The People Problem in Vehicle Cybersecurity – Great Services and Automation
About me

Bryan Blancke
Director of Labs at Block Harbor
Leading the teams for automotive security testing, new product solutions and research

• Electrical Engineering
  ❖ Michigan State University
• CISSP holder 2018
• Top 3 in Defcon Car Hacking Village 2018-2022
• Focused in Automotive & Cybersecurity since 2013
Our Journey

2020: ???
Let’s pivot
Asked ourselves: what great solutions could we build to secure the future of mobility?

2021: Rebuilding
BH Labs V2 & V3
Opened our second and Third vehicle lab in Detroit and Troy Michigan.

2022
Standardization & Regulation
Common services for vehicle cybersecurity are becoming clear as the industry is forced to adopt a standard approach and then audited.

2016
J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
Services start to see traction due to industry pressure.

Sc. B, Computer Engineering w/ a research focus on automotive cybersecurity.

2014
Our Journey
Securing vehicles is a people and process problem more than a technical problem. BH is founded as an automotive security service provider.

2023+
Products and Services
In the last decade Automotive figured out safety. In the present Block Harbor is defining how to solve the challenges in automotive security. BH is growing its team and leveraging our deep technical experiences from its service engagements to create product solutions that will solidify the future maturity of the industry.
MISSION
BUILDING GREAT SOLUTIONS FOR AUTOMOTIVE CYBERSECURITY TO KEEP MOBILITY SAFE.

VISION
A WORLD WHERE TECHNOLOGY & PEOPLE COEXIST SAFELY.

S - Security for Safety
H - Hunger for Success
I - Innovate the Industry
P - Pride in our Effort
Great Solutions. Where to start?
Vehicle Type

- Design Work Products
- Functional Safety ISO26262
- Nominal Function
- Design Function
- Design Functional Safety Concept
- Design Technical Security Concept
- Define Component SW & HW Safety Requirements
- Design Component SW & HW
- Verify Component SW & HW Safety Requirements
- Verify Component SW & HW
- Verify Technical Safety Concept
- Verify System
- Verify Technical Security Concept
- Design System
- Design Architecture
- Design Technical Security Concept
- Design Functional Safety Concept
- Define Security Goals
- Define Safety Goals
- Supplier-Created Work Products
- Supplier Defines Additional Technical Security Requirements
- Verification and Validation Work Products
- Production and Operations Work Products
- CSMS

NEW VULNERABILITY OR SOFTWARE UPDATE

Automaker & Supplier Create HW & SW Solution
NEW VULNERABILITY OR SOFTWARE UPDATE

Vehicle Type

Production and Operations Work Products

UNR 155 TYPE APPROVAL

Suppliers

CSMS
Work products throughout the lifecycle of the vehicle for regulatory approval.

It takes a lot of hands. It’s a people problem.

It takes a lot of tools. It’s an integration and automation problem.
Key challenges we run into:

- **One person** cybersecurity teams.
- Trying to use pre-21434 processes and tools.
- **Siloed** organizations.
  - Poor information exchange and organization
- Cybersecurity efforts are seen as **abrasive**.
  - Internal resistance can be high
- Cybersecurity is treated as important but **not always a priority** — tasked with the job, but not equipped to do it well.
  - Top level leadership must support cybersecurity as a priority
- Key activities are skipped or left incomplete making future steps in the V model ineffective
  - Everything falls on Pentesting at the end which is costly

So, who are the vehicle security engineers tackling this?
The People Problem

Key challenges we run into:

- **One person** cybersecurity teams.
- Trying to use pre-21434 processes and tools.
- **Siloed** organizations.
  - Poor information exchange and organization
- Cybersecurity efforts are seen as **abrasive**.
  - Internal resistance can be high
- Cybersecurity is treated as important but **not always a priority** – tasked with the job, but not equipped to do it well.
  - Top level leadership must support cybersecurity as a priority
- Key activities are skipped or left incomplete making future steps in the V model ineffective
  - Everything falls on Pentesting at the end which is costly
- IT security folks that pivoted.
- Automotive engineers that pivoted.
- Functional safety folks that took on additional responsibility.
- Recent graduates from the extremely new vehicle cybersecurity programs.
- Car hackers that turned it into a career.
Key challenges we run into:
• One person cybersecurity teams.
• Trying to use pre-21434 processes and tools.
• Siloed organizations.
• Cybersecurity efforts are seen as abrasive.
• Cybersecurity is treated as important but not always a priority – tasked with the job, but not equipped to do it well.

What does it mean to be a good automotive security engineer, anyway?
What does it mean to be a good automotive security engineer, anyway?

Understands...
• the fundamental cyber risks to vehicles.
• how vehicles are made and the technical details.
• the distribution of cyber responsibility through the supply chain.
• the standards and regulations well.
• how to build scalable processes to support in meeting the standards and regulations.
What does it mean to be a good automotive security engineer, anyway?
Key challenges we run into:
- One person cybersecurity teams.
- Trying to use pre-21434 processes and tools.
- Siloed organizations.
- Cybersecurity efforts are seen as abrasive.
- Cybersecurity is treated as important but not always a priority – tasked with the job, but not equipped to do it well.

And there sure are a lot of job openings...
What does it mean to be a good automotive security engineer, anyway?
Work products throughout the lifecycle of the vehicle for regulatory approval.

It takes a lot of hands. It’s a people problem.

It takes a lot of tools. It’s an integration and automation problem.
What about the toolchain, then?
It’s a logical toolset to start with. But what do we think it should look like?
Traceable and maintainable TARAs/Concepts at the Vehicle, System, and Component layers, integrated with Requirements Management System (RMS).

The first time around...

Automated V&V integrated with corresponding TARAs/Concepts

Supplier testing integrated into Automaker V&V process.

Monitoring in Production & Operations.

SUPPLIER DEFINES ADDITIONAL TECHNICAL SECURITY REQUIREMENTS

AUTOMAKER & SUPPLIER CREATE HW & SW SOLUTION

NEW VULNERABILITY OR SOFTWARE UPDATE

RE-DESIGN

RE-VERIFY

TARAs/Concepts are integrated with supplier-performed TARAs/Concepts
Maintenance...

Update TARA, Cybersecurity Concept

Work with supplier to get update or patch created

Supplier does their own V&V

Run automated V&V tests to update work products.

Release patch.

NEW VULNERABILITY OR SOFTWARE UPDATE

RE-DESIGN

RE-VERIFY

Automaker & Supplier Create HW & SW Solution

Supplier defines additional technical security requirements
Work products throughout the lifecycle of the vehicle for regulatory approval.

It takes a lot of hands. It’s a people problem.

It takes a lot of tools. It’s an integration and automation problem.
So, why does Block Harbor exist? What value do we add?
Block Harbor. Great Services First

Vehicle Cybersecurity Labs
- Vehicle/Subsystem/Component Penetration Testing
- Vehicle/Subsystem/Component Fuzzing
- Verification/Validation-as-a-Service (VaaS)
- Vehicle Cybersecurity Lab Buildout

Vehicle Security Operations
- Vehicle Security Operation Center (VSOC)
- Vehicle/Subsystem/Component Threat Analysis & Risk Assessment (TARA)
- Vehicle Cybersecurity Management System (CSMS)

Vehicle Cybersecurity Consulting
- ISO/SAE 21434, WP.29, & More

Some of our great customers.
est. 2014 in Detroit.
Threat Analysis & Risk Assessment (TARA) as a Service

Vehicle Cybersecurity Management System (CSMS)

Vehicle Cybersecurity Consulting: ISO/SAE 21434, UNECE WP.29, & more

Verification & Validation as a Service

Vehicle Security Operation Center

Vehicle Cybersecurity Lab Buildout

Vehicle, System, and Component Penetration Testing & Fuzzing
How are we addressing the people problem?
The Plunge

- **Phase 1: Automotive Cybersecurity Fundamentals I**
  
  Phase 1 is designed to orient you in the world of automotive cybersecurity. You should finish this phase with a general understanding of the importance of automotive cybersecurity, the risks involved in the industry, and the steps we take to manage the ever-increasing complexity of connected vehicles. Readings are listed at the top of each section. Assessments along the way will help guide your learning.

  - 1.1: Vehicle Cybersecurity Overview
  - 1.2: Automotive Attacks, Threats, and Vulnerabilities
  - 1.3: Introduction to Standards and Regulations
  - 1.4: Introduction to Risk Management
  - 1.5: Crypto Basics

- **Phase 2: Automotive Cybersecurity Fundamentals II**

  You got the basic concepts down. Now, it’s time to join us in analyzing the cutting edge of vehicle cybersecurity and the challenges that come with it. In truth, vehicle cybersecurity is not hard to achieve in isolation. Classic cybersecurity controls would go a long way. However, with so many different hands contributing to the development of a vehicle, with tight budgets, and very few industry experts, it becomes incredibly challenging. Thus, vehicle cybersecurity is not always a technical solution, but instead, a business solution. In this part, you’ll get a deeper understanding of what a solution in automotive cybersecurity means in reality.

  - Vehicle Cybersecurity Design Fundamentals
  - Vehicle Cybersecurity Verification & Validation Fundamentals

- **Phase 3: Deep Dive**

  If you’ve made it to this point, congratulations! You have a basic understanding of the fundamentals of automotive cybersecurity. It’s time for you to advance into your role-specific training.

  - Business Development
  - Vehicle Cybersecurity Labs
  - Organization
  - Vehicle Security Operations
But really, two birds with one stone: tools for automation.
Block Harbor. Great Solutions

Let's get started

**The Plunge**
On Demand Vehicle Cybersecurity Engineering Training

**Vehicle Breakdown**
Break down your vehicle into systems and components

**Lighthouse**
Import a TARA, generate a cybersecurity concept

**Harborbay**
Access virtual or physical vehicles for testing and training, including Block Harbor's Breakwater tests

**Harbormaster**
Automated vehicle cybersecurity requirement verification

**Harborview**
Live dashboard of cybersecurity requirement compliance across vehicles, systems and components
Our solution for Automated Verification & Validation (V&V) for Vehicle Cybersecurity built on top of Keysight’s Lab Operations platform.

Harbormaster.

BH designed this solution that we call Harbormaster. BH sets up and operates labs around co-designed Keysight HW/SW tailor built for ISO/SAE 21434 and UNR 155 V&V.

Breakwater: a suite of base vehicle cybersecurity test scenarios for UNR 155 Mitigations

Vehicle Cybersecurity Lab

Keysight Automotive Cybersecurity Testing Platform

Vehicle cybersecurity V&V test results

Keysight LabOps platform orchestrates testing and manages results for UNR 155.
Establish win-win partnerships with Vehicle Cybersecurity Design and Engineering (e.g. TARA) tool providers to build toward integration for left-side-of-V model activities into Harborview.
Further open and research projects.
Open Source CSMS, AVCDL

The AVCDL is a set of identified processes, requirements of those processes, generated products, and mappings from the generated products to their corresponding certification standard (ISO/SAE 21434, UNECE WP.29 R155-7) work products: for the purpose of ensuring the creation of secure systems.

https://github.com/nutonomy/AVCDL, Lead: Charles Wilson
OpenXSAM – Data exchange format between tools for vehicle cybersecurity.

```xml
<openXSAM>
  <ItemDefinition>
    <Functions>…</Functions>
    <Components>…</Components>
    <Data>…</Data>
    <Channels>…</Channels>
  </ItemDefinition>
  <CSConcept>
    <Risks>
      <Risk name="Confidentiality of UDS-based FOTA update on CAN 7" treatment="REDUCE">
        <CSGoal verificationStatus="passed" validationStatus="passed">
          <CSRequirement verificationStatus="passed" validationStatus="passed">
        </CSRequirement>
      </CSGoal>
    </Risk>
  </Risks>
</openXSAM>
```

Open data format for tool integration for real-time vehicle cybersecurity engineering.
Other BH Projects

- 2021 Ford Mach E, demonstration/research vehicle.
- Virtual Vehicle Cybersecurity Lab: enable remote interfacing on physical vehicle products to reduce the hardware needs for research and training.
- ASRG
- ASRG Threat Catalog – Database of threats.
- ASRG CVEs – Database of CVEs focused specifically on vehicles.
At Block Harbor, we’ve been building great solutions to keep mobility safe since 2014.

We have the right onboarding program to build competent people to perform our services.

We build great products to automate the workload for UNR 155, and we’re building the ecosystem of products and services to support in making vehicle cybersecurity engineering efficient.
Building great solutions to keep mobility safe.
contactus@blockharbor.io