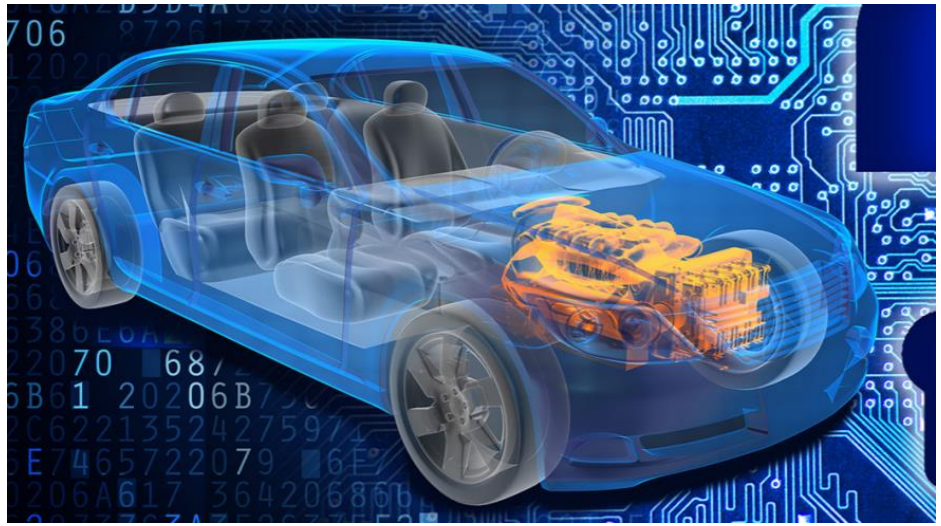
Vehicle Electronics and Cybersecurity

Research Objectives

- Support the safety assurance of vehicle electronics, software, and cybersecurity such that they do not pose public acceptance barriers for proven safety technologies and driving automation systems.
- Support improvements in the cybersecurity posture of motor vehicles, and understand and promote contemporary methods in software development, testing practices, and requirements management as they pertain to robust management of underlying hazards and risks across the vehicle life-cycle.



Research Overview

- Electronics
  - Functional Safety of Automated Driving Systems
  - Software Assurance Approaches
- Cybersecurity
  - Research to Enhance Cybersecurity Readiness
  - Research Contemporary Tools, Methods for Vehicle Cybersecurity Resiliency
  - Collaborative Research
    - Auto-ISAC, OEMS, SAE, ISO, and other government agencies.

1. Automotive Cyber Resiliency Research
2. Cybersecurity Vulnerabilities of Vehicle Sensors
3. VRTC Capabilities and Applied Cybersecurity Research
4. Heavy Vehicle Cybersecurity
5. Hazard Analysis of Heavy Truck Platooning Concepts
6. Functional Safety Research

Automotive Cyber Resiliency Research

Art Carter

Automotive Cyber Resiliency Research - Overview

- Scope
  - Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events.
  - Research the concept of cyber-resiliency, as it relates to the automotive sector.
- Objective
  - Investigate and identify strategies and methods that could enhance the containment of, response to, and recovery from cyber incidents for automotive platforms
  - Develop information and work products from industry standards and best practices, and potential testing frameworks and methods that could be leveraged in the automotive industry

Cybersecurity Vulnerabilities of Vehicle Sensors

Art Carter

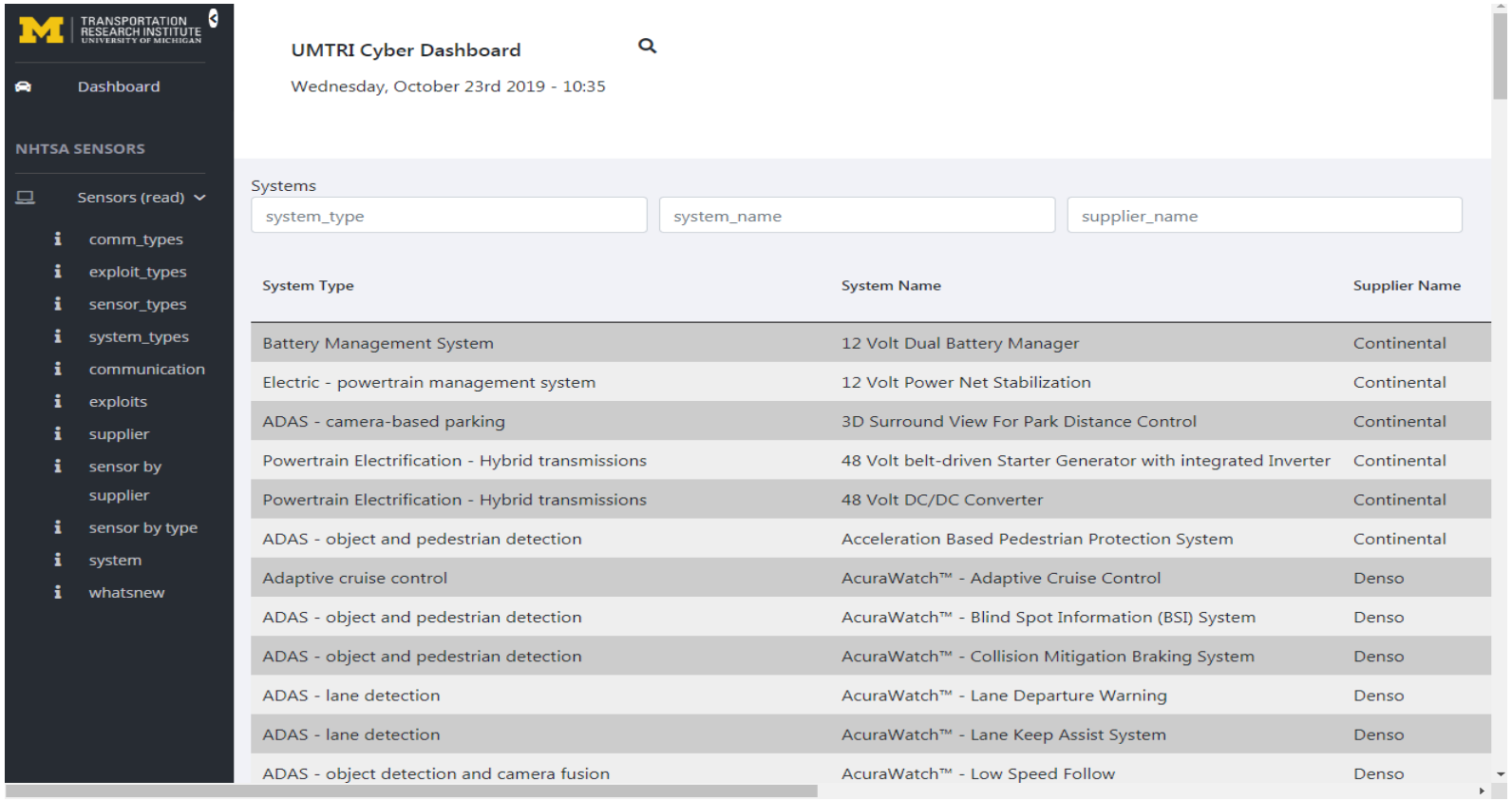
Cybersecurity Vulnerabilities of Vehicle Sensors

Project Overview

1. Identify and Categorize Sensors
   - Website + Database
   - Categorized by sensor type, supplier, usage, known exploits
2. Research & Investigate published sensor exploits
3. Test sensors for new & previously known vulnerabilities
4. Investigate controls, mitigations and countermeasures

Cybersecurity Vulnerabilities of Vehicle Sensors

1. Identify and Categorize Sensors



Website Features

- Authentication
- Database (export)
- Fully Searchable

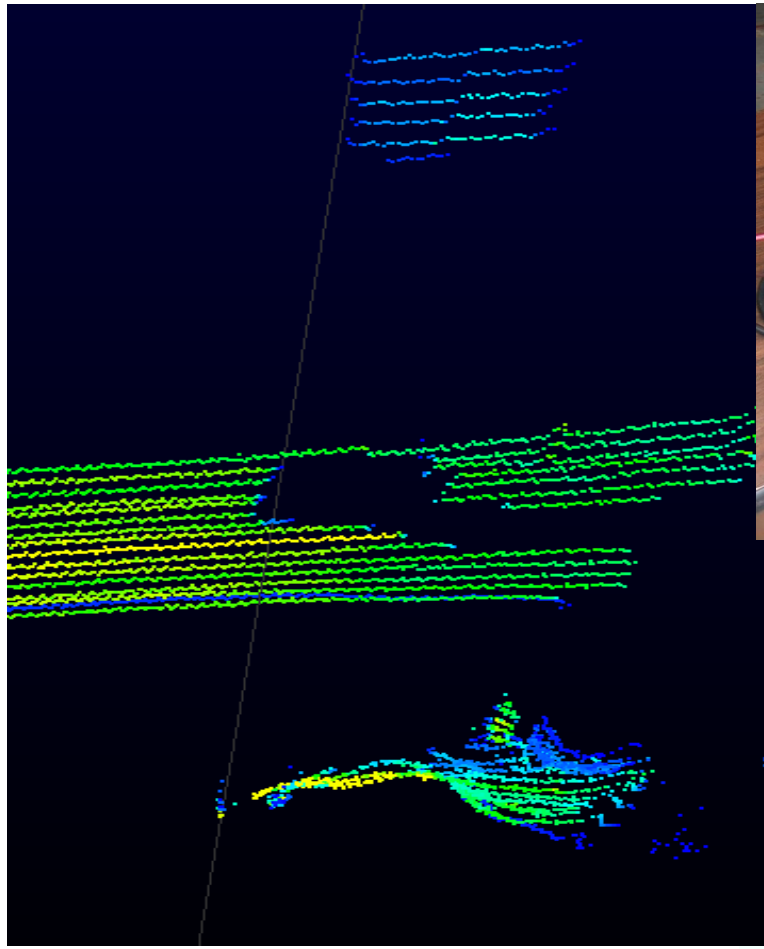
Catalogs everything sensor related from communication types to suppliers and known exploits.

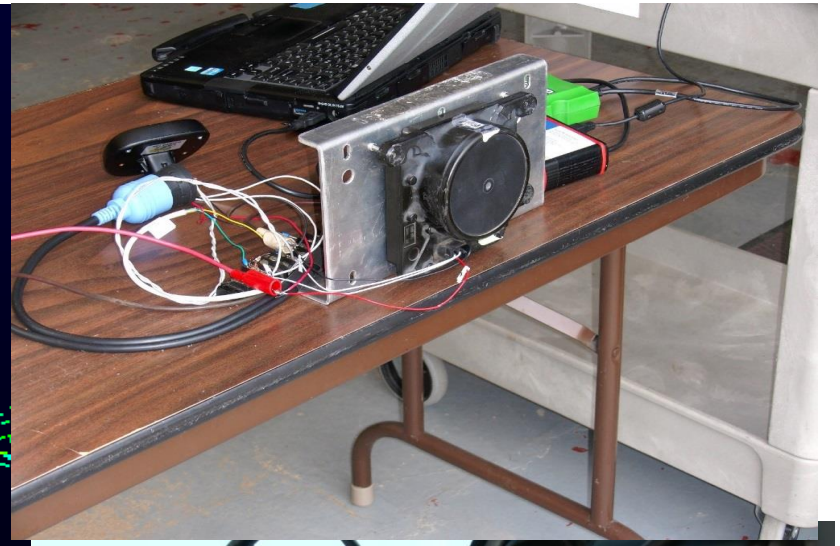
2. Investigate published sensor exploits

Added to the website.

Cybersecurity Vulnerabilities of Vehicle Sensors

3. Test sensors for new & previously known vulnerabilities





- Focus on sensor output
  i.e. the input to fusion systems
- Repeatable testing procedures

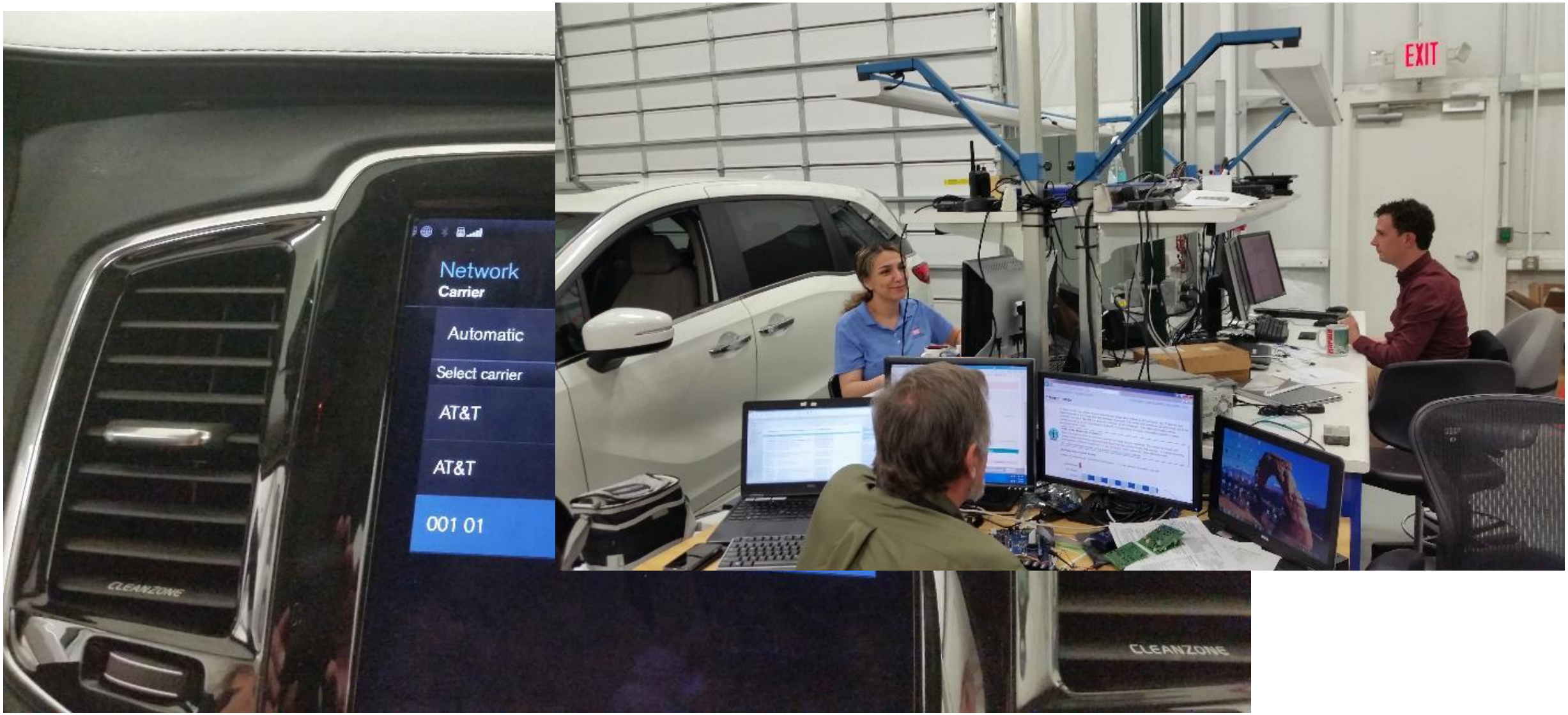
Sensors include

- Radar (24+77GHz)
- LiDAR
- Camera/Vision systems

VRTC Capabilities and Applied Cybersecurity Research

John Martin

Cybersecurity Research at VRTC



Cybersecurity Research at VRTC

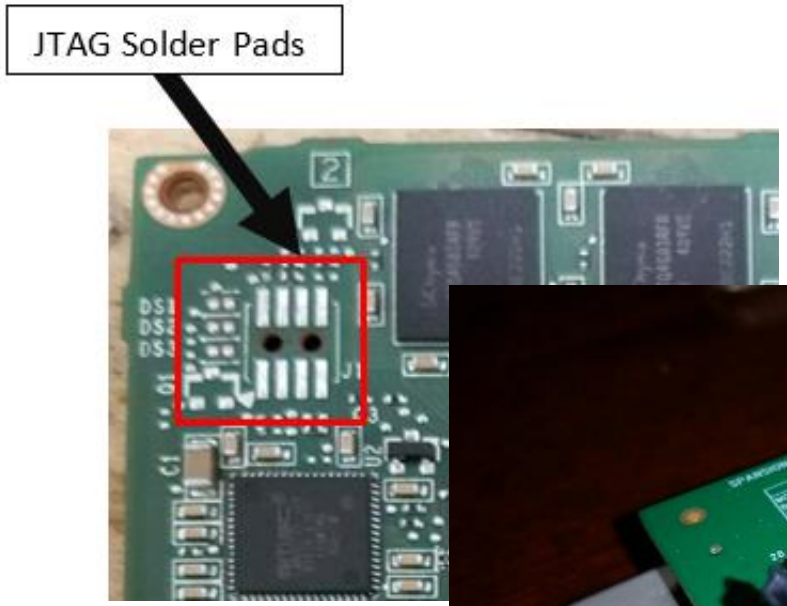
- General applied cybersecurity research goals:
  - Explore the state of vehicle cybersecurity posture by testing vehicle electronic systems and observing responses
  - Develop the internal techniques and expertise necessary to effectively test modern vehicles that are –in large- defined by the software they run
  - Establish internal independent assessments in reported vehicle cybersecurity incidents and support agency decisions.

Cybersecurity Research at VRTC

- Research
  - Performing penetration testing on a modern vehicles with a focus on wireless connection interfaces
  - Funding academic research on firmware analysis techniques
  - Funding academic research on wireless analysis tools
  - Funding academic research on developing cybersecurity metrics
- Capabilities
  - Extract firmware
  - Identify diagnostic interfaces
  - Identify open wireless interfaces
  - Analyze firmware
    - Disassemble firmware with common tools
    - Execute extracted firmware in an instrumented environment
- Connect infotainment systems to a local 2G wireless base station
- Spoof GPS signals

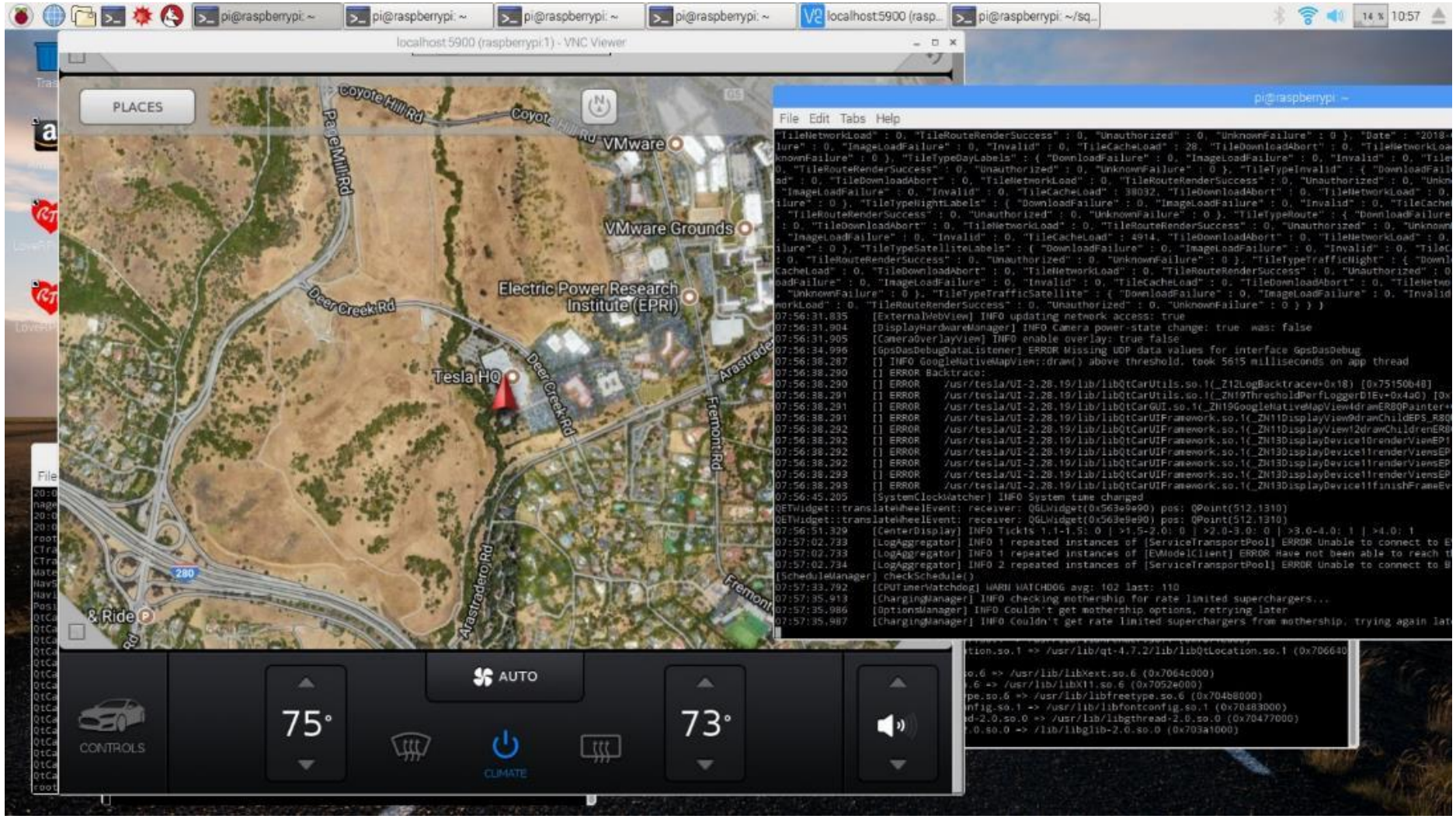
VRTC Capabilities

Extracting firmware, using wired diagnostic interfaces



VRTC Capabilities

Executing Program Binaries in an Instrumented Environment



VRTC Capabilities

Firmware Modification

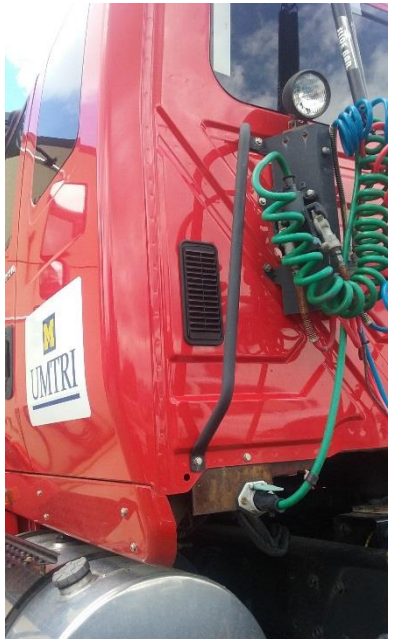
- Software only modification
- Software modified over a wired diagnostic interface
- Software updating systems' security is important

Heavy Vehicle Cybersecurity

Alrik Svenson

Cybersecurity Considerations for Heavy Vehicles

- Background
  - Heavy Vehicles, similar to light vehicles, can have cybersecurity vulnerabilities that could lead to safety concerns, but have different CAN data bus architectures and/or protocols.
  - Study looks at the special considerations for heavy vehicles.
- Approach
  - Design an investigative Framework to compare heavy vehicle cybersecurity to passenger vehicle cybersecurity.
  - Review vulnerability landscape and risk assessment.
- Results
  - Medium Duty/HD vehicles could be more vulnerable to scalable attacks that could target SAE J1939 CAN protocol which is common across manufacturers.
  - Passenger and heavy vehicles generally have the same security concerns in terms of wired and wireless interfaces.
  - Fleet management and telematics solutions come with a particular threat in medium and heavy duty trucks since fleets in this segment are highly homogeneous.
  - Final Report is published



Cybersecurity for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles

- Background
  - Heavy Vehicles use many aftermarket and telematics devices which can introduce a new common attack vector for cybersecurity threats.
  - Joint research in cooperation with FMCSA
- Approach
  - Survey of existing research on automotive cybersecurity - specific focus on retrofit systems into heavy vehicles (trucks and buses)
  - Identifying cybersecurity risks, threats, and potential mitigations for aftermarket systems.
  - Develop recommended guidance to help truck/bus manufacturers as well as aftermarket system providers address cybersecurity concerns.
- Results
  - Guidance document is intended for truck/bus manufacturers, Telematics Service Providers (TSPs), carriers, dealers/installers, fleet managers, mechanics, drivers, and government entities.

Hazard Analysis of Heavy Truck Platooning Concepts

Alrik Svenson

Hazard Analysis of Heavy Truck Platooning Concepts

Background

- Develop an understanding of heavy truck platooning concepts.
- Explore how safety hazards can be assessed and vary based on different levels of implementation.
- Identify variety within truck platooning systems (current and future concepts).
- Perform hazard analyses on typical heavy truck platooning system concepts and identify cross-cutting and unique items.

Hazard Analysis of Heavy Truck Platooning Concepts

- Approach
  - Market study to identify current and future concept systems.
  - Conduct hazard analysis and risk assessment.
  - Select representative, “generic,” systems to exercise additional analyses used in functional safety approaches.

- Expected Results
  - Describe techniques for managing a safety program for platooning including system description and hazards and risks.
  - Fault Tree Analysis and Safety of the Intended Function (SOTIF) analysis across different levels of automation.
    - For generic simple and complex truck platooning systems.

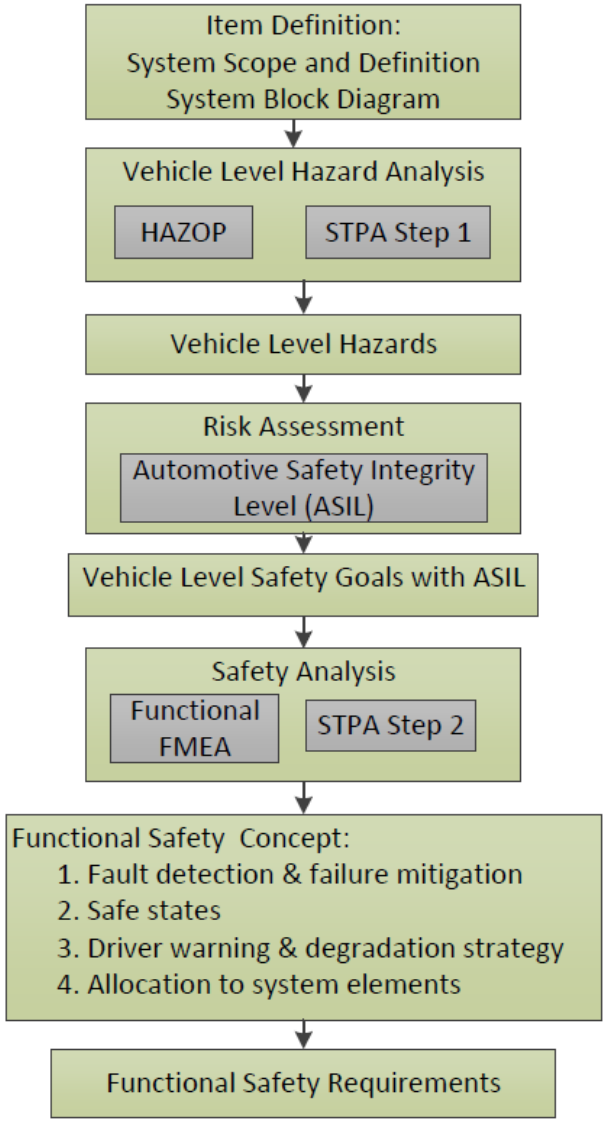
Functional Safety Research

Paul Rau

Functional Safety Research

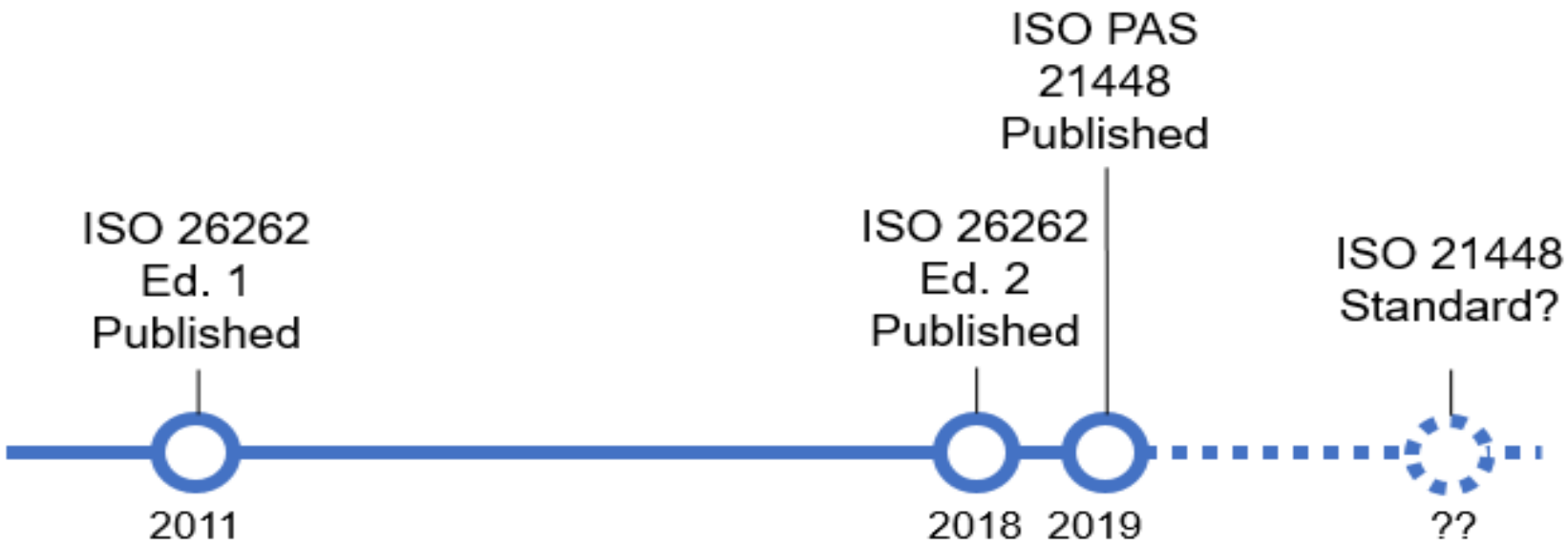
- **BACKGROUND**
  - There are established hazard analysis and fail-safe design processes (e.g. ISO 26262, STPA, etc.) that could be applied to combined functions
    - ASIL: Automotive Safety Integrity Level
    - FMEA: Failure Modes and Effects Analysis
    - HAZOP: Hazard and Operability Analysis
    - STPA: System Theoretic Process Analysis

- **OBJECTIVES**
  - Apply concept-phase of established functional safety processes to combined function automation and also identify means to identify hazards that could be caused by human errors. Identify high level safety requirements



Functional Safety Research

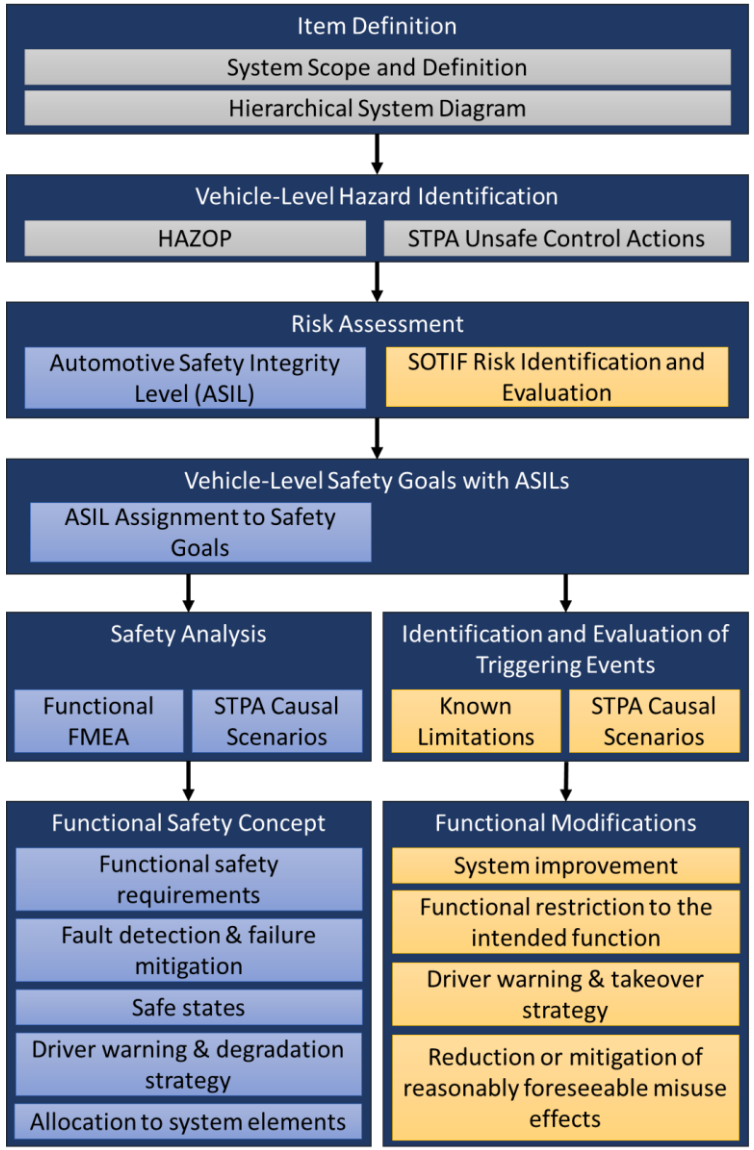
Standard Development Timeline



- ISO 26262: Road vehicles—Functional Safety
- ISO PAS 21448: Road vehicles—Safety of the Intended Functionality

PAS: Publicly Available Specification – Informal, a response to an urgent market need.

Integrating Elements of the Functional Safety Concept Phase and SOTIF



Completed and Published

Safety of the Intended Functionality– Level 3 Lane Maneuvers –

Addresses hazards that may arise when the system is functioning correctly. Applied a SOTIF analysis to the ALC system; Incorporate SOTIF into the current functional safety analysis process; Identify potential validation methods for SOTIF safety requirements.

Functional Safety of a Generic Accelerator Control System with Electronic Throttle Control

Produced functional safety assessments of generic accelerator control systems including hazard analysis reports; draft functional safety requirements; and draft driver-vehicle interface design recommendations. Diesel Internal Combustion Engine Vehicles, Electric Vehicles, Fuel Cell Hybrid Electric Vehicles, Gasoline Internal Combustion Engine Vehicles, Hybrid Electric Vehicles with Gasoline Internal Combustion Engines.

Functional Safety of Automated Lane Centering Controls

Automated Lane Centering (ALC) System and Related Foundational Vehicle Systems; Electric Power Steering System with Active Steering and Four-Wheel Steering Features; Conventional Hydraulic Braking (CHB) System with Antilock Braking System (ABS), Traction Control System (TCS), and Electronic Stability Control (ESC) Features; Steer-by-Wire (SbW) Steering System with Active Steering and Four-Wheel Steering Features.

Initiated and Underway

Vehicle-Level Hazard Analysis of a Concept Level 4 Automated Driving System

Build the knowledge base and provide a benchmark for industry to compare their internal hazard analysis; Illustrate the connection between functional safety and SOTIF at the vehicle system level, and considerations for applying these industry approaches to Level 4 ADS; and Identify the types of safety constraints that the system should adhere to under various operating conditions to inform future testing.

Foundations of Automotive Software Development

This project will produce a comprehensive primer for transportation scientists, engineers, and others, by developing an in-depth framework of factors affecting the lifecycle development, production, and maintenance of automotive software.