Foreword

ANSI/ISA-61511-2018 Part 1 gives requirements for specification, design, installation, operation, maintenance, modification and decommissioning, so that the safety instrumented system (SIS) 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-61511-2018 Part 1 Figure 7 and described in ANSI/ISA-61511-2018 Part 1 Table 2.

The ISA84 committee has developed a series of complementary 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 SIS lifecycle. Figure 7 and Table 2 have been adapted for this foreword as shown in ISA-TR84.00.04 Figure 1.1 and Table 1.1, 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-61511 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 automation asset integrity (AAI) 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 AAI requirements for any given SIL. Once a SIS is designed and installed, the ability to maintain the specified SIL requires the implementation of a structured AAI program as described in ISA-TR84.00.03.

ISA-TR84.00.03- Automation Asset 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 AAI program that provides quality assurance of the installed SIS performance. This technical report is an informative document providing guidance on establishing an effective AAI program that demonstrates through traceable and auditable documentation that the SIS and its equipment are maintained in compliance with the safety requirements specification. The technical report addresses the identification of personnel roles and responsibilities when establishing a plan, important considerations in establishing an effective AAI program, and detailed examples to illustrate user work processes used to support various activities of the AAI program. Data and information collected as part of the AAI 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-61511—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-61511. This report covers many aspects of the safety lifecycle including such topics as: "grandfathering" existing SISs (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 AAI program, which is discussed in ISA-TR84.00.03.

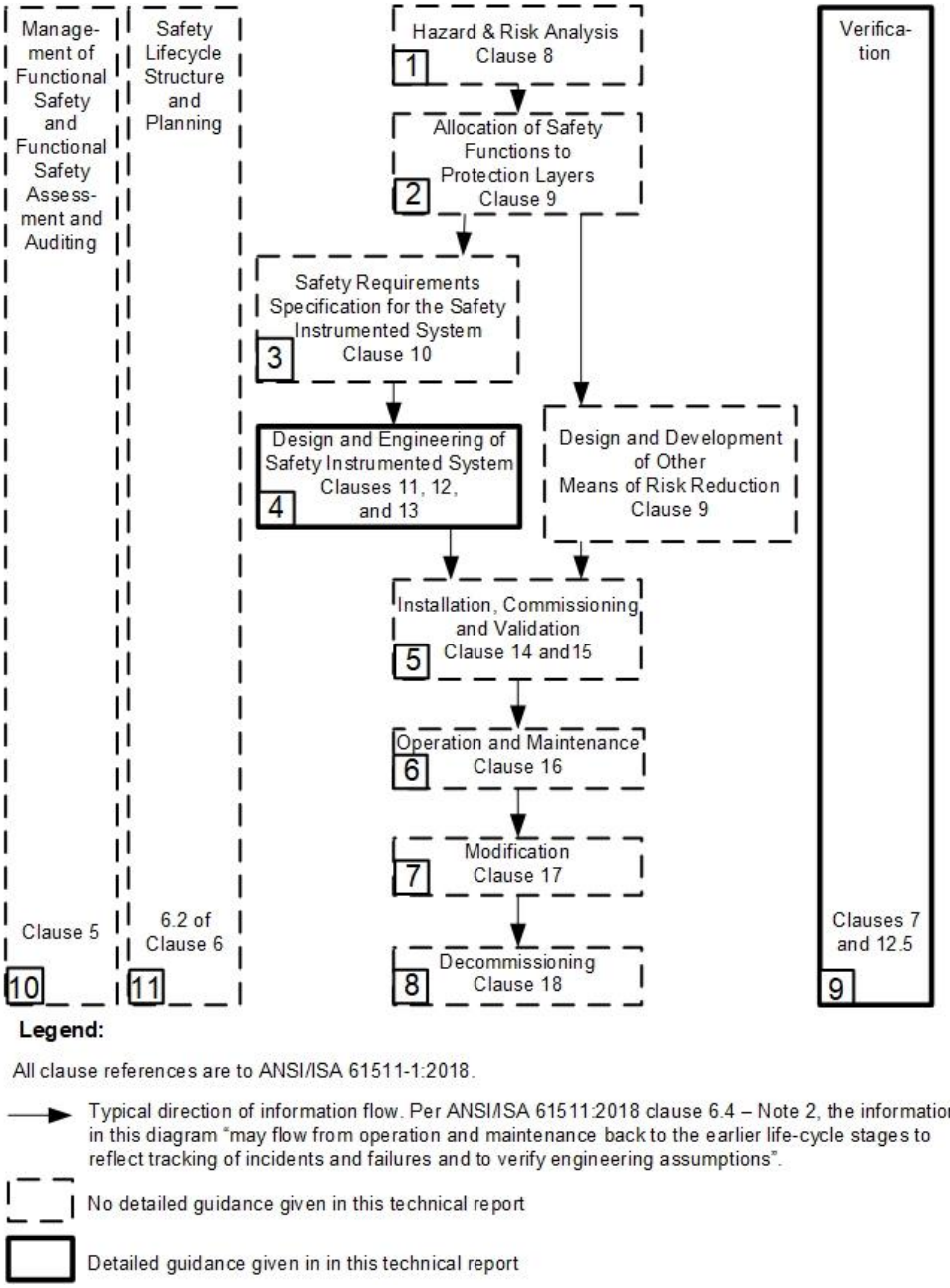

Figure 1.1 – SIS safety lifecycle phases (modified ANSI/ISA-61511-2018 Figure 7)

Table 1.1 – SIS safety life-cycle overview (modified ANSI/ISA-61511-2018 Table 2)

Safety life-cycle phase or activity		Objectives	ANSI/ISA-61511-2018 Requirements Clause	ISA84 Technical Report Reference
Figure 7 box number	Title			
1	H&RA	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 SIF, the associated SIL	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 SIF 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 and engineering	To design the SIS to meet the requirements for SIF and their associated safety integrity	11, 12	ISA-TR84.00.04 Annexes F, G, I, K, L, M, N, O, P, and Q ISA-TR84.00.02
5	SIS installation commissioning and 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 SIF and their associated safety integrity	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

(Table 1.1 cont'd from previous page)

Safety life-cycle phase or activity		Objectives	ANSI/ISA-61511-2018 Requirements Clause	ISA84 Technical Report Reference
Figure 7 box number	Title			
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL 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 SIF remains 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, 12.5	ISA-TR84.00.04 Annex C, ISA-TR84.00.03, and ISA-TR84.00.02
10	SIS FSA	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
11	Safety lifecycle structure and planning	To establish how the lifecycle steps are accomplished	6.2	ISA-TR84.00.04 Annex C

New clauses or clauses that have been extensively edited for this 2022 version are highlighted in yellow in the table of contents. The major changes are as follows:

1. Added generic equations for fault tree analysis and Markov analysis for PFD and PFH.
2. Added generic equations for spurious trip rate.
3. New annex of examples comparing fault tree analysis and Markov analysis.
4. New annex of examples on how to model motor controls and variable speed drives.
5. New annex of examples on modeling multiple instrumented safeguards used for the same hazardous event, including SIF and BPCS IPL (i.e., shared control valve), multiple SIF, and stacking multiple functions for a risk reduction >10000.
6. New annex of examples on modeling complex measurements, such as temperature compensated flow.
7. New annex with an example on combining instrumented safeguards with mechanical safeguards to obtain an overall risk reduction for a hazardous event.
8. New annex on calculating the risk reduction of a SIS alarm. This material was relocated from ISA TR84.00.04 Annex B and updated.
9. New example on partial test coverage using ISA-TR96.05.01 information.
10. New clause on selecting PFH versus PFD calculations based on mode of operation and automation asset integrity strategy.
11. References to IEC 61511, ANSI/ISA-84.00.01, and the many permutations of either, are changed to ANSI/ISA-61511-2018 .
12. MI changed to AAI per update to ISA-TR84.00.03.
13. Definitions have been reduced to only those words that are not defined by ANSI/ISA-61511-2018.

1 Scope

ISA-TR84.00.02-2022 is informative and does not contain any mandatory clauses. ISA-TR84.00.02-2022 is intended for use by those with a thorough understanding of ANSI/ISA-61511-1:2018. The user is referred to ANSI/ISA-61511-3:2017 and to the Center for Chemical Process Safety books, *Guidelines for Hazard Evaluation Procedures* and *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis,* for guidance on assigning the SIL.

Prior to proceeding with use of ISA-TR84.00.02-2022, the hazards and risk analysis and the allocation of safety functions to protection layers should be completed and the following information provided:

- The functional requirements of the safety instrumented function (SIF)
- The integrity requirements of the SIF
- The spurious trip rate constraints on the SIF

ISA-TR84.00.02-2022 provides guidance on the following:

- Assessing random and systematic failures, classifying failure modes, and estimating the failure rates for individual devices of a SIF;
- Assessing the impact of diagnostic and automation asset integrity (AAI) choices on the performance of the SIF and its devices;
- Assessing and estimating the potential for common cause and common mode failures; and
- Verifying that the SIF achieves a specified safety integrity level (SIL) and spurious trip rate.

ISA-TR84.00.02-2022 provides guidance on techniques for evaluating the following:

- Average probability of failure on demand (PFD) and probability of failure per hour (PFH)
- Spurious trip rate

2 Introduction

ANSI/ISA-61511-1:2018 describes a safety lifecycle model (Figure 1.1) for the implementation of safety instrumented systems (SIS) for the process industry. The standard defines four levels of safety integrity (Safety Integrity Levels, SIL) that may be used to benchmark the capability that a safety instrumented function (SIF) within the SIS to operate under all stated conditions within the time required.

ISA-TR84.00.02-2022 provides methodologies, formulas, and examples for verifying that each SIF achieves its specified SIL. The approaches outlined in this document are performance-based. Consequently, examples provided in this document do not represent prescriptive architectural configurations or automation asset integrity requirements for any given SIL.

THE METHODOLOGIES ARE DEMONSTRATED THROUGH EXAMPLES (SIS ARCHITECTURES) THAT REPRESENT POSSIBLE SYSTEM CONFIGURATIONS AND SHOULD NOT BE INTERPRETED AS RECOMMENDATIONS FOR SIS.

THE READER/USER IS THEREFORE CAUTIONED TO CLEARLY UNDERSTAND THE ASSUMPTIONS ASSOCIATED WITH THE METHODOLOGIES AND EXAMPLES IN THIS DOCUMENT BEFORE DERIVING ANY CONCLUSIONS REGARDING THE PERFORMANCE VERIFICATION OF ANY SPECIFIC SIF.