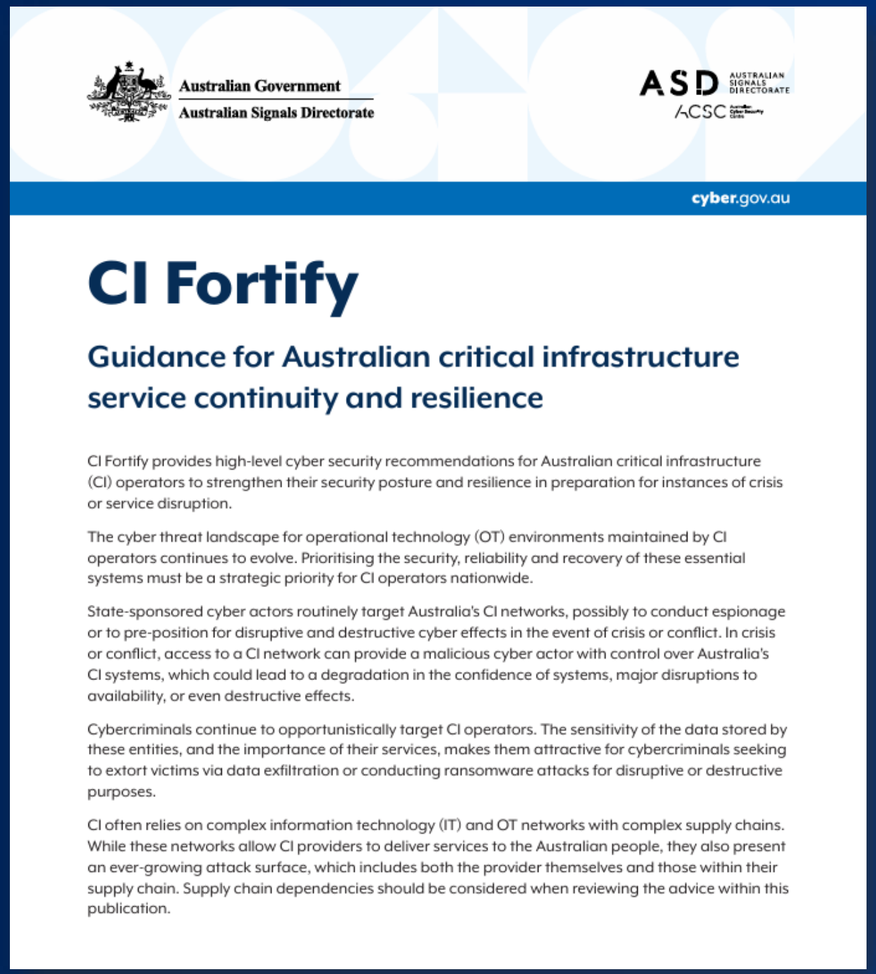
SKADI SOLUTIONS
RESILIENCE READY

Resilience is not the absence of threats — it is the ability to keep operating while threats are present.

Clear shift in the Approach:

- Assume breach, protect operating priorities

- ASD ACSC's CI-Fortify – Published 13th October 2025
  - Ability to isolate vital OT/enabling systems for 3 months while maintaining critical services
  - Ability to rapidly rebuild systems to minimise critical-service disruption



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

cyber.gov.au

CI Fortify

Guidance for Australian critical infrastructure service continuity and resilience

CI Fortify provides high-level cyber security recommendations for Australian critical infrastructure (CI) operators to strengthen their security posture and resilience in preparation for instances of crisis or service disruption.

The cyber threat landscape for operational technology (OT) environments maintained by CI operators continues to evolve. Prioritising the security, reliability and recovery of these essential systems must be a strategic priority for CI operators nationwide.

State-sponsored cyber actors routinely target Australia's CI networks, possibly to conduct espionage or to pre-position for disruptive and destructive cyber effects in the event of crisis or conflict. In crisis or conflict, access to a CI network can provide a malicious cyber actor with control over Australia's CI systems, which could lead to a degradation in the confidence of systems, major disruptions to availability, or even destructive effects.

Cybercriminals continue to opportunistically target CI operators. The sensitivity of the data stored by these entities, and the importance of their services, makes them attractive for cybercriminals seeking to extort victims via data exfiltration or conducting ransomware attacks for disruptive or destructive purposes.

CI often relies on complex information technology (IT) and OT networks with complex supply chains. While these networks allow CI providers to deliver services to the Australian people, they also present an ever-growing attack surface, which includes both the provider themselves and those within their supply chain. Supply chain dependencies should be considered when reviewing the advice within this publication.

Sources:

[1] CI-Fortify | Cyber.gov.au

Cyber Resilience in CI

SKADI SOLUTIONS
RESILIENCE READY

Resilience is not the absence of threats — it is the ability to keep operating while threats are present.

Clear shift in the Approach:

- Assume breach, protect operating priorities

- ASD ACSC's CI-Fortify – Published 13th October 2025
  - Ability to isolate vital OT/enabling systems for 3 months while maintaining critical services
  - Ability to rapidly rebuild systems to minimise critical-service disruption

- Consultation Paper on proposed changes to SOCI Act obligations
  - Currently under active public consultation
  - Explicitly calls out 3-month isolation and rebuild mandate
  - Sets clear expectation for asset-owners to move from prevention to "enduring / recovering"

What we propose

We propose that responsible entities must outline in their CIRMP how they have implemented the greatest practical level of segregation between their asset's critical systems, and other internet-connected, or less secure components that could result in the compromise of, substantive loss of access to, or deliberate or accidental manipulation of a critical system. Critical systems include vital operational technology, enabling services, and critical components vital to the delivery of the asset's function, or whose compromise or degradation could cause significant harm to the asset. This will require the responsible entity to identify their critical systems and components, and implement the greatest practical level of segregation between their critical systems from all other networks, which could include:

- maintaining an inventory of critical systems important to the delivery of the function of the asset;
- ensuring critical systems are operationally independent from other IT systems and networks to the greatest extent possible, such that they can be isolated for a period of 3 months while maintaining critical services;
- implementing logical access controls for network traffic between critical systems and all other networks;
- consistently reviewing access logs for communication paths between critical systems and other networks; and
- implementing principles of least-privilege across networks that connect to critical systems

Should network segregation or isolation measures not be effective at preventing compromise of critical systems, and where not already present, it is proposed that the responsible entity builds redundancy plans into their CIRMP. Recovery and restoration controls are vital to minimising the potential impact of compromise or sabotage of an asset's critical systems and reducing potential downtime or disruptions to

Consultation Paper OFFICIAL Page **10** of **26**

Sources:

[1] Consultation Paper Proposed Amendments Enhance CIRMP | homeaffairs.gov.au

Defensible Architecture

SKADI SOLUTIONS
RESILIENCE READY

The basis by which we achieve resilience

Guidance **from industry** on defensible architecture:

- CISA: Seven Steps to Effectively Defend ICS
- DoE: 21 Steps to Improve Cyber Security of SCADA Networks
- NIST 800-82 R3: Defence-in-depth architecture

4. BUILD A DEFENDABLE ENVIRONMENT

Limit damage from network perimeter breaches. Segment networks into logical enclaves and restrict host-to-host communications paths. This can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves. Containment provided by enclaving also makes incident cleanup significantly less costly.[c]

Sources:

[1] 7 Steps to Effectively Defend ICS | www.cisa.gov

Defensible Architecture

SKADI SOLUTIONS
RESILIENCE READY

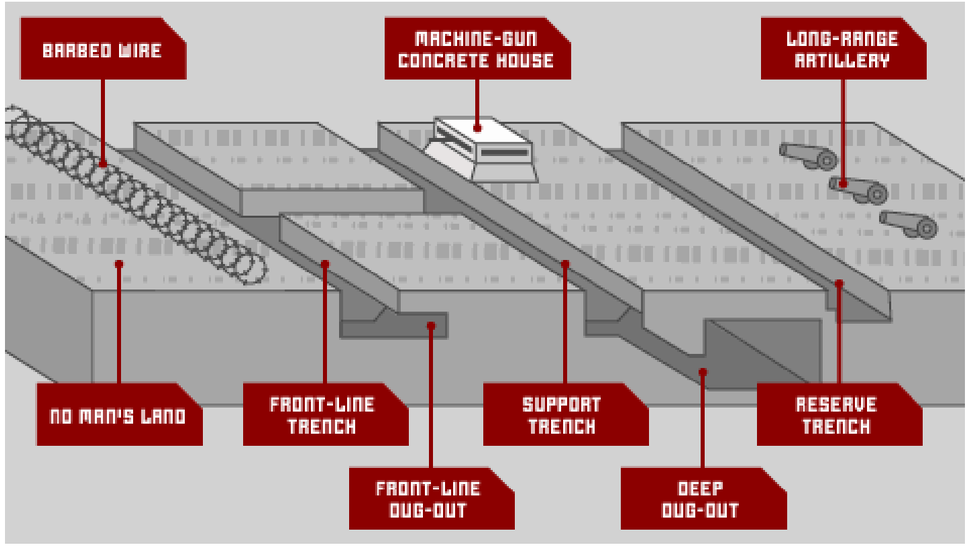
The basis by which we achieve resilience

Guidance **from industry** on defensible architecture:

- CISA: Seven Steps to Effectively Defend ICS
- DoE: 21 Steps to Improve Cyber Security of SCADA Networks
- NIST 800-82 R3: Defence-in-depth architecture

Defence-in-depth vs **Defensible architecture**

- Defence-in-depth: **Layered security controls** across enterprise
- Defensible architecture: Can be likened to **WW1 trench warfare**
- Defensible architecture **must be supplemented** with defence-in-depth security controls to functionally achieve enterprise resilience



Behind the front system of trenches there were usually at least two more partially prepared trench systems, kilometres to the rear, ready to be occupied in the event of a retreat. The Germans often prepared multiple redundant trench systems; in 1916 their Somme front featured two complete trench systems, one kilometre apart, with a third partially completed system a further kilometre behind. This duplication made a decisive breakthrough virtually impossible. In the event that a section of the first trench system was captured, a "switch" trench would be dug to connect the second trench system to the still-held section of the first.

