C2A security

AutoSec by C2A

THE PATHWAY TO COMPLIANCE

A Cybersecurity Management System (CSMS)

WP.29 | ISO 21434 COMPLIANT

CONCEPT PHASE > **DEVELOPMENT PHASE** > **POST DEVELOPMENT PHASE**

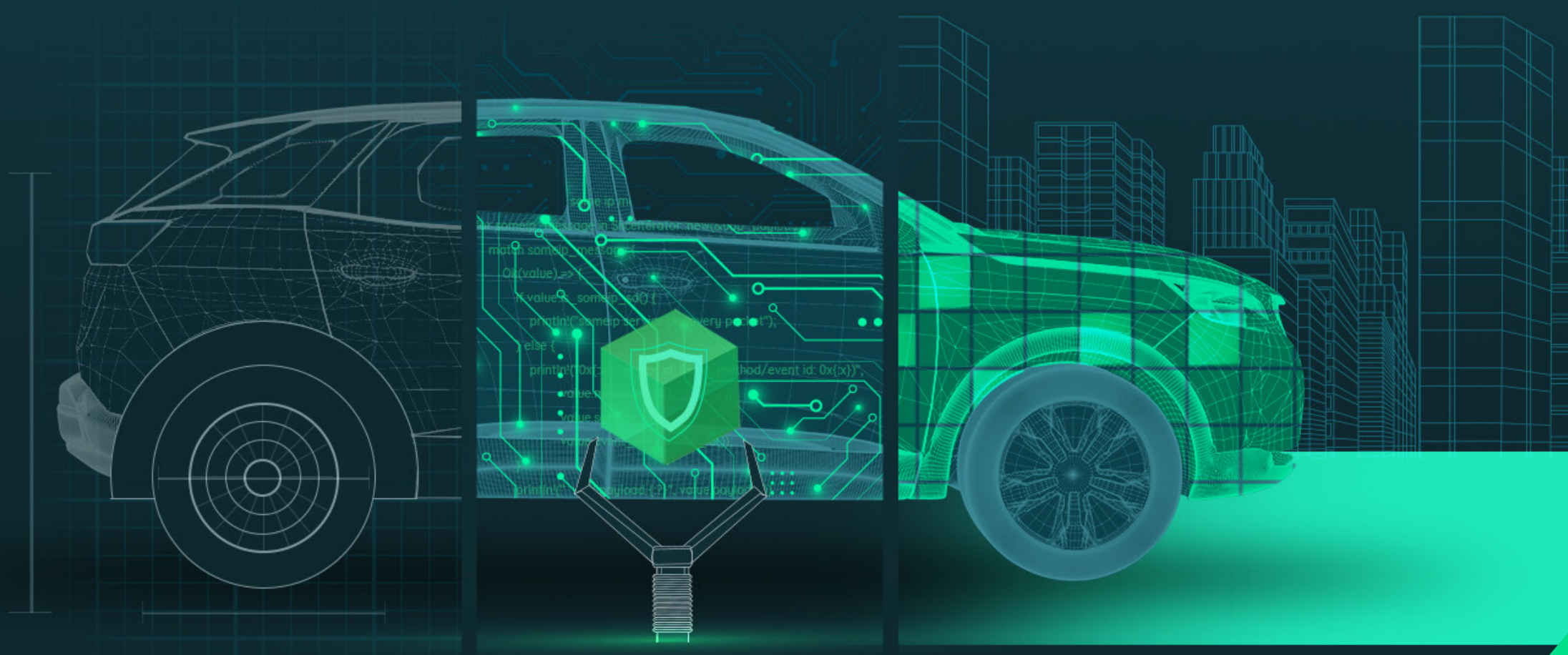


TABLE OF CONTENTS

ABOUT THIS WHITE PAPER

AutoSec empowers OEMs and Tier-1s with the visibility and control required to meet all the cybersecurity needs of connected vehicles throughout their entire lifecycle.

This white paper introduces the need for OEMs' and Tier-1s' compliance with ISO 21434 and WP.29 and presents AutoSec- C2A Security's end-to-end cloud-based solution for managing, collaborating and automating a vehicle's entire lifecycle of cybersecurity standards compliance.

