Developing Cyber Resilience Together:

Industry Cooperation for a More Secure Railway

Alexander Patton

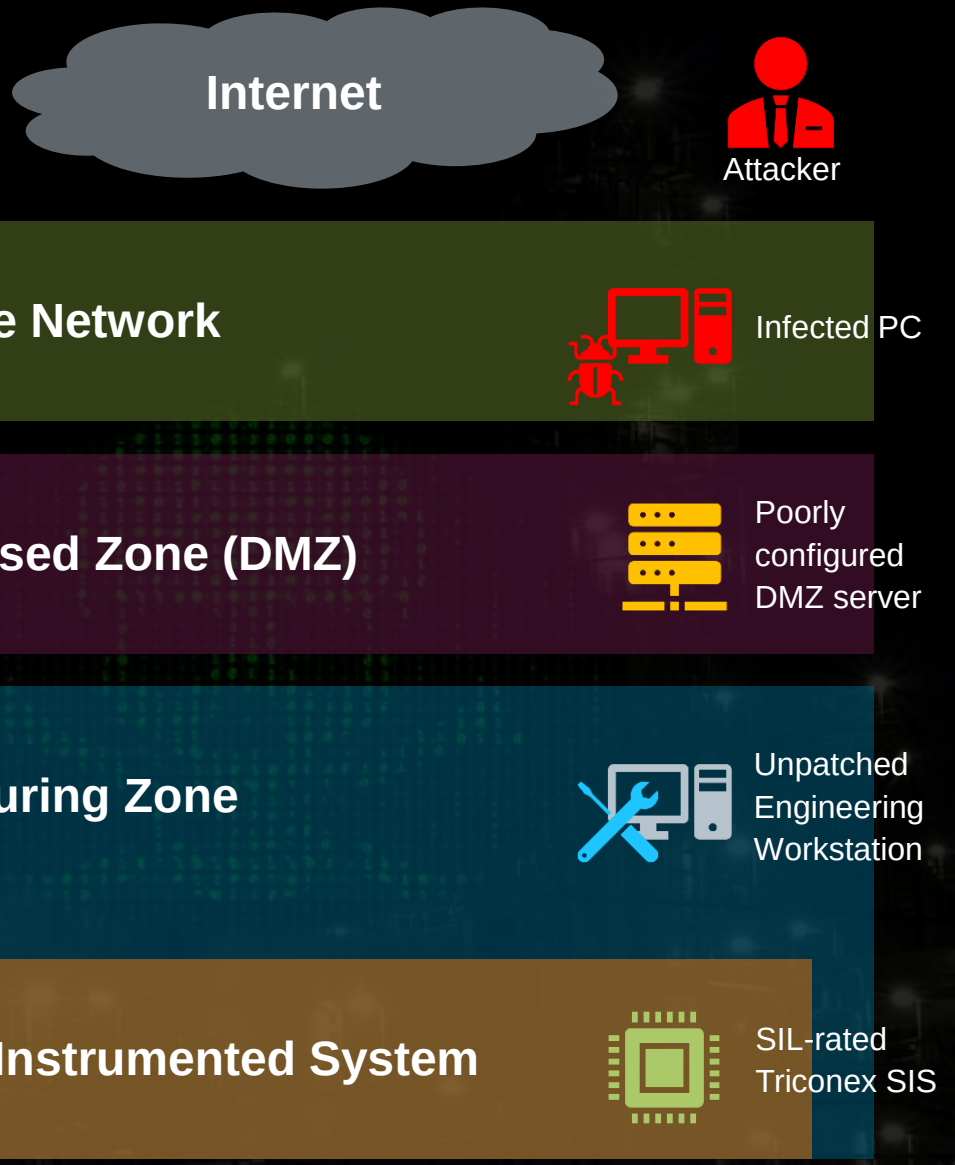
23rd October 2019 – IRSE ASPECT2019 Conference, Delft, Netherlands

July 2017, years ago...

A petrochemical plant in Saudi Arabia

Hackers break through DMZ firewall

RDP vulnerabilities exploited on the Engineering Workstation



years ago...

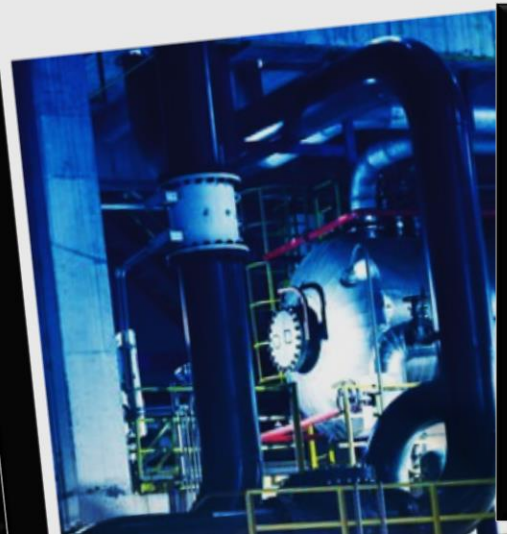
Vulnerability in the Triconex software allows Trojan to be installed on SIL-rated Safety Instrumented System

two years ago...

Could this have happened to the railway?

