EIT Engineering Institute of Technology. | ECT Engineering College of Technology. | ECST Engineering College of Science and Technology. | IDC Technologies

How Cybersecurity Threats Influence Control Systems and Process Safety

Watch Webinar Recording Here

Paresh Kerai

OT Cyber Security Lead



About EIT

We are dedicated to ensuring that you receive a world-class education and gain skills that you can immediately implement in the workforce.

World-Class Australia Accredited Education

Our vocational programs and higher education degrees are registered and accredited by the Australian Government. We have programs that are also recognized under three international engineering accords.

Engineering Specialists

EIT is one of the only institutes in the world specializing in Engineering. We deliver professional certificates, diplomas, advanced diplomas, undergraduate and graduate certificates, bachelor's and master's degrees, and a Doctorate of Engineering.

Industry Experienced Lecturers

Our lecturers are highly experienced engineers and subject specialists with applied knowledge. The technologies employed by EIT, both online and on-campus, enable us to source our lecturers from a large, global pool of expertise.

Industry Oriented Programs

Our programs are designed by industry experts, ensuring you graduate with cutting-edge skills that are valued by employers. Our program content remains current with rapidly changing technology and industry developments.

Unique Delivery Model

We deliver our programs via a unique delivery methodology that makes use of live and interactive webinars, an international pool of expert lecturers, dedicated learning support officers, and state-of-the-art such as hands-on workshops, remote laboratories, and simulation software.

ECT delivers interactive and online **UK qualifications**. ECT is committed to providing students with a world-class education, where they acquire the knowledge and skills that are applicable and valued in industry.

- Bachelor of Engineering (Honours) in Industrial Automation
- Bachelor of Engineering (Honours) in Electrical Engineering
- Master of Science (Power System Analysis and Renewable Integration)
- Master of Science (Industrial Automation and Instrumentation Control)

Learn more here.

Registered UK Higher Education Provider | UKPRN: 10089771

ECST delivers a **South African accredited qualification** on-campus. ECST is committed to providing students with a world-class education, where they acquire the knowledge and skills that are applicable and valued in industry.

- Bachelor of Engineering Technology in Electrical Engineering (SAQA 123645)

Learn more here.

The Engineering College of Science and Technology (Pty) Ltd is provisionally registered with the Department of Higher Education and Training until 31/12/2028 as a private higher education institution under the Higher Education Act, 1997. Registration certificate no. 2025/HE07/007.

IDC Technologies – Practical Engineering & Technical Training

Founded in 1992 to deliver engineering and technical training that supports industry needs.

Specializes in professional development across:

- Electrical Engineering
- Instrumentation & Process Control
- Information Technology
- Mechanical Systems
- Project Management

Focuses on practical, real-world learning with skills that can be applied immediately in the workplace. Courses, workshops, and conferences are developed in consultation with industry to ensure relevance and impact. Supports engineers, technicians, and technical professionals in building job-ready expertise. Over 30 years of training experience with a strong presence across Australia and international markets. Continues to play a key role in upskilling the engineering workforce and strengthening technical capability across industries



Disclaimer

The courses and qualifications mentioned in this presentation are offered by separate legal entities operating in different jurisdictions – one in Australia, one in South Africa and one in the United Kingdom. Each entity is subject to its own local regulatory requirements and accreditation standards.

Prospective students should refer to the relevant institution's official website for accurate, up-to-date information specific to their location, including course availability, fees, regulatory status, and enrolment conditions.

- For the Engineering Institute of Technology (EIT) visit: https://www.eit.edu.au/
- For the Engineering College of Technology (ECT) visit: https://www.ect.ac.uk/
- For the Engineering College of Science and Technology (ECST) visit: https://www.ecst.ac.za/

Introduction – Presenter

Paresh Kerai



- OT Cyber Security Lead at MWS Risk
- BCompSC(Hons), BCompNS
- 15+ years of Experience in various roles in cyber security and technology supporting:
  - Cyber Security Consulting
  - Cyber Security Engineering
  - Software Product Management
- Strategic technology and infrastructure engineer who has worked with leading-edge cybersecurity and threat intelligence solutions for industrial control systems and enterprise networks
- Provided expert consultation for both private and government sectors in various security standards, including AS IEC 62443 standards, NIST CSF, SOCI Act and AESCF
- paresh.kerai@mwsrisk.com

MWS Risk

Integrated engineering and risk expertise

We help industrial organisations understand and manage technical risk, supporting informed engineering decisions.

Supporting projects from concept through to operation.

Our capabilities

- Technical Risk Management
- Process Safety
- Industrial Fire Engineering
- Hazardous Areas
- Functional Safety
- Cyber Security
- Safety in Design across the project lifecycle

Why are we talking about Cyber Risk?

- Cyber risk matters to process safety because the digital systems we rely on to control and protect the process can themselves become pathways for hazardous events or loss of protection.



