# IEC TS 62580-2

Edition 1.0 2016-06

# TECHNICAL SPECIFICATION

colour inside

## Electronic railway equipment – On-board multimedia and telematic subsystems for railways –
## Part 2: Video surveillance/CCTV services

IEC TS 62580-2:2016-06(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

**About the IEC**
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

**About IEC publications**
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

**IEC Catalogue - webstore.iec.ch/catalogue**
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

**IEC publications search - www.iec.ch/searchpub**
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

**IEC Just Published - webstore.iec.ch/justpublished**
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

**Electropedia - www.electropedia.org**
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

**IEC Glossary - std.iec.ch/glossary**
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

**IEC Customer Service Centre - webstore.iec.ch/csc**
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TS 62580-2

Edition 1.0 2016-06

# TECHNICAL SPECIFICATION


## Electronic railway equipment – On-board multimedia and telematic subsystems for railways –
## Part 2: Video surveillance/CCTV services

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 45.060

ISBN 978-2-8322-3413-6

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# ELECTRONIC RAILWAY EQUIPMENT – ON-BOARD MULTIMEDIA AND TELEMATIC SUBSYSTEMS FOR RAILWAYS –

## Part 2: Video surveillance/CCTV services

## FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a Technical Specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical Specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC TS 62580-2, which is a Technical Specification, has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

The text of this specification is based on the following documents:

| Enquiry draft | Report on voting |
|---|---|
| 9/2112/DTS | 9/2151A/RVC |

Full information on the voting for the approval of this Technical Specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62580 series, published under the general title *Electronic railway equipment – On-board multimedia and telematic subsystems for railways*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

# INTRODUCTION

The IEC 62580 series defines on-board multimedia and telematic sub-systems (OMTS) for railways, so as to achieve interoperability between subsystems in the same vehicle and between subsystems in different vehicles of the same train.

The on-board video surveillance/CCTV system is a subsystem of OMTS, providing services for on-board surveillance and the security issue of the train and passengers. It serves as the crucial source of information for train operator, security organizations and first responders. The basic system functionality contains video/audio capture, recording, retrieval, replay, display, etc.

This Technical Specification will be useful to those responsible for establishing operational requirements, writing specifications, selecting devices, installing, commissioning, using and maintaining the on-board video surveillance/CCTV system. This specification is divided into the following sections:

a) system breakdown: divides the on-board video surveillance/CCTV system into four components based on their functionality, including video capture component, video storage component, video display component and video analysis component;

b) function breakdown: gives the function list that system may offer from the user's point of view, and presents the function blocks of system according to the functional breakdown, which includes video environment, system management and system security. Within video environment, it contains the basic functions that system could provide, such as to capture video, to record video, to retrieve video, to export video, to replay video, to display video, to analyse video and manage interconnection;

c) requirements: describes the requirements of video environment, system management and security as well as video transmission in which transmission performance, protocol and IP interoperability implementation based on Web service have been introduced;

Some use cases of the on-board video surveillance/CCTV system are given in Annex A.

# ELECTRONIC RAILWAY EQUIPMENT – ON-BOARD MULTIMEDIA AND TELEMATIC SUBSYSTEMS FOR RAILWAYS –

## Part 2: Video surveillance/CCTV services

## 1 Scope

This part of IEC 62580, which is a Technical Specification, specifies the on-board video surveillance/CCTV system functionality and requirement for the purpose of interoperability between components of on-board video surveillance/CCTV systems in the same vehicle and subsystems in different vehicles of the same train, which means two levels of interoperability are considered, one is interoperability between components and another is between subsystems.

This specification gives guidelines for:

- system breakdown structure of the on-board video surveillance/CCTV system;
- function breakdown structure of the on-board video surveillance/CCTV system, and
- requirement of the on-board video surveillance/CCTV system.

This specification is applicable to any type of train, for example open trains, multiple unit trains and closed trains.

As illustrated in Figure 1, this part of IEC 62580 provides video surveillance/CCTV services of monitoring, recording and retrieval of data, etc. This specification follows the general OMTS requirement defined in IEC 62580-1. The communication network of on-board video surveillance/CCTV system is based on the network defined by the IEC 61375 series, in which IEC 61375-2-5 and IEC 61375-3-4 define communication between and within consists, respectively, IEC 61375-2-3 lays out the communication profile for the backbone which is used for the train coupling, and IEC 61375-2-6[1] provides the support for the communication between on-board system and ground wayside infrastructures. The general system requirement of on-board video surveillance/CCTV system is developed based on IEC 62676 series with supplementing the special requirement for railway application. For interoperability implementation between components of system and subsystems, this specification makes reference to IEC 62676-2-3, which specifies a compliant IP video protocol and interface based on Web services. Special requirements for railway, such as device discovery between consists and within a consist, as well as network compliant to the IEC 61375 series are also defined here. In addition, IEC 62676-4 gives recommendations and requirements for the selection, planning, installation, commissioning, maintaining and testing for use in security applications. Finally, the requirement of exported data of on-board video surveillance/CCTV system is compliant with ISO 22311 if system is for security purpose.

---

1 Under consideration.

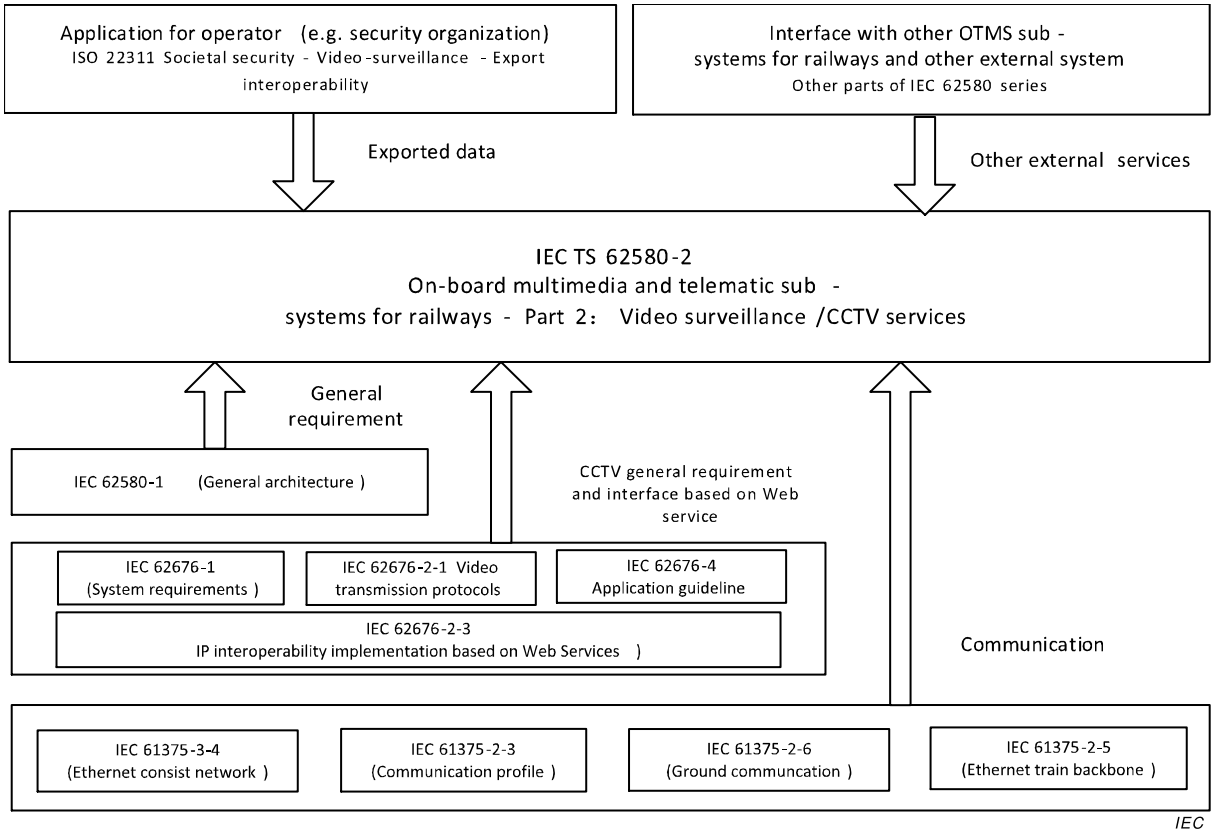



**Figure 1 – Relation of IEC TS 62580-2 with other standards**

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61375 (all parts), *Electronic railway equipment – Train communication network (TCN)*

IEC 61375-2-3:2015, *Electronic railway equipment – Train Communication Network (TCN) – Part 2-3: TCN communication profile*

IEC 61375-2-5, *Electronic railway equipment – Train Communication Network (TCN) – Part 2-5: Ethernet Train Backbone*

IEC 61375-2-6 [2], *Electronic railway equipment – Train Communication Network (TCN) – Part 2-6: On-board to ground communication*

IEC 61375-3-4, *Electronic railway equipment – Train Communication Network (TCN) – Part 3-4: Ethernet Consist Network (ECN)*

IEC 62580-1:2015, *Electronic railway equipment – On-board multimedia and telematic subsystems for railways – Part 1: General architecture*

2 Under consideration.

IEC 62676-1-1:2013, *Video surveillance systems for use in security applications – Part 1-1: System requirements – General*

IEC 62676-1-2:2013, *Video surveillance systems for use in security applications – Part 1-2: System requirements – Performance requirements for video transmission*

IEC 62676-2 (all parts), *Video surveillance systems for use in security applications – Part 2: Video transmission protocols*

IEC 62676-2-3:2013, *Video surveillance systems for use in security applications – Part 2-3: Video transmission protocols – IP interoperability implementation based on Web services*

ISO 22311, *Societal security – Video-surveillance – Export interoperability*

IEEE 802.1Q, *IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks*

RFC 2326, *Real Time Streaming Protocol (RTSP)*

RFC 3016, *RTP Payload Format for MPEG-4 Audio/ Visual Streams*

RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*

RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*

RFC 3984, *RTP Payload Format for H.264 Video*

*FERRIS, C., KARMARKAR, A, YENDLURI, P., WS-I, Basic Profile Version 2.0 – Working Group Draft, October 2007 (available at* http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html).

# 3 Terms, definitions and abbreviations

## 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61375-1, IEC 62580-1 and IEC 62676-1-1, as well as the following apply.

**3.1.1**
**alarm**
warning of the presence of any hazard to life, property or the environment

**3.1.2**
**camera IO**
video capturing devices involved in analogue capture devices with Codec and IP capture devices (digital capture devices)

**3.1.3**
**compression**
reduction in the number of bits used to represent an item of data

**3.1.4**
**control plane**
media control functions, such as device control, and media configuration commands

**3.1.5**
**consist**
single vehicle or group of vehicles which are not separated during normal operation, and which contains no, one or several consist networks

**3.1.6**
**data identification**
capability to find, retrieve or delete specific data without ambiguity

**3.1.7**
**data integrity**
condition when data has not been modified or altered from its source either maliciously or by accident and in which data are maintained during any operation, such as transmission, storage, and retrieval, in order to preserve data for their intended use

**3.1.8**
**data management**
management of user-actions, audio-/video-data and general information that are not part of the activity management

**3.1.9**
**event**
incident in the real world

**3.1.10**
**frame rate**
numbers of frames per second

**3.1.11**
**function**
application process which exchanges messages with another application process

**3.1.12**
**gateway**
connection between different communication technologies

**3.1.13**
**train location**
specific location of a train defined by one of several means to represent its latitude, longitude, altitude as well as relative coordinates in a rail network

**3.1.14**
**image**
visible representation of a frame as rectangular grid of pixels

**3.1.15**
**image handling**
any activity that transforms an input image into an output image with as little changes as possible

**3.1.16**
**incident**
occurrence or activity of interest that on-board video surveillance/CCTV system is intended to view or record and which may need a response by an operator

**3.1.17**
**integrity**
property of a system to recognize and to reject wrong data in case of malfunction of its parts

**3.1.18**
**JPEG**
common standard for image compression

Note 1 to entry: This common standard for image compression was defined by the Joint photographic experts group.

**3.1.19**
**latency time**
time delay between the moment something is initiated, and the moment one of its effects begins

Note 1 to entry: The time from the source sending a signal to the destination receiving it.

**3.1.20**
**media plane**
media stream, such as video, audio and metadata

**3.1.21**
**network**
set of possibly different communication systems which interchange information in a commonly agreed way

**3.1.22**
**open train**
train composed of a set of consists, where the configuration may change during operation

Note 1 to entry: International UIC trains are an example of open trains.

**3.1.23**
**operator**
authorized user operating on-board video surveillance/CCTV system for intended purpose

**3.1.24**
**receiver**
electronic device which may receive signals from the physical medium

**3.1.25**
**resolution**
pixels per inch or number of pixels of a video-frame, monitoring device or print out

**3.1.26**
**recording**
container for a set of audio, video and metadata tracks

Note 1 to entry: A recording can hold one or more tracks. A track is viewed as an infinite timeline that holds data at certain times.

**3.1.27**
**service**
capabilities and features of a component of subsystem or subsystem provided to a user

**3.1.28**
**streaming**
process of sending video over a network to allow instant operation as the video is received, rather than requiring the entire file to be downloaded prior to operation

**3.1.29**
**system security**
protection of the system against failures as tampering, illegal access, vandalism.

Note 1 to entry: The system security controls physical or electronic access to on-board video surveillance/CCTV system or any component to prevent unauthorised access.

**3.1.30**
**topology**
possible cable interconnection and number of devices a given network supports

**3.1.31**
**track**
individual data channel consisting of video, audio or metadata

**3.1.32**
**train communication network**
TCN
data communication network for connecting programmable electronic devices on on-board rail vehicles

**3.1.33**
**train backbone**
bus connecting the vehicles of a train and which conforms to the TCN protocols

### 3.2 Abbreviations

| | |
|---|---|
| CCTV | closed circuit television |
| DHTP | dynamic host configuration protocol |
| CS | consist switch |
| ECN | ethernet consist network |
| ETB | ethernet train backbone |
| ETBN | ethernet train backbone node |
| HTTP | hypertext transfer protocol |
| ICMP | Internet control message protocol |
| IGMP | Internet group management protocol |
| IP | Internet protocol |
| I/O | input/output |
| JPEG | Joint photographic experts group |
| MCG | mobile communication gateway |
| MPEG | Moving picture experts group |
| NAT-ALG | network address translation-application layer gateway |
| NTP | network time protocol |
| OMTS | on-board multimedia and telematic sub-systems |
| RTCP | RTP control protocol |
| RTP | real-time transport protocol |
| RTSP | real time streaming protocol |
| SOAP | simple object access protocol |
| SSL | secure sockets layer |
| TBN | train backbone network |
| TCMS | train control and management system |
| TCN | train communication network |
| TCP | transmission control protocol |
| TLS | transport layer security |

| | |
|---|---|
| UDP | user datagram protocol |
| UIC | International union of railways (the international railways operators association) |
| URI | uniform resource identifier |
| URL | uniform resource locator |
| WS | Web service |
| WS-I | Web service interoperability |
| XML | extensible markup language |

## 4 System breakdown structure

An on-board video surveillance/CCTV system usually consists of the capturing device, storage devices, display devices, analysis devices, etc. A single device may perform more than one functionality. For example, an IP camera can capture the image, handle it, and transmit it via the network. It may also provide analysis function on the data and store it temporally. Therefore, it is possible that an on-board video surveillance/CCTV system only consists of a single camera at a minimum physically. Alternatively, other devices in an on-board video surveillance/CCTV system can perform several functions. Thus, single physical device and its requirements are not defined in this specification.

Instead, this specification defines the system components which perform a specific function and may consist of one or several devices. In addition, the relationship between system components is described in this specification.

The major components of an on-board video surveillance/CCTV system are classified into four categories based on their functionality, including video capture component, video storage component, video display component and video analysis component.

- Video capture component

  A component (an IP network camera or analog camera with encoder device, for example) that captures visual information, encodes it digitally, compresses it and transmits it over the network to other components.

- Video storage component

  A component (a network video recorder, for example) that records media and metadata received from a video capture component over the network, to a storage medium, and also enables operator to search and retrieve the stored data.

- Video display component

  A component (an IP network video monitor, for example) that receives media data and metadata from the network, and presents them.

- Video analysis component

  A component that performs analysis on live data received from video capture component or on recorded data from video storage component.

Each component can perform both the service consumer and service provider depending on its capabilities. The video display and analysis component can be regarded as the service consumer of video capture and storage component. Besides the service exchanges between these components within an on-board video surveillance/CCTV system, the system also provides interfaces for other external system such as TCMS, OMTS and ground CCTV, as well as user such as train operator or security organization. For instance, it communicates with TCMS for obtaining time and location, and it enables the driver to visually detect the passengers and security staff to retrieve the recorded data when necessary. Figure 2 shows the typical structure of an on-board video surveillance/CCTV System and interface with other systems.

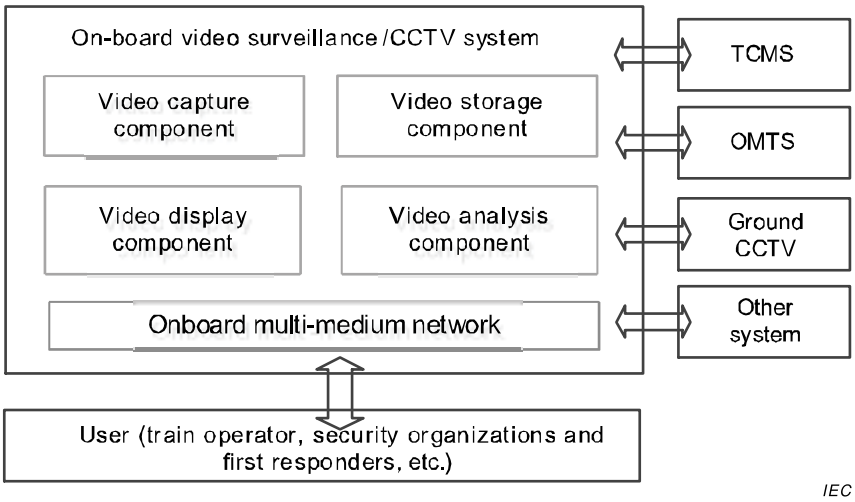



**Figure 2 – Typical structure of on-board video surveillance/CCTV system and interface with other systems**

## 5 Function breakdown structure

### 5.1 General

From the user's point of view, the function of on-board video surveillance/CCTV system may mainly include:

- to monitor and investigate the operational issues

  The operational issues may include train (or devices on the train) fault, track anomalies, driver behaviours, pantograph failure, accidents, etc. This function brings out the significant safety and performance benefits and can be used to assist in determining the responsibilities, fault prevention, trouble-shooting and analysis.

- to assist the driver during the train dispatch

  This function could help the driver to determine if there is a potential risk of accident and to respond quickly to the potential accident, such as persons running to the train, entering the space between the train and platform, trapped by the door or holding on the train side.

  In addition, this function could be associated with the passenger alarm (if a passenger alarm related system exists). When passenger alarm is triggered, the on-board video surveillance/CCTV system could carry out the corresponding functions, such as automatically displaying and recording accident images.

- to protect the safety of passenger and organization well-being

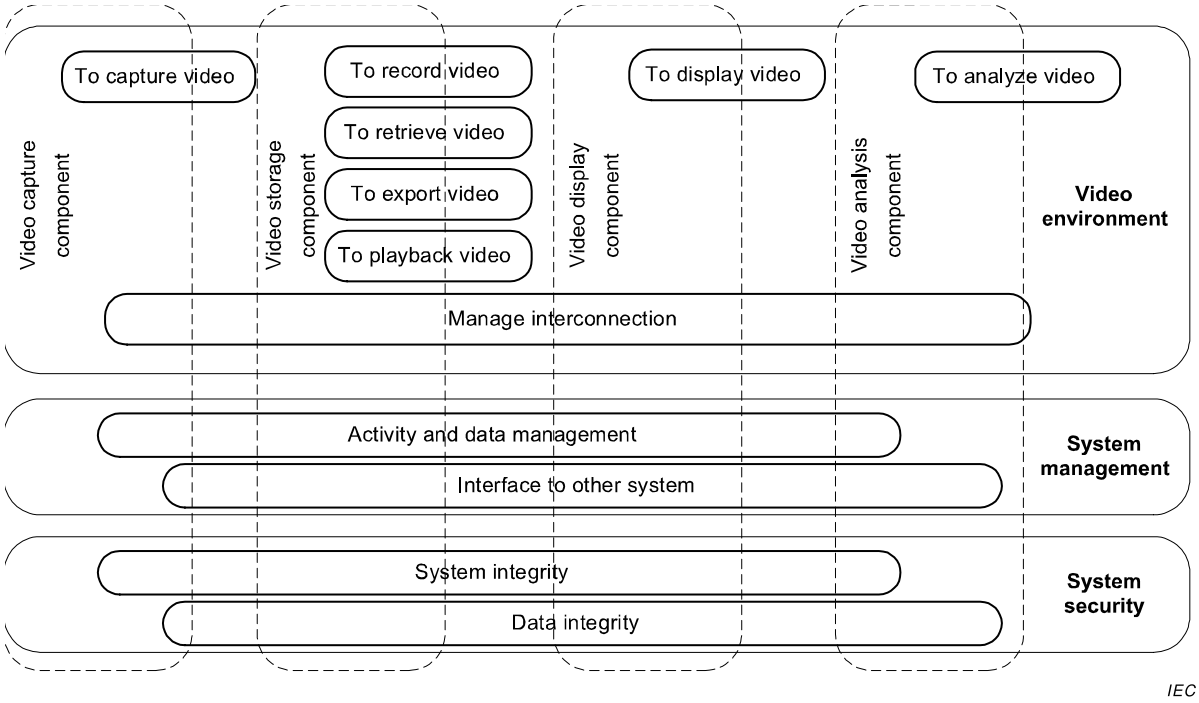
  To monitor the area of passenger compartment such as seating area, walkway, entrances and exits, this function could protect against the threats to the well-being of passenger and organization, and be usually associated with the passenger alarm system.

The above mentioned functions are the most common application and are not exhaustive. The function 3 listed here is more related to the security purpose. Based on the application, a function breakdown of the on-board video surveillance/CCTV system is given in Table 1.

**Table 1 – A function breakdown of on-board video surveillance/CCTV system**

| 1st level function | 2nd level function | 3rd level function |
|---|---|---|
| 1 to monitor and investigate the operational issues | 1.1 front-view monitoring: live videos from front-view cameras recording the image of forward condition of the train such as the track, signal, level crossing, speed limits, etc.; | 1.1.1 to capture video<br>1.1.2 to record video<br>1.1.3 to retrieve video<br>1.1.4 to replay video<br>1.1.5 to export video |
| | 1.2 rear-view monitoring: to capture and record the live videos from rear cameras, including platform and other rail infrastructures; | The same as above |
| | 1.3 cab interior monitoring: to capture and record the driver behaviours, panel, the ambient sound, etc.; | The same as above |
| | 1.4 interior monitoring: to monitor the status of train or on-board devices, for example cameras on the roof of the vehicle for monitoring the pantograph, especially the contact between the pantograph and the overhead line; or cameras for the special on-board devices such as the converter cabinet; | The same as above |
| 2 to assist the driver for train dispatch | 2.1 to enable the driver to visually detect persons or passenger related items that are anywhere within the train dispatch corridor, for example, rear-view mirror and side cameras betting on the door for assisting driver during the opening and the closing of the door; | 2.1.1 to capture video<br>2.1.2 to display video<br>2.1.3 to record video |
| | 2.2 passenger alarm and accident management: when emergency alarm is triggered, video from the specified cameras would be recorded for few seconds/minutes before and after the alarm for offline analysis by operators or the police; and displayed to the drivers to help them in the alarm management. | The same as above |
| 3 to protect the safety of passenger and organization well-being | 3.1 to have the visual and audio evidence into passenger compartment; | The same as above |
| | 3.2 passenger alarm and accident management (see 2.2 above). | The same as above |
| NOTE The above mentioned functions of the on-board video surveillance/CCTV system are summarized from the user's point of view and some functions may be missing. The user may choose to implement a set of the functions based on the agreement between operators and providers.<br><br>From the function breakdown structure, it can be seen that there are a number of basic functions at 3rd level for implementing the higher level functionality. A 3rd level function could be used in different 2nd level function, for example, to capture video is used in both front view monitoring and cab monitoring for different purpose, but they applies the same scheme and interface or service. Meanwhile, for a certain functionality such as to help driver during train dispatch, besides video capture, record and display, some operators could ask for video analysis from the device. Therefore, other 3rd level function could be used depending on the operator's functional requirement. In other word, this function breakdown table only shows the basic functions which are commonly used. Each function is assigned from the corresponding component, and could be performed by one or several devices which physically make up the on-board video surveillance/CCTV system. | | |

According to the functional breakdown, an on-board video surveillance/CCTV system can be presented as functional blocks which portray the various parts and functions of the system for realizing above-mentioned functions (see Figure 3).




NOTE The functional block of on-board video surveillance/CCTV system in this specification is basically in accordance with IEC 62676-1-1:2013. This specification replaces the concept of image handling which is given in Figure 1 of IEC 62676-1-1:2013 by using more detailed function classification of video environment, including record, display, analysis, retrieve, export and replay, without being in contradiction with IEC 62676-1-1:2013.

**Figure 3 – Function blocks of an on-board video surveillance/CCTV system**

## 5.2 Video environment

### 5.2.1 General

The entities consisting of the on-board video surveillance/CCTV system devices and interconnections between these devices can be described as video environment. The video environment is further divided into eight functions:

- to capture video;
- to record video;
- to retrieve video;
- to export video;
- to replay video;
- to display video;
- to analyse video; and
- to manage interconnection (transmission of media and control signals).

The above-mentioned functions may reside in various hardware or software components of the system, and only logically match up with the four components defined in Clause 4, rather than necessarily always mapping to separate devices. This is because several functions can be performed by a single device.

### 5.2.2 To capture video

The purpose of video capture is to generate an image and audio of the interior or exterior scene of the vehicle. The video capture component captures the image of scene, encodes and compresses it, and delivers it to other components for further handling. The video component

produces the output image data in digital format (such as ITU-T H.264) to facilitate video display, analysis, record, etc.

### 5.2.3 To record video

The function stores the video images (as well as audio or metadata) received from video capture component over a network on a permanent storage medium in a specified format for later retrieval.

### 5.2.4 To retrieve video

This function enables the client to search and obtain the video images (as well as audio or metadata) of interest stored on the storage medium. There are many ways to retrieve the data such as to replace and convey the storage medium to ground facility, or download the video sequence through wireless. The method of video retrieve is not discussed in this specification.

### 5.2.5 To export video

A single image or video sequence could be exported from the storage medium of the system to a suitable digital storage medium for later replay or analysis.

### 5.2.6 To replay video

To replay video provides a mechanism for playback of the stored and retrieved video, audio and metadata, which may also be used to download the data from storage medium for data export.

### 5.2.7 To display video

Video information can be viewed in the form of either image or video on monitor screens. Video display component receives the video information, decodes it and presents it. One or several video images may be displayed simultaneously. Additionally, video display component may also enable the audio data and metadata to be presented.

### 5.2.8 To analyse video

This function enables to extract information from the live or recorded video data for image analysis. In addition to the video image, the analysis function also uses other data as inputs, for example audio stream, and metadata.

Analysis could be utilized for several purposes, such as:

- proving the integrity of the system (e.g. camera position);
- interpreting the captured scene (e.g. alarming areas incursion);
- analysing the live video to generate an event or an alarm (e.g. arc discharge of pantograph or smoke detection);
- providing a decision aid; and
- functional performance evaluation.

### 5.2.9 Manage interconnection

Interconnection enables all media and control data signals to be exchanged within components of on-board video surveillance/CCTV system, between subsystems of OMTS as well as between other systems on the train. The interconnection is not only dedicated to OMTS, namely, shared with other systems.

## 5.3 System management

### 5.3.1 General

The system management of an on-board video surveillance/CCTV system consists of two logical functions, as defined in IEC 62676-1-1:

- activity and data management that captures, transmits, stores and presents video images, audio or metadata. This also handles the operator commands and system-generated activities, for example alarm procedures and alerting of operators; and
- interfaces that connect the on-board video surveillance/CCTV system to other systems.

### 5.3.2 Data management

The on-board video surveillance/CCTV system manages the video data, including data capturing, transmission, storage, display and etc. The system may also generate and handle metadata, which could be classified into:

- data that is linked to the video data. It can be acquired from other systems within train communication network or generated by the system itself (e.g. time stamps, vehicle information, train location);
- system data, such as system operational condition, storage media usage and device status.

In addition, log files that record system activities, operational and maintenance information may be generated, stored and managed by the system.

### 5.3.3 Activity management

Activity management comprises all the activities driven by events and any user actions. The activity management includes system configuration, system control, post event analysis and other activities started by the operator, including internal activities (e.g. data backup and export, auto recording) as well as notification of external system.

### 5.3.4 Interfaces management

The on-board video surveillance/CCTV system may interface to other system, for example

- TCMS (e.g. smog alarm, over-heat alarm, emergency door open and emergency brake, train location and time synchronization);
- PIS (e.g. passenger triggering alarm);
- train operator/maintainer system (e.g. firmware upgrade, device status check, data retrieval); and
- ground CCTV facilities (e.g. wayside cameras on the platform).

The interfaces between the systems could manage data communication, mutual system control, common databases and common user interfaces.

## 5.4 System security

### 5.4.1 General

As defined in IEC 62676-1-1, the purpose of system security function is to alter any failures of system and prevent the external interference, consisting of system integrity and data integrity. System integrity comprises physical protection of all system components as well as interconnection between them, and control of physical and logical access to the system. Data integrity covers logical access to the data and prevention of loss and manipulation of the data.

#### 5.4.2 System integrity

According to IEC 62676-1-1, system integrity consists of three parts:

- detection of failures of components, software and interconnections;
- protection against tampering;
- protection against unauthorized access to the system.

#### 5.4.3 Data integrity

According to IEC 62676-1-1, data integrity covers several important items:

- data identification (ensuring accurate identification of data source, time, train location, vehicle information etc.);
- data authentication (prevention of modification, deletion or insertion of data);
- data protection (prevention of unauthorised access to the data).

## 6 Requirements

### 6.1 Video environment requirement

#### 6.1.1 To capture video

##### 6.1.1.1 General

The captured image shall contains the sufficient information and quality to fulfil the customer's requirement for further handling by other components of the on-board video surveillance/CCTV system or authorized external system. In addition, the output image data from video capture component shall only be digital format (see ITU-T H.264), and the compression and encoding of the captured images shall be strictly specified based on the existing standards for interoperability of further handling such as display, storage, and especially export.

##### 6.1.1.2 Capturing, compressing and encoding

The compression and encoding of video and audio should comply with the following prescription:

- Video compression should be compliant with ITU-T H.264/MPEG4-AVC as defined in ITU-T H.264 and ISO/IEC 14496-10, or JPEG as defined in ITU-T T.83 and ISO/IEC 10918-1, or MPEG-4 Visual as defined in ISO 14496-2;
- The profile used should be either Constrained Baseline, Baseline, Main, or High, and the level should have a maximum value of 4.0 (all levels below 4.0 are accordingly allowed);
- It should be possible to associate to each video frame its absolute capture time (with an accuracy better than one video frame and in any case better than 100 ms referred to UTC if system is for societal security purpose). Individual data streams only (video, audio and metadata) should be used;
- Audio should be encoded either as per ITU-T G.711 Law A as defined in ITU-T G.711 or per MPEG4-AAC in Low Complexity Profile (AAC-LC) as defined in ISO/IEC 14496-14.

The above international standards are acceptable but not exclusive considering the future technical development (such as ITU-T H.265).

##### 6.1.1.3 Streaming

After being captured and encoded, the video or audio data needs to be packed and delivered to other components of the on-board video surveillance/CCTV system or external device. The video capture component shall comply to the general video streaming and stream control

requirements of Clause 7 and Clause 8 of IEC 62676-1-2:2013 and to the requirements of 6.4.3.3.

#### 6.1.1.4 Performance

The captured images of the area of interest shall have sufficient accuracy and detail to enable users to extract appropriate information to meet image handling requirement, for example presentation and recording. The image quality requirements should be in accordance with 6.5 of IEC 62676-1-1:2013.

The performance of video capture concerning video frame rate (fps), resolution (pixel) and latency time (ms) should be considered. Different objectives could have various requirements on performance of video capturing. The recommendations of performance on capturing video are given in this specification instead of strict requirement. It is recommended that a minimum 25 fps should be applied where the output resolution is 4 CIF or below, and at least 15 fps should be used for higher resolution. For example, for continuous forward-facing video of the vehicle, video from passenger area or area containing any form of emergency call, video source should be up to HD, and at least 15 fps is expected. On the contrary, relative low resolution can be acceptable for minor purpose of monitoring such as live videos from rear cameras helping the driver during normal manoeuvring.

The function of capturing video should also enable the operator to set the quality of each data stream according to the requirement by providing an interface for controlling the capturing parameters. For example, a capturing device can provide two type of video streams from one source simultaneously, for video display and storage respectively. In order to realize it, the imaging setting and media setting interfaces should be provided.

The imaging setting provides operations used to control and configure imaging on a video capturing component. The parameters such as back light compensation, brightness, sharpness, colour saturation, contrast, exposure, focus, IR cut filter and white balance are suggested to be configured.

The media setting is used to configure the device media streaming properties. For the video stream, video resolution, frame rate and bit rate, compressing and encoding algorithms are recommended to be configured. The audio encoding format, audio sampling rate and snapshot setting also should be changed through this interface.

### 6.1.2 To record video

#### 6.1.2.1 General

To record video enables a client to receive the media data or metadata from data sources, to create or delete the recordings, and to configure the transfer of data from source to video storage component continuously during the train operation. The data could be stored on a variety of memory devices, such as anti-vibration hard drives or solid state memory which are robust and scalable.

The recording of video images should not be influenced by any live image display and requests or by image backup and export from operation of the system itself as well as by the operation or failure of other connected systems.

The recording shall be in digital format. In this specification, it is not necessary to define the specified recording format (such as MP4 file) in storage medium. To record the video, this function should provide the interface for configuration, such as:

- number of video input channels being recorded;
- resolution and size of stored images;
- maximum frame per stream;

- maximum bitrate per storage device and per stream;
- maximum continuous recording time.

If a constant frame rate is specified, the sequences of pictures shall provide images at equidistant intervals.

#### 6.1.2.2 Metadata

Besides the medium data, metadata associated with the train shall be added into recording. The information source could be components of the on-board video surveillance/CCTV system itself (e.g. sensor information from camera) or authorized external system from the train communication network (e.g. train information from TCMS).

If the on-board video Surveillance/CCTV system is designed for societal security purpose, it should comply with the metadata requirement defined in ISO 22311. When metadata requirement defined in ISO 22311 is applied, the following metadata items concerning source information are mandatory:

- codec name and profile;
- name of the container;
- video resolution;
- video frame rate (fps);
- time and date of the record;
- time and date of the camera.

Other dynamic metadata concerning event, including event time and description, should also be provided, such as smog alarm, driver alarm and passage alarm.

Besides the above-mentioned metadata, the following content about the train are strongly suggested to be provided:

- train location (such as longitude and latitude);
- train number;
- train consist name;
- station name;
- vehicle ID;
- driver ID.

The metadata contained within the on-board video surveillance/CCTV system shall, as a minimum, permit a time stamp (associate to each frame its absolute capture time) and camera identifier to be superposed on the image.

The time stamps of on-board video surveillance/CCTV system shall only be determined by clock source on the train in accordance with 6.4.2.1.

#### 6.1.2.3 Recording

The function shall be capable of automatically deleting images once they have been stored for the set maximum period of time. Recorded images marked as protected from being deleted may be stored for a longer period of time. The maximum storage time allowable by the applicable national legislation should not be exceeded. In addition, the function should offer information about the image storage usage in capacity and recording time as well as remaining storage capacity. When capacity is running low, the function should be capable of indicating.

When applying the automatic segmentation recording method in which streaming media could be stored by segments, the interval between two recording segments should be continuous.

#### 6.1.2.4 Encryption

The images should not be encrypted in case it delays and prevents legitimate access to video evidence. The data format may contain checksums or other methods for ensuring that changes to the data may be detected but, where used, they shall not alter the compressed image information.

### 6.1.3 To retrieve and export video

To retrieve and export video enables the authorized user to find data of interest within a set of recordings on a storage device and to duplicate data from the original storage device to the targeted device for further investigation. Besides video, this function should also enable the still image, audio and metadata to be exported where applicable.

The primary expectation of exported data is that they can be identified, replayed and analysed in a standard format. When the purpose of system is related to societal security, image export should be in compliance with ISO 22311 to achieve export interoperability using the common output file format. The export file could be self-contained Audio-Video Packages as defined in ISO 22311, which contains all information associated with images without requiring accessing to source system.

The standard format and container could also be used for video export when system is applied for general purpose, for example, exporting the recorded video of train pantograph. The following containers are recommended to be applied:

- MP4 (see ISO/IEC 14496-14);
- MPEG-A (see ISO/IEC 23000-10);
- JPEG Baseline (see ISO/IEC 10918-1 and ITU-T T.81) for still image which is stored and will be exported.

The export method of system (through removable storage medium or wireless transmission) should be appropriate to the capacity of the system and its expected use, and is not discussed in this specification. Whatever export method is applied, original recording shall not be influenced. Other functionalities shall not be influenced during data export. In addition, data exported from a recorder shall have no loss of individual frame quality, change of frame rate or audio quality. There should be no duplication or loss of frames in the export process.

The function of retrieving and exporting video should be able to offer the selection of time range and image source to be searched, and exported. Other information such as vehicle ID, train No., driver ID, train location and event can be used as selection condition for record search.

During the export, an estimated time to complete the export of the requested data should be displayed. The software application needed to replay the exported images should be included on the storage media used for replaying the tool offering, otherwise viewing by authorized third parties can be hindered. Each export operation should be recorded in system log.

### 6.1.4 To replay video

The export data of standard format should be replayed using non-proprietary player. If metadata which is associated with video data needs to be played, the specialized played should also be offered. The replay should:

- have variable speed control, including real time play, stop, pause, fast forward, rewind, and frame-by-frame forward and reverse viewing;

- display single and multiple cameras and maintain aspect ratio, i.e. the same relative height and width;
- display a single camera at the maximum recorded resolution;
- zoom the individual camera view;
- permit the recordings from each camera to be searched by time and date, or other information such as train number or train location according to recorded metadata;
- allow saving (e.g. bitmap or JPEG) of still images with time and date of recording;
- allow for time synchronized multi-screen replay;
- allow for time synchronized switching between cameras upon replay;
- allow replay of associated audio and other metadata;
- be able to export the image sequences in a standard format (see 6.1.3) at an equivalent quality to the original and still displaying time and date information with no significant increase in file size;
- clearly show the time and date, and any other information associated with each displayed image, without obscuring the image.

### 6.1.5 To display video

This function is optional. If the on-board video surveillance/CCTV system is equipped with the video display component, it shall provide this function for authorized user to control and configure the display device, and to explore all functionalities.

To display video should

- cover live image from all monitoring points for the driver or the on-board crew to check;
- be capable of supporting multiple displays which enables the viewing of more than one image source on the screen simultaneously;
- provide the interface for user to select the display mode, including poll mode which will automatically present one image or multiple images in a given order, and manual mode which enables user to view the specific image manually;
- switch display to the image which contains the scene of accident automatically and immediately, in case of accident such as smog, over-heat or passenger emergency call. It is preferred that event mark is superimposed on the image.

When displaying images, whether the entire image source or a part of it, the proportions of the displayed image should be the same as in the original image source. Any superimposed information, for example timestamps, train information or alarming information, produced by the system should not affect the image itself.

