CONTINUOUS SECURITY ASSESSMENT IN AUTOMOTIVE

White paper

Rel 2.0 October 2023

Index

Abstract

Cybersecurity assessment is becoming a paramount problem in the automotive market and, in general, in all the different Internet of Things (IoT) verticals. New National and Regional Regulations are requesting Manufacturers (OEMs) and Suppliers (TIER1s) of IoT solutions to consider cybersecurity resilience as a requirement of all new products, to certify the application of best practices, and to set up a process to continuously monitor for new vulnerabilities and threats.

This scenario is generating a strong need to improve the processes and methods used to validate cybersecurity requirements and test the cybersecurity posture of automotive products. **Risks are continuously changing**. New vulnerabilities can be found in different stages of a product lifecycle; they are challenging to discover and fix. New threats are constantly emerging. Hence, continuous monitoring is crucial.

Unlike many other subjects, cybersecurity is not a measurable performance. For its intrinsic nature, cybersecurity is a process for managing and mitigating risks to acceptable levels. Hence, it is a moving target.

Drivesec is proposing a novel approach that increases the reliability, speed, replicability, and accuracy of cybersecurity tests. It extends the coverage of the tested perimeter, supports testing automation, and guarantees the proper storage of acquired knowledge and lessons learnt from one vehicle model to another.

Drivesec has designed **WESETH®**, a platform for cybersecurity testing automation that supports the automotive industry to improve its capacity to continuously validate and assess the security posture of new and existing vehicle models and components.

Assessing Cybersecurity posture

Cybersecurity posture verifications are mandatory to pursue legislation and product integrity.

Verifications and penetration tests are critical for this verification, but they are affected by several important factors:

- Tight time to market;
- Increasing cost and scarcity of parts;
- Continuous update of vehicle's software and features;
- Increasing risks **due to increasing complexity of the attack's scenario.**

OEMs and TIER1s are setting up processes and improving vehicle design to comply with regulations.

Vehicle-level penetration tests at the end of the design phase are the choice of preference for most OEMs to certify and assess the cybersecurity posture.

Penetration tests as they are executed today on stationary vehicles in the labs or on roller bench are not enough to guarantee a full coverage of the operational scenarios. Testing must become a continuous and fast process integrated with a continuous monitoring effort.

Penetration Test (PT) on vehicles is not the most efficient way to validate security.
PTs are often costly activities, whose final value is directly influenced by the subjects who will run them and the time we pay for their services.

The whole PT process is in most cases not replicable because of missing information, hence, it does not ensure a broad coverage
on vehicle SW and features, and it does not consider lessons learnt from the previous vehicle models.

The needs

Lack of skills and trained resources

Shorter Time to market

Automotive and IoT components require a brand-new approach to cybersecurity testing, making it **Transparent, Autonomous, Continuous and Proactive**, providing OEMs and TIER1s with cost-efficient tools **to outperform attackers** in the search for threats and vulnerabilities in assessing the cybersecurity risks.

Increasing homologation requirements

- Must Increase tests' reliability, reduce logistics and costs and enhance efficiency while assuring coverage of homologation requirements
- Can be integrated with proto vehicles, integration benches, and HIL systems. Testing on HIL is preferable to extend e coverage of the security assessment
- Can support continuous testing processes while bringing full test automation
- Shall Reduce the need for human interaction and support lessons learnt
- Should be proactive in the search for vulnerability and implement a continuous improvement process

