Complying with AIS 189

Indian Automotive Cybersecurity Management System Regulation

Overview

As India continues to be a growing player in vehicle and parts manufacturing, the approval of vehicles with regards to cybersecurity and vehicle product security aligns the nation's automotive ecosystem manufacturers with WP.29's R155 Cybersecurity Management System (CSMS) requirements.

It applies to cybersecurity in vehicles of Categories M and N. It also applies to Category T (agricultural) vehicles with at least one electronic control unit and Category L7 vehicles with level 3 or higher automated driving functionalities. This standard does not override other national or regional standards or legislation on vehicle access, data privacy, and replacement parts. Below are the main CSMS requirements and an explanation of how Cybellum helps with each:

	Section 7 'Specifications' for a Cyber Security and Management System (CSMS)	How Cybellum Helps
7.0	SPECIFICATIONS	
7.2	Requirements for the CSMS	
7.2.1	For the assessment the test agency shall verify that the vehicle manufacturer has a CSMS in place and shall verify its compliance with this Standard.	
7.2.2	The CSMS shall cover the following aspects:	
7.2.2.1	The vehicle manufacturer shall demonstrate to an test agency that their CSMS applies to the following phases:	
	(a) Development phase;	
	(b) Production phase;	- Cybellum's Product Security Platform automates the validation of security requirements and helps with gap analysis and resolutions. - Lifelong information, from development through production, can be tracked to identify the cybersecurity posture at all times. - Secure coding standards such as MISRA C and others are also automatically tested and checked as part of Cybellum's Product Security Platform
	(c) Post-production phase.	- OS hardening and common security guidelines such as OWASP are automatically evaluated as part of Cybellum's platform - Violations to WP.29 Annex 5 threats are automatically evaluated as part of Cybellum's Product Security Platform - Cybellum's platform supports both AUTOSAR-based and non-AUTOSAR ECUs and components

	Section 7 'Specifications' for a Cyber Security and Management System (CSMS)	How Cybellum Helps
7.2.2.2	The vehicle manufacturer shall demonstrate that the processes used within their CSMS ensure security is adequately considered, including risks and mitigations listed in Annex D. This shall include:	
	(a) The processes used within the manufacturer's organization to manage cyber security;	The Cybellum Product Security Platform stores all asset and risk data, continuously reassessing risk and matching it with new information as it is created. - The vehicle's architecture and its ECUs configuration are defined in the system with the inter-connections risk levels, to accurately represent the risk levels imposed at the system, product and component level. - Security policies are managed centrally and allow the standardization of security and OS hardening best practices. The assets are constantly being evaluated against these policies to ensure the assessments are kept current.
	(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex D, Part A, and other relevant threats shall be considered;	The platform's Product Incident Response module automatically tracks new vulnerabilities, threats, exploits, etc. and monitors your assets to trigger the relevant events in case they are affected-- all without being installed on the vehicle. - Cybellum includes a full Vulnerability Management System, to perform all vulnerability-related activities from data collection to triaging, event triggering, and remediation. - Investigations can be opened for the assessment and management of relevant events. - All activities are documented and ready to be exported for auditing and reporting.
	(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 cyber security of a vehicle type;	
	(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, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.	
	(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	

	Section 7 'Specifications' for a Cyber Security and Management System (CSMS)	How Cybellum Helps
7.2.2.3	The vehicle manufacturer shall demonstrate that the processes used within their CSMS will ensure that, based on categorization referred to in clause 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.	The Product Security Platform's risk management KPI dashboards allow full visibility of when and how a risk was mitigated. The platform also facilitates workflows that allow teams to address an issue, conduct vulnerability detection, triaging and management, generate reports, and track the status at any time—so the designated person can remain transparent both internally and with customers. Cybellum facilitates the sharing of vulnerability information from external users into the company through: - Triage and validation reports - Automated workflows can intake user reports and initiate analysis by product security teams to reproduce and validate reported bugs. - Centralized tracking allows users to store and track all vulnerability reports from users in the same system used internally for end-to-end management.
7.2.2.4	The vehicle manufacturer shall demonstrate that the processes used within their CSMS will ensure that the monitoring referred to in clause 7.2.2.2 (g) shall be continual. This shall:	
	(a) Include vehicles after first registration in the monitoring;	
	(b) Include the capability to analyze and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect clause 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.	
7.2.2.5	The vehicle manufacturer shall be required to demonstrate how their CSMS will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of clause 7.2.2.2.	The Product Security Platform facilitates collaboration across the supply chain by sharing asset and risk data with relevant parties. Furthermore, if needed, it allows for integration with third-party systems, such as ticketing systems used by suppliers, so that findings and support tickets can be instantly shared with external development teams to expedite the resolution of security issues.
7.3	Requirements for vehicle types:	
7.3.1	The manufacturer shall have a valid Certificate of Compliance for the CSMS relevant to the vehicle type being approved.	The Product Security platform allows for ongoing product security activities, which help organizations earn and retain CSMS certification through transparent data sharing and reporting.
	However, for new model type approvals prior to All Model implementation date (after new model implementation date), if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.	Security testing and analysis processes can be implemented for any vehicle. Its connected data can be analyzed to confirm the implementation of security steps aligned with stringent product security standards.

	Section 7 'Specifications' for a Cyber Security and Management System (CSMS)	How Cybellum Helps
7.3.2	The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.	The Product Security Platform can identify risk throughout the full software supply chain, providing visibility into suppliers' origin of risks, generating reports with relevant information, and opening tickets via integrations that allow teams to manage risk.
7.3.3	The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex D, Part A, as well as any other relevant risk.	Cybellum's integration with Itemis' automotive TARA and threat analysis technology works harmoniously with the Product Security Platform, allowing teams to conduct thorough research to identify potential weaknesses and incorporate those findings into the overall design. These include: - **Improved traceability:** The solution improves traceability for risks, threats, and vulnerabilities throughout the product lifecycle from development to post-market. This will help automotive companies quickly and easily identify and mitigate cyber risks and follow ISO 21434 guidelines. - **Better risk assessment:** The combined solution will give automotive companies a more comprehensive view of their cyber risks, helping them make better decisions about mitigating those risks. - **Compliance with regulations:** The combined solution will help automotive companies comply with this regulation and UNECE WP.29 R155.
7.3.4	The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex D, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex D, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented. In particular, for new model type approvals prior to All Model implementation date (after new model implementation date), the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex D, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.	

	Section 7 'Specifications' for a Cyber Security and Management System (CSMS)	How Cybellum Helps
7.3.5	The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.	
7.3.6	The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.	
7.3.7	The vehicle manufacturer shall implement measures for the vehicle type to:	
	(a) Detect and prevent cyber-attacks against vehicles of the vehicle type;	The Product Security Platform allows organizations to continuously create evidence of their product security activities and bolster disclosure with 3rd parties (regulators, users, etc.). These include VEX reports that provide clear and concise information about the relevancy of a vulnerability to a specific product and its triaging status. Such reports can be generated at any point to provide ongoing status information to suppliers, internal teams, and auditors until the issue has been resolved.
	(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;	
	(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.	
7.3.8	Cryptographic modules used for the purpose of this Standard shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.	
7.4	Reporting provisions:	
7.4.1	The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the test agency the outcome of their monitoring activities, as defined in clause 7.2.2.2. (g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the test agency that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.	Automated workflows allow product security teams to trigger scans with new activities or check for new risks and vulnerabilities based on a predetermined schedule. The scans are then automatically generated reports that can be shared both internally and externally to support rapid mitigation of new threats.

	Section 7 'Specifications' for a Cyber Security and Management System (CSMS)	How Cybellum Helps
7.4.2	The test agency shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.	
	If the reporting or response is not sufficient the test agency may decide to withdraw the CSMS in compliance with clause 6.8.	