Seamless **WP.29** Implementation

Preparing for the cybersecurity regulation changes coming to the automotive industry

AUTOCRYPT

Secure First, Then Ride

CONTENTS

03 ..... STATE OF CONNECTED VEHICLES

04 ..... WHAT IS WP.29?

04 ..... BACKGROUND

06 ..... CSMS / SUMS

07 ..... TIMELINE

08 ..... CHECKLIST FOR COMPLIANCE

09 ..... STEPS TO COMPLIANCE

09 ..... CONSULTING & TRAINING

09 ..... ECU SECURITY

10 ..... INTRUSION DETECTION SYSTEM

11 ..... TESTING

11 ..... WP.29 WITH AUTOCRYPT

12 ..... CONCLUSION

13 ..... APPENDIX

STATE OF CONNECTED VEHICLES

Connected vehicle technology is quickly becoming standard in modern vehicles.

Many modern vehicles on the market have some sort of automated technology, ranging from basic Advanced Driver-Assistance Systems (ADAS) features like cruise control to more advanced features like collision warning systems, lane change monitoring, and automatic lane centering,

Currently, the new autonomous vehicles making it onto the market are nearing Level 3, based on the Society of Automotive Engineers (SAE), meaning that the Automated Driving System (ADS) is the primary driver. However, the human driver is still required to stand by, expected to override when the system is unable.

There is no doubt that autonomous and connected vehicles will continue to improve and develop in technology, and expand its prevalence on public roads. It is estimated that one in 10 cars will be fully automated by 2030.*

However, there are still major issues that loom overhead. Consumers are still hesitant about the trustworthiness and security of autonomous vehicles. According to a recent poll, nearly 3 in 4 Americans say they do not believe that AV technology is ready. 20% said that they do not believe that AVs will ever be safe.**

These concerns are understandable, as the industry and society as a whole have not done enough to appease the general public that AVs are safe.

Regulations and standards can vary from state to state, country to country, causing issues with jurisdiction, liability, and cybersecurity across the board. This is an area that the automotive industry, cybersecurity companies, and overseeing governments can cooperate in, working towards a future where autonomous vehicles become a seamless, secure part of transportation and society.

* Statista, Autonomous Vehicles Report, 2019.
** Partners for Automated Vehicle Education, Survey USA, 2020 Poll.

WHAT IS WP.29?

BACKGROUND

Although many may think that the term "WP.29" refers to new regulations released in June 2020,

“WP.29” in actuality is the shorthand title of the working party within the United Nations Economic Commission for Europe (UNECE). The ”Working Party on the Construction of Vehicles” or "WP.29" was formed over 50 years ago for the purpose of initiating and pursuing actions for worldwide harmony when it comes to the development of regulations for vehicles and transportation. The Working Party is the largest international vehicle regulatory system in the world.

The Working Party, WP.29, recently garnered attention from the automotive industry because of new regulations that a sub-working party, GRVA, or Working Party on Automated/Autonomous and Connected Vehicles, drafted up. With the rise of connected and autonomous vehicles on the market, the GRVA's regulations state that countries must require that comprehensive cybersecurity measures be implemented for all new vehicle models after July 2022. All 54 countries contracted under the 1958 Agreement Concerning Wheeled Vehicles* must implement these regulations.

Countries signed to the 1958 Agreement (as of December 2018)

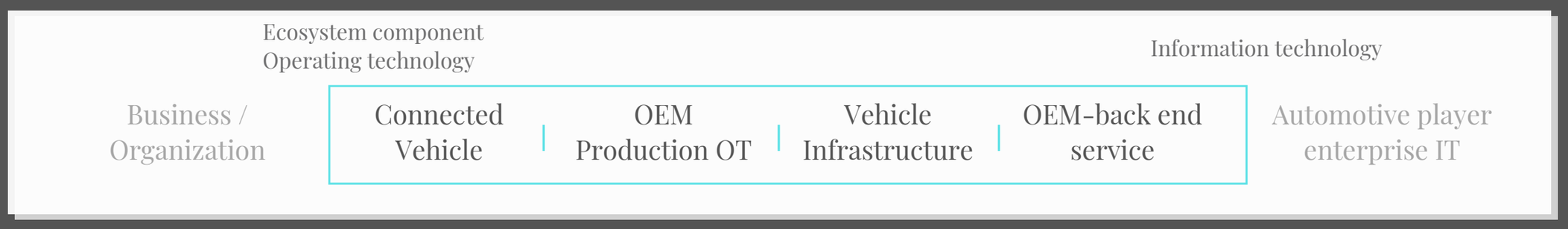
For these 54 countries, as well as the countries who have business operations in any of the countries, this means that within the next few years, they will have to make major adjustments in the way vehicles are manufactured, programmed, and distributed.

* Full title: Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be fitted and /or be used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, of 20 March 1958

The regulations are implemented across four distinct disciplines:

Manage vehicular cyber risks	Secure vehicles by design, mitigating risks along the value chain	Detect and respond to security incidents across the vehicle fleet	Provide safe, secure software updates, and ensure vehicle safety is not compromised, introducing legal basis for O.T.A. updates to on-board vehicle software

As the deadline for implementation grows closer, governments have begun long discussions of how to properly change legislations in order to be in compliance. However, although the contracted parties are government nations, the industry directed affected is the automobile industry. Be it an automobile manufacturer, an OEM or Tier-1 supplier, software or service provider, most parts of the industry will be affected by the impending changes.



Although the onus of the cybersecurity management lies upon the manufacturers and OEMs, Tier 1 and Tier 2 suppliers are not exempt from compliance. OEMs are required to collect and verify information for compliance throughout the supply chain so that risks are identified and managed.

In terms of the vehicles themselves, the regulations apply to vehicles in categories M and N (essentially, vehicles with four or more wheels with specific load capacities), though categories of O, R, S, and T are under consideration. If the vehicles are equipped with automated driving functions at a level 3 or beyond, they will also fall under the regulations.

If the vehicle in question...

- [x] Utilizes a wired or wireless connection to the vehicle's internal communication network
- [x] Utilizes a wired or wireless connection to the external communication network of the vehicle
- [x] Connects indirectly to the vehicle network
- [x] Utilizes electronic or optoelectronic hardware
- [x] Includes software
- [x] Includes sensors

...the vehicle will have to be compliant with the WP.29's regulations.

CSMS / SUMS

The two regulations distinctly divide into regulations for a Cybersecurity Management System (CSMS), R155, and Software Update Management System (SUMS), R156.

Those with background in engineering and computing may find the terminology confusing, as "system" in both these cases does not refer to a hardware or software system handled by a server; rather, "system" refers simply to a process to go through in terms of placing the right people, products, and protocol to meet the goal of compliance.

For connected and autonomous vehicles, software updates are crucial and essential, SUMS focuses on this aspect of the autonomous vehicles, ensuring that updates and their impacts are visible to the driver, vehicle, and external authorities.

CSMS gets more of the attention when it comes to the WP.29 regulations because of its holistic approach. It facilitates security for the whole lifecycle of a vehicle, from design up to the end of support.

To be compliant, all new vehicles will have to go through a certification and approval process. With the CSMS regulation, CSMS certification as well as a more specific Vehicle Type approval will be required. Vehicle Type approval will involve a comprehensive testing and certification process, analyzing the design of the vehicle, risk assessment, and cybersecurity controls. Vehicle Type approval will need to be maintained throughout the modification of vehicles and --extensions of the vehicle if it affects the vehicle's technical performance in terms of cybersecurity.

TIMELINE

June 2020

UNECE releases two new regulations for software updates and cyber security management in vehicles

January 2021

The UN regulations automatically "enter into force," which means that countries signed to the agreement can begin legislation integration.

July 2022

New vehicle types with electronic architecture will be required to obtain certificates for cyber security management system approval as part of vehicle type approval

July 2024

The regulation states that system type approval for all vehicles produced after July 2024 will be mandatory for vehicle registration

The regulations officially enter into force in January 2021. However, this is merely the date when countries that have signed the 1958 agreement can begin to integrate the regulations into national legislation.

For example, while Japan has stated that it will apply regulations upon the entry-into-force date, in the European Union, the regulations will be mandatory beginning in July 2022. Korea has stated a stepwise approach, introducing the provisions of the regulations into national guidelines in the second-half of 2020.

Varied approaches by different governments means automotive manufacturers will have to consider the region in which their automotive business operations take place. Though their headquarters may be in one country, if sales and software providers are located in another region, jurisdiction will take precedent.

Although the timelines are varied, because WP.29's regulations are binding for the contracting parties, those that do not comply may face trade issues and challenges in brand imaging, as the lack of prioritizing safety and security will not allow for a trusting, long-term relationship with partners or consumers.

CHECKLIST FOR COMPLIANCE

According to the UNECE WP.29 working party, manufacturers and those related in the supply chain will have to ensure compliance in the following ways:

CYBER SECURITY MANAGEMENT SYSTEMS (CSMS)

Automotive Industry / Sector

- ☑ Identify and manage cyber security risks in vehicle design
- ☑ Verify that the risks are managed, including testing
- ☑ Ensure that risk assessments are kept current
- ☑ Monitor cyber-attacks and effectively respond to them
- ☑ Support analysis of successful or attempted attacks
- ☑ Assess if cyber security measures remain effective for new threats and vulnerabilities

Manufacturers

- ☑ CSMS is in place and its application to vehicles on the road is available
- ☑ Provide risk assessment analysis, identify what is critical
- ☑ Mitigation measures to reduce risks are identified
- ☑ Evidence that mitigation measures work as intended
- ☑ Ensure measures are in place to detect and prevent cyber-attacks, and support data forensics
- ☑ Monitor activities specific for the vehicle type
- ☑ Transmit reports of monitoring activities to relevant approval authority

SOFTWARE UPDATE MANAGEMENT SYSTEMS (SUMS)

Automotive Industry / Sector

- ☑ Record hardware/software versions for vehicle type
- ☑ Identifying software relevant for type approval
- ☑ Verifying the software on a component
- ☑ Identify interdependencies, especially with regards to software updates
- ☑ Identify vehicle targets and verify compatibility with update
- ☑ Assess if software update affects type approval or legally defined parameters (including adding / removing functions)
- ☑ Assess if an update affects safety or safe driving Inform vehicle owners of updates

Manufacturers

- ☑ SUMS is in place and its application to vehicles on the road is available
- ☑ Protect SU delivery mechanism and ensure integrity and authenticity
- ☑ Protect software identification numbers
- ☑ Ensure that software identification number is readable from the vehicle

OVER-THE AIR (OTA) SOFTWARE UPDATES

- ☑ Restore function if update fails
- ☑ Execute update only if sufficient power
- ☑ Ensure safe execution
- ☑ Inform users about each update and their completion
- ☑ Ensure vehicle can conduct updates
- ☑ Inform user when a mechanic is needed

Source: United Nations Economic Commission for Europe Information Unit, Press Release, 25 June 2020.
DISCLAIMER: This document is for informational purposes only. It should not be relied upon or construed as legal opinion or legal advice regarding any specific issue or factual circumstance. For more information about how AUTOCRYPT can help you and your company meet WP.29 needs, contact our team directly.

STEPS TO COMPLIANCE

Brought to you by AUTOCRYPT

Many companies in the automotive sector have mapped out a timeline to ensure that new vehicle models will be compliant when their respective countries begin implementation into legislation. However, with the comprehensive nature of the compliance regulations, the road ahead may be complex.

The criteria for CSMS and vehicle approval for cyber security are extensive, and this is where automotive cyber security solutions providers come in to ensure that proper protocols are followed, and that there is no part of the vehicle that is left out of the system.

AUTOCRYPT provides a three-fold, comprehensive approach to CSMS compliance, beginning with consultation with automotive security specialists.

Consulting & Training

Our security experts conduct:

- Overview of existing CSMS
- TARA-based Risk Assessment *
- Recommendations for security engineering

Solutions

AutoCrypt IVS:

- ECU Security
- Intrusion Detection System

Testing

CSMS routine testing with:

- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

* Threat Assessment and Remediation Analysis

SOLUTIONS

ECU SECURITY

AutoCrypt IVS (In-Vehicle Systems). AutoCrypt IVS has two components that ensure that the vehicle as well as the connections that it relies on are not at risk of attacks, the first of which is ECU security.

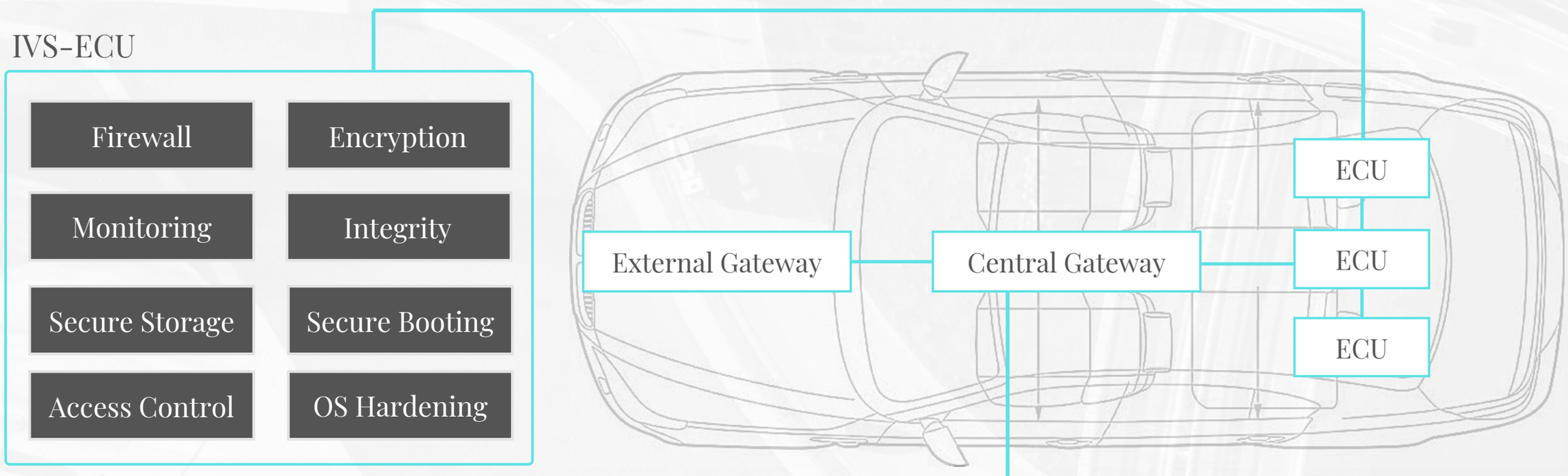
To be properly functional a vehicle must be able to perform many functions simultaneously. Steering, braking, accelerating are the basic functions, but with the evolution of the automobile, we now have other functions integrated into the vehicle like GPS, infotainment, lighting systems, vehicle access systems, remote links, and ADAS (Advanced Driver-Assistance Systems).

These systems are controlled by **ECUs** or **Electronic Control Units**, small hardware devices embedded into a vehicle, which are responsible for controlling specific functions. Each ECU will contain software, programmed for the specific action, and will require power and data connection to operate.

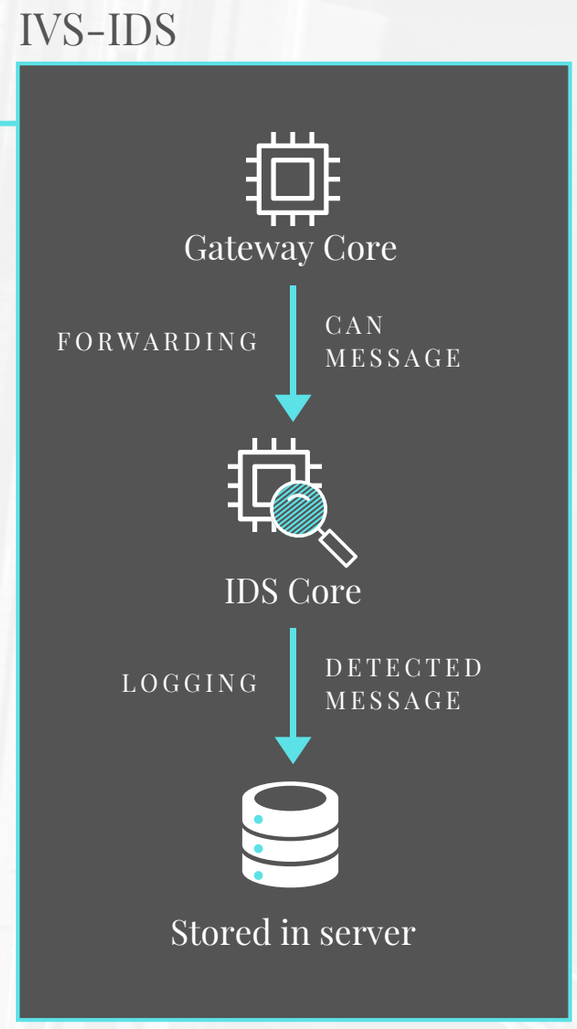
The modern-day connected vehicle may contain over 80 ECUs, all working together to ensure that the driver, passenger, and those around the vehicle remain safe.

The ECU can be compared to a gateway. With access to the ECU, a hacker could implant malware into its firmware, and take control of the car with catastrophic results. Needless to say, ECU security is a crucial part of the cyber security management system.

AutoCrypt IVS provides comprehensive ECU security through IVS-ECU. Through features like an automotive firewall to secure storage and booting, security is reinforced and monitored continually.



However, as ECUs are connected to the CAN (Controller Area Network) bus, the communications between them need to also be secured, which is covered with AUTOCRYPT's Intrusion Detection System (IDS).



SOLUTIONS

INTRUSION DETECTION SYSTEM (IDS)

To monitor the messages through the CAN bus, an Intrusion Detection System is essential.

AutoCrypt IVS-IDS analyzes network packets for any signs of abnormal behavior or attack for both internal and external communication networks. Messages are securely stored in a server for monitoring purposes.

TESTING

AUTOCRYPT works with manufacturers and suppliers not only to put security components in place, but also follows with routine testing.

Vulnerability Scanning	Vulnerability analysis at each stage of product development allows for mitigating risks and eliminating additional threats. ▪ **Software static testing:** Test without executing code to find and eliminate errors or ambiguities ▪ **Software dynamic testing:** Test with execution of code to find weak areas in runtime environment and behavior of dynamic variables
Fuzz Testing	Providing invalid or random data to analyze unknown security vulnerabilities, **fuzzing** allows for monitoring of crashes, potential memory leaks, etc.
Penetration Testing	Utilizing known cyberattacks or vulnerabilities found by TARA to initiate simulated attacks, identifying potential vulnerabilities, and selecting countermeasures to mitigate those vulnerabilites

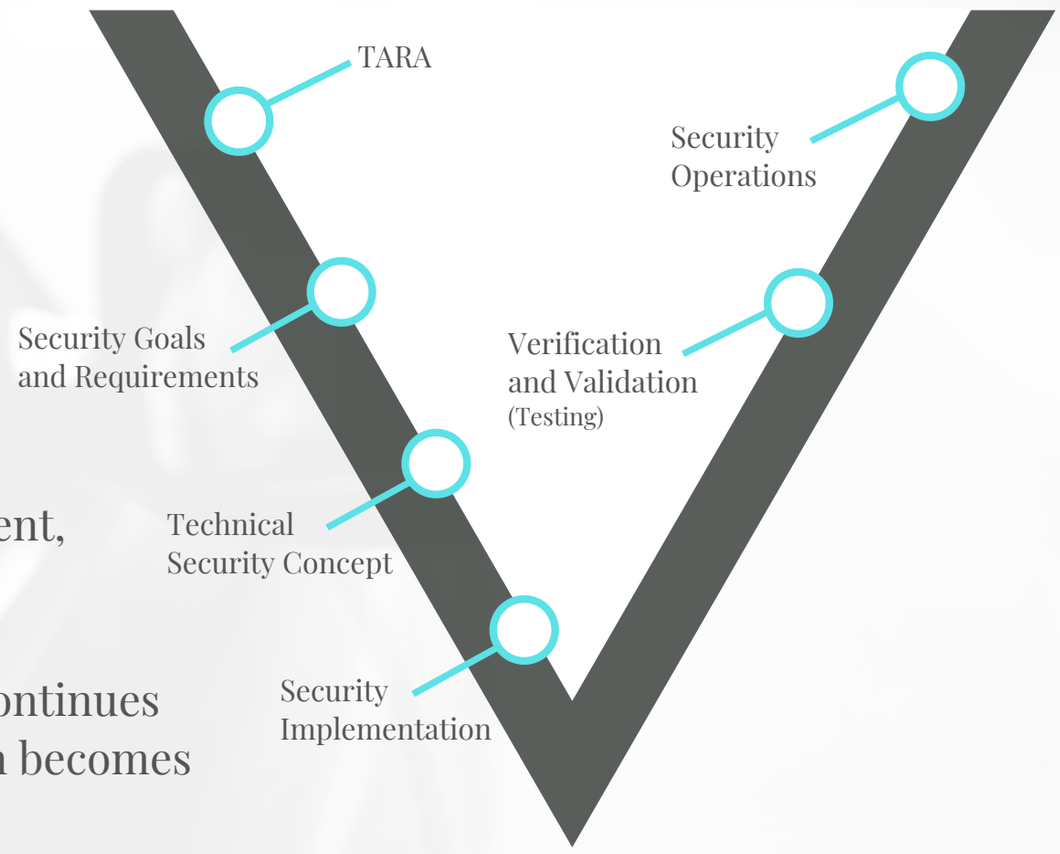
WP.29 with AUTOCRYPT

Security is not a simple, one-step process and with the changing developments in automotive technology, it is crucial that security measures are tested routinely in order to ensure elimination of errors and mitigate risks.

The way to achieve compliance, is also not a one-step process, and we like to utilize the ISO/SAE 21434 risk assessment system model to exemplify our approach.

For every function within the development of the CSMS from the manufacturer or the supplier, development, implementation, and testing occur.

The cycle does not stop at the end, but continues as adjustments are made, and the system becomes increasingly secure.



CONCLUSION

Within the next few years, the industry is sure to see major changes in the technology and design of how vehicles operate and connect. As vehicles become increasingly connected and autonomous, they will only continue to become a more lucrative target for hackers.

There is growing concern about how best to prevent cyber attacks on the road, and while there are cyber security standards and guidelines set by organizations, manufacturers and suppliers may not be required to abide by these guidelines because they are not enforced by any one entity.

Though the regulations from the WP.29 may seem to be complex, as part of national legislation, they encourage all of the automotive sector to delve into the necessary precautions that a vehicle needs in order to securely operate for those both in and around the vehicle.

We encourage all those involved to get a head start on structuring their CSMS and preparing for type approval because ultimately, AUTOCRYPT and WP.29's goals are one and the same. We look forward to having all roads and those on it secure.

For more information on AUTOCRYPT and its security offerings,
visit www.autocrypt.io

To speak to our team about preparing for WP.29 compliance,
contact us at info@autocrypt.io

APPENDIX

Official Press Release :
UN Regulations on Cybersecurity and Software Updates to Pave the Way for Mass Roll out of Connected Vehicles
https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html.

Full regulation text :
http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

Statista, Autonomous Vehicles 2019 :
https://www.statista.com/study/69417/autonomous-vehicles/

Partners for Automated Vehicle Education 2020 Poll :
https://pavecampaign.org/wp-content/uploads/2020/05/PAVE-Poll_Fact-Sheet.pdf

Original 1958 Agreement :
https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XI-B-16&chapter=11

AUTOCRYPT Official Website :
https://www.autocrypt.io

AUTOCRYPT