For a full description of how to use AutoSec, contact us to request a demo at **info@c2a-sec.com.**

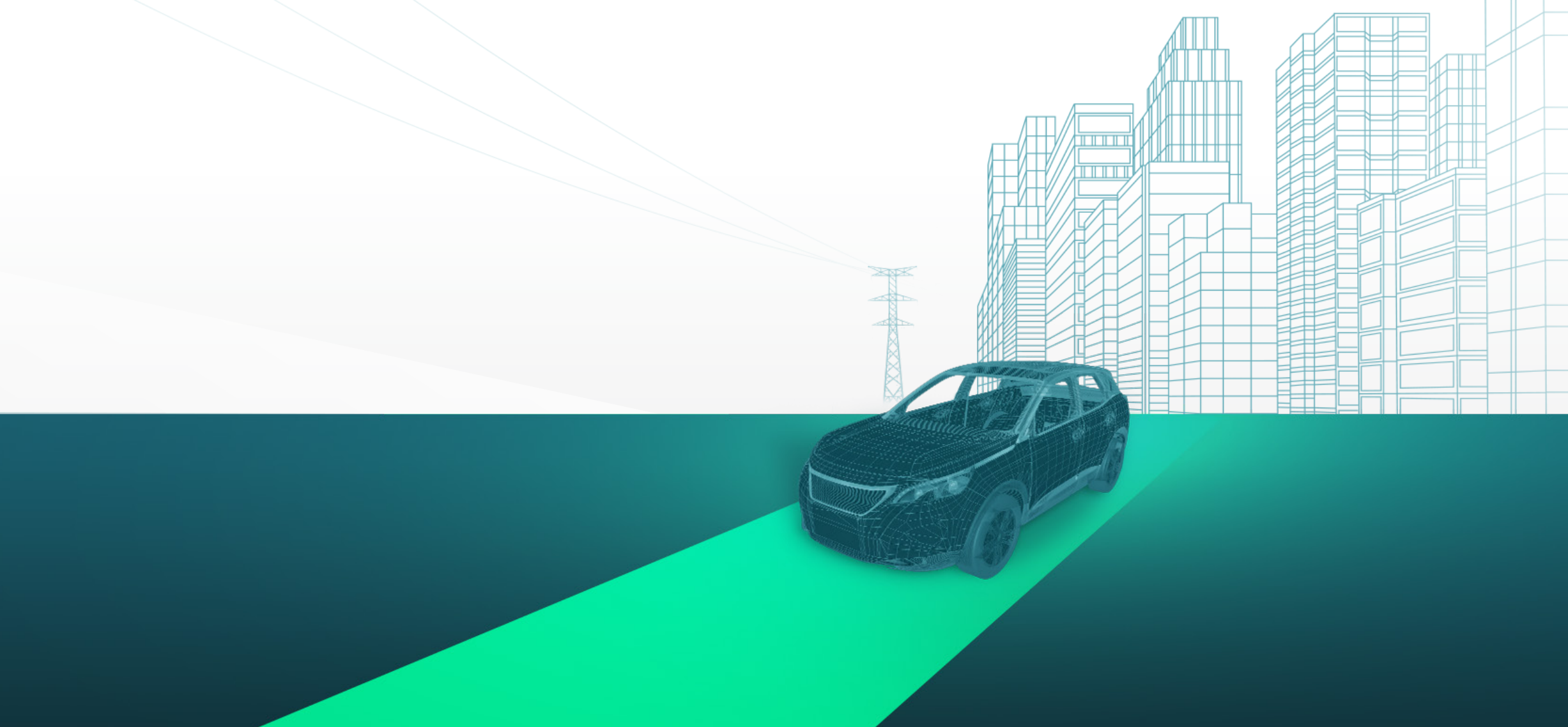
01
INTRODUCTION

The automotive industry is evolving rapidly, with modern vehicles operating on increasingly more complex hardware and software systems that are more vulnerable to cyber-attacks. OEMs, Tier 1s and other suppliers are facing multiple challenges as they attempt to meet the fast-changing requirements of the industry – the most important of which is the need to efficiently and effectively protect vehicles from cyber-attacks.

Today's vehicle supply chain is comprised of multitudes of components, from a wide variety of sources, making it much harder to manage. The fragmented supply chain complicates this challenge by making cybersecurity planning and maintenance even more difficult.

Cybersecurity teams at OEMs, Tier-1s and other automotive industry suppliers struggle to communicate with each other and coordinate tasks across a vehicle's entire lifecycle. These same teams are under pressure to work methodically and systematically to rapidly improve cybersecurity processes and outcomes in order to comply with the ISO 21434 standard and UNECE WP .29 regulation.

The main goal of these standards is to create security processes in OEM and Tier-1 companies that will drive risk management activities in their systems development procedures. The intention is for these standards to become requirements for all involved companies throughout the entire lifecycle of vehicles.



02
INDUSTRY COMPLIANCE CHALLENGES

URGENCY

Cybersecurity teams at OEMs, Tier-1s and other automotive industry suppliers are on a tight schedule to incorporate the new ISO 21434 standard and UNECE WP.29 regulations that will be adopted during 2022 (full enforcement is expected in 2024). As these regulations become tangible, cybersecurity teams must quickly update their cybersecurity practices and start implementing methodical and systematic procedures before vulnerabilities become crises.

METHODOLOGY GAP

OEMs and Tier-1s are well aware of the necessity of taking the steps to ensure compliance with these regulations by performing Threat Analysis and Risk Assessment (TARA) processes and adopting new approaches for handling cybersecurity lifecycle management challenges. However, automotive companies now face the challenge of translating this practical knowledge into action.

Significant resources must be invested in order to acquire the technically complex and detail-oriented skills that are required for creating and executing risk and assessment monitoring flows, as well as for learning and implementing the methodologies and best practices for achieving compliance.

LACK OF MANAGEMENT TOOLS

Streamlined cybersecurity lifecycle management processes are required to support companies as they begin to implement these new requirements. These new regulations define directives for implementing cybersecurity management systems for the protection of vehicles across their entire lifecycle, without prescribing specific technologies or cybersecurity management solutions. OEMs must now find a practical Cybersecurity Management System (CSMS) to tackle the challenge of cybersecurity lifecycle management, while adhering to these new regulations.

The main challenge is to find a concrete and collaborative implementation solution. Without such a solution, managing and coordinating cybersecurity lifecycle processes across different teams and suppliers is difficult; and achieving visibility on different car models and implementing the various security lifecycle steps for each model is possible, but extremely laborious.

03
WHAT IS AUTOSEC?

AUTOSEC IS A CYBERSECURITY **LIFECYCLE MANAGEMENT PLATFORM**

AutoSec is the first comprehensive cybersecurity lifecycle management platform that empowers OEMs and Tier-1s with the visibility, control and protection required to meet vehicles' lifelong cybersecurity needs. AutoSec's practical, transparent cybersecurity lifecycle management platform provides a unique orchestration layer that gives manufacturers unparalleled transparency into vehicles' entire cybersecurity lifecycle, enabling **streamlined management of each phase – risk assessment, planning, policy creation and enforcement, which provides the true resilience needed to tackle the cybersecurity management challenge.**

VISIBILITY, CONTROL AND PROTECTION **IN A SINGLE CLOUD-BASED PLATFORM**

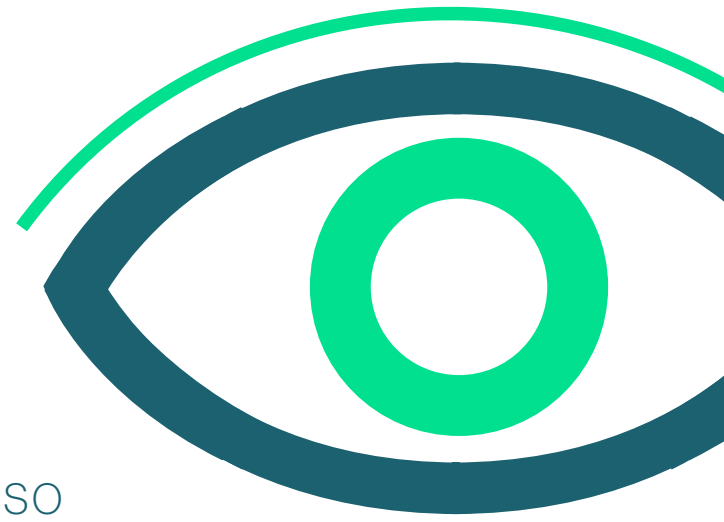
WATCH
Gain visibility of cybersecurity status across all models

DETECT
Analyze vehicles' complex multi-network system

DESIGN
Generate and customize in-vehicle cybersecurity according policies

PROTECT
Deploy and Maintain in-vehicle cybersecurity

RESPOND
Perform ongoing risk assessment, quickly identity and mitigate cyberattacks



AUTOSEC PROVIDES
FULL-SPECTRUM VISIBILITY

Full-spectrum visibility is critical for the successful implementation of ISO 21434. With visibility into their vehicles' cybersecurity lifecycles, OEMs and Tier-1s can perform risk assessment and analyze potential threats, plan their desired security policies and enforce the chosen policies across single or multiple models in order to achieve complete knowledge and full ownership.

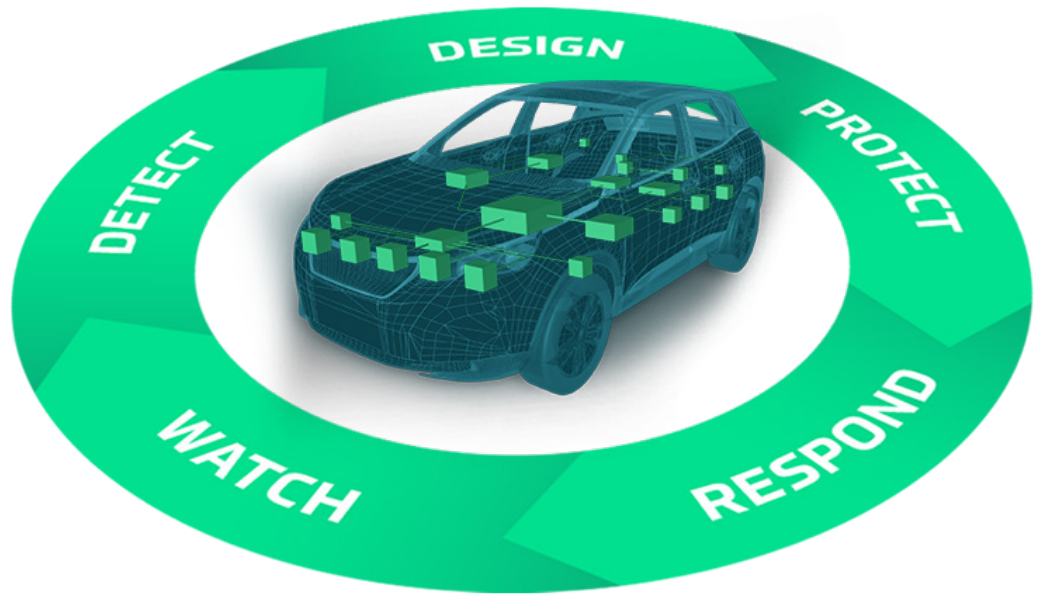
AutoSec provides full spectrum visibility of the cybersecurity data and status across all models, including all their MCUs and ECUs, as well as all vehicle topologies and all their binary functions. **With AutoSec you have security visibility of your entire fleet from vehicle E/E level and down to single lines of code.**

AutoSec uncovers unique security insights, alerts users in the event of policy noncompliance and/or identified risk and helps OEMs monitor the status of enforcement points and stay alert to potential threats, including:

- **Automated visual analysis for all assets (Network, MCU and Binary).**
- **Realtime asset security risk status view.**
- **Cross-check assets – From full vehicle topology to single function level.**

AUTOSEC ENABLES
END-TO-END CONTROL

Cybersecurity teams of OEM and Tier-1 companies must be able to control, collaborate and coordinate cybersecurity tasks throughout the entire lifecycle of their vehicles. These same teams are under pressure to work methodically and systematically in order to rapidly implement and improve cybersecurity processes and outcomes so as to comply with the control and protection aspects of the ISO 21434 standard and UNECE WP.29 regulations.



AutoSec automates the TARA process and enables the building of a conceptual model. AutoSec also verifies the model's components and requirements with the actual components of the system implementation.

AutoSec enables the **customization of in-vehicle cybersecurity architecture** and hand picks the security policies that best suit your needs. With these new capabilities, OEMs and Tier-1s can deploy security where it is really needed and configure embedded security products for all types of assets.

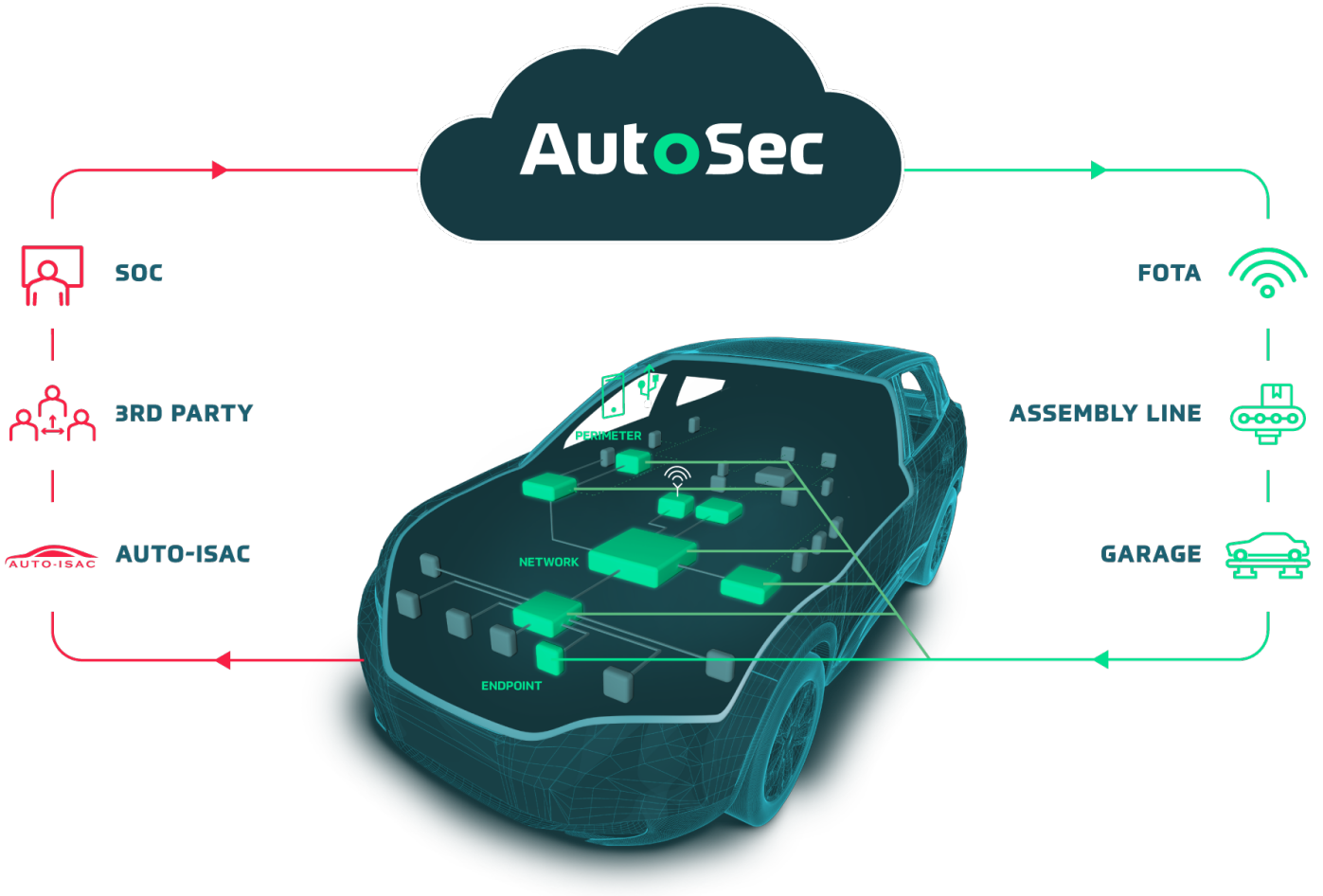
AutoSec empowers OEMs and Tier-1s with the control needed to protect connected vehicles by **protecting the entire system and each of its components with appropriate mitigation measures,** according to the kind and level of protection of their security policies.

AutoSec enables the **deployment of embedded cybersecurity solutions** and appropriate configuration files inside vehicles in a range of ECUs in order to provide protection for vehicles on the road, to prevent cyberattacks in real time and to protect the safety of drivers and passengers.

AutoSec is built to **evolve with the needs of the vehicles' defenses**, leveraging various data types onboarded into the system in order to generate insights and security policies and to deploy protections.

AUTOSEC BRIDGES
THE CYBERSECURITY GAP

AutoSec creates the requisite linkage between the ever-changing reality of cybersecurity challenges and the ability to deploy protection quickly based on an open ecosystem approach. AutoSec is built to evolve with the cybersecurity needs of the vehicle. **AutoSec detects new threats, alerts, provides protection elements to be deployed and enables the update of all stages of cybersecurity plans, including conceptual, development, production and post-production stages in order to ensure full compliancy with ISO 21434 and WP.29.**



AUTOSEC PROTECTS
THROUGHOUT A VEHICLE'S ENTIRE LIFECYCLE

AutoSec generates the security components that your vehicles require as new threats arise. AutoSec automatically generates the actual binaries/code snippets to update your vehicle's binaries (such as through over the air updates) in order to update vehicles for full protection.

For example, AutoSec will provide you with the exact code for updating a required firewall rule.

AutoSec can also provide prioritized recommendations for deploying vehicle component updates.

AUTOSEC IS GOING ABOVE AND BEYOND
THE STANDARDS

AutoSec provides a variety of additional benefits that contribute to your system, your organization and its users – over and above those required for compliance with the ISO 21434 and WP.29 standards. While automatically performing a variety of risk impact analysis calculations, AutoSec can help you create a better security product. Its various risks management features enable you to prioritize mitigation according to risk factors and to better serve and protect your own organization in ways that would otherwise require significant budget and resource investments. For example, for each detected threat, the ISO 21434 standard requires the assessment of security risk from the aspect of its safety impact on road users. AutoSec enables you to extend this configuration in order to analyze the same threats for their impact on your business.

AWARD WINNING SOLUTION

SECURITY ORCHESTRATION SOLUTION OF THE YEAR 2021

AUTOMOTIVE SECURITY SOLUTION 2021

CYBERSECURITY INDUSTRY SOLUTION 2021

INNOVATION OF THE YEAR 2020

04
AUTOSEC REGULATION COVERAGE

INTRODUCTION TO WP. 29 AND ISO 21434

The World Forum for the Harmonization of Vehicle Regulations (WP.29) is a global regulatory forum within the institutional framework of the UN Economic Commission for Europe (UNECE). UNECE WP. 29 cybersecurity regulations refer to the new ISO 21434 standard as its implementation standard. The cybersecurity regulations of WP.29 are comprised of two parts, **Cybersecurity Management System (CSMS)** and **Type Approval** which together covers the necessary security processes needed for security of the car lifecycle including development, production and post production.

01. CYBERSECURITY MANAGEMENT SYSTEM (CSMS)

For managing all aspects of vehicle security lifecycle, which is comprised of three parts –

1. Development phase
2. Production (implementation) phase
3. Post-production phase

For each of these phases, the vehicle manufacturer must demonstrate compliance with the cybersecurity management processes defined in the regulations.

02. TYPE APPROVAL

Approval of each vehicle coming off the production line. The Type Approval of each vehicle consists of a list of the cybersecurity processes managed by the CSMS, meaning that the prerequisite for cybersecurity type approval is a CSMS certificate.

AUTOSEC: REGULATORY COMPLIANCE MADE EASY

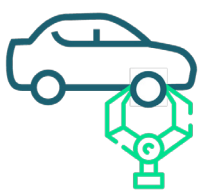
ALIGN WITH VEHICLE SECURITY LIFECYCLE

AutoSec ensures full coverage of regulation requirements throughout a vehicle's entire lifecycle – starting from the **Conceptual phase**, throughout the **Product Development phase** and including the **Post-Production phase.** AutoSec's simplifies and guides you through the complexity of the multitude of requirements and detailed methodology sequences required by the ISO 21434 standard.

AutoSec Ensures Full Compliance by Guiding You Through the Stages Required by the Regulation:

Conceptual Phase

Consists of defining the TARA model, creating real requirements and using the AutoSec risk analysis decision support tool.



Product Development (Implementation) Phase

AutoSec's product development features help you plan the implementation of hardware and software components and maps the actual implementation of each component to those planned in the TARA model during the Conceptual phase (described above).

Post-Production Phase

Alerts you regarding emerging threats and enables you to pinpoint their exact location in your system, while guiding you through updating the TARA, according to the various aspects of the standards' requirements.

COMPLIANCE GUIDANCE

The AutoSec user interface guides you through the process of understanding various aspects of automotive security compliance and provides the workflows and user interface for for adhering to them. Simply following along the straightforward forms and workflows provided by AutoSec will leave you rest assured of complying with ISO 21434 and WP.29 requirements.

COMPLIANCE EVIDENCE

AutoSec ushers you through the activities that are required in order to submit compliance evidence to auditors. AutoSec provides a single management tool that enables a compliance auditor to see and analyze the entire cybersecurity project, as well as the processes that were used, the security rules, the requirements and the decisions that were taken. AutoSec automatically generates and fills out all necessary work product forms and documentation of security management, methodologies and compliance in order to provide evidence for compliance auditors.

AUTOSEC'S ISO 21434 COVERAGE

The ***ISO/SAE 21434 – Road vehicles – Cybersecurity Engineering*** describe how to implement a cybersecurity management system that includes cybersecurity risk management. The following specifies each of the clauses in the ISO 21434 standard and the support provided by AutoSec in order to enable your compliance.

ORGANIZATIONAL PROJECT MANAGEMENT

CLAUSE 5

ORGANIZATIONAL CYBERSECURITY MANAGEMENT

Clause 5 (5.4.1–5.4.7) involves Organizational Cybersecurity Management.
It includes directives regarding how the organization should handle its cybersecurity management and how it should specify its organizational cybersecurity policies, rules, documentation, training, configuration, change management and general processes.

AUTOSEC SUPPORT

AutoSec will integrate with these processes for supplying the necessary security information for the different management processes.

CLAUSE 6

PROJECT DEPENDENT CYBERSECURITY MANAGEMENT

Clause 6 includes the cybersecurity management and cybersecurity activities at the project level. OEM companies typically produce multiple products that may involve multiple Tier-1 suppliers. Each project requires its own cybersecurity management throughout each system's entire lifecycle – all must comply with WP.29 regulations and must produce documented evidence that proves this compliance.

AUTOSEC SUPPORT

- AutoSec handles Clause 6 (6.4.1 – 6.4.2), which is Project Dependent Cybersecurity Management. AutoSec's will soon be handling clauses 6.4.3 through 6.4.9.
- AutoSec provides a **single comprehensive platform** for managing all such projects.
- AutoSec enables the **definition of various user roles and responsibilities for creating, updating and monitoring various aspects of a vehicle's cybersecurity plan.** Each user role is authorized to access data and functionality according to their responsibilities. AutoSec then enforces these user authorizations throughout the AutoSec platform interface.

CLAUSE 7 | SUPPLY CHAIN HARMONIZATION

DISTRIBUTED CYBERSECURITY ACTIVITIES

Clause 7 deals with distributed cybersecurity activities. This includes requirements for assigning supply chain cybersecurity responsibilities and activities between customers and suppliers. This includes providing the user interface for managing the supply chain and providing a channel for them to communicate.

AUTOSEC SUPPORT

AutoSec provides **visibility across the entire supply chain** and provides APIs and delegation options that enable the distribution of the security work and integrate security results across the supply chain.

VULNERABILITY MANAGEMENT

CLAUSE 8

CONTINUAL CYBERSECURITY ACTIVITIES

This clause specifies standards for ongoing cybersecurity activities, such as activities that provide information for ongoing risk assessments, and defines vulnerability management of systems throughout the entire cycle of cybersecurity support. This involves defining the channels of information used to monitor vulnerabilities in your product (security events) and how these events are documented and analyzed. These continuous cybersecurity activities are ongoing – starting from the development phases and lasting throughout the post-development phases.

AUTOSEC SUPPORT

- AutoSec provides **integrated vulnerability information about the project's assets, which is based on the risk assessments that it performs.** This information is generated by both manual assessments and security tools, such as AutoSec Protector binary analysis.
- In addition AutoSec's API supports interfaces with 3rd party solutions for any purpose, such as to use external tools for vulnerability tracking (such as AVL) or to enable the integration of security events into AutoSec. Events that have been derived from these external systems are analyzed and included in AutoSec's risk assessments and in its cybersecurity mitigations in the same way as all other vulnerabilities.

CONCEPTUAL PHASE

CLAUSE 9 | CONCEPT AND CLAUSE 15, CONCEPT, THREAT ANALYSIS AND RISK ASSESSMENT METHODS

CONTINUAL CYBERSECURITY ACTIVITIES

The standards described in Clause 9 involve the security activities of the concept design stage and include activities that determine cybersecurity risks, cybersecurity goals and cybersecurity requirements for each item.

AUTOSEC SUPPORT

AutoSec enables a **security assessor** to define an item and then perform all necessary TARA activities.

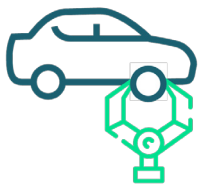
CLAUSE 15

THREAT ANALYSIS AND RISK ASSESSMENT METHODS (15.3 – 15.9)

These clauses include modular methods for analysis and assessment that determine the extent of cybersecurity risk.

AUTOSEC SUPPORT

AutoSec provides **comprehensive support for all the work projects and activities required by the conceptual clauses of ISO 21434,** including item definitions (clause 9.3), cybersecurity goals (clause 9.4) and cybersecurity concept (clause 9.5) definitions. AutoSec also guides you through all necessary stages of defining a TARA and tracking your progress as you do so.



DEVELOPMENT PHASE

CLAUSE 10

PRODUCT DEVELOPMENT

These clauses apply to the implementation/ product development stage of the system's development lifecycle, including implementation and testing requirements.

AUTOSEC SUPPORT

AutoSec's helps you **protect the implementation design** by fleshing out the Conceptual phase and by defining and implementing specific hardware and software components and mapping the actual implementation of each component to those planned in the TARA model during the Conceptual phase. In addition, AutoSec helps you define security specifications and to manage the vulnerabilities found during the Development phase.

AUTOSEC TRACEABILITY SUPPORT

AutoSec provides **comprehensive traceability between the Product Development (implementation) phase** and the Conceptual phase. AutoSec provides the visibility that enables security assessors to easily navigate between every security requirement defined in the Conceptual phase and its implementation in the Product Development phase and vice versa.

CLAUSE 11

CYBERSECURITY VALIDATION

Clause 11 includes the cybersecurity validation of each item at the vehicle level.

AUTOSEC REFINEMENT SUPPORT

AutoSec provides refined **detail-oriented validation features** that enable users to verify that the high-level definitions specified in the Conceptual phase are fully detailed (fleshed out) in the most technical manner in the Product Development (Implementation phase).

POST DEVELOPMENT PHASE

CLAUSE 12

CYBERSECURITY VALIDATION

Clause 12 includes the cybersecurity-related aspects of manufacturing and assembly of an item or component, including key (cryptographic) management.

AUTOSEC SUPPORT

Clause 12 will be supported by AutoSec soon.

CLAUSE 13

CYBERSECURITY VALIDATION

Clause 13 covers activities relating to cybersecurity incident response and item/component updates.

AUTOSEC SUPPORT

- AutoSec provides **decision-making and management support** for situations where the result of an incident is the need for a vehicle component update. Using AutoSec will help determine which component needs to be updated, exactly which update is required and how the product's risk management is affected.
- The overall structure of how incident response is populated inside an organization is expected to be handled at the organizational level.
- Clause 13.4 specifies the need for decision-making processes for updating vehicle components and will soon be supported by AutoSec.

CLAUSE 14

CYBERSECURITY VALIDATION

Clause 14 includes cybersecurity considerations for end of support and decommissioning of an item or component.

AUTOSEC SUPPORT

Clause 14 is expected to be handled by the organization itself.

05
CONCLUSION

The automotive industry is in the midst of an upheaval, as automakers struggle with connected vehicle architectures, new standards, regulations and a fragmented supply chain.

An opportunity has emerged to transform archaic approaches to cybersecurity lifecycle management into digital solutions that provide visibility and control throughout the vehicle lifecycle. With new solutions, the industry can better manage modern vehicle architectures, in order to significantly speed up the reaction to attacks for the entire supply chain and better collaborate to implement an ISO 21434 framework, and other regulations for the future.

Our findings have only reinforced that visibility and traceability are essential to the implementation of ISO 21434 in performing accurate and fast risk assessment processes and to deploying and maintaining protection of automotive cybersecurity.

Furthermore, the supply chain is in desperate need for harmonized communication through a central management system that will enable all parties to speak the same language and tackle problems efficiently, and as one entity. All of this can be enabled with automation and digitization, which should have a larger share in dealing with cybersecurity needs of connected cars.

This opportunity is one that should be taken now, and with urgency. Armed with visibility, the industry will be able to come together to streamline cybersecurity lifecycle management to bring safer vehicles to the road for drivers, passengers and pedestrians alike.

With new solutions like AutoSec, the industry can better manage modern vehicle architecture, significantly speed up the reaction to attacks and better collaborate to implement ISO 21434 framework.

ABOUT C2A SECURITY

C2A Security is a trusted end-to-end automotive cybersecurity solutions provider. Its embedded cybersecurity solutions and cybersecurity lifecycle management platform empower the automotive industry with visibility and control over the bespoke solutions needed to protect today's and tomorrow's connected vehicles. Armed with the understanding that cybersecurity is a process, not a product, C2A's holistic approach includes a comprehensive, multi-layered technology suite scalable enough for the entire vehicle lifecycle. C2A products' minimal footprint and compute resources consumption give them the flexibility to fit into any automotive ECU.

With market neutrality, complete fluency in the needs of the automotive industry and ease of integration, C2A is redefining the automotive cybersecurity ecosystem as the sole provider of the most flexible, comprehensive, and transparent cybersecurity solution on the market.

To learn more about AutoSec: info@c2a-sec.com www.c2a-sec.com