Vehicle Cybersecurity Management System (CSMS) Consulting

ISO/SAE 21434 and UNECE WP.29 are creating pressure to implement a Cybersecurity Management System (CSMS) throughout the supply chain.

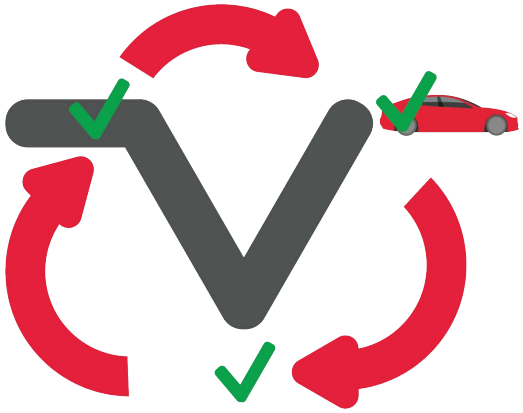
The automotive industry is undergoing vehicle security standardization and regulation that enforces consistent process and work products as proof to auditors. Automakers and suppliers are implementing CSMS following ISO/SAE 21434 for UN R155.

What is CSMS?

A Cybersecurity Management System is an organizational framework commonly used in Automotive to provide a consistent and thorough framework to engineer vehicles securely and ensure they stay secure. With ISO/SAE 21434 as an industry standard, that means defining the item and identifying risks in the Concept Phase, designing/implementing/verifying/validating in the Product Development Phase, and ensuring ongoing security efforts in the Post-Development Phase. The risks identified along the way are required to be managed by mandate of UNR 155 and further controlled by UNR 156.

A CSMS consists of a set of processes to generate work products as evidence for auditors. With ISO/SAE 21434 following the well-known V-Model in the automotive industry and structured to parallel ISO 26262 for functional safety, a CSMS is intentionally a slow and deliberate process. In functional safety, the V-Model works well because once the vehicle is designed safely, it typically stays safe. However, Cybersecurity (unlike functional safety) moves very fast: a new feature release via a software update or a vulnerability release could result in vulnerable vehicles on the road. That means a CSMS has to be both deliberately slow and able to identify and process new risks quickly to release a patch and keep road users secure and safe.

A CSMS is a large effort that typically requires stakeholders from all parts of the organization to be involved, with a core product cybersecurity team leading the way. Rather than starting from scratch, **Block Harbor contributes to and leverages the open-source "Autonomous Vehicle Cybersecurity Development Lifecycle" (AVCDL) to help customers more quickly and effectively implement a CSMS.***



How we work

Before Project Kick-off

Getting started

Customers provides project, product safety and security processes based on our questionnaire to help define the scope of CSMS implementation. Once we have a strong understanding of the existing organization's capabilities, Block Harbor provides a quote and proposal that details the effort it'll take to define a road map for a successful CSMS.

After Project Kick-off

Block Harbor leverages the AVCDL to map the customer's existing processes capabilities to the framework. Then, with a clear understanding of the gaps to a functioning CSMS, Block Harbor identifies and tailors AVCDL processes and templates to provide the core framework for the customer's CSMS based on our experience with different automakers and suppliers. Block Harbor supports the customer in making core decisions, such as distributing security responsibilities among existing resources through training or by identifying the roles necessary to fulfill the necessary responsibilities.

Block Harbor will provide template processes, template work products, a detailed CSMS implementation plan and report with an overview of the recommendations shared.

*https://github.com/nutonomy/AVCDL

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.

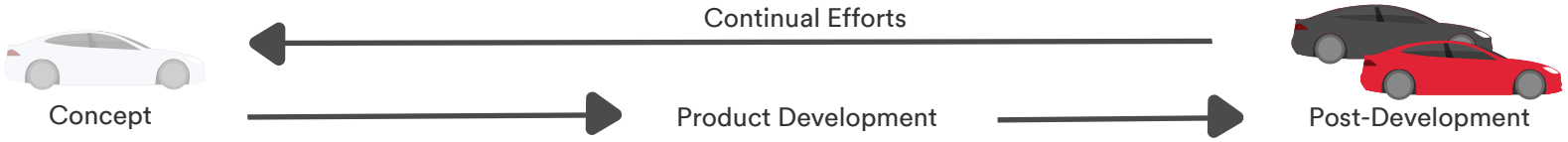
- Vehicle Cybersecurity Labs
  - -Penetration Testing
  - -Fuzzing
  - -V&V-as-a-Service
  - -Vehicle Cybersecurity Lab Buildout
- Vehicle Security Operations
  - -Vehicle Security Operation Center (VSOC)
  - -Threat Analysis and Risk Assessment (TARA)
  - -Vehicle Cybersecurity Management System (CSMS)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

Block Harbor. Cybersecurity

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

Vehicle Cybersecurity Management System (CSMS) Consulting

ISO/SAE 21434 and UNECE WP.29 are creating pressure to implement a Cybersecurity Management System (CSMS) throughout the supply chain.



Solution In Depth

Common Challenges Implementing CSMS

Getting Started with ISO/SAE 21434

Whether autonomous vehicle company, supplier, or automaker, we frequently encounter organizations just getting started with ISO/SAE 21434. Typically, it begins with cybersecurity responsibilities being added to those responsible for functional safety or a new role being created to address new requirements and customer asks. When looking to the standard itself, it provides little guidance on how to realistically implement a functioning cybersecurity management system at your organization. That's why we start with a proven approach -- the AVCDL -- that both supports in meeting ISO/SAE 21434 while taking into account modern development processes and challenges. AVCDL provides an unparalleled starting point for vehicle cybersecurity management systems. And best of all, it's free and open.

Understanding the Organization

One of the biggest challenges in implementing ISO/SAE 21434 is trying to make it fit into how the organization functions. Questions quickly arise like:

- Will you need a new, dedicated cybersecurity team to fulfill the work products of a CSMS?
- Can you distribute the responsibilities among existing team members?
- Can you simply build ISO/SAE 21434 processes on top of existing processes for ISO 26262 (functional safety)?
- How do traditional IT security processes fit in with ISO/SAE 21434 processes?

Block Harbor spends a significant amount of time understanding how your organization works first to have a clear understanding of how to design a CSMS that will function well.

Execution & Delivery

Mapping Existing Processes & Process Development

With a clear understanding of the customer's processes & capabilities, Block Harbor maps each existing process for possible reuse in the CSMS. Where there are remaining gaps, Block Harbor works with the customer to develop a new process via workshops to ensure that each requirement of ISO/SAE 21434 is met. Then, Block Harbor workshops each work product template within the AVCDL to ensure the customer has a clear understanding of the intended function of each part of the CSMS, including possible tool usage to properly perform functions in the CSMS. With processes and template work products defined, Block Harbor spend additional time focusing on the intended outcome of the engineering process in ISO/SAE 21434: the cybersecurity case. By doing this, we ensure that the customer has a clear understanding of what the customer is ultimately intending to make an argumentation for around their processes and work products to make a case for its cybersecurity.

Weekly or bi-weekly meetings with the customer can be hosted to share the status of the compliance model development and supporting activities and tool configuration. These discussions are agile and facilitate sharing of any early findings which may provide an opportunity to the customer to fix critical process shortcomings sooner in their than waiting for the final report.

CSMS Implementation Plan

In addition to providing the framework processes and templates around the CSMS, Block Harbor identifies the roles and responsibilities that need to be fulfilled in the resulting CSMS. We spend time understanding the organizations resources and goals to identify a realistic road map and plan to realize the CSMS. For example, we identify the possible new hires, including role description, that the organization may make over the following year to achieve the efforts necessary in the CSMS. The intention of the CSMS implementation plan is to help the customer plan and budget accordingly to be successful in their implementation.

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