ANSI/ISA–84.00.01–2004 Part 1
(IEC 61511-1 Mod)

Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Defintions, System, Hardware and Software Requirements

Approved 2 September 2004

ISA–The Instrumentation, Systems, and Automation Society

ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1: Mod)
Functional safety: Safety Instrumented Systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

ISBN: 1-55617-919-7

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709 USA

Preface

This preface, as well as all footnotes, is included for information purposes and is not part of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).

This document has been prepared as part of the service of ISA – the Instrumentation, Systems, and Automation Society – toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE STANDARD, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE STANDARD OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS STANDARD, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE STANDARD MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE STANDARD. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE STANDARD OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE STANDARD FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS STANDARD WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE STANDARD NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER. ADDITIONALLY, THE USE OF THIS STANDARD MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE STANDARD CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN – HAZARDOUS CONDITIONS. THE USER OF THIS STANDARD MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS STANDARD.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

The following people served as active members of ISA-SP84:

NAME	AFFILIATION
W. Johnson, Chair	E.I. DuPont
K. Bond, Managing Director	Consultant
R. Dunn, Recorder	DuPont Engineering
R. Adamski	Premier Consulting Services
B. Adler	AE Solutions
R. Bailliet	Syscon International Inc.
N. Battikha	BergoTech Inc.
L. Beckman	Safeplex Systems Inc.
J. Berge	SMAR Singapore Pte Ltd.
H. Bezecny	Dow Deutschland
D. Bolland	ExxonMobil Research & Engineering Co.
D. Brown	Emerson Process Management
S. Brown	E.I. DuPont
S. Brown	Health & Safety Executive
J. Campbell	ConocoPhillips
H. Cheddie	Bayer Inc.
W. Cohen	KBR
J. Cusimano	Siemens Energy & Automation, Inc.
K. Dejmek	Baker Engineering & Risk Consultants
A. Dowell	Rohm & Haas Co.
P. Early	Langdon Coffman Services
S. Gallagher	ConocoPhillips
L. Gamboa	Rockwell Automation Inc.
K. Gandhi	KBR
I. Gibson	Fluor Australia Pty Ltd
J. Gilman	JFG Technology Transfer LLC
W. Goble	Exida Com LLC
D. Green	Rohm & Haas Co.
R. Green	Green Associates
P. Gruhn	L&M Engineering
C. Hardin	CDH Consulting Inc.
J. Harris	UOP LLC
T. Hurst	Hurst Technologies Corp.
T. Jackson	Bechtel Corp.
J. Jamison	OPTI Canada Inc.
J. Jarvi	Automation Partners Oy
K. Klein	Solutia Inc.
R. Kotoski	Honeywell
L. Laskowski	Emerson Process Management
T. Layer	Emerson Process Management
V. Maggioli	Feltronics Corp.
E. Marszal	Kenexis
J. Martel	Invensys-Triconex
R. McCrea-Steele	Premier Consulting Services
N. McLeod	Atofina
M. Moderski	ABB Lummus Global Inc.
W. Mostia	WLM Engineering Company
R. Nelson	Celanese
D. Ogwude	Creative Systems International
L. Owen	Dooley Tackaberry, Inc.
R. Peterson	Lyondell Chemical Co.
G. Ramachandran	Systems Research International Inc.
G. Raney	Triconex Systems Inc.
G. Robertson	Oxy Information Technology
M. Scott	AE Solutions
R. Seitz	Artech Engineering
J. Siebert	Invista
B. Smith	Nova Chemicals

D. Sniezek	Lockheed Martin Federal Services
C. Sossman	WGI-W Safety Management Solutions
P. Stavrianidis	FM Approvals
R. Stevens	US Dept. of Energy
H. Storey	Shell Global Solutions
R. Strube	Intertek Testing Services NA, Inc.
A. Summers	SIS-Tech Solutions LLC
L. Suttinger	Westinghouse Savannah River Co.
W. Taggart	Waldemar S. Nelson & Co.
R. Taubert	BASF Corp.
H. Tausch	Honeywell Inc.
H. Thomas	Air Products & Chemicals Inc.
I. Verhappen	Syncrude Canada Ltd.
T. Walczak	GE Fanuc Automation
M. Weber	System Safety Inc.
L. Wells	Georgia-Pacific Corp.
J. Williamson	Bechtel Corp.
A. Woltman	Shell Global Solutions
P. Wright	BHP Engineering & Construction, Inc.
D. Zetterberg	ChevronTexaco Energy Technology Co.

This document was approved for publication by the ISA Standards and Practices Board on 2 August 2004.

NAME	AFFILIATION
V. Maggioli, Chair	Feltronics Corp.
K. Bond	Consultant
D. Bishop	David N. Bishop, Consultant
D. Bouchard	Paprican
M. Cohen	Consultant
M. Coppler	Ametek, Inc.
B. Dumortier	Schneider Electric
W. Holland	Consultant
E. Icayan	ACES, Inc.
A. Iverson	Ivy Optiks
R. Jones	Dow Chemical Co.
T. McAvinew	I&C Engineering, LLC
A. McCauley, Jr.	Chagrin Valley Controls, Inc.
G. McFarland	Emerson Process Management
D. Rapley	Rapley Consulting Inc.
R. Reimer	Rockwell Automation
J. Rennie	Factory Mutual Research Corp.
H. Sasajima	Yamatake Corp.
I. Verhappen	Syncrude Canada Ltd.
R. Webb	Consultant
W. Weidman	Parsons Energy & Chemicals Group
J. Weiss	KEMA Inc.
M. Widmeyer	Stanford Linear Accelerator Center
R. Wiegle	CANUS Corp.
C. Williams	Eastman Kodak Co.
M. Zielinski	Emerson Process Management

This page intentionally left blank.

CONTENTS

This page intentionally left blank.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

UNITED STATES NATIONAL FOREWORD

All text of IEC 61511-1 Ed. 1.0 (2003-03) is included. United States National Deviations are shown by ~~strikeout~~ through deleted text and underline under added text.

IEC FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control. The text of this standard is based on the following documents:

FDIS	Report on voting
65A/368/FDIS	65A/372/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) consists of the following parts, under the general title *Functional safety: Safety instrumented systems for the process industry sector* (see Figure 1):

- Part 1: Framework, definitions, system, hardware and software requirements
- Part 2: Guidelines in the application of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) .
- Part 3: Guidance for the determination of the required safety integrity levels

The committee has decided that the contents of this publication will remain unchanged until 2007. At that date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

A bilingual version of this standard may be issued at a later date.

INTRODUCTION

Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industries. If instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards and performance levels.

This international standard addresses the application of safety instrumented systems for the Process Industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This international standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This standard addresses safety instrumented systems which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This International Standard is process industry specific within the framework of IEC 61508 (see Annex A).

This International Standard sets out an approach for safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This International Standard on safety instrumented systems for the process industry

- addresses all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

This International Standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example, national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

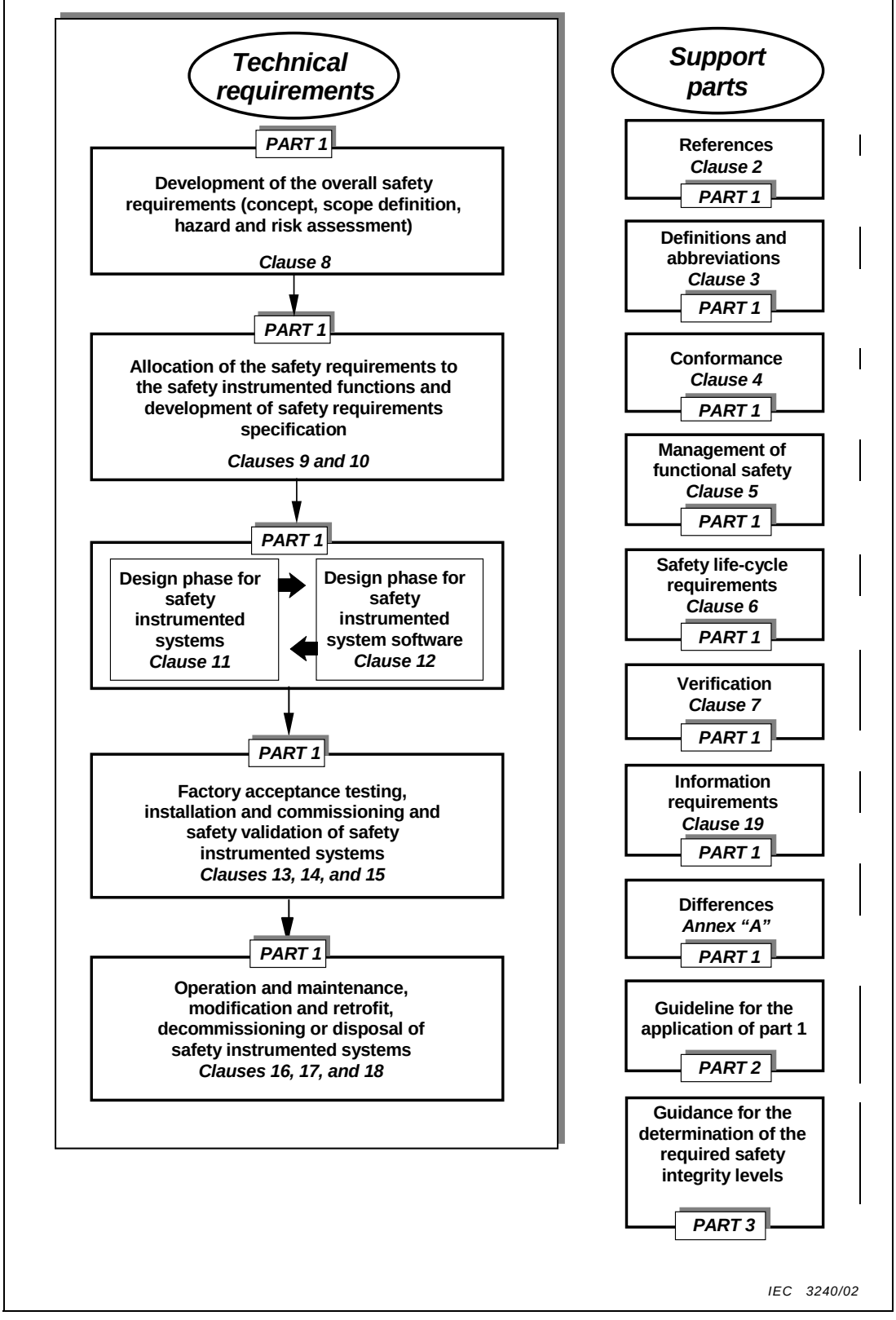

Figure 1 – Overall framework of this standard

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

1 Scope

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.

In particular, this standard

a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility will be assigned to different parties according to safety planning and national regulations;

b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);

c) defines the relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511Mod), and IEC 61508 (Figures 2 and 3);

d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);

e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;

NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.

f) outlines the relationship between safety instrumented functions and other functions (Figure 4);

g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;

h) specifies requirements for system architecture and hardware configuration, application software, and system integration;

i) specifies requirements for application software for users and integrators of safety instrumented systems (clause 12). In particular, requirements for the following are specified:

- safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;
- information relating to the software safety validation to be passed to the organization carrying out the SIS integration;