Shorter development cycle

Complex logistic of parts

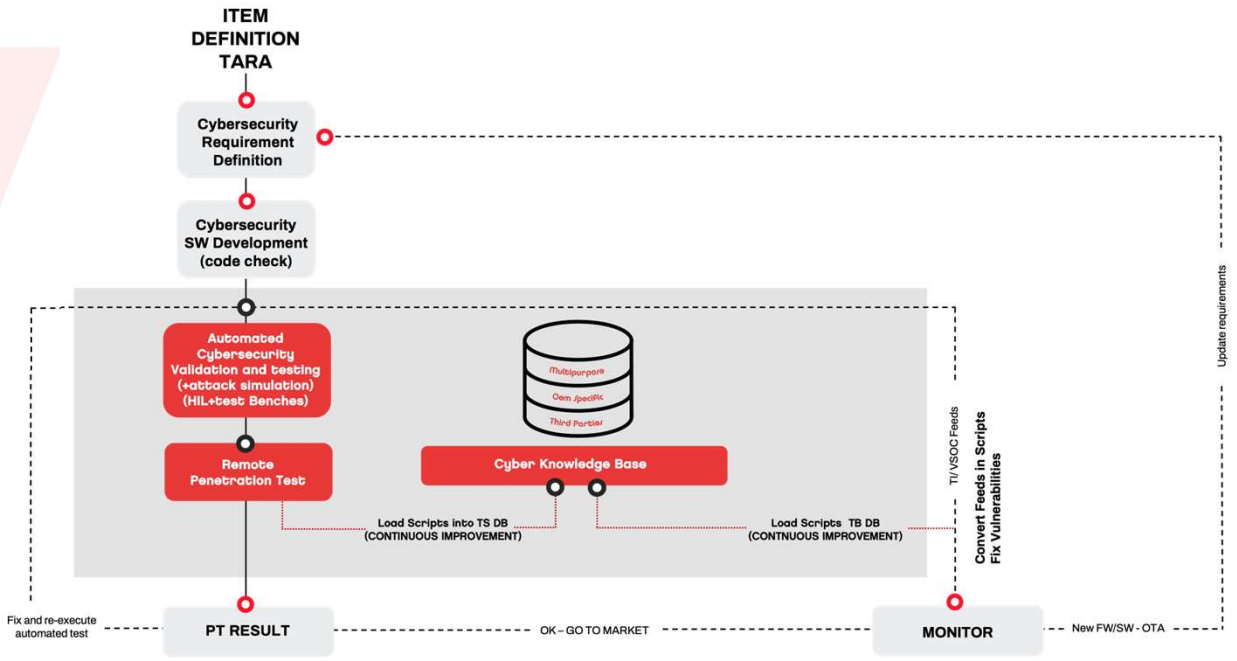
Continuous SW update

Security
Assessment in the loop

Assessing cybersecurity posture is a continuous process that must not end with the start of production.

Every software-defined system is subject to upgrades and updates in its lifecycle, and new vulnerabilities can be found anytime. Moreover, it is also important that organizations, like OEMs and Tier1s, grow in experience and knowledge as they continue to design new systems and new features.

For these reasons, it is important to define a model where the product is at the center of the story. The following picture shows how this continuous assessment model could be designed. The proposed model is aligned with the UNECE Regulation 155.



Following UNECE R 155, everything starts with a TARA (Threat Analyses and Risk Assessment), originating from the so-called “Item definition”. This analysis defines the goals and consequently the security requirements of the product (e.g. vehicle). When the code is complete and checked (formal checking), the validation phase starts**.** **Drivesec’s** cybersecurity assessment model starts with an automatic vulnerability assessment using the WESETH platform, WESETH is associated with a set of scripts (Knowledge Base) that include code that tests cybersecurity requirements, simulates attacks, and fuzz software and networks either on single components or on complex systems. A comprehensive Knowledge Base and advanced reasoning features allow a very extensive Vulnerability and Weaknesses assessment.

The Knowledge Base is the enabling element of the entire model. It is a “living thing” that preserve all the experience, acquired by OEMs and Tier1s, formally modelled and well organized.

Scripts are added to the Knowledge Base when new requirements are defined, new vulnerabilities are identified, or new issues are found in the field. Growing the KB allows the system owner to enter a continuous improvement process keeping track of the lessons learnt.

After the extended automated validation, a key part of the story is a human-executed penetration testing.

