IEC/PAS 62814

Edition 1.0 2012-12

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

Dependability of software products containing reusable components – Guidance for functionality and tests

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XA

ICS 03.120.01

ISBN 978-2-83220-501-3

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms, definitions and abbreviations 8
3.1 Terms related to software engineering 8
3.2 Terms related to software dependability 9
3.3 Terms related to software reuse 10
3.4 General terms 13
3.5 Abbreviations 13
4 Dependability of software reuse methodology – Reusability-driven software development 13
4.1 General 13
4.2 Dependability methods for reuse 15
4.3 Dependability-related objectives of software reuse 16
4.4 Ingredients of software reuse and hypotheses for reuse dependability 17
5 Software reuse dependability methodology applications 18
5.1 Application aspects and organization of dependable software reuse 18
5.1.1 General 18
5.1.2 Pre-*store* characteristics of reusability 19
5.1.3 Pre-*use* characteristics of reusability 20
5.1.4 Build-*for*-reuse 20
5.1.5 Build-*by*-reuse 21
5.1.6 Coupling “build-for-reuse” and “build-by-reuse” 22
5.2 Validation, re-validation and reliability of software reuse 25
5.3 Naïve assumptions and rules for improving software reuse dependability 26
5.4 Dependability and reuse aspects of software/hardware interaction 26
5.4.1 General 26
5.4.2 Reuse of software with an upgrade / remanufactured hardware 26
5.4.3 Limitations of hardware 27
5.4.4 Limitations due to incompatibilities 27
5.4.5 Dependability, energy consumption and ecology 27
6 Software reuse assurance 27
6.1 General 27
6.2 Build for reuse – Validation and qualification of components to be reused 28
6.2.1 General 28
6.2.2 Validation and qualification 28
6.2.3 Assessment of quantifiable quality targets 28
6.3 Build by reuse – Validation and qualification of the receiving system 28
6.3.1 General 28
6.3.2 Validation and qualification 28
6.3.3 Assessment of quantifiable quality targets 29
7 Warranty and documentation 29
7.1 General 29
7.2 Life cycle, contextual criticality, warranty period 29
7.3 Product documentation 29

7.4 Product safety and control 29
7.5 Legal aspects 29
7.5.1 General 29
7.5.2 Contractual issues 29
7.5.3 Product liability 30
Annex A (informative) General remarks on software reuse 31
Annex B (informative) Qualification and integration of reusable software components 33
Annex C (informative) Testing and integration of reusable software components – Issues for industrial best practice 37
Annex D (informative) Example of software pre-use 46
Annex E (informative) Influence of reused software to hardware components and products 50
Bibliography 52

Figure 1 – Approaches to software reuse and its elements 15
Figure 2 – Elements of the reuse process 17
Figure 3 – Integration of the reusable component 17
Figure 4 – Characteristics of reusability 19
Figure 5 – Build-for-reuse framework 21
Figure 6 – Build-by-reuse framework 22
Figure 7 – Combining “build-for-reuse” and “build-by-reuse” 24
Figure A.1 – Service-oriented architecture 31
Figure C.1 – A test process in vendor-oriented component testing [30] 38
Figure C.2 – A validation process for completely reused components [30] 40
Figure C.3 – A Validation process for adapted and customized components 41
Figure C.4 – Maturity levels for a component testing process 43
Figure D.1 – Example of a supervision task 49

Table 1 – Summary of reuse classification 14
Table C.1 – Testing issues of reusable software components 43
Table D.1 – Operating experience, monolithic view 47
Table D.2 – Operating experience, use of the individual paths 47
Table D.3 – Production demands, use of the individual paths; the values of p_i did not change 48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY OF SOFTWARE PRODUCTS CONTAINING REUSABLE COMPONENTS – GUIDANCE FOR FUNCTIONALITY AND TESTS

FOREWORD

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

A PAS is a technical specification not fulfilling the requirements for a standard, but made available to the public.

IEC/PAS 62814 has been processed by IEC technical committee 56: Dependability.

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
56/1479/PAS	56/1490/RVD

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

This PAS shall remain valid for an initial maximum period of 3 years starting from the publication date. The validity may be extended for a single period up to a maximum of 3 years, at the end of which it shall be published as another type of normative document, or shall be withdrawn.

INTRODUCTION

Technological growth is accelerating; development cycles for products are becoming shorter and shorter. At the same time software is taking an increasingly important part in the control and functionality of products and in integrating the functions of hardware components. The disciplined development of software has been going on for more than 40 years and software is now available in many forms and formats. Apparently, the cost of software development can easily be amortized if it is embedded as often, and in as many different products, as possible. This potential benefit of software reuse should at no time be at the expense of dependability. Dependability is the ability of a system to perform as and when required to meet specific objectives under given conditions of use.

Any innovative product that has matured enough to hit the shelves needs a new and progressive approach. Dependability of the products is an attribute that is mandatory for newly developed or reused software (and the complete product into which the software is embedded) to be accepted and sold. Therefore, the dependability of software and its components should be assured in just the same way that the dependability of hardware and its components have been assured for many decades. This requires the standardization of software and software components to keep up with the ever higher levels which hardware components continue to achieve.

The dependability of a system infers that the system is trustworthy and capable of performing the desired service upon demand to satisfy user needs. Whereas a software component may be perfectly suited to one application, it may prove to cause severe faults in other applications. To allow the innovators to concentrate on their main task – to create new and better products with an extended functionality – it is fundamental to provide the certainty that reused software is dependable in its new application and does not need to be re-designed from scratch. Safety and security aspects might be combined if required. Therefore an adequate test process considering the changed purpose and the different application configuration in combination with new, reused, or further used components is needed. Altogether, testing of software products containing reused components is an important target to be reached.

An additional, important aspect to be considered is the energy efficiency and eco-friendliness of hardware products controlled by software. Reuse of a component with a bad energy consumption behaviour will multiply this bad behaviour, and thus negatively impact the entire energy consumption of the new system that is composed of such components; the same way as an undependable component impacts the dependability of the system into which it will be built. A rule of thumb is that reused software should not result in a product consuming more energy than a comparable energy-efficient product on the market.

This publicly available specification (PAS) addresses the functionality, testing and dependability of software components to be reused and products that contain software to be used in more than one application; that is, reused by the same or by another development organization, regardless of whether it belongs to the same or another legal entity than the one that has developed this software.

DEPENDABILITY OF SOFTWARE PRODUCTS CONTAINING REUSABLE COMPONENTS – GUIDANCE FOR FUNCTIONALITY AND TESTS

1 Scope

This publicly available specification introduces the concept of assuring reused components and their usage within new products. It provides information and criteria about the tests and analysis required for products containing such reused parts. The objective is to support the engineering requirements for functionality and tests of reusable software components and composite systems containing such components in evaluating and assuring reuse dependability.

Focus is on the dependability of software reuse and, thus, this PAS complements IEC 62309 which exclusively considers hardware reuse. In addition to this previous hardware-related IEC standard, the present PAS also crosses further, appropriate software-related standards to be applied in the development and qualification of software components that are intended to be reused and products that reuse existing components. In other words, this PAS encompasses the features of software components for reuse, their integration into the receiving system, and related tests. Their performance and qualification and the qualification of the receiving system is subject to existing standards, for example ISO/IEC 25000 [01][1], IEC 61508-3 [01] and IEC 61508-4 [03]. The process framework of ISO/IEC 12207 [04] on systems and software engineering and ISO/IEC 25000 [01] on system aspects of dependability on software engineering apply to this PAS.

The purpose of this PAS is to ensure through analysis and tests that the functionality, dependability and eco-friendliness of a new product containing reused software components is comparable to a product with only new components. This would justify the manufacturer providing the next customer with a warranty for the functionality and dependability of a product with reused components. As each set of hardware/software has a unique relationship and is governed by its operational scenario, the dependability determination has to consider the underlying operational background. Dependability also influences safety. Therefore, wherever it seems necessary, safety aspects have to be considered the way IEC 60300-1 addresses safety issues.

This PAS can also be applied in producing product-specific standards by technical committees responsible for an application sector.

This PAS is not intended for certification purposes.

2 Normative references

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

IEC 60300-1, *Dependability management – Part 1: Dependability management systems*

IEC 62628, *Guidance on software aspects of dependability*

---

1 Numbers in square brackets refer to the Bibliography.

IEC 62309, *Dependability of products containing reused parts – Requirements for functionality and tests*