Defining Cyber Security in IT vs OT

Information Technology (IT):

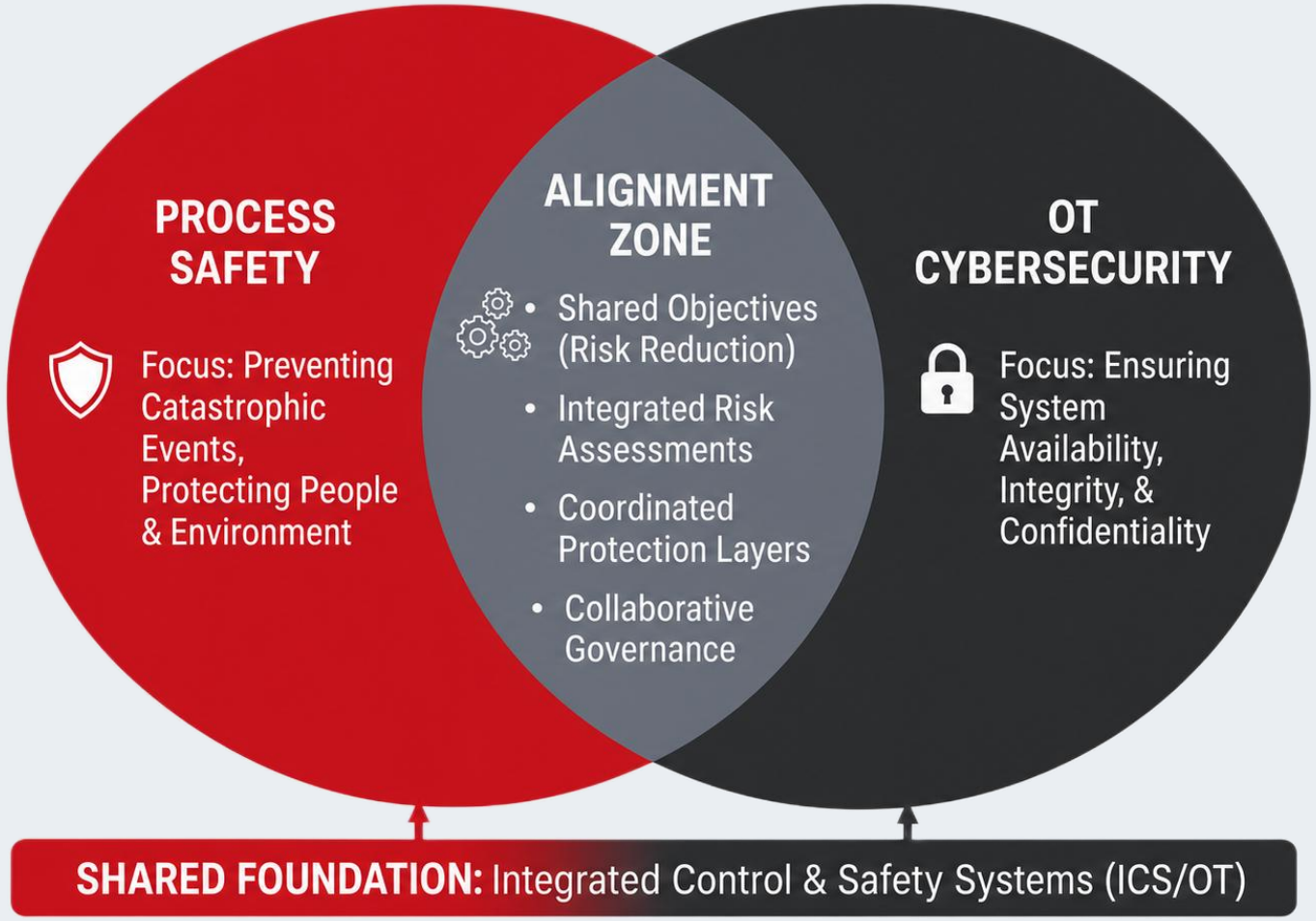
Focuses on preventing intentional or unintentional access to sensitive data, ensuring secure internet connections, and detecting/preventing cyberattacks. Priorities are Confidentiality, Integrity, and Availability.

Operations Technology (OT):

Focuses on preventing intentional or unintentional interference with the intended operation of industrial automated and control systems. Priorities are Safety, Availability, Integrity, and Confidentiality. For OT, preserving safety and operational availability is paramount, whereas for IT, data confidentiality often takes precedence.



