BS EN 50436-6:2015

BSI Standards Publication

Alcohol interlocks — Test methods and performance requirements

Part 6: Data security

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 50436-6:2015.

The UK participation in its preparation was entrusted to Technical Committee AUE/16, Data Communication (Road Vehicles).

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 81850 9

ICS 43.040.10; 71.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50436-6

March 2015

ICS 43.040.10; 71.040.40

English Version

Alcohol interlocks - Test methods and performance requirements - Part 6: Data security

Éthylotests antidémarrage - Méthodes d'essai et exigences de performance - Partie 6: Sécurité des données

Alkohol-Interlocks - Prüfverfahren und Anforderungen an das Betriebsverhalten - Teil 6: Datensicherheit

This European Standard was approved by CENELEC on 2014-12-29. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 50436-6:2015 E

Contents

Page

Foreword **5**
Introduction **6**
1 Scope **7**
1.1 General 7
1.2 Conformance claim 8
2 Normative references **8**
3 Terms and definitions **9**
4 General **11**
4.1 Use of the alcohol interlock 11
4.2 Major security features 11
4.3 Hardware, software and firmware not being part of the alcohol interlock and the service application 12
5 Alcohol interlock classes **12**
5.1 General 12
5.2 Class A: transparent service application without broker 12
5.3 Class B: transparent service application with broker 13
5.4 Class C: opaque service application 14
5.5 Class D: service application without broker and without register 15
6 Security objectives **15**
6.1 General 15
6.2 Security objectives for the alcohol interlock and the service application 16
6.3 Security objectives for the operational environment (informative) 18
6.3.1 Overview 18
6.3.2 General security objectives for the operational environment 19
6.3.3 Security objectives for the register 19
6.3.4 Security objectives for the broker 20
7 Security requirements **21**
7.1 Terms 21
7.2 Security Functional Requirements 22
7.2.1 General 22
7.2.2 FAU_GEN.1 Audit event records generation 23
7.2.3 FAU_STG.1 Protected data memory 24
7.2.4 FAU_STG.3 Action in case of possible event records loss 24
7.2.5 FAU_STG.4 Prevention of event records loss 24
7.2.6 FCS_COP.1(1) Cryptographic operation 24
7.2.7 FCS_COP.1(2) Cryptographic operation 25
7.2.8 FCS_COP.1(3) Cryptographic operation 25
7.2.9 FDP_ACC.1 Subset access control 25
7.2.10 FDP_ACF.1 Security attribute based access control 25

7.2.11 FDP_ITT.1 Basic internal transfer protection 26
7.2.12 FDP_ITT.3 Integrity monitoring 27
7.2.13 FDP_RIP.1 Subset residual information protection 27
7.2.14 FIA_UAU.2 User authentication before any action (not applicable if the authentication is done in the operational environment) 27
7.2.15 FIA_UID.2 User identification before any action (not applicable if the authentication is done in the operational environment) 27
7.2.16 FPT_PHP.1(1) Passive detection of physical attack 28
7.2.17 FPT_PHP.1(2) Passive detection of physical attack 28
7.2.18 FPT_STM.1 Reliable time stamps 28
7.3 Cryptographic algorithms 28
7.4 Security assurance requirements 29
Annex A (informative) **Security problem definition** **30**
A.1 General **30**
A.2 Assets **30**
A.3 Threat agents **30**
A.4 Threat overview **30**
A.5 Threats **32**
A.5.1 Interfering with the sensors and the signals to the vehicle (I) **32**
A.5.2 Prevention of detection of events (II) **33**
A.5.3 Prevention of generation of event records or generation of undesirable event records (III) **33**
A.5.4 Failure to correctly store event records in the alcohol interlock (IV) **33**
A.5.5 Failure to correctly transfer event records between alcohol interlock and service application (V) **34**
A.5.6 Failure to correctly handle the event records in the service application (VI) **34**
A.5.7 Failure to correctly transfer event records between service application and register (VII) **35**
A.5.8 Failure to correctly register event records at the register (VIII) **35**
A.5.9 Failure to correctly transfer event records between service application and broker (IX) **35**
A.5.10 Failure to correctly convert event records at the broker (X) **36**
A.5.11 Failure to correctly transfer event records between broker and register (XI) **36**
Annex B (informative) **Rationales** **37**
B.1 General **37**
B.2 Security objectives rationale **37**
B.2.1 Interfering with the sensors and the signals to the vehicle (I) **37**
B.2.2 Prevention of detection of events (II) **38**
B.2.3 Prevention of generation of event records or generation of undesirable event records (III) **38**
B.2.4 Failure to correctly store event records in the alcohol interlock (IV) **39**
B.2.5 Failure to correctly transfer event records between alcohol interlock and service application (V) **40**
B.2.6 Failure to correctly handle the event records in the service application (VI) **41**
B.2.7 Failure to correctly transfer event records between service application and register (VII) **42**
B.2.8 Failure to correctly register event records at the register (VIII) **44**

B.2.9 Failure to correctly transfer event records between service application and broker (IX) **44**
B.2.10 Failure to correctly convert event records at the broker (X) **46**
B.2.11 Failure to correctly transfer event records between broker and register (XI) **46**
B.3 Security requirements rationale **47**
B.4 Dependencies **51**
Annex C (informative) **Security testing** **52**
Annex D (informative) **Use of this standard** **53**
D.1 Additional information required to use this standard **53**
D.2 Additional requirements for the data handling process **53**
Blibliography **55**

Foreword

This document (EN 50436-6:2015) has been prepared by CLC/BTTF 116-2 "Alcohol interlocks".

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-12-29
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2017-12-29

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

Introduction

The series of European Standards EN 50436 specifies test methods and essential performance requirements for alcohol interlocks and gives guidance for decision makers, purchasers and users. The content and requirements of the European Standard EN 50436-1 "Alcohol interlocks – Test methods and performance requirements, Part 1: Instruments for drink-driving-offender programs" are based on the experience and necessities of drink driving offender programmes in different countries over several decades.

The present document should be used in conjunction with the European Standard EN 50436-1 and optionally with EN 50436-2. It defines additional requirements for the security of event records which are stored in the data memory of the alcohol interlock and which may be downloaded, processed and transferred to supervising persons or organizations.

The security objectives describing how the threats are addressed are divided into security objectives for the alcohol interlock with the service application and for the operational environment.

The security objectives for the alcohol interlock and the service application describe what is necessary for the alcohol interlock and the service application to do to address the threats. In the context of this European Standard, the combination of alcohol interlock and service application are to meet all listed security objectives, and this is to be assessed as part of determining compliance with this European Standard.

The security objectives for the operational environment describe what other entities should do to address the threats. In the context of this European Standard, whether these entities actually achieve these objectives are not to be assessed as part of determining compliance with this European Standard. Therefore, in this European Standard these security objectives are informative only.

This European Standard is intended also to be listed as a Protection Profile for alcohol interlocks under the Common Criteria Recognition Arrangement and the Senior Officials Group - Information Systems Security (SOG-IS). For the purpose of being a Protection Profile, all sections (including also the operational environment) are considered normative.

1 Scope

1.1 General

This European Standard specifies security requirements for the protection and handling of event records which are stored in the data memory of breath alcohol controlled alcohol interlocks and which may be downloaded, processed and transferred to supervising persons or organizations.

This European Standard is a supplement to EN 50436-1. It is to be decided by the respective jurisdiction whether the present standard has to be applied in addition to EN 50436-1.

This European standard may also be used as a supplement to EN 50436-2 if a jurisdiction or a vehicle fleet operator decides that the data security in his preventive application has to have the same high level of requirements as for alcohol interlocks used in drink-driving-offender programmes.

This European Standard is mainly directed to test houses, manufacturers of alcohol interlocks, legislating authorities and organizations which handle and use the alcohol interlock event records.

In this European Standard, the alcohol interlock consists basically of handset and control unit. Optional accessory devices (e.g. cameras or GPS systems generating data related to event data of the alcohol interlock, as well as accessory devices handling or transferring data for a drink-driving-offender programme) authorized by the manufacturer as being part of the alcohol interlock system and which are intended to be used in the vehicle during operation are also to be considered part of the alcohol interlock, where applicable.

The service application communicates with the alcohol interlock and sends out the event records to a register, either directly or alternatively indirectly through a broker.

The scheme is depicted in Figure 1. It also shows which parts are within the scope of this European Standard and which are outside of the scope.

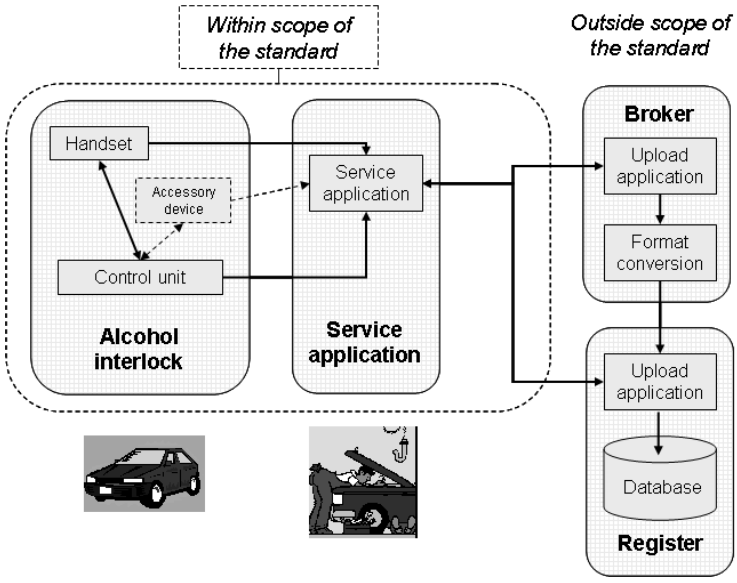

Figure 1 – Alcohol interlock, service application, broker and register

NOTE In this, and all other figures, the direction of the arrows indicates the flow of event records.

This European Standard applies to

– the alcohol interlock,

– the service application.

This European Standard does not apply to

– data security of the broker,

– data security of the register,

– storage of downloaded data,

– requirements for organizational processes, for example defining rights of access to the data.

1.2 Conformance claim

This European Standard conforms according to the Common Criteria for Information Technology Security Evaluation as Protection Profile to:

– Common Criteria, Version 3.1, Revision 4, as defined by CCp1, CCp2, CCp3 and CEMe,

– Common Criteria - Part 2 as Common Criteria - Part 2 conformant,

– Common Criteria - Part 3 as Common Criteria - Part 3 conformant.

NOTE 1 An earlier revision of CCp1 is published as ISO/IEC 15408-1.

NOTE 2 An earlier revision of CCp2 is published as ISO/IEC 15408-2.

NOTE 3 An earlier revision of CCp3 is published as ISO/IEC 15408-3.

NOTE 4 An earlier revision of CEMe is published as ISO/IEC 18045.

This European Standard is not based on any other Protection Profile.

This European Standard conforms to the evaluation assurance level EAL3 + ALC_FLR.2 (for explanation see 7.4).

