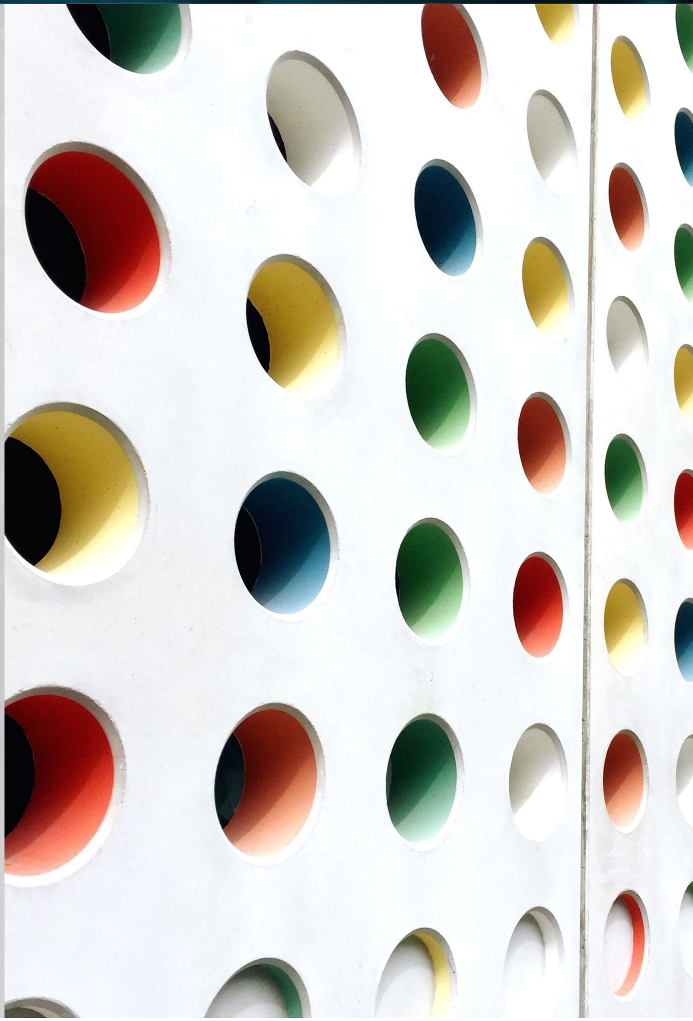
SANS
APAC ICS
Summit & Training 2022

#APACICSSummit22

Applying OT cyber security to projects



/whois @beLarge

- Operational Technology (OT) Security Team Leader at Powerlink
- A cyber security architecture enthusiast & infrastructure tourist
- Worked in IT and OT in Network Engineering and Cyber Security roles for 15 years
- Bach Eng (Telecomms) QUT and Master Business (Applied Finance) QUT

GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST ISA

ISA/IEC 62443 CYBERSECURITY MAINTENANCE SPECIALIST ISA

ISA/IEC 62443 CYBERSECURITY RISK ASSESSMENT SPECIALIST ISA

ISA/IEC 62443 CYBERSECURITY DESIGN SPECIALIST ISA

SABSA FOUNDATION LEVEL SCF

alc Cyber Security Foundation+Practitioner CERTIFIED

Today’s Agenda

1. The context

2. Tools for applying security to projects

3. My approach

The context

Does this sound familiar …

Do what do you usually do?

Someone said I have to pen test this???

Why do I have to do this on **_MY_** Project?

We need to have this done yesterday!

How long do you need to do cyber security?

Don’t you just have a standard checklist?

What do I have to do for <FRAMEWORK X>?

We are already behind schedule.

Can we just get a schedule?

I budgeted you a week to do the security review.

Don’t worry it’s just a POC

We can’t do that, we’ve already signed the contract.

Wouldn’t this be better …

Hey, we are doing this new project can we have a chat about the threat model?

Here is our standard list of security requirements as a base and we can extend it for this project

We learnt about this issue on the previous project let’s add the time into the schedule at the start of the project

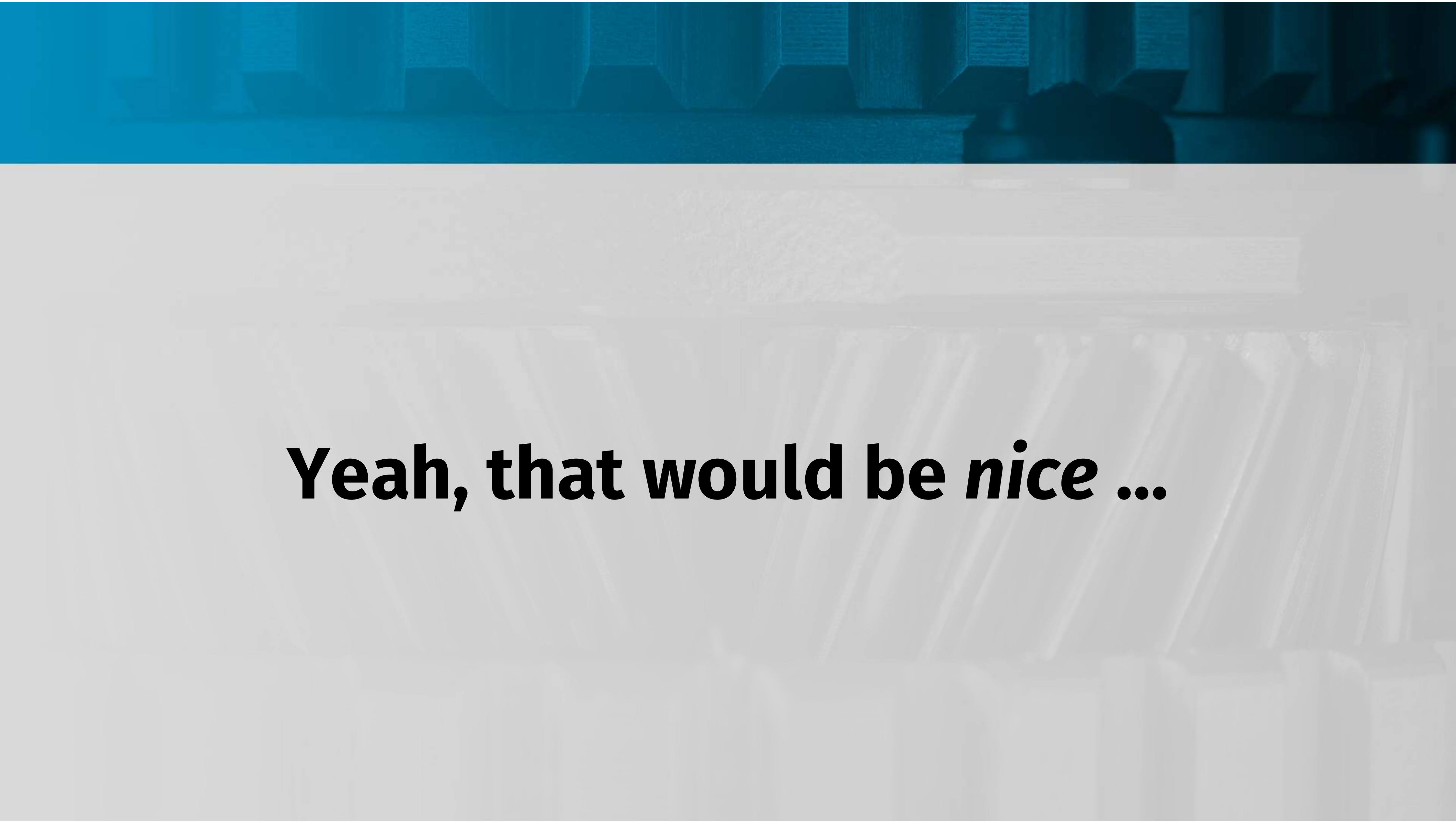
Here is a starting schedule of activities that we can use for the estimate

