



NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Vehicle Cybersecurity and Electronics

NHTSA Safety Research Portfolio Public Meeting: Fall 2021

October 19, 2021



Panel Presentations

1

Vehicle Research and Test Center Electronics and Software Capabilities – John Martin

2

Comments to the Cyber Best Practices for the Safety of Modern Vehicles – John Martin

3

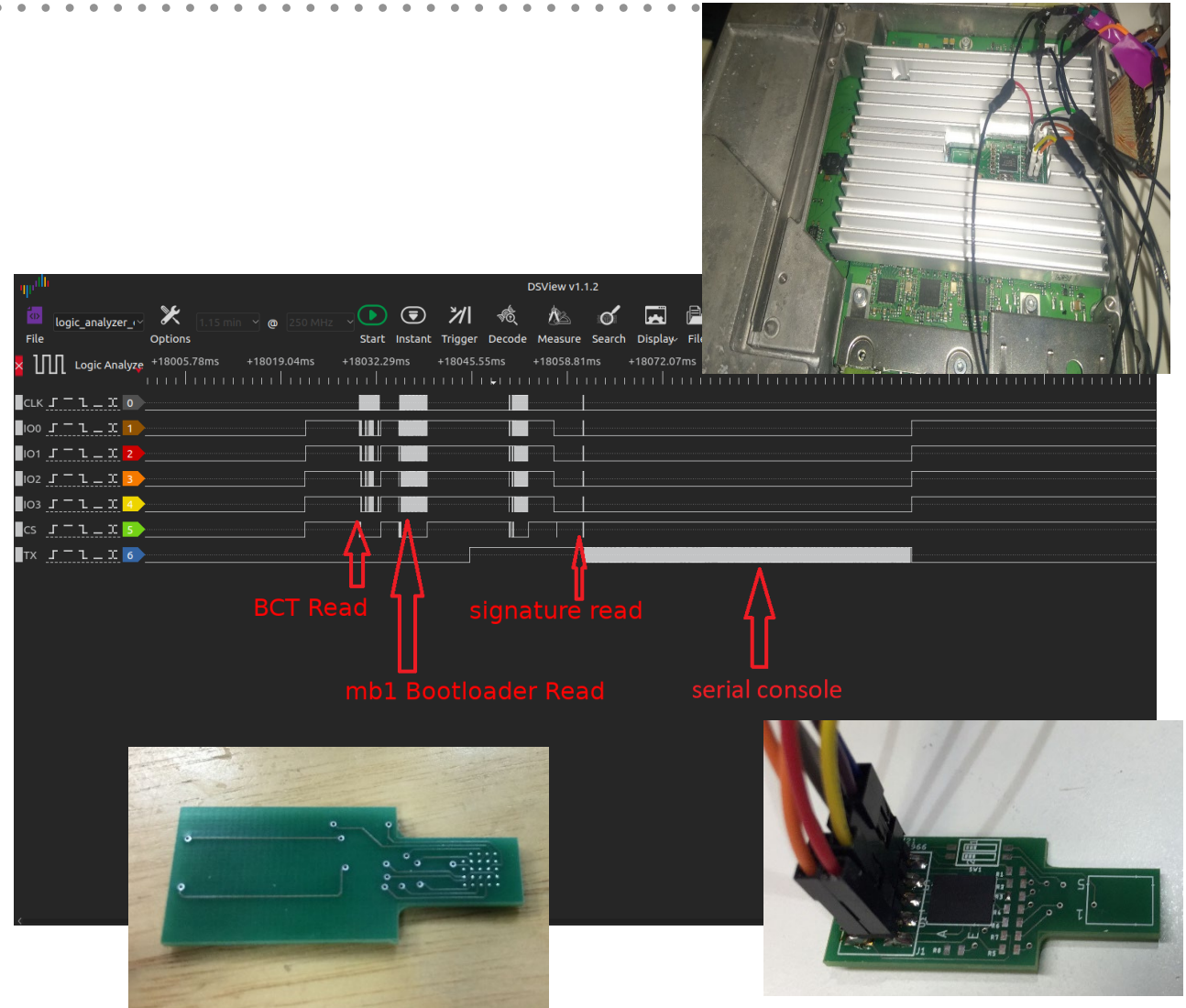
Cyber and Resiliency Research Project Summaries – Darryl Shepard

Vehicle Research and Test Center Improving Electronics Hardware Analysis

John Martin

VRTC – Applied Cybersecurity Lab

- Help inform policy by providing the agency with expertise and technical data on modern cybersecurity safety risks.
- Develop expertise and tools to better assess cybersecurity risk and support incident response capabilities.
- Ensure electronic systems work as intended and are designed to mitigate safety risks.



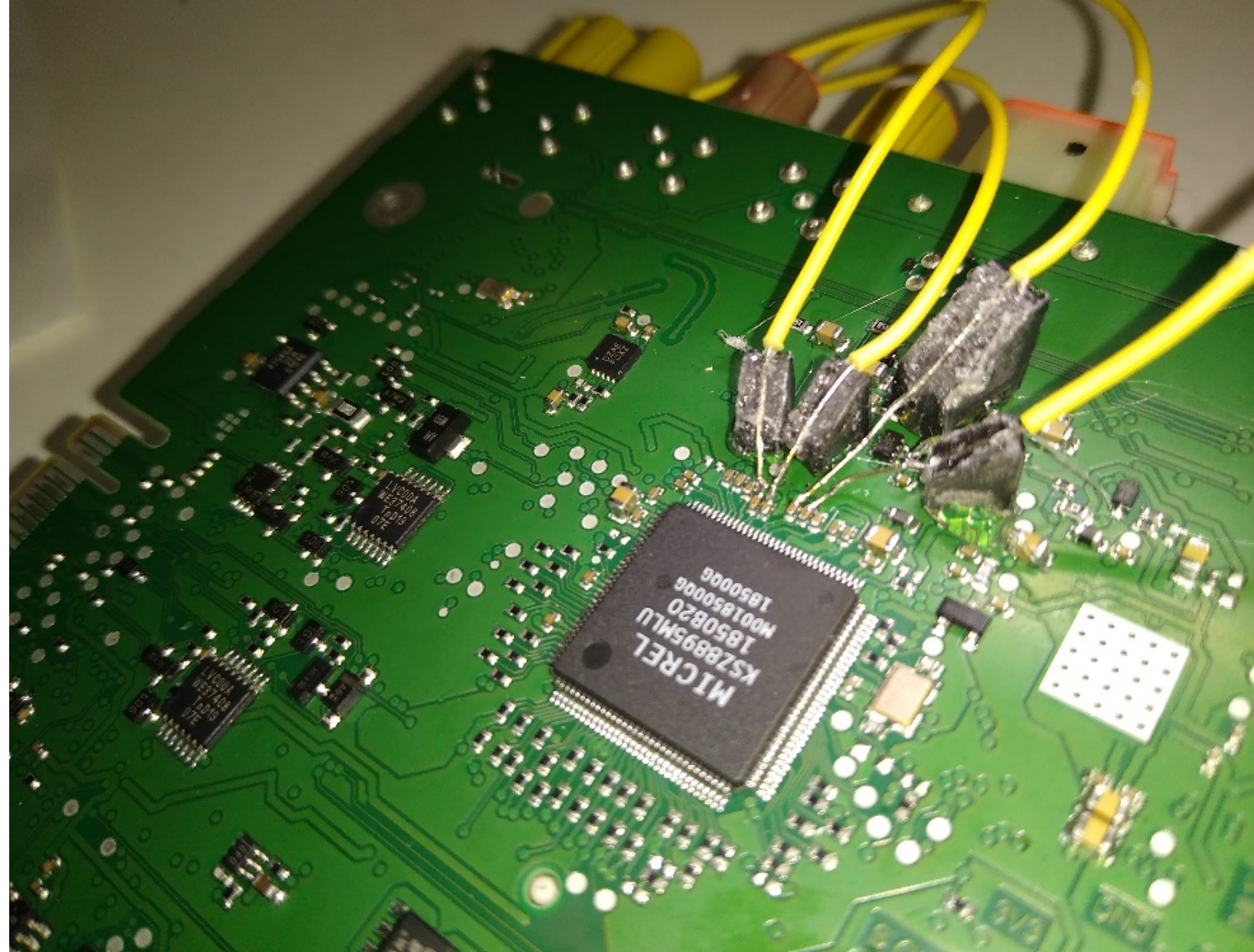
VRTC Cyber Capabilities

General Capabilities

- Device media removal and reading
- Firmware analysis
- Firmware simulation
- Bench testing devices
- Interface emulation

Goals

- Access the device under test
 - Console access
 - Filesystem access
- Learn about the device interfaces and general cybersecurity posture



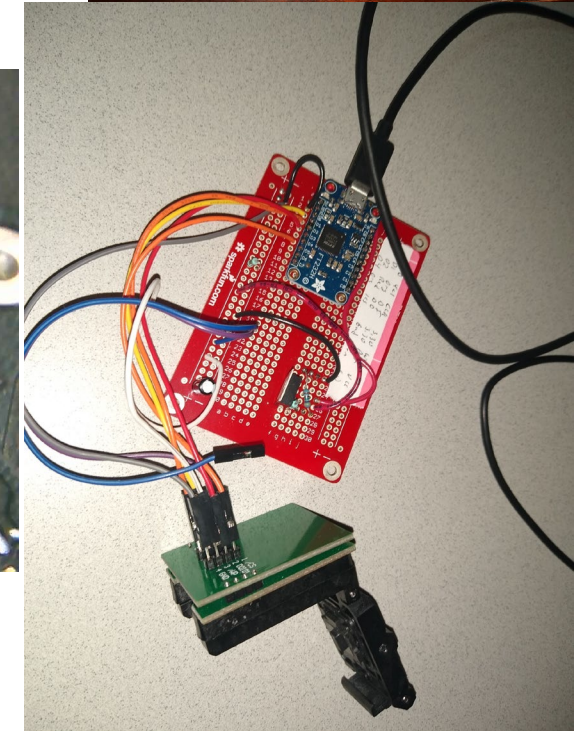
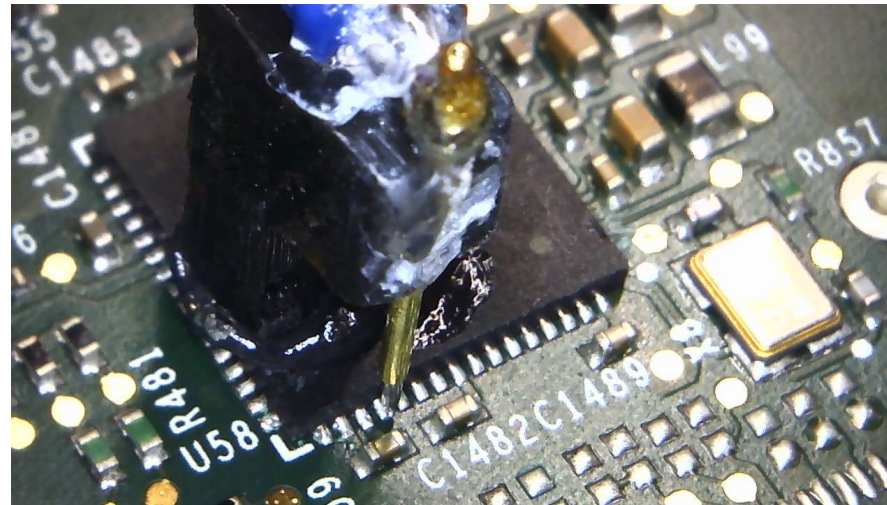
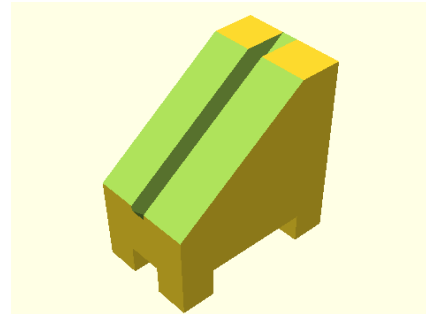
Current Tools and Capabilities

Analysis Tools

- Logic Analyzer
- Ghidra... disassembly/reverse engineering
- Similar development boards
- Emulators such as Unicorn
- Wireless analysis tools
 - Bluetooth
 - WiFi
 - Software defined radio

Manipulation Tools

- BGA machine
- Pogo Pins and associated structures
- Chip sockets, readers, writers
- PCB design
- Surface mount soldering capabilities



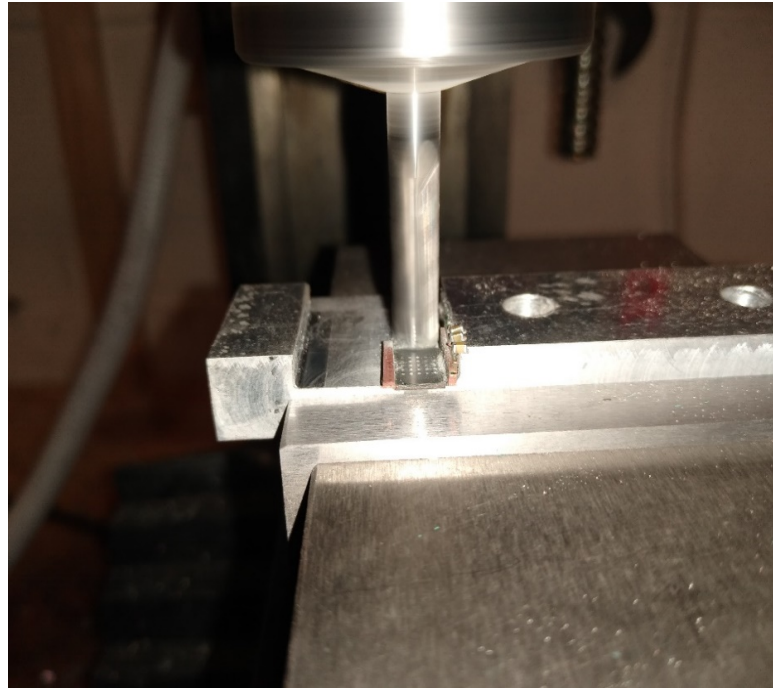
Adding Capabilities

Remove media chips from boards and read them

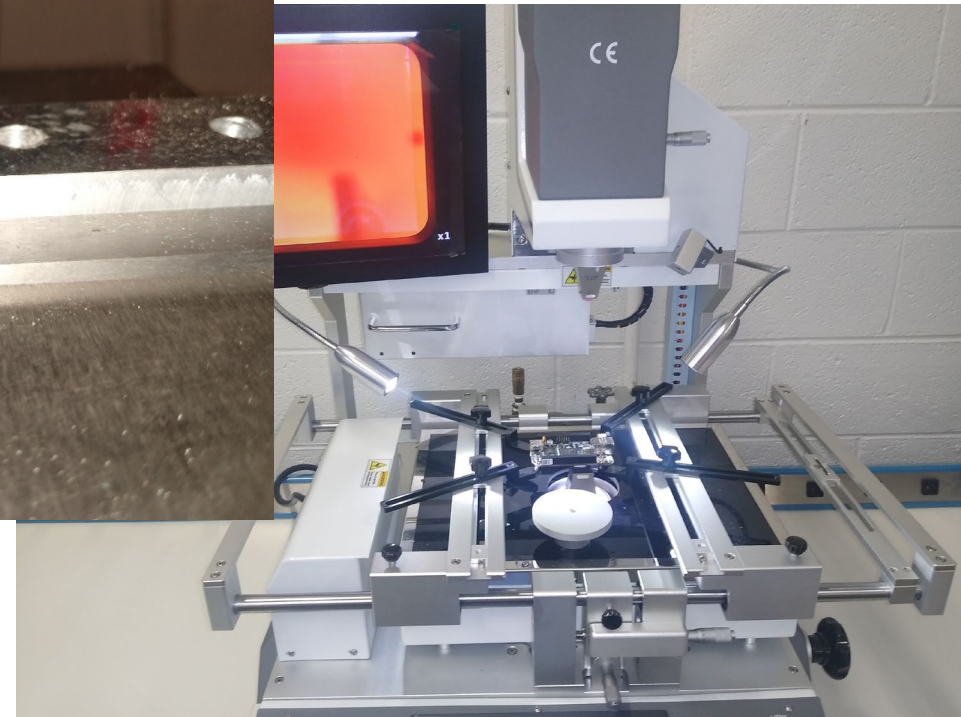
- Filesystems, executables, data
- Use emulation or try to execute recovered programs on similar development systems

Investigate internal interfaces

- Serial... UART, SPI, I2C
- Intra-device Ethernet



Milling machine cleaning fiberglass and epoxy from BGA pads

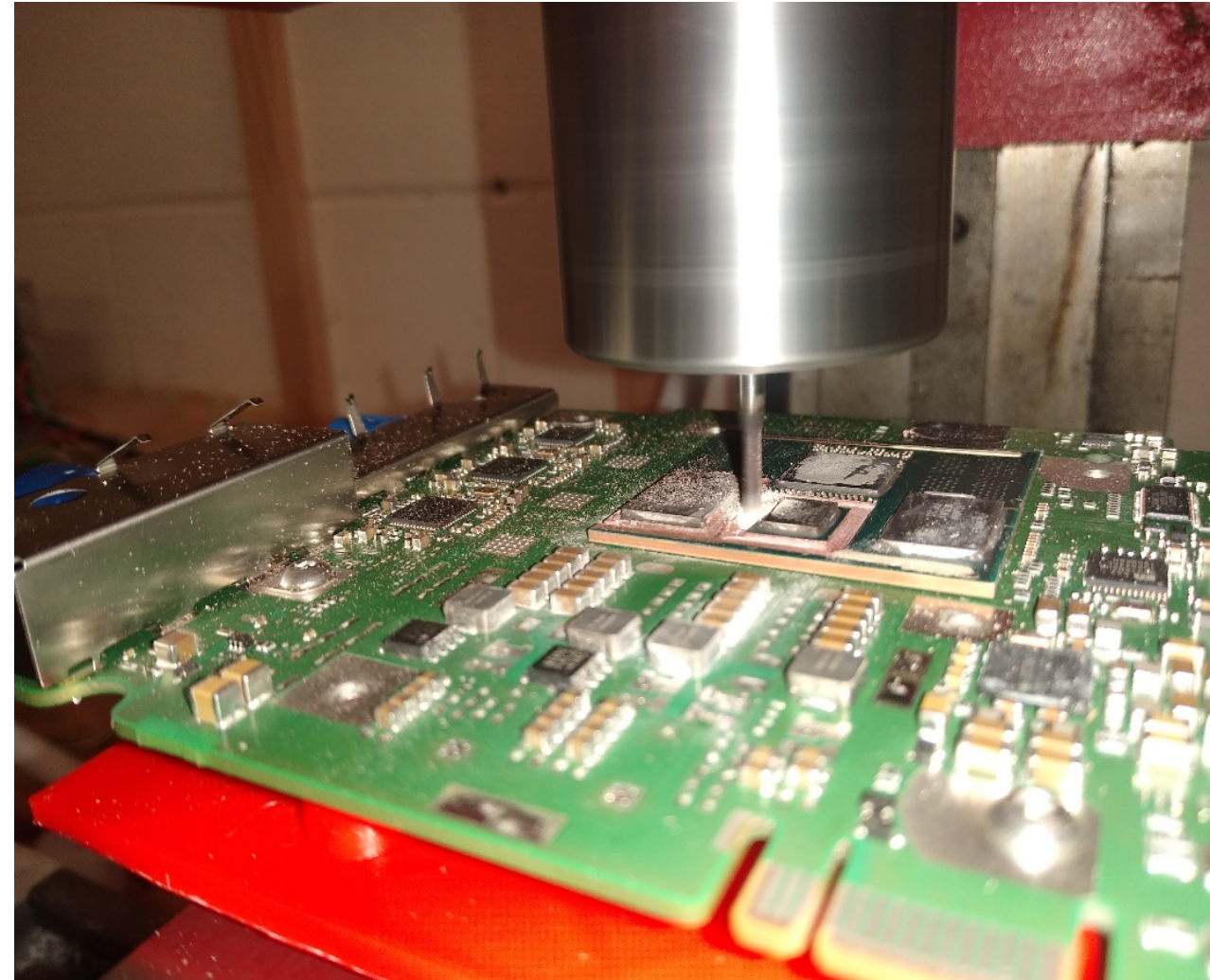


BGA chip removing/installing machine

Why are we adding capabilities?

ECUs are becoming more difficult to access. (This is good)

- Diagnostic interfaces are no longer easy to access
- Board-level interfaces once were open for developer convenience, now are locked down
- Boot processes are no longer trivial to interrupt and modify (for example, pressing a key on a U-boot console)
- Boot code appears to follow a chain of trust all the way back to ROM on the microcontroller



Comments to the Cyber Best Practices for the Safety of Modern Vehicles

John Martin

The Cybersecurity Best Practices for the Safety of Modern Vehicles

There is a continuing, expanded use of electronic systems, software and wireless connectivity in vehicle design

- Today's vehicles are some of the most complex computerized products available to consumers
- There are substantial benefits to highway transportation safety, mobility and efficiency
- Modern vehicle design needs to consider additional failure modes, vulnerabilities and threats that could jeopardize these benefits
- NHTSA's Cybersecurity Best Practices provide 43 items of general guidance along with 23 items of technical guidance to industry
- Addresses some of the priorities, additional failure modes, vulnerabilities and threats

The Best Practices' Contents (examples)

- 43 items of general guidance
 - General guidance discusses corporate processes and priorities
 - **[G.2]** *Companies developing or integrating vehicle electronic systems or software should prioritize vehicle cybersecurity and demonstrate executive management commitment and accountability by...*
 - **[G.19]** *Manufacturers should fully document any actions, design choices, analyses, supporting evidence, and changes related to its management of vehicle cybersecurity.*
- 23 items of technical guidance
 - Technical guidance discusses specific details of vehicle architecture
 - **[T.4]** *Any credential obtained from a single vehicle's computing platform should not provide access to multiple vehicles.*
 - **[T.10]** *Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication method to limit the possibility of message spoofing.*

High Level Observations

- 36 Organizations/Individuals responded with comments
- Variety of Stakeholders
 - Automotive OEMs
 - Automotive suppliers
 - Aftermarket suppliers
 - Trade organizations
 - Research labs
 - Technology companies
 - Cybersecurity solution providers
 - Public sector
 - Private citizens

Comment Overview

Four major categories of comments:

- NHTSA should make the best practices more specific or less specific
- NHTSA should address right to repair issues
- NHTSA should address privacy
- NHTSA should be more sensitive to how it designates various entities

Next Steps

- NHTSA is currently evaluating next steps for the best practices, based upon careful consideration of the comments submitted by the public.

Cyber and Resiliency Research Project Summaries

Darryl Shepard

Automotive Cybersecurity: Sensor Vulnerabilities Study

Purpose

- Catalogue commonly used sensors for automotive advanced driver assistance systems,
- Identify and profile known sensor exploits and vulnerabilities,
- Investigate potential new exploits, and
- Develop possible mitigation strategies and countermeasures.

Camera: Documented Exploits and Observed Impact

Attack Type	Attacker Action	Influences Sensor Data Output	Potential Influence on Fusion Systems or Vehicle Control
Sign Manipulation	Manipulation of (Speed Limit) Signage	Partial	Possible
Blind/Disorient	Use of a flashlight	Partial	Possible
Blind/Disorient	Use of a laser pointer	Yes	Possible
Blind/Disorient	Subject camera to a LiDAR sensor	No	No
Blind/Disorient	Use of an IR Range Finder (beam)	No	No

LiDAR: Documented Exploits and Observed Impact

Attack Type	Attacker Action	Influences Sensor Data Output	Potential Influence on Fusion Systems or Vehicle Control
Spooof Objects	Use of a Garden Hose Waster Stream	Yes	Possible
905nm Laser Pointer	Use of an (IR) Laser pointer	No	No
Red Laser Pointer	Use of a laser pointer	No	No
Mirrored Glass	Use of mirrored glass to disorient	Yes	Possible
Convex Mirrors	Use of convex mirrored glass to disorient	No	No
Cloak an object	Use of radar absorbent foam	No	No
Physical Attack	Use of clear tape on the LiDAR lens	Minimal	Possible
Physical Attack	Use of opaque tape on the LiDAR lens	Yes	Possible

Radar: Documented Exploits and Observed Impact

Attack Type	Attacker Action	Influences Sensor Data Output	Potential Influence on Fusion Systems or Vehicle Control
Radar vs. (Unmodified) Radar	Improper use of a radar to manipulate other radars	Partial	Possible
Radar vs. Waveguided Radar	Improper use of a radar to manipulate other radars	Partial	Possible
Cloak objects	Use of radar absorbent foam to cloak an object	Yes	Possible

Potential Mitigations and Countermeasures

Attack Type	Camera	LiDAR	Radar
Physical	<p>Vehicle Windscreen Block – full or partial interference (i.e., opaque marker/paint)</p> <p>- Mitigation: Installing camera where FOV is cleaned by windshield wiper</p>	<p>Use a piece of opaque (gaffer) tape to a specific area (azimuth section) of the sensor.</p> <p>- Mitigation: Attack may be prevented by simply inspecting the sensor for tampering before use</p>	
Remote	<p>Direct Photonic Attacks: Flashlight</p> <p>- Mitigation: use of dual camera for redundancy and resiliency</p>	<p>Manipulated with other sources of laser light, (i.e., laser pointer).</p> <p>- Mitigation: An optical band-pass filter on the casing that prevents noise from UV, NIR and high-power visible light sources (i.e., laser pointers).</p>	<p>Jamming attacks and are focused on radar parameter management affecting the following areas:</p> <p>power</p> <p>- Mitigation: variability of power output</p>
Inductive or Interference	<p>Interference of road-side traffic signs by flashlight or laser pattern, reflections, etc.)</p> <p>- Mitigate by use of polarized filter on camera lens to reduce light interference</p>	<p>Debris from the road (i.e., dirt, mud)</p> <p>- Countermeasure: A physical actuator or spray device (i.e., wiper blade or windshield washer like device)</p>	<p>Foreign Object or Debris (FOD) Attacks</p> <p>- Mitigation: Radar and camera for same function will mitigate FOD on one sensor (not both).</p>

Automotive Cyber Resiliency Research

Purpose

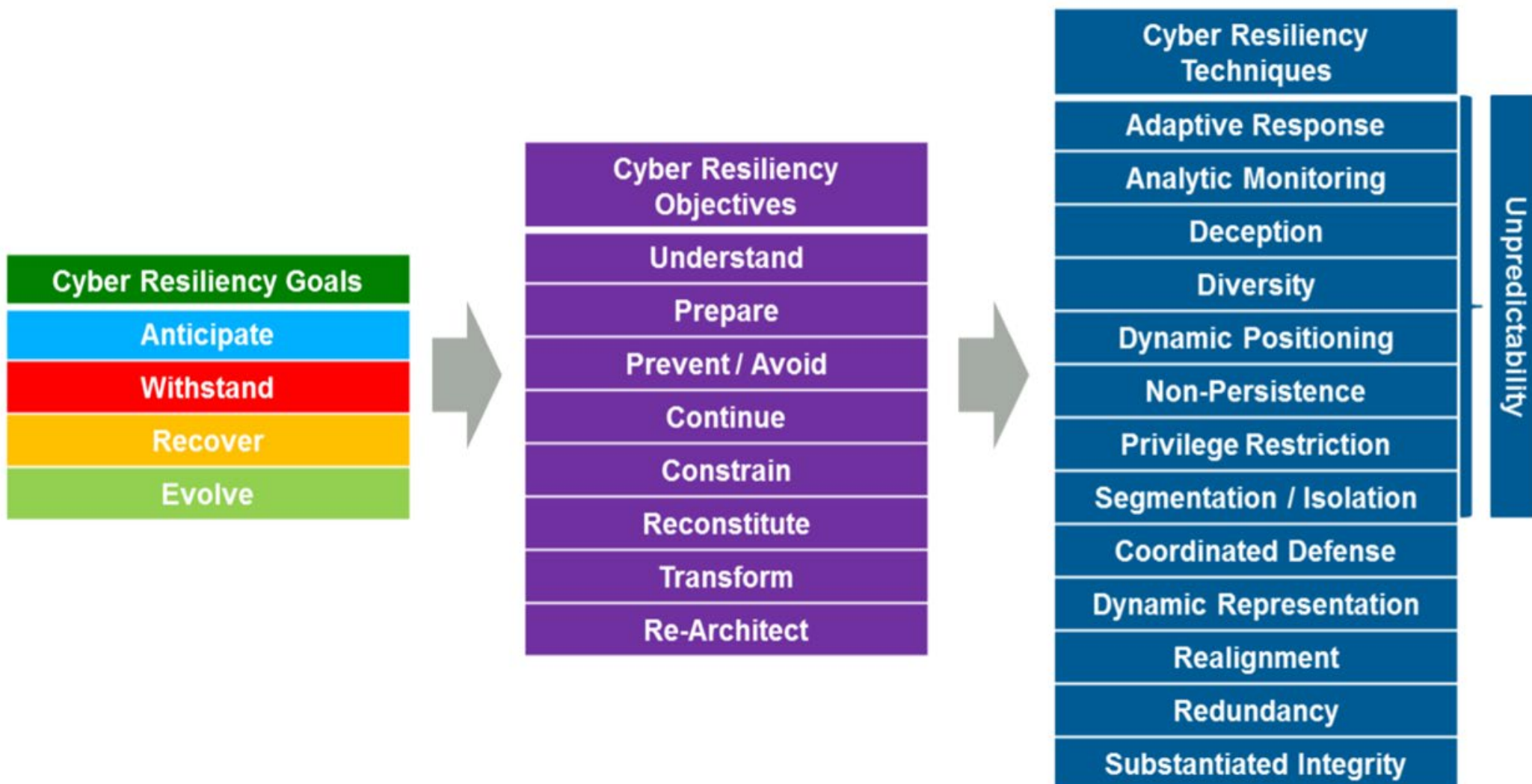
- Identify and investigate resiliency strategies and methods used in nonautomotive domains that could also be applied to vehicles.
- Examine automotive architectures and how cyber-resiliency frameworks might be applied to potentially improve resiliency in vehicles.
- Examine testing methods and strategies used by other industries to develop a vehicle cyber-resiliency testing and assessment framework aligned with the primary resiliency goals of anticipate, withstand, recover, and evolve.

Definition of Cyber Resiliency

MITRE's Cyber Resiliency Engineering Framework (CREF) definition:

*“the ability of a system to **anticipate, withstand, recover from, and evolve** in response to adverse effects of some actual or predicted event with the goal of returning a system to its original state or another acceptable operational state when normal operation is disturbed”.*

Cyber Resiliency Goals, Objectives, and Techniques



Approaches to Cyber Resiliency in Different Domains

Domain	Resilience Strategy	Cyber Resiliency Engineering Framework Goals			
		Anticipate	Withstand	Recover	Evolve
Energy	Automatic Power Rerouting		X	X	
	Fault Isolation		X		
	Distributed Generation	X	X		
Space	Component Hardening	X	X		
	Single Error Upset Mitigation		X	X	
	Distributed Systems	X	X		
Industrial Control Systems	Network Isolation	X	X	X	
	Real-time Detection, Investigation, and Mitigation		X	X	X
Aviation	Fault-Tolerant System Design		X	X	
	System Redundancy		X	X	

Automotive Architecture Categories

- **Light Duty, High Complexity** – These vehicles have higher cost and complexity.
- **Light Duty, Medium Complexity** – These vehicles have a mid-range cost and complexity.
- **Light Duty, Low Complexity** – These vehicles are traditional budget and low-cost vehicles.
- **Commercial Medium and Heavy Duty** – These are like light duty but are highly modular to allow for advanced telematics and monitoring; based on J1939 Controller Area Network (CAN) bus.
- **Defense** - This category includes specialty commercial vehicles with aftermarket upgrades for physical security, connectivity, and obfuscation.

Resiliency Techniques Applied to Functions & Systems

Functions	Technique										
	Adaptive Response	Analytic Monitoring	Coordinated Defense	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Re-alignment	Redundancy
Critical Risk											
Braking		X			X		X	X		X	
Throttle	X	X									X
CAN	X	X	X	X	X		X				
OBD-II											
High Risk											
Wi-Fi	X	X		X				X	X		
GPS		X	X								
ECU				X							
Medium Risk											
Remote Keyless Entry					X						
Cellular				X				X	X		
Bluetooth				X					X		
Low Risk											
Power Locks, Windows, Mirrors		X						X			

Key: X – Asset may use cyber resilience technique(s)

Outline for resiliency assessment reporting

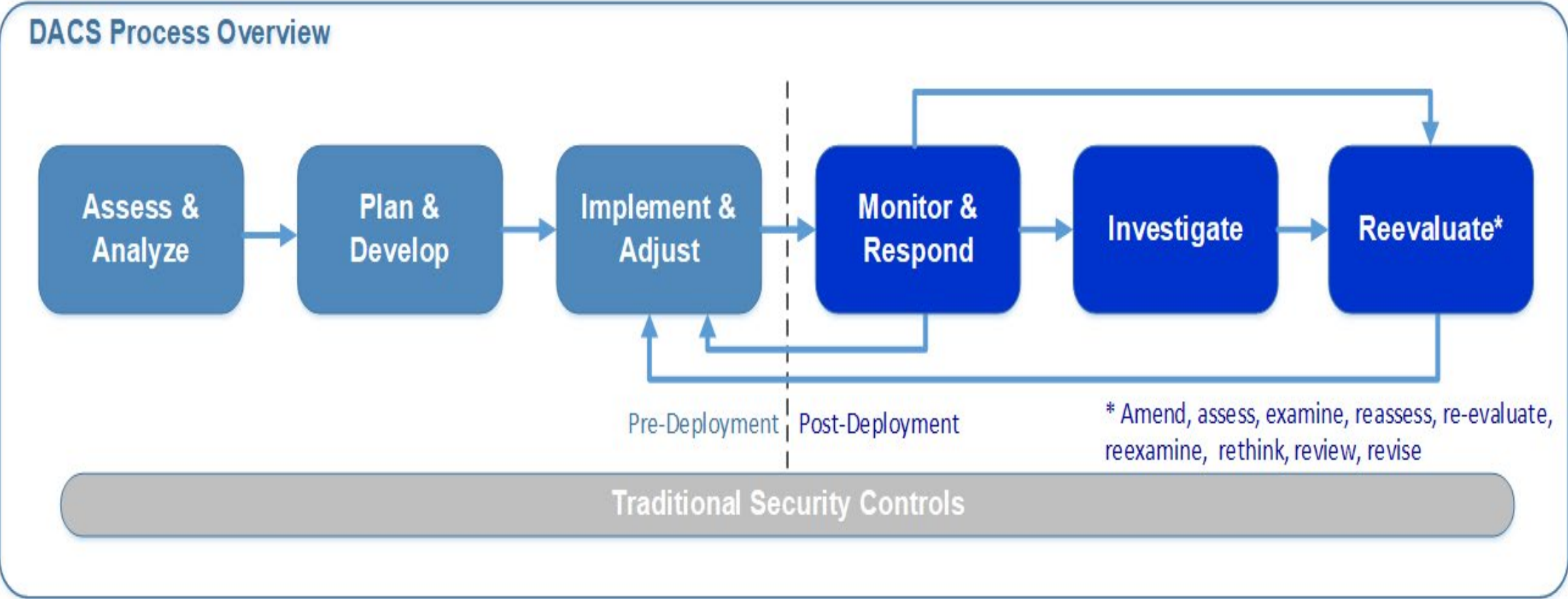
Test Attribute	Description
Level of Abstraction	<p>Vehicle – monitored with minimal intrusion from the user (e.g., vehicle health monitoring via infotainment unit)</p> <p>Subsystem – specified system (e.g., communication access points)</p> <p>Component – specific element of a subsystem (e.g., USB ports on head units)</p> <p>Software –specific software and static code</p>
Resiliency Goals	Anticipate (A), Withstand (W), Recover (R), Evolve (E) as defined by the NIST SP 800-160 Vol. 2 draft and the MITRE CREF
Test Objective	The description of what is tested based on the assessed risk of vehicle subsystems/components/functions, attack chain, and potential resiliency strategies
Method	How to test, at a high-level, to assess cybersecurity and resiliency according to the test objective or question.
Metrics/Criteria	High-level measures to assess performance of the system against the test objective.
Notes	Additional information necessary to conduct the test or general testing considerations;
Testing Level of Expertise	Recommended level of expertise and system knowledge necessary to conduct test: Non-technical assessment, High-level Technical Assessment, Detailed Technical Assessment/Penetration Testing, Expert Technical Assessment/Proprietary
Criticality/Importance	Potential risk to the vehicle if a vehicle cannot pass the test: Critical, High, Medium, and Low, as defined in the automotive architecture cyber-resiliency risk assessment

Automotive Cyber Data Analytics: An Implementer's Guide

Purpose

- Identify data and criteria to determine if a modern vehicle has been compromised through exploit of a cybersecurity vulnerability;
- Assess how data analytics can help understand the safety implications of the compromise after a successful exploit;
- Understanding of how data analytics could be used to trigger real-time recovery modes after a successful exploit;
- Identify how CDA can be used to enable approaches and techniques to forensically analyze post-exploit data to facilitate potential system improvements.

Vehicle CDA Reference Process



Key Considerations and Takeaways

- CDA is only one aspect of a larger cybersecurity program and management system.
- OEMs and suppliers can employ vehicle and supporting infrastructure data and information taxonomies for CDA development.
- Standing up an effective CDA program requires considerable effort in analyzing data sources and Indicators of Compromise (IoCs), and then developing, testing, and training the different CDA methods.
- OEMs can operationalize CDA through a Vehicle Security Operations Center (VSOC) function.
- CDA is not always the best option.

Thank you for your time and attention

John Martin:

john.martin@dot.gov

Darryl Shepard:

darryl.shepard@dot.gov