Alignment of Process Safety and OT Cyber Security



Two Sides of the Same Coin

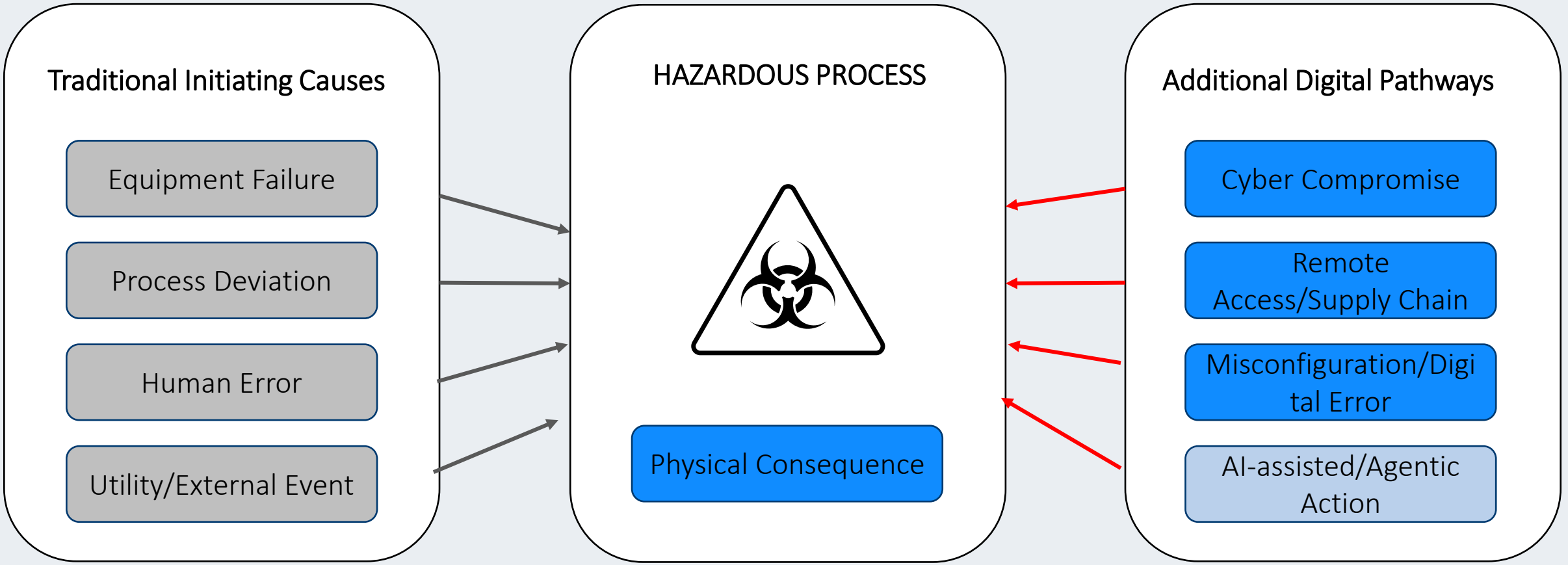
The Same Devices, The Same Consequences

- Process safety and cybersecurity are no longer separate disciplines. They are two sides of the same operational risk coin, protecting the same critical assets.
- Controlled by the same system and the same operator.

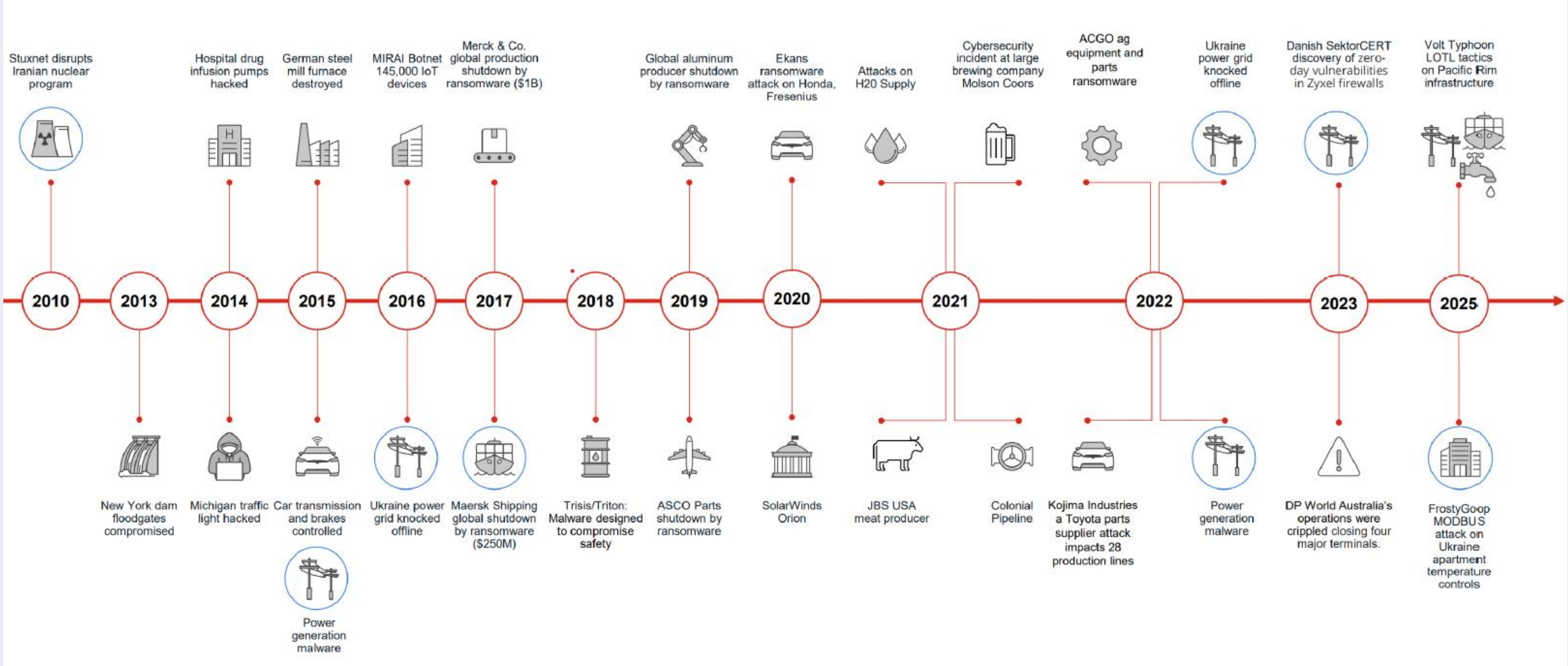


- Loss of life
- Environmental releases
- Asset loss
- Reputation

Initiating Factors



Cyber Security Incidents Targeting OT Systems



Cyber Security Incidents

Jun–Dec 2017

01

TRITON / TRISIS Attack

Petrochemical plant, Saudi Arabia

First-ever malware built to target a Safety Instrumented System (SIS). Attackers pivoted from IT to OT and reprogrammed Schneider Electric Triconex safety controllers. A software bug tripped a safe-state shutdown, exposing the intrusion.

Impact: Attributed to Russia. Designed to disable safety systems — potential loss of life.

FY 2023–24

02

NSW Energy Supplier DDoS

Energy provider, New South Wales (AU)

Reported in the ASD Annual Cyber Threat Report 2023–24. A Distributed Denial-of-Service (DDoS) attack disrupted an internet-facing connection linked to the supplier's operational technology environment.

Impact: Highlights DDoS over-representation in critical infrastructure (~2× other sectors) at the IT/OT boundary.

Jul 2026

03

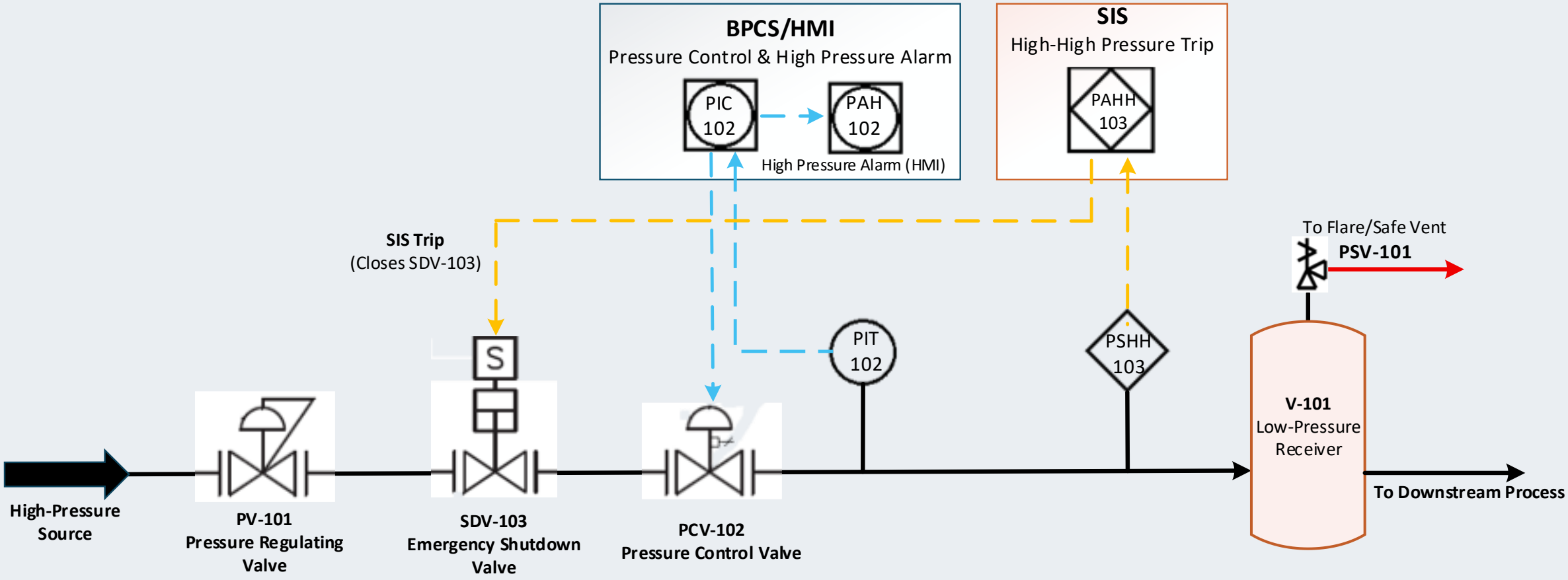
UK Power Generator Shutdown

Small-scale generator, United Kingdom

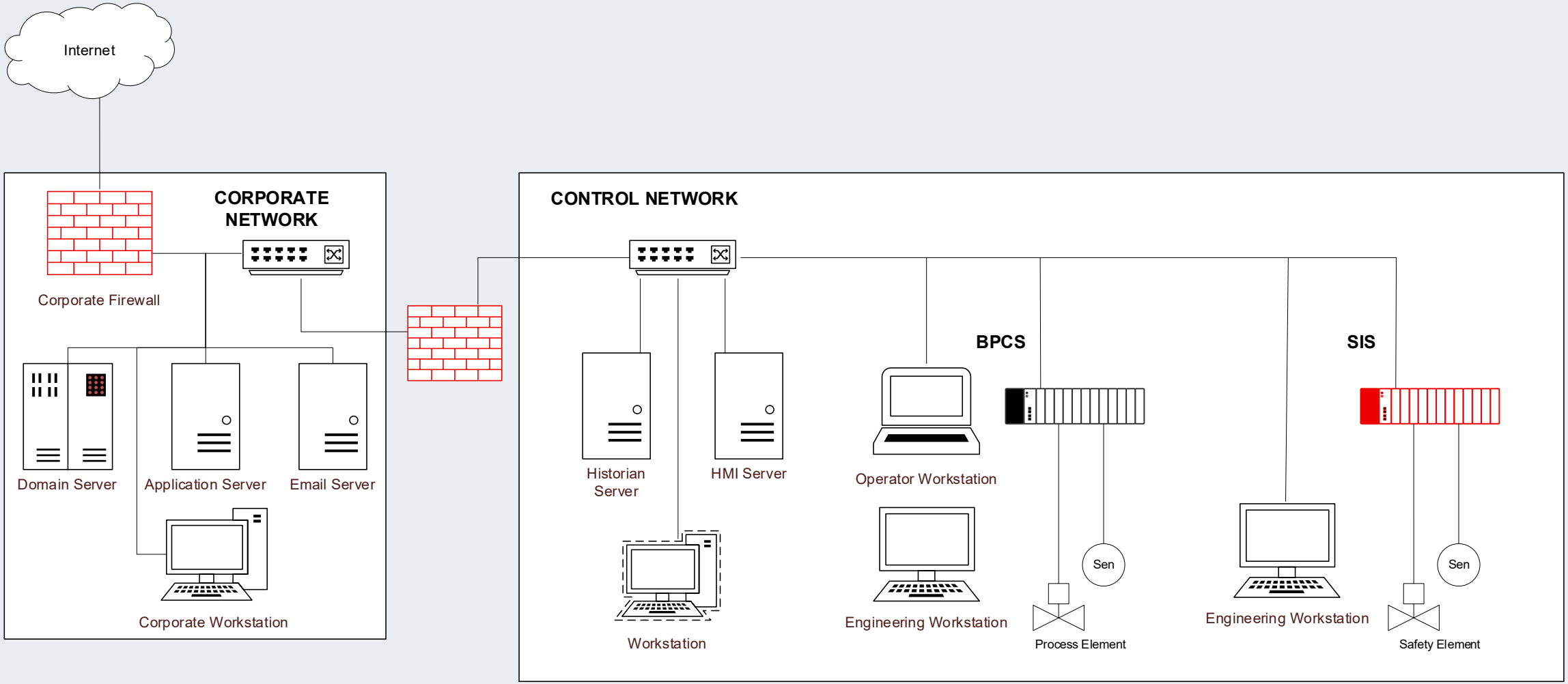
A cyberattack forced a small UK power generator offline for four days. Press reporting attributes it to Iran-linked actors (IRGC "CyberAv3ngers"), known for targeting internet-exposed PLCs.