Security Ops are going to be so happy with this Cyber Security Requirements Specification (CSRS)!

This is the portfolio of projects at their cyber security review gates.

The project sponsor has let me know that we can’t sign the contract until we have the Security team's input.

Have you issued our standard OT Cyber security questionnaire so we can evaluate the vendor?



Yeah, that would be *nice* …

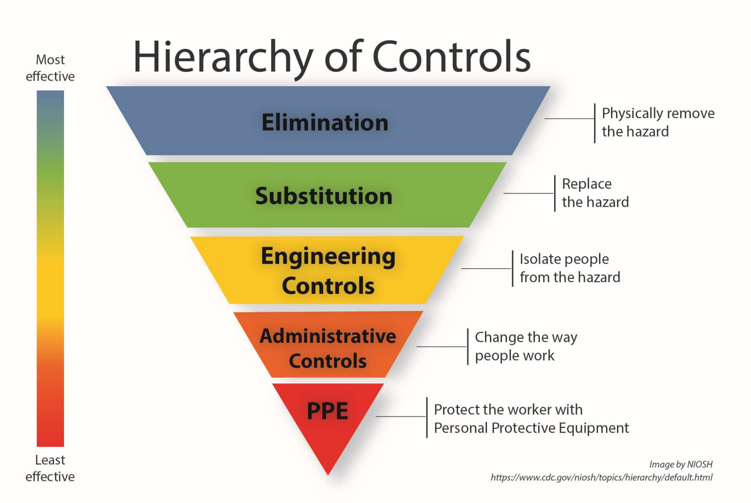
Some Tools

Concepts & tools I find useful

- Align Cyber Security and Safety
- System Engineering Concepts
- Project and Program Management Tools
- Security Layers & Abstraction
- Security Standards and Frameworks
- The Cyber V-Model

Align Cyber Security and Safety

- Engineering & Asset Operator organisations understand the importance of involving safety in all activities
- Existing safety standards that require cyber security (e.g. IEC 61508, ISA TR 84)
- Aim to Eliminate (*Engineer out*) Cyber Risk – like we do with Safety Risk
- Think in terms of the Heinrich (Safety) Triangle


Hierarchy of Controls
Most effective
Least effective
Elimination
Physically remove the hazard
Substitution
Replace the hazard
Engineering Controls
Isolate people from the hazard
Administrative Controls
Change the way people work
PPE
Protect the worker with Personal Protective Equipment
Image by NIOSH
https://www.cdc.gov/niosh/topics/hierarchy/default.html

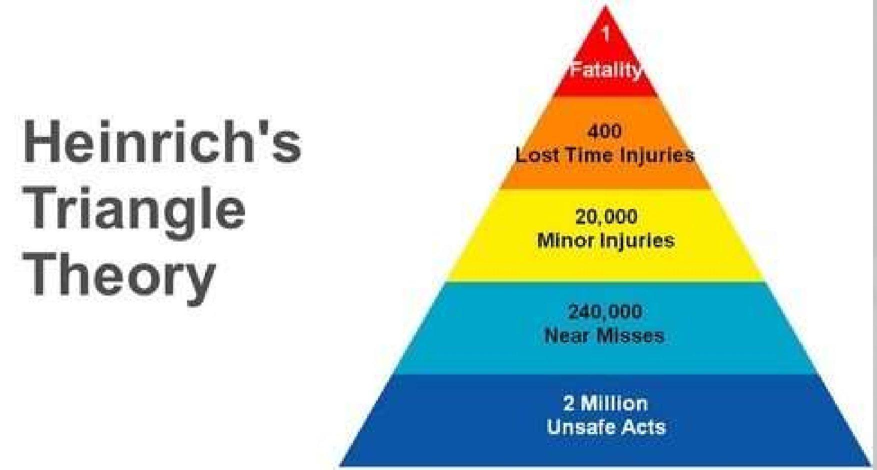
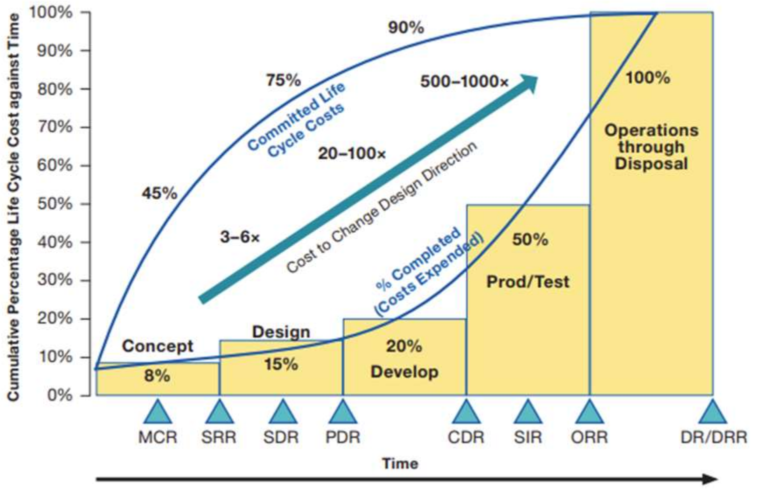


Image Source - https://www.shponline.co.uk/common-workplace-hazards/heinrichs-triangle-health-and-safety-cpd/ & https://www.cdc.gov/niosh/topics/hierarchy/default.html

System Engineering Concepts

- System Engineering is the discipline that aims to optimise the system as a whole rather than its individual components (hardware, software, people and process)
- Considers the whole of life performance and cost of the system and looks at from "the big picture"
- Starts with the Concept of Operations (ConOps), develops requirements, models and ultimately design solutions
- The NASA Systems Engineering Handbook is an excellent reference and starting point to learn more



MCR	Mission Concept Review	CDR	Critical Design Review
SRR	System Requirements Review	SIR	System Integration Review
SDR	System Definition Review	ORR	Operational Readiness Review
PDR	Preliminary Design Review	DR/DRR	Decommissioning/Disposal Readiness Review

Adapted from INCOSE-TP-2003-002-04, 2015

FIGURE 2.5-1 Life-Cycle Cost Impacts from Early Phase Decision-Making

Source - https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook_0.pdf

A quick primer on Projects and Programs

Portfolio (Benefits)

- The whole of company investment activity to manage benefits for the business
- Benefits **should** be measurable in financial terms

Program (Outcomes)

- Interrelated and interdependent projects that are managing integrated outcomes for the business
- Flexibility in time and project scopes
- Outcomes are not always measurable but are considered improvements

Project (Outputs)

- Individual packages of work with clearly defined outputs

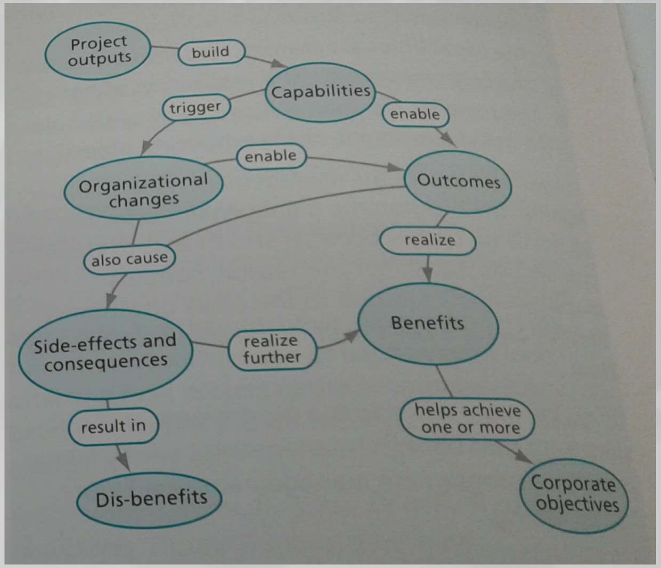


Image source – A Photo from the AXELOS/TSO Managing Successful Programmes 4th Ed

Project Management Tools

Waterfall

- Draft Requirements that consider security
- Ensure that the right level of effort is applied to the requirements elicitation phase, don’t rush this!
- Also, make sure you are managing requirements and their impact to cyber security through the project life cycle preferably with a tool
- **Requirements!**

Agile

- Focus on building the right rituals and awareness of why security is important from the beginning
- Don’t try to fix it all in one sprint or assign security to one epic
- Use concepts like the paved road and make the most secure option the easiest option for projects

Program Management Tools

- What is the sequencing and timing of projects, how is the cyber security team resourced?
- How are you learning from early projects, what is the knowledge management approach?
- Are you properly managing outcomes and benefits, are you also using support teams like procurement well?

Layers of Security

- **Conceptual** – Do you understand security capabilities and your security architecture
- **Logical & Physical** – Where and how do you deliver security services (e.g. Segmentation or Continuous Monitoring)
- **Component** – How are you configuring and building components to be secure, how are you managing your individual security components
- Avoid having just *one* security approach for everything

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Project Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
LOGICAL ARCHITECURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Process Schedule
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Mgmt, Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools

Source - From W100 *SABSA White Paper (2009)* - https://sabsa.org/white-paper-requests/

The V-Model

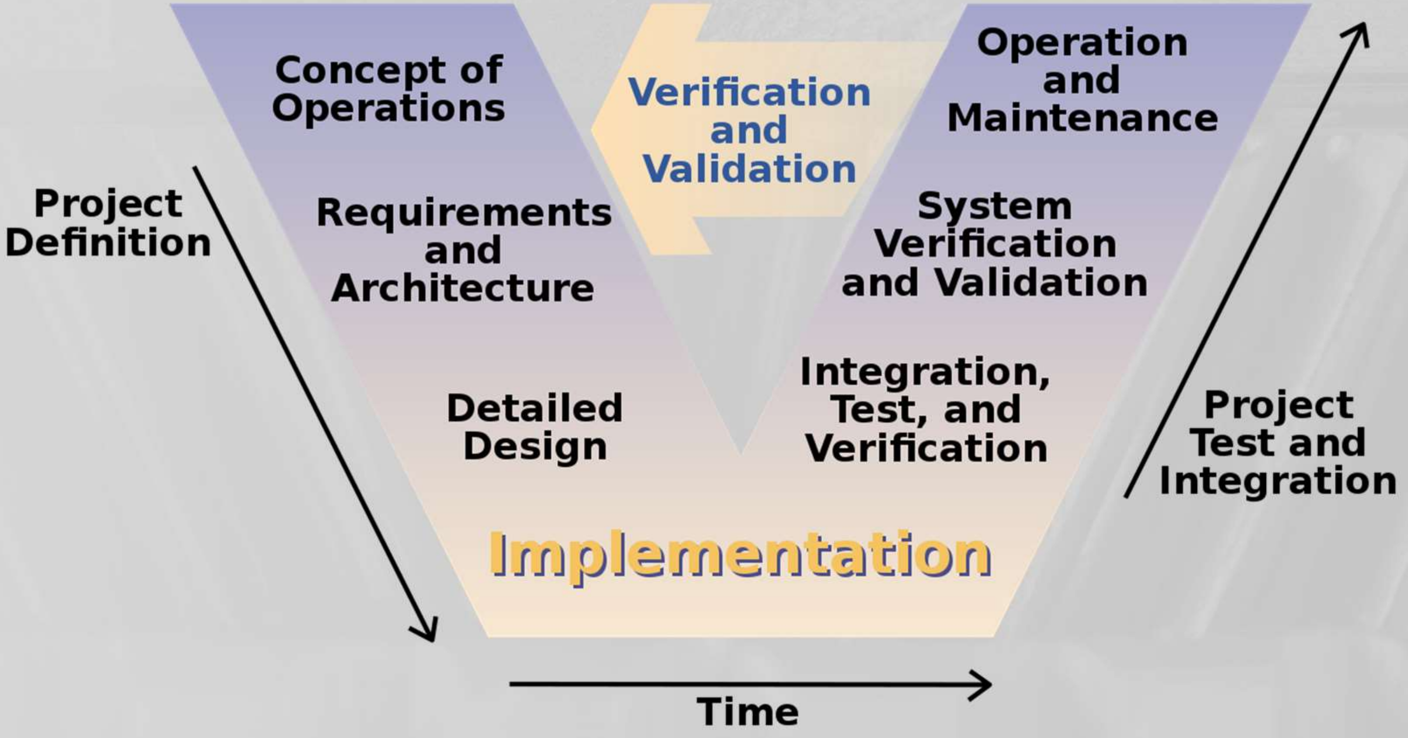
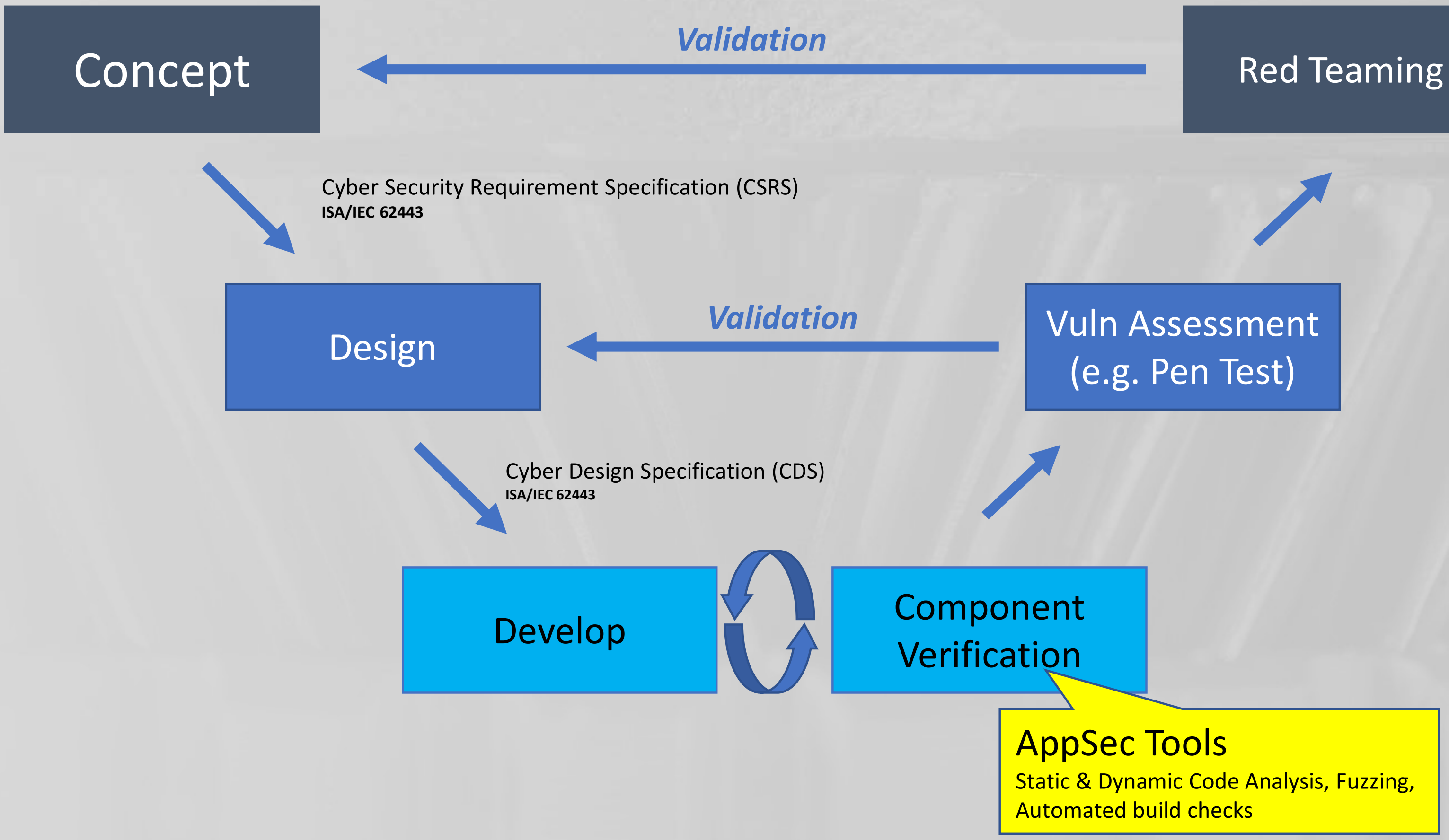