Sources:

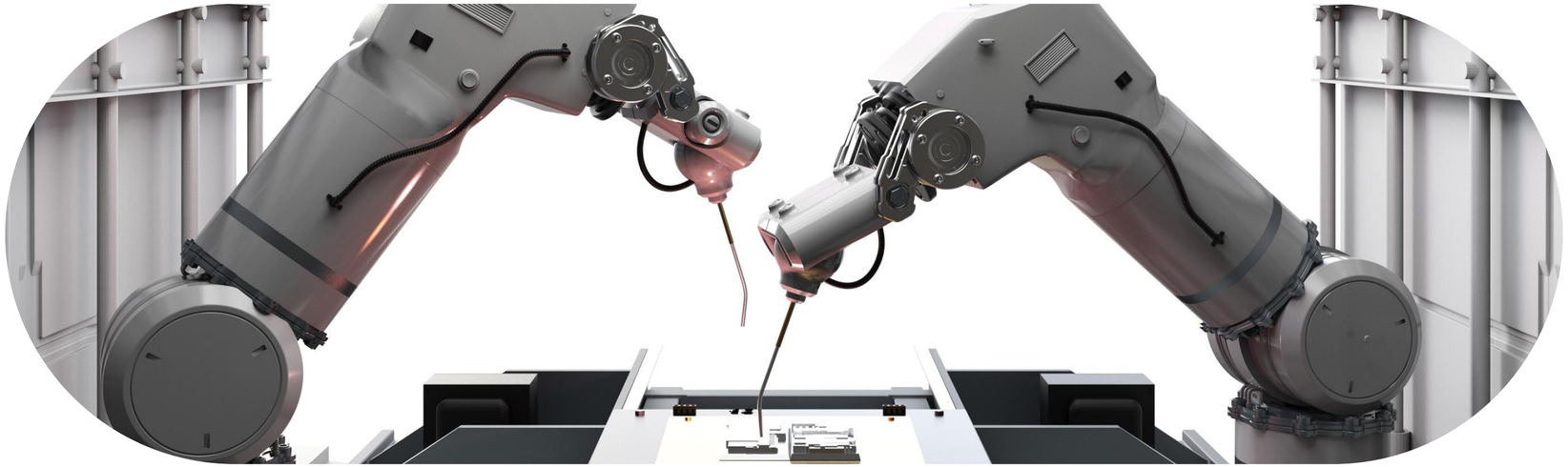
[1] WW1 Trench Warfare | wwi-trenchwarfare.weebly.com

[2] Trench Warfare | en.Wikipedia.org

5 Principles for Architecture in CI

SKADI SOLUTIONS
RESILIENCE READY

Things I think about when developing architectures for CI environments



The Context & Goal: Develop defensible & resilient architectures that support rapid isolation and rebuild procedures.

5 Principles for Architecture in CI

SKADI SOLUTIONS
RESILIENCE READY

Principle 1: Maintain OT Sovereignty

Reasons to enforce **OT Sovereignty** in your architecture:

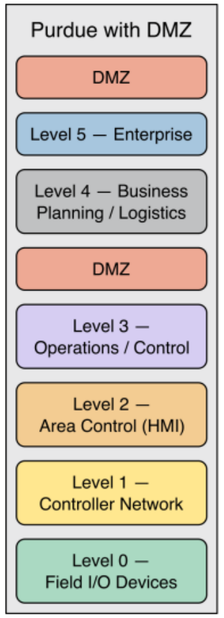
- IT environments present the **largest attack surface**
- Most threat groups target the IT environment
- Thoughtful segregation is a key enabler for isolation

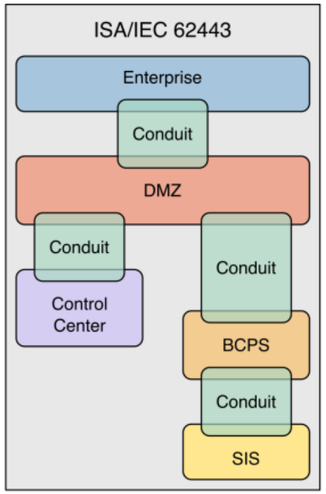
Sensitive OT assets which demand isolation:

- Core Management services: Hypervisors, backup servers, domain controllers, jump-boxes, firewalls, process critical applications (MIS / ERP)
- Information assets: Network diagrams, OT password databases, controller configuration, SCADA graphics files, switch configuration
- Controls Equipment: PLCs, RTUs, SIS, assets with engineering software

Consideration of Workflows:

- **Where** does control equipment **configuration** occur from? IT SoE?
- **What** assets are used to **access** to the OT network? Tool Laptops?





Purdue Model is **not a security architecture** – but is an effective tool for classifying assets to be **bound IT or OT**

Sources:

[1] NIST SP 800-82r3 (Fig.16): High-level example of Purdue model for network segmentation with DMZ segments

5 Principles for Architecture in CI

SKADI SOLUTIONS
RESILIENCE READY

Principle 2: Restrict IT / OT Interfaces & Dataflows

Boundary controls & network segmentation:

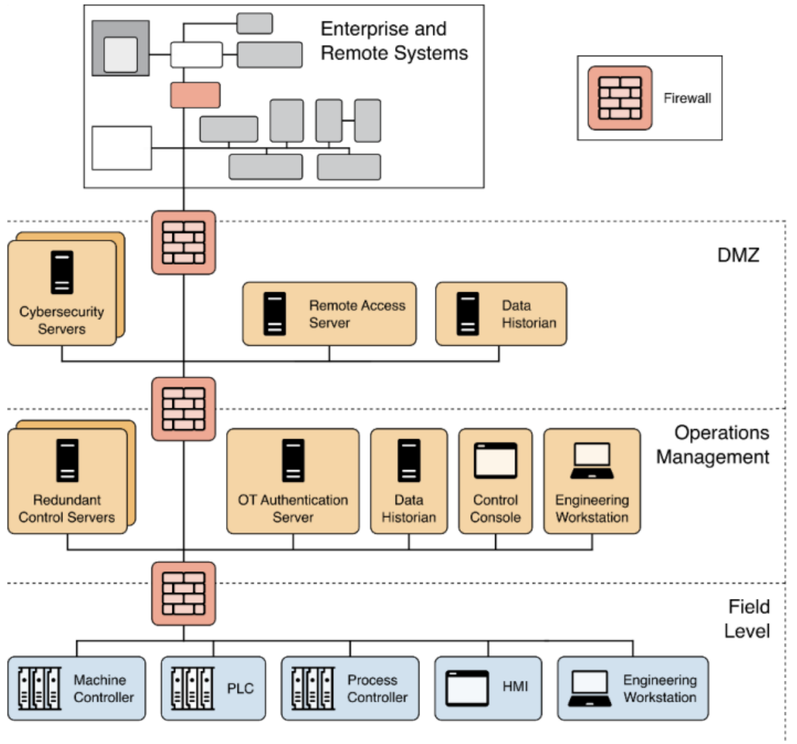
- Limits initial **blast radius** of an incident
- Often function as conduits where **isolation** can be performed
- May serve as locations to perform **inspection or monitoring**

