TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 17875

December 2022

ICS 03.220.20; 13.200; 35.240.60

English Version

Intelligent transport systems - eSafety - Incident Support Information System (ISIS) Architecture

Systèmes de transport intelligents - eSafety - Architecture du système d'information sur la prise en charge des incidents (ISIS)

Intelligente Verkehrssysteme - ESicherheit - Abstützen bei Vorfällen Informationssystem (ISIS) Architektur

This Technical Specification (CEN/TS) was approved by CEN on 30 October 2022 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 17875:2022 E

Contents

Page

Introduction 4
1 Scope 6
2 Normative references 6
3 Terms and definitions 6
4 Symbols and abbreviations 8
5 Conformance 9
6 Phases of the ISIS 9
6.1 Summary of phases 9
6.2 Phase 1: Instigation 10
6.3 Phase 2: Initiation 11
6.3.1 Nature of the Communication 11
ISO 5616 “ITS Secure Interface” architecture 11
6.3.2 Architectural Foundation of the “Secure ITS Data Management and Access Interface” 11
6.3.3 Global Transport Data Format 16
6.3.4 ISIS in the context of the Secure Interface for data access 17
6.3.5 Security Authentication 19
6.3.6 Call establishment 29
6.4 Phase 3: Multiple Provider Management 29
6.5 Phase 4: Establish capability 30
6.6 Phase 5: Search and offering 30
6.7 Phase 6: Data/service provision 30
6.8 Phase 7: Shutdown provisions 30
6.9 Phase 8: Terminate ISIS 30
7 Service Provision Architecture 31
Bibliography 33

European foreword

This document (CEN/TS 17875:2022) has been prepared by Technical Committee CEN/TC 278 “Intelligent transport systems”, WG15 eSafety, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Introduction

A 112-eCall is an incident alert system, specified in Regulation 305/2013/EC and Regulation 758/2015/EC, which specify that the 112-based eCall in-vehicle system " *'eCall' means an in-vehicle emergency call to 112, made either automatically by means of the activation of in-vehicle sensors or manually, which establishes a 112-based audio channel between the occupants of the vehicle and a PSAP over which it sends a minimum set of data as defined in EN 15722 to the PSAP and subsequently opens the audio channel for dialogue between the PSAP and the occupants of the vehicle".* The PSAP instigates response by sending emergency responders to the scene, talks with the occupants of the vehicle if possible, and at some point at the PSAP's choosing, terminates the eCall.

A 112-eCall is described as an incident alert system, because

a) it is a call between a vehicle and a Public Service Answering Point;

b) Regulation 758/2015 specifies (Article 6 (8)) that *"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: 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)'. No additional data shall be transmitted by the 112-based eCall in-vehicle system*, "; and

c) Regulation 758/2015 further specifies (whereas (15)) *Manufacturers shall ensure that the 112-based eCall in-vehicle system and any additional system providing TPS eCall* or an added-value service *are designed in such a way that no exchange of personal data between them is possible.*

eCall therefore, by Regulatory definition, terminates once emergency responders have been activated and the PSAP elects to terminate the call (in some circumstances that may only be when the responders arrive on the scene of the incident, but in most cases, well before).

EU CEF Project sAFE, and CEF Project I-HeERO before it, identified that as in-vehicle technology advances, new opportunities to provide additional helpful data to emergency responders arise. Data from cameras and sensors can be of significant assistance to emergency responders. Project iHeERO identifies:

— *Additional sensor information could be*

  — *Cameras (video or still image)*

  — *Special sensors e.g. gas or leakage*

  — *Passenger detection sensors*

and

1. PSAP operator initiates a query to get a list of all accessible data sources (including sensors) on the vehicl

2. The IVS accepts the request and posts all available data sources including sensors

3. PSAP notes that an internal camera in the cabin is available for query

But does not say how this is to be achieved. We know that because of the Regulation, it will not be achieved by the PSAP in the eCall, and Activity (3.6) of project sAFE has identified that

a) The crucial participants to this action are the affected vehicle (and its occupants) and the 'emergency responders' – the paramedic and police etc., who arrive on the scene to handle the incident (not the PSAP [although in some 112 response configurations the level 1 PSAP may remain in contact or control until the incident is concluded]).

b) This information support is not an eCall, but a post eCall incident support activity between the emergency responders and vehicles at the scene of the incident and their occupants.

It is further observed, though not elsewhere commented in the main body of the sAFE project report, that aerial drones are increasingly being used to provide information to emergency responders. Providing the opportunity to link these devices with these other new capabilities therefore also makes sense.

However, rather than a loose indication of what might happen next, this document proposes the architecture to provide an 'Incident Support Information System' ISIS.

The objective of the ISIS at the highest level is shown in Figure 1.

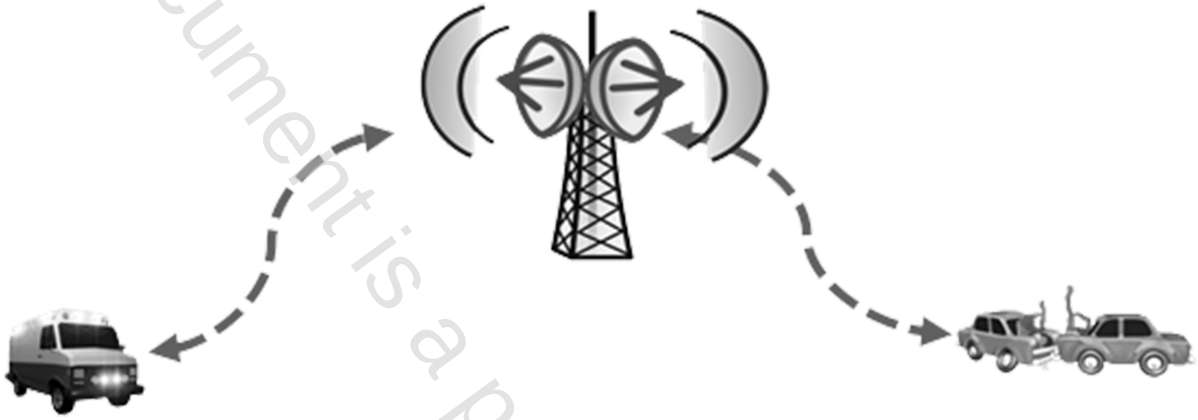

Figure 1 — ISIS –1 – Architecture - Objective

1 Scope

This document describes the architecture of a secure process flow between a source ITS system and a destination ITS system to provide an 'incident support information system' (ISIS) to emergency responders by accessing (with the agreement of the vehicle owners/keepers) data from a crashed vehicle and/or other vehicles, or drones, in the vicinity of the incident.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/DIS 21177, *Intelligent transport systems — ITS-station security services for secure session establishment and authentication between trusted devices*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1
bounded secured managed domain
ITS-stations

Note 1 to entry: The ITS-station concept provides for secure peer-to-peer communications between entities that are themselves capable of being secured and remotely managed; while this is an abstract definition, it has very specific physical consequences; the bounded nature is derived from the requirement for ITS-stations to be able to communicate amongst themselves, i.e. peer-to-peer, as well as with devices that are not secured; realising that to achieve this in a secure manner often requires distribution and storage of security-related material that must be protected within the boundaries of the ITS-station, leads to the secured nature of the entity; thus ITS-stations are referred to as bounded secured managed domains (BSMD).

3.2
data
representations of static or dynamic objects in a formalized manner suitable for communication, interpretation, or processing by humans or by machines

Note 1 to entry: In packet switched networks, voice is carried in packets of data.

3.3
data concept
any of a group of *data* structures (i.e. object class, property, value domain, *data elements*, message, interface dialogue, association) referring to abstractions or things in the natural world that can be identified with explicit boundaries and meaning and whose properties and behaviour all follow the same rules