Impact: No risk to the wider grid. Prompted NCSC guidance on protecting internet-exposed OT devices.

Back to High Pressure Scenario



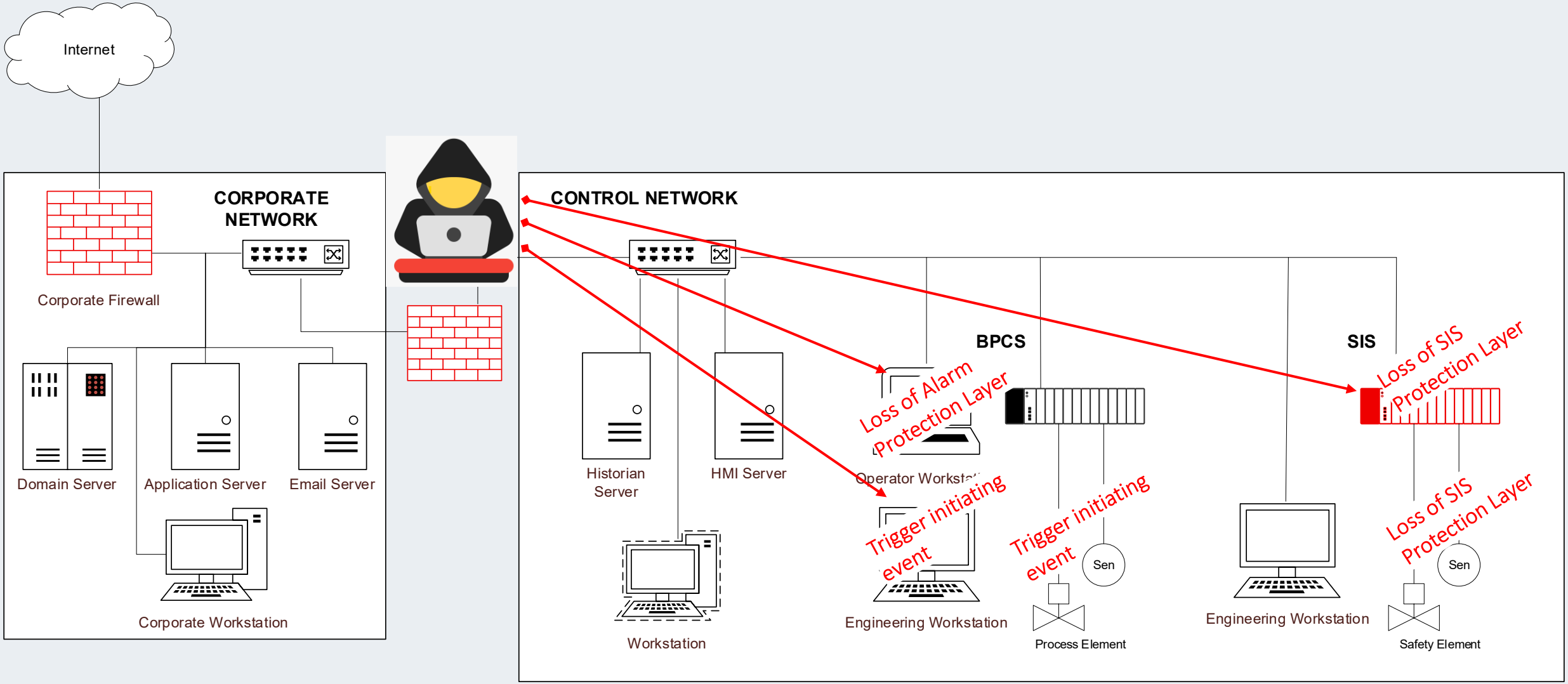
Control System Architecture Behind the P&ID



Traditional LOPA Scenario

LOPA Scenario	Initiating Event		Consequence	Protection Layers		MEF
Exceed Maximum Design Working Pressure of Vessel	Failure of pressure regulating valve	0.1	Leading to over pressure of downstream vessel, potential loss of containment and potential fatality (TEF = 1 x 10^-5 /yr)	BPCS pressure control loop.	0.1	1 x 10^-5 /yr
				High Pressure alarm and operator response	1	
				High-High Pressure SIS Trip closes the isolation valve	0.1	
				Pressure relief valve PSV	0.01	

