OT CYBERSECURITY

WHAT, WHY & YOU

Craig Morris

ABOUT ME

- Director OT Cybersecurity – KPMG Australia
- Ex-CISO (Middle East)
- Ex-Asset Owner

Thoughts are my own and do not represent the views of any of my employers or clients, past, present or future.
Any vendor names are copyright and do not represent an endorsement or opinion.
Also: Not a Lawyer, Engineer or a Doctor – Sorry Parental Units….

SAFETY MOMENT

HEARING PROTECTION BLOCKS NOISE FROM REACHING YOUR EARDRUM BY FORMING AN AIRTIGHT SEAL

Industrial Noise Source	Decibels
Normal conversation	60
Office noise	70
Gas Flare	95
Steel Mill – Factory floor	110
Heavy machinery	120
Turbine Generator	133

- Do not wear hats underneath muff-style hearing protectors.
- Foam- and insert-style hearing protectors must be fully inserted into the hearing canal to be effective.
- Extremely noisy work environments may require wearing **both** foam-style plugs and a muff-style hearing protector
- Check with local HSE/Safety Representative.

TIP: Always lead a discussion with a safety moment

IMPORTANCE OF SAFETY

- Industrial environments consist of mechanical, electrical and chemical processes
- Significant risk of injury, death, environmental impact
- Everyone wants to go home safely

Williams Olefins Plant Explosion and Fire | CSB 2013, 2 Fatalities, 167 IP's. Overpressure event in an offline reboiler, vessel was isolated from pressure relief resulting in explosion

Example HSE **Safety** Card
Source: North Oil Company Qatar

WHAT

WHAT IS OPERATIONAL TECHNOLOGY?

Operational Technology (OT)

"… is hardware and software that ***detects or causes a physical change,*** *through the direct monitoring and/or control of industrial equipment, assets, processes and events".*

OT Cybersecurity

"Practices and technologies used to (a) protect people, assets, and information, (b) monitor and/or control physical devices, processes and events, and (c) initiate state changes to enterprise OT systems."

Gartner 2014

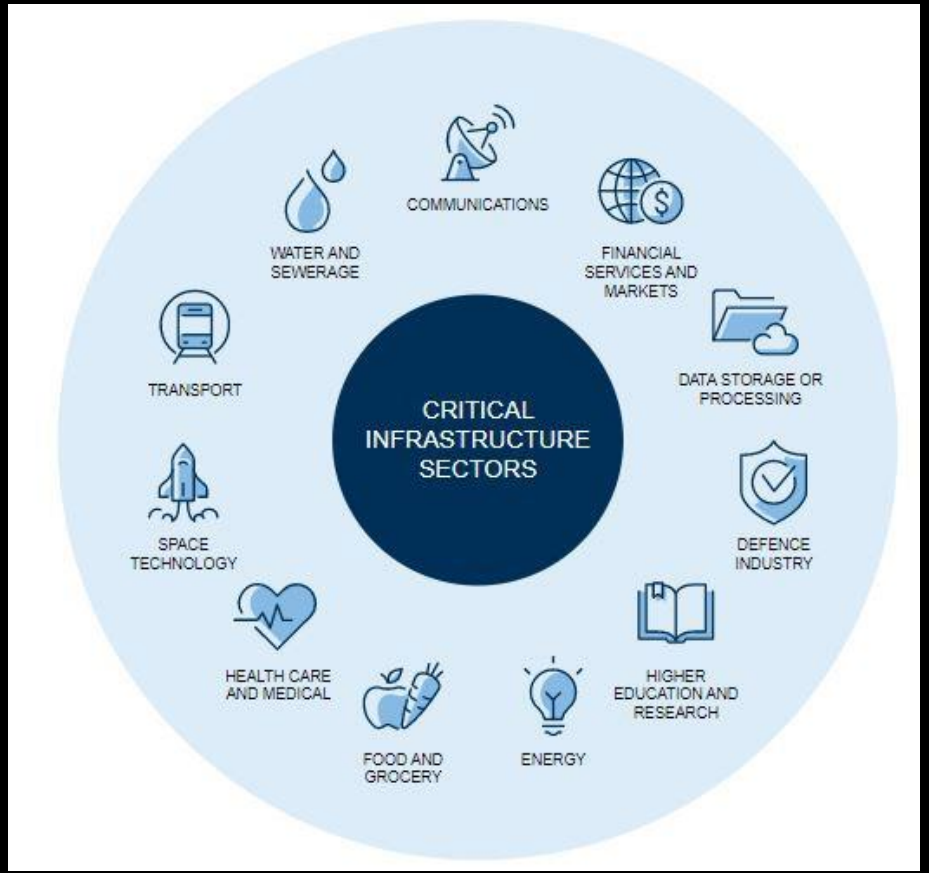
WHAT IS CRITICAL INFRASTRUCTURE?

Critical Infrastructure (CI)

"those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would ***significantly impact the social or economic wellbeing*** *of the nation or* ***affect Australia's ability to conduct national defence and ensure national security***"

Australian Government - 2017

OT ≠ CI



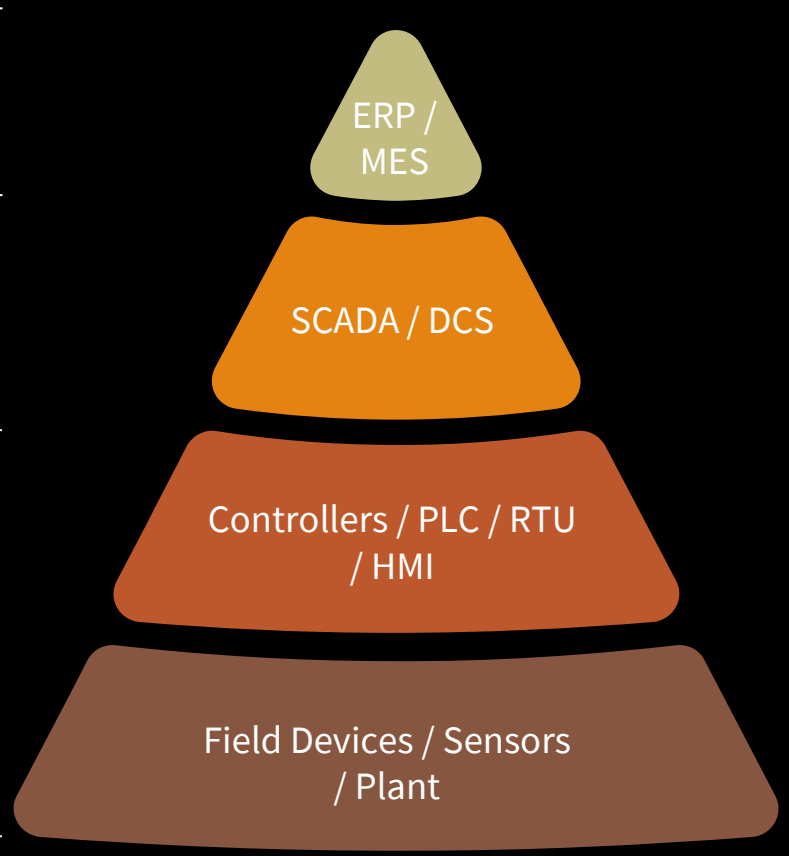
SOCI Act 2018 – 11 Sectors
Diagram : https://www.lexology.com/library

AUTOMATION PYRAMID

- Dashboarding,
- Performance Metrics
- Stock Management
- Business Decisions

- Supervision / Monitoring
- Historical analysis
- High-Level Control
- Batching / Scheduling

- Source of data for upstream
- Low-Level Operator Control
- Low-Level Automatic Control
- Safety systems
- Interface to Electrical / Chemical / Hydraulic / Mechanical processes



OT AND THE PURDUE (ISA95) MODEL

Engineering Workstation

- Develop, download code to PLC/RTU's etc.. Usually has access to all devices. **High Risk, need to be protected**

Programmable Logic Controller (PLC)

- Lowest level of control. Used in both DCS & SCADA to provide field-level, local control of process.

Remote Terminal Unit (RTU)

- Radio interface. Used to communicate with remote field devices. PLCs with radio communication capabilities are also used in place of RTUs.

Data Historian

- A centralized database supporting data analysis using statistical process control techniques. E.g.. OSISOFT, PI, IP21 *High Risk, needs to be protected*

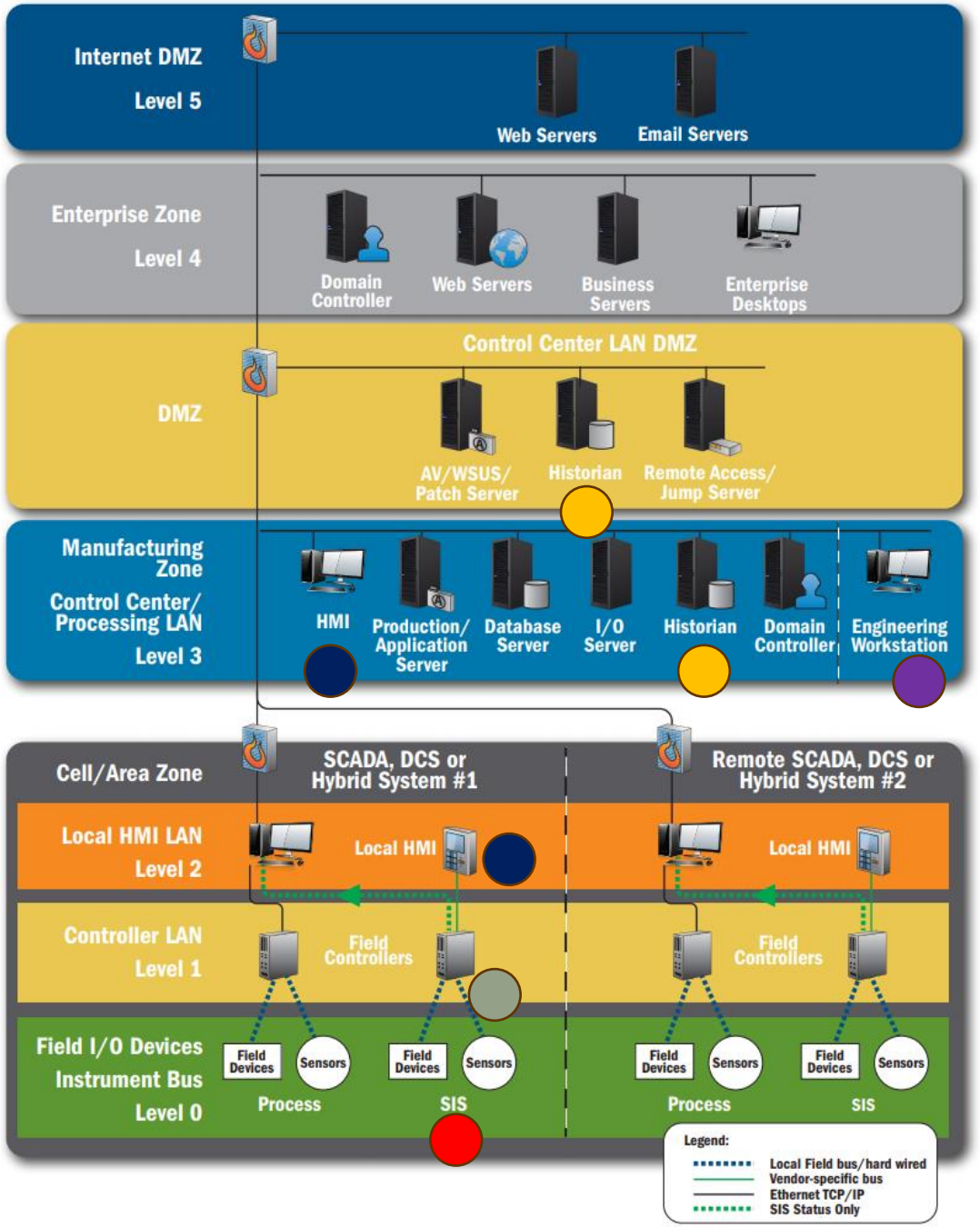
Human Machine Interface (HMI)

- Operator interface - Workstation, screen, lights & buttons

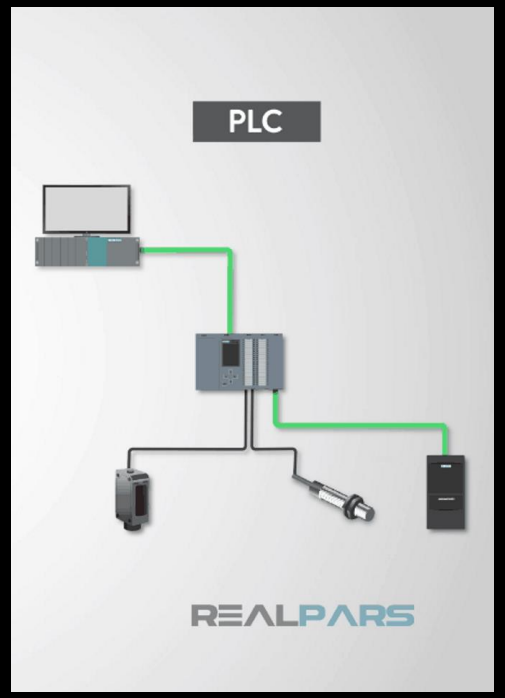
Safety Instrumented System (SIS)

- A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated. **Critical component**

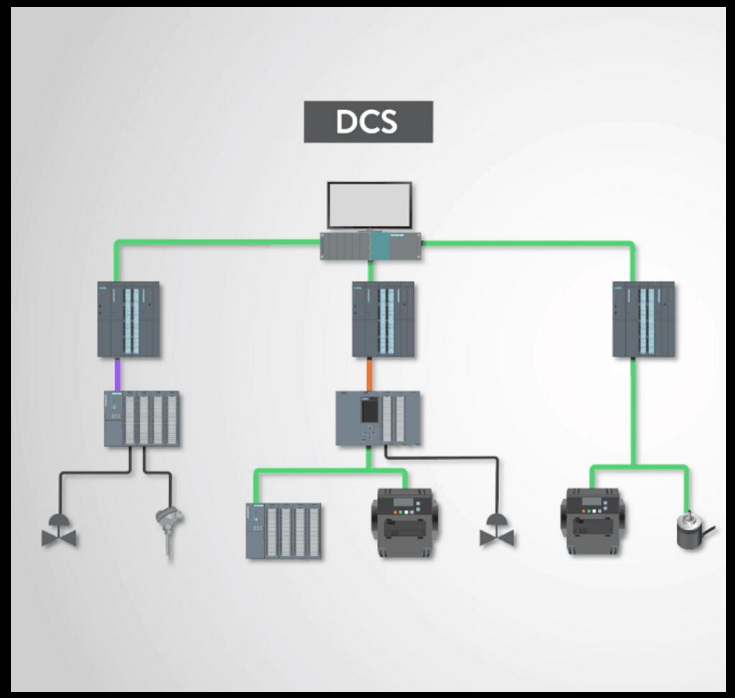
ISA 95 is a reference **model**, not an architecture



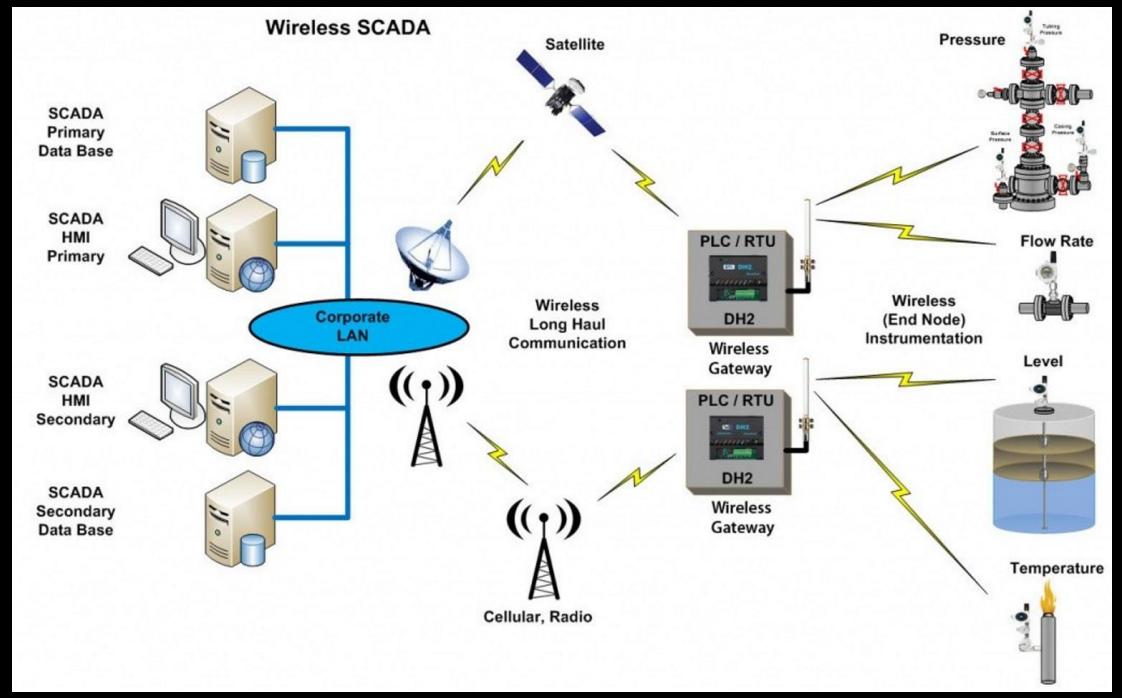
PLC V DCS V SCADA



- Controls *specific tasks* or processes
- A single process line, or task. Limited scalability
- E.g. Food & Bev, Packing



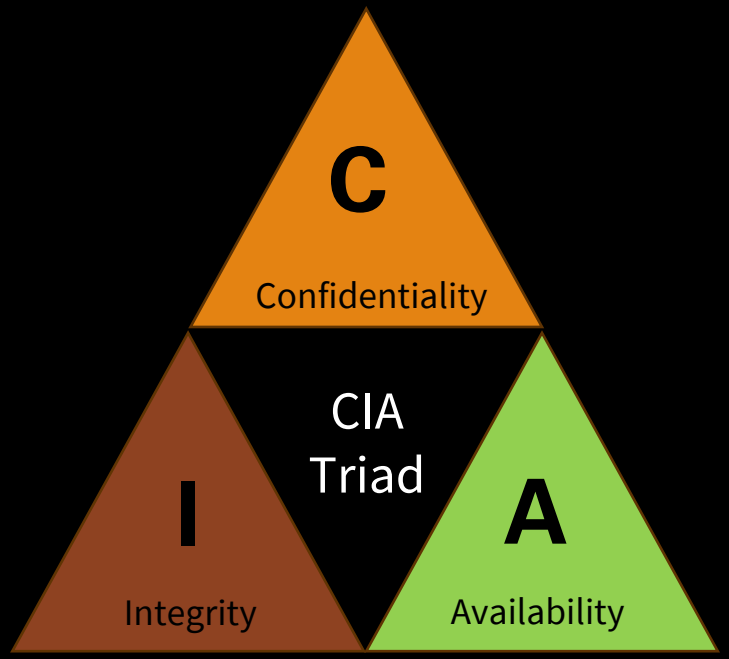
- Controls *complex, continuous* processes
- Typically, local plant. Scalable within plant
- E.g. Chemical, manufacturing

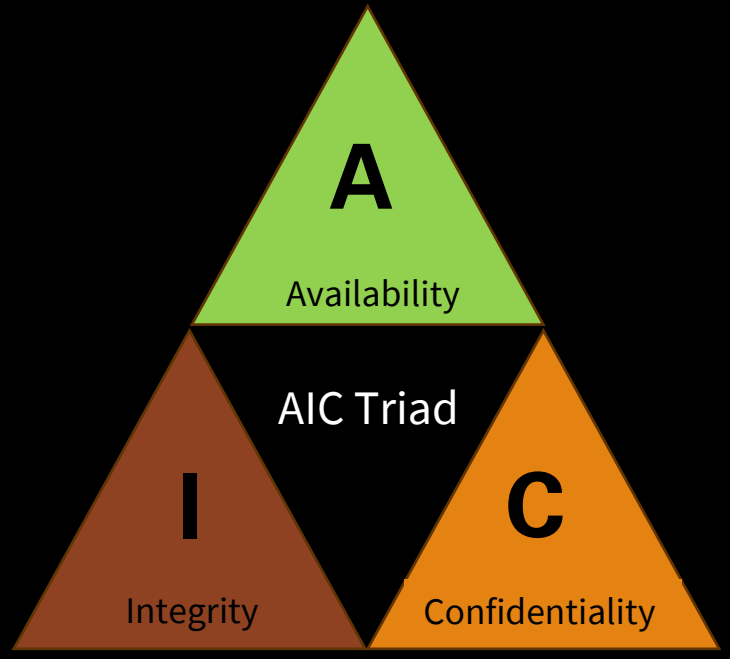


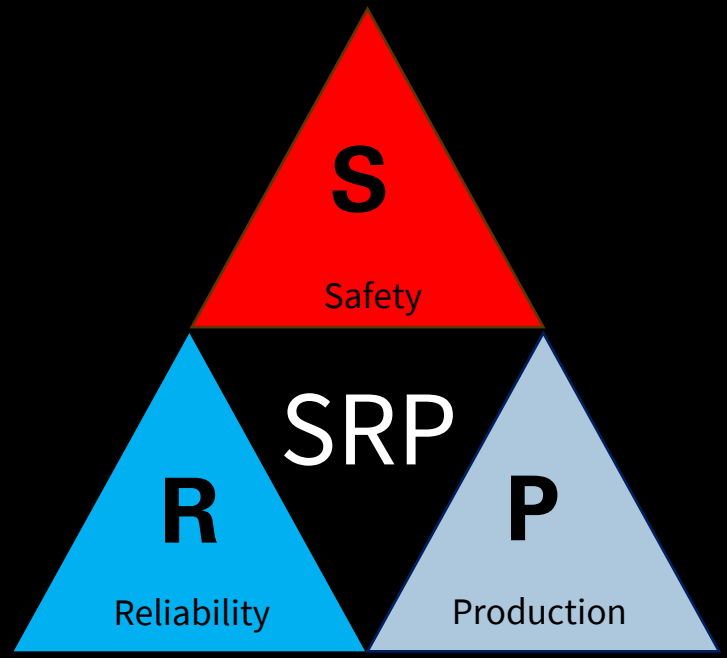
- Monitors and controls *remote operations*
- Geographically dispersed. Highly scalable
- E.g. Oil and Gas, Water, Power

Source: realpars.com

WHAT ARE WE PROTECTING WITH OT CYBERSECURITY?







- Physics & Engineering
- Consequences
- Context

EXAMPLES OF OT SYSTEMS

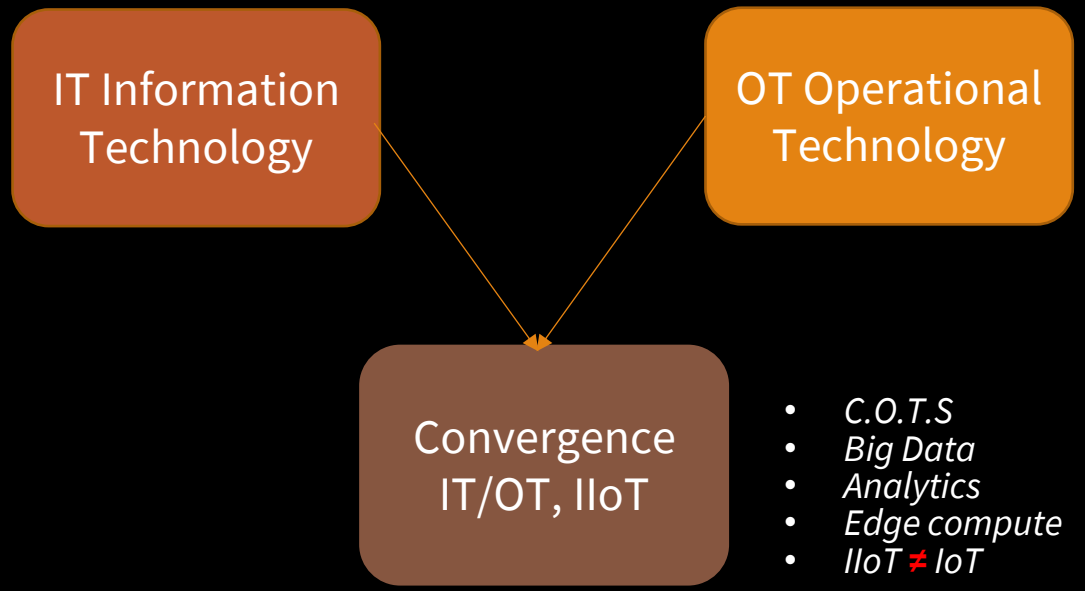
WHY

IT/OT CONVERGENCE – WHAT DO WE MEAN AND HOW DID WE GET HERE?

INFORMATION TECHNOLOGY

- Data Center Equipment
- ERP / SAP Systems
- Client-server (Mail, databases)
- DevOps, CI/CD etc.

- **Who:** CIO & CISO



- *C.O.T.S*
- *Big Data*
- *Analytics*
- *Edge compute*
- *IIoT ≠ IoT*

OPERATIONS TECHNOLOGY

- Control Room
- Plant / Manufacturing Execution Systems
- SCADA / Historian Systems
- Human Machine Interfaces
- Safety systems
- Engineering Workstations PLC's, RTU's, DCS's, IED's, IIoT Sensors

- **Who:** COO, Engineering Manager, Controls and Instrumentation Manager

Major Risks

- Loss of Data Confidentiality
- Loss of Data Integrity
- Loss of Data Availability

Major Risks

- IT Security issues in OT and IIoT environment with physical consequences

Major Risks

- *Process Safety* and Integrity
- *Reliability* issues, equipment failure, system availability, asset integrity
- *Production* loss (inc. Quality)

Focus : **Safety, Reliability, Production** - Not Cybersecurity

ATTACKS ON CRITICAL INFRASTRUCTURE AND OT SYSTEMS INCREASING

Media Statement: Update on Cybersecurity Incident

Australia, 28 November 2023

Australia, 28 November 2023: This is an update on the recent cybersecurit
DP World Australia.

On Friday 10 November 2023, the DP World Australia technology team dete
access to the company's Australian corporate network. To contain the incide

shipping operations.

DP World hack: port operator gradually restarting operations around Australia after cyber-attack

Read more

In its annual cyber threat report released on Wednesday, ASD revealed that in the last financial year the agency responded to 143 incidents at critical infrastructure entities such as ports, up from 95 incidents in the previous year.

The vast majority of the reports related to low-level attacks or isolated issues, such as compromised accounts or credentials.

ASD said critical infrastructure tends to have a broad attack surface, remote access, connected systems and third parties, which make it of interest to malicious actors.

"Even when [operational technology] is not directly targeted, attacks on connected corporate networks can disrupt the operation of critical infrastructure providers."

Second Australian rare-earth mineral compa targeted in cyber attack

A second Australian rare-earth metals organisation has suffered a cyber attack, Western Australia-based Northern Minerals suffered a ransomware attack.

Daniel Croft • Mon, 17 Jun 2024 • SECURITY

SHARE

Iluka Resources announced that threat actors attempted to disrupt its external website through a denial-of-service (DoS) attack, but that they did not gain access to the company's systems or exfiltrate any data.

Whilst the threat actor is yet to be identified, the attack comes just as Iluka Resources managing director Tom O'Leary called out China, claiming the country was rigging the prices of rare-earth metals to minimise the profits made by producers and gain a greater foothold on the

ASX ANNOUNCEMENT
4 June 2024

NORTHERN

Cyber security breach

Northern Minerals Limited (ASX: NTU) (Northern Minerals or Cor
the subject of a cyber security breach and was today advised by i
some of the exfiltrated data has now been released on the dark w

Northern Minerals became aware in late March 2024 of the brea
governance practices and protocols, Northern Minerals

‹ Back to overview

Home › Green Marine ›

Maritime industry remains 'easy target' for cyber attacks as ransom payment demands skyrocket

IT & SOFTWARE

October 17, 2023, by Jasmina Ovcina Mandra

The maritime industry remains an "easy target" for cybercriminals, and the cost of attacks and demand for ransom payments across the sector have skyrocketed over the past 12 months, according to the research findings from law firm HFW and maritime cyber security company CyberOwl.

The research reveals that the average cyberattack in the maritime industry now ends up costing the target organization $550,000 – up from $182,000 in 2022.

One of the findings also indicates that demands for ransom have increased by more than 350%, with the average ransom payment now $3.2m – up from $3.1m last year.

Staff unable to access patient files after Eastern Health cyber attack

Melissa Cunningham
March 29, 2021 — 7.15pm

Save Share A A A

Staff at a major Melbourne health network are unable to access critical patient medical histories a fortnight after a ransomware attack that is also causing significant delays to elective surgeries.

Eastern Health, which operates Box Hill, Maroondah, Healesville and Angliss hospitals, was forced to shut down some of its IT systems following a widespread cyber attack that crippled its server on March 16.

Intelligence Brief: Impact of FrostyGoop ICS Malware on Connected OT Systems

In April 2024, FrostyGoop, an ICS malware, was discovered in a publicly available malware scanning repository. FrostyGoop can target devices communicating over Modbus TCP to manipulate control, modify parameters, and send unauthorized command messages. Modbus TCP is a commonly used protocol across all industrial sectors.

The Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine, shared details with Dragos about a cyber attack that impacted a municipal district energy company in Ukraine in January 2024. At the time of the attack, this facility fed over 600 apartment buildings, supplying customers with central heating. Remediation of the incident took almost two days, during which time the civilian population had to endure sub-zero temperatures. Dragos assessed that FrostyGoop and internet-exposed ICS devices facilitated this attack.

OT CYBERSECURITY CHALLENGES, THEMES AND TRENDS – 2024

Lack of Security Architecture and Strategy for OT	**Conflicting priorities : Safety & Production v Cybersecurity**
Insecure Remote Access and Default Configs	**Lack of proper Network Segmentation & Visibility**
Legacy Systems	**Lack of Incident Detection, Response & Recovery capability**
Identity and Access Management	**Lack of Employee Education & Awareness**
Asset Inventory & Asset Management	**Lack of clear ownership & responsibility & governance**
Remediation capability (or lack of)	**Lack of OT cyber talent**

Supply Chain – Increasingly complex chains, combined with remote access requirements and poor cybersecurity controls, and ill defined contractual arrangements

Geopolitics – Provides ongoing opportunities for development of offensive cyber capabilities against ICS

Generative AI – Increase in actors using GenAI for malicious purposes - mainly IT, slowly impacting ICS

Malware - continues to be the main activity on critical infrastructures via IT environments

File Transfer Attacks – Increasing exploitation to gain access to OT environments

Physical consequences – Increase in cyber attacks resulting in a physical consequence

71%
Increase in attacks using valid credentials.

11%
Recorded attacks occurred against Utility sector (Water, Power)

Source: IBM X-Force Threat Intelligence Index 2023

50%
Of all OT incidents resulted in significant production losses >$50m

68
Resulted in physical consequences (Outages, equipment damage, environmental damage

Source: Waterfall 2024 Threat Report

70%
Attacks on OT - originated from within the IT environment

73%
Of known vulnerabilities, have ***NO*** practical mitigation provided by ICS/OT vendor.

68%
Recorded incidents could have been prevented by network monitoring, segmentation and MFA

54%
Incidents exploited remote access vulns & shared authentication domains

Source: Dragos 2023 Year in Review

CONSEQUENCE/IMPACTS ON TARGET

Consequence/ Impact	Description	Potential targets	Mitre ATT&CK ID	Examples
Loss of View (LoV)	Attacker prevents Operator (or controller) from viewing the state or condition of a process • May cause sustained or permanent loss of view. • System will require local, hands-on intervention e.g manual restart or operation • Loss of View can occur without affecting the physical processes themselves	• HMI's	T0829	• Industroyer • LockerGoga (Norsk Hydro) • Ultronics Defacement)
Manipulation of View (MoV)	Attacker manipulates the information reported back to operators or controllers. – this results in incorrect responses being taken by Operator or controller. • Manipulation may be short term or sustained. • During this time the process itself will be in a much different state than what is reported	• HMI's • Sensors • PLC/RTU	T0832	• Industroyer • Stuxnet • Trisis (Safety System)
Loss of Control (LoC)	Attacker achieves a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided • Intended to create unsafe conditions – there is significant risk to manual processes (people) in this state	• HMI's • Network Infra • Historians	T0827	• 2015 Ukraine Electric Power Attack • Industroyer • LockerGoga (Norsk Hydro)
Manipulation of Control (MoC)	Attacker manipulates physical process control within the industrial environment e.g changes to set point values, tags, or other parameters. • Manipulation of control systems devices or possibly leverage their own, to communicate with and command physical control processes. • Duration of manipulation may be temporary or longer sustained, depending on operator detection.	• Historians • Sensors • PLC/RTU	T0831	• 2015 Ukraine Electric Power Attack • Industroyer • Stuxnet • Trisis (Safety System)

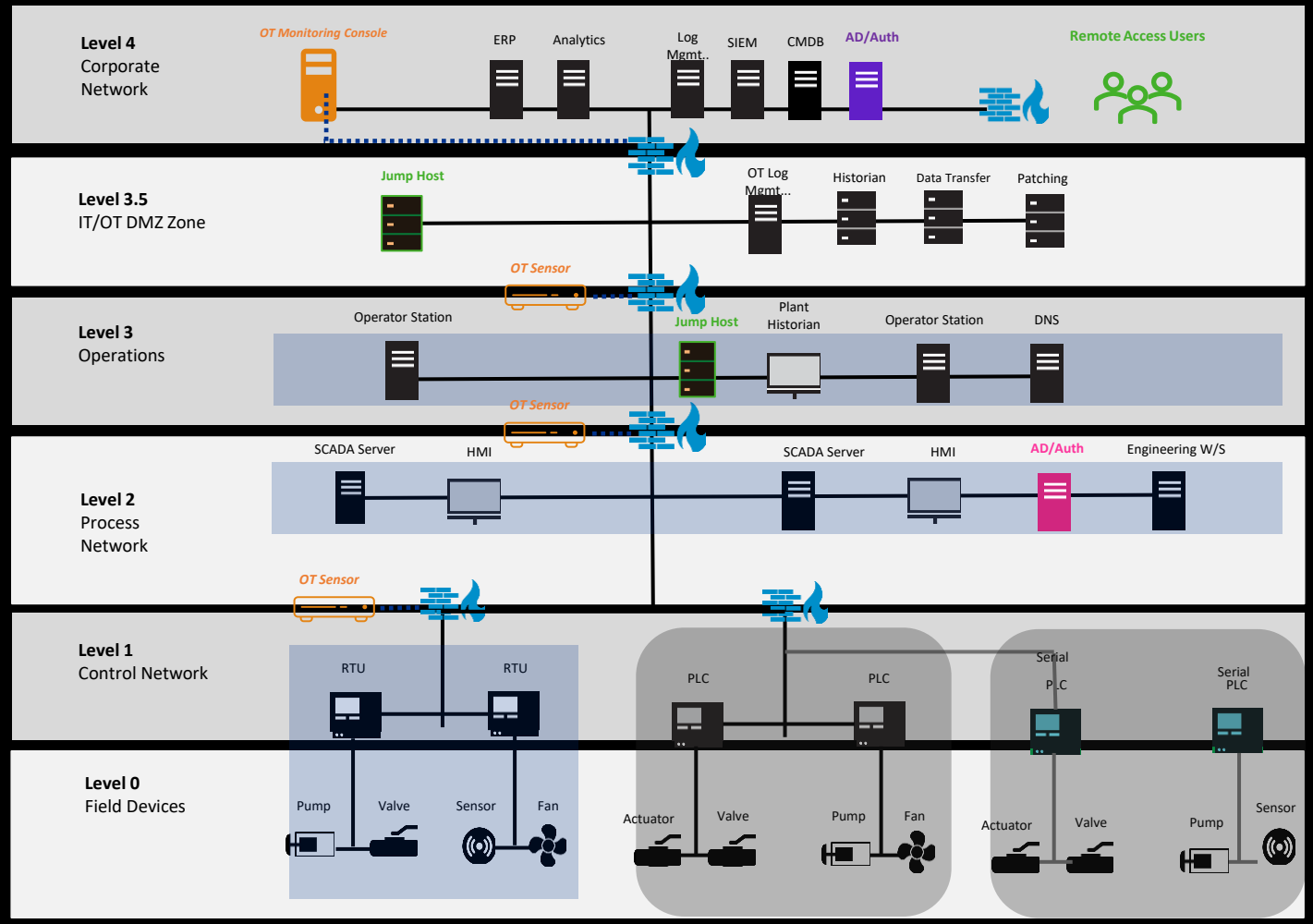
THE TOP 5 ICS CYBERSECURITY CRITICAL CONTROLS (SANS & DRAGOS)

TOP 5 ACTIONS TO REDUCE OT CYBER-ATTACKS, BASED ON SANS AND DRAGOS IR ENGAGEMENTS

 **ICS Incident Response Plan**	 **Defensible Architecture**	 **Network Visibility and Monitoring**	 **Secure Remote Access**	 **Risk-based Vulnerability Management**
• Detect and contextualise threats • Establish Forensic capability • Response playbooks • Training & Exercises	• Establish defensible network architecture to support monitoring, response, reduce attack surface	• Continuous monitoring • Asset identification & Management • OT protocol aware • Integration with IT and OT teams	• Identification and inventory of *all* remote access methods • Connections monitored and recorded.	• Understand OT risks, context and drivers • Establish risk-based vulnerability management program

Source: SANS.ORG https://sansorg.egnyte.com/dl/R0r9qGEhEe
Dragos : Dragos-5-Critical-Controls-OT-Cybersecurity-Guide-v1.pdf

DEFENSIBLE OT ARCHITECTURE



Network Segmentation (Zones & Conduits), ZTNA

Separate Identity & Access Management)

Continues Asset ID and Situational Awareness

Secure Remote Access


YOU
5.0 t
WÄRTSILÄ

STAY STANDING IF YOU HAVE ….

- 3-5+ years cybersecurity experience
- Bachelor's degree or higher in Engineering, Cybersecurity, Information Technology (or equivalent)
- Knowledge of network security, endpoint security, and identity security concepts
- Knowledge of Windows, Linux, Cisco technologies and administration
- Knowledge of cybersecurity policies and standards related to OT/ICS/SCADA (NIST CSF, IEC 62443, ISO 27001, C2M2)
- Knowledge of OT technologies, protocols, threats and risks (SIS, DCS, SCADA)
- Knowledge of Incident Response for IT & OT
- CISSP and GICSP certifications
- Project management qualifications and experience of projects >$5m

WHAT DOES THE MARKET WANT?

Qualifications

Here's what you'll need

- Higher Degree (Bachelor or Master) in Automation, Electronics or Computer Science (IT)
- Minimum 2-3 years of working experience in the field of industrial cyber security
- Knowledge of internationally recognized OT security standards, e.g. IEC 62443/ISA 99, NIST SP 800-82, NERC CIP.
- Knowledge of internationally recognized cyber security standards, e.g. NIST-CSF, ISO27k series.
- General knowledge of industrial communication protocols and technologies from main vendors including Rockwell, Siemens, ABB and Schneider Electric

Bonus points if you have

- Knowledge and experience (designing, commissioning or maintaining) with OT / ICS systems (e.g. SCADA, DCS, EMS, etc) is a plus
- Experience in supporting or troubleshooting industrial protocols such as OPC, Modbus TCP, HART etc. is a plus
- Advanced knowledge and hands-on experience in security architecture and network infrastructure utilized in Industrial and Automation Control Systems (IACSs) is a plus

Qualifications:

- Bachelor's degree in Computer Science, Engineering, or a related technical field. Candidates with strong core networking and security skillsets could be considered with the expectation of developing skills/certifications focused on Manufacturing, ICS, and OT Networking/Security. Experience in implementing and managing IT security measures.
- At least 3 years of experience in managing IT network systems, preferably within a manufacturing environment, focusing on industrial control systems
- Strong understanding of OT technologies, including SCADA, PLCs, and industrial networking.
- Knowledge of cybersecurity principles and practices as they relate to OT environments.
- Familiarity with IT/OT integration challenges and solutions.
- Detail-oriented with a strong focus on system reliability and security.
- Excellent problem-solving and technical troubleshooting skills.
- Strong communication and project management abilities.
- Ability to work collaboratively across IT and engineering teams.

- Perform basic risk assessments and communicate security risks;
- Investigate security breaches in accordance with established procedures;
- Contribute to selection and deployment of vulnerability assessment tools;
- Maintain operational security processes and check;
- Participate in Cyber Security and Operational Technology projects.

Key experience:

- Previous experience in a Cyber security AND Operational Technology support role;
- Technical experience supporting SCADA systems , control systems OR other OT technology environments;
- Security experience with Microsoft, Linux AND/ OR cloud environments;
- Certifications in CISSP, GIAC OR relevant security areas;
- Experience with frameworks including ISA/IEC 62443, ACSC Essential Eight, AESCSF OR NIST C2M2;
- Experience in areas including: Kusto Query Language (KQL), Privileged Access Management, SIEM Platforms including Elastic Stack ,Tenable/vulnerability management , End-Point protection, PowerShell or Linux Bash.

Unsave | Apply

Home | Recommended 28 | My Activity | Profile

Competency)

Degree in Computer Engineering, C
Electronics Engineering; or equivale
Good knowledge and understandin
cybersecurity frameworks, IEC 624
Cybersecurity experience in OT/IC
Those with GICSP, CRISC, CISS
Strong leadership, communica
environment
Good project management

The ideal candidate should poss

- Bachelor's degree in Cybers
- Minimum 3-5 years relevant
- Experienced cybersecurity pro
- Experienced SCADA or DCS engi
- Experienced Internet of Things (IoT)
- Certifications in cybersecurity e.g. CISSP,
- Certifications in OT cybersecurity e.g. GICSP,
- Committed to continuously learn and develop oneself
- Aptitude of consulting including managing oneself, pro
- Able to think logically and communicate clearly.
- Effective interpersonal skills and able to work well in a team
- Good presentation skills might be advantageous.

WHAT ATTRIBUTES AND KNOWLEDGE DO YOU NEED

- Soft skills
  - Curiosity
  - Empathy (SRP)
  - Strong Communication & presentation skills

- Technical
  - Cybersecurity foundations (Risk etc)
  - Network and OS Ops (routing, backups, patching etc)
  - OT Technologies – Architectures, protocols
  - Industry-specific knowledge

CATCH 22 : NO EXPERIENCE, NO JOB

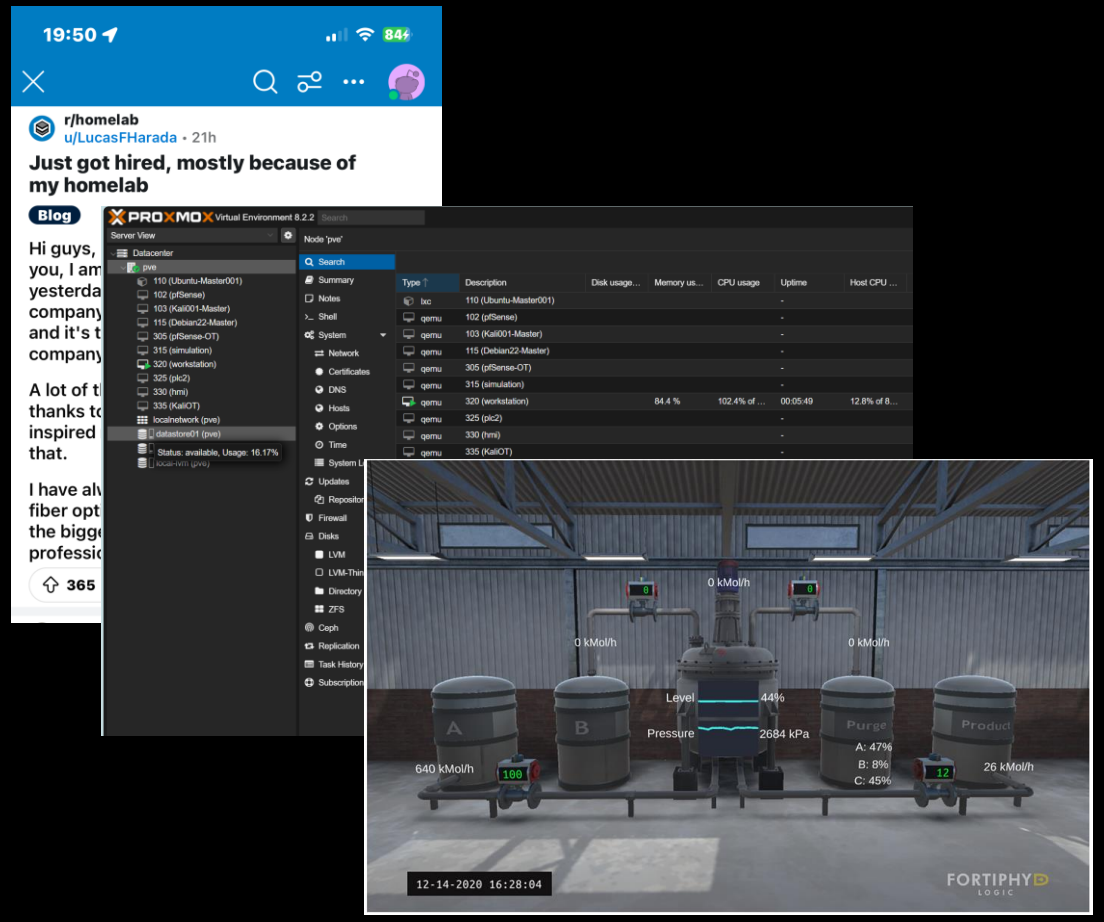
Curiosity & Self-Learning

Existing Skills and Knowledge

Networking (with actual people ☺)

Where are you now?

Training ($)



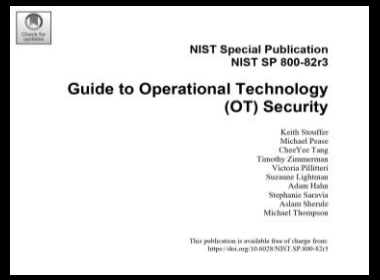
Obligatory, yet confusing AI image

FRAMEWORKS AND STANDARDS

NIST CSF V2

https://www.nist.gov/cyberframework

- Generic (and free)
- Broad (IT and OT)
- References inc.. IEC 62443, 27001, COBIT etc..
- Good starting point for any industry


NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

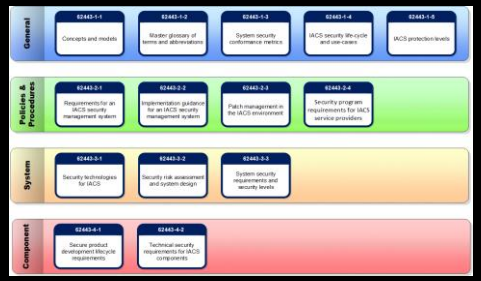
Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Victoria Pillitteri
Suzanne Lightman
Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

NIST 800-82 r3

https://csrc.nist.gov/pubs/sp/800/82/r3/final

- Generic ICS and OT/IIOT (and free)
- Aligns with NIST CSF, 27001 etc..
- Should be mandatory reading



ISA/IEC 62443 series

https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

- Cross-industry
- Not Free! ($$$) but … *isa.org
- Risk Assessment, SL's, Zones & Conduits
- Aligns to 27001, referenced by others

OTHER FRAMEWORKS, STANDARDS AND REGULATIONS

- SOCI - Security of Critical Infrastructure Act 2018 (Aust)
- AESCSF - AEMO Cybersecurity Framework (Aust)
- C2M2 - Cybersecurity Capability Maturity Model
- ISO 27001/2
- AS 7770 – Rail
- TS 50701 – Rail
- API 1164 - Pipelines
- ISA/TR84.009 – Cybersecurity and Safety Lifecycle
- NIS2 (UK) – Similar to SOCI
- IEC 62351 (Smart Grid)
- BS EN 16747 – Maritime and Ports
- BIMCO - The Guidelines on Cyber Security Onboard Ships
- …. Many more

SOME LEARNING RESOURCES (DEFINITELY NOT ALL) . . .

PEOPLE, ORGS & VENDORS

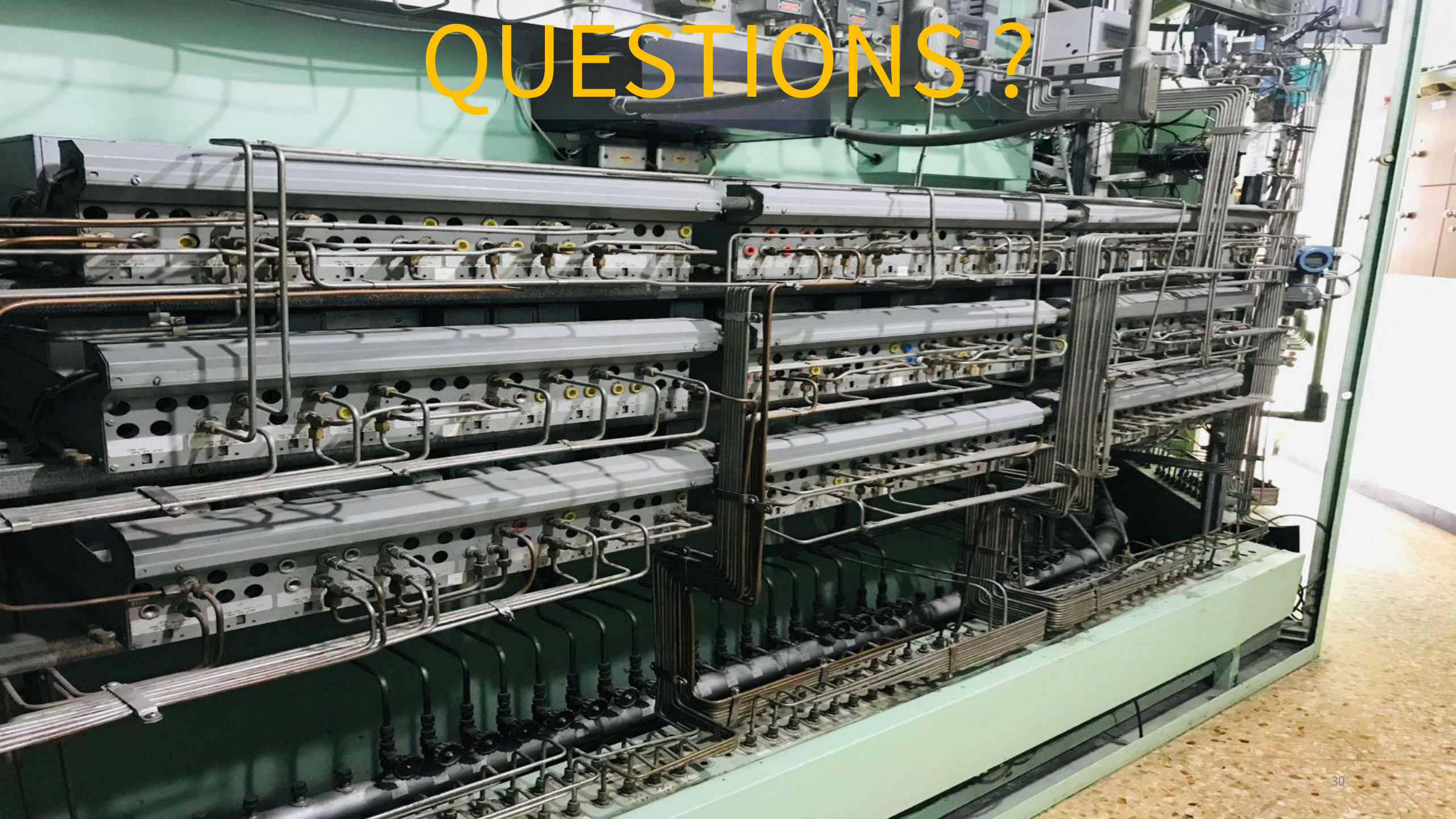
- Dale Petersen
- Robert M. Lee
- Clint Bodungen
- Pascal Akerman
- Andrew Ginter
- Mike Holcomb
- Dragos
- Nozomi
- Claroty
- CS2AI
- ISA.ORG (*Membership*)

PODCASTS & VIDEO

- S4 Onramp
- ICS Basics Youtube Playlist
- SANS ICS Concepts Youtube Playlist
- ProtectItAll (Aron Crow)
- Waterfall (Andrew Ginter)
- @BEERISAC – IT/OT Podcast
- CS2AI (Derek Harp)
- Unsolicited Response (Dale Petersen)

TRAINING & BOOKS

- ISA IEC 62443 Training ($$)
- CISA ICS Training VLP (Free & $)
- SANS.ORG - GICSP, GRID etc. ($$$)
- UDEMY & LINKEDIN ($)
  - Marcel Rick-Cen,
  - Sourabh Suman
- *Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT* (Brookes, Craig)*
- *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions* (Bodungen)
- *Industrial Cybersecurity: Case Studies and Best Practices* (Mustard)
- *Implementing IEC 62443 - A Pragmatic Approach to Cybersecurity* (Medoff)


QUESTIONS?

TAKEAWAYS

1. **S**afety, **R**eliability & **P**roduction
2. Think physics, consequences & context all the time
3. Be curious, self-study (Lab) & network yourself

camorrisaus

Infosecmorc