LILY HAY NEWMAN SECURITY 01.18.18 07:17 PM

MENACING MALWARE SHOWS THE DANGERS OF INDUSTRIAL SYSTEM SABOTAGE

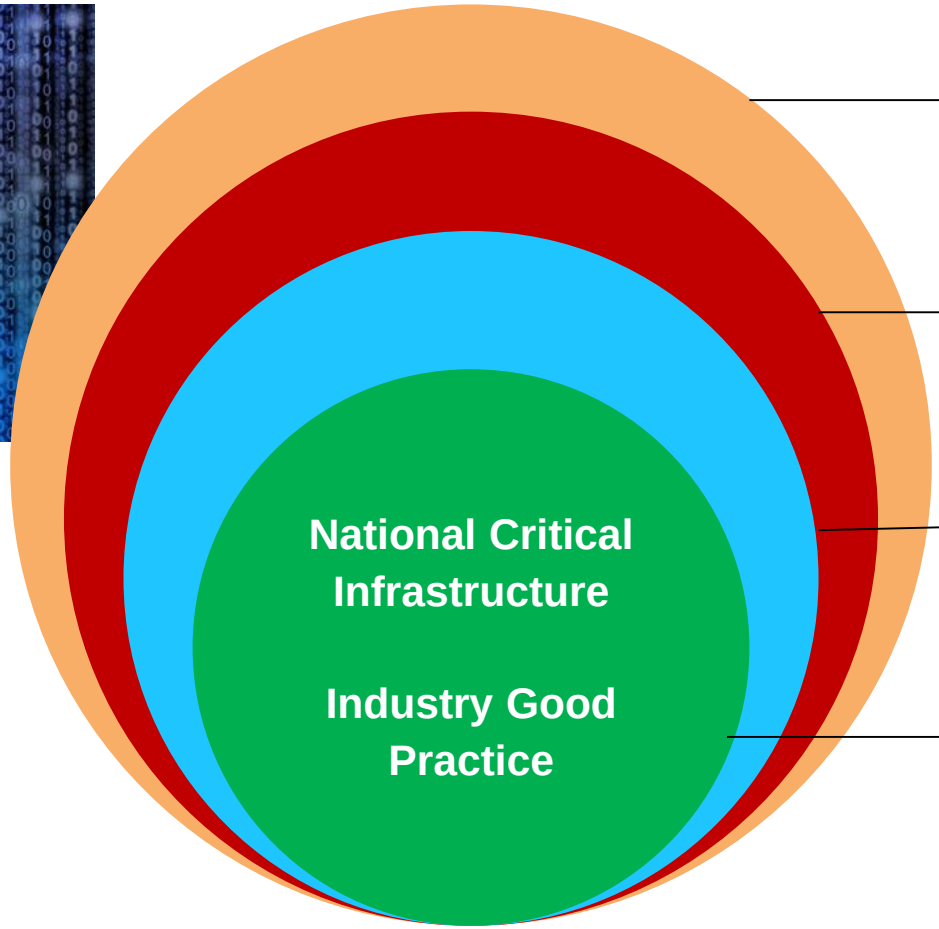


Trisis nation-state authored malware leaked onto internet

Schneider Electric accidentally puts malware online that could shut down power plants. Nation state authored malware has been mistakenly put online that could enable hackers to compromise safety systems at power plants.

Governments are taking notice.

Non-compliance:
Up to €20 million fine



A. Manage Security Risk

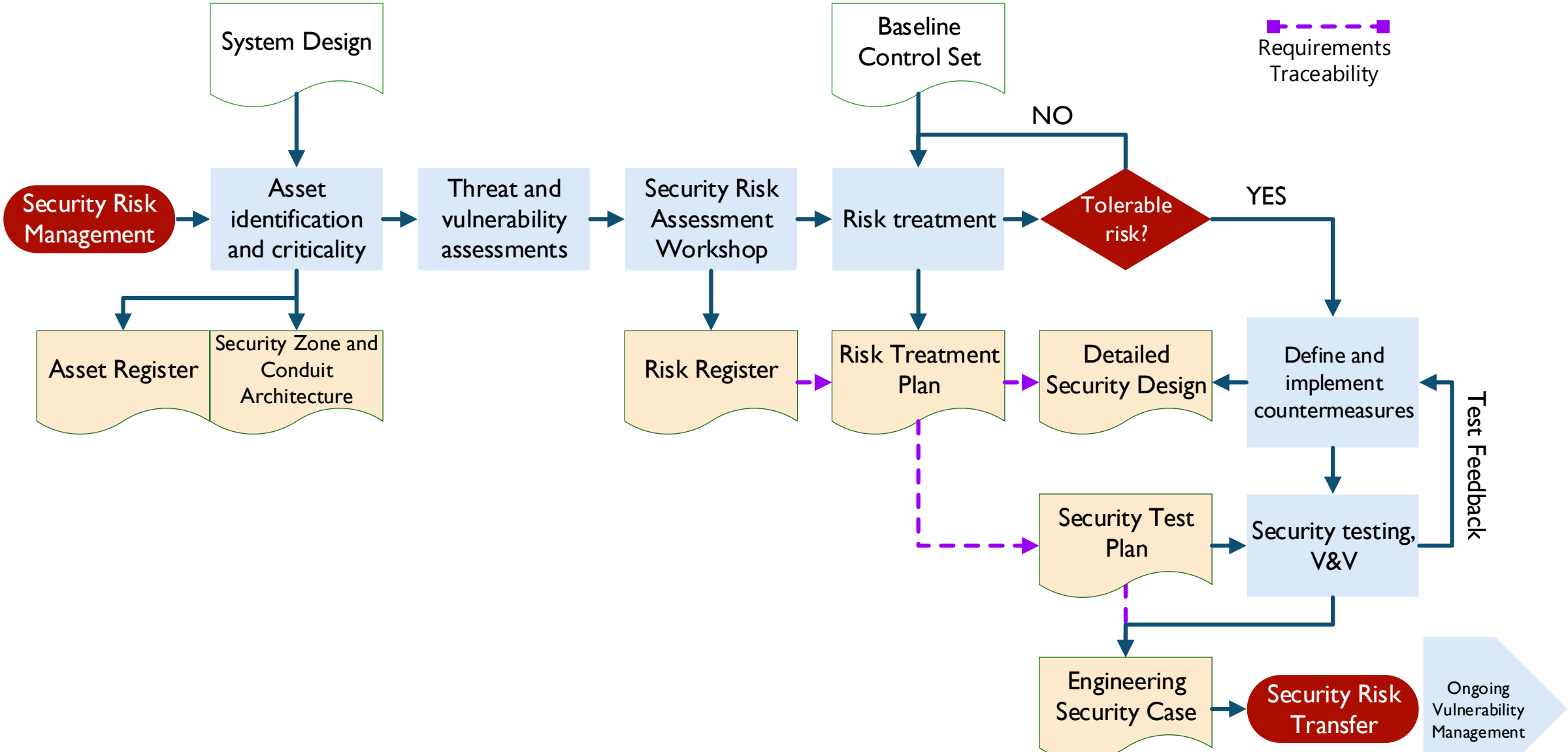
B. Protect the System

C. Detect Incidents

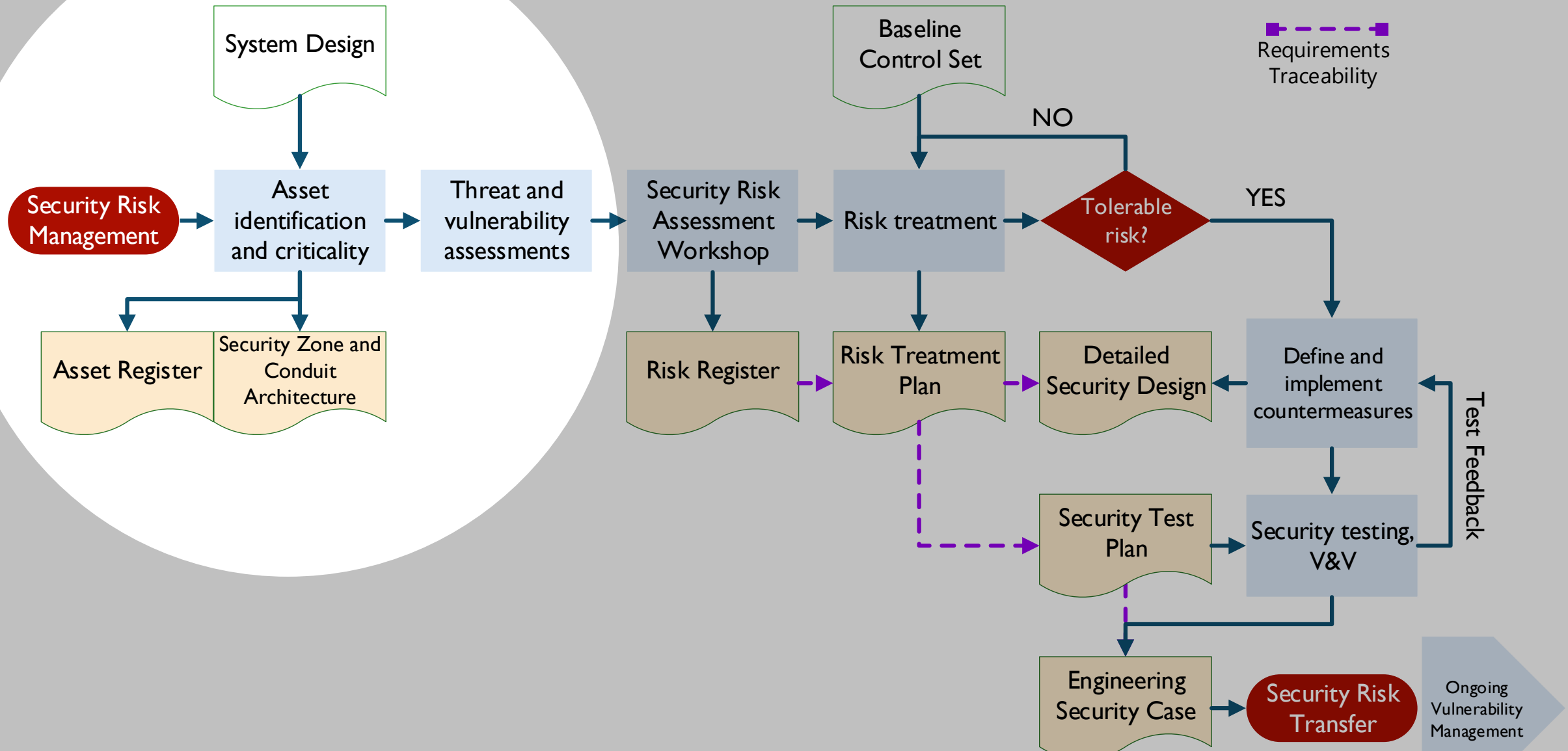
D. Minimise Impact

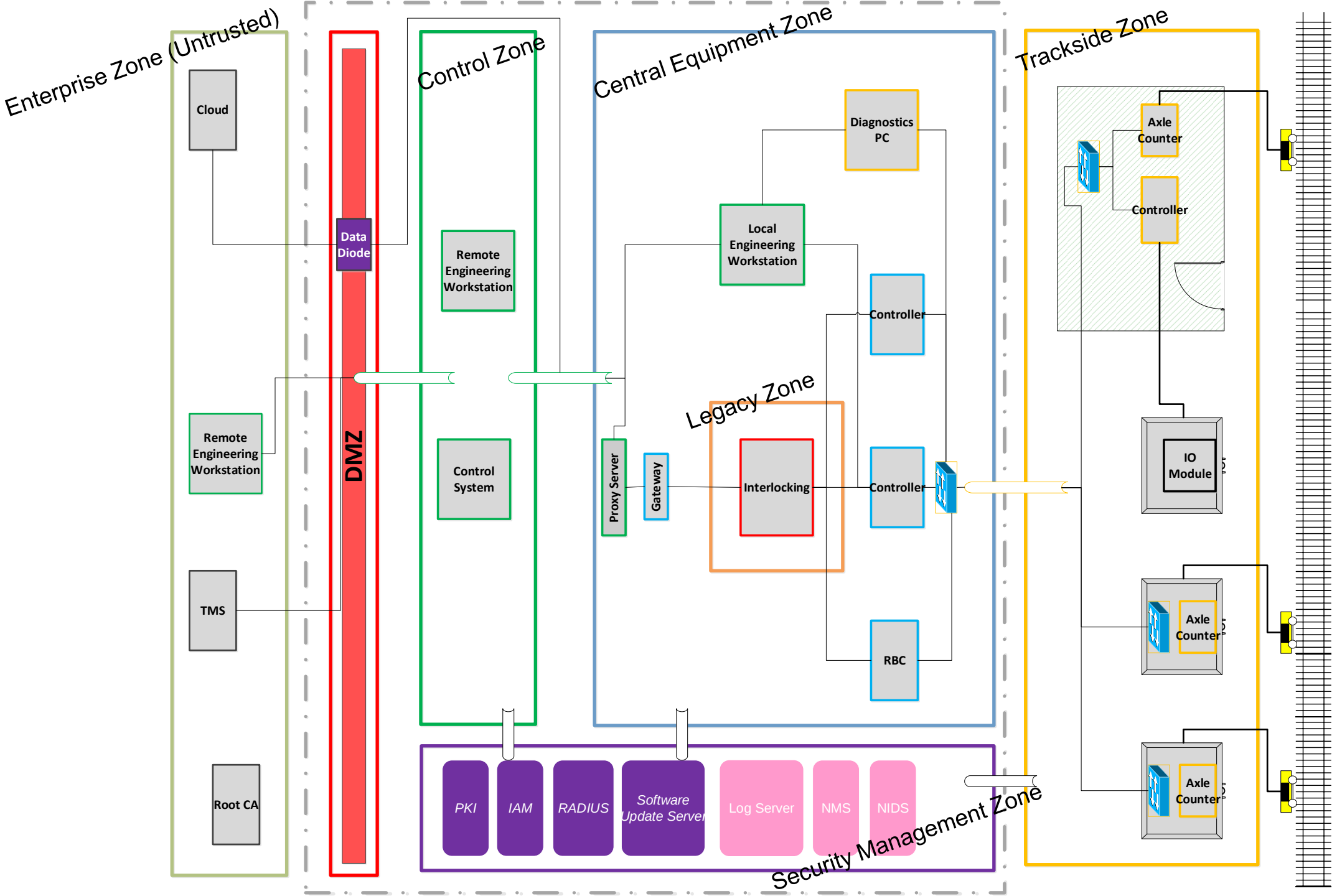
Procurement | Delivery | Operation

Cyber Security Risk Methodology

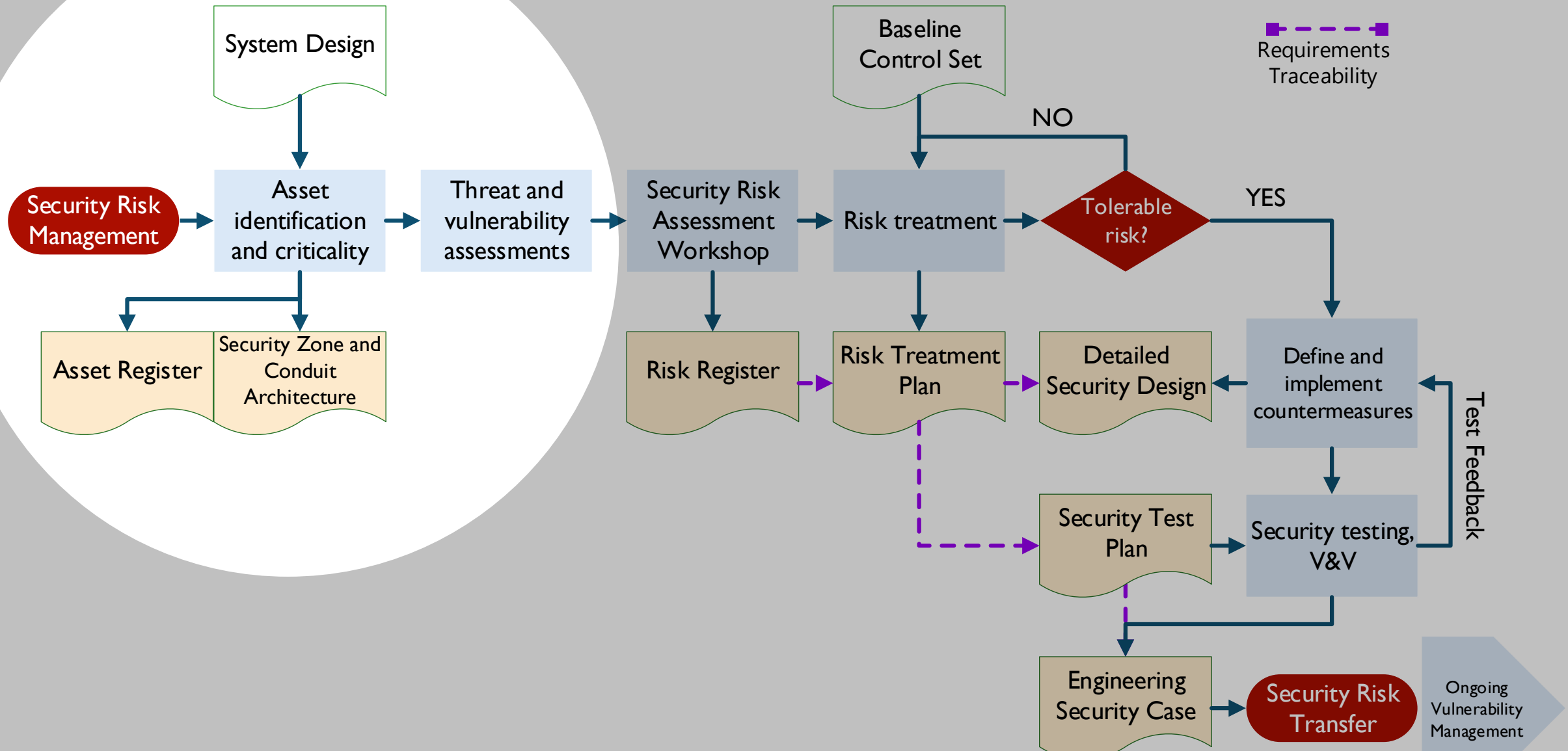


Cyber Security Risk Methodology




Enterprise Zone (Untrusted)
Cloud
Remote Engineering Workstation
TMS
Root CA
DMZ
Data Diode
Control Zone
Remote Engineering Workstation
Control System
Central Equipment Zone
Diagnostics PC
Local Engineering Workstation
Controller
Legacy Zone
Proxy Server
Gateway
Interlocking
Controller
RBC
Trackside Zone
Axle Counter
Controller
IO Module
Axle Counter
Axle Counter
PKI
IAM
RADIUS
Software Update Server
Log Server
NMS
NIDS
Security Management Zone

Cyber Security Risk Methodology



DRAGOS

National Cyber Security Centre
a part of GCHQ

BRITISH TRANSPORT POLICE

ALLANITE
Since 2017

Mode of Operation
Watering-hole and phishing leading to ICS recon and screenshot collection

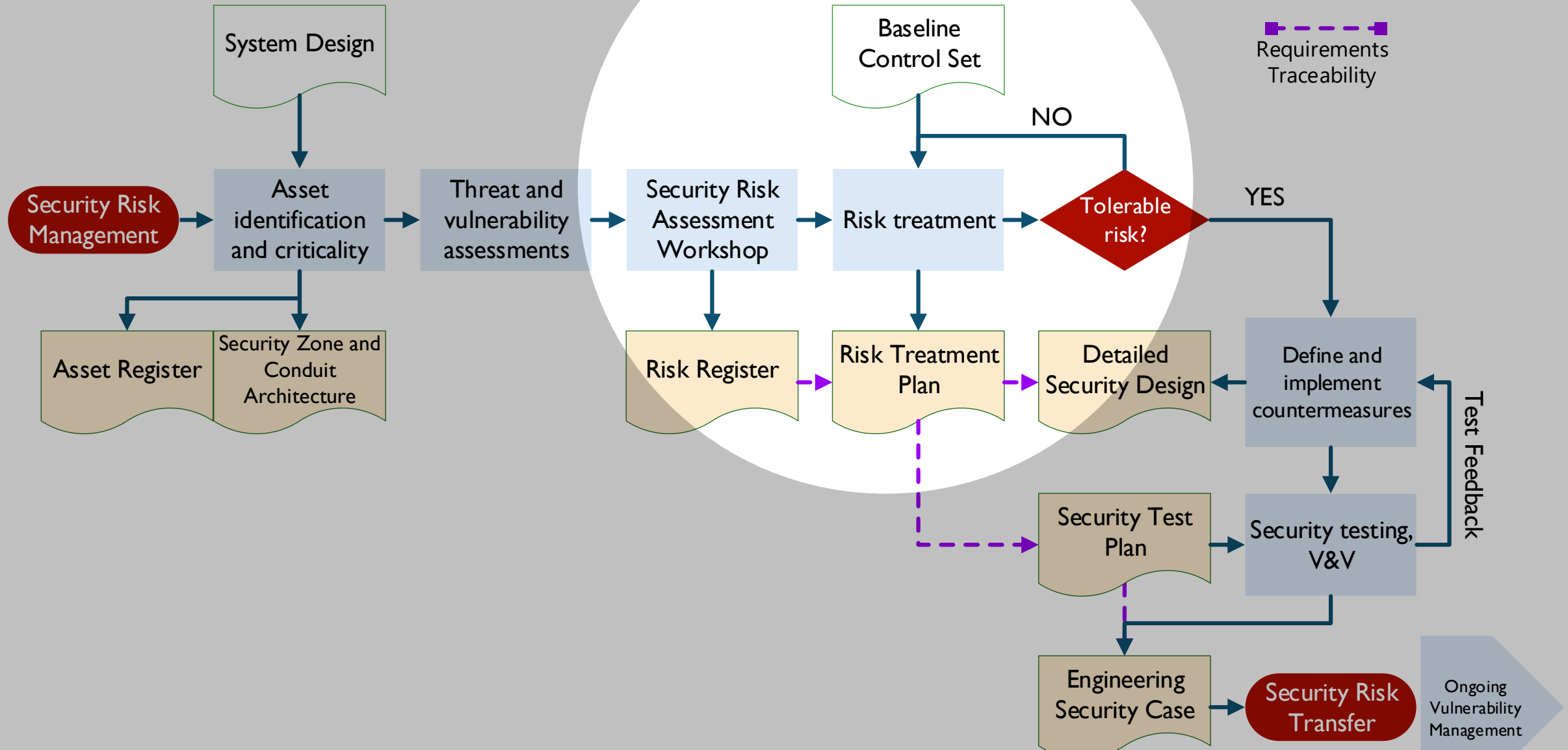
Capabilities
Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSExec

Victimology
Electric utilities, US & UK

Links
Palmetto Fusion

SIEMENS

Cyber Security Risk Methodology



User Authentication

SL1	• Shared account/password for each role
SL2	• Unique user accounts with role-based privileges
SL3	• Multifactor authentication (remote users only)
SL4	• Multifactor authentication

Device Authentication

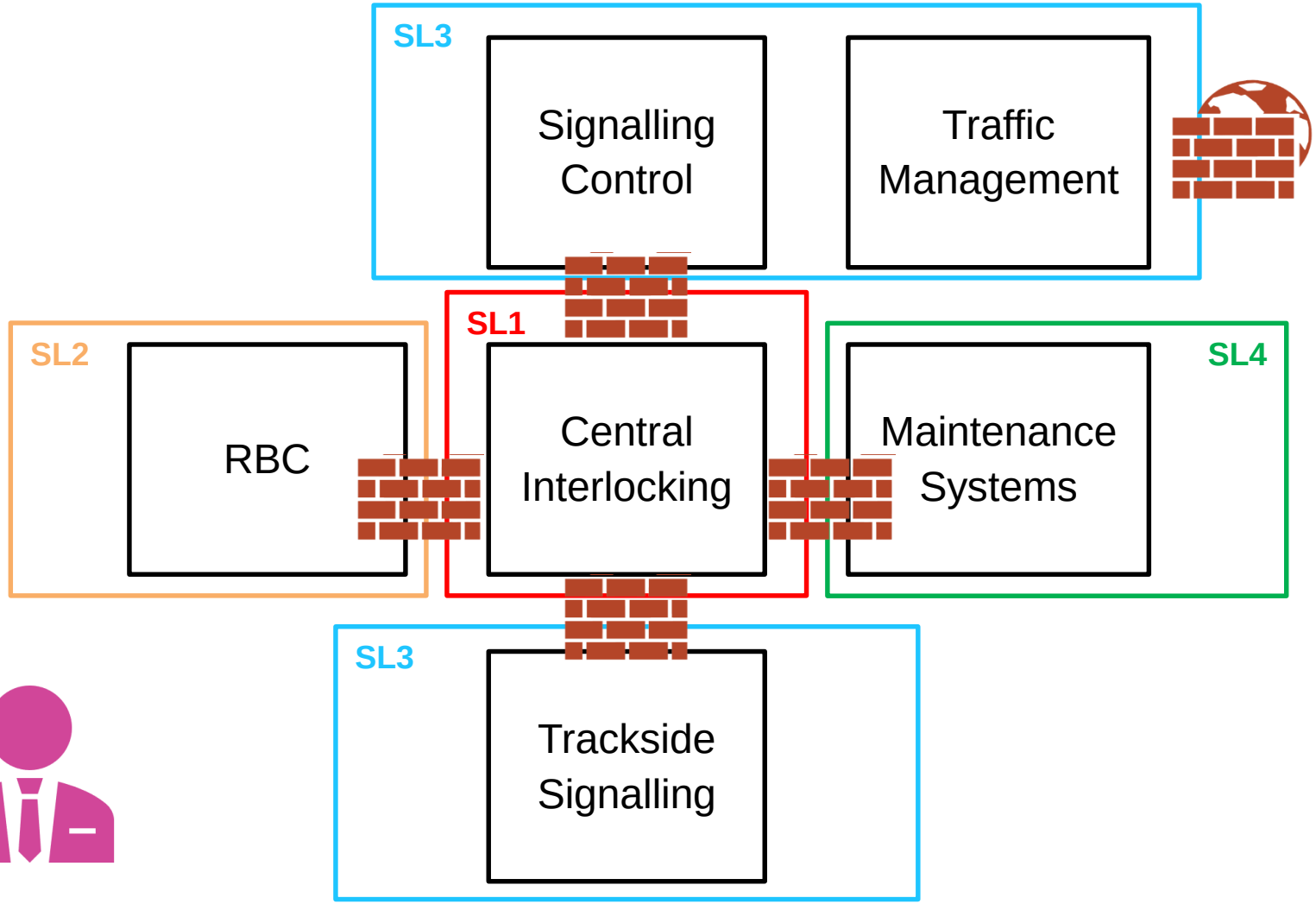
SL1	• No device authentication
SL2	• Shared credentials for authenticating devices to the system
SL3	• Unique keypair for authentication
SL4	• Unique keypair for authentication

Objective A: Manage Security Risk

How do we **procure** a
cyber secure signalling system?

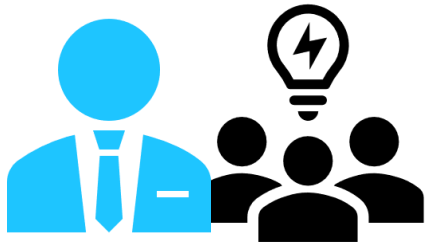
Defining Baseline Security Requirements

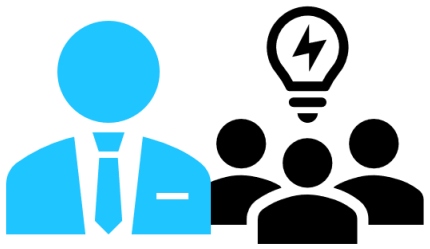
Probability		Severity: Catastrophic	Hazardous	Major	Minor	Negligible
		A	B	C	D	E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E



Cooperative Risk Assessment

Probability		Severity				
		Catastrophic	Hazardous	Major	Minor	Negligible
		A	B	C	D	E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

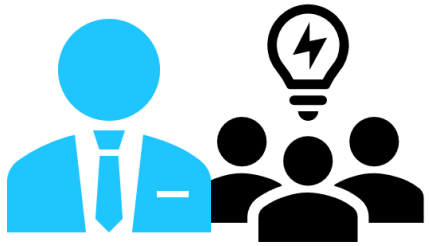


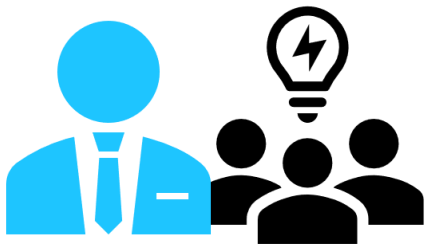


- Proactively engage the supply chain and invite a full breadth of stakeholders to the initial system-of-systems SRA.
- This will ensure:
  - Better security requirements are in place at tender stage.
  - Suppliers have better direction on where they should steer their product and solution security roadmaps.

Cooperative Risk Assessment

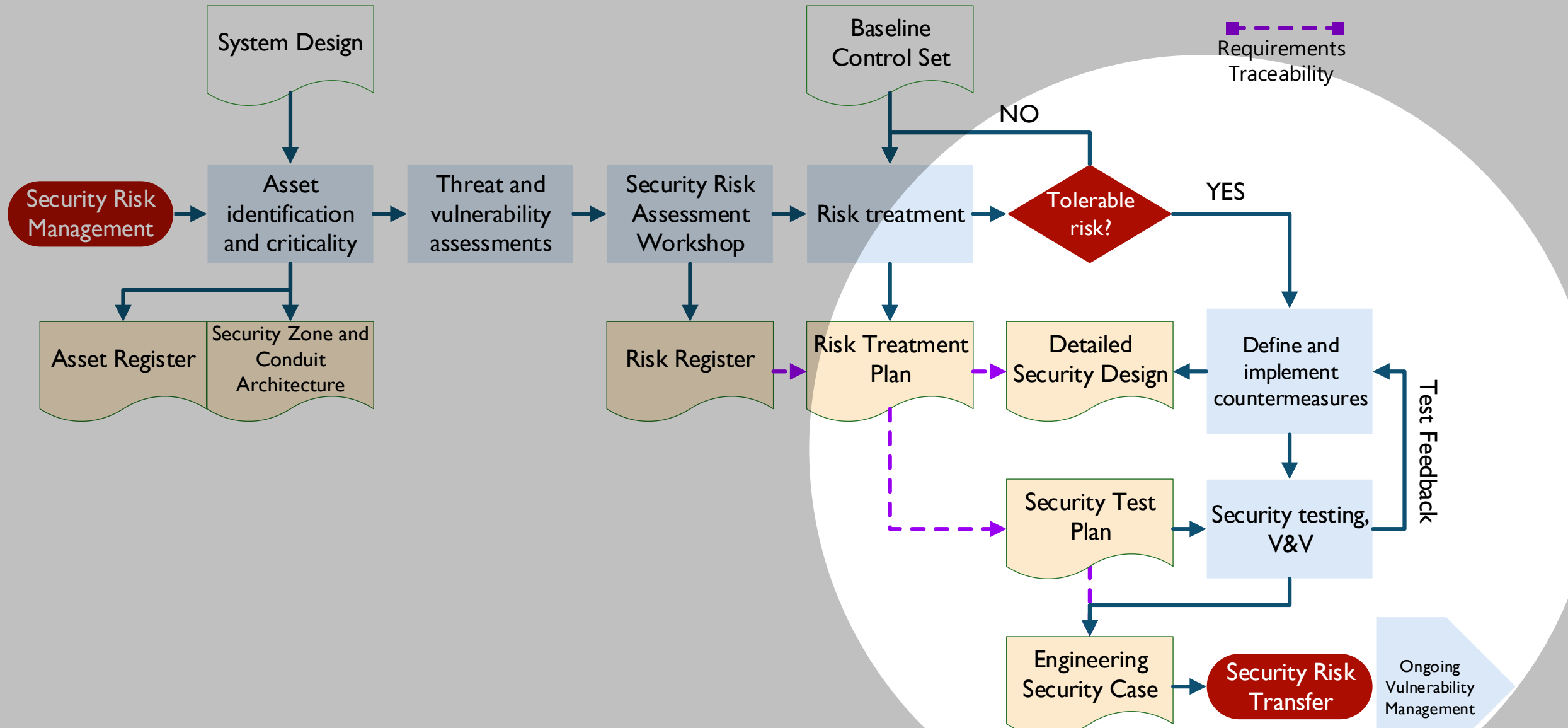
Probability		Severity				
		Catastrophic	Hazardous	Major	Minor	Negligible
		A	B	C	D	E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E





Commercial concerns quickly flare up when multiple vendors are placed together in a workshop to reveal potential vulnerabilities and weaknesses of key products and solutions.

Cyber Security Risk Methodology

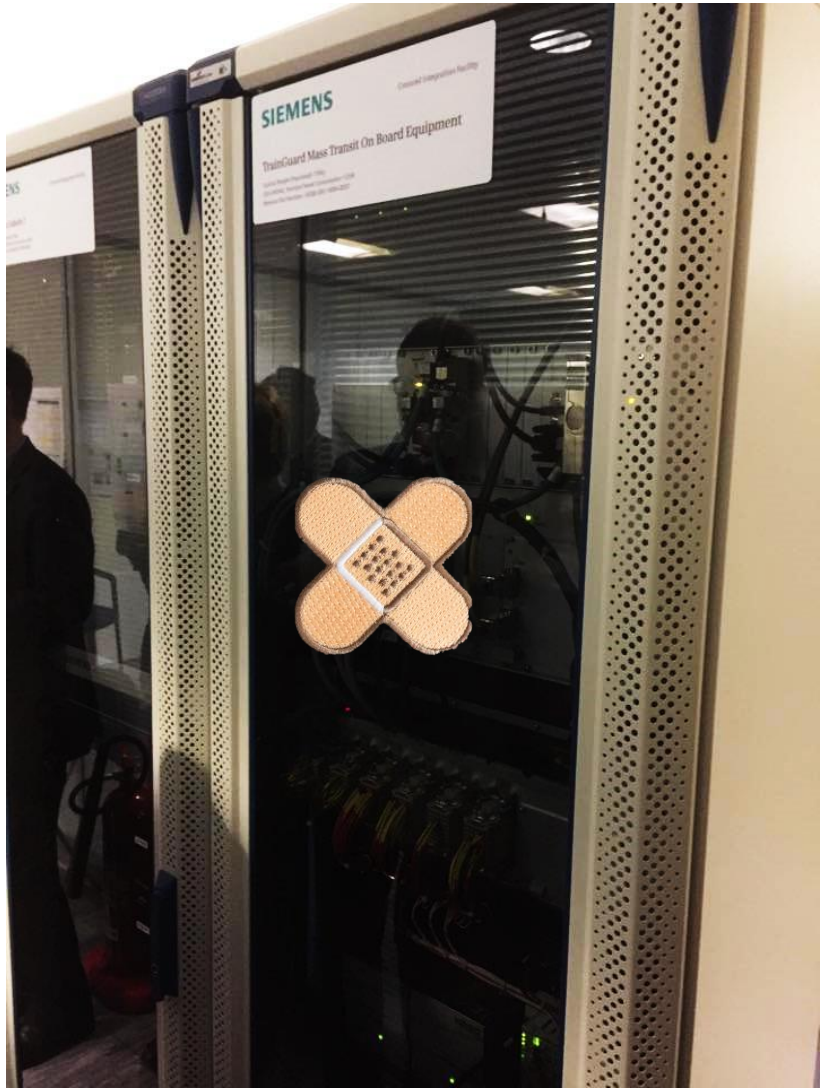


Objective B: Protect the System

How do we **patch** a cyber secure signalling system?

Operators, suppliers and vendors need clear agreements around

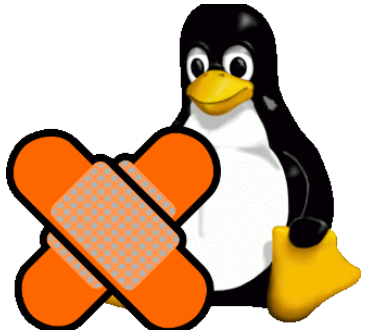
- Ongoing vulnerability testing;
- Patch development;
- Patch testing;
- Patch deployment.



Patching SIL-rated Components

Safety critical

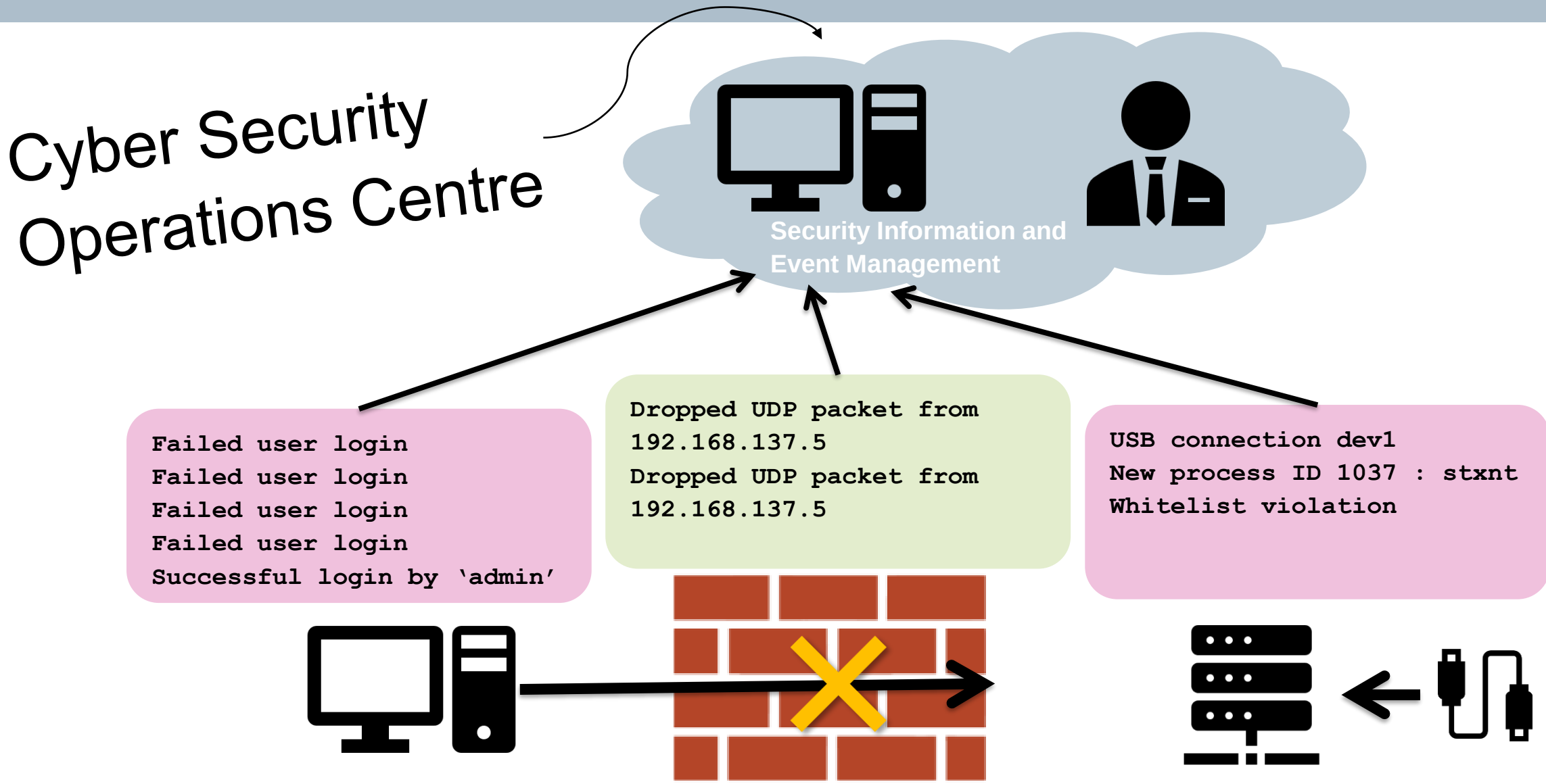
(e.g. interlocking logic)



Security critical

(e.g. network comms)

Objective C: Detect Incidents



Objective D: Minimise the Impact

See you at dinner!

Developing Cyber Resilience Together:

Industry Cooperation for a More Secure Railway