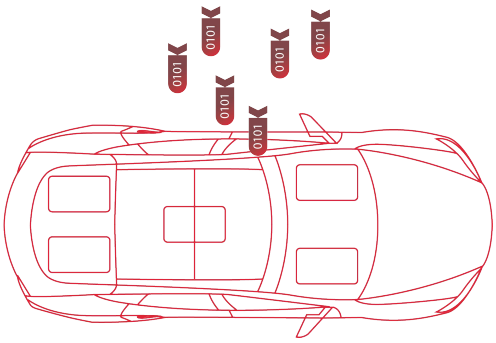
Fuzzing-as-a-Service

Testing targets with unknown input - Vehicles, Systems, and Components

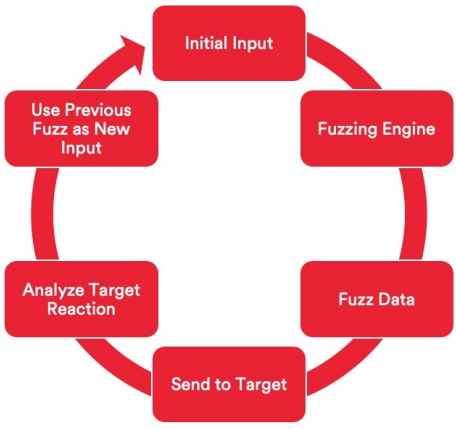
ISO/SAE 21434 and UNECE WP.29 are creating pressure to execute fuzz testing throughout the supply chain.

Fuzz testing is a key component of security testing referred to in the standard to detect unknown vulnerabilities. Automakers are responsible to analyze fuzz testing results or perform robust security testing themselves and provide work products for regulators. Many OEMs are requiring suppliers perform fuzz testing.



What is Fuzz Testing?

Fuzz testing is a technique commonly used to discover potential unknown security vulnerabilities by security researchers and hackers. **Fuzzing** is an automated software testing technique which **tests the targets ability to handle and respond to malformed data**. Fuzz testing will send a large number of random and specifically crafted malformed communication packets to devices to see how a module may respond. Fuzz inputs are generated recursively such that each new input is a combination of randomness and the previous input, generating inputs into the system that would never otherwise be tested. Thorough **fuzz testing will discover bugs and ensure software robustness.**



Why Fuzz?

In automotive the software exists in the field for up to 10 years or longer. It is only a matter of time before vulnerabilities are discovered. Releasing software that is robust from launch can provide confidence in the security posture of the vehicle. Fuzz testing is an early stage technique attackers may use to discover other more damaging exploits in your vehicle ecosystem. Doing fuzz testing catches bugs early and gives time in the development life cycle to fix critical vulnerabilities before release. It is more cost effective to discover and mitigate security vulnerabilities in development than waiting until attacks cause damage and patching them on in field products.

Challenges in Fuzzing

While fuzzing as a technique has been around for decades, **very few commercial tools are well suited for automotive environments to perform fuzzing effectively even with expert guidance.** Effective fuzzing relies on application logic that cannot be captured in a generic tool. For vehicle technologies like CAN, it's especially challenging because fuzzing is only effective if it is reaching application-layer logic with sensible input.

Why Block Harbor?

Block Harbor was founded in 2014 in Detroit providing services to automakers and automotive suppliers to keep vehicles safe, ranging from penetration testing to running a 24/7/365 Security Operation Center (SOC). We're on a mission to build great solutions to keep mobility safe.

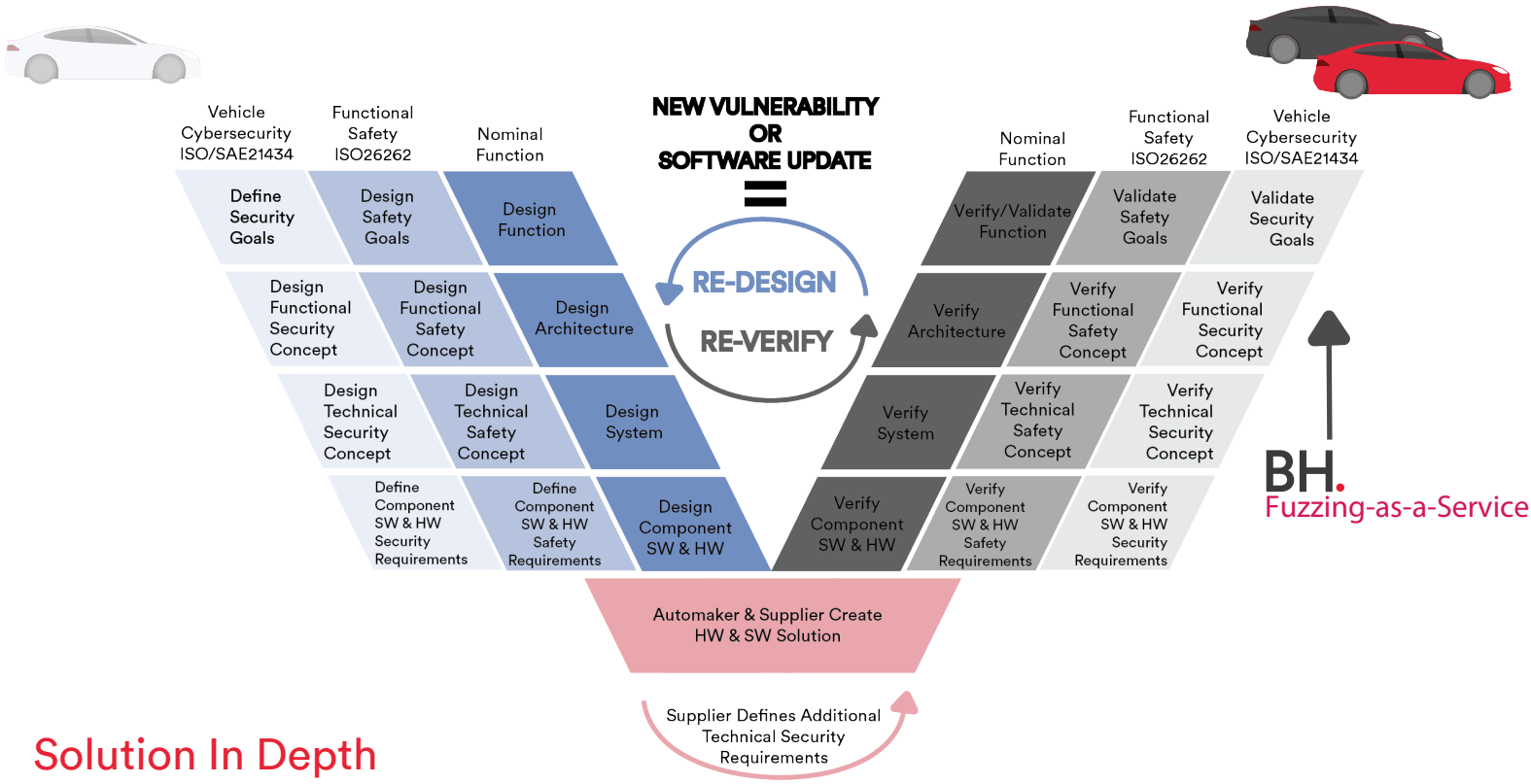
- Vehicle Cybersecurity Labs
  - -Penetration Testing
  - -Fuzzing
  - -V&V-as-a-Service
  - -Vehicle Cybersecurity Lab Buildout
- Vehicle Security Operations
  - -Vehicle Security Operation Center (VSOC)
  - -Threat Analysis and Risk Assessment (TARA)
  - -Vehicle Cybersecurity Management System (CSMS)
- Vehicle Cybersecurity Consulting

Block Harbor. Cybersecurity

To learn more about working with our team to meet your vehicle security needs, please visit blockharbor.io

Fuzzing-as-a-Service

Testing targets with unknown input - Vehicles, Systems, and Components



Solution In Depth

GETTING STARTED

Before Project Kick-off

Customers may provide security requirements to guide the goals of fuzz testing. Block Harbor can identify the appropriate scope for fuzz testing when customers don't have their own definition. **Block Harbor will identifying the components, interfaces, and protocols to be tested with the appropriate number of generated fuzzing test cases.** This information will be provided in a quote with a detailed project timing plan.

Hardware Delivery

Customers will deliver the necessary hardware to create multiple test set ups to support the project. Block harbor can assemble the test environment with the provided equipment. It is **recommended to have three modules for fuzz testing** and all the peripheral equipment and cables necessary to support all the communication interfaces.

EXECUTION & DELIVERY

Conduct Fuzz Testing

Block Harbor will configure the fuzzing tools and instrument the device under test to execute the test plan. Bi-weekly meetings with the customer are hosted to share the status of fuzz testing, address road blocks, and discuss significant findings. This offers customers **an opportunity to fix critical vulnerabilities early in their development timeline.** Once fuzzing is complete, Block Harbor will analyze all the fuzz test results and determine if fuzz inputs generated an unexpected response from the target system.

Final Report

At the end of the engagement Block Harbor will provided a detail fuzz testing report with a full analysis of the findings. Any fuzz testing failures will be documented with an analysis of the root cause.

Why Block Harbor?

Block Harbor was founded in 2014 in Detroit providing services to automakers and automotive suppliers to keep vehicles safe, ranging from penetration testing to running a 24/7/365 Security Operation Center (SOC). We're on a mission to build great solutions to keep mobility safe.

- Vehicle Cybersecurity Labs
  - -Penetration Testing
  - -Fuzzing
  - -V&V-as-a-Service
  - -Vehicle Cybersecurity Lab Buildout
- Vehicle Security Operations
  - -Vehicle Security Operation Center (VSOC)
  - -Threat Analysis and Risk Assessment (TARA)
  - -Vehicle Cybersecurity Management System (CSMS)
- Vehicle Cybersecurity Consulting

Block Harbor. Cybersecurity

To learn more about working with our team to meet your vehicle security needs, please visit blockharbor.io