Cyber Compromise Impact



Traditional LOPA Scenario

LOPA Scenario	Initiating Event		Consequence	Protection Layers		MEF
Exceed Maximum Design Working Pressure of Vessel	Failure of pressure regulating valve	0.1	Leading to over pressure of downstream vessel, potential loss of containment and potential fatality (TEF = 1 x 10^-5 /yr)	BPCS pressure control loop	0.1	1 x 10^-5 /yr
				High Pressure alarm and operator response	1	1 x 10^-3 /yr
				High-High Pressure SIS Trip closes the isolation valve	0.1	
				Pressure relief valve PSV	0.01	

AS IEC 62443 Standards

What Are the AS IEC 62443 Standards?

The AS IEC 62443 series of standards was developed by the ISA99 Committee and the IEC Technical Committee to define requirements and processes for implementing and maintaining electronically secure control systems.

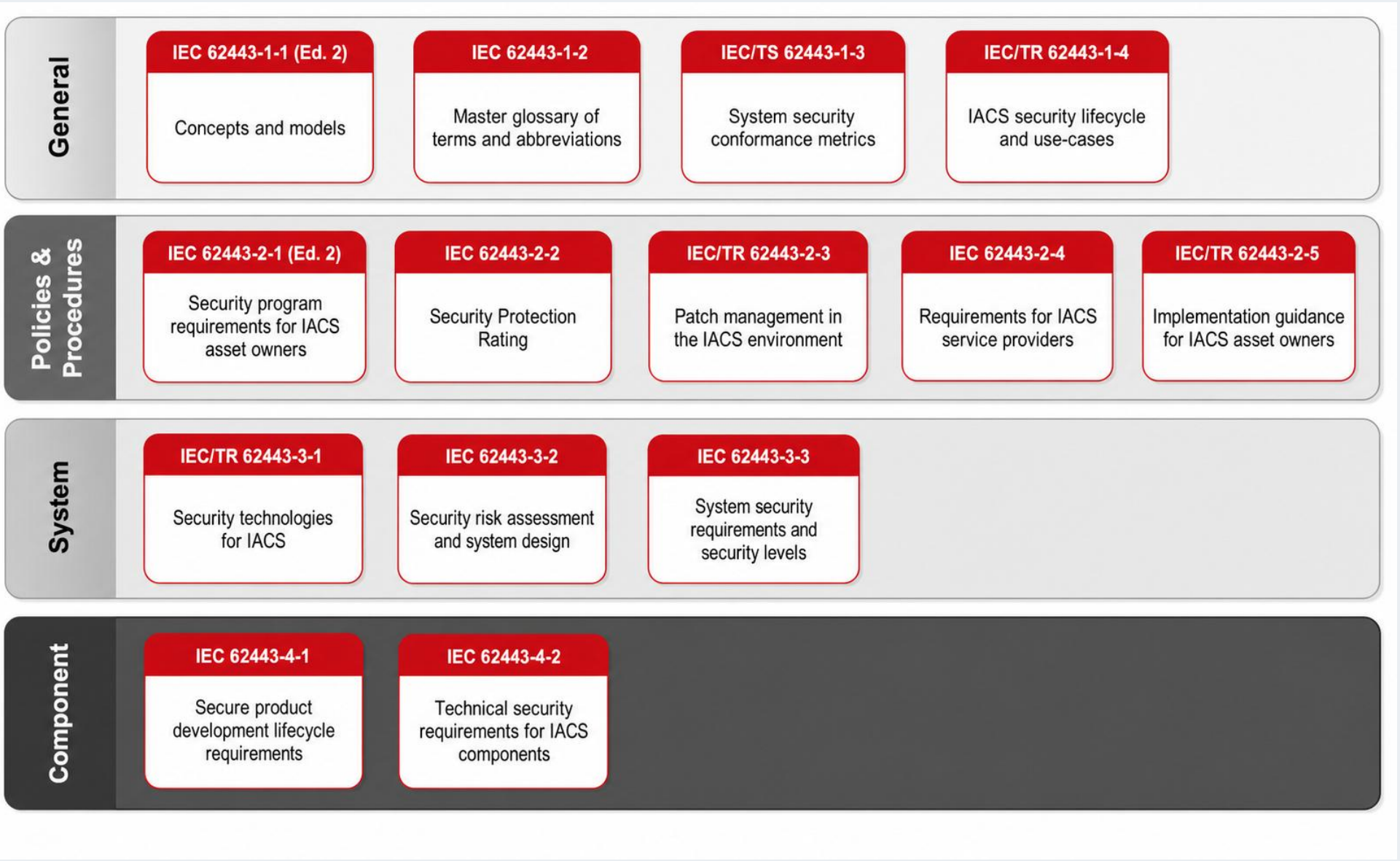
- **Standardised Security Requirements**: The AS IEC 62443 standards establish consistent security requirements across different industrial sectors and environments

- **Risk-Based Approach**: Organisations can prioritise security investments based on actual risk assessments rather than generic security measures

- **Lifecycle Integration**: Security considerations are embedded throughout the entire system lifecycle, from design to decommissioning

- **Stakeholder Alignment**: Clear guidance for asset owners, system integrators, and component suppliers ensures coordinated security efforts

AS IEC 62443 Relevance



AS IEC 62443 Cyber Security Lifecycle

Assess Phase

- Gap Assessment (Scope and Identify Critical Assets and Systems)
- Establish Zone and Conduits
- Analyse Cyber Security Risk for each Zone/Conduit
- Cyber Security Requirements Specification (Assing SL to each Zone/Conduit)

Implement Phase

- Apply Cyber Security Countermeasures
- Validation of Design (Achieved SL)
- Construction
- Verification (FAT and SAT)

Maintain Phase

- Maintain Cyber Security (Patching and Anti Virus Management)
- Monitor Cyber Security (Intrusion Detection System, SIEM, etc.)
- Management of Change (MoC) of System or Decommission
- Periodic Risk Assessments, Audits and Compliance

Example Requirement from AS IEC 62443.4.2

Segment the control system via **zones and conduits** to limit the unnecessary flow of data.

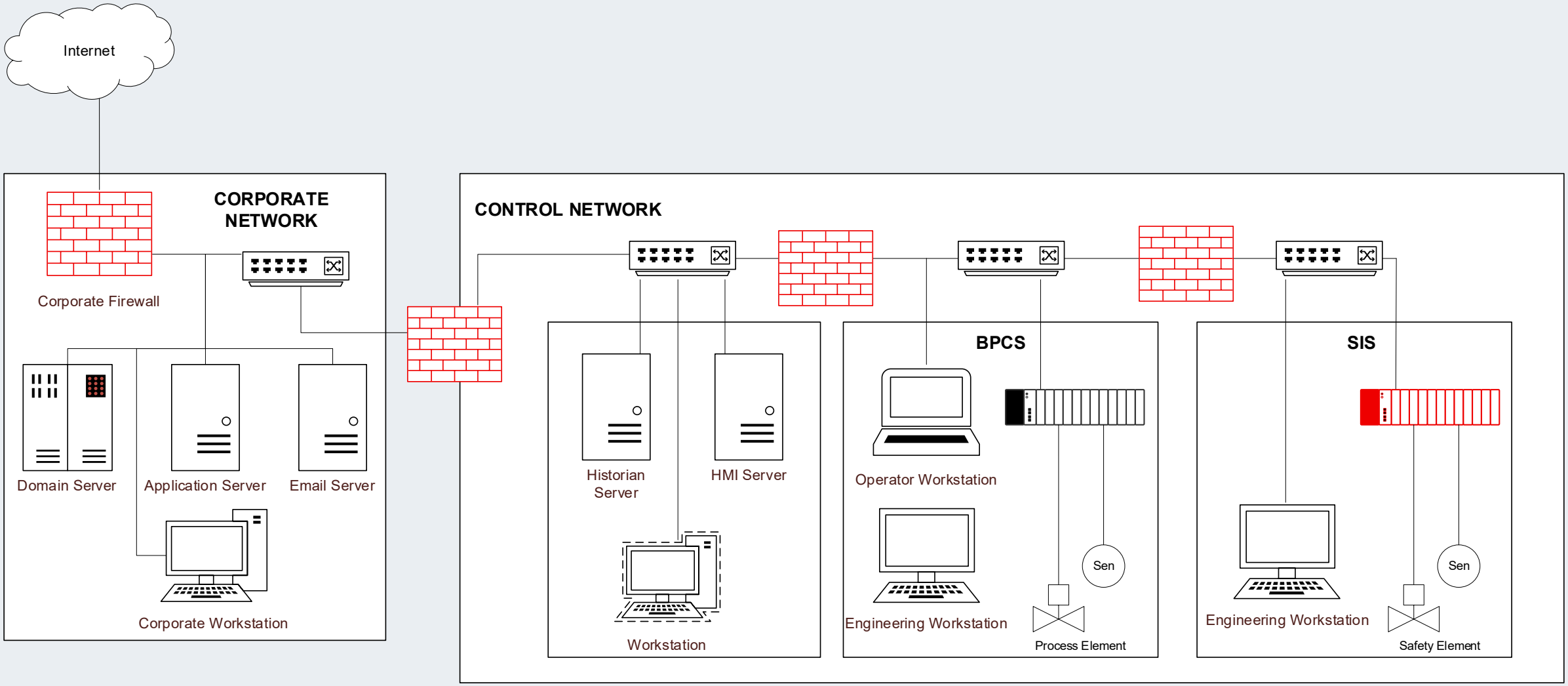
9.3.1 REQUIREMENT

"Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality."

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or **ingress**, of network traffic *into* a control system, and reduce the spread, or **egress**, of network traffic *from* a control system.

Functional Requirement - Restricted data flow - Network segmentation -	SL 1	SL 2	SL 3	SL 4
Prevent the casual or coincidental circumvention of zone and conduit segmentation.	✓	✓	✓	✓
Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation.		✓	✓	✓
Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.			✓	✓
Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.				✓

Cyber Defence Architecture



A Special Note: Safety Related Control System

There are already mandatory requirements around security requirements for safety and control systems.

Standard / Legislation	Clause / Regulator	Requirement	Status
Security of Critical Infrastructure (SOCI) Act 2018	Dept of Home Affairs	• Asset Registration • Cyber Incident Reporting • Risk Management Program • Data Provider Notification	Regulated
Australian Energy Sector Cyber Security Framework (AESCF)	AEMO	Cyber security maturity framework for the energy sector	Regulated
AS 61511.1	Section 8.2.4	A security risk assessment shall be carried out	Mandatory
AS 61511.1	Section 11.2.12	The design of the SIS shall provide the necessary resilience against the identified security risks	Mandatory
AS IEC 62443 – Security for industrial automation and control systems	IACS standards series	Suggested guidance for the process to assess threats and vulnerabilities	Guidance

Integrated Process Safety Management

PROCESS SAFETY

PHA / HAZOP • LOPA • barrier management • operating envelope

FUNCTIONAL SAFETY

SIF identification • SIL / SRS • SIS lifecycle • AS IEC 61511.1 security risk assessment & resilience

OT CYBERSECURITY

System boundary • threat/risk assessment • zones & conduits • security requirements

What Organisation Should Do Differently

1 **Identify safety-critical digital dependencies**

Know which control, alarm, SIS, remote-access and support systems underpin process-safety barriers.

2 **Complete structured OT cyber risk assessment**

Use AS IEC 62443 methods at the system level, then detailed zones/conduits where required.

3 **Implement and verify security requirements**

Treat architecture, access control, segmentation, monitoring and recovery as engineered controls.

4 **Maintain assurance through the lifecycle**

Integrate cyber into management of change, testing, incident response, governance and periodic review.

The objective is not more paperwork. It is to preserve confidence in the systems and barriers on which safe operation depends.

Key Takeaways

Connectivity has changed the risk

- Cyber and process safety can no longer be managed in isolation.

Cyber can cause physical harm

- Digital compromise can defeat process safeguards.

Vulnerabilities sit at the seams

- Legacy interfaces, IT/OT convergence and the supply chain.

AI cuts both ways

- Use it defensively before it's used against you.

Integrate cyber as part of your risk strategy

- Consider and implement cyber as part of process safety, operational risk and assurance.

Conclusion

- While process safety management has evolved significantly from historical lessons, the emergence of sophisticated cyber threats demands a parallel and integrated approach to security.
- Awareness, comprehensive risk assessments, and robust layered defences are essential to protect critical infrastructure from both traditional and digital hazards.

EIT Engineering Institute of Technology. | ECT Engineering College of Technology. | ECST Engineering College of Science and Technology. | IDC Technologies

Thank You!

Upcoming Webinars

Register today! https://www.eit.edu.au/news-events/events/?tribe_events_cat=webinars/

- Doctoral Research Toolbox Chat With Emeritus Professor Akhtar Kalam - 5 November
- Modelling Pre- and Post-Localization Behavior of Partially Saturated Soils - 6 November
- The Transformer That Changed Tap Position by Itself - 12 November
- EIT Africa Open Day: Engineering Your Future. From Africa. To the World. - 14 November
- Shape Memory Alloys for Resilient Civil Structures: Applications, Innovations and Future Prospects – 18 November

Upcoming Courses

Please note: courses listed below are subject to their own regulatory requirements—refer to the relevant website for further information.

Engineering Institute of Technology (EIT) *Australian Accredited Qualifications & Short Courses*	Start Date
Professional Certificate of Competency in Instrumentation, Automation and Process Control	1 December 2026
Online - Graduate Certificate in Industrial Automation Engineering	4 January 2027
Graduate Certificate in Industrial Automation and Machine Learning	4 January 2027
Online - Master of Engineering (Industrial Automation)	4 January 2027
52886WA Advanced Diploma of Industrial Automation Engineering	19 January 2027
Professional Certificate of Competency in Programmable Logic Controllers (PLCs) & SCADA Systems	27 January 2027
Professional Certificate of Competency in Safety Instrumentation Systems for Process Industries	9 February 2027
Professional Certificate of Competency in Digital Twins and Simulation Monitoring	9 February 2027
Professional Certificate of Competency of Practical Troubleshooting and Problem Solving of PLCs and SCADA Systems	16 February 2027
Professional Certificate of Competency in Industrial Control Systems Cybersecurity	13 April 2027
Professional Certificate of Competency in Industrial Data Communications	13 April 2027

Upcoming Courses

Please note: courses listed below are offered by separate institutions in the UK and South Africa, each subject to their own regulatory requirements - refer to the relevant website for location-specific details.

Engineering College of Technology (ECT) *UK qualifications*	Start Date
Bachelor of Engineering (Honours) in Industrial Automation	8 February 2027
Bachelor of Engineering (Honours) in Electrical Engineering	8 February 2027
Master of Science (Power System Analysis and Renewable Integration)	1 February 2027
Master of Science (Industrial Automation and Instrumentation Control)	1 February 2027

Engineering College of Science and Technology (ECST) *South African accredited qualification & ECSA-endorsed*	Start Date
Bachelor of Engineering Technology in Electrical Engineering	23 February 2027

EIT
Engineering Institute of Technology.

ECT
Engineering College of Technology.

ECST
Engineering College of Science and Technology.

Contact Us:

Website
www.eit.edu.au

Head Office
6 & 8 Thelma Street, West Perth,
Perth, WA 6005

Phone
Inside Australia: 1300 138 522
Outside Australia: +61 8 9321 1702

Email
webinars@eit.edu.au

Courses
https://www.eit.edu.au/schedule/

Website
www.ect.ac.uk

Head Office
Whittle Way, Stevenage SG1 2FS,
United Kingdom

Phone
Inside UK: 0208 335 4014
Outside UK: +44 208 335 4014

Programmes
https://www.ect.ac.uk/programmes/

Website
www. ecst.ac.za

Head Office
Unit 3, Elevation Gardens,
Elevation Close, Waterfall
Office Park, Midrand, 1686

Phone
Within South Africa: 010 823 4497
Outside South Africa: +27 11 823 4497

Programmes
www.ecst.ac.za/course-types/bachelor-of-engineering/