DELIVERABLE 2.4: SECURITY AND PRIVACY IMPACT ANALYSIS

Version number:	1.0
Authors:	Dr. Fatih Özel & Mr Scott Cadzow
Activity lead	OECON
Supporting partners	C3L, VITKOVICE, ISKRATEL, IMR TECHNOLOGIES, SA CATAPULT
Due date:	31/12/2019
Delivery date:	11/12/2019
Delivery date updated document	

Co-financed by the Connecting Europe Facility of the European Union

This project is funded under the Connected Europe Fund Annual Programme
Grant agreement no. 2018-EU-TM-0079-S

CONTROL SHEET

Version history			
Version	**Date**	**Main author**	**Summary of changes**
0.1	18.07.2019	Dr. Fatih Özel	Added privacy assessment section
0.2	22.07.2019	Scott Cadzow	Initial text in security analysis section
0.3	03.10.2019	Scott Cadzow	Addition of quantitative analysis tables. Addition of e2e analysis. Correction of template
0.4	09.10.2019	Dr. Fatih Özel	Amendments to draft
0.5	10.10.2019	Scott Cadzow	More updates
0.6	6.11.2019	Scott Cadzow	Final draft proposal
1.0	22.11.2019	Scott Cadzow	Final draft submission
	Name		**Date**
Prepared	Dr Fatih Özel & Mr Scott Cadzow		18/07/2019
Reviewed	Andy Rooke		27/11/2019
Authorized	Andy Rooke		11/12/2019

TABLE OF CONTENTS

Control sheet 2

Table of contents 3

Tables 5

PURPOSE OF THE DOCUMENT 6

1 INTRODUCTION 7

1.1 sAFE Contractual References 7

1.1.1 Overview 7

1.1.2 Communication details of the Agency: 7

1.1.3 Communication details of the beneficiaries 7

Definitions of retrofit & after-market ecall systems 8

2 SECURITY ANALYSIS 11

2.1 Overview 11

2.2 Why security? 11

2.3 The application of TVRA to sAFE 13

2.4 sAFE - identification of security borders and objectives 17

2.4.1 Steps 1 through 3 of TVRA method 17

2.4.2 Steps 6 through 8 of the TVRA analysis 20

2.5 Regulatory compliance risks 21

2.6 Quantitative Risk Assessment 22

2.6.1 Introduction and method 22

2.6.2 Requirements arising from Regulation (EU) 2015/758 of the European Parliament and of the Council 22

2.6.3 Attacks on data addressed by CIA protections 22

3 PRIVACY (DATA PROTECTION IMPACT) ASSESSMENT 26

3.1 Introduction 26

3.2 Data Protection Impact Assessment Methodology: Article 35 of GDPR 26

3.3 Data Protection Impact Assessment 27

3.3.1 Impact of the Envisaged Processing Operations on the Protection of Personal Data 27

3.3.2 Advice of the Data Protection Officer 33

3.3.3 DPIA Requirement 33

3.3.4 Processing Operations (1) 33

3.3.5 Processing Operations (2) 33

3.3.6 Offering of Goods or Services to Data Subjects or to the Monitoring of Their Behaviour in Several Member States 34

3.3.7 Systematic Description of the Envisaged Processing Operations and Other Requirements 34

3.4 Conclusions 34

4 Conclusions and recommendations 36

4.1 Security 36

4.1.1 Conclusions of analysis 36
4.1.2 Recommendations resulting from analysis for future work 36
4.2 Privacy 37
4.2.1 Conclusions of analysis 37
4.2.2 Recommendations resulting from analysis for future work 38
REFERENCES 40

TABLES

TABLE 1: DIFFERENCES BETWEEN 112 ECALL AND TPS-ECALL SERVICES (REGIER ET AL., 2019). 31

Co-financed by the Connecting Europe Facility of the European Union

PURPOSE OF THE DOCUMENT

This document summarises the results of the work undertaken under the activity 2.4: Security and Privacy impact analysis. The requirements for this activity, as stated in the grant agreement are given below:

"This activity will consider the security implications for after-market 112 eCall, especially due to the increasing risk and prevalence of cyber threats. sAFE will conduct a study, building on the security assessment study for new vehicles in I_HeERO, but focussing on the after-market, where the potential for risk and vulnerability is increased. The study will look at the full end to end chain of the after-market 112 eCall, risks and vulnerabilities both current and future, real and potential will be analysed and solutions for risk mitigation will be proposed. The integrity of the eCall service relies on the use of a certified In-Vehicle System (IVS), secure network and well protected PSAP infrastructure. After-market of eCall increases the number of attack vectors originating from the IVS and the vehicle. In addition, in NG112 eCall, the transmission of the eCall traffic (voice and data) beyond the mobile network to the PSAP through fixed lines can be subject to additional cyber-attack. This work package will analyse the risks that eCall may be exposed to due to the after-market provisioning, along with the implication of current and future technologies. The study will also attempt to analyse the optimal balance between usability, security and safety. For example, an emergency call shall not be rejected because of missing or expired certificates. The interaction of after-market eCall with expectations of privacy shall also be examined. In this latter case the project shall include a summary Data Protection Impact Assessment (DPIA) consistent with the expectation of GDPR Article 35.".

Deliverable: D2.4 Security Analysis

1 INTRODUCTION

1.1 sAFE Contractual References

1.1.1 Overview

sAFE stands for After-market eCall For Europe.

sAFE is an action under the Grant Agreement number INEA/CEF/TRAN/M2018/1798161 with a project duration of 24 months, effective from 01 January 2019 until 31 December 2020. It is a contract with the Innovation and Networks Executive Agency (INEA), under the powers delegated by the European Commission.

1.1.2 Communication details of the Agency:

Any communication addressed to the Agency by post or e-mail shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)

Department C – Connecting Europe Facility (CEF)

Unit C3 Transport

B - 1049 Brussels

Fax: +32 (0)2 297 37 27

E-mail addresses:

for general communication: inea@ec.europa.eu

For submission of requests for payment, reports (except ASRs) and financial statements: INEA-C3@ec.europa.eu

Any communication addressed to the Agency by registered mail, courier service or hand-delivery shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)

Avenue du Bourget, 1

B-1140 Brussels (Evere)

Belgium

TEN-Tec shall be accessed via the following URL:

https://webgate.ec.europa.eu/tentec/

1.1.3 Communication details of the beneficiaries

Any communication from the Agency to the beneficiaries shall be sent to the following address:

OECON Products & Services GmbH: for the attention of Frank Brennecke

Hermann-Blenk-Straße 22a,

38108 Braunschweig,

Germany

E-mail address: brennecke@oecon-line.de

Definitions of retrofit & after-market ecall systems

Term	Expansion	Comments, observations
AH	Authentication Header	Part of the IPsec suite. Largely deprecated in favour of the ESP mode
	AFTER-MARKET eCall	The installation and/or use of a European 112-eCall system into a vehicle after the first use of the vehicle, that is not a retrofit eCall system but that independently provides the European 112 eCall service.
	AFTER-MARKET TPS-eCall	The installation and/or use of a third party eCall system into a vehicle after the first use of the vehicle, that is not a retrofit eCall system but that independently provides a TPS- eCall service.
	RETROFIT eCall	The installation by a vehicle manufacturer or its authorised agent, prior to first sale of a vehicle, or after the first sale of a vehicle, of an eCall in-vehicle system, approved for use in another model of vehicle, or otherwise satisfactorily certified to meet regulatory performance and conformance, that meets the requirements for the specific eCall retrofit type
C-ITS	Co-operative ITS	The variant of ITS in which each enabled vehicle (or station) broadcasts details of its type and location. On receipt the string of messages may be processed to enable advanced safety and awareness services (e.g. collision warning and avoidance)
CAV	Co-operative and Autonomous Vehicles	
CIA	Confidentiality, Integrity and Availability	
ComSec	Communications Security	Those security technologies dealing with data in transit from A to B
CSA	Cyber Security Act	To be formalised in regulation in 2019 and leading to a number of provisions in assurance of security for consumer and industrial networked devices (IoT, IIoT, …)
DTLS	Datagram Transport Layer Security	A VPN technology developed by Cisco
eSIM	Embedded SIM	A hardware security module for cellular network access designed for permanent installation in a device
ESP	Encrypted Secure Payload	Mode of operation of IPsec that provides each of confidentiality, integrity and identity protection
ETSI	European Telecommunications Standards Institute	One of the EU's 3 recognised official standards bodies. Involved in all aspects of ICT standardisation. Open membership model.
GDPR	General Data Protection Regulation	Regulation that enshrines many of the OECD provisions for protection of private data in law

geo-fence	—	Reference to a scheme of filtering by limiting activities to only be allowed within a defined (fenced) geographic area
HSM	Hardware Security Module	
IEC	International Electrotechnical Commission	Global standards body dealing with (primarily) large electrical equipment
IPsec	Internet Protocol Security	
ISO	International Standards Organisation	Global standards body dealing with almost everything traded across borders
ITS	Intelligent Transport Systems	
MAC	Message Authentication Code	Generally refers to a cryptographic hash that is encrypted with a shared symmetric key
MPPE	Microsoft Point-to-Point Encryption	Microsoft developed technology for VPNs
NAT	Network Address Translation	Gateway protocol that allows a single IP-address/port-pair to be mapped to multiple IP-address/port-pairs. Often used to isolate address space of a LAN from the wider internet
OpSec	Operational Security	Everyday maintenance of security and thus considers how to resolve breaches, how to patch/fix systems, staff selection and such like
PhySec	Physical Security	The physical security of devices and includes such things as tamper proofing, tamper evidence, and things like the provision of hardware roots of trust
PIP	Policy Information Point	
PKC	Public Key Certificate	
PKI	Public Key Infrastructure	
PPP	Point to Point Protocol	
PPTP	Point to Point Tunnelling Protocol	
SIM	Subscriber Identity Module	The smart-card application used in cellular networks to carry the user identity (IMSI) and associated security credentials independently of the communications device (phone, identified by the IMEI)
SSH	Secure Shell	
SSL	Secure Socket Layer	
SSTP	Microsoft Secure Socket Tunnelling Protocol	

TCP	Transport Control Protocol	Connection oriented mode of transferring data across an IP connection
TLS	Transport Layer Security	
TPM	Trusted Platform Module	
TSS	TPM Software …	
TVRA	Threat Vulnerability Risk Analysis	
UDP	Universal Datagram Protocol	Connectionless mode of transferring data across an IP connection
UICC	Universal Integrated Circuit Card	The generic term for the “smart-card” used in SIMs and banking cards. The UICC is the platform that supports applications such as SIM or Banking.
VPN	Virtual Private Network	

2 SECURITY ANALYSIS

2.1 Overview

The present document is the output of an analysis of the security implications of deploying after-market devices for support of the regulated 112 eCall.

The analysis presented in the current document builds on the security assessment study for new vehicles in I_HeERO, but with an altered focus on the after-market, where the potential for risk and vulnerability may be altered.

The integrity of the eCall service relies on the use of a certified In-Vehicle System (IVS), secure network and well protected PSAP infrastructure. The scope of the certification of the IVS from a security stance is addressed in the present document, as is the means to install an IVS when it is originated as an after-market device (i.e. where the IVS certification has 2 parts – the base eCall unit, and the installation to become an IVS).

After-market eCall devices modify the form and viability of attack vectors originating from the IVS and the vehicle as integration is not assured by the vehicle manufacturer. In addition, in NG112 eCall, the transmission of the eCall traffic (voice and data) beyond the mobile network to the PSAP through fixed lines can be subject to additional cyber-attack. This work package presents the results from a Threat Vulnerability Risk Analysis of after-market eCall. This addresses risks that may be exposed due to the after-market provisioning, along with the implication of current and future technologies. The results present the analysis of scenario building to determine the optimal balance between usability, security and safety. For example, an emergency call shall not be rejected because of missing or expired certificates. The interaction of after-market eCall with expectations of privacy is examined in detail in section 3 although this section does consider the impact of security provisions (especially those surrounding identification and liability) on privacy. In this analysis it is reinforced that the right to privacy is not absolute but is considered as qualified right (i.e. in the event of an incident, such as those that trigger an eCall, it is reasonable that the PSAP and the attending professionals can make reasonable requests for private and other identifying data and should not require explicit detailed consent (in other words the greater good statements of GDPR Article 6.1.d and 6.1.e apply)).

2.2 Why security?

The purpose of security technology is to manage risk and, as a consequence, assist in managing liability when things go awry. Key to understanding of where to apply security technology is understanding where there is risk to the system. Conventionally the undertaking of a security risk analysis is a fairly complex task requiring expert knowledge and some degree of iterative analysis of scenarios wherein the roles of system under attack and attacker are played against each other. There are a number of methods of undertaking a risk analysis that include the ETSI Threat Vulnerability Risk Analysis (TVRA) approach, various approaches in the ISO 27000 series of security management standards, the ISO/IEC 15408 series of Common Criteria standards, and others developed in part from the CIS-Controls (also published by ETSI) including schemes from Cisco, Microsoft, Apple and many others. What all of these tend to have in common is a simple calculation of risk as the product of impact of loss and likelihood of loss. Once an understanding of risk of a simple (unprotected) system is known then the designer determines where to place countermeasures to bring the risk to an acceptable level. The residual risk will then determine to some extent the degree of liability that has to be managed in the system, in other words having assessed the risk, applied mitigations to the risk, there is a remaining degree of risk that has to be managed.

Conventionally, security is considered in terms of breaches or loss. Cyber-security is somewhat specialised as theft can be achieved by copying whilst keeping the original where it was, disruption can be caused by misconfiguration, but the primary difficulty is often that there is limited visibility of an attack compared to the non-cyber world. Compare somebody breaking into a locked building with breaking into a computer. In the former there are often clear physical signs of the break-in and forensic evidence left at the scene of crime. In the cyber world there is rarely any trace of physical damage and forensic evidence is often difficult to find and quite often straightforward to conceal. A cyber security framework has to not just make it difficult to break-in to systems, but also has to make it difficult to conceal the event. The technology of successful cyber security is often based on the mathematical certainties of cryptography but of itself cryptographic tools do not make a system secure.

If a system has assets that need to be protected, then it is essential to be able to identify, for each asset, who has access to it (by some formal identity management scheme), and for what purpose. Access should be made hard at both the cyber and the physical level. Security should be multi-layered. The intent is similar in some ways to a Russian doll model where access to the next doll requires solving a different problem. So physically secure access and provide traps that inform when that level is breached and follow this model down through the system. Every level will be breached but to get to the golden nugget at the core of the system, no level should be by passable (to get to the asset every level or layer of protection has to be broken), and as levels get breached the defence forces are informed to be able to take additional measures.

A few caveats apply to security that need to be recognised:

- Security can never be absolute - it is only ever sufficient to thwart a certain type and intensity of attack for a particular period of time
- Added on security rarely, if ever, can be up to the task of protecting the asset. There are really only 2 ways to protect an asset: Redesign it to remove its vulnerabilities; Mask it from exposing its vulnerabilities. Most security features, those required to minimise risk, are masking features. The risk calculation (product of value of the asset and the likelihood of attack) will always assume that high value assets cannot be made into low value assets, so the design strategy is to lower the likelihood of attack on the asset.
- Security by obscurity will not work in the long term, in other words how the system is secured should be open to scrutiny
- Risk may be considered as synonymous with liability - whoever determines the residual risk also has responsibility to manage the system to ensure that that risk is managed and to accept liability when the system is breached

In communications systems in general the paradigm to be followed is the CIA (Confidentiality, Integrity and Availability) one where the core message is to know who is trying to do something and to ensure that they have authority to do it. This is captured in the “Availability” tag and this captures a set of knowledge that includes identity management, access control, reliability, resilience. Integrity is often synonymous with proof that the data transferred is free from manipulation but when placed alongside Availability also addresses provenance (i.e. where data came from).

Underpinning all of security is the concept of trust. Simplistically security is based on a series of assertions that are provable, when using cryptography the proof is mathematically sound. For example in digital signature the recipient trusts that the claimant who signs a document is really the holder of the private key, this trust is in part enabled in a public key infrastructure by the issuer of the certificate: If you trust the issuer of a certificate to have performed some checks of the key holder to, for example, store the private key in such a way that it cannot be transferred to another party (or, worse, cloned and given to another party), then you trust, by knowing the issuer of the public key certificate, the holder of the private key to be who they claim.

2.3 The application of TVRA to sAFE

A quantitative risk analysis is presented in the following sub-sections with the intent of giving assurance to any future security audit, such as those mandated under GDPR, and to be cited in the various approaches to certification that are going to result from implementation of the Cyber Security Act.

The normal steps in such an analysis (the TVRA method defined in ETSI TS 102 165-1 is used for this purpose) have been somewhat assumed and a summary is given below.

1. Identification of the Target of Evaluation (TOE) resulting in a high-level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.
2. Identification of the objectives resulting in a high-level statement of the security aims and issues to be resolved.
3. Identification of the functional security requirements derived from the objectives from step 2.
4. Inventory of the assets as refinements of the high-level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.
5. Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.
6. Quantifying the occurrence likelihood and impact of the threats.
7. Establishment of the risks.
8. Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.
9. Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.
10. Specification of detailed requirements for the security services and capabilities from step 9

In the particular case of an after-market eCall device certain security provisions have been made by design (i.e. the PLMN connection shall follow the provisions established by the carrier, the security provisions of the eCall itself shall be identical for both IVS and after-market provisions).

The eCall service has a small number of security services defined. The after-market eCall unit shall support all the IVS based eCall functions including any for security. The MSD (Minimum Data Set) is defined in EN 15722 and the content is shown in the various pictures from CSI-UK copied below. It should be noted that it is possible to initiate

an eCall with only the timestamp and VIN in the content (all other data fields, even where mandatory, can be set to convey no information).

MSD			
msdVersion	INTEGER (1..255)	M	MSD format version The format described in this document carries version 2 *See 6.1.3 for detailed information.*
Msd			
msdStructure			
messageIdentifier	INTEGER (1..255)	M	Message identifier, starting with 1 for each new eCall transaction and to be incremented with every application layer MSD retransmission following a new 'Send MSD' request after the incident event
Control		M	
automaticActivation	BOOLEAN		true = Automatic activation false = Manual activation
testCall	BOOLEAN		true = Test call false = Emergency
positionCanBeTrustd	BOOLEAN		true = Position can be trusted false = Low confidence in position "Low confidence in position" shall mean that there is less than 95 % confidence that exact position is within a radius of ± 150 m of reported position

VIN[1]	VIN[1]	M	VIN number according to ISO 3779
vehiclePropulsionStorageType		M	*Contains information about the presence of propulsion storage inside the vehicle sending the MSD.*
gasolineTankPresent	BOOLEAN		true = present; false = not present If no information about the propulsion storage is known, all elements should be set to FALSE.
dieselTankPresent	BOOLEAN		
compressedNaturalGas	BOOLEAN		
liquidPropaneGas	BOOLEAN		
electricEnergyStorage	BOOLEAN		
hydrogenStorage	BOOLEAN		
otherPropulsionStorage	BOOELAN		
timeStamp	INTEGER (0..2^{32}-1) sec	M	Timestamp of the initial data message generation within the current eCall incident event. NOTE 1 The timestamp is represented in seconds elapsed since midnight January 1st, 1970 UTC. NOTE 2 The initial message generation immediately follows the eCall generation sequence subsequent to a (confirmed) trigger. NOTE 3 Subsequent transmissions within the given incident use the same timestamp, but the messageIdentifier changes. NOTE 4 Failure value for time stamp set to "0"
vehicleLocation		M	*The last known vehicle position determined at the latest moment possible before message generation.*
positionLatitude	INTEGER (-2^{31}..2^{31}-1) milliarcsec		Position latitude (WGS84) calculation example: *48.3003333 = 48°18'1.20" N = 48*60*60.000" + 18*60.000" + 1.20" = 173881.200" = 173881200 milliarcsec* maximum value: 90°00'00.000" = 324000000 minimum value: -90°00'00.000" = -324000000 If latitude is invalid or unknown, the representation of value 2147483647 shall be transmitted.

[1] The field is named vehicleIdentificationNumber in the ASN.1 definition. The ASN.1 type VIN is defined in Annex A and codes for a correct representation of the World Manufacturer Index (WMI), the Vehicle Type Descriptor (VDS) and the Vehicle Identification Sequence (VIS) that make up a VIN number, taking into account the preconditions of each part.

vehicleDirection	INTEGER (0..255)	2° (2 degree)	M	The vehicle's last known real direction of travel (expressed in 2°-degrees steps from magnetic north (0– 358, clockwise) determined at the latest moment possible before message generation. calculation example: *due North = 0° = 0 * 2°* *due East = 90° = 45 * 2° => 45* *due South = 180° = 90 * 2°* *due West = 270° = 135 * 2°* The direction shall be unaffected by random fluctuations of GNSS signals. If direction of travel is invalid or unknown, the representation of value 255 shall be transmitted
recentVehicleLocationN1			O	*Known location of the vehicle some time before the generation of the data for the MSD message.* The recent location shall be chosen such that they could normally assist the receiving party to confirm the current location of the vehicle in different driving environments such as city or motorway.
latitudeDelta	INTEGER (-512..511)	100 milliarcsec		Latitude Delta (+ for North and – for South; WGS84) with respect to vehicleLocation. 1 Unit = 100 miliarcseconds, which is approximately 3m (on Earth) maximum value: 511 = 0°0'51.100" (±1580m) minimum value: -512 = -0°0'51.200" (± -1583m)
longitudeDelta	INTEGER (-512..511)	100 milliarcsec		Longitude Delta (+ for East and – for West; WGS84) with respect to vehicleLocation. *See latitudeDelta for details*

recentVehicleLocationN2			O	Known location of the vehicle some time before recentVehicleLocationN1. The recent location shall be chosen such that they could normally assist the receiving party to confirm the current location of the vehicle in different driving environments such as city or motorway.
latitudeDelta	INTEGER (-512..511)	100 milliarcsec		Latitude Delta (+ for North and – for South) with respect to recentVehicleLocationN1. *See recentVehicleLocationN1.latitudeDelta for details*
longitudeDelta	INTEGER (-512..511)	100 milliarcsec		Longitude Delta (+ for East and – for West) with respect to recentVehicleLocationN2. *See recentVehicleLocationN1.latitudeDelta for details*
numberOfPassengers	INTEGER (0..255)		O	Number of occupants in the vehicle according to available information. This information is indicative only as it may be not always be reliable in providing exact information about the number of passengers (e.g. because seatbelts may not be fastened by passengers or seatbelts may be fastened for other reasons). If no information about the number of occupants is available, this parameter needs to be omitted or filled with the representation of value 255
optionalAdditionalData			O	
oid	RELATIVE-OID			*See 6.1.5*
data	OCTET STRING			See *6.1.5*

2.4 sAFE - identification of security borders and objectives

2.4.1 Steps 1 through 3 of TVRA method

As noted above the ToE is key to identifying the suite of security countermeasures. As has also been noted the ToE is the boundary where everything inside the boundary is protected and attacks come from outside the boundary. The after-market eCall unit is one such bounded system, the PSAP is another bounded system. The eCall unit is connected and configured through a number of open interfaces, the PSAP is connected to another set of systems through open interfaces.

To populate the eCall with the mandated data set the eCall unit has to have access to geolocation (e.g. GNSS), dynamic vehicle data (e.g. data from the vehicle systems (e.g. CANbus, OBD2 port)), passenger cell data (e.g. number of passengers from vehicle systems, passenger recognition, manual input) and may require other data to ensure both voice and data connectivity.

Assumptions are as follows:

- eCall connects to the PSAP through the PLMN using available cellular technology
- an eCall unit is recognised as a legitimate PLMN subscriber (i.e. it is equipped with a SIM (or eSIM))
- an eCall unit is registered to, identified and authenticated to the PLMN
- an eCall unit has no roaming restriction (enabled by the PLMN)
- an eCall unit does not signal itself as an integrated IVS (by the vehicle manufacturer) or any other possible variant
- the corollary is that the PSAP is unable to determine the nature of the eCall unit from data present in the eCall
- the PSAP is a physically secured domain with vetted staff
- the PSAP records all incoming calls (eCall and all other emergency service requests)
- the PLMN has native ability to protect signalling and data from consumer terminals (including eCall units) from interception, masquerade and manipulation at the radio interface and inside the core network

The assumptions above influence the determination of the boundary. The other main consideration is the determination and documenting of objectives. The following are the primary objectives to be met by the **security** elements of an after-market eCall system:

1. Data entered (by the user) to configure the system should be tested for plausibility
2. Data transferred to the PSAP from the sAFE unit (after-market eCall unit) should be protected from manipulation by an adversary
3. The PSAP should be able to identify the sAFE unit as an eCall unit (semantic identifier)
4. eCall collision detection should be validated by multiple independent sources (e.g. airbag deployment detection, accelerometer threshold detection)

An after-market eCall unit cannot modify the base security expectations or provisions of the integrated eCall, i.e. an after-market eCall unit shall not impose an additional security burden on PSAPs.

In very simple terms the eCall system consists of 3 elements:

1. The eCall unit (either as a manufacturer installed and certified IVS, or as a combination of after-market device and certified installation to be treated as an IVS)
2. The PLMN and associated core telecommunications infrastructure (treated as a single entity)
3. The PSAP and associated emergency services units (treated as a single entity)

Whereas when conventional eCall is addressed the vehicle plus the unit is viewed as a single IVS the after-market eCall unit cannot be simply considered as equivalent to an IVS. From an attacker perspective the PLMN and PSAP may reasonably be considered as benign. However, the PLMN may be attacked by non-eCall units to drive calls towards the PSAP. Mitigations against such attacks are not considered in the present document.

Who is at risk? This is core to understanding of the need for security provisions.

Risks to the vehicle and its occupants are mostly likely from the following:

- Failure to recognise conditions necessary to trigger an eCall;
- Incorrect or incomplete data sent from the eCall unit to the PSAP;
- Incorrect recognition of conditions leading to false triggering of eCall (cry-wolf scenario);
- Once triggered having no access to the voice channel (assuming that there is no transmission of any sound from the site, including no ambient noise transmission).

The impact of each of these failures is either moderate or very high to the vehicle occupants. The level of control available to the vehicle occupants will to a large degree be device dependent, and to a lesser degree, installation dependent.

EXAMPLE 1: Reporting more than the actual occupancy of the vehicle may result in the responders wasting time attempting to find and recover people who are not there.

EXAMPLE 2: Incorrect report of GNSS coordinates may result in responders looking in the wrong place.

EXAMPLE 3: If the audio microphone and speaker become disconnected as a result of the triggering event the voice element of eCall will fail. The PSAP will be unable to verify with the affected persons the nature of the incident.

EXAMPLE 4: Under-reporting the actual occupancy of the vehicle and failing to report the numbers of affected people, property, infrastructure or vehicles may result in responders being inadequately resourced to deal with the incident.

NVH (Noise Vibration Harshness) concerns may be considered to dominate the likelihood of failure of an after-market eCall installation and may lead to loss of data integrity by loss of data connectivity. Of itself NVH protection is not generally considered as a security issue, rather it is a symptom of a wider reliability and availability issue. The general requirement is that the eCall unit shall be available to generate an eCall whenever the necessary trigger conditions are met. In addition data sources necessary to populate the data elements of the eCall shall be available at the beginning of the journey and to the triggering event and for some designated time period afterwards (it is assumed that an eCall event occurs during a journey (i.e. where the vehicle is actively involved in movement from A to B)). The underlying objective is that the installation of the after-market eCall device should not trigger an eCall event as a result of NVH issues at the installation site.

2.4.2 Steps 6 through 8 of the TVRA analysis

NOTE: The detail result of steps 4 and 5 of the TVRA method have been suppressed for this report as they are present by examination of the remainder of the steps and are implicit in the overall description.

Establishment of risk is determined by the product of impact of an attack (security breach) and the likelihood of the attack. The general assumption is that only malicious attacks are considered (i.e. where an attacker deliberately exploits a vulnerability in the system). Leaving aside motivation for now the metrics for determining likelihood of an attack are as follows (the wording in this summary can also be found in ETSI TR 103 534-1 and from ETSI TS 102 165-1):

- System knowledge:
  - Refers to the level of knowledge of the asset available to Eve and ranges from public information such as can be found on the internet , through to access to critical information about the asset (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking).

NOTE: As stated in TS 102 165-1 open source software is an example of asset design or implementation that is wholly in the public domain, however the level of risk represented by open source is tempered by the level of vulnerability it exhibits. There is some evidence that open source software is open to greater scrutiny when it comes to resolving errors.

- Time:
  - The amount of time Eve has to be able to access the system to identify that a particular, potential, weakness may exist, then to develop an attack method (threat agent) and to sustain effort required to mount the attack.

- Expertise:
  - This metric refers to the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows) required to attack the system. The levels of expertise to be applied within this factor range from laymen through to expert and includes consideration of teams of experts working together.

- Opportunity:
  - The metric for opportunity addresses the issue that identification or exploitation of a vulnerability may require considerable amounts of access to an asset, it is noted though that spending more time around the asset under attack may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the asset to exploit. Access may also need to be continuous, or for a specific number of sessions.

EXAMPLE: Historical examples include the Stuxnet attack on a particular make and model of industrial equipment that required direct physical access to the equipment. In contrast the Mirai botnet identified equipment without the attacker needing direct physical access, nor did the attacker have any knowledge of which specific IoT devices were exploited.

- Equipment:

- The metric for equipment addresses the form of equipment that Eve will need to exploit and range from standard (i.e. off the shelf with zero or minimal configuration) through to bespoke and multiple-bespoke equipment. There is an implicit link between expertise and equipment where it is often considered that an expert and motivated attacker is more likely to invest in bespoke or customised equipment.

A significant concern is that for certain models/implementations of an eCall unit the likelihood will vary. Thus, some assumptions have to be made regarding the nature of an eCall unit to arrive at a simplified base level. Hence assumptions about the operating system and physical nature of the device will be initially left out of the analysis, rather it is assumed that the eCall service shall be run on a hardened device with a somewhat hardened (or minimal) operating system

NOTE: In part this is to take out of the immediate reckoning those parts of an eCall service that are not directly impacted by the deployment environment. So for example building eCall into an Android operating system may result in different risks from building the same functional system it into a real time Unix variant, or a specialised hardware centric real time OS.

The nature of an attacker, and the motivation of the attacker, is an important dimension in assessing risk to the system. It may be that a motivated attacker will utilise eCall and other channels to overload a PSAP in order to inhibit calls related to another criminal activity. It is suggested that such motivations of attack cannot be resolved in the eCall unit or the wider eCall system but only by high level view of all traffic on both the telecommunications network and on the wider traffic network (it is a reasonable assumption that almost all eCall will be generated on or close to recognisable roads and whilst eCall may be triggered by off-road vehicles having incidents far from the recognised road network they are sufficiently rare or isolated to be seen as outliers).

2.5 Regulatory compliance risks

Any failure to comply to regulation by design is considered as an existential risk, i.e. the equipment **shall not** be allowed on the market.

Criteria	Assessment	Rationale
Impact assessment of any failure with respect to regulatory compliance	High	As noted above regulatory compliance failure bars equipment from market entry and can be classified as existential failure, i.e. with respect to the market the equipment does not exist
Likelihood assessment of any failure to achieve regulatory compliance	Low	Whilst this is not directly attributable as an attack from an adversary it is expected that the designer of the after-market eCall unit is cognisant of the regulatory environment and will take all reasonable steps to ensure compliance. In addition it is expected that a competent design authority

		shall take steps to confirm regulatory compliance prior to market entry. This is viewed as normal business practice and this attributed as low likelihood.

As mentioned in section 3 of the present document, specific compliance to the expectations of GDPR is addressed by 3.3.1.6 After-market 112-eCall Data Protection Provisions and in line with the risk assessment above no specific action is required.

In addition to GDPR other regulation will apply over the lifetime of the after-market eCall device that includes obligations under the Network Information Security Directive (NIS-D), the Cyber Security Act and others. In all cases the impact and likelihood analysis applies with a commensurate risk rating of medium.

The countermeasures for all regulatory compliance risks is to appoint a regulatory compliance officer with the authority to prevent shipment of any unit unless all compliance obligations have been met. In particular this applies to the Radio Equipment Directive (RED) statement of conformance and any necessary safety regulation deemed to apply to the equipment. With regards to the RED specific action may need to be taken to clarify the definition of the radio equipment, since the nature of installation may impact the boundary at which the equipment is deemed to be radio equipped.

2.6 Quantitative Risk Assessment

2.6.1 Introduction and method

The quantitative (and qualitative) risk analysis presented here follows, as far as is practical, the method described in ETSI TS 102 165-1. The intent is to identify the impact of an attack on the system and to determine the likelihood of the attack occurring. In addition the analysis addresses wider forms of attack that whilst not directly against the after-market eCall system, or the after-market eCall unit, may negatively impact the performance of the eCall service.

2.6.2 Requirements arising from Regulation (EU) 2015/758 of the European Parliament and of the Council

As is stated in section 3.3.1.2 of the present document there are specific measures that need to be taken to address the requirements outlined in Article 5 of the regulation.

An eCall unit is assumed to be continuously available and to have access to the PLMN. The concern raised in Article 5.1 over traceability by unauthorised entities is addressed in the PLMN standards and conformance to those standards ensures that only the relevant entities in the PLMN, those being the processes in the mobility management sub-system (that populate the VLR/VSS data record), have knowledge of the cell location of the eCall unit. There is no provision in PLMN for any unauthorised entity to have access to the GNSS based geographic location of the eCall unit contained in eCall signalling.

2.6.3 Attacks on data addressed by CIA protections

2.6.3.1 Summary of CIA protections

The long-standing CIA paradigm refers to provisions that assure the Confidentiality, Integrity and Availability of a service offered to Alice. The convention in this document is to refer to the primary parties as Alice and Bob (representing the eCall unit and PSAP respectively) and to refer to the adversary as Eve.

2.6.3.2 Attacks targeted to the eCall unit

As previously discussed, the eCall unit is largely assumed to be a closed device, however as the eCall unit is actively attached to the PLMN it may be open to attack by malicious actors to redirect data to an adversary.

NOTE: The eCall unit is not an active "phone" in the normal sense – it is a single function device which whilst a member of the PLMN roaming community (i.e. when registered to the PLMN it is visible on the VLR/VSS registers) is not expected to have a conventional keypad or address book to direct calls. Therefore, the user interface and storage mechanisms may be more restricted than a conventional phone.

An eCall unit has to implement the base ComSec capabilities necessary to connect to the PLMN and those required of the eCall legislation. This addresses concerns of authenticity (by authentication of the IMSI associated to the eCall unit and assigned by the PLMN), and, may enforce confidentiality of the content of transmissions on the radio interface from the eCall unit to the PLMN (subject to local legislation).

It is strongly suggested that the NVH threat is put aside at this point as the countermeasure for false triggering as a result of NVH issues is mechanically locked at the point of installation. Thus the countermeasure is likely to be mechanical to give assurance of immunity to NVH interference. A secondary measure for those after-market eCall units that are intended to be "permanent" installations may be to add a tamper-evident-seal to the unit after installation. For any eCall unit where installation is less permanent the likelihood of an NVH false trigger is too high to safely endorse such units. It is assumed that the mechanical integrity of the eCall unit is assured by the installation, i.e. that audio capability, antenna connections and base NVH countermeasures are sufficient to ensure that a triggering incident is faithfully reported.

Assuming an after-market eCall unit complies with the core standards and that there is a means to populate the data in the MSD (as defined in EN 15722) the concerns are summarised as follows:

- Manipulation of the MSD to present a false narrative of the vehicle and the triggering incident
- Leakage of MSD data to unauthorised entities (this addresses issues related to acquisition of personal data, of location and of behavioural data)

There are some operational risks related to the Availability attribute that need to be considered. These include the following lusted items:

- Manipulation of the core programming of the device

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
Manipulation of the MSD to present a false narrative of the vehicle and the triggering incident	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Specialized	3				

Threat Group	Attack					Impact	Risk
	Factor	**Range**	**Value**	**Potential**	**Likelihood**		
Leakage of MSD data to unauthorised entities	Time	≤ 1 week	1	8 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Specialized	3				
Manipulation of the core programming of the device	Time	≤ 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Standard	0				
	Time	≤ 1 day	0	12	2	3	6

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
Acquisition of personal information	Expertise	Proficient	2	(Moderate)	(Possible)	(High)	(Critical)
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Standard	0				
Acquisition of behavioural details	Time	≤ 1 day	0	18 (High)	1 (Possible)	2 (Medium)	2 (Major)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Difficult	12				
	Equipment	Specialized	3				
Acquisition of location information	Time	≤ 1 day	0	18 (High)	1 (Possible)	2 (Medium)	2 (Major)
	Expertise	Proficient	2				
	Knowledge	Restricted	1				
	Opportunity	Difficult	12				
	Equipment	Specialized	3				

2.6.3.3 Attacks targeted to the PSAP

The PSAP is the intended recipient of the eCall. There is nothing in the signalling, as identified in the MSD, to indicate that the eCall unit is an after-market device. There is nothing in the signalling field to give an indication (either by means of failure of verification of a cryptographic hash or of a conventional checksum) that data has not been manipulated. The broad assumption of the PSAP as a technical entity is that the provisions of the communications network are such that what is delivered is exactly as was sent by the eCall unit.

2.6.3.4 Attacks targeted to the core networks linking the eCall unit and PSAP

Whilst is may be considered as a trivial point it is important to stress that not all networks, and not all technologies, are competent to carry emergency calls. Only those networks competent and enforced by a national regulator, or licencing are considered. Any network that is not competent to handle such calls are out of scope of this document.

Attacks against emergency call handling require attack against the network core functionality. For the perspective of an after-market eCall service there is no additional risk over that offered for any other eCall service or any other emergency call service.

3 PRIVACY (DATA PROTECTION IMPACT) ASSESSMENT

3.1 Introduction

The eCall service requires the collection and transmission of data. However, personal data is protected by General Data Protection Regulation (GDPR) 2016/679 (EU, 2016) and additional data protection regulations specified for the eCall service (EU, 2015) These regulations limit the use of data for rescue operations only. It is prohibited to use data for other objectives or to pass data to a third party.

In this section, the results of an examination of the interaction of after-market eCall with expectations of privacy is therefore presented. The format of this section of the report is that of a data protection impact assessment (DPIA), with notes and extensions to address items not directly addressed in the reference method. The method is applied following the definition in EU GDPR (EU, 2016) article 35.

3.2 Data Protection Impact Assessment Methodology: Article 35 of GDPR

Article 35 of the EU GDPR 2016/679 (EU, 2016) identifies the requirements and the scope of a DPIA. It is noted in later parts of the present document that many of the required elements of a DPIA have been extensively addressed for eCall and the delta expressed for an after-market eCall have also been addressed. With reference to the obligations of Article 35 it is clear that the service provider is the party responsible for the conduct of the DPIA. In recognising that in this project (sAFE), the study refers to the provision of eCall as an abstraction layer rather than as a service for commercial use, the remainder of this section addresses primarily those aspects of a DPIA that are outlined in Article 35.3. More specifically the eCall service has been analysed with respect to assist data controllers in addressing their obligations under Article 35.

The following text (in italics) is quoted from the GDPR:

1. *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*
2. *The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*
3. *A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
    - *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
    - *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
    - *(c) a systematic monitoring of a publicly accessible area on a large scale.*
4. *The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*

5. *The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.*
6. *Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*
7. *The assessment shall contain at least:*
    (a) *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
    (b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
    (c) *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
    (d) *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*
8. *Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.*
9. *Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.*
10. *Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.*
11. *Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.*

3.3 Data Protection Impact Assessment

In the following sub-sections, each requirement from Article 35 of GDPR (EU, 2016), that was introduced in the previous section, has been examined in the context of eCall after-market systems to assist responsible parties (i.e. the designated data controller) in conducting a DPIA.

3.3.1 Impact of the Envisaged Processing Operations on the Protection of Personal Data

The first requirement of Article 35 of the EU GDPR 2016/679 (EU, 2016) states that

> *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of*

personal data. A single assessment may address a set of similar processing operations that present similar high risks"

It is therefore required that an assessment of the impact of the envisaged processing operations on the protection of personal data should be conducted for eCall after-market systems. Since eCall systems are already used in the European market and adequate data protection provisions for eCall systems are also in place (and have been assessed as adequate), the critical concern is to determine any differences with respect to data content, data handling, and data processing. However, before examining those differences, a summary of data protection provisions for the regulated eCall are discussed in the following sub-sections.

3.3.1.1 Article 29 Working Party: Working Document on Data Protection and Privacy Implications in eCall Initiative

A working party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy and its tasks were described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The working party created a working document (1609/06/EN WP125, 2006) in 2006 to outline data protection and privacy concerns arising in connection with the introduction of a harmonised pan European eCall service. The document (1609/06/EN WP125, 2006) not only recognised the socio-economic benefit that the eCall service could bring to citizens, but also addressed the privacy and data protection implications of eCall.

To address the privacy and data protection implications of eCall, the principle of eCall was firstly summarised. Secondly, eCall was analysed from the privacy and data protection point of view and legal reasoning, including mandatory and voluntary eCall services, security issues, databases, proportionality, nature of data controller as well as storage period. The document concluded that:

"From a data protection point of view, an emergency call released automatically by a device or triggered manually and transmitted via mobile networks resulting in geo-localization of the emergency event is in principle admissible, provided that there exists a respective specific legal basis and sufficient data protection safeguards are provided. However, the purposes of the emergency call system and the relevance of the data to be processed must always be taken into account, in particular if the processing involves the so-called Full Set of Data".

This judgement was provided before regulation EU GDPR 2016/679 (EU, 2016) although it is clearly stated in Article 94 of the GDPR that it assumes all prior provisions from the pre-existing directive with the following specific text:

"Directive 95/46/EC is repealed with effect from 25 May 2018.

"References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation."

Further, in Article 95 the relation to Directive 2002/58/EC is covered as follows:

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

3.3.1.2 The consequence of each of Articles 94 and 95 is that the opinions expressed by the Article 29 working party continue to apply.Commission Implementing Regulation (EU) 2017/78 of 15 July 2016

Another relevant regulation is (EU) 2017/78 of 15 July 2016 (EU, 2017). The regulation establishes administrative provisions for the EC type-approval of motor vehicles with respect to their 112-based

eCall in-vehicle systems and uniform conditions for the implementation of Regulation (EU) 2015/758 of the European Parliament and of the Council with regard to the privacy and data protection of users of such systems. Article 5 of the regulation outlines the privacy and data protection rules, as given below:

1. *"The manufacturer shall take the necessary measures to ensure that the 112-based eCall in-vehicle system or the 112-based eCall in-vehicle STU is not traceable and is not subject to any constant tracking in its normal operational status. The manufacturer shall further ensure that data in the internal memory of that system or STU is automatically and continuously removed and is not available outside the in-vehicle system or STU to any entities before the eCall is triggered.*
2. *The manufacturer shall inform the owner of the vehicle of the measures taken in accordance with Article 6(9) of Regulation (EU) 2015/758 by using the template set out in Part 3 of Annex I to this Regulation.*
3. *The manufacturer shall take appropriate safeguard measures (such as use of encryption technologies) to protect the security of personal data in the internal memory of the 112-based eCall in-vehicle system or 112-based eCall in-vehicle STU and to prevent surveillance and misuse. Such measures shall be appropriate, strictly proportionate to and necessary for the intended purpose".*

3.3.1.3 Regulation (EU) 2015/758 of the European Parliament and of the Council

Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC (EU, 2015) also set significant data protection rules, as given below:

> *"(21) Any processing of personal data through the 112-based eCall in-vehicle system should comply with the personal data protection rules provided for in Directive 95/46/EC of the European Parliament and of the Council (3) and in Directive 2002/58/EC of the European Parliament and of the Council (4), in particular to guarantee that vehicles equipped with 112-based eCall in-vehicle systems, in their normal operational status related to 112 eCall, are not traceable and are not subject to any constant tracking and that the minimum set of data sent by the 112-based eCall in-vehicle system includes the minimum information required for the appropriate handling of emergency calls. This should take into account the recommendations made by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC ('Article 29 Data Protection Working Party') and contained in its 'Working document on data protection and privacy implications in eCall initiative', adopted on 26 September 2006".*

The European Commission consulted again with Article 29 WP (1609/06/EN WP125, 2006) after the notification of the introduction of GDPR (EU, 2016) and were advised that there was no change required. In its communication (EC, 2018), the European Commission also stated that

> *"With the new rules, the function of eCall will become easier, simpler and more efficient in terms of data protection. It is a data protection principle that when personal data is collected for one or more purposes it should not be further processed in a way that is incompatible with the original purposes. This does not prohibit processing for a different purpose or restrict 'raw data' for use in analytics."*

3.3.1.4 Commission Delegated Regulation (EU) 2017/79 of 12 September 2016

This Regulation establishes detailed technical requirements and test procedures for the EC type-approval of the vehicles referred to in Article 2 of Regulation (EU) 2015/758 in respect of their 112-

based eCall in-vehicle systems and of 112-based eCall in-vehicle separate technical units ('STUs') and components.

In ANNEX VIII of the regulation, dedicated technical requirements and test procedures related to privacy and data protection are specified. It is expected that certification of aftermarket eCall devices will be similar to this dedicated regulation.

3.3.1.5 To sum up, in respect of regulated eCall, adequate data protection provisions are in place, and they have been deemed by the highest authority in Europe. Hence, the question is to establish any differences in data, data handling, and data processing in respect of retrofit and after-market eCall. In that context, these differences will be examined in the following sections for addressing the privacy and data protection implications. Retrofit eCall Data Protection Provisions

Although installed in different models or at a different time, retrofit eCall executes similar data transactions, data storage as well as data management as regulated in typical eCall systems, therefore no additional risk is incurred.

This data protection impact assessment therefore concludes that in respect of Retrofit eCall adequate data protection provisions are in place and have been deemed by the highest authority in EC in respect of these matters (Article 29 Working Party) and by formal EC Communication to be adequate in respect of GDPR.

3.3.1.6 After-market TPS-eCall Data Protection Provisions

Although the eCall initiative requires the car/device to be directly connected to 112 (Europewide single emergency number), other systems may offer separate emergency networks or other additional supports as well. These systems are called as third-party service (TPS) eCall. The main difference between TPS eCall and 112 eCall is that while the 112 eCall is directly connected to PSAPs and is aimed to be a public (free) service, TPS eCall alerts firstly go to a third party, where they are usually evaluated before addressing the relevant PSAPs in turn. TPS eCall systems are therefore usually paid services and are regulated by different European Standards (EN16102) compared to the public 112 eCall (EN16062 - High Level Application Protocols, EN16072 - Operating Requirements).

In terms of the data, TPS eCall services provided by car manufacturers do not have to comply with the strict regulations of eCall. As a consequence, TPS-eCall services can collect more information than regular eCall services. Moreover, whereas 112 eCall systems are activated only in an emergency case, TPS-eCall systems can be permanently online. Although some consumer protectors see this critical, being afraid that car manufacturer might be tempted to collect more data than necessary and make collected data available for additional commercial services, TPS-eCall need to comply with the standards and eCall IVS Regulations. A contract between vehicle owner and Third-Party Service Provider is also required, in which data handling, storage and access is an explicit consent in that contract. For a better understanding the differences between the two types of eCall services are demonstrated in the table below.

Table 1: Differences between 112 eCall and TPS-eCall services (Regier et al., 2019).

Categories	EU-eCall Service	TPS-eCall Services
Services	Only emergency calls	Emergency call service combined with additional services, e.g. tracking, regular calls to service centres
Regulations	Legislation adopted by the European Parliament. It contains clearly specified regulations regarding the collection and processing of data	Privat-law agreement with the customer based on data protection regulations.
Emergency call forwarding	Forwarding to the next local emergency call centre (112)	Forwarding to a privat call centre of the supplier
Data content	Datatypes are contained in the minimal data set of EU-eCall	Contains more data than the data contained in the minimal data set.
Call priority	Has the same priority like a phone emergency call.	Normal call without priority
Can the service be deactivated?	Not possible	Possible

In respect of after-market TPS-eCall, this is functionally identical to TPS eCall on regulated vehicles discussed above, and conformant to EN 16102 and eCall IVS Regulations. Both of them require that there is a contract between vehicle owner and Third-Party Service Provider in which data handling, storage and access is an explicit consent in that contract, which by itself, in any event, has to comply to GDPR. In that context, no additional risk is incurred. However, it is significant to mention that as TPS eCall is standardised and it is validated during type approval, a similar approach is required for after-market TPS-eCall

3.3.1.7 After-market 112-eCall Data Protection Provisions

In respect of after-market 112-eCall, the data transaction is identical to Regulated eCall. However, the user will have to get the relevant vehicle data populated into the IVS memory prior to first use.

Activity 3 may (or may not) determine that in some circumstances the MSD data may be less specific because of the risk of a user entering incorrect technical data. Nevertheless, the Regulation (EU) 2015/758 (EU, 2015) clearly determines the data protection issues regarding the MSD data, as given below:

> *"8. The MSD sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2011 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)'. No additional data shall be transmitted by the 112-based eCall in-vehicle system. That MSD shall be stored in such a way as to make its full and permanent deletion possible".*

Article 6 of the same regulation (EU, 2015), which outlines the rules on privacy and data protection also clarify that

1. *"This Regulation is without prejudice to Directives 95/46/EC and 2002/58/EC. Any processing of personal data through the 112-based eCall in-vehicle system shall comply with the personal data protection rules provided for in those Directives.*

2. *The personal data processed pursuant to this Regulation shall only be used for the purpose of handling the emergency situations referred to in the first subparagraph of Article 5(2).*
3. *The personal data processed pursuant to this Regulation shall not be retained longer than necessary for the purpose of handling the emergency situations referred to in the first subparagraph of Article 5(2). Those data shall be fully deleted as soon as they are no longer necessary for that purpose".*

In respect of data handling by the PSAP, Article 6 of the Regulation 305/2013 (EU, 2013) clearly identifies the rules on privacy and data protection for PSAPs, as given below:

1. *The PSAPs, including eCall PSAPs, shall be regarded as data controllers within the meaning of Article 2(d) of Directive 95/46/EC. Where the eCall data is to be sent to other emergency control centres or service partners pursuant to Article 3(5), the latter shall also be considered as data controllers. Member States shall ensure that the processing of personal data in the context of the handling of the eCall by the PSAPs, the emergency services and service partners is carried out in accordance with Directives 95/46/EC and 2002/58/EC, and that this compliance is demonstrated to the national data protection authorities.*

2. *In particular, Member States shall ensure that personal data are protected against misuse, including unlawful access, alteration or loss, and that protocols concerning personal data storage, retention duration, processing and protection are established at the appropriate level and properly observed".*

This data protection impact assessment therefore concludes that in respect of after-market 112- eCall, whose data is populated by the owner during installation and commissioning (i.e. not shared with any other third party) adequate data protection provisions are also in place and have been deemed by the highest authority in EC in respect of these matters (Article 29 Working Party) and by formal EC Communication to be adequate in respect of GDPR.

However, as the EN 15722 "Minimum Set of Data" includes technical data, such as the Vehicle Identification Number (VIN) of the vehicle and the UNECE category of the vehicle, it cannot be precluded that a vendor may offer to undertake populating the vehicle data onto the device as part of its service, or as an additional fee charged service. In either event that would entail the purchaser sharing his/her vehicle data with the vendor, and this, associated with the name and address of the purchaser, would, under GDPR, constitute personal data. In these circumstances, a vendor selling in Europe would be also bound by GDPR and would be required to handle such data in accordance with GDPR.

It cannot, however, be ruled out in these days of purchase via the internet, that the vendor may be located outside the EU. Whilst GDPR would technically apply to the service that is provided to the purchaser; enforcement may be more problematic. Nevertheless, the MSD itself does not contain personal data, and is only transmitted in the event of a crash and, as the transaction is the same as that for regulated eCall.

It may be argued that the VIN number of a vehicle can be traced to the vehicle keeper through the National Vehicle Registration Authority, and therefore might, under GDPR, be considered personal data. However, on the one hand, the National Vehicle Registration Authority is subject to GDPR, so it may be reasonably assumed that, as this data can only be associated with the vehicle keeper when obtained via the National Vehicle Registration Authority records, that those records are properly protected by the National Vehicle Registration Authority. On the other hand, there is no certainty that the registered keeper of the vehicle is the vehicle driver or is an occupant of the vehicle at the time of the incident. Hence, even such trace would be a speculative association at best. Further, as the vehicle is required by law to display registration plates, the association of registration plate to vehicle keeper would be a simpler association to make and, therefore, knowledge of the VIN adds little or nothing to risk (The MSD does not transmit the number plate information).

All in all, in respect of after-market 112-eCall, whose data is populated by the vendor or his agent prior to installation and commissioning, and any MSD data programmed does not in itself contain personal data, and, therefore, it does not present a significant additional personal data risk.

3.3.2 Advice of the Data Protection Officer

The second requirement of Article 35 of the EU GDPR 2016/679 (EU, 2016) states that

> *"2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment".*

This requirement is not directly applicable in the case of this report although as a matter of due diligence it is imperative that users/holders of eCall units are able to identify the data controller and the controlling authority for the data regime. Such data is normally available by labelling on the device, by labelling on the packaging of the device, or in specific parts of the user interface to the device. It is noted that failure to provide this marking may be a regulatory compliance error leading to a penalty. Thus, whilst the PSAP in general acts as the data controller for eCall the specific PSAP that will receive data cannot be determined prior to invocation of the eCall itself.

3.3.3 DPIA Requirement

The third requirement of Article 35 of the EU GDPR 2016/679 (EU, 2016) states that

> *"3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
>
> *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
>
> *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
>
> *(c) a systematic monitoring of a publicly accessible area on a large scale".*

The risks described in (a) are precluded by the decision no 585/2014/EU of the European Parliament and of the Council (EU, 2014) as it strictly controls the use and retention of data by PSAPs. Other risks described in (b) and (c) are not applicable in the case of eCall and eCall after-market systems.

3.3.4 Processing Operations (1)

The fourth requirement of Article 35 of the EU GDPR 2016/679 (EU, 2016) states that

> *"4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68".*

This requirement is governed by eCall regulations, particularly EU 305-2015 and EC 585-2014 (EU, 2014) in respect of PSAPs, and EU 2017-758 in the case of IVS.

3.3.5 Processing Operations (2)

The fifth requirement of Article 35 of the EU GDPR 2016/679 (EU, 2016) require that:

> *"5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board".*

Similar to the previous requirement, this requirement is also governed by eCall regulations, mainly EU 305-2015/EC 585-2014 in respect of PSAPs, and EU 2017-758 in the case of IVS.

3.3.6 Offering of Goods or Services to Data Subjects or to the Monitoring of Their Behaviour in Several Member States

The sixth requirement of Article 35 of the EU GDPR 2016/679 (EU, 2016) is given below:

> *"6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union".*

This requirement is also governed by eCall regulations, particularly EU 305-2015/EC 585-2014 in respect of PSAPs, and EU 2017-758 in the case of IVS.

3.3.7 Systematic Description of the Envisaged Processing Operations and Other Requirements

Other requirements of Article 35 of the EU GDPR 2016/679 (EU, 2016) are also given below:

> *"7. The assessment shall contain at least:*
>
> *(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
>
> *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
>
> *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
>
> *…….*
>
> *11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations".*

The requirements described in 7 (a) and (b) are documented and standardised in EN 16072 and EN 15722 documents. For other requirements except than the 11th requirement, section 2.3.3 summarises the results. 11th requirement is also not appropriate within the context of this study, as explained in the section 2.3.3, no or minimal increase in risk can be identified.

3.4 Conclusions

In this section, the interaction of after-market eCall with expectations of privacy were discussed by conducting a DPIA. The method applied followed that defined in EU GDPR (EU, 2016) article 35. It was found that:

- eCall systems are already used in European market and adequate data protection provisions for regulated eCall systems are in place, including:
  - *PSAPs:* EU 305-2013 and EC 585-2014 (the use and retention of data by PSAPs)
  - *IVS privacy and data protection rules:* EU 2017-78
  - *MSD data protection rules:* EU 2015/758
- There are also standards for the regulated eCall services:
  - *EN 16072:* systematic description of the envisaged processing operations and the purposes of the processing
  - *EN 15722:* assessment of the necessity and proportionality of the processing operations in relation to the purposes (i.e. data protection issues regarding MSD)
  - *EN 16102:* Operating requirements for third party support

- The differences in data, data handling, and data processing for after-market eCall systems were therefore explored, and following conclusions were made:
    - *Retrofit eCall:* As it has same data transaction, data storage as well as data management as regulated eCall, no additional risk is incurred.
    - *After-market TPS-eCall:* Functionality is identical to TPS eCall on regulated vehicles, and conformant to EN 16102 and eCall IVS Regulations. There needs to be a contract between vehicle owner and Third-Party Service Provider in which data handling, storage and access is an explicit consent in that contract. As the contract also has to comply to GDPR, no additional risk is incurred.
    - *After-market 112-eCall:* The data transaction is identical to Regulated eCall. However, the user will have to get the relevant vehicle data populated into the IVS memory prior to first use. As the programmed MSD data does not contain personal data, it does not represent significant additional personal data risk.

4 Conclusions and recommendations

4.1 Security

4.1.1 Conclusions of analysis

The general conclusion is that if an after-market eCall unit is compliant to the measures defined for an IVS eCall unit there is no additional risk when viewed from the connected PSAP.

The most glaring concern is that an after-market eCall unit may be susceptible to false triggering of eCall by the nature of the installation. The risk is significant when viewed as the likelihood of a poor installation. This is particularly true for nomadic devices (i.e. devices that can be moved from vehicle to vehicle), as opposed to fully installed devices (i.e. devices that once installed are not designed for removal).

4.1.2 Recommendations resulting from analysis for future work

4.1.2.1 Two stage validation of unit

An eCall unit has to be recognisable an such and this should be properly attested to. From a security perspective an eCall unit is a critical safety device and within the structure of the Cyber Security Act[1] should be classified with a security assurance level of at least "substantial" and ideally at level "high". Such a security classification should be clearly marked on the device and the provenance of the granting of such a classification should be visible and verifiable both prior to installation and at any time during operation.

With a properly marked eCall unit as above it should then be subject to a regulated or controlled installation procedure such that it can be shown that the MSD data set is correctly derived from the vehicle and that false triggers by poor isolation of NVH issues is negated.

For a device complying to the cyber security act assurance level of "high" the proof of assurance may need to be performed post installation.

4.1.2.2 Vulnerability disclosure process

Every manufacturer and the supply chain should operate a vulnerability disclosure policy. This is addressed at some length in TS 103 645 and a process is specified in ISO/IEC 29147. In undertaking such a policy there is a core requirement to continuously assess vulnerability and to describe the process by which updates are provided. This is tied into the recommendation for mutability and crypto agility given below.

4.1.2.3 Provisions for mutability of security functionality and countermeasures (crypto-agility)

It is recognised that security provisions should be mutable to address new and modified attacks on the system. It is also recognised that network technologies are not static but are under continuous development. In the domain of eCall or emergency call provision the role of the core network to deliver the call (voice and data) from the eCall unit to the PSAP will always be maintained but no assumptions should be made regarding the nature of the intervening technology. Thus whilst some networks will be built using a switching fabric (primarily circuit mode) others will use a wholly packet routing fabric, some networks will be wholly physical, some will be wholly virtualised (i.e. the function assigned to a

[1] https://eur-lex.europa.eu/eli/reg/2019/881/oj . Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

specific hardware element is determined by the software it is running at any particular point in time, such as the model of VNF).

Whilst eCall is a voice service with some data provided via a side-channel the level of cryptographic protection that can be provided is recognisably limited. Any device level protection however has to be designed with the recognition that it may be broken and as such may need to be updated (see also vulnerability disclosure policy above).

4.1.2.4 End to end integrity and source verification

The core conceit of eCall is that a trusted device calls a trusted PSAP and the call is routed through a trusted network. A properly installed device will not make false calls and the likelihood of false data presents a low risk (the content of the MSD is confirmed in the voice call).

As eCall and the supporting networks evolve the role of trust also evolves to the point where the primary trust relationship will be between the PSAP and the eCall unit. This requires consideration to be given to evolve towards an end-to-end security model which lowers the expectation of the carrier networks to be trusted. This has only limited impact for a voice based eCall but may be essential for a data centric eCall in the future.

4.1.2.5 Provision of HSM at eCall unit

The more security provisions that are made in the eCall unit then the greater the need to tie that provision into the hardware. This is a consequence of the long-term evolution of eCall, of the increasing requirements of the Cyber Security Act, and of the need to ensure any personal data is fully protected (as a consequence of the GDPR).

4.2 Privacy

4.2.1 Conclusions of analysis

Re-stating some of the text found in section 3.4 with the primary findings highlighted in **Bold**:

- eCall systems are already used in European market and **adequate data protection provisions for regulated eCall systems are in place**, including:
    - *PSAPs:* EU 305-2013 and EC 585-2014 (the use and retention of data by PSAPs)
    - *IVS privacy and data protection rules:* EU 2017-78
    - *MSD data protection rules:* EU 2015/758
- With respect to any delta in data and data processing for after-market eCall systems:
    - *Retrofit eCall:* As it has same data transaction, data storage as well as data management as regulated eCall, **no additional risk is incurred**.
    - *After-market TPS-eCall:* Functionality is identical to TPS eCall on regulated vehicles, and conformant to EN 16102 and eCall IVS Regulations. There needs to be a contract between vehicle owner and Third-Party Service Provider in which data handling, storage and access is an explicit consent in that contract. As the contract also has to comply to GDPR, **no additional risk is incurred**.
    - *After-market 112-eCall:* The data transaction is identical to Regulated eCall. However, the user will have to get the relevant vehicle data populated into the IVS memory prior to first use. As the programmed MSD data does not contain personal data, it **does not represent significant additional personal data risk**.

It can therefore be clearly stated that as regards any privacy risk there is no additional impact from provision of an after-market eCall unit.

4.2.2 Recommendations resulting from analysis for future work

The only issue of relatively minor concern is that the user has to get relevant vehicle data into the IVS memory. This may introduce errors but as there is no personal data this is not a direct privacy concern. The user interface to the unit that allows the user to enter data should therefore be designed in such a way that the introduction of errors is reduced. This may be achieved using strongly linked data and wherever possible limiting the number of selections to be made by the user-programmer.

Co-financed by the Connecting Europe Facility of the European Union

REFERENCES

1609/06/EN WP125 (2006) *Article 29 Working Party: Working document on data protection and privacy implications in eCall initiative*. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf (Accessed: 16 July 2019).

EC (2018) *European Commission (EC) - Fact Sheet: Questions and Answers. General Data Protection Regulation, Press release database*. Available at: http://europa.eu/rapid/press-release_MEMO-18-387_en.htm (Accessed: 16 July 2019).

EU (2013) *Commisssion Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall, Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R0305&from=GA (Accessed: 16 July 2019).

EU (2014) *Decision no 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service, Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014D0585&from=EN (Accessed: 17 July 2019).

EU (2015) *Regulation (EU) 2015/758 of the European Parliament and of the council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC, Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R0758&from=EN (Accessed: 18 July 2019).

EU (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 in the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN (Accessed: 17 July 2019).

EU (2017) *Commission Implementing Regulation (EU) 2017/78 of 15 July 2016 establishing administrative provisions for the EC type-approval of motor vehicles with respect to their 112-based eCall in-vehicle systems and uniform conditions for the implementation of Reg*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0078&from=EN (Accessed: 18 July 2019).