ICS 43.040.10, 71.040.40 SLOVENSKÁ TECHNICKÁ NORMA August 2015

STN	**Uzamykanie reagujúce na alkohol. Skúšobné metódy a požiadavky na funkčné vlastnosti. Časť 6: Bezpečnosť údajov.**	**STN EN 50436-6** 30 4010

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 07/15

Obsahuje: EN 50436-6:2015

121083

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2015
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

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

© 2015 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

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.

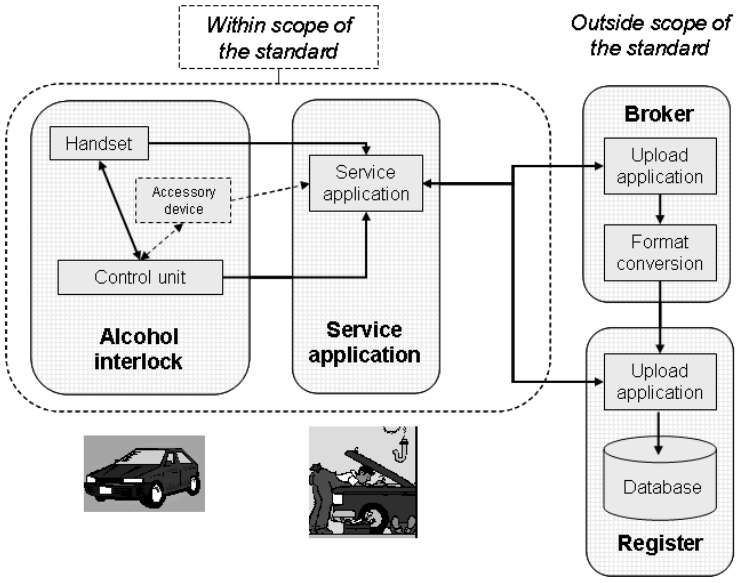

Figure 1 – Alcohol interlock, service application, broker and register

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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN