

IEEE Standard for Software Safety Plans

Sponsor

Software Engineering Standards Committee
of the
IEEE Computer Society

Reaffirmed 25 March 2010
Approved 17 March 1994

IEEE-SA Standards Board

Reaffirmed 18 April 2003
Approved 2 September 1994

American National Standards Institute

Abstract: The minimum acceptable requirements for the content of a software safety plan are established. This standard applies to the software safety plan used for the development, procurement, maintenance, and retirement of safety-critical software. This standard requires that the plan be prepared within the context of the system safety program. Only the safety aspects of the software are included. This standard does not contain special provisions required for software used in distributed systems or in parallel processors.

Keywords: safety-critical software, software safety plan, software safety program, safety requirements

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1994 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1994. Printed in the United States of America.

Print: ISBN 1-55937-496-6 SH94255
PDF: ISBN 0-7381-0419-1 SS94255

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not part of IEEE Std 1228-1994, IEEE Standard for Software Safety Plans.)

This standard describes the minimum acceptable requirements for the content of a software safety plan. This standard contains four clauses. Clause 1 discusses the application of the standard. Clause 2 lists references to other standards. Clause 3 provides a set of definitions and acronyms used in the standard. Clause 4 contains the required content of a software safety plan. In order to be in compliance with this standard, users of the standard shall adhere to clause 4. The informative annex discusses software safety analyses.

This standard was written for those who are responsible for defining, planning, implementing, or supporting software safety plans.

Participants in the working group were individually supported by their employers with travel expenses and working days. This support does not constitute or imply approval or endorsement of this standard.

This standard was developed by the Software Safety Plans Working Group consisting of the following members who attended two or more meetings, provided text, or submitted comments on two or more drafts of the standard.

Cynthia L. Wright, *Chair*

Anthony J. Zawilski, *Vice chair*

Patricia Trellue, *Configuration manager*

Dick Bair
Leo Beltracchi
Mordechai Ben-Menachem
P. V. Bhansali
David Burrows
Betty Chao
John Cherviasvsky
Tony Clark
Taz Daughtrey
David Dini
L. G. Egan
Alwyn Goodloe
Herb Hecht

John Horch
Grady Lee
Nancy Leveson
Stanley Levinson
Ben Livson
D. P. Mannering
Scott Mathews
John McHugh
Archibald McKinlay
Bonnie Melhart
Bret Michael
Tammy Pelnik
John Perry

Norman Schneidewind
David Schultz
Anita Shagnea
Peter Shilling
Edgar Sibley
Mel Smyre
Jack Spraul
Leslie Stepanek
V. K. Srivastava
Leonard Tripp
Ron Vaickavski
Delores Wallace
Chuck Weinstock

The following individuals also contributed to the development of the standard by attending one meeting or providing comments on one draft:

Paul Ammann
Jordan Anderson
Ron Berlack
Richard Blauw
Thomas Braudt
J. Brazendale
Fletcher Buckley
David Card
James Cardow
Geoff Cozens
Ron Daly
Paul Davis
C. G. Diderich
Audrey Dorofee
Caroline Evans
Peter Farrell-Vinay
Fred Freiburger
Al Friend
David Gelperin
Donna Grush

John Harauz
Albert Hoheb
Charles Horn
Frank Houston
Diane Jachinowski
Jon Jacky
George Kambic
Alasdair Kemp
Phil Keys
Thomas Kurihara
Victor Maggioli
John Matras
A. D. McGettrick
Rovert Metro
Judy Moore
Bahman Mostafazadeh
Melissa Murphy
Dennis Nickle
Mark Oliver
Tuncer Oren

Dave Peercy
Dev Raheja
Steven Rakitin
Juri Reinfelds
Heinz Rogen
Art Rubino
Leonard Russo
Damian Saccochio
Hans Schaefer
Robert Shillato
Richard Thayer
Jerry Thrasher
Dinos Tsagoes
David Vickers
Jim Widmyer
Eugene Wilhelm
Bill Wood
N. Yogaramanan
Janusz Zalewski
Peter Zoll

The following persons were on the balloting committee:

William Bates	William Hefley	Dave Peercy
Mordechai Ben-Menachem	Janene Heinzman	Tammy Pelnik
Ron Berlack	David Heron	Juri Reinfelds
Sandro Bologna	John Horch	James Ronback
Fletcher Buckley	Charles Howell	Stephen Schach
Kay Bydalek	Lynn Ihlenfeldt	Hans Schaefer
David Card	William Junk	Norman Schneidewind
Betty Chao	George Kambic	David Schultz
Tony Clark	Thomas Kurihara	Gregory Schumacher
Geoff Cozens	Robert Lane	Robert Shillato
Taz Daughtrey	Charles Lavine	Edgar Sibley
Paul Davis	Dennis Lawrence	Mel Smyre
Einar Dragstedt	Nancy Leveson	V. K. Srivastava
L. G. Egan	Stanley Levinson	Richard Thayer
Caroline Evans	Ben Livson	George Tice
John Fendrich	Joseph Maayan	Patrica Trellue
Joanna Frawley	John MacMillan	Leonard Tripp
Roger Fujii	Jukka Marijarvi	Ron Vaickavski
David Gelperin	Roger Martin	David Vickers
Yair Gershkovitch	Scott Mathews	Udo Voges
Julio Gonzalez-Sanz	Ivano Mazza	Delores Wallace
David Gustafson	John McHugh	Paul Work
John Harauz	James Michael	Cynthia Wright
Herb Hecht	Dennis Nickle	Janusz Zalewski

When the IEEE Standards Board approved this standard on March 17, 1994, it had the following membership:

Wallace S. Read, *Chair*

Donald C. Loughry, *Vice Chair*

Andrew G. Salem, *Secretary*

Gilles A. Baril	Donald N. Heirman	Joseph L. Koepfinger*
Bruce B. Barrow	Richard J. Holleman	D. N. "Jim" Logothetis
José A. Berrios de la Paz	Jim Isaak	L. Bruce McClung
Clyde R. Camp	Ben C. Johnson	Marco W. Migliaro
James Costantino	Sonny Kasturi	Mary Lou Padgett
Stephen L. Diamond	Lorraine C. Kevra	Arthur K. Reilly
Donald C. Fleckenstein	E. G. "Al" Kiener	Ronald H. Reimer
Jay Forster*	Ivor N. Knight	Gary S. Robinson
Ramiro Garcia		Leonard L. Tripp

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
James Beall
Richard B. Engelman
David E. Soffrin
Stanley I. Warshaw

Rachel A. Meisel
IEEE Standards Project Editor

Contents

CLAUSE	PAGE
1. Overview.....	1
1.1 Purpose.....	1
1.2 Scope.....	1
1.3 Application.....	1
1.4 Disclaimer.....	2
2. References.....	2
3. Definitions and abbreviations	3
3.1 Definitions.....	3
3.2 Abbreviations.....	3
4. Contents of a software safety plan.....	4
4.1 Purpose (Section 1 of the Plan).....	5
4.2 Definitions, acronyms and abbreviations, and references (Section 2 of the Plan)	5
4.3 Software safety management (Section 3 of the Plan)	5
4.4 Software safety analyses (Section 4 of the Plan)	10
4.5 Post development (Section 5 of the Plan).....	12
4.6 Plan approval (Section 6 of the Plan)	14
ANNEX	
Discussion of software safety analyses (informative)	15
A.1 Software safety requirements analyses	15
A.2 Software safety design analysis	15
A.3 Software safety code analysis	16
A.4 Software safety test analysis	17
A.5 Software safety change analysis	17

IEEE Standard for Software Safety Plans

1. Overview

1.1 Purpose

This standard establishes the minimum acceptable requirements for the content of a Software Safety Plan (also referred to as the Plan) to address the processes and activities intended to improve the safety of safety-critical software.

1.2 Scope

This standard applies to the Plan used for the development, procurement, maintenance, and retirement of safety-critical software; for example, software products whose failure could cause loss of life, serious harm, or have widespread negative social impact. This standard requires that the Plan be prepared within the context of the system safety program. The scope of this standard includes only the safety aspects of the software. This standard does not contain special provisions required for software used in distributed systems or in parallel processors.

1.3 Application

The Plan is prepared under the direction of project or system safety program management to address the identified potential software safety risks.

Compliance with this standard requires the creation of a written plan that addresses each topic, subtopic, and stipulation described in clause 4. The level of detail in, and the resources required by an software safety plan will be determined by factors including the type and level of risks associated with the software product, the complexity of the application, and external forces such as contractual requirements.

Software is a portion of a system. Other portions of that system include computer hardware, other devices (possibly including mechanical, electrical, chemical, or nuclear devices), and people. Software alone is not a safety issue; it is only an issue in the context of this larger system. Hence, software safety must begin with the larger system. Software safety must be considered in the context of its associated hardware, environment, and operators. The Plan needs to address interfaces with these elements.

The existence of this standard should not be construed to discourage or prohibit the imposition of additional or more stringent requirements where the need exists. An assessment should be made for the specific software project to ensure adequacy of coverage and safety assurance. Where this standard is invoked for a