DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

External (WP3) & Internal evaluation of solutions (WP2 + WP4)

25th October 2022, Brussels

HORIZON 2020
LC-MG-1-4-2018
Grant agreement ID: 814951

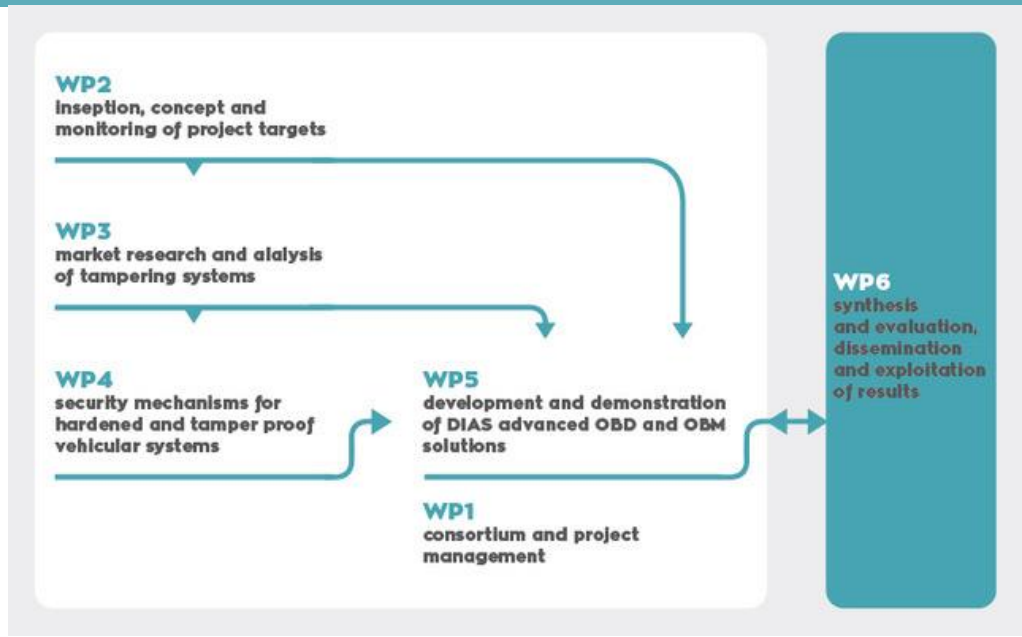
DIAS
Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION
HORIZON 2020
LC-MG-1-4-2018
Grant agreement ID: 814951

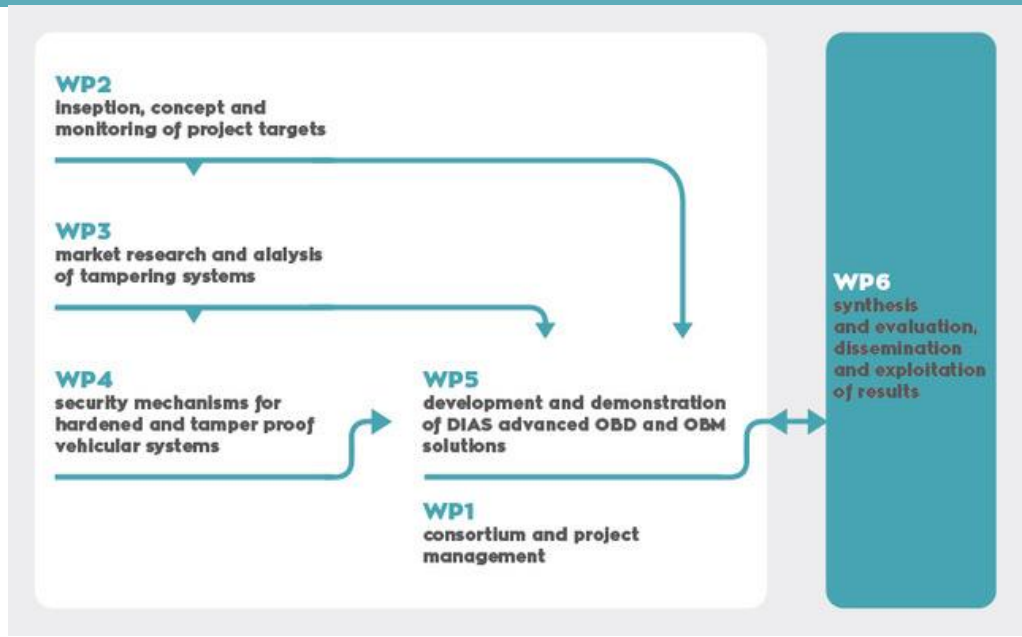
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814951.

Contents

- **External evaluation**
  - Hackathon#1
  - Hackathon#2
- **Internal evaluation**
  - Evaluation based on the pre-set targets
  - Verification and validation methodology and overview
  - Pentesting on ECU/ECU+SCU
  - Concept review/Design review/Code review
- **Q&A**



- **External evaluation**
  - Hackathon#1
  - Hackathon#2
- **Internal evaluation**
  - Evaluation based on the pre-set targets
  - Verification and validation methodology and overview
  - Pentesting on ECU/ECU+SCU
  - Concept review/Design review/Code review
- **Q&A [10 min.]**

