TECHNICAL REPORT
ISA-TR84.00.04-2011, Part 1

Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

Approved 14 October 2011

ISA-TR84.00.04-2011

Part 1 - Guideline for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)

ISBN: 978-1-937560-24-9

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

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.04.

This document has been prepared as part of the service of the International Society of Automation (ISA) 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.

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 DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NON-DISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NON-DISCRIMINATORY.

ISA REQUESTS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT 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 DOCUMENT.

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 served as members of ISA84 in developing this technical report:

NAME	COMPANY
W. Johnson, Chair	DuPont Sustainable Solutions
V. Maggioli, Co-Managing Director	Feltronics Corp
D. Zetterberg, Co-Managing Director	Chevron Energy Technology Company
A. Summers, TR Working Group Leader	SIS-TECH Solutions LP
R. Adamski	RA Safety Consulting LLC
T. Ando	Yokogawa Electric Co
R. Avali	Westinghouse Electric Corp
L. Beckman	Safeplex Systems Inc
J. Campbell	ConocoPhillips
I. Chen	Aramco
R. Chittilapilly	Oil & Natural Gas Corp
M. Coppler	Ametek Inc
M. Corbo	ExxonMobil
P. Early	Langdon Coffman Services
C. Fialkowski	Siemens Inc
K. Gandhi	KBR
I. Gibson	Consultant
J. Gilman	JFG Technology Transfer LLC
W. Goble	Exida
P. Gruhn	ICS Triplex
B. Hampshire	BP
J. Harris	UOP A Honeywell Company
J. Jamison	EnCana Corporation Ltd
R. Johnson	Dow Process Automation
K. Klein	Celanese Corp
T. Layer	Emerson Process Management
E. Marszal	Kenexis Consulting Corp
N. McLeod	ARKEMA
M. Mollicone	SYM Consultoria
G. Ramachandran	Systems Research Intl Inc
R. Roberts	Suncor Energy Inc
M. Scott	AE Solutions
D. Sniezek	Lockheed Martin Federal Services
C. Sossman	CLS Tech-Reg Consultants
R. Strube	Strube Industries
L. Suttinger	Savannah River Nuclear Solutions
T. Walczak	Conversions Inc
M. Weber	System Safety Inc
A. Woltman	Shell Global Solutions
P. Wright	BHP Engineering & Construction Inc

This technical report was approved for revision by the ISA Standards and Practices Board on 14 October 2011.

NAME	COMPANY
D. Dunn, Vice President	Aramco Services Co.
E. Cosman, Vice President-Elect	The Dow Chemical Co.
D. Bartusiak	ExxonMobil Research & Engineering
P. Brett	Honeywell Inc.
J. Campbell	ConocoPhillips
M. Coppler	Ametek Inc.
B. Dumortier	Schneider Electric
J. Federlein	Federlein & Assoc. Inc.
J. Gilsinn	NIST/MEL
E. Icayan	ACES Inc.
J. Jamison	EnCana Corporation Ltd.
K. Lindner	Endress+Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
T. McAvinew	Jacobs Engineering
R. Reimer	Rockwell Automation
S. Russell	Valero Energy Corp.
N. Sands	DuPont
H. Sasajima	Yamatake Corp.
T. Schnaare	Rosemount Inc.
J. Tatera	Tatera & Associates Inc.
I. Verhappen	Industrial Automation Networks Inc.
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa IA Global Marketing (USMK)
D. Zetterberg	Chevron Energy Technology Company

This page intentionally left blank.

Foreword

ANSI/ISA-84.00.01-2004 gives requirements for the specification, design, installation, operation and maintenance of SIS, so that it can be confidently entrusted to place and/or maintain the process in a safe state. These requirements are presented in the standard, using the safety lifecycle shown in ANSI/ISA-84.00.01-2004-1, Figure 8, and described in ANSI/ISA-84.00.01-2004-1 Table 2.

The ISA84 committee has developed a series of complimentary technical reports to provide guidance, as well as practical examples of implementation, on various topics and applications. Three of these technical reports, ISA-TR84.00.02, ISA-TR84.00.03 and ISA-TR84.00.04, provide informative guidance related to specific phases of the Safety Instrumented System (SIS) lifecycle. Figure 8 and Table 2 have been adapted for this foreword as shown in ISA-TR84.00.04 Figure 1 and Table 1, respectively. A brief overview of each technical report is given below, including the report's relationship to the lifecycle requirements and the intended scope of each report's guidance.

ISA-TR84.00.02—Safety Integrity Level (SIL) Verification of Safety Instrumented Functions— Lifecycle phase 4 requires verification that the intended or installed SIS meets its specified SIL. To support the calculation of the average probability of failure on demand as required by ANSI/ISA-84.00.01 Clause 11.9, ISA-TR84.00.02 provides guidance on the following: a) assessing random and systematic failures, failure modes and failure rates; b) understanding the impact of diagnostics and mechanical integrity (MI) activities on the SIL and reliability; c) identifying sources of common cause, common mode and systematic failures; and d) using quantitative methodologies to verify the SIL and spurious trip rate. The approaches outlined in this document are performance-based; consequently, the reader is cautioned to understand that the examples provided do not represent prescriptive architectural configurations or MI requirements for any given SIL. Once an SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured MI program as described in ISA-TR84.00.03

ISA-TR84.00.03—Mechanical Integrity of Safety Instrumented Systems (SIS)—Lifecycle phases 5 and 6 involve the installation and testing of the SIS, the validation that the SIS meets the safety requirements specification, and the assurance that functional safety is maintained during long-term operation and maintenance. An important aspect of achieving and maintaining the SIS integrity and its specified SIL is the implementation of an MI program that provides quality assurance of the installed SIS performance. This technical report is an informative document providing guidance on establishing an effective MI program that demonstrates, through traceable and auditable documentation, that the SIS and its equipment are maintained in the "as good as new" condition. The technical report addresses the identification of personnel roles and responsibilities when establishing an MI plan, important considerations in establishing an effective MI program, and detailed examples to illustrate user work processes used to support various activities of the MI program. Data and information collected as part of the MI program can be used to validate the SIL Verification calculations, as discussed in ISA-TR84.00.02 and the selection, and continued use of devices, as discussed in ISA-TR84.00.04 Annex L.

ISA-TR84.00.04-Guidelines for the Implementation of ANSI/ISA-84.00.01—Lifecycle phases 2, 4, 9 and 10 address the management of functional safety, allocation of safety functions to protection layers, SIS design and engineering, and SIS verification. This technical report is divided into two parts. Part 1 provides an overview of the SIS lifecycle with references to annexes containing more detailed guidance on various subjects. Part 2 provides an end-user example of how to implement ANSI/ISA-84.00.01. This report covers many aspects of the safety lifecycle, including such topics as: "grandfathering" existing SIS (Clause 3 and Annex A); operator initiated functions (Annex B), separation of the Basic Process Control System (BPCS) and SIS (Annex F), field device and logic solver selection (Annex L), manual shutdown considerations (Annex P), and design/installation considerations (e.g., wiring, power, relationship to BPCS, common mode impacts, fault tolerance, etc. – Annex N). ISA-TR84.00.02 expands Annex G, which only provides a brief introduction to the topic of failure calculations. ISA-TR84.00.04 does not address the MI program, which is discussed in ISA-TR84.00.03.

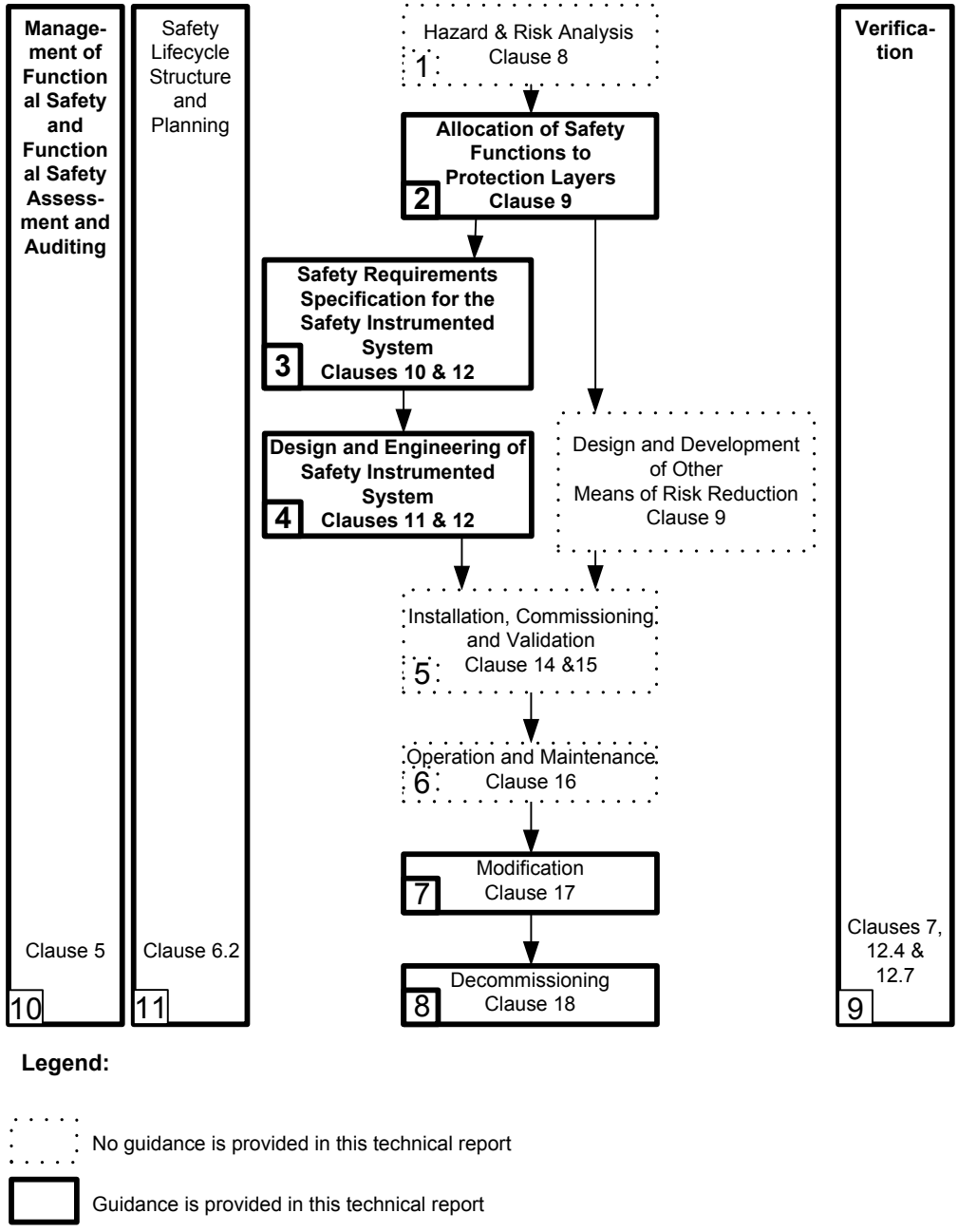

Figure 1 – SIS Safety Lifecycle (modified ANSI/ISA-84.00.01-1 Figure 8)

Table 1 - SIS safety life-cycle overview (modified ANSI/ISA-84.00.01-1 Table 2)

Safety lifecycle phase or activity		Objectives	ANSI/ISA-84.00.01 Requirements Clause	ISA-84 Technical Report Reference
Figure 1 box number	Title			
1	Hazard and risk analysis	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction, and the safety functions required to achieve the necessary risk reduction.	8	None
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level.	9	ISA-TR84.00.04 Annexes B, F, and J
3	SIS safety requirements specification (SRS)	To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety.	10	No specific guidance on documenting the SRS. An example is shown in ISA-TR84.00.04 Part 2. All three technical reports (ISA-TR84.00.02, 03, and 04) provide fundamental considerations for SRS development.
4	SIS design & engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity.	11 & 12.4	ISA-TR84.00.04 Annexes F, G, I, K, L, M, N, O, P, and Q ISA-TR84.00.02
5	SIS installation commissioning & validation	To integrate and test the SIS. To validate that the SIS meets, in all respects, the requirements for safety in terms of the required Safety Instrumented Functions and the required safety integrity.	12.3, 14, 15	ISA-TR84.00.03
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance.	16	ISA-TR84.00.03

(Continued on next page)

(Table 1 continued from previous page)

Safety lifecycle phase or activity		Objectives	ANSI/ISA-84.00.01 Requirements Clause	ISA-84 Technical Report Reference
Figure 1 box number	Title			
7	SIS modification	To make corrections, enhancements, or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained.	17	Apply appropriate safety lifecycle phase during management-of-change activity.
8	Decommissioning	To ensure proper review, sector organization, and ensure Safety Instrumented Function (SIF) remain appropriate.	18	Apply appropriate safety lifecycle phase during project execution
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.	7, 12.7	ISA-TR84.00.04 Annex C, ISA-TR84.00.03, and ISA-TR84.00.02
10	SIS functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the SIS.	5	ISA-TR84.00.04, Clause 3, and Annexes A, C, D, E, and S

CONTENTS

This page intentionally left blank.

1 Purpose

ANSI/ISA-84.01-1996 has been retired and replaced with ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod). The new standard is the ANSI/ISA adoption of the international standard, IEC 61511, and includes one additional clause, a grandfather clause covering existing SIS (ANSI/ISA-84.00.01-2004 Part 1 Clause 1.0 y).

This technical report is divided into two parts.

- Part 1 provides guidance on a wide range of topics related to the standard.
- Part 2 provides a single user example to illustrate some of the lifecycle steps in ANSI/ISA-84.00.01-2004.

ISA-TR84.00.04 Part 1 (ISA-TR84.00.04-1) contains four main clauses.

- Clause 1 is the purpose.
- Clause 2 explains the origins of the new standard and discusses its relationship to other regulations, standards, and practices.
- Clause 3 and Annex A specifically address the grandfather clause and provide guidance on the evaluation of existing SIS.
- Clause 4 provides an overview of the SIS lifecycle and references to subject-specific annexes for additional guidance on key issues.

There is nothing in this guideline that precludes, replaces, or makes obsolete any requirement of ANSI/ISA-84.01-1996 or ANSI/ISA-84.00.01-2004-1. This guideline is a "how to" approach and provides informative, non-mandatory methods.

2 Introduction

In the United States of America, the Occupational Safety and Health Administration (US-OSHA) regulation, 29CFR1910.119 (OSHA 1910.119), requires the identification and management of the instrumented systems responsible for safe operation. ISA Standards Panel 84 (ISA84) developed ANSI/ISA-84.01-1996 to define how to manage Safety Instrumented Systems (SIS) using a lifecycle approach. The standard provided a formal, documented process for addressing the design, operation, maintenance, testing and management of change for SIS. The efforts of the ISA84 committee resulted in US-OSHA recognizing ANSI/ISA-84.01-1996 as representing good engineering practices for SIS.

During its initial development, the ISA84 committee relied on existing US functional safety practices, such as those documented in OSHA 1910.119 and by the Center for Chemical Process Safety (CCPS) *Guidelines for the Safe Automation of Chemical Processes.* Working in parallel to the ISA84 committee effort, the International Electrotechnical Commission (IEC) was developing IEC 61508. Concepts introduced in the draft international standard were incorporated into ANSI/ISA-84.01-1996, resulting in ANSI/ISA-84.01-1996 being accepted as the US functional safety standard for the process sector. Through ANSI/ISA-84.01-1996, owners/operators have become familiar with terms, such as safety integrity levels, safety instrumented systems, and safety functions (i.e., safety instrumented function).

Since 1996, some countries have utilized ANSI/ISA-84.01-1996, while others have used their own national standard or adopted IEC 61508 when it was released in 1999. In an era where design, engineering, and operation can occur in multiple countries, this diversity of standards resulted in an immediate need for an international, consensus process-sector standard.