Protection profiles or security targets that conform to this Protection Profile shall apply "Strict Protection-Profile-Conformance".

For more information, see CCp1, Annex B5.

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.

EN 50436-1:2014, *Alcohol interlocks – Test methods and performance requirements – Part 1: Instruments for drink-driving-offender programs*

EN 50436-2:2014, *Alcohol interlocks – Test methods and performance requirements – Part 2: Instruments having a mouthpiece and measuring breath alcohol for general preventive use*

3 Terms and definitions

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

3.1
alcohol interlock
device which is normally in the blocking state when installed to prevent the starting of a vehicle engine, and which can be brought into the not-blocking state only after the presentation and analysis of an accepted breath sample with an alcohol concentration below a limit value

Note 1 to entry: In this European Standard the expression “starting of the vehicle engine” includes provision of an output signal from the alcohol interlock to the vehicle to enable the starting or operation of the vehicle.

Note 2 to entry: In this European Standard, the alcohol interlock consists of the following parts: handset, control unit and optional accessory devices.

Note 3 to entry: According to the Common Criteria the alcohol interlock and the service application are the Target of Evaluation (TOE).

3.2
handset
part of the alcohol interlock which is usually located inside the driver compartment of the vehicle, which contains an alcohol measuring system, may store event records in a data memory, is connected to the control unit and is able to interact with the driver

3.3
control unit
part of the alcohol interlock which is usually located under the dashboard of the vehicle, which is electrically connected to the vehicle to prevent or to allow the starting of the vehicle engine, and which may store event records in a data memory

Note 1 to entry: The electrical connections to the vehicle are considered to be part of the control unit.

3.4
accessory device
optional supplementary device being part of the alcohol interlock intended to be used in the vehicle during operation

Note 1 to entry: Accessory devices may for example be a camera or a module for data transmission.

Note 2 to entry: The use of certain accessory devices may be required by national regulations.

3.5
event records
record of breath test results, other events and supporting data with date and time generated by the alcohol interlock

Note 1 to entry: For this European Standard it is assumed that the event records are stored in the data memory of the control unit and/or of the handset and optionally of the accessory devices.

Note 2 to entry: This European Standard uses the term “event records" instead of the Common Criteria term “audit records”.

3.6
service application
computer programme being used for functions such as adjustment of the alcohol interlock, downloading and optionally viewing the event records and other data of the alcohol interlock, as well as for uploading event records from the alcohol interlock to a register or broker

Note 1 to entry: A service application may have some or all of these functions, depending on its implementation and the alcohol interlock class (see Clause 5).

Note 2 to entry: The service application is usually located inside a service centre.

Note 3 to entry: The service application may be used by a technician or an automatic system.

Note 4 to entry: The service application may be either transparent or opaque.

3.7
transparent service application
service application which is not able to decrypt the event records

Note 1 to entry: The functionality of the transparent service application for uploading event records from the alcohol interlock to a register or broker may be incorporated into the alcohol interlock. In this case the alcohol interlock uploads the event records to the register or boker.

3.8
opaque service application
service application that is able to decrypt the event records and performs the required conversion of event records

3.9
adjustment
operation that calibrates and/or adjusts the sensor systems, sets parameters and/or changes the firmware of the alcohol interlock

3.10
register
central register of event records, which stores the event records for future use

Note 1 to entry: The register is usually operated by the alcohol interlock manufacturer and/or the authorities.

3.11
broker
processing centre which converts the records into a required format and then sends them to the register or the service application

Note 1 to entry: The broker is usually operated by the service provider of the alcohol interlock.

3.12
security target
description and analysis of the assets, the threats to those assets, the countermeasures (in the form of security objectives) and a demonstration that the countermeasures are sufficient to counter the threats

Note 1 to entry: For details see CCp1, clause 7.1.1.

3.13
security objective
concise statement of the intended solution to the problem defined by the security problem definition

Note 1 to entry: For details see CCp1, clause A.7.

3.14
security problem definition
statement which in a formal manner defines the nature and scope of the security that the alcohol interlock and the service application are intended to address, consisting of a combination of threats to be countered by the alcohol interlock and the service application, the organizational security policies enforced by the alcohol interlock and the service application, and the assumptions that are upheld for the alcohol interlock and the service application and their operational environment

Note 1 to entry: For details see CCp1, clause A.6.

3.15
operational environment
environment in which the alcohol interlock and the service application are operated, containing all entities that the alcohol interlock and the service application interact with, such as broker, register service centre, vehicle, driver

4 General

4.1 Use of the alcohol interlock

Before the engine of the vehicle can start, the driver has to deliver an accepted breath sample into the handset. If the measured alcohol concentration is equal to or above the limit value, the control unit does not allow the vehicle engine to start.

At random intervals while driving, the driver may have to deliver an additional accepted breath sample into the handset. Passing or failing a breath alcohol test generates event records. Additionally, other events may generate event records (e.g. interruption of power to the control unit, or vehicle motion without starting of the motor, indicating bypass of the alcohol interlock).

At set intervals, when the memory of the alcohol interlock fills up, or after certain events the handset instructs the driver to go to a service centre. These service centres (which are for drink-driving-offender programmes normally certified by the government) possess a service application. Service centre personnel can use the service application to read out (download) the encrypted event records from the alcohol interlock.

NOTE The service application may or may not decrypt these event records (see Clause 5).

The service application sends out the event records:

– directly to the register, or

– to the broker which sends the event records to the register, or

– to the broker which sends the event records back to the service application and which then sends it to the register.

The service application requires a confirmation from the register and/or broker that it has received the event records. Upon reception of this confirmation, the service centre personnel may use the service application to delete the event records by erasing the data memory in the alcohol interlock.

4.2 Major security features

The alcohol interlock has the following major security features:

– The alcohol interlock is able to detect events (for example starting the vehicle engine or failed breath test) and store these events;

– Authenticated service personnel can use the service application to read out these event records and send them onwards. The service personnel can also use the service application to delete the event records and erase the data memory;

– All parts of the alcohol interlock protect the event records against unauthorized modification, deletion, insertion and disclosure.

4.3 Hardware, software and firmware not being part of the alcohol interlock and the service application

The alcohol interlock requires installation in a vehicle.

The service application may require an operating system and computer or similar setup in order to function. The security target shall clarify the required hardware, software or firmware (if applicable) required for the service application.

NOTE This depends on the class of the alcohol interlock (see Clause 5).

5 Alcohol interlock classes

5.1 General

This European Standard defines different classes of alcohol interlocks with their service application (A, B1, B2, C1, C2 and D), each of which has slightly different requirements and objectives.

The security target shall define the class of the alcohol interlock (as part of the alcohol interlock overview).

This difference in classes is caused by the following facts.

– The register has a strictly defined format in which it wishes to store event records. As there is no standard for this format yet, each country or organization tends to use its own proprietary format.

– The alcohol interlock may not be able to support all of these formats.

If the alcohol interlock does not support the required format, the files have to be converted somewhere:

– either in the service application, or

– at the broker.

As event records can only be converted when they are not encrypted, they are very vulnerable to unauthorized reading or modification at that point, so special care shall be taken to prevent this.

There may also be alcohol interlocks only using the service application, but not using a register and/or broker, or alcohol interlocks not storing event records at all.

5.2 Class A: transparent service application without broker

Transparent refers to the fact that the service application is not able to decrypt the event records.

This class of alcohol interlocks is characterized by end-to-end encryption between the alcohol interlock and the register. The alcohol interlock already generates the event records in the correct format required by the register. This is depicted in Figure 2.

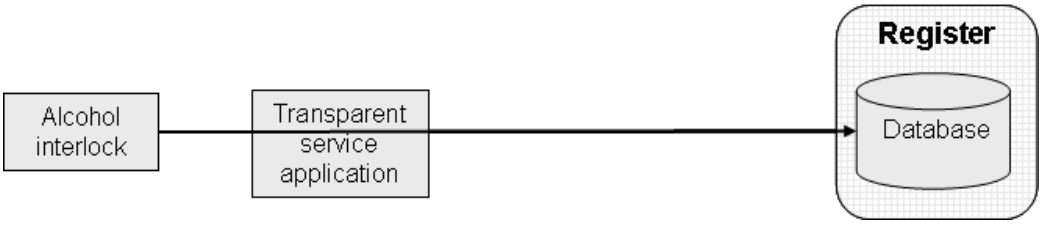

**Figure 2 – Class A alcohol interlock:
the alcohol interlock generates the correct format for the register**

In class A alcohol interlocks:

– the service application never gets access to the unencrypted event records and therefore the service application itself requires relatively little protection;

– there is no broker, so threats for the broker are not relevant and there are no security objectives for the broker.

5.3 Class B: transparent service application with broker

Transparent refers to the fact that the service application is not able to decrypt the event records.

For this class of alcohol interlocks, the broker performs the required conversion. This means that the broker has access to unencrypted event records, and should therefore protect them.

Two subclasses of class B alcohol interlocks are to be distinguished:

– *Class B1 alcohol interlocks:*

The service application sends the event records to the broker. The broker converts the event records, and sends the converted event records onwards to the register. This is depicted in Figure 3.

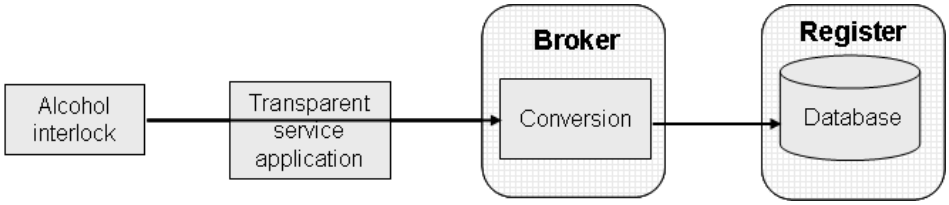

**Figure 3 – Class B1 alcohol interlock:
the broker converts and sends to the register**

– *Class B2 alcohol interlocks:*

The service application sends the event records to the broker. The broker converts the event records, and sends the converted event records back to the service application. The service application then sends the converted event records onwards to the register. This is depicted in Figure 4.

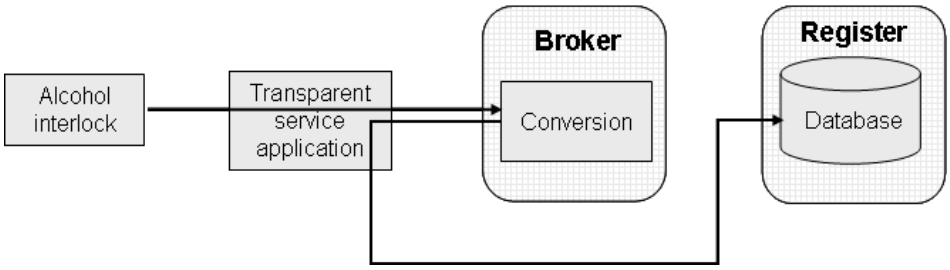

**Figure 4 – Class B2 alcohol interlock:
the broker converts and sends to the service application**

In class B alcohol interlocks:

– the service application never gets access to the unencrypted event records and therefore the service application itself requires relatively little protection;

– a broker is required, so there are threats and objectives for the broker.

5.4 Class C: opaque service application

Opaque refers to the fact that the service application performs the required conversion.

This means that the service application has access to unencrypted event records, and shall therefore be able to protect them.

It is distinguished between two subclasses of alcohol interlocks:

Two subclasses of class C alcohol interlocks are to be distinguished:

– *Class C1 alcohol interlocks:*

  The service application itself shall provide the protection. This means that the service application shall partly consist of some sort of tamper-evident and/or tamper-responsive hardware.

– *Class C2 alcohol interlocks:*

  The environment of the service application shall provide the protection. The service application may then be a simple software application running on a non-alcohol interlock workstation, but the environment of that workstation shall meet stringent requirements to be able to protect the event records.

This is depicted in Figure 5.

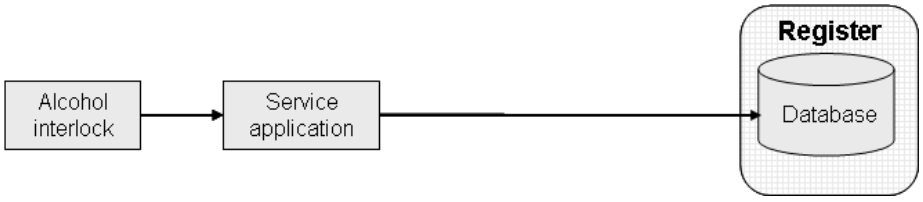

**Figure 5 – Class C1 and C2 alcohol interlock:
the service application converts the event records**

In class C alcohol interlocks:

– there is no broker utilized;

– so threats for the broker are not relevant and there are no security objectives for the broker.

5.5 Class D: service application without broker and without register

This class of alcohol interlocks uses only a service application.

There are no broker and no register involved. The event records may be stored in and seen with the service application. This is depicted in Figure 6.

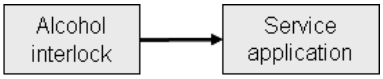

**Figure 6 – Class D alcohol interlock:
the event records are transferred to the service application**

In class D alcohol interlocks:

– there is no broker and no register utilized;

– so threats for the broker and register are not relevant and there are no security objectives for the broker and the register.

6 Security objectives

6.1 General

These security objectives describe how the threats described in Annex A are addressed. It is divided into (see Figure 7):

– The security objectives for the alcohol interlock and the service application ("O"), describing what the alcohol interlock and the service application shall do to address the threats. In the context of this European Standard, the combination of alcohol interlock and service application shall meet all security objectives that are listed for their class, and this shall be assessed as part of determining compliance with this European Standard.

– The security objectives for the operational environment ("OE"), describing what other entities should do to address the threats. In the context of this European Standard, whether these entities actually achieve these objectives are not to be assessed as part of determining compliance with this European Standard. Therefore, these security objectives are informative only.

A rationale that the combination of all of these security objectives indeed addresses the threats is found in Annex B of this standard.

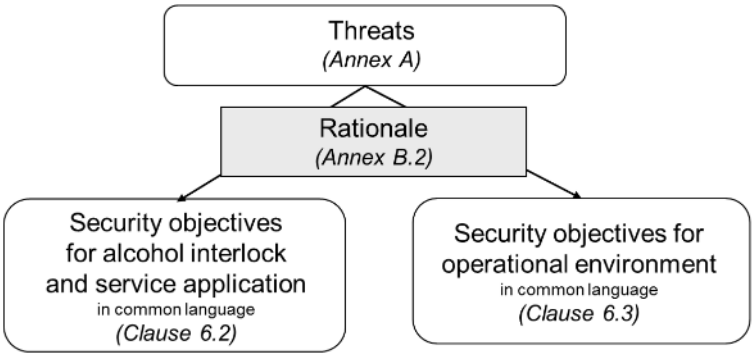

Figure 7 – Relations between threats and security objectives

6.2 Security objectives for the alcohol interlock and the service application

Clause 5 defines several classes of alcohol interlocks, which differ from each other in various aspects. This chapter describes a number of security objectives, but not all security objectives are valid for all classes. This is indicated in Table 1.

Table 1 - Objectives for different classes of alcohol interlocks

Objective	A	B1	B2	C1	C2	D
O.DETECT_EVENTS	X	X	X	X	X	X
O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_ CONTROL_UNIT_AND_ACCESSORY_DEVICE	X	X	X	X	X	X
O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK	X	X	X	X	X	X
O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE	X	X	X	X	X	X
O.TAMPER_EVIDENT_SERVICE_APPLICATION				X		
O.NO_OVERFLOW_IN_DATA_MEMORY	X	X	X	X	X	X
O.ALCOHOL_INTERLOCK_AND_SERVICE_APPLICATION	X	X	X	X	X	X
O.SERVICE_APPLICATION_AUTHENTICATION	X	X	X	X	X	X
O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS	X	X	X	X	X	X
O.SEND_TO_CORRECT_PARTY	X	X	X	X	X	

O.DETECT_EVENTS

The alcohol interlock shall detect:

– all events required by the applicable laws and regulations,

– adjustment of the alcohol interlock,

– other events and supporting data,

– deletion of event records.

O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_CONTROL_UNIT_AND_ ACCESSORY_DEVICE

The handset, control unit and accessory devices shall protect information about detected events as this is exchanged between them against insertion, deletion and modification.

O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK

The alcohol interlock shall store all required information for each event in event records in the data memory of the alcohol interlock.

Each event record shall contain at least:

– the information required by the applicable laws and regulations,

– a unique consecutive number for each event record.

The alcohol interlock shall not store event records on events that are not allowed to be recorded.

The alcohol interlock shall store all event records in such a way that they cannot be read or modified by unauthorized entities.

The alcohol interlock shall encrypt all event records before allowing them to be read out in such a way that they cannot be read or modified by unauthorized entities.

NOTE 1 The consecutive numbers may solve part of the protection against modification, but other measures (for example MAC, CRC inside the encryption or CBC-mode) may also be necessary, depending on the implementation.

The event records shall be encrypted before storing them.

O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE

The handset, control unit, accessory devices and connections from the control unit to the vehicle shall be tamper-evident. Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

O.TAMPER_EVIDENT_SERVICE_APPLICATION

The service application shall be tamper-evident. Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

O.NO_OVERFLOW_IN_DATA_MEMORY

When the memory of the alcohol interlock is filled with event records for:

– 90 %, the alcohol interlock shall issue an early recall warning to the driver,

– 100 %, the alcohol interlock shall no longer allow the vehicle engine to start.

O.ALCOHOL_INTERLOCK_AND_SERVICE_APPLICATION

The alcohol interlock shall only allow the service application to:

– read out event records from the alcohol interlock,

– delete event records from the alcohol interlock,

– adjust the alcohol interlock.

NOTE 2 This does not preclude the access to the alcohol interlock by specific programmes used for example during production and/or maintenance of the alcohol interlock by the manufacturer on his premises or during verification.

O.SERVICE_APPLICATION_AUTHENTICATION

Before service personnel can use the service application, this service personnel shall first be identified and authenticated.

NOTE 3 “Be identified and authenticated” does not mandate that the service application shall perform identification and authentication itself. It is allowed for the environment (the operation system, a remote web server or other entity) to perform this identification and authentication.

O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS

The service application shall not allow its service personnel (or other entities) to insert or modify event records. The service application shall not allow unauthorized service personnel to read event records from the service application.

O.SEND_TO_CORRECT_PARTY

The service application shall send the event records only to the correct party in the correct manner in such a way that they cannot be read or modified by unauthorized entities.

The service application shall be able to receive a confirmation that the event records have been correctly received and shall record the confirmation in the alcohol interlock.

– For class B1 alcohol interlocks, the event records shall be sent to the broker, using the method specified by the broker, and the confirmation should be received from the broker.

– For class B2 alcohol interlocks, the event records shall be sent to the broker, using the method specified by the broker, then the event records received by the broker should be sent to the register, using the method specified by the register, and the conformation shall be received by the service application from the register.

– For all other classes of alcohol interlocks, the event records shall be sent to the register, using the method specified by the register, and the confirmation shall be received by the service application from the register.

6.3 Security objectives for the operational environment (informative)

6.3.1 Overview

Clause 5 defines several classes of alcohol interlocks, which differ from each other in various aspects. This chapter describes a number of security objectives, but not all security objectives are valid for all classes. This is indicated in Table 2.

Table 2 - Objectives for different classes of alcohol interlocks

Objective	A	B1	B2	C1	C2	D
OE.INTERLOCK_EN_50436-1_OR_EN_50436-2	X	X	X	X	X	X
OE.DELETE_ONLY_AFTER_CONFIRMATION	X	X	X	X	X	X
OE.PROTECTED_SERVICE_APPLICATION					X	
OE.REGISTER_PROTECT_INCOMING_RECORDS	X	X	X	X	X	
OE.REGISTER_PROTECT_RECORDS	X	X	X	X	X	
OE.REGISTER_CHECK_AND_CONFIRM	X	X	X	X	X	
OE.BROKER_PROTECT_INCOMING_RECORDS		X	X			
OE.BROKER_PROTECT_RECORDS		X	X			
OE.BROKER_CORRECT_CONVERSION		X	X			
OE.BROKER_SEND_TO_CORRECT_PARTY		X	X			
OE.BROKER_RELAY_CONFIRMATION		X	X			

6.3.2 General security objectives for the operational environment

OE.INTERLOCK_EN_50436-1_OR_EN_50436-2

The interlock should be type tested and fulfil the requirements according to EN 50436-1 and/or EN 50436-2.

OE.DELETE_ONLY_AFTER_CONFIRMATION

The service personnel using the service application should delete event records from the alcohol interlock only when a confirmation has been received that these event records have been correctly received.

OE.PROTECTED_SERVICE_APPLICATION

The service centre environment should use a combination of technical and organizational means to ensure that unauthorized modification, deletion, insertion and/or reading of event records that are processed by the service centre is impossible.

6.3.3 Security objectives for the register

OE.REGISTER_PROTECT_INCOMING_RECORDS

The register should provide an application to entities that wish to provide event records to it. This application should provide:

– authentication of the sender,

– detection of any modification or insertion of event records while in transit,

– prevent third parties reading the event records while in transit.

The register only should accept event records provided to it through this application.

OE.REGISTER_PROTECT_RECORDS

The register should use a combination of technical and organizational means to prevent unauthorized modification, deletion, insertion, retention and/or reading of event records that are stored in the register.

OE.REGISTER_CHECK_AND_CONFIRM

The register should check all event records that it receives (after possibly converting them) for completeness and reply the result of this check to the sender of the event records (either broker or service application).

6.3.4 Security objectives for the broker

OE.BROKER_PROTECT_INCOMING_RECORDS

The broker should offer a means of transfer of event records from service applications to itself (e.g. a https connection). This means of transfer should ensure that:

– the sender is authenticated,

– the event records cannot be read by unauthorized entities while in transfer,

– modification, insertion and deletion of event records can be detected.

OE.BROKER_PROTECT_RECORDS

The broker should use a combination of technical and organizational means to prevent unauthorized modification, deletion, insertion, retention and/or reading of event records that are processed by the broker.

NOTE National regulations may require, that the broker permanently deletes all copies of or parts of event records once the register indicates that the event records have been received correctly.

OE.BROKER_CORRECT_CONVERSION

The broker should convert the event records into a prescribed format of event records. The broker should demonstrate by rigorous testing that:

– the converted event records contain all the information required by the applicable laws and regulations,

– the converted event records are in the required format,

– the information in the converted event records is correctly derived from the information in the original event records.

The required format should be defined by national regulations.

OE.BROKER_SEND_TO_CORRECT_PARTY

The broker should send the event records only to the correct party:

– for class B1 alcohol interlocks to the register, using the register supplied application,

– for class B2 alcohol interlocks, to the service application. Before sending the event records, the broker shall encrypt the event records such that:

  – the event records can only be read by the register,

– modification, insertion and deletion of the event records can be detected.

OE.BROKER_RELAY_CONFIRMATION

The broker should relay the result of the check by the register to the service application.

If the broker receives the result of the register check (see OE.REGISTER_CHECK_AND_CONFIRM), the broker should relay this result to the service application.

7 Security requirements

7.1 Terms

The following terms are used in the security requirements.

Subjects/external entities:

– handset,

– control unit,

– accessory device,

– service application,

– register,

– broker.

All of these are defined in Clause 3. They have no security attributes.

Objects:

– alcohol interlock (treated as object by the adjust operation),

– event records.

All of these are defined in Clause 3. They have no security attributes.

Operations:

– Adjust: an operation that adjusts the alcohol interlock.

– Read: an operation that reads non-encrypted event records.

– Readout: an operation that makes a local copy of encrypted event records without decrypting them.

– Convert: an operation that creates a new set of event records from an old set in a different syntactic format.

– Delete: an operation that permanently removes event records.

– Broker-send: an operation that sends event records to the broker by a method approved by that broker.

– Register-send: an operation that sends event records to the register by a method approved by that register.

– Receive: an operation that receives a confirmation or a set of event records.

7.2 Security Functional Requirements

7.2.1 General

These security functional requirements are a more exact description of the security objectives for the alcohol interlock listed in 6.2 (see Figure 8). They are written in a special “security language” defined in the Common Criteria CCp. The use of this language ensures that the requirements do not allow for ambiguity or misinterpretation by an evaluator and that they are testable.

The evaluation of an alcohol interlock determines whether or not a specific alcohol interlock meets the security functional requirements in this section.

A demonstration that the combination of all of these security functional requirements indeed addresses the security objectives for the alcohol interlock may be found in A.2.

NOTE Throughout this clause, the term "TSF " (TSF = TOE Security Functionality; TOE = Target Of Evaluation = alcohol interlock and service application) has been refined many times to show to which part of the TSF the SFRs (Security Functional Requirements) apply. These refinements are printed in bold type.

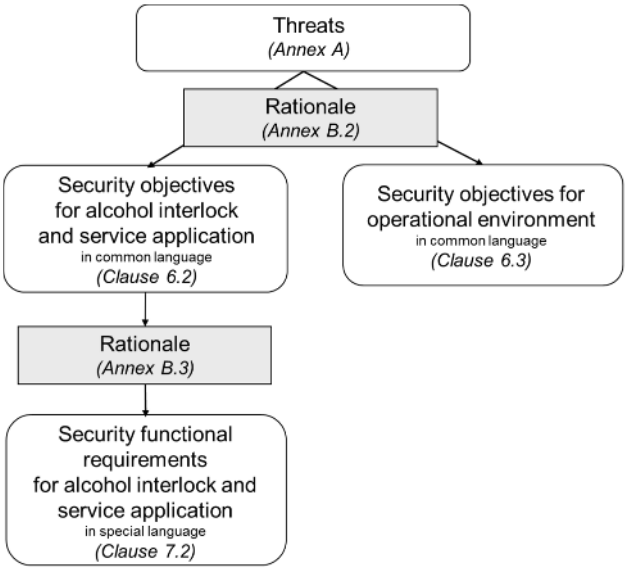

Figure 8 – Relations between threats, security objectives and security functional requirements

Clause 5 defines several classes of alcohol interlocks, which differ from each other in various aspects. This chapter describes a number of security requirements, but not all security requirements are valid for all classes. This is indicated in Table 3.

Table 3 - Security requirements for different classes of alcohol interlocks

Security requirement		A	B1	B2	C1	C2	D
FAU_GEN.1	Audit event records generation	X	X	X	X	X	X
FAU_STG.1	Protected data memory	X	X	X	X	X	X
FAU_STG.3	Action in case of possible event records loss	X	X	X	X	X	X
FAU_STG.4	Prevention of event records loss	X	X	X	X	X	X
FCS_COP.1(1)	Cryptographic operation	X	X	X	X	X	X
FCS_COP.1(2)	Cryptographic operation				X	X	
FCS_COP.1(3)	Cryptographic operation				X	X	
FDP_ACC.1	Subset access control	X	X	X	X	X	X
FDP_ACF.1	Security attribute based access control	X	X	X	X	X	X
FDP_ITT.1	Basic internal transfer protection	X	X	X	X	X	X
FDP_ITT.3	Integrity monitoring	X	X	X	X	X	X
FDP_RIP.1	Subset residual information protection				X	X	
FIA_UAU.2	User authentication before any action	X	X	X	X	X	X
FIA_UID.2	User identification before any action	X	X	X	X	X	X
FPT_PHP.1(1)	Passive detection of physical attack	X	X	X	X	X	X
FPT_PHP.1(2)	Passive detection of physical attack				X		
FPT_STM.1	Reliable time stamps	X	X	X	X	X	X

7.2.2 FAU_GEN.1 Audit event records generation

FAU_GEN.1.1

The alcohol interlock shall be able to generate an event record of the following auditable events:

a) start-up and shutdown of the event functions,

b) **not specified,**

NOTE 1 "not specified" was chosen, and the entire element was then refined away for readability.

c) [**deletion of event records,**
adjustment of the alcohol interlock,
assignment: *other specifically defined auditable events*],

[selection[“”,and shall not generate event records of the following specifically defined auditable events [assignment: events or types/classes of events]]

FAU_GEN.1.2

The alcohol interlock shall record within each event record at least the following information:

a) date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event, **a unique consecutive number**; and

NOTE 2 This is a refinement.

b) for each event type, based on the auditable event definitions of the functional components included in the security target, [assignment: *other audit relevant information*].

The required events and information should be defined by national regulations.

7.2.3 FAU_STG.1 Protected data memory

FAU_STG.1.1

The **alcohol interlock** shall protect the **stored event records** in the data memory from unauthorized deletion **and reading**.

NOTE 1 This is a refinement.

NOTE 2 The word “data memory” is used as the common criteria term “audit trail storage”.

FAU_STG.1.2

The **alcohol interlock** shall be able to [selection: choose one of: *prevent, detect*] unauthorized modifications to the **stored event records** in the data memory.

7.2.4 FAU_STG.3 Action in case of possible event records loss

FAU_STG.3.1

The **alcohol interlock** shall **issue an early recall warning to the driver** if the **data memory** exceeds **90 % of storage space**.

7.2.5 FAU_STG.4 Prevention of event records loss

FAU_STG.4.1

The **alcohol interlock** shall **prevent the vehicle engine from starting** and **ignore audited events** if the **data memory** is full.

7.2.6 FCS_COP.1(1) Cryptographic operation

FCS_COP.1.1

The **alcohol interlock** shall perform **encryption of event records before storing them** in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

NOTE See 7.3 for information on completing this requirement.

7.2.7 FCS_COP.1(2) Cryptographic operation

FCS_COP.1.1

The **service application** shall perform **decryption of event records** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

NOTE See 7.3 for information on completing this requirement.

7.2.8 FCS_COP.1(3) Cryptographic operation

FCS_COP.1.1

The **service application** shall perform **encryption of converted event records** in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

NOTE See 7.3 for information on completing this requirement.

7.2.9 FDP_ACC.1 Subset access control

FDP_ACC.1.1

The TSF shall enforce the **alcohol interlock policy** on

– **service application, alcohol interlock, register, broker**,

– **event records**,

– **adjust, convert, delete, read, readout**.

7.2.10 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the **alcohol interlock policy** to objects based on the following:

– **service application, alcohol interlock, register, broker**,

– **event records.**

NOTE 1 None of these has security attributes.

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

For all classes of alcohol interlocks:

– service application may readout event records from alcohol interlock,

– service application may delete event records from alcohol interlock,

– service application may adjust the alcohol interlock.

For class A alcohol interlocks:

- **service application may register-send event records to register,**
- **register may read event records,**
- **service application may receive confirmation from register.**

For class B1 alcohol interlocks:

- **service application may broker-send event records to broker,**
- **broker may read event records,**
- **service application may receive confirmation from broker.**

For class B2 alcohol interlocks:

- **service application may broker-send event records to broker,**
- **broker may read event records,**
- **service application may receive and then register-send event records to register,**
- **register may read event records,**
- **service application may receive confirmation from register.**

For class C alcohol interlocks:

- **service application may read event records,**
- **service application may convert event records,**
- **service application may register-send event records to register,**
- **register may read event records,**
- **service application may receive confirmation from register.**

FDP_ACF.1.3

None.

NOTE 2 The assignment is completed with "none" and then refined away for readability.

FDP_ACF.1.4

None.

NOTE 3 The assignment is completed with "none" and then refined away for readability.

7.2.11 FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1

The TSF shall enforce the **alcohol interlock policy** to prevent the **disclosure and/or undetected modification of event records** when **they are** transmitted between **alcohol interlock and service application**.

NOTE 1 "Undetected" is a refinement to show that modification can only be detected and not prevented.

NOTE 2 User data is refined to "event records" to show which user data is meant.

NOTE 3 "they are" is an editorial refinement to make the sentence correct English.

NOTE 4 “Physically separated parts of the alcohol interlock” was refined into “alcohol interlock and service application” to show which parts are meant.

7.2.12 FDP_ITT.3 Integrity monitoring

FDP_ITT.3.1

The **alcohol interlock** shall monitor **information about detected events** transmitted between **handset, control unit and any accessory devices** for the following errors: **insertion, modification and deletion**.

NOTE 1 As there is no relevant access control policy covering this, part of the security functional requirement was refined away.

NOTE 2 User data was refined to “information about detected events” to show which user data is meant.

NOTE 3 “Physically separated parts of the alcohol interlock” was refined into “handset, control unit and accessory devices” to show which parts are meant.

FDP_ITT.3.2

Upon detection of an integrity error, the **alcohol interlock** shall [assignment: specify the action to be taken upon integrity error].

NOTE 4 Modifying or exchanging the handset without being detected and using this to insert, delete or modify information about detected events being sent to the control unit would be a violation of the FDP_ITT.3 requirement.

7.2.13 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

The **service application** shall ensure that any previous information content of a resource **in the service application** is made unavailable upon the **de-allocation of the resource from** the following objects: **event records**.

7.2.14 FIA_UAU.2 User authentication before any action (not applicable if the authentication is done in the operational environment)

FIA_UAU.2.1

The **service application** shall require each service personnel to be successfully authenticated before allowing any other **service application** or mediated actions on behalf of that service personnel.

7.2.15 FIA_UID.2 User identification before any action (not applicable if the authentication is done in the operational environment)

FIA_UID.2.1

The **service application** shall require each service personnel to be successfully identified before allowing any other **service application** or mediated actions on behalf of that service personnel.

7.2.16 FPT_PHP.1(1) Passive detection of physical attack

FPT_PHP.1.1

The **alcohol interlock** shall provide unambiguous detection of physical tampering that might compromise the **alcohol interlock**.

FPT_PHP.1.2

The **alcohol interlock** shall provide the capability to determine whether physical tampering with the **alcohol interlock** has occurred. **Evidence of tampering shall be field-detectable under close scrutiny of a trained person.**

NOTE 1 An alcohol interlock may detect tampering with the wires leading from the control unit to the vehicle and record this in the data memory. This is considered to be tamper-evidence as far as this requirement is concerned. The act of logging is not considered as tamper-evidence for tampering with the control unit itself.

NOTE 2 Security function and security functions devices and elements were refined several times to show which part of the security function is meant.

NOTE 3 The wires from the control unit to the vehicle are considered to be part of the control unit (see 3.3).

7.2.17 FPT_PHP.1(2) Passive detection of physical attack

FPT_PHP.1.1

The **service application** shall provide unambiguous detection of physical tampering that might compromise the **service application**.

FPT_PHP.1.2

The **service application** shall provide the capability to determine whether physical tampering with the **service application** has occurred.

Evidence of tampering shall be field-detectable under close scrutiny of a trained person.

7.2.18 FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The **alcohol interlock** shall be able to provide reliable time stamps.

7.3 Cryptographic algorithms

The alcohol interlock and the service application perform various cryptographic operations. All of these shall use strong cryptographic algorithms. In this European standard, single Data Encryption Standard (DES) is not considered to be strong, while Triple-DES (3DES), Advanced Encryption Standard (AES), RSA 1024 (according to Rivest, Shamir, Adleman) and greater are considered to be strong.

NOTE Other algorithms may be defined by national regulations.

This standard does not contain the various dependencies of FCS_COP.1, because it does not mandate key management solutions. The security target author shall still address these dependencies to specify the key management solution.

7.4 Security assurance requirements

The security assurance requirements for this European standard are EAL 3 + ALC_FLR.2.

The reasons for this choice are that:

– EAL 3 (EAL = Evaluation Assurance Level) is deemed to provide a good balance between assurance and costs. It contains a site audit to examine the developers process and enough information to determine the main security features: cryptographic architecture and tamper-evidence.

– ALC_FLR.2 (ALC = Assurance class Life Cycle; FLR = FLaw Remediation) provides a good structure for the remediation of security flaws. This supports accreditation structures where not every version of a product will be certified.

NOTE For details see CCp3.

Annex A
(informative)

Security problem definition

A.1 General

This European Standard only uses threats and does not use organizational security policies or assumptions. To allow to understand the scope and completeness of the European Standard, a fairly sizable list of threats has been included.

NOTE For details see CCp1, Annex A.6.

A.2 Assets

The purpose of the alcohol interlock is to protect the following four assets:

a) Prevention and/or detection of an engine start without having delivered an accepted breath sample.

b) The integrity of the event records to allow detection as in paragraph a): therefore deletion or unauthorized modification of event records shall not be possible.

c) The non-repudiation of the validity of the event records, so they constitute proof in legal procedures: therefore unnoticed deletion or modification or insertion of event records shall not be possible.

d) The confidentiality of the event records: to protect the privacy of the driver.

A.3 Threat agents

The assets are threatened by the following threat agents:

a) The driver and/or agents in his employ: the driver may wish to drive while intoxicated, or seek to prevent detection that he has done so or attempted to do so.

b) Parties that seek to bring the system into disrepute: if parties can prove they modified or inserted event records without this being detected, this will invalidate the non-repudiation status of all other event records. If they can show that they can delete event records without this being detected they will undermine the reputation of the system.

c) Parties that seek to invade the privacy of drivers. For example, a journalist might be interested in finding out that a well-known figure attempted to drive while intoxicated.

For each of the threats in A.4, it should be obvious to which asset and threat agent they apply. To maintain readability, this has not been listed with every threat.

A.4 Threat overview

This European Standard provides a detailed analysis of threats, directly to the alcohol interlock, to the service application and to their environment.

NOTE The scope of this European Standard applies to handset, control unit, accessory devices and service application of the alcohol interlock. It does not apply to data security of the broker or register itself, and does not apply to organizational processes as defining rights of access to the event records. Requirements for entities not being under the scope of this European Standard may be defined by national regulations. However, to give a complete overview these entities are also described in this European Standard.

The threats are grouped into classes. Each light grey box in Figure A.1 depicts a class of threats. Each class of threats is described in a separate subsection below.

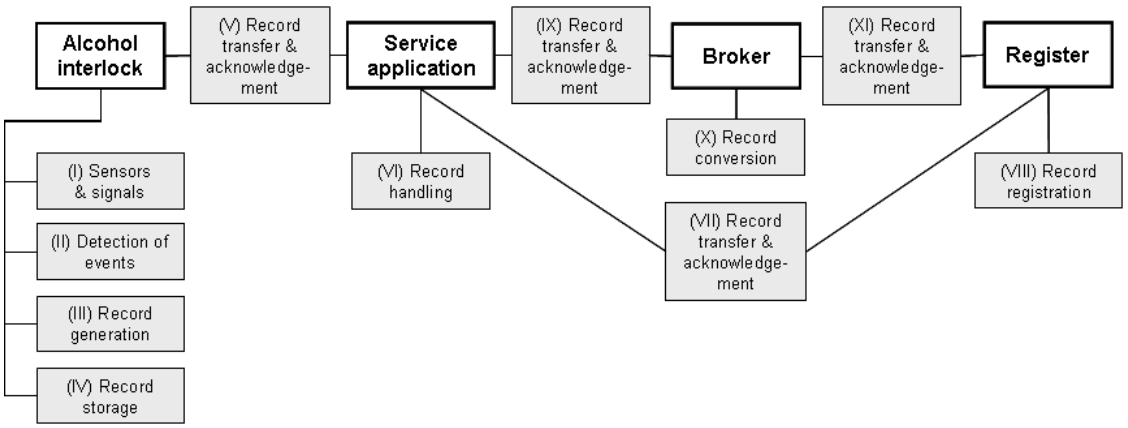

Figure A.1 – Threats to the alcohol interlock, the service application and the environment

Clause 5 defines several classes of alcohol interlocks, which differ from each other in various aspects. This chapter describes a number of threat categories, but not all categories are valid for all classes. This is indicated in Table A.1.

Table A.1 - Threats for different classes of alcohol interlocks

	Threats	A	B1	B2	C1	C2	D
I	*Sensors & signals:* Interfering with the sensors and the signals to the vehicle	X	X	X	X	X	X
II	*Detection of events:* Prevention of detection of events	X	X	X	X	X	X
III	*Record generation:* Prevention of generation of event records or generation of undesirable event records	X	X	X	X	X	X
IV	*Record storage:* Failure to correctly store event records in the alcohol interlock	X	X	X	X	X	X
V	*Record transfer & acknowledgement:* Failure to correctly transfer event records between alcohol interlock and service application	X	X	X	X	X	X
VI	*Record handling:* Failure to correctly handle the event records in the service application	X	X	X	X	X	X
VII	*Record transfer & acknowledgement:* Failure to correctly transfer event records between service application and register	X		X	X	X	
VIII	*Record registration:* Failure to correctly register event records at the register	X	X	X	X	X	
IX	*Record transfer & acknowledgement:* Failure to correctly transfer event records between service application and broker		X	X			
X	*Record conversion:* Failure to correctly convert event records at the broker		X	X			
XI	*Record transfer & acknowledgement:* Failure to correctly transfer event records between broker and register		X				

A.5 Threats

A.5.1 Interfering with the sensors and the signals to the vehicle (I)

This class of threats attempts to interfere with the alcohol sensor and/or the connections between the control unit and the vehicle.

I.1: Let other people deliver the breath sample.

I.2: Chemical and/or physical attacks that change, modify and/or substitute the breath sample delivered to the alcohol interlock and/or the measurement process.

NOTE This European Standard only considers the attacks on the alcohol sensor and/or the measurement process as specified in EN 50436-1. More advanced threats to the alcohol sensor and/or the measurement process are outside the scope of this standard.

I.3: The alcohol interlock is somehow bypassed, allowing the vehicle to be started, regardless of whether there was a (successful) alcohol test.

A.5.2 Prevention of detection of events (II)

This class of threats attempts to prevent the detection of the relevant events.

II.1: Failure to detect any relevant event, e.g. because the alcohol interlock has been misadjusted.

A.5.3 Prevention of generation of event records or generation of undesirable event records (III)

This class of threats attempts to prevent event records from being generated or being correctly generated, even though an auditable event has occurred. This class of threats also prevents the generation of undesirable event records.

III.1: Failure to generate an event record, e.g. by:

- disconnecting the handset from the control unit or otherwise interfering with the connection between them, or
- disconnecting the accessory device from the handset and/or control unit, or otherwise interfering with the connection between them.

III.2: Modification of generation of an event record, e.g. by:

- applying extreme external conditions, such as voltage spikes, high or low temperature, or
- physical modification of the alcohol interlock, or
- modifying information between handset and control unit as it is transferred between them, or
- modifying information between handset, control unit and/or any accessory device as it is transferred between them.

III.3: Failure to generate an event record due to storage overflow.

III.4: Unauthorized operation of adjustment.

III.5: An event record is generated of an event, but it is undesirable that this event is recorded, due to e.g. privacy and/or legal constraints.

A.5.4 Failure to correctly store event records in the alcohol interlock (IV)

This class of threats attempts to modify, delete, create and/or read event records while they are being stored by the alcohol interlock.

IV.1: Undetected modification of event records. This includes:

- accidental modification (e.g. memory errors),
- deliberate modification.

IV.2: Undetected deletion of event records. This includes:

- deletion of (part of) the data memory contents,
- removal, replacement, damaging or destruction of the memory itself.
- authorized deletion, but the event records have not yet been received by the register or broker.

IV.3: Undetected insertion of event records.

IV.4: Unauthorized reading of event records. This includes:

– reading the event records directly from the integrated circuits where it resides.

A.5.5 Failure to correctly transfer event records between alcohol interlock and service application (V)

This class of threats attempts to modify, delete, create and/or read event records while they are being transferred between the alcohol interlock and the service application.

V.1: Modification of event records in transit between alcohol interlock and service application. This includes:

– accidental modification (e.g. transmission errors),

– reading the event records with a wrong version of the service application, thus misinterpreting the event records,

– sending an invalid or truncated set of event records,

– deliberate modification.

V.2: Deletion of event records in transit between alcohol interlock and service application.

V.3: Insertion of event records in transit between alcohol interlock and service application.

V.4: Reading of event records in transit between alcohol interlock and service application. This includes:

– reading the event records by other means than a service application,

– reading the event records by a service application, but by a person that is not authorized to use this service application.

V.5: Deletion of event records through application of the service application before these event records have been correctly received by the register or broker.

NOTE This includes solutions that make a backup in the alcohol interlock whenever the alcohol interlock is read out, overwriting the old backup. By reading out the alcohol interlock twice, first the event records are moved to the backup, and then they are overwritten, thus deleting it.

A.5.6 Failure to correctly handle the event records in the service application (VI)

This class of threats attempts to modify, delete, create and/or read event records while they are in the service application.

VI.1: Modification of event records while in the service application. This includes:

– accidental modification (e.g. storage, conversion or processing errors),

– deliberate modification.

VI.2: Deletion of event records while in the service application.

VI.3: Insertion of event records while in the service application.

VI.4: Reading of event records while in the service application. This includes:

– the service application retaining copies of parts of event records which may be read at a later date. This could be explicit copies of event records, but also accidental copies left in for example swap files or deleted disk sectors.

A.5.7 Failure to correctly transfer event records between service application and register (VII)

This class of threats attempts to modify, delete, create and/or read event records while they are being transferred between the service application and the register.

VII.1: Modification of event records in transit between service application to register. This includes:

– accidental modification (e.g. transmission errors),

– sending an invalid or truncated set of event records,

– deliberate modification.

VII.2: Deletion of event records in transit between service application and register.

VII.3: Insertion of event records in transit between service application and register. This includes:

– event records being sent twice (either deliberately or by accident),

– unauthenticated or unknown parties sending event records.

VII.4: Reading of event records in transit between service application and register.

A.5.8 Failure to correctly register event records at the register (VIII)

This class of threats attempts to modify, delete, create and/or read event records while they are at the register.

VIII.1: Modification of event records while at the register. This includes:

– accidental modification (e.g. storage, processing or conversion errors),

– deliberate modification.

VIII.2: Unauthorized deletion of event records while at the register.

VIII.3: Insertion of event records while at the register.

VIII.4: Unauthorized reading of event records while at the register.

VIII.5: Unauthorized retention of event records at the register.

A.5.9 Failure to correctly transfer event records between service application and broker (IX)

This class of threats attempts to modify, delete, create and/or read event records while they are being transferred between the service application and the broker.

IX.1: Modification of event records in transit between service application and broker. This includes:

– accidental modification (e.g. transmission errors),

- sending an invalid or truncated set of event records,
- deliberate modification.

IX.2: Deletion of event records in transit between service application and broker.

IX.3: Insertion of event records in transit between service application and broker. This includes:

- event records being sent twice (either deliberately or by accident),
- unauthenticated or unknown parties sending event records.

IX.4: Reading of event records in transit between service application and broker. This includes:

- event records being sent by the service application to the wrong broker,
- event records being sent by the broker to the wrong service application.

A.5.10 Failure to correctly convert event records at the broker (X)

This class of threats attempts to modify, delete, create and/or read event records while they are being converted by the broker.

X.1: Modification of event records while at the broker. This includes:

- accidental modification (e.g. storage, processing or conversion errors),
- deliberate modification.

X.2: Unauthorized deletion of event records while at the broker.

X.3: Insertion of event records while at the broker.

X.4: Unauthorized reading of event records while at the broker.

X.5: Unauthorized retention of event records at the broker.

A.5.11 Failure to correctly transfer event records between broker and register (XI)

This class of threats attempts to modify, delete, create and/or read event records while they are being transferred between the broker and the register.

XI.1: Modification of event records in transit between broker and register. This includes:

- accidental modification (e.g. transmission errors),
- deliberate modification.

XI.2: Unauthorized deletion of event records in transit between broker and register.

XI.3: Insertion of event records in transit between broker and register. This includes:

- event records being sent twice (either deliberately or by accident),
- unauthenticated or unknown parties sending event records.

XI.4: Unauthorized reading of event records in transit between broker and register.

Annex B
(informative)

Rationales

B.1 General

The tables below lists all threats on the left side. For each threat the objectives ("O") and the objectives for the environment ("OE") are listed on the right side that counter this threat, with a short rationale on why they counter this threat.

As this standard does not use organizational security policies (OSP) or assumptions, there is no further security objectives rationale.

B.2 Security objectives rationale

B.2.1 Interfering with the sensors and the signals to the vehicle (I)

Threats	Objectives
I.1: Let other people deliver the breath sample	OE.INTERLOCK_EN_50436-1_OR_EN_50436-2 is capable that the driver is tested periodically when driving (4.8 of EN 50436-1 and EN 50436-2). It is still possible for the driver to take a sober passenger, and let him deliver the breath samples, but this risk is seen as very unlikely and hence accepted: why would sober people risk their lives as passenger of a drunk driver?
I.2: Basic chemical and/or physical attacks that change, modify and/or substitute the breath sample delivered into the handset (the attacks are listed in the EN 50436-1)	OE.INTERLOCK_EN_50436-1_OR_EN_50436-2 explicitly includes this threat in its certification (Clause 12 of EN 50436-1 and EN 50436-2), thereby countering it.
I.3: The alcohol interlock is somehow bypassed, allowing the vehicle to be started, regardless of whether there was a (successful) breath test	OE.INTERLOCK_EN_50436-1_OR_EN_50436-2 specifies that there shall be a detection of the bypassing (12.11 of EN 50436-1 and EN 50436-2). O.DETECT_EVENTS ensures that this event is detected. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_ AND_ACCESSORY_DEVICE ensures that neither the control unit nor the connections can be modified to change this without this being evident.

B.2.2 Prevention of detection of events (II)

Threats	Objectives
II.1 Failure to detect any relevant event, e.g. because the alcohol interlock has been misadjusted	O.DETECT_EVENTS ensures that all relevant events are detected. O.DETECT_EVENTS also records all adjustments, so that errors in the process (or even deliberate misadjustment) can be detected by the service application, broker or register. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory devices cannot be modified to change this.

B.2.3 Prevention of generation of event records or generation of undesirable event records (III)

Threats	Objectives
III.1 Failure to generate an event record e.g. by: – disconnecting the handset from the control unit or otherwise interfering with the connection between them – disconnecting the accessory device from the handset and/or control unit, or otherwise interfering with the connection between them	O.DETECT_EVENTS ensures that disconnecting the handset or accessory device generates an event and is thus be detected. O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that information between handset, control unit and accessory device cannot be deleted/modified without this being detected. O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK ensures that an event record is stored with the correct information. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.
III.2 Modification of generation of an event record, for example by: – applying extreme external conditions, such as voltage spikes, high/low temperature, or – physical modification of the alcohol interlock, or – modifying information between handset, control unit and accessory device as it is transferred between them	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK ensures that an event record is stored with the correct information. O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that information between handset, control unit and accessory device cannot be modified. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this. OE.INTERLOCK_EN_50436-1_OR_EN_50436-2 prescribes additional environmental tests that support this (different clauses of EN 50436-1 and EN 50436-2).
III.3 Failure to generate an event record due to storage overflow	O.NO_OVERFLOW_IN_DATA_MEMORY specifies the actions needed in case of overflow and impending overflow, thus countering this threat. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that the alcohol interlock cannot be modified to change this.

III.4 Failure to generate an event record because the alcohol interlock has been deliberately incorrectly adjusted	O.ALCOHOL_INTERLOCK_AND_SERVICE_APPLICATION counters this threat by preventing anyone except the service application to perform adjustment. O.DETECT_EVENTS records all adjustments, so that errors in the process (or even deliberate misadjustment) can be detected by the service application, broker or register. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_ AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.
III.5 An event record is generated of an event, but it is undesirable that this event is recorded, due to e.g. privacy and/or legal constraints.	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_ INTERLOCK ensures that undesirable events are not recorded. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_ AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.

B.2.4 Failure to correctly store event records in the alcohol interlock (IV)

Threats	**Objectives**
IV.1 Undetected modification of event records while being stored. This includes: – accidental modification (e.g. memory errors) – deliberate modification	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_ INTERLOCK ensures that the event records cannot be changed by unauthorized entities. If encryption is used, it explicitly addresses the fact that the encryption should be done in such a way that modification can always be detected. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_ AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.
IV.2 Undetected deletion of event records while being stored. This includes: – deletion of (part of) the memory contents – removal / replacement / damaging / destruction of the memory itself	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_ INTERLOCK specifies that a unique consecutive number is stored within the event record. Therefore one can detect deletion of event records, as some of the numbers would go missing. O. ALCOHOL_INTERLOCK_AND_SERVICE_APPLICATION assists in this by only allowing the service application to perform a deletion of event records. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_ AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.
IV.3 Undetected insertion of event records while being stored	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_ INTERLOCK specifies that unauthorized entities cannot modify event records and that a unique consecutive number is stored within the event record. Therefore one cannot create new event records from scratch and one cannot replay event records. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_ AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.

IV.4 Unauthorized reading of event records while being stored. This includes: – reading the event records directly from the integrated circuits where it resides – authorized deletion, but the event records have not yet been received by the register	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK specifies that the event records cannot be read by unauthorized entities. O. ALCOHOL_INTERLOCK_AND_SERVICE_APPLICATION assists in this by only allowing the service application to readout the event records from the alcohol interlock. O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE ensures that the handset, control unit and accessory device cannot be modified to change this.

B.2.5 Failure to correctly transfer event records between alcohol interlock and service application (V)

Threats	**Objectives**
V.1: Modification of event records in transit between alcohol interlock and service application. This includes: – accidental modification (e.g. transmission errors) – reading the event records with a wrong version of the service application, thus misinterpreting the event records – sending an invalid or truncated set of event records – deliberate modification	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK specifies encryption of the event records to ensure that they cannot be changed or misinterpreted without this being detectable. O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK also specifies that a unique consecutive number is encrypted within the event record. Therefore one can detect an invalid or truncated set of event records. OE.DELETE_ONLY_AFTER_CONFIRMATION specifies that eventually the event records will be deleted from the control unit, further supporting this objective.
V.2: Deletion of event records in transit between alcohol interlock and service application	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK specifies that a unique consecutive number is encrypted within the event record. Therefore one can detect deletion of event records, as some of the numbers would go missing.
V.3: Insertion of event records in transit between control unit and service application	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK specifies that a unique consecutive number is encrypted within the event record. Therefore one cannot create new event records from scratch and one cannot replay event records.
V.4: Reading of event records in transit between control unit and service application. This includes: – reading the event records by another means than a service application – reading the event records by a service application, but by a person that is not authorized to use this service application	O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK specifies that the event records are encrypted thus making it impossible to read them.