Concept of Operations
Verification and Validation
Operation and Maintenance
Project Definition
Requirements and Architecture
System Verification and Validation
Integration, Test, and Verification
Detailed Design
Project Test and Integration
Implementation
Time

Image source - https://en.wikipedia.org/wiki/V-Model

The Cyber V-Model



Concept

Validation

Red Teaming

Cyber Security Requirement Specification (CSRS)
ISA/IEC 62443

Design

Validation

Vuln Assessment
(e.g. Pen Test)

Cyber Design Specification (CDS)
ISA/IEC 62443

Develop

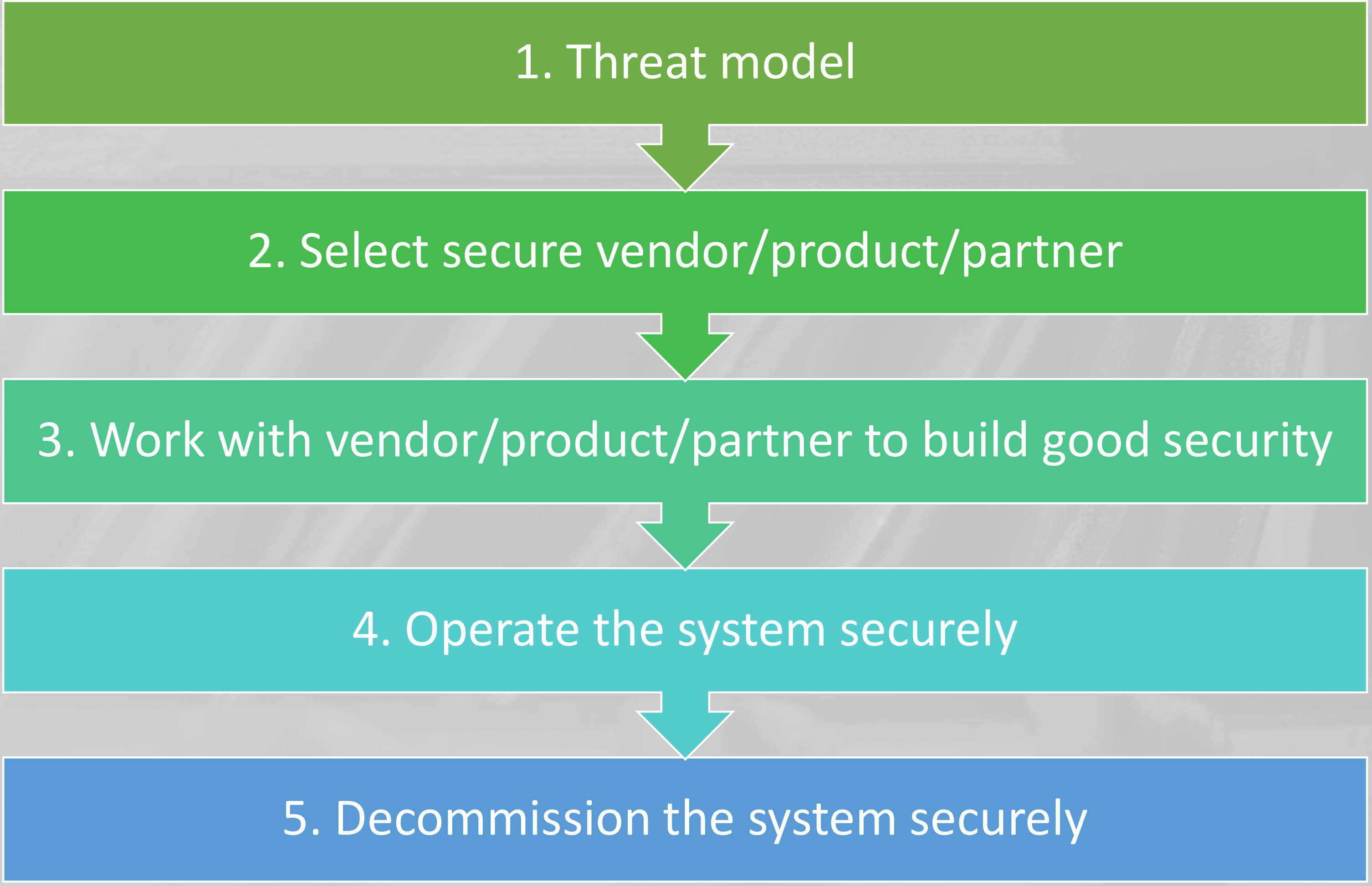
Component Verification

AppSec Tools
Static & Dynamic Code Analysis, Fuzzing, Automated build checks

Standards and Frameworks

- ISA/IEC 62443
  - Part 2-1 – Establish and operate a Cyber Security Management System (CSMS) to build whole of organisation OT cyber security capability
  - Part 3-2 – Guidance on how to assess cyber security risk and manage cyber risk for projects
  - Part 3-3 – Prescriptive OT Cyber security requirements for Industrial Automation and Control Systems (IACS) at a system level
  - Part 4-2 – Prescriptive guidance OT Cyber security controls for IACS components
- ISA TR 84.00.09 & Security PHA Reviews (SPR)
  - Linking Cyber Security and Safety Engineering Activities
- NIST 800-82 r3 (Draft)
  - Specific control guidance and application for Industrial Control Systems as per NIST 800-53
- ES-C2M2 (And AESCSF)
  - A capability framework that can help you self assess your existing security capabilities and identify areas for improvement

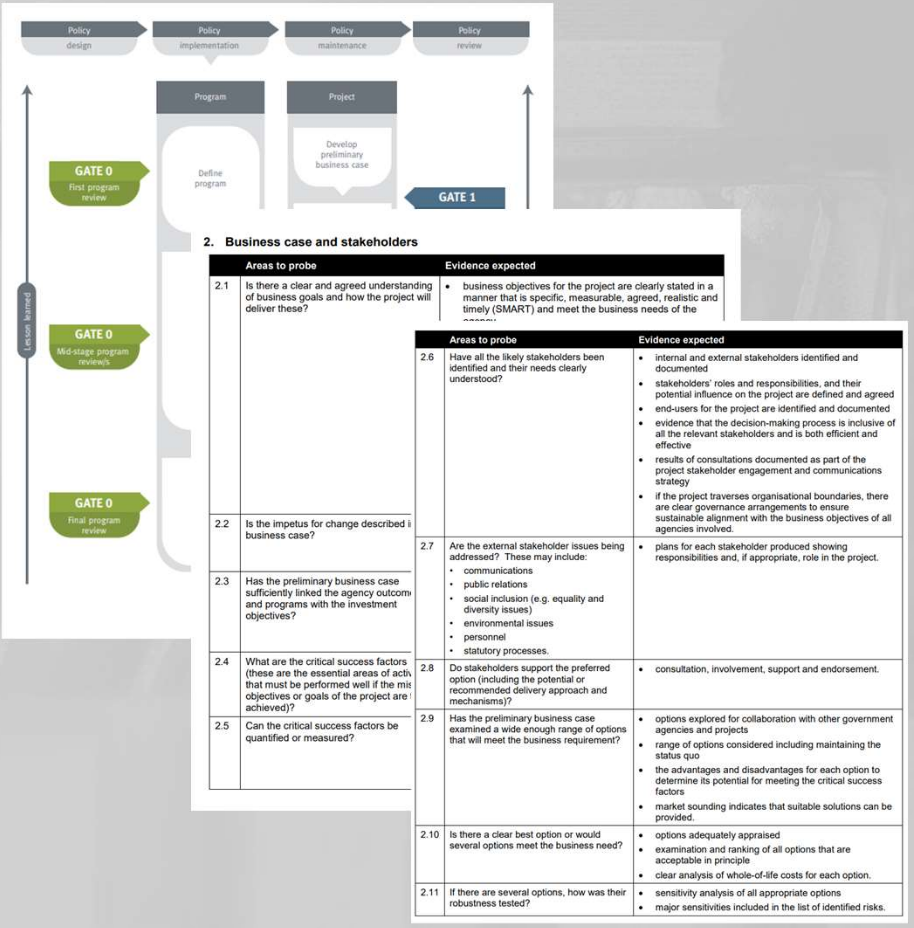
My Approach



1. Threat model
2. Select secure vendor/product/partner
3. Work with vendor/product/partner to build good security
4. Operate the system securely
5. Decommission the system securely

Inspired by the Qld Treasury Gateway Model

- My approach was inspired by the Queensland Treasury Gateway Review (Assurance) Model (https://www.treasury.qld.gov.au/programs-and-policies/project-assessment-framework/gateway-reviews/)
- Consists of 5 Gates for Projects and a Gate 0 for Programmes
- Has detailed guidance on areas to review and expected evidence for each Gate


Policy
design
Policy
implementation
Policy
maintenance
Policy
review
Program
Project
Define
program
Develop
preliminary
business case
GATE 1
GATE 0
First program
review
GATE 0
Mid-stage program
review/s
GATE 0
Final program
review
Lesson learned

2. **Business case and stakeholders**

	Areas to probe	Evidence expected
2.1	Is there a clear and agreed understanding of business goals and how the project will deliver these?	• business objectives for the project are clearly stated in a manner that is specific, measurable, agreed, realistic and timely (SMART) and meet the business needs of the
2.2	Is the impetus for change described i business case?	
2.3	Has the preliminary business case sufficiently linked the agency outcom and programs with the investment objectives?	
2.4	What are the critical success factors (these are the essential areas of acti that must be performed well if the mis objectives or goals of the project are achieved)?	
2.5	Can the critical success factors be quantified or measured?	

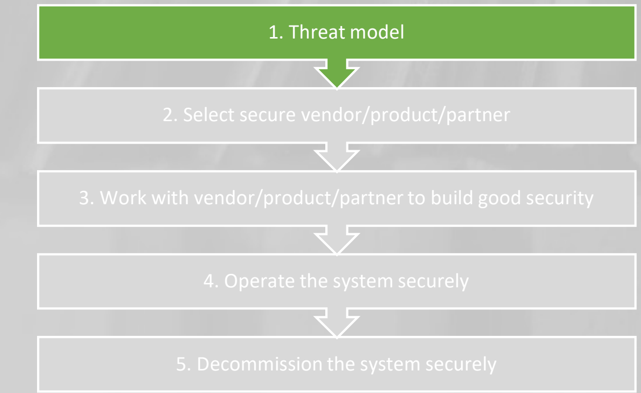
	Areas to probe	Evidence expected
2.6	Have all the likely stakeholders been identified and their needs clearly understood?	• internal and external stakeholders identified and documented • stakeholders' roles and responsibilities, and their potential influence on the project are defined and agreed • end-users for the project are identified and documented • evidence that the decision-making process is inclusive of all the relevant stakeholders and is both efficient and effective • results of consultations documented as part of the project stakeholder engagement and communications strategy • if the project traverses organisational boundaries, there are clear governance arrangements to ensure sustainable alignment with the business objectives of all agencies involved.
2.7	Are the external stakeholder issues being addressed? These may include: • communications • public relations • social inclusion (e.g. equality and diversity issues) • environmental issues • personnel • statutory processes.	• plans for each stakeholder produced showing responsibilities and, if appropriate, role in the project.
2.8	Do stakeholders support the preferred option (including the potential or recommended delivery approach and mechanisms)?	• consultation, involvement, support and endorsement.
2.9	Has the preliminary business case examined a wide enough range of options that will meet the business requirement?	• options explored for collaboration with other government agencies and projects • range of options considered including maintaining the status quo • the advantages and disadvantages for each option to determine its potential for meeting the critical success factors • market sounding indicates that suitable solutions can be provided.
2.10	Is there a clear best option or would several options meet the business need?	• options adequately appraised • examination and ranking of all options that are acceptable in principle • clear analysis of whole-of-life costs for each option.
2.11	If there are several options, how was their robustness tested?	• sensitivity analysis of all appropriate options • major sensitivities included in the list of identified risks.

1. Threat Model

- Start as early as possible defining the block diagram of the system and then build a threat model.
- This should be done before involving any external parties and it is a method to build a common understanding of the system, the applicable threats and areas of focus for security within the organisation.
- Use this stage to review your existing architecture, risk registers and lessons learnt from previous projects.

Activities and Gates

1. Block Diagram of the System
2. Threat Model of the System



1. Threat model

2. Select secure vendor/product/partner

3. Work with vendor/product/partner to build good security

4. Operate the system securely

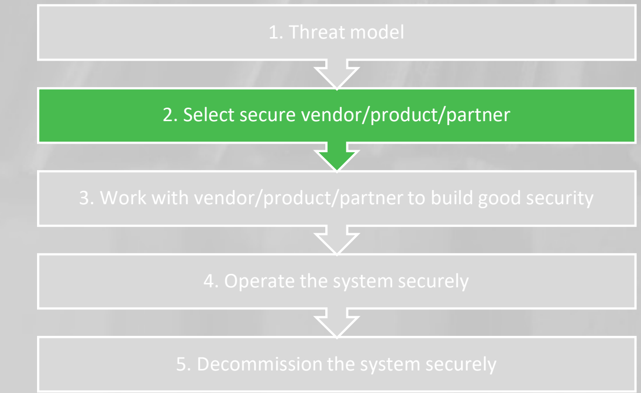
5. Decommission the system securely

2. Select a secure vendor/product/partner

- This stage is when you align the procurement activities and cyber security.
- This stage is where you work with the vendor/product/partner to understand their cyber security capabilities and if they meet your security requirements.
- The right time to understand the vendor recommended practices.

Activities and Gates

1. Satisfactory Cyber Security Assessment
2. Execute Procurement activities and define Contract that addresses cyber security
3. Initial (High Level) Cyber Security Risk Assessment Complete


1. Threat model

2. Select secure vendor/product/partner

3. Work with vendor/product/partner to build good security

4. Operate the system securely

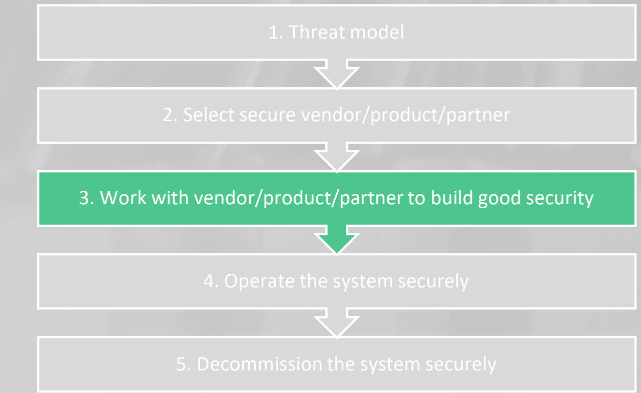
5. Decommission the system securely

3. Work with vendor/product/partner to do security

- This stage is where you work with the vendor/product/partner to build the system securely.
- This is where you issue your organisations relevant security architecture, standards and patterns.
- This is where you also test the system prior to go live and complete the Cyber Security Factory and Site Acceptance testing.
- This is also when you would complete any Cyber Security Penetration testing activities.
- Finally this is where you would ensure the operations team have all the required information and accept the system prior to go live.

Activities and Gates

1. Detailed Risk Assessment Complete
2. Cyber Security Requirements Specification (CSRS) & Cyber Security Design Specification (CDS)
3. Achieve Conformance with security standards and architecture
4. Perform Cyber Security FAT and SAT
5. Perform Cyber Security Penetration Testing
6. Complete Cyber Security Production Readiness Handover

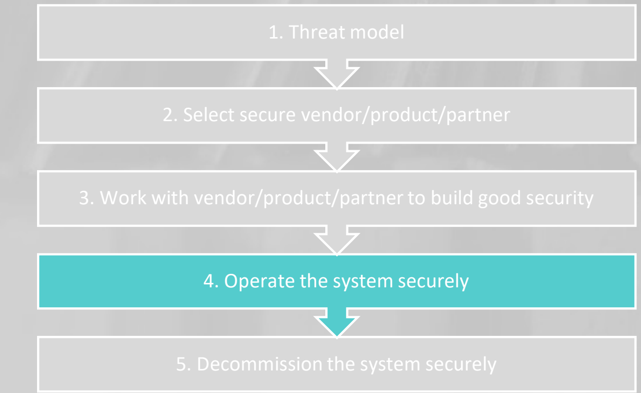

1. Threat model
2. Select secure vendor/product/partner
3. Work with vendor/product/partner to build good security
4. Operate the system securely
5. Decommission the system securely

4. Operate the system securely

- In this stage, the system is operated as per guidance and required cyber maintenance is undertaken.
- Enact the Cyber Security provisions as per your contract and ensure that the vendor is keeping you informed of any relevant security incidents, threats and discovered vulnerabilities.
- This is where you also should be receiving vendor patches etc.

Activities and Gates

1. Operate the System Security Plan
2. Enact the Vendor Management Plan

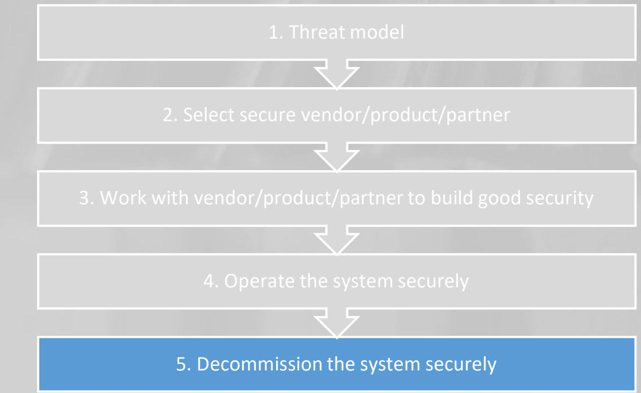

1. Threat model
2. Select secure vendor/product/partner
3. Work with vendor/product/partner to build good security
4. Operate the system securely
5. Decommission the system securely

5. Decommission the system securely

- Once the system has reached the end of its life it must be securely decommissioned.
- The system will likely have secrets and passphrases that should be destroyed and the system media should be securely erased prior to any systems being on sold. For high risk assets physical destruction may be appropriate.

Activities and Gates

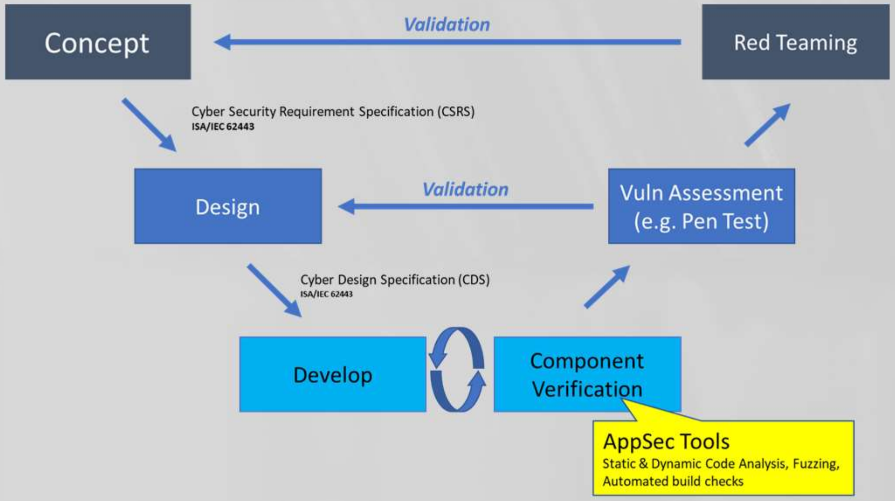
1. Execute the System Decommissioning Plan
2. Assure the system has been wiped before disposing


1. Threat model
2. Select secure vendor/product/partner
3. Work with vendor/product/partner to build good security
4. Operate the system securely
5. Decommission the system securely

Quick Recap

1. **Align** Cyber Security and Safety
2. **Think in** Security Layers & Abstraction (e.g. Conceptual, Logical and Component)
3. **Use** Security Standards and Frameworks

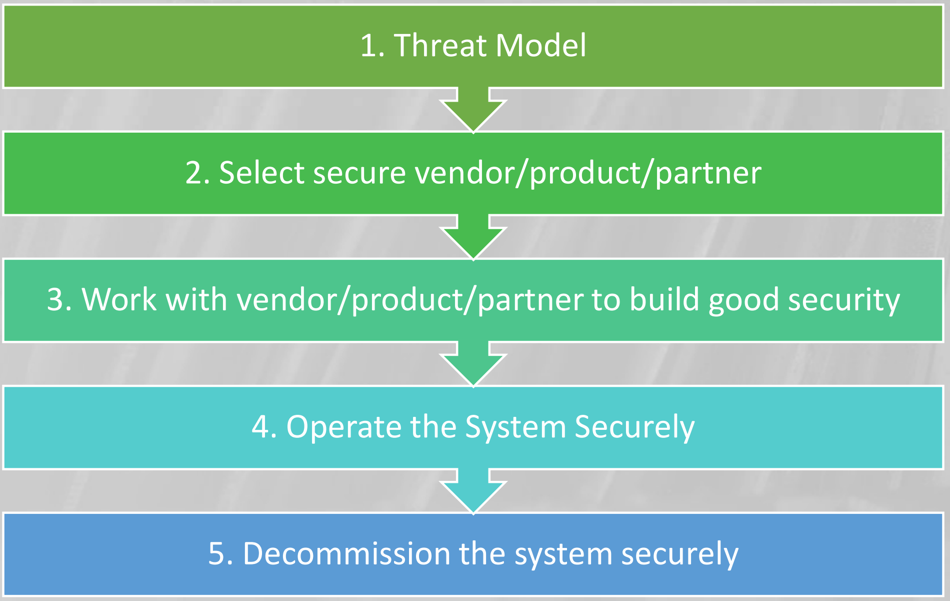
The Cyber V Model


Concept
Validation
Red Teaming
Cyber Security Requirement Specification (CSRS)
ISA/IEC 62443
Design
Validation
Vuln Assessment (e.g. Pen Test)
Cyber Design Specification (CDS)
ISA/IEC 62443
Develop
Component Verification

AppSec Tools

Static & Dynamic Code Analysis, Fuzzing, Automated build checks

My Project Approach


1. Threat Model
2. Select secure vendor/product/partner
3. Work with vendor/product/partner to build good security
4. Operate the System Securely
5. Decommission the system securely

SANS
APAC ICS
Summit & Training 2022

ICS
#APACICSSummit22

Q&A

Ask Your Questions in Slack:
#1a-questions-for-speakers

Feedback Survey:
summitsurl.com/apac-ics-summit-eval

in https://linkedin.com/in/blargeau https://github.com/beLarge @beLarge