Block Harbor. Cybersecurity

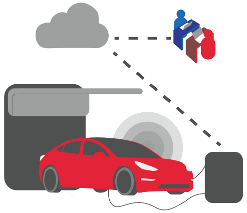
Security Testing Services

Vehicle Cybersecurity Lab (VCL)

Overview.

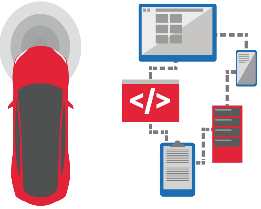
- Services
- Differentiators
- ASPICE V-Model Security Testing
- Lab Services
  - Offerings
  - Customers
  - Expertise at Work
  - Process
- Next Steps

Block Harbor. Services



Vehicle Cybersecurity Labs (VCL)

- Functional Security Assessments (Verification)
- Penetration Assessments (Validation)
- Fuzz Testing
- Reverse Engineering
- Secure Code Review
- Regression Testing



Vehicle Security Operations (VSO)

- Vehicle Security Operation Center (VSOC)
- Threat Analysis & Risk Assessment (TARA)
- Cybersecurity Management System (CSMS)
- Security Concept Design & Requirement Definitions

Some of our great customers.

HARM VOLVO NIKOLA Ford

STELLANTIS DANA LORDSTOWN

BorgWarner DENSO Togg

APTIV GENTHERM DANLAW

Volkswagen BOSCH HL Mando

Est. 2014 in Detroit, MI.

BH.

Block Harbor. Differentiators

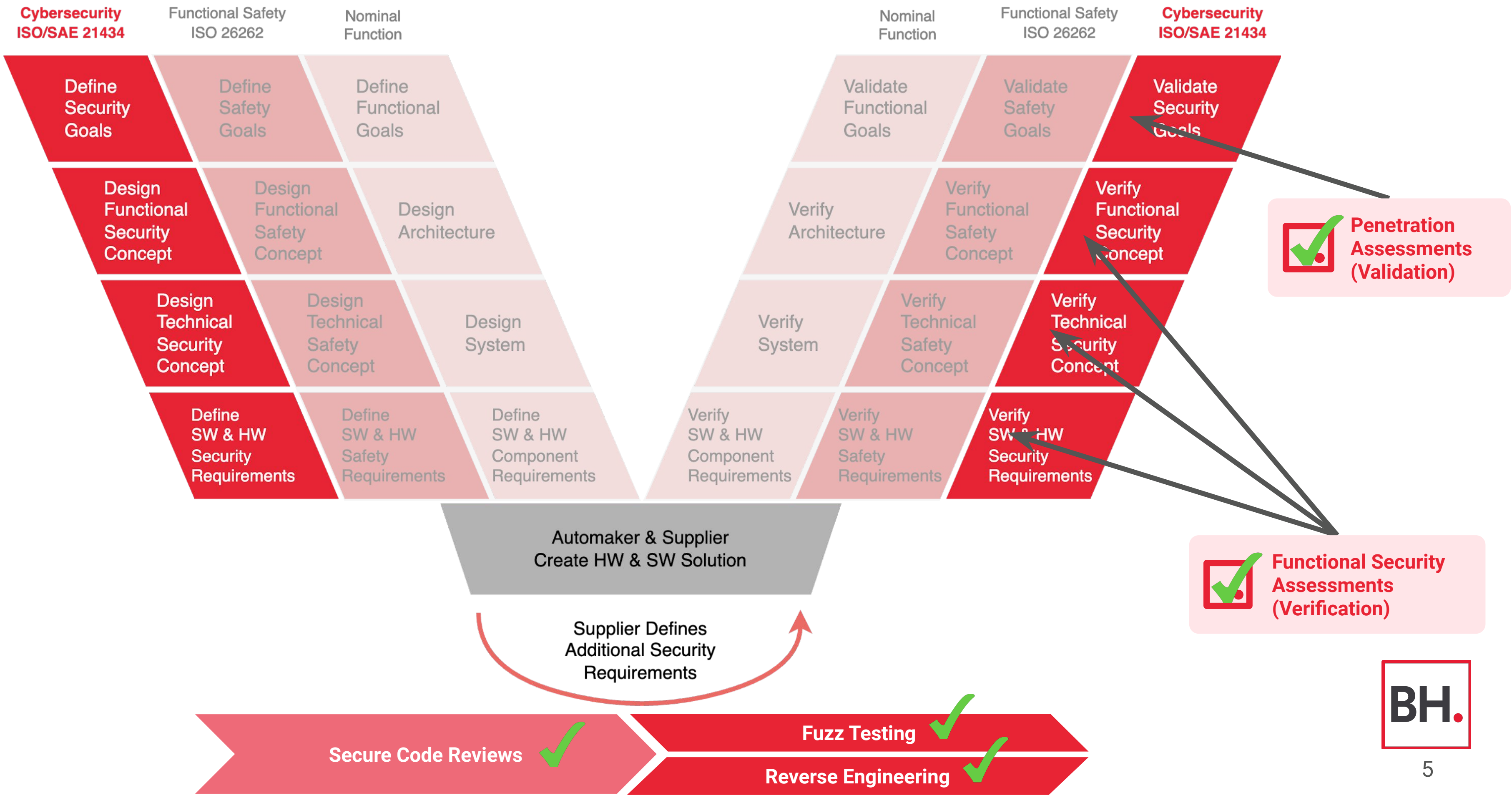
Expertise:

- Block Harbor has years of experience working alongside OEMs and Tier 1 suppliers.
- Focused on what we do best, automotive cybersecurity.
- Block Harbor engineers have consistently placed in the DEFCON Car Hacking Village CTF.
  - 2023 - 2nd Place
  - 2022 - 2nd Place
  - 2021 - 2nd Place
  - 2020 - 2nd Place
  - 2019 - 1st Place
  - 2018 - 3rd Place

Customer-Centric Approach:

- We do what it takes to make the client successful and project a success.
- Critical vulnerabilities or weaknesses are immediately reported.
- As a boutique security firm we are quick to deliver results and flexible in meeting challenging timelines.

ASPICE V-Model. Security Testing



Cybersecurity ISO/SAE 21434

Functional Safety ISO 26262

Nominal Function

Define Security Goals

Define Safety Goals

Define Functional Goals

Design Functional Security Concept

Design Functional Safety Concept

Design Architecture

Design Technical Security Concept

Design Technical Safety Concept

Design System

Define SW & HW Security Requirements

Define SW & HW Safety Requirements

Define SW & HW Component Requirements

Nominal Function

Functional Safety ISO 26262

Cybersecurity ISO/SAE 21434

Validate Functional Goals

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 SW & HW Component Requirements

Verify SW & HW Safety Requirements

Verify SW & HW Security Requirements

Automaker & Supplier Create HW & SW Solution

Supplier Defines Additional Security Requirements

Penetration Assessments (Validation)

Functional Security Assessments (Verification)

Secure Code Reviews ✓

Fuzz Testing ✓

Reverse Engineering ✓

BH.

Lab Services. Offerings

Functional Security Assessment (Verification)

★ Starting around

USD $20,000+

★ Timeline

2 - 4 weeks

When to Consider?

- Verifying the security requirements of a device
- Support for UN R 155 and ISO/SAE 21434

Entails:

- Conformance Testing
- Vulnerability Scanning
- Binary Composition Analysis

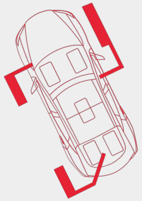
Penetration Assessment (Validation)

★ Starting around

USD $40,000+

★ Timeline

4+ weeks



When to consider?

- Validating the security goals of device
- Testing the unknown, similar to safety validation testing (ISO 26262)

Entails:

- Vulnerability Scanning
- Binary Composition Analysis
- Configuration Reviews
- In-Depth Vulnerability Exploitation
- Interface / Protocol Testing
- Dynamic Security Testing

Add-On Services

★ Timeline

Customer Defined

Fuzz Testing

★ Starting around

USD $20,000+

Reverse Engineering

★ Starting around

USD $50,000+

Secure Code Review

★ Starting around

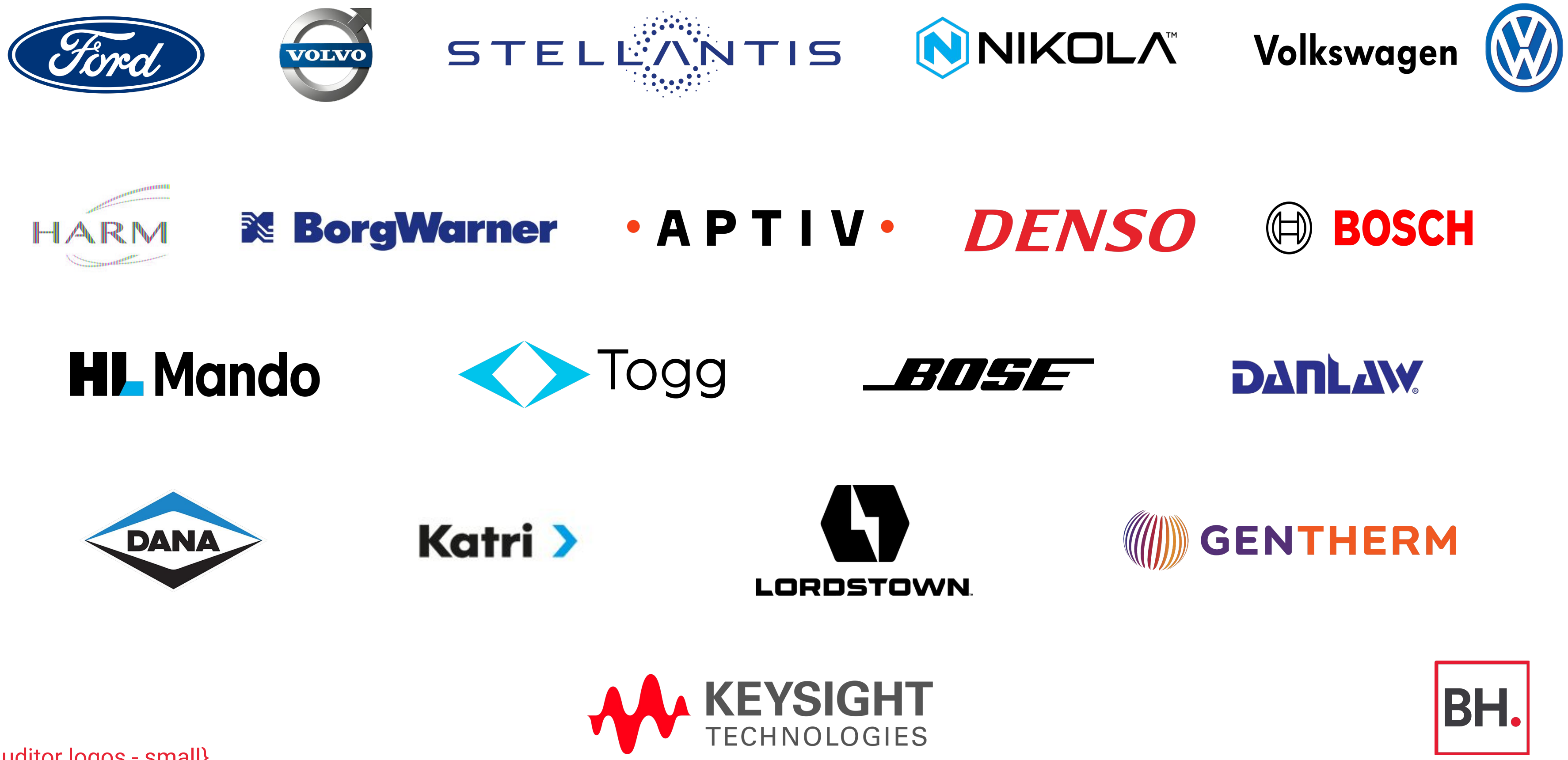
USD $20,000+

Regression Testing

★ Starting around

USD $20,000+

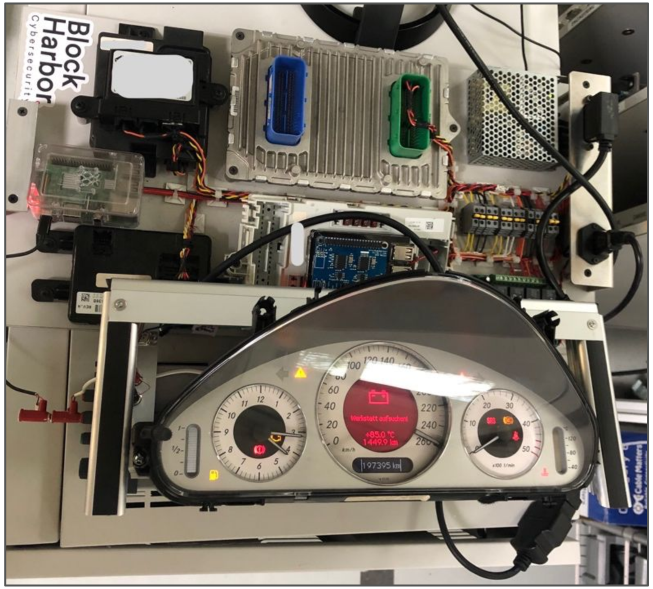
Lab Services. Customers



{Insert auditor logos - small}

BH.

Lab Services. Expertise at Work



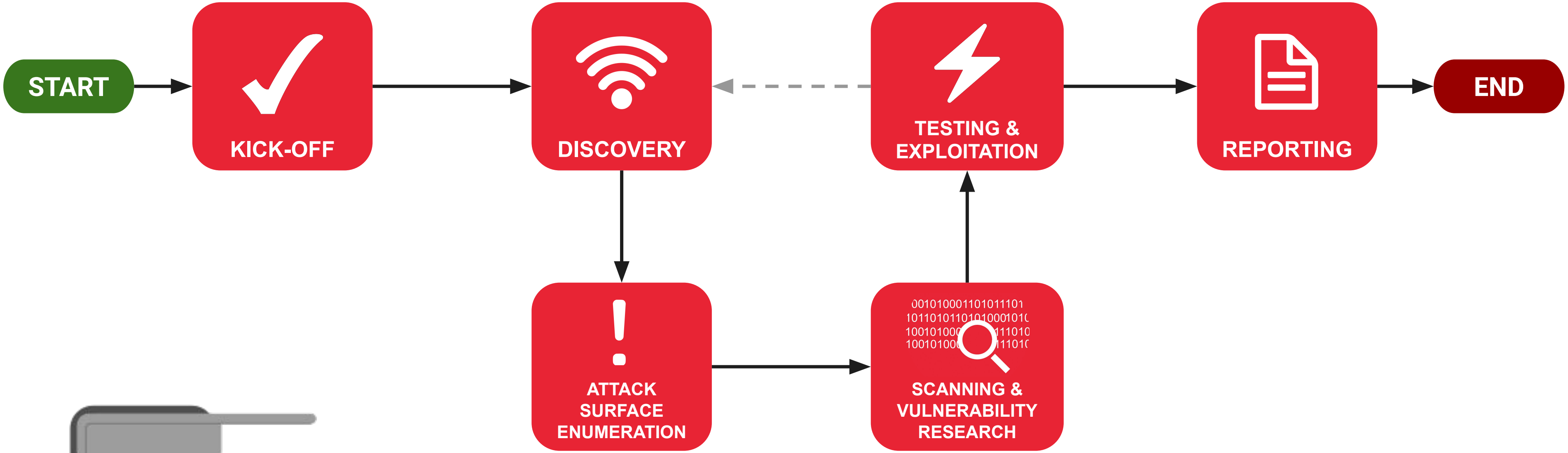
Component(s)

Hardware-in-the-loop

Full Vehicle

Automotive / Heavy Trucking / Electric

Lab Services. Process


START

KICK-OFF

DISCOVERY

ATTACK SURFACE ENUMERATION

SCANNING & VULNERABILITY RESEARCH

TESTING & EXPLOITATION

REPORTING

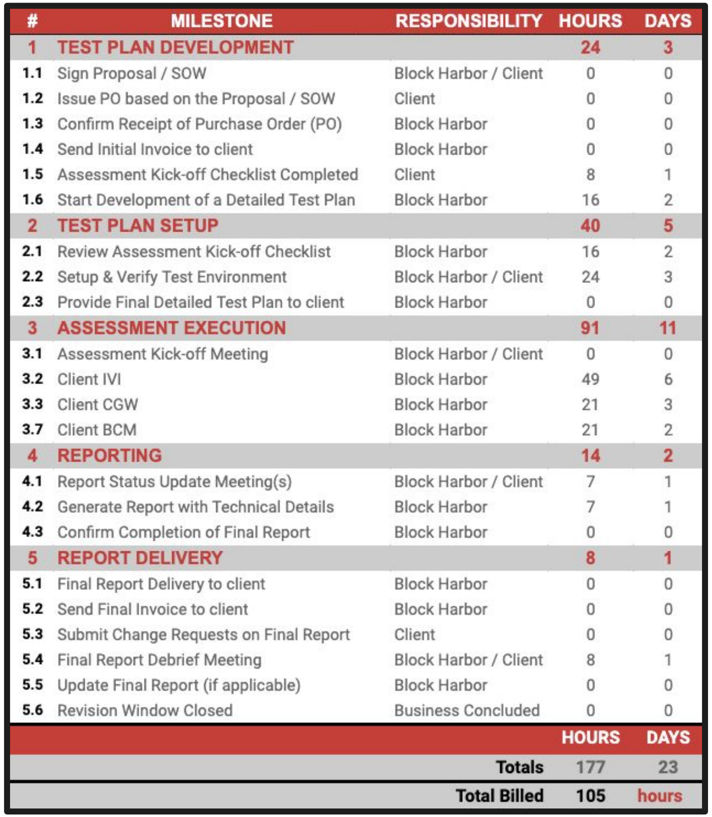
END

Next Steps. Discovery Phase (~2-4 weeks)

1. **[Introduction Meeting]**
   Meeting to discuss Block Harbor Security Testing Services.
2. **[NDA Exchange]**
3. **[Scope / Objectives Meeting]**
   Meeting to understand the scope of the system(s) and/or device(s) to be assessed.
4. **[Rules of Engagement Meeting]**
   Meeting to detail the rules of engagement and finalize the scope for the assessment.
   [Output: Proposal and Estimated Statement of Work]

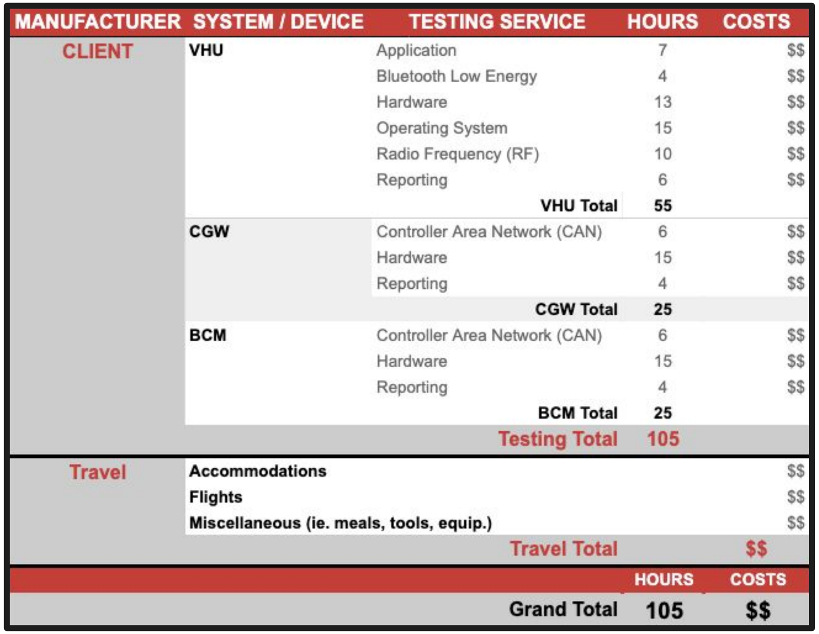
Discovery Phase. Proposal + SOW

Sample Statement of Work



#	MILESTONE	RESPONSIBILITY	HOURS	DAYS
1	TEST PLAN DEVELOPMENT		24	3
1.1	Sign Proposal / SOW	Block Harbor / Client	0	0
1.2	Issue PO based on the Proposal / SOW	Client	0	0
1.3	Confirm Receipt of Purchase Order (PO)	Block Harbor	0	0
1.4	Send Initial Invoice to client	Block Harbor	0	0
1.5	Assessment Kick-off Checklist Completed	Client	8	1
1.6	Start Development of a Detailed Test Plan	Block Harbor	16	2
2	TEST PLAN SETUP		40	5
2.1	Review Assessment Kick-off Checklist	Block Harbor	16	2
2.2	Setup & Verify Test Environment	Block Harbor / Client	24	3
2.3	Provide Final Detailed Test Plan to client	Block Harbor	0	0
3	ASSESSMENT EXECUTION		91	11
3.1	Assessment Kick-off Meeting	Block Harbor / Client	0	0
3.2	Client IVI	Block Harbor	49	6
3.3	Client CGW	Block Harbor	21	3
3.7	Client BCM	Block Harbor	21	2
4	REPORTING		14	2
4.1	Report Status Update Meeting(s)	Block Harbor / Client	7	1
4.2	Generate Report with Technical Details	Block Harbor	7	1
4.3	Confirm Completion of Final Report	Block Harbor	0	0
5	REPORT DELIVERY		8	1
5.1	Final Report Delivery to client	Block Harbor	0	0
5.2	Send Final Invoice to client	Block Harbor	0	0
5.3	Submit Change Requests on Final Report	Client	0	0
5.4	Final Report Debrief Meeting	Block Harbor / Client	8	1
5.5	Update Final Report (if applicable)	Block Harbor	0	0
5.6	Revision Window Closed	Business Concluded	0	0
			HOURS	DAYS
		Totals	177	23
		Total Billed	105	hours

Sample Proposal



MANUFACTURER	SYSTEM / DEVICE	TESTING SERVICE	HOURS	COSTS
CLIENT	VHU	Application	7	$$
		Bluetooth Low Energy	4	$$
		Hardware	13	$$
		Operating System	15	$$
		Radio Frequency (RF)	10	$$
		Reporting	6	$$
		VHU Total	55	
	CGW	Controller Area Network (CAN)	6	$$
		Hardware	15	$$
		Reporting	4	$$
		CGW Total	25	
	BCM	Controller Area Network (CAN)	6	$$
		Hardware	15	$$
		Reporting	4	$$
		BCM Total	25	
		Testing Total	105	
Travel	Accommodations			$$
	Flights			$$
	Miscellaneous (ie. meals, tools, equip.)			$$
		Travel Total		$$
			HOURS	COSTS
		Grand Total	105	$$

BH.

Next Steps. Engagement Phase

5. **[Proposal Signed and Purchase Order Received]**

6. **[Final Scope Meeting]**
   Meeting to confirm the scope and rules of engagement for the assessment are aligned and scheduled.

7. **[Assessment Kick-Off Meeting]**
   Meeting to officially state that testing has begun.

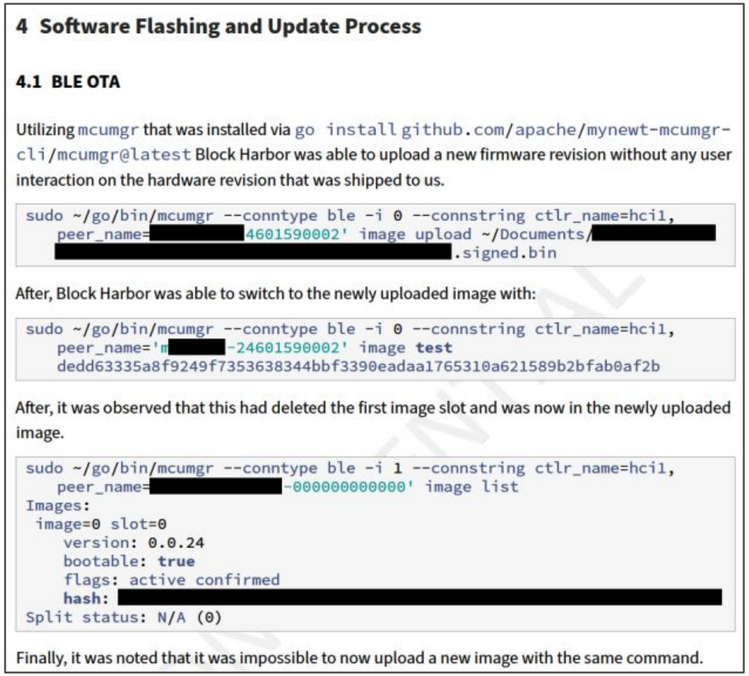
8. **[Reporting Meeting(s)]**
   Weekly or Bi-Weekly status update meetings to discuss any issues, urgent findings or request for additional information.

9. **[Report Delivery]**
   Completed report of the assessment for the system(s) and/or device(s) under assessment.
   [Output: Final Report]

10. **[Final Report Review Meeting]**
    Meeting to review the completed report of the assessment for the system(s) and/or device(s) under assessment.
    [Output: Updated Final Report] (OPTIONAL)

Engagement Phase. Reporting

Redacted Report Example



4 Software Flashing and Update Process

4.1 BLE OTA

Utilizing `mcumgr` that was installed via `go install github.com/apache/mynewt-mcumgr-cli/mcumgr@latest` Block Harbor was able to upload a new firmware revision without any user interaction on the hardware revision that was shipped to us.

```
sudo ~/go/bin/mcumgr --conntype ble -i 0 --connstring ctlr_name=hci1,
    peer_name=[redacted]4601590002' image upload ~/Documents/[redacted]
    [redacted].signed.bin
```

After, Block Harbor was able to switch to the newly uploaded image with:

```
sudo ~/go/bin/mcumgr --conntype ble -i 0 --connstring ctlr_name=hci1,
    peer_name='[redacted]-24601590002' image test
    dedd63335a8f9249f7353638344bbf3390eadaa1765310a621589b2bfab0af2b
```

After, it was observed that this had deleted the first image slot and was now in the newly uploaded image.

```
sudo ~/go/bin/mcumgr --conntype ble -i 1 --connstring ctlr_name=hci1,
    peer_name=[redacted]-000000000000' image list
Images:
 image=0 slot=0
    version: 0.0.24
    bootable: true
    flags: active confirmed
    hash: [redacted]
Split status: N/A (0)
```

Finally, it was noted that it was impossible to now upload a new image with the same command.

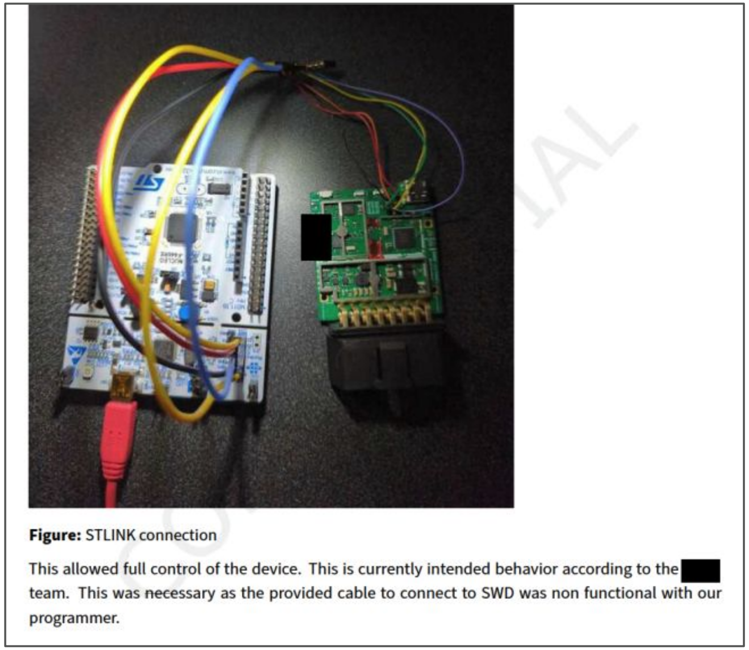


Figure: STLINK connection

This allowed full control of the device. This is currently intended behavior according to the [redacted] team. This was necessary as the provided cable to connect to SWD was non functional with our programmer.

https://blockharbor.io/wp-content/uploads/2024/03/BH_Redacted-Report_2024.pdf

Block Harbor.

Cybersecurity

Building great solutions to keep mobility safe.

contactus@blockharbor.io