V.5: Deletion of event records through application of the service application before these event records have been correctly received by the register. This includes: – solutions that make a backup in the alcohol interlock whenever the alcohol interlock is read out, overwriting the old backup. By reading out the alcohol interlock twice, first the event records are moved to the backup, and then they are overwritten, thus deleting it.	OE.REGISTER_CHECK_AND_CONFIRM ensures that the register checks the event records and send back the result. OE.BROKER_RELAY_CONFIRMATION specifies that (if the broker is used) it will relay the result to the service application. OE.DELETE_ONLY_AFTER_CONFIRMATION specifies that the service personnel takes care of this. It is not necessarily automatically enforced by the service application (although the service application may choose to do so in addition). O.SERVICE_APPLICATION_AUTHENTICATION specifies that only authenticated service personnel can use the service application, lessening the chance that this threat will happen even further.

B.2.6 Failure to correctly handle the event records in the service application (VI)

Threats	Objectives
VI.1 Modification of event records while in the service application. This includes: – accidental modification (e.g. storage or conversion or processing errors) – deliberate modification	O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS specifies that the service application should protect against modification. O.SERVICE_APPLICATION_AUTHENTICATION specifies that only authenticated service personnel can use the service application, lessening the chance that this threat will happen even further.
	For class C1 alcohol interlocks, this is supported by: O.TAMPER_EVIDENT_SERVICE_APPLICATION to protect the event records in the service application against physical tampering.
	For class C2 alcohol interlocks, this is supported by: OE.PROTECTED_SERVICE_APPLICATION, where the service centre environment protects the event records in the service application against tampering.
VI.2 Deletion of event records while in the service application	O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS specifies that the service application should protect against deletion. O.SERVICE_APPLICATION_AUTHENTICATION specifies that only authenticated service personnel can use the service application, lessening the chance that this threat will happen even further.
	For class C1 alcohol interlocks, this is supported by: O.TAMPER_EVIDENT_SERVICE_APPLICATION to protect the event records in the service application against physical tampering.
	For class C2 alcohol interlocks, this is supported by: OE.PROTECTED_SERVICE_APPLICATION, where the service centre environment protects the event records in the service application against tampering.

VI.3 Insertion of event records while in the service application	O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS specifies that the service application should protect against insertion. O.SERVICE_APPLICATION_AUTHENTICATION specifies that only authenticated service personnel can use the service application, lessening the chance that this threat will happen even further.
	For class C1 alcohol interlocks, this is supported by: O.TAMPER_EVIDENT_SERVICE_APPLICATION to protect the event records in the service application against physical tampering.
	For class C2 alcohol interlocks, this is supported by: OE.PROTECTED_SERVICE_APPLICATION, where the service centre environment protects the event records in the service application against tampering.
VI.4 Reading of event records while in the service application. This includes: – the service application retaining copies of parts of event records which may be read at a later date. This could be explicit copies of event records, but also accidental copies left for example in swap files or deleted disk sectors	O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS specifies that the service application should protect against reading. O.SERVICE_APPLICATION_AUTHENTICATION specifies that only authenticated service personnel can use the service application, lessening the chance that this threat will happen even further.
	For class C1 alcohol interlocks, this is supported by: O.TAMPER_EVIDENT_SERVICE_APPLICATION to protect the event records in the service application against physical tampering.
	For class C2 alcohol interlocks, this is supported by: OE.PROTECTED_SERVICE_APPLICATION, where the service centre environment protects the event records in the service application against tampering.

B.2.7 Failure to correctly transfer event records between service application and register (VII)

Threats	**Objectives**
VII.1: Modification of event records in transit between service application and register. This includes: – accidental modification (e.g. transmission errors) – sending an invalid or truncated set of event records – deliberate modification	For class B1 and D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all modifications and a means for sender authentication. Consider that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed.
VII.2: Deletion of event records in transit between service application and register	For class B1 and D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all deletions. Consider that in the case of transparent service applications, this means may rely on the original encryption of the event records,

	and this is explicitly allowed.
VII.3: Insertion of event records in transit between service application to register. This includes: – event records being sent twice (either deliberately or by accident) – unauthenticated or unknown parties sending event records	For class B1 and D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all insertions and a means for sender authentication. Consider that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed.
VII.4: Reading of event records in transit between service application and register	For class B1 and D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that prevents reading of the event records while in transit. Consider that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed. O.SEND_TO_CORRECT_PARTY additionally ensures that the event records are only be sent to the register, further decreasing the risk of this threat.

B.2.8 Failure to correctly register event records at the register (VIII)

Threats	Objectives
VIII.1 Modification of event records while at the register. This includes: – accidental modification (e.g. storage, processing or conversion errors) – deliberate modification	For class D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_RECORDS specifies that modifications are prevented.
VIII.2 Deletion of event records while at the register	For class D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_RECORDS specifies that deletion is prevented.
VIII.3 Insertion of event records while at the register	For class D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_RECORDS specifies that insertion is prevented.
VIII.4 Reading of event records while at the register	For class D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_RECORDS specifies that the reading of event records is prevented.
VIII.5 Unauthorized retention of event records at the register	For class D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_RECORDS specifies that the retention of event records is prevented.

B.2.9 Failure to correctly transfer event records between service application and broker (IX)

Threats	Objectives
IX.1: Modification of event records in transit between service application and broker. This includes: – accidental modification (e.g. transmission errors) – sending an invalid or truncated set of event records – deliberate modification	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all modifications and a means for sender authentication. Note that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed.
	For class B2 alcohol interlocks: OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for class B2 alcohol interlocks, the event records are protected between broker and service application.
IX.2: Deletion of event records	For class A, C and D alcohol interlocks this threat is not relevant.

in transit between service application and broker	For class B alcohol interlocks: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all deletions. Note that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed.
	For class B2 alcohol interlocks: OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for class B2 alcohol interlocks, the event records are protected between broker and service application.
IX.3: Insertion of event records in transit between service application and broker. This includes: – event records being sent twice (either deliberately or by accident) – unauthenticated or unknown parties sending event records	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all insertions and a means for sender authentication. Note that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed.
	For class B2 alcohol interlocks: OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for class B2 alcohol interlocks, the event records are protected between broker and service application.
IX.4: Reading of event records in transit between service application and broker. This includes: – event records being sent by the service application to the wrong broker – event records being sent by the broker to the wrong service application	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_INCOMING_RECORDS provides a means of data transfer that prevents reading of the event records while in transit. Note that in the case of transparent service applications, this means may rely on the original encryption of the event records, and this is explicitly allowed. O.SEND_TO_CORRECT_PARTY additionally ensures that the event records are only be sent to the correct broker, further decreasing the risk of this threat.
	For class B2 alcohol interlocks: OE.BROKER_SEND_TO_CORRECT_PARTY ensures that for class B2 alcohol interlocks, the event records are protected between broker and service application, and that they are sent to the correct service application.

B.2.10 Failure to correctly convert event records at the broker (X)

Threats	Objectives
X.1 Modification of event records while at the broker. This includes: – accidental modification (e.g. storage, processing or conversion errors) – deliberate modification	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_RECORDS specifies that modifications are prevented. OE.BROKER_CORRECT_CONVERSION specifies additionally that the conversion process is accurate.
X.2 Deletion of event records while at the broker	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_RECORDS specifies that deletion is prevented.
X.3 Insertion of event records while at the broker	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_RECORDS specifies that insertion is prevented.
X.4 Reading of event records while at the broker	For class A, C and D alcohol interlocks this threat is not relevant.
	For class B alcohol interlocks: OE.BROKER_PROTECT_RECORDS specifies that the reading of event records is prevented, and also specifies secure deletion once the event records have been transferred to the register, thus further reducing the risk of unauthorized reading.
X.5 Unauthorized retention of event records at the broker	For class D alcohol interlocks this threat is not relevant.
	For all other classes: OE.REGISTER_PROTECT_RECORDS specifies that the retention of event records is prevented.

B.2.11 Failure to correctly transfer event records between broker and register (XI)

Threats	Objectives
XI.1: Modification of event records in transit between broker and register. This includes: – accidental modification (e.g. transmission errors) – deliberate modification	For class A, B2, C and D alcohol interlocks this threat is not relevant.
	For class B1 alcohol interlocks: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all modifications.
XI.2: Deletion of event records in transit between broker and register.	For class A, B2, C and D alcohol interlocks this threat is not relevant.
	For class B1 alcohol interlocks: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that detects all deletions.
XI.3: Insertion of event records in transit between broker and register. This includes: – event records being sent	For class A, B2, C and D alcohol interlocks this threat is not relevant.
	For class B1 alcohol interlocks: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a

twice (either deliberately or by accident) – unauthenticated or unknown parties sending event records	means of data transfer that detects all insertions and a method for sender authentication.
XI.4: Reading of event records in transit between broker and register	For class A, B2, C and D alcohol interlocks this threat is not relevant.
	For class B1 alcohol interlocks: OE.REGISTER_PROTECT_INCOMING_RECORDS provides a means of data transfer that prevents reading of the event records while in transit. OE.BROKER_SEND_TO_CORRECT_PARTY additionally ensures that the event records are only be sent to the register, further decreasing the risk of this threat.

B.3 Security requirements rationale

The table below lists all security objectives (see 6.2) on the left side. For each security objective the security functional requirements (SFR) addressing the security objectives are listed on the right side.

Security objective	**Security functional requirements addressing the security objective**
a) O.DETECT_EVENTS The alcohol interlock shall detect all events required by the applicable laws and regulations.	This objective is met by: – FAU_GEN.1 (see 7.2.2) specifying that event records shall be generated from the events (and that they shall therefore be detected). The application note under the security functional requirements specifies that completion of the security functional requirements shall conform to the applicable laws and regulations. – FPT_STM.1 (see 7.2.18) specifying that the alcohol interlock shall contain a reliable clock, to be able to store date and time of an event.
b) O.PROTECT_EVENTS_BETWEEN_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE The handset, control unit and accessory device shall protect information about detected events as this is exchanged between them against insertion, deletion and modification.	This objective is met by: – FDP_ITT.3 (see 7.2.12) which restates the objective and additionally specifies the action to be taken when this occurs.

c) O.RECORD_AND_ENCRYPT_EVENTS_IN_ALCOHOL_INTERLOCK The alcohol interlock shall store all required information for each event in event records in the alcohol interlock. Each event record shall contain at least: – the information required by the applicable laws and regulations – a unique consecutive number for each event record. The alcohol interlock shall not store event records on events that are not allowed to be recorded. The alcohol interlock shall store all event records in such a way that they cannot be read or modified by unauthorized entities. The alcohol interlock shall encrypt all event records before allowing them to be read out in such a way that they cannot be read or modified by unauthorized entities.	This objective is met by: – FAU_GEN.1 (see 7.2.2) and its note that specify that the event records shall contain the information required by the applicable laws and regulations and that, optionally, certain events are not to be recorded. – FAU_STG.1 (see 7.2.3) specifying that they shall be stored in such a way that they cannot be modified (or deleted) or read by unauthorized entities. – FCS_COP.1(1) (see 7.2.6) specifying that the event records shall be encrypted before storing them (and therefore cannot be read by unauthorized entities). – FDP_ITT.1 (see 7.2.11) further specifying that the event records cannot be modified and/or disclosed by unauthorized entities when they are read out.
d) O.TAMPER_EVIDENT_HANDSET_AND_CONTROL_UNIT_AND_ACCESSORY_DEVICE The handset, control unit and accessory device shall be tamper-evident. Evidence of tampering does not have to be detectable in the field, but shall be detectable under close scrutiny of an expert.	This objective is met by: – FPT_PHP.1(1) (see 7.2.16) which together with its notes restates the objective.
e) O.TAMPER_EVIDENT_SERVICE_APPLICATION (applicable to class C1 alcohol interlocks only) The service application shall be tamper-evident. Evidence of tampering does not have to be detectable in the field, but shall be detectable under close scrutiny of an expert.	For class A, B, C2 and D alcohol interlocks this threat is not relevant. For class C1 alcohol interlocks this objective is met by: – FPT_PHP.1(2) (see 7.2.17) which together with its note restates the objective. The header indicates that the security functional requirement is only valid for class C1 alcohol interlocks.
f) O.NO_OVERFLOW_IN_DATA_MEMORY When the memory of the alcohol interlock is filled with event records for: – 90%, the alcohol interlock shall issue an early recall warning to the driver, – 100%, the alcohol interlock shall no longer allow the vehicle to start.	This objective is met by: – FAU_STG.3 (see 7.2.4) which restates the first indent, – FAU_STG.4 (see 7.2.5) which restates the second indent.
g) O. ALCOHOL_INTERLOCK_AND_SERVICE_APPLICATION The alcohol interlock shall allow only the service application to: – read out event records from the alcohol interlock, – delete event records from the alcohol	This objective is met by: – FDP_ACC.1 (see 7.2.9) and FDP_ACF.1 (see 7.2.10). The rules in FDP_ACF.1 restate the objective.

interlock, – adjust the alcohol interlock.	
h) O.SERVICE_APPLICATION_AUTHENTICATION Before a person can use the service application, this service personnel shall first be identified and authenticated.	If identification and authentication is done by the alcohol interlock, this objective is met by: – FIA_UID.2 (see 7.2.15) and FIA_UAU.2 (see 7.2.14) which restate the objective. If identification and authentication is done by the operational environment, this objective is automatically met.
i) O.SERVICE_APPLICATION_PROTECT_EVENT_RECORDS The service application shall not allow its users (or other entities) to insert, modify or read event records from the service application. This includes reading of event records after they have been sent onwards.	This objective is met by: – FDP_ACC.1 (see 7.2.9) and FDP_ACF.1 (see 7.2.10) which strictly limit the operations that the service application can do. Additionally, for class C1 and C2 alcohol interlocks (which decrypt the event records), FDP_RIP.1 (see 7.2.13) guarantees that the event records are securely deleted. For other alcohol interlocks, the event records are never available in the clear, so this is unnecessary. The class C1 and C2 alcohol interlocks shall also decrypt and re-encrypt the event records to protect them, so FCS_COP.1(2) (see 7.2.7) and FCS_COP1(3) (see 7.2.8) also support this objective.
j): O.SEND_TO_CORRECT_PARTY The service application shall send the event records only to the correct party in the correct manner. The service application shall be able to receive a confirmation that the event records have been correctly received. – For class B1 alcohol interlocks, the event records shall be sent to the broker, using the method specified by the broker, and the confirmation should be received from the broker. – For class B2 alcohol interlocks, the event records shall be sent to the broker, using the method specified by the broker, then the event records received by the broker shall be sent to the register, using the method specified by the register, and the conformation shall be received from the register. – For all other classes of alcohol interlocks, the event records shall be sent to the register, using the method specified by the register, and the confirmation should be received from the register.	For class D alcohol interlocks this threat is not relevant. For class A alcohol interlock this objective is met by: – FDP_ACC.1 (see 7.2.9) and FDP_ACF.1 (see 7.2.10): – that specify that for class A alcohol interlocks the service application can only send event records to the register in the manner specified by the register, – that specify that for class A alcohol interlocks the confirmation is received from the register. For class B1 alcohol interlock this objective is met by: – FDP_ACC.1 (see 7.2.9) and FDP_ACF.1 (see 7.2.10): – that specify that for class B1 alcohol interlocks the service application can only send event records to the broker in the manner specified by the broker, – that specify that for class B1 alcohol interlocks the confirmation is received from the broker. For class B2 alcohol interlock this objective is met by:

	– FDP_ACC.1 (see 7.2.9) and FDP_ACF.1 (see 7.2.10):
	  – that specify that for class B2 alcohol interlocks the service application sends the event records to the broker in the manner specified by the broker, that receives new event records in return from the broker and then sends them to the register in the manner specified by the register,
	  – that specify that for class A, B2 and C alcohol interlocks the confirmation is received from the register.

	For class C alcohol interlock this objective is met by:
	– FDP_ACC.1 (see 7.2.9) and FDP_ACF.1 (see 7.2.10):
	  – that specify that for class C alcohol interlocks the service application can only send the event records to the register in the manner specified by the register,
	  – that specify that for class C alcohol interlocks the confirmation is received from the register.

B.4 Dependencies

The table below lists all security functional requirements on the left side. For each security functional requirement the dependencies are listed on the right side.

Security functional requirement	**Dependencies**
FAU_GEN.1	FPT_STM.1: met
FAU_STG.1	FAU_GEN.1: met
FAU_STG.3	FAU_STG.1: met
FAU_STG.4	FAU_STG.1: met FAU_STG.3: met
FCS_COP.1(1)	(FDP_ITC or FDP_ITC.2 or FCS_CKM.1): not met, see 7.3 for details. FCS_CKM.4: not met, see 7.3 for details.
FCS_COP.1(2)	(FDP_ITC or FDP_ITC.2 or FCS_CKM.1): not met, see 7.3 for details. FCS_CKM.4: not met, see 7.3 for details.
FCS_COP.1(3)	(FDP_ITC or FDP_ITC.2 or FCS_CKM.1): not met, see 7.3 for details. FCS_CKM.4: not met, see 7.3 for details.
FDP_ACC.1	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met FMT_MSA.3: unnecessary, since there are no security attributes
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1: met by FDP_ACC.1
FDP_ITT.3	FDP_ACC.1 or FDP_IFC.1: unnecessary, since the reference to the policy was refined away. There exists an access policy in this standard, but this does not concern the communication between handset, control unit and accessory device and is therefore irrelevant to this security functional requirement. FDP_ITT.1: unnecessary, as it is not required for the alcohol interlock to prevent modification/loss of use on the connection between handset, control unit and accessory device. It needs only to detect this and then take action. There is an FDP_ITT.1 security functional requirement included in this standard but this is not related to this FDP_ITT.3 security functional requirement and therefore is unrelated to this dependency.
FDP_RIP.1	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_UID.2	-
FPT_PHP.1(1)	-
FPT_PHP.1(2)	-
FPT_STM.1	-
EAL3	All dependencies within an evaluation assurance level (EAL) are satisfied.
ALC_FLR.2	-

Annex C
(informative)

Security testing

The alcohol interlock should be type tested according to this European Standard by an independent laboratory satisfying the following requirements:

– the laboratory is an IT Security Evaluation Facility which has been licensed by a Certificate-Authorizing Member of the Common Criteria Recognition Arrangement;

– both the laboratory and the Certificate-Authorizing Member are based in the EU (European Union) or the EFTA (European Free Trade Association);

or

the alcohol interlock should be certified according to this European Standard by a Certification Body satisfying the following requirements:

– the certification body is a Certificate-Authorizing Member of the Common Criteria Recognition Arrangement;

– the laboratory performing the evaluation that underlies the certification is licensed by the Certification Body.

Annex D
(informative)

Use of this standard

D.1 Additional information required to use this standard

This European standard is intended to cover the needs of multiple organizations, whose specific requirements may differ. For this reason, the organization using this European standard needs to further specify a number of additional requirements, so as to ensure that the alcohol interlock they employ meets their specific demands. This cannot be done by the manufacturer of the alcohol interlock.

These specifications include:

– choosing which classes of alcohol interlock will be used (A, B1, B2, C1, C2, D), depending on organizational, privacy and legal requirements;

– ensuring that the alcohol interlock also meets EN 50436-1 or EN 50436-2, whichever is applicable;

– defining the set of events which the alcohol interlock shall record and/or is not allowed to record (see FAU_GEN.1);

– defining the specific information that shall be recorded by the alcohol interlock on each event (see FAU_GEN.1);

– defining any specific cryptographic requirements, as countries may have national cryptographic policies (see 7.3);

– confirming that the assurance level (EAL 3 + ALC_FLR.2) provides appropriate assurance;

NOTE Consider that higher assurance levels can result in very significant additional costs.

– defining how compliance with this European Standard is realised (see Annex C).

D.2 Additional requirements for the data handling process

This European standard allows various options, and does not completely cover the security of the entire data handling process. The security of the broker and register, and in some cases the service centre are explicitly not covered by this European standard.

However, the security of these entities is important. An organization wishing to use this standard should therefore consider:

– if classes A, B1, B2, C1 or C2 are allowed, defining precise requirements on how the register should meet

  OE.REGISTER_PROTECT_INCOMING_RECORDS,

  OE.REGISTER_PROTECT_RECORDS, and

  OE.REGISTER_CHECK_AND_CONFIRM

  to ensure that the register handles the event records securely;

– if classes B1 and B2 are allowed, defining precise requirements on how the broker should meet

  OE.BROKER_PROTECT_INCOMING_RECORDS,

  OE.BROKER_PROTECT_RECORDS,

  OE.BROKER_CORRECT_CONVERSION,

  OE.BROKER_SEND_TO_CORRECT_PARTY, and

  OE.BROKER_RELAY_CONFIRMATION

to ensure that the broker handles the event records securely;

– if class C2 is allowed, defining precise requirements on how the service centre should meet

  OE.PROTECTED_SERVICE_APPLICATION

  to ensure that the service centre handles any unencrypted event records securely.

Details given in ISO/IEC 27001 may be used as a guidance for an information security management system.

Blibliography

ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

NOTE 1 A later revision is published as:CCp1: September 2012, Version 3.1, Revision 4, *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*

ISO/IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

NOTE 2 A later revision is published as: CCp2: September 2012, Version 3.1, Revision 4, *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components*

ISO/IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

NOTE 3 A later revision is published as:CCp3: September 2012, Version 3.1, Revision 4, *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components*

ISO/IEC 18045:2008, *Information technology – Security techniques – Methodology for IT security evaluation*

NOTE 4 A later revision is published as:CEMe: September 2012 , Version 3.1, Revision 4, *Common Methodology for Information Technology Security Evaluation - Evaluation methodology*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™