Penetration tests will go beyond what can be tested automatically and bring human experience into the test cycle. Also, what is produced during penetration tests, as scripts, should enter the Knowledge Base and increase the capacity to discover vulnerabilities in an early stage of product development.

Once the product is in the field, monitoring through VSOC (Vehicle Secure Operation Center) and TI (Threat Intelligence) must be in place to gather indications from the running fleet.

As with penetration tests, when an alert is generated by the VSOC or a feed is received from TI, these should be converted into test scripts to be added to the KB.

The Drivesec model is intended to be applied to any software changes, and the definition of a strong Knowledge Base will help OEMs and TIERS1s to build a robust continuous improvement process that keeps track of the issues found on products and their updates.

Testing
Automation platform

Weseth® by drivesec

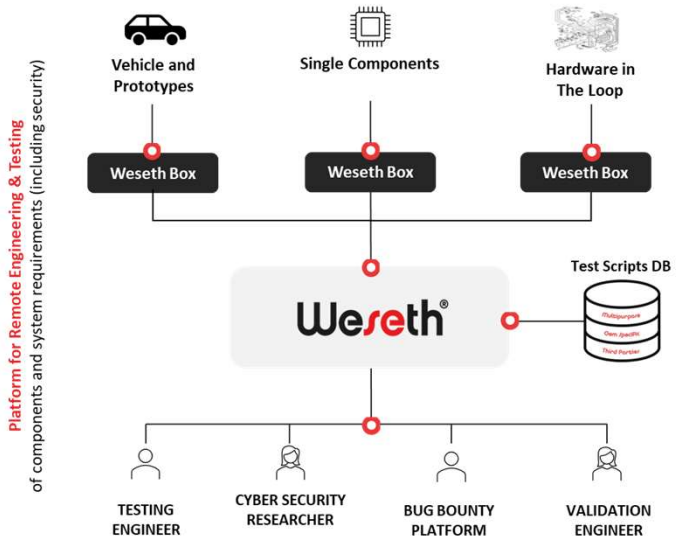
WESETH is a testing automation platform, expressly designed for **cybersecurity verification of cyber physical systems.**

WESETH is a **security platform** designed to **support the remote and automated validation of cybersecurity requirements and contro**l on **Benches, HIL or Proto Vehicles**.

WESETH implements a wide variety of **use cases** including:

- Automated verification of cyber and functional requirements;
- Remote security Assessment through Penetration Test;
- Cooperative vulnerabilities fixing;
- Simulation of attacks.

WESETH's **high-security standards** allow **fully autonomous requirements verification** as well as the integration of **human experts in the loop for penetration testing.**



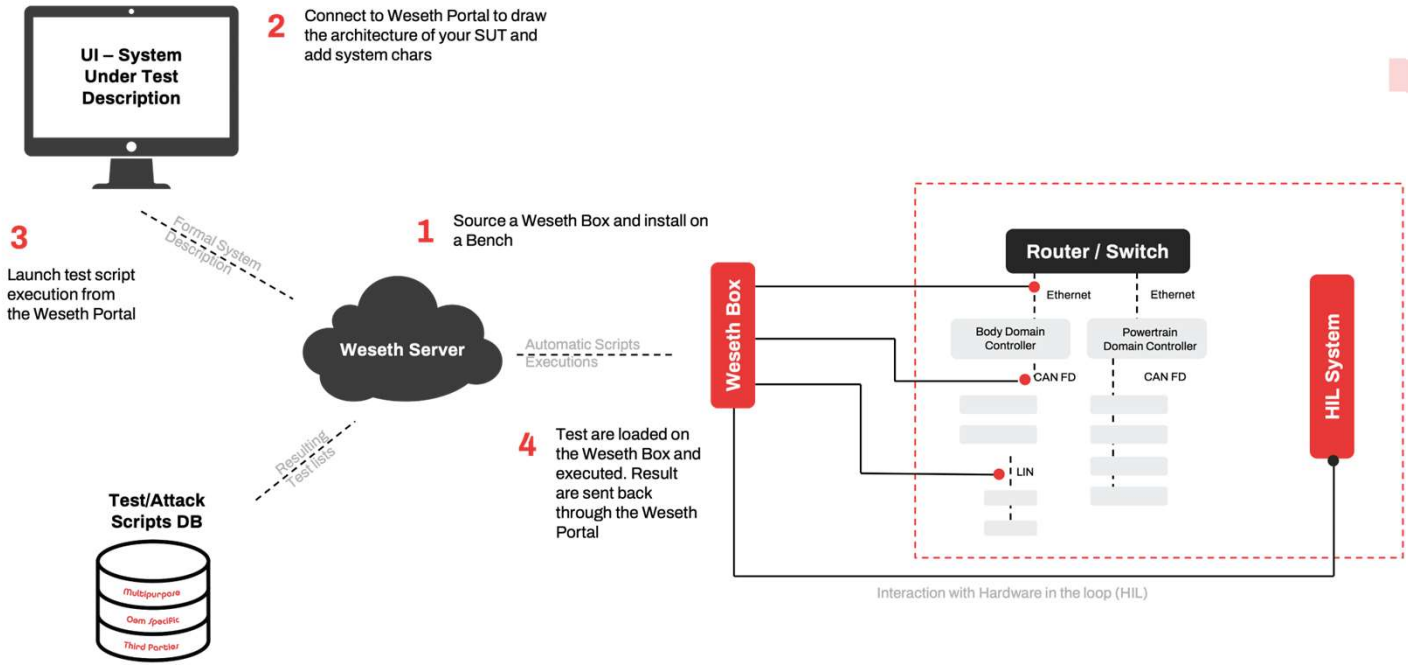
- **Customer hardware remains with customer**
  ECU, vehicle, sub-system, Hardware in the Loop systems ...
- **Customer attaches Weseth remote box to target hardware which shall be tested / validated**
  Physical connection via CAN/CANFD/ETHERNET, Bluetooth, USB, streaming of video, multiple Digital IOS.
- **Cloud Based server manages the secure integration between System Under Tests and remote Users**
  Test scripts are stored in a safe environment and are automatically loaded on the Boxes when needed
- **Test Engineers describe the system under test;** based on this, Scripts are automatically selected and loaded on the respective Box for automatic execution
- **Remote Users can access the system under test** to perform penetration tests, emulate attacks, verify requirements and collect data

Weseth is integrated with a database of scripts that are designed either to simulate attacks, check for vulnerabilities, fuzzing on different interfaces, and test common cybersecurity requirements.

Once the WESETH BOX is physically connected, the owner of the System Under Test (SUT) can instruct the WESETH Server to load a selection of scripts on the WESETH BOX and execute them.

The WESETH Server will manage the interaction with the WESETH BOX, making them transparent to the users.

Once executed, the WESETH BOX will send back the results of the tests to the owner of the SUT.

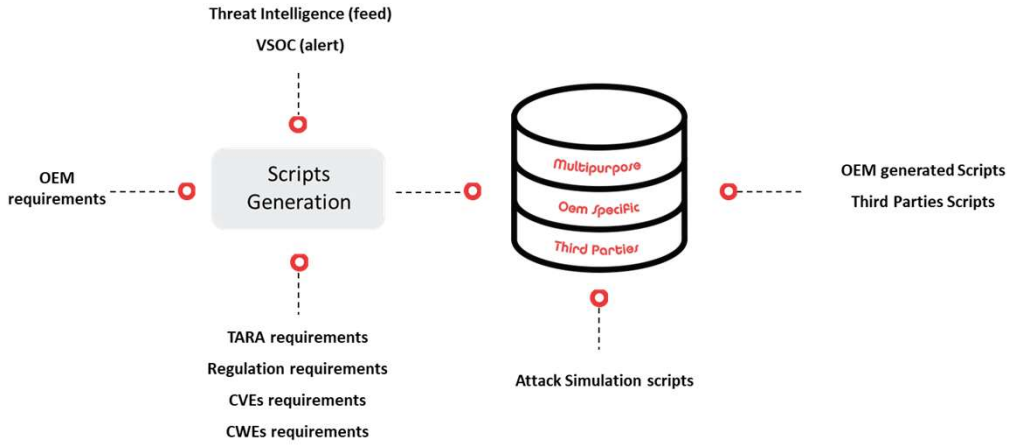


The BOX, once activated, connects to the SERVER via a mobile link (4G) on a Drivesec proprietary APN. The BOX does not use existing Customer's ICT infrastructure for multiple reasons:

- Allow isolation of system to be accessed by remote cybersecurity engineer
- Allow Drivesec to manage proper end-to-end platform security and integrity
- Allow testing in mobility (vehicle or prototype-based testing).

WESETH relies on DRIVESEC's design test scripts database, which covers multiple attack scenarios and various requirements validation tools.

Execution of those test scripts is made automatic by the support of the Weseth platform execution mechanism.



Drivesec has designed an initial set of scripts, which can be executed automatically on the WESETH BOX, to cover all the requirements indicated in Annex 5 of the UNECE R 155.

This initial set of scripts covers attack simulation, systems and network fuzzing and requirements testing. The scripts database is a living object, and the number of scripts increases continuously based on the number of inputs.

New scripts can be generated analyzing CVE, CWE, new regulations and TARA's results from different projects. But new scripts can be generated from the analyses of feeds coming from VSOC and Threat intelligence.

These last two are particularly important because can help to keep track of lessons learnt and record what has been done by attackers to intrude into systems with the aim to reuse this knowledge in the next projects.

Scripts generated during VA/PT activities could also be included in the database to enlarge the perimeter of the automated testing.

ZERO setup time

Weseth is simple and can be installed by no-IT staff in a matter of 1 hour, without impacting on IT infrastructure.

Flexibility

Weseth can be used to connect every type of systems with any type of interface, can be programmed and ca support remote controls (through Digital I/O management)

Security

Weseth is fully managed and monitored to guarantee security, integrity and prevent tampering

Capabilities

the features and the number of potential use cases supported by Weseth are such that a comparison with a other solution is too reductive

The Authors

Giuseppe Faranda Cordella
Founder & CEO

Earned his master's degree in Computer Science at Turin University and is a senior executive with over 25 years' experience in the design and development of automotive electronics, connected car services, and vehicle cybersecurity. Throughout his career he has worked in different roles at leading automotive companies either as an OEM or as a Tier1 supplier. In recent years he has served as VP and Head of Research and Development of infotainment for a large European OEM. He was also appointed Head of Vehicle Cybersecurity for leading OEM in EMEA, managing the introduction of digital protection countermeasures in connected cars.

Luca Ferrua
CTO

Got his master's degree in telematics and telecommunication engineering at Politecnico of Turin. He is a Senior Manager with more than 15 years of automotive experience in design and development of automotive electronics, telematics and exterior lighting components. In his carrier he has worked for different Tier1 suppliers covering different roles from technical development leading to program management in international environment. As supplier, he had the opportunity to cooperate with several OEMs becoming familiar with different Research & Development organizations, procedures and mindset consolidating his automotive culture.

About Drivesec

Drivesec is an innovative cybersecurity company founded in 2017 with the aim of developing security solutions for the Automotive and IoT market.

Drivesec provides, as a player in the cybersecurity market, consulting services to design and validate the cybersecurity posture of cyber-physical systems.
We focus on developing methodologies and products for testing and validating the security requirements for connected systems.

Drivesec helps Customers to reach certification for UNECE Regulation 155. In these years Drivesec has supported OEMs and Tier1s either to develop a Cyber Security Management System (CSMS) or to design and validate secure Products.

Drivesec has designed a platform (WESETH®) for cybersecurity testing automation that supports the automotive industry to improve its capacity to validate and assess the security posture of new and existing vehicle models.

drivesec

www.drivesec.com
marketing@drivesec.com