Learning ICS to develop a fleet Incident Response plan

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

POWERED BY NMFTA
National Motor Freight Traffic Association, Inc.

Presented by Chloe Callahan, Security +, Pen Test+

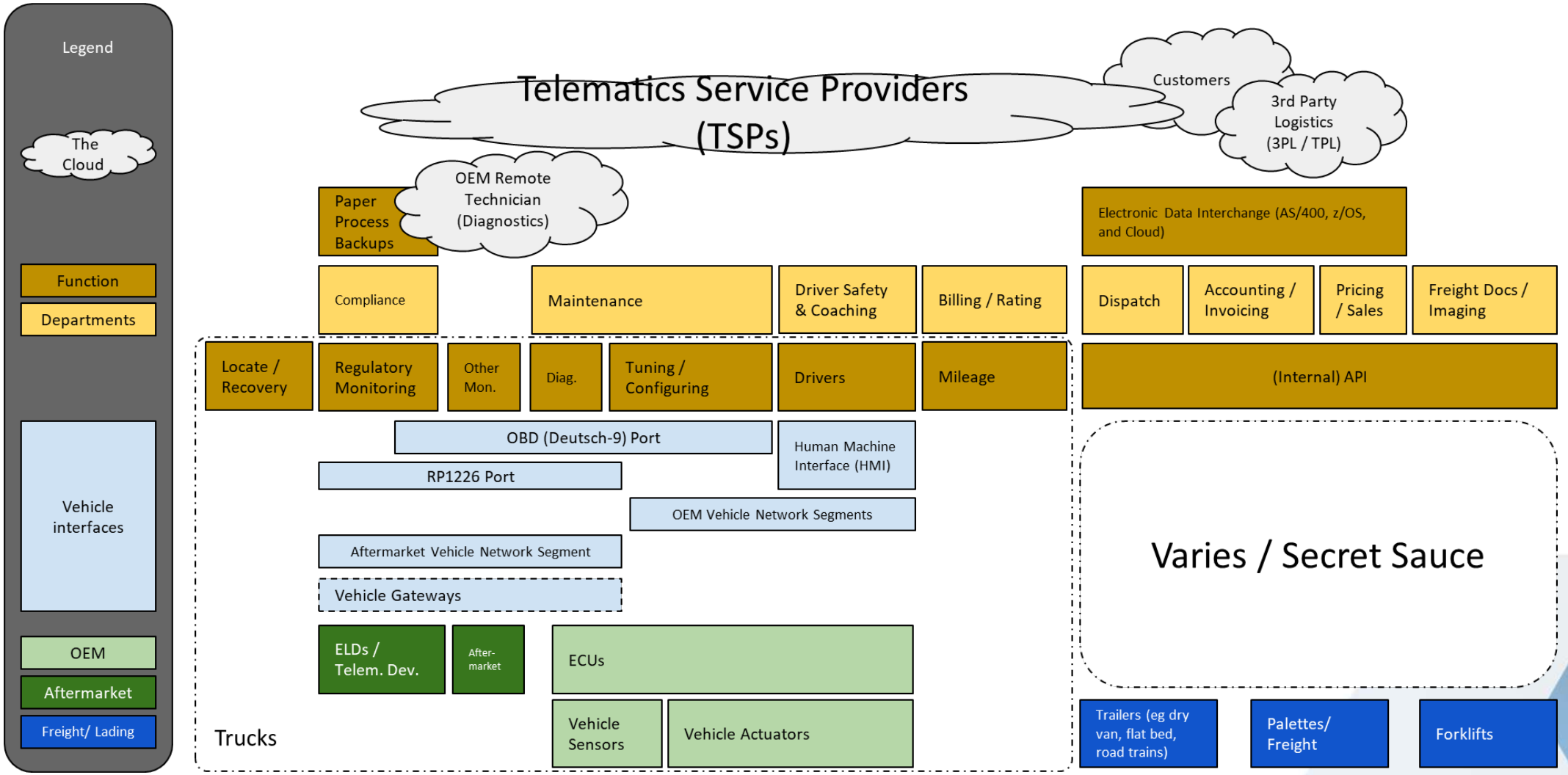
I am the IT Operations Manager at Peninsula Truck Lines Inc. My passion is to share cybersecurity skills with people of all knowledge levels. My goal is creating a security minded culture in our industry.

What we will cover

- Parallels between ICS and Trucks
- Learn from ICS incident response
- Building a fleet IR plan

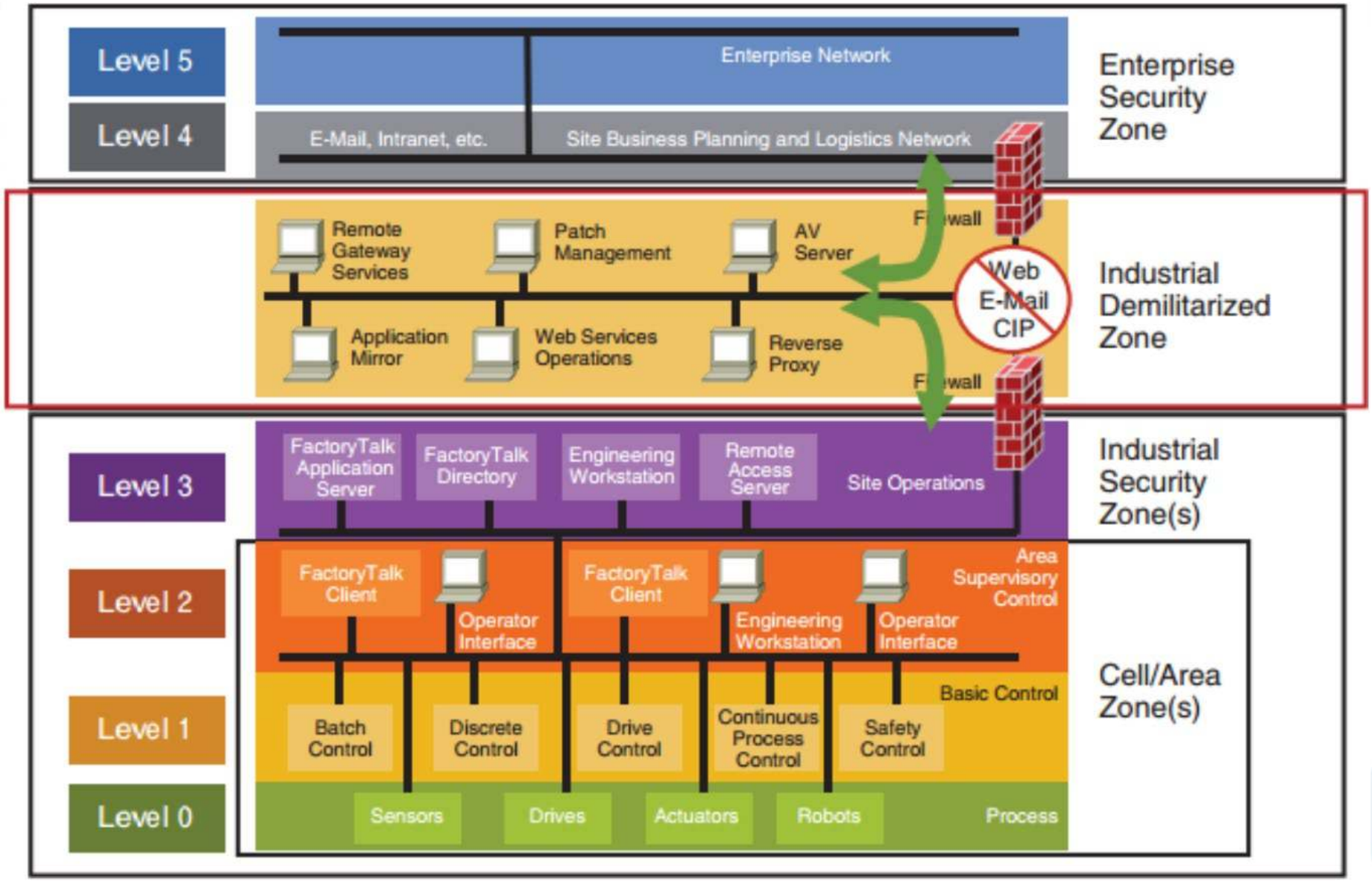
Who cares about security?

Literally



Key ICS Terms

- ICS (Industrial Control System)
- SCADA (Supervisory Control and Data Acquisition)
- SIS (Safety Instrumented System)
- PLC (Programmable Logic Controller)
- Telemetry Systems
- HMI (Human Machine Interface)
- Historian
- Alarm Handling
- Crown Jewel Analysis


Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
Enterprise Network
E-Mail, Intranet, etc.
Site Business Planning and Logistics Network
Enterprise Security Zone
Remote Gateway Services
Patch Management
AV Server
Application Mirror
Web Services Operations
Reverse Proxy
Web
E-Mail
CIP
Industrial Demilitarized Zone
FactoryTalk Application Server
FactoryTalk Directory
Engineering Workstation
Remote Access Server
Site Operations
Industrial Security Zone(s)
FactoryTalk Client
Operator Interface
FactoryTalk Client
Engineering Workstation
Operator Interface
Area Supervisory Control
Batch Control
Discrete Control
Drive Control
Continuous Process Control
Safety Control
Basic Control
Sensors
Drives
Actuators
Robots
Process
Cell/Area Zone(s)

In ICS	In CT (for vehicles)
Programmable Logic Controller (PLC)	Engine Control Unit (ECU)
Distribution Control System	Telematics Service
Field devices (modems)	Telematics Modem
Production Network	Vehicle Networks
Human Machine Interfaces	Cabin Controls and Dash
Historian	N/A (but should be)
Maintenance (the operation/step)	Service
Field Engineers	Maintenance (the department)
Mostly standard protocol, but proprietary extensions: Modbus+, HART, etc	Mostly standard protocol, but proprietary extensions: J1939

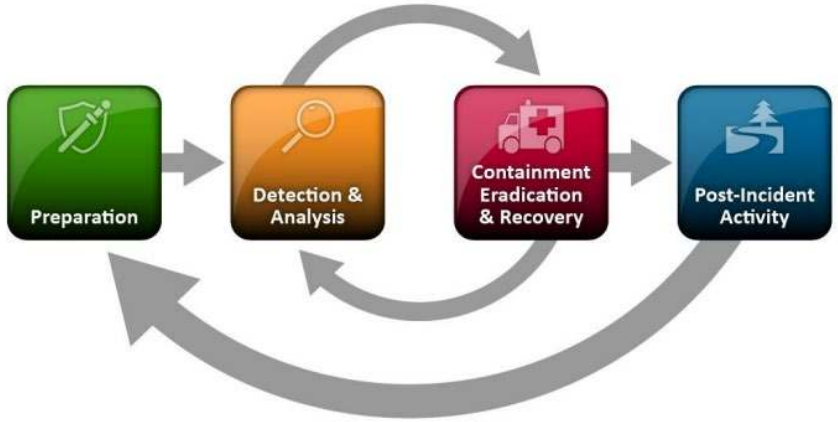
Parallels between ICS and Fleet Security

- Threat Modeling
- Sites without security staff (Unmanned ICS sites / Trucks)
- Protocols
- Unique Hardware
- Standards and guidance
- Safety, Safety, Safety

https://www.youtube.com/watch?v=RzcpZODAJE0

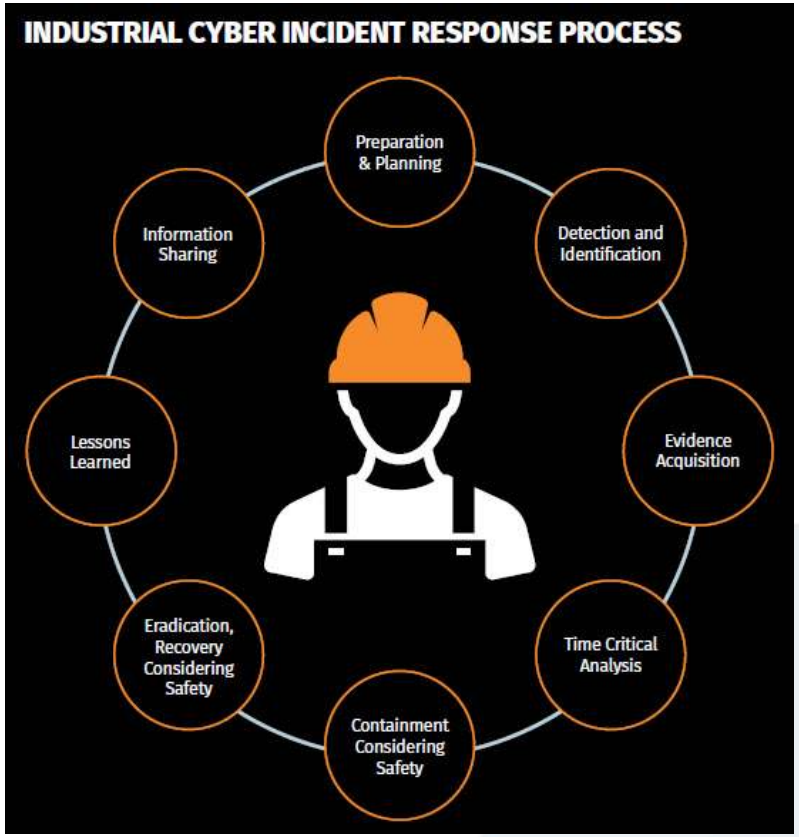
Incident Response

Traditional NIST IR Plan



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Industrial Control IR Plan



https://www.sans.org/posters/industrial-control-system-cyber-incident-response/

IR Roles

- ICS Roles
  - Incident Response Director
  - Lead Responder
  - Incident Handlers
  - Fire & Security, Safety and Law Enforcement teams

- Traditional IT IR Roles
  - Leader
  - Coordinator
  - Responders
  - Communicator

Assets, Threat and Risk Analysis

- MITRE's ATT&CK for ICS - https://attack.mitre.org/matrices/ics/

- NIST Risk assessment guidelines https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Tools

- Typical ICS Tools
  - Concentrate on the prep again
- Traditional IT Tools
  - Firewalls
  - IPS/IDS
  - Training
- Fleet Tools
  - Decoders

The Plan

- Who is on the team
- What are your assets
- Threat assessment
- Risk assessment
- What tools do you have
- When do you initiate an incident response

Tabletops

Tabletop Exercises

- https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/
- https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Security Incident Response Postmortem

Incident Name

CONTENTS

NMFTA Resources

- https://nmfta.org/wp-content/media/2022/11/Participant-Handbook.pdf https://nmfta.org/wp-content/media/2022/11/Facilitator-Handbook.pdf
- https://nmfta.org/wp-content/media/2022/11/Ransomware-Playbook-Template.pdf
- https://nmfta.org/cybersecurity/cybersecurity-research/