PD CEN/TS 16501:2013

BSI Standards Publication

Air Traffic Management — Specification for software assurance levels

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TS 16501:2013.

The UK participation in its preparation was entrusted to Technical Committee ACE/58, Environmental and operating conditions for aircraft equipment.

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.

ISBN 978 0 580 80429 8

ICS 35.240.60

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2013.

Amendments issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16501

April 2013

ICS 35.240.60

English Version

Air Traffic Management - Specification for software assurance levels

Gestion du trafic aérien - Spécification des niveaux d'assurance logicielle

Flugverkehrsmanagement - Spezifikation für Software-Sicherheitsanforderungsstufen

This Technical Specification (CEN/TS) was approved by CEN on 12 February 2013 for provisional application.

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

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

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

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 16501:2013: E

Contents

Page

Foreword 3

Introduction 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 5

4 Software Assurance Levels (SWAL) 6
4.1 General 6
4.2 Allocation 6
4.3 Likelihood assessment 6
4.4 Likelihood justification 6

5 SWAL Objectives per Process 6
5.1 General 6
5.2 Primary Life Cycle Processes 7
5.2.1 The Acquisition Process 7
5.2.2 The Supply Process 7
5.2.3 The Development Process 7
5.2.4 The Operation Process 7
5.2.5 The Maintenance Process 7
5.3 Supporting Life Cycle Processes 7
5.3.1 The Documentation Process 7
5.3.2 The Configuration Management Process 7
5.3.3 The Quality Assurance Process 7
5.3.4 The Verification Process 7
5.3.5 The Joint Review Process 7
5.3.6 The Audit Process 8
5.3.7 The Problem/Change Resolution Process 8
5.4 Organisational Life Cycle Processes 8
5.5 COTS processes 8
5.5.1 COTS planning process 8
5.5.2 COTS acquisition process 8
5.5.3 COTS verification process 8
5.5.4 COTS configuration management process 8

Bibliography 9

Foreword

This document (CEN/TS 16501:2013) has been prepared by Technical Committee CEN/TC 377 “Air Traffic Management”, the secretariat of which is held by DIN.

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

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

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

This Technical Specification specifies the technical, operational and maintenance requirements for Software Assurance Levels to support the demonstration of compliance with some elements of the Essential Requirements “Safety” and “Principles governing the construction of systems” of the Regulation (EC 552/2004) of the European Parliament and of the Council on the interoperability of the European Air Traffic network (“the Interoperability regulation”).

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

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

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.

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

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
commercially available application sold by vendors through public catalogue listings and not intended to be customised or enhanced

3.3
EATMN
European Air Traffic Management Network

3.4
EC
European Community

3.5
EU
European Union

3.6
EUROCAE
European Organisation for Civil Aviation Equipment

1) Published by: EUROCAE, 102 rue Etienne Dolet, 92240 Malakoff – France

3.7
SES
Single European Sky

3.8
software
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 1 to entry: Non-developmental software includes proprietary software, COTS software, re-used software

3.9
SWAL
Software Assurance Level

4 Software Assurance Levels (SWAL)

4.1 General

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.

4.2 Allocation

The allocation of a Software Assurance Level shall comply with the requirements specified in ED-153.

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.

4.3 Likelihood assessment

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

4.4 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. Clauses 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, EN 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 specified 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 specified 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 specified 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 specified 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 specified 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 specified 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 specified in ED-153, 5.2. In addition, for SWAL 1, software configuration management shall be performed at executable level.

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 specified 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 specified 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 specified 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 specified 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 specified in ED-153, 5.8. For objectives 5.8.1, 5.8.3 and 5.8.4 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 specified in ED-153, 6.1.

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

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

NOTE 4 The Training Process that details the objectives and tasks of all concerned parties is specified 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 specified in ED-153, 7.2.2.

5.5.2 COTS acquisition process

The acquisition process that details the objectives and tasks that shall be complied with is specified in ED-153, 7.2.3.

5.5.3 COTS verification process

The verification process detailing the objectives and tasks that shall be complied with is specified in ED-153, 7.2.4.

NOTE Some alternative methods are described in ED-153, 7.2.4.2 and 7.2.4.3.

5.5.4 COTS configuration management process

The configuration management process that details the objectives and tasks that shall be complied with is specified in ED-153, 7.2.5.

Bibliography

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

[2] EN 61508 (all parts), *Functional Safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508, all parts)*

[3] 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

[4] Commission Implementing Regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010

[5] Regulation (EC) No 549/2004 (as amended) of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation), OJ L 96, 31.03.2004.

[6] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 204, 21.07.1998 (modified by Directive 98/48/EC, OJ L 217, 05.08.1998).

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.™