DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Market analysis, Tampering testing (WP3), Security analysis (WP4)

25th October 2022, Brussels

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

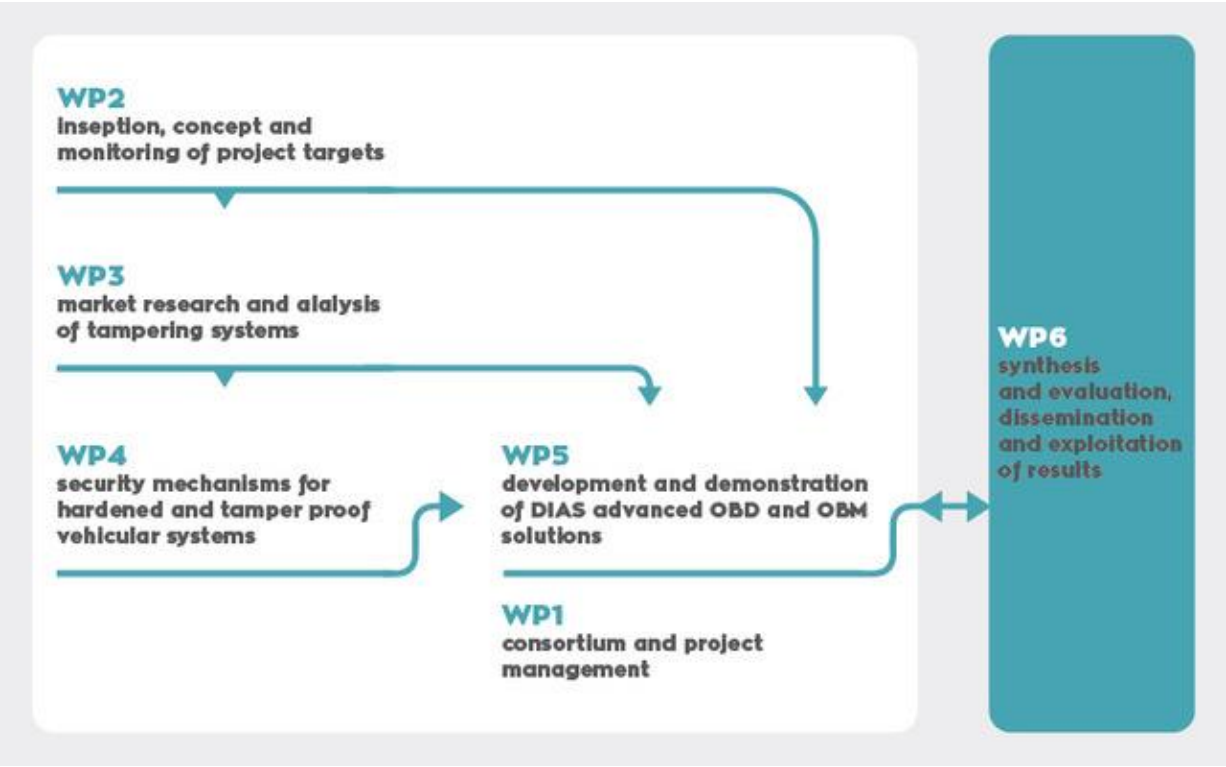
DIAS
Smart Adaptive Remote Diagnostic Antitampering Systems

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

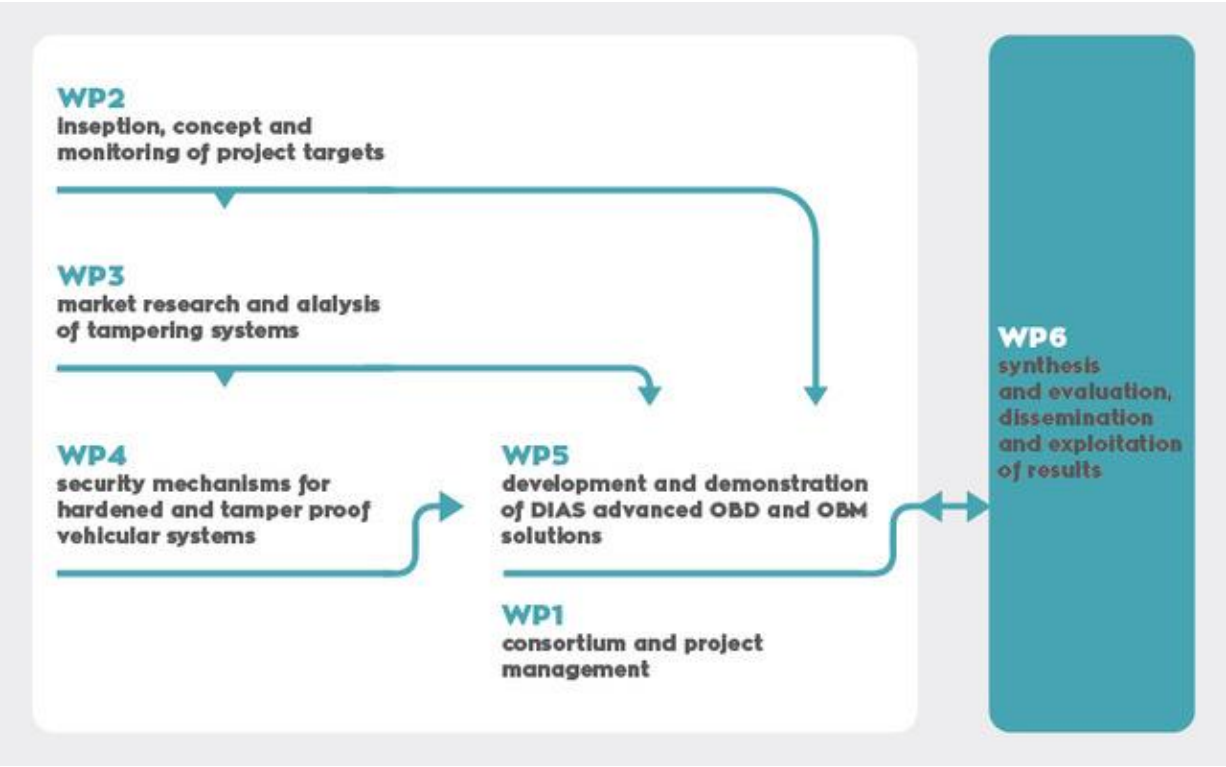
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814951.

Contents

- **Market analysis**
- **Tampering testing**
- **Security analysis**
- **Q&A**



- **Market analysis**
- Tampering testing
- Security analysis
- Q&A



Market analysis and testing

- Tampering market
  - Demand and supply: motivations, tampering goals
  - Supply: list with tampering offered
  - Environmental Protection Systems affected
  - Keep track of possible new types of tampering during project
  - Categorisation and prioritization of critical tampering techniques for:

- Tampering testing and evaluation
  - Purchase tampering (35 pcs ordered, 31 received)
  - Desktop testing and on-vehicle testing to determine **the impact on vehicle systems**, **working principles** and to **reveal vulnerabilities** and check claims

- Definition of general requirements for the development of DIAS countermeasures to prevent, detect and report tampering

Current tampering ‘market’

Tampering motivations (demand)

- Prevent cost of repair, maintenance, downtime and / or costs for consumables or extend time to repair and maintenance of vehicles and machinery equipped with sophisticated Environmental Protection Systems
- Increase engine power, reduce FC, increase exhaust sound level

Main tampering types offered (supply)

- ECU flashing, emulators, modifiers
- From very simple DIY solutions to professional products, hard and software tools
- Internet web shops, online market places (DIY with instructions), tuning workshops

Environmental protection systems affected

- LD / HD / NRMM diesel: SCR +(AMOC), DPF (+DOC), EGR: deactivation, removal, unrepaired malfunctions
- LD gasoline: TWC: unrepaired malfunctions, GPF removal
- OBD: suppression of inducement or DTCs, unrepaired malfunctions

Sources: interviews with tuning workshops representatives, stakeholders, police, literature, internet websites, internet fora.