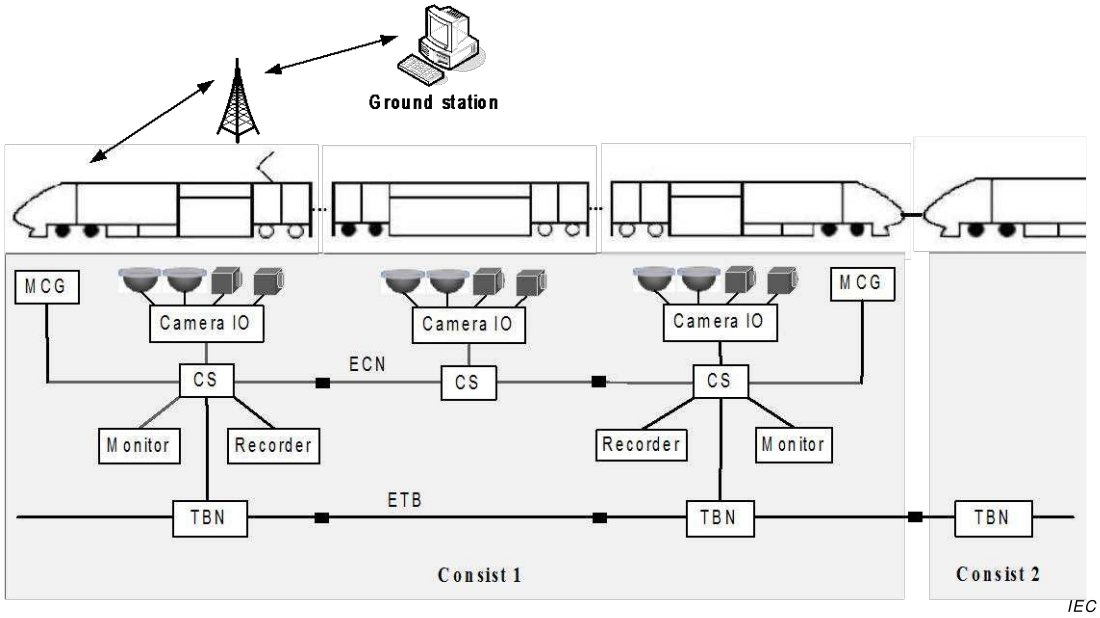
### 6.1.6 To analyse video

This function is also optional. The on-board video surveillance/CCTV system exposes the functionality of video analysis through a number of services for different purposes. The input of video analysis component could be live data from an IP streaming device or recorded data from storage device. Therefore, the format of input data should be compliant with 6.1.1 and 6.1.3.

In addition, any superimposed information produced by the system itself or other systems shall be processed as metadata. It shall not affect the image itself and the requirement of data and image integrity either (see 6.3.3). Only a privacy mask that blocks out sensitive areas from the view is allowed to affect the area of interest of an image for privacy reasons.

### 6.1.7 Manage interconnection

In order to facilitate data communication, the devices of the on-board video surveillance/CCTV system are connected to the on-board multimedia network, and communicate with the operational network through a gateway. Figure 4 shows a possible on-board video surveillance/CCTV system topology.




NOTE The train communication network architecture for both the operational service and comfort service may reference to 4.2.2 of the IEC 61375-2-3:2015.

**Figure 4 – On-board video surveillance/CCTV System topology**

The requirement of the Ethernet interfaces, including the physical layer, the data link layer, the network layer, the transport layer and the application layer shall be in accordance with the specifications of end devices in IEC 61375-2-5 or IEC 61375-3-4 for communication between and within consists, as well as IEC 61375-2-6 for on-board to ground communication respectively. The application layer for the stream data transmission is specified in 6.4.

For international trains, where several consists belonging to different operators are associated in a single convoy for a given mission, devices of the on-board video surveillance/CCTV system need to communicate with each other across different consists. When train configuration changes during the coupling and decoupling process, these devices should also be able to communicate without requiring human interventions.

Image streams sharing common interconnection shall be designed and configured in a way that they do not adversely affect each other and any message transferred in normal operation mode. If an on-board video surveillance/CCTV system is designed and configured in a way that a single or multiple operators can request video images via common interconnections, the design of the system shall ensure sufficient capacity to handle the anticipated streaming traffic in the system. This may be achieved by configuring the maximum throughput of image streams on the system.

## 6.2 System management requirement

### 6.2.1 Activity and data management

#### 6.2.1.1 General

As defined in IEC 62676-1-1, the on-board video surveillance/CCTV shall clearly distinguish between user's requested data and event-driven data. Alarm data may be given higher priority over continuously displayed data.

#### 6.2.1.2 Status of system functions

Information about the status of the essential functions and devices, at least including video capture (e.g. status of the audio and video device) and video storage (e.g. remaining storage space, total storage space), should be offered through this function.

#### 6.2.1.3 Events and event-driven activities

If the on-board video surveillance/CCTV system is designed to handle event-driven activities, the requirements defined in 6.2.2.3 of IEC 62676-1-1:2013 should be applied.

The on-board video surveillance/CCTV system should offer means to indicate an alarm visually and audibly in order to get the train operator's attention.

The on-board video surveillance/CCTV system should offer the function to acknowledge alarms. If an alarm is triggered, alarm related information should be displayed. The information presented for each alarm message should include:

- the origin or source of the alarm;
- the type of the alarm;
- the time and date of the alarm.

#### 6.2.1.4 System log

Accurate and complete system logs are strongly recommended to be generated through this function and maintained for a defined period of time. The requirements of log should comply with 6.2.2.4 of IEC 62676-1-1:2013.

The items of log which should be recorded could vary according to different purposes. If the on-board video surveillance/CCTV system is applied for societal security purpose, the requirements for system of security grades 3 and 4 as defined in IEC 62676-1-1 are recommended.

### 6.2.2 Interfacing to other systems

The on-board video surveillance/CCTV may interface to TCMS or other OMTS, consuming the external service such as timing and train information, which could be defined in IEC TS 61375-2-4 and other parts of the IEC 62580 series.

This applies directly, when several complying systems from different owners are interfaced together, and consistent information shall be provided.

All system security requirements as defined in 6.3 shall be fulfilled even in the case where the on-board video surveillance/CCTV system is accessed or controlled by the other system. The other system shall be seen as a system user with defined access rights which can be seen in 6.3.2.3.2. Access level shall not give unauthorised access to the on-board video surveillance/CCTV system and vice versa.

## 6.3 System security requirement

### 6.3.1 General

The security of the on-board video surveillance/CCTV system consists of system integrity and data integrity. System integrity includes physical security of all system components and control of access to the system. Data integrity includes prevention of loss and manipulation of data before clearance.

### 6.3.2 System integrity

#### 6.3.2.1 Detection of failures

##### 6.3.2.1.1 Failures notification

The failure of system functionality or devices should be notified at any time during train operation, new user logs in and system restarts.

The information to be presented should include:

- time and date;
- origin and type of failure.

##### 6.3.2.1.2 Monitoring of power supply

For the on-board video surveillance/CCTV system designed for societal security purpose, power supplies to the system should be monitored and indicated. The system should attempt to resume normal operation after recovering from power loss.

The on-board video surveillance/CCTV system should not lose data when power is switched off. Images should not be held in a buffer for longer than 5 s without being written into the storage medium.

##### 6.3.2.1.3 Monitoring of system functions and components

The on-board video surveillance/CCTV system should manage device failure by indicating any failure of the essential functions. The requirement for system of security grades 3 and 4 as defined in IEC 62676-1-1 is recommended.

##### 6.3.2.1.4 Monitoring of interconnection

Interconnections between system components of the on-board video surveillance/CCTV system should be monitored. Monitoring may take the form of listening for jamming when a video transmission device communicates via sharing interconnections with other devices or other applications. The requirement for system of security grades 3 and 4 as defined in IEC 62676-1-1 is recommended.

#### 6.3.2.2 Tamper protection and detection

The on-board video surveillance/CCTV system should be protected against tamper. The system should detect video loss, deliberately obscuring or blinding of image capturing device range, and substitution of image data source. A temper condition should be set and an alarm should be generated if a temper is detected, meanwhile an alarm should be logged.

#### 6.3.2.3 Protection against unauthorized access

##### 6.3.2.3.1 General

Access to operation and data of the on-board video surveillance/CCTV system should be governed by an authorisation scheme. The party accessing to operation and data can be either an operator or other external system.

#### 6.3.2.3.2 Access level

The accessing level of on-board video surveillance/CCTV system includes three categories: the operator, the system administrator and the service personnel or manufacturer.

- Operator level

  Operator is an authorized user who operates the system, which could be either operating personnel or external system.

  Operator can access to the basic functions of the system including video display, reply and download, without changing the configuration of system.

  Access to the user accessible functions shall be restricted by means of key, password, code or similar access-limiting means or device.

- System administrator level

  System administrator can access to the function which could affect the configuration of the system.

  Access to the administrator accessible functions shall be restricted by means of key, password, code or similar access-limiting means or device.

- Service personnel or manufacturer level

  Service personnel or manufacturer can access to the system component so as to change the system design or to perform system maintenance.

  Access to service personnel or manufacturer accessible functions shall be restricted by means of key, password, code or similar access-limiting means or device. Access at this level is prevented unless access has been granted by operator or administrator.

NOTE There are four accessing levels defined in IEC 62676-1-1. Considering the security of system and data, the functions of the on-board video surveillance/CCTV system cannot be accessed by any person. Therefore, Level 1 given in IEC 62676-1-1 (Access by any person) is omitted in this specification.

Table 2 specifies which functions can be accessible by different user.

**Table 2 – Access level**

| Function description | User category | | |
|---|---|---|---|
| | Operator | System administrator | Service personnel or manufacturer |
| Basic function such as data download, display and reply | Permitted | Permitted | Permitted |
| System configuration | Not permitted | Permitted | Permitted |
| Change of individual authorisation codes | Not permitted | Permitted | Permitted |
| Restoration to factory defaults, including deleting data | Not permitted | Permitted | Permitted |
| Upgrading of system | Not permitted | Not permitted | Permitted |
| Start/stop system or component | Not permitted | Permitted | Permitted |

#### 6.3.2.3.3 Authorisation

The requirements of authorisation for system of security grade 3 or 4 defined in IEC 62676-1-1 are recommended for the on-board video surveillance/CCTV system.

#### 6.3.2.3.4 Data access

The on-board video surveillance/CCTV system shall control user access to data, as specified in Table 3.

**Table 3 – Data access**

| Function description | User category | | |
|---|---|---|---|
| | Operator | System administrator | Service personnel or manufacturer |
| View live images and data | Permitted | Permitted | Permitted |
| View stored images and data | Permitted | Permitted | Permitted |
| Search and export stored images and data | Permitted | Permitted | Permitted |
| View information of train or device status | Permitted | Permitted | Permitted |
| Deletion of images and data (only with confirmation) | Not permitted | Permitted | Permitted |

#### 6.3.2.3.5 Access to system logs

The on-board video surveillance/CCTV system shall control user access to log data, as specified in Table 4.

**Table 4 – Access to system logs**

| Function description | User category | | |
|---|---|---|---|
| | Operator | System administrator | Service personnel or manufacturer |
| View system log | Permitted | Permitted | Permitted |
| Exporting from log | Not permitted | Permitted | Permitted |
| Deleting log | Not permitted | Permitted | Permitted |

### 6.3.3 Data integrity

The video data shall be identified according to the metadata requirements defined in 6.1.2.2. The on-board video surveillance/CCTV system shall not alter the compressed image information.

The on-board video surveillance/CCTV system shall always uniquely label data by time and date, location (name of monitoring site), and source (e.g. capturing device labelled by camera number). Date and time shall refer to the time when the image is captured.

## 6.4 Video transmission requirement

### 6.4.1 General

For the fully interoperability of devices of the on-board video surveillance/CCTV system from different venders, and systems within several consists belonging to different operators which could be associated in a single convoy for a given mission, 6.4 defines the minimum performance requirement on video transmission, and introduces the basic transmission protocol requirements and IP device interoperability implementation based on Web services.

### 6.4.2 Performance requirement

#### 6.4.2.1 Time synchronization

It is preferred to get synchronized with TCMS time source by private protocol or NTP protocol, which is up to operator’s choice.

In case no interface to the TCMS is provided, there should be a separate time source for the on-board video surveillance/CCTV system, or the on-board video surveillance/CCTV system could use its own time source such as GPS.

All collected information associated with video data should be referenced to the same time source.

Global scale synchronization within the operator's transit system is preferred.

#### 6.4.2.2 Connection setup and teardown time

Time to setup or teardown a video stream connection should be less than 2 000 ms as specified in 4.3.2 of IEC 62676-1-2:2013.

#### 6.4.2.3 Network capacity

Bandwidth requirement shall be calculated using the configuration of maximum concurrent video streams in the system.

The system should be deployed on top of a network with the capacity to meet the bandwidth requirement that video streams shall consume no more than 75 % of the link bandwidth as specified in 5.3.2.2 of IEC 62676-1-2:2013.

#### 6.4.2.4 QoS

The underlying network shall support QoS mechanism based on IEEE 802.1Q and DiffServ to prioritize certain streams over others.

#### 6.4.2.5 Latency and jitter

As defined in 4.4.1 of IEC 62676-1-2:2013, there are several ways to cause stream latency, including:

- Transmission delay – The length of time a video packet takes to cross the given media. Transmission delay is determined by the speed of the transmission media and the size of the video packet.
- Forwarding delay – The length of time an internetworking device such as a switch takes to send a packet that it has received.
- Processing delay – The time required by a networking device for looking up the route, changing the header, and other switching tasks. In some cases, the packet header has also to be manipulated. For example, the encapsulation type has to be changed. Each of these steps can contribute to the processing delay.
- Coding/Decoding delay – The time required to encode and/or decode an image to or from a video stream, which is influenced by the performance of the video capture component and the type, profile and level of CoDec. For instance the H.264 profiles Main with 350 ms and Baseline Profile with 120 ms coding delay or MPEG4 may offer a delay of 110 ms and MPEG2 Low Delay with less than 180 ms.

If there is a variable delay in network, it causes jitter.

For different purposes of the on-board video surveillance/CCTV system, the performance requirements of video streaming could vary. For example, there is easier performance requirement of video streaming on "to record video" because it is not sensitive to delay and jitter (because of buffering application). On the other way, for security application, like video presentation to train operator, it requires higher performance.

The latency of video stream should be less than 600 ms and the jitter of video steam should be less than 160 ms unless otherwise specified according to the requirements given in IEC 62676-1-2.

### 6.4.3 Transmission protocol

#### 6.4.3.1 General

To achieve the full interoperability between connected devices in the on-board video surveillance/CCTV system, the system shall adopt the standardized protocols to accomplish the video streaming and stream control, event handling, device discovery, capability description, system management and other functions described in 6.4.1, 6.4.2 and 6.4.3. A common set of building blocks based on existing standards is needed as a basis to develop the video transmission standards as shown in Figure 5. The building block of existing standards given here is informative.

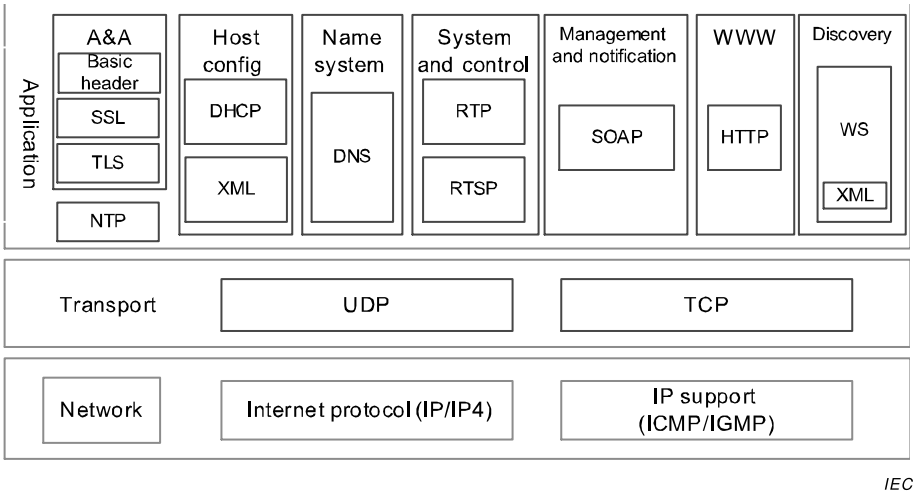



**Figure 5 – Building block of existing standards**

The on-board video surveillance/CCTV system shall fully support the protocol of communication profile according to IEC 61375-2-3.

The device shall have at least one network interface that gives it IP network connectivity and allow video and data exchange between devices of on-board video surveillance/CCTV system.

The on-board video surveillance/CCTV system shall support compatible video streaming and stream control implementation which can be fulfilled by existing standards, for example, all media streams transferred by the RTP protocol shall conform to RFC 3550, RFC 3551, RFC 3984, RFC 3016 and JPEG over RTP according to IEC 62676-2 series, and RTSP according to RFC 2326 is required for live streaming and replay.

#### 6.4.3.2 General IP interoperability requirement

The IP video protocol suite is the foundation for networking and connectivity for devices in the on-board video surveillance/CCTV system. The system network environment requires supporting network infrastructure, such as access points, bridges, gateways, routers, and switches.

Any IP video protocol shall be independent of any specific hardware and software so as to be implemented in principle on any video transmission platform. The video transmission device compliant to this specification shall offer an IP protocol interface to:

- support TCP/ IP networking, real-time streaming, stream control;

- be configured with at least one IP address, unique on the network, either manually or dynamically;
- be discovered in an IP network and provide the device URL;
- be configured via network;
- send notifications about device status and events to a configured receiving address;
- comply to the quality and performance requirements of this specification.

In addition, the following IP protocol interfaces should be offered:

- device description and capabilities via network;
- maintenance API functions (initial setup, firmware upload, diagnostic functions, health monitoring, etc.).

#### 6.4.3.3 Video streaming and stream control requirements

In order to accomplish a minimal interoperability of video transmission between components of the on-board video surveillance/CCTV system, the system shall comply to the general video streaming and stream control requirements of IEC 62676-1-2. Additionally, the following protocol shall apply as well. Note that not all blocks in the protocol stack are mandatory.

This specification defines media streaming options and formats. A distinction is made between media plane and control plane, as illustrated in Figure 6.

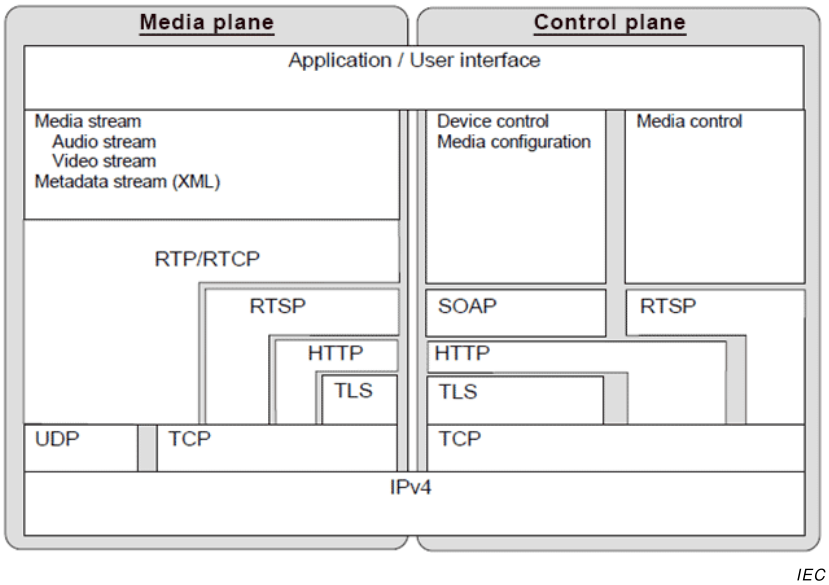



**Figure 6 – Structure layer**

A set of media streaming (audio, video and metadata) options all based on RTP (RFC 3550) are needed in order to provide interoperable media streaming services.

Media configuration is done over SOAP/HTTP. Media control is accomplished over RTSP as defined in RFC 2326. This specification utilizes RTP, RTCP and RTSP profiling and multicast control mechanisms.

Streaming specification shall include the video/audio codec defined in 6.1.1.2.

### 6.4.4 IP interoperability implementation based on Web service

#### 6.4.4.1 General

Two types of high level IP video interface are introduced in the IEC 62676-2 series, which are video IP interoperability based on Web services according to IEC 62676-2-3, and video IP interoperability based on HTTP and REST service according to IEC 62676-2-2. Future architecture such as Session Initiation Protocol (SIP) may be introduced.

For complying with the OMTS general architecture defined by IEC 62580-1, this specification applies the architecture for a IP interoperability implementation based on Web service defined in IEC 62676-2-3 which covers data types, data exchange patterns, device discovery, device configuration, events and real time streaming functionality for live video, as well as search, replay and recording management functionality for recorded video, and provides the interface which is a suite of software services, for the fully interoperability requirements.

Considering the special implementation of on-board surveillance/CCTV system for railway such as subsystems locating in different vehicles of the same train as well as consists belonging to different operator, and network which is compliant to the IEC 61375 series, this specification defines more specific device discovery scheme and IP configuration requirement. Other function and services reuse the existing relevant clauses of IEC 62676-2-3.

The IP interoperability implementation base on Web service shall be platform and OS independent. IP based proprietary or undisclosed Vendor Specific API, either IP-based or not, are not compliant to the requirements of this specification. All services described in IEC 62676-2-3 share a common XML schema and all data types are provided in the ONVIF schema file.

#### 6.4.4.2 Web service framework

Application-level interoperable interfacing between components of on-board surveillance/CCTV system or between subsystems of different vehicles is based on Web services, which uses the open, platform independent Web services standards such as XML, SOAP 1.2 (Part 1) and WSDL 1.1 over an IP network. The Web service framework of on-board surveillance/CCTV system shall be compliant to the requirement of IEC 62676-2-3 and 4.5 of IEC 62580-1:2015.

For network-based on-board surveillance/CCTV system, all system management and configuration command are based on Web service. As described in IEC 62580-1, all subsystems of OMTS can work as service provider or consumer, and a system which provides service probably has multiple clients. The Web service provider and consumer communicate using the SOAP message exchange protocol. The method of device discovery in this specification is based on WS-Discovery technique, combined with special scheme suitable for railway application which is defined in 6.4.4.5. The standard profiles and guidelines in the WS-I Basic Profile 2.0 shall be followed to guarantee the interoperable Web service.

The ONVIF service structure, the command definition syntax, error handling principles and the adopted Web service security mechanisms are defined well in Clause 5 of IEC 62676-2-3:2013, and also applicable to this specification.

#### 6.4.4.3 Relationship with services of IEC 62676-2-3

The device of on-board video surveillance/CCTV system shall support of a number of Web service which are well defined from Clauses 8 to 21 of IEC 62676-2-3:2013 based on ONVIF specification, to realize the functionality of each component of system defined in Clause 6. For each component, a set of function and services are mandatory. Device and Event service shall be supported by all components, and other services may be supported by a device depending on its capabilities.

Table 5 shows the mandatory services given in IEC 62676-2-3 which are required to implement the function of components of on-board video surveillance/CCTV system.

**Table 5 – Mandatory services given in IEC 62676-2-3 required for different functions**

| Category | Function of component in IEC TS 62580-2 | Service and function given in IEC 62676-2-3 |
|---|---|---|
| Video capture component | * to capture video | *Core (Device discovery, management and event)<br>*Media *Streaming<br>*Device I/O *Imaging |
| Video storage component | *to record video<br>*to retrieve video<br>*to export video<br>*to replay video | *Core (Device discovery, management and event)<br>*Recording search *Recording control<br>*Streaming *Replay control *Receiver |
| Video display component | *to display video | *Core (Device discovery, management and event)<br>*Streaming *Receiver<br>*Device I/O *Display |
| Video analysis component | *to analyse video | *Core (Device discovery, management and event)<br>*Streaming *Receiver<br>*Analytics *Video analytics device |

- For Device management, which defines the management command, including capabilities, network, system, security and I/O, implementation of Device Management service shall be in accordance with Clause 9 of IEC 62676-2-3:2013;
- For Event handling, which defines how to subscribe to and receive data from network video events (notifications), implementation of Event Handling service shall be in accordance with Clause 15 of IEC 62676-2-3:2013;
- For Imaging and Media, which describe the configuration commands related to imaging and media settings, implementation of these two services shall be in accordance with Clauses 10 and 11 of IEC 62676-2-3:2013;
- For Streaming, which provides requirements for interoperable video, audio and metadata streaming, implementation of Streaming service shall be in accordance with Clause 12 of IEC 62676-2-3:2013;
- For Device I/O, which defines commands to handle physical inputs and outputs of device, implementation of Device I/O service shall be in accordance with Clause 9 of IEC 62676-2-3:2013;
- For Receiver, which offers commands to manage Receiver objects used to receive media streams from other devices, implementation of Receiver service shall be in accordance with Clause 13 of IEC 62676-2-3:2013;
- For Recording control and Recording search, which define mechanism for the configuring of recordings, and provide commands for retrieval of recorded media including metadata, implementation of these two services shall be in accordance with Clauses 19 and 20 of IEC 62676-2-3:2013;
- For Replay control, which defines the control command to playback the retrieved recording, implementation of Replay control service shall be in accordance with Clause 21 of IEC 62676-2-3:2013
- For Display, which defines commands to handle the display devices, implementation of Display shall be in accordance with Clause 14 of IEC 62676-2-3:2013;

- Video Analytics defines the ONVIF analytics model, analytics object description and analytics rules configurations, and Video analytics device defines commands to deal with video analytics devices which perform processes on media stream or metadata. Implementation of these two services shall be in accordance with Clauses 17 and 18 of IEC 62676-2-3:2013.

Device of on-board video surveillance/CCTV system compliant to this specification should also be ONVIF compliant, but the type of ONVIF Web service interface and commands should be agreed between supplier and customer beforehand.

#### 6.4.4.4 IP configuration

The network of on-board surveillance/CCTV system shall be fully compliant to the requirement of the IEC 61375 series.

#### 6.4.4.5 Device discovery

All devices of on-board video surveillance/CCTV system shall provide device discovery and description service to offer information about device features and capabilities. And all service consumers shall be able to receive and interpret these device discovery and description messages from service provider no matter that devices are within one vehicle or from different vehicles of the same train, or from different supplier.

A client searches for available devices using the dynamic Web services discovery protocol (WS-Discovery). But if the client and the server do not reside in the same consist, it is not possible to transmit the message to the server by using the multicast address (239.255.255.0) defined in WS-Discovery. The backbone node needs to make a network address translation in order to convert the local consist group address to a train group IP address, so the Probe messages and the Probe match message could be transmitted between consists. Therefore, to achieve interoperability over different consists, there should be two additional protocol add-ons implemented on ETBNs.

a) WS-Discovery Proxy

   Probe message is sent to multicast address 239.255.255.0, which is not in the target range that ETBN will forward over ETB to other consists. To make the Probe message globally visible on the train, we need to set up a discovery proxy on ETBN of the consist. This proxy will receive the Probe message and encapsulate the payload in a new packet with destination address in range of 239.192.0.0 to 239.192.0.255, which is defined in IEC 61375-2-5 as a reserved range for OMTS.

   The Proxy will also do the reverse address translation on the other direction. It receives Probe message from ETB, and then encapsulates it with destination multicast address 239.255.255.0 to reach the target service providers.

b) WS-Discovery NAT-ALG

   For all the WS-Discovery messages like Probe match, a specially designed protocol ALG (application layer gateway) is required to achieve inter-consist interoperability.

   Locally allocated addressing information like IP address is included in Probe match message, but it is invalid for train level communication. This problem is solved in IEC 61375-2-5 by using R-NAT and NAT-ALG.

   NAT-ALG could check each Probe match message sent from its consist, extract the addressing part and calculate its globally mapped address, and then a global addressing part is filled back. So far, the probe match carries a service provider address with global meaning for all the consists in the train.

Figure 7 shows a typical inter-consist device discovery scenario:

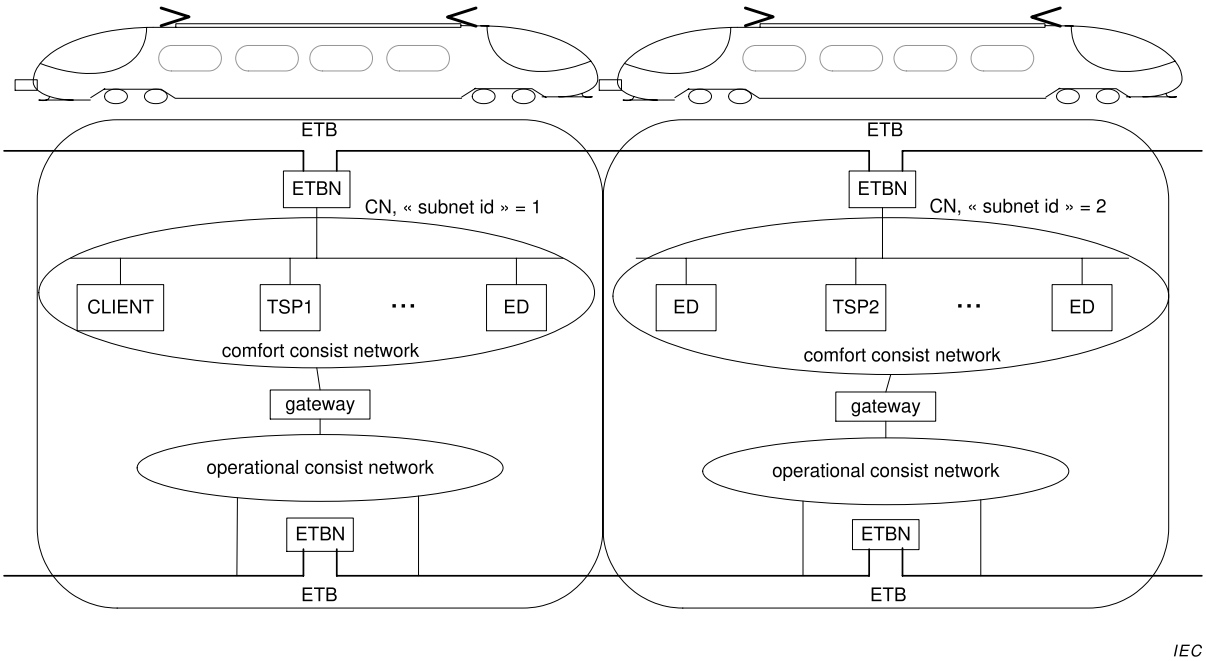



**Figure 7 – Device discovery in a multiple consist case**

Service client resides in consist 1, and target service provider 1 and 2 (TSP1, TSP2) reside in consist 1 and 2 respectively. WS-Discovery Proxy and WS-Discovery NAT-ALG are software components in ETBN.

Message sequence between client and TSP1 and TSP2 are shown in Figure 8 and Figure 9 respectively.

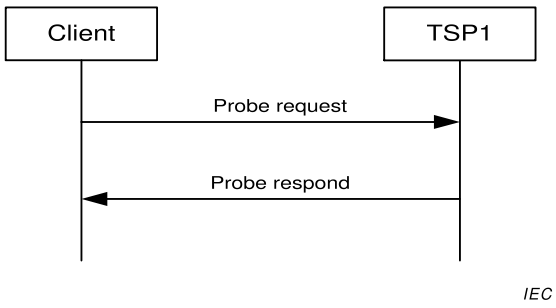



**Figure 8 – Message sequence for client and TSP1 within the same consist**

a) CLIENT sends Probe out in consist 1;

b) TSP1 responds with Probe match.

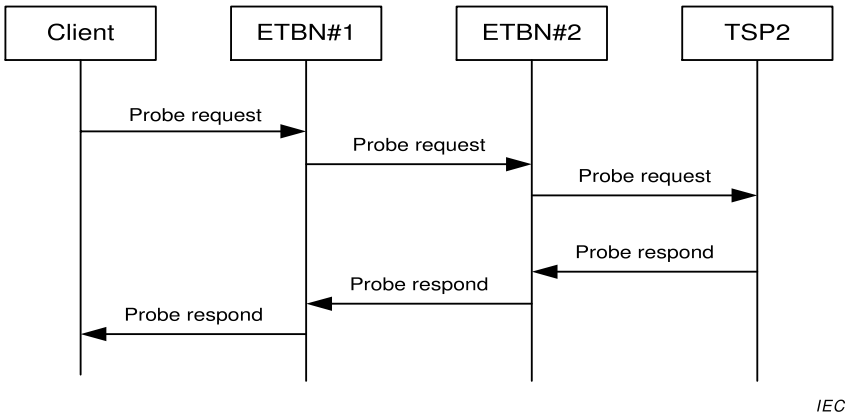



**Figure 9 – Message sequence for client and TSP2 within two consists**

a) CLIENT sends Probe out in consist 1;

b) ETBN#1 CN interface receives Probe, and passes it to WS-Discovery Proxy to handle it;

c) WS-Discovery Proxy does the target multicast address translation and sends it on ETB;

d) ETBN#2 ETB interface gets the Probe, and passes it to WS-Discovery Proxy to handle it;

e) WS-Discovery Proxy does the reverse proxy to get the original Probe, and sends it out in consist 2;

f) TSP2 gets the Probe and responds with Probe match;

g) WS-Discovery NAT-ALG within ETBN#2 gets the Probe match message, and does an address mapping and replacement before sending out over ETB;

h) ETBN#1 gets TSP2's Probe match from ETB, and send it to CLIENT;

i) CLIENT gets TSP2's Probe match with global address inside.

CLIENT can request service from TSP1 in consist 1 and TSP2 consist 2 now. As a service provider, it shall support the WS-discovery and discovery scheme defined above, support discovery configuration and scope operations as covered by device service.

# Annex A
(informative)

## Use case of on-board video surveillance/CCTV system

Scenario 1: Post-event incident assessment

This use case, related to the security of citizen and organizations (Figure A.1), is based on the post-event replay of the video(s) collected in the passenger compartment.

- During the train operation, the camera videos (and if available/permitted audio) of the passenger compartments are recorded continuously with metadata (e.g. date and time, camera name, consist name, train location) into the train on-board video recorders.
- When a serious incident occurs resulting in a passenger alarm on board the train, the video recorders tag and save a short video sequence (e.g. ±15 min) up to the legal storing time (generally physical storage capacity is lower than the legally authorized storing time).
- On request from competent authorities (generally the police), authorised staff retrieves the recorded video from on board the trains by replacing and conveying the storage medium to a ground facility.
- The authorized staff plays-back the video from the storage medium using a dedicated work station to locate the relevant video sequences.
- This authorized persons copies the required video sequences on a suitable digital storage medium (e.g. DVD)
  - without video degradation;
  - with metadata (at least date and time);
  - with all software programs required for replay without needing installation process (legacy systems) or in the ISO 22311 interoperable format
- The medium which contains the exported video sequences is handed-out to the competent authorities.

In this use case, especially for international trains, the rolling stock operator shall have ground facilities available at each main station, and compliance with ISO 22311 is essential for a timely process.

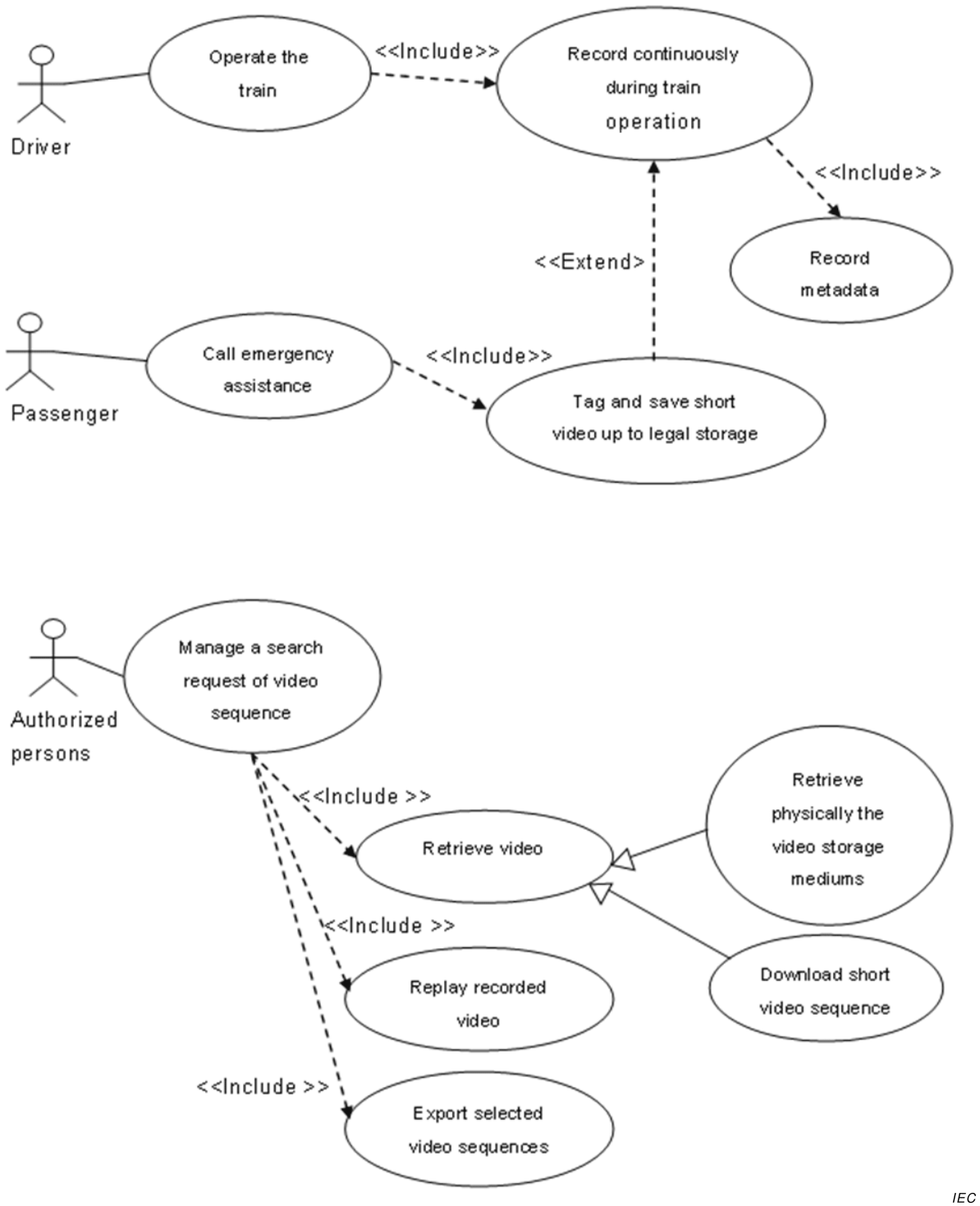



**Figure A.1 – Synthesis of use case 1**

Scenario 2: Live incident assessment

This use case, related to the security of citizen (Figure A.2) covers the situation where a passenger on board a train needs to call emergency assistance.

- A passenger on board a train presses the button to call emergency assistance.

- This action sends an alarm and provides the location of this alarm (e.g. train number, coach number, location in the coach, location of the train)
  - to the staff on board the train;
  - to the traffic regulation.
- The staff on board or the traffic regulation can assess the current context (camera(s) nearest to the emergency button) while having an audio connection with the passenger. Any other camera in the train can be used as required at any time.
- The staff on board or the traffic regulation may have the possibility to display the few minutes before the alarm by accessing to the video recorder on board the train (Figure A.4) to fully understand the origin of the problem.
- The staff on board or the traffic regulation closes the audio and video communication.
- Depending on the seriousness, emergency services or police will be asked to intervene. In some case, traffic may have to be interrupted.

If the train is a mix of consists, interoperability derived from this specification will allow a consistent behaviour wherever the incident occurs in the convoy (communications, video display and localization).

If the train operates on a third-party infrastructure, especially with international trains, and response is handed-out to the traffic regulation, this specification is crucial for making sure that the traffic regulation can handle all the trains travelling over its zone of control.

Detailed Scenario 2 with SBS block is shown in Figure A.3.

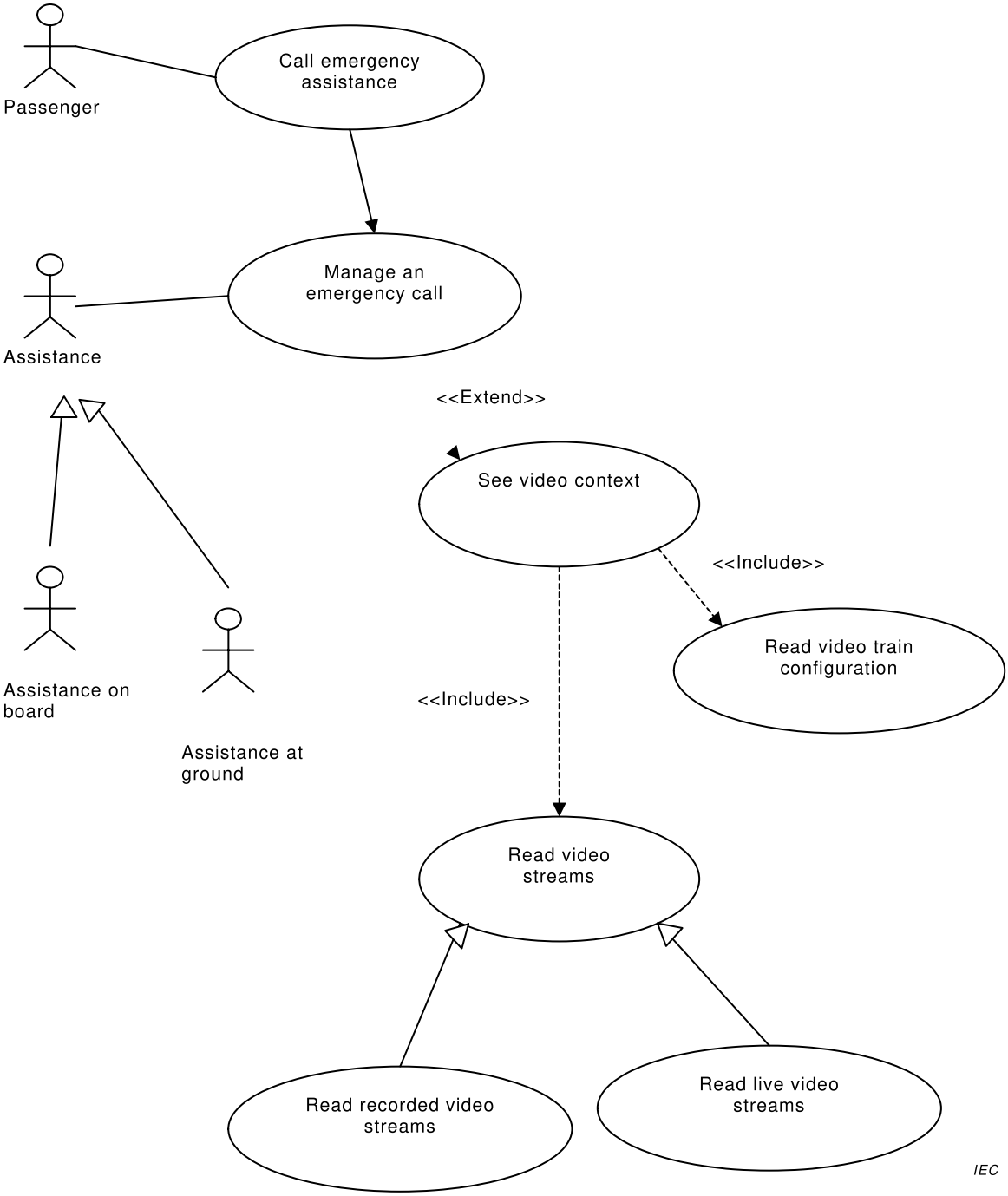



**Figure A.2 – Synthesis of use case 2**

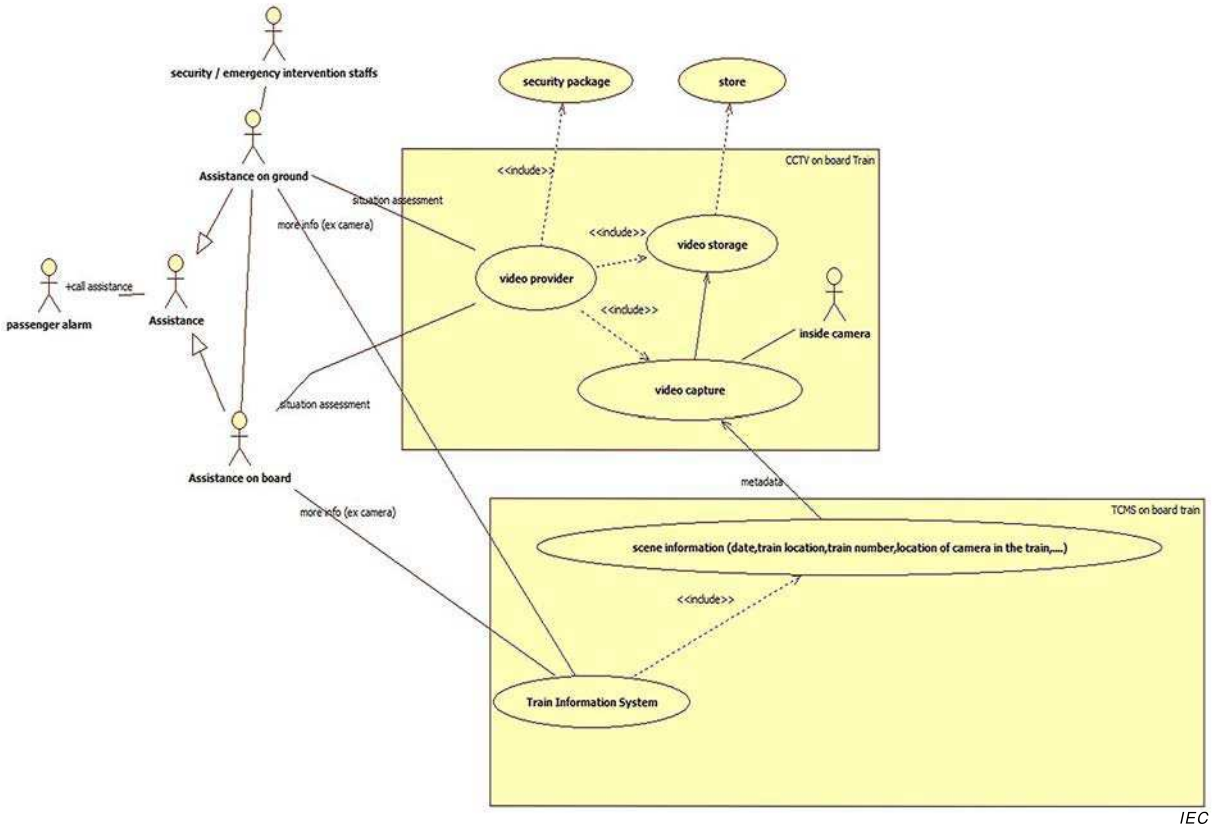



**Figure A.3 – Detailed Scenario 2 with SBS block**

Scenario 3: Platform surveillance for driver

This use case (Figure A.4) is related to driver-only train operation by enabling the driver to visually detect persons or passenger related items that are anywhere within the "dispatch corridor".

- The train stops at station.
- The display system in the cab of the driver shows the side cameras of the platform(s) wherefrom passengers enter the train, in the right order and direction and with a low latency. There are two cases:
  - the cameras belong to the train and are located on its flanks;
  - the cameras are fixed on the platform.
- The driver has the possibility to choose and display one camera at full screen (a selection done at the display level).
- Optionally the side cameras can be recorded by the on-board video recorder, as they are displayed to the driver.
- When the train has completely left the platform, the display system is blanked.

In the rare situation where the train is a mix of consists and train cameras are used, interoperability derived from this specification will allow a consistent behaviour, especially regarding sequencing and in latency.

If the train operates on a third-party infrastructure with platform cameras, especially with international trains, this specification is crucial for making sure that the systems communicate and perform in all stations, as described.

Detailed Scenario 3 with SBS block is shown in Figure A.5.

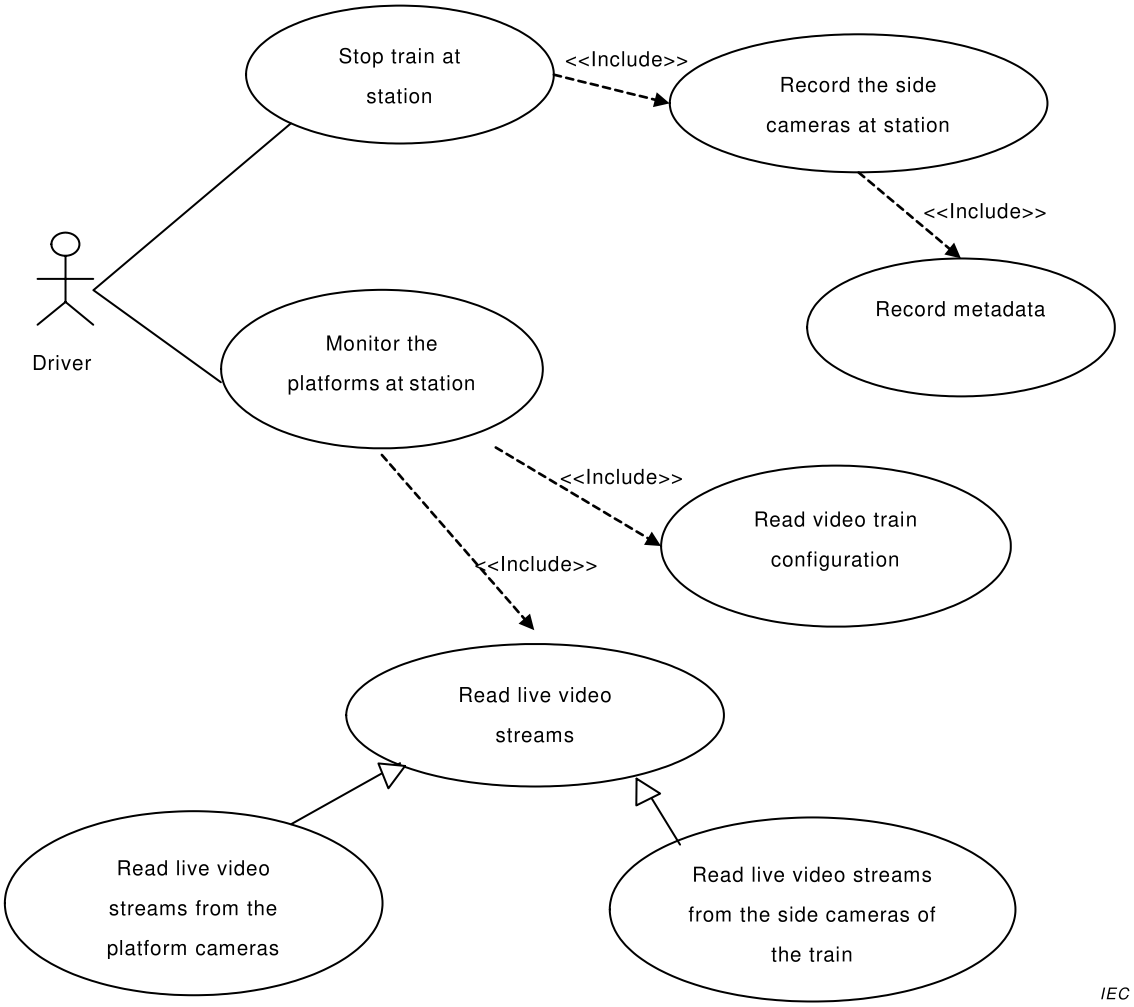



**Figure A.4 – Synthesis of use case**

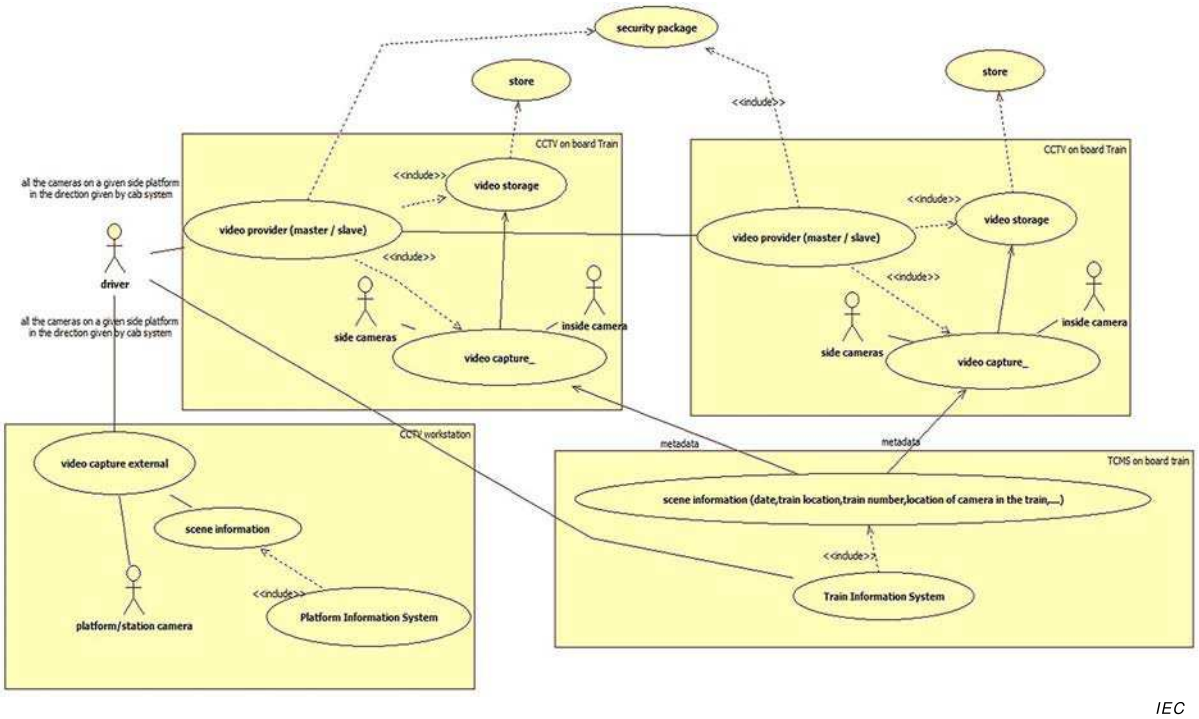



**Figure A.5 – Detailed Scenario 3 with SBS, two consists are displayed**

Scenario 4: Person accident at train door.

This use is an extension of Scenario 1.

A passenger falls between the train and the platform as the train arrives in a station and is badly injured.

Train will be released only when

- the injured passenger has been taken in charge by medical staff;
- police has collected all necessary information to classify the incident between an accident (due to a bad door closure or to passenger fault) or a crime (victim pushed).

Alternative 1 (Figure A.6): It is assumed that the train has on-board CCTV with transmission to a security centre with a capacity to visualize up to eight video streams at a time, with quality allowing situation assessment and search in on-board stored data.

- The staff at the security centre plays-back the video received from the on-board storage medium using a dedicated work station to locate the relevant video sequences.
- The authorized persons copies the required video sequences on a suitable digital storage medium (e.g. DVD)
  - without video degradation;
  - with metadata (at least date and time);
  - with all software programs required for replay without needing installation process (legacy systems) or in the ISO 22311 interoperable format.
- The medium which contains the exported video sequences is handed-out to the competent authorities.

  If the train operates on a third-party infrastructure (especially with international trains) and/or if transport police has a duplicated access to the trains, this specification is crucial for allowing the police to

– access to time stamped properly localized videos from the train, including for the last period;

– access also to the same type of videos from the platform cameras and synchronized display with videos from the train.

Alternative 2 (no diagram): There is no adequate transmission between the train and the security centre, and the sequence of Scenario 1 applies:

- The authorised person retrieves the right recorded video on board the trains by replacing and conveying the storage mediums to the ground facility.

Compliance with ISO 22311 is then essential for a timely process.

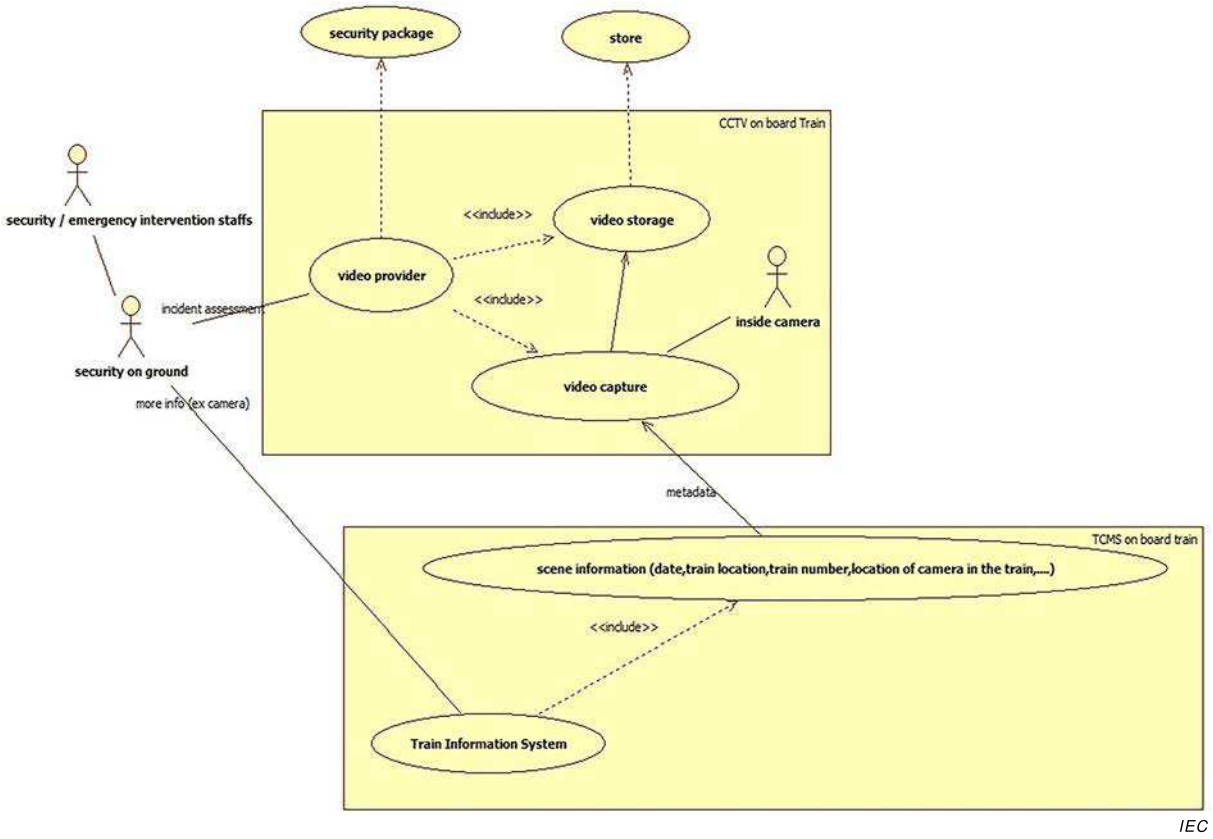



**Figure A.6 – Detailed Scenario 4 with SBS**

Scenario 5: Passengers raise an alarm at a door.

This use case (Figure A.7) combines Scenarios 2 and 4.

A passenger falls between the train and the platform as the train arrives in a station and is badly injured.

on-board staff/driver is alerted, communicates with passenger and sees the vicinity of the door from inside the train. Train/station staff calls emergency services indicating platform and approximate position on the platform.

Staff in charge at the security centre replays video from the nearest cameras in the train going backwards to see the incident time; several individuals are around near the door but no obvious incident visible.

Associated transport police called to see these videos asks for visualizing the videos from the matching platform cameras, based on train position and position of the relevant door in the train.

Option 1: It is obvious that incident is an accident due to passenger without any malfunction; train can be released.

Option 2: It is clear that two passengers were in an argument, one of them being the victim, the other one left the train at the station. Tracking of this individual is performed in the network of the station cameras, allowing good quality identification and interception; suspect negates any involvement.

Police needs the full quality video evidence to convince the suspect.

Full quality video recorded on the train and in the station is removed (physical cartridge swap or extraction of the relevant files through a specialized terminal). Staff of the security centre exports all the required video sequences in an interoperable format defined by ISO 22311 and gives them to the police.

As all collected files are as per ISO 22311, the forensics investigators can use only one single tool. They select in the extracted files the relevant scenes and run them on a multiple windows display to observe the same scene from different angles and assess the sequence of events in the five seconds preceding the event to see if the victim was pushed or not. It is obvious that in this process, the accuracy of the time stamping is important to well synchronize the video from different recorders to avoid misinterpretations.

This complex scenario, which may imply multiple operators and transborder situations, illustrates benefits of interoperability deriving from both this specification (especially using geo-location on train to match platform position and absolute time-stamping) and direct ISO 22311 implementation

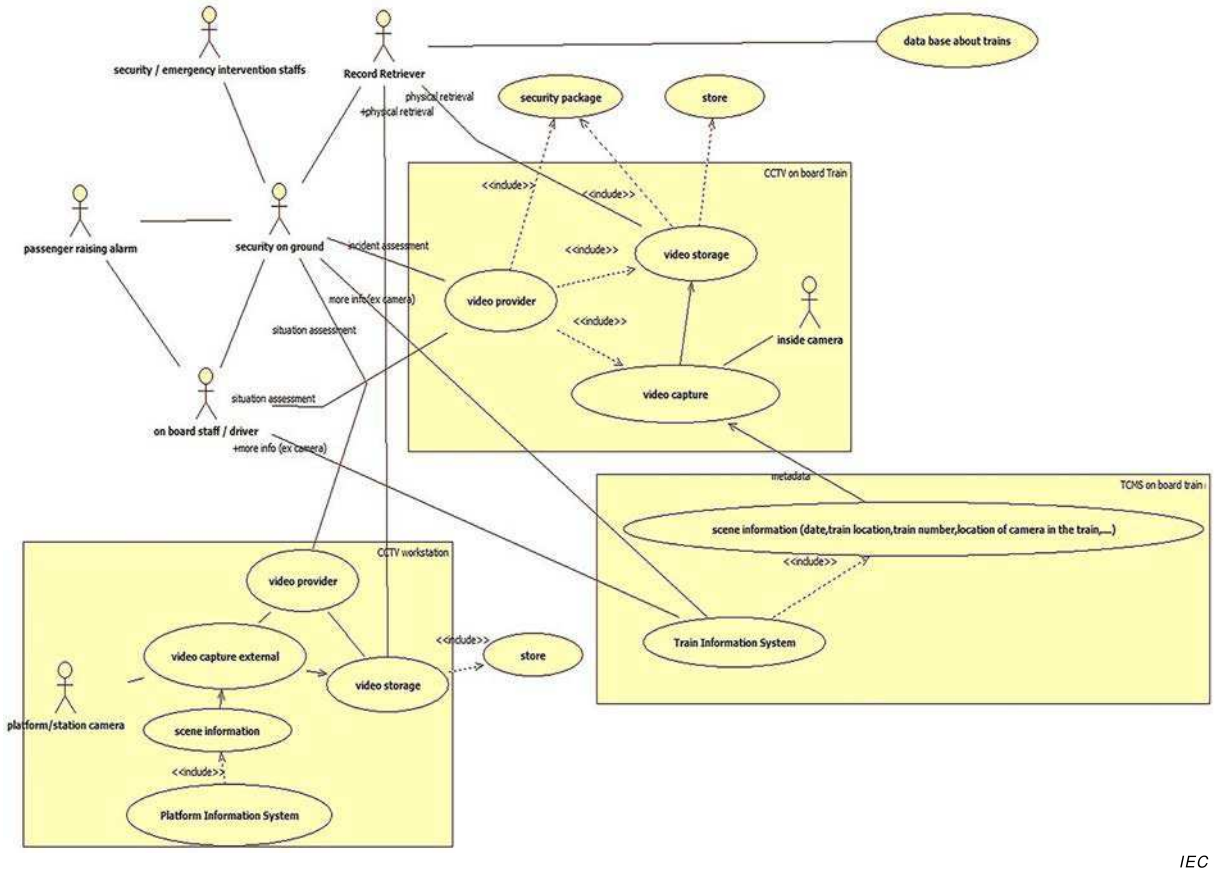



**Figure A.7 – Detailed Scenario 5 with SBS**

# Bibliography

IEC 61375-1, *Electronic railway equipment – Train communication network (TCN) – Part 1: General architecture*

IEC TS 61375-2-4, *Electronic railway equipment – Train Communication Network (TCN) – Part 2-4: TCN Application profile*

IEC 62498-1, *Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock*

IEC 62580 (all parts), *Electronic railway equipment – On-board multimedia and telematic subsystems for railways*

IEC 62676-2-1, *Video surveillance systems for use in security applications – Part 2-1: Video transmission protocols – General requirements*

IEC 62676-2-2, *Video surveillance systems for use in security applications – Part 2-2: Video transmission protocols – IP interoperability implementation based on HTTP and REST services*

IEC 62676-4*, Video surveillance systems for use in security applications – Part 4: Application guidelines*

ISO 14496-2, *Information technology – Coding of audio-visual objects – Part 2: Visual*

ISO/IEC 10918-1, *Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines*

ISO/IEC 14496-10, *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding*

ISO/IEC 14496-14, *Information technology – Coding of audio-visual objects – Part 14: MP4 file format*

ISO/IEC 23000-10, *Information technology – Multimedia application format (MPEG-A) – Part 10: Surveillance application format*

ITU-T G.711, *Pulse code modulation (PCM) of voice frequencies*

ITU T H.264, *Reference software for ITU-T H.264 advanced video coding*

ITU-T T.81, *Information technology – Digital compression and coding of continuous-tone still images – Requirements and guidelines*

ITU-T T.83, *Information technology – Digital compression and coding of continuous-tone still images: Compliance testing*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch