Safety Instrumented Systems

A Life-Cycle Approach

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

ISA

Setting the Standard for Automation™

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.

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

ISBN: 978-1-945541-54-4

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 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.

