Jama software®

EBOOK

A Guide to Road Vehicle Cybersecurity According to ISO 21434

Table of Contents

1 Introduction

Introduction

As the automotive industry becomes more complex, and more connected, cybersecurity is emerging as a major concern, and therefore priority, for development teams.

While vehicles have been traditionally isolated systems that had to be physically accessed to tamper with, increasingly, more and more vehicles include wireless connectivity. According to Juniper Research, the number of vehicles with wireless connectivity will rise from 110 million in 2020 to an excess of 200 million by 2025. These vehicles pose a much greater cybersecurity risk than previous designs.

One standard in particular has been developed to address cybersecurity risks in the design and development of car electronics – ISO SAE 21434 “Road vehicles — Cybersecurity Engineering.”

In this guide, we will examine this important automotive cybersecurity standard, how it is impacting automotive development, and lastly how Jama Software® can help.

2 What is Automotive Cybersecurity?

What is Automotive Cybersecurity?

Cybersecurity, within the context of road vehicles, is the protection of automotive electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation.

What is ISO 21434?

Regarded as one of the most comprehensive approaches to connected vehicle cybersecurity, ISO 21434 specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance, and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

This standard supports the implementation of a Cybersecurity Management System (CSMS).

The first edition of ISO 21434 was published in 2021 and automotive suppliers and OEMs should strongly consider integrating ISO 21434 into their current process.

What is a Cybersecurity Management System (CSMS)?

A Cybersecurity Management System is a systematic risk-based approach defining organizational rules and processes, security policies, resources, and responsibilities to manage risk associated with cyber threats to vehicle road users and protect them from cyber-attacks.

3 What is the Urgency Behind Automotive Cybersecurity?

What is the Urgency Behind Automotive Cybersecurity?

From a Market Perspective:

As automobiles are growing increasingly connected, digitized, and complex, cybersecurity has become top of mind. Made up of hundreds of “tiny computers” – each with their own networks and servers – a singular vehicle is open to millions of opportunities for cyber-attack.

In fact, computers control almost every system in a vehicle, from steering to brakes, to the engine itself. Electric Vehicles (EV) have even more opportunity for cyber-attacks, as a standard EV runs over 100 million lines of code.

Without proper precautions and protection, an automobile’s data can be stolen – or worse, hackers can take remote control of the car.

From a Regulatory Perspective:

UNICE WP.29 is a global forum (comprised of 58 states) for road vehicles, agricultural vehicles, and some off-road vehicles. This governing body sets mandatory homologation requirements for member-states. Original Equipment Manufacturers (OEMs) are required to comply with the requirements to put new vehicles on the road.

Adopted by UNICE, UN R155 requires developers of automotive parts or vehicles to have a Cybersecurity Management System (CSMS). Additionally, UN R156 is a regulatory requirement for a Security Update Management System (SUMS).

Implementation of ISO 21434 fulfills the requirements for a CSMS according to R155. These requirements apply to the vehicle and all components of the vehicle that access vehicle internal communication buses.

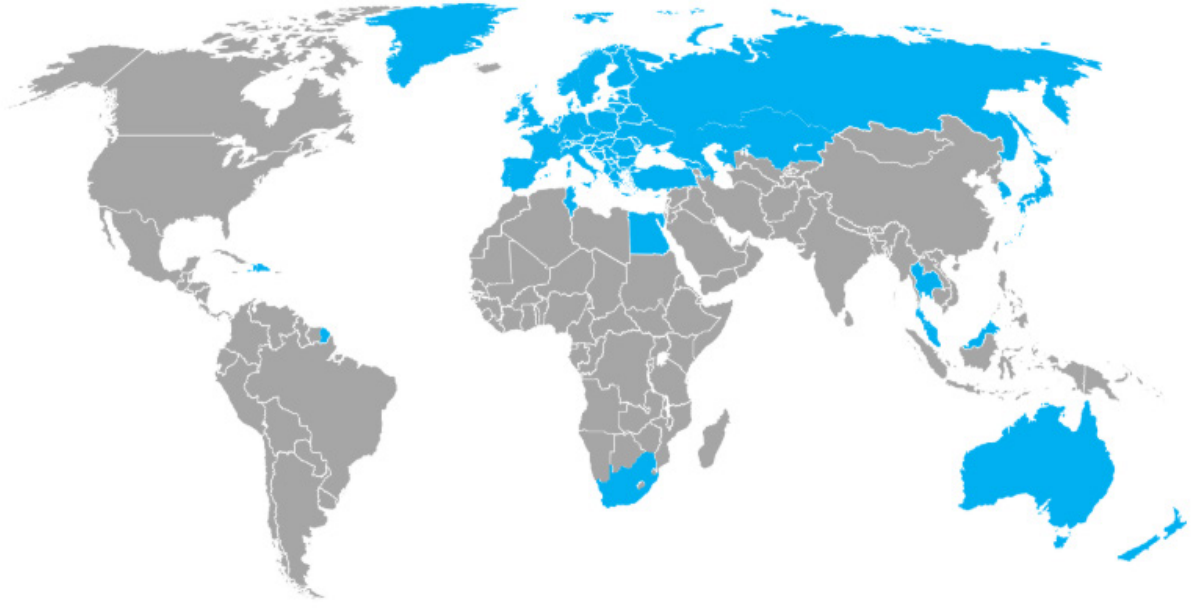
4 UN R155 and R156 – Who Does This Apply to and When Does it Take Effect?

UN R155 and R156 – Who Does This Apply to and When Does it Take Effect?

Starting in January 2021, UN R155 and R156 were officially released. The regulations apply to all passenger cars, vans, trucks, and buses in the UNECE WP.29 global forum. Additionally, Japan has indicated that it plans to apply these regulations to all automobiles entering the market. The Republic of Korea has adopted a stepwise approach, introducing the provisions of the regulation on cybersecurity in a national guideline in the second half of 2020, and proceeding with the implementation of the regulation in a second step.

As of in July of 2022, the European Union (EU) mandates the regulation on cybersecurity for all new vehicle types and is mandatory for all new vehicles produced from July 2024 (including components).

Given the widespread use of UN Regulations in the automotive sector around the world, the broad adoption of these regulations across the world is expected, among and beyond the 54 Contracting Parties to UNECE's 1958 Agreement.



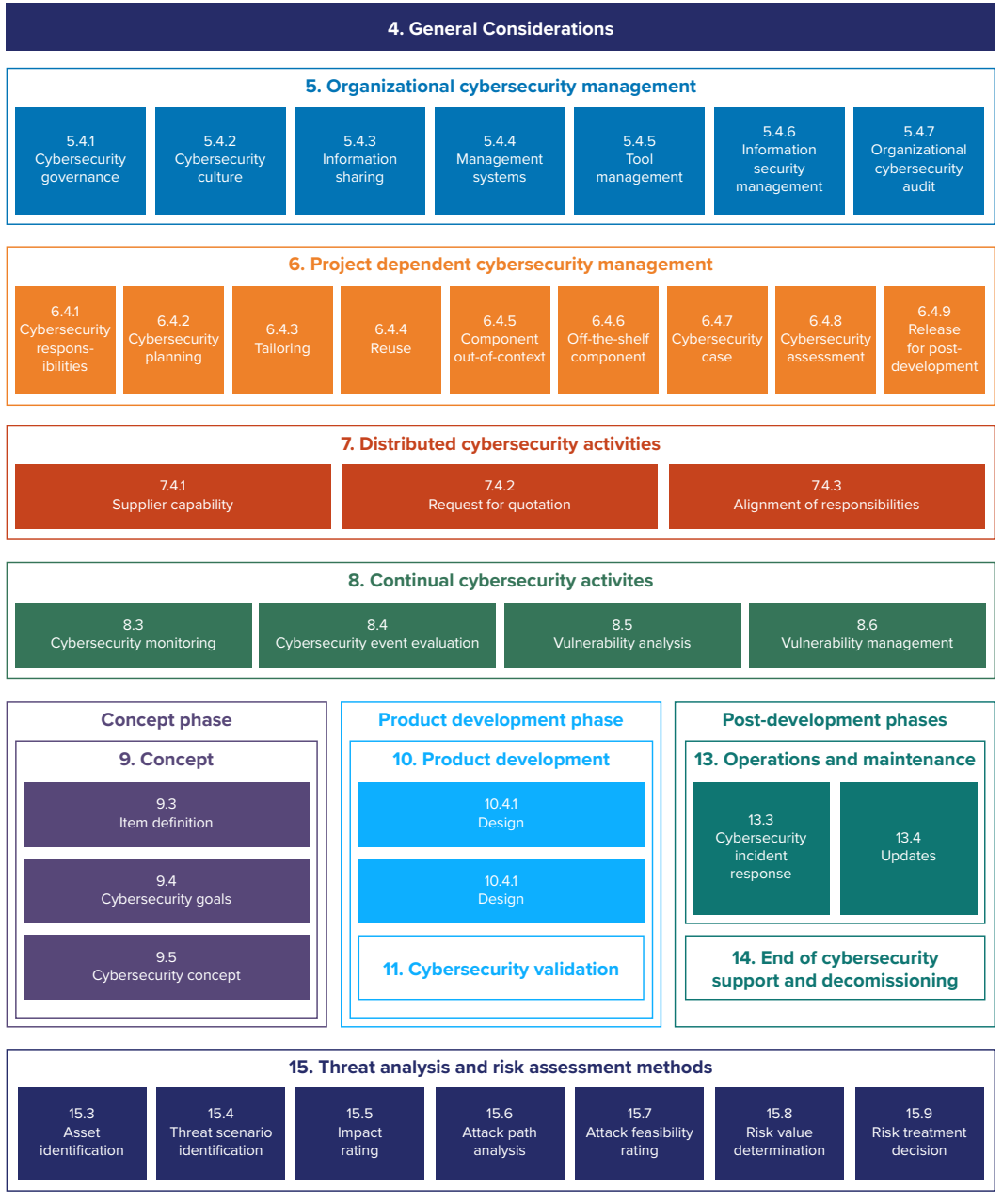
5 ISO 21434 Standard Overview

ISO 21434 Standard Overview

ISO 21434 provides vocabulary, objectives, requirements, and guidelines for cybersecurity engineering in the context of electrical and electronic systems within road vehicles. The goal of the standard is to enable the engineering of electrical and electronic systems to keep up with the state-of-the-art technology and evolving cybersecurity attack methods. Adhering to the standard will allow organizations to define cybersecurity policies and processes, develop a cybersecurity culture, and manage cybersecurity risk.

The structure of the standard is as follows:

- 15 clauses, 11 are normative
- Similar structure and vocabulary as ISO 26262
- Each clause has at least one requirement and one work product, with the exception of clauses 1-4.
- Some clauses have RC (recommendations), and PC (permissions)
- Nine informative appendixes



Terminology

To achieve the goal of a common vocabulary within cybersecurity engineering for road vehicles, ISO 21434 defines a number of terms.

Asset: A part of an item that has cybersecurity properties (ex: OBD II port, safety requirements)

Attack Path: A series of steps that an intruder could use to compromise an asset

Cybersecurity Goal: Top level product requirement resulting from the TARA (see below for TARA definition)

Cybersecurity Claim: An identified risk that will be accepted, typically mitigated by liability transfer

Cybersecurity Concept: Cybersecurity requirements on the item and operating environment that implement controls to protect against threats

Damage Scenario: The potential damage to a road user caused by the realization of a threat scenario

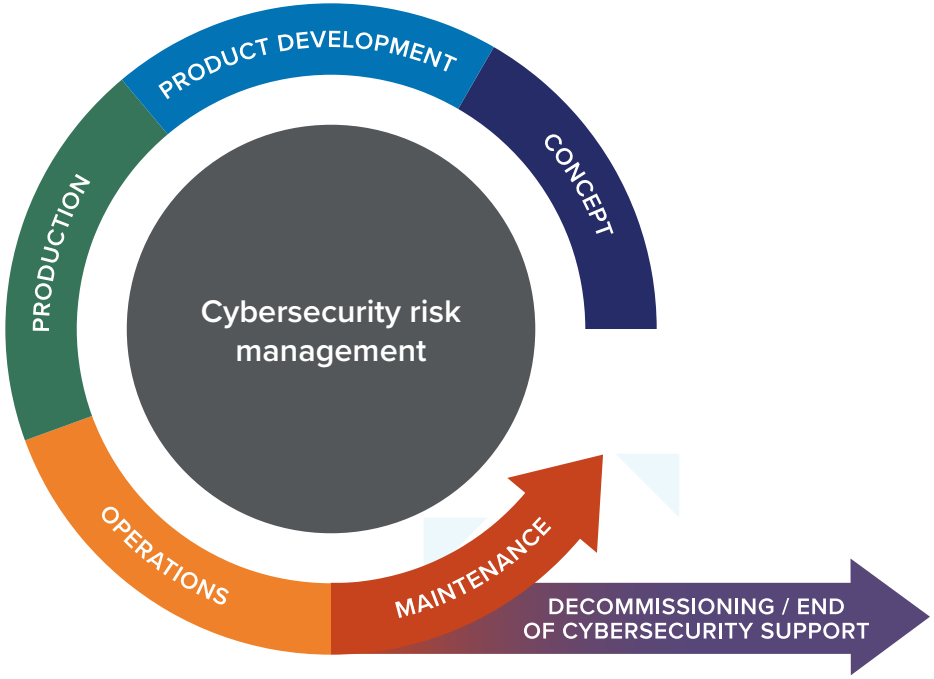
Item: A component or a set of components that implements a function at the vehicle level. Could be identical to the functional safety item

TARA: Threat and Risk Assessment. Assets with cybersecurity properties are identified and damage scenarios are identified if the asset is compromised. Threat scenarios are identified and supported with attack paths. Risk values are assigned, and cybersecurity goals are established for unacceptable risk

Threat Scenario: Potential cause of the compromise of the cybersecurity properties of one or more assets that leads to a damage scenario

Lifecyle

ISO 21434 defines a cybersecurity lifecycle that starts with the definition of a new vehicle system and ends with that vehicle system being decommissioned or support by the OEM ending. This means that cybersecurity activities continue after a system is put into production to ensure that new vulnerabilities that are discovered after a system enters production are still identified and mitigations added if necessary.



Learn more about the impact of ISO 26262 on both the development process and support tool chains for automotive electronics, and what it means for modern automotive developers.

Download the paper, *The Impact of ISO 26262 on Automotive Development* »

6 Cybersecurity Management According to ISO 21434

Cybersecurity Management According to ISO 21434

Organizational

ISO 21434 defines requirements for an entire organization developing automotive systems to ensure that the necessary cybersecurity governance and culture are in place to support cybersecurity engineering. This includes ensuring that the organization acknowledges that there are cybersecurity risks, executive management is committed to the management of the risks, and that the organization has defined rules and processes to implement the requirements of ISO 21434.

In addition, the organization must have personnel in cybersecurity roles that are competent, policies that define how information can be shared both internally and externally, an appropriate quality management system, management of all product development tools, and robust information security. Audits must be performed to ensure that the organization achieves the objectives.

According to the new ASPICE SEC-PAM, “The ASPICE framework now contains support for cybersecurity processes with the release of the new SEC-PAM allowing cyber-related processes to be assessed using traditional ASPICE resources and methodologies.

Project-Specific

Each project that develops or updates a road vehicle system or component must manage the cybersecurity engineering activities specific to that project. This includes the following considerations:

a) Assigning the responsibilities regarding the project's cybersecurity activities to specific individuals

b) Planning the cybersecurity activities that will be performed during the project

c) Creating a cybersecurity case that provides the argument for the cybersecurity of the system or component

d) Performing a cybersecurity assessment if the project risks deem it necessary

e) A decision of whether the system or component can be released for post-development from a cybersecurity perspective.

7 Cybersecurity V-model

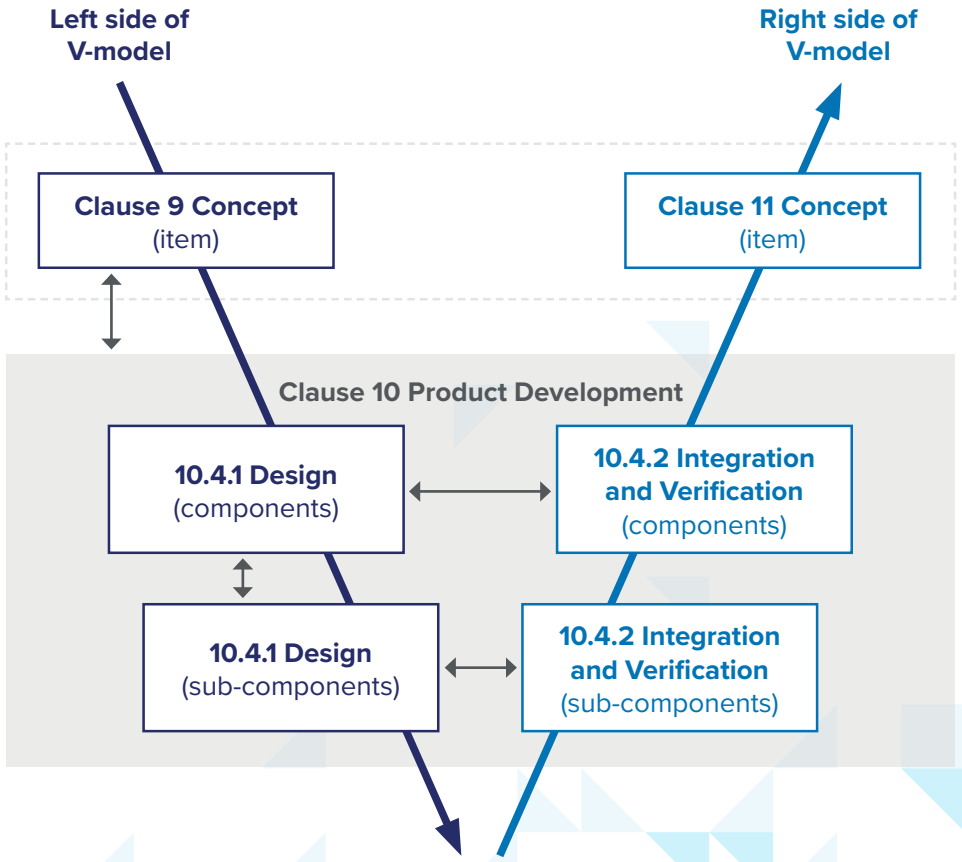
Cybersecurity V-model

Much like other automotive standards, ISO 21434 defines a system engineering V-model to be followed for the development of cybersecurity features.

Concept Development

The cybersecurity V-model starts with the definition of the exact “item” that will be developed. The item is a component or set of components that implement functionality at the vehicle level and is defined in an *item definition*. In many cases, the same item *definition* may be used for both functional safety analysis and cybersecurity analysis.

Once the item has been clearly defined, a Threat Analysis and Risk Assessment (TARA) is performed to identify what cybersecurity



threats exist for the item and what the risk of those threats are. For threats where the risk must be reduced, concept level requirements are developed, known as *cybersecurity goals*. *Cybersecurity goals* form the highest-level requirements for the system being developed from a cybersecurity perspective. For risks that will remain after *cybersecurity goals* are achieved, cybersecurity claims are documented to explain what, if any, risks still exist and why they can be accepted.

After defining *cybersecurity goals*, a *cybersecurity concept* is created. This documents the high-level concept that will be used to achieve the *cybersecurity goals*. The concept takes the form of cybersecurity requirements as well as requirements on the operating environment.

Product Development

Once a *cybersecurity concept* has been developed, the system must be designed in a way that will satisfy the cybersecurity requirements. Any existing architecture must be updated to consider the cybersecurity requirements. Each component of the system should be designed to support the cybersecurity requirements.

Although ISO 21434 provides an example of developing a system in two layers of abstraction, no specific number of layers is required. Instead, the standard leaves it to the product development organization to define a process appropriate for the complexity of their system. This ensures that organizations can adapt the standard to a wide range of systems and, for many, means that their existing system engineering process will satisfy ISO 21434.

Once the components of the system have been designed and integrated, the system must be verified to ensure that it meets the cybersecurity requirements.

The methods for verifying the system can include:

- Requirements-based testing
- Interface testing
- Resource usage evaluation
- Verification of the control flow and data flow
- Dynamic analysis
- Static analysis

The integration and verification activities should be documented in a verification specification and the results of verification documented in a verification report.

Validation of Cybersecurity Goals

While the focus of verification is ensuring that the item meets the cybersecurity requirements, validation ensures that the item achieves the cybersecurity goals. This is done by first validating that the cybersecurity goals are adequate and then validating that the item achieves the cybersecurity goals. Validation may involve reviewing work products, performing penetration testing and reviewing all the managed risks previously identified. A rationale for the validation activities is required. The completed validation is documented in a validation report.

8 Post-Development Activities

Post-Development Activities

Even after product development is complete, the cybersecurity lifecycle continues.

Production

During the production phase, the item that has been developed is manufactured and assembled. A production control plan is required to ensure that cybersecurity requirements for post-development that were identified earlier in the lifecycle are applied to ensure that no vulnerabilities are introduced during production.

Operations and maintenance

Once an item has been integrated into a vehicle and the vehicle is on the road, new cybersecurity threats can still be identified. ISO 21434 requires organizations to have a plan for how to respond to this scenario.

Organizations must create a cybersecurity incident response plan each time a new cybersecurity incident occurs. This plan includes what remedial actions are required and how they will be performed. The response may range from providing new information to vehicle owners, to over-the-air updates, to recalls where the owner must bring the vehicle in for service.

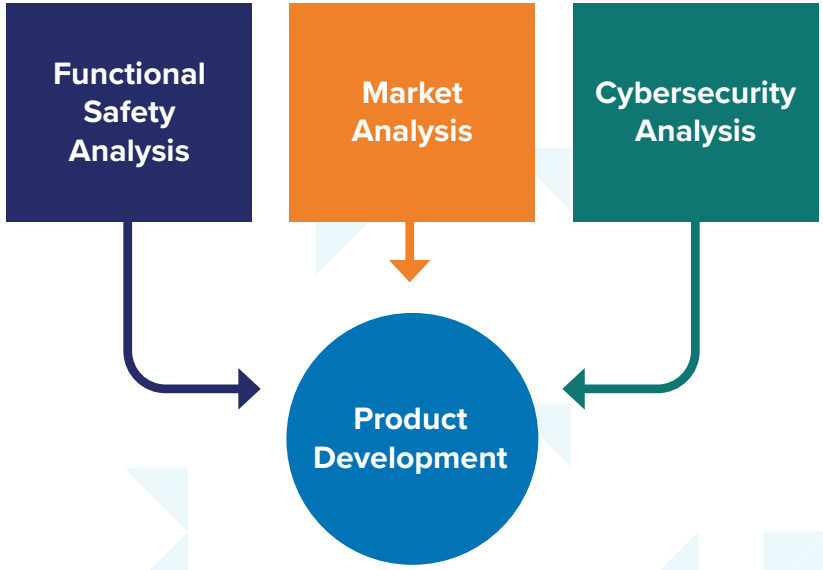
End of cybersecurity support and decommissioning

Given that the cybersecurity lifecycle continues after vehicles have been sold to consumers, a method for ending cybersecurity support for those vehicles is needed. ISO 21434 focuses on developing a plan for communicating with customers when cybersecurity support ends. Since decommissioning can occur without the organization's knowledge and in such a way that decommissioning procedures cannot be enforced, ISO 21434 only requires making documentation available to explain how to decommission the item with regards to cybersecurity, if this is even required.

9 Integrating the Cybersecurity with Overall System Engineering

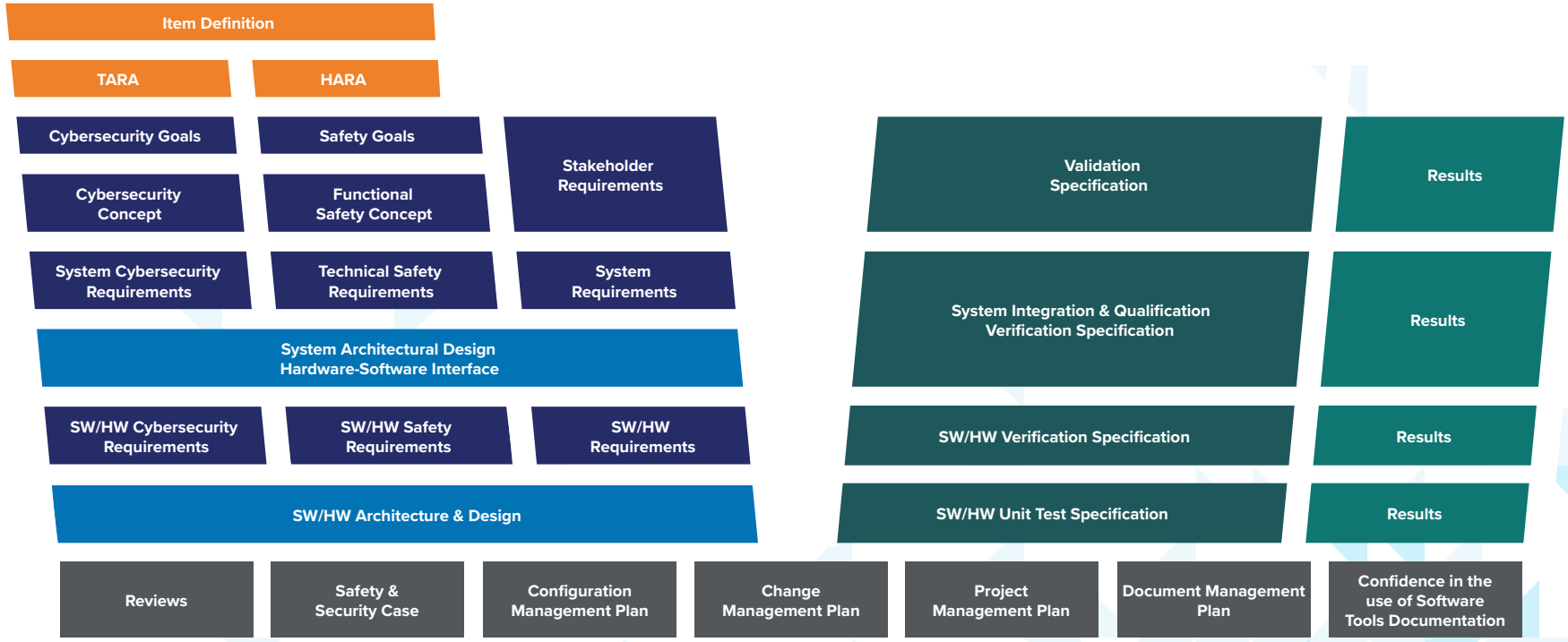
Integrating the Cybersecurity with Overall System Engineering

ISO 21434 defines many cybersecurity-specific requirements and requires personnel with specific cybersecurity knowledge and skills. Because of this, it may be tempting for organizations to silo cybersecurity engineering activities from other engineering activities, but this would be a mistake. While risk analysis required by ISO 21434 can be considered as a separate activity from other system engineering activities, a single product still must be developed that meets a wide range of requirements, including cybersecurity requirements. For this reason, it is best to manage a unified database for requirements, architecture, and design, rather than tracking cybersecurity artifacts separate from others.



To support this, think of cybersecurity analysis as another input to product development, just like functional safety analysis and market analysis.

By taking a unified approach, a single system engineering V-model can be implemented that describes an overall product development process that incorporates cybersecurity without creating silos. While specialists will be focused on performing cybersecurity analysis, implementing known best practices and validating the final system achieves cybersecurity, this must be done in cooperation and coordination with the rest of product development.



10

How Jama Connect® Supports Cybersecurity Engineering

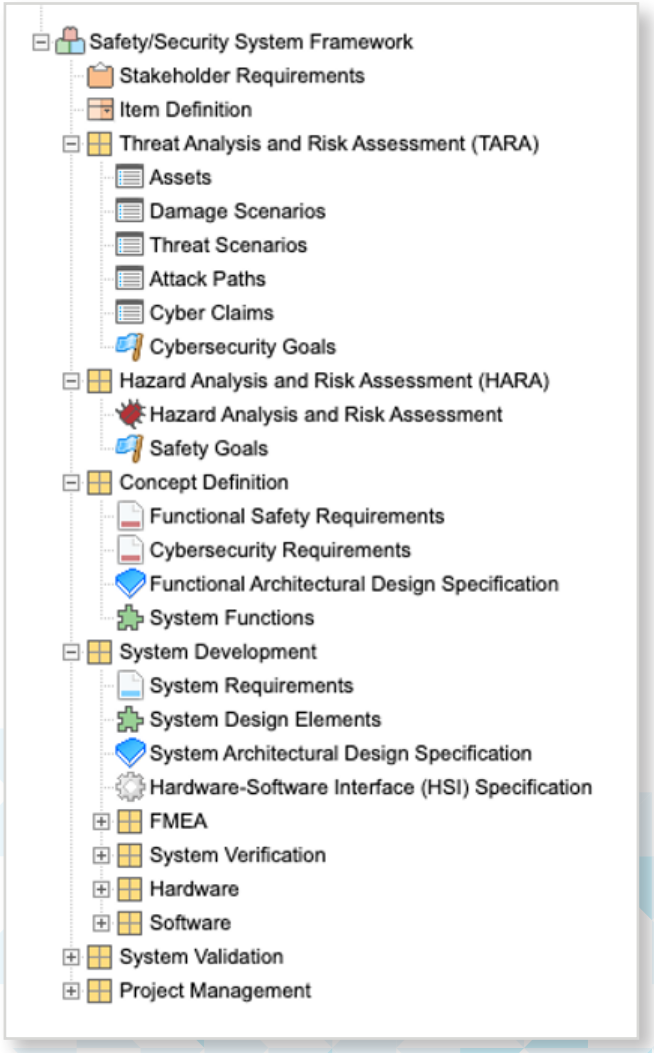
How Jama Connect® Supports Cybersecurity Engineering

One way to implement a unified requirements, architecture, and design database is by using Jama Connect®. Jama Connect for Automotive provides a framework that incorporates the key requirements of ISO 21434 into a single project structure along with overall system engineering.

Specifically, Jama Connect for Automotive provides guidance on supporting the following activities:

- TARA
- Cybersecurity goals
- Cybersecurity concept
- Design
- Integration and verification
- Validation

An example of the framework is shown to the right.



11 Conclusion

Conclusion

ISO 21434 introduces a robust framework for organizations to apply the state-of-the-art in cybersecurity to their product development. This framework is necessary from both a market and regulatory perspective. The high-level of connectivity available in vehicles today means that there many ways for someone to maliciously change a vehicle's operation. While many consumers may be unaware of the risks today, if there are ever accidents that result from cyber-attacks, that will change quickly. A vehicle OEM's brand will surely be impacted by such as incident. In addition, regulators have already imposed strong cybersecurity requirements in many regions. ISO 21434 is quickly becoming an essential regulation for companies developing products at all levels of the automotive supply chain.

Whether your team is young or seasoned, small, or large, all together or scattered across boundaries, Jama Connect for Automotive can help improve processes, reduce costs, improve time to market, and help achieve ASPICE compliance. To learn more about Jama Connect for Automotive, **download our datasheet**.

> Interested in learning more about how Jama Connect for Automotive can help provide your team meet market demands more quickly and efficiently? Visit **jamasoftware.com/solutions/automotive** or **contact us** to learn how Jama Connect can optimize success for your organization.

Jama Software® is focused on maximizing innovation success in multidisciplinary engineering organizations. Numerous firsts for humanity in fields such as fuel cells, electrification, space, software-defined vehicles, surgical robotics, and more all rely on Jama Connect® requirements management software to minimize the risk of defects, rework, cost overruns, and recalls. Using Jama Connect, engineering organizations can now intelligently manage the development process by leveraging Live Traceability™ across best-of-breed tools to measurably improve outcomes. Our rapidly growing customer base spans the automotive, medical device, life sciences, semiconductor, aerospace & defense, industrial manufacturing, consumer electronics, financial services, and insurance industries. To learn more, please visit us at jamasoftware.com.