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"
CSMS uses a risk-driven approach to **mitigate** in-vehicle and out-of-vehicle threats for a given **vehicle type**.
How 21434 and WP.29 Fit Together

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.
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?

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

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

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.

- 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.

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

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

Requirements given to supplier to implement to.

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

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

- 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).

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.

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

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.

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

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

TARA produces requirements (left side of V-model).
Automation and Reusability in your Vehicle CSMS

<table>
<thead>
<tr>
<th>Vehicle Cybersecurity ISO/SAE21434</th>
<th>Functional Safety ISO26262</th>
<th>Nominal Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define Security Goals</td>
<td>Design Safety Goals</td>
<td>Design Function</td>
</tr>
<tr>
<td>Design Functional Security Concept</td>
<td>Design Functional Safety Concept</td>
<td>Design Architecture</td>
</tr>
<tr>
<td>Design Technical Security Concept</td>
<td>Design Technical Safety Concept</td>
<td>Design System</td>
</tr>
<tr>
<td>Define Component SW &amp; HW Security Requirements</td>
<td>Design Component SW &amp; HW</td>
<td>Verify/Validate Function</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Architecture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Functional Safety Concept</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Functional Technical Concept</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Component SW &amp; HW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify Component SW &amp; HW Safety Requirements</td>
</tr>
</tbody>
</table>

NEW VULNERABILITY OR SOFTWARE UPDATE

RE-DESIGN

RE-VERIFY

Automaker & Supplier Create HW & SW Solution

Supplier Defines Additional Technical Security Requirements

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

Fuzzing, vulnerability scanning, other security tools
Open Source Test Automation Platform*

(OpenTAP)

Vehicle Test Bench Targets

Interfaces

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

Keysight Automotive Cybersecurity Pen Test Platform

Rochester, Michigan

*Learn more at opentap.io
• 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