AMERICAN NATIONAL STANDARD

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

Approved 2 September 2004

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

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

Copyright © 2004 by ISA. All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher).

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

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

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.

Documents
Document Sharing Hub

Copyright 2004 ISA. All rights reserved.

Full document details: ANSI ISA 84.00.01-2004 Part 1

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

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

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

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

This page intentionally left blank.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

CONTENTS

UNITED STATES NATIONAL FOREWORD 11
IEC FOREWORD 11
INTRODUCTION 13
1 Scope 15
2 Normative references 20
3 Abbreviations and definitions 21
3.1 Abbreviations 21
3.2 Definitions 22
4 Conformance to this International Standard 36
5 Management of functional safety 36
5.1 Objective 36
5.2 Requirements 36
6 Safety life-cycle requirements 41
6.1 Objectives 41
6.2 Requirements 41
7 Verification 43
7.1 Objective 43
8 Process hazard and risk assessment 44
8.1 Objectives 44
8.2 Requirements 44
9 Allocation of safety functions to protection layers 45
9.1 Objectives 45
9.2 Requirements of the allocation process 45
9.3 Additional requirements for safety integrity level 4 46
9.4 Requirements on the basic process control system as a protection layer 47
9.5 Requirements for preventing common cause, common mode and dependent failures 48
10 SIS safety requirements specification 49
10.1 Objective 49
10.2 General requirements 49
10.3 SIS safety requirements 49
11 SIS design and engineering 50
11.1 Objective 50
11.2 General requirements 50
11.3 Requirements for system behaviour on detection of a fault 52
11.4 Requirements for hardware fault tolerance 53
11.5 Requirements for selection of components and subsystems 54
11.6 Field devices 57
11.7 Interfaces 58
11.8 Maintenance or testing design requirements 60
11.9 SIF probability of failure 60
12 Requirements for application software, including selection criteria for utility software 61
12.1 Application software safety life-cycle requirements 62
12.2 Application software safety requirements specification 68
12.3 Application software safety validation planning 70

Copyright 2004 ISA. All rights reserved.

AVA Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

12.4 Application software design and development 70
12.5 Integration of the application software with the SIS subsystem 75
12.6 FPL and LVL software modification procedures 76
12.7 Application software verification 76
13 Factory acceptance testing (FAT) 77
13.1 Objectives 77
13.2 Recommendations 78
14 SIS installation and commissioning 79
14.1 Objectives 79
14.2 Requirements 79
15 SIS safety validation 80
15.1 Objective 80
15.2 Requirements 80
16 SIS operation and maintenance 82
16.1 Objectives 82
16.2 Requirements 83
16.3 Proof testing and inspection 84
17 SIS modification 85
17.1 Objectives 85
17.2 Requirements 85
18 SIS decommissioning 86
18.1 Objectives 86
18.2 Requirements 86
19 Information and documentation requirements 87
19.1 Objectives 87
19.2 Requirements 87
Annex A (informative) Differences 89
A.1 Organizational differences 89
A.2 Terminology 89

Figure 1 – Overall framework of this standard 14
Figure 2 – Relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) and IEC 61508 17
Figure 3 – Relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) and IEC 61508 (see 1.2) 18
Figure 4 – Relationship between safety instrumented functions and other functions 19
Figure 5 – Relationship between system, hardware, and software of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) 20
Figure 6 – Programmable electronic system (PES): structure and terminology 29
Figure 7 – Example SIS architecture 32
Figure 8 – SIS safety life-cycle phases and functional safety assessment stages 39
Figure 9 – Typical risk reduction methods found in process plants 48
Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle 62

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

Figure 11 – Application software safety life cycle (in realization phase) 64
Figure 12 – Software development life cycle (the V-model) 65
Figure 13 – Relationship between the hardware and software architectures of SIS 68

Table 1 – Abbreviations used in ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) 21
Table 2 – SIS safety life-cycle overview 42
Table 3 – Safety integrity levels: probability of failure on demand 46
Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF 46
Table 5 – Minimum hardware fault tolerance of PE logic solvers 53
Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers 54
Table 7 – Application software safety life cycle: overview 66

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

This page intentionally left blank.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

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):

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub
Full document details: ANSI ISA 84.00.01-2004 Part 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.

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

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.

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

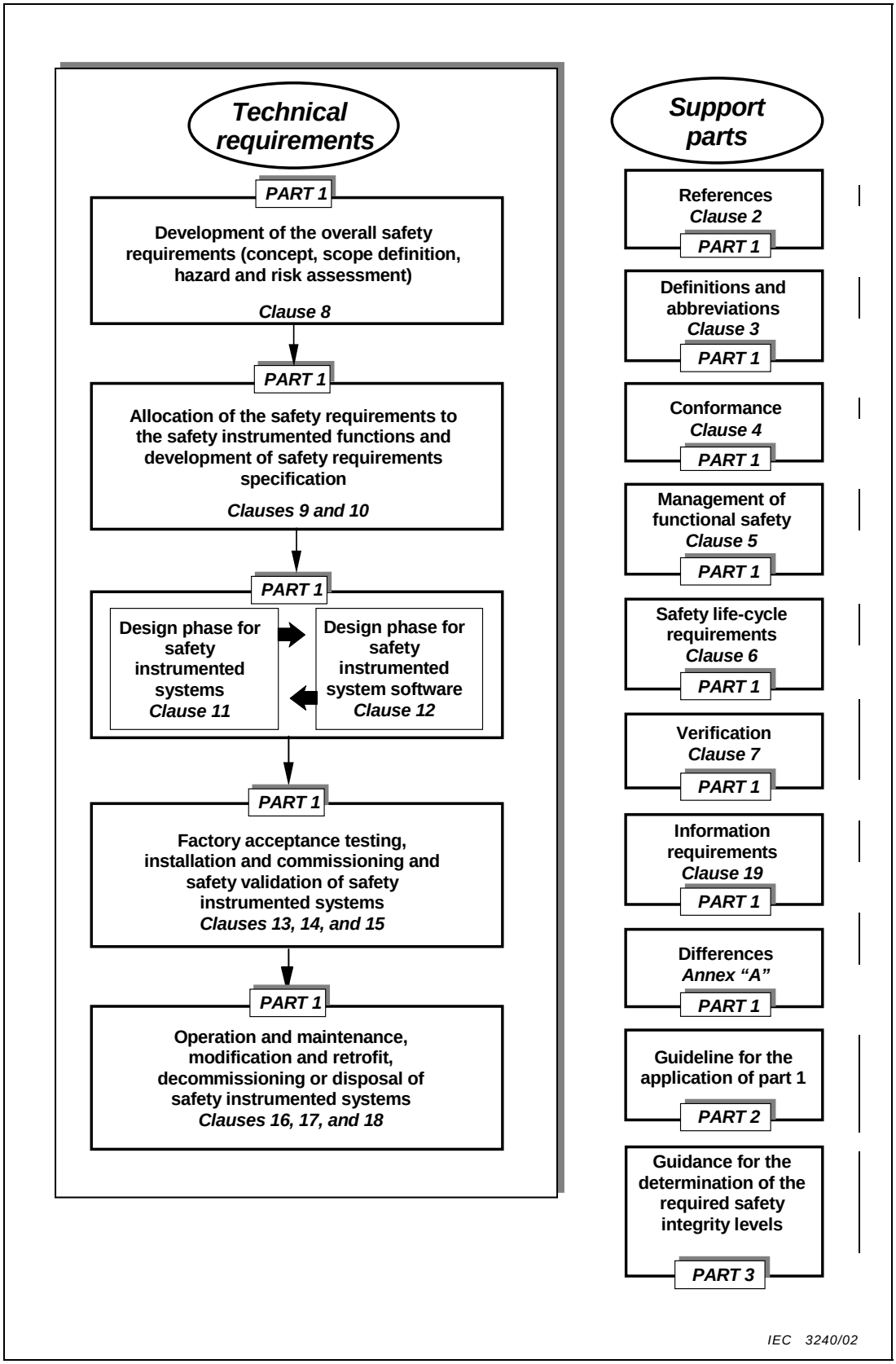


Figure 1 – Overall framework of this standard

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

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;

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

– preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;

– procedures and specifications to be met by the organization carrying out modifications to safety software;

j) applies when functional safety is achieved using one or more safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment;

k) may be applied in non-safety applications such as asset protection;

l) defines requirements for implementing safety instrumented functions as a part of the overall arrangements for achieving functional safety;

m) uses a safety life cycle (Figure 8) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems;

n) requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

NOTE See Figure 9 for an overview of risk reduction methods.

o) establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels;

p) specifies minimum requirements for hardware fault tolerance;

q) specifies techniques/measures required for achieving the specified integrity levels;

r) defines a maximum level of performance (SIL 4) which can be achieved for a safety instrumented function implemented according to this standard;

s) defines a minimum level of performance (SIL 1) below which this standard does not apply;

t) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications (which should be established based on knowledge of the particular application);

u) specifies requirements for all parts of the safety instrumented system from sensor to final element(s);

v) defines the information that is needed during the safety life cycle;

w) requires that the design of a safety instrumented function takes into account human factors;

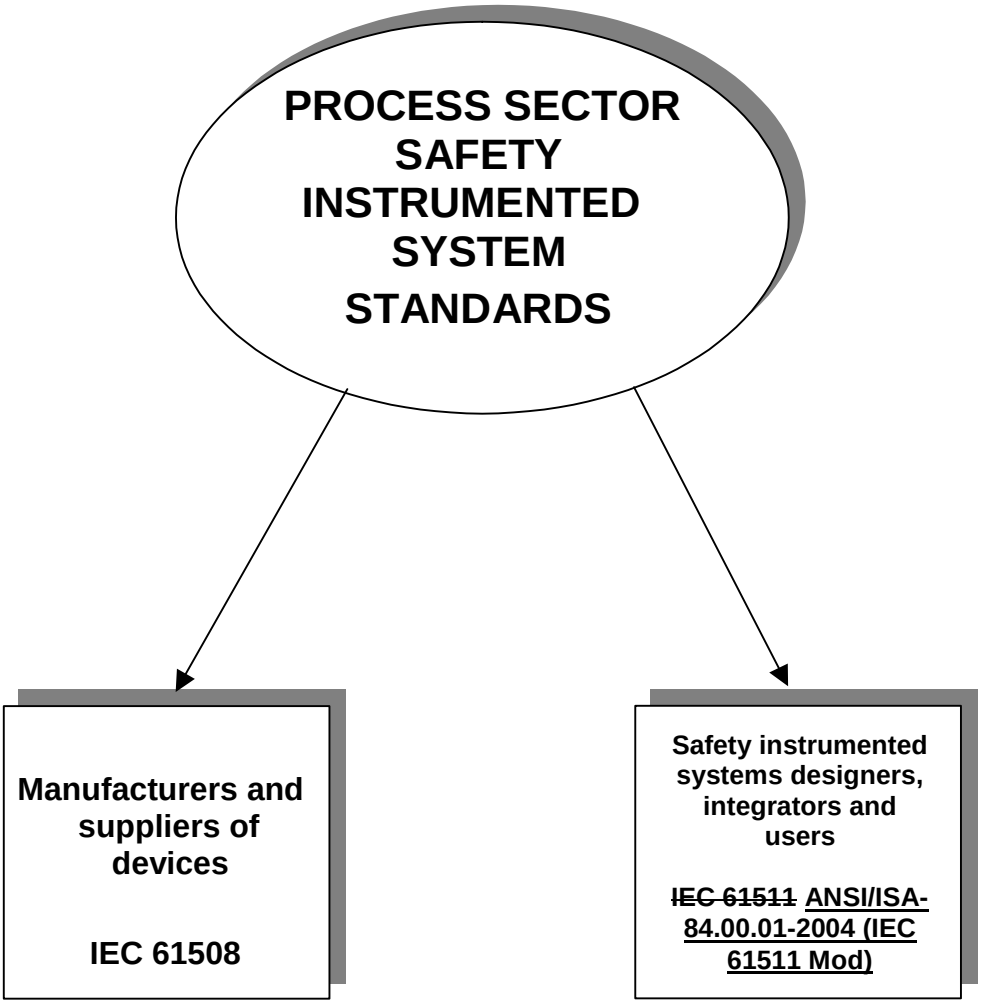
x) does not place any direct requirements on the individual operator or maintenance person.

y) For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1



IEC 3241/02

Figure 2 – Relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) and IEC 61508

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

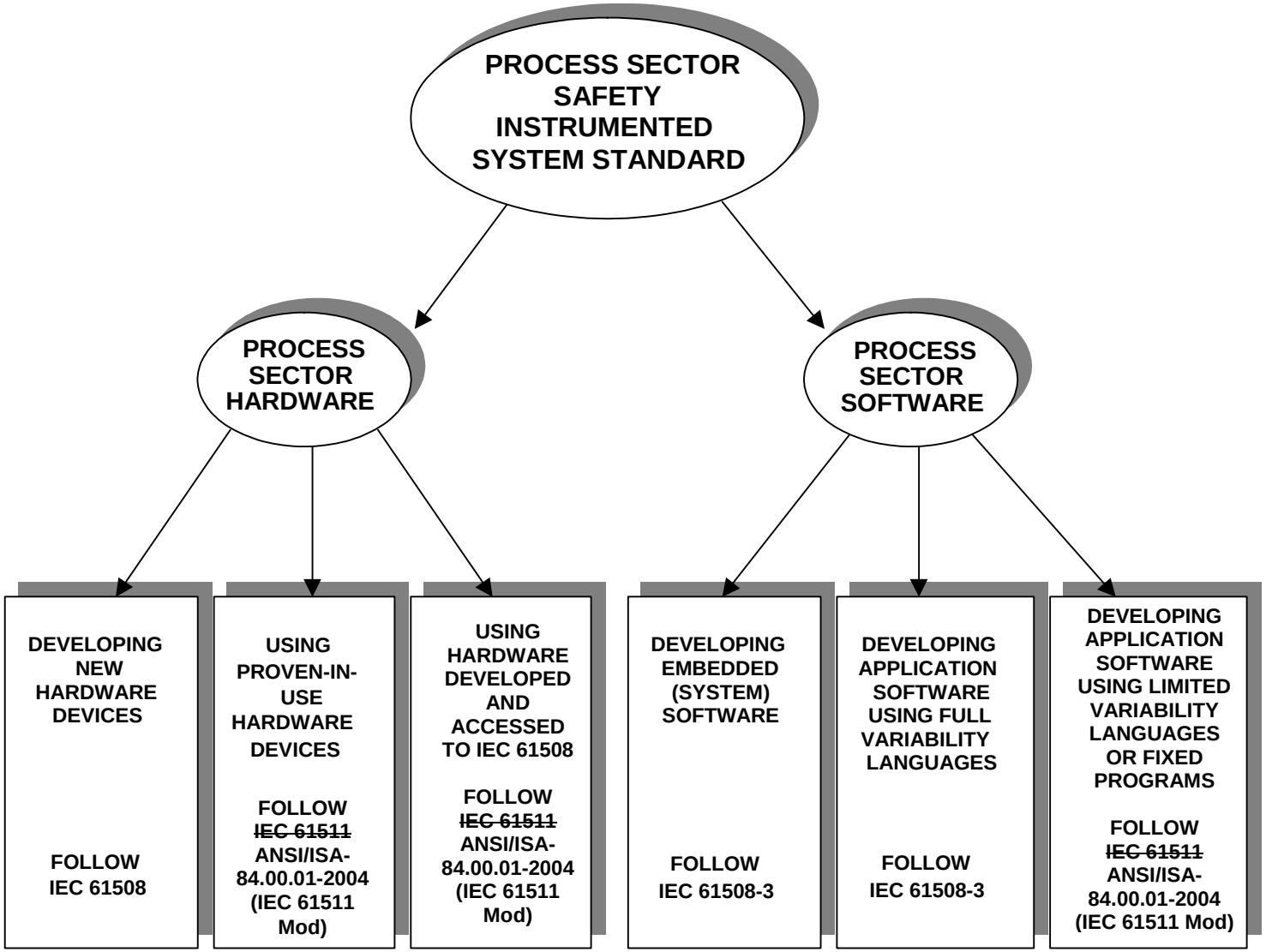


Figure 3 – Relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) and IEC 61508 (see clause 1)

Copyright 2004 ISA. All rights reserved.

Full document details: ANSI ISA 84.00.01-2004 Part 1

AVA Documents
Document Sharing Hub

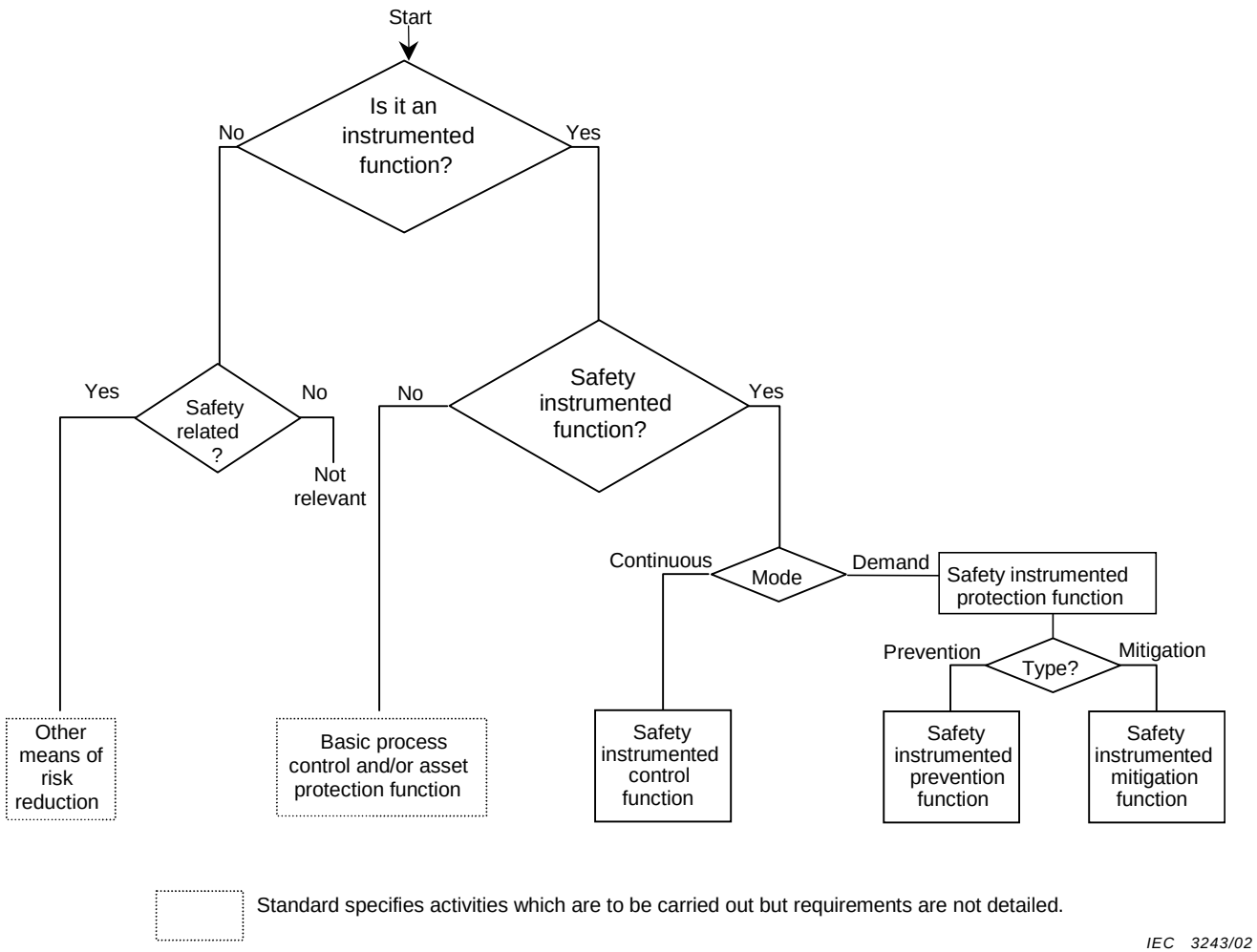
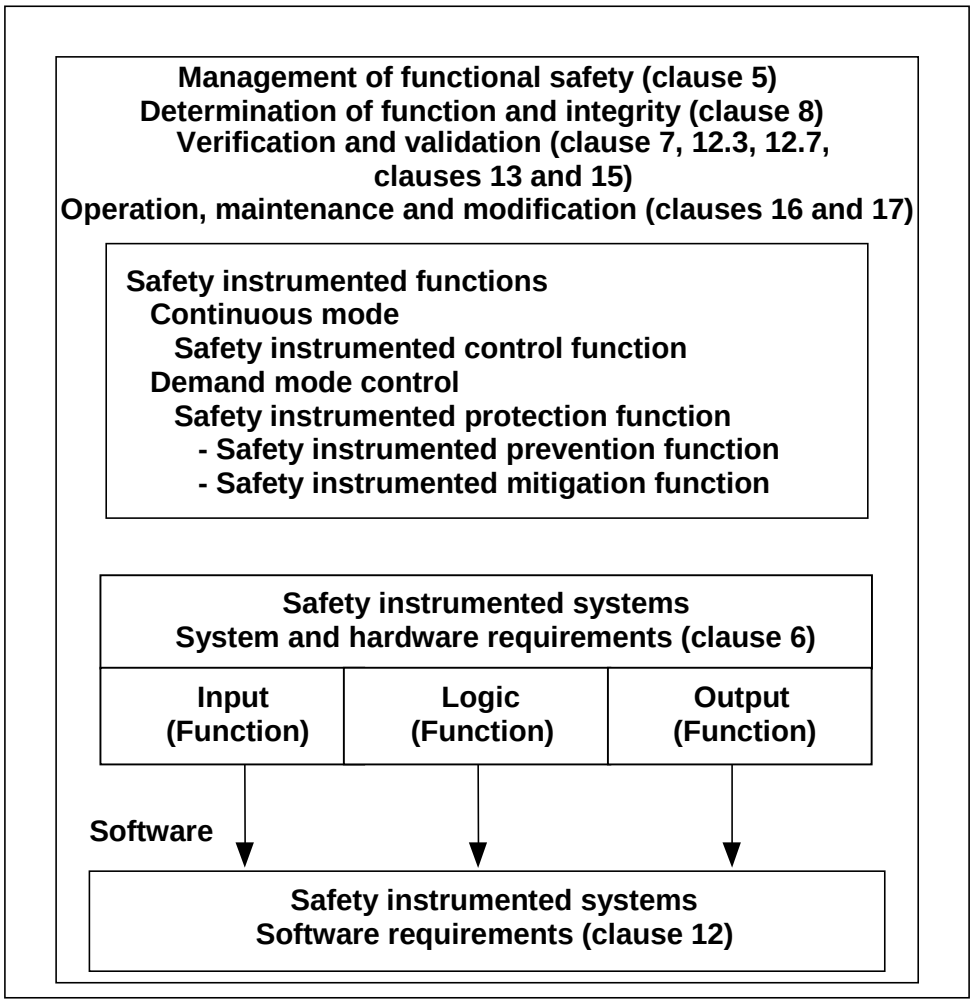


Figure 4 – Relationship between safety instrumented functions and other functions

Copyright 2004 ISA. All rights reserved.

Full document details: ANSI ISA 84.00.01-2004 Part 1

Documents
Document Sharing Hub



IEC 3244/02

Figure 5 – Relationship between system, hardware, and software of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)

2 Normative references

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

IEC 60654-1:1993, *Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions*

IEC 60654-3:1998, *Industrial-process measurement and control equipment – Operating conditions – Part 3: Mechanical influences*

IEC 61326-1:*Electrical equipment for measurement, control and laboratory use – EMC requirements*

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

~~IEC 61511-2~~: ANSI/ISA-84.00.01-2004 Part 2 (IEC 61511-2 Mod) *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines in the application of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).*

3 Abbreviations and definitions

3.1 Abbreviations

Abbreviations used throughout ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) are given in Table 1.

Table 1 – Abbreviations used in ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

Abbreviation	Full expression
AC/DC	Alternating current/direct current
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
BPCS	Basic process control system
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
E/E/PES	Electrical/electronic/programmable electronic system
EMC	Electro-magnetic compatibility
FAT	Factory acceptance testing
FPL	Fixed program language
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
HMI	Human machine interface
H&RA	Hazard and risk assessment
HRA	Human reliability analysis
H/W	Hardware
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISA	Instrumentation, Systems and Automation Society
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	“M” out of “N” (see 3.2.45)
NP	Non-programmable
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of failure on demand
PFD_{avg}	Average probability of failure on demand
PLC	Programmable logic controller
SAT	Site acceptance test
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification
S/W	Software

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2 Definitions

For the purposes of this document, the following definitions apply.

3.2.1
architecture
arrangement of hardware and/or software elements in a system, for example,

(1) arrangement of safety instrumented system (SIS) subsystems;

(2) internal structure of an SIS subsystem;

(3) arrangement of software programs

NOTE This term differs from the definition in IEC 61508-4 to reflect differences in the process sector terminology.

3.2.2
asset protection
function allocated to system design for the purpose of preventing loss to assets

3.2.3
basic process control system (BPCS)
system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1

NOTE See Clause A.2.

3.2.4
channel
element or group of elements that independently perform(s) a function

NOTE 1 The elements within a channel could include input/output (I/O) modules, logic systems (see 3.2.40), sensors, final elements.

NOTE 2 A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function.

NOTE 3 The term can be used to describe a complete system or a portion of a system (for example, sensors or final elements).

3.2.5
coding
see “programming”

3.2.6

3.2.6.1
common cause failure
failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure

3.2.6.2
common mode failure
failure of two or more channels in the same way, causing the same erroneous result

3.2.7
component
one of the parts of a system, subsystem, or device performing a specific function

3.2.8
configuration
see “architecture”

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.9
configuration management
discipline of identifying the components of an evolving (hardware and software) system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life cycle

3.2.10
control system
system which responds to input signals from the process and/or from an operator and generates output signals causing the process to operate in the desired manner

NOTE The control system includes input devices and final elements and may be either a BPCS or an SIS or a combination of the two.

3.2.11
dangerous failure
failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state

NOTE Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall hazardous or fail-to-function state.

3.2.12
dependent failure
failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it

NOTE 1 Two events A and B are dependent, where P(z) is the probability of event z, only if P(A and B) > P(A) × P(B).

NOTE 2 See 9.5 as an example of dependent failure consideration between layers of protection.

NOTE 3 Dependent failure includes common cause (see 3.2.6).

3.2.13
detected
revealed
overt
in relation to hardware failures and software faults, detected by the diagnostic tests or through normal operation

3.2.14
device
functional unit of hardware or software, or both, capable of accomplishing a specified purpose (for example, field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes field wiring, sensors, final elements, logic solvers, and those operator interface devices hard-wired to SIS I/O terminals)

3.2.15
diagnostic coverage (DC)
ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests.

NOTE 1 The diagnostic coverage is used to compute the detected ($\lambda_{detected}$) and undetected failure rates ($\lambda_{undected}$) from the total failure rate ($\lambda_{total\ failure\ rate}$) as follows: $\lambda_{detected}$ = DC × $\lambda_{total\ failure\ rate}$ and $\lambda_{undected}$ = (1-DC) × $\lambda_{total\ failure\ rate}$.

NOTE 2 Diagnostic coverage is applied to components or subsystems of a safety instrumented system. For example, the diagnostic coverage is typically determined for a sensor, final element or a logic solver.

NOTE 3 For safety applications the diagnostic coverage is typically applied to the safe and dangerous failures of a component or subsystem. For example, the diagnostic coverage for the dangerous failures of a component or subsystem is DC = $\lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate.

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.16
diversity
existence of different means performing a required function

NOTE Diversity may be achieved by different physical methods or different design approaches.

3.2.17
electrical/electronic/programmable (E/E/PE)
based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

NOTE The term is intended to cover any and all devices or systems operating on electrical principles and would include

- electro-mechanical devices (electrical);
- solid-state non-programmable electronic devices (electronic);
- electronic devices based on computer technology (programmable electronic) (see 3.2.55).

3.2.18
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE Adapted from IEV 191-05-24 by excluding the notes.

3.2.19
external risk reduction facilities
measures to reduce or mitigate the risks, which are separate and distinct from the SIS

NOTE 1 Examples include a drain system, fire wall, bund (dike).

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector terminology.

3.2.20
failure
termination of the ability of a functional unit to perform a required function

NOTE 1 This definition (excluding these notes) matches ISO/IEC 2382-14-01-09:1997.

NOTE 2 For further information, see IEC 61508-4.

NOTE 3 Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

NOTE 4 Failures are either random or systematic (see 3.2.62 and 3.2.85).

3.2.21
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. [ISO/IEC 2382-14-01-09]

3.2.22
fault avoidance
use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety life cycle of the safety instrumented system

3.2.23
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

NOTE The definition in IEV 191-15-05 refers only to sub-item faults. See the note for the term fault in 3.2.21.

[ISO/IEC 2382-14-04-06]

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.24
final element
part of a safety instrumented system which implements the physical action necessary to achieve a safe state

NOTE Examples are valves, switch gear, motors including their auxiliary elements, for example, a solenoid valve and actuator if involved in the safety instrumented function.

3.2.25
functional safety
part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.26
functional safety assessment
investigation, based on evidence, to judge the functional safety achieved by one or more protection layers

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.27
functional safety audit
systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

NOTE A functional safety audit may be carried out as part of a functional safety assessment.

3.2.28
functional unit
entity of hardware or software, or both, capable of accomplishing a specified purpose

NOTE 1 In IEV 191-01-01 the more general term “item” is used in place of functional unit. An item may sometimes include people.

NOTE 2 This is the definition given in ISO/IEC 2382-14-01-01.

3.2.29
hardware safety integrity
part of the safety integrity of the safety instrumented function relating to random hardware failures in a dangerous mode of failure

NOTE 1 The term relates to failures in a dangerous mode. That is, those failures of a safety instrumented function that would impair its safety integrity. The two parameters that are relevant in this context are the overall dangerous failure rate and the probability of failure to operate on demand.

NOTE 2 See 3.2.86.

NOTE 3 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.30
harm
physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment

NOTE This definition matches ISO/IEC Guide 51.

3.2.31
hazard
potential source of harm

NOTE 1 This definition (without notes) matches 3.4 of ISO/IEC Guide 51.

NOTE 2 The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

Documents
Document Sharing Hub
Copyright 2004 ISA. All rights reserved.
Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.32
human error
mistake
human action or inaction that produces an unintended result

NOTE This is the definition found in ISO/IEC 2382-14-02-03 and differs from that given in IEV 191-05-25 by the addition of "or inaction".

3.2.33
impact analysis
activity of determining the effect that a change to a function or component will have to other functions or components in that system as well as to other systems

3.2.34
independent department
department which is separate and distinct from the departments responsible for the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation

3.2.35
independent organization
organization which is separate and distinct, by management and other resources, from the organizations responsible for the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation

3.2.36
independent person
person who is separate and distinct from the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation and does not have direct responsibility for those activities

3.2.37
input function
function which monitors the process and its associated equipment in order to provide input information for the logic solver

NOTE An input function could be a manual function.

3.2.38
instrument
apparatus used in performing an action (typically found in instrumented systems)

NOTE Instrumented systems in the process sector are typically composed of sensors (for example, pressure, flow, temperature transmitters), logic solvers or control systems (for example, programmable controllers, distributed control systems), and final elements (for example, control valves). In special cases, instrumented systems can be safety instrumented systems (see 3.2.72).

3.2.39
logic function
function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions); logic functions provide the transformation from one or more input functions to one or more output functions

NOTE For further guidance, see IEC 61131-3 and IEC 60617-12.

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.40
logic solver
that portion of either a BPCS or SIS that performs one or more logic function(s)

NOTE 1 In ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) the following terms for logic systems are used:

- electrical logic systems for electro-mechanical technology;
- electronic logic systems for electronic technology;
- PE logic system for programmable electronic systems.

NOTE 2 Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, hydraulic systems. Sensors and final elements are not part of the logic solver.

3.2.40.1
safety configured logic solver
general purpose industrial grade PE logic solver which is specifically configured for use in safety applications in accordance with 11.5

3.2.41
maintenance/engineering interface
maintenance/engineering interface is that hardware and software provided to allow proper SIS maintenance or modification. It can include instructions and diagnostics which may be found in software, programming terminals with appropriate communication protocols, diagnostic tools, indicators, bypass devices, test devices, and calibration devices

3.2.42
mitigation
action that reduces the consequence(s) of a hazardous event

NOTE Examples include emergency depressurization on detection of confirmed fire or gas leak.

3.2.43
mode of operation
way in which a safety instrumented function operates

3.2.43.1
demand mode safety instrumented function
where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS

3.2.43.2
continuous mode safety instrumented function
where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it

NOTE 1 Continuous mode covers those safety instrumented functions which implement continuous control to maintain functional safety.

NOTE 2 In demand mode applications where the demand rate is more frequent than once per year, the hazard rate will not be higher than the dangerous failure rate of the safety instrumented function. In such a case, it will normally be appropriate to use the continuous mode criteria.

NOTE 3 The target failure measures for safety instrumented functions operating in demand mode and continuous mode are defined in Tables 3 and 4.

NOTE 4 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.44
module
self-contained assembly of hardware components that performs a specific hardware function (i.e., digital input module, analogue output module), or reusable application program (can be internal to a program or a set of programs) that support a specific function, for example, portion of a computer program that carries out a specific function

NOTE 1 In the context of IEC 61131-3, a software module is a function or function block.

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.2.45
MooN
safety instrumented system, or part thereof, made up of "**N**" independent channels, which are so connected, that "**M**" channels are sufficient to perform the safety instrumented function

3.2.46
necessary risk reduction
risk reduction required to ensure that the risk is reduced to a tolerable level

3.2.47
non-programmable (NP) system
system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

NOTE Examples would include hard-wired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

3.2.48
operator interface
means by which information is communicated between a human operator(s) and the SIS (for example, CRTs, indicating lights, push-buttons, horns, alarms); the operator interface is sometimes referred to as the human-machine interface (HMI)

3.2.49
other technology safety related systems
safety related systems that are based on a technology other than electrical, electronic, or programmable electronic

NOTE A relief valve is "another technology safety related system". "Other technology safety related systems" may include hydraulic and pneumatic systems.

3.2.50
output function
function which controls the process and its associated equipment according to final actuator information from the logic function

3.2.51
phase
period within the safety life cycle where activities described in this standard take place

3.2.52
prevention
action that reduces the frequency of occurrence of a hazardous event

3.2.53
prior use
see "proven-in-use" (see 3.2.60)

Copyright 2004 ISA. All rights reserved.

Documents
Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1

3.2.54
process risk
risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

NOTE 1 The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety).

NOTE 2 Process risk analysis is described in ~~IEC 61511-3~~ ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod). The main purpose of determining the process risk is to establish a reference point for the risk without taking into account the protection layers.

NOTE 3 Assessment of this risk should include associated human factor issues.

NOTE 4 This term equates to "EUC risk" in IEC 61508-4.

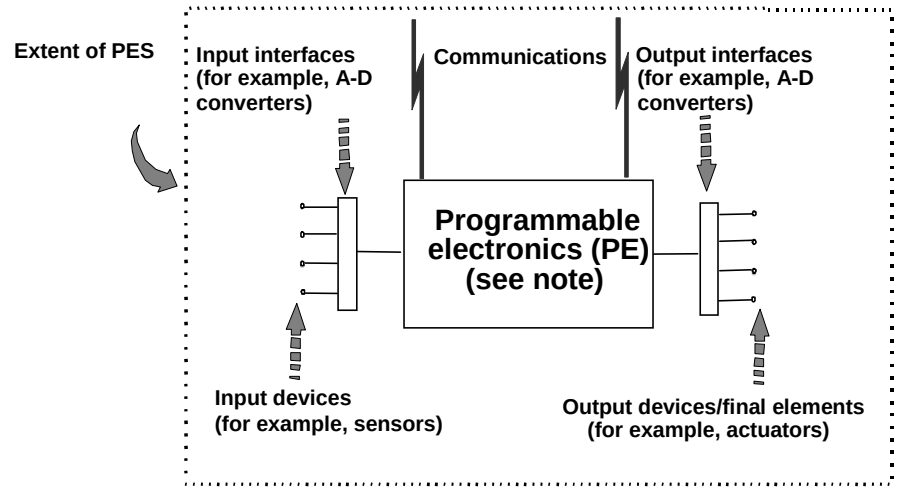
3.2.55
programmable electronics (PE)
electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units

NOTE 1 This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector programmable electronics include

- smart sensors and final elements;
- programmable electronic logic solvers including
  - programmable controllers;
  - programmable logic controllers.
  - loop controllers.

NOTE 2 This term differs from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.56
programmable electronic system (PES)
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices (see Figure 6).



Basic PES structure

NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.

IEC 3245/02

Figure 6 – Programmable electronic system (PES): structure and terminology

Copyright 2004 ISA. All rights reserved.

AVA Documents Document Sharing Hub

Full document details: ANSI ISA 84.00.01-2004 Part 1