Basics of IACS Cybersecurity for IT Professionals

Overview

General Concepts

Purdue Model

IEC 62443

Building a Security Program

- Risk Assessment
- Segmentation

What is IACS?

IACS – Industrial Automation and Control Systems

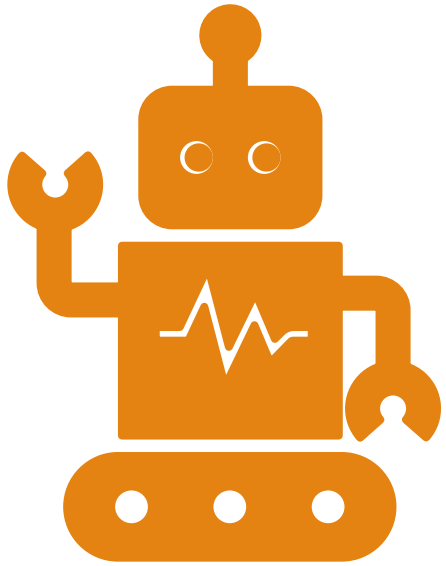
OT – Operational Technology

OT focuses on devices that control physical processes – actuators, sensors, etc.

Everything in OT is about safety

OT has a mature risk management process

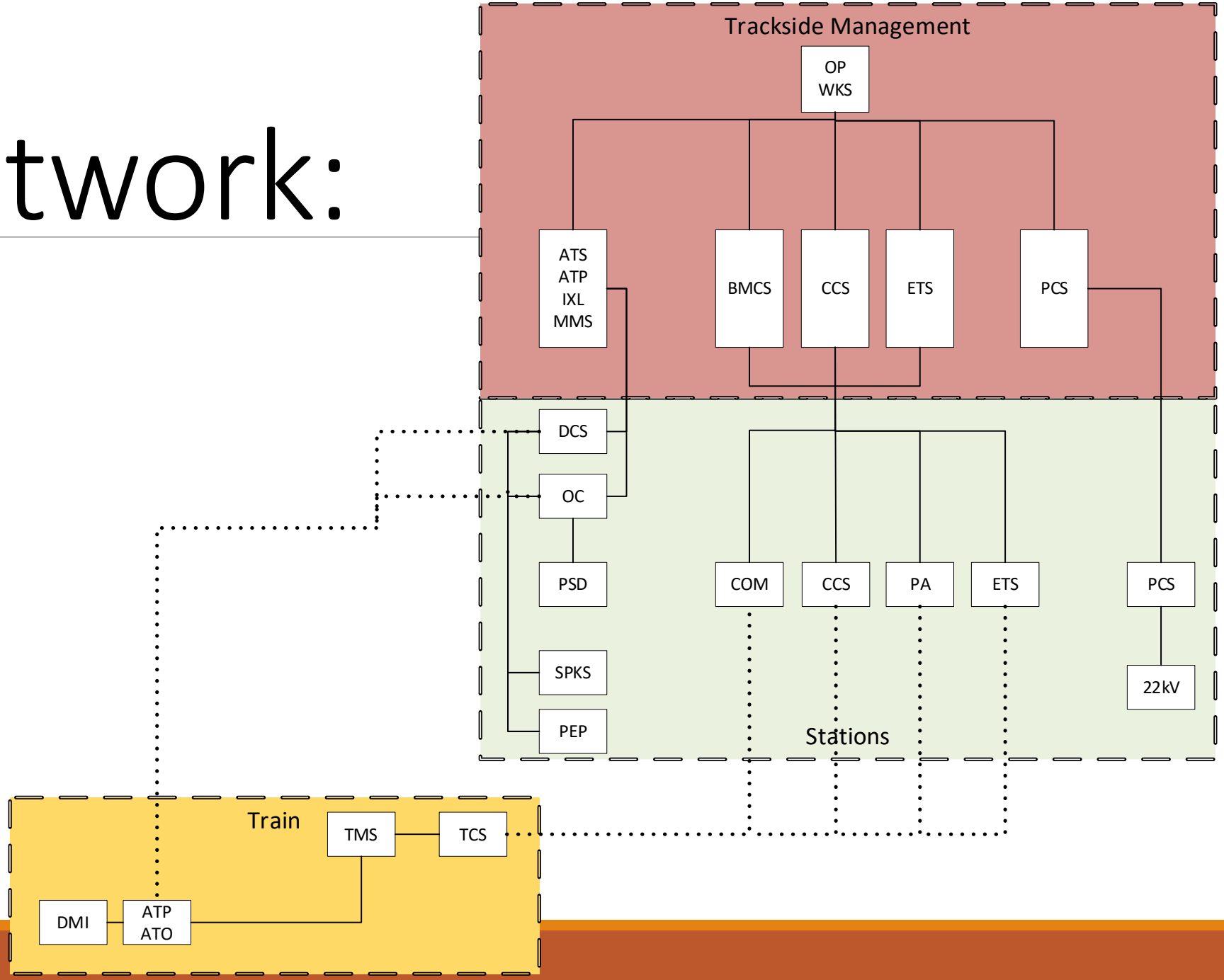
Security = Safety



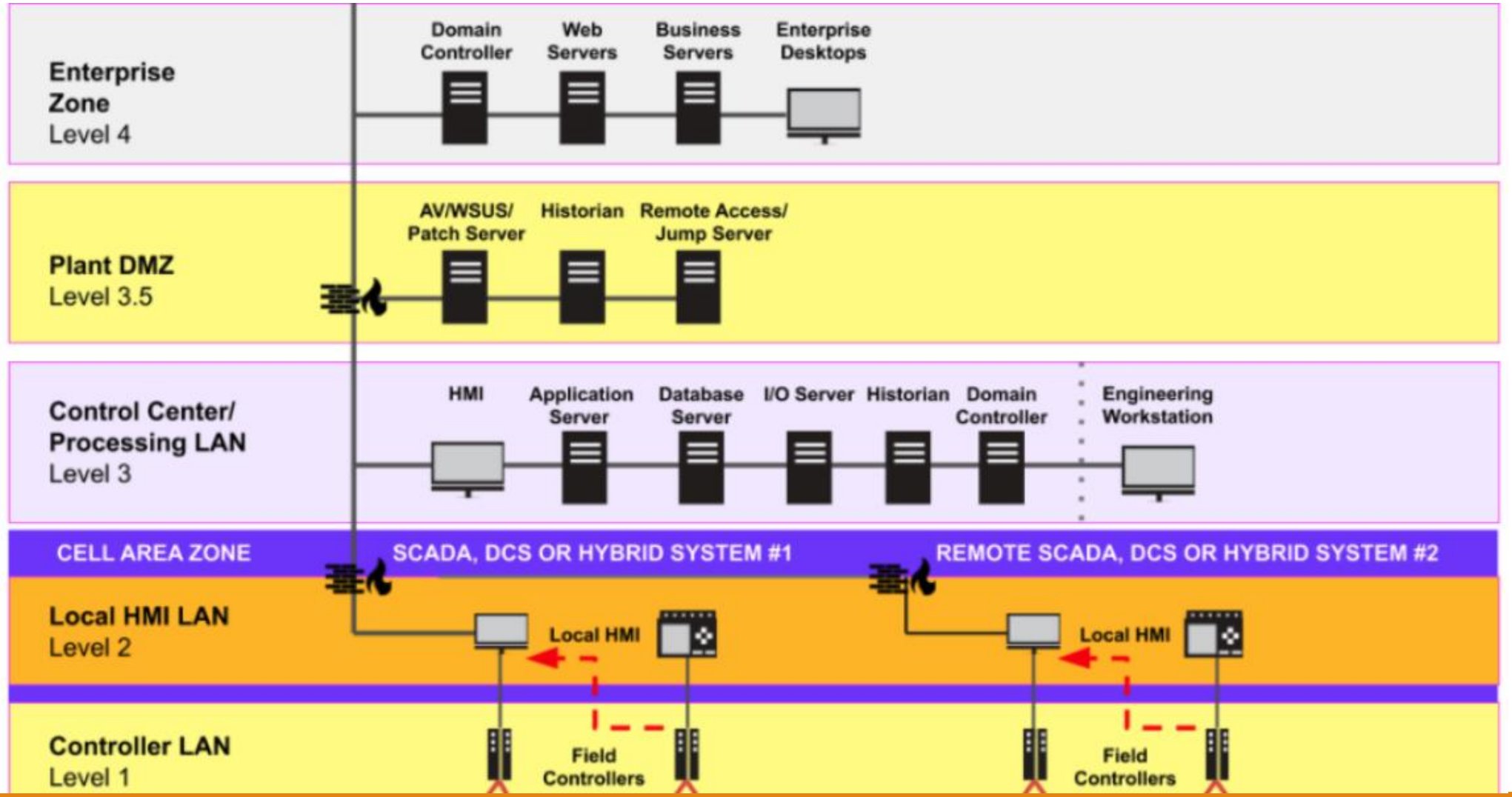

Cybersecurity = Safety

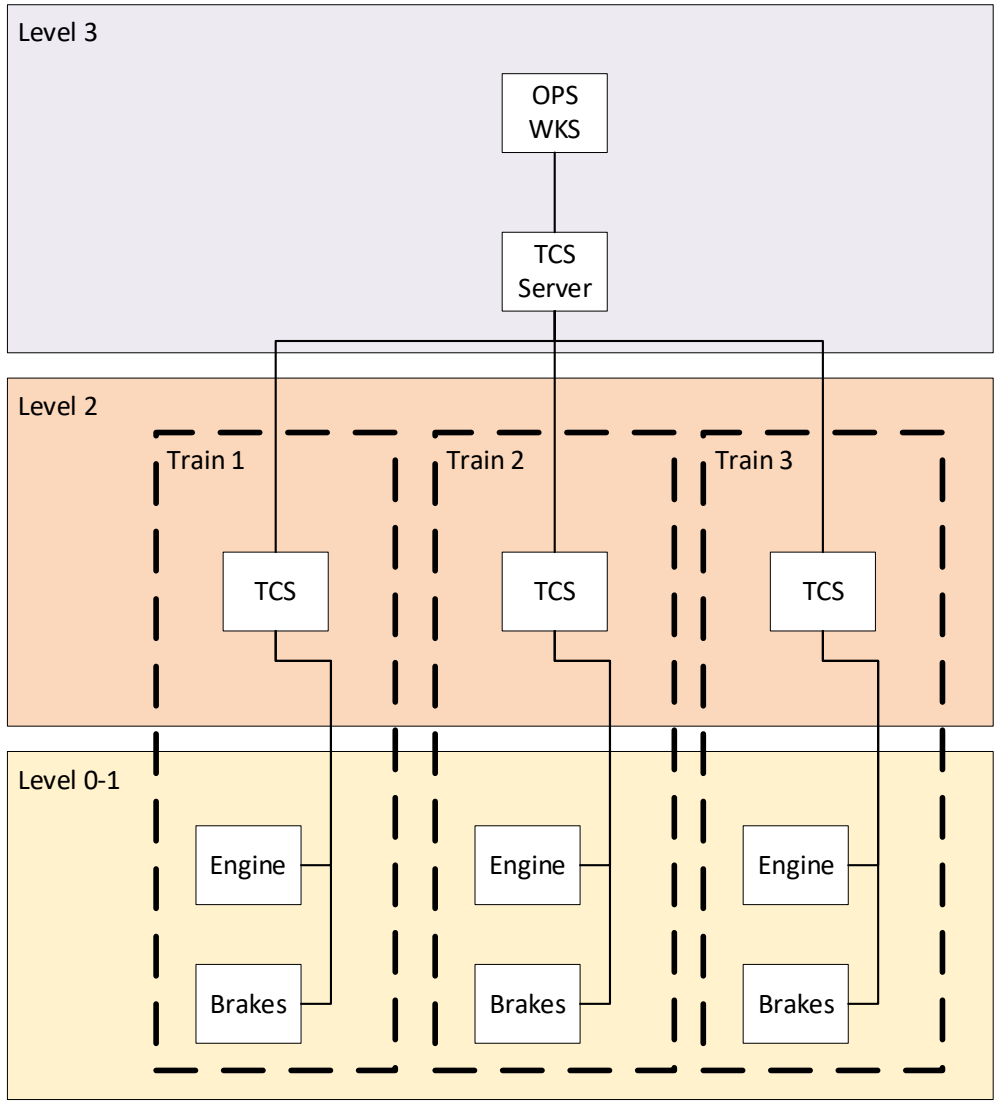
IACS

IACS Network: Trains!



Purdue Model





Purdue Model

Level 0: Interact with the real world

Level 1: Sense something, or manipulate the physical process

Level 2: Supervises, monitors, controls the physical process.

Level 3: Manages entire workflow.

Learn the Purdue Model

IEC 62443

Standard Series for IACS cybersecurity

Guidelines, Best Practices, Controls, Requirements

Four sections:

- General topics (glossary, etc)
- Policies and Procedures
- System
- Components and Requirements

Building a Security Program

Detailed in IEC 62443-3-2

Cybersecurity is a matter of risk management

Not all IACS can have security controls implemented

Break down the risk into chunks and controls that matter

Security Levels

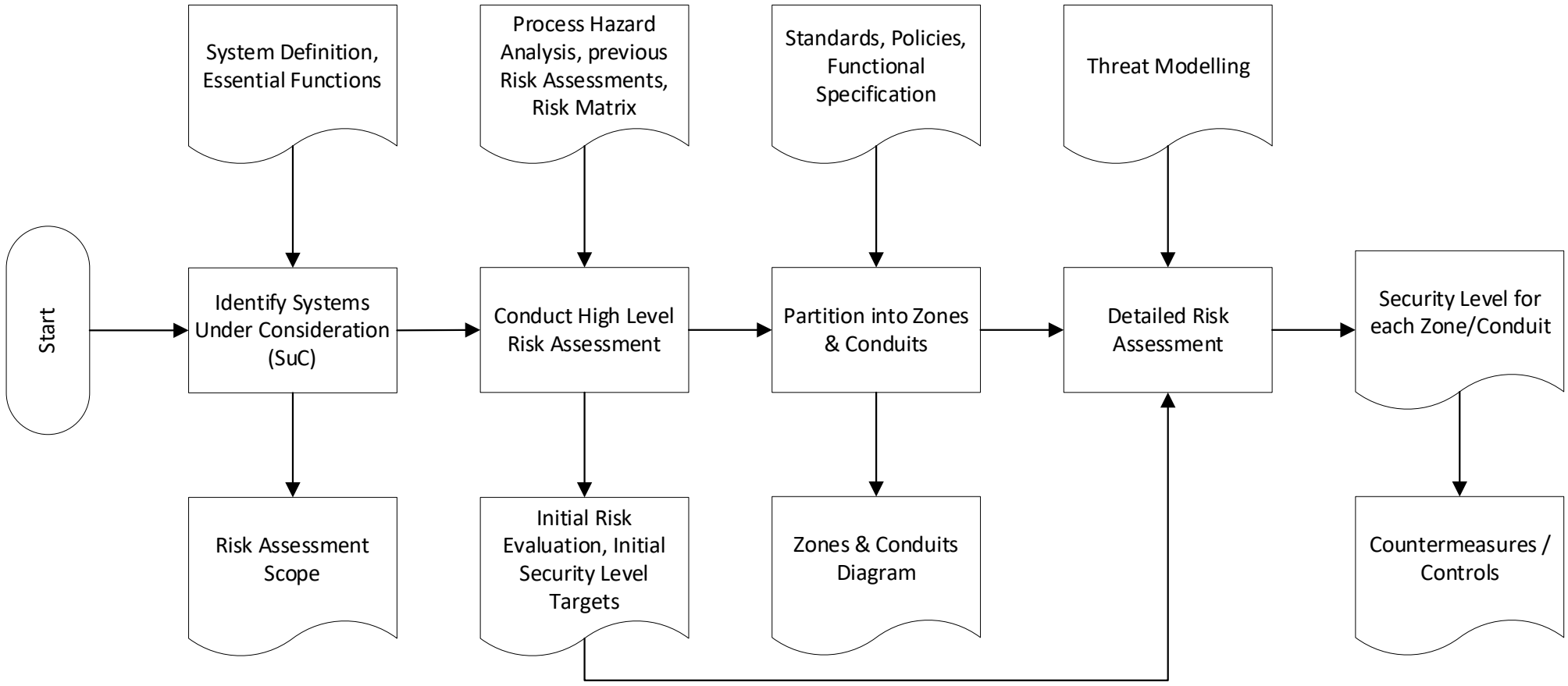
SL 0: No special requirement or protection required.

SL 1: Protection against unintentional or accidental misuse

SL 2: Protection against intentional misuse by simple means with few resources, general skills, and low motivation

SL 3: Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation.

SL 4: Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation.



Basic Process

Identify Systems Under Consideration

Refers to any constituent part of the overall environment

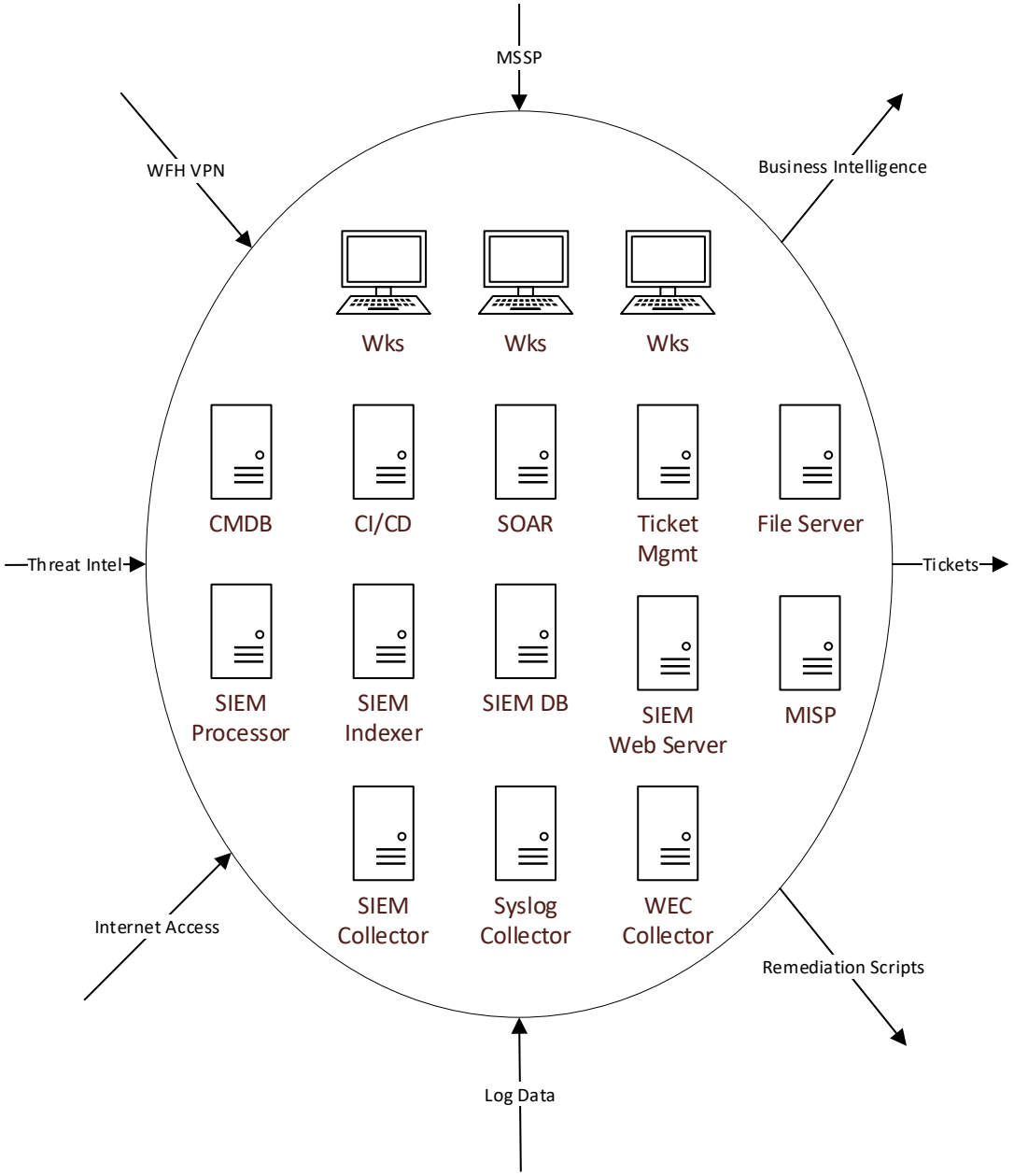
“System of nested systems, each comprising subsystems and components, which together provide the required functionality”

Defines scope and boundary of the assessment

Defines functionality

Defines general access

Essential functions needed for operation of environment



SuC Example

Cybersecurity systems located in PDC1

Manages security alerting for enterprise systems

Remote and Local User access

Data ingestion and egress

Not directly critical to business functionality

Data analytics essential to SuC

High Level Risk Assessment

Understand Criticality of System

Identify likely risks – focus on end consequence

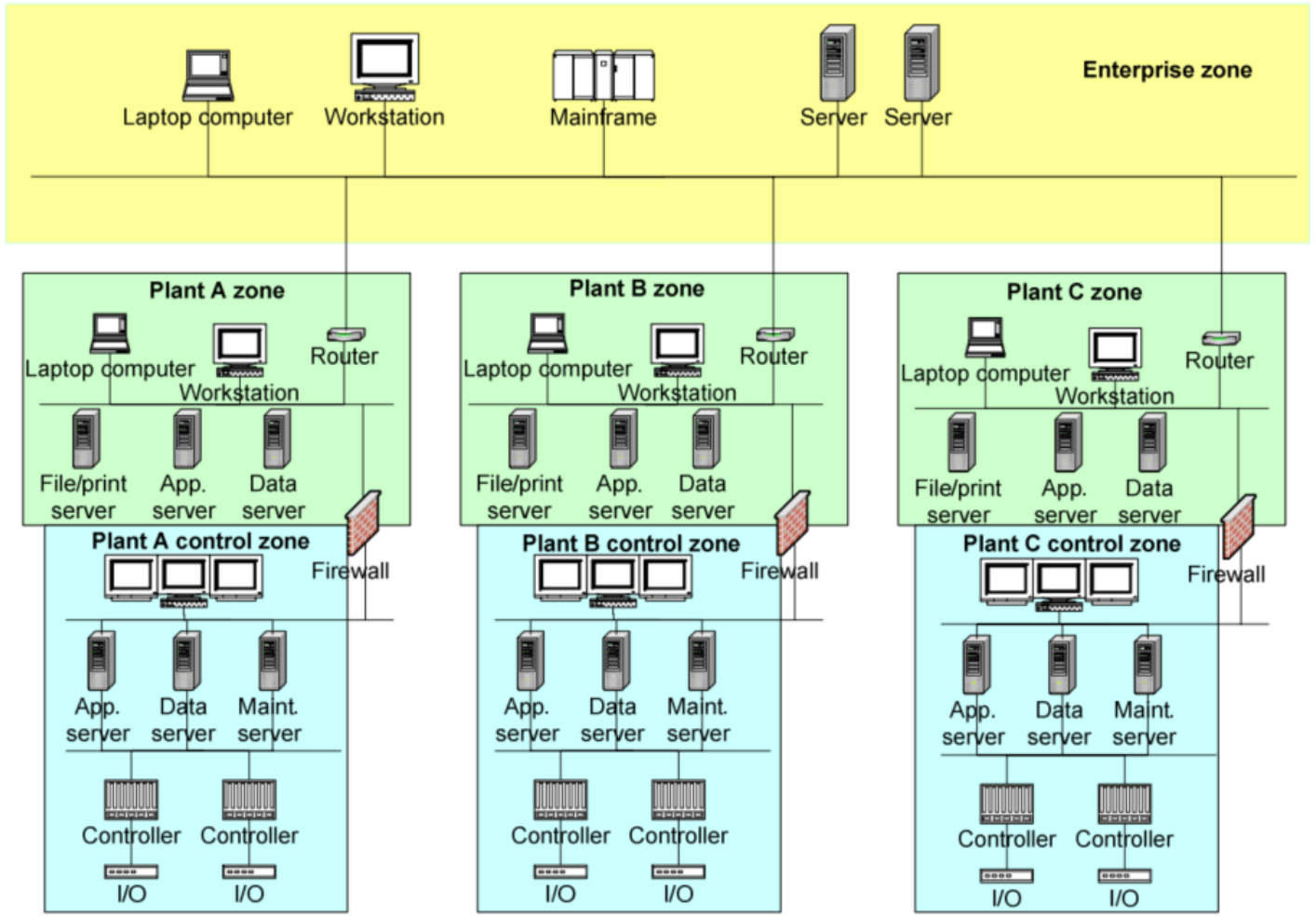
Look at the CIA triangle for each system

Impact of something going wrong

Conduct assessment assuming it *will* happen

Determining Impact – Risk Matrix

	Minor	Moderate	Major	Severe
Health and Safety	Minor Injuries not requiring treatment	Recoverable Lost Time Incident	< 10 major injuries requiring hospitalisation	Fatality or permanent disability
Reputation	Negative article in local media	Extended negative coverage in local media. Trust able to be regained within existing budget	Extended negative coverage in national media. Trust recoverable at considerable cost	Confidence and trust in organisation are severely damaged, possibly irreparably
Environment	Highly localised event	Well contained event, minor remedial actions	Impacts external ecosystems. Considerable remediation	Irreversible large-scale impact with loss of ecosystems.
Regulatory	Low level non-compliance.	Moderate non-compliance. Small Fine	Major Breach resulting in fines, litigation.	Prosecution leading to imprisonment of personnel.
OPEX	< $100k	$100k - $1m	$1m - $10m	>$10m



Zones & Conduits Partition

Not network segmentation

Zones represent common grouping of assets

Conduits represent the transmission of data intra- and inter- zone.

You can have sub-zones but you cannot have sub-conduits

Zones & Conduits Partition

Need to Know:

Risk of Assets

Internal and External Interfaces

Physical and Logical Location

Access Requirements

Operational Function

Organisational Responsibility

Need to Do:

Separate Business & Control Systems

Separate Safety Systems

Separate Mobile Systems

Separate Wireless Systems

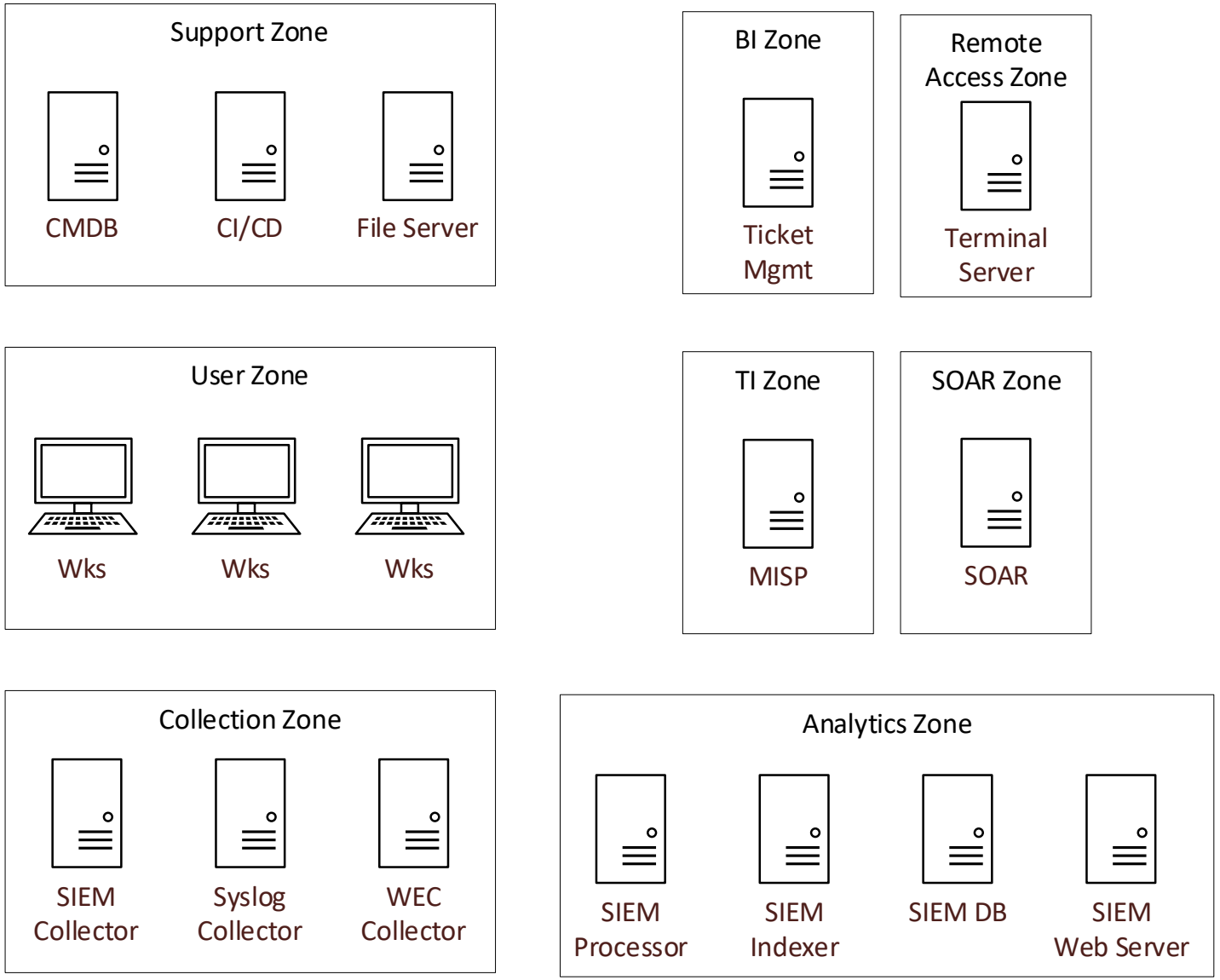
Separate Devices with External Connections

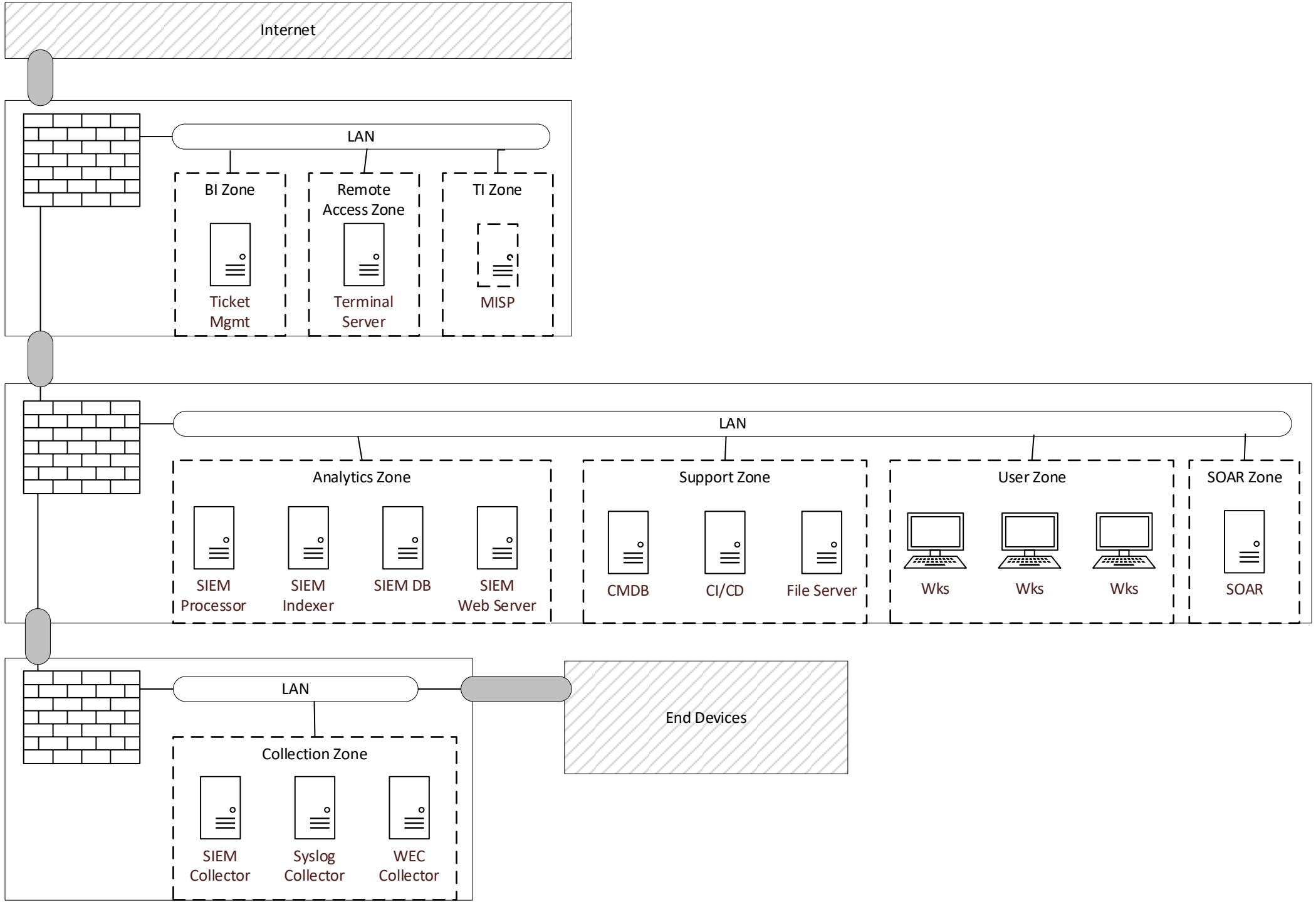
Zones Example

Our SuC has a lot of external interfaces

- Business Intel
- MSSP / VPN
- Threat Intel
- SOAR
- Log Data

MSSP shouldn't interact with the Control Systems (SIEM) directly




Internet
LAN
BI Zone
Ticket Mgmt
Remote Access Zone
Terminal Server
TI Zone
MISP
LAN
Analytics Zone
SIEM Processor
SIEM Indexer
SIEM DB
SIEM Web Server
Support Zone
CMDB
CI/CD
File Server
User Zone
Wks
Wks
Wks
SOAR Zone
SOAR
LAN
Collection Zone
SIEM Collector
Syslog Collector
WEC Collector
End Devices

Threat Assessment

Compare the Assessed Criticality of systems to the Zones & Conduits

Consider Threat Actors (Internal, External)

Consider Likelihood

Review Threat Intelligence

Review known or possible vulnerabilities

Value	C	A	R	V	E	R
5	Loss would be mission stopper	Easily accessible. No effective security	Extremely difficult to replace. Long down time	A dedicated adversary has the capability and expertise to attack	Very high sociological, economical, political impact; considerable loss of lives and/or injured	Easily recognized by all with no confusion
4	Loss would reduce mission performance considerably	Accessible	Difficult to replace with long down time	A dedicated adversary most likely has the capability and expertise to attack	High impact; some loss of lives or injuries	Easily recognized by most
3	Loss would reduce mission performance	Somewhat accessible	Can be replaced in a relatively short time	A dedicated adversary may have the capability and expertise to attack	Moderate impact; some adverse impact on persons	Recognized with some training
2	Loss may reduce mission performance	Difficult to gain access	Easily replaced in a short time	A dedicated adversary most likely does not have the capability and expertise to attack	Little impact; no adverse impact on persons	Hard to recognize. Confusion probable
1	Loss would not affect mission performance	Very difficult to gain access	Immediate replacement. Spare parts are readily available or asset redundancy	A dedicated adversary does not have the capability and expertise to attack	No unfavorable impact	Extremely difficult to recognize without assistance

CARVER Matrix

Establish Countermeasures

Questions?