UN-ECE-WP.29 Cybersecurity Management System (CSMS) Requirements

and

Karamba Security Product & Services supports according to ISO/SAE-21434

By: Karamba Security

June 2020

For more details pls contact
contact@karambasecurity.com

Israel
Tel: +972 9 88 66 113
24 HaNagar Street
Hod Hasharon
4527713
www.karambasecurity.com

Michigan, USA
Tel: +1 248 574 5171
41000 Woodward Avenue
Building East, Suite 350
Bloomfield Hills, MI 48304
contact@karambasecurity.com

Germany
Tel: +49 151 1471 6088
Wasserburger Landstr. 264
81827
Munich
www.karambasecurity.com

Contents

1 Summary

UN-ECE-WP.29 is being adopted in various countries. OEMs and Tier-1 are now required to integrate Cybersecurity Management System (CSMS) processes into development and manufacturing processes. Karamba Security products and services are available to speed up the adoption phase, utilizing Karamba's experience in automotive architecture and ECUs, embedded device development and cybersecurity.

UNECE – WP.29 CSMS Requirement	**Processes required according to ISO/SAE-21434**	**Karamba Security Offering**
(A) The processes used within the manufacturer's organization to manage cybersecurity;	Chapters 5 and 6 define the process required for managing cybersecurity in the manufacturer's organization. For example: - 5.4.1 Cybersecurity Governance - 5.4.2 Cybersecurity Culture - 6.4.2 Cybersecurity Plan - 6.4.7 Cybersecurity Case	Training Services
(B) The processes used for the identification of risks to vehicle types and **(C) the processes used for the assessment, categorization and treatment of the risks identified;**	Chapter 8 defines the Risk Assessment methods, including: - 8.3 Asset Identification - 8.4 Threat Scenario Identification - 8.5 Impact Rating - 8.6 Attack Path Analysis - 8.7 Attack Feasibility - 8.8 Risk Determination - 8.9 Risk Treatment Decision	Threat Analysis and Risk Assessment (TARA)
(D) The processes in place to verify that the risks identified are appropriately managed and **(E) the processes used for testing the security of the system throughout its development and production phases;**	Chapter 10 in ISO/SAE-21434 suggests various verification activities to be performed to confirm the implementation of the cybersecurity design: - 10.4.2. Integration and validation	VCode™ Code Review Service Penetration Testing Service
(F) The processes used for ensuring that the risk assessment is kept current;	-	Version Validation Service
(G) The processes used to monitor for, detect and respond to cyber-attacks on vehicle types;	Chapter 7 defines the need for continuous cybersecurity activities, such as: 7.3 Cybersecurity Monitoring	XGuard® Embedded Platform
(H) The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types;	Chapter 7 defines the need for continuous cybersecurity activities, such as: 7.5 Vulnerability Analysis 7.6 Vulnerability Management	-

UNECE – WP.29 CSMS Requirement	Processes required according to ISO/SAE-21434	Karamba Security Service
(I) The processes used to appropriately react to new and evolving cyber threats and vulnerabilities	Chapter 13 defines the Operations and Maintenance processes, such as: 13.3 Cybersecurity incident response	-

2 UN-ECE-WP.29 and the need for a Cybersecurity Management System (CSMS)

UN-ECE-WP.29 defines principles to address key cyber threats and vulnerabilities identified in order to assure vehicle safety in case of cyber-attacks. It further defines detailed guidance or measures for how to adhere to these principles. Currently, The European Union (EU) has adopted UN-ECE-WP.29 cybersecurity regulations affective July 2022 for all new vehicle types, and July 2024[1] for registration of existing vehicles. In addition, Japan has adopted it, affective April 2020, for all autonomous vehicles level 3 and higher.

The adoption of UN-ECE-WP.29 defines that a manufacturer should provide a Cybersecurity Management System (CSMS) certificate for approval of a new vehicle model. The CSMS is "*a systematic risk-based approach defining organizational processes, responsibilities and governance to mitigate cyber threats and protect vehicles from cyber-attacks.*"

The CSMS is an ongoing process, and the manufacturer should maintain it through the device life-cycle: it should cover the ECU Development phase, Production phase and Post-production phase.

Using the CSMS, the vehicle manufacturer shall demonstrate the processes ensure that cybersecurity is adequately considered:

(A) The processes used within the manufacturer's organization to manage cybersecurity;

(B) The processes used for the identification of risks to vehicle types;

(C) The processes used for the assessment, categorization and treatment of the risks identified;

(D) The processes in place to verify that the risks identified are appropriately managed;

(E) The processes used for testing the security of the system throughout its development and production phases;

(F) The processes used for ensuring that the risk assessment is kept current;

(G) The processes used to monitor for, detect and respond to cyber-attacks on vehicle types;

(H) The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types;

(I) The processes used to appropriately react to new and evolving cyber threats and vulnerabilities.

[1] https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-06-19r1e.pdf

UN-ECE-WP.29 identifies ISO/SAE 21434 , “Road vehicles — Cybersecurity engineering” as "A key standard that may be used for implementing CSMS processes".

Defining, training and establishing CSMS in the organization and the adoption of ISO/SAE-21434 requires an intensive effort. In this paper we present how Karamba Security supports establishing the CSMS processes, according to ISO/SAE 21434, speeding up the adoption and certification phases.

3 CSMS Processes and ISO/SAE-21434

The adoption of ISO/SAE-21434 is required in order to obtain the CSMS Certificate. This section reviews the requirement of each process, and the supported service by Karamba Security.

3.1 (A) The processes used within the manufacturer’s organization to manage cybersecurity

Chapters 5 and 6 in ISO/SAE-21434 defines the process required for managing cybersecurity in the manufacturer’s organization.

Chapter 5 defines the overall cybersecurity management suggested process, including:

(a) define a cybersecurity policy and the organization-specific rules and processes for cybersecurity;

(b) assign the responsibilities and corresponding authorities that are required to perform cybersecurity activities;

(c) support the implementation of cybersecurity, including the provision of resources and the management of the interactions between cybersecurity processes and related processes;

(d) institute and maintain a cybersecurity culture, including competence management, awareness management and continuous improvement;

(e) perform an organizational cybersecurity audit;

(f) manage the sharing of cybersecurity information;

(g) institute and maintain management systems that support the cybersecurity activities; and

(h) provide evidence that the tools used do not adversely affect cybersecurity.

Chapter 6 defines project dependent cybersecurity management suggested process, including:

(a) assign the responsibilities regarding the project’s cybersecurity activities;

(b) plan the cybersecurity activities, including the definition of the tailored cybersecurity activities;

(c) create a cybersecurity case that provides the argument for the achieved degree of cybersecurity;

Karamba Security Training Service supports the on-boarding of the new assigned authorities with intensive on-going training courses, including: “Think Like a Hacker”, “Introduction to Cybersecurity in Embedded Devices”, “Threats and Mitigations” and more.

3.2 (B) The processes used for the identification of risks to vehicle types and (C) the processes used for the assessment, categorization and treatment of the risks identified

Chapter 8 in ISO/SAE-2143 presents systematic methods to perform a vehicle or a sub-system risk assessment. The Risk Assessment Methods are used during the vehicle (or sub-system) life cycle and include the following building blocks:

a) Asset identification – identifying all the assets with cybersecurity properties whose compromise leads to a damage scenario.

b) Threat Scenario identification – describing for each targeted asset, the compromised cybersecurity property, and the action to accomplish a damage scenario.

c) Impact rating – independently assessing the impact of each of the threat scenarios in the following domains: safety, financial, operational, and privacy (S, F, O, P)

d) Attack path analysis – analyzing and describing the various attack paths for each threat scenario. The analysis can be done top-down (deductive approach - used mainly in the concept and development phase) or bottom-up (inductive approach – used mainly when an implementation of the vehicle or sub-system is available).

e) Attack feasibility rating – determining the attack feasibility of each of the attack paths according to attack potential (including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment) or according to CVSS approach (including attack vector, attack complexity, privileges required, and user interaction).

f) Risk determination – defining the risk treatment for each attack path, including: removing the risk source, reducing the risk, sharing/transferring the risk or accepting/retaining the risk.

Karamba Security Threat Analysis and Risk Assessments (TARA) Service is based on ISO/SAE-21434 guidelines. Karamba Security's deep experience in cybersecurity, embedded devices and Automotive ECUs ensures the creation of detailed professional TARA documents as required for certification.

3.3 (D) The processes in place to verify that the risks identified are appropriately managed and (E) the processes used for testing the security of the system throughout its development and production phases

Chapter 10 in ISO/SAE-21434 suggests various verification activities to be performed to confirm the implementation of the cybersecurity design. The activities may include standard engineering quality management process and additional cybersecurity verification types of activities. The verification activities should include:

(a) Defining test cases
(b) System Coverage metrics
(c) Unidentified vulnerabilities – using penetration testing, vulnerability scanning and fuzz testing
(d) Covering coding guidelines – e.g., using MISRAc:2012 guidelines for secure coding in the "C" programming language

With the development of Agile programming and the need for continuous cybersecurity risk verification, **Karamba Security provides three verification services:**

1. **VCode –** tool for ongoing system cybersecurity verification, allowing the product manager and the team leader to constantly monitor the status of the component risks. The tool is part of the CI/CD environment (build automation with Jenkins, ticketing in Atlassian Jira, etc.) and also provides practical mitigation advisories. VCode provides a standard report that complies with the certification process.
2. **Cybersecurity Code Review –** Deep review of the developed component, including vulnerabilities in 3rd-party components, secure coding mistakes, security finding in the build process and more. The Cybersecurity Code Review report complies with the certification requirements.
3. **Penetration Testing –** Based on a Black-box or White-box approach, Karamba's researchers search for vulnerabilities in the integrated devices, prioritize the findings and propose mitigation steps. The Penetration Testing report complies with the certification requirement.

3.4 (F) The processes used for ensuring that the risk assessment is kept current

The validation process is an on-going process through the entire life-cycle of the vehicle or sub-system (development, production and post-production).

Karamba Security's Version Validation Service is a package for an on-going sub-system, providing existing TARA validation, Code Review and System Vulnerabilities analysis. Each of the findings is compared to the design and mitigation decisions in previous phases.

The Version Validation Service report includes a list of prioritized finding and mitigations which complies with the certification requirements.

3.5 (G) The processes used to monitor for, detect and respond to cyber-attacks on vehicle types

Section 7.3 in ISO/SAE-21434 defines internal and external sources that shall be monitored for collection of cybersecurity information. The internal sources can include:

(a) results of vulnerability analyses;
(b) information received from the field (e.g., vulnerability scanning reports, repair information, consumer usage information;
(c) configuration information such as a hardware or software bill of materials

Karamba Security's XGuard Platform provides field monitoring capabilities, reporting the sub-system status, and triggering incident reporting for anomalous operating-system or application behavior. The XGuard Platform is integrated during the development phase; Post-production, the OEM V-SoC receives runtime reports on the required cybersecurity information for use by the OEM's incident-response team.

3.6 (H) The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types;

TBD with the customer

3.7 (I) The processes used to appropriately react to new and evolving cyber threats and vulnerabilities

TBD with the customer