Importance of ICS knowledge from an engineer's perspective

Defcon 2024 | ICS Village | Ray Baeza

Overview

- Introduction
- Cyber vs asset owners
- AOR’s
- Hidden asset knowledge
- Questions to ask Engineers
- Close the circle

Introduction

- Ray Baeza, Founder, Agriculture Defense Group
- From Davis, CA – Yolo County
- Background – Power grid ICS / OT Cyber security and farming

CSOC vs. SCADA Engineer mindset

CSOC:
Primary Focus: Protecting the SCADA system from cyber threats.

Challenges: May lack deep understanding of the physical processes controlled by SCADA systems

Asset Owners:
Primary Focus: Ensuring the continuous and efficient operation of SCADA systems, which control critical infrastructure processes like water treatment, power distribution, and manufacturing.

Challenges: Often prioritize uptime and operational efficiency, which can sometimes conflict with stringent cybersecurity measures.

The GAP
Potential Conflicts: Cybersecurity measures that are too rigid or not aligned with operational realities can lead to conflicts with engineers who prioritize system availability and efficiency. ***Focused too much on the cybersecurity side.***

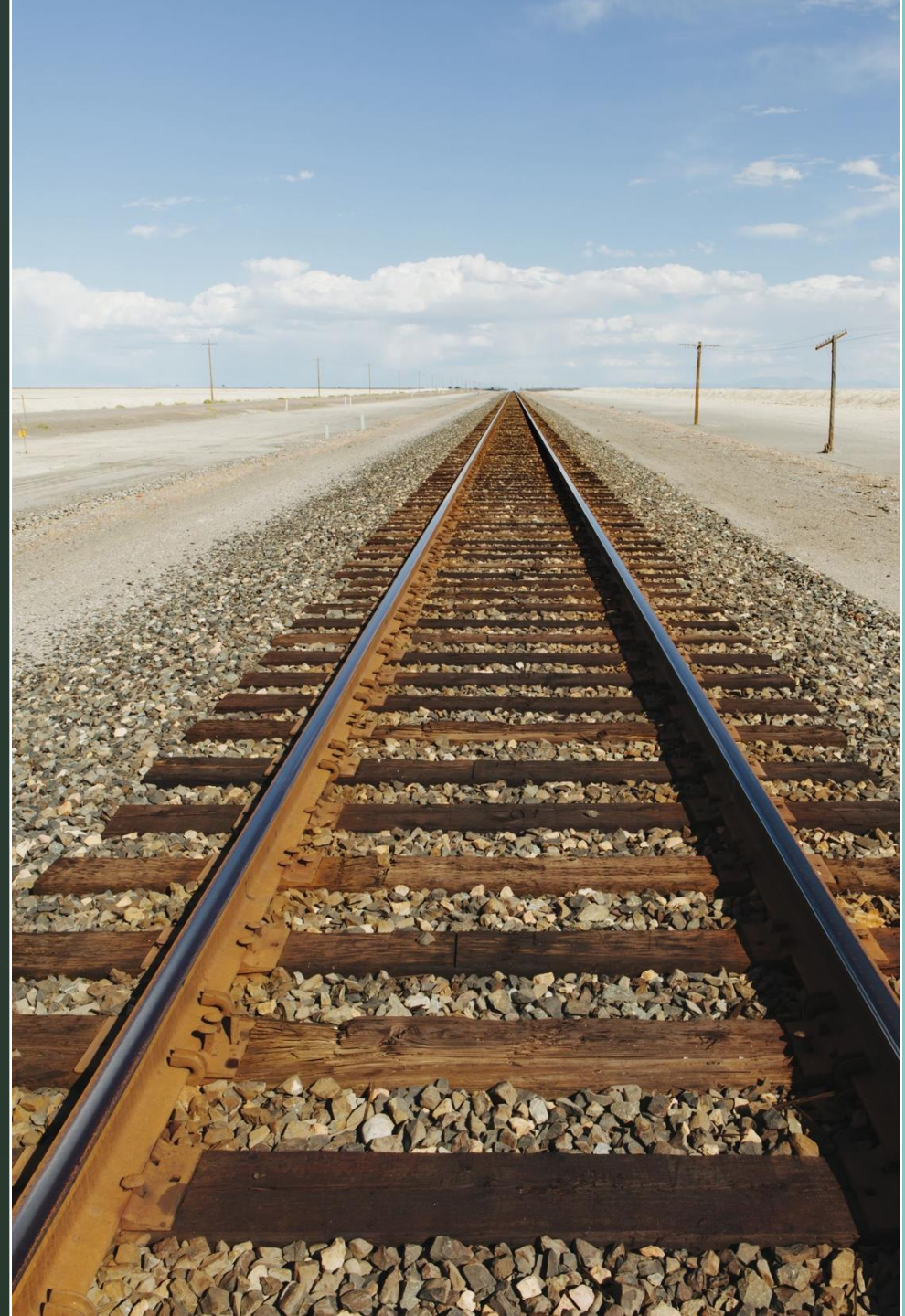
Area of responsibilities

Cybersecurity Responsibilities:
- Security Implementation
- Monitoring and Response
- Compliance
- Risk Assessment

SCADA Engineer Responsibilities:
- System Operation: Ensuring the SCADA system operates efficiently
- System Maintenance
- Troubleshooting
- System optimization

Intersection of Responsibilities:
- **Operational Security:** Both teams share responsibility for ensuring the security and reliability of the SCADA system, but they approach it from different angles.

- **Effective Collaboration:** Effective collaboration requires understanding and respecting each other's roles, working together to find solutions that meet both security and operational needs.



Hidden knowledge

Unique System Insights:
- Configuration Nuances
- Operational Practices
- Operational Context
- System Behavior
- Impact of Security Measures

Historical Data:
- Incident History
- Anomalies and Patterns
- System Weak Points
- Legacy Systems
- Custom Integrations
- Operational Workarounds

Questions to Ask

System Architecture:
Question: ”Can you provide a detailed walkthrough of the system architecture and how critical components like PLCs, RTUs, and HMIs are interconnected?”

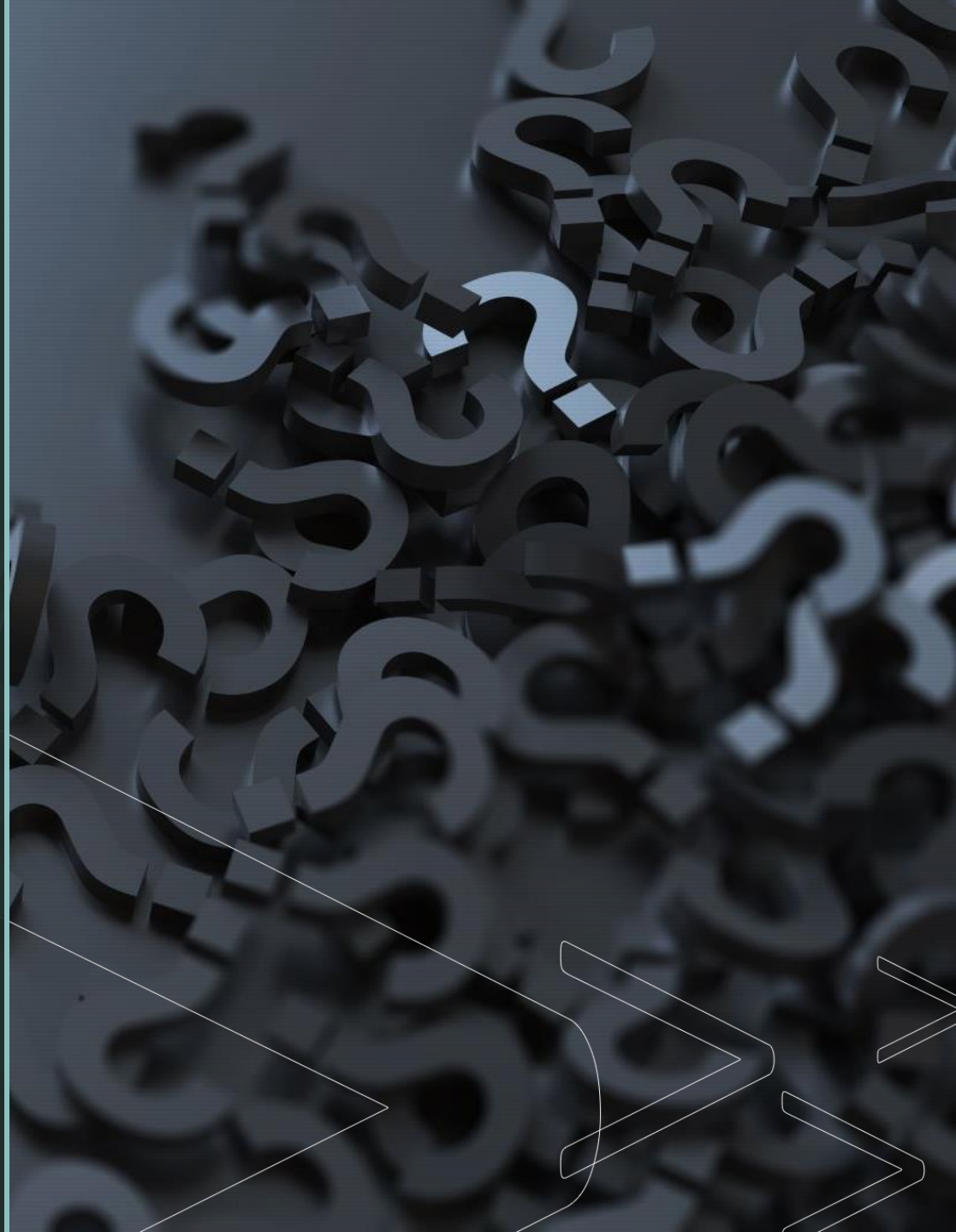
Packet flow:
Question: “Can you walk me down the packet flow through each level of the Purdue model?”

Operational Workflow:
Question: “What are the typical operational workflows, and where do you see potential vulnerabilities?”

Asset Inventory:
Question: “What is the make and model of each device used in this environment?”

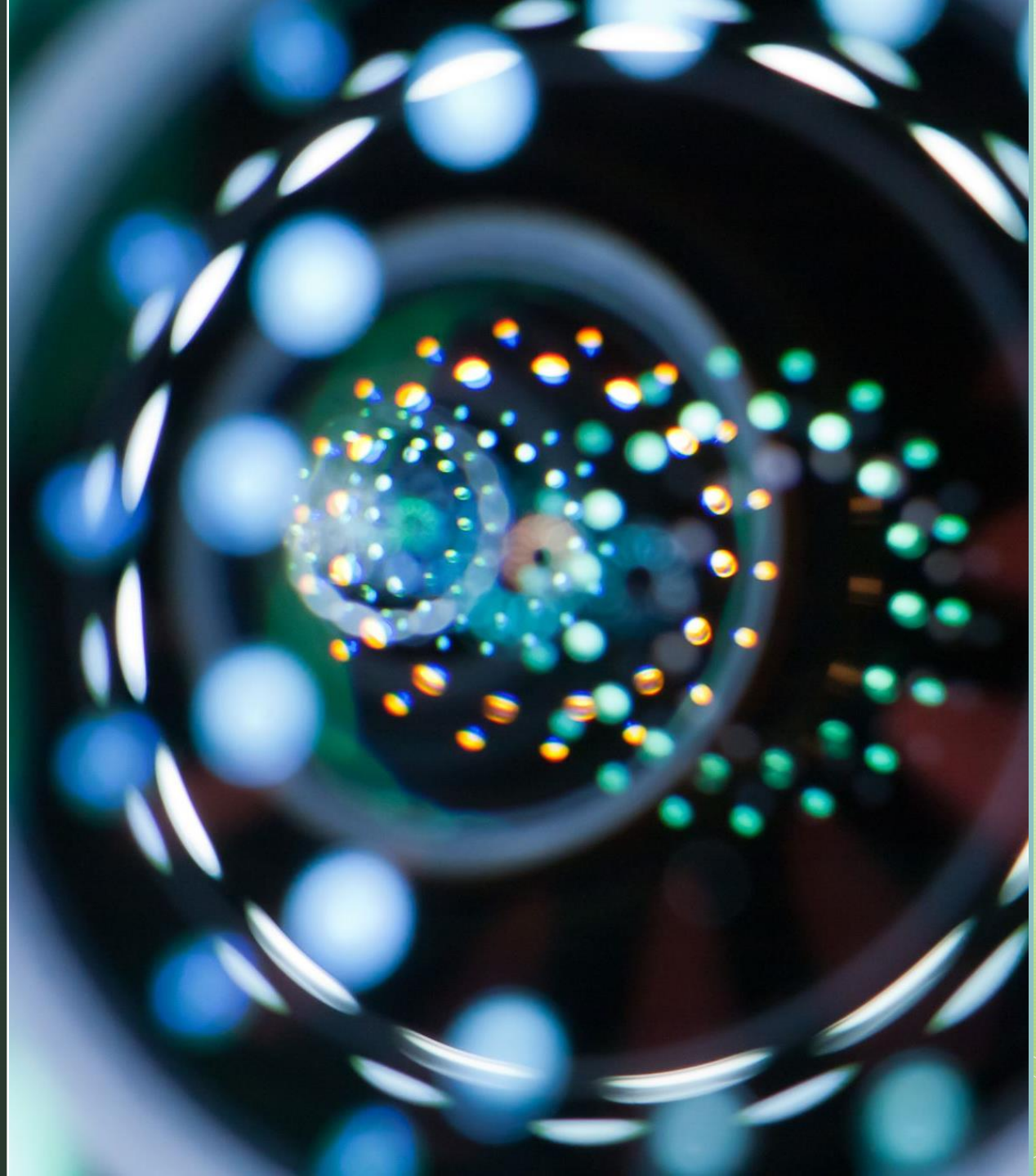
Custom Configurations:
Question: “Are there any custom configurations I should be aware of?”

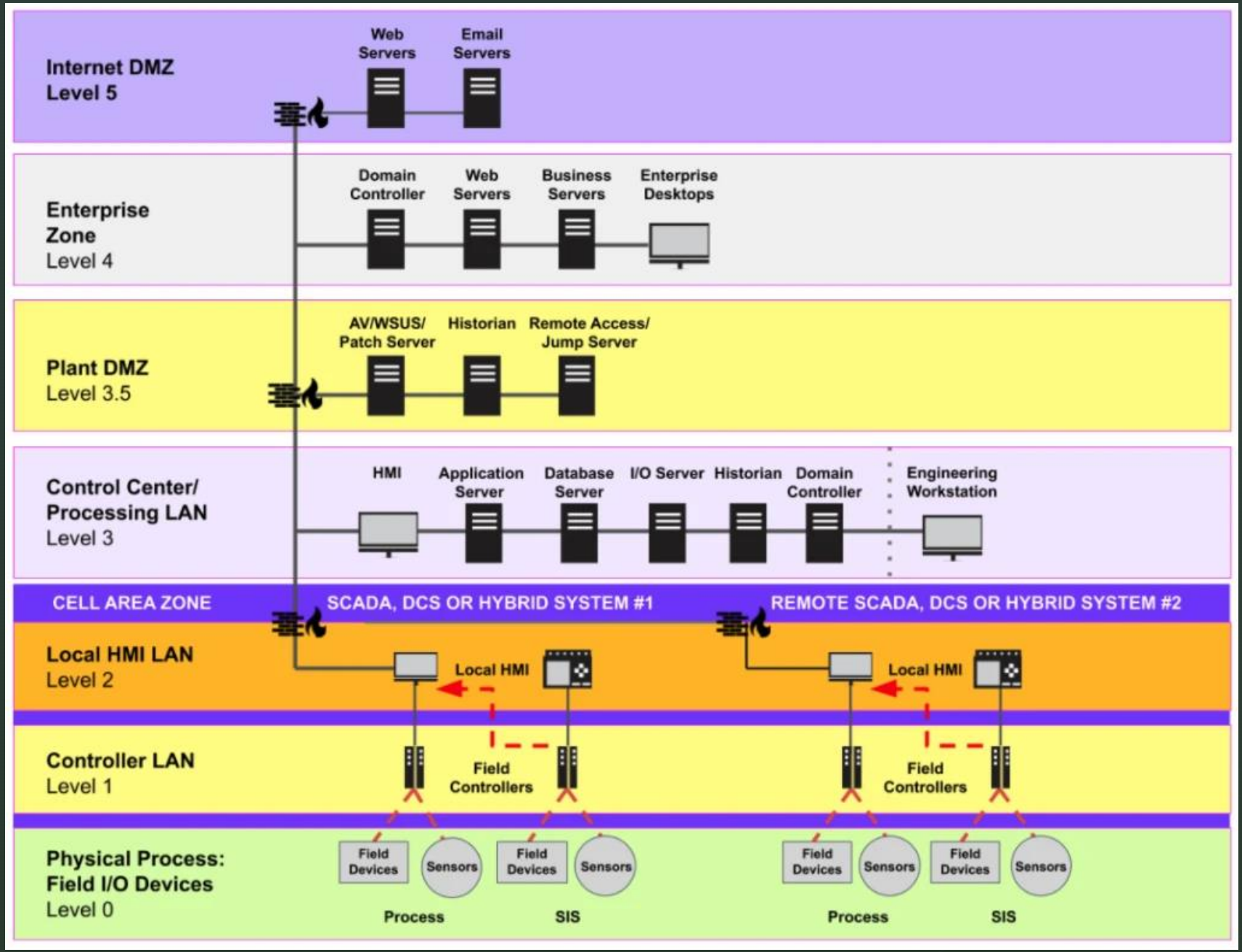
Baseline:
Question: “Can you provide a copy of the baseline configurations? How are changes done?”



Close the circle

Take what you have learned from the Asset owners and then map it your:
- OT IR framework
- OT forensics collection
- OT Crown jewel Analysis
- CSOC documentation
- Risk understanding




Internet DMZ
Level 5
Web Servers
Email Servers
Enterprise Zone
Level 4
Domain Controller
Web Servers
Business Servers
Enterprise Desktops
Plant DMZ
Level 3.5
AV/WSUS/ Patch Server
Historian
Remote Access/ Jump Server
Control Center/ Processing LAN
Level 3
HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation
CELL AREA ZONE
SCADA, DCS OR HYBRID SYSTEM #1
REMOTE SCADA, DCS OR HYBRID SYSTEM #2
Local HMI LAN
Level 2
Local HMI
Local HMI
Controller LAN
Level 1
Field Controllers
Field Controllers
Physical Process:
Field I/O Devices
Level 0
Field Devices
Sensors
Field Devices
Sensors
Field Devices
Sensors
Field Devices
Sensors
Process
SIS
Process
SIS

Thank you

- Ray Baeza,
- Agriculture Defense Group
  - Cell: (530) 867-4120
  - Email: agdefensegroup@gmail.com
  - LinkedIn: Ray Baeza
  - Instagram: Ag_defense_group
  - X : Cybercowboy