# Supporting Connected, Autonomous, Shared, and Electric (CASE) Vehicle Security Using SBOMs

FINITE STATE

FINITE STATE

**Software bill of materials (SBOM) for emerging connected, autonomous, shared, and electric (CASE) vehicles is a sensible cybersecurity control in this emerging area. The Finite State platform[1] is shown to be effective in supporting CASE threat protection objectives.**

The rising use of connected, autonomous, shared, electric (CASE) vehicles is an unmistakable trend in both the United States and abroad. With sustainability being the driving force behind this shift, it has also introduced a wide range of new cybersecurity risks, since these emerging vehicles will be so highly dependent on software and connectivity.

**The automotive industry is facing a crossroads:** It has to evolve to support more complex use cases for customers as much as it needs to refactor cybersecurity standards to ensure driver safety and manufacturer assurance. The reality is that insecure versions of open-source components in first and third-party automotive products are the most common security weakness in automotive software. In some cases, vulnerabilities identified can be patched, but the component, once used in a vehicle, has not been or cannot be updated.

[1] See https://finitestate.io/ for information on the Finite State cybersecurity platform including its support for Software Bill of Materials (SBOM).

FINITE STATE

**This is a software supply chain problem of epic proportions:** The lack of updates for open-source components containing vulnerabilities is now a problem for automakers worldwide. While patching software in automobiles presents a challenge, ensuring the software supply chain is continuously secure brings a level of complexity that many AppSec and product security teams are not prepared to deal with. Creating software transparency in the automotive sector starts with an SBOM (Software Bill of Materials).

An SBOM provides a detailed inventory of the packages, libraries, and components that were used to create the software. Experts have already begun to offer useful comments on the usefulness of SBOMs for emerging vehicle security.

In this note, we discuss how SBOMs can help protect CASE vehicles from cyber threats. In particular, we show how an SBOM can reduce the day-to-day cyber risk to vehicles and their support infrastructure, while also helping to establish and maintain compliance with cybersecurity requirements. The Finite State platform is shown to provide effective support for these objectives.

## What is an SBOM?

As suggested above, the global software industry has begun to address cyber risk through the use of a software bill of materials (SBOM), which is an artifact created using various techniques, including compositional analysis of the software. The goal of an SBOM is increased visibility into the software to highlight cyber risk issues related to software status, versioning, update, origin, and so on. Mainstream observers sometimes refer to an SBOM as an ingredient listing.

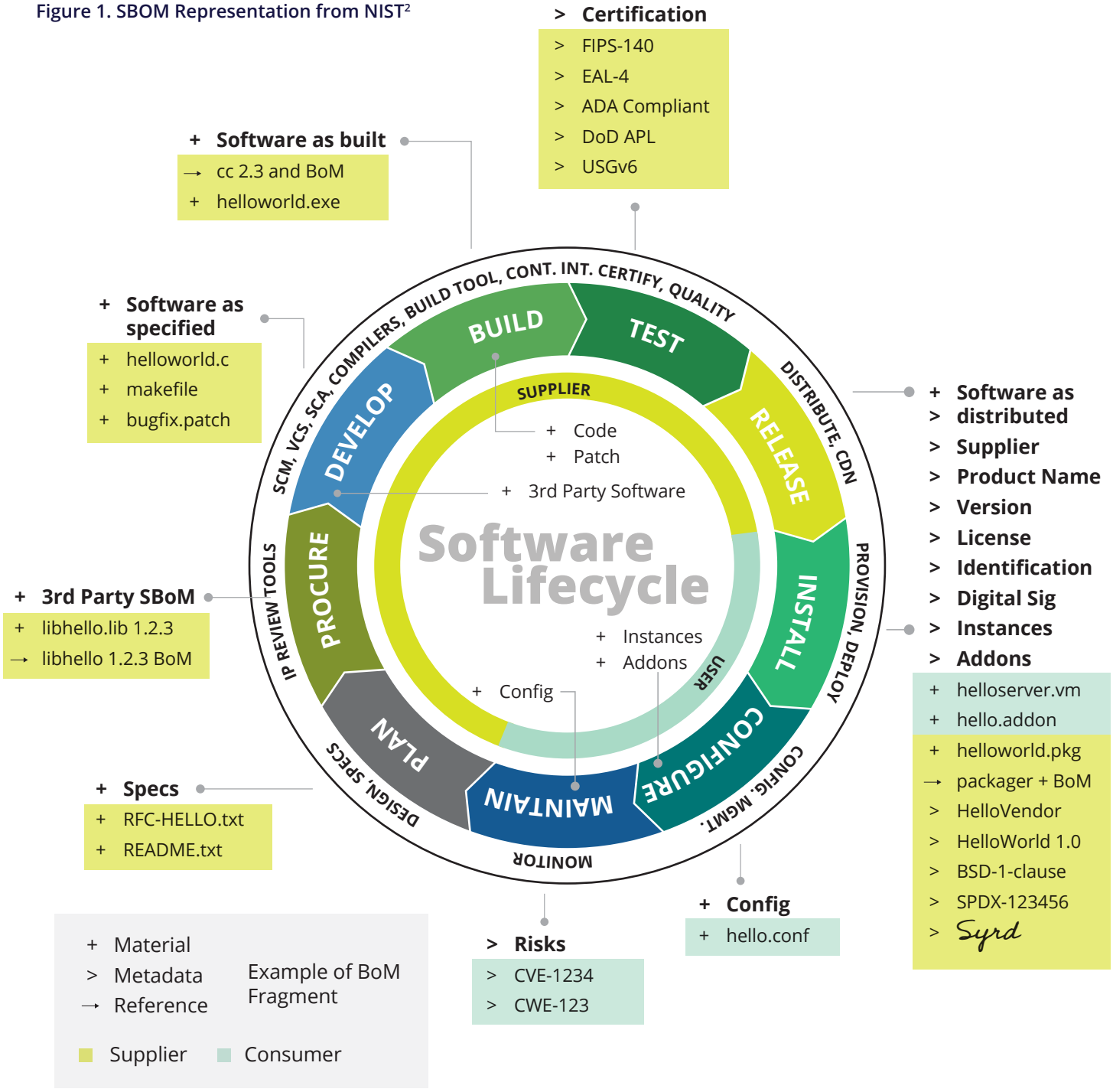
A software bill of materials (SBOM) specifically provides useful detailed data about open-source and third-party components included in the codebase. This information provides insight into the software licenses, lists the versions of software components, and highlights patch status of relevant components. From a security perspective, the main objective for SBOMs is to support vulnerability management, incident response, and other tasks.

Ultimately, an SBOM is an inventory, which is not different than one would find in any type of product manufacturing. (The software industry has lagged in this area for many years but is now catching up.) Consider that when vehicles are assembled, the manufacturer maintains a list of components used for that specific vehicle. If product defects demand a recall, then this bill of materials streamlines the notification and repair process.

SBOMs are driven by cybersecurity use-cases involving reported vulnerabilities in open-source or third-party software utilities. Any security team, especially in industrial control system (ICS) and operational technology (OT) settings, could use an SBOM to determine if their product or service includes a given vulnerable component, which would obviously simplify the incident response and update process.

Ultimately, an SBOM is an inventory,
**which is not different than one would find in any type of product manufacturing.**

Figure 1. SBOM Representation from NIST[2]




[2] See https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1 for detailed information on SBOM usage across government, business, and industrial control settings.

## What is the Regulatory Situation for Vehicles?

Recent regulations including UN Regulation No 155 on Cyber Security and Cyber Security Management Systems have heightened the conversation regarding vehicle security. One would expect such momentum to accelerate as cars and other types of transport become more connected and autonomous, consistent with CASE trends. The types of requirements included in the UN Regulations and that are representative of best practice in this area include:

- Establishing an explicit program that manages the cyber risks to vehicles.
- Developing vehicles consistent with a demonstrable secure by design approach.
- Implementing a security detection and response program for vehicles and fleets.
- Ensuring secure software updates for vehicles to prevent malware transmission.
- Securing over the air (OTA) updates to vehicles.

The introduction of such constraints is a welcome regulatory action, and in the next section, we outline how SBOMs, in particular, can offer useful support for the security and integrity of vehicles — especially in the context of CASE.

## Can SBOMs Help Address Cyber Threats to CASE?

Two categories of cyber threat issues will most certainly emerge with respect to CASE vehicles. The first involves the evolution of security compliance frameworks to include CASE usage scenarios. The second involves the day-to-day operational threats that will come from a range of actors including mischievous hackers (dating back to the earliest public hack of a moving vehicle) to nation-state actors targeting the transportation infrastructure of their adversary.

In the context of compliance, CASE vehicles will be subjected to two type of framework requirements:

**Specialized Frameworks —** These will drive detailed CASE security compliance obligations and will be developed by industry experts. ISO/SAE 21434 and UNECE WP.29 R155 come to mind as typical standards with some domain specificity here.

**General Frameworks —** This will include the more generic cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF), which could easily be amended to include reference to CASE, given its massive future prominence as a use-case.

**In addition to the software (the most complex aspect of any CASE vehicle), the hardware components, including the battery, will also benefit from bill of materials attention.**

In each of these compliance cases, it is worth mentioning that compositional analysis and software provenance are likely to be required — which bodes well for the use of SBOMs. In the context of day-to-day cyber threats, one should expect CASE vehicles to be subjected to cyber-attacks involving the following areas of emphasis:

**Moving Vehicles —** This will involve attacks to vehicles across its communication interface. They can originate from other vehicles, smart road signs, or other environmental components that are either hijacked or malicious.

**Support Infrastructure —** This will involve attacks from the support, maintenance, and operational infrastructure for the CASE vehicle. Manufacturers will have the primary obligation to keep this aspect of the ecosystem secure.

**Vehicle Supply Chain —** This involves Trojans, malware, trap doors, and viruses finding their way into the CASE vehicle through some package, component, patch, or update to the CASE software.

As one might expect, SBOMs are useful in each of these threat cases, but connect most directly with the supply chain requirement. It should be expected that along with the traditional "sticker" for existing vehicles displayed in a showroom, that future CASE vehicles might come with an SBOM "sticker" that will help buyers understand the composition of the CASE vehicle.

It should be noted that while our emphasis here is on the software, which will be by far the most interesting and complex aspect of any CASE vehicle, the hardware components, including the battery will also benefit from bill of materials attention.

## Case Study: Finite State SBOM Management

Finite State offers an SBOM platform for use by enterprise security teams, including in the ICS and OT space. Such emphasis makes Finite State a good future choice for emerging CASE vehicles and their environment. The platform can be deployed to the CASE ecosystem to identify vulnerabilities, exploitable weaknesses, and zero-day issues in newly deployed CASE infrastructure, including manufacturing environments.

Finite State helps to illuminate supply chain issues, especially for connected devices and embedded systems, which are two application areas tightly integrated with emerging CASE ecosystems and that are particularly prone to cyber-attacks with high consequences. As such, Finite State directs cyber risk profile analysis using SBOMs via the following functional platform features:

**Continuous Visibility —** This involves providing data regarding supply chain components for all software packages, which is expected to be particularly important in complex emerging CASE environments.

**Knowledge and Confidence —** This involves providing cybersecurity teams with an understanding of the risk that new or existing software/devices are introducing into their environments. CASE manufacturers and drivers will require this confidence.

**Context —** This involves providing a mechanism such as objective scoring by which CASE security performance against competitors and historical progress can be measured. (Perhaps this will be part of the SBOM "sticker" concept mentioned earlier.)

**Comprehensive SBOM —** This is the construct for a bill of materials that CASE ecosystems can use to reduce their cyber risk profiles. The typical CASE operational environment will be highly complex, so SBOMs will grow in complexity as well.

**Owner Verification —** This involves collaboration with the CASE manufacturer and any ecosystem partners including software developers, drivers, and other entities to establish and provide verification of source origin.

Each of these Finite State features has the great advantage of providing live views into risk being introduced into future CASE infrastructure. The resulting improvements to the management of software supply chain risk will help with prevention of threats as well as assurance of continuous compliance with required frameworks.

## About Finite State

Finite State empowers organizations to gain control of application and product security for their connected devices and software supply chains. Across the software supply chain lifecycle, Finite State is the single pane of glass for customers that provides continuous visibility into software supply chain risk.

Backed by a team of seasoned experts, Finite State's platform arms customers with the automation to scale risk mitigation and 2B+ data points to deliver actionable SBOM's and insights, critical vulnerability data and the remediation guidance necessary to mitigate AppSec and product risk to protect the connected attack surface.

FINITE STATE

finitestate.io