Traditional ICS Cybersecurity Controls

In Trucks

DIGITAL SOLUTIONS CONFERENCE
CYBERSECURITY

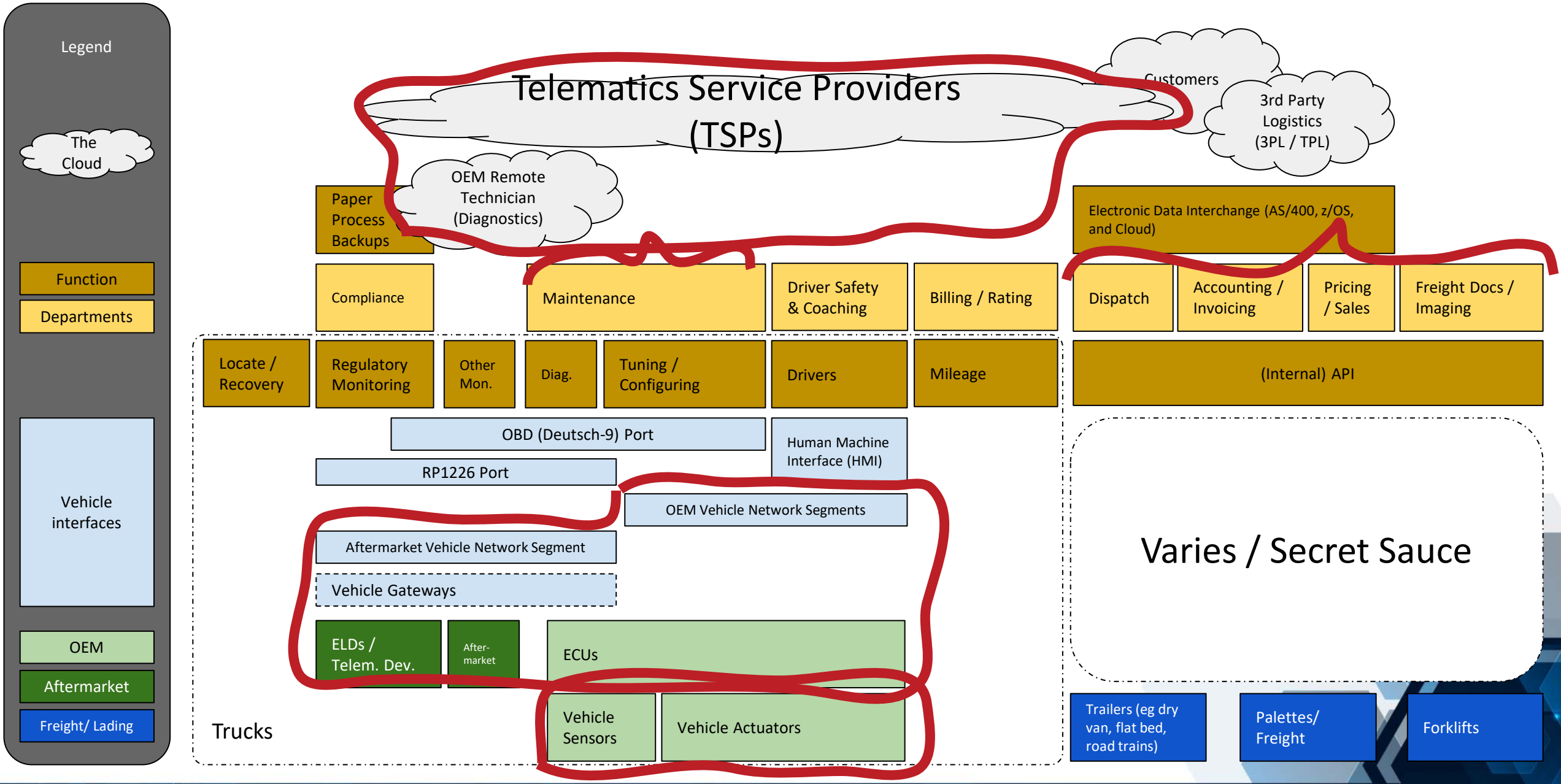
Agenda

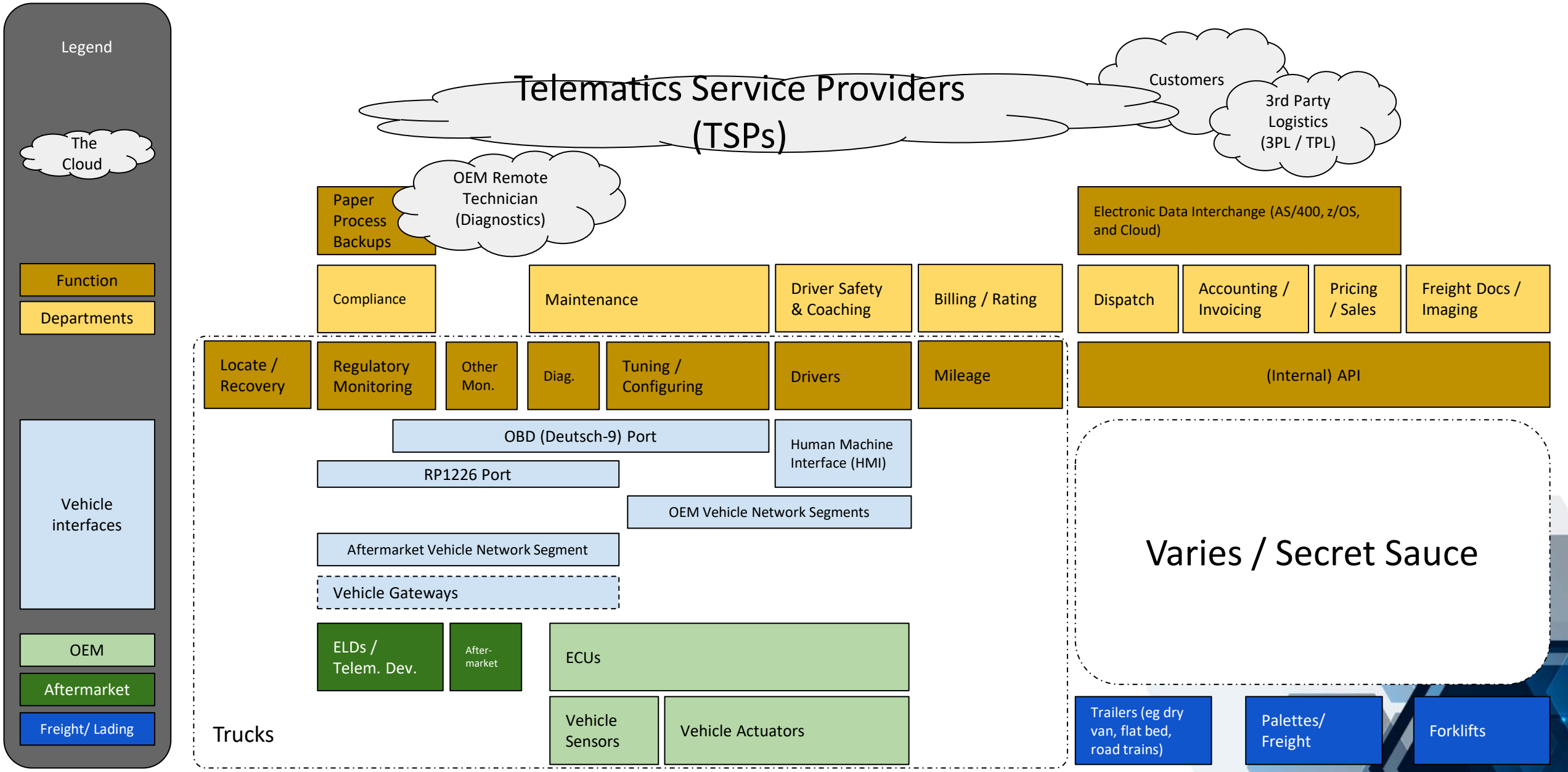
- Trucking-ICS Similarities
  - Some obvious missing pieces
- The Purdue Model
  - P-M alternatives
- NIST CS Controls OT Overlay
- Conclusions

Please ask questions at any time

Trucking ⇔ ICS Similarities

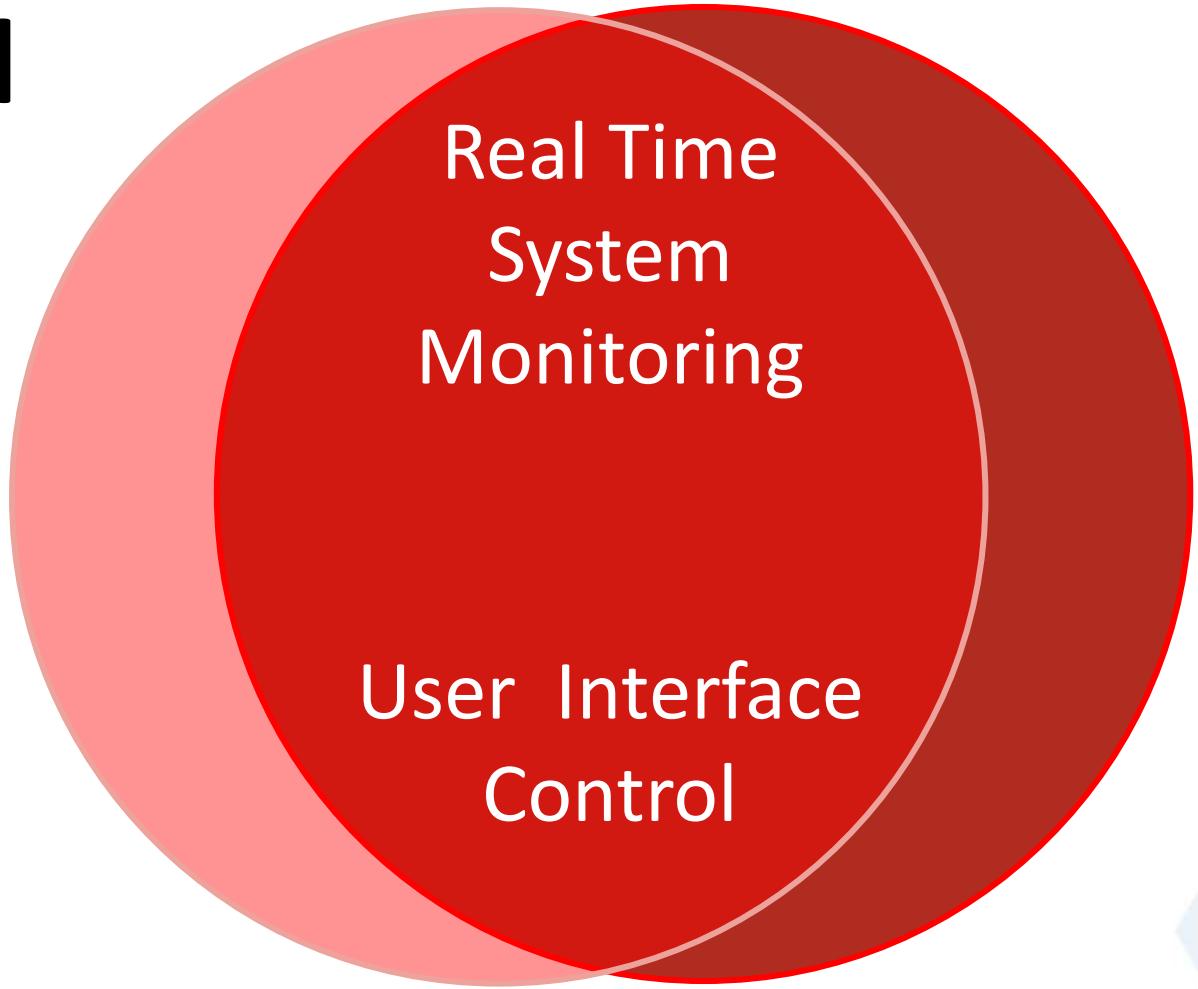
AKA Trucking ⇔ OT Similarities





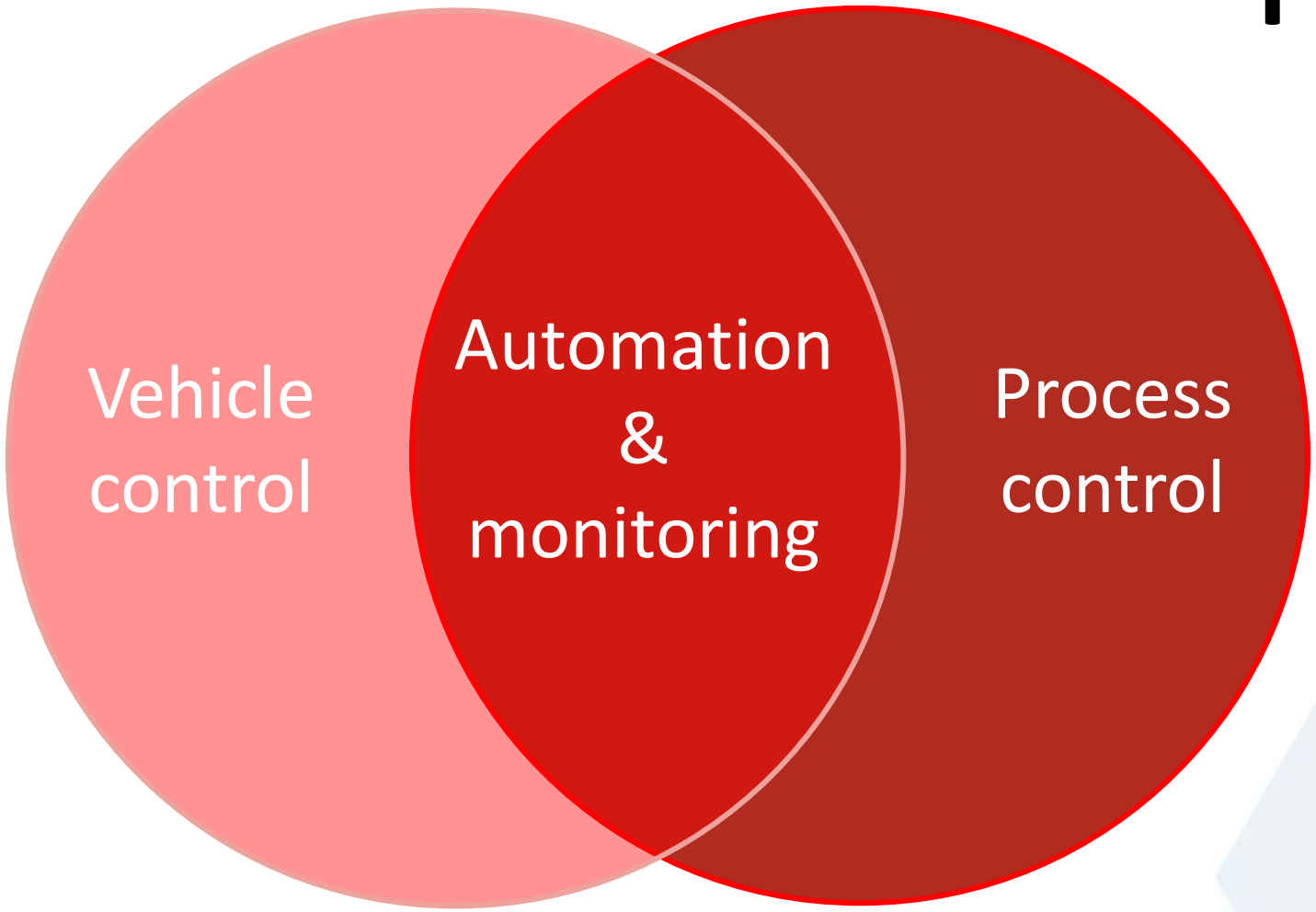
Cabin Controls & Dashboard

HMI



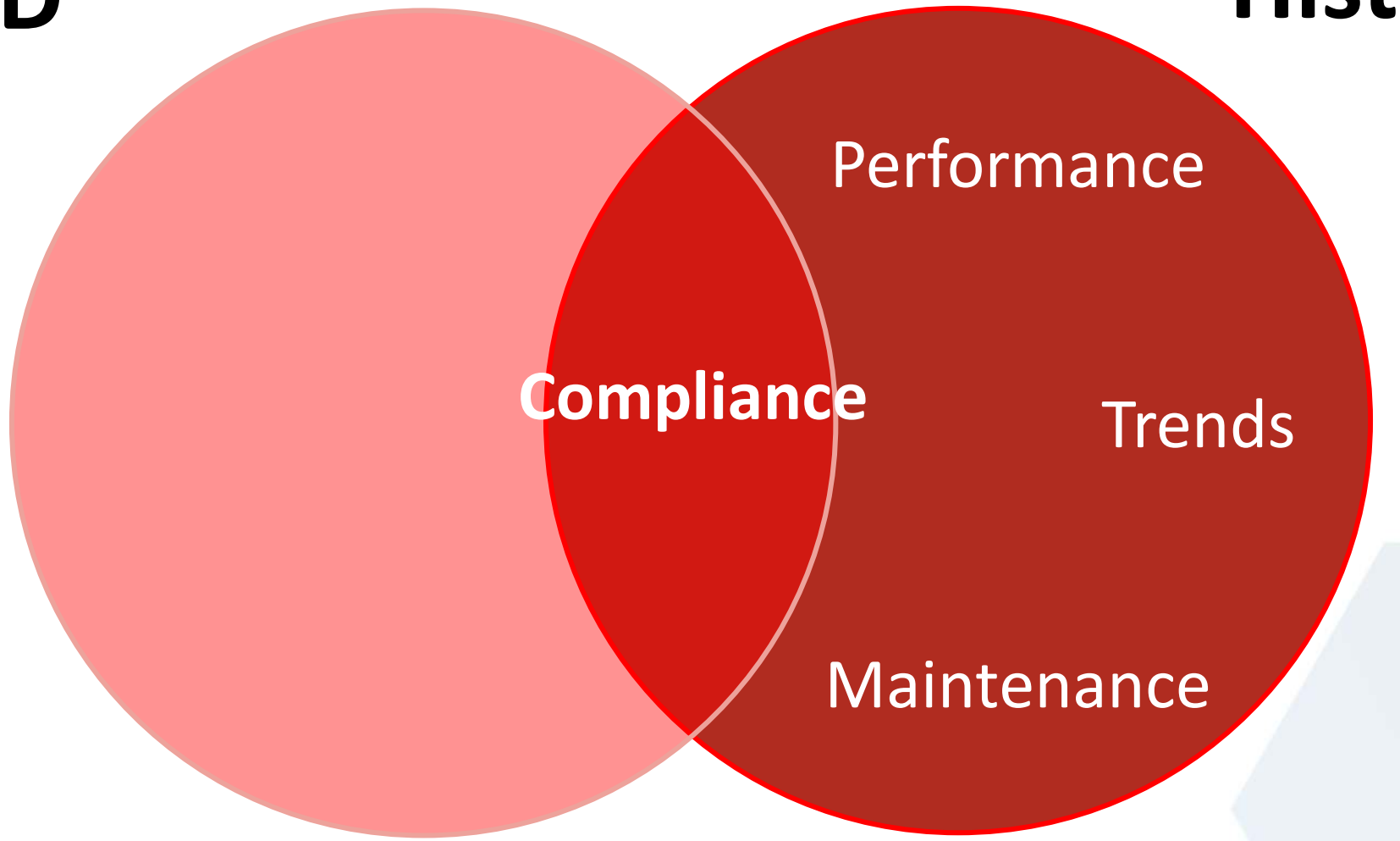
ECU

PLC



ELD

Historian



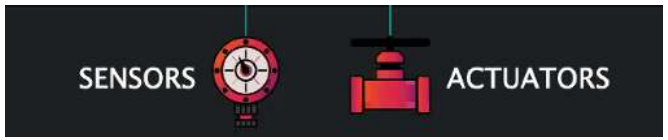
Summary of (Seemingly) Obvious Gaps

- No Data Historian in Trucking
- Despite **more** mobile connectivity

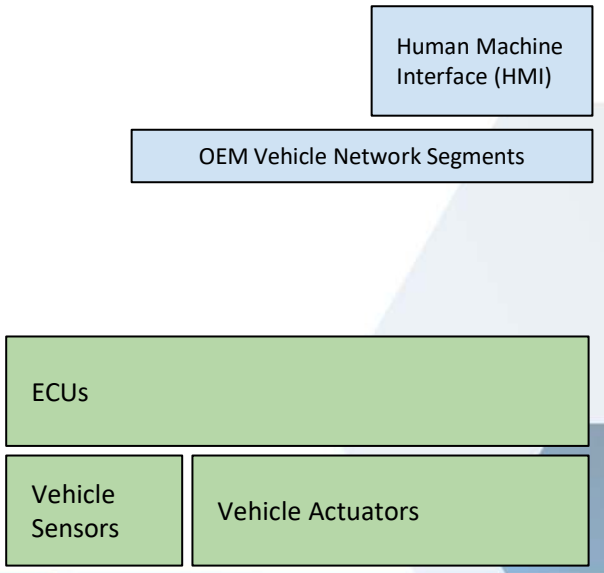
But also: let's continue to discuss and find more

Why do ICS Networks Have Issues?

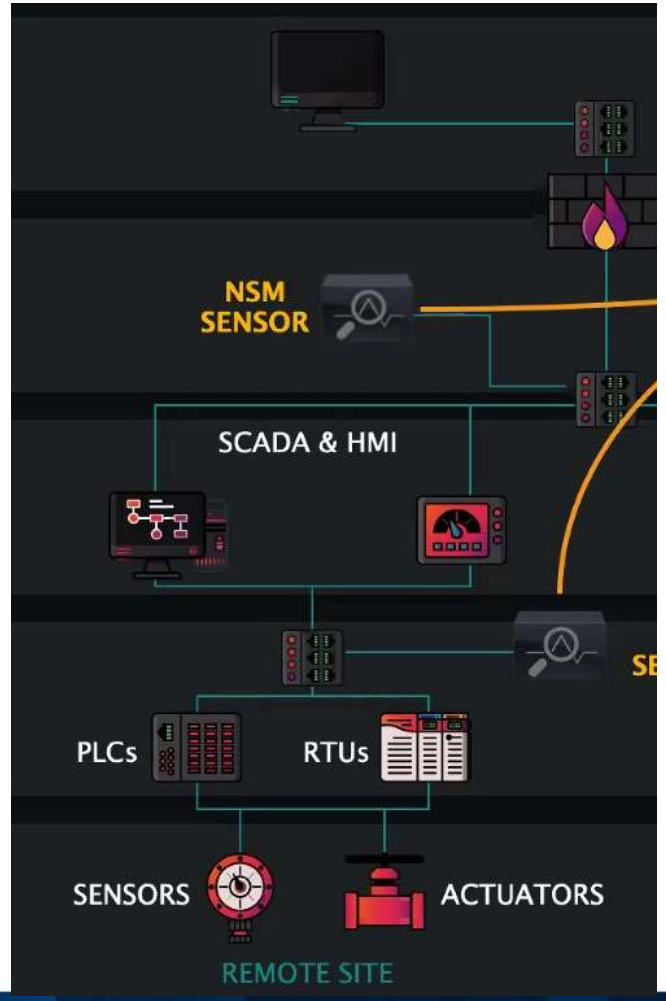
- Ideal / Secure Case is Sensors and Actuators just doing their functions



- Ideal / Secure Case is Trucks just rolling



Why do ICS Networks Have Issues?



Human Machine Interface (HMI)

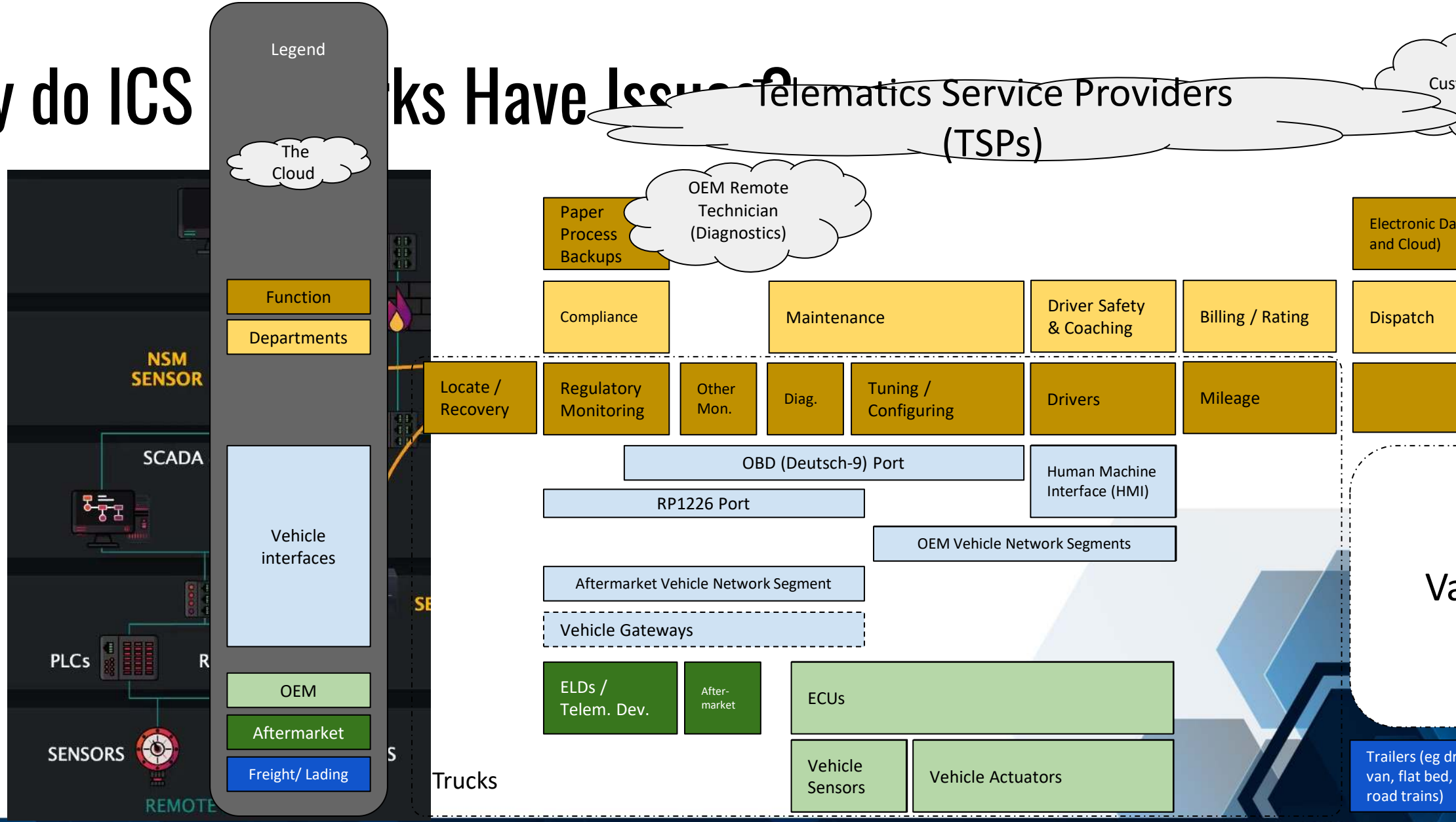
OEM Vehicle Network Segments

ECUs

Vehicle Sensors

Vehicle Actuators

Why do ICS [illegible]ks Have Issues?



Why do ICS Networks Have Issues?

ICS

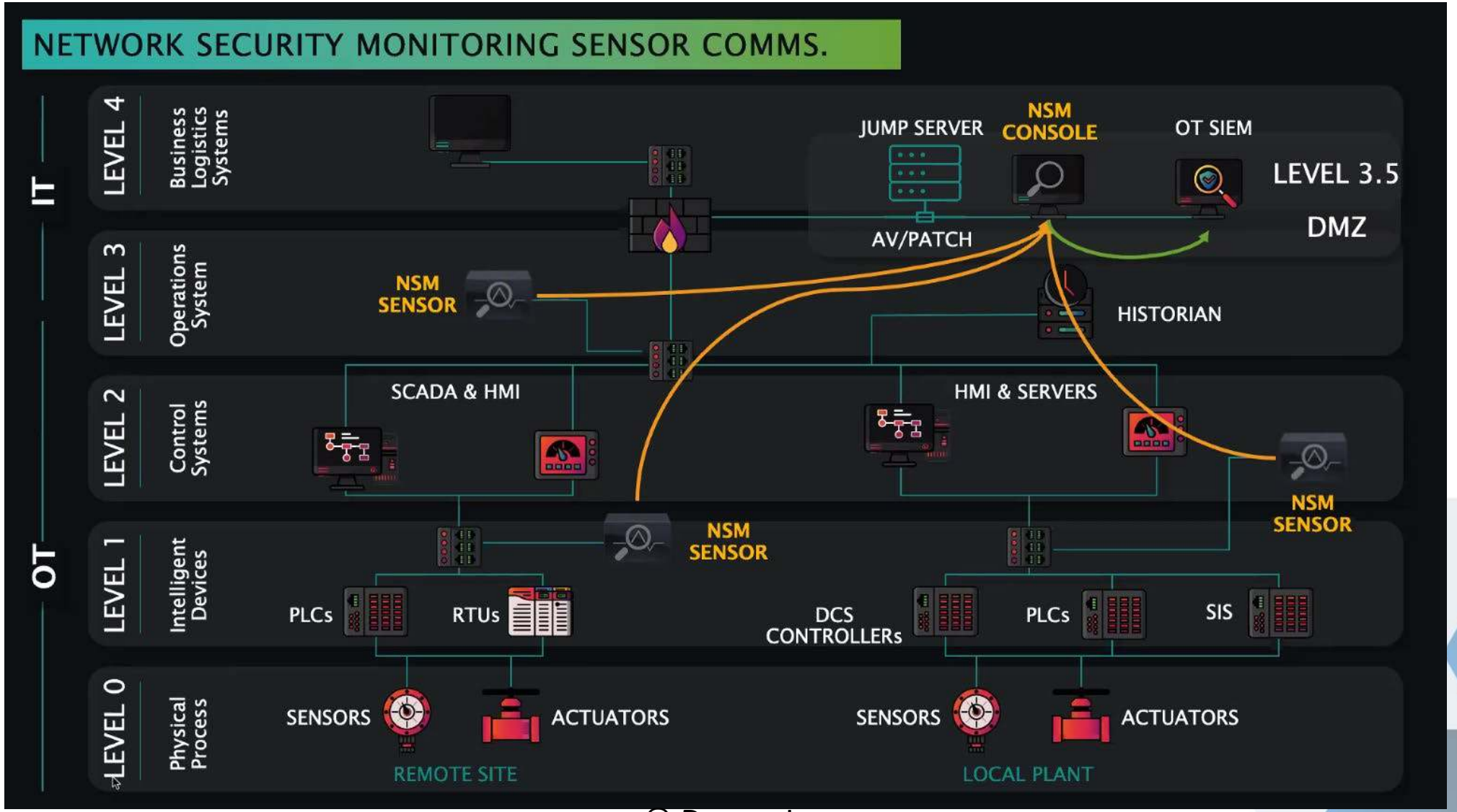
- Remote access for
  - Remote management
  - Remote business cases/process
  - OEM/vendor updates, controls and etc
  - Other issues

Trucking

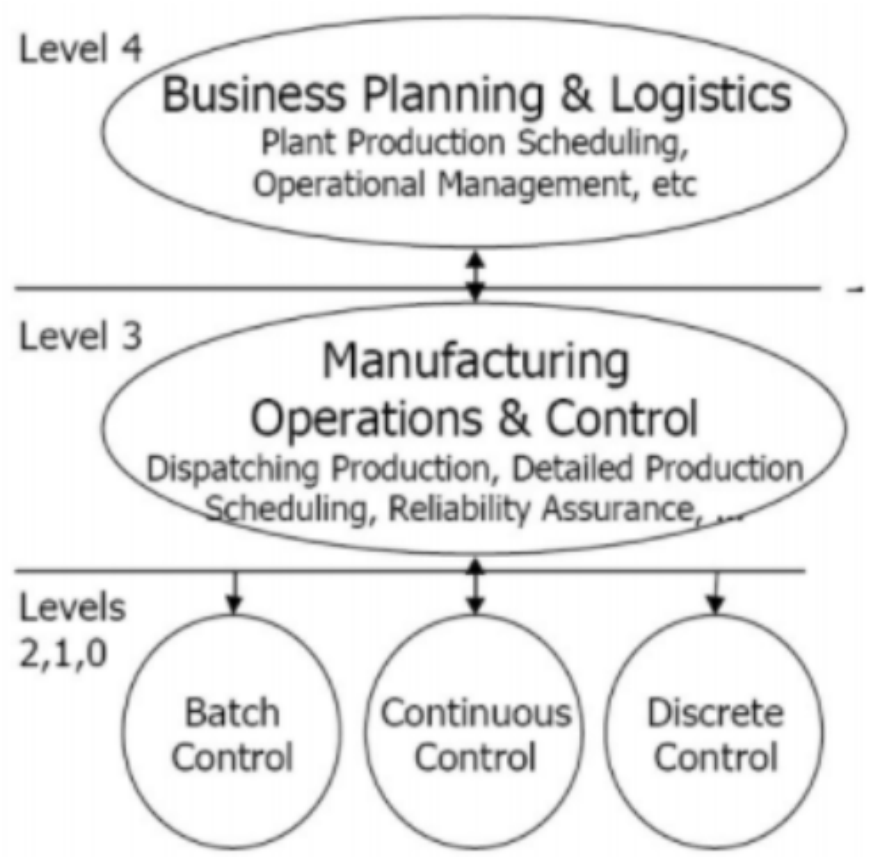
- Remote access for:
  - Remote diagnostics
  - Remote business cases/process: e.g., dispatching, monitoring, regulatory (ELD)
  - Other issues

The Purdue Model

A DRAGOS Inc. Purdue Model



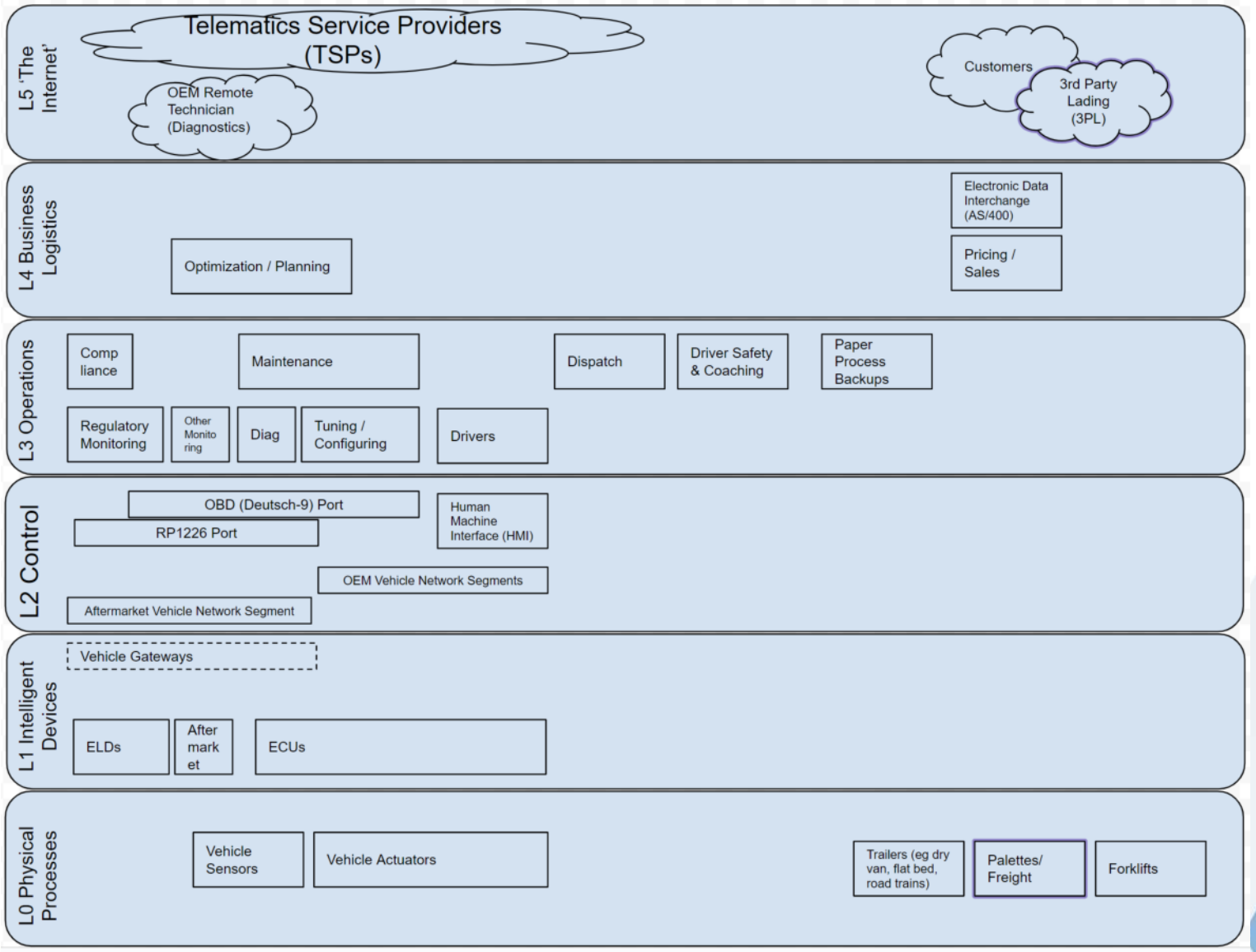
Define: Purdue Model

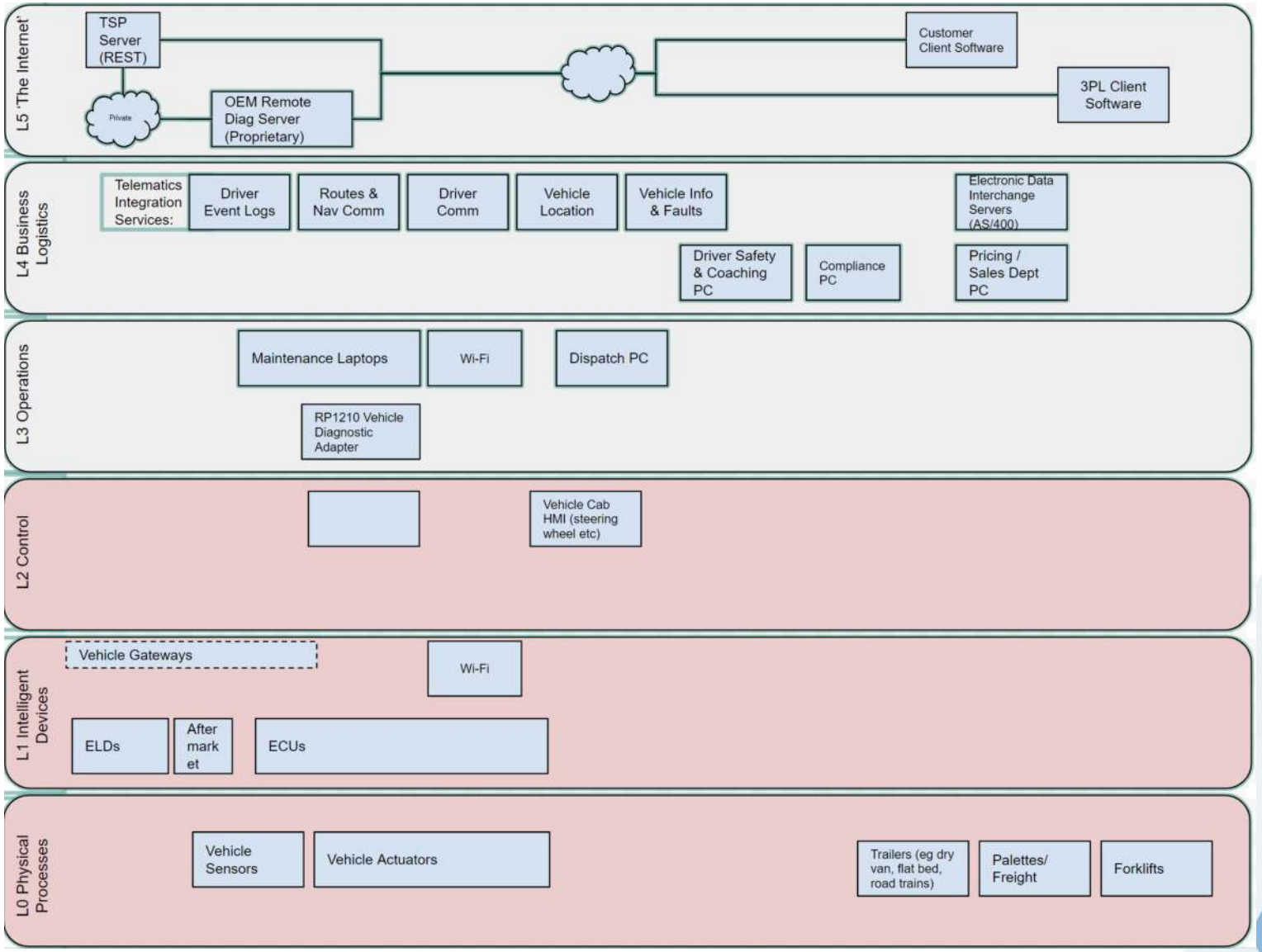


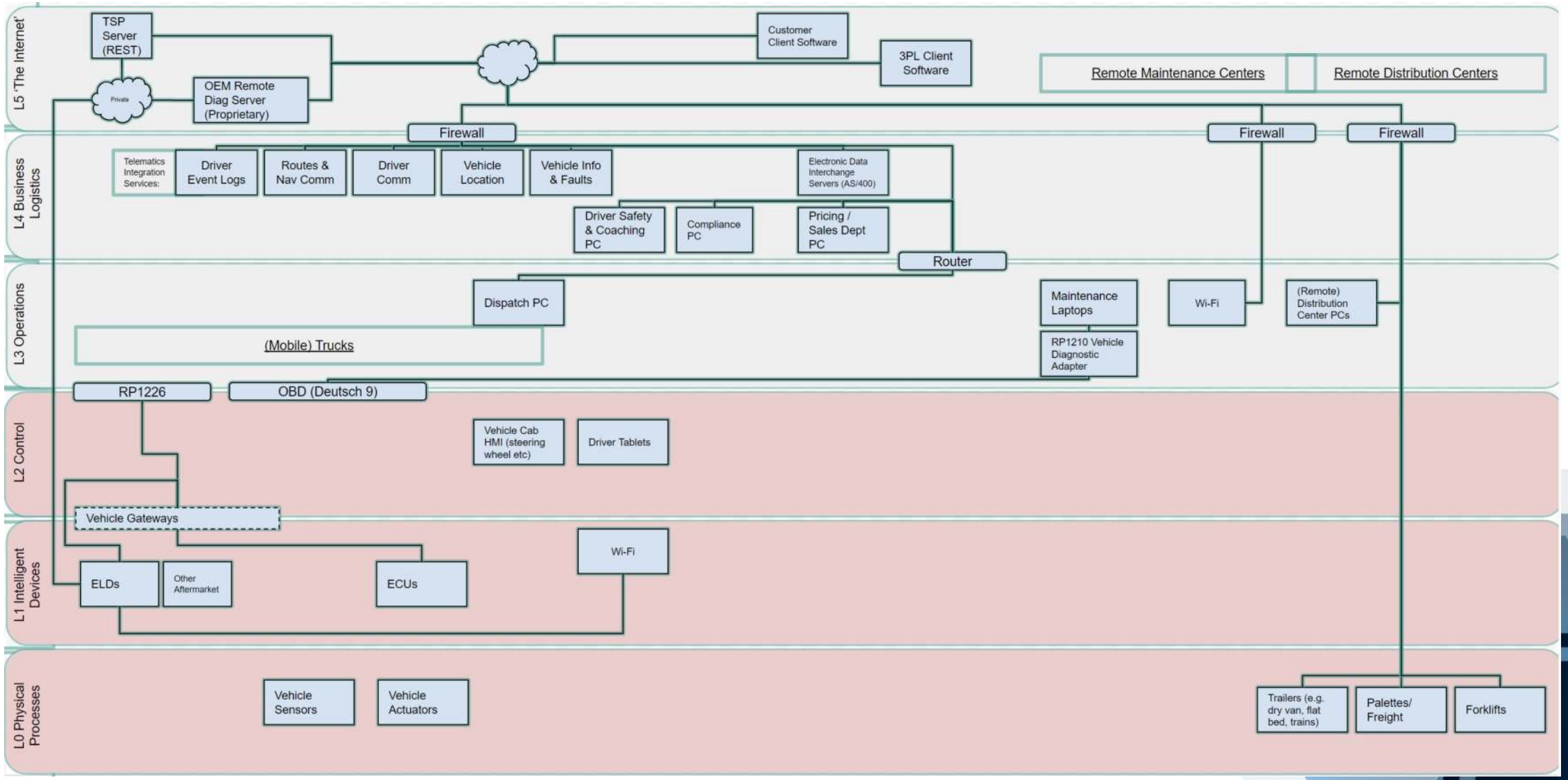
- Level 0 — The physical process.
- Level 1— Intelligent devices (sensors/actuators)
- Level 2 — Control systems (SCADA/HMI)
- Level 3 — Manufacturing operations systems
- Level 4 — Business logistics systems (ERP)

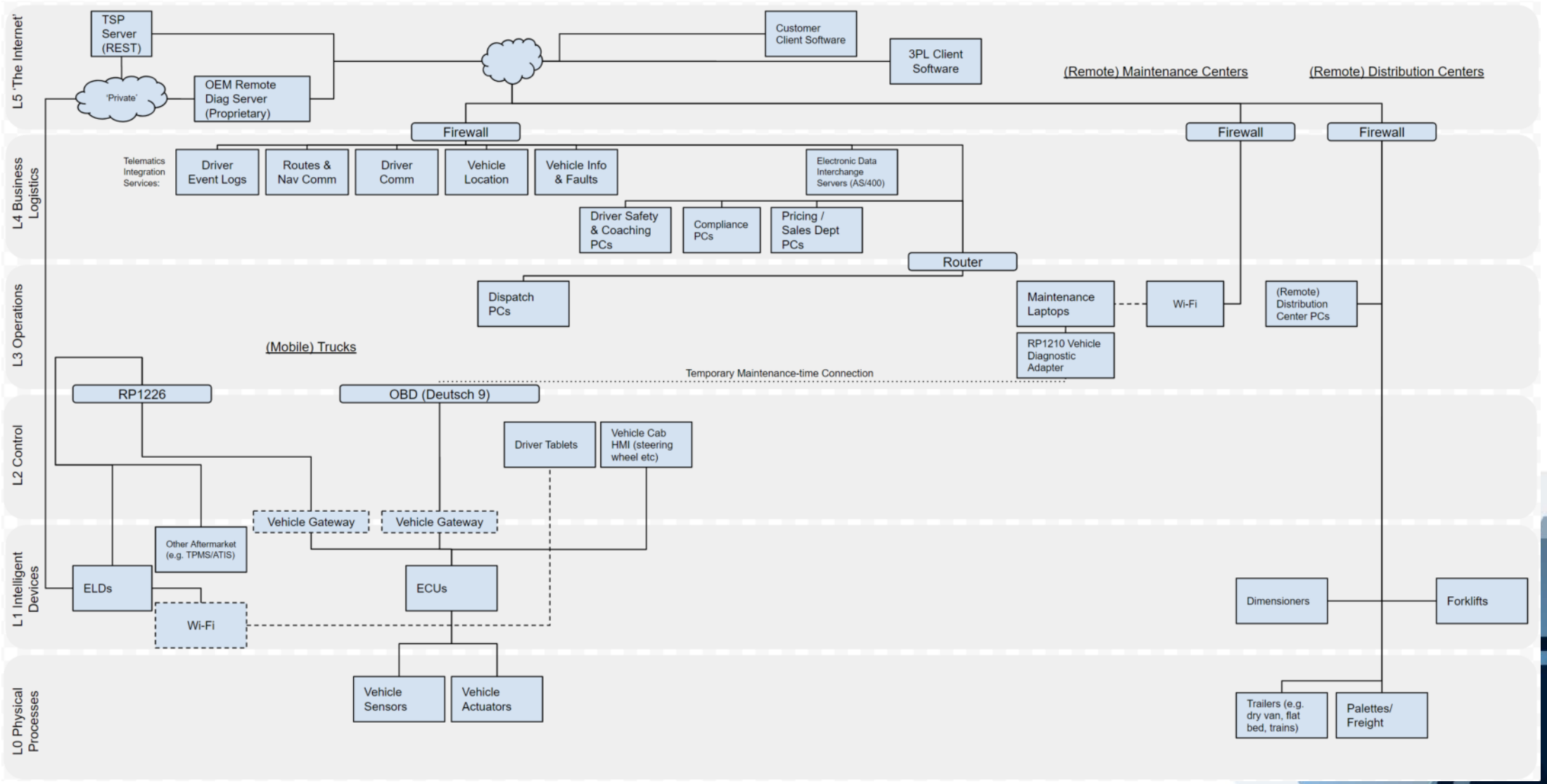
Mapping LTL Architecture to the Purdue Model

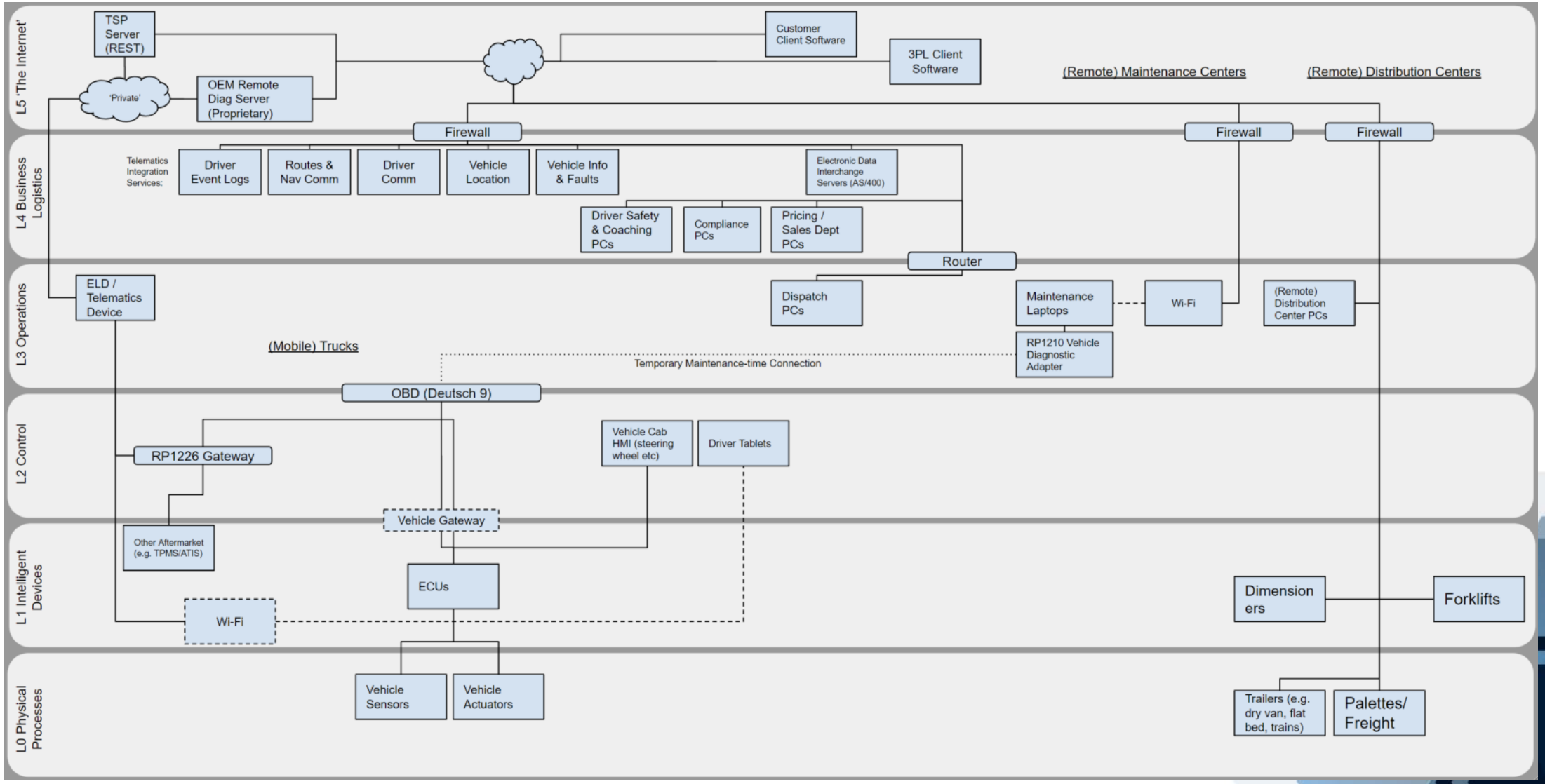
- A case study
- Kate V @ Dragos and I had a reasonable network architecture
- We wanted to cast it into Purdue to show ICS people how they could think about trucking


L5 'The Internet'
Telematics Service Providers (TSPs)
OEM Remote Technician (Diagnostics)
Customers
3rd Party Lading (3PL)
L4 Business Logistics
Optimization / Planning
Electronic Data Interchange (AS/400)
Pricing / Sales
L3 Operations
Comp liance
Maintenance
Dispatch
Driver Safety & Coaching
Paper Process Backups
Regulatory Monitoring
Other Monito ring
Diag
Tuning / Configuring
Drivers
L2 Control
OBD (Deutsch-9) Port
RP1226 Port
Human Machine Interface (HMI)
OEM Vehicle Network Segments
Aftermarket Vehicle Network Segment
L1 Intelligent Devices
Vehicle Gateways
ELDs
After mark et
ECUs
L0 Physical Processes
Vehicle Sensors
Vehicle Actuators
Trailers (eg dry van, flat bed, road trains)
Palettes/ Freight
Forklifts


L5 'The Internet'
TSP Server (REST)
Private
OEM Remote Diag Server (Proprietary)
Customer Client Software
3PL Client Software
L4 Business Logistics
Telematics Integration Services:
Driver Event Logs
Routes & Nav Comm
Driver Comm
Vehicle Location
Vehicle Info & Faults
Electronic Data Interchange Servers (AS/400)
Driver Safety & Coaching PC
Compliance PC
Pricing / Sales Dept PC
L3 Operations
Maintenance Laptops
Wi-Fi
Dispatch PC
RP1210 Vehicle Diagnostic Adapter
L2 Control
Vehicle Cab HMI (steering wheel etc)
L1 Intelligent Devices
Vehicle Gateways
Wi-Fi
ELDs
After mark et
ECUs
L0 Physical Processes
Vehicle Sensors
Vehicle Actuators
Trailers (eg dry van, flat bed, road trains)
Palettes/ Freight
Forklifts


L5 'The Internet'
TSP Server (REST)
Private
OEM Remote Diag Server (Proprietary)
Customer Client Software
3PL Client Software
Remote Maintenance Centers
Remote Distribution Centers
Firewall
Firewall
Firewall
L4 Business Logistics
Telematics Integration Services:
Driver Event Logs
Routes & Nav Comm
Driver Comm
Vehicle Location
Vehicle Info & Faults
Electronic Data Interchange Servers (AS/400)
Driver Safety & Coaching PC
Compliance PC
Pricing / Sales Dept PC
Router
L3 Operations
Dispatch PC
(Mobile) Trucks
Maintenance Laptops
RP1210 Vehicle Diagnostic Adapter
Wi-Fi
(Remote) Distribution Center PCs
RP1226
OBD (Deutsch 9)
L2 Control
Vehicle Cab HMI (steering wheel etc)
Driver Tablets
Vehicle Gateways
L1 Intelligent Devices
ELDs
Other Aftermarket
ECUs
Wi-Fi
L0 Physical Processes
Vehicle Sensors
Vehicle Actuators
Trailers (e.g. dry van, flat bed, trains)
Palettes/ Freight
Forklifts

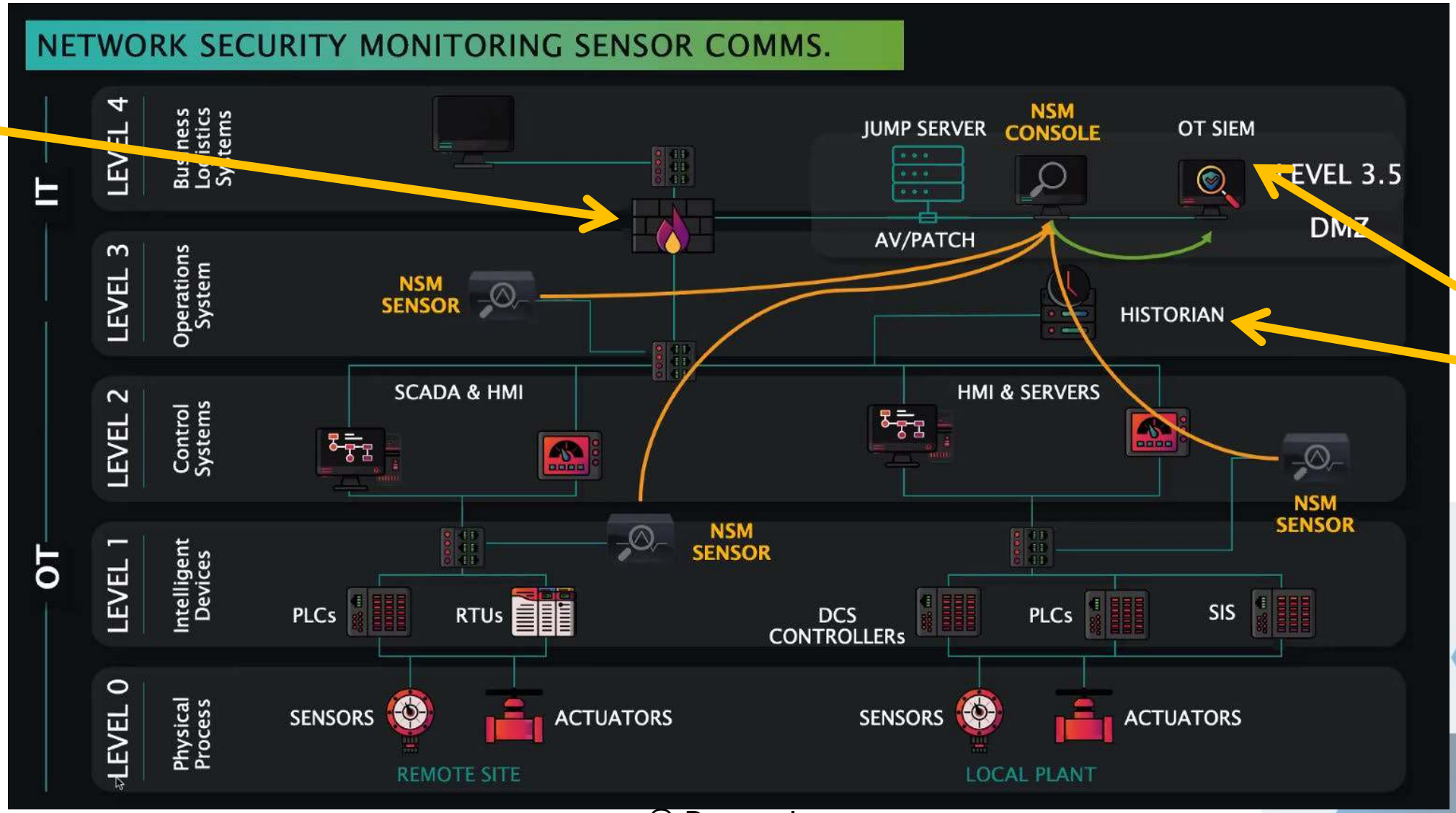

L5 'The Internet'
L4 Business Logistics
L3 Operations
L2 Control
L1 Intelligent Devices
L0 Physical Processes
TSP Server (REST)
'Private'
OEM Remote Diag Server (Proprietary)
Customer Client Software
3PL Client Software
(Remote) Maintenance Centers
(Remote) Distribution Centers
Firewall
Firewall
Firewall
Telematics Integration Services:
Driver Event Logs
Routes & Nav Comm
Driver Comm
Vehicle Location
Vehicle Info & Faults
Electronic Data Interchange Servers (AS/400)
Driver Safety & Coaching PCs
Compliance PCs
Pricing / Sales Dept PCs
Router
Dispatch PCs
Maintenance Laptops
Wi-Fi
(Remote) Distribution Center PCs
RP1210 Vehicle Diagnostic Adapter
(Mobile) Trucks
Temporary Maintenance-time Connection
RP1226
OBD (Deutsch 9)
Driver Tablets
Vehicle Cab HMI (steering wheel etc)
Vehicle Gateway
Vehicle Gateway
Other Aftermarket (e.g. TPMS/ATIS)
ELDs
Wi-Fi
ECUs
Dimensioners
Forklifts
Vehicle Sensors
Vehicle Actuators
Trailers (e.g. dry van, flat bed, trains)
Palettes/ Freight


L5 'The Internet'
L4 Business Logistics
L3 Operations
L2 Control
L1 Intelligent Devices
L0 Physical Processes
TSP Server (REST)
'Private'
OEM Remote Diag Server (Proprietary)
Customer Client Software
3PL Client Software
(Remote) Maintenance Centers
(Remote) Distribution Centers
Firewall
Firewall
Firewall
Telematics Integration Services:
Driver Event Logs
Routes & Nav Comm
Driver Comm
Vehicle Location
Vehicle Info & Faults
Electronic Data Interchange Servers (AS/400)
Driver Safety & Coaching PCs
Compliance PCs
Pricing / Sales Dept PCs
Router
ELD / Telematics Device
Dispatch PCs
Maintenance Laptops
Wi-Fi
(Remote) Distribution Center PCs
(Mobile) Trucks
RP1210 Vehicle Diagnostic Adapter
Temporary Maintenance-time Connection
OBD (Deutsch 9)
RP1226 Gateway
Vehicle Cab HMI (steering wheel etc)
Driver Tablets
Vehicle Gateway
Other Aftermarket (e.g. TPMS/ATIS)
ECUs
Wi-Fi
Dimension ers
Forklifts
Vehicle Sensors
Vehicle Actuators
Trailers (e.g. dry van, flat bed, trains)
Palettes/ Freight

Purdue Model Alternatives

- The Computer Integrated Manufacturing Pyramid model
  - better at capturing the fact that there is more communication between the layers than what is captured in Purdue
- The Open Process Automation Forum Architecture
  - Excellent talk by Rafael Maman of Sygnia
  - The OPAF is a response to the integration of IIoT into ICS/OT. Connectivity is there from the start
  - Looks more like rolling assets + telematics

Canonical Purdue Model Controls



ICS Security Controls (Canonical / Purdue Model Ones)

- Firewalls / “Application Gateways”
- Physical Access Controls
- Data in Transit protections: integrity, confidentiality protection
- Data at Rest protections: same
- Data Historian

NIST 800-82: OT Overlay

From Appendix F
(a translation of NIST 800-53 controls to OT)

What is NIST 800-82?

- A ‘special publication’ (like the IT controls 800-53 is also)
  - *GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY*
  - Has best practices / guidance for: security architectures & security programs
- This newest revision, r3, Sept 2023 has:
  - ICS -> “OT”
  - Updates to threats, vulnerabilities, risk management, recommended practices, architectures, current activities, capabilities and tools for ICS.
  - **<u>And:</u> an ‘overlay’ of 800-53 security controls for OT and compensating controls for OT**
- It complements (and quotes parts of) the ISO/IEC 62443-series

What are (800-53) “Overlays”?

- Introduced by NIST to develop community-wide and specialized sets of security controls
- A means of avoiding duplication of tailoring effort by multiple organizations in a common industry

c.f. SP 800-53 Section 3.3 and Appendix I

What are (the Overlay's) "Compensating Controls"?

- Not a great name
- Because: a 'compensating' control is an alternative means of securing things that still accomplishes the intent of the 800-53 security control.
- i.e. it is a security control that is at least as good as the 800-53 control

c.f. SP 800-53 PL-11

Caveats

- "controls that are exclusively related to privacy have not been included in this OT overlay"

An *overlay* of *800-53 security controls* for OT and *compensating controls* for OT

800-53 security controls	The mechanisms/processes/technologies that you (your IT experts) know and 'love'
Overlay	Bringing the IT security controls to a new domain
Compensating Controls	Offering improvements to the controls there
OT	Aka ICS i.e. nearly equivalent to trucks

IT vs OT Cybersecurity (by 800-82)

Category	Information Technology	Operational Technology
		OT systems often have custom applications.
Managed Support	Allow for diversified support styles	Service support is usually provided through a single vendor.
Component Lifetime	Lifetime on the order of three to five years	Lifetime on the order of 10 to 15 years
		deployment testing.
Risk Management Requirements	Manage data Data confidentiality and integrity is paramount. Fault tolerance is less important; momentary downtime is not a major risk. The major risk impact is a delay of business operations.	Control physical world Human safety is paramount, followed by protection of the process. Fault tolerance is essential; even momentary downtime may be unacceptable. The major risk impacts are regulatory non-compliance, environmental impacts, and the loss of life, equipment, or production.
System Operation	Systems are designed for use with typical OSs. Upgrades are straightforward with the availability of automated deployment tools.	Systems often use different and possibly proprietary OSs, sometimes without security capabilities built in. Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and potentially modified hardware and software
		involved.
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications, such as security solutions.	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities.
Communications	Standard IT communications protocols are used. Primarily wired networks with some localized wireless capabilities. Typical IT networking practices are employed.	Many proprietary and standard communication protocols are used. Several types of communications media are used, including dedicated wired and wireless (e.g., radio and satellite). Complex networks exist that sometimes

OT Overlay (all)

Table 22. From p. 215

Table 22. Control baselines

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Policy and Procedures	**AC-1**	**AC-1**	**AC-1**
AC-2	Account Management	**AC-2**	**AC-2** (1) **(2)** (3) (4) **(5)** **(13)**	**AC-2** (1) **(2)** (3) (4) **(5)** (11) (12) **(13)**
AC-3	Access Enforcement	**AC-3**	**AC-3**	**AC-3** (11)
AC-4	Information Flow Enforcement		**AC-4**	**AC-4** (4)
AC-5	Separation of Duties		**AC-5**	**AC-5**
AC-6	Least Privilege		**AC-6 (1) (2) (5)** (7) **(9)** **(10)**	**AC-6 (1) (2) (3) (5)** (7) **(9)** **(10)**
AC-7	Unsuccessful Logon Attempts	**AC-7**	**AC-7**	**AC-7**
AC-8	System Use Notification	**AC-8**	**AC-8**	**AC-8**
AC-10	Concurrent Session Control			**AC-10**
AC-11	Device Lock		**AC-11 (1)**	**AC-11 (1)**
AC-12	Session Termination		**AC-12**	**AC-12**
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	**AC-17** (9)	**AC-17 (1) (2) (3)** (4) (9) (10)	**AC-17 (1) (2) (3)** (4) (9) (10)
AC-18	Wireless Access	**AC-18**	**AC-18 (1)** (3)	**AC-18 (1)** (3) (4) **(5)**
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Systems	**AC-20**	**AC-20** (1) (2)	**AC-20** (1) (2)
AC-21	Information Sharing		AC-21	AC-21
AC-22	Publicly Accessible Content	**AC-22**	**AC-22**	**AC-22**
AT-1	Policy and Procedures	**AT-1**	**AT-1**	**AT-1**
AT-2	Literacy Training and Awareness	**AT-2** (2)	**AT-2** (2) (3) **(4)**	**AT-2** (2) (3) **(4)**
AT-3	Role-Based Training	**AT-3**	**AT-3**	**AT-3**
AT-4	Training Records	AT-4	AT-4	AT-4
AU-1	Policy and Procedures	**AU-1**	**AU-1**	**AU-1**
AU-2	Event Logging	**AU-2**	**AU-2**	**AU-2**
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1)

215

…to p. 223

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
SI-6	Security and Privacy Function Verification			**SI-6**
SI-7	Software, Firmware, and Information Integrity		**SI-7 (1) (7)**	**SI-7 (1) (2) (5) (7) (15)**
SI-8	Spam Protection		**SI-8** ~~(2)~~	**SI-8** ~~(2)~~
SI-10	Information Input Validation		SI-10	SI-10
SI-11	Error Handling		SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention			SI-13
SI-16	Memory Protection		SI-16	SI-16
SI-17	Fail-Safe Procedures	**SI-17**	**SI-17**	**SI-17**
SR-1	Policy and Procedures	**SR-1**	**SR-1**	**SR-1**
SR-2	Supply Chain Risk Management Plan	SR-2 (1)	SR-2 (1)	SR-2 (1)
SR-3	Supply Chain Controls and Processes	SR-3	SR-3	SR-3
SR-5	Acquisition Strategies, Tools, and Methods	SR-5	SR-5 (1)	SR-5 (1)
SR-6	Supplier Assessments and Reviews		SR-6	SR-6
SR-8	Notification Agreements	SR-8	SR-8	SR-8
SR-9	Tamper Resistance and Detection			SR-9 (1)
SR-10	Inspection of Systems or Components	SR-10	SR-10	SR-10
SR-11	Component Authenticity	SR-11 (1) (2)	SR-11 (1) (2)	SR-11 (1) (2)
SR-12	Component Disposal	SR-12	SR-12	SR-12

F.4. Tailoring Considerations

The OT overlay in this publication leverages the NIST SP 800-53B control baselines that account for the unique characteristics of OT systems, such as an increased need for availability, safety, and environmental or operating environment considerations. Additionally, OT systems vary widely in their architecture and technology selection. The NIST SP 800-53B control baselines were tailored for these general considerations, including the addition of controls relevant for OT environments. Organizations can use this overlay as a starting point and further tailor controls to meet specific operational needs to address the variability of OT systems.

As organizations further tailor controls to meet their internal security requirements, limitations (e.g., technology, operational constraints, environmental considerations) may necessitate the

223

Record Failed Login Attempts

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-7	**Unsuccessful Logon Attempts**	**Select**	**Select**	**Select**

OT Discussion: Many OT systems remain in continuous operation, and operators remain logged onto the system at all times. A "log-over" capability may be employed. Example compensating controls include logging or recording all unsuccessful logon attempts and alerting OT security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded. Unsuccessful logon attempt limits are enforced for accounts (e.g., administrator) or systems (e.g., engineering workstations) that are not required for continuous operation.

AC-20: Establish Limits for Trusts of External Systems

AC-20 USE OF EXTERNAL SYSTEMS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-20	**Use of External Systems**	**Select**	**Select**	**Select**
AC-20 (1)	*USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE*		Select	Select
AC-20 (2)	*USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE MEDIA*		Select	Select

OT Discussion: Organizations refine the definition of "external" to reflect lines of authority and responsibility, the granularity of an organization entity, and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, falls under different management authorities, or does not provide sufficient visibility into the implementation of controls to allow the establishment of a satisfactory trust relationship. For example, an OT system and a business data processing system may be considered external to each other depending on the organization's system boundaries.

Access to an OT for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external systems is reexamined with respect to OT functions, purposes, technology, and limitations to establish a clearly documented technical or business case for use and an acceptance of the risk inherent in the use of an external system.

AC-22: Don’t Make OT Publicly Accessible

AC-22 PUBLICLY ACCESSIBLE CONTENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-22	**Publicly Accessible Content**	**Select**	**Select**	**Select**

OT Discussion: Generally, public access to OT systems is not permitted. Select information may be transferred to a publicly accessible system, possibly with added controls. The organization should review what information is being made accessible prior to publication.

The AT-* Awareness Training Series

- Could be particularly useful in a guide for training fleet maintenance and drivers.

Capturing for OT IR will Require Big Storage

AU-4 AUDIT LOG STORAGE CAPACITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AU-4	**Audit Log Storage Capacity**	Select	Select	Select
AU-4 (1)	*AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Add	Add	Add

No OT Discussion for this control.

Rationale for adding AU-4 (1) to LOW, MOD, and HIGH baselines: Organizational requirements may require the storage of very large amounts of data, which OT components may not be able to support directly.

Log Important Events in OT

AU-2 EVENT LOGGING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-2	Event Logging	Select	Select	Select

OT Discussion: Organizations may want to include relevant OT events (e.g., alerts, alarms, configuration and status changes, operator actions) in their event logging, which may be designated as audit events.

The CA-* Assessment Series

- Guidance on inspecting, documenting, reviewing and (ultimately) assessing OT cybersecurity

Legacy Abounds & Legacy Resists Change

CA-5 PLAN OF ACTION AND MILESTONES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-5	**Plan of Action and Milestones**	Select	Select	Select

OT Discussion: Corrective actions identified in assessments may not be immediately actionable in an OT environment. Therefore, short-term mitigations may be implemented to reduce risk as part of the gap closure plan or plan of action and milestones.

Least Functionality & Allowlisting : aka Firewalls

CM-7 LEAST FUNCTIONALITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-7	**Least Functionality**	**Select**	**Select**	**Select**
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION*		**Select**	**Select**

OT Discussion: The organization implements least functionality by allowing only the specified functions, protocols, and/or services required for OT operations. For non-routable protocols, such as serial communications, interrupts could be disabled or set points could be made read-only except for privileged users to limit functionality. Ports are part of the address space in network protocols and are often associated with specific protocols or functions. For routable protocols, ports can be disabled on many networking devices to limit functionality to the minimum required for operation.

Control Enhancement: (5) OT Discussion: The set of applications that run in OT is relatively static, making allowlisting practical. DHS recommends using application allowlisting for OT equipment.

The MA-* Maintenance Series

- You almost certainly don’t need to read this; most flets could write the book on this.

Backup Telematics

CP-8 TELECOMMUNICATIONS SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-8	**Telecommunications Services**		**Select**	**Select**
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*		Select	Select
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*		Select	Select
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS*			Select
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*			Select

OT Discussion: Quality of service factors for OT include latency and throughput.

Control: Establish alternate telecommunications services, including necessary agreements to permit the resumption of [*Assignment: organization-defined system operations*] for essential mission and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate

Remote Diagnostics Recommedation

MA-4 NONLOCAL MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
MA-4	**Nonlocal Maintenance**	Select	Select	Select
MA-4 (1)	*NONLOCAL MAINTENANCE | LOGGING AND REVIEW*		Add	Add
MA-4 (3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION*			**Select**

Control Enhancement: (3) OT Discussion: The organization may need access to nonlocal maintenance and diagnostic services in order to restore essential OT operations or services. Example compensating controls include limiting the extent of the maintenance and diagnostic services to the minimum essential activities and carefully monitoring and auditing the nonlocal maintenance and diagnostic activities.

Rationale for adding MA-4 (1) to MOD and HIGH baselines: OT environments are often heavily dependent on nonlocal maintenance providers, so organizations should have the ability to review logs about relevant maintenance activities.

The Overlay isn't Overkill

- The baselines don't have to be extreme.
- This enhancement of the overlay applies only to HIGH Baseline
- Remember: the baselines are where organizations start in the tailoring process; changes from baseline can and should be made based on any number of organization-specific rationales

c.f. SP 800-53 Section 3.2 Tailoring Guidance

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AC-3	**Access Enforcement**	**Select**	**Select**	**Select**
AC-3 (11)	*ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES*			**Add**

OT Discussion: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the OT. Example compensating controls include encapsulation. The policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control. However, it may not provide sufficient granularity when users require access to different functions.

Control Enhancement: (11) OT Discussion: The organization identifies and restricts access to information that could impact the OT environment and accounts for information types that are sensitive, proprietary, contain trade secrets, or support safety functions.

Conclusions

Conclusions

- OT ⇔ Trucking ; NIST 800-53 IT controls ⇔ OT
- There are controls missing from Trucks Today:
  - Data Historian
  - (Application Gateway) Telematics Firewall
  - Failed seed-key attempts (AC-7)
  - Authenticating remote commands (AC-17 (9))
  - Backup Telematics
  - Logging Remote Commands

- Next steps?
  - 800-53 Trucking Overlay => Truck Matrix seed?


Thank you

Fleet Authorizations Needed

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AC-17	**Remote Access**	**Select**	**Select**	**Select**
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*		**Select**	**Select**
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*		**Select**	**Select**
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*		**Select**	**Select**
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*		Select	Select
AC-17 (9)	*REMOTE ACCESS | DISCONNECT OR DISABLE ACCESS*	**Add**	**Add**	**Add**
AC-17 (10)	*REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS*		Add	Add

OT Discussion: When the OT cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Rationale for adding AC-17 (9) to LOW, MOD, and HIGH baselines: As more OT systems become accessible remotely, the capability to disconnect or disable remote access is critical to managing risk and may be required to provide stable and safe operations.

Rationale for adding AC-17 (10) to MOD and HIGH baselines: The ability to authenticate remote commands is important to prevent unauthorized commands that may have immediate or serious consequences, such as injury, death, property damage, the loss of high-value assets, the failure of mission or business functions, or compromise of sensitive information.

AC-18 WIRELESS ACCESS

Wireless Limited Access

AC-18 WIRELESS ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-18	**Wireless Access**	**Select**	**Select**	**Select**
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*		**Select**	**Select**
AC-18 (3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*		Select	Select
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*			Select
AC-18 (5)	*WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS*			**Select**

OT Discussion: When OT cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Assets?

Discussion: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Other Assets?

CM-8 SYSTEM COMPONENT INVENTORY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-8	**System Component Inventory**	Select	Select	Select
CM-8 (1)	*SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		Select	Select
CM-8 (2)	*SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*			Select
CM-8 (3)	*SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		Select	Select
CM-8 (4)	*SYSTEM COMPONENT INVENTORY | PROPERTY ACCOUNTABILITY INFORMATION*			Select