SLOVENSKI STANDARD
oSIST prEN 16154:2010

01-december-2010

Upravljanje zračnega prometa - Stopnje varovanja programske opreme

Air Traffic Management - Software assurance levels

Flugverkehrsmanagement - Software-Sicherheitsanforderungsstufen

Gestion du trafic aérien - Niveaux d'assurance logicielle

Ta slovenski standard je istoveten z: **prEN 16154**

ICS:

03.220.50	Zračni transport	Air transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

oSIST prEN 16154:2010 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 16154

September 2010

ICS

English Version

Air Traffic Management - Software assurance levels

Gestion du trafic aérien - Niveaux d'assurance logicielle

Flugverkehrsmanagement - Software-Sicherheitsanforderungsstufen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 377.

If this draft becomes a European Standard, CEN 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.

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

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

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (prEN 16154:2010) has been prepared by Technical Committee CEN/TC 377 “Air Traffic Management”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a mandate given to the CEN by the European Commission and developed in cooperation with EUROCAE to support Essential Requirements of the Single European Sky Interoperability Regulation.

Under this regulation, the use of a Community Specification (CS) is a means of compliance to the Essential Requirements of the Regulation and/or the relevant implementing rules for interoperability.

For the relationship with the Single European Sky Interoperability Regulation see Annex SA, the Standards Annex, of this document.

Introduction

The European Union launched the "Single European Sky" (SES) Legislation in 2002 which was adopted in 2004.

The SES legislation is based on a framework of 4 regulations, which includes the Interoperability Regulation (EC 552/2004). The objective of the Interoperability Regulation is to ensure interoperability of the European Air Traffic Management Network (EATMN) consistent with air navigation services.

An increasing proportion of functions of the EATMN are implemented by software and these functions are becoming more safety-critical. It is therefore necessary to define guidance on how to standardise the assurances that may be provided for software.

1 Scope

The present document is for the production of assurance evidence for software used in ground-based systems and their constituents.

This Community Specification on Software Assurance Levels (SWAL) is intended to apply to software that is part of the EATMN, focusing only on it's "ground" segment and providing a reference against which stakeholders can assess their own practices for software specification, design, development, operation, maintenance, evolution and decommissioning.

This Community Specification defines the Technical, Operational and Maintenance requirements for Software Assurance Levels to demonstrate compliance with the applicable (see Annex A) Essential Requirements of the Regulation (EC) N° 552/2004 of the European Parliament and of the Council on the interoperability of the European Air Traffic network ("the Interoperability regulation").

Requirements in the present document which refer to "should" statements or recommendations in the normatively referenced material (2.1) are to be interpreted as fully normative ("shall") for the purpose of compliance with the present document.

2 References

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

2.1 Normative references

EUROCAE ED-153 (august 2009), *Guidelines for ANS software safety assurance*[1)].

2.2 Informative references

ED-109 Guidelines for the Communication Navigation Surveillance and Air Traffic Management (CNS/ATM) systems software integrity assurance

IEC 61508 Functional Safety of electrical/electronic/programmable electronic safety-related systems

Regulation (EC) No 552/2004 (as amended) of the Regulation of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (interoperability Regulation), OJ L 96, 31.03.2004 as amended by Regulation (EC) No 1070/2009 of the European Parliament and of the Council of 21 October 2009 amending Regulations (EC) No 549/2004, (EC) No 550/2004, (EC) No 551/2004, (EC) No 552/2004 in order to improve the performance and sustainability of the European aviation system

1) ED 153 has been made available to the responsible CEN technical body, CEN/TC 377 'Air Traffic Management', as document TC377 N 112.

3 Terms and definitions

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

3.1
ANS
Air Navigation Service

3.2
COTS
Commercial off the shelf software, means a commercial available application sold by vendors through public catalogue listings and not intended to be customised or enhanced;

3.3
CS
Community Specification

3.4
EATMN
European Air Traffic Management Network

3.5
EC
European Commission

3.6
EUROCAE
European Organisation for Civil Aviation Equipment

3.7
SES
Single European Sky

3.8
Software
means computer programmes and corresponding configuration data, including non-developmental software, but excluding electronic items, namely application specific integrated circuits, programmable gate arrays or solid-state logic controllers.

NOTE Non-developmental software includes proprietary software, COTS software, re-used software

3.9
SWAL
Software Assurance Level

4 Software Assurance Levels (SWAL)

The processes detailed below are those that are required in order to be able to provide assurance evidence for software in EATMN in compliance with the present document.

