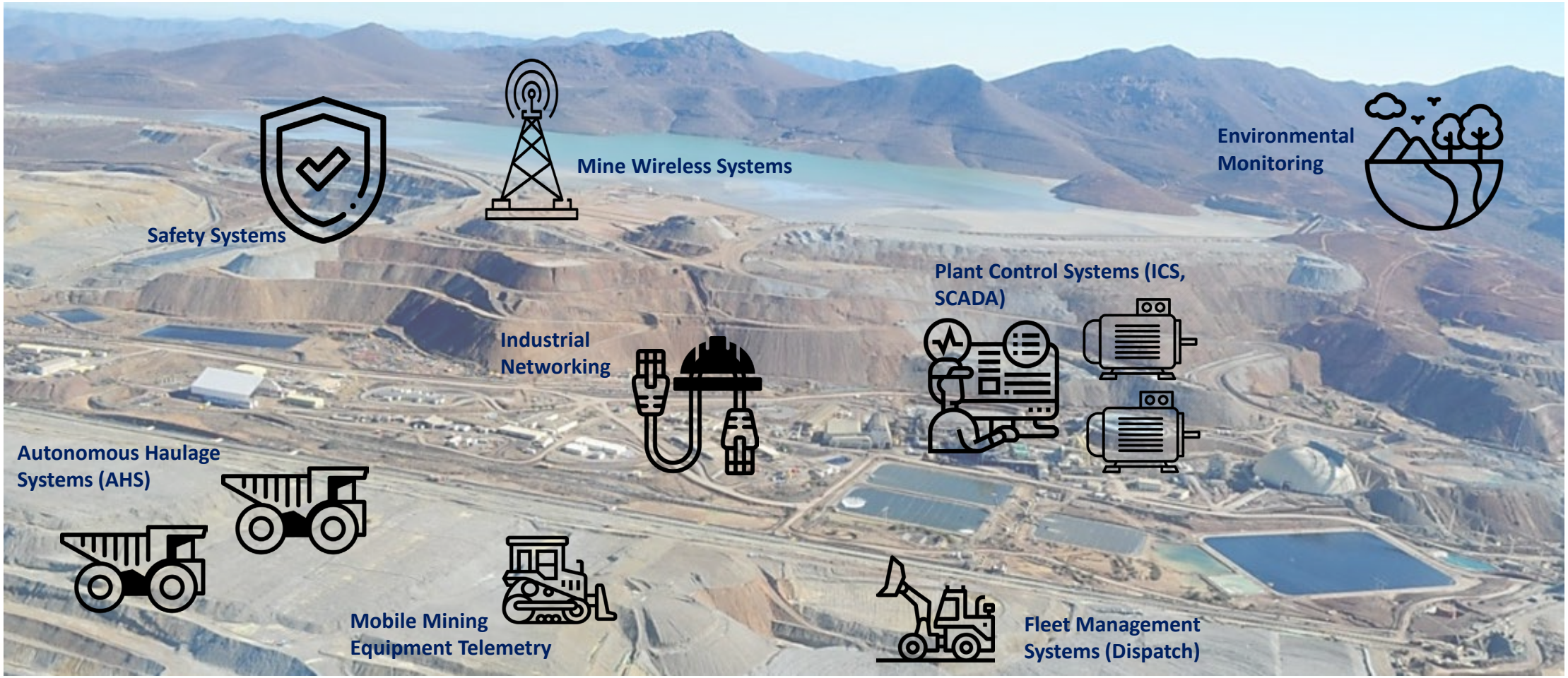
Secure Deployment of Autonomous Haulage Systems

Rob Labbé
Chair, MM-ISAC
Director, Information Security, Teck Resources

Presentation Overview

- ✓ Level setting
  - ✓ What is Operational Technology (OT)?
  - ✓ How is OT Security different?
  - ✓ What is AHS and why security matters?
- ✓ How do we secure AHS?
- ✓ MM-ISAC Working Group and existing AHS standards
- ✓ What are appropriate security controls for AHS?
  - ✓ OT-IT Integration
  - ✓ 3rd Party and OEM Management
  - ✓ Segmentation
  - ✓ Access and Authorization
  - ✓ Wireless
  - ✓ Vulnerability Management and Endpoint Protection
- ✓ Securing the mine of the future
- ✓ Wrap-up and questions

What is Operational Technology (OT)?



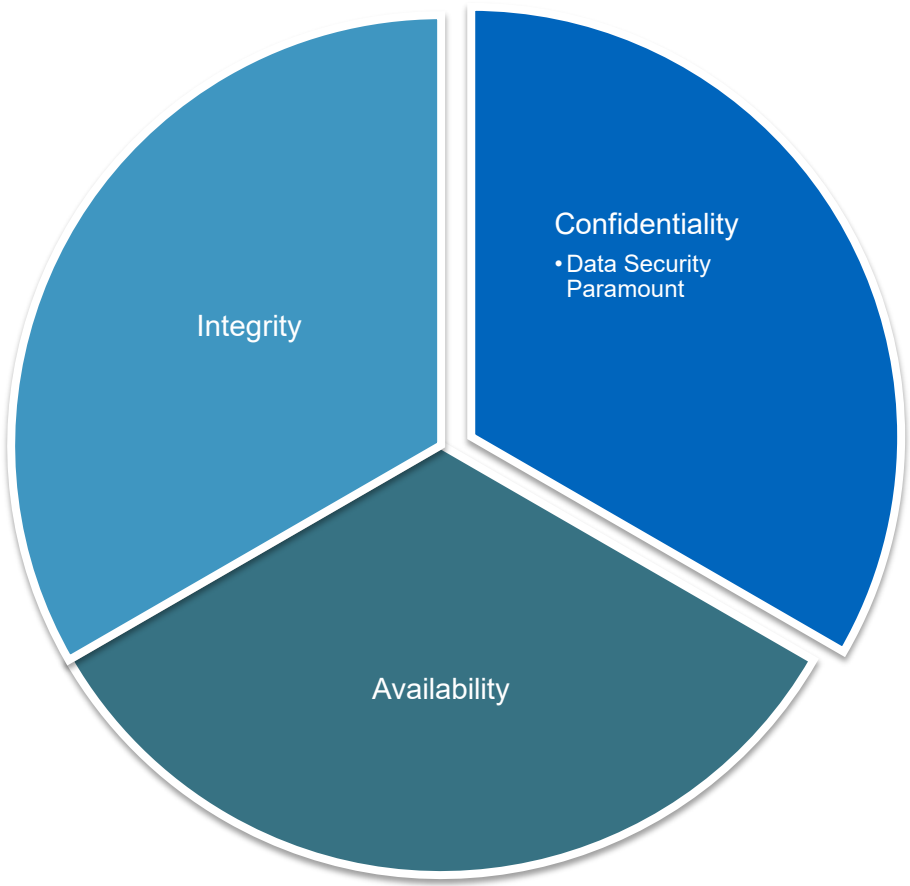
"**Operational technology** is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events." - Gartner

How is OT Security Different?

CIA vs. SAIC

IT

Security is about protecting data



OT

Security is about protecting operational assets and supporting safe production

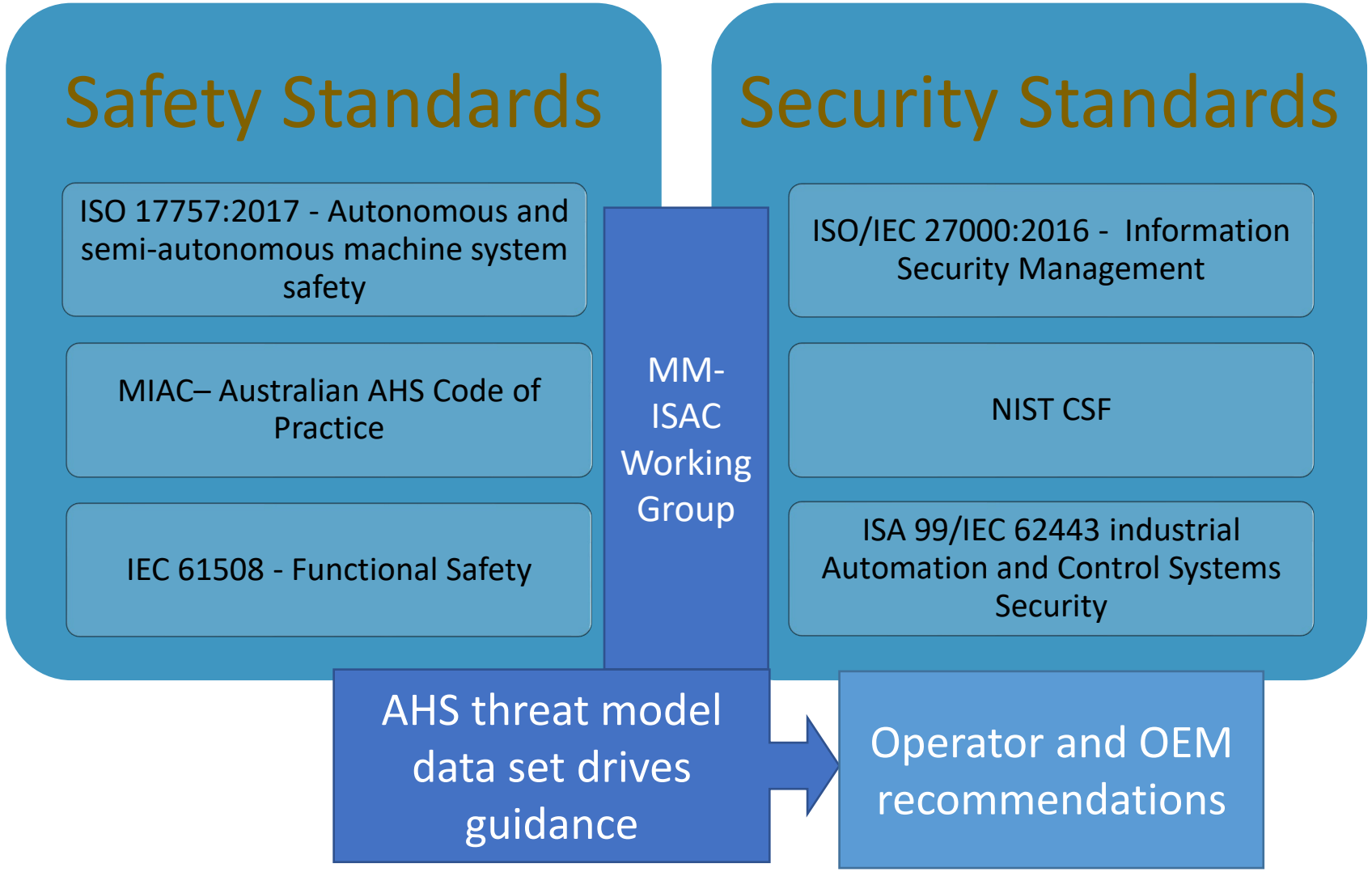
What is AHS and why securing it matters?

- AHS or Autonomous Haulage Systems are conventional haul trucks outfitted with OEM provided Operational Technology that allows for safe unmanned operation
- Security needs to be designed into the implementation of AHS
  - Due to a changing and evolving threat landscape that now targets OT assets
  - Heightened risk profile of AHS vs. traditional manned vehicle operation
  - Total reliance on wireless technologies for safe production and operational control
  - Existing AHS relevant standards focus on safety, but cybersecurity is only barely considered

MM-ISAC Working Group and existing AHS standards

The MM-ISAC AHS working group has been working to:

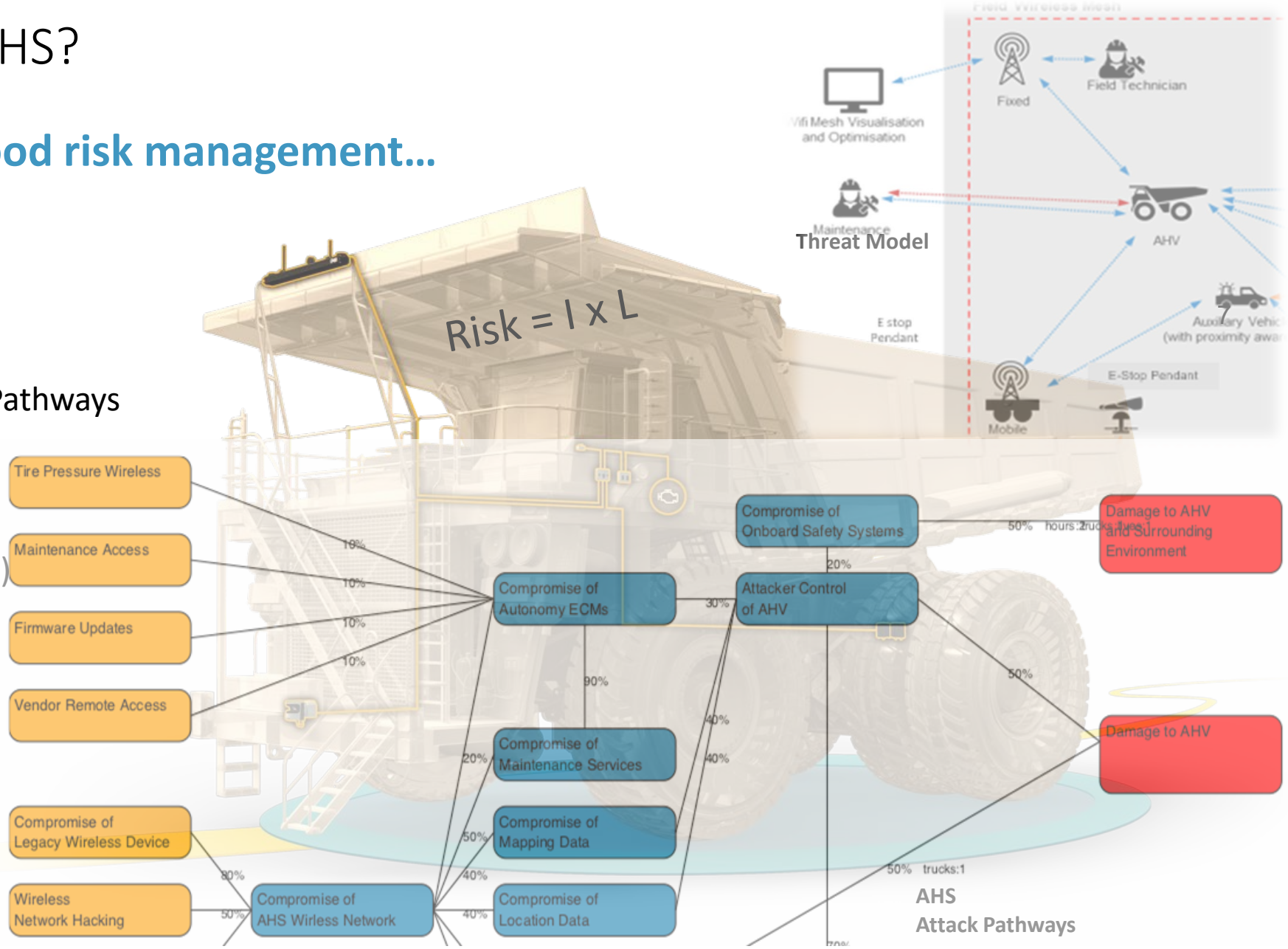
- Employ system level threat modelling and risk analysis
- Derive security guidance from threat modelling data set
- Create actionable security recommendations for both operators and OEM's
- Align existing safety focused AHS standards to cybersecurity standards



How do we secure AHS?

It all comes down to good risk management…

1. Establishing Impact
   - OT Dependencies
   - Loss
2. Vulnerabilities
   - Exposure and Attack Pathways
3. Threats
   - Threat Modeling
4. Assessing Risk
   - Likelihood (Frequency)
5. Risk Treatment
   - Accept or Mitigate
   - Applying Controls



What are appropriate controls for AHS?

- Threats, risks, and risk appetite vary for each organization and mine site
- Each AHS site and system should have a unique security deployment design
- The MM-ISAC working group has created risk assessment process for members complete with controls and mitigations guidance to help with design process
- In the upcoming slides we will review some of these controls at a high level

AHS Controls – OT-IT integration

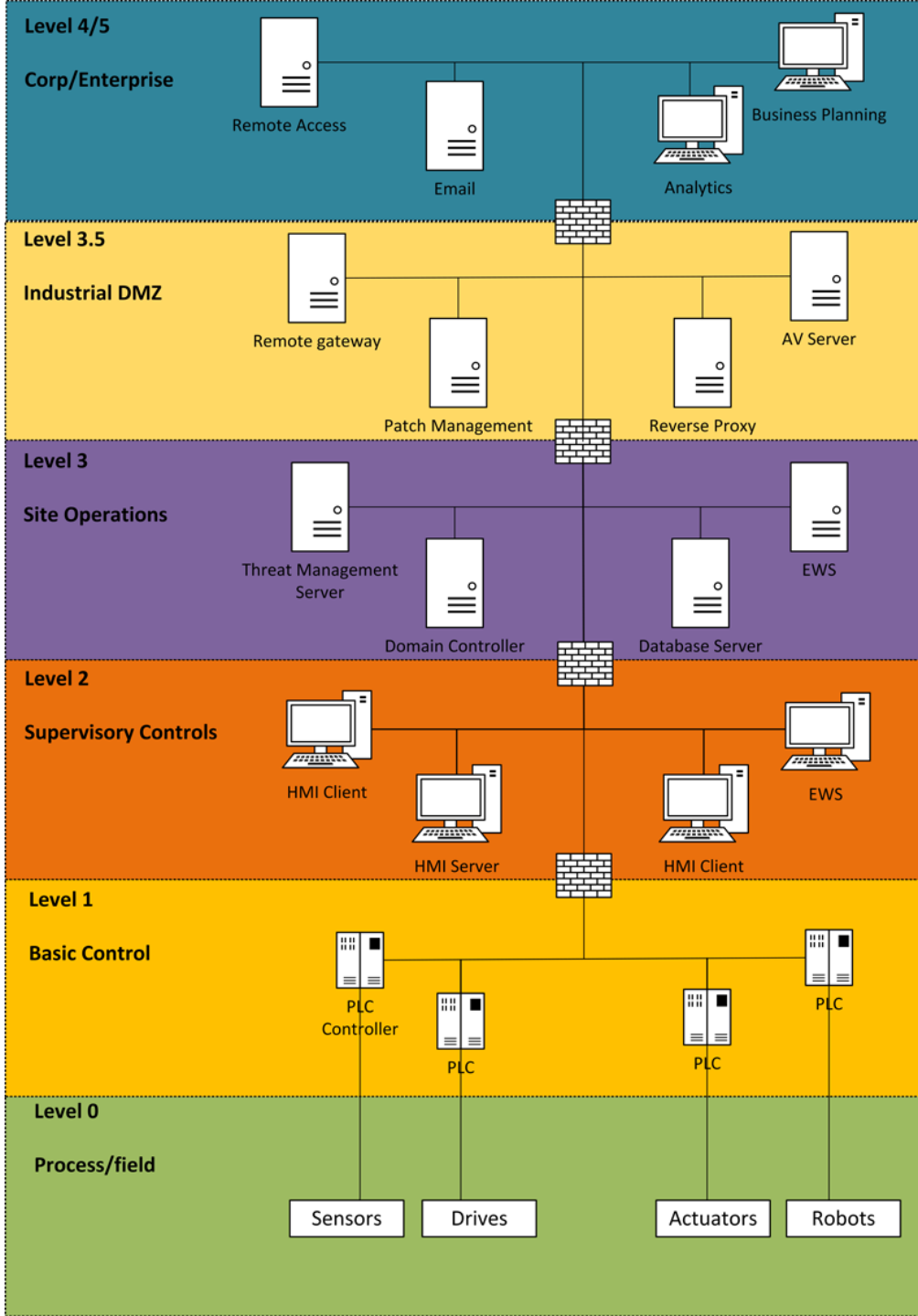
- When done well OT-IT Integration can help ensure secure AHS deployments
- Many components of an OT environment use traditional IT commodity technologies (AD, backups, remote access, AAA etc.)
- Trained security incident response teams can reduce potential losses from security incidents
- Possible opportunity to introduce enterprise governance processes

AHS Controls – 3rd Party/OEM

- Engaging with potential OEMs before the first contract is signed or pilot is conducted is critical for the success of securing an AHS deployment
- Large count of OEM maintenance personnel remote access requirements
- MM-ISAC Supply Chain Resilience program

AHS Controls - Segmentation

- OT assets are considered insecure by design due to the use of communications that are in clear text
- AHS is no different utilizing command-and-control protocols to direct autonomous vehicle routing that use neither encryption nor authentication
- Segmentation reduces exposure of OT assets from external untrusted networks
- Industrial segmentation standards like the IEC 62443 zones and conduits model or the Purdue reference model are suitable for AHS



AHS Controls – Access and authorization

- Secure Remote Access with MFA required
- Dedicated Active Directory domain for OT to limit credential theft and privilege escalation attacks from business systems
- Enable accounting controls such as log forwarding on all capable devices
- Modern identity features on next gen firewalls can help limit access to least privilege levels

AHS Controls - Wireless

- AHS requires the use of traditional wifi technologies or private LTE systems to operate
- OEM's such as CAT and Komatsu have not certified the use of WPA2 Enterprise so static keys must be managed appropriately
- Wireless attack surface increases exposure to segmented networks
- High Precision GPS with cm precision required. GPS jamming attacks possible
- Monitor wireless devices and communications and forward logs

- MM-ISAC working group looking to add private LTE to attack pathways and threat model soon

AHS Controls – Vulnerability Management and Endpoint Protection

- Asset Management
- Patch management strategy
- Vulnerability Identification
- Endpoint Protection Support
- Routine Security Assessments

Securing the mine of the future

- A new vision for mining
- Unmanned mining vehicles remove personnel safety risks
- Mining operations move from fleet management to a factory optimization mind set
- Autonomous trucks, drills and blasting trucks
- Tele-remote on shovels and support equipment

Wrap-up and Questions

- Questions???