

ISA-TR84.00.09-2013

**Security Countermeasures Related to
Safety Instrumented Systems (SIS)**

Approved 6 November 2013

ISA-TR84.00.09-2013

Security Countermeasures Related to Safety Instrumented Systems (SIS)

ISBN: 978-0-876640-52-4

Copyright © 2013 by ISA. All rights reserved. Not for resale. Printed in the United States of America.

ISA

67 Alexander Drive

P. O. Box 12277

Research Triangle Park, NC 27709 USA

PREFACE

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.09-2013.

This document has been prepared as part of the service of ISA, the International Society of Automation, 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, NONDISCRIMINATORY 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 PROCESS EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS TECHNICAL REPORT SHOULD EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER SHOULD ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

The following members of ISA84 Working Group 9 served as active contributors in the development of this technical report:

NAME	AFFILIATION
Harold W Thomas, Working Group Chair	exida
Marc Baque	Total
Keith Bellville	Emerson
Michael Corbo	ExxonMobil
John Cusimano	exida
Ed Crawford	Chevron
James Gilsinn	Kenexis
William Hearn	SIS-Tech
Kevin Klein	Chevron
Joel Langill	Scadahacker
Vic Maggioli	Feltronics

This technical report was approved for publication by the ISA Standards and Practices Board on 6 November 2013.

NAME	AFFILIATION
E. Cosman, Vice President	The Dow Chemical Company
D. Bartusiak	ExxonMobil Chemical Company
P. Brett	Honeywell Inc.
J. Campbell	Consultant
M. Coppler	Det Norske Veritas Certification Inc.
B. Dumortier	Schneider Electric
D. Dunn	Aramco Services Co.
J. Federlein	Federlein & Assoc. Inc.
J. Gilsinn	Kenexis Consulting
E. Icahan	Atkins
J. Jamison	Spectra Energy Ltd.
K. P. Lindner	Endress + Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
T. McAviney	Instrumentation and Control Engineering, LLC
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
R. Reimer	Rockwell Automation
S. Russell	Valero Energy Corp.
N. Sands	DuPont
H. Sasajima	Azbil Corp.
T. Schnaare	Rosemount Inc.
J. Tatera	Tatera & Associates Inc.
I. Verhappen	Industrial Automation Networks Inc.
W. Weidman	WCW Consulting
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa IA Global Marketing (USMK)
D. Zetterberg	Chevron Energy Technology Company

CONTENTS

PREFACE	3
CONTENTS	5
0 Introduction	9
1 Scope	11
2 References	11
3 Terms, definitions, abbreviated terms, acronyms, and conventions	11
3.1 Terms and definitions	11
3.2 Abbreviated terms and acronyms	11
4 Management of functional safety (Clause 5)	12
5 Hazard and risk analysis (Clause 8)	13
6 Allocation of safety functions to protection layers (Clause 9)	14
7 Safety requirements specification (SRS) for the safety instrumented system (Clauses 10 and 12)	15
8 Design and engineering of safety instrumented system (Clauses 11 and 12)	15
8.1 Independence and segregation	15
8.2 Access	16
8.3 Security concept	17
9 Design and development of other means of risk reduction (Clause 9)	17
10 Installation, commissioning and validation (Clauses 14 and 15)	18
10.1 Overview	18
10.2 Documentation	18
11 Operation and maintenance (Clause 16)	19
11.1 Security events	19
Any events associated with the SIS security countermeasures should be logged and continuously monitored.	19
11.2 Normal maintenance	19
11.3 Mechanical integrity	19
11.4 Inspection/Audit	19
11.5 Remote access	20
11.6 Bypasses	21
11.7 Tools	21
12 Modification (Clause 17)	21
13 Decommissioning (Clause 18)	22
Annex A (Informative) Example SIS interfaces to the enterprise network	25
A.1 Overview	25
A.2 Air-gapped	25
A.3 Interfaced	28
A.4 Integrated 2 zone	30
A.5 Integrated 1 zone	32
BIBLIOGRAPHY	34

Figure 1 – Graphical representation of the Safety Life Cycle 9

Figure A.1 – Example Network Security Architecture with Air-Gapped SIS..... 27

Figure A.2 – Example Network Security Architecture with Interfaced SIS 29

Figure A.3 – Example Network Security Architecture with Integrated 2 Zone SIS 31

Figure A.4 – Example Network Security Architecture with Integrated 1 Zone SIS..... 33

FOREWORD

This technical report is part of a series of standards and technical reports that address the issue of safety instrumented system security. It has been developed by Working Group 9 of the ISA84 committee in cooperation with the ISA99 committee.

This technical report describes performance criteria to guard against internal and external security threats to the safety instrumented system and provides guidance on how to comply with IEC 61511 and ANSI/ISA-84.00.01-2004 with respect to cybersecurity. This is the first issue of this technical report. Members of the ISA84 and ISA99 committees contributed to this effort.

Readers of this technical report are asked to send comments on the content and suggestions for coverage in future revisions to the following email address:

standards@isa.org

This page intentionally left blank.

0 Introduction

The underlying premise of this technical report is that the means to implement, operate, and maintain system security should not compromise the performance of the safety instrumented systems (SIS). To this end, SIS installations should be designed and maintained using the foundational requirements found in IEC 61511 and ANSI/ISA-84.00.01-2004, and in the ISA/IEC 62443 series. This document assumes that the applicable requirements and recommendations specified in the ISA/IEC 62443 series of standards have been implemented by the user.

The work process to ensure security of the SIS should account for its entire life cycle, including design, manufacture, factory acceptance testing (FAT), site acceptance testing (SAT), commissioning, operation, and maintenance, and for its ongoing mechanical integrity program. As part of the safety life cycle (SLC) for the SIS (see Figure 1), security should be addressed at appropriate phases or stages.

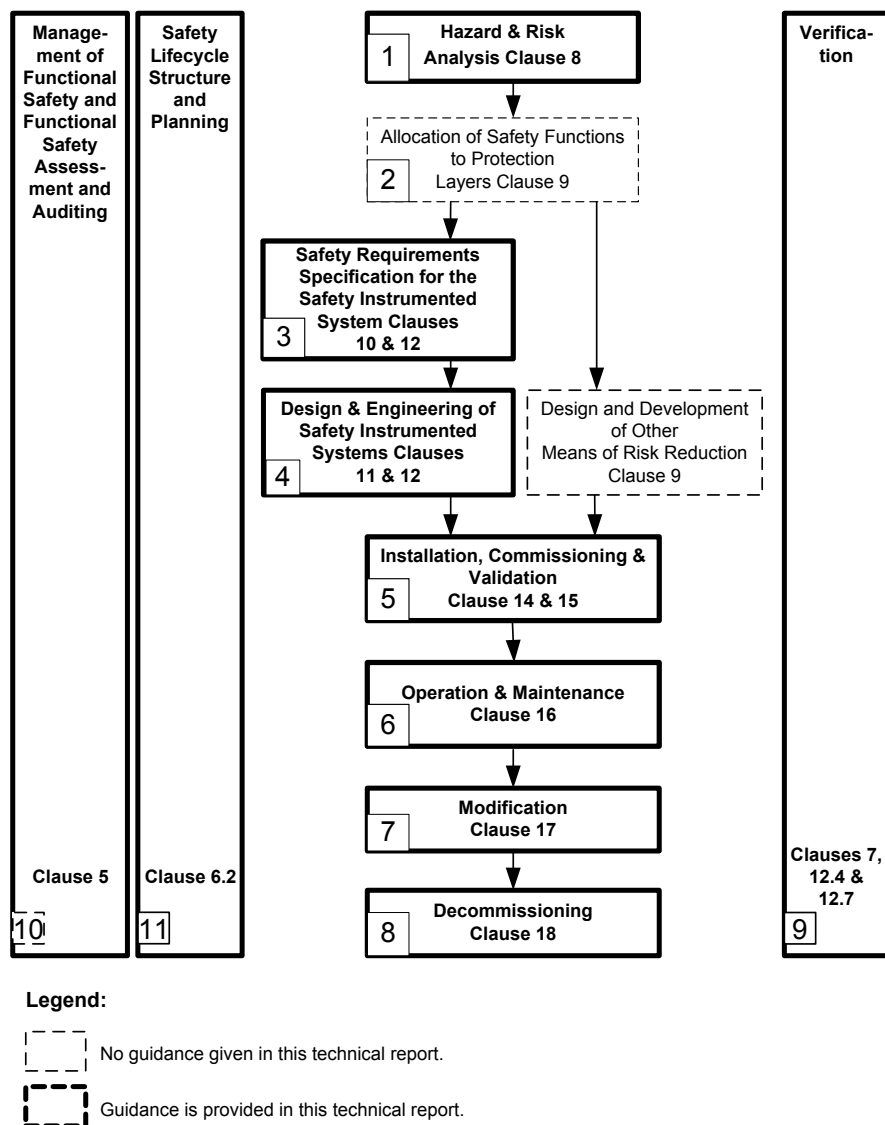


Figure 1 – Graphical representation of the Safety Life Cycle

NOTE: The clause numbers within the elements of Figure 1 above refer to clauses in ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).

1 Scope

The scope of this document is to address and provide guidance on the countermeasures used to reduce the likelihood of a security breach of the SIS that degrades its ability to perform its function(s). This relates to cybersecurity from both inside and outside the plant boundary.

The scope does not address physical plant protection (for example, fences, cameras, and grounding), but does address physical issues related to cybersecurity of the SIS (section 8.2 of this technical report).

2 References

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

In addition, readers should be aware of the ongoing development of additional standards in the ISA/IEC 62443 series, *Security for Industrial Automation and Control Systems*, beyond those listed below. For an update on the status of these standards, visit www.isa99.org.

- 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*
- IEC 61511-1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels*
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program*
- ANSI/ISA-62443-1-1 (99.01.01)-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61511, ANSI/ISA-84.00.01-2004, and ANSI/ISA-62443-1-1 apply (see references above).

3.2 Abbreviated terms and acronyms

The abbreviated terms and acronyms used in this document are defined as follows:

ANSI	American National Standards Institute
BPCS	Basic Process Control System
EMC	Electromagnetic Compatibility
FAT	Factory Acceptance Testing
H&RA	Hazard and Risk Assessment
HMI	Human Machine Interface