4.1 Allocation

The allocation of a Software assurance level shall comply with the requirements defined in ED-153, 3.6.2.0 while replacing the table with the following table 1:

Table 1

Effect Severity Class / Likelihood of generating such an effect (Pe x Ph)	1	2	3	4
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL4	SWAL4
Very Unlikely	SWAL3	SWAL4	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

The Grading Policy, i.e. the aim of a SWAL including what kind of overall objective is intended shall comply with the requirements in ED-153, 3.6.4.0 and 3.6.4.1. “Independence in performing the prevention” in table 11 (column 4) of 3.6.4.1 shall be understood as “Independence in checking the prevention”.

NOTE Examples of the use of the SWAL allocation process are described in ED-153, 3.6.3 and 3.6.1.0.

4.2 Likelihood assessment

Within the SWAL allocation process, for the assessment of the likelihood of an effect, ED-153, 3.6.2.1 shall apply.

4.3 Likelihood justification

The factors detailed in ED-153, 3.6.2.2. shall be considered when justifying the likelihood of an effect during the SWAL allocation process.

5 SWAL Objectives per Process

5.1 General

The identification of objectives applicable to each SWAL is addressed in ED-153, i.e. Chapters 4, 5 and 7 in terms of Primary Life Cycle Processes, Supporting Life Cycle Processes and COTS-related processes.

NOTE 1 If different assurance levels from other reference documents such as ED-109, IEC 61508 are used, annex A of ED-153 provides a method for gap analysis.

NOTE 2 Description and scenarios for roles and responsibilities are detailed in ED-153 Annex B.

5.2 Primary Life Cycle Processes

5.2.1 The Acquisition Process

The Acquisition Process that details the objectives and tasks that shall be complied with by the acquirer is defined in ED-153, 4.1. For objectives 4.1.2 and 4.1.3 of ED-153 independence is only required for SWAL 1 and 2.

5.2.2 The Supply Process

The Supply Process that details the objectives and tasks that shall be complied with by the supplier is defined in ED-153, 4.2.

5.2.3 The Development Process

The Development Process detailing the objectives and tasks that shall be complied with by the developer is defined in ED-153, 4.3. For objectives 4.3.1 and 4.3.2 of ED-153 independence is only required for SWAL 1 and 2.

5.2.4 The Operation Process

The Operation Process that details the objectives and tasks that shall be complied with by the operator is defined in ED-153, 4.4. For objectives 4.4.5 of ED-153 independence is only required for SWAL 1 and 2.

5.2.5 The Maintenance Process

The Maintenance Process that details the objectives and tasks that shall be complied with by the maintainer is defined in ED-153, 4.5. For objectives 4.5.2 and 4.5.5 of ED-153 independence is only required for SWAL 1 and 2.

5.3 Supporting Life Cycle Processes

5.3.1 The Documentation Process

The Documentation Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.1.

5.3.2 The Configuration Management Process

The Configuration Management Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.2. The software configuration management shall be performed at the Software executable level (for SWAL 1 Software, only).

5.3.3 The Quality Assurance Process

The Quality Assurance Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.3.

5.3.4 The Verification Process

The Verification Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.4.

5.3.5 The Joint Review Process

The Joint Review Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.6.

5.3.6 The Audit Process

The Audit Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.7. Process implementation is not required for SWAL 4.

5.3.7 The Problem/Change Resolution Process

The Problem/Change Resolution Process that details the objectives and tasks that shall be complied with by all concerned parties is defined in ED-153, 5.8. For objectives 5.8.1, 5.8.3 and 5.8.4 of [1] independence is only required for SWAL 1 and 2.

5.4 Organisational Life Cycle Processes

Organisational Life Cycle objectives shall be met per SWAL.

NOTE 1 The Management Process that details the objectives and tasks of all concerned parties is defined in ED-153, 6.1.

NOTE 2 The Infrastructure Process that details the objectives and tasks of all concerned parties is defined in ED-153, 6.2.

NOTE 3 The Improvement Process that details the objectives and tasks of all concerned parties is defined in ED-153, 6.3.

NOTE 4 The Training Process that details the objectives and tasks of all concerned parties is defined in ED-153, 6.4.

5.5 COTS processes

5.5.1 COTS planning process

The planning process that details the objectives and tasks that shall be complied with is defined in ED-153, 7.2.2.