

UL 1998

ISBN 0-7629-0321-X

Software in Programmable Components

Underwriters Laboratories Inc. (UL)
333 Pfingsten Road
Northbrook, IL 60062-2096

UL Standard for Safety for Software in Programmable Components, UL 1998

Second Edition, Dated May 29, 1998

The revisions dated May 2, 2000 include a reprinted title page (page1) for this Standard.

UL is in the process of converting its Standards for Safety to the Standard Generalized Markup Language (SGML), and implementing an SGML compliant document management and publishing system. SGML - an international standard (ISO 8879-1986) - is a descriptive markup language that describes a document's structure and purpose, rather than its physical appearance on a page. Significant benefits that will result from UL's use of SGML and these new systems include increased productivity, reduced turnaround times, and data and information consistency, reusability, shareability, and portability. However, the fonts, pagination, and general formatting of UL's new electronic publishing system differ from that of UL's previous publishing system. Consequently, when revision pages are issued for a Standard with the new publishing system, these differences may result in the printing of pages on which no requirements have been changed - these additional pages result from relocation of text due to repagination and reformatting of the Standard with the new publishing system. **As a result of UL's use of this new electronic publishing tool, the current copy of UL 1998 will need to be replaced with this copy. The entire original text has been retained, only the location of the page contents has been changed.**

As indicated on the title page (page 1), this UL Standard for Safety is an American National Standard. Attention is directed to the note on the title page of this Standard outlining the procedures to be followed to retain the approved text of this ANSI/UL Standard.

The master for this Standard at UL's Northbrook Office is the official document insofar as it relates to a UL service and the compliance of a product with respect to the requirements for that product and service, or if there are questions regarding the accuracy of this Standard.

UL's Standards for Safety are copyrighted by UL. Neither a printed copy of a Standard, nor the distribution diskette for a Standard-on-Diskette and the file for the Standard on the distribution diskette should be altered in any way. All of UL's Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of UL.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise without prior permission of UL.

Revisions of UL Standards for Safety are issued from time to time. A UL Standard for Safety is current only if it incorporates the most recently adopted revisions.

UL provides this Standard "as is" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability or fitness for any purpose.

In no event will UL be liable for any special, incidental, consequential, indirect or similar damages, including loss of profits, lost savings, loss of data, or any other damages arising out of the use of or the inability to use this Standard, even if UL or an authorized UL representative has been advised of the possibility of such damage. In no event shall UL's liability for any damage ever exceed the price paid for this Standard, regardless of the form of the claim.

UL will attempt to answer support requests concerning electronic versions of its Standards. However, this support service is offered on a reasonable efforts basis only, and UL may not be able to resolve every support request. UL supports the electronic versions of its Standards only if they are used under the conditions and operating systems for which it is intended. UL's support policies may change from time-to-time without notification.

UL reserves the right to change the format, presentation, file types and formats, delivery methods and formats, and the like of both its printed and electronic Standards without prior notice.

Purchasers of the electronic versions of UL's Standards for Safety agree to defend, indemnify, and hold UL harmless from and against any loss, expense, liability, damage, claim, or judgement (including reasonable attorney's fees) resulting from any error or deviation introduced while purchaser is storing an electronic Standard on the purchaser's computer system.

If a single-user version electronic Standard was purchased, one copy of this Standard may be stored on the hard disk of a single personal computer, or on a single LAN file-server or the permanent storage device of a multiple-user computer in such a manner that this Standard may only be accessed by one user at a time and for which there is no possibility of multiple concurrent access.

If a multiple-user version electronic Standard was purchased, one copy of the Standard may be stored on a single LAN file-server, or on the permanent storage device of a multiple-user computer, or on an Intranet server. The number of concurrent users shall not exceed the number of users authorized.

Electronic Standards are intended for on-line use, such as for viewing the requirements of a Standard, conducting a word search, and the like. Only one copy of the Standard may be printed from each single-user version of an electronic Standard. Only one copy of the Standard may be printed for each authorized user of a multiple-user version of an electronic Standard. Because of differences in the computer/software/printer setup used by UL and those of electronic Standards purchasers, the printed copy obtained by a purchaser may not look exactly like the on-line screen view or the printed Standard.

An employee of an organization purchasing a UL Standard can make a copy of the page or pages being viewed for their own fair and/or practical internal use.

The requirements in this Standard are now in effect, except for those paragraphs, sections, tables, figures, and/or other elements of the Standard having future effective dates as indicated in the note following the affected item. The prior text for requirements that have been revised and that have a future effective date are located after the Standard, and are preceded by a "SUPERSEDED REQUIREMENTS" notice.

New product submittals made prior to a specified future effective date will be judged under all of the requirements in this Standard including those requirements with a specified future effective date, unless the applicant specifically requests that the product be judged under the current requirements. However, if the applicant elects this option, it should be noted that compliance with all the requirements in this Standard will be required as a condition of continued Listing and Follow-Up Services after the effective date, and understanding of this should be signified in writing.

Copyright © 2000 Underwriters Laboratories Inc.

This Standard consists of pages dated as shown in the following checklist:

Page	Date
1-20.....	May 2, 2000
A1-A12	May 2, 2000

MAY 29, 1998
(Title Page Reprinted: May 2, 2000)



1

UL 1998

Standard for Software in Programmable Components

First Edition – January, 1994

Second Edition

May 29, 1998

The most recent approval of UL 1998 as an American National Standard (ANSI) occurred on January 28, 1999. Approval of UL 1998 as an American National Standard is maintained using the continuous maintenance process. Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Written comments are to be sent to UL-RTP Standard Department, 12 Laboratory Drive, Research Triangle Park, NC 27709.

An effective date included as a note immediately following certain requirements is one established by Underwriters Laboratories Inc.

Revisions of this Standard will be made by issuing revised or additional pages bearing their date of issue. A UL Standard is current only if it incorporates the most recently adopted revisions, all of which are itemized on the transmittal notice that accompanies the latest set of revised requirements.

ISBN 0-7629-0321-X

COPYRIGHT © 1994, 2000 UNDERWRITERS LABORATORIES INC.

No Text on This Page

CONTENTS

FOREWORD	4
-----------------	----------

PREFACE	5
----------------	----------

1 Scope	6
2 Definitions of Terms Used	6
3 Risk Analysis	11
4 Process Definition	11
5 Qualification of Design, Implementation, and Verification Tools	11
6 Software Design	12
7 Critical and Supervisory Sections of Software	12
8 Measures To Address Microelectronic Hardware Failure Modes	13
9 Product Interface	14
10 User Interfaces	14
11 Software Analysis and Testing	15
11.1 Software analysis	15
11.2 Software testing	15
11.3 Failure mode and stress testing	16
12 Documentation	17
12.1 User documentation	17
12.2 Software plan	17
12.3 Risk analysis approach and results	17
12.4 Configuration management plan	17
12.5 Programmable system architecture	18
12.6 Programmable component and software requirements specification	18
12.7 Software design documentation	18
12.8 Analysis and test documentation	18
13 Off-the-Shelf (OTS) Software	19
14 Software Changes and Document Control	20
15 Identification	20

APPENDIX A – EXAMPLES OF MEASURES TO ADDRESS MICROELECTRONIC HARDWARE FAILURE MODES

A1 Scope	A1
A2 Examples of Acceptable Measures for Microelectronic Hardware Failure Modes	A1
A3 Software Classes	A7
A4 Description of Fault Models	A8
A5 Description of System Structures	A8
A6 Example of the Application of Table A2.1	A9
A7 Descriptions of Acceptable Measures for Providing the Required Fault/Error Coverage Specified in Table A2.1	A9
A7.1 Descriptions of fault/error control techniques	A10
A7.2 Description of memory tests	A11
A7.3 Word protection	A12

FOREWORD

A. This Standard contains basic requirements for products covered by Underwriters Laboratories Inc. (UL) under its Follow-Up Service for this category within the limitations given below and in the Scope section of this Standard. These requirements are based upon sound engineering principles, research, records of tests and field experience, and an appreciation of the problems of manufacture, installation, and use derived from consultation with and information obtained from manufacturers, users, inspection authorities, and others having specialized experience. They are subject to revision as further experience and investigation may show is necessary or desirable.

B. The observance of the requirements of this Standard by a manufacturer is one of the conditions of the continued coverage of the manufacturer's product.

C. A product which complies with the text of this Standard will not necessarily be judged to comply with the Standard if, when examined and tested, it is found to have other features which impair the level of safety contemplated by these requirements.

D. A product employing materials or having forms of construction which conflict with specific requirements of the Standard cannot be judged to comply with the Standard. A product employing materials or having forms of construction not addressed by this Standard may be examined and tested according to the intent of the requirements and, if found to meet the intent of this Standard, may be judged to comply with the Standard.

E. UL, in performing its functions in accordance with its objectives, does not assume or undertake to discharge any responsibility of the manufacturer or any other party. The opinions and findings of UL represent its professional judgment given with due consideration to the necessary limitations of practical operation and state of the art at the time the Standard is processed. UL shall not be responsible to anyone for the use of or reliance upon this Standard by anyone. UL shall not incur any obligation or liability for damages, including consequential damages, arising out of or in connection with the use, interpretation of, or reliance upon this Standard.

F. Many tests required by the Standards of UL are inherently hazardous and adequate safeguards for personnel and property shall be employed in conducting such tests.

PREFACE

The requirements in UL 1998 address non-networked embedded software residing in programmable components which are application-specific. Embedded software is software that resides in a programmable component and that performs some of the requirements of the programmable component. Non-networked embedded software is embedded software that executes on a single microprocessor/microcontroller or on redundant microprocessors/microcontrollers residing in the same physical enclosure. Application-specific means that the software is limited to a designated application which permits effective evaluation of the hazards and risks associated with the software. Programmable components are any microelectronic hardware that can be programmed in the design center, the factory, or in the field.

The requirements in UL 1998 are applicable when used in conjunction with an application-specific standard that contains requirements for safety-related functions implemented using software. UL 1998 does not apply to software in programmable components used in general purpose applications when the risks for the end-application cannot be identified. Safety-related functions are control, protection, and monitoring functions which are intended to reduce the risk of fire, electric shock, or injury to persons. When UL 1998 is applied to a specific product, it is intended that the requirements address product safety risks associated with the specific purpose (as components only) use of software in the programmable component. A product is an instrument, apparatus, implement, or machine intended for personal, household, industrial, laboratory, office, or transportation use.

The requirements in UL 1998 are not intended to be used as the sole basis for reviewing programmable components. UL 1998 is intended to be used in conjunction with other safety standards that address the programmable component hardware. Requirements in UL 1998 may be amended or superseded by requirements in a product safety standard, a directive, regulation, or a purchasing specification.

Due to the diversity of software functions and the application-specific nature of testing programmable components, UL 1998 indicates neither testing protocols nor tools. Instead, UL 1998 contains requirements that define test objectives and criteria for the general case. This permits the user to choose from many testing protocols and tools as long as the test objectives and criteria are met. Users of UL 1998 are encouraged to specify and make available to the public the test protocols and tools used when applying the requirements of UL 1998.

The UL 1998 Standard covers handling of changes to the software in the programmable component after release. The recognition of maintenance processes for the handling and qualification of software and programmable component modifications that occur after release will be considered. This consideration will include consideration of all requirements stipulated by Authorities Having Jurisdiction.

The use of field performance data to demonstrate compliance with the software analysis and test, off-the-shelf software, and tool validation requirements of UL 1998 will be considered for a period determined for each product type.

1 Scope

1 effective November 30, 1998

1.1 These requirements apply to non-networked embedded microprocessor software whose failure is capable of resulting in a risk of fire, electric shock, or injury to persons.

1.2 This is a reference standard in which the requirements are to be applied when specifically referenced by other standards or product safety requirements.

1.3 These requirements address the risks unique to product hardware controlled by software in programmable components.

1.4 These requirements are intended to supplement applicable product or component standards and requirements, and are not intended to serve as the sole basis for investigating the risk of fire, electric shock, or injury to persons.

1.5 These requirements are intended to address risks that occur in the software or in the process used to develop and maintain the software, such as the following:

- a) Requirements conversion faults that cause differences between the specification for the programmable component and the software design;
- b) Design faults such as incorrect software algorithms or interfaces;
- c) Coding faults, including syntax, incorrect signs, endless loops, and other coding faults;
- d) Timing faults that cause program execution to occur prematurely or late;
- e) Microelectronic memory faults, such as memory failure, not enough memory, or memory overlap;
- f) Induced faults caused by microelectronic hardware failure;
- g) Latent, user, input/output, range, and other faults that are only detectable when a given state occurs; and
- h) Failure of the programmable component to perform any function at all.

1.6 Product standard requirements may amend or supersede the requirements in this standard, as appropriate.

2 Definitions of Terms Used

2 effective November 30, 1998

2.1 For the purpose of this standard, the following definitions apply.

2.2 APPLICATION-SPECIFIC INTEGRATED CIRCUIT (ASIC) – An electronic device comprised of many transistors and other semiconductor components which integrate standard cells and arrays from a library into one piece of silicon intended for a particular use.

2.3 BUILT-IN TEST – A design method that allows a product to test itself by adding logic for test signal generation and analysis of test results.

2.4 CENTRAL PROCESSING UNIT (CPU) – The unit of a computing and controlling system that includes the circuits controlling the interpretation of instructions and their execution.

2.5 CRITICAL SECTION – A segment of the software that is intended to perform the functions that address or control risks.

2.6 DATA – A representation of facts, concepts, or instructions in a manner suitable for storage, communication, interpretation, or processing.

2.7 DESIGN – The process of defining the software architecture, components, modules, interfaces, test approach, and data for a software system to satisfy specified requirements.

2.8 ELECTRONICALLY ERASABLE PROGRAMMABLE READ ONLY MEMORY (EEPROM) – A reprogrammable read-only memory in which cells may be erased electrically and in which each cell is capable of being reprogrammed electrically.

2.9 EMBEDDED SOFTWARE – Software that is physically part of a product and whose primary purpose is to maintain some property or relationship between other components of the product in order to achieve the overall system objective.

2.10 ERASABLE PROGRAMMABLE READ ONLY MEMORY (EPROM) – A type of programmable memory device which can only be read and not altered under normal use. The memory is capable of being erased by ultraviolet light and reprogrammed.

2.11 ERROR – A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

2.12 FAIL-OPERATIONAL PROCEDURE – A procedure executed in the event that a failure has occurred which continues product operation but provides degraded performance or reduced functional capabilities.

2.13 FAIL-SAFE PROCEDURE – A procedure executed to maintain the Risks Addressed (RA) state of a product while transitioning into a non-operational mode.

2.14 FAILURE – The inability of a product or component to perform its specified function.

2.15 FAILURE MODE – The physical or functional manifestation of a failure.

2.16 FAILURE MODE TEST – A suite of tests that have been specifically developed based upon the failure modes that exist in a programmable component or product.

2.17 FAULT – A deficiency in a product or component which is capable of, under some operational conditions, contributing to a failure.

2.18 FAULT-TOLERANT – The capability of software to provide continued correct execution in the presence of a defined set of microelectronic hardware and software faults.

2.19 FLASH MEMORY – A type of non-volatile memory which is capable of being erased electrically and reprogrammed, but only in blocks, as opposed to one byte increments.

2.20 HAZARD – A potential source of physical injury to persons.