

Safety Instrumented Systems

A Life-Cycle Approach

Paul Gruhn PE, CFSE

Simon Lucchini, CFSE, MIEAust, CPEng



Safety Instrumented Systems: A Life-Cycle Approach

Safety Instrumented Systems: A Life-Cycle Approach

**By Paul Gruhn, PE, CFSE
Simon Lucchini, CFSE, MIEAust, CPEng**



Notice

The information presented in this publication is for the general education of the reader. Because neither the author nor the publisher has any control over the use of the information by the reader, both the author and the publisher disclaim any and all liability of any kind arising out of such use. The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.

Additionally, neither the author nor the publisher has investigated or considered the effect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.

Any references to commercial products in the work are cited as examples only. Neither the author nor the publisher endorses any referenced commercial product. Any trademarks or tradenames referenced belong to the respective owner of the mark or name. Neither the author nor the publisher makes any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on the use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Copyright © 2019 International Society of Automation (ISA)
All rights reserved.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2

ISBN: 978-1-945541-54-4

No part of this work 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 T. W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

Library of Congress Cataloging-in-Publication Data in process

Acknowledgments

No book is written in a vacuum, and few authors can claim to have developed all their material on their own. I have specialized in safety instrumented systems for almost 30 years, and it has been a never-ending learning cycle, one that will never be completed. I am indebted to my various employers and supervisors who supported my activities within the International Society of Automation (ISA), which ranged from the ISA84 standards committee and writing and presentation opportunities to the development of classes and books. I am grateful to all those I have learned from: authors of dozens of excellent textbooks, ISA84 standards committee members, co-presenters at conferences, co-authors, alternate instructors to my courses, as well as my students who have shared their stories. Thank you all.

Paul Gruhn, PE, CFSE

I would like to acknowledge the following Fluor colleagues with whom I have discussed many safety topics over the years and thank them for providing invaluable feedback: Andre Fijan, Michael Riley, Kristine Huff, Morgan Rodwell, and Stephen Johnson. I would like to especially thank Umesh Gyawali, another Fluor colleague, for creating many graphics for the book from my rough hand sketches.

Simon Lucchini, CFSE, MIEAust, CPEng

Contents

About the Authorsxvii
Chapter 1 Introduction	1
What Is a Safety Instrumented System?	2
Who This Book Is For	5
Why This Book Was Written	5
Confusion in the Industry	7
Technology Choices	7
Redundancy Choices	8
Field Devices	8
Common Cause and Systematic Errors	8
Test Intervals	8
Proof Test Methods	9
Reliability Data, Useful Life, and Maintenance	9
Conflicting Vendor Stories	9
Certification versus Prior Use	10
Software and Configuration Failures	10
Operational Requirements	10
Project Execution	11
Overreliance on Instrumentation	11
Industry Guidelines, Standards, and Regulations	11
AIChE CCPS	12
IEC 61508	12
ISA-84 and IEC 61511	12
U.S. OSHA 29 CFR 1910.119 Process Safety Management of Highly Hazardous Chemicals	13
Standards Are Changing Their Direction	15

- Things Are Not as Obvious as They May Seem..... 16
- The Danger of Complacency..... 17
- There’s Always More to Learn..... 18
- Summary 19
- References 19

- Chapter 2 Design Life Cycle.....21**
 - Hindsight/Foresight 22
 - Findings of the HSE 23
 - Design Life Cycle 29
 - Management 30
 - Verification 30
 - Hazard and Risk Analysis..... 31
 - Allocation of Safety Functions to Protective Layers 32
 - Develop the Safety Requirements Specification (SRS) 32
 - SIS Design and Engineering 33
 - Installation and Commissioning 34
 - Validation..... 34
 - Operations and Maintenance 35
 - Modifications..... 35
 - Decommissioning..... 36
 - Summary 36
 - References 36

- Chapter 3 Project Management37**
 - Everyone Has a Functional Safety Plan, Right?..... 38
 - Safety Life-Cycle and Real-World Project Complications 38
 - Aligning the Safety Plan with the Project Execution..... 40
 - What Is a Project and Project Management? 41
 - Key Elements of the Safety Plan..... 45
 - The Schedule Details 46
 - Who Is Involved in the Safety Plan? 48
 - We Have a Safety Plan and a RACI Matrix, Now What?..... 49
 - Summary 55
 - References 55

- Chapter 4 Process Control versus Safety Control.....57**
 - Control and Safety Defined 58
 - Process Control – Active/Dynamic 59
 - The Need for (and Ease of) Making Frequent Changes 60
 - Safety Control – Passive/Dormant 60
 - The Need for Restricting Changes 61
 - Low Demand, High Demand, and Continuous Mode 62
 - Separation of Control and Safety Systems 62
 - Integrated Control and Safety..... 63

Similar or Diverse Hardware/Software?	64
Security Concerns	65
Separation According to ISA-84	65
Common Cause and Systematic/Functional Failures	67
Human Issues	68
Summary	68
References	69
Chapter 5 Protection Layers	71
Prevention Layers	76
Process Plant Design	76
Process Control System	77
Alarm Systems	77
Human Reliability	78
Safety Instrumented Systems	79
Physical Protection	79
Mitigation Layers	80
Containment Systems	80
Scrubbers and Flares	80
Fire and Gas Systems	80
Evacuation Procedures	81
Diversification	82
Summary	83
References	84
Chapter 6 Safety Requirements Specification	85
The Need to Specify versus the Desire to Design and Build	86
Specifications, Requirements, and Incidents	87
Developing the SRS	89
Description of Functional Safety and the Required Integrity	91
Structure and Contents	94
Difficulties with Specifying and Documenting Requirements ...	102
Summary	108
References	108
Chapter 7 Selecting Safety Integrity Levels (SIL)	111
Introduction	112
Who's Responsible?	113
Which Technique?	113
Common Issues	114
Evaluating Risk	115
Hazard	115
Risk	115
Fatality Rates	116
Risks Inherent in Modern Society	117

Voluntary versus Involuntary Risk	118
Tolerable Risk	119
Tolerable Risk in the Process Industries	120
Safety Integrity Levels	122
SIL Determination Method #1: Safety Layer Matrix	124
Evaluating the Frequency	124
Evaluating the Severity	125
Evaluating the Overall Risk	125
Evaluating the Effectiveness of Additional Layers	126
Method #2: Risk Graph	128
Method #3: Layer of Protection Analysis (LOPA)	130
Tolerable Risk	131
Initiating Event Frequencies	132
Independent Protection Layers and Their Performance	132
Example Using LOPA	134
Summary	138
References	138
Chapter 8 Choosing a Technology	141
Pneumatic Systems	142
Relay Systems	142
Solid-State Systems	144
Microprocessor/PLC (Software-Based) Systems	145
Flexibility: Cure or Curse?	146
Software Issues	146
General-Purpose PLCs	148
Safety PLCs	151
Communications with Other Systems	157
Certified versus Prior Use	158
Summary	159
References	160
Chapter 9 Initial System Evaluation	161
Things Are Not as Obvious as They May Seem	162
Why Systems Should Be Analyzed Before They're Built	162
Caveats	163
Where to Get Failure Rate Information	164
Maintenance Records	164
Vendor Records	165
Third-Party Databases	165
Military Style Calculations	166
Failure Modes	167
Safe and Dangerous Failures	167
Detected/Undetected Failures	168
Metrics	168

Failure Rate, MTBF, and Life 171

Degree of Modeling Accuracy 173

Modeling Methods 174

 Reliability Block Diagrams 174

 Fault Trees 174

 Markov Models 175

The Real Impact of Redundancy 176

Basic Formulas 179

Analysis of a Relay System 182

Analysis of a Nonredundant General-Purpose PLC 183

Analysis of Other Logic Systems 185

System Analysis Including Field Devices 186

 Modeling Fault Tolerant Field Devices 187

 Achieving SIL 2 Without Fault Tolerance 190

Imperfect Manual Testing 192

The Impact of Bypassing 194

Systematic Failures 194

Fault Tolerance Requirements 195

 Safe Failure Fraction 196

Sample SIS Design Cookbook 197

Engineering Tools Available for Analyzing System Performance 199

Summary 199

References 200

Chapter 10 Field Devices 203

Where the Real Action Happens! 204

Timing of Field Device Specification 205

Reliability and Systematic Capability 205

 Fault Tolerance 207

 A Bit of Historical Context 209

 Basic Specifications for Field Devices Used in Safety Functions 217

 Do the Field Devices Play Nice with the SIS Logic Solver? 221

Measurements, Sensor Elements, and Transmitters 223

 Measurement Types 223

 Accuracy and Calibration Stability 227

 Process Connections 230

 Smarter Diagnostics 232

 Process and Position Switches 235

Final Elements 236

 Automated On/Off Valves 237

 Valve Actuators 244

 Actuator Accessories 247

 Partial Stroke Testing and Diagnostics 255

 Motors, Pumps, and Compressors 256

 Control Valves 257

Diagnostics, Redundancy, and Reliable Operations	260
Summary	261
References	262
Chapter 11 Engineering a System	265
We Have a Safety Requirements Specification, What's Next?	266
Project Schedule versus Out of Sequence Design	266
Architecture Drawing	267
BPCS Interface	269
Vibration Monitoring Systems	270
Motor Control Center	271
FGS and HVAC Interface	273
Mechanical Skid Packages	274
I/O Signal Interface	274
Signal Source	275
Energize versus De-Energize to Trip	275
Transient Surge and Spike Suppression	280
Relay Isolation	281
Miscellaneous I/O Considerations	283
Important Operator Interfaces with the SIS	284
Operational Bypasses	285
Maintenance Bypasses	286
Reset Action	288
Emergency Shutdown Switches	288
Plant Boundary Isolation Switches	290
Layout, Panels, and Equipment Rooms	290
Common Cause Considerations	291
Grounding	297
Environmental Conditions	298
EMI Protection	299
Summary	299
References	300
Chapter 12 Software	301
We Have Set Up All the Hardware, the Rest Is Just Software!	302
A Systematic Approach to Software Development	303
Software Life Cycle	303
Control HAZOP	306
Program and Language Types	309
Important Requirements from ISA/IEC 61511	312
The What and How of Programming	313
Understanding the Program Scan Cycle	313
Operator and BPCS Interface to the SIS	315
Additional HMI Considerations	321
Response to Diagnostics	322

Function Blocks, Templates, and Simplified Design.....	322
Engineering Tools for Programming.....	324
Miscellaneous Considerations	324
Summary	326
References	327
Chapter 13 System Testing	329
It Wasn't Supposed to Work That Way?!.....	330
Testing Philosophy and Concepts.....	331
Setting Up the Test Plan	334
Test Documents and Logistics	335
Fault Rectification and Punch Lists	337
Hardware Acceptance Test.....	338
Software Acceptance Test.....	342
Factory Acceptance Test	344
Testing at the Module Yard and Vendor Shops	346
Mechanical Completion	347
Site Acceptance Testing.....	347
Summary	348
References	349
Chapter 14 Installing a System	351
The Installation and a Bit of Philosophy.....	353
Construction Requirements and Interface	354
What Can Happen at the Construction Site.....	356
Construction Quality Assurance and Control	359
Transportation, Incomplete Installation, Warehouse Receiving, and Preservation.....	360
Reliability and the Installation.....	362
Instrument Air Supply	362
SIS Logic Solver, Power Supplies, Grounding, Wiring, and Cabling	366
Field Devices.....	370
Motor Trips	388
Criticality and Maintenance Access	389
Material Selection.....	390
Access to Manufacturer Knowledge.....	390
Additional Considerations	391
Summary	392
References	392
Chapter 15 Cybersecurity.....	395
Similarities and Differences Between Functional Safety and Cybersecurity.....	396
Open Systems Are Vulnerable	397

- Basic Concepts of ISA/IEC 62443 Standards 398
 - Cybersecurity Assessments 400
 - Assigning Security Levels 402
 - Cybersecurity Requirements Specification 403
 - Cybersecurity Design, Engineering, and Implementation 404
 - Other Means of Cyber Risk Reduction 405
 - Security Level Verification 405
 - Detailed Design 405
 - Detailed Design Verification 406
 - System Integration (Buy/Build/Configure) 406
 - Cybersecurity Factory Acceptance Test (CFAT) 406
 - Installation and Validation 407
 - Operate and Maintain 407
 - Management of Change 407
- Vulnerability Assessments of Existing Systems 407
- References 409
- Additional Information 409

Chapter 16 Operations and Maintenance 411

- Pressing the Start Button 412
- Documentation for the Operations versus the Project Phase 413
 - Wiring Drawings and Loop Diagrams 414
 - Operating Manuals 418
 - Keeping the Design and Documentation Up to Date 420
 - Updating Project Documentation 422
- Commissioning and Start-Up 423
 - Benchmarks 425
 - Start-Up Checks and the Plan 427
 - Resources 430
 - All Systems Are Go 431
- System Testing, Analysis, and Maintenance 432
 - Proof Test Design Basis and Implementation 433
 - Software and Proof Testing 439
 - Proof Test Analysis 439
 - Testing by Operations 442
 - Repairs, Replacements, and Recalibration 443
 - Bypasses 443
- Some Philosophical Remarks 444
- Management Systems 444
 - Appointment Competency Register 445
 - System Register 447
 - Audits and Gap Analysis 448
- Summary 449
- References 450

Chapter 17 Management of Change	451
When and Why Did We Change That?!	452
Managing Changes	452
ISA/IEC 61511 Modification Safety Life-Cycle Approach	453
Design Intent	460
Project MOC	462
Construction	465
Testing and Commissioning	466
Plant Operations	467
Decommissioning	467
Summary	467
References	468
Chapter 18 SIS Design Checklist	469
Introduction	470
Section 1: Management Requirements	473
Section 2: Process Hazards Analysis	474
Section 3: Safety Requirements Specification	475
Section 4: Conceptual SIS Design	477
Section 5: Detailed SIS Design	478
Section 6: Instrument Air	480
Section 7: Power and Grounding	481
Section 8: Field Devices	482
Section 9: Operator Interface	484
Section 10: Maintenance/Engineering Interface	486
Section 11: Communications	487
Section 12: Hardware Specification of SIS Logic Solver	488
Section 13: Hardware Manufacture	489
Section 14: Embedded (Vendor) Software	490
Section 15: Software Coding/Programming	491
Section 16: Factory Acceptance Test	492
Section 17: Installation and Commissioning	493
Section 18: Validation	495
Section 19: Operations and Maintenance	496
Section 20: Testing	498
Section 21: Management of Change	500
Section 22: Decommissioning	501
Section 23: Documentation	502
Additional Information	503
Chapter 19 Case Study	505
What's in a Case Study?	506
Making Sense of the Safety Life Cycle and Some Philosophy	507
Background Process, Process Control, and Hazard Description	510
Defining the Safety System Requirements	513

Relief Studies and Functional Safety 514
Hazard Identification and PHA 516
Safety Instrumented Function Allocation..... 520
A Moment for Reflection..... 526
Safety Requirements Specification..... 527
Software Specification 537
Designing the Safety System..... 537
 Field Instrumentation Selection 537
 SIS Logic Solver Selection 539
 SIL Verification 539
 SIL Verification Calculation Comments 542
 Design Documents for Installation 544
 Other Environmental Considerations 545
 Testing for Commissioning and Ongoing Maintenance..... 545
Stop the Press: Change Ahead!..... 546
Summary 546
References 547

Annex A Things to Consider When Selecting an SIS Logic Solver 549

Index 573

About the Authors

Paul Gruhn, PE, CFSE

Paul Gruhn is a global functional safety consultant with aeSolutions in Houston, Texas.

Paul is an ISA Life Fellow, a 25+ year member and co-chair of the ISA84 standards committee (on safety instrumented systems), the developer and instructor of ISA courses on safety systems, the author of two ISA textbooks, and the developer of the first commercial safety system software modeling program over 20 years ago.

Paul has a BS in mechanical engineering from Illinois Institute of Technology. He is a licensed Professional Engineer (PE) in Texas, a member of the control systems engineering PE exam committee, and both a Certified Functional Safety Expert (CFSE) and an ISA84 Safety Instrumented Systems Expert.

Simon Lucchini, CFSE, MIEAust, CPEng

Simon Lucchini received Bachelor's degrees in both electrical engineering and science from Sydney University, Australia, and he is a Chartered Professional Engineer in Australia. Lucchini has worked for 23 years in the petrochemical industry in roles ranging from operations and maintenance to corporate engineering and project engineering. He has worked at Fluor for the past 16 years in the Control Systems department. He is a Fluor Fellow in safety systems

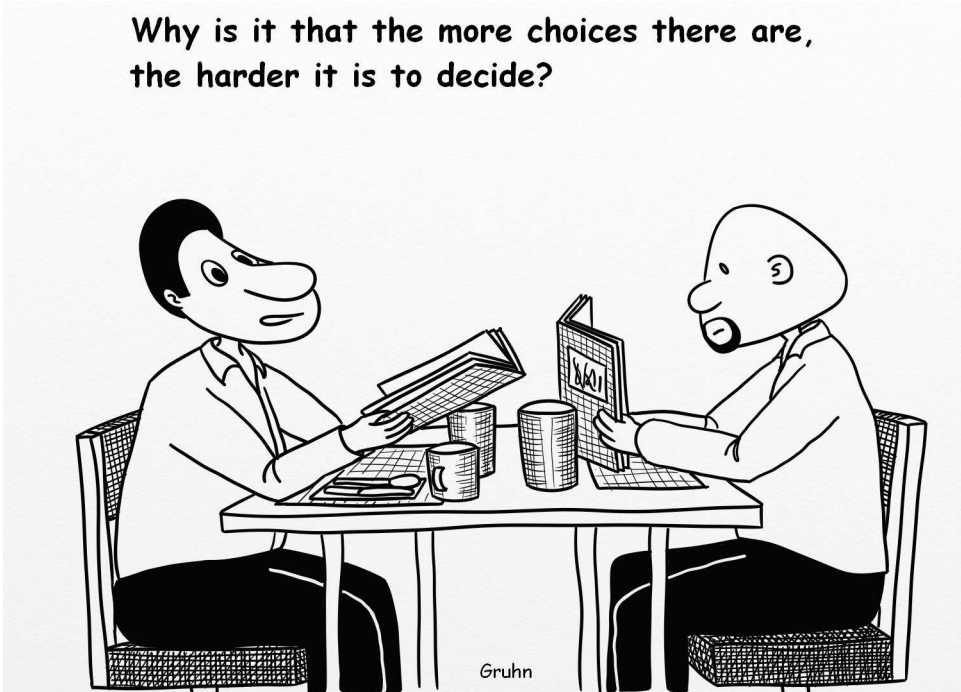
design and the chief controls specialist based at the Fluor Calgary, Alberta, Canada office.

Lucchini has written papers on safety systems for various industries and academic venues, including two chapters in Béla Lipták's *Instrument and Automation Engineers' Handbook: Process Measurement and Analysis*, fifth edition, published in 2016. Lucchini is currently the chair of the Safety Systems Committee for the International Society of Automation (ISA) Safety and Security Division for which he produces web articles on matters of importance for the safety systems industry. He is also an active contributor to local control system networks that include several global oil and gas operators.

1

Introduction

Why is it that the more choices there are,
the harder it is to decide?



*“Engineering responsibility should not require the stimulation
that comes in the wake of catastrophe.” ~ S. C. Florman*

What Is a Safety Instrumented System?

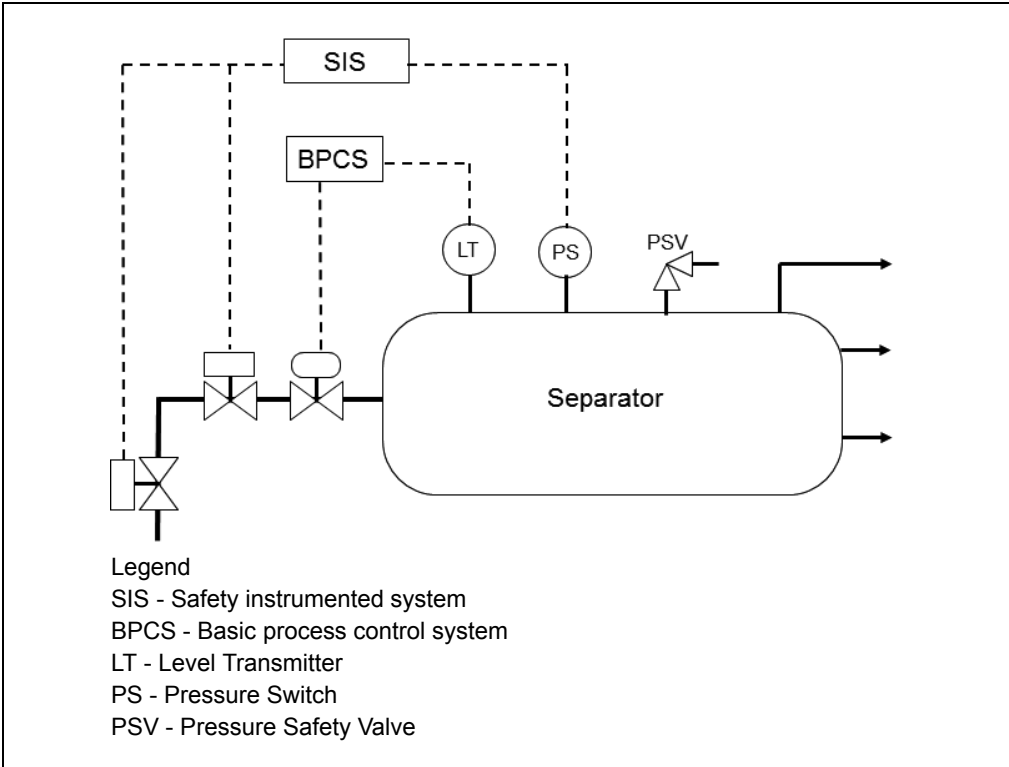


Figure 1-1. Control Function and Safety Function

Figure 1-1 shows a control function and a safety instrumented function. As the name implies, control functions *control* pressure, level, temperature, flow, and the like. Early systems in the process industries were purely mechanical/pneumatic, then electronic, and are now software based. Do you believe control functions are perfect and will never fail? (That question usually draws giggles and grins in classes.) Do you believe designers and engineers can envision *every* possible hazardous situation that could occur and design control systems to prevent *all* of them? If that were the case, we would not need to install alarm systems (as there would never *be* an alarm), relief valves (as there would never *be* an overpressure), flare systems (as there would never *be* a process upset), or fire and gas systems (as there never would *be* a release). We obviously don't live in such a dream world. There are many reasons why process facilities are designed with multiple layers of protection.

When a control function fails, the next layer of defense is often a safety instrumented function. The safety instrumented function in the process industry by and large does not *control* anything. It *monitors* many of the same variables, but only takes actions when a variable is outside its normal range, which generally means the control function has failed. The typical action of the safety function is to shut down the process or bring it to a predetermined safe state (e.g., recycle). This is a fundamentally different strategy compared to some other industries, such as aircraft. We don't really want to shut down the flying process at an altitude of 35,000 feet!

Control function failures most often conjure up notions of “things” breaking down (e.g., pressure transmitter electronics burning out or going out of calibration). However, as modern digital electronics have become more reliable with respect to random faults, other classes of failure may be prevalent. Systematic failures and human actions may be the initiating causes for a potential hazard. Furthermore, as the software-based control systems become more complex, hazards are frequently emergent properties and may not be related to any physical/permanent fault (i.e., a transient interaction between the process, control system, safety function, and the human operator). Questions may then include, “Does the safety function guard against these types of failures? Has the safety function been designed to be robust with respect to systematic failures?”

Systems performing safety functions have gone by many different names: emergency shutdown system, safety shutdown system, instrument protection system, safety interlock system, safety instrumented system, and more. Different companies within the process industry still use a variety of names for these systems. The shortest and perhaps most generic term might be *safety system*, but this too means different things to different people. For many chemical engineers, “safety systems” refer to management procedures and practices, not instrumented systems. One very common term has been *emergency shutdown system* (ESD), but to electrical engineers, ESD means electrostatic discharge. To some, ESD is a means of *manually* shutting down the process independent to the safety system. Many don't want the word *emergency* in the name at all, due to its negative connotation.

When the American Institute of Chemical Engineers' Center for Chemical Process Safety (AIChE CCPS) published the first edition of *Guidelines for Safe Automation of Chemical Processes* in 1993 [1], the term it used was *safety interlock system*—SIS. Some members of the ISA84 committee thought the term “interlocks” was only one subset of many different types of safety-related systems.

The ISA84 committee settled on the term *safety instrumented system* in order to keep the same acronym used in the AIChE text—SIS. A related AIChE CCPS text titled *Layer of Protection Analysis* released in 2001 also uses the acronym SIS, but uses the more recent terminology of “safety instrumented system.”

The first edition of the ISA-91 standard, ANSI/ISA-91.01-1995, *Identification of Emergency Shutdown Systems and Controls That Are Critical to Maintaining Safety in Process Industries*, published in 1995 used the phrase *emergency shutdown system* with the following definition: “Instrumentation and controls installed for the purpose of taking the process, or specific equipment in the process, to a safe state. This does not include instrumentation and controls installed for nonemergency shutdowns or routine operations. Emergency shutdown systems may include electrical, electronic, pneumatic, mechanical, and hydraulic systems (including those systems that are programmable).” In other words, these systems are designed to respond to conditions of a plant, which may be hazardous in themselves, or if no action were taken could eventually give rise to a hazardous event. They must generate the correct outputs to prevent or mitigate the hazardous event.

The international community has other ways of referring to these systems. The International Electrotechnical Commission Standard 61508-1 (IEC 61508-1:2010), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 1: General Requirements* [2], first published in 1998 used the term safety-related systems, but also introduced the combined acronym E/E/PES. As used in the title, E/E/PES stands for electrical, electronic, and programmable electronic. In other words, relay, solid-state, and software-based systems.

The standards generally focus on systems related to personnel safety. However, the same concepts apply to systems designed to protect equipment, the environment, and company reputation. After all, there are more things at risk to a company than just people.

As with any subject, there are a variety of acronyms and technical terms. Some terms do not have complete agreement or common usage in industry and different texts. This naturally adds to the confusion. Unless otherwise noted, all the terms used in this text are defined in ISA-61511-1-2018, *Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements* [3]. Acronyms are typically defined the first time they are used and other terms are explained where appropriate.

Who This Book Is For

This book is intended for the thousands of professionals employed in the process industries who are involved with safety instrumented systems in any way and who are expected to follow the appropriate industry standards. These individuals are employed by end users, engineering firms, system integrators, consultants, and vendors. Managers and sales individuals will also benefit from a basic understanding of the material presented.

The first edition of the ISA-84 standard, ISA-84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*, was published in 1996 and defined the intended audience as those who are involved in areas of “design and manufacture of SIS products, selection, and application, installation, commissioning, and prestart-up acceptance testing, operation, maintenance, documentation, and testing.” Basically, if you’re involved with safety systems in any way, there are portions of the standards and this book that will be of interest to you.

The first edition of the standard also defined the process industry sector as “those processes involved in, but not limited to, the production, generation, manufacture, and/or treatment of oil, gas, wood, metals, food, plastics, petrochemicals, chemicals, steam, electric power, pharmaceuticals, and waste material(s).” Following editions had similar definitions.

Why This Book Was Written

Would you rather learn from the mistakes of others, or make them all yourself? We learn better when we make our own mistakes. However, we’re engineering industrial processes—and using computer-based systems to control them—that have the potential for large-scale destruction. Single accidents are often disastrous and have resulted in multiple fatalities and significant financial losses. We simply do not have the luxury of learning process safety by trial and error. We must try to anticipate and prevent accidents *before* they occur. This has been one of the hard lessons learned from past accidents and why various process safety legislation has been passed in different parts of the world. Similarly, many U.S. states passed legislation requiring the involvement of Professional Engineers after various engineering disasters that resulted in the deaths of hundreds of people. Hopefully this book, in its own little way, will help make the world a safer place.

This book is a practical “how to” on the analysis, specification, selection, design, installation and maintenance of safety instrumented systems. It includes practical knowledge needed to apply safety instrumented systems. It will hopefully serve as a guide for implementing the procedures outlined in various standards.

Aren't the standards alone enough? The answer depends upon you and your company's knowledge and experience. The normative (mandatory) portion of ISA-84.01-1996 was only about 30 pages long, with about 80 pages of annexes and informative material. While committee members knew what certain phrases and requirements meant, not everyone else did. Some committee members wanted certain wording to be specifically vague in order to have the freedom to be able to implement the requirements in different ways. Others wanted clear-cut prescriptive requirements. The second edition of the standard contained much more detail. Part 1 of the standard—the normative portion—was over 80 pages in length. Part 2—the informative portion on how to implement Part 1—was also over 80 pages. Part 3 of the standard summarized various safety integrity level selection techniques and was over 60 pages in length. The ISA84 committee felt additional material was *still* needed. At the time of this writing, eight additional technical reports have been written, totaling over 500 pages. Topics of the technical reports include system modeling, mechanical integrity, guidelines on implementing the standard, burner management systems, safety fieldbuses, fire and gas systems, wireless, and cybersecurity. Many of the technical reports have gone through multiple revisions.

Standards aren't written to teach. They tell you *what* to do, but not necessarily *why*, or even *how* to do it. They are often dry, boring, and downright painful to read. This book is intended to both explain and teach, and do it in a manner that is easier and more enjoyable to read. (Earlier variations of this book have consistently received high ratings and received “best seller” awards.) This book covers the entire life cycle of safety instrumented systems, from determining what sort of systems are required through decommissioning. It covers the difference between process control and safety control, the separation of control and safety, independent protection layers, determining safety integrity levels, logic system and field device issues, installation, maintenance, and management of change—all the phases of the life cycle covered in the primary standard of interest. The book focuses on establishing design requirements, analysis techniques, technology choices, purchase, installation, documentation, and testing of safety instrumented systems. The focus throughout is on real-world, practical solutions with many actual examples.

This is the third iteration of this book. The first edition was titled *Safety Shutdown Systems: Design, Analysis and Justification*. It was published in 1998 following the release of the first ISA-84 standard in 1996. The second edition was titled *Safety Instrumented Systems: Design, Analysis and Justification*. It was published in 2006 following the release of the second edition of the ISA-84 standard in 2004, which is in fact the first edition of IEC 61511 with one additional sentence from a U.S. regulation. The second edition of the standard was a considerable departure from the first, so a new book edition was appropriate. A second edition of IEC 61511 was released in 2016. Unfortunately, there were errors with the second edition that was released. A corrigendum (a list of corrections that *did not* require a committee ballot) and an amendment (a longer list of corrections that *did* require a committee ballot) were released later that year. It took a full year to approve the changes. The ISA84 committee voted to accept the 61511 standard without changes in late 2017 (although a new forward will be added to the U.S. version of part 2). The review process by ANSI took additional time, and ISA published ISA 61511 in 2018. There were enough changes in the standard to warrant a new edition of the ISA book. A new co-author was involved with this book, so a new title was deemed appropriate: *Safety Instrumented Systems: A Life-Cycle Approach*.

Confusion in the Industry

One goal of this book is to clarify the general confusion in the industry over the myriad choices involved in the design of safety systems. Many would have hoped to turn to industry standards for their recommendations. However, the standards are performance oriented and not prescriptive, so there are no specific recommendations. The standards essentially state what needs to be done, not specifically how to do it. For example, what follows are just a few of the choices that need to be made:

Technology Choices

What technology should be used—relay, solid state, or microprocessor? Does this depend on the application? Relay systems are still common for small applications, but would you want to design and wire a 500 I/O (input/output) system with relays? Would you consider it economical to design a 20 I/O system using a triple modular redundant software-based system? Some people prefer not to use software-based systems in safety applications at all; others have no such qualms. Solid-state systems were designed to replace relay systems, yet they do not utilize software. Like relays, these systems are essen-

- quad 9
- quality assurance 14
- quality assurance and quality control program (QA/QC) 347
- quality control (QC) 330

- RACI matrix 45, 48–49
- rack and pinion 253
- range 102, 535
- reactors 80
- Reason, James 74
- redundancy 8, 155, 176–177, 260
- redundant 374
- registration 447
- relay 215, 283
 - isolation 281
 - ladder logic 313, 322
 - logic 323
 - systems 142, 144, 147, 159, 182
- reliability 9, 78, 94, 173, 195, 205, 275, 377, 432
 - block diagrams (RBDs) 174
- relief 514
- remote I/O
 - capabilities 559
 - monitoring 558
- requests for quotations (RFQs) 549
- reset 107, 239, 288, 531
 - action 318, 320
- resistance temperature detector (RTD) 213, 225
- resources 430
- response time 528
- responsible, accountable, consulted, and informed (RACI) 45
- rising edge reset 320
- risk 115, 117–120, 509
 - analysis 31
 - assessment 31
 - frequency 124
 - graph 128–129
 - inherent in the process 82
 - management 47
 - matrix 124, 516–517
 - overall 125–126
 - ranking (RR) 516–517
 - reduction factor 122–123, 136, 508
 - severity 125
 - tolerable 131
- room layout drawings 355
- rotating equipment 429

- safe failure 167
- safe failure fraction (SFF) 196, 362
- safe state 528, 530

- safety 58
 - availability 122
 - communications 558
 - control 60
 - function action 102
 - functions 32
 - interlock system 3
 - layer matrix 124
 - layers 74–75
 - life cycle 11, 38, 41, 453, 507
 - logic solver ranking 566
 - plan 40, 45, 48–49
 - PLCs 151
 - shutdown system 3
 - standards 236
 - system 3
 - system design 537
 - system logic 100
 - system requirements 513
 - systems 68–69, 103, 275
- safety instrumented function (*see also* SIF) 2, 31, 40, 86, 100, 205, 305, 352
- safety instrumented system (*see also* SIS) 3–4, 8, 38, 79, 112, 204, 302, 330, 412, 506
 - logic solver 549
- safety integrity level (*see also* SIL) 31, 62, 86, 91, 100, 112, 122, 128, 145, 359, 420, 506
- safety interlock system 3
- safety requirements 50, 87, 91, 98
- safety requirements specification (SRS) 32, 38, 41, 47, 86, 89, 96, 266, 330, 342, 352, 475, 506, 527
 - documentation 513
 - index 95
- safety-configured PLCs 150
- SCADA 102
- scaffolding 356
- SCAI 58
- scan execution 314
- scan time 555
- schedules 41, 44, 46, 266
- scope 41
- scrubbers 80
- sealing 218–219
- security 565
 - concerns 65
 - level verification 405
 - levels 399, 402–403
 - life cycles 398
- sensors 204
- sequence of events 556
- sequential flow charts 323
- sequential function charts 100
- shutdown 535
 - keys 99

- shuttle valves 252
- SIDA 133
- SIF 528
 - allocation 45, 47, 91, 93, 520, 525
- signal source 275
- SIL
 - allocation 53, 86, 513
 - capability 112
 - claim limit 112
 - determination 45, 47, 93, 124
 - determination reports 422
- SIL verification 48, 53–54, 94, 103–104, 217, 251, 361–362, 465, 539, 541–542
 - parameters 97
 - reports 421
- simplex 162, 552
- simplified design 322
- simulation capabilities 564
- SIS 3, 47, 93, 273, 297
 - design 477–478
 - design cookbook 197
 - logic 104
 - logic solver 86, 98, 221, 255, 330, 352, 366, 539
 - operating system (OS) 302
 - process measurements 535
 - safety requirements 97
- site acceptance test (SAT) 347
- size 105, 554, 562
- skid 274
- smart devices 8, 214, 255
- software 302–303, 352, 439, 457, 537
 - acceptance test (SAT) 342
 - coding/programming 491
 - issues 146
 - life cycle 303–304
 - program development and design 305
 - program implementation 305
 - program verification and testing 305
 - requirements 98
 - safety requirements specification (SRS) 305
 - SIS integration testing 306
 - templates 344
 - version control 563
- software-based systems 145, 159
- solenoid 215
 - valves 250
- solid-state systems 144–145, 147, 159
- specifications 23
- speed of response 239, 555
 - temperature 380
- spike suppression 280
- spurious 526, 536
 - trip rate (STR) 47
- standards 6, 15
 - start-up 423, 426–427, 430
 - supervisor function 317
 - supports 373
 - surge 280, 514
 - switches 235
 - emergency shutdown 288
 - plant boundary isolation 290
 - system performance 155
 - system register 447
 - system testing 51, 432
 - systems performing safety functions 3
- Technischer Überwachungsverein (TÜV) 35, 156, 158, 557
- temperature 225, 229, 378
- templates 322, 324
- terminations 372
- terminology 334
- test
 - documents 335
 - intervals 8
 - plan 334
 - procedures 333
- testing 144, 331–332, 335, 466, 498
 - logistics 335
- Texas City refinery disaster 73
- thermocouple 225
- third-party contractor 401
- threat vectors 401
- Three Mile Island 80
- tight shutoff (TSO) 239
- time delay block 252
- time limit 317
- time synchronization 557
- timing 106
- tolerable risk level 83
- total installed cost (TIC) 38
- transient protection 219
- transmission control protocol (TCP) 533
- trip 239
 - action 528
 - levels 514
 - list 102
 - open valves 244
 - points 535
 - valves 387–388, 545
- triple 162
- triple modular redundant (TMR) systems 155
- tubing 252, 376
- turndown capability 227
- U.K. Health and Safety Executive (HSE) 23–24, 87
- U.S. Refrigerator Safety Act of 1956 76
- ultraviolet (UV) 386

- unavailability 169
- undocumented features 147
- uninterruptible power supplies (UPSs) 246
- unprecedented accuracy 227
- upscale/downscale burnout 232

- validation 30, 34–35, 495
- valve actuators 244, 246
- variable frequency drives (VFDs) 388
- variable restrictor 252
- variable speed drives 388
- vendor records 165
- venturi meters 223
- verification 30–31, 35, 250, 359
- vibration 215, 219, 270, 373
- volume boosters 251
- vulnerability 401, 407–408

- wearout 171
- wedge meters 223
- well-meaning insider 401
- wiring 366, 368, 372, 414–416
- wiring termination 355

- XV safety time
 - design basis 462

- zero suppression 210