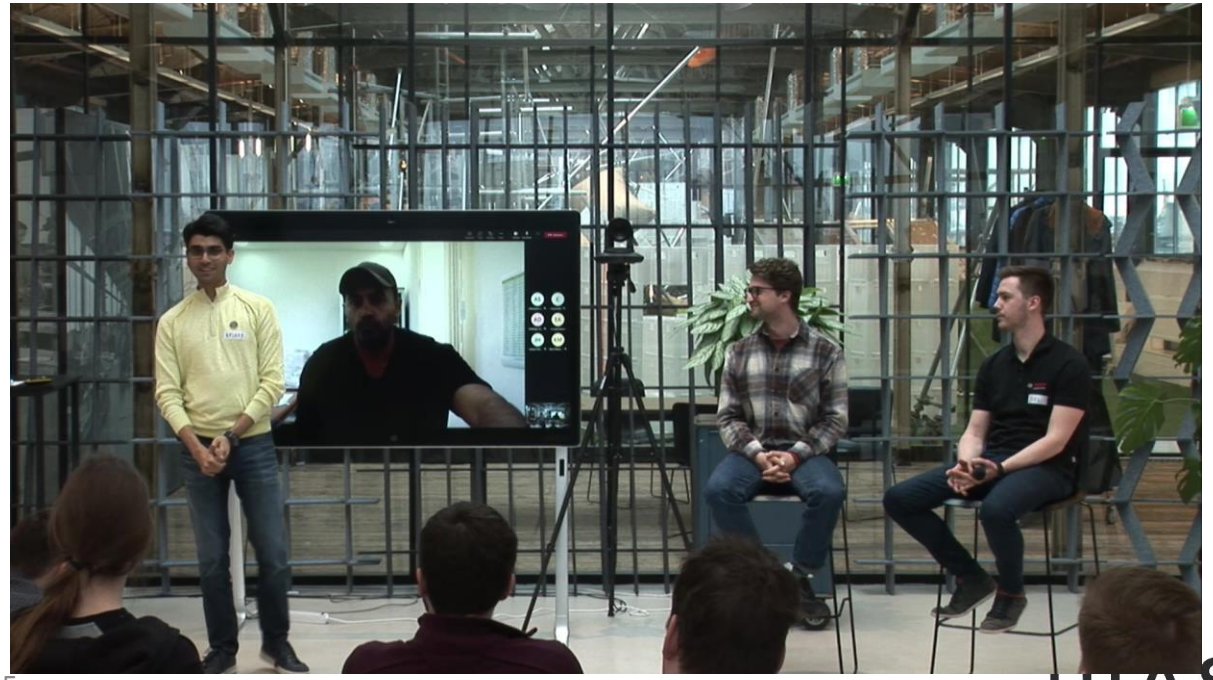


External evaluation of solutions

- WP3 - Market analysis and assessment of tampering systems
  - Task 3.4: DIAS concept evaluation
    - Organization of a successful ethical hacking event for real-world testing after completion of each of the two DIAS levels.
    - The goal is to reveal potential vulnerabilities within the developed countermeasures

Hack-a-Truck part 1, May 2021

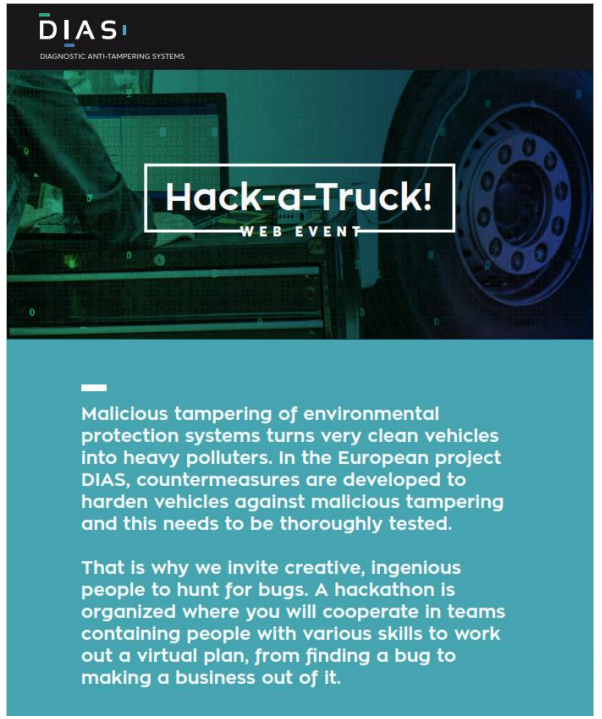
Hack-a-Truck part 2, March 2022



Hack-a-Truck part 1

- Hackathon 1: ECU and emission control systems on vehicle level
- Two day online event, due to Covid-19 restrictions, with a day in between
- In-depth presentations on DIAS, the Ford truck hardware and software, currently available tampering and the level 1 countermeasures
- Team contest with monetary awards for the teams that developed the best tampering plans

"...Your challenge is to find an attack vector or attack vectors, exploiting it to deactivate or remove an environmental protection system of a truck and develop a tampering device or service with a goal to commercialize the tampering product on the EU market..."



