drivesec

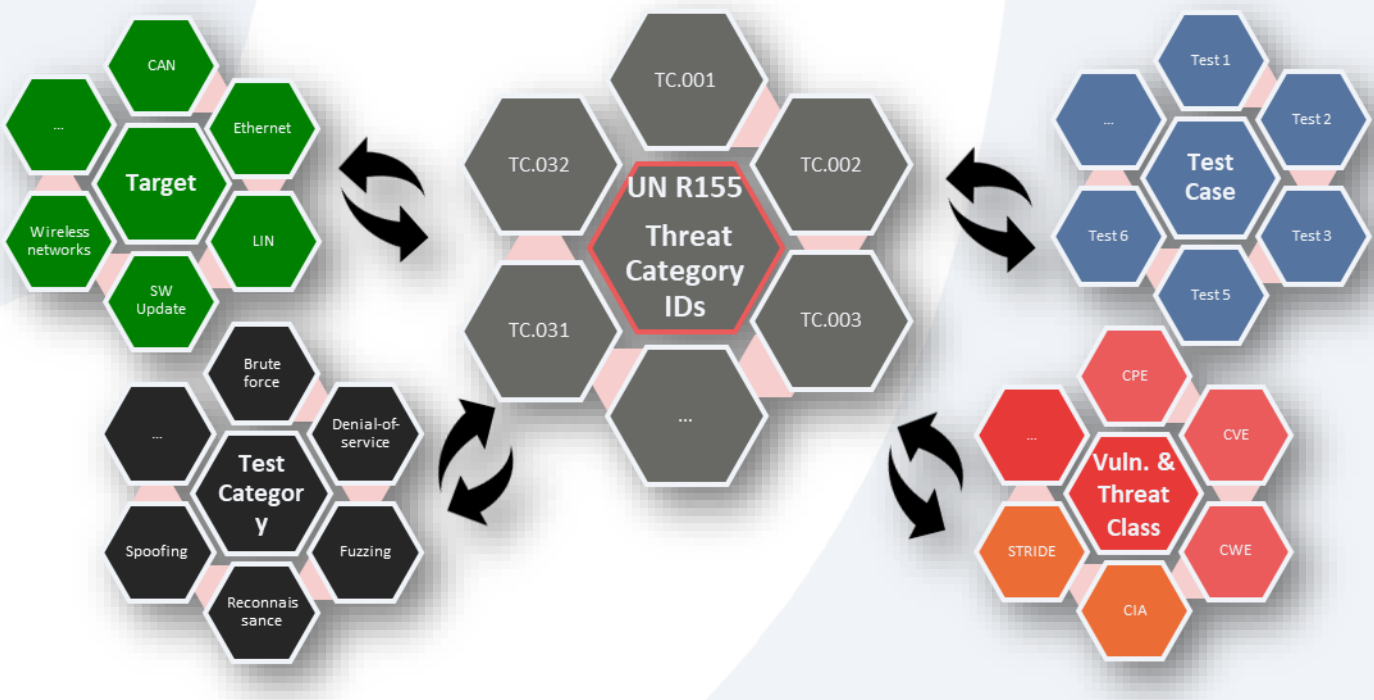
THE TEST GUIDELINES FOR UNECE R155

1. The Test List

Based on UN R155, **Drivesec** has defined a list of cybersecurity test cases that vehicle manufacturers and component suppliers can perform to demonstrate their compliance with the Regulation.

The test list developed by **Drivesec** is mainly derived from Annex 5 of the UN 155 Regulation. The list includes all the threats/vulnerabilities contained in Annex 5 and allows customers to ensure and demonstrate that all the cybersecurity mitigations are successfully implemented, as requested by the Regulation.

Annex 5 takes into consideration different categories of threats/vulnerabilities according to their scope. The list of tests fits with real use cases, thanks to the application of threat categories defined by Annex 5 on the more common attack vectors, seen in modern vehicles.

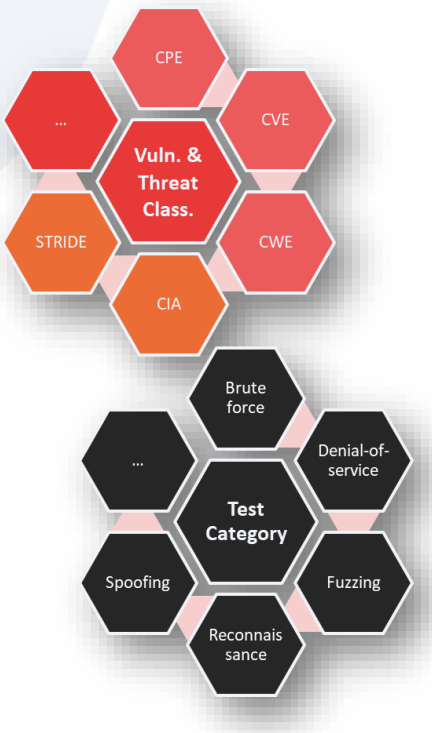


2.The Test List's structure

The current trends in the Automotive Industry (e.g., Connectivity and Infotainment, Electrification, Autonomous Driving) transformed vehicles into such complex systems, exposing them to a large number of threats due to an increasing attack surface.

The test list designed by **Drivesec** aims to cover the more common targets for vehicles, from the in-vehicle networks, such as:

- CAN Bus,
- Automotive Ethernet or LIN,
- Wireless networks,
- ECU SW services.



To improve and enrich the test list, additional inputs rather than Annex 5 are considered, such as:

- Real cyber attacks against vehicles and ECUs,
- Vulnerabilities publicly disclosed.

Each Test Case is evaluated according to the STRIDE and CIA threat models and assigned to a specific test category.

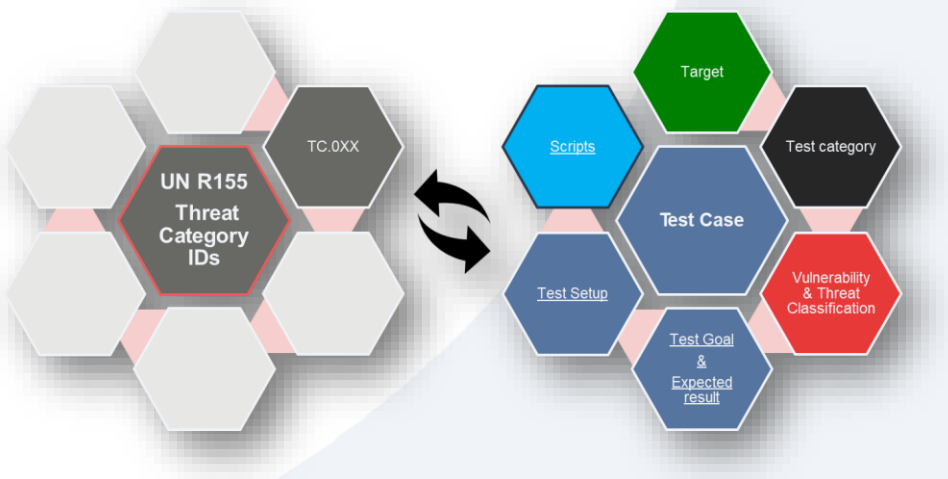
2.1 The Test List overview

Test cases include some prominent information:

- **Summary**: a high-level description of the test,
- **Test goal and Expected result**: what are you going to verify, and what is the expected result, in case of successful execution,
- **Target(s)**: the attack vector, i.e., the physical or logical interface on which the test must be run. E.g., in-vehicle networks, like the CAN Bus,
- **Test setup**: the high-level steps that must be performed to set up the test case,
- **Vulnerabilities and Threat Classification**: classification of the test case based on the “STRIDE” and “CIA” methodology,
- **Test category**: e.g., reconnaissance, fuzz testing, ...
- **Script:** script with an implementation of a specific test case.

Each test case in the list is mapped on one or more threats listed within Annex 5 of the UN 155 Regulation.

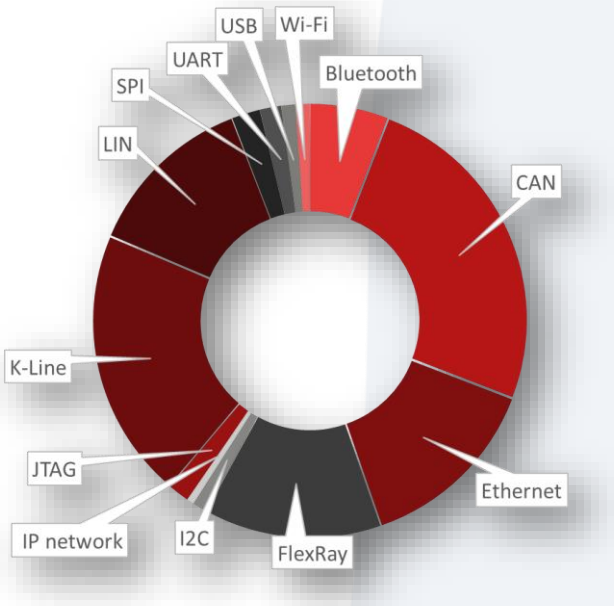
The output of a test script may include one or more vulnerabilities discovered during the execution of the test (if any), as well as warnings indicating suspicious behaviour identified during testing.



The following figure is a high-level overview of the test cases **Drivesec** has developed. The test cases cover different interfaces, considering both logical and physical interfaces, to target the most common attack vectors. Several scripts are developed to cover different variants for each test case.

Support for:

73	Test Case
13	Different Interfaces
188	Scripts



2.2 Reporting and more

The output of the test can be used to:

- Collect information to demonstrate that risks are identified and managed,
- Document Risk Assessment reports,
- Submit to Approval Authority all evidence for achieving Certification,
- Detect appropriate Cybersecurity measures,
- Detect and respond in advance to possible cybersecurity attacks,
- Write and share lessons learnt and improve organization processes.

3. The extract of our test list

Drivesec provides the complete test list, which you can read a little example in the following figure.

Interface	Type of attack	UN R155 (sub-level descriptions of vulnerability/ threat)	Test case summary	Test case Objectives	Expected Result (Test successful)	STRIDE	CIA
CAN	ECU Security Access seed randomness	Cryptographic technologies can be compromised or are insufficiently applied	Verify if the ECU makes use of an acceptable level of randomness to generate seeds for Security Access.	Verify if target ECU makes use of strong randomness for seeds generation to mitigate brute force attacks against diagnostic access authentication.	Target ECU generates non-static and unpredictable seeds.	Escalation of Privilege	Integrity
CAN	In-vehicle fuzz testing	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	Inject malformed, semi-malformed and invalid messages on in-vehicle communication network to identify software bugs, unintended behaviours or potential memory corruptions on connected ECUs.	Verify if unexpected behaviors occur on target ECUs when malformed and/or invalid messages are injected on in-vehicle communication network.	Target ECU remains available and continues working as intended during the test.	Spoofing DoS	Integrity Availability
Ethernet	In-vehicle fuzz testing	Disruption of systems or operations	Inject malformed, semi-malformed and invalid messages on in-vehicle communication network to identify software bugs, unintended behaviours or potential memory corruptions on connected ECUs.	Verify if unexpected behaviors occur on target ECUs when malformed and/or invalid messages are injected on in-vehicle communication network.	Target ECU remains available and continues working as intended during the test.	Spoofing DoS	Integrity Availability

If you are interested in our complete test list, you can request our Weseth® Platform, which is integrated with the database of scripts that are designed either to simulate attacks, check for vulnerabilities, fuzzing on different interfaces, and test common cybersecurity requirements.

Contact Us

marketing@drivesec.com