Demystifying Asset Management in Critical Infrastructure

Craig Morris

About Me

- Director – KPMG Australia
- Ex-CISO
- Ex-Asset Owner

Thoughts are my own and do not represent my employer
Any vendor names are copyright and do not represent an endorsement or opinion.

SLIDO

How confident are you in your OT asset management efforts and OT asset visibility?

Do you know where your OT assets are, and in what condition?

- **Very confident** – We have complete visibility across our OT assets
- **Moderately confident** – Pretty good, may have some unknown and unmanaged assets in the environment
- **Not confident** – We don’t have a good understanding at all, we have a lot of work to do/just starting

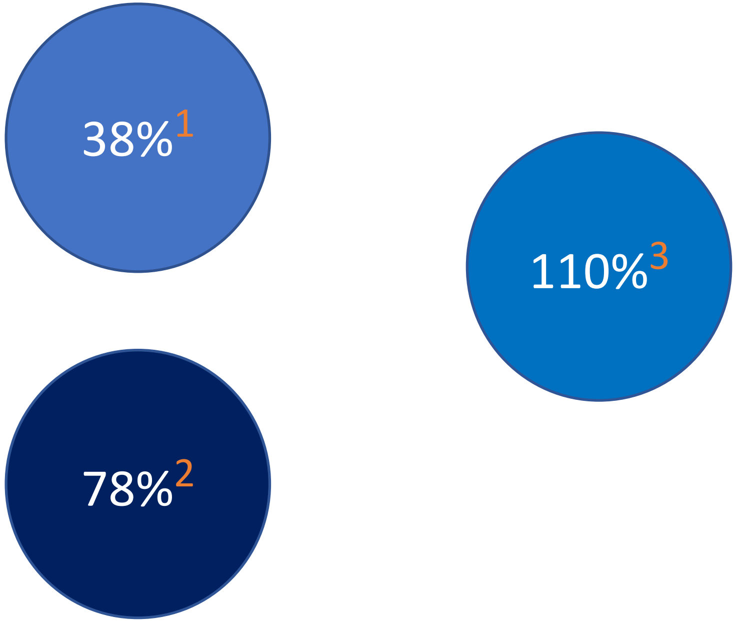
GOALS

- Understand asset management for OT Cyber Assets
- Enterprise Asset Management alignment
- Implementation approach

Drivers for OT Asset Management

What is driving the need for OT Cyber Asset Management?

- Standards and Frameworks
- Regulation (and best practice)



38%[1]

110%[3]

78%[2]

1. [KPMG & CS2AI Control System Cyber Security Annual Report 2022](#)
2. [SANS 2021 Survey: OT/ICS Cybersecurity](#)
3. https://claroty.com/press-releases/ics-vulnerability-disclosures-grew-110-over-last-four-years

Managing Assets v Asset Management

ISO 55000 aligned definition

Asset – Anything that has potential or actual **Value** and for which the organisation has **responsibility**

Managing Assets

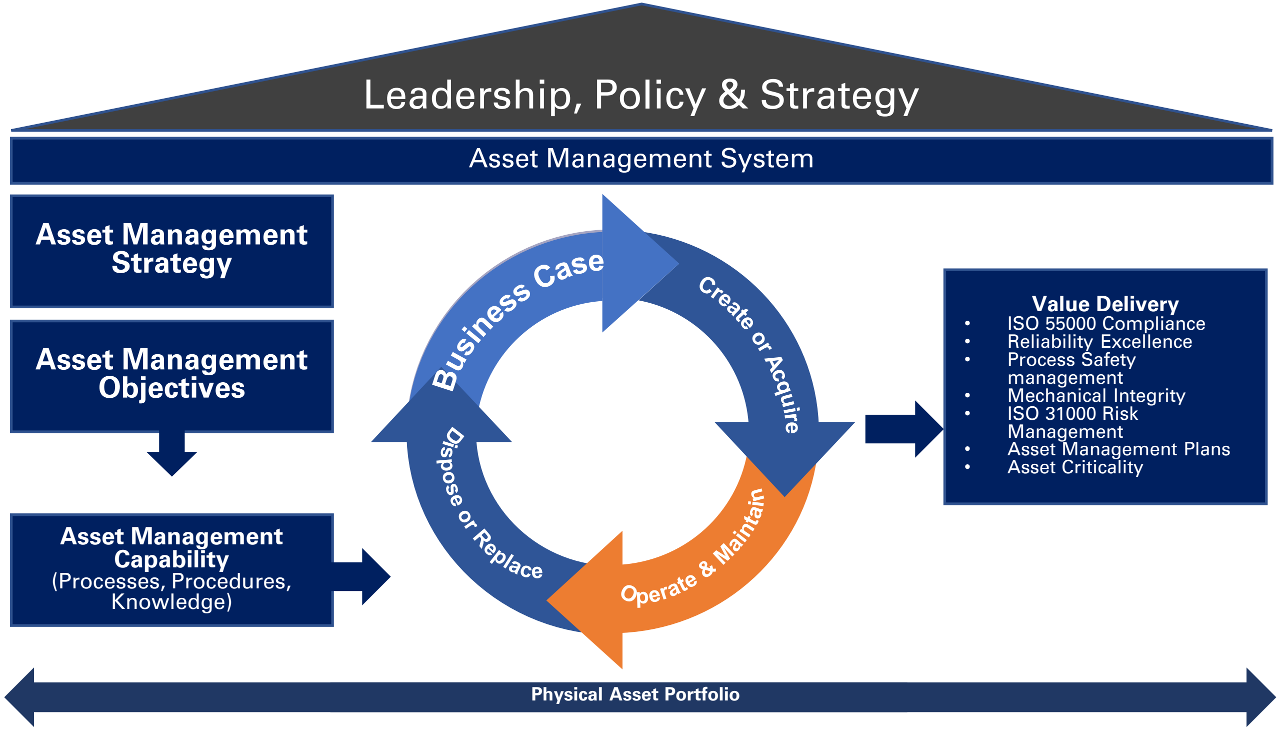
- Things done TO assets
- Tactical
- Maintain & Operate, Protect

Asset Management

- Structured, systematic, co-ordinated
- Strategic, purpose-led
- Maximises the value of assets - Lifecycle

Enterprise Asset Management

ISO 55000 Asset management lifecycle, Benefits



Leadership, Policy & Strategy

Asset Management System

Asset Management Strategy

Asset Management Objectives

Asset Management Capability
(Processes, Procedures, Knowledge)

Value Delivery

- ISO 55000 Compliance
- Reliability Excellence
- Process Safety management
- Mechanical Integrity
- ISO 31000 Risk Management
- Asset Management Plans
- Asset Criticality

Physical Asset Portfolio

1. Optimisation & visibility of assets throughout their lifecycle
2. Better risk management
3. Informed investment & decision making
4. Demonstrated security & regulatory compliance
5. Improved Resilience

Who, in your organisation, is responsible for OT cyber asset management ?

SLIDO

Do you have the structures, processes in place?

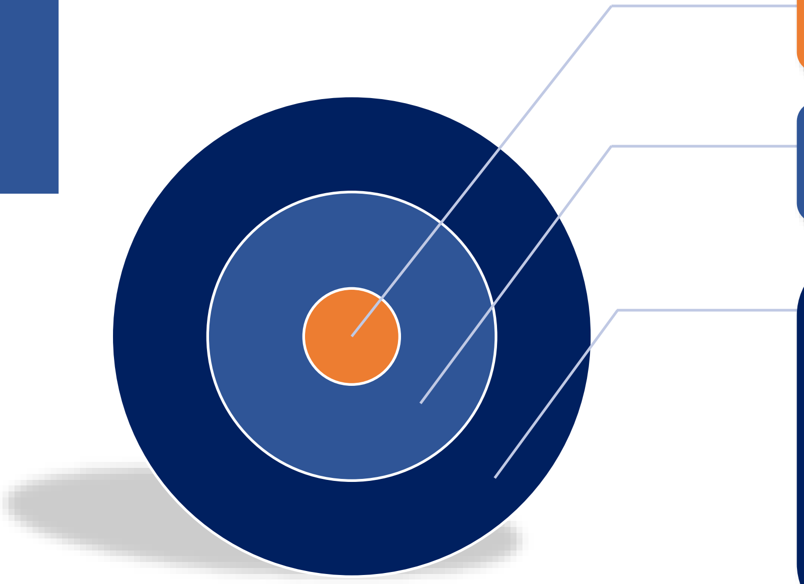
- **IT owned** – CIO, CTO, CISO
- **OT owned** – COO, Engineering Manager
- **Hybrid ownership** – Jointly managed
- **No Idea** – Hint: It might be you…

Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

SOCI Requirements

Drive uplift in security and resilience of Australia's critical infrastructure



Provide **ownership and operational information** to Register of Critical Assets (*8th Oct 2022)*

Mandatory reporting of serious cyber incidents – 12hrs Significant Impact, 72hrs relevant impact. *(8th July 2022)*

Adopt and maintain an **all-hazards** critical infrastructure **risk management program (RMP)** inc annual reporting

- Physical & Natural Hazards
- Cyber & Information
- Personnel
- Supply Chain

(Consultation until 22nd Nov 2022)

All assets are equal, some are more equal than others

George Orwell – mid-20th Century Asset manager (and author)

Asset Types

What gets reported to the DHA Asset Register?

How are you currently performing OT cyber asset detection?

SLIDO

- **Manual** – Excel all the way
- **Semi-Automated** – Scans and scripts
- **Continuous** – 24*7, Automated

Approaches to Asset Management in OT

Manual

- Excel & Visio
- Resource intensive
- No integration
- Point in time
- Site walk downs
- Often neglected ☹

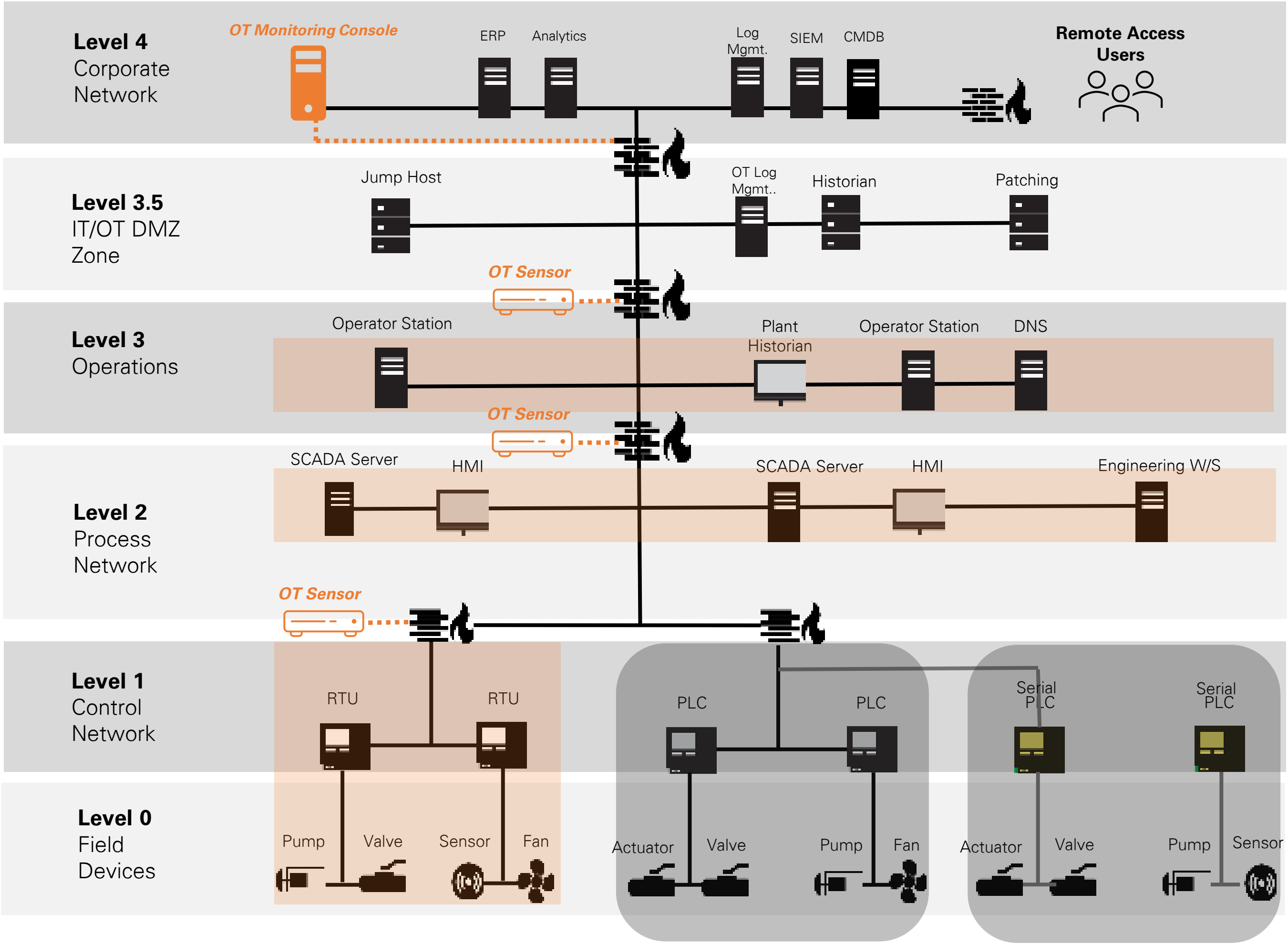
Semi-Automated

- Excel, Visio, Nmap, scripts
- Scheduled
- Some integration
- Misses devices
- Site walk downs

Continuous

- 24*7, Automatic
- On network = Detected
- Multiple Integration options, API’s etc
- Reduced workload for field staff
- + Additional Benefits

Implementing Continuous Asset Monitoring



Benefits

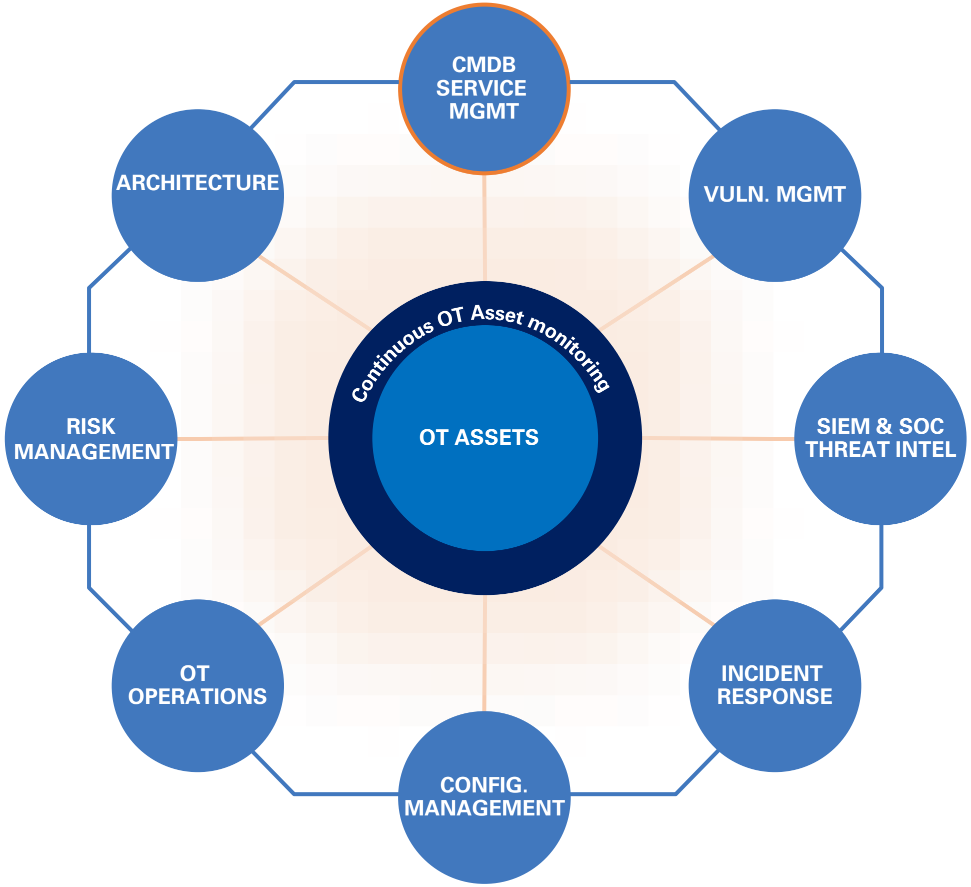
- Asset Visibility (Passive)
- Vulnerability Detection
- Anomaly detection
- Contextual Threat Intel
- Support for I&C and Engineers
- Reduce workload to maintain registers, diagrams etc

Implementation Challenges

- Management of Change
- Asset planning Schedules
- Network Architecture
- Non-IP Devices
- Standalone devices

OT Cyber Asset Management – Model

What can we do with the asset data?



- SOCI Enterprise Asset Management (Lifecycle)
- SOCI Governance & Reporting
- SOCI Business Resilience
- SOCI Crisis Management
- ● Data Visualisation & BI
- ● Workforce Planning & Work orders (ERP)

Implementation Approach

High level approach to implement OT Cyber Asset management in your organisation

Assess & Design

- Assess Network Capability & decide
- Deployment design & schedule
- ISO 55000 alignment (or other EAM)
- Governance framework (inc policies, Roles etc)
- **Management of Change**

Implement

- Deploy monitoring , tune & verify
- Process integration – IR, SOC/SIEM, ERP, Vuln Mgmt. etc
- Governance framework
- Reports & Dashboards

Run & Maintain

- Governance
- Reporting & Compliance
- Improve processes
- **Don't Forget: System upgrade and maintenance!**

Takeaways

1. Adopt/Align **Enterprise Asset Management**
2. **Continuous**, Automated approach
3. Integrate with other processes – **leverage your data!**
4. Address **regulatory requirements**

Thank You