Event design

- 25 external participants of which 20 students/recent graduates and 5 hacking experts, with expertise ranging from automotive engineering to IT security
- The 5 teams were each guided by a mentor from the consortium and their questions answered by a pool of consortium experts
- The tampering plans were evaluated by the jury on:
  - Tampering success and impact
  - Detection on-board and at technical inspection
  - Complexity and cost
  - Market potential

Results

- Six attacks, none on the ECU (perhaps due to limited time)
- Additional testing and evaluation performed

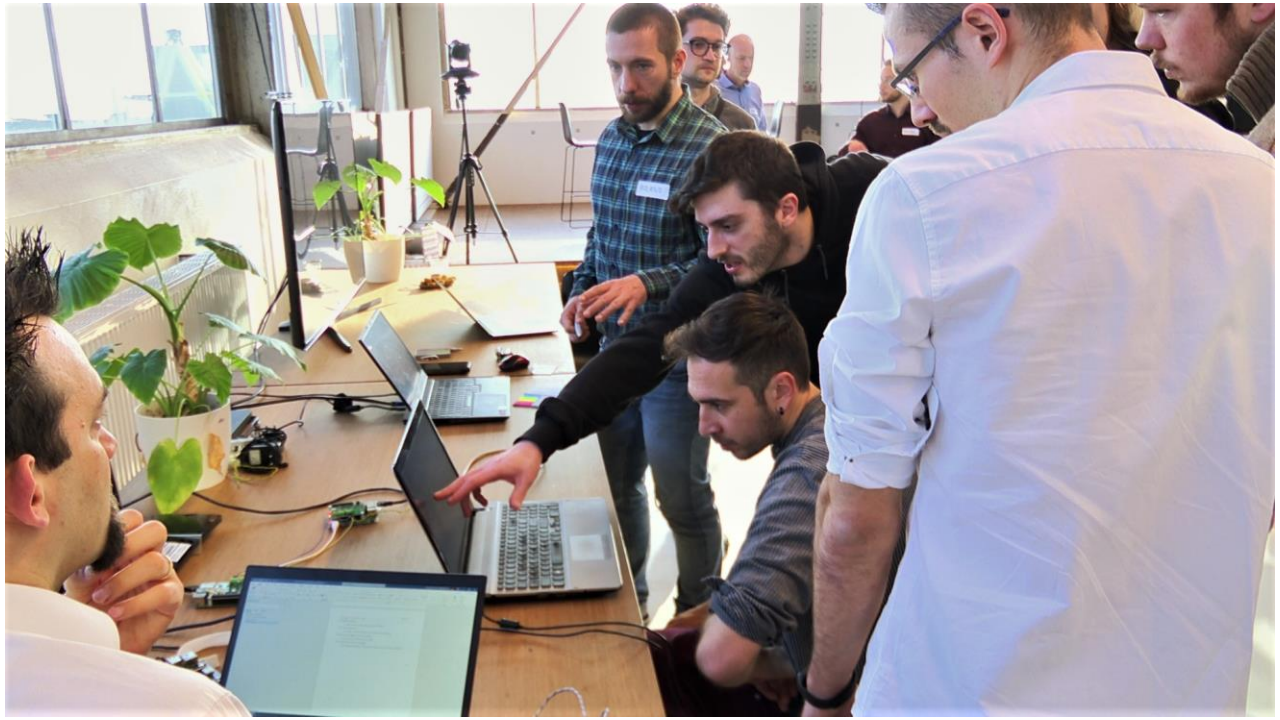
Attack vector	Conclusion
OBD Inducement activation delay time	Visibly detectable, also by OBD, and low market attractiveness.
NOx sensor analogue circuit	TARA performed and deemed low risk. Additional attacks have been executed in WP4, were it turned out that specialist equipment was required. This makes tampering very hard, very expensive and detectable by inspection.
NOx sensor SCU reflash	TARA performed and deemed low risk. Additional attacks have been executed in WP4, were it turned out that it was extremely difficult. No additional countermeasures needed.
NOx sensor margins	Only possible when the attack above succeeds. Even then impact is limited
Analogue signals	Current DIAS countermeasures prevent large exploit.
CAN bus with SecOC (For DPF removal)	Attacks were detected and the DIAS countermeasures protected the secure CAN communication against tampering.

- Not one high risk tampering solution was found

Hack-a-Truck part 2

- Hackathon 2: Communication from vehicle to ‘cloud’
- Level 2 countermeasures into test beds

Testbed 1: communication between ECU and CCU (SecOC)



Testbed 2: communication between CCU and cloud (HTTP)

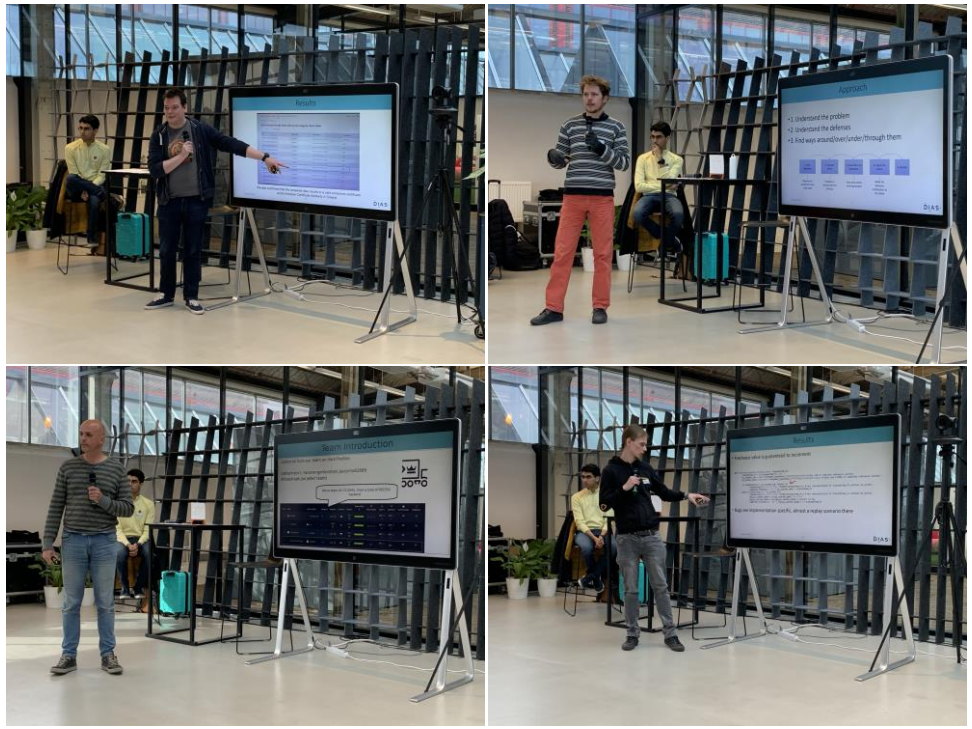
DIAS

Event design

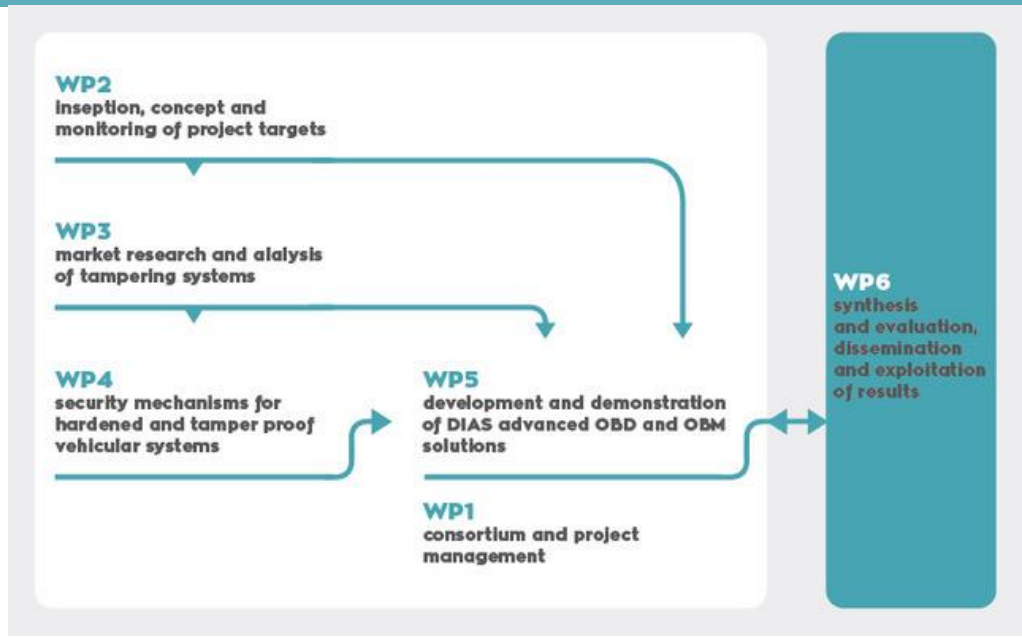
- Digital information session with in-depth presentations on DIAS, level 2 countermeasures and both test beds
- Two day event at RDM in Rotterdam, the Netherlands
- 15 external independent participants, ranging from students to professional hackers, with expertise in the field of cyber security

Results

- Five attacks on test bed 1
  - Two successful in reducing reported emissions have been further evaluated
    - One attack used “frame dropping”, but only a small reduction in recorded emissions was achieved and it was only possible with prototype hardware.
    - The other one desynchronized the CCU and the ECU, which is solved by including a Freshness Value Manager in the real implementation.
- Two attacks on test bed 2
  - One successful in authenticating emissions has been further evaluated
    - Using a way to bypass the PTI and create an authenticated emissions report. However, this was only exploitable in the prototype setup and because the credentials and specifications of the PTI endpoint were “leaked” by the test bed experts. Extremely unlikely in real world application and easily solved by splitting data endpoints in the real implementation.
- Not one high risk tampering solution was found and additional security recommendations have been implemented



- External evaluation
  - Hackathon#1
  - Hackathon#2
- **Internal evaluation**
  - Evaluation based on the pre-set targets
  - Verification and validation methodology and overview
  - Pentesting on ECU/ECU+SCU
  - Concept review/Design review/Code review
- Q&A



Definitions of specific targets for the solutions

- **Technology neutrality and applicability industry-wide:**
  - Can the basic principle of the solution be used in all vehicles?
  - Does it require technology-specific know-how and patents?
- **Lead time:**
  - How much time is needed from the start of developing a solution until its implementation?
- **(Technological) Complexity**:
  - Which is the needed technological level for the design and manufacture of a solution?
- **Cost:**
  - Which is the estimated financial resources needed for development and operation of the technology used?
  - Note: 2 basic targets are extracted:
    - Development (or initial) cost
    - Operational cost

Evaluation of solutions
Anti-tampering **diagnostic** functions

- The majority of the diagnostic solutions:
  - Are not restrictive towards a specific technology (**technology neutrality**)
  - Utilize physical-based algorithms and logical controls to succeed in monitoring and plausibilization of EPS-related signals
  - Exception: The PM sensor readiness diagnosis demands the use of a specific technology i.e. the PM resistive sensor
- All diagnostics solutions are **applicable industry-wide**
  - Concern: solutions that may demand high computational resources like detectors based on recurrent neural networks, autoregressive moving average and graph analytics
- **Lead time, complexity and development cost** are strongly correlated
  - All of them vary mainly depending on the “starting point” and extra burden needed to reach the Start of Production (SOP) phase
  - Some solutions built upon existing functions (e.g. Consumption Deviation Monitor observer)
  - The estimations changes to medium or high for solutions requiring a high level of technical knowledge, and which are only partly developed, investigated and demonstrated

DIAS

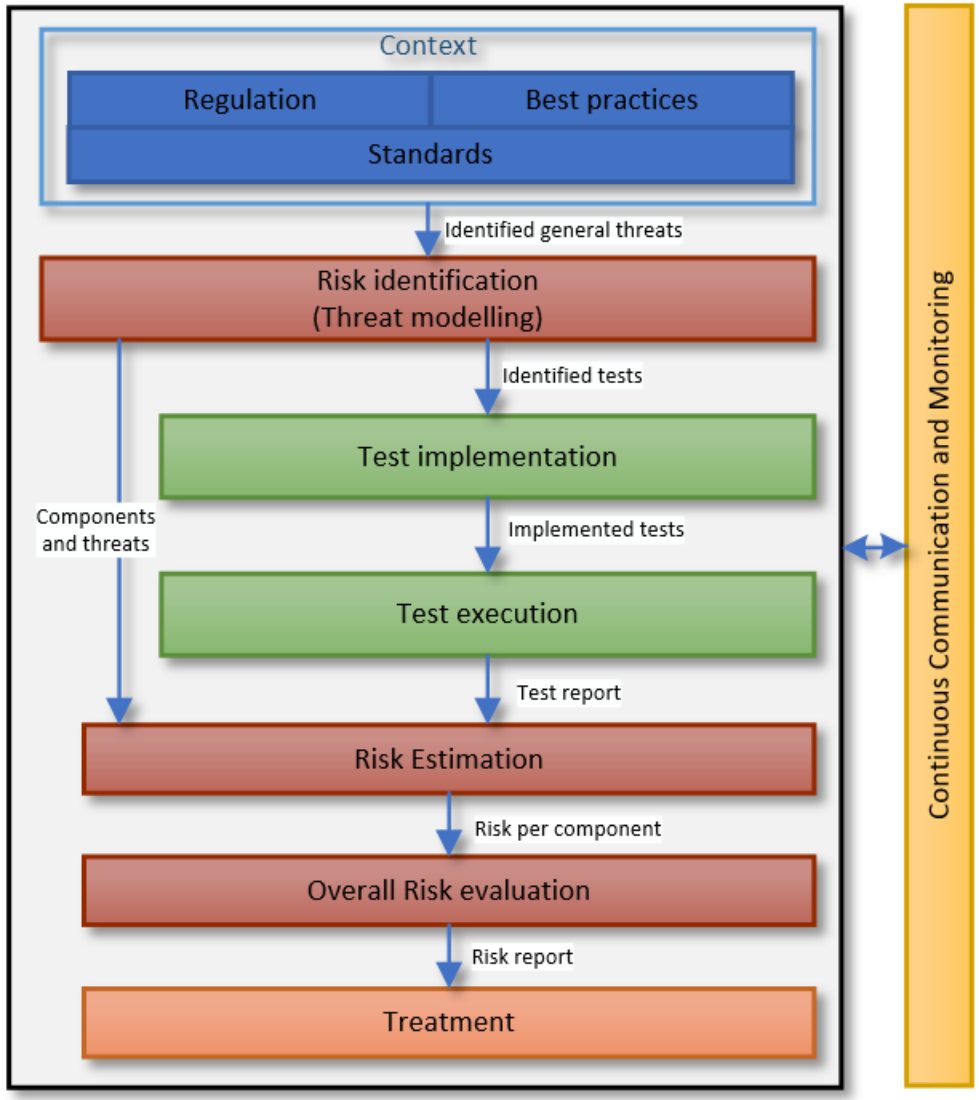
Evaluation of solutions
Anti-tampering **security** functions

- The security solutions are characterized as **technology-neutral** and they build upon:
  - Worldwide accepted security-related standards and protocols
  - EU or non-EU regulatory frameworks
  - Open-source security techniques
  - Scientific publications
- **Lead time, complexity and cost**:
  - Overall, medium to low complexity and cost is observed, while lead time seems proportionate and closely correlated to the complexity and cost
- Note regarding additional technical constraints identified in security solutions:
  - Even if targeting applicability to all xCUs, the ECDH (Elliptic curve Diffie-Hellman) key exchange scheme is challenging for resource-constrained controllers.
  - Sensors using SENT as transmission protocol are highly resource-constrained to execute the common security measures on them. The secure SENT solution currently does not fulfil these constraints and therefore, it is not suitable for serial production of SENT sensors.

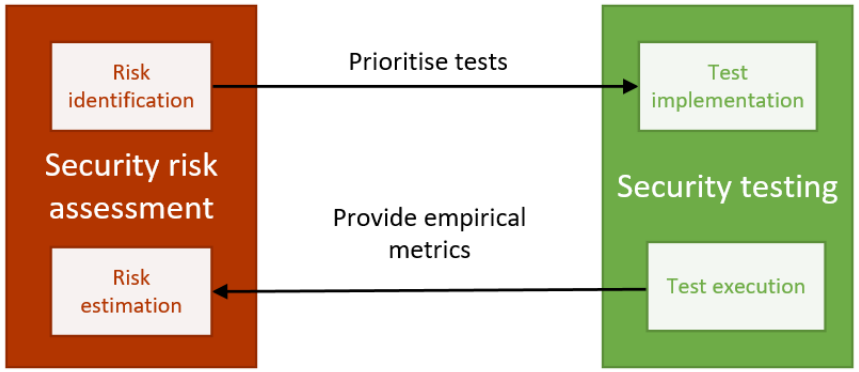
Evaluation of solutions
Anti-tampering **reporting** functions

- **Technology neutrality** is overall ensured as they are built upon known and available schemes and infrastructures
- All DIAS reporting solutions are expected to be **applicable industry-wide**
- Reporting solutions **lead time** is difficult to be estimated, especially for sharable/revokable data-driven certificates which depend on the development of other solutions or standards or infrastructure.
- Half of the six solutions are estimated at a medium level of **complexity**
- The **cost** of most reporting solutions is low, at least when compared to the existing solutions

Verification and validation methodology and overview

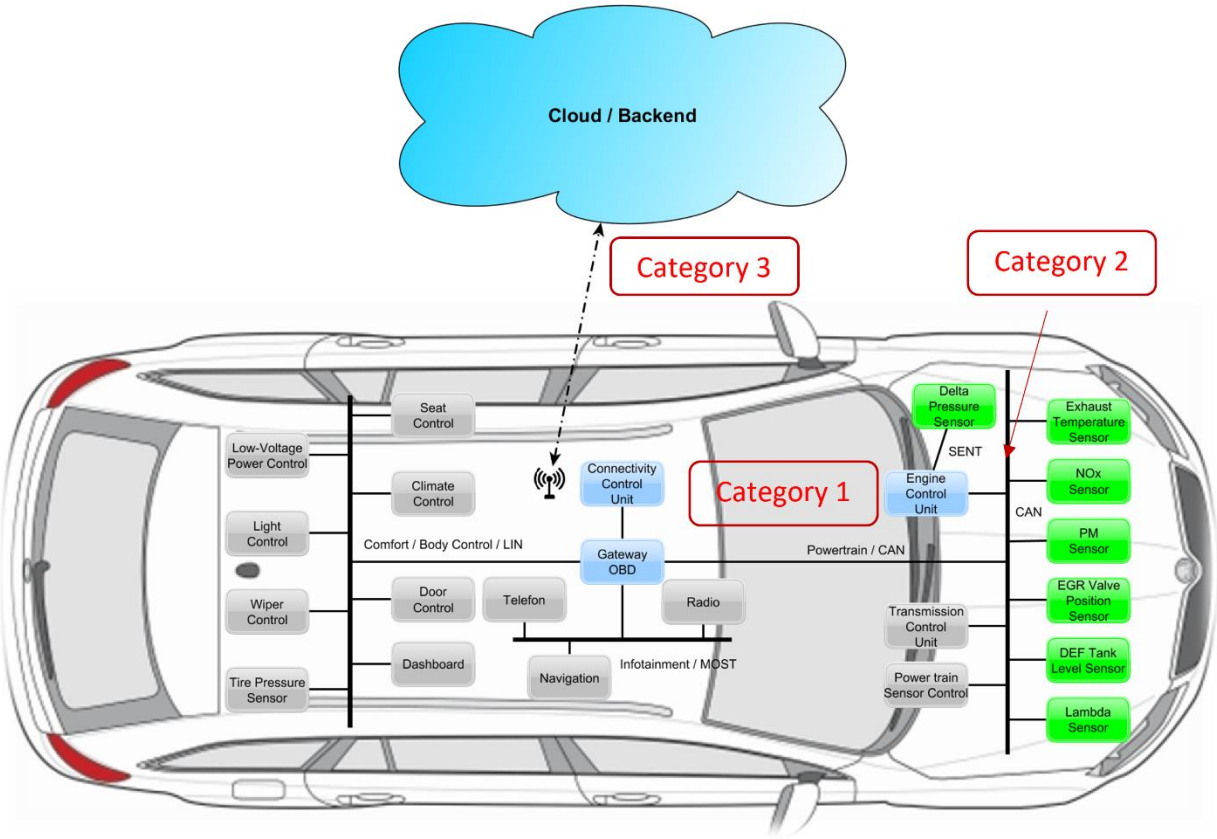


- Verification and validation in DIAS focuses on:
  - Security evaluation methodology – build a framework for processes
  - Security testing – identify security vulnerability
- The proposed methodology can be associated to the V model in the ISO/SAE 21434
- Cybersecurity process is iterative and continuous:
  - Risk assessment prioritizes the security testing.
  - Security testing improves the risk assessment.



Verification and validation methodology and overview

- Based on the market assessment and security analysis, three categories of security are critical and chosen in the verification and validation to test
  1. Engine Control Unit (ECU) reprogramming
  2. CAN-bus communication between the ECU and the sensors
  3. Data sending to the cloud
- Approaches used are mainly:
  - **Penetration test**: to test ECU reprogramming and secure CAN communication (Category 1 and 2)
  - **Concept review (TARA):** to evaluate the Key Exchange RSA Asymmetric Approach (Category 2)
  - **Design review (TARA):** to evaluate the distributed ledger technology and cloud-based methods for the provisioning of certified data (Category 3)
  - **Code review**: to check the implementation of the prototype (Category 3)