Key **use-cases** for interfacing IT & OT:

- Ad-Hoc File transfer: Patches, software installers.
- Real-time data transfer: Data analytics, routine reporting.
- Remote access workflows: Vendor access, operator access.

Considerations for zoning & interfaces:

- Strictly limit **downstream data-flows**; Establish **centralised patterns**.
- Never permit **control protocols** from IT zones.
- Avoid data-flows / workflows which **bypass enforcement points**.
- Privileged activities are to be restricted to **privileged servers & zones**



Sources:

[1] NIST SP 800-82r3 (Fig.19): Security architecture example for DCS system

5 Principles for Architecture in CI

SKADI SOLUTIONS
RESILIENCE READY

Principle 3: Operationalise Shield Up

Defining a shields up state:

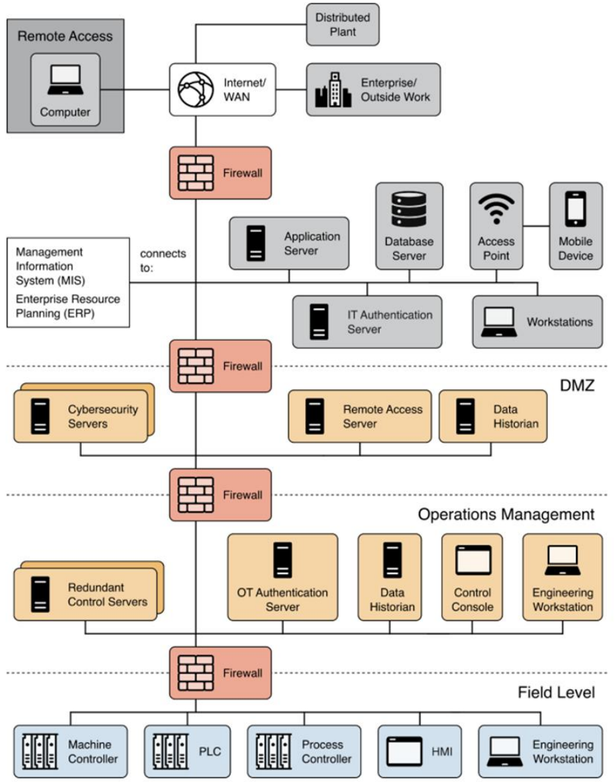
- Actions to **isolate** key zones (IT / OT, IT / internet, OT / OT)
- Supplementary workflows to support **extended isolation**

Defensible architecture capability for shields up:

- Supports **multiple tiers** of increasingly degraded operation
- Supports **greater flexibility** with containment actions
- Granular retreat vs pull the cable (can cause more harm than good)
- Longer feasible **duration** to comfortably maintain degraded status

Considerations for shields up / isolation:

- Does the architecture technically **support isolation**. Where?
- Testing and **familiarity** with isolation procedures
- Process **dependencies** impacted by isolation procedures
- Relationship with field crews required to coordinate



Sources:

[1] NIST SP 800-82r3 (Fig.18) Security architecture example for DCS system

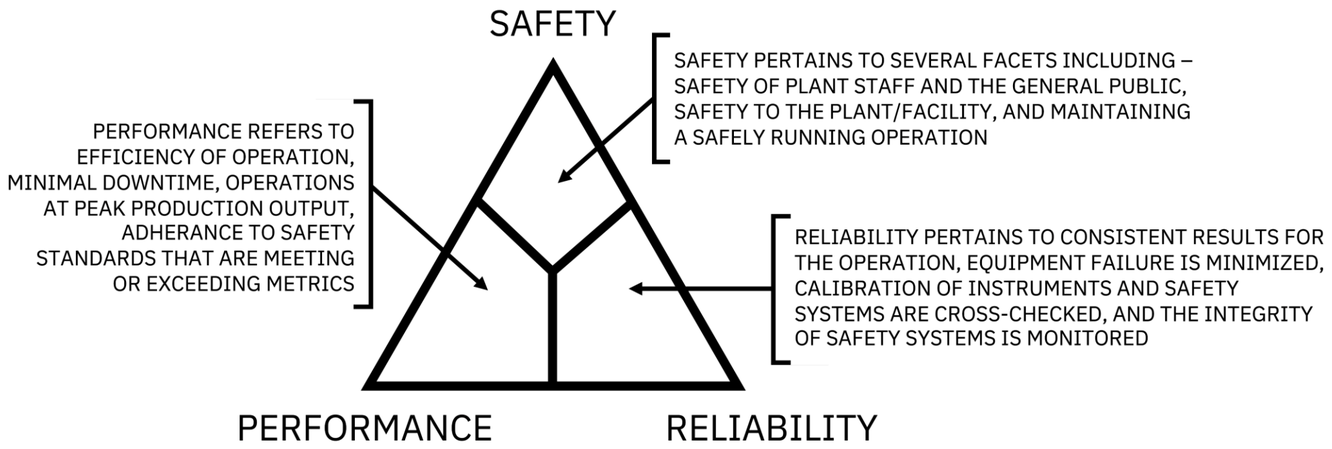
5 Principles for Architecture in CI

SKADI SOLUTIONS
RESILIENCE READY

Principle 4: Prioritise Safety & Functionality

Considerations for **prioritising resiliency outcomes** from defensible architecture implementation:

- Assess whether defined “shields up” states enabled by defensible architecture capability supports **SRP (Safety, Performance, Reliability)**
- **Deterministic** degradation is key – should be clearly defined in design work
- Understand as a cyber professional that safety and functionality will **always be the primary concern** within a CI environment



Sources:
[1] http://srpmodel.infracritical.com/srpmodel.php

5 Principles for Architecture in CI

SKADI SOLUTIONS
RESILIENCE READY

Principle 5: Implement Proactively

Architectural changes must be made pre-incident:

- Defensible architecture is generally disruptive to implement. Impacts existing workflows and availability of core services (AD, SCADA)
- Requires specific software and hardware
- Requires an enterprise approach (not just the IT / OT boundary)

Containment activities are always architecture dependent:

- Higher **cost** to respond
- Higher **threat** to safety, reliability, and performance

Considerations for road-mapping implementation:

- Tie defensible architecture implementation into **OT asset strategy**
- Develop an aligned **reference architecture blueprint(s)** to guide decisions around technology adoption and lifecycle projects – prioritise high utility patterns
- Consider defensible architecture when defining specifications for **3rd party systems**

Sources:

[1] The Five ICS Cybersecurity Critical Controls | www.sans.org

Common Pit-Falls

SKADI SOLUTIONS
RESILIENCE READY

Architectural signs your environment is not defensible

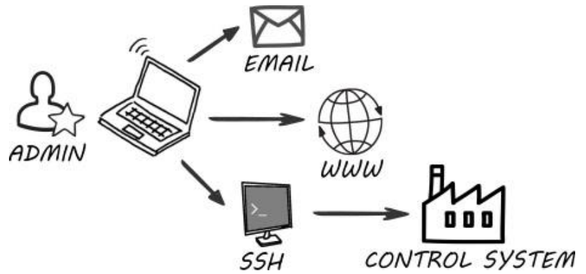
Anti-Patterns to look out for:

- **Shared domain** between IT and OT environments (or **domain trust**)
- Shared **IT / OT security tooling** administered from IT zones or IT credentials
- Shared **IT / OT boundary firewall** administered using IT credentials
- Workflows involving **OT configuration management** from IT network zones / assets
- Workflows involving **direct access** to OT environment from internet or IT (Over-permissive VPN user profiles, lack of dedicated OT MFA, or jump-host)
- Workflows involving any **'browse-up' administration**
- Workflows involving any **'management bypass'**

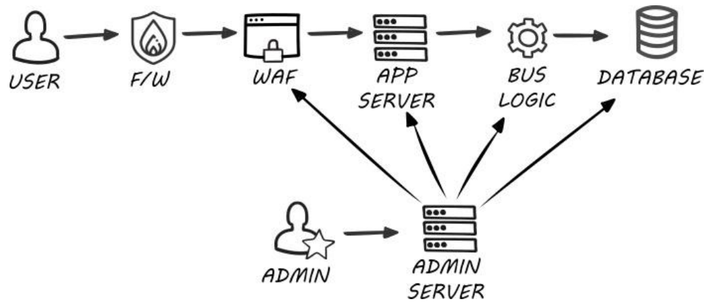
Security anti-patterns as above can **massively compromise** what is otherwise a highly defensible architectural implementation.

- **What not to do:** NCSC Security Architecture Anti-Patterns Whitepaper
- **What you should do:** ASD ACSC Secure connectivity principles for OT

Example 1: 'Browse-up' Administration



Example 2: Management bypass



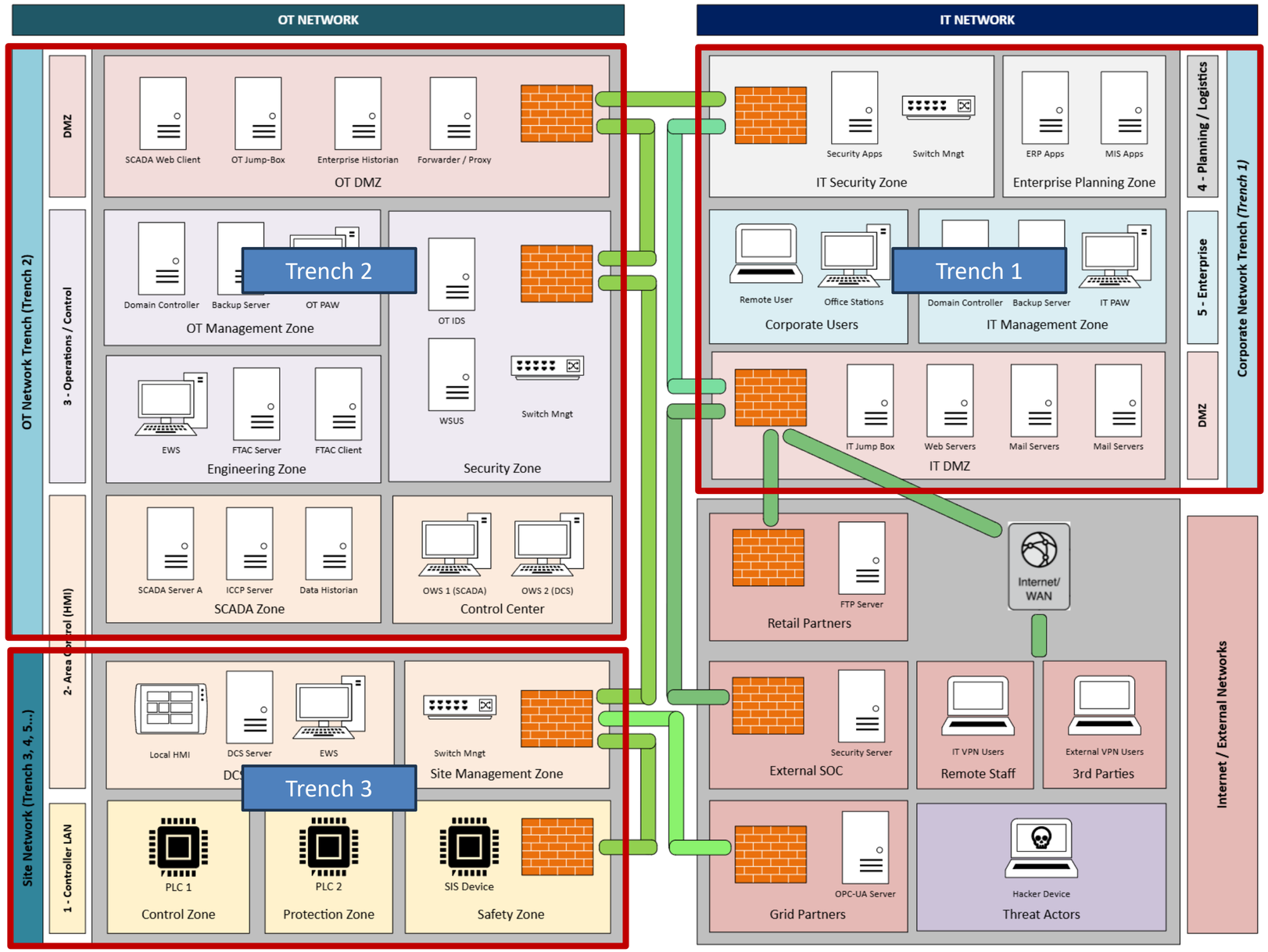
Sources:

[1] NCSC Security Architecture Anti-Patterns Whitepaper | www.ncsc.gov.uk

Worked Example

A theoretical implementation using the Energy Sector:

- Capability to island into 3 discrete trenches
  - Trench 1 – Corporate Network
  - Trench 2 – OT Network
  - Trench 3 – Site Network



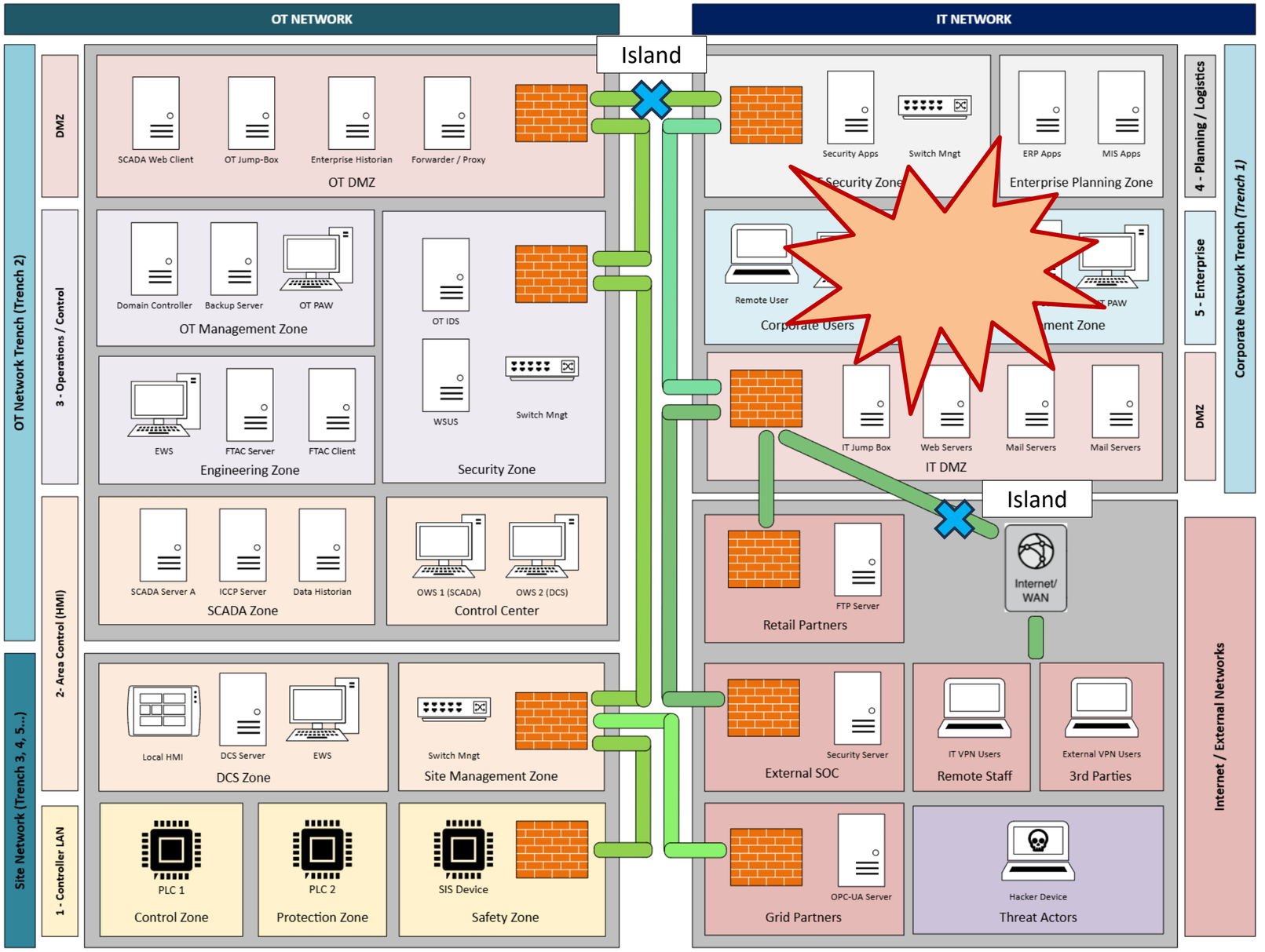
Worked Example

A theoretical implementation using the Energy Sector:

- Capability to island into 3 discrete trenches
  - Trench 1 – Corporate Network
  - Trench 2 – OT Network
  - Trench 3 – Site Network

Scenario 1 – **Internet borne threat**

- Proactively disable remote services
- Impact limited to corporate network
- Island the OT and IT networks



Worked Example

A theoretical implementation using the Energy Sector:

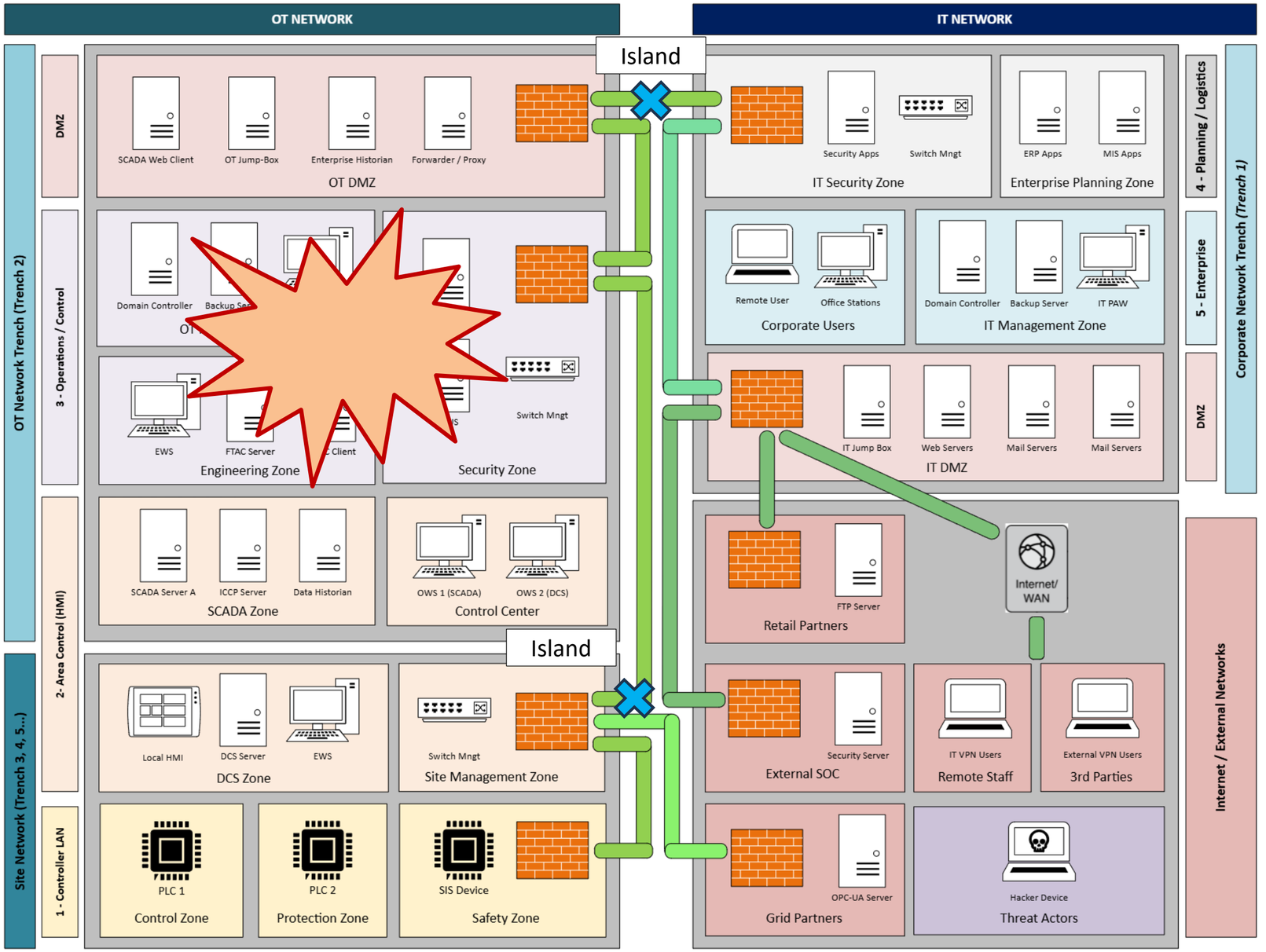
- Capability to island into 3 discrete trenches
  - Trench 1 – Corporate Network
  - Trench 2 – OT Network
  - Trench 3 – Site Network

Scenario 1 – **Internet borne threat**

- Proactively disable remote services
- Impact limited to corporate network
- Island the OT and IT networks

Scenario 2 – **OT network Compromised**

- Impact limited to OT network
- Restrict communications or island OT network from remote DCS sites



Worked Example

A theoretical implementation using the Energy Sector:

- Capability to island into 3 discrete trenches
  - Trench 1 – Corporate Network
  - Trench 2 – OT Network
  - Trench 3 – Site Network

Scenario 1 – **Internet borne threat**

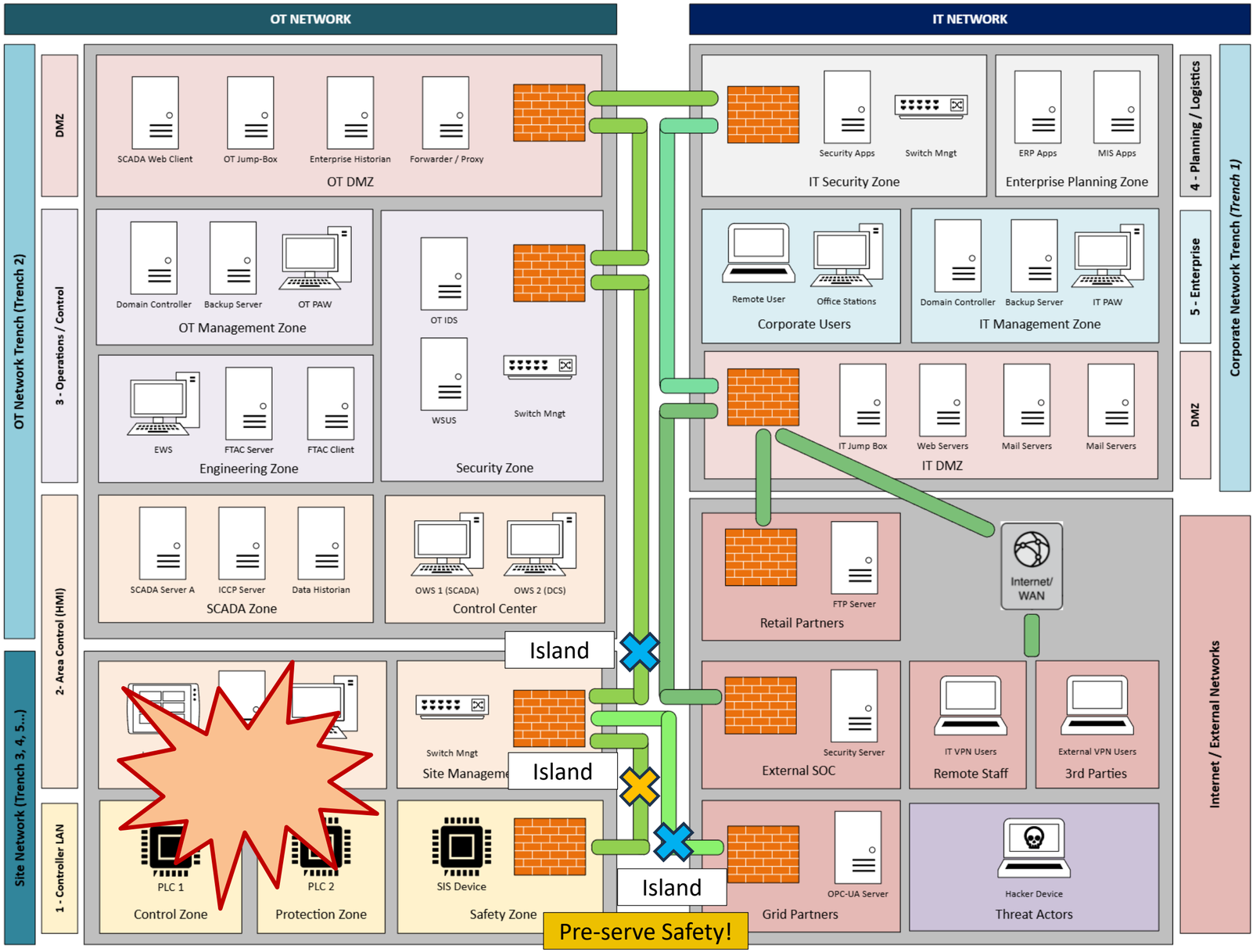
- Proactively disable remote services
- Impact limited to corporate network
- Island the OT and IT networks

Scenario 2 – **OT network Compromised**

- Impact limited to OT network
- Restrict communications or island OT network from remote DCS sites

Scenario 3 – **DCS system compromised**

- Impact limited to the local DCS
- Island site from central SCADA, other DCS sites, and connected grid partners
- Island safety zone from DCS



Key Takeaways

SKADI SOLUTIONS
RESILIENCE READY

Key aspects for success with CI Fortify

- Workshop isolation and rebuild as fundamental design elements when architecting for CI environments
- Maintain awareness of architectural anti-patterns common to CI environments when working with relevant sector clients
- Prioritise resilience over prevention
- Always think about safety, performance and reliability (SRP) as fundamental requirements when working OT environments.

SKADI SOLUTIONS
RESILIENCE READY

THANK YOU

FOR YOUR ATTENTION AND PARTICIPATION

Now Open for Question & Answers

Contact Us:

+61 404-630-324

www.skadisolutions.com.au

hello@skadisolutions.com.au

Download this presentation