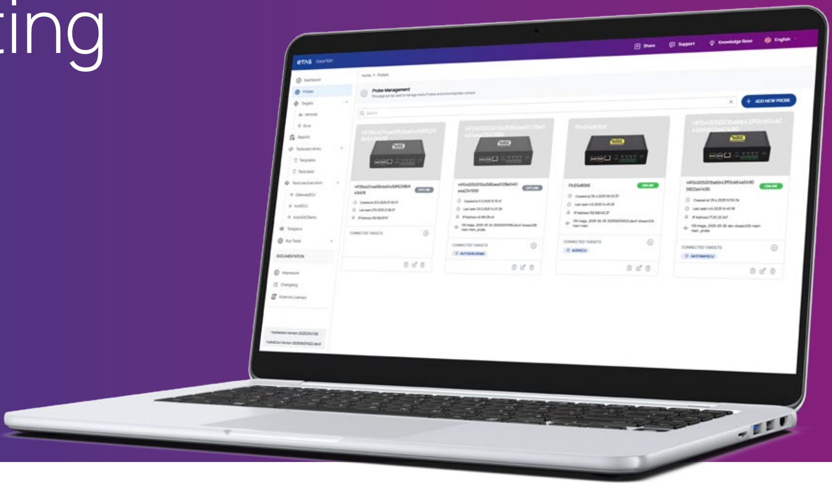
Empowering Tomorrow's Automotive Software
www.etas.com

Simplifying and automating penetration testing ESCRYPT CycurTEST



Automating compliance-ready cybersecurity testing for automotive components

Attacks on vehicle systems systematically target identified vulnerabilities and potential security gaps. Especially modern vehicles are becoming increasingly complex and interconnected, offering a multitude of attack points, and consequently, the security risk is rising dramatically. **ESCRYPT CycurTEST** starts right here and addresses the challenges of manual, resource-intensive testing by providing a comprehensive platform with pre-defined test cases and plans.

Areas of application

- **Cybersecurity testing platform:** Automating cybersecurity tests with a focus on component penetration testing for automotive
- **Compliance checks:** Fulfill required cybersecurity regulations for the most relevant automotive markets – preparation of vehicle type approval
- **Increase product security:** By using comprehensive pre-defined test scenarios for automotive use cases
- **Various testing capabilities:** An extensive range of testing requirements can be accommodated, encompassing compliance checks, penetration tests, functional cybersecurity testing, and integration with existing ETAS testing tools

Features

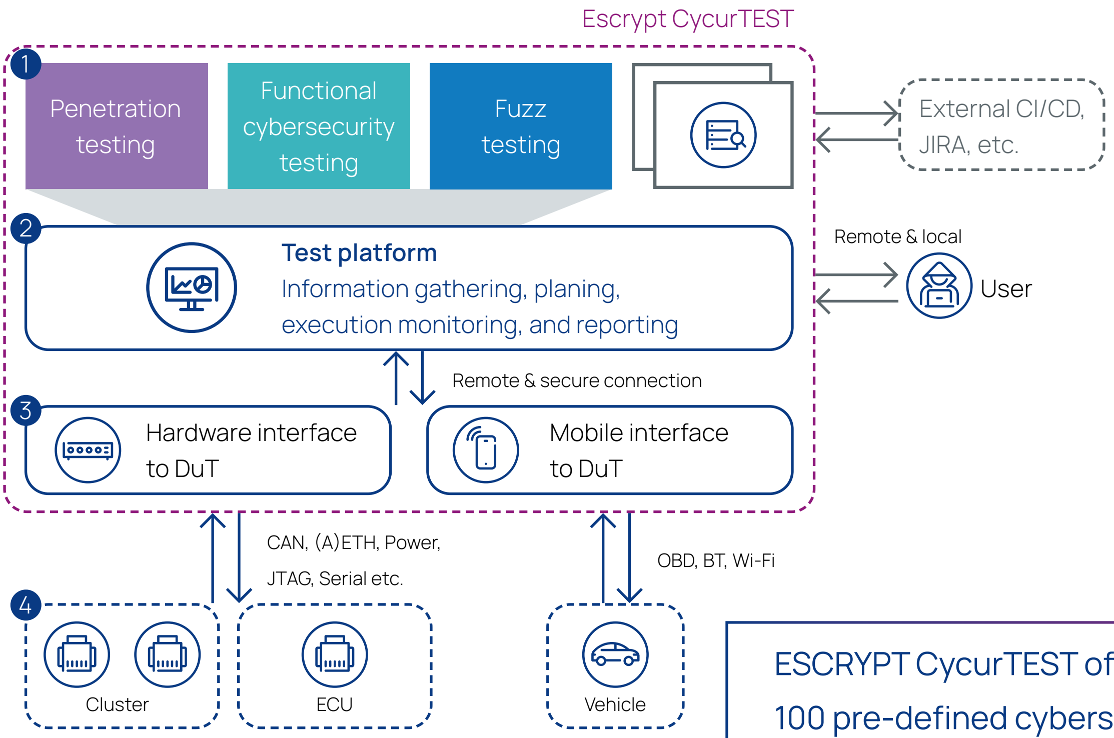
- **On-premise deployment:** Flexible on-premise deployment at the customer's location
- **Browser-based interface:** Users interact with the platform through an intuitive, browser independent ETAS GUI
- **Dedicated hardware interface:** A hardware interface connects devices under test to the penetration testing platform and offers in addition open interfaces to connect devices under test in alternative ways
- **Comprehensive test suite:** Includes approximately 100 continuously updated and expanding cybersecurity test cases such as UDS scanning, sniffing and secure debug interface testing

Benefits

- **Leverage pre-defined test cases:** Utilize comprehensive automotive penetration test cases and plans within ESCRYPT CycurTEST, eliminating the need for creating them from scratch
- **Compliance-ready testing:** Perform cybersecurity tests and compliance checks against global regulations e.g. UN R 155, Chinese GB and Indian AIS-189 standards using pre-built resources
- **Reduced testing costs:** Minimize expenses and resource needs by leveraging the provided testing platform
- **Extensible and integrable:** Easy integration of additional test scenarios such as functional testing and fuzzing

Architecture of the end-to-end cybersecurity testing process

1. Test scenarios are implemented using pre-defined, customizable, extensible, and version-controlled test cases (written in Python).
2. The user orchestrates the information gathering from the device under test (DuT) and composes test executions within a web-based UI. The built-in reporting engine automates and simplifies test documentation.
3. Devices are monitored, and test cases are executed locally via (hardware) interfaces over physical, serial, or automotive protocol links.
4. Different contexts enable various test scenarios, ranging from single component testing to full vehicle testing.


Escrypt CycurTEST
1
Penetration testing
Functional cybersecurity testing
Fuzz testing
External CI/CD, JIRA, etc.
2
Test platform
Information gathering, planing, execution monitoring, and reporting
Remote & local
User
Remote & secure connection
3
Hardware interface to DuT
Mobile interface to DuT
CAN, (A)ETH, Power, JTAG, Serial etc.
OBD, BT, Wi-Fi
4
Cluster
ECU
Vehicle

ESCRYPT CycurTEST supports the following test target types and distinguishes between different execution contexts

ECU context
Testing of individual ECU components

Vehicle context
The full vehicle is considered one test object, whereby single components (ECUs) can be detected and tested

Cluster context
Several ECUs can be combined into one testable cluster

ESCRYPT CycurTEST offers more than 100 pre-defined cybersecurity test cases written in Python for:

- ISOTP: e.g, SingleFrame, FirstFrame, ConsecutiveFrame
- Ethernet: e.g. network sniffing, TLS-Scans, DoIP
- CAN: e.g. CAN bus communication, fuzzing, wakeup
- UART: e.g. fuzzing, debug testing
- Power behavior: e.g. timing variation
- XCP: e.g. scans over CAN, UDP, TCP
- Gallia/UDS: e.g. UDS service scans
- AUX: e.g. JTAG testing
- Bluetooth: e.g. device discovery
- UDS: e.g. exhaustive UDS protocol tests)
- CVE: e.g. exploitation of specific vulnerabilities
- OBD: e.g. OBD protocol tests

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
etas.com/escrypt-cycurtest