Penetration testing on ECU/ECU+SCU

Nr.	Type of the attack	Attack target	Description	Platform
1	Brute force attack	ECU reprogramming	Brute force the secure access service of UDS to verify the countermeasure of unauthorized ECU reprogramming	Desktop test setup
2	Tampering attack	ECU reprogramming	Tamper the flash image and test the integrity check of ECU software during reprogramming	Desktop test setup
3	Man-in-the-middle attack	ECU+SCU (SecOC light)	Test the authentication and integrity of the communication between ECU and SCU	Desktop/On-vehicle test setup
4	Frame injection attack	ECU+SCU (SecOC light)	Test the authentication and the integrity of the communication between ECU and SCU.	Desktop/On-vehicle test setup
5	Replay attack	ECU+SCU (SecOC light)	Test the authentication of the communication between ECU and SCU.	Desktop/On-vehicle test setup
6	Circuit modification	Analogue signal of NOx sensor	Check the risk of analogue signal tampering, which causes integrity issue.	Desktop test setup
7	Flash dump	Memory of NOx SCU	Check the possibility of the memory dump through hardware pins, which can be an attack path to breach the integrity of the system.	Desktop test setup

Penetration testing on ECU/ECU+SCU

- Desktop test setup
  - A development ECU
  - A Raspberry Pi 4 with connected CAN adapters
  - Python script
- Attack target
  - ECU reprogramming – Security Access service (UDS service 0x27)
- Approaches
  - Brute force attack: unauthorized software and dataset reprogramming
  - Tampering attack: program and dataset modification
- Results
  - Negative responses indicate the attacks failed. The tests passed, such as
    - 0x24 (*requesSequenceError*)
    - 0x35 (*invalidKey*)
    - 0x36 (*exceededNumberOfAttempts*)
    - 0x72 (*generalProgrammingFailure*)

```
#0227010000000000
#10226701B0470DD4
#3000320000000000
#2138B7C043B0FE53
#22F1B0E8974FC337
#234714F2FD17B752
#246745CF9DCB98B3
#10422702C20D8DC3
#300000
#2174A33524655340
#223A390F4ADE40E2
#236DE25FB2905E8A
#24BA74B7D5EEC608
#258AE4A1510A5A14
#26BB289A313CA7BF
#2711D4F2AA78A5CF
#28959656338CD488
#29BAB4B9EF
#037F277800000000
#037F273500000000
#10422702C20D8DC3
#300000
#2174A33524655340
#223A390F4ADE40E2
#236DE25FB2905E8A
#24BA74B7D5EEC608
#258AE4A1510A5A14
#26BB289A313CA7BF
#2711D4F2AA78A5CF
#28959656338CD488
#29BAB4B9EF
#037F272400000000
```

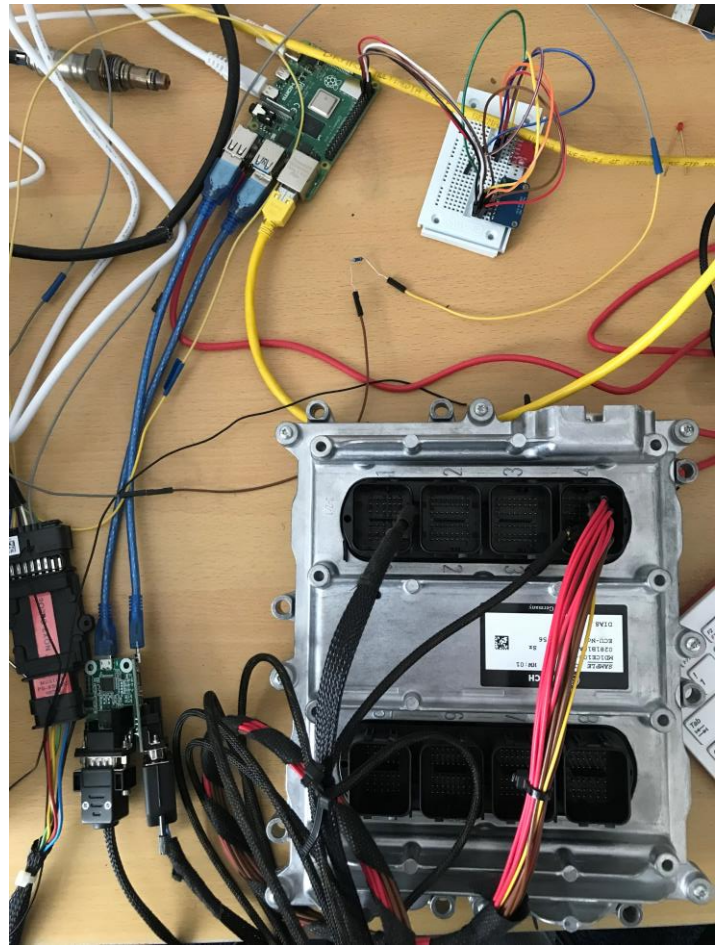
Request challenge

Send response (1st try)

Negative response 0x35

Send response (2nd try)

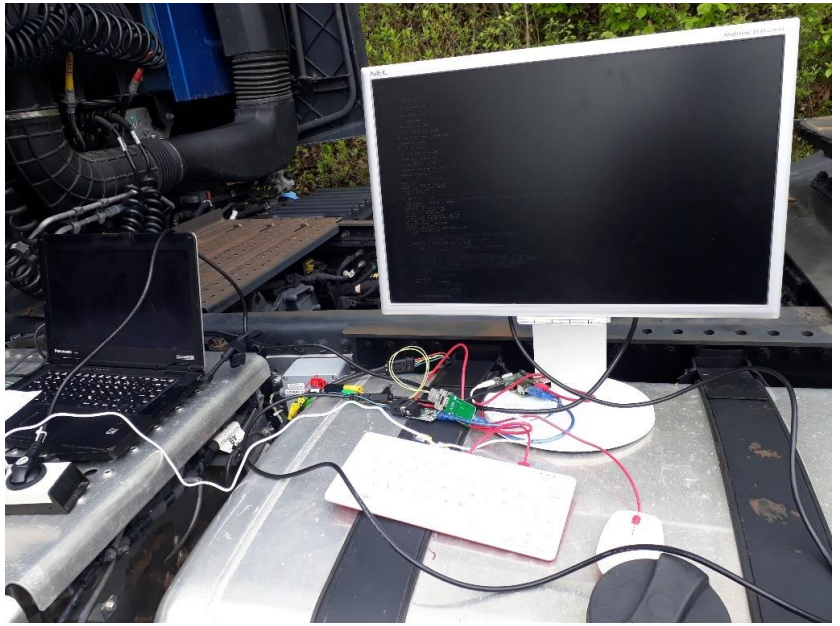
Negative response 0x24



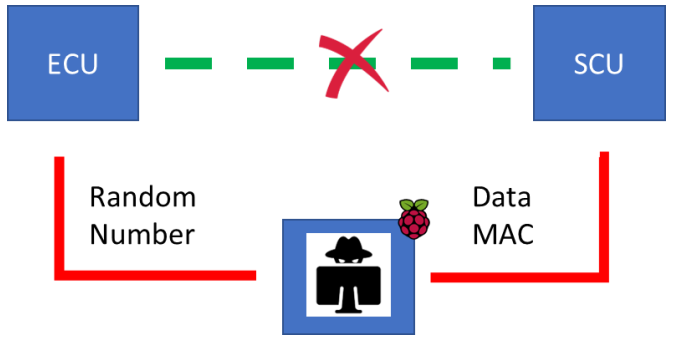
DIAS

Penetration testing on ECU/ECU+SCU

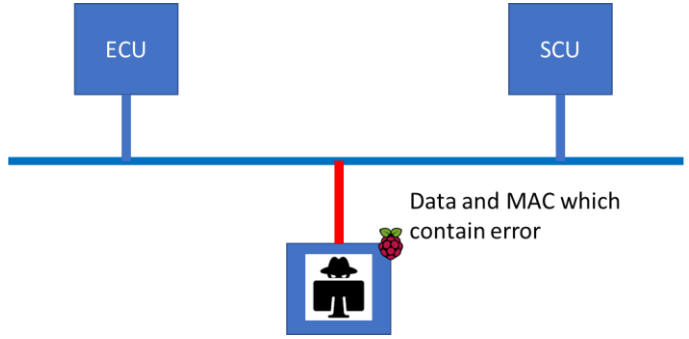
- On-vehicle test setup
  - A Raspberry Pi 4 connected to the vehicle CAN
  - Python script
  - A laptop with INCA to monitor the Diagnostic Trouble Code (DTC)
- Attack target:
  - ECU + SCU CAN communication – SecOC light
- Results:
  - Error flags monitored by INCA proved that the ECU detected the tampering. The tests passed.



Messtabelle [7907]		Messtabelle [7908]	
DFES_numDFC_[0]	DFC_ComNoxMacCorrectness [-]	DFES_stChk_[0]	Defect [-]
DFES_numDFC_[1]	DFC_FlSysClgDet [-]	DFES_stChk_[1]	Defect [-]
DFES_numDFC_[2]	DFC_Unused [-]	DFES_stChk_[2]	OkNoTst [-]
DFES_numDFC_[3]	DFC_Unused [-]	DFES_stChk_[3]	OkNoTst [-]
DFES_numDFC_[4]	DFC_Unused [-]	DFES_stChk_[4]	OkNoTst [-]
DFES_numDFC_[5]	DFC_Unused [-]	DFES_stChk_[5]	OkNoTst [-]
DFES_numDFC_[6]	DFC_Unused [-]	DFES_stChk_[6]	OkNoTst [-]
DFES_numDFC_[7]	DFC_Unused [-]	DFES_stChk_[7]	OkNoTst [-]
DFES_numDFC_[8]	DFC_Unused [-]	DFES_stChk_[8]	OkNoTst [-]
DFES_numDFC_[9]	DFC_Unused [-]	DFES_stChk_[9]	OkNoTst [-]



Man-in-the middle



Frame injection

Concept review/Design review/Code review

- Concept review on Key Exchange RSA Asymmetric Approach
  - Focus on **threat assessment** – using TARA based on SAE J3061
  - Different **potential attack vectors** are discussed, two attack vectors are identified as valid and evaluated.
  - **Deployment aspects** are also discussed.
- Design review of the cloud-based methods for the provisioning of certified data (Subcontract)
  - Conduct cybersecurity analysis on the **system architecture, involved assets and their functionality**
  - **TARA based on ISO/SAE 21434**
  - The main findings can compromise the correct functioning of the system, but no direct impact on tampering
- Code review of out-of-vehicle communication (Subcontract)
  - Identification of the **possible Common Weakness Enumerations** (CWEs) for each attack path
  - Assessment of **CWE technical impact**
  - Identification of the **possible Common Vulnerabilities and Exposures** (CVEs) associated with the specific technologies used in the prototype;
  - Assessment of **Common Vulnerability Scoring System (CVSS) severity** for each CVE identified.
  - Conclusion: the implemented prototype is **a good proof of concept for DIAS Antitampering system**. Some security issues are reported and recommended to solve when the prototype will be engineered for production.

DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Thank you

Q & A

DIAS
SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS