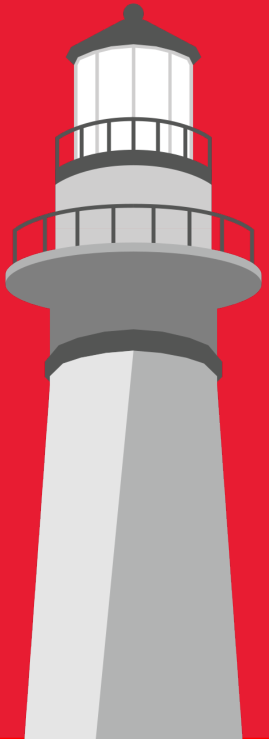
Block Harbor.
Cybersecurity



Making Sense of Security Testing for ISO/SAE 21434 & UNR 155

Brandon Barry

What I’ll walk through.

- Overview of testing in ISO/SAE 21434 and UNR155.
- A high-level overview of different types of testing outlined in ISO/SAE 21434.
- A solution we’re working on to automate cybersecurity testing.

Founder
Block Harbor Cybersecurity

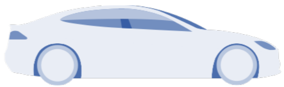
Americas Lead
Automotive Security Research Group (NPO)

Full CISSP Holder @ 23

1st place, DEF CON Car Hacking Village, 2019
CANucks

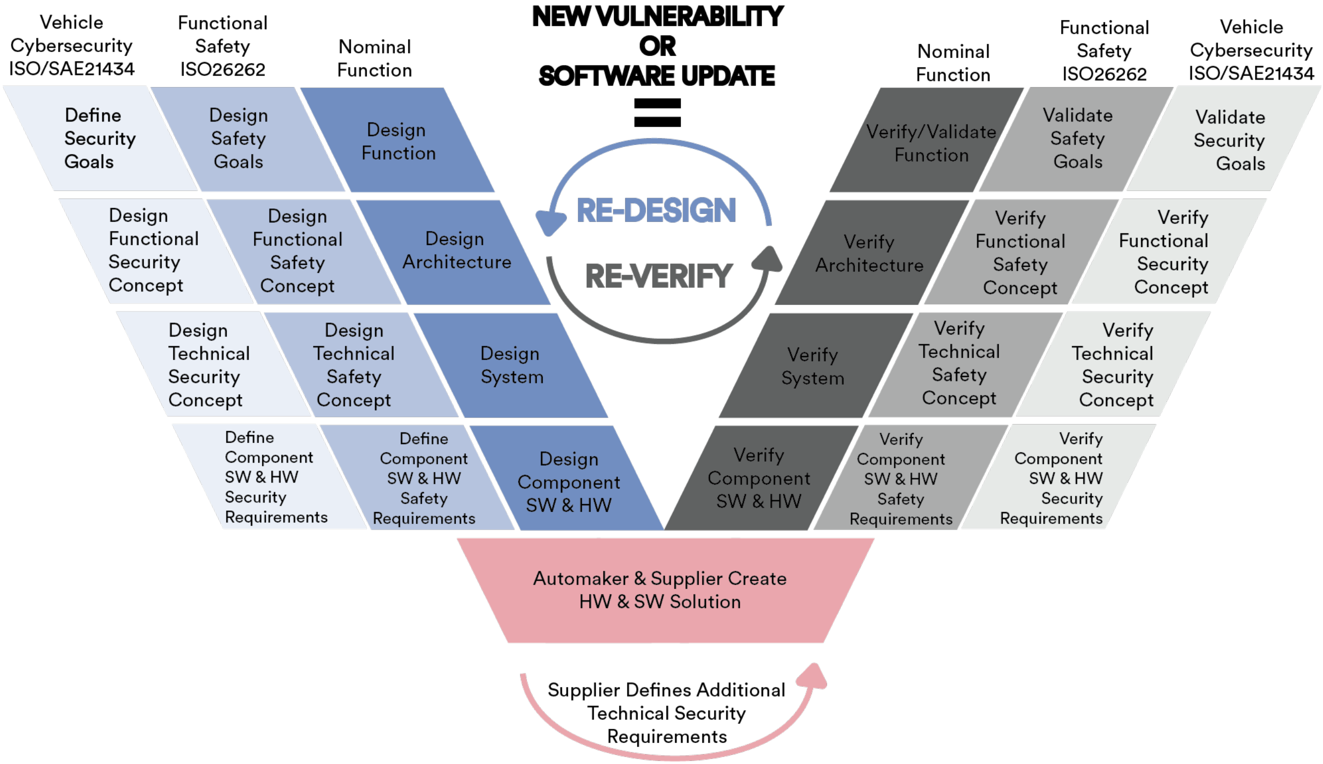
In general, cybersecurity testing is critical to verify your cybersecurity design is working and document it to show others.

”Trust, but verify”



Concept

Production & Operations



Vehicle Cybersecurity ISO/SAE21434	Functional Safety ISO26262	Nominal Function
Define Security Goals	Design Safety Goals	Design Function
Design Functional Security Concept	Design Functional Safety Concept	Design Architecture
Design Technical Security Concept	Design Technical Safety Concept	Design System
Define Component SW & HW Security Requirements	Define Component SW & HW Safety Requirements	Design Component SW & HW

NEW VULNERABILITY OR SOFTWARE UPDATE =

RE-DESIGN

RE-VERIFY

Nominal Function	Functional Safety ISO26262	Vehicle Cybersecurity ISO/SAE21434
Verify/Validate Function	Validate Safety Goals	Validate Security Goals
Verify Architecture	Verify Functional Safety Concept	Verify Functional Security Concept
Verify System	Verify Technical Safety Concept	Verify Technical Security Concept
Verify Component SW & HW	Verify Component SW & HW Safety Requirements	Verify Component SW & HW Security Requirements

Automaker & Supplier Create HW & SW Solution

Supplier Defines Additional Technical Security Requirements

UNECE WP.29

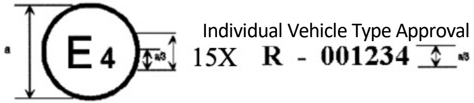
Threats

Connectivity

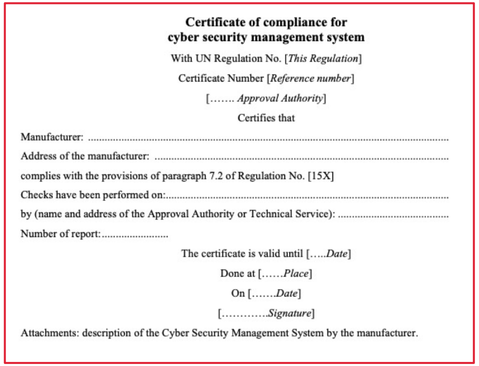
Mitigation

Mitigation

Mitigation



CSMS uses a risk-driven approach to mitigate in-vehicle and out-of-vehicle threats for a given vehicle type



Certificate of compliance for cyber security management system

With UN Regulation No. [*This Regulation*]

Certificate Number [*Reference number*]

[……. *Approval Authority*]

Certifies that

Manufacturer: ……………………………………………………………………………

Address of the manufacturer: ……………………………………………………………

complies with the provisions of paragraph 7.2 of Regulation No. [15X]

Checks have been performed on:……………………………………………………………

by (name and address of the Approval Authority or Technical Service): ………………………

Number of report:……………………

The certificate is valid until […..*Date*]

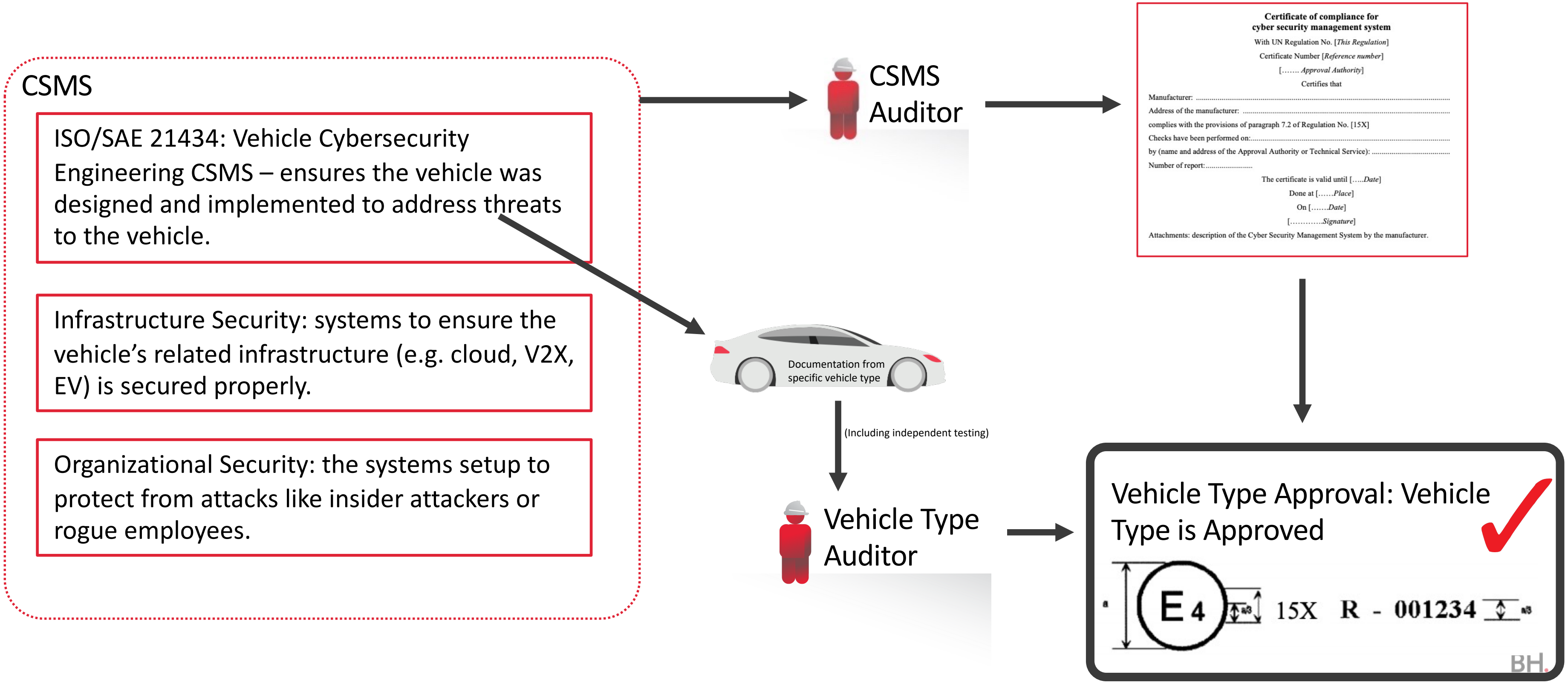
Done at [……*Place*]

On […….*Date*]

[…………*Signature*]

Attachments: description of the Cyber Security Management System by the manufacturer.

How 21434 and WP.29 Fit Together



CSMS

ISO/SAE 21434: Vehicle Cybersecurity Engineering CSMS – ensures the vehicle was designed and implemented to address threats to the vehicle.

Infrastructure Security: systems to ensure the vehicle's related infrastructure (e.g. cloud, V2X, EV) is secured properly.

Organizational Security: the systems setup to protect from attacks like insider attackers or rogue employees.

CSMS Auditor

Certificate of compliance for
cyber security management system

With UN Regulation No. [*This Regulation*]

Certificate Number [*Reference number*]

[……. *Approval Authority*]

Certifies that

Manufacturer: ....

Address of the manufacturer: ....

complies with the provisions of paragraph 7.2 of Regulation No. [15X]

Checks have been performed on:...

by (name and address of the Approval Authority or Technical Service): ....

Number of report:........................

The certificate is valid until […..*Date*]

Done at [……*Place*]

On […….*Date*]

[…………*Signature*]

Attachments: description of the Cyber Security Management System by the manufacturer.

Documentation from specific vehicle type

(Including independent testing)

Vehicle Type Auditor

Vehicle Type Approval: Vehicle Type is Approved ✓

The Players in Testing

Supplier Tester

- Receives cybersecurity requirements from Automaker.
- Usually responsible at the component level for:
  - Cybersecurity Requirement Verification
  - Cybersecurity Goal Validation: fuzz testing and penetration testing

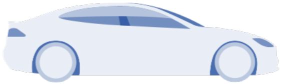
Automaker Tester

- Operating per their CSMS in compliance with UNR 155.
- Usually responsible at the vehicle level for:
  - Cybersecurity Requirement Verification
  - Cybersecurity Goal Validation: fuzz testing and penetration testing

Vehicle Type Auditor

- Operating per their CSMS in compliance with UNR 155.
- Usually responsible at the vehicle level for:
  - Cybersecurity Requirement Verification
  - Cybersecurity Goal Validation: fuzz testing and penetration testing

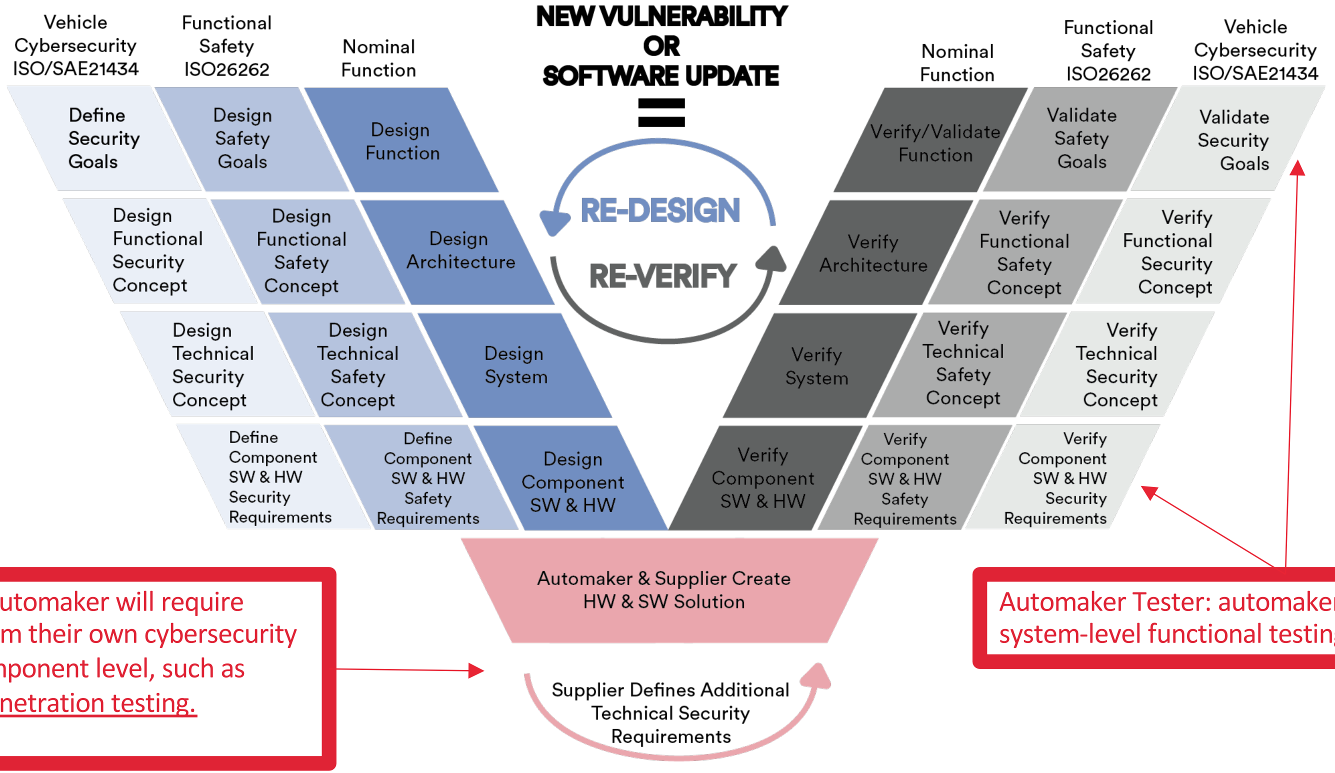
When to test?



Concept

<u>Vehicle Type Auditor</u>: auditing body tests vehicle as a part of the UNR 155 Type Approval process.

Production & Operations



Vehicle Cybersecurity ISO/SAE21434	Functional Safety ISO26262	Nominal Function
Define Security Goals	Design Safety Goals	Design Function
Design Functional Security Concept	Design Functional Safety Concept	Design Architecture
Design Technical Security Concept	Design Technical Safety Concept	Design System
Define Component SW & HW Security Requirements	Define Component SW & HW Safety Requirements	Design Component SW & HW

NEW VULNERABILITY OR SOFTWARE UPDATE

=

RE-DESIGN

RE-VERIFY

Nominal Function	Functional Safety ISO26262	Vehicle Cybersecurity ISO/SAE21434
Verify/Validate Function	Validate Safety Goals	Validate Security Goals
Verify Architecture	Verify Functional Safety Concept	Verify Functional Security Concept
Verify System	Verify Technical Safety Concept	Verify Technical Security Concept
Verify Component SW & HW	Verify Component SW & HW Safety Requirements	Verify Component SW & HW Security Requirements

Automaker & Supplier Create HW & SW Solution

Supplier Defines Additional Technical Security Requirements

<u>Supplier Tester</u>: automaker will require supplier to perform their own cybersecurity testing at the component level, such as <u>functional and penetration testing.</u>

Automaker Tester: automaker will perform system-level functional testing, fuzz

Types of Testing: “Functional Testing”

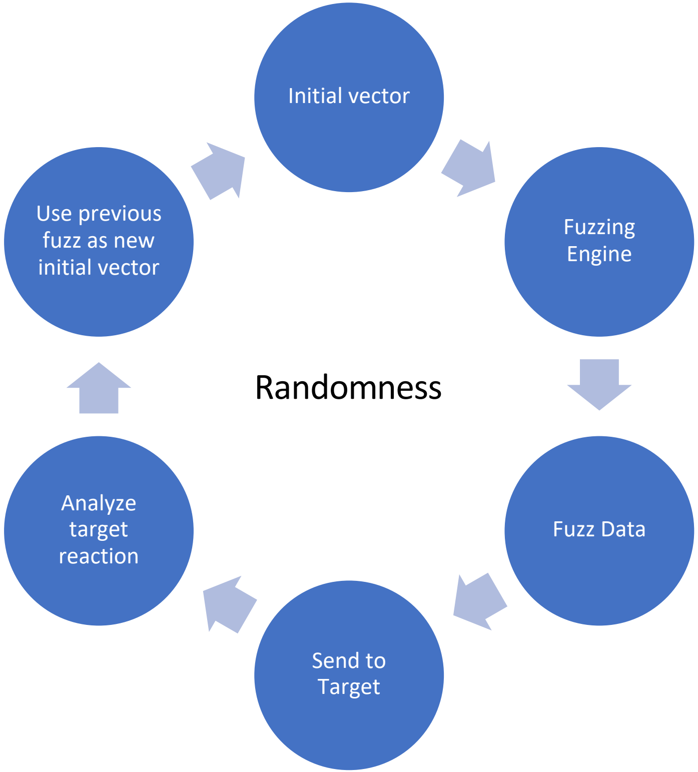
Test a system to determine if the cybersecurity design and its implementation is functioning as intended.

- Generate a verification specification for a cybersecurity requirement that ensures that the requirement is properly implemented.
- Acquire a test setup that properly implements the item.
- Execute the specification and document the results.
- Do so for each cybersecurity requirement.

Types of Testing: “Fuzz Testing”

Test a system for unknown vulnerabilities using randomized input that removes preconceptions.

- Acquire a test setup that properly implements the item.
- Instrument test interfaces to be fuzzed (e.g. a CAN interface).
- Choose initial fuzz vectors that give the fuzzer a starting point to iterate on.
- Choose conditions in which to log an unusual behavior of the target
- Start fuzzer with initial vectors and run for some defined period.
- Analyze resulting data to determine problematic payloads.



Types of Testing: “Vulnerability Scanning”

Scan a system for known, published vulnerabilities.

- Internal Vulnerability Scanning
  - Given a list of known software/hardware versions (SBOM/HBOM), correlate against known CVEs to determine if there are matches.
  - Sort through the matches for relevancy.
- External Vulnerability Scanning
  - Use characteristics of the system (e.g. a port scan, inventory of hardware) to identify likely vulnerabilities.

Types of Testing: “Penetration Testing”

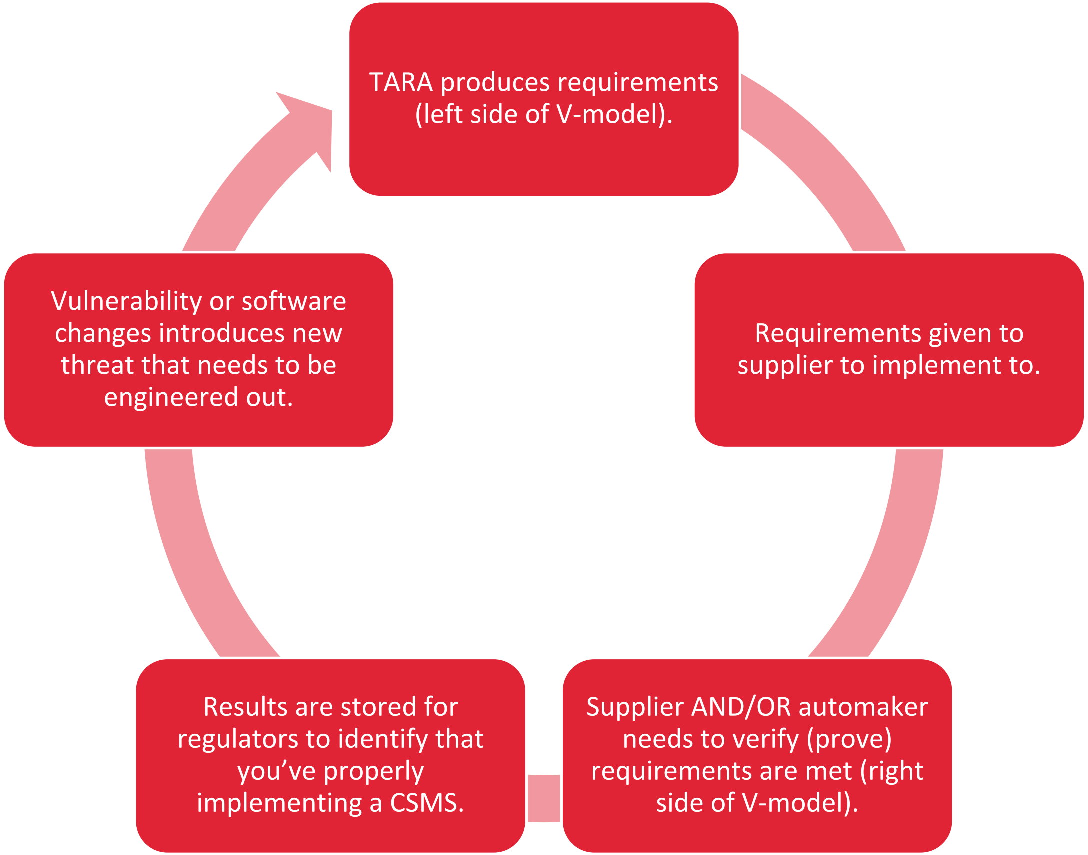
Utilizing a team of system experts, attempt to exploit the target using any means possible to determine the robustness of the cybersecurity design.

- At BH, we follow a 6 step process in our vehicle cybersecurity labs:
  - Threat Modeling
  - Attack Surface Enumeration and Passive Reconnaissance
  - Security Defense/Protection Check & Vulnerability Detection
  - Active Scanning & Vulnerability Research
  - Deep Testing & Attempt to Exploit
  - Assessment Reporting
- Penetration testing may use tactics like fuzzing and vulnerability scanning to exploit the target.
- Penetration testing is **an end-of-line check** to validate that you’ve met your cybersecurity goals for the system. It should be relied on only after the previous types of testing has been thoroughly performed.

What About UNR155 Audit Testing?

- To be determined.
- What it may look like for each vehicle type approval:
  - Vehicle for type approval is received at auditor’s lab.
  - Vehicle is tested for weaknesses using CSMS work products as guidance.
  - If any weaknesses are uncovered, the test fails.
- Feels like a crash test.

One and done? Not so fast.



TARA produces requirements (left side of V-model).

Requirements given to supplier to implement to.

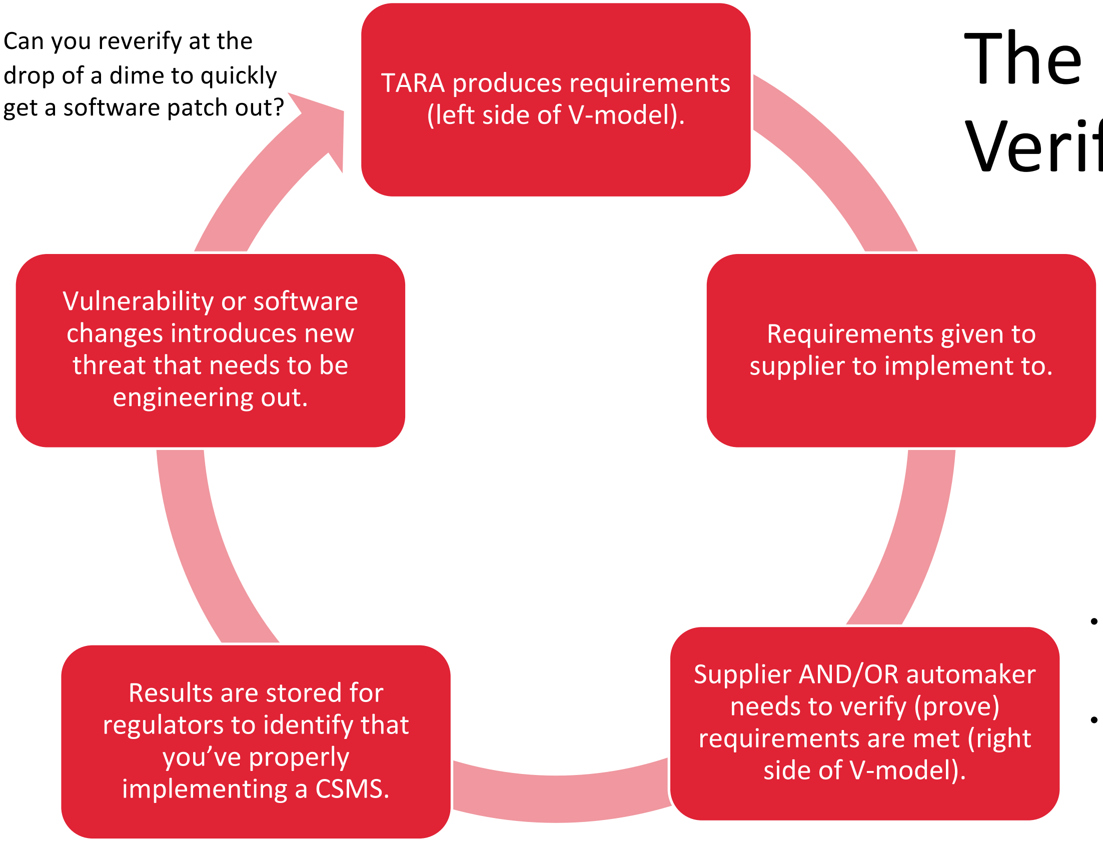
Supplier AND/OR automaker needs to verify (prove) requirements are met (right side of V-model).

Results are stored for regulators to identify that you’ve properly implementing a CSMS.

Vulnerability or software changes introduces new threat that needs to be engineered out.

- A new vulnerability = new update/recall = pass changes through CSMS.
- WP.29 accounts for a **changing threat landscape** due to new vulnerabilities and software updates. This process is iterative.
- Lots of room for automation.

The Challenge in Verification



TARA produces requirements (left side of V-model).

Requirements given to supplier to implement to.

Supplier AND/OR automaker needs to verify (prove) requirements are met (right side of V-model).

Results are stored for regulators to identify that you've properly implementing a CSMS.

Vulnerability or software changes introduces new threat that needs to be engineering out.

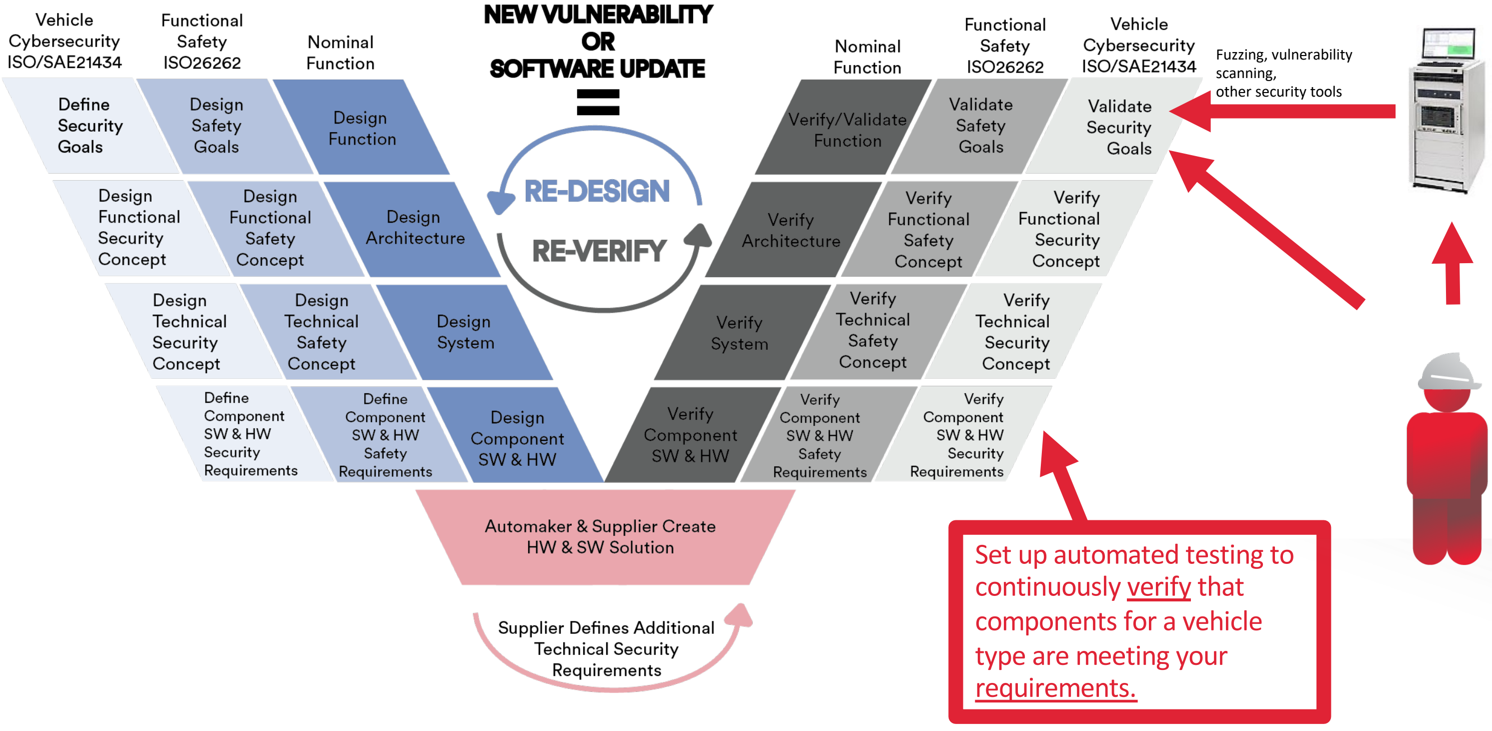
Can you reverify at the drop of a dime to quickly get a software patch out?

Requirements defined by OEM are likely too "high level". Supplier will need to define their own technical requirements via their own CSMS and provide documentation.

- Multiple Responsible Parties: who is responsible for verifying that requirements are met? The automaker or the supplier?
- Scalability and repeatability: Can you effectively verify requirements across vehicles types faster than the pace of innovation or vulnerability discovery? If done manually (e.g., via a test plan in excel, the answer is no).

Are all verification test results stored and centralized so you can quickly access them for type approval?

Automation and Reusability in your Vehicle CSMS



Vehicle Cybersecurity ISO/SAE21434

Functional Safety ISO26262

Nominal Function

Define Security Goals

Design Safety Goals

Design Function

Design Functional Security Concept

Design Functional Safety Concept

Design Architecture

Design Technical Security Concept

Design Technical Safety Concept

Design System

Define Component SW & HW Security Requirements

Define Component SW & HW Safety Requirements

Design Component SW & HW

NEW VULNERABILITY OR SOFTWARE UPDATE =

RE-DESIGN

RE-VERIFY

Automaker & Supplier Create HW & SW Solution

Supplier Defines Additional Technical Security Requirements

Nominal Function

Functional Safety ISO26262

Vehicle Cybersecurity ISO/SAE21434

Verify/Validate Function

Validate Safety Goals

Validate Security Goals

Verify Architecture

Verify Functional Safety Concept

Verify Functional Security Concept

Verify System

Verify Technical Safety Concept

Verify Technical Security Concept

Verify Component SW & HW

Verify Component SW & HW Safety Requirements

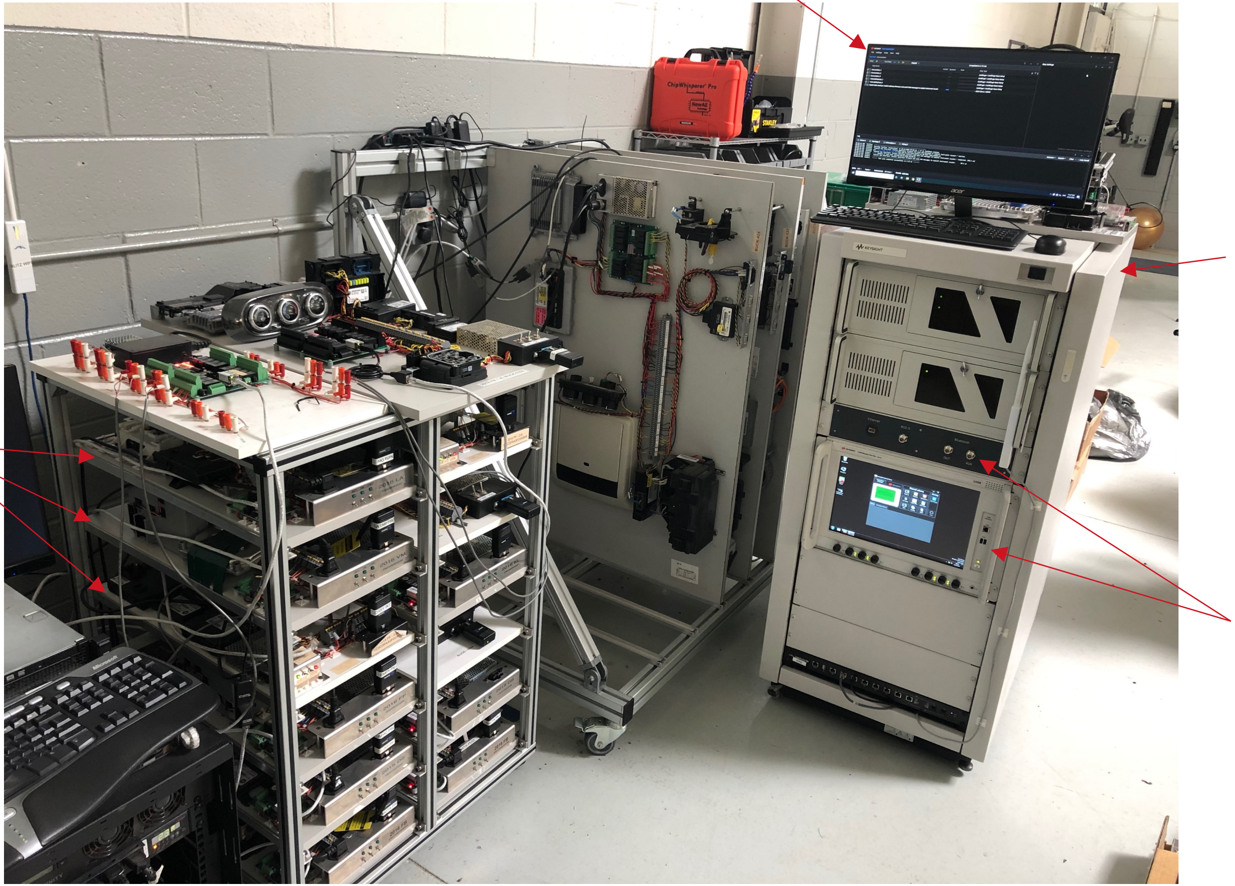
Verify Component SW & HW Security Requirements

Fuzzing, vulnerability scanning, other security tools

Set up automated testing to continuously verify that components for a vehicle type are meeting your requirements.

Open Source Test Automation Platform*

(OpenTAP)



Vehicle Test Bench Targets

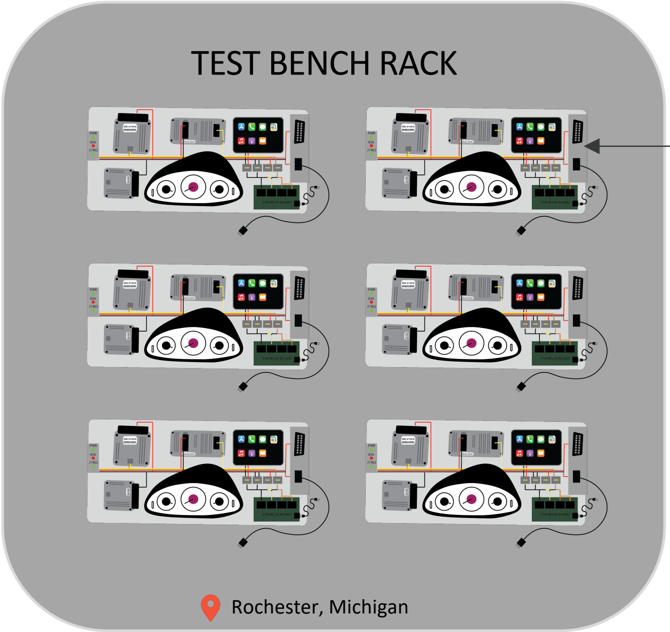
Keysight Automotive Cybersecurity Pen Test Platform

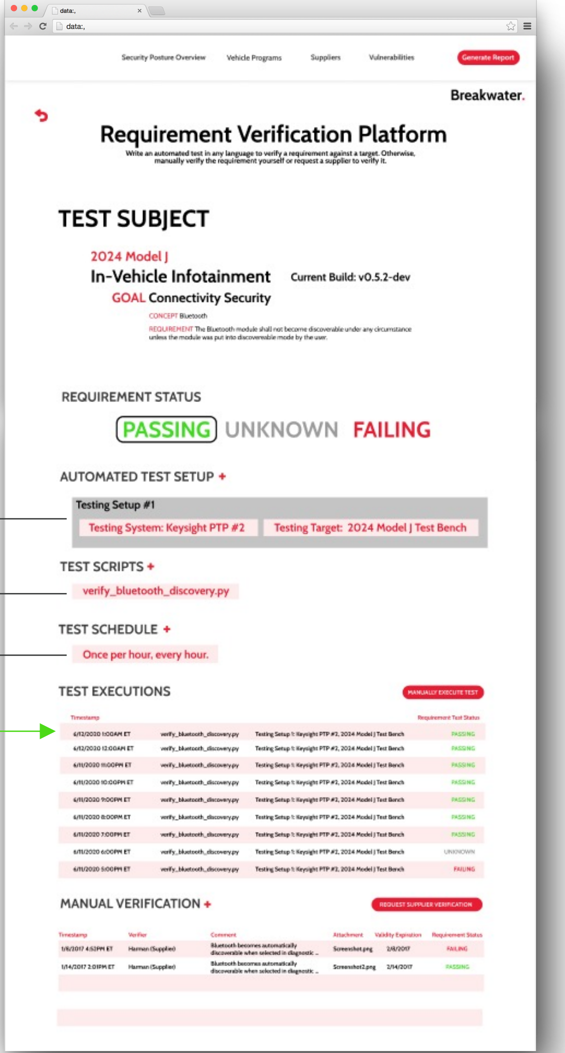
Interfaces

Bluetooth
Wi-Fi
Cellular
CAN Bus
Ethernet
Automotive Ethernet
Etc.

Rochester, Michigan

*Learn more at opentap.io





Requirement Verification Platform

Write an automated test in any language to verify a requirement against a target. Otherwise, manually verify the requirement yourself or request a supplier to verify it.

TEST SUBJECT

2024 Model J

In-Vehicle Infotainment Current Build: v0.5.2-dev

GOAL Connectivity Security

CONCEPT Bluetooth

REQUIREMENT The Bluetooth module shall not become discoverable under any circumstance unless the module was put into discoverable mode by the user.

REQUIREMENT STATUS

PASSING UNKNOWN FAILING

AUTOMATED TEST SETUP +

Testing Setup #1

Testing System: Keysight PTP #2 Testing Target: 2024 Model J Test Bench

TEST SCRIPTS +

verify_bluetooth_discovery.py

TEST SCHEDULE +

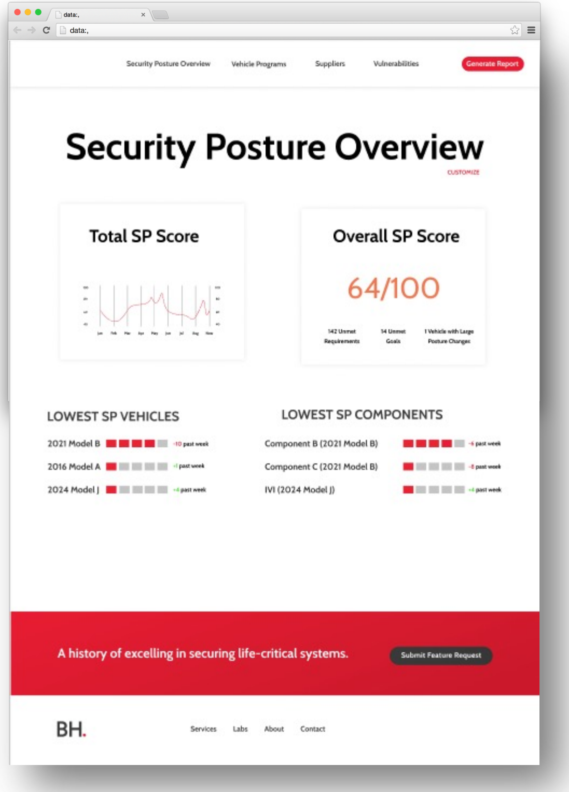
Once per hour, every hour.

TEST EXECUTIONS

Timestamp			Requirement Test Status
6/12/2020 1:00AM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/12/2020 12:00AM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/11/2020 11:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/11/2020 10:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/11/2020 9:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/11/2020 8:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/11/2020 7:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	PASSING
6/11/2020 6:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	UNKNOWN
6/11/2020 5:00PM ET	verify_bluetooth_discovery.py	Testing Setup 1: Keysight PTP #2, 2024 Model J Test Bench	FAILING

MANUAL VERIFICATION +

Timestamp	Verifier	Comment	Attachment	Validity Expiration	Requirement Status
1/8/2017 4:53PM ET	Harman (Supplier)	Bluetooth becomes automatically discoverable when selected in diagnostic ...	Screenshot.png	2/8/2017	FAILING
1/14/2017 2:01PM ET	Harman (Supplier)	Bluetooth becomes automatically discoverable when selected in diagnostic ...	Screenshot2.png	2/14/2017	PASSING



Security Posture Overview

Total SP Score

Overall SP Score

64/100

142 Unmet Requirements

14 Unmet Goals

1 Vehicle with Large Posture Changes

LOWEST SP VEHICLES

2021 Model B	🟥🟥🟥🟥⬜	-10 past week
2016 Model A	🟥⬜⬜⬜⬜	+1 past week
2024 Model J	🟥⬜⬜⬜⬜	+4 past week

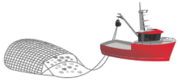
LOWEST SP COMPONENTS

Component B (2021 Model B)	🟥🟥🟥🟥⬜	-6 past week
Component C (2021 Model B)	🟥⬜⬜⬜⬜	-8 past week
IVI (2024 Model J)	🟥⬜⬜⬜⬜	+4 past week

A history of excelling in securing life-critical systems.

BH.

- Store and export work products for auditors.
- Aggregate testing for real time insight into current status of vehicle w/r/t its cybersecurity requirements.
- Automate.



Security Assessments

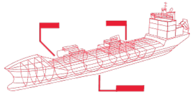
Vehicle/Subsystem/Component Penetration Testing

Vehicle/Subsystem/Component Threat Analysis & Risk Assessment (TARA)

Managed Security

Managed Security Operation Center (SOC)

Continuous Fuzzing



Security Consulting

ISO/SAE 21434 Design & Implementation

Security Research

Let’s Connect.

contactus@blockharbor.io

https://blockharbor.io/jobs

(313) 246-1860