Threat Modeling Report

Created on 19-Apr-25 10:33:16 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

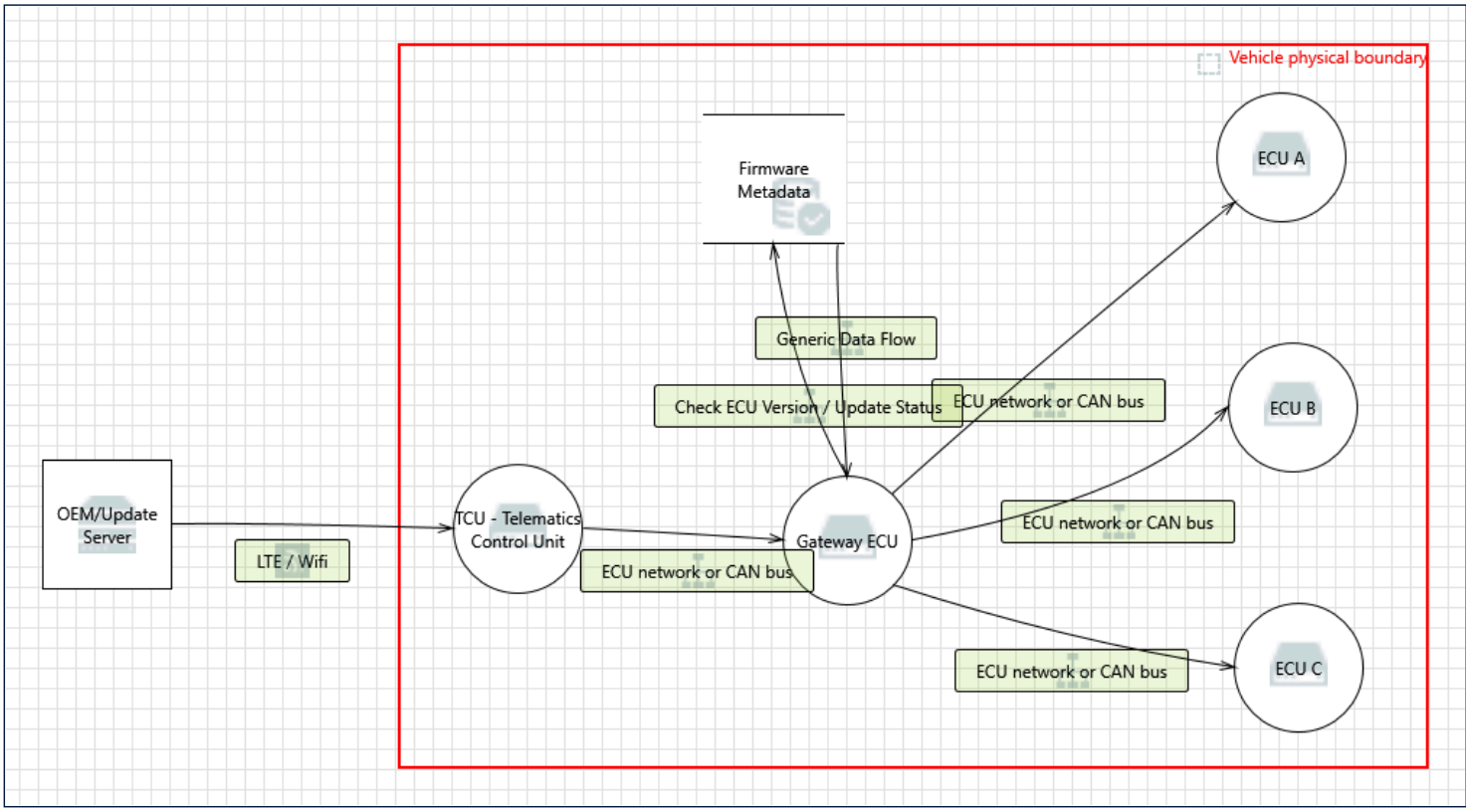
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	69
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	69
Total Migrated	0

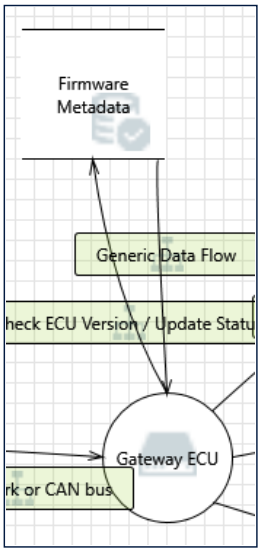
Diagram: Response



Response Diagram Summary:

Not Started	69
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	69
Total Migrated	0

Interaction: Check ECU Version / Update Status



1. Gaining unauthorised access to files or data [State: Not Started] [Priority: High]

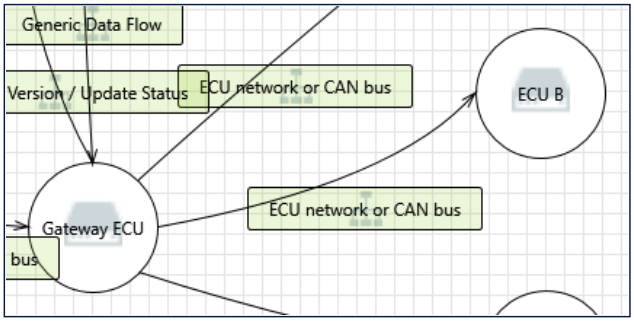
Category:	Information Disclosure
Description:	Gaining unauthorised access to files or data
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action via communication channel with direct effect on vehicular network
Access Method:	Single-hop | Physical : x | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Data confidentiality breach : x | Other, including criminality : x

2. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability

Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

Interaction: ECU network or CAN bus



3. Compromise of local/physical software update procedures. This includes fabricating system update program or firmware [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Compromise of local/physical software update procedures. This includes fabricating system update program or firmware
Justification:	<no mitigation provided>
Category of threat:	Update process used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action on software updates which has direct effect on ECU performance/ vehicle behavior
Access Method:	Single hop | Physical : x
Attack propagation:	ECU : 1 | Infotainment system : 1 | Hosted 3rd party software : 1
Potential outcome of attack:	

4. Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Data compromised at vehicle
Access Method:	Single- Hop | Physical : N/A | Remote : N/A
Attack propagation:	Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x | V2X communications : x

Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

5. Unauthorised changes to system diagnostic data [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Unauthorised changes to system diagnostic data
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Affected asset is the data(vehicle diagnostic data) stored within the vehicle.
Access Method:	Single-hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

6. Introduce malicious software or malicious software activity [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Introduce malicious software or malicious software activity
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/Direct/ Cascading
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Single-hop/ Multi-Hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

7. Fabricating software of the vehicle control system or information system [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Fabricating software of the vehicle control system or information system
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Outcome | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

8. Combination of short encryption keys and long period of validity enables attacker to break encryption [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Combination of short encryption keys and long period of validity enables attacker to break encryption
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

9. Insufficient use of cryptographic algorithms to protect sensitive systems [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Insufficient use of cryptographic algorithms to protect sensitive systems
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

10. Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software) [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software)
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

11. Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack

Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	If the vehicle asset is engineered to enable an attack or lacks design criteria to stop an attack then the cause of the issue is a factor that is internal to the system in consideration, which would make this entry a vulnerability
Access Method:	Single hop | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Remotely operated vehicle systems : 1 | External server : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

12. Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

13. Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) to gain access to ECUs or gain higher privileges [State: Not Started] [Priority: High]

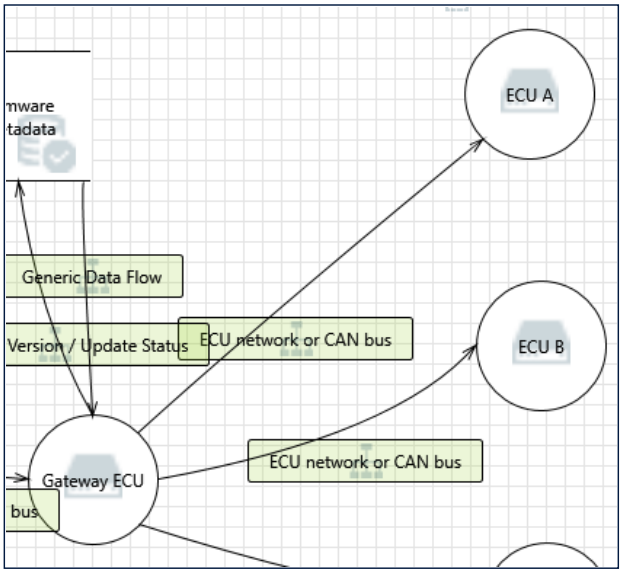
Category:	Elevation Of Privilege
Description:	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) to gain access to ECUs or gain higher privileges
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Other ports : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

14. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service

Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

Interaction: ECU network or CAN bus



15. Compromise of local/physical software update procedures. This includes fabricating system update program or firmware [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Compromise of local/physical software update procedures. This includes fabricating system update program or firmware
Justification:	<no mitigation provided>
Category of threat:	Update process used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action on software updates which has direct effect on ECU performance/ vehicle behavior
Access Method:	Single hop | Physical : x
Attack propagation:	ECU : 1 | Infotainment system : 1 | Hosted 3rd party software : 1
Potential outcome of attack:	

16. Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Data compromised at vehicle
Access Method:	Single- Hop | Physical : N/A | Remote : N/A
Attack propagation:	Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x | V2X communications : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

17. Unauthorised changes to system diagnostic data [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Unauthorised changes to system diagnostic data
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Affected asset is the data(vehicle diagnostic data) stored within the vehicle.
Access Method:	Single-hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

18. Introduce malicious software or malicious software activity [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Introduce malicious software or malicious software activity
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/Direct/ Cascading
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Single-hop/ Multi-Hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

19. Fabricating software of the vehicle control system or information system [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Fabricating software of the vehicle control system or information system
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle

Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Outcome | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

20. Combination of short encryption keys and long period of validity enables attacker to break encryption [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Combination of short encryption keys and long period of validity enables attacker to break encryption
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

21. Insufficient use of cryptographic algorithms to protect sensitive systems [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Insufficient use of cryptographic algorithms to protect sensitive systems
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

22. Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software) [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software)
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber

Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

23. Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	If the vehicle asset is engineered to enable an attack or lacks design criteria to stop an attack then the cause of the issue is a factor that is internal to the system in consideration, which would make this entry a vulnerability
Access Method:	Single hop | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Remotely operated vehicle systems : 1 | External server : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

24. Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

25. Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) to gain access to ECUs or gain higher privileges [State: Not Started] [Priority: High]

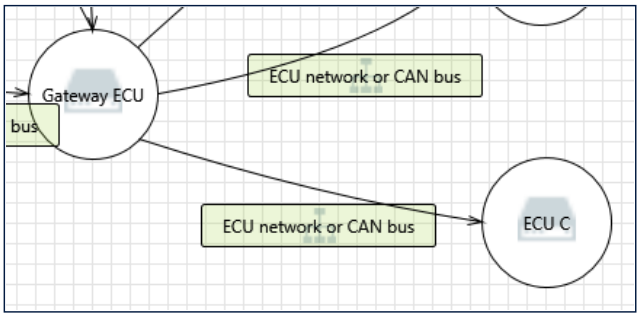
Category:	Elevation Of Privilege
Description:	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) to gain access to ECUs or gain higher privileges
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber

Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Other ports : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

26. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

Interaction: ECU network or CAN bus



27. Compromise of local/physical software update procedures. This includes fabricating system update program or firmware [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Compromise of local/physical software update procedures. This includes fabricating system update program or firmware
Justification:	<no mitigation provided>
Category of threat:	Update process used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action on software updates which has direct effect on ECU performance/ vehicle behavior
Access Method:	Single hop | Physical : x

Attack propagation:	ECU : 1 | Infotainment system : 1 | Hosted 3rd party software : 1
Potential outcome of attack:	

28. Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Data compromised at vehicle
Access Method:	Single- Hop | Physical : N/A | Remote : N/A
Attack propagation:	Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x | V2X communications : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

29. Unauthorised changes to system diagnostic data [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Unauthorised changes to system diagnostic data
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Affected asset is the data(vehicle diagnostic data) stored within the vehicle.
Access Method:	Single-hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

30. Introduce malicious software or malicious software activity [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Introduce malicious software or malicious software activity
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/Direct/ Cascading
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Single-hop/ Multi-Hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

31. Fabricating software of the vehicle control system or information system [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Fabricating software of the vehicle control system or information system
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Outcome | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

32. Combination of short encryption keys and long period of validity enables attacker to break encryption [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Combination of short encryption keys and long period of validity enables attacker to break encryption
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

33. Insufficient use of cryptographic algorithms to protect sensitive systems [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Insufficient use of cryptographic algorithms to protect sensitive systems
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

34. Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software) [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Using deprecated cryptographic algorithms (e.g. MD5, SHA-1) e.g. to gain access to ECUs (by signing and installing unauthorized software)

Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

35. Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	If the vehicle asset is engineered to enable an attack or lacks design criteria to stop an attack then the cause of the issue is a factor that is internal to the system in consideration, which would make this entry a vulnerability
Access Method:	Single hop | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Remotely operated vehicle systems : 1 | External server : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

36. Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

37. Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) to gain access to ECUs or gain higher privileges [State: Not Started] [Priority: High]

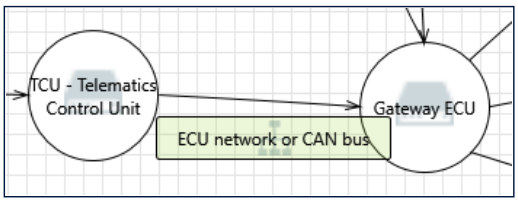
Category:	Elevation Of Privilege
Description:	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) to gain access to ECUs or gain higher privileges

Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Other ports : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

38. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

Interaction: ECU network or CAN bus



39. Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Data compromised at vehicle

Access Method:	Single- Hop | Physical : N/A | Remote : N/A
Attack propagation:	Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x | V2X communications : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

40. Unauthorised changes to system diagnostic data [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Unauthorised changes to system diagnostic data
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct
Reason/comments for classification/ threat path:	Affected asset is the data(vehicle diagnostic data) stored within the vehicle.
Access Method:	Single-hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

41. Introduce malicious software or malicious software activity [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Introduce malicious software or malicious software activity
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/Direct/ Cascading
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Single-hop/ Multi-Hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

42. Fabricating software of the vehicle control system or information system [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Fabricating software of the vehicle control system or information system
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome
Reason/comments for classification/ threat path:	Malicious software can be introduced into the vehicle network to compromise the normal operation of the vehicle, it can be also be seen as a first step of a cascading attack(E.g. to gain unauthorized access and manipulate data)
Access Method:	Outcome | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

43. Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a malicious payload [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a malicious payload
Justification:	<no mitigation provided>
Category of threat:	Target of an attack on a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Outcome/ Direct/ Cascading
Reason/comments for classification/ threat path:	Flooding the CAN bus is a direct form of DOS attack, where as using a malicious payload to provoke fault is a cascading attack
Access Method:	Single- hop | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

44. Combination of short encryption keys and long period of validity enables attacker to break encryption [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Combination of short encryption keys and long period of validity enables attacker to break encryption
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

45. Insufficient use of cryptographic algorithms to protect sensitive systems [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Insufficient use of cryptographic algorithms to protect sensitive systems
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : ? | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

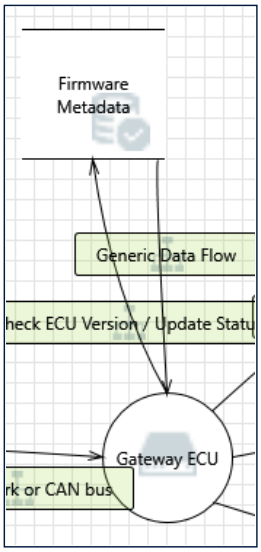
46. Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Software bugs. The presence of software bugs is a basis for potential exploitable vulnerabilities ... software bugs are more likely to happen than Hardware failures over the lifetime of a car
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Hosted 3rd party software : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

47. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

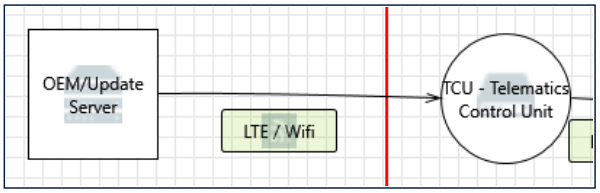
Interaction: Generic Data Flow



48. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

Interaction: LTE / Wifi



49. Man in the middle / session hijacking. [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Man in the middle / session hijacking.
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action via communication channel with direct effect on vehicular network
Access Method:	Multi-hop or Single hop | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

50. Accepting information from an unreliable or untrusted source [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Accepting information from an unreliable or untrusted source
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber

Threat effect:	Direct
Reason/comments for classification/ threat path:	Action via communication channel with direct effect on vehicular network
Access Method:	Multi-hop or Single hop | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

51. Introduce (write data code) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Introduce (write data code)
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action is via communication channel which directly impact the vehicle
Access Method:	Multi-hop or Single hop | Physical : x | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

52. Erase data/code [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Erase data/code
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action is via communication channel which directly impact the vehicle
Access Method:	Multi-hop or Single hop | Physical : x | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

53. Overwrite data/code [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Overwrite data/code
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action is via communication channel which directly impact the vehicle
Access Method:	Multi-hop or Single hop | Physical : x | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

54. Manipulate data/code [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Manipulate data/code
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action is via communication channel which directly impact the vehicle
Access Method:	Multi-hop or Single hop | Physical : x | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Other, including criminality : x

55. Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road) [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action is directly on the vehicle and affected asset is the vehicle.
Access Method:	Multi-hop(V2X network -> Vehicle network) or Single hop (infected device via OBD) | Remote : x
Attack propagation:	
Potential outcome of attack:	

56. Spoofing of messages (e.g. 802.11p V2X during platooning, GPS messages, etc.) by impersonation [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Spoofing of messages (e.g. 802.11p V2X during platooning, GPS messages, etc.) by impersonation
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action is directly on the vehicle and affected asset is the vehicle.
Access Method:	Multi-hop(V2X network -> Vehicle network) or Single hop (infected device via OBD) | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Other, including criminality : x

57. Information leakage or sharing (e.g. admin errors, storing data in servers in garages) [State: Not Started] [Priority: High]

Category:	Information Disclosure
Description:	Information leakage or sharing (e.g. admin errors, storing data in servers in garages)
Justification:	<no mitigation provided>
Category of threat:	Compromise of back-end server
Attack or Vulnerability:	Vulnerability
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Affected asset is the data stored in the server and not in vehicle
Access Method:	Single hop | Physical : x
Attack propagation:	External server : 1
Potential outcome of attack:	Data confidentiality breach : x | Other, including criminality : x

58. Transmission of false/unreliable/contaminated data to infrastructure [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Transmission of false/unreliable/contaminated data to infrastructure
Justification:	<no mitigation provided>
Category of threat:	Vehicle used as a means to propagate an attack Category agreed as out of scope due to vehicle needing to be compromised first
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Cascading
Reason/comments for classification/ threat path:	Data compromised at source(vehicle) and sent to connected infrastructure which has secondary effects
Access Method:	Multi-hop | Remote : x
Attack propagation:	V2X communications : 1
Potential outcome of attack:	Other, including criminality : x

59. Superfluous internet ports left open, providing access to network systems [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Superfluous internet ports left open, providing access to network systems
Justification:	<no mitigation provided>
Category of threat:	System design exploits (inadequate design and planning or lack of adaption)
Attack or Vulnerability:	Vulnerability

Type of entry:	cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : N/A | Remote : N/A
Attack propagation:	ECU : x | CAN bus : x | Gateway : x | Wider vehicle network : x | Infotainment system : x | Other ports : x
Potential outcome of attack:	Safe operation of vehicle affected : N/A | Vehicle functions stop working : N/A | Software modified, performance altered : N/A | Software altered but no operational effects : N/A | Data integrity breach : N/A | Data confidentiality breach : N/A | Other, including criminality : N/A

60. Interference with short range wireless systems or sensors [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Interference with short range wireless systems or sensors
Justification:	<no mitigation provided>
Category of threat:	Compromise of external connectivity
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct/Cascading
Reason/comments for classification/ threat path:	If the interference is with a V2X system, the attack effect is on the communication channel between the vehicle and infra(direct effect), which can in turn deny some V2X functions present in the vehicle(Cascading and Multi-hop path)
Access Method:	Single-hop or multi-hop | Physical : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

61. Manipulation of telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Manipulation of telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
Justification:	<no mitigation provided>
Category of threat:	Compromise of external connectivity
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action is on the remotely operated system which directly connects to the corresponding receiver system in the vehicle.
Access Method:	Single-hop | Physical : x | Remote : x
Attack propagation:	ECU : 4 | CAN bus : 3 | Gateway : 2 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | Remotely operated vehicle systems : 1 | External server : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

62. Compromise of over the air software update procedures, This includes fabricating system update program or firmware [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Compromise of over the air software update procedures, This includes fabricating system update program or firmware
Justification:	<no mitigation provided>
Category of threat:	Update process used to attack a vehicle

Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action on software updates which has direct effect on ECU performance/ vehicle behavior
Access Method:	Multi hop (OEM backend server network-> vehicular network) | Remote : x
Attack propagation:	OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | External server : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : 2.0 | Data confidentiality breach : 2.0 | Other, including criminality : 2.0

63. Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier) [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Cascading
Reason/comments for classification/ threat path:	Attack action on OEM backend infrastructure which in turn has a negative effect on the vehicular network
Access Method:	Multi-hop(Compromised proprietary network-> Compromised vehicle network) | Physical : x | Remote : x
Attack propagation:	ECU : 4 | CAN bus : 3 | Gateway : 2 | Wider vehicle network : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Other wireless : 1 | Radio antenna : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

64. Virus embedded in communication media infects vehicle systems [State: Not Started] [Priority: High]

Category:	Tampering
Description:	Virus embedded in communication media infects vehicle systems
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action via communication channel with direct effect on vehicular network
Access Method:	Single hop | Physical : x | Remote : x
Attack propagation:	ECU : 1 | Gateway : 1 | Infotainment system : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1
Potential outcome of attack:	

65. An unprivileged user gains privileged access, for example root access [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	An unprivileged user gains privileged access, for example root access
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack

Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Action via communication channel with direct effect on vehicular network
Access Method:	Single hop | Physical : x | Remote : x
Attack propagation:	ECU : 5 | CAN bus : 4 | Gateway : 3 | Wider vehicle network : 2 | Infotainment system : 2 | OBD port : 1 | End user interfaces : 1 | Other ports : 1 | Other physical access to vehicle networks : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Software modified, performance altered : x | Software altered but no operational effects : x | Data integrity breach : x | Data confidentiality breach : x | Other, including criminality : x

66. Interception of information / interfering radiations / monitoring communications [State: Not Started] [Priority: High]

Category:	Information Disclosure
Description:	Interception of information / interfering radiations / monitoring communications
Justification:	<no mitigation provided>
Category of threat:	Communication channels used to attack a vehicle
Attack or Vulnerability:	Attack
Type of entry:	cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	ENISA defines this threat as a physical threat where the attackers directly influences the in vehicular network
Access Method:	Single-hop | Remote : x
Attack propagation:	Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Data confidentiality breach : x | Other, including criminality : x

67. Jamming (via natural or unnatural interferences) of radio based (wireless) systems including navigation systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Jamming (via natural or unnatural interferences) of radio based (wireless) systems including navigation systems
Justification:	<no mitigation provided>
Category of threat:	Communication loss to/from vehicle (potentially out of scope as not cyber security)
Attack or Vulnerability:	Attack
Type of entry:	non-cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action is on the communication medium between the vehicle and the external device
Access Method:	Single- hop | Physical : x | Remote : x
Attack propagation:	Wider vehicle network : 2 | Infotainment system : 2 | Hosted 3rd party software : 2 | Other physical device : 2 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : ? | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x

68. Failures or disruptions of communications links, network outage or other systems (e.g. through disruptions of power/main supply) [State: Not Started] [Priority: High]

Category:	Denial Of Service

Description:	Failures or disruptions of communications links, network outage or other systems (e.g. through disruptions of power/main supply)
Justification:	<no mitigation provided>
Category of threat:	Communication loss to/from vehicle (potentially out of scope as not cyber security)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Direct
Reason/comments for classification/ threat path:	Attack action is on the communication medium between the vehicle and the external device
Access Method:	Single- hop | Remote : x
Attack propagation:	Wider vehicle network : 2 | Infotainment system : 2 | Hosted 3rd party software : 2 | Other physical device : 2 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : ? | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Vehicle functions stop working : x | Other, including criminality : x

69. Failures / malfunctions of (parts of) devices or systems [State: Not Started] [Priority: High]

Category:	Denial Of Service
Description:	Failures / malfunctions of (parts of) devices or systems
Justification:	<no mitigation provided>
Category of threat:	Non-cyber security vehicle threats (potentially out of scope)
Attack or Vulnerability:	Vulnerability
Type of entry:	non-cyber
Threat effect:	Vulnerability
Reason/comments for classification/ threat path:	
Access Method:	Vulnerability | Physical : x
Attack propagation:	ECU : 1 | CAN bus : 1 | Gateway : 1 | Wider vehicle network : 1 | Infotainment system : 1 | Hosted 3rd party software : 1 | Other physical device : 1 | Short range comms : 1 | Remotely operated vehicle systems : 1 | Immobiliser or security systems : 1 | TCU : 1 | TPMS : 1 | Paired mobile phone : 1 | Other wireless : 1 | External server : 1 | V2X communications : 1 | Radio antenna : 1 | Cellular Network : 1 | Other external system : 1
Potential outcome of attack:	Safe operation of vehicle affected : x | Vehicle functions stop working : x | Other, including criminality : x