OVERVIEW OF THE ISA 62443 FRAMEWORK

ISA Brisbane Section June 2020

Please don’t sue me

- This is general advice and your environment 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***

/whois

- Graduated Bachelor Engineering (Telecommunications) First Class Honours at QUT in 2009
- Worked as a telecommunications engineer for 7 years
- Did some other stuff – went back to Uni and studied a Master of Business in Applied Finance and I am now interested in Asset Management (engineering not the finance type)
- Currently an Operational Technology Cyber Security Specialist
- Treasurer of the Brisbane Branch of the International Society of Automation (ISA)

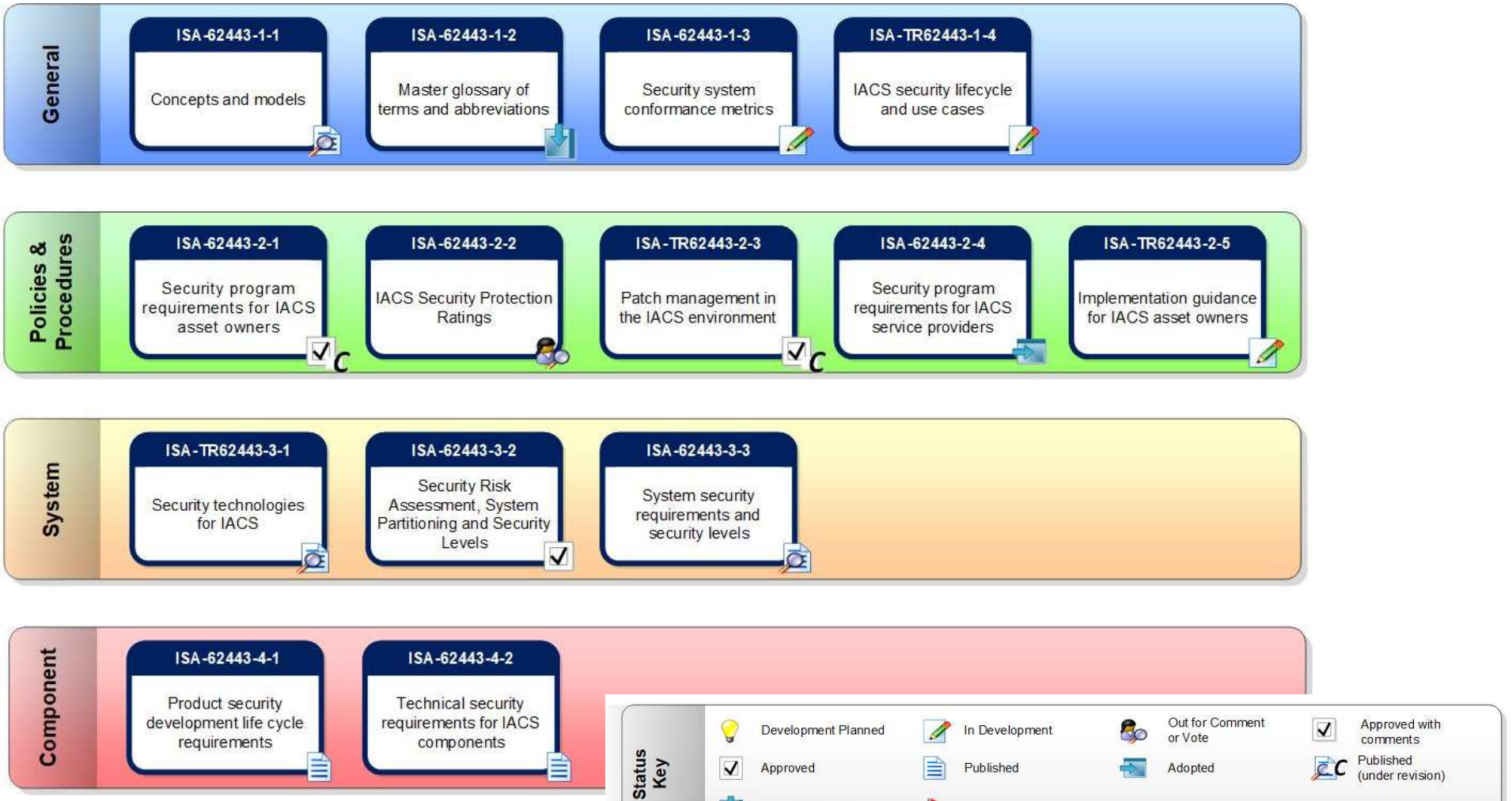
This evening's agenda

- Overview of the 62443 Standard Framework
- Review of:
  - 62443-1-1 – Terminology, concepts and models
  - 62443-2-1 – Establishing an IACS security program
  - 62443-3-2 - Security Risk Assessment for system design
  - 62443-3-3 – System security requirements and security levels
- Additional resources
- Q&A

What is the ISA 62443

- ISA/IEC 62443 is a Framework of Cyber Security Standards for Industrial Automation and Control Systems (IACS)
- ISA 99 is the Working group and the standards were originally published with ANSI as ISA 99 but are now published in partnership with the IEC and are designated ISA/IEC 62443
- You might see ISA 95 – Enterprise-Control System Integration – it is based on the Purdue Model but it is separate to ISA 62443
- ISA62443 is referenced by the NIST Cyber Security Framework but only 2 of the 14 standards referenced (2-1 and 3-3)
- Is referred to in NIST 800-82 *Guide to Industrial Control Systems (ICS) Security*

ISA 62443 Framework



[Image source https://www.isa.org/isa99/](https://www.isa.org/isa99/)

ISA 62443 Framework (cont.)

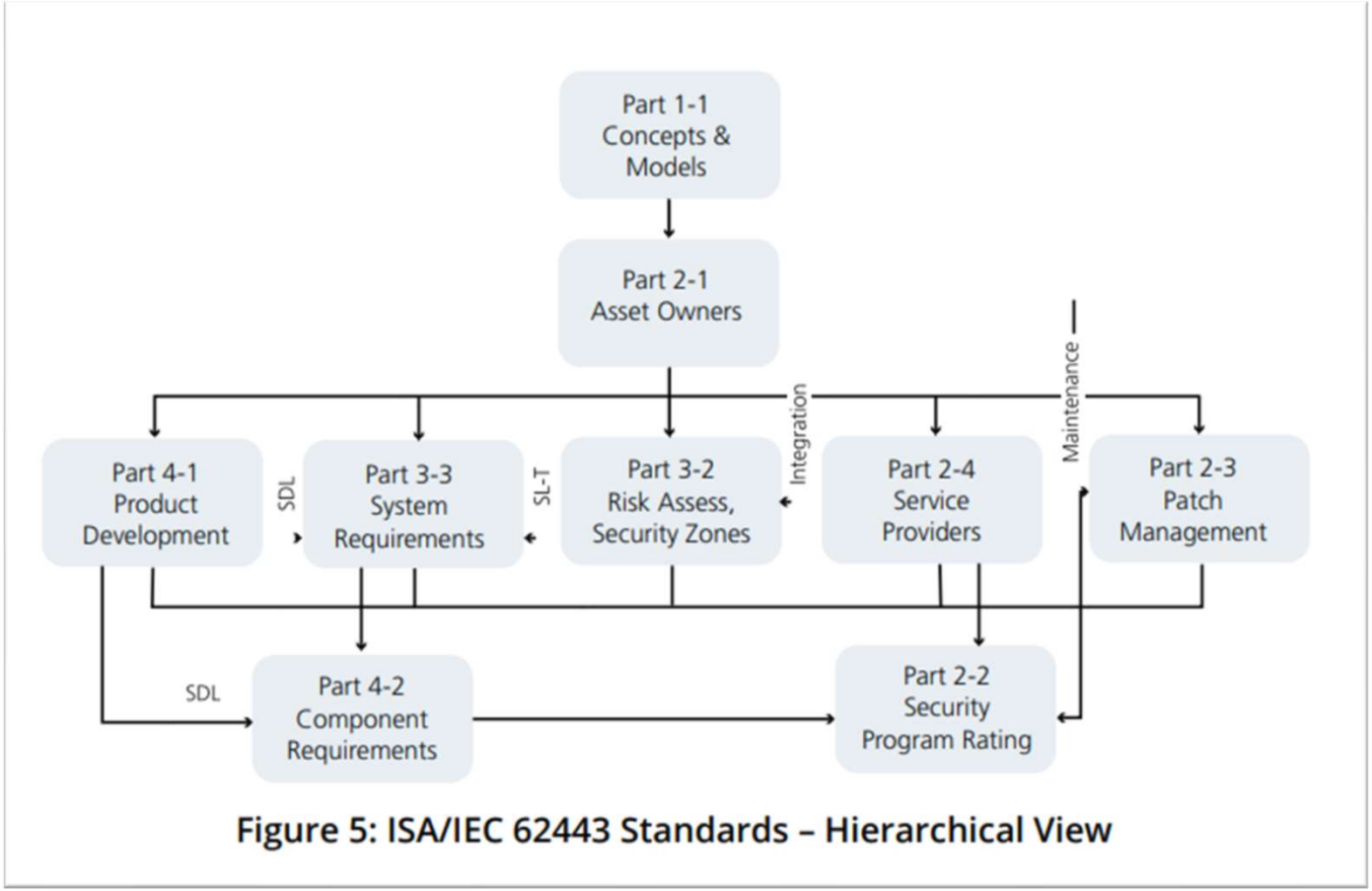


Figure 5: ISA/IEC 62443 Standards – Hierarchical View

From ISAGCA Quick Start Guide: An Overview of the ISA/IEC 62443 Standard

62443-1-1 *Concepts & Models*

- Definitions (What is an asset!!!)
- Defines an asset model taxonomy
- Zones and Conduits
- Defines Security Levels (Target, Achieve, Capability)
- Defines Policies and Procedures Requirements
- and more ...

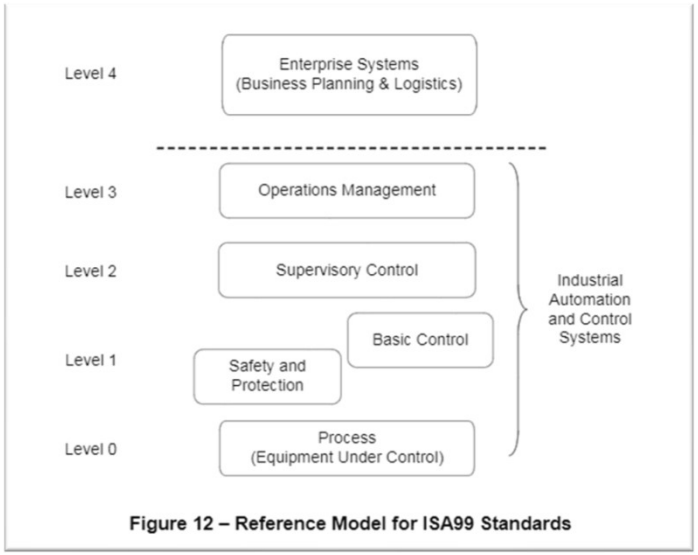


Figure 12 – Reference Model for ISA99 Standards

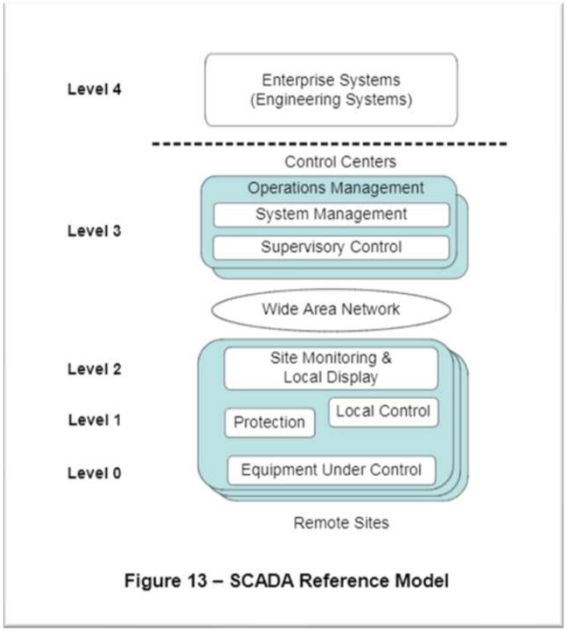


Figure 13 – SCADA Reference Model

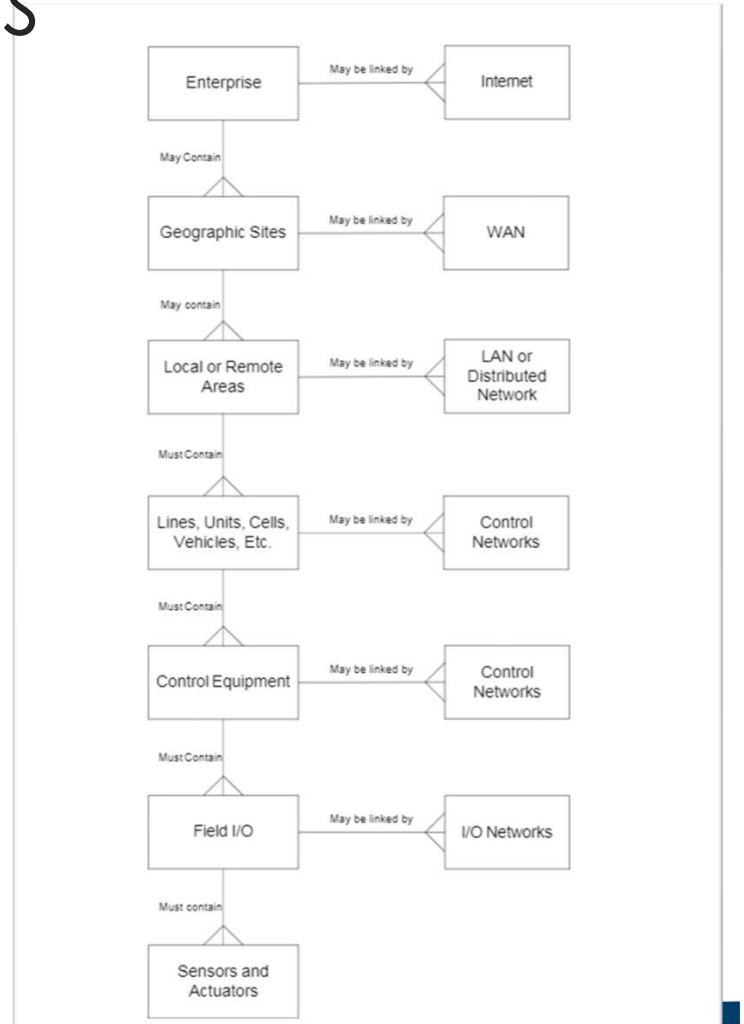


Figure 14 – Process Manufacturing Asset Model Example

Referenced from ISA 62243-1-1

62443-1-1 *Concepts & Models (cont.)*

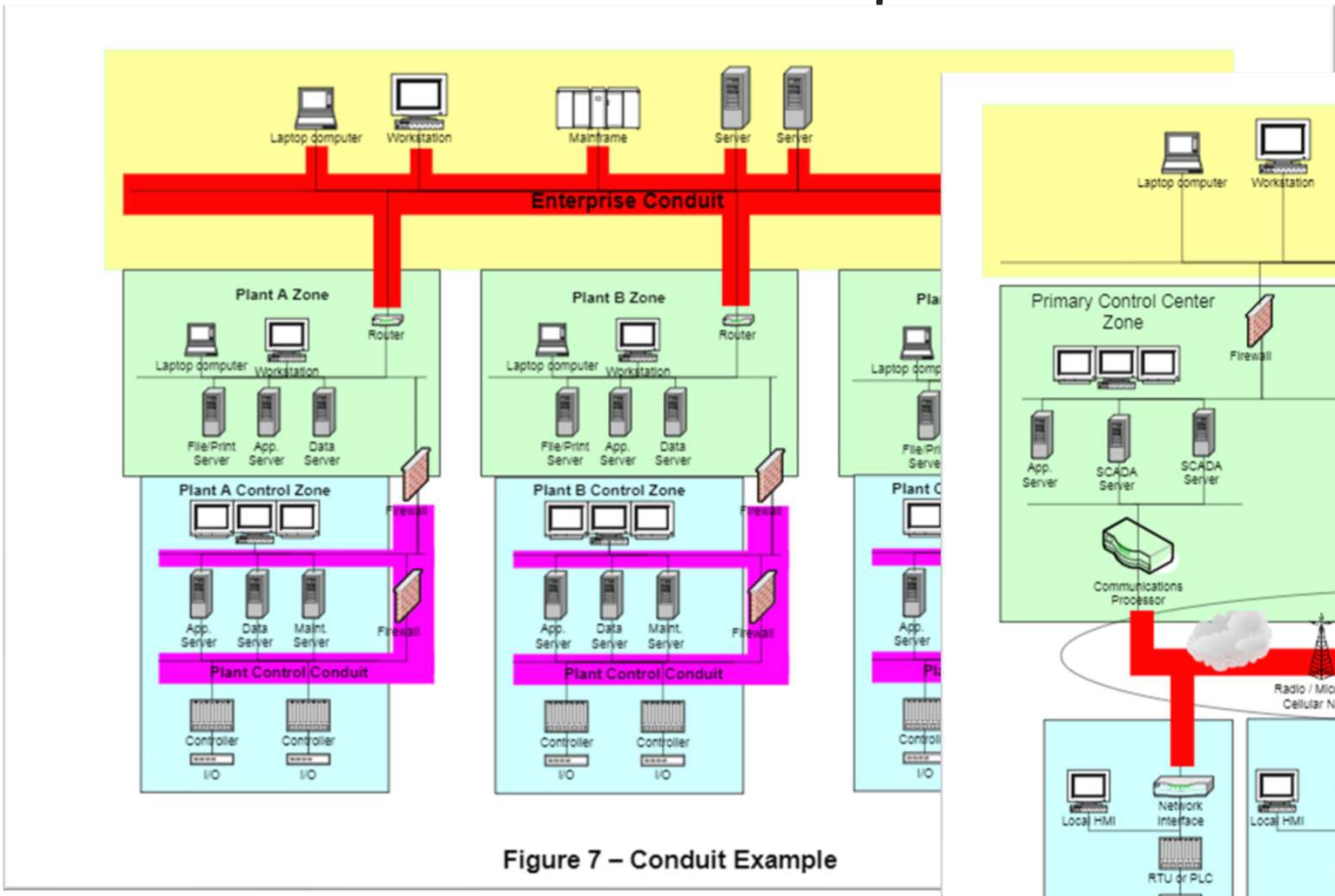


Figure 7 – Conduit Example

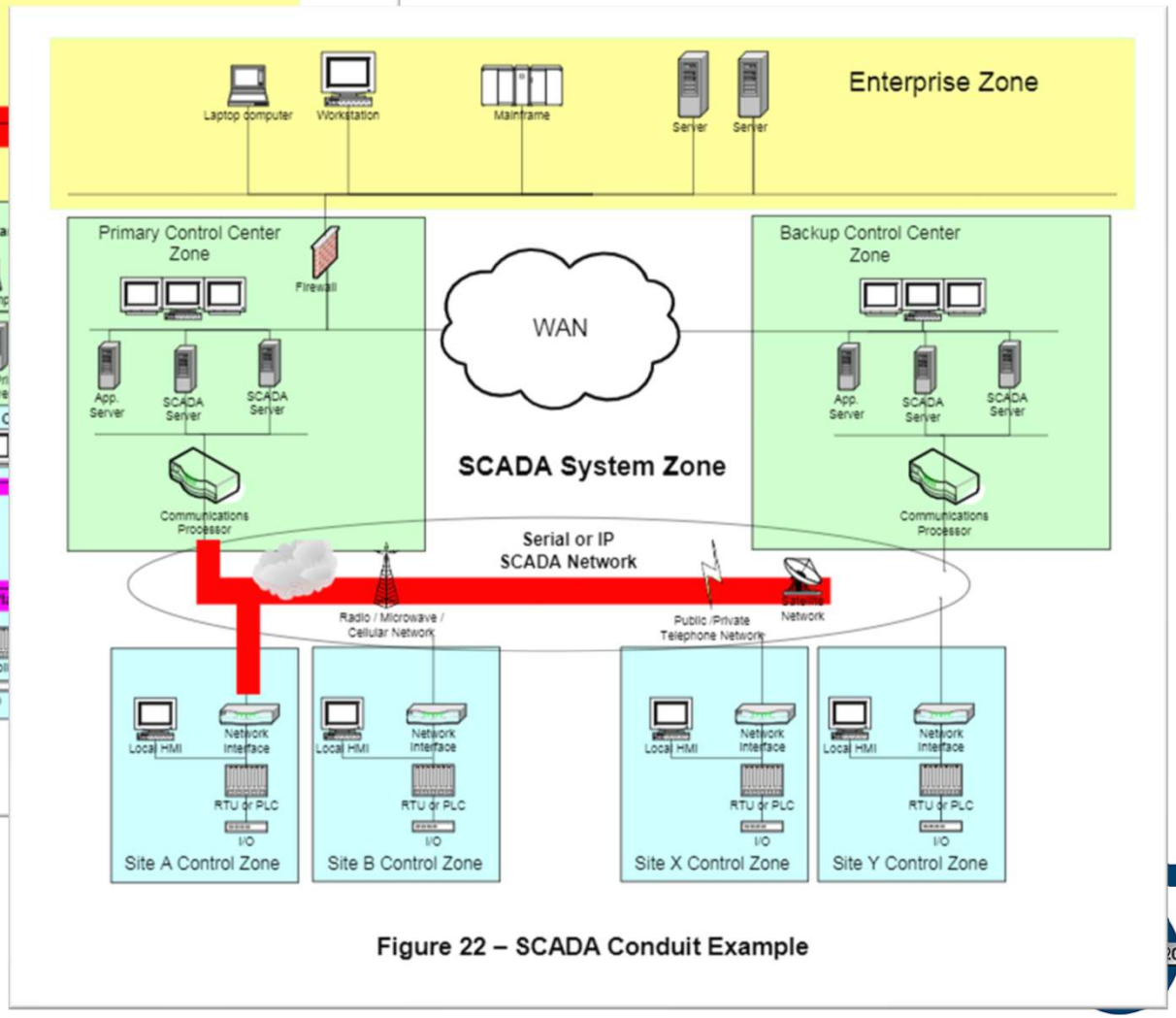


Figure 22 – SCADA Conduit Example

Referenced from ISA 62243-1-1

62443-1-1 *Concepts & Models (cont.)*

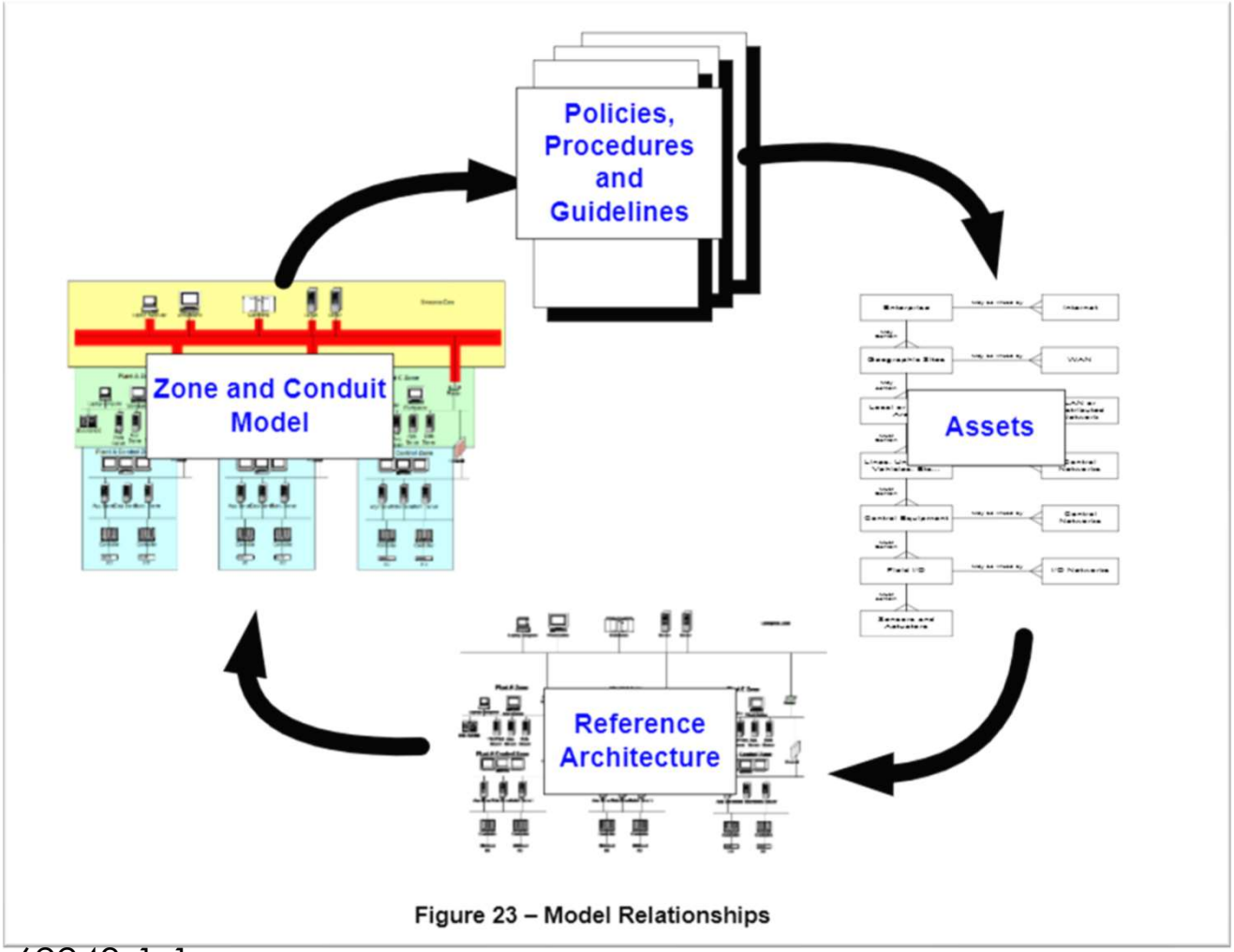


Figure 23 – Model Relationships

Referenced from ISA 62243-1-1

2-1 *Establishing an IACS Security Program*

- To be completed …

3-2 *Security risk assessments for system design*

- Formally Zones and Conduits but now Security risk assessments for system design
- Is still in Draft (was finalised in 2020)
- From the quick start guide it lists the risk management process
- From the Quick Start Guide:
  - *"A Zone is defined as a grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access, or responsible organization"*
  - *"A Conduit is defined as a logical grouping of communication channels that share common security requirements connecting two or more zones."*

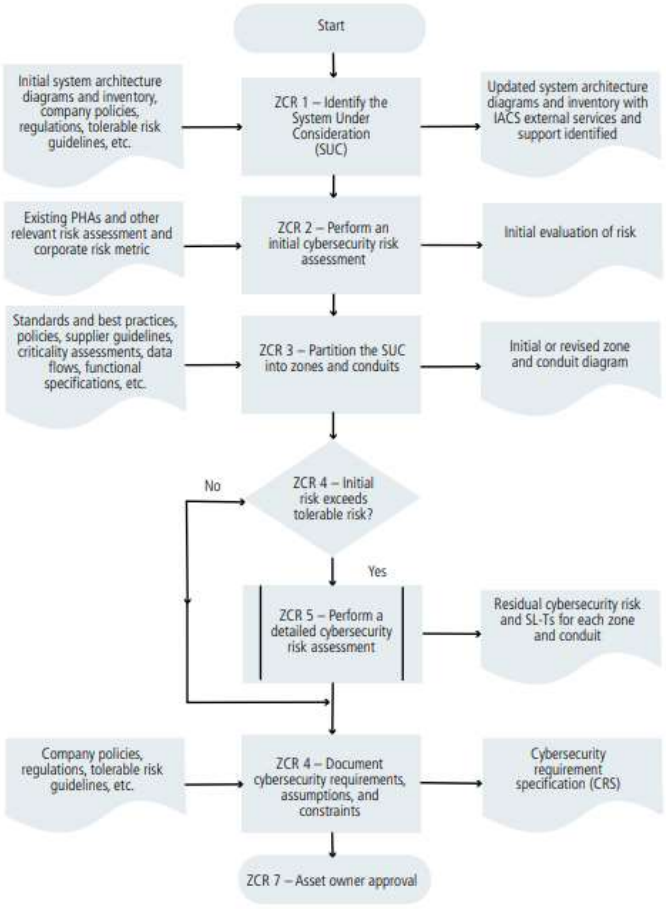


Figure 3: Risk Assessment Process

From ISAGCA Quick Start Guide: An Overview of the ISA/IEC 62443 Standard

3-3 System security requirements and security levels

Foundational Requirements

- FR 1 – Identification and Authentication Control (IAC)
- FR 2 – Use Control (UC)
- FR 3 – System Integrity (SI)
- FR 4 – Data Confidentiality (DC)
- FR 5 – Restricted Data Flow (RDF)
- FR 6 – Timely Response to Events (TRE)
- FR 7 – Resource Availability (RA)
- *Also has the concept of a Requirement Enhancement*

The associated four SLs are defined as:

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

Referenced from ISA 62243-3-3

3-3 System security requirements and security levels (cont.)

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
SR 5.1 – Network segmentati				
RE (1) Physical network s				
RE (2) Independence fro networks				
RE (3) Logical and physic networks				
SR 5.2 – Zone boundary prote				
RE (1) Deny by default, a				
RE (2) Island mode				
RE (3) Fail close				

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

9.3.2 Rationale and supplemental guidance

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. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirem

Network segmentation and the leve overall network architecture used by within their control systems. Logical some measure of protection, but m compromised. Physically segmentin that single-point-of-failure case, bu These trade-offs will need to b ISA-62443-2-1 (99.02.01)).

In response to an incident, it may network segments. In that event, th

9.3.3 Requirement enhancements

(1) Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.

(2) Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

(3) Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

Referenced from ISA 62243-3-3

Certification

- ***Security Development Lifecycle Assurance (SDLA)*** which certifies that the Security Development Lifecycle of a Product Supplier meets the requirements in Part 4-1.

Certified Site (SDLA)
ISASecure®
ISA/IEC 62443-4-1

- ***System Security Assurance (SSA)*** which certifies that Control System products have the capability to meet the requirements in Part 3-3 and have been developed in accordance with an SDLA program.

Certified Site (SSA)
ISASecure®
ISA/IEC 62443-4-1
ISA/IEC 62443-3-3

- ***Component Security Assurance (CSA)*** which certifies that Component products have the capability to meet the requirements in Part 4-2 and have been developed in accordance with an SDLA program. Certified Component products can be: Embedded Devices, Host Devices, Network Devices, and Software Applications

Certified Site (CSA)
ISASecure®
ISA/IEC 62443-4-1
ISA/IEC 62443-4-2

From ISAGCA Quick Start Guide: An Overview of the ISA/IEC 62443 Standard

Would you like to know more?

Image Source - https://www.mandatory.com/culture/1223945-great-memes-movie-starship-troopers

Additional Resources

- The ISA Global Cyber Security Alliance – Quick Start Guide to ISA 62443 - https://gca.isa.org/isagca-quick-start-guide-62443-standards
- Read the Standards! Read the standards for free with your Membership benefit https://www.isa.org/standards-and-publications/isa-standards/member-access-to-standards/
- Follow @ISA99Chair on Twitter
- Consider ISA training https://www.isa.org/training-and-certification/

- The Brisbane Section are considering future training delivery options as well!

From ISAGCA Quick Start Guide: An Overview of the ISA/IEC 62443 Standard

Thank you

Q&A