Blue Teaming Yo ICS

@beLarge
BSides Brisbane 2019

¡!¡ WARNING ¡!¡

- This is general advice and your network will be **different** and I don't know how it works – so think before making any changes

- The information presented today has not been obtained from any single one of my previous employers* and my views do not represent them

- Please don't sue me

- Please don't

*Except AESCSF

/whois

@beLarge

- Telecommunications Engineer who has worked across IT and OT in Network Engineering and Cyber Security roles over the last 10 years

- Bach Eng (Telecomms) and Master Business (Applied Finance) – I like spreadsheets!

- Recently been working in the Big4 – focusing on Cyber Security (Risk Management, Security Architecture and Frameworks)

- My aim today is to share things that I have found useful and to help the practitioners connect with the bigger picture

- I would've found this discussion useful a few years ago!

Today's agenda

1. Risk Management
2. Threat Modelling
3. Segmentation
4. Frameworks
   a) NIST CSF
   b) AESCSF
5. Useful textbooks
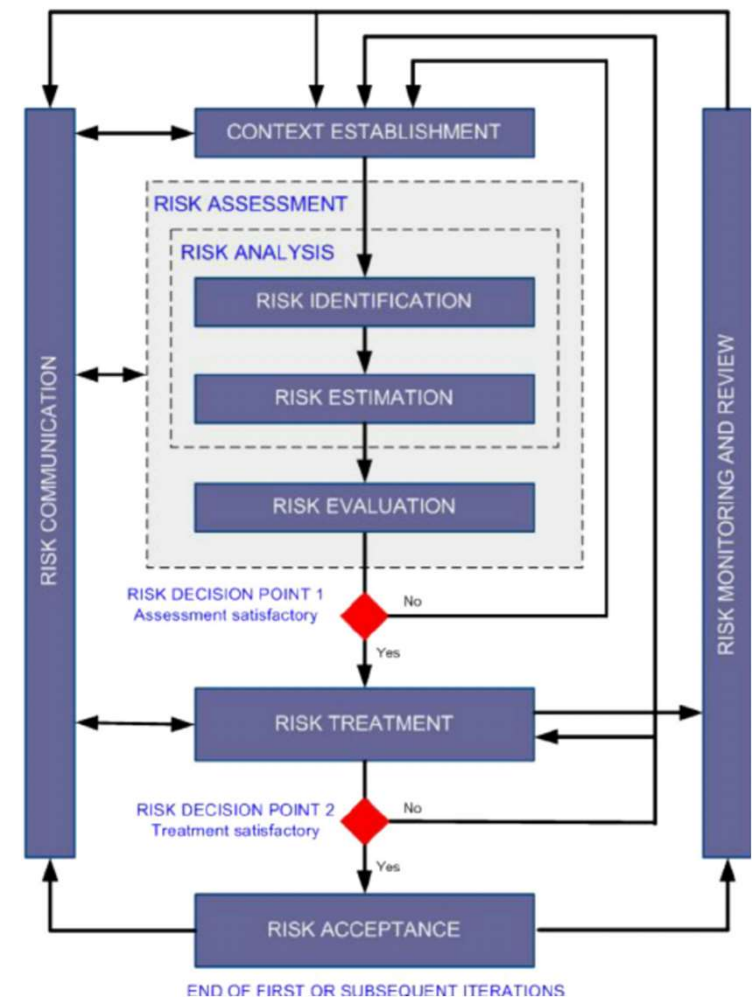6. Online Resources
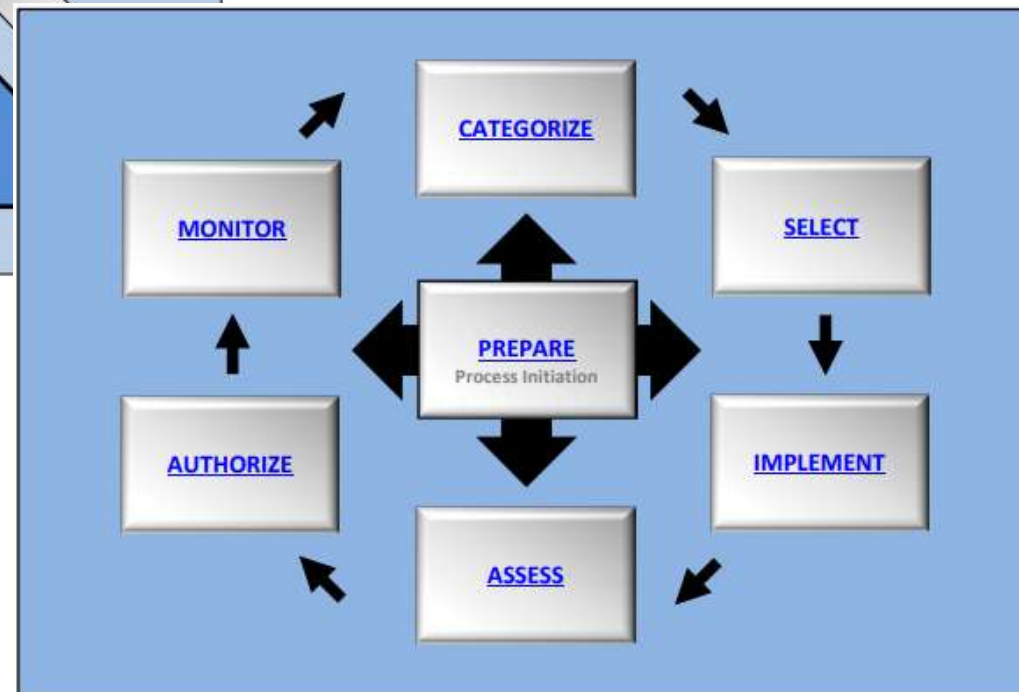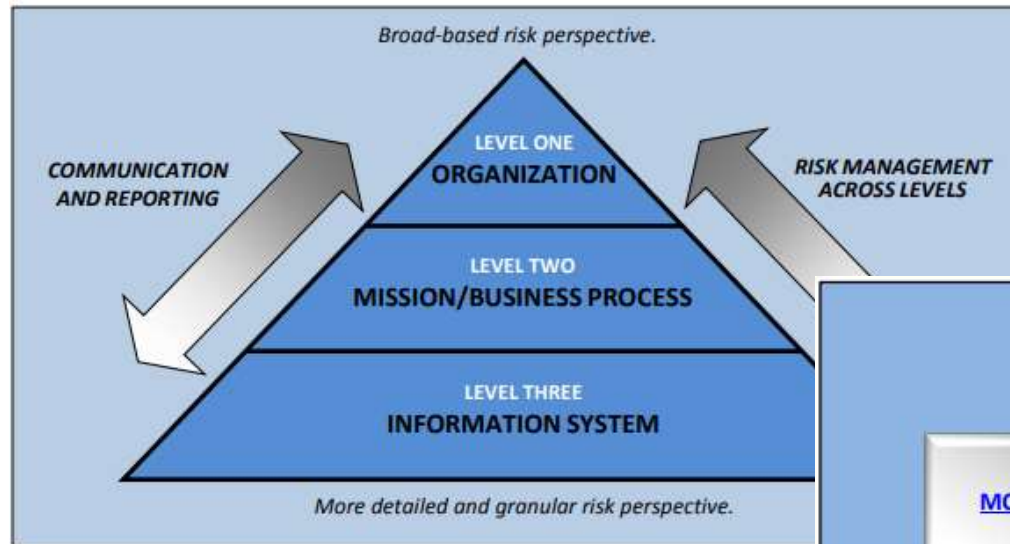7. Useful tips

Risk Management

- Cyber Security is a by-product of good risk management

- So WTF is Risk Management?

- ISO 31000 defines risk management as "effect of uncertainty on objectives"

- *What*?

- Risk management is a way to consider and communicate the "what-if" (**uncertainty**) and identify bad (*and good*) (**effect**) stuff that could happen to the business (**objectives**)

- It's important because it enables technology practitioners to:
  - Communicate complexity to people who do not understand the detail
  - Prioritise control selection, manage systems and prioritise remediation if required

- Doing it earlier in the System Development Life Cycle makes life better for everyone

- It also helps you build a <u>consistent</u> and <u>defensible</u> approach to Cyber Security

Risk Management – ISO 27005

- Assets – things of value to the business – physical or intangible
- Vulnerabilities – weaknesses in a system that can be exploited by a threat actor
- Threats – the combination of a threat actor and it acting on a vulnerability
- Risk – The combination of a Threat using a vulnerability on an asset (maybe with a frequency …)
- Frequency – a method of determining the likelihood of the risk being realised (this one is very tricky)
- Risk Treatment – Accept, Modify/Mitigate, Transfer, Avoid (Ignore – not really one but happens)
- 27005 Annex D – List of Vulns (useful!)

https://www.researchgate.net/figure/Information-security-risk-management-process-from-ISO-IEC-27005_fig8_265704308

Risk Management – NIST 800-37 r2

Ref -
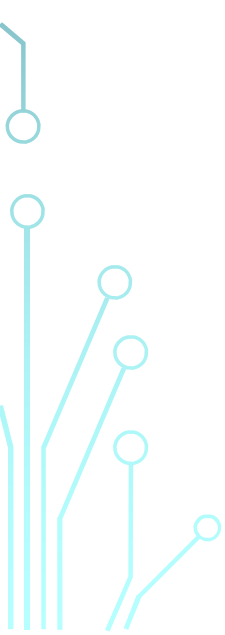https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Risk Management

- I wish I knew this so I could communicate better to management why the things were doing were wrong (Think - **Risk Register** and **Dashboards**)

- Rather than trying to boil the ocean – could prioritise remediation where it mattered most
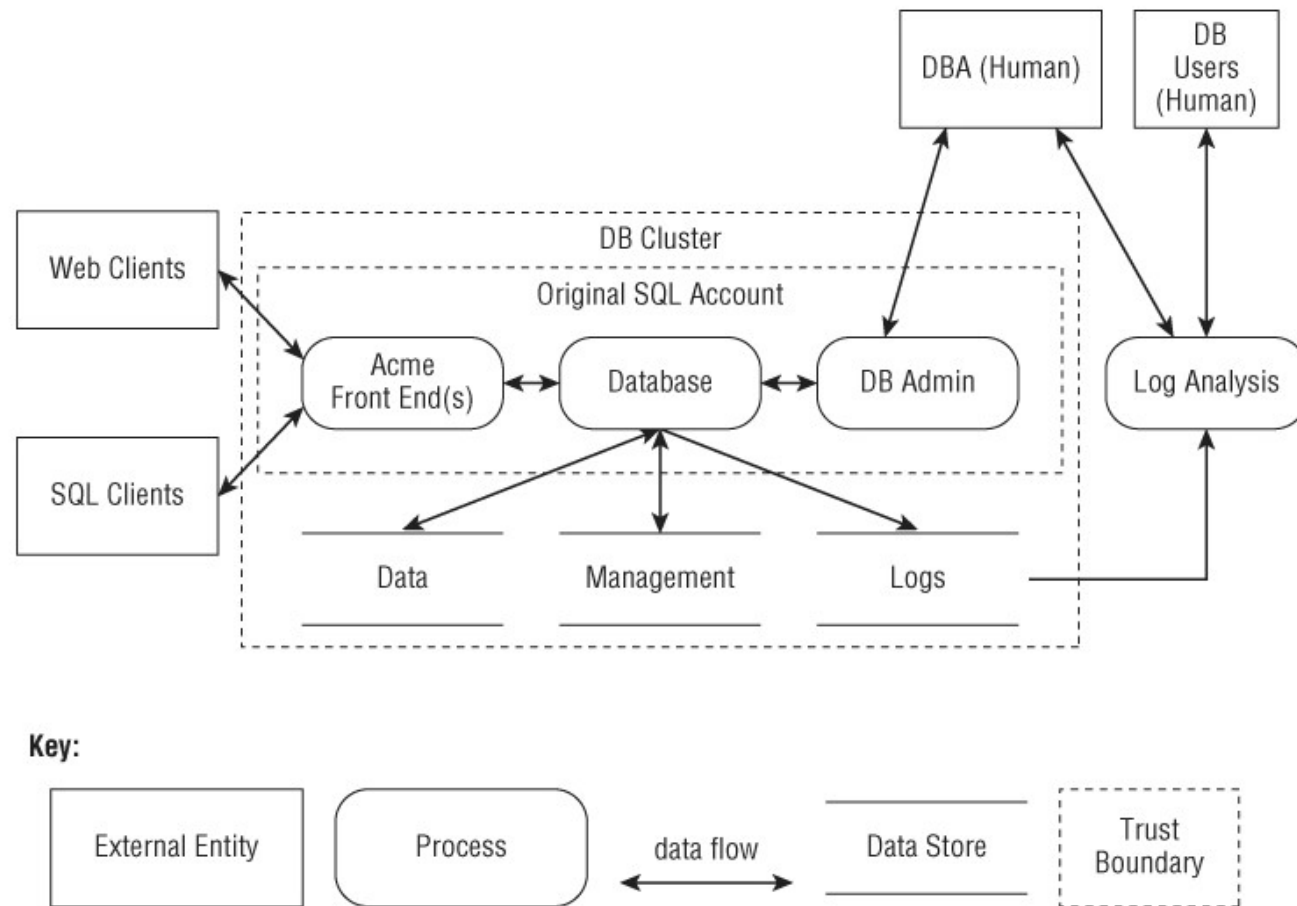
Threat Modelling

- Risk Management is great but can be abstract

- Threat modelling makes it **real!**

  - Shostacks *Threat Modelling Designing for Security, 2014* – Discusses Microsoft STRIDE Methodology

  - Data Flow Diagrams

  - Then Enumerate STRIDE across the DFD

- I think this is awesome because

  - It is a simple tool to get everyone on the same page "Oh, you forgot this sneaky backdoor 4G …"

  - A structured process that drives for coverage
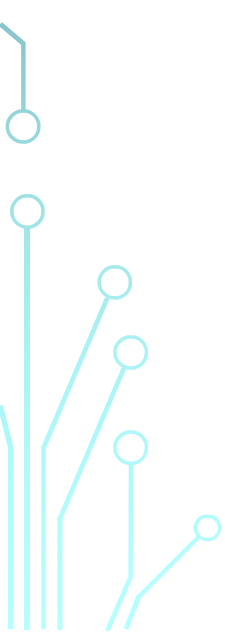
Threat Modelling – Data Flow Diagram

Sourced – Shostack *Threat Modelling Designing for Security, 2014 Chapter 2 Fig 2.4*

Network Segmentation

- Network Segmentation is very important in OT/ICS environments because a lot of the endpoints do not have adequate security capability
    - Limited Authentication
    - Limited platform hardening
    - Legacy network protocols

- Network segmentation can also allow for Proof of Concept (POC) & functional outsourcing – "I don't trust this stuff, you get your own bubble"

- Good network segmentation at its worst can delay breaches (frustrate Red Teamers) and at its best stop* breaches
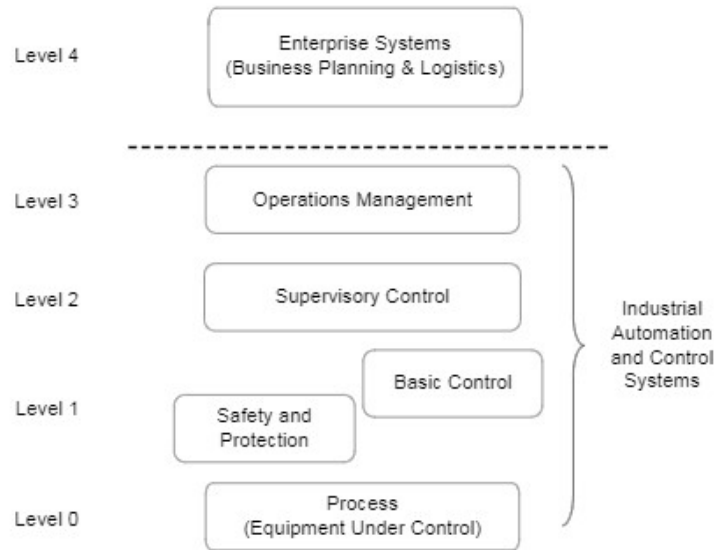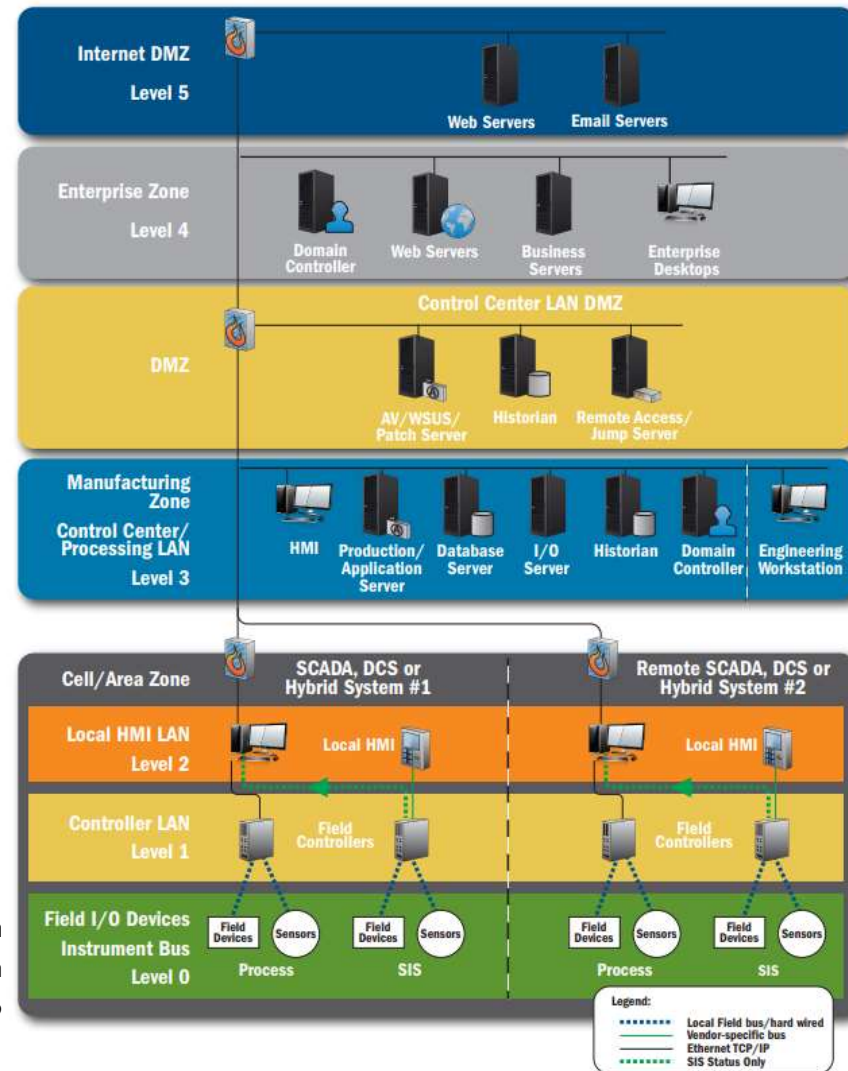
Network Segmentation + Purdue Model

Figure 12 – Reference Model for ISA99 Standards

From ISA 62443-1-1

Ref - Improving Industrial Control System
Cybersecurity with Defense-in-Depth
Strategies – ICS CERT 2016

Frameworks

- Frameworks help you to identify your unknown unknowns – it gives you **coverage & comfort**

- Don't mess with the defaults unless you know what you are doing (*eventually you should!*)

- There are many, many frameworks but today I want to talk about:

- NIST Cyber Security Framework (CSF) (and its informative references)

- The Australian Energy Sector Cyber Security Framework (AESCSF) (derived from US Dept of Energy – Electricity Subsector – Cyber Security Capability Maturity Model (US DoE ES-C2M2)

Frameworks – NIST CSF

- Framework development started by NIST after executive order by US Pres. Obama in 2013 to assist Critical Infrastructure Cybersecurity

- Framework structure
  - 5 Functions > 23 Categories > 104 Sub Category
  - Implementation Tiers
    (Partial, Risk Informed , Repeatable, Adaptive)
  - Framework Profiles
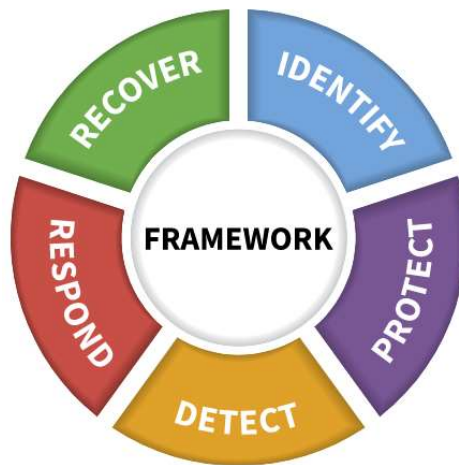
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Ref - https://www.nist.gov/cyberframework/framework-resources-0

Frameworks – NIST CSF

- Informative References

  - CIS CIC (Formally SANS Top 20)

  - COBIT

  - IEC/ISA 62443

  - ISO 27001

  - NIST SP 800-53

- Framework Resources

  - https://www.nist.gov/cyberframework/framework-resources-0
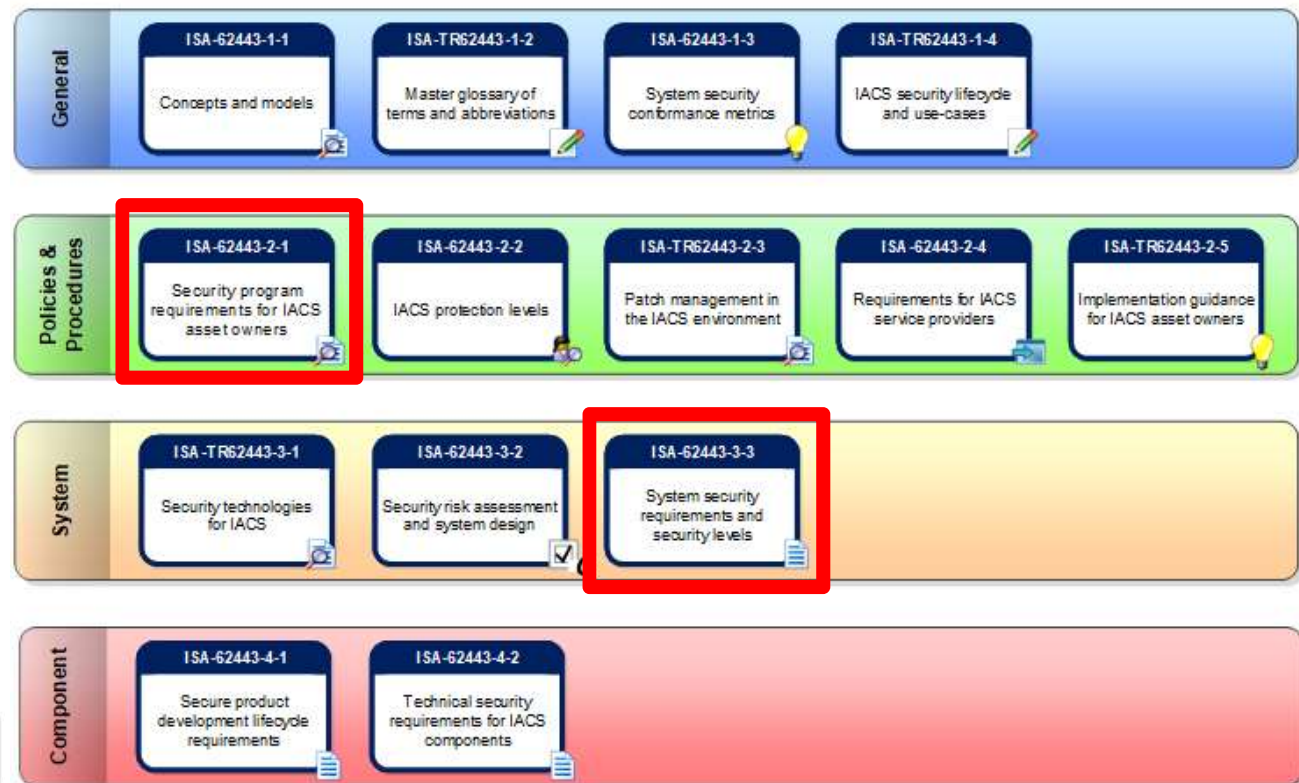
Frameworks – IEC/ISA 62443

- Formally ISA-99, though the ISA refer to the ISA 99 Working Group

- Cyber Security specifically for ICS, it is a framework of individual standards

NIST CSF only refers to:

- 62443-2-1

- 62443-3-3

Ref – ISA 99 -
https://www.isa.org/isa99/

Frameworks – AESCSF

- Finkel's *Blueprint For the Future – Rec* 2.10 "An annual report into the cyber security preparedness of the National Electricity Market should be developed by the Energy Security Board …. "

- The result is the AESCSF

- Framework structure

  - 11 Domains, 28 Objectives, 240 Practices

  - A Practice corresponds with a Maturity Indicator Level (MIL)

  - The Assessment results are presented as *Donuts*
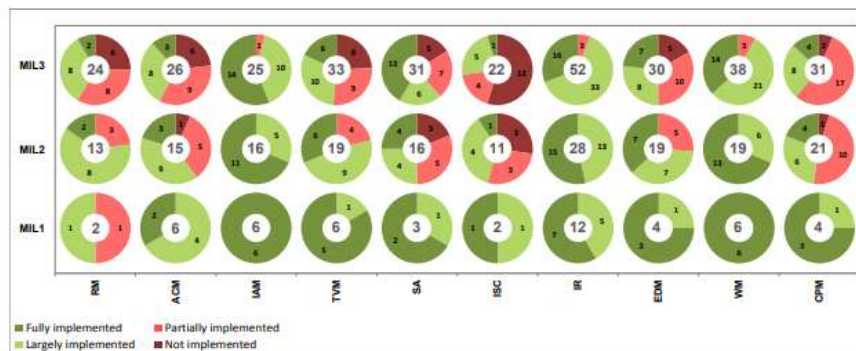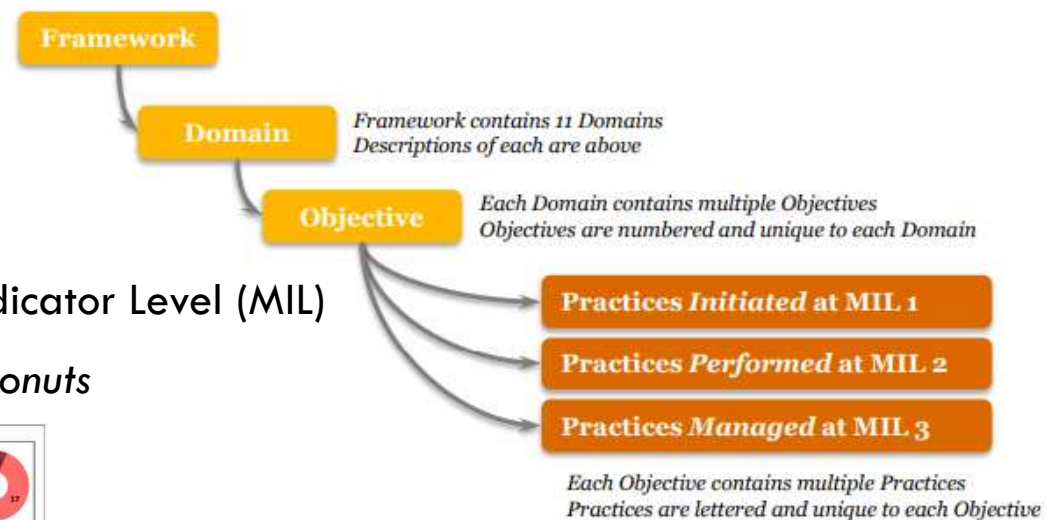
Frameworks – AESCSF - Domains

- Risk Management (RM)
- Cyber Security Program Management (CPM)

- Workforce Management (WM)
- Supply Chain and External Dependencies Management (EDM)
- Information Sharing and Communications (ISC)
- Australian Privacy Management (APM)

- Asset, Change and Configuration Management (ACM)
- Identity and Access Management (IAM)
- Threat and Vulnerability Management (TVM)
- Situational Awareness (SA)
- Event and Incident Response, Continuity of Operations (IR)

Frameworks – AESCSF – Resources

- aemo.com.au > Electricity > National Electricity Market or Wholesale Electricity market > Cyber Security
- You can get access to Framework Core, Quick Reference Guide, CAT guidance, Support Videos, FAQ
- Framework Core contains
  - The Practices
  - Anti Patterns (awesome!)
  - Context & Guidance
  - Australian References
  - Informative References

Frameworks – AESCSF – Anti Patterns (examples)

- The organisation has not identified which assets support the delivery of critical functions.
- Asset inventories have not been updated in the past 24 months.
- OT networks can route traffic directly to the Internet
- Remote access or third-party access circumvents your network Security controls. E.g. OT assets with direct 3G/4G connections to enable remote support over the Internet.
- You are unable to isolate critical systems from non-critical systems in the event of a Cyber Security threat or incident
- You cannot individually identify all identities (whether by user identifier or secondary means) with access to technology networks or systems.
- People are given administrator access to systems by default. A common example is end users being local administrators on their corporate laptop/workstation.
- Cyber Security risk management activities are not aligned with the corporate risk management strategy/framework.
- Risks remain unresolved for prolonged periods of time awaiting senior management decision-making or resource allocation to resolve.
- **Logs are not time-synchronised.**
- Logging is only used to support operational performance monitoring and not Security monitoring.
- … and more!

Frameworks – AESCSF – How to answer

How Do I Assess Implementation?
Quick Reference Guide – Management Characteristics

Ref – AESCSF Resources

Useful Textbook Resources

- Knapp
  - Industrial Network Security
  - Applied Cyber Security and the Smart Grid

- Shostack *Threat Modelling Designing for Security, 2014*

- CISM – All In One

Knapp – *Industrial Network Security (1ˢᵗ Ed)*

Excellent introduction textbook regarding ICS and cyber security

- Discusses:
    - What are Industrial Networks
    - Introduction to Industrial Network Security
    - Industrial Network Protocols (very useful!)
    - How Industrial Networks Operate
    - Vulnerability and Risk Assessment
    - Secure Enclaves (think Logical Zones/DMZs)
    - Exception, Anomaly and Threat Detections
    - Monitoring Enclaves
    - Standards and Regulation
    - Common Pitfalls and Mistakes (Excellent Design Prompt)
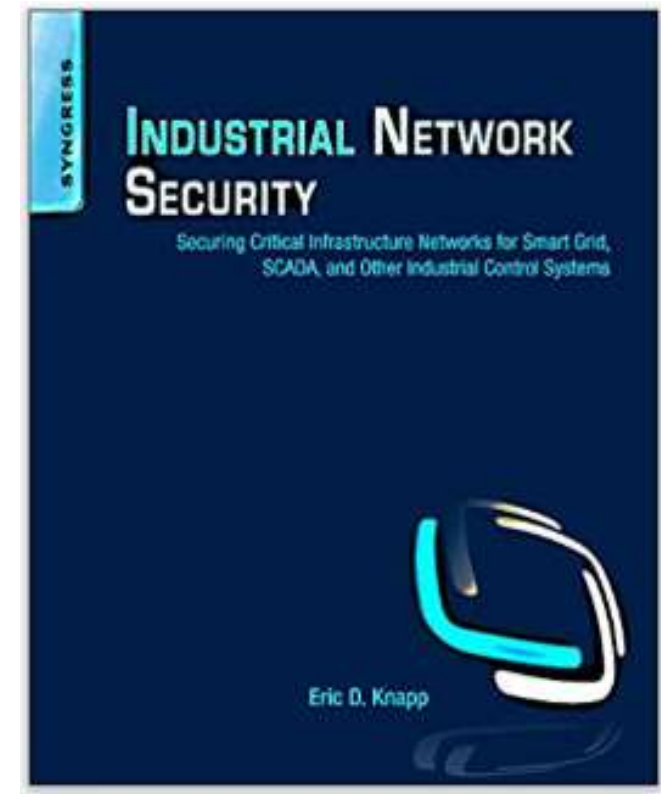
Knapp – *Applied Cyber Security and the Smart Grid*

I found this book was an excellent supplementary resource for Industrial network

Security regarding the electricity sector

Discusses:

- What is the smart grid

- Smart Grid Network Architecture

- Hacking the Smart Grid

- Privacy concerns with the Smart Grid

- Security models for SCADA, ICS and the Smart Grid

- Securing the Smart Grid

- Security the supply chain
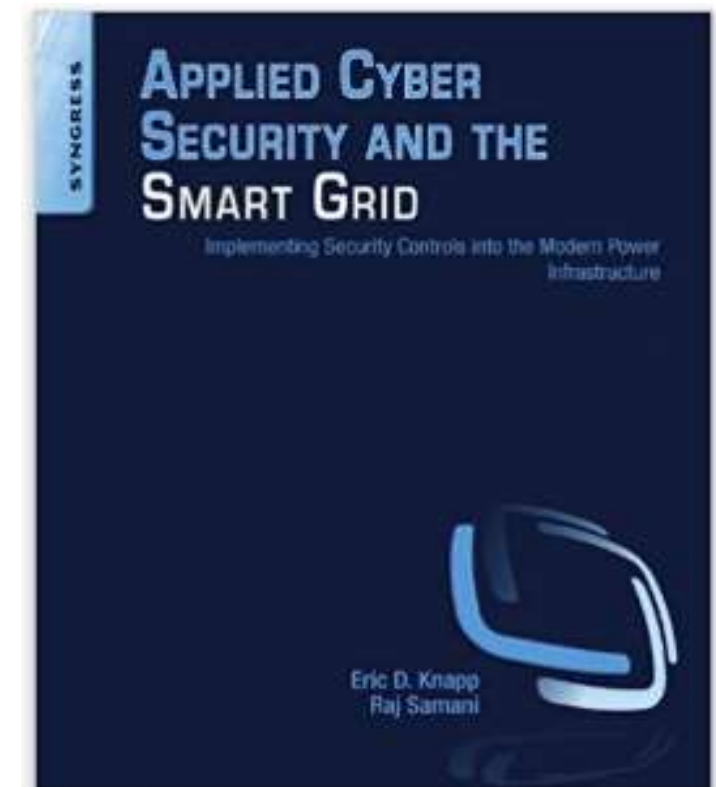
Shostack – *Threat Modelling*

This book really spoke to me about how to model systems – I am only 3 chapters in

Discusses:

- Strategies for Threat Modelling
- Finding Threats
- Managing and Addressing Threats
- Threat Modelling in Technologies and Tricky Areas
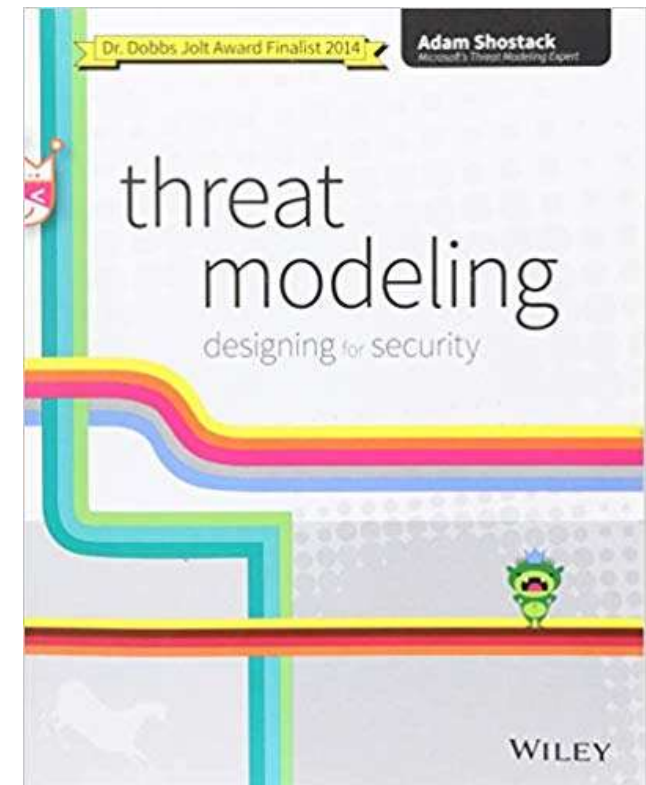
CISM All In One

This book really helped fill in the gaps for my Security Management and Governance knowledge

Discusses:

- Becoming a CISM
- Information Security Governance
- Information Risk Management
- Information Security Program Development and Management
- Information Security Incident Management
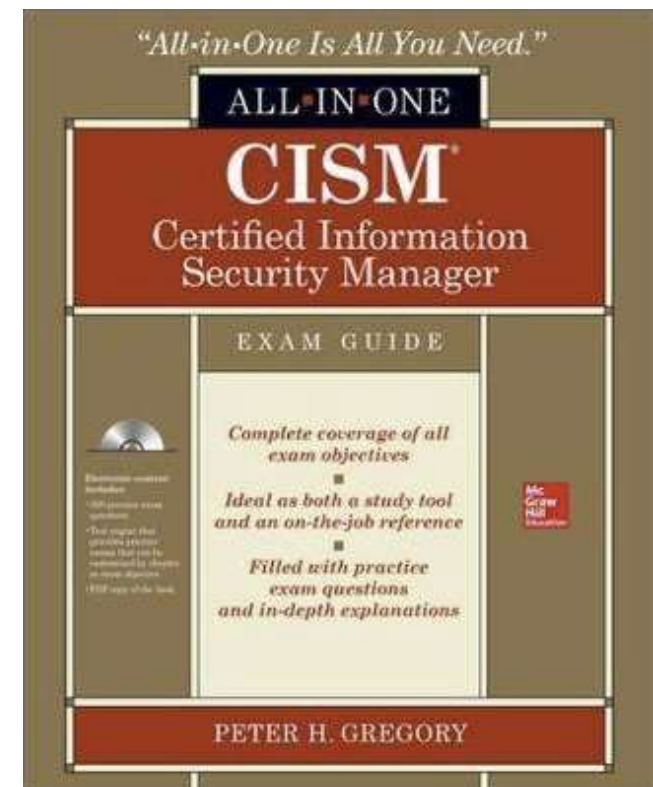
Useful online resources

- ICS-CERT

- ACSC

- US Department of Energy

- NIST

ICS-CERT

- Recommended Practices (https://ics-cert.us-cert.gov/Recommended-Practices)
  - Improving ICS Cyber Security with Defense-In-Depth Strategies
  - Cyber Forensics Plan for Control Systems
  - Developing an ICS Incident Response Plan
  - Patch Management for Control Systems

- Standards And References (https://ics-cert.us-cert.gov/Standards-and-References)

- Virtual Learning Portal (VLP) (https://ics-cert-training.inl.gov/lms/)
  - On my To Do List!
  - Hours of Free Training – I have heard it's good!

- Vulnerability Updates (https://ics-cert.us-cert.gov/alerts)
  - Email service of vulnerabilities – I have a gmail rule to filter now

ICS-CERT (cont.)

Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies

An excellent summary resources to given to non cyber security professionals who work with ICS – think Control System Engineers, Project Managers, Management, Support Maintenance/Technicians etc

Discusses:

- Risk Management
- Asset Inventory
- Physical Security
- ICS Network Architectures
- Security architectures
- Host Security
- Security Monitoring
- Vendor Management and Security

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
Industrial Control Systems Cyber Emergency Response Team
September 2016

Homeland Security
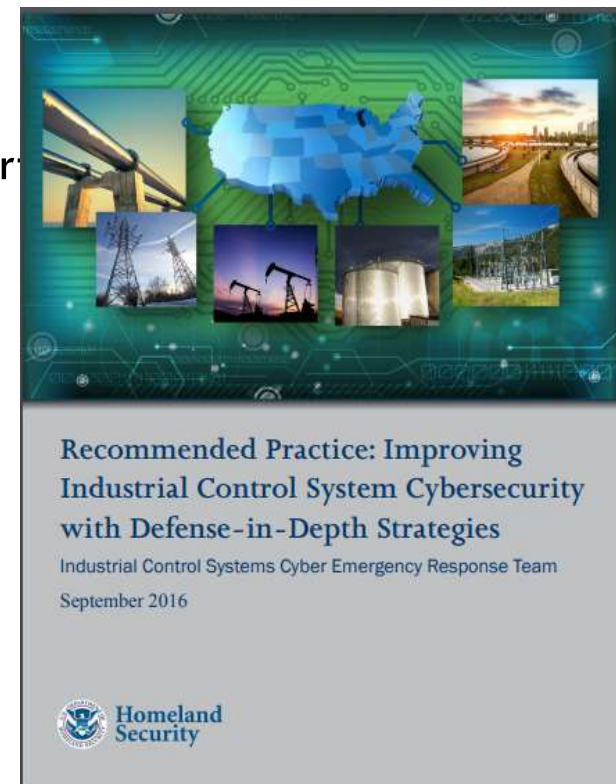
Australian Cyber Security Centre

- Strategies to Mitigate Cyber Security Incidents (Top 37, formally Top 35)

- Essential 8 Maturity Model

- Protecting Control Systems

- Remote Access Protocol

- Information Security Manual (ISM)

ACSC – Protecting Control Systems
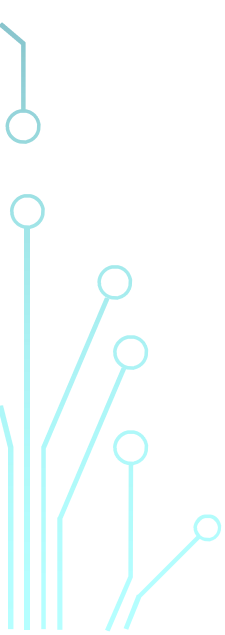
1. **Tightly control or prevent external access to the control system network**; segregate it from other networks such as the corporate network and the Internet.

2. **Implement two-factor authentication** for privileged accounts and access originating from corporate or external networks.

3. **Disable unused external ports** on control system devices.

4. **Visibly mark authorised devices** inside the control system environment with organisation-unique anti-tamper stickers.

5. **Make regular backups of system configurations** and keep them isolated. Test the restoration procedure and validate the backup integrity periodically.

6. **Regularly review firewall settings** are in an expected state.

7. Prevent devices inside the control system network from making connections to the corporate network or the Internet.

8. **Enable logging on control system devices** and store logs in a centralised location. Institute regular monitoring and incident response practices to ensure that anomalies are identified, investigated and managed in a timely fashion.

9. **Define a process for introducing external software** and patches into the control system. Where necessary (on exceptionally critical components), review code and whitelist approved binaries.

10. **Use vendor-supported applications and operating systems,** and patch associated security vulnerabilities in a timely manner.

https://www.cyber.gov.au/advice/protecting-control-systems

US Department of Energy (DoE)

- The ES-C2M2 (https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1)
  - Make sure you look at the Core Framework, Facilitators Guide and the C2M2 Toolkit
- The Risk Management Process (RMP) (https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-1)

NIST

- 800-37 r1 – *Guide for Conducting Risk Assessments*

- 800-61 r2 – *Computer Security Incident Handling Guide*

- 800-82 r2 – Guide to Industrial Control Systems (ICS) Security

- 800-100 r1 – Information Security Handbook: A Guide for Managers

- 800-53 r4 – Security and Privacy Controls for Federal Information Systems and Organizations

Useful Tips

- Knapp 3x3 Model

- PwC's Cyber Savvy

- Security Principles – Saltzer and Schroder

Useful Tips – Knapp's 3x3 Model

It is not as simple as OT/IT DMZ, or my favourite the 'air gap'!

This is a nice high level model for conversations

Use this to think about where controls are placed and potential blind spots but remember to consider compensating controls

	Enterprise	SCADA	Device Network
Data	Enterprise Applications & Data	SCADA Applications & Production Data	Controller Logic
Network	Enterprise Network	SCADA / Operations Network	Device Networks
Endpoint	Enterprise Endpoints	SCADA Servers, Process HMI	Process Controllers, Device HMI, IED

Ref - https://www.securityweek.com/new-cyber-security-model-scada
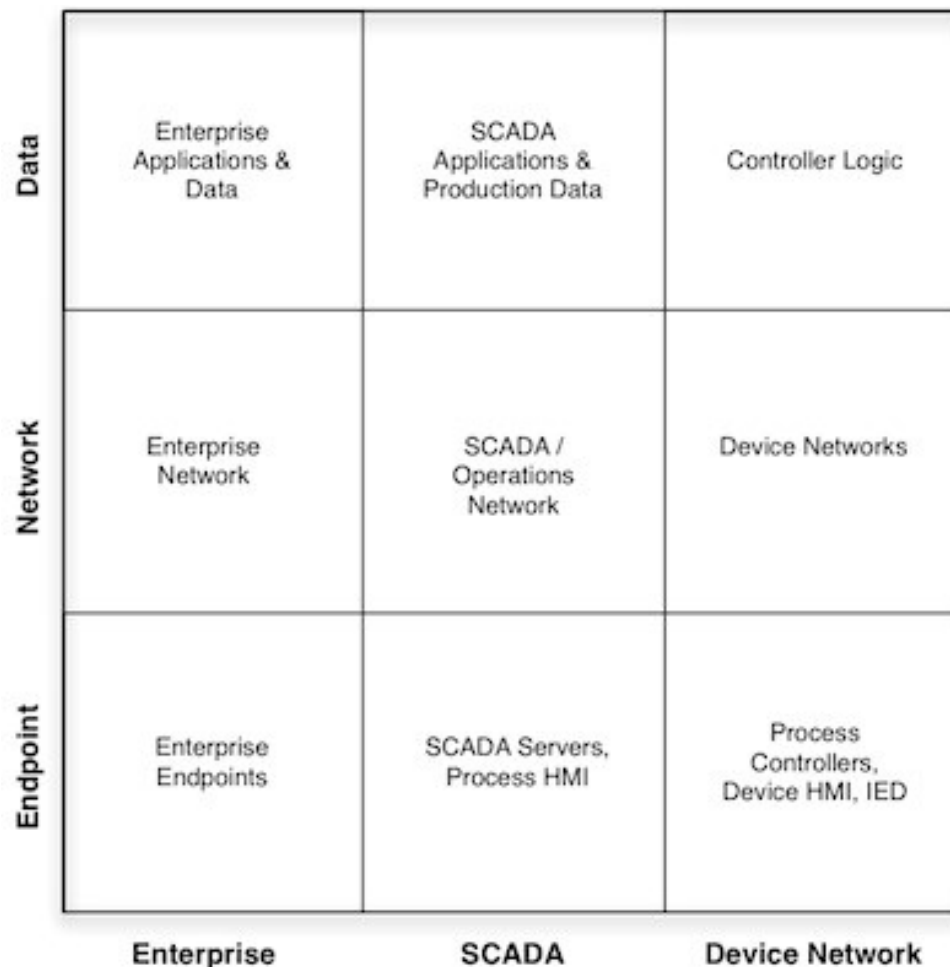
Useful Tips – PwC's Cyber Savvy

- This is a nice management ready document to share regarding the security of IT/OT Systems

- It also has a Top 10 list of things to consider

Publicly accessible OT systems

Insecure remote connectivity to OT networks

Missing security updates

Poor password practices

Insecure firewall configuration and management

OT systems located within corporate IT networks

Weak protection of the corporate IT network from OT systems

Lack of segmentation within OT networks

Unrestricted outbound internet access from OT networks

Insecure encryption and authentication for wireless OT networks.

10 most likely ways your operational technology network will be compromised
December 2015

Cyber savvy: Securing operational technology assets

pwc

www.pwc.com.au

https://www.pwc.com.au/publications/cyber-savvy-securing-operational-technology-assets.html

Useful Tips – Saltzer and Schroder

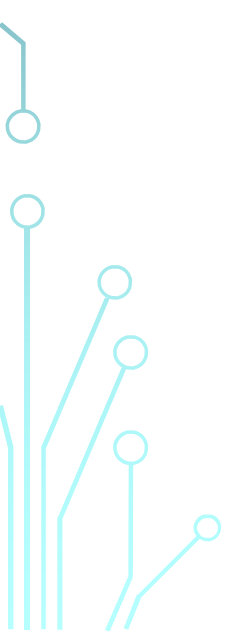These are an excellent list of design principles.

- **Economy of mechanism:** Keep the design as simple and small as possible.

- **Fail-safe defaults:** Base access decisions on permission rather than exclusion.

- **Complete mediation:** Every access to every object must be checked for authority.

- **Open design:** The design should not be secret.

- **Separation of privilege:** Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.

- **Least privilege:** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.

- **Least common mechanism:** Minimize the amount of mechanism common to more than one user and depended on by all users.

- **Psychological acceptability:** It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

- **Work factor:** Compare the cost of circumventing the mechanism with the resources of a potential attacker.

- **Compromise recording:** It is sometimes suggested that mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss.

Ref - https://en.wikipedia.org/wiki/Saltzer_and_Schroeder%27s_design_principles

Thank you!

- There is a lot of material in this deck so I will make it available on my GitHub at https://github.com/belarge/BSides2019 (After the conference)

- Follow me on Twitter @beLarge

- I'm always keen for a beer or coffee, hit me up!