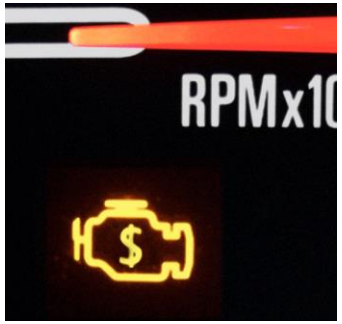
DIAS

Specific tampering motivations and targets per EPS

Environmental protection system	Main motivations	Tampering target
DPF (+DOC) **Diesel**	Avoid costs for replacement of filter Avoid costs for maintenance, filter cleaning Decrease costs for fuel, increase power Avoid costs for downtime due to malfunction	Removal of the filter Avoid replacement of broken filter
SCR (+AMOC) **Diesel**	Avoid costs for maintenance and repair / replacement of catalyst and SCR system components (NOx sensor, pump, dosing unit) Avoid costs for possible downtime Avoid costs for refills with reagent Extend refill period	Stop or reduce reagent dosing Removal of catalyst Avoid replacement of broken, worn or aged components (pump, NOx sensor, dosing unit) Suppress AdBlue refill message
EGR **Diesel**	Avoid costs for repair / replacement Decrease costs for fuel, increase power Avoid costs for downtime due to malfunction	Valve fixed in closed position or blockage of piping
TWC **Gasoline**	Avoid costs for repair / replacement of catalyst or lambda sensor Probably a niche mostly for performance tuning	Removal of catalyst Avoid replacement of broken or worn / aged components (catalyst, lambda sensor)
OBD	Supress DTCs, Malfunction Indicator and inducement Bypass periodic inspection with removed, deactivated or faulty parts (e.g., EGR, DPF, SCR, EGR) Avoid costs for repair / replacement Enable tampering of EPS by deleting the trouble codes arising from the tampering of these systems This may affect all environmental protection systems	Deletion of trouble codes, MI off, prevent inducement
GPF **Gasoline**	Increase engine power output Change exhaust sound No indication that cost of replacement is a motivation, but there is no long-standing experience or information about GPF durability.	Removal of the filter element

Categorisation and prioritisation

- Sophisticated EPS with an increased risk for malfunctions or durability issues and associated costs for repair, maintenance and downtime and consumables are said to be tampered most:



  - Diesel EPS: SCR, DPF, EGR (LD, HD and NRMM)
  - OBD (HD) added later as targeted system. Reported by Danish police, targeted to suppress inducement.
  - Three-way catalyst (LD gasoline).

  - GPF: added later. But different motive: Tuning / exhaust sound. So far no signs of durability issues.
  - 'Performance tuning' can impact EPS and engine control integrity. Not investigated in DIAS.

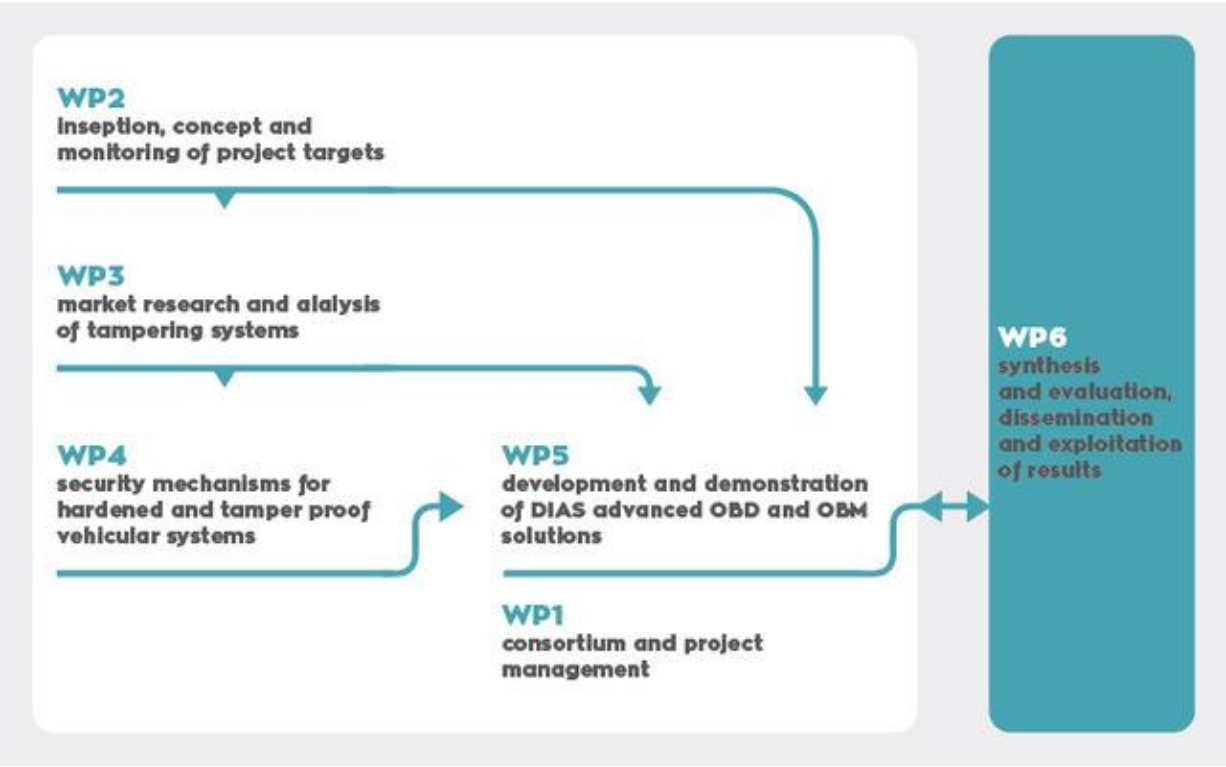
- Main types of tampering vehicles:
  1. **ECU flashing can potentially affect all EPS and OBD of LDV, HDV and NRMM. Probably prevalent for future vehicles.**
  2. **Emulators are still prominent for recent and current gen. HDV (and NRMM?)**
  3. Modifiers:
     1. TWC lambda sensor spacer / catalyst
     2. Temperature sensor emulation resistor / bushing
  4. OBD delete devices

Conclusions market assessment

- There is a substantial market for tampering with a demand and supply.
- Main motivation for tampering is to reduce costs of operation

- For HDV clear evidence of tampering was found.
  - Tampering is offered for all EPS of modern trucks and found on trucks in the form of **Emulators**, **ECU flashing** and **modifiers**.
- For PC/LDV less statistical data is available
  - But several cases are known and tampering is offered such as EGR off and DPF removal for older OBD generations.
  - Few tampering or evidence for tampering LD DeNOx systems to date.
  - Poses a risk for newer vehicle generations with EGR, DPF and SCR when systems age, break down or require refill.
- NRMM are totally out of sight of authorities
  - No (periodic) inspection, no statistics,
  - But a clear market with products (**Emulators and ECU flashing)** and risks due to possible malfunctions of EPS (stage IV and V).
- Development of tampering is lagging as it has to respond to new control features and the changing demand or rising demand when failures emerge and warranty is over.
- Tampering was categorized and prioritized for testing to determine working principles of tampering and vulnerabilities exploited.

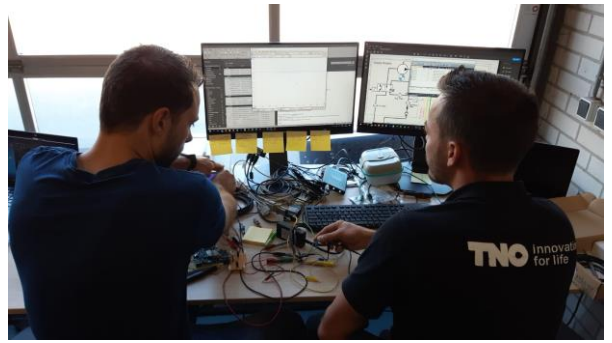
- Market analysis
- **Tampering testing**
- Security analysis
- Q&A

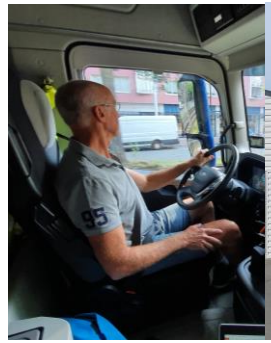


Tampering testing

- 35 tampering products, 31 received
- Desktop testing
  - Allows broader view on market, as we see many devices
  - To determine construction, first view of working principles
  - Devices may look different but may work in a similar way
  - Devices may work similar but be programmed for different brands / types (e.g. CAN matrix)
  - Allows to investigate if we find different techniques and categorise according to the differences

- On road and chassis dyno testing
  - Measure the impact of tampering on the vehicle systems to understand working principles and determine vulnerabilities
  - Verify the claim(s) of tampering provider (ECU flashing and emulators), verify if known tampering techniques work
  - Measure the impact on emissions





Overview of test matrix and on-vehicle test results

	ECU flashing	Emulators	Modifier
HD1 (Diesel, N3, prototype VI-D)	SCR+DPF+EGR → no AdBlue dosing, DPF removed, EGR delete caused DTC	SCR-AdBlue → No AdBlue dosing, 0 DTC	EGT resistor @130°C → No AdBlue dosing, no DTC after short test, EGT bushing → AdBlue dosing shortly delayed, no DTC, AAT @-21°C → No AdBlue dosing, no EGR, no DTC
HD2 (Diesel, N3, VI-C)		SCR-AdBlue → No AdBlue dosing, 3 DTC's SCR-AdBlue → No AdBlue dosing, 0 DTC SCR-AdBlue → No AdBlue dosing, 0 DTC NOx sensor → No AdBlue dosing, 1 DTC	
HD3 (Diesel, N2, VI-D)		SCR-AdBlue → AdBlue dosing reduced by 50%	
LD1 (Diesel, M1, EU6c)	OBD EGR/SCR/DPF → Worked, some DTCs after 1st EGR test (a fix solved this) Flashing pins EGR/SCR/DPF → Worked without DTCs	DPF emulator → Not working	
LD2 (Gasoline, M1, EU5)			Lambda sensor spacers → DTC's, Lambda sensor spacers → 0 DTC TWC mini catalysts → DTC's TWC mini catalysts → 0 DTC
LD3 (Diesel, M1, -)			Bushings EGT → AdBlue dosing slightly delayed
NRMM1 (Diesel, Stage IV)		SCR AdBlue → Not working NOx sensor → Not working	
NRMM2 (Diesel, Stage IV)		SCR AdBlue → AdBlue dosing stopped, 0 DTC	

Additional test data of emulators as received by ACEA was taken into account (not reported in this presentation)

DIAS

Current main tampering types.

ECU flashing

- Inject (flash) malware to ECU memory
- LD, HD and NRMM
- ~150 EUR / single target to 900 EUR / multiple targets (eg. EGR+SCR+DPF)
- Tools (100-1500 EUR) for non-professional use which use ECU images 300 EUR / image or subscriptions, eg. 30 kEUR / yr
  - SCR, DPF removal
  - AdBlue off
  - EGR off
  - OBD Suppress inducement, avoid DTC's
  - Increase power, torque engine
- Sub types
  - Dedicated flashing tools to flash images, via OBD port or ECU plug
  - Third party service tools
  - Opening ECU: connecting to internal circuitry (older ECU types)
  - Replacing chips or flash on external bench (older ECU types)


Emulators

- Inject false messages on CAN-bus and ECU
- Simple circuitry and software integrated in a casing
- Often: integrated DTC delete
- Mainly HD and NRMM
- ~200-1000 EUR
  - Switch off or reduce AdBlue
  - Removal of parts (SCR, DPF)
  - Avoid repair of SCR, DPF related components
- Sub types
  - AdBlue off
  - SCR+DPF removal
  - NOx sensor emulator
  - Integrated ECU+ACM vs. separate 2-box systems, emulators for the latter require DPF removal as the whole ACM is shut of and emulated


Modifiers

- Simpler form of signal manipulation
- ~10-40 EUR typically
- 350 EUR, GPF delete
- Sub types
  - Bushings: reduce AdBlue use
  - Resistors: AdBlue off, reduce AdBlue use, GPF removal
  - Mini catalysts: Avoid repair or removal of TWC or lambda sensor

DIAS

ECU Flashing

- Inject (flash) malware to ECU memory. Also called ‘ECU remapping/reprogramming’.
- LD, HD and NRMM diesel
- ~150 EUR / single target to 900 EUR / multiple targets (eg. EGR+SCR+DPF delete)
- Tools (100-1500 EUR) for non-professional use which use ECU images 300 EUR / image or subscriptions to be used by workshops, eg. 30 kEUR / yr

- Goals
  - SCR removal
  - DPF removal
  - AdBlue off
  - EGR off
  - OBD Suppress inducement, avoid DTC’s
  - Increase power, torque engine

- Sub types
  - Dedicated flashing tools to flash images, via OBD port or ECU plug/interface
  - Third party service tools
  - Opening ECU: connecting to internal circuitry (older ECU types)
  - Replacing chips or flash on external bench (older ECU types)

Emulators

- Inject false messages on CAN-bus.
- In some cases emulate actuator controls.
- In some cases with integrated frequent DTC delete.
- Simple electronic circuitry and software integrated in a casing with wiring for CAN, power and actuators.
- Mainly HD and NRMM diesel
- ~200-1000 EUR

- Goals
  - Switch off or reduce AdBlue consumption
  - Removal of parts (SCR, DPF)
  - Avoid repair of SCR, DPF related components

- Sub types
  - AdBlue off
  - SCR+DPF removal
  - NOx sensor emulator
  - Integrated ECU vs. 2-box (ECU+ACM) systems. Advertised for ‘Adblue off’. Emulators for 2-box systems require DPF removal as the whole ACM is shut down and emulated.

DIAS

Modifiers

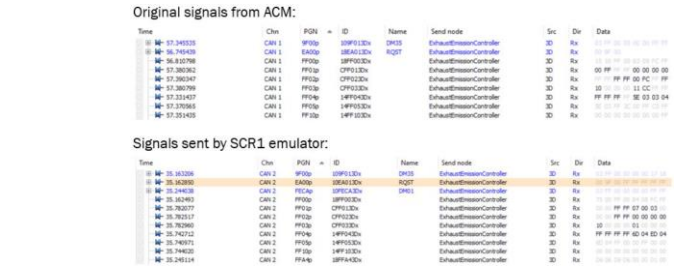
- Simpler form of signal manipulation
- ~10-40 EUR typically, 350 EUR, GPF delete
- LD petrol, HD diesel

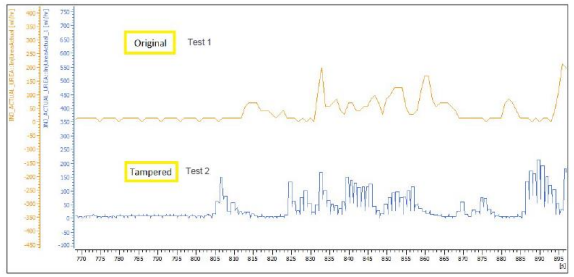
- Goals
  - Switch off or reduce AdBlue consumption
  - Avoid repair or removal of TWC or lambda sensor
  - Removal of GPF (only specific vehicle brand-types)

- Sub types
  - Bushings: reduce AdBlue use
  - Resistors: AdBlue off, reduce AdBlue use, GPF removal
  - Mini catalysts: Avoid repair or removal of TWC or lambda sensor

Testing conclusions

- Claims verified
  - The quality of tampering is mixed. Testing results ranged from successful tampering to tampering that didn't work at all. Also, tampering was tested were immediately or eventually, diagnostic trouble codes were stored, and malfunction indications popped up.
- Impact measured
  - Severe tampering with complete deactivation or removal of components can set back vehicles emissions to the level of vehicle generations of decades ago. Avoiding repair of components can cause an increases of noxious emissions as the correct functionality of the system is compromised.





- Different working principles of current tampering and vulnerabilities of current Environmental protection systems were identified and reported within the DIAS project.
- The results and general recommendations from the market assessment and the testing programme and the outcome of the security analyses formed the basis for the development of countermeasures.

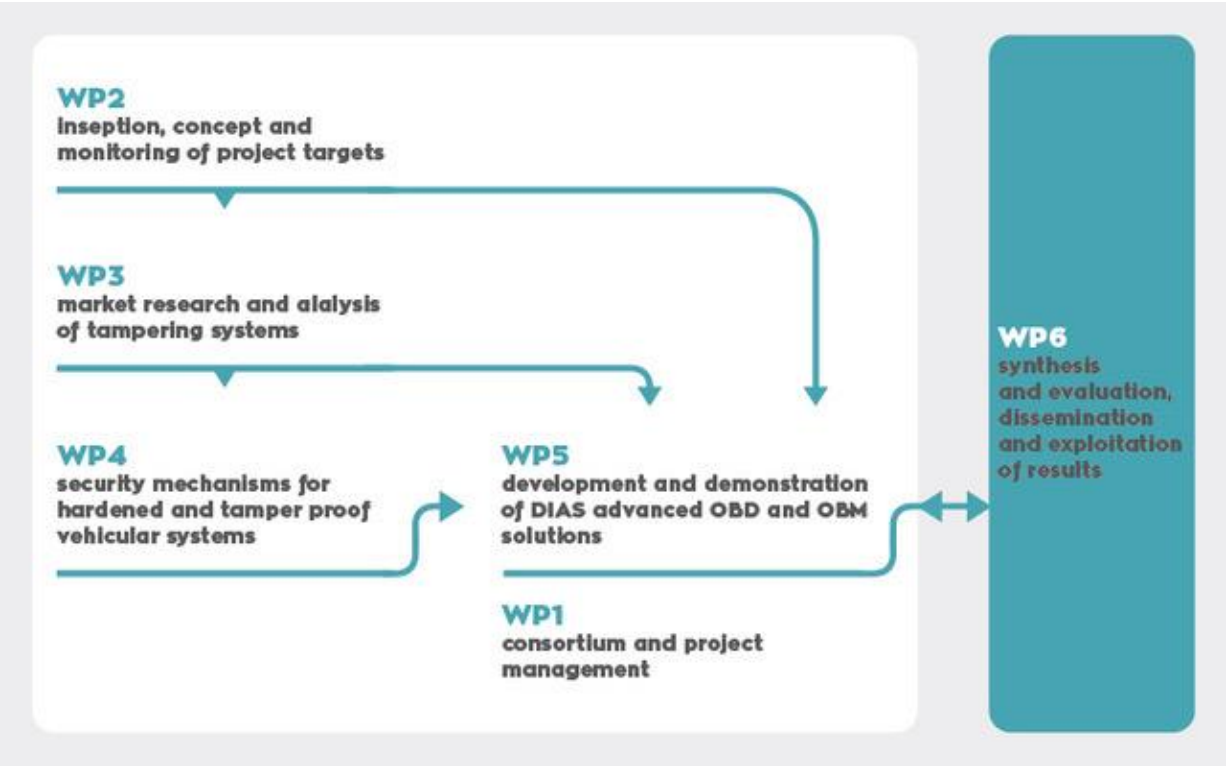
General recommendations

- Based on **market assessment** and **testing** programme the status quo of current tampering was defined and general recommendations could be proposed for countermeasures to prevent or detect and report current tampering. This entails:

- **Assuring the data integrity of signals** of sensors and actuators that take part in the control of the EPS and the on-board diagnostics system.
  - For digital signals by detecting or preventing the injection of false signals by authentication of digital signals and assuring the integrity of sensor control units.
  - The integrity of analog and digital signals can be checked using advanced data rationality checks.
- **Assuring the integrity of the ECU**. This by detecting or preventing unauthorized flashing of ECUs by advanced security features.
- **Detection or prevention of malicious erasing of the fault code memory** of the on-board diagnostics system
- Since current OBD does hardly foresees in functionality to detect and report tampering it is advised to consider requirements for **continuous tampering diagnostics with tampering probability monitoring and reporting**. It is also recommended to consider tampering checks for periodic inspections. The tampering diagnostics could assist enforcement of proper use of the EPS at regular periodic inspections, roadside inspections or for monitoring of tampering in the fleet through the cloud.

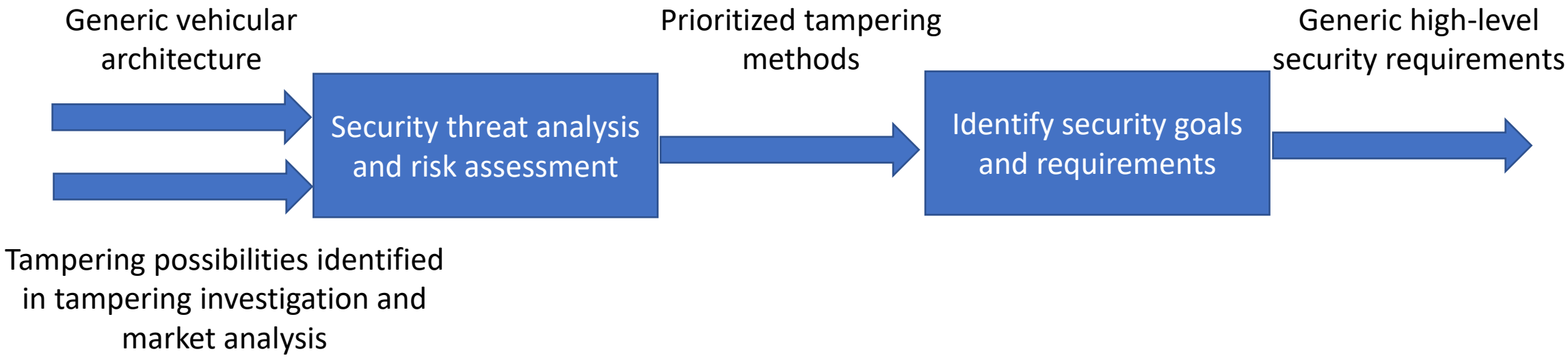
DIAS

- Market analysis
- Tampering testing
- **Security analysis**
- Q&A



Security analysis approach

- Introduction of a **generic vehicle architecture**
- Study of the **tampering possibilities** identified in tampering investigation and market analysis
- Using **Threat analysis and risk assessment** (TARA) to prioritize the tampering methods with security level
- Identification of **generic high-level security requirements**
- The generic high-level security requirements are **inputs to the security solution development** and they **will be refined to detailed security requirements based on TARA of specific system**



TARA of tampering possibilities

- The TARA conducted in DIAS was based on SAE J3061
- Two dimensions of parameters are evaluated:
  - **Threat level**
  - **Impact level**
- Two specific parameters are introduced in DIAS:
  - **Financial motive**: the financial gain that the tamperer will achieve by performing the attack.
  - **Environmental impact**: directly relevant to the work performed in the DIAS, which replaces the operational impact
- The threat level and impact level are combined together to obtain the security level

Threat level	Impact level
Expertise	Safety
Knowledge of the Target	Financial
Window of Opportunity	**Environmental** (replace operational)
Required Equipment	Privacy and legislation
Financial Motive	

Security Level (SL)		Impact Level (IL)					
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

DIAS

TARA of tampering possibilities

Category	Assets	Attack	Threat	Security level
1 – ECU	ECU	Unauthorized reflashing of ECU software and ECU data	Unauthorized software runs on the ECU, calibrated data can be changed	Critical
2 – Secure communication	Sensor, CAN	Sensor emulation	Wrong emission values are reported by the vehicle leading to loss of integrity	Critical
	CAN	Spoof CAN message by inserting false data on the CAN bus impersonating a particular emission sensor/ECU.	Wrong emission values are reported on behalf of a sensor which is working properly	High
	CCU	False emission data inserted on the powertrain CAN by compromising the CCU	Wrong emission values are reported by the vehicle	Medium
	CCU	Fake communication unit to compromise telematics unit and deploy rogue firmware	Use of malicious communication unit to spread a malware of just disrupting the infrastructure communications	High
3 - Backend	CCU	Large scale deployment of rogue firmware after hacking OEM backend servers	Penetration of OEM backend servers with the aim to initiate malicious firmware updates could lead to devastating results as this kind of attacks is highly scalable	High

DIAS

Generic high-level security requirements

Category	Generic high-level security requirements
1 – ECU (and general control units)	• Secure boot must be provided • secure software update • code signing • Specific events, such as software updates, should be stored in a tamper-proof log for audit

2 – Secure communication	• Data with security risk communicating over the CAN bus must be protected through authentication and for integrity
	• Hardware Security Module (HSM) must be used on the capable end nods such as the ECU/xCUs for enhanced security
	• Secure key generation, storage and exchange must be supported on the end nodes
	• Firewall and network intrusion detection system
	  • The white-listing and black-listing of traffic patterns
	  • Policy management based on access control
	  • Packet inspection at all the available layers
	  • Secure logging of detected events

3 - Backend	• Data with security risk communicating between a vehicle and the backend must be mutually authenticated and integrity protected • Data storage must be integrity protected • Data storage of important data must be confidential • The backend infrastructure must provide a secure mechanism for software and firmware updates

DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Thank you

Q & A

DIAS
SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS