AUTOCRYPT

CYBERSECURITY MANAGEMENT FOR **SOFTWARE DEFINED VEHICLES**

Regulatory compliance, testing, and beyond

TABLE OF CONTENTS

INTRODUCTION

In the span of human history, security has been a constant necessity in society.

From the beginning of time, humans have focused on securing what is ours. As society evolved with industrial and technological advances, the scope of securing resources expanded to not just tangible belongings like food, shelter, and money, but to non-tangible resources like data, the cloud, and even the blockchain.

Ironically, securing non-tangible resources can be much trickier than securing tangible ones, as virtual connections and pathways are not visible to the human eye. This is where we see the rise of IT security and the securing on applications and systems. Security solutions for both personal and enterprise usage became prioritized and even commonplace.

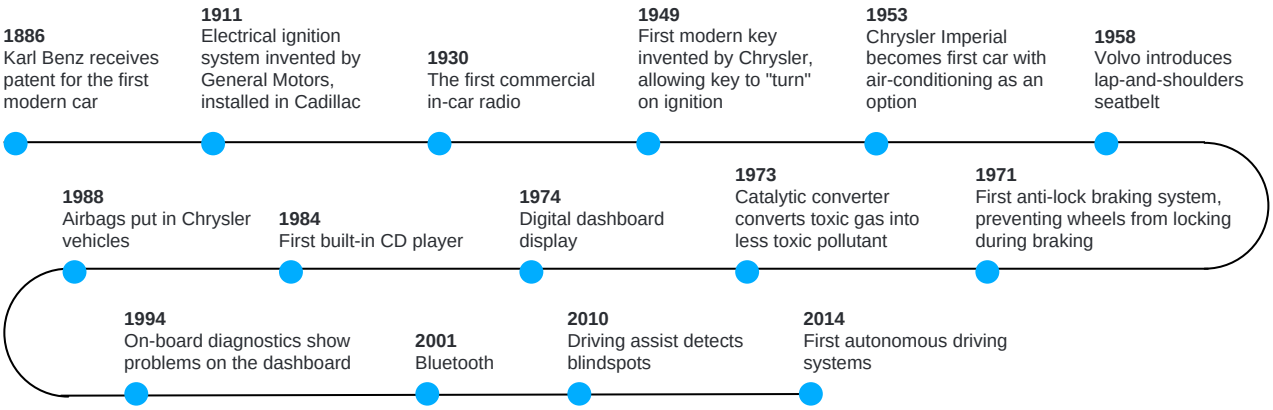
However, as society is bound to do – technology continues to advance, and now we see connectivity implemented in complex ecosystems like transportation and mobility. Vehicles are becoming more connected than ever, with a push to become fully autonomous, but connecting software-driven, moving vehicles is a feat of a whole new dimension.

This white paper will look at the growing industry of software-defined vehicles (SDVs), related security risks, as well as regulatory compliance for those involved and offerings to facilitate this compliance. This will not be a one-time implementation, but as technology changes and advances to become more connected and ultimately support fully autonomous driving, a comprehensive and cyclical approach to ensuring that the entire mobility ecosystem stays safe will be a necessity.

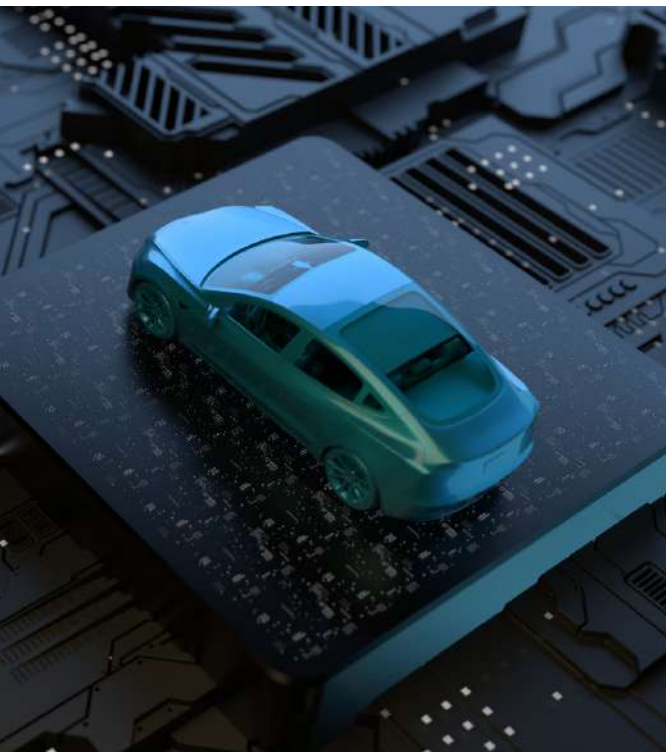
THE RISE OF THE SOFTWARE DEFINED VEHICLE

Vehicle Technology

Throughout the history of the automobile, technological advances have come quickly and steadily. In the 20th century, vehicle ownership has become commonplace for the many, and due to a surge in demand, new features continued to be added. Technological advances like the key fob, radio, and even decarbonization via electric vehicles have contributed greatly to automotive technology history.



Source: Abridged version of "Infographic: The History of Automotive Technology" by Autocrypt, 2020.



The new technological features were visible to the driver and passengers of the car, but there was also a shift in the technology hidden inside the vehicle. It's widely believed that around 1978, General Motors first introduced an electronics system into an automobile, and this thus began the evolution of the Electronic Control Unit (ECU).[1]

Essentially a microcontroller, an ECU can control the electrical systems and subsystems of a vehicle. Though cars started out with only a handful of ECUs to control essential functions like power or steering control, modern-day vehicles have evolved to contain 60 to 100 ECUs per vehicle – in fact, some luxury car models may contain up to 150 ECUs.

Each ECU acts independently as a node, but also as a network – a supercomputer, of sorts. They contribute to the larger vehicle network architecture and contain millions of lines of code, executing simultaneously. Therefore, we see the change from a car simply being a work of mechanical art, to it being a truly connected phenomenon.

1. Moynahan, Nathan A., "Development of a vehicle road load model for ECU broadcast power verification in on-road emissions testing" (2005). Graduate Theses, Dissertations, and Problem Reports. 1675. https://researchrepository.wvu.edu/etd/1675.

The Connected Car

With this supercomputer on wheels, it was only a matter of time before connectivity was added into the mix. In essence, a connected car connects to the Internet, sharing data and messages between the vehicle and whatever endpoint it is connecting to.

This opened up vehicle technology to a completely new realm of possibilities. Vehicles' systems (both embedded or tethered) could now send and receive messages, connect with other devices, and utilize applications, similar to a smartphone or a computer.

Applications of V2X technology include:

- Collision avoidance
- Hazard warning
- Vulnerable road user (VRU) protection
- Emergency services support
- Intersection assistance
- Signal phase and timing (SPaT)
- Vehicle platooning
- Traffic data sharing

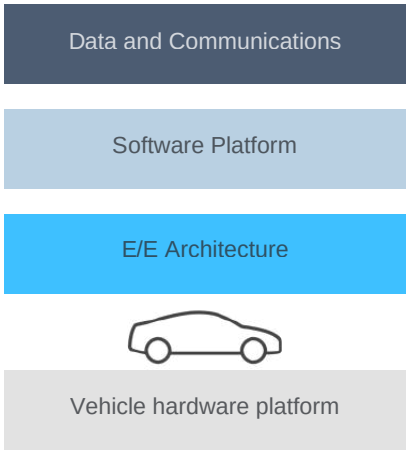
Connectivity also brought to the forefront the now very real possibility of autonomous driving. A phenomenon depicted in science fiction and futuristic films for decades, "self-driving" vehicles seemed to now be a "when" and not just "if" scenario. Connectivity meant that cars could now communicate with other vehicles, devices, infrastructure, and the network – via Vehicle-to-Everything (V2X) technology. The implementation of V2X technology opens up a wide array of possibilities for autonomous driving and moreover, pedestrian safety.

Because V2X technology allows for near real-time communications, vehicles as well as road users like pedestrians or cyclists can connect directly with cars on the move, alerting each other of their locations and impending situations.

Software-Defined Vehicles

When many of us buy a vehicle, we are well aware of its hefty price tag. And it's true – hardware vehicles are priced accordingly depending on their horsepower, performance, as well as brand value. But as we have seen throughout automotive history, car technology is ever-evolving. The next iteration of the connected car is the Software-Defined Vehicle, or SDV. As its name implies, a "software-defined vehicle" describes a vehicle that is enabled through various features and functions like driving assistance, infotainment, or parking assistance – all powered by software.

Now, what difference does this make? With the fast-paced changes in the automotive industry and vehicular technology, software-defined vehicles are a game changer.



Source: Adapted version of Hyundai Motor Group "Software House", 2022.

For the driver, SDVs allow for greater customization and convenient usage of the vehicle. For example, vehicle applications will be much more customizable on the spot through Features on Demand (FoD) and upgrades will be "over-the-air" (OTA) without the hassle of having to visit a mechanic or an engineer.

For manufacturers, this means a more scalable deployment without the need for hardware upgrades or expensive recalls. For optimized usage, ECUs mentioned previously can now utilize the data taken from inside the vehicle and give software providers as well as vehicle manufacturers insight into the vehicle model's life cycle.

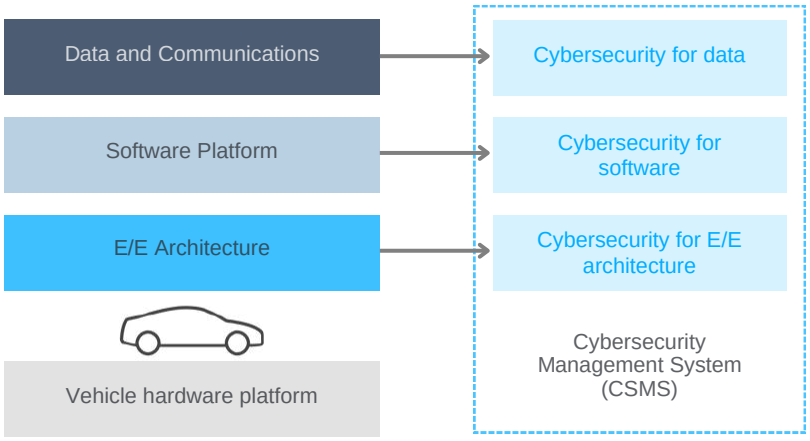
For the automotive industry as a whole, the software-defined vehicle essentially makes the vehicle a a true supercomputer, where the vehicle's hardware, E/E architecture, software, and data are all working together, optimized and updated as a powerhouse of connectivity.

Software vulnerabilities on the road

While software enables greater depth and breadth to what a connected vehicle is capable of, it also expands the cumulative area in which a vehicle needs security. It's no longer just about securing the hardware or the data that the vehicle uses to communicate with other vehicles. But what exactly does it mean in terms of security?

Firstly, many manufacturers work with different software suppliers in order to provide this type of diverse software driven platform that drivers look for. Due to that diversity, it may be difficult to manage the different vendors and their individual tools and security measures.

Second, the aforementioned vehicle layers of hardware, E/E architecture, software, and data will all require different security that works together in order to secure the entire system.



A thorough approach to cybersecurity is especially important because software-based operations and functionalities expand the breadth of connected entities and potential entry points involved in the vehicular environment. For example, connection from the SDV to another vehicle, to a charging point, a mobile device, or to road-side units.

Potential Entry Points of Cyberattacks in Connected Cars

- **OBD-II Port**

  The onboard diagnostics (OBD) tracks a vehicle's condition and driving behavior. Such information is used by fleet operators for management and maintenance. The OBD-II port provides access to information on the powertrain, emission control systems, and all kinds of other driving information.

- **Infrastructure**

  Software communications is not limited to the vehicle. They can extend to roadside units and network operators, who will relay those messages to other end-entities for data analysis, autonomous driving, or mobility services.

- **Head Unit**

  The vehicle's head unit is the closest entry point to the internal system, often containing a mainboard ECU that serves the infotainment system, and a gateway ECU that directs application requests to the CAN bus. If a hacker gains access, they are only one step away from potentially taking over the vehicle

- **Smart Key** *(Mobile)*

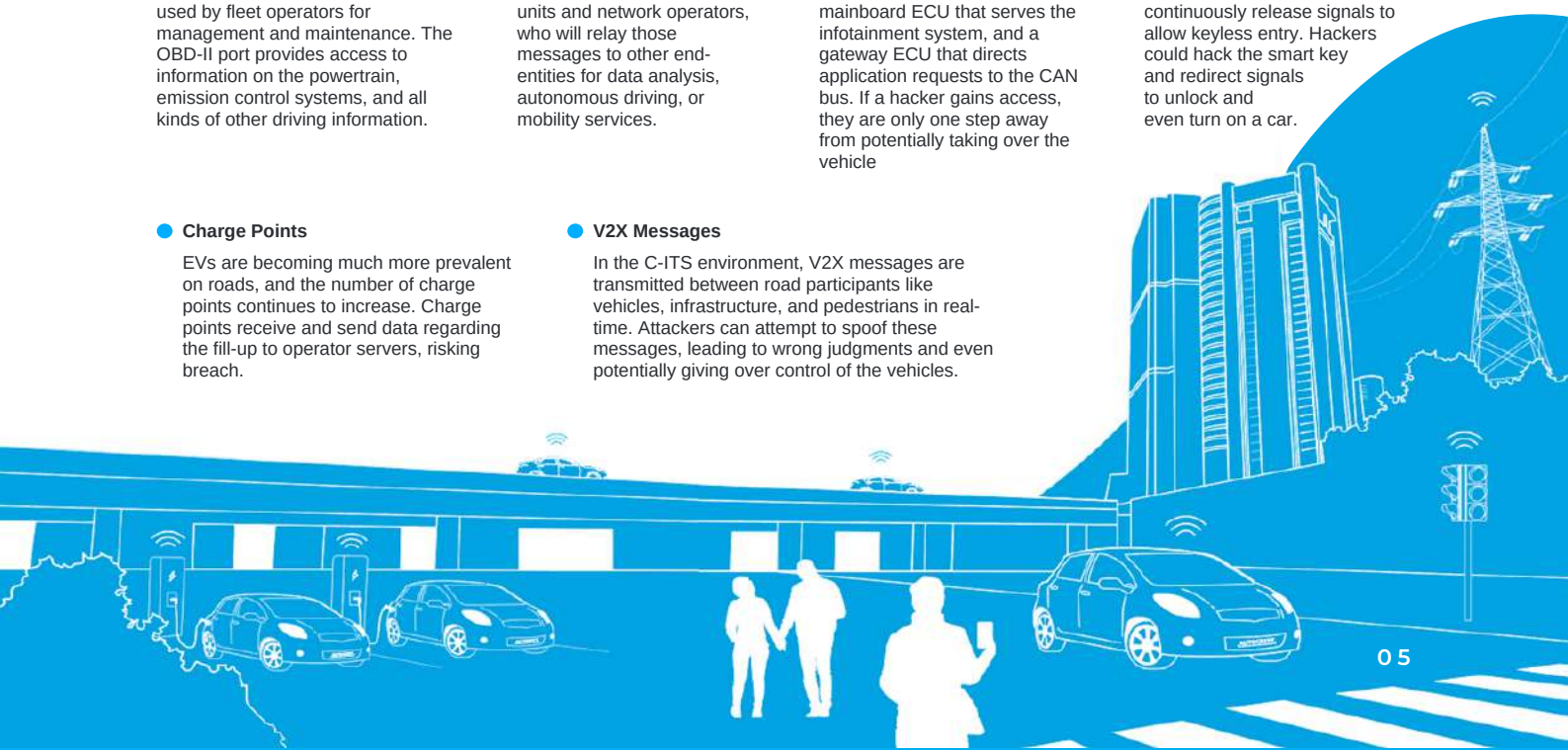
  Smart keys unlock a vehicle with electronic signals. Unlike keys with buttons, smart keys continuously release signals to allow keyless entry. Hackers could hack the smart key and redirect signals to unlock and even turn on a car.

- **Charge Points**

  EVs are becoming much more prevalent on roads, and the number of charge points continues to increase. Charge points receive and send data regarding the fill-up to operator servers, risking breach.

- **V2X Messages**

  In the C-ITS environment, V2X messages are transmitted between road participants like vehicles, infrastructure, and pedestrians in real-time. Attackers can attempt to spoof these messages, leading to wrong judgments and even potentially giving over control of the vehicles.



REGULATORY COMPLIANCE

The types of software and the connections that they will cover will only continue to increase as we move towards getting more SDVs on the road, and this means that the network of suppliers, vendors, and end-entities will continue to expand exponentially – a risk that manufacturers and suppliers need to be well aware of before vehicles hit the market.

As with other types of security and cybersecurity in particular, protecting against these kinds of vulnerabilities often requires several different approaches, but all need to follow a holistic philosophy of security. Thankfully, legislators and regulators are beginning to see the importance of cybersecurity in vehicles and are rolling out cybersecurity regulations and standards worldwide.

Many of us are used to thinking of regulatory compliance as a seal of approval, a certificate bestowed upon makers of a product at the very beginnings of the venture – a one-off deal. And in fact, this type of certificate exists – traditionally, vehicles are given type approval before hitting the market. Regulations dictate what vehicles are fit to be sold on the market and driven on the roads, and the regulation is dictated by the United Nations Economic Commission for Europe (UNECE).

In terms of cybersecurity, different countries have different regulations and standards for validating what may or may not be secure in a connected car. However, as our vehicles become more connected, and more software-defined, compliance is not quite so simple. In fact, many manufacturers and suppliers are left stumped when trying to figure out the ins and outs of a regulation, and when this differs by region or solution, it becomes even more complex.

First off, it is the very nature of SDVs to be able to completely change its software at the click of a button, triggering an over-the-air (OTA) update. But this update, in fact, can affect multiple functions of the vehicle, meaning that validation at one point in time may not apply to the vehicle at another point in time.

And second, there is always the underlying issue of keeping the vehicle safe from security threats which are constantly evolving as the industry evolves.

UNECE's WP.29

To address these concerns, in 2021 the UNECE's World Forum for Harmonization of Vehicle Regulations (WP.29), a special regulatory working party within the UNECE, released two new regulations dealing with adding on a cybersecurity element to the type approval.[2] This was considered a landmark, historic move in the industry, as it was the first time there were cybersecurity regulations for vehicles put in place internationally.

With the two regulations, R155 and R156, the 54 countries contracted under the 1958 Agreement Concerning Wheeled Vehicles were mandated to implement these regulations by 2022. Although there are some major countries that are not a part of the original agreement, the international nature of the industry has made it so that it is nearly impossible to not comply with the regulation in order to continue operations.

2. UNECE. (2020, June 24). UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles . UNECE. Retrieved December 5, 2022, from https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll.

Autocrypt currently offers a comprehensive WP.29 compliance program, a three-step process consisting of consultation, implementation of an in-vehicle systems security solution, and then offensive and defensive testing in order to ensure steps have been completed correctly.

ISO/SAE 21434

> Both the standard and regulation look at securing the entire lifecycle of the vehicle – from vehicle production to post-production.

Alongside WP.29's regulations, ISO/SAE 21434 was jointly developed by the International Organization for Standardization (ISO) and Society of Automotive Engineers (SAE). Titled "Road Vehicles – Cyber Security Engineering,"[3] the standard was officially published in August 2021 though it had been in the works for quite some time.

The WP.29 regulations and the ISO/SAE 21434 standards are not all that different. Both the standard and regulation look at securing the entire lifecycle of the vehicle – from vehicle production to post-production. These guidelines look at security as a process, not a one-stop fix.

What is the difference, then?

The differences lie more in the mandate – while the WP.29 regulations are legally binding for the 54 countries signed to the original agreement, ISO/SAE 21434 is just an international standard that individual companies may, or may not, abide by. However, abiding by the standard and receiving official certification of compliance will put emphasis on the fact that the manufacturer or supplier in question is focused on securing their clients and partners.

The two aren't mutually exclusive, and ideally are to be used complementarily. However, as with the WP.29 regulations, standards can often be difficult to navigate for manufacturers and suppliers, especially those who are not familiar with cybersecurity architecture and the approaches involved in ensuring secure hardware and software within the vehicle.

3. International Organization for Standardization. (2021). Road vehicles—Cybersecurity engineering (ISO Standard No. 21434:2021). https://www.iso.org/standard/70918.html

COMPREHENSIVE CYBERSECURITY MANAGEMENT

Software driven vehicles are unique...

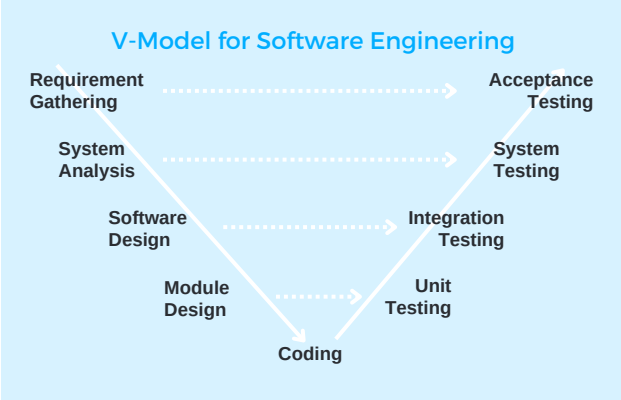
...in the sense that they are likely to contain software from multiple providers all working with different standards and requirements. In order to navigate and secure this sort of environment, a holistic solution is required.

Due to the evolving nature of technology and the industry as a whole, we encourage manufacturers as well as suppliers to seek a comprehensive cybersecurity solution that not only covers the bases of the vehicle's security, but also for complies with mandated regulations and industry-accepted standards, as well as tests using proven defensive and offensive methods in order to ensure vehicles will stay secure.

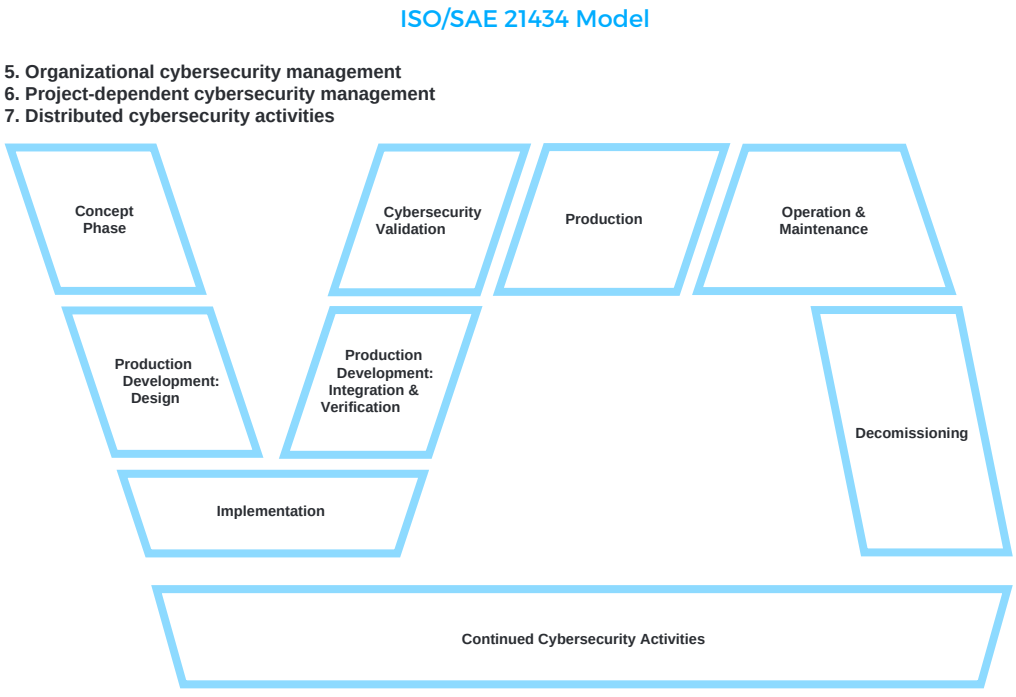
The V Model

A V model is traditionally a software engineering model. Also known as the "Verification and Validation Model," the standard was developed by Paul Rook in the 1980s,[4] and follows a sequence of processes that are not linear but focus on sequences and associated phases of testing.

Due to its iterative nature and reduced risk, the ISO/SAE 21434 standard also uses the V model as a foundation for vehicular cybersecurity.



ISO/SAE 21434 goes through clauses defining the requirements of the standard. Chapters 5-7 are general cybersecurity management practices, and from 8 onward are specific approaches to securing the vehicles.

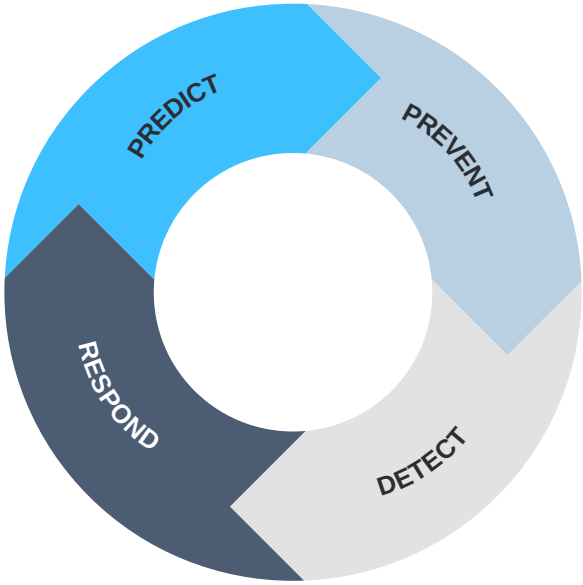


4. Rook, P. (1986). Controlling software projects. Software Engineering Journal, 1(1), 7–16. https://doi.org/10.1049/sej.1986.0003

The model is complex in nature - but that is understandable as one of the most difficult parts of vehicular cybersecurity is the fact that a vehicle does not run on a unified operating system. It instead is made up of hundreds of unique ECUs, interoperating through the Controller Area Network (CAN bus). There is no "off-the-rack" turnkey software or tool. However, a holistic overview of the process can make understanding the needs for security much easier.

To simplify it a bit more, we can look at securing the entire lifecycle of the vehicle in four iterative steps.

1. Predict the risks
2. Prevent the risks with a solution
3. Detect using the solution and other verification and validation methods
4. Respond to the risks and incidents



Because these steps are iterative, they are cyclical in nature - meaning that when step four is complete, that the process will repeat itself again.

Corresponding to the four steps are the following categories of actions that both manufacturers and suppliers can take to implement cybersecurity:

- Consulting and TARA
- Implementation of In-Vehicle Systems Security
- Verification and Validation
- Incident Reporting

We'll be going through each of these categories a bit more in-depth.

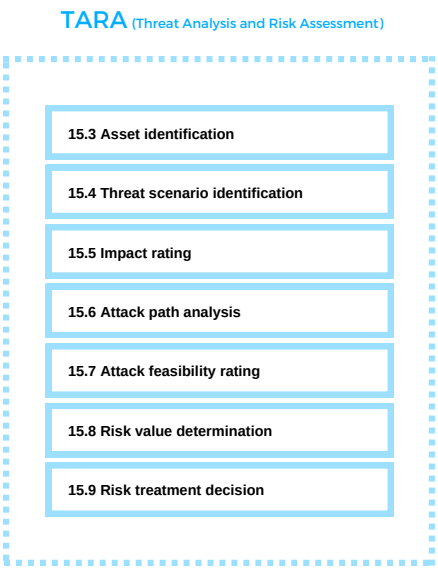


Figure: TARA methods for ISO/SAE 21434

Consulting and TARA

Consider a classic car, perhaps the 1967 Chevy Impala. No car-enthusiast would dare to touch the mechanics of this car without first assessing the engine, what kind of parts it has, and what the status of the vehicle is.

Similarly, before one implements security, a thorough review and assessment is necessary in order to prevent damage to an existing system. In a connected vehicle, this step of the security implementation process is an engineering methodology called TARA, or Threat Analysis and Risk Assessment.

A key component of standards like ISO/SAE 21434, TARA is widely used in the industry to assess cybersecurity risks, based on an in-depth analysis of the vehicle's architecture. After a thorough assessment of the risks, security engineers can then select a list and sequence of necessary countermeasures to mitigate those risks.

Analysts look for known and unknown vulnerabilities using catalogs as well as risk factors like time, accessibility, and equipment, and come up with an estimated feasibility of risk. This gives the security team ample information in order to come up with a "Risk Treatment Decision" or a map of sorts to set up the necessary security system for the vehicle at hand.

Implementation of In-Vehicle Systems Security

As noted earlier, a vehicle's internal system is made up of 60 to 100 ECUs, all controlling different subsystems and functionalities of the SDV at hand.

The ECUs communicate with each other through the CAN bus, a commonly used network protocol. While the CAN network is designed to allow these ECUs to communicate without a uniform host server, they are not built with the intention of tracking where communicated messages come from, meaning that the in-vehicle system can be vulnerable to external threats and actors.

This is why in-vehicle systems security is essential - because otherwise we would see scenarios where the vehicle could be in jeopardy: message fabrication, random malicious CAN packets, data breach, remote jumpstarting -- these are just some of the risks that a vehicle could encounter without security.

However, especially with SDVs, security isn't as simple as an antivirus install. Solutions providers and manufacturers must work together to ensure that each layer and system of the vehicle is secured - from the external network to the internal network, a number of factors must be considered.

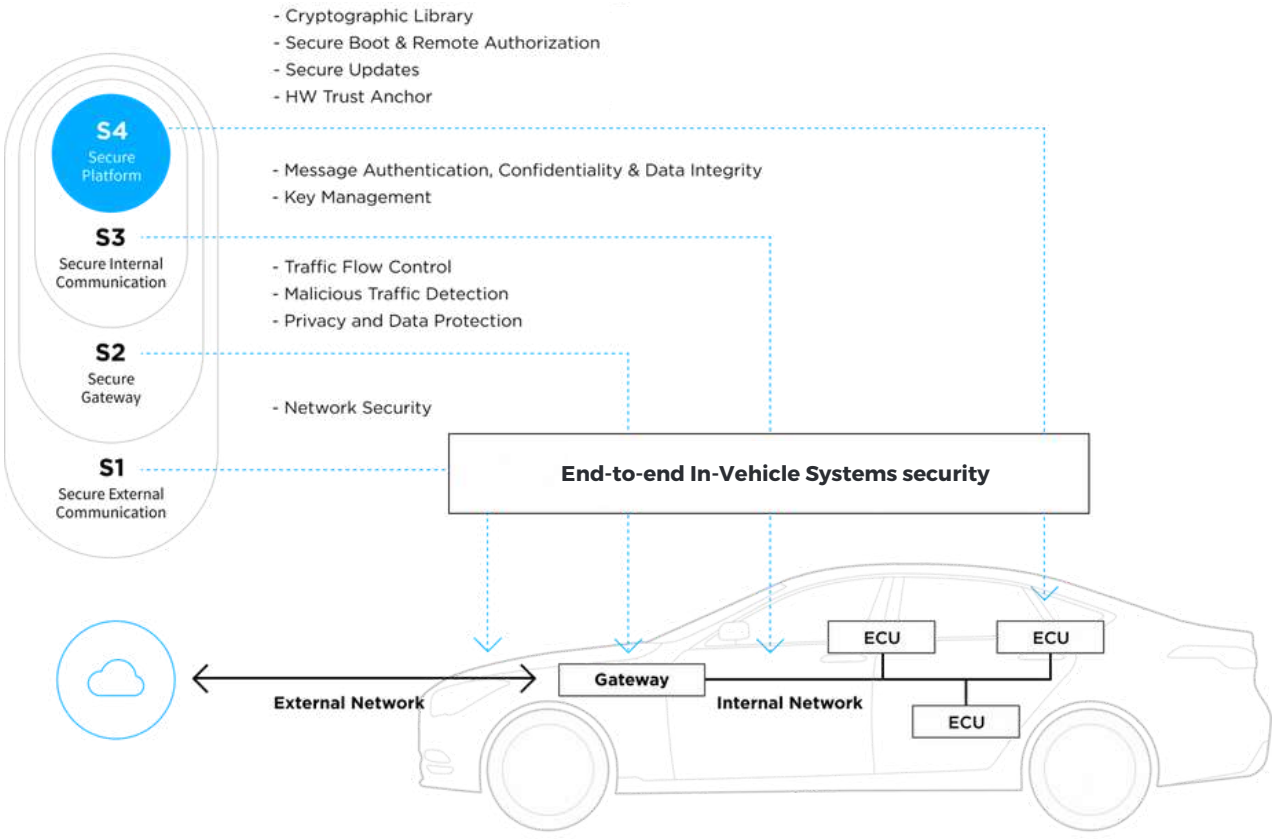


Figure: Layers of security and related offerings by Autocrypt

Verification and Validation

While implementation is a necessary and major part of cybersecurity, security is not complete until it is verified and validated multiple times over.

> Verification and validation are both vital to ensuring that the solution at hand is working properly

Verification vs. Validation

Verification involves checking to see if the software or hardware achieves what it is meant to achieve without any issues. It *verifies* whether or not the product fulfills the customer's requirements. Verification oftentimes does not execute code, and therefore is considered *static testing*.

On the other hand, validation checks for the quality of the product and whether it lives up to high-level requirements. Validation does involve code execution, and is considered *dynamic testing*.

Verification and validation are both vital to ensuring that the solution at hand is working properly.

Types of Testing

Vulnerability Scanning	• **Software static testing**: Uncover major issues in early development stages like leaks, buffer overflows, and standard deviations. Prevention of increased development timescales • **Software dynamic testing**: Executed code testing vulnerabilities in runtime environments and behavior of dynamic variables
Fuzz Testing	• Test target reaction to invalid or random data (“fuzz”), monitoring for crashes, memory leaks, and failed code. High benefit-to-cost ratio, as fuzzing utilizes undefined behavior to trigger hidden bugs that were unforeseen
Penetration Testing	• Utilize known vulnerabilities and cyberattack methods to simulate attacks on a combination of hardware, software, and services. Threat database ensures that vulnerabilities of various severity are utilized to initiate attack tests

Incident Reporting

In the midst of the processes of preventing cyberattack, there needs to be countermeasures taken when incidents do occur, to revise and patch these issues, analyze the cause of these incidents and also to continue to review security vulnerabilities and threats.

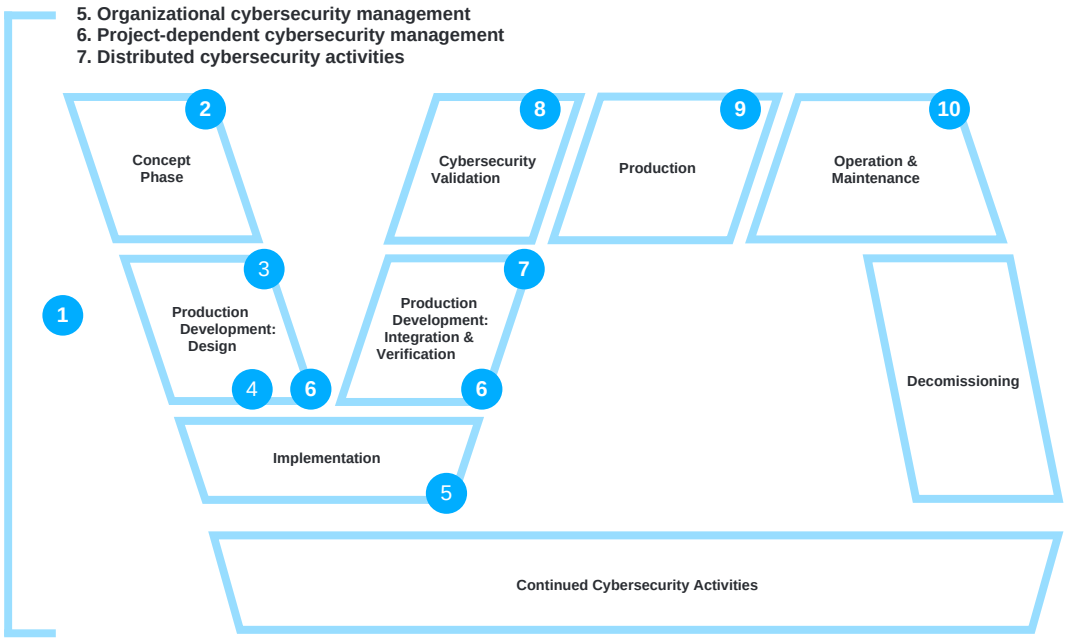
Many manufacturers choose to have a Vehicle Security Operations Center that monitors incidents around the clock. This can be an in-house or outsourced team, and often utilizes a customized platform to monitor vehicle systems 24/7.

AUTOCRYPT OFFERINGS

As mentioned before, if using multiple vendors, the process of implementing solutions for security can become highly segmented and difficult to manage. To assist manufacturers and suppliers with this issue, Autocrypt provides an alternative approach to ensuring compliance by offering customized support and implementation from the beginning to end of the V model. This allows for enhanced transparency for manufacturers and suppliers from pre-production till after market.

Autocrypt matches each step of ISO/SAE 21434 as well as WP.29 regulations to its suite of offerings and consultation services.

Autocrypt Comprehensive Management Model



Autocrypt Solutions Offerings

1. CSMS / ISO 21434 consulting
2. TARA (Threat Analysis and Risk Assessment)
3. OEM requirement analysis
4. Security design & engineering
5. Security solution implementation (porting, customizing)
6. Vulnerability analysis and management
7. Fuzzing test
8. Penetration test
9. Incident response
10. Production-line integration

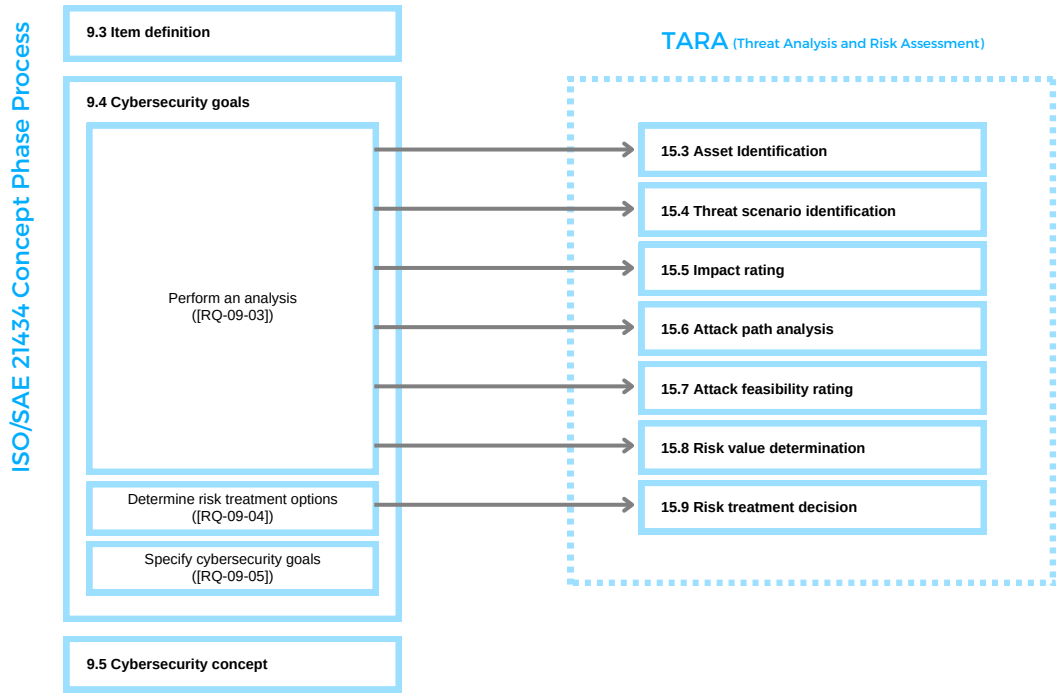
While there are many components to the process of compliance, Autocrypt works with each partner to go through each step comprehensively and customizes all solutions according to the manufacturer's specific needs. The following portion of the white paper will go through Autocrypt's offerings in more detail.

1 CSMS / ISO 21434 consulting

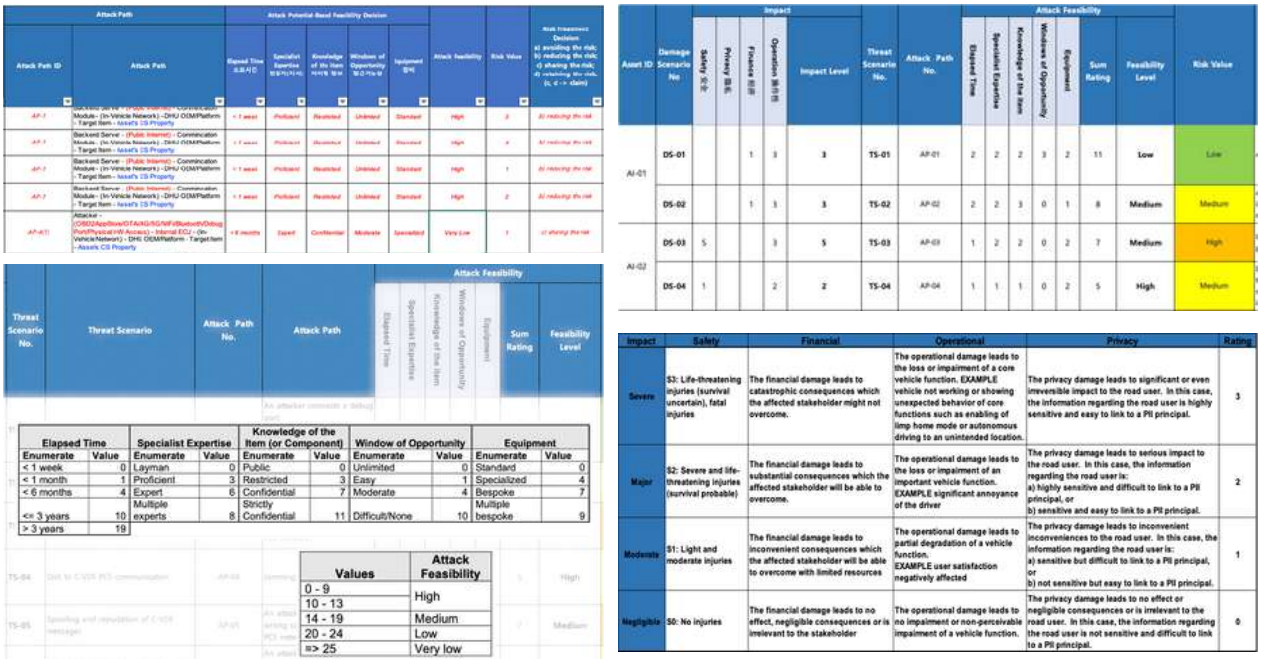
Autocrypt provides expert consulting services for establishing a Cyber Security Management System (CSMS) as well as compliance with both WP.29's R155, R156 regulations and ISO/SAE 21434 standard.

2 TARA (Threat Analysis and Risk Assessment) & 3 OEM requirement analysis

The TARA process as part of the concept phase allows for a clear direction for both the security experts and manufacturers in terms of implementing the security management systems.



Each OEM has its own architectural design and corresponding requirements. Autocrypt works with each customer to conduct a thorough analysis, then provides customized, comprehensive reports on findings.



Elapsed Time		Specialist Expertise		Knowledge of the Item (or Component)		Window of Opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
< 1 week	0	Layman	0	Public	0	Unlimited	0	Standard	0
< 1 month	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
< 6 months	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
<= 3 years	10	Strictly Multiple experts	8	Strictly Confidential	11	Difficult/None	10	Multiple bespoke	9
> 3 years	19								

Values	Attack Feasibility
0 - 9	High
10 - 13	
14 - 19	Medium
20 - 24	Low
=> 25	Very low

Impact	Safety	Financial	Operational	Privacy	Rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries	The financial damage leads to catastrophic consequences which the affected stakeholder might not overcome.	The operational damage leads to the loss or impairment of a core vehicle function. EXAMPLE vehicle not working or showing unexpected behavior of core functions such as enabling of limp home mode or autonomous driving to an unintended location.	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.	3
Major	S2: Severe and life-threatening injuries (survival probable)	The financial damage leads to substantial consequences which the affected stakeholder will be able to overcome.	The operational damage leads to the loss or impairment of an important vehicle function. EXAMPLE significant annoyance of the driver	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.	2
Moderate	S1: Light and moderate injuries	The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources	The operational damage leads to partial degradation of a vehicle function. EXAMPLE user satisfaction negatively affected	The privacy damage leads to inconvenient inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.	1
Negligible	S0: No injuries	The financial damage leads to no effect, negligible consequences or is irrelevant to the stakeholder	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.	The privacy damage leads to no effect or negligible consequences or is irrelevant to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.	0

Figures: Post-TARA analyses reports (sample only)

4 Security design & engineering

After the consultation and assessment stage comes the major part of the process, where the procedure for designing the system, implementation, and verification comes into play.

Autocrypt has developed a suite of offerings for the implementation of a comprehensive cybersecurity system, including (but not limited to) secure boot, access control, file system encryption, as well as host IDPS and firewall and CAN-IDS/Ethernet-IDS.

However, as stated before, customization is key. Autocrypt works with each partner and client in order to design the proper combination of offerings to meet specific needs.

	Category	OEM requirements	HSM	TrustZone API	ASK API	Firewall	SMACK	dm-crypt	App Security	OS hardening	Pen/Fuzz Test	Static/ dynamic test
1	MCU	Secure Flash	✓		✓						✓	
2		ASK			✓							
3		HSM	✓									
4		HW	✓	✓								
5		SW		✓								✓
6		Secure Flash		✓								
7		HSM(TrustZone)	✓	✓								
8		OS								✓		
9	CPU (AP)	Secure Algorithm	✓	✓								
10		Firewall				✓	✓					
12		Communications				✓						
13		Personal Data Protection	✓	✓				✓				
14		File System Encryption		✓				✓				
16		OS security								✓		
17		Mobile app security							✓			
18		SMACK					✓					
19		TARA										
20	Non Functional	Security evaluation										✓
21		Pen testing									✓	
22		OSS vulnerability analysis										✓
23		Fuzz testing									✓	

Figure: Security design & engineering items (sample only)

5 Security solution implementation

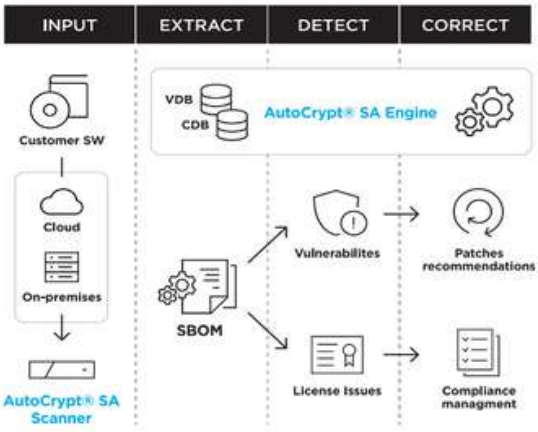
AutoCrypt IVS provides reinforced security and monitoring for ECUs, and detects abnormal behaviors and attack attempts across both internal and external communications.

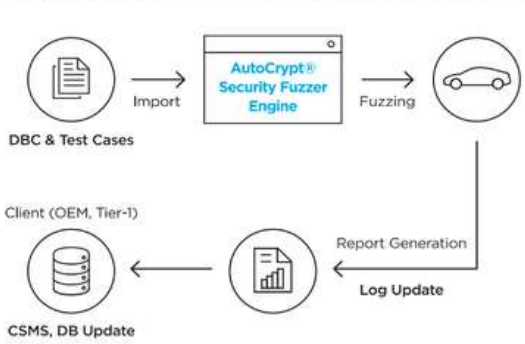
Autocrypt works with partners to implement the right combination of solutions to cover the in-vehicle system.

	Autocrypt Solutions	AP	MCU+HSM	MCU	GW/CCU
1	Secure Boot	O	O	O	O
2	Secure Flashing (OTA Client)	O	O	O	O
3	HW-based Crypto Lib.	O	O	-	O
4	SW-based Crypto Lib.	-	O	O	-
5	Access Control	O	-	-	-
6	File System Encryption	O	-	-	-
7	Host IDPS & Firewall	O	-	-	O
8	CAN-IDS / Ethernet-IDS	-	-	-	O
9	Etc. (customizing tool)	O	O	O	O

6 Vulnerability analysis and management

In order to thoroughly scan for vulnerabilities, Autocrypt developed AutoCrypt Security Analyzer, which detects and manages vulnerabilities in vehicular open-source software (OSS). The program accurately identifies, categorizes, and lists its components in a software bill of materials (SBOM), implementable at all stages of the software development life cycle (SDLC).





7 Fuzzing

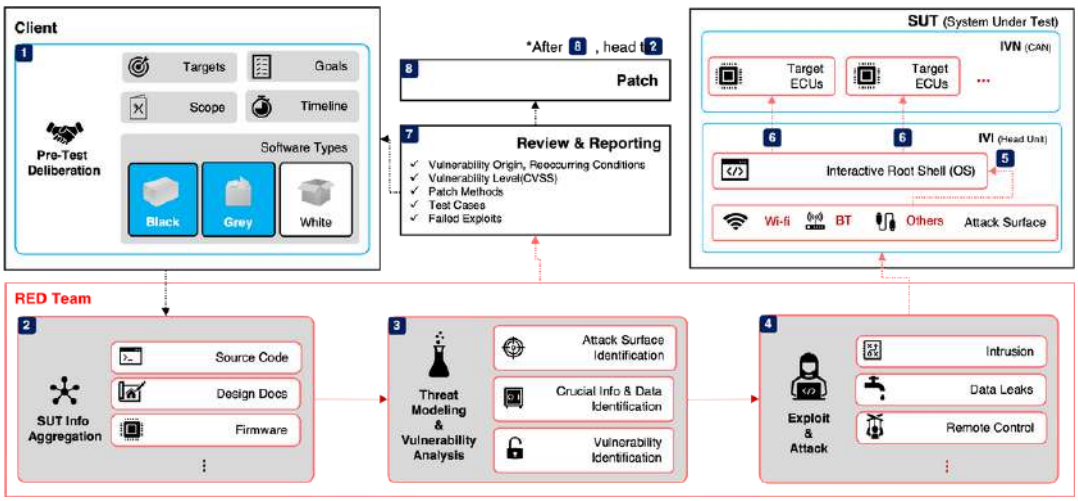
Fuzz testing is an automated software testing technique that finds hidden coding errors by injecting random/semi-random data inputs into a targeted program. AutoCrypt Security Fuzzer makes this process quick and efficient, consuming minimal time for maximum results.

8 Penetration test

Autocrypt's penetration testing or "pentesting" is supported by its award-winning in-house Red Team. The team is comprised of trained, expert ethical hackers, who design attack scenarios and initiate them to discover weaknesses and vulnerabilities with the system.

Figure (right): Autocrypt Red Team comes in first place in 2021 Cyber Security Challenge, hosted by the Ministry of ICT, Seoul, Korea.

(below): Autocrypt Red Team cycle process for pen-testing with client.



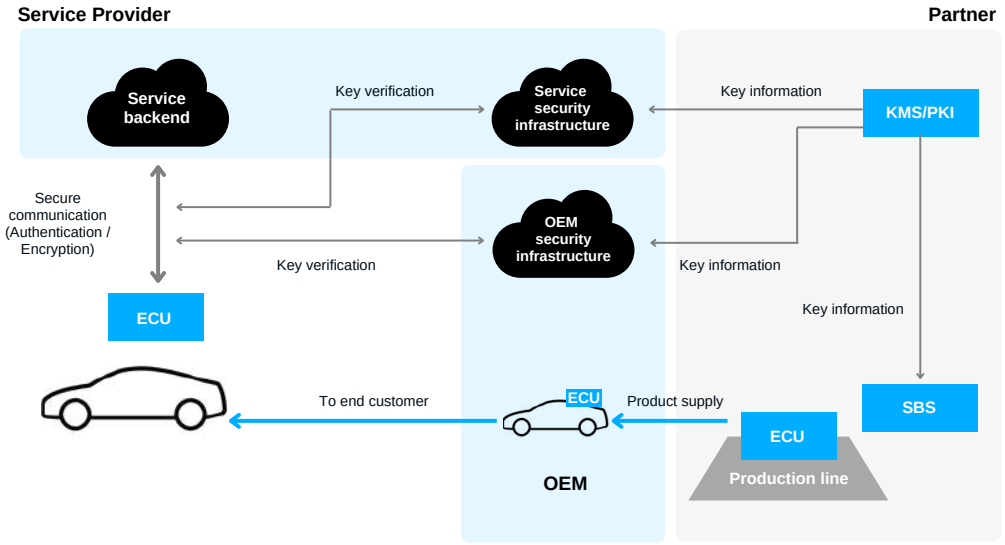
9 Incident response

AutoCrypt vSOC is offered in conjunction with other in-vehicle systems security solutions in order to manage the vehicles post-production. The platform hosts an intuitive and easy-to-navigate user interface, and manufacturers can gain insight into threat intelligence in real-time.

Figure: vSOC user interface (sample)

10 Production-line integration

For the production line, Autocrypt provides server solutions, including a key management system and Public Key Infrastructure (PKI), as well as Secure Bootstrapping (SBS).



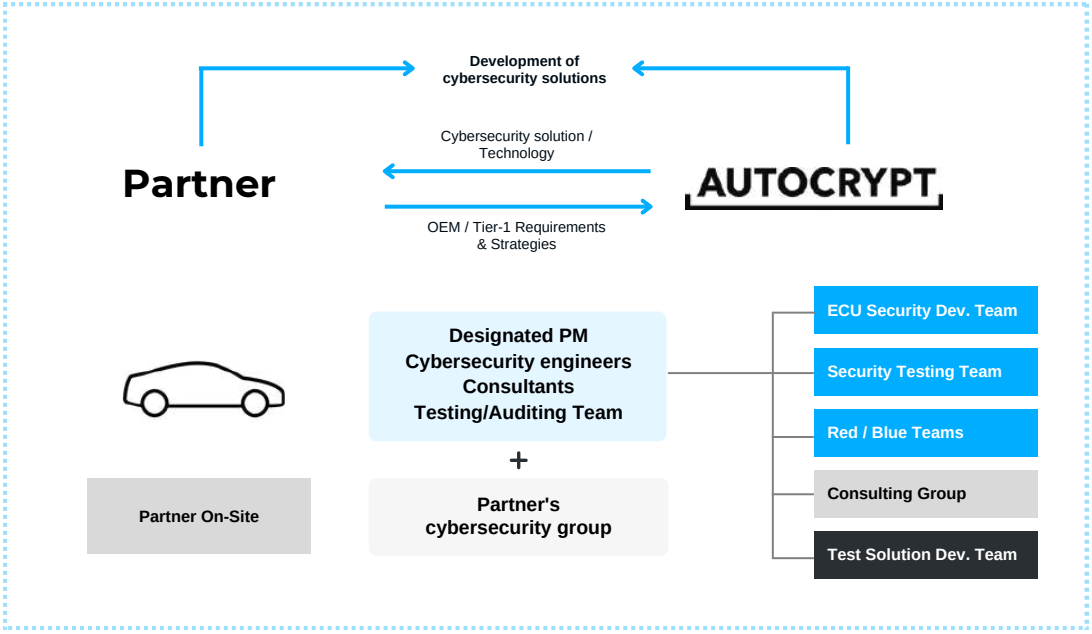
CONSIDERATIONS FOR IMPLEMENTATION

The changing tides of the automotive industry into more software, and less hardware, indicate that vehicles will be a greater target for attacks and data breach.

Moreover, due to the nature of the variety of software involved, as well as the various software providers involved in each vehicle model, there will be a greater complexity when it comes to securing a vehicle.

This is why holistic, comprehensive cybersecurity is essential in securing the next wave of SDVs. Different solutions and approaches will need to cooperate in order to ensure vehicles are safe before hitting the road. However, contrary to opinion, holistic and comprehensive does not have to be difficult.

Autocrypt believes in cooperative cybersecurity where organizational models of teamwork, technology, and testing are utilized to provide the utmost secure experience.



Autocrypt's decades-long experience in cybersecurity technology for the connected world is an asset for manufacturers and suppliers who understand that the industry is changing and it will continue to change as vehicle technology evolves. We believe that security is never a one-size-fits-all model, and pride ourselves in customizing for each partner and their architectural and structural needs.

For more information about Autocrypt's comprehensive cybersecurity offerings for SDVs, CAVs, and EVs, visit www.autocrypt.io or contact global@autocrypt.io