Vehicle Cybersecurity Requirements Working Group (VCRWG) Update:

Gateways then the Truck Matrix

NMFTA
National Motor Freight Traffic Association, Inc.

Agenda

- 50 Minutes
- Goals and Purpose of Truck Matrix
- History and Context
- Common/Abstract Vehicle Topology
- Basic Risk Analysis
- Requirements Management
- Trying out Strictdoc (vcr-experiment)
- Current vcr-experiment status
- Current NMFTA-vehicle cybersecurity requirements status
- Next Steps
- Conclusions

Goals and Purpose of the Truck Matrix

NMFTA
National Motor Freight Traffic Association, Inc.

What's the Problem?

- Fleets – especially the big ones – specify their truck orders down to every last component and detail.
- Cybersecurity is mostly opaque to them
- Some fleets are discerning enough to drop certain components with perceived risk (e.g. OEM telematics/virtual diagnostics)
- How to enable transparency of Cybersecurity?
- Dropping components might not be an option forever

Truck Matrix Goals

- Provide a comprehensive set of requirements and accompanying supplier questionnaires which can be used by fleets to:
  1. Assess Cybersecurity posture of equipment before purchase
  2. Afford some contractual guarantees of Cybersecurity presence in the equipment
  3. Drive adoption of comprehensive Cybersecurity by the OEMs by tying it closer to the $

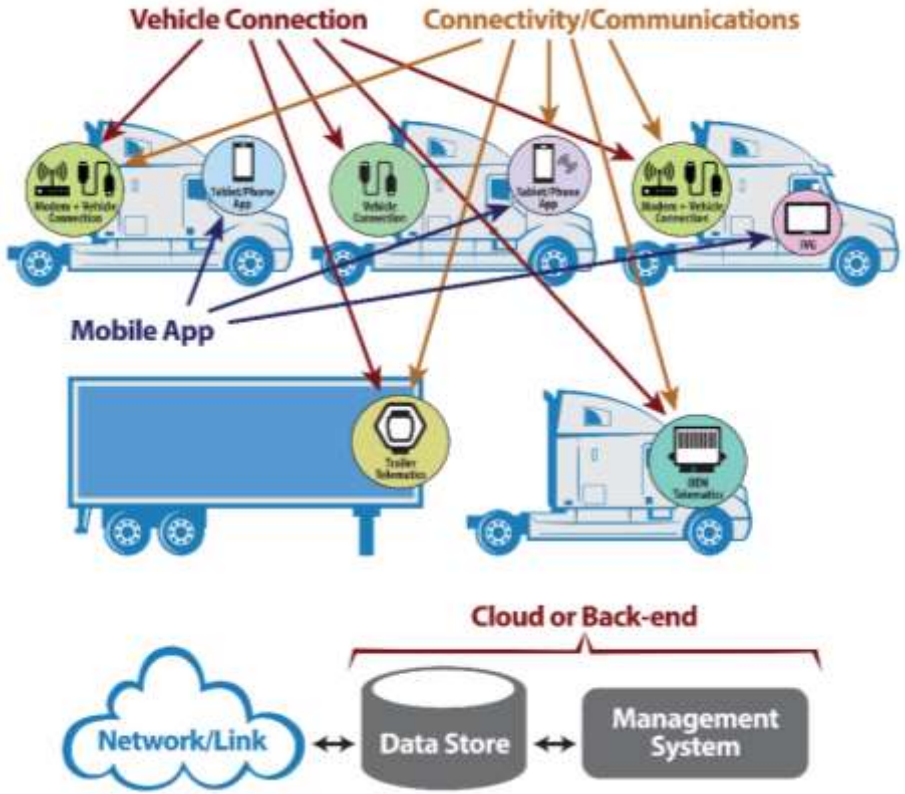
Ideally:

- Make the requirements easy to consume by OEMs
- Make the requirements testable by the fleets

History and Context

The TSRM

- Very similar goals - but for telematics devices
- Good participation from TSPs - they were receiving varied security requirement questions from their customers
- Created a single set they could answer from
- Over all 4 possible components of a telematics system

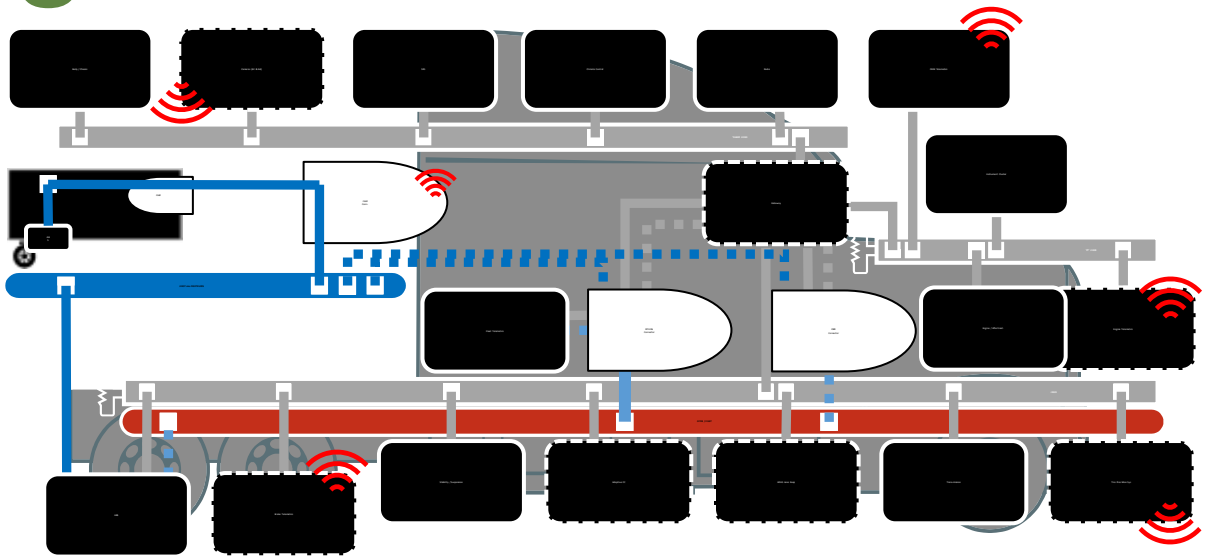


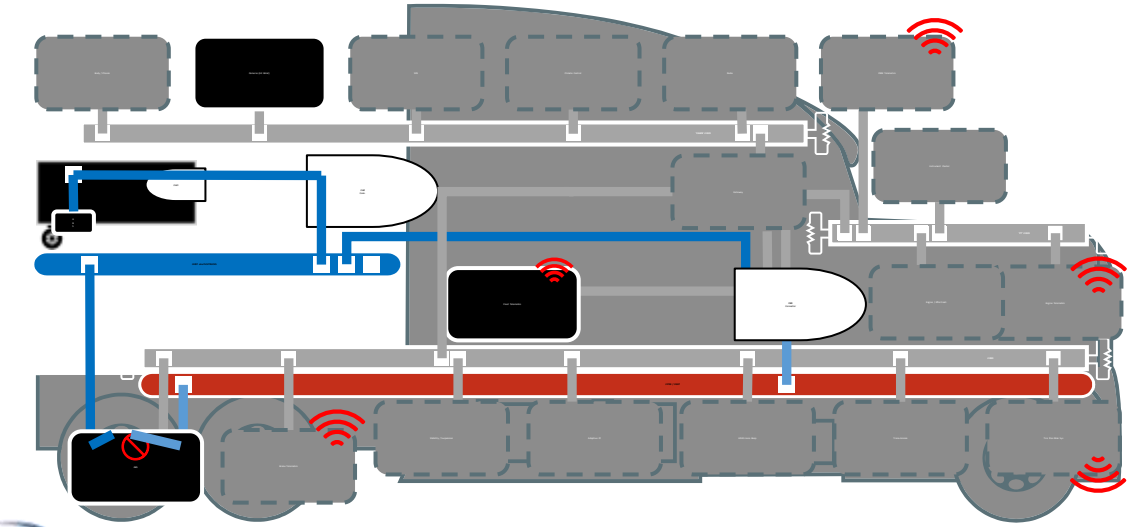
Truck Order Sheets

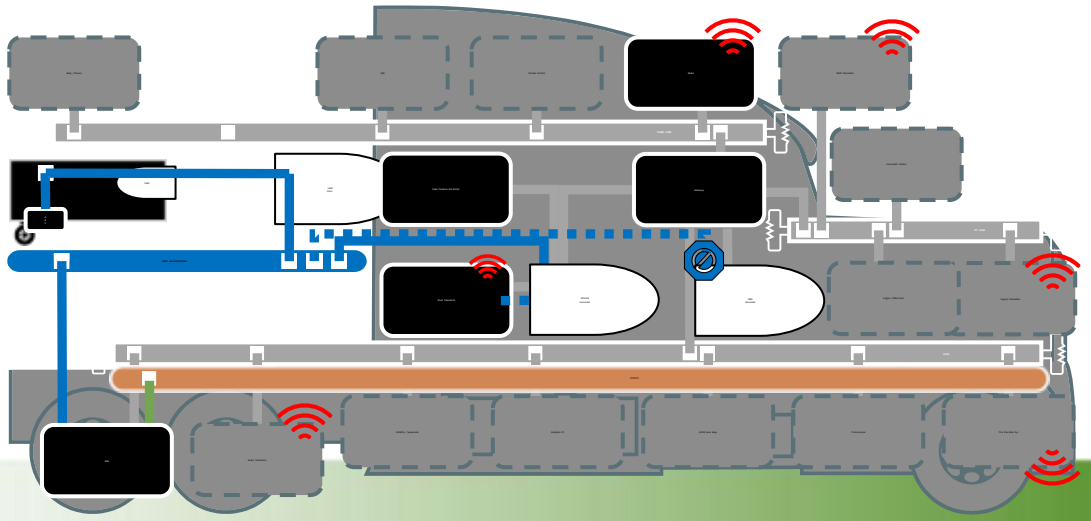
- The de-facto means of fleets spec'ing a truck
- Specify everything from radio/cd-player to lug nuts
- We found 16 order sheet lines with obvious electronic components (e.g. things like paint excluded for now)

Truck Network Architectures/Topologies

- Gets pretty hairy
- WG (eventually) identified 162 unique electronic components that might be on a truck
- Multiple points of access: OBD, RP1226, J560, RP170, wireless, telematics







NMFTA
National Motor Freight Traffic Association, Inc.

Common/Abstract Vehicle Topology

NMFTA
National Motor Freight Traffic Association, Inc.

The Development Approach

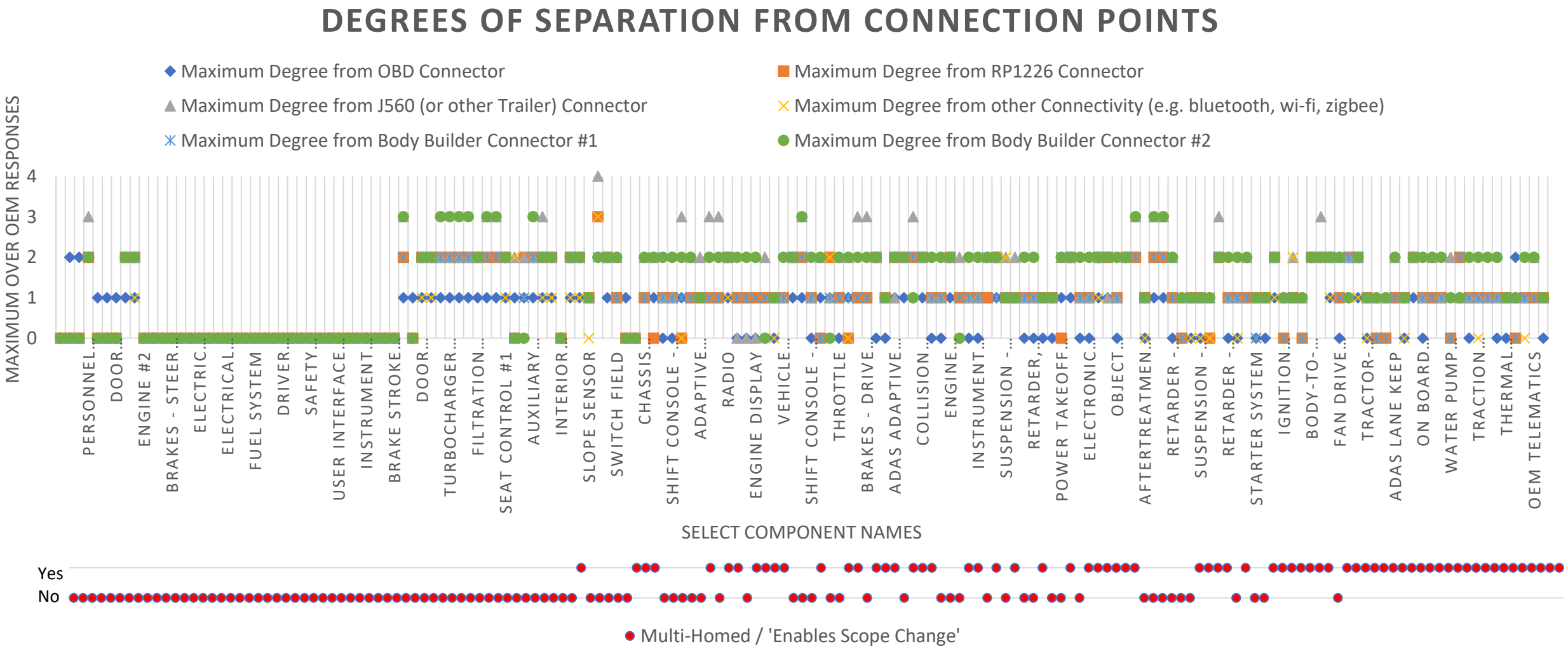
- Re-use or otherwise leverage the work from the RFPCTL workgroup – started by Volpe – resulting in the Telematics Security Requirements Matrix (TSRM)
- Create a new mapping of those requirements for truck components
- Listing requirements for each of the 162 controller applications which could be components was infeasible.
  - ➞ started with classifying the controller applications by risk tier

- Risks estimated via EVITA: probability x impact
  - But probability based on topology survey; i.e. EVITA attack potential based on window of opportunity only, all other aspects considered equal.

Survey of Vehicle Network Topologies (1/3)

- Without having to see the network architectures that the OEMs don't want to share
- OEM Homework #1: survey and respond with the 'degrees of separation' of the component from a few key points in the vehicle networks:
  - Degree from OBD connector
  - Degree from RP1226 connector
  - Degree from J560 connector
  - Degree from other connectivity (BT, WiFi, Zigbee, TPMS, any)
- And also report if a component connects to multiple vehicle network segments
  - (i.e. enables scope change / pivot on compromise)

Survey of Vehicle Network Topologies (2 of 3)



NMFTA
National Motor Freight Traffic Association, Inc.

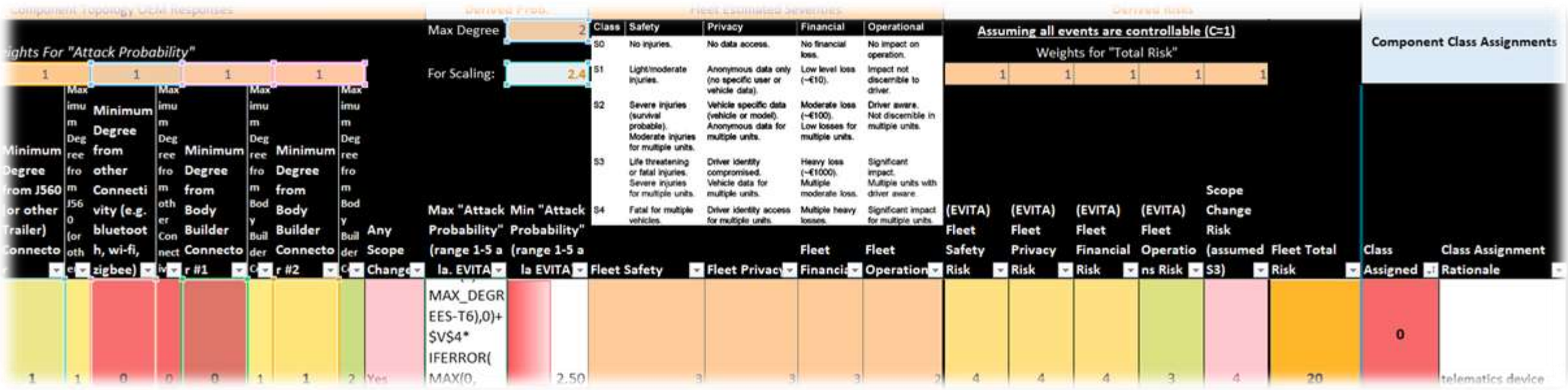
Survey of Vehicle Network Topologies (3/3)

		Potential Implications (EVITA)				
Matrix Order Sheet	Matrix Component Name	Fleet Privacy	Fleet Safety	Fleet Operational	Fleet Financial	Component Cybersecurity Class
ENGINE	Engine #1					f('Potential Impacts', 'Scope Change', 'Attack Vector')
ENGINE	Engine #2					
ENGINE	Engine Cylinder Pressure Monitoring System					'Attack Vector')

- We used those results to estimate 'probability of compromise' via 'Scope Change' and 'Attack Vector' (without controls) and combine it with our estimated fleet impacts to get risk levels

- BONUS: 28 controller applications were identified as 'not common' – WG resolved to not worry about classifying them

NMFTA
National Motor Freight Traffic Association, Inc.



Max Degree	2
For Scaling:	2.4

Class	Safety	Privacy	Financial	Operational
S0	No injuries.	No data access.	No financial loss.	No impact on operation.
S1	Light/moderate injuries.	Anonymous data only (no specific user or vehicle data).	Low level loss (~€10).	Impact not discernible to driver.
S2	Severe injuries (survival probable). Moderate injuries for multiple units.	Vehicle specific data (vehicle or model). Anonymous data for multiple units.	Moderate loss (~€100). Low losses for multiple units.	Driver aware. Not discernible in multiple units.
S3	Life threatening or fatal injuries. Severe injuries for multiple units.	Driver identity compromised. Vehicle data for multiple units.	Heavy loss (~€1000). Multiple moderate loss.	Significant impact. Multiple units with driver aware.
S4	Fatal for multiple vehicles.	Driver identity access for multiple units.	Multiple heavy losses.	Significant impact for multiple units.

Assuming all events are controllable (C=1)

Weights for "Attack Probability"				
1	1	1	1	

Weights for "Total Risk"				
1	1	1	1	1

Minimum Degree from J560 (or other Trailer) Connecto	Maximum Degree from J560 (or other	Minimum Degree from other Connectivity (e.g. bluetooth, wi-fi, zigbee)	Maximum Degree from other Connectivity	Minimum Degree from Body Builder Connecto r #1	Maximum Degree from Body Builder C	Minimum Degree from Body Builder Connecto r #2	Maximum Degree from Body Builder C	Any Scope Change	Max "Attack Probability" (range 1-5 a la. EVITA	Min "Attack Probability" (range 1-5 a la EVITA	Fleet Safety	Fleet Privacy	Fleet Financi	Fleet Operation	(EVITA) Fleet Safety Risk	(EVITA) Fleet Privacy Risk	(EVITA) Fleet Financial Risk	(EVITA) Fleet Operations Risk	Scope Change Risk (assumed S3)	Fleet Total Risk	Class Assigned	Class Assignment Rationale
1	1	0	0	0	1	1	2	Yes	MAX_DEGREES-T6),0)+V4*IFERROR(MAX(0,	2.50	3	3	3	2	4	4	4	3	4	20	0	telematics device

A Basic Risk Analysis

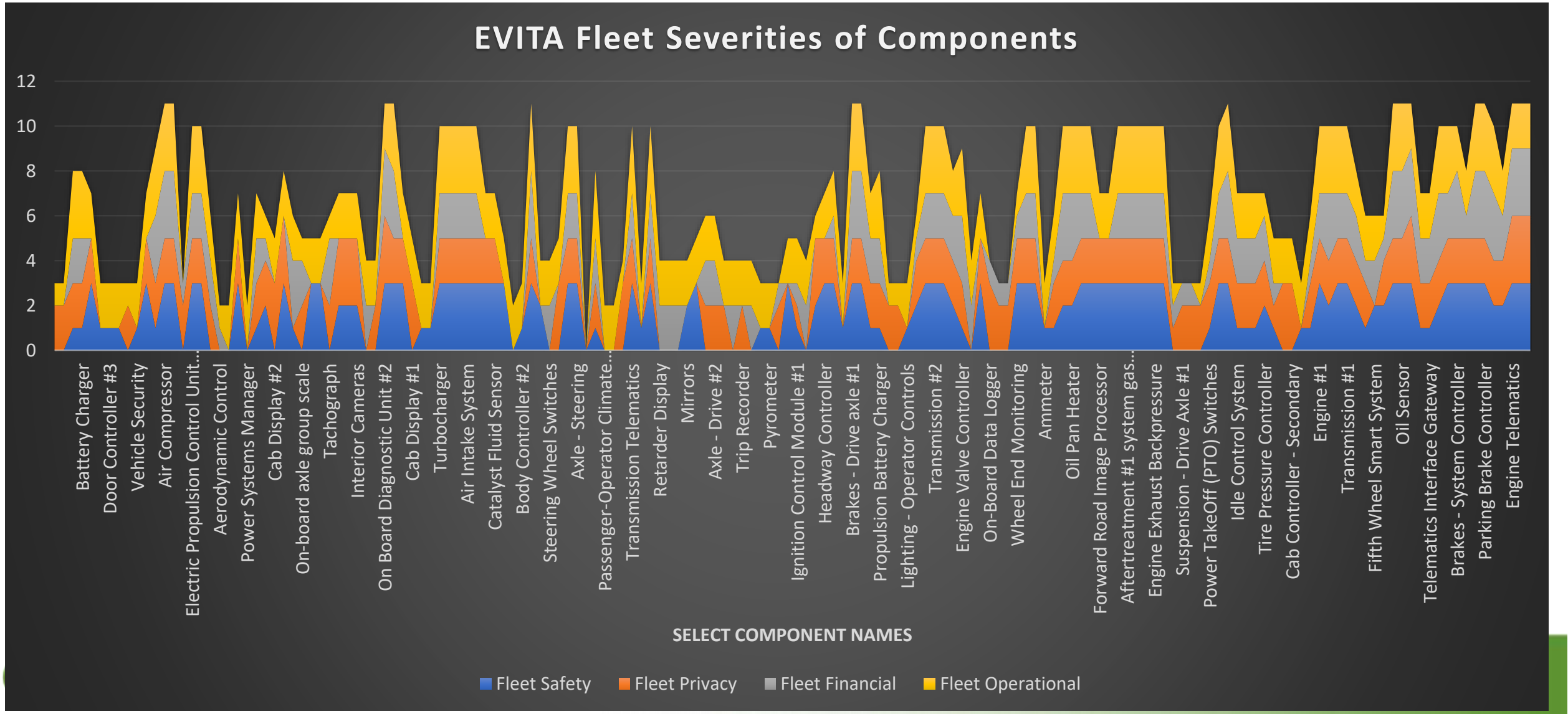
Fleet Impacts

- We elected to follow (in the spirit of) EVITA 4 possible impacts with 5 severities each Combined with attack success likelihood
- We interviewed fleet participants and extracted severities for successful attacks.

H	AH	AI	AJ	AK	AM	AN	AO	AP	AQ	AR
	Fleet Estimated Severities				Derived Risks					
	Class	Safety	Privacy	Financial	Operational	Assuming all events are controllable (C=1)					
	S0	No injuries.	No data access.	No financial loss.	No impact on operation.	Weights for "Total Risk"					
	S1	Light/moderate injuries.	Anonymous data only (no specific user or vehicle data).	Low level loss (~€10).	Impact not discernible to driver.	1	1	1	1	1	
	S2	Severe injuries (survival probable). Moderate injuries for multiple units.	Vehicle specific data (vehicle or model). Anonymous data for multiple units.	Moderate loss (~€100). Low losses for multiple units.	Driver aware. Not discernible in multiple units.						
	S3	Life threatening or fatal injuries. Severe injuries for multiple units.	Driver identity compromised. Vehicle data for multiple units.	Heavy loss (~€1000). Multiple moderate loss.	Significant impact. Multiple units with driver aware.						
	S4	Fatal for multiple vehicles.	Driver identity access for multiple units.	Multiple heavy losses.	Significant impact for multiple units.						
Matrix Default Name	Fleet Safety	Fleet Privacy	Fleet Financi	Fleet Operation	(EVITA) Fleet Safety Risk	(EVITA) Fleet Privacy Risk	(EVITA) Fleet Financial Risk	(EVITA) Fleet Operations Risk	Scope Change Risk (assumed S3)	Fleet Total Risk
Engine Telematics	3	3	3	2	4	4	4	3	4	20
OEM Telematics	3	3	3	2	4	4	4	3	4	20
Onboard Diagnostics Connector Gateway	3	3	3	2	4	4	4	3	4	20
Tractor/Trailer Bridge #2	2	2	2	2	4	4	4	4	5	19
Thermal Management System Controller	2	2	3	3	3	3	4	4	4	19
Antilock Brake System (ABS)	3	2	3	3	4	3	4	4	4	18

NMFTA
National Motor Freight Traffic Association, Inc.

Fleet Impacts



Probability of Events

- The goal was to sort and group the devices. We assumed all devices had everything else equal (e.g. security assurance/code quality)
- Leaving the biggest factor in successful attack probability: connectivity
- Attacks could come from many points of connection
- OEMs each gave their own degrees of freedom estimates for each point of connection
- We created a probability index substitute for EVITA based on the minimum degree of separation from the OEM responses

Successful Attack Probability

For each component:

$$\frac{1}{S}\sum_{\text{'conn pts'}} \max\left\{0, M - \min_{\text{'OEM responses'}} \text{'deg from conn pt'}\right\}$$

, where *M* is the degrees sufficient to be ‘safe’: **2**

and *S* was selected to scale the index to EVITA’s expected [0,5]: **2.4**

NB: uniform weighting – WG decided all connection points are of equal concern

EVITA Risk Calculation (modified)

- We were able to get severities from fleets; they weren't ready to comment on controllability
- ⏭ assumed C=1 throughout

- Risks were calculated for all four impacts: Financial, Operational, Safety, Privacy
- And an additional risk we added: Scope change risk. Created as an additional S3.
- Then summed all 5 for 'total risk.'

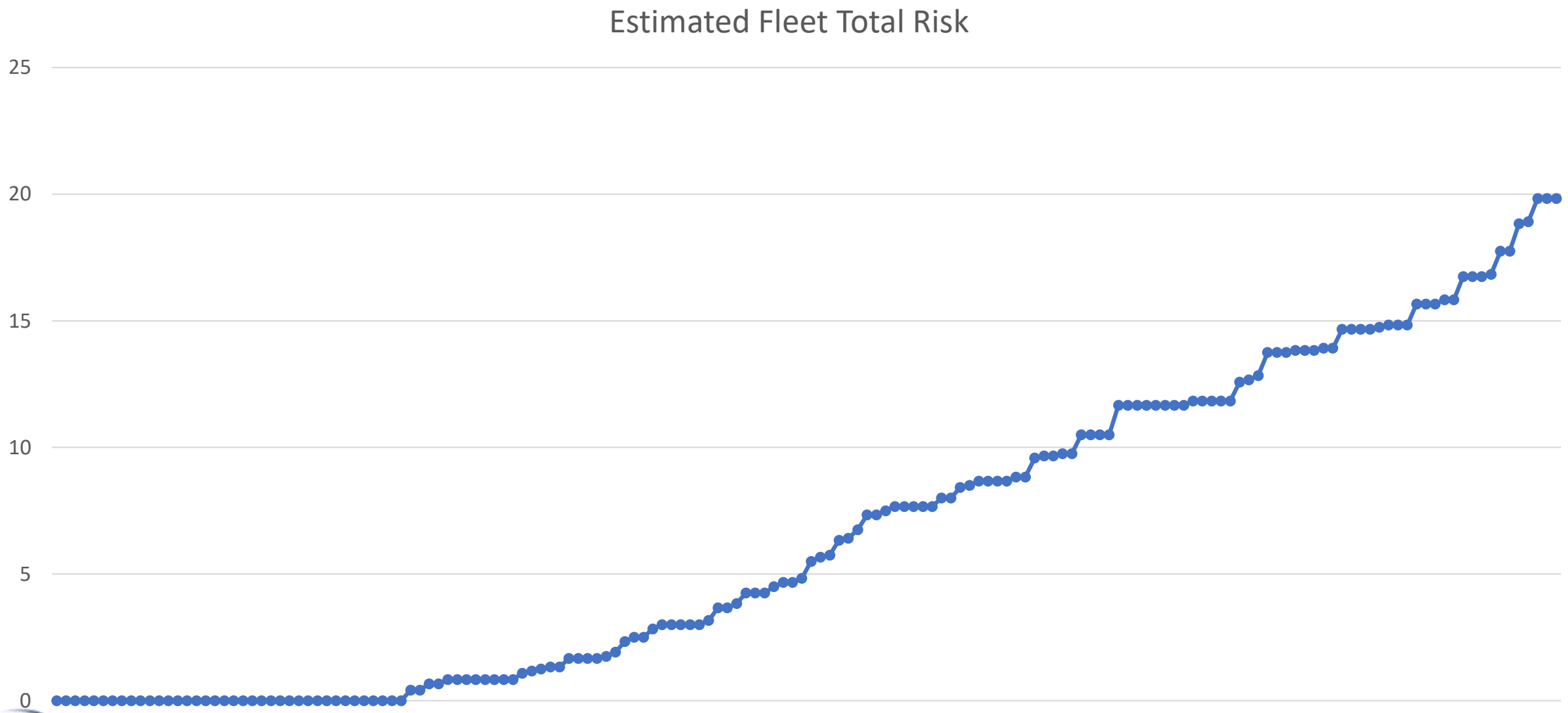
Non-safety aspects addressed with table for controllability C=1 (C>1 only for safety issues)

Controllability	Severity (S_i)	Combined Attack Method Probability (A)				
		1	2	3	4	5
C=1	S_i=1	R0	R0	R1	R2	R3
	S_i=2	R0	R1	R2	R3	R4
	S_i=3	R1	R2	R3	R4	R5
	S_i=4	R2	R3	R4	R5	R6
C=2	S_S=1	R0	R1	R2	R3	R4
	S_S=2	R1	R2	R3	R4	R5
	S_S=3	R2	R3	R4	R5	R6
	S_S=4	R3	R4	R5	R6	R7

https://www.evita-project.org/Publications/Rud10.pdf

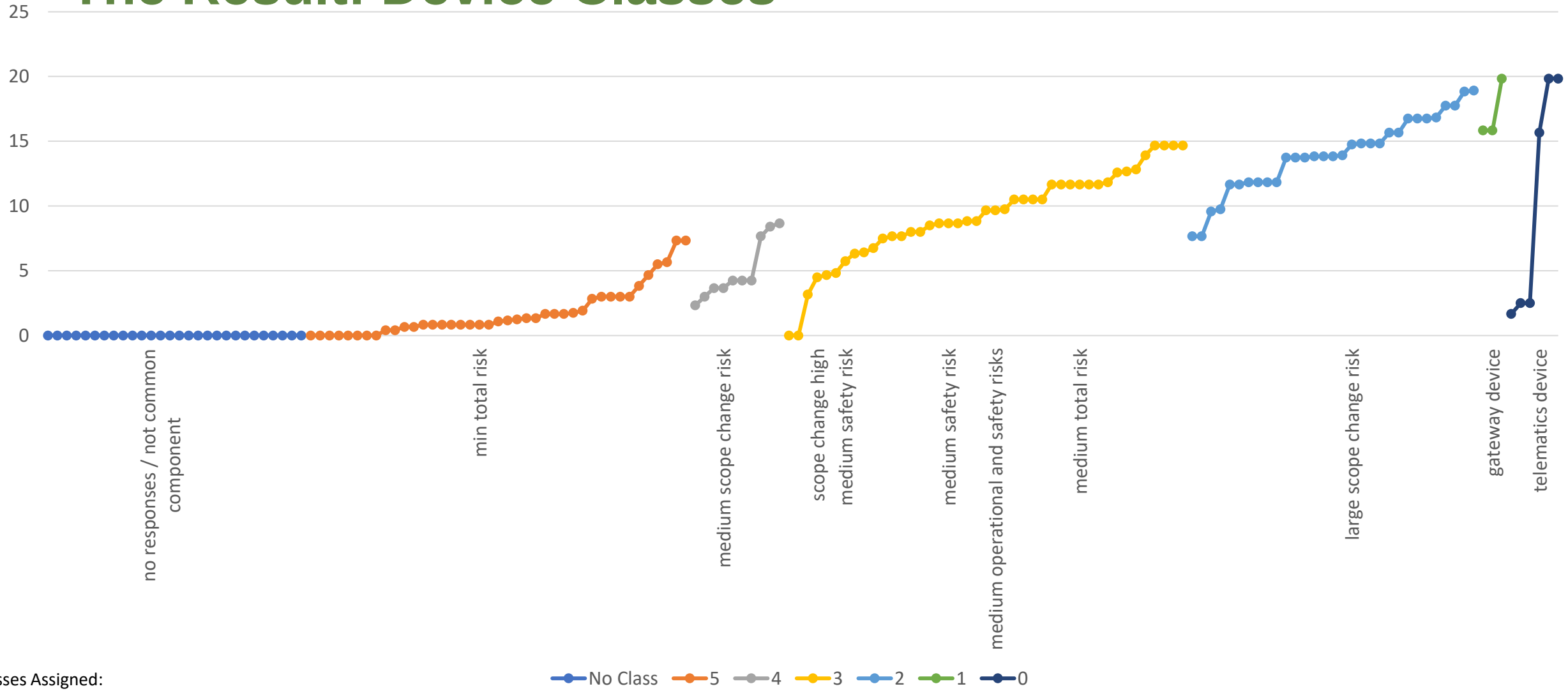
NMFTA National Motor Freight Traffic Association, Inc.

Device Risks



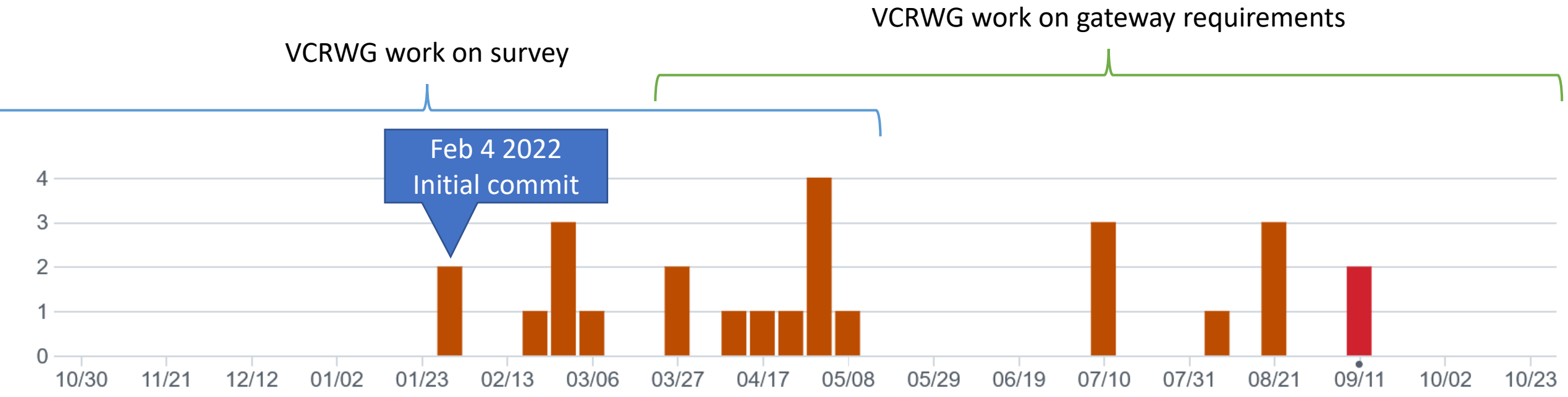
NMFTA
National Motor Freight Traffic Association, Inc.

The Result: Device Classes



NMFTA
National Motor Freight Traffic Association, Inc.

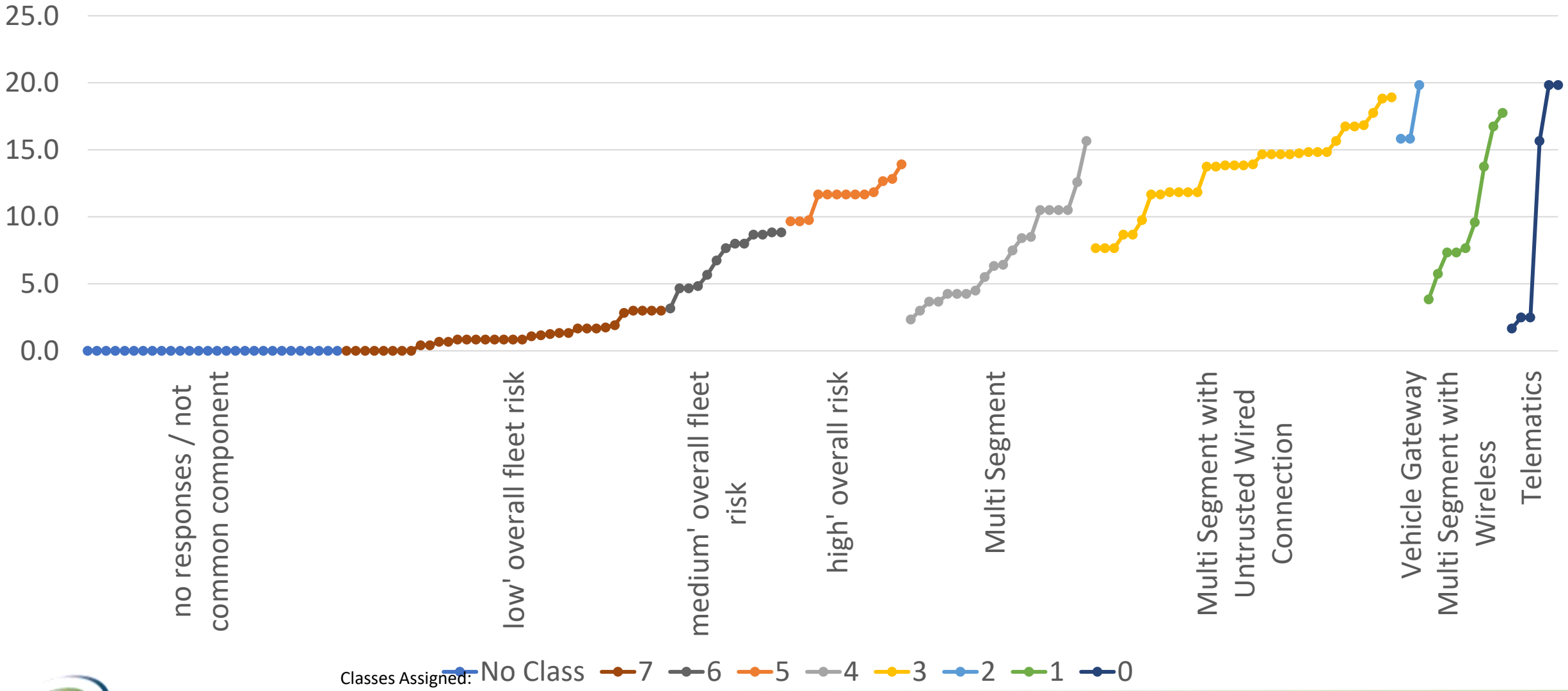
Work Continued; Classes Refined



Commits to https://github.com/nmfta-repo/nmfta-vehicle_cybersecurity_requirements

NMFTA
National Motor Freight Traffic Association, Inc.

The Result: Device Classes



NMFTA
National Motor Freight Traffic Association, Inc.

Requirements Management

NMFTA
National Motor Freight Traffic Association, Inc.

History: TSRM Management in Excel

The WG for the TSRM:

- Created 77 unique cybersecurity requirements
- …With their own public references
- …With their own V&V steps
- …Over a few years
- …All in an excel sheet (maintained by yours truly)

TSRM Management in Excel !!!

NMFTA
National Motor Freight Traffic Association, Inc.

TSRM Management in Excel

The release process for the TSRM is manual

A. Update the printable form
B. Unhide some columns in the questionnaires
C. Sort
D. Add/remove rows
E. Unsort
F. Re-hide columns
G. Save + Close

OSS Requirements Management: Doorstop and Strictdoc

- Doorstop is a free version developed to work in the spirit of DOORS
  - 👎One file per requirement
  - ✅Text-based requirements
- Strictdoc (started as a doorstop fork) has the same function
  - ✅ One file per document
  - ✅ Text-based requirements
  - ✅ Requirement interchange export & export
  - ✅ Requirement Coverage
  - ✅ Browsable Docs
  - 👎Beta maturity software

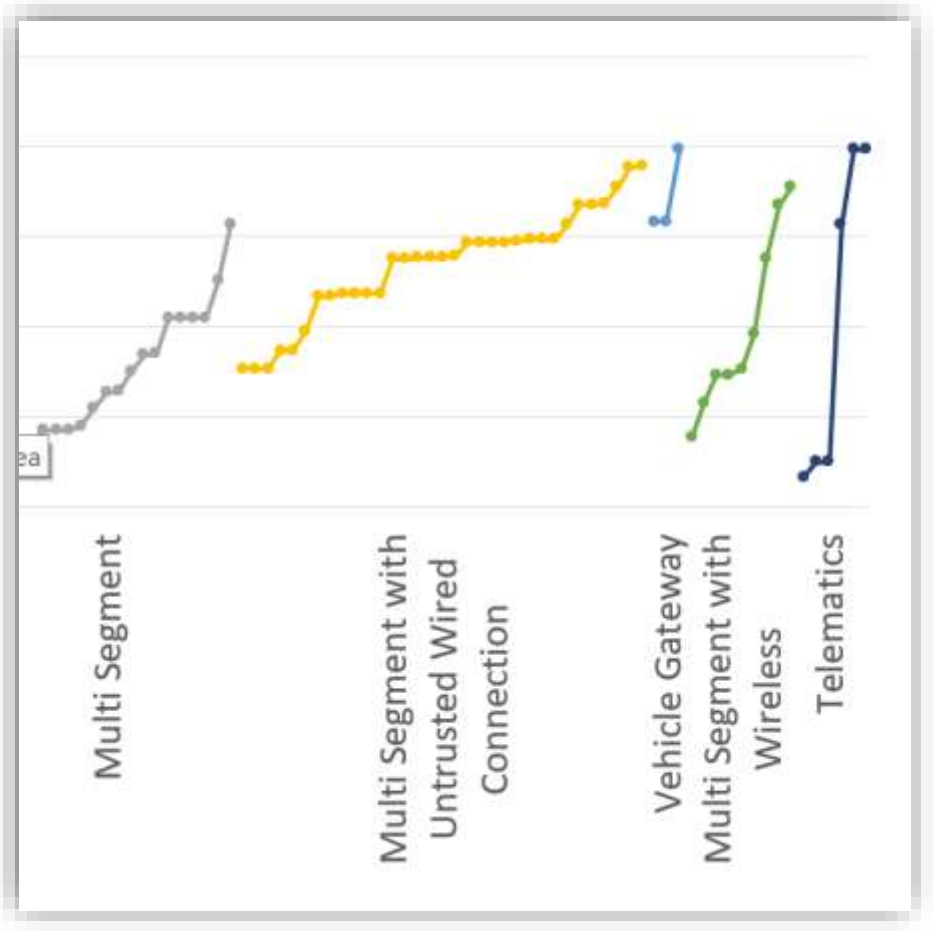
Trying-out Strictdoc

The vcr-experiment

NMFTA
National Motor Freight Traffic Association, Inc.

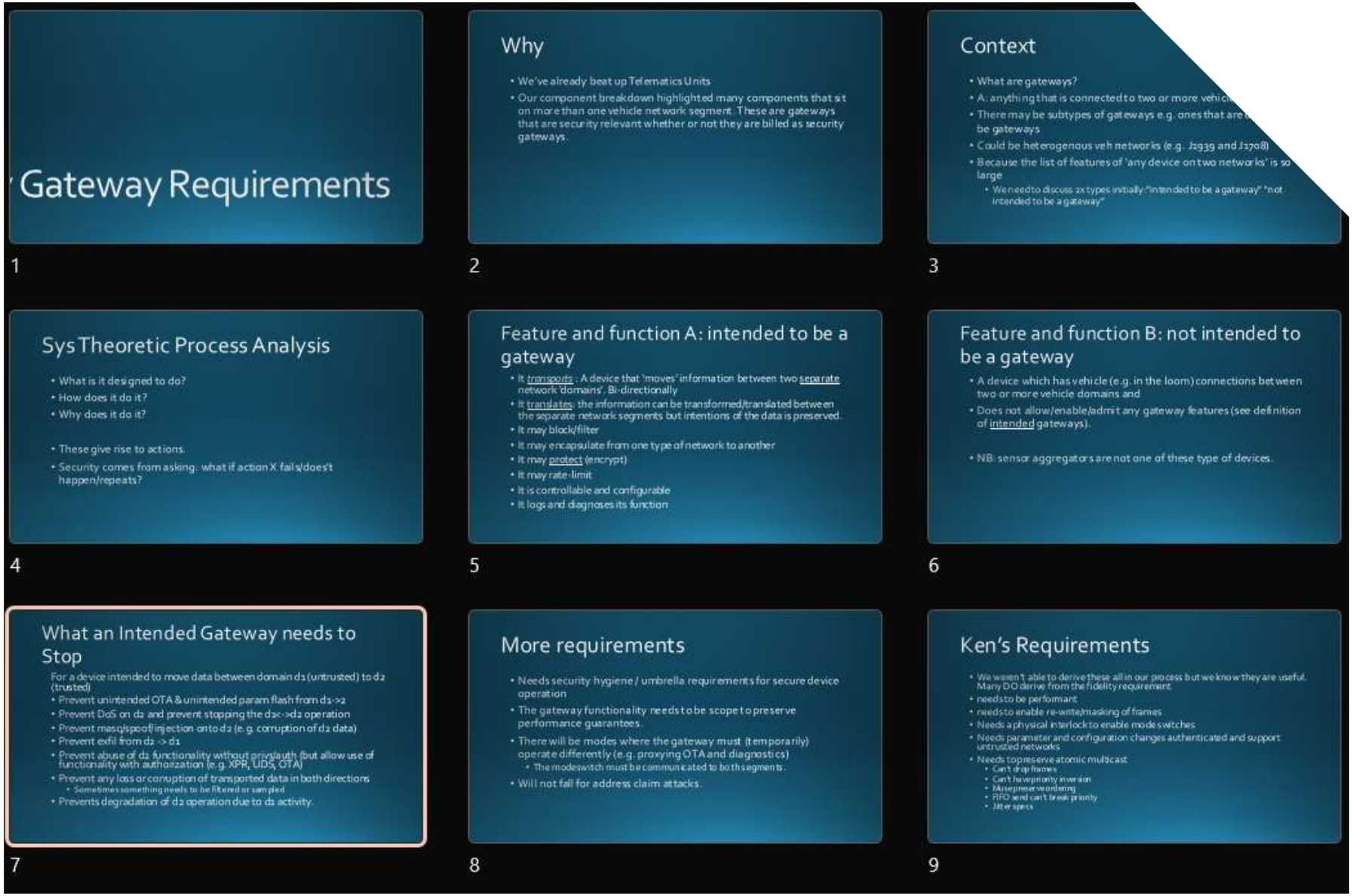
The next biggest risk: Gateway Devices

- Both in terms of next logical attack step AND
- modeled risks:
- NB: both intended gateways and unintended gateways are the next biggest risk



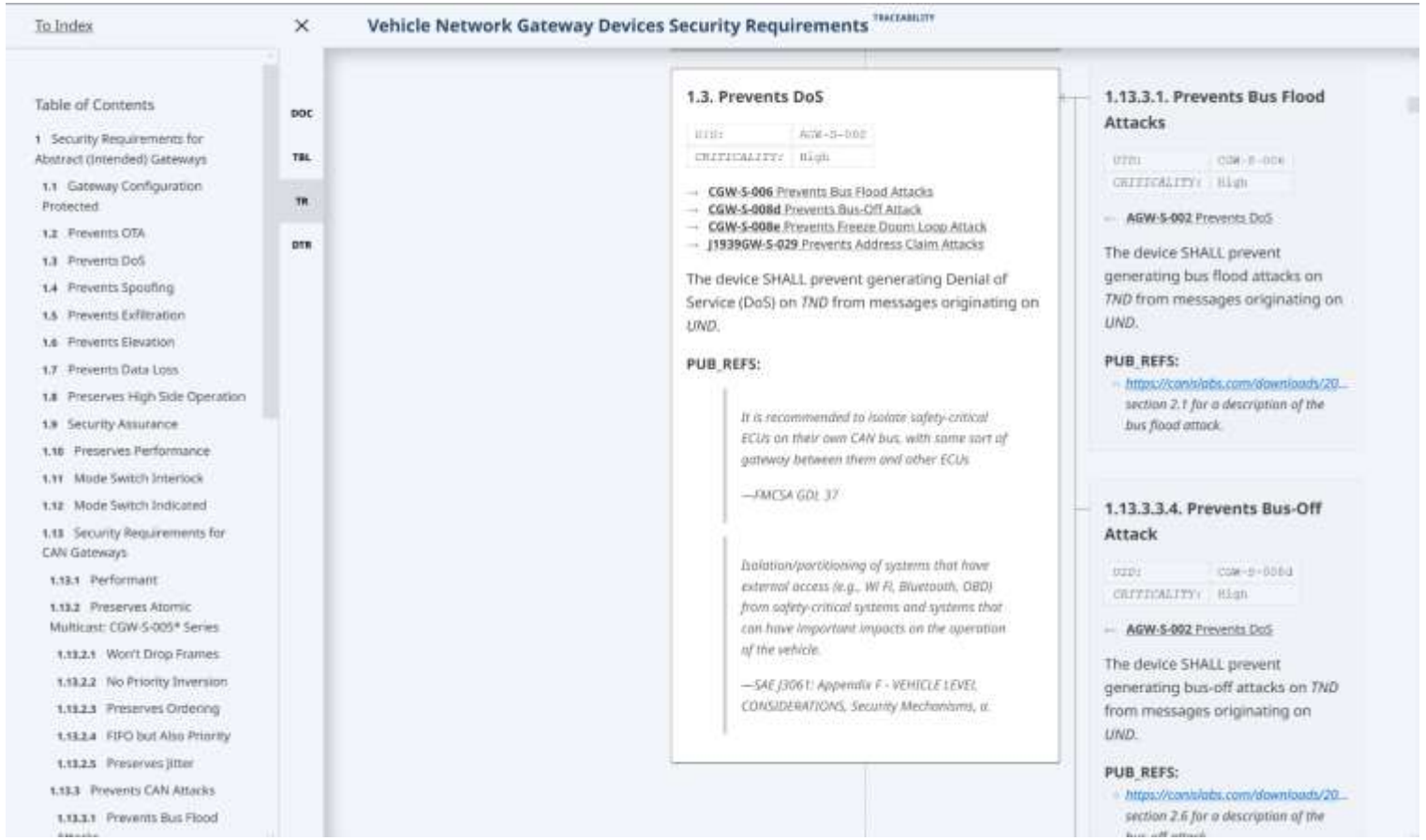
CTSRP Workshop Nov 2021 Breakout Session

- 1 hr (only) session with ~ ½ of the workshop's ~60 attendees
- Discussed and tried to answer:
  - Definitions: gateways, unintended and intended, trust domains, untrusted domains
  - Features/functions of an intended gateway
  - Of an un-intended gateway: security requirement that it will not perform any gateway functions
  - Security requirements of intended gateways
- While I furiously took notes and prepared a deck for return session
- We also luckily had a presentation on security gateway devices earlier that day (from Dr. Ken Tindell of Canis Labs)

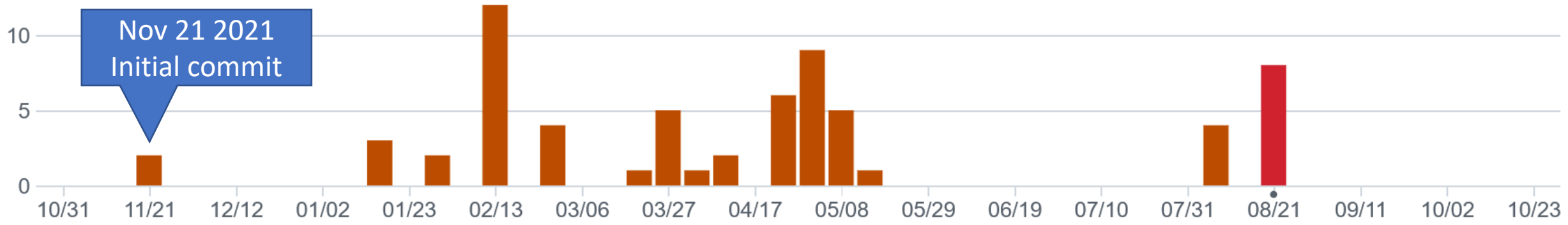

Gateway Requirements
1
Why
• We've already beat up Telematics Units
• Our component breakdown highlighted many components that sit on more than one vehicle network segment. These are gateways that are security relevant whether or not they are billed as security gateways.
2
Context
• What are gateways?
• A: anything that is connected to two or more vehi
• There may be subtypes of gateways e.g. ones that are
be gateways
• Could be heterogenous veh networks (e.g. J1939 and J1708)
• Because the list of features of 'any device on two networks' is so large
• We need to discuss 2x types initially: "intended to be a gateway" "not intended to be a gateway"
3
Sys Theoretic Process Analysis
• What is it designed to do?
• How does it do it?
• Why does it do it?
• These give rise to actions.
• Security comes from asking: what if action X fails/does't happen/repeats?
4
Feature and function A: intended to be a gateway
• It transports : A device that 'moves' information between two separate network 'domains'. Bi-directionally
• It translates: the information can be transformed/translated between the separate network segments but intentions of the data is preserved.
• It may block/filter
• It may encapsulate from one type of network to another
• It may protect (encrypt)
• It may rate-limit
• It is controllable and configurable
• It logs and diagnoses its function
5
Feature and function B: not intended to be a gateway
• A device which has vehicle (e.g. in the loom) connections between two or more vehicle domains and
• Does not allow/enable/admit any gateway features (see definition of intended gateways).
• NB: sensor aggregators are not one of these type of devices.
6
What an Intended Gateway needs to Stop
For a device intended to move data between domain d1 (untrusted) to d2 (trusted)
• Prevent unintended OTA & unintended param flash from d1->2
• Prevent DoS on d2 and prevent stopping the d2<->d2 operation
• Prevent masq/spoof/injection onto d2 (e.g. corruption of d2 data)
• Prevent exfil from d2 -> d1
• Prevent abuse of d2 functionality without privsauth (but allow use of functionality with authorization (e.g. XPR, UDS, OTA)
• Prevent any loss or corruption of transported data in both directions
• Sometimes something needs to be filtered or sampled
• Prevents degradation of d2 operation due to d1 activity.
7
More requirements
• Needs security hygiene / umbrella requirements for secure device operation
• The gateway functionality needs to be scope to preserve performance guarantees.
• There will be modes where the gateway must (temporarily) operate differently (e.g. proxying OTA and diagnostics)
• The mode switch must be communicated to both segments.
• Will not fail for address claim attacks.
8
Ken's Requirements
• We weren't able to derive these all in our process but we know they are useful. Many DO derive from the fidelity requirement
• needs to be performant
• needs to enable re-write/masking of frames
• Needs a physical interlock to enable mode switches
• Needs parameter and configuration changes authenticated and support untrusted networks
• Needs to preserve atomic multicast
• Can't drop frames
• Can't have priority inversion
• Must preserve ordering
• FIFO send can't break priority
• Jitter specs
9

The vcr-experiment

- We took what was discussed in the breakout session and captured it as a strictdoc
- And kept refining it
- https://github.com/nmfta-repo/vcr-experiment



vcr-experiment commits



Commits to https://github.com/nmfta-repo/vcr-experiment

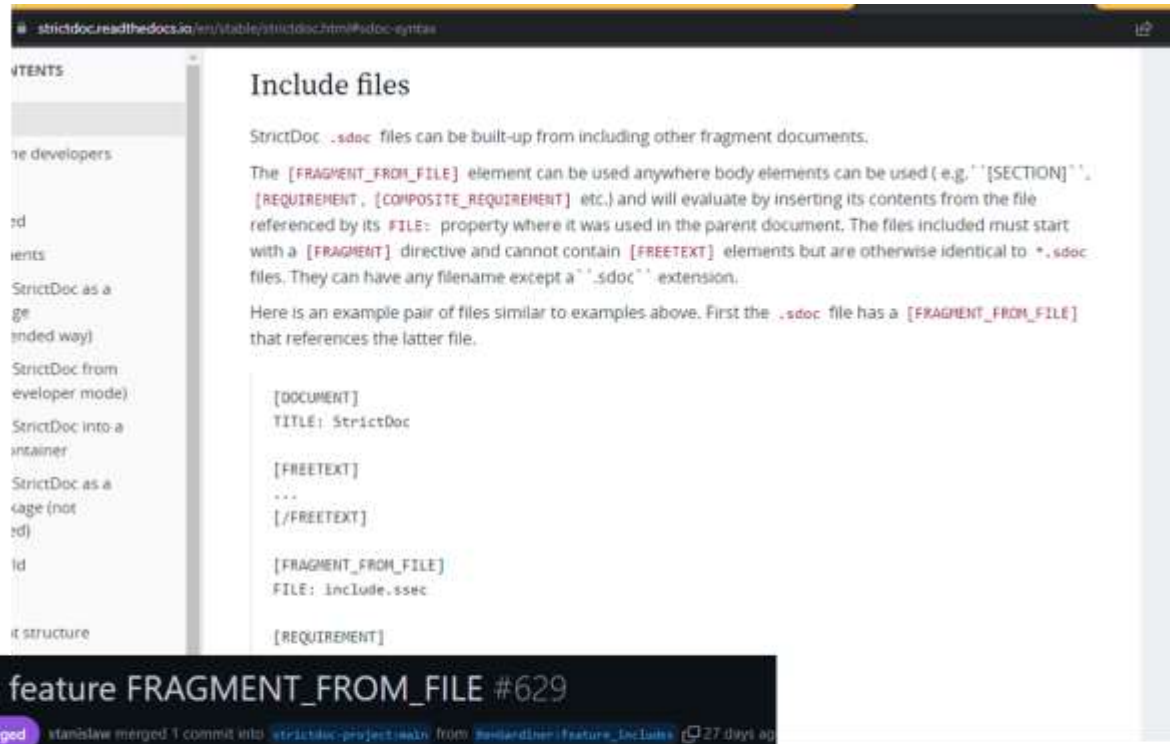
NMFTA
National Motor Freight Traffic Association, Inc.

Re-working the Requirements: How to Model?

- After some refinement and WG meetings…
- We had requirements where an abstract (goal) requirement must have all the more-concrete requirements satisfied : all-of
- We had requirements where an abstract requirement could be satisfied by one or more concrete requirements: one-of
- Not clear how to model this in strictdoc.
- Plus capturing them in a ReqIF exportable form would be best
- ReqIf does not have a way to model all-of/one-of children requirements. It has only parent-child; therefore we need to capture all-of children or one-of children in the text.

Strictdoc feature: Include Files

- We added an include file feature for re-use of requirements document fragments



NMFTA
National Motor Freight Traffic Association, Inc.

Strictdoc feature: Excel

- We added excel import so that we could re-use the TSRM Excel held requirements.

- We also made a mostly automated TSRM import script and captured the result in vcr-experiment for now.

Importing the TSRM into vcr-experiment

- Using the excel importer
- Create a main requirements file and
- One ‘stub’ for each applies-to component: Cloud, Communication, Mobile, Vehicle
  - Stub requirements are just ‘must satisfy XXX’ with parent XXX

NMFTA
National Motor Freight Traffic Association, Inc.

Canis Labs Gap Analysis

- Canis Labs has developed CAN security gateways with a great deal of thought into preserving CAN atomic multicast property and security requirements also
- Ken Tindell of Canis Labs has participated in the WG since the breakout session and
- Canis Labs has performed requirements coverage/gap analysis of the current vcr-experiment requirements and the Canis Labs security gateway:

https://kentindell.github.io/assets/docs/2201 2022-03-22 36507b1b09a6dd9cdbc07c4e0686c4b16ed8a1a0d317726ccc9e3cc3060a4e39.pdf

Demo of vcr-experiment Strictdoc Documentation

NMFTA
National Motor Freight Traffic Association, Inc.

Current NMFTA Vehicle Cybersecurity Requirements (VCR) status

NMFTA
National Motor Freight Traffic Association, Inc.

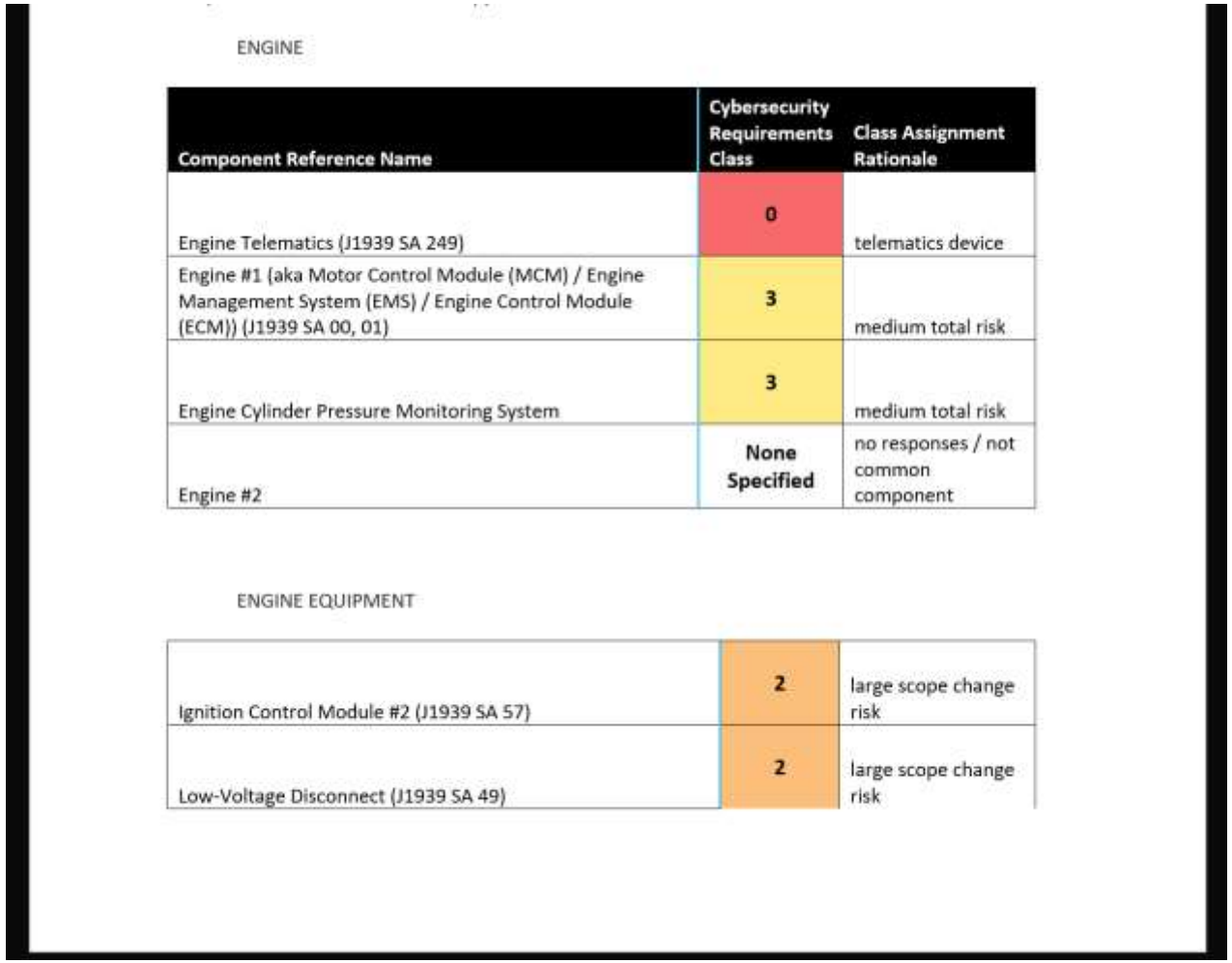
Network Topology Survey and Risk Analysis

- All the survey results from OEMs collected
- Basic risk analysis and device classification
- Could be improved too:
  - More impact input from fleets
  - More vehicle survey results from OEMs
- Note: can be used to run analysis of a particular vehicle to compare against this classification

NMFTA
National Motor Freight Traffic Association, Inc.

Order Sheet View

- We've re-organized the device classification into a document with the order sheet lines as the categorization.
- Since order sheets are the primary way to spec trucks we hope this is the most useful format for fleets.



ENGINE

Component Reference Name	Cybersecurity Requirements Class	Class Assignment Rationale
Engine Telematics (J1939 SA 249)	0	telematics device
Engine #1 (aka Motor Control Module (MCM) / Engine Management System (EMS) / Engine Control Module (ECM)) (J1939 SA 00, 01)	3	medium total risk
Engine Cylinder Pressure Monitoring System	3	medium total risk
Engine #2	None Specified	no responses / not common component

ENGINE EQUIPMENT

Ignition Control Module #2 (J1939 SA 57)	2	large scope change risk
Low-Voltage Disconnect (J1939 SA 49)	2	large scope change risk

Class Heuristics View

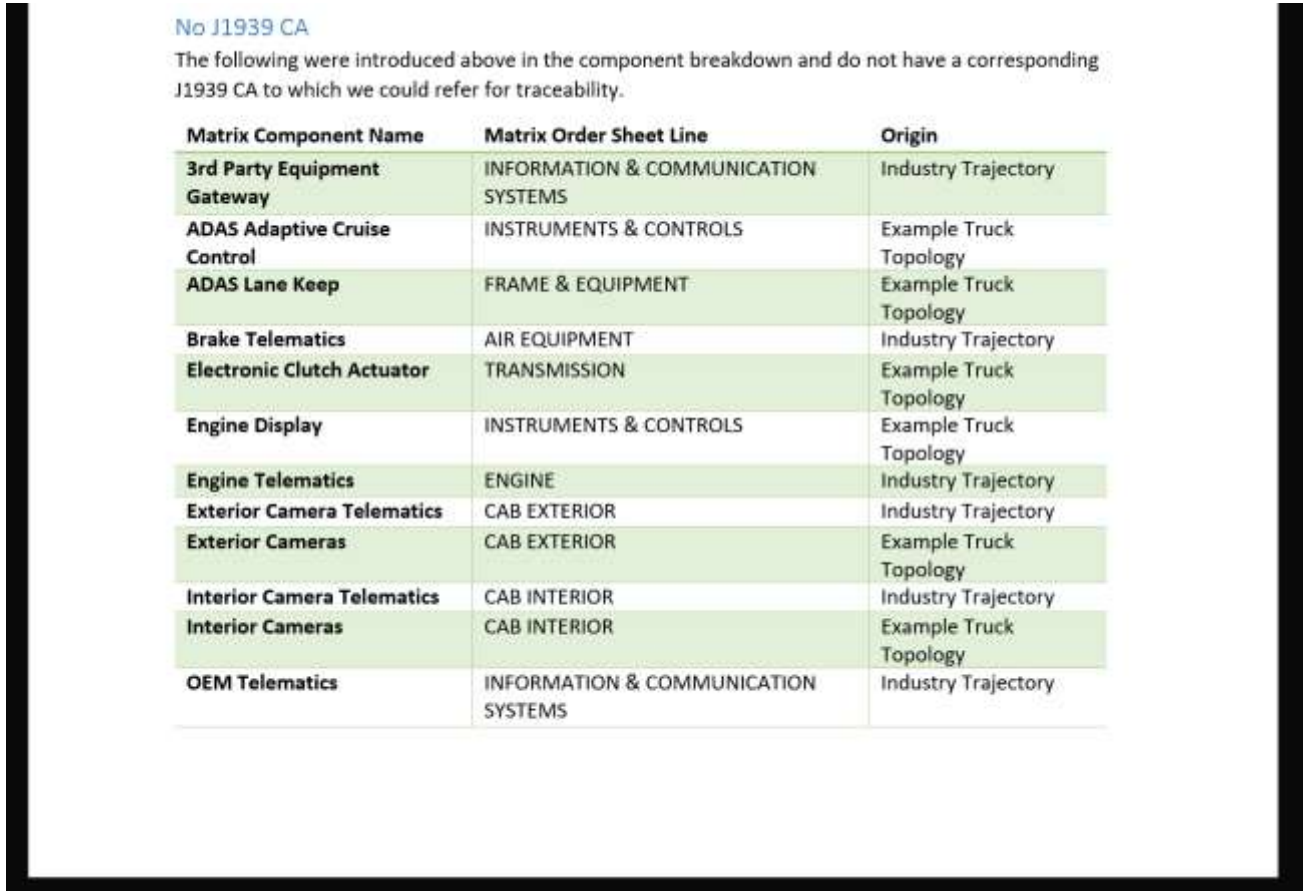
- It’s possible that a during fleet-OEM discussions there is a component which has not already been analyzed or classified.
- We provide heuristics (rules) to apply to classify a device in those cases

Class	Devices	Heuristic
0 Telematics	...	Components of a telematics system or truck modules that otherwise connect to cellular, satellite or other Wide Area Networks (WANs), or the internet
1 Multi Segment with Wireless	...	Truck modules that may or may not be intended to perform gateway functions (transport, translate, transform, filter or encapsulate data) and has at least one wireless interface
2 Vehicle Gateway	...	Truck modules intended to perform gateway functions (transport, translate, transform, filter or encapsulate data) between two or more vehicle network segments
3 Multi Segment with Untrusted Wired Connection	...	Truck modules that are not intended to be Vehicle Gateways but nonetheless are connected to two or more vehicle network segments where one or more of those segments are untrusted.

Other Resources: Component Names

There were, however, lots of incongruencies in names which we documented

- Components that aren't named at all in the most recent J1939 DA
- Components which have more common industry names (aliases) than the DA captures
- Duplicated components within the DA
- (we also documented all the J1939 components which we did not analyze because they were outside the truck matrix scope of North American Class 7+8)



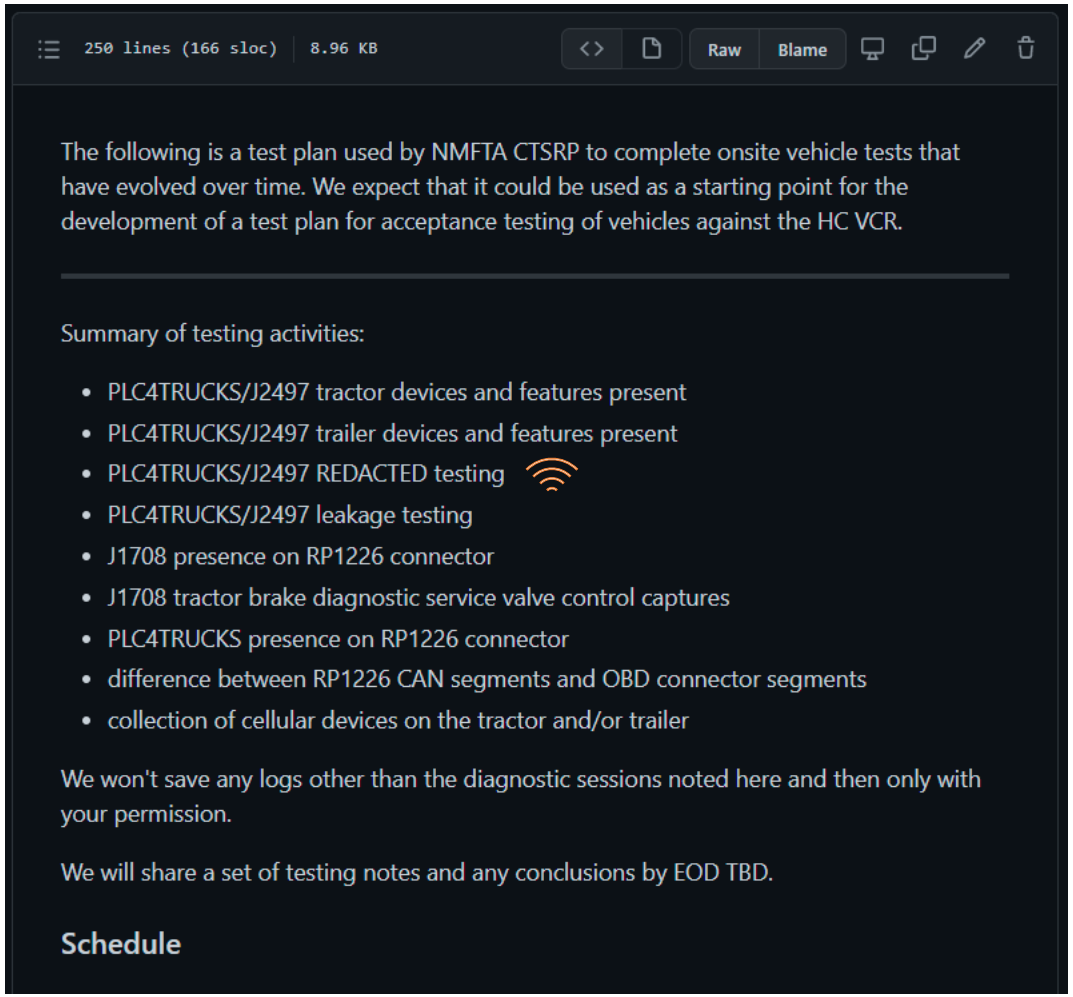
No J1939 CA

The following were introduced above in the component breakdown and do not have a corresponding J1939 CA to which we could refer for traceability.

Matrix Component Name	Matrix Order Sheet Line	Origin
3rd Party Equipment Gateway	INFORMATION & COMMUNICATION SYSTEMS	Industry Trajectory
ADAS Adaptive Cruise Control	INSTRUMENTS & CONTROLS	Example Truck Topology
ADAS Lane Keep	FRAME & EQUIPMENT	Example Truck Topology
Brake Telematics	AIR EQUIPMENT	Industry Trajectory
Electronic Clutch Actuator	TRANSMISSION	Example Truck Topology
Engine Display	INSTRUMENTS & CONTROLS	Example Truck Topology
Engine Telematics	ENGINE	Industry Trajectory
Exterior Camera Telematics	CAB EXTERIOR	Industry Trajectory
Exterior Cameras	CAB EXTERIOR	Example Truck Topology
Interior Camera Telematics	CAB INTERIOR	Industry Trajectory
Interior Cameras	CAB INTERIOR	Example Truck Topology
OEM Telematics	INFORMATION & COMMUNICATION SYSTEMS	Industry Trajectory

Other Resources: Truck Testing Plan

- We hope to have fleet-testable requirements.
- To that end we have committed our heavy vehicle testing plan to the repo to serve as a seed for hosting the eventual test plan corresponding to the vehicle security requirements.



250 lines (166 sloc) | 8.96 KB

Raw Blame

The following is a test plan used by NMFTA CTSRP to complete onsite vehicle tests that have evolved over time. We expect that it could be used as a starting point for the development of a test plan for acceptance testing of vehicles against the HC VCR.

Summary of testing activities:

- PLC4TRUCKS/J2497 tractor devices and features present
- PLC4TRUCKS/J2497 trailer devices and features present
- PLC4TRUCKS/J2497 REDACTED testing
- PLC4TRUCKS/J2497 leakage testing
- J1708 presence on RP1226 connector
- J1708 tractor brake diagnostic service valve control captures
- PLC4TRUCKS presence on RP1226 connector
- difference between RP1226 CAN segments and OBD connector segments
- collection of cellular devices on the tractor and/or trailer

We won't save any logs other than the diagnostic sessions noted here and then only with your permission.

We will share a set of testing notes and any conclusions by EOD TBD.

Schedule

NMFTA
National Motor Freight Traffic Association, Inc.

Next Steps

Still TODO

In vcr-experiment:

- Capture fleet acceptance tests for each of the requirements, just like the TSRM
- Publish an interim report on this work and the requirement details

In nmfta-vehicle_cybersecurity_requirements: (over)

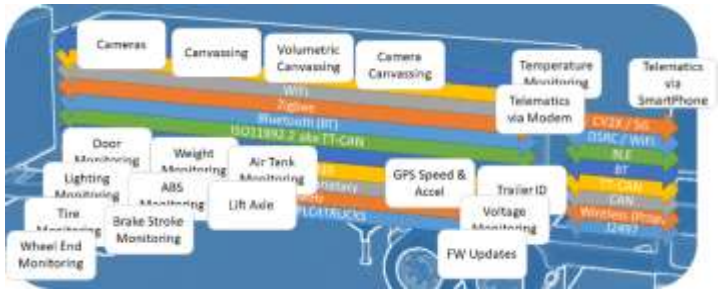
Expand to a Coherent and Comprehensive Set

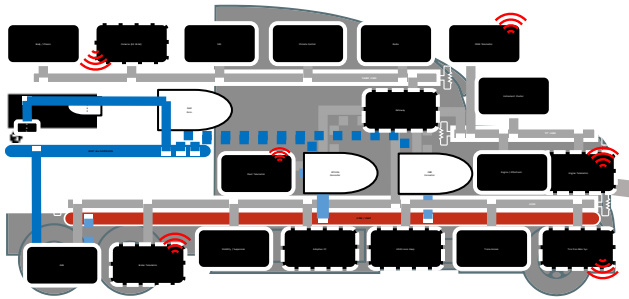
- We have a comprehensive set of telematics requirements
- We have a comprehensive set of gateway requirements
- We can abstract/extract many from those to apply to all vehicle components BUT
- We know more will be needed.
- This is the biggest part of the next steps and with the most unknowns

Iterate and Refine the “How to Use” with Fleets

- We’ve outlined a process that we think will work during fleet procurement of equipment
- The ‘discovery of device classes’ part of the process needs the most development

- It is of paramount importance that this is useful to the fleets
- We must get a trial run of this process and/or fleet feedback on how to enable uptake of the requirements into their equipment purchasing





OEM

Components and Classes

Discovery Questions

Procurement

RFP

OEM

RFP-Response

Questionnaire

Eval. Table

Eval. Table

Eval. Table

Cybersecurity Requirements Matrix

TEMPLATE Request for Proposals

Procurement Expert

TEMPLATE Proposals Assessment

Cybersecurity Requirements Matrix

Eval

OEM

Fleet

VCRWG Artifacts

NMFTA
National Motor Freight Traffic Association, Inc.

Conclusions

Observations Along the Way

- OSS requirements management and exchange is in a workable state thanks to strictdoc
- There are a lot of different names for vehicle components
- The SAE controller application names don’t capture all the obvious candidates on a modern truck
- There are many un-gatewayed components on a modern truck
- Gatewaying CAN (and probably any other control loop path vehicle network) is not just a firewall

Deliverables So Far

1. Picture of a ‘typical’ class 8 truck network architecture
2. List of common components and their aliases
   - Mapped to J1939 names wherever possible
3. Risk analysis of common components based on typical/average truck network architecture and fleet impact
4. Assignment of components to risk classes based on the above
   - Plus a heuristic for classifying future components
5. Draft cybersecurity requirements for vehicle network gateways and multi-segment components
   - In machine-readable (ReqIF) format
   - Plus a gap analysis of requirements against a current gateway solution
6. Heavy Vehicle Testing Plan

Next Deliverables

- Publish interim report of requirements for gateways and multi-segment components
  - PDF whitepaper and In ReqIF for easy interchange and coverage analysis
- Comprehensive vehicle component security requirements
  - In ReqIF for easy interchange and coverage analysis
  - In questionnaire format for the rest
- A ‘discovery’ process focusing on truck order sheet view and guiding the compilation of requirements/questionnaires for procurement conversations

Conclusion

Work is ongoing.

Watch this space:
github.com/nmfta-repo/nmfta-vehicle_cybersecurity_requirements

If interested in contributing, apply for membership to the working group:
ben.gardiner@nmfta.org

NMFTA
National Motor Freight Traffic Association, Inc.

Thank You

Send feedback to John.Talieri@nmfta.org

NMFTA
National Motor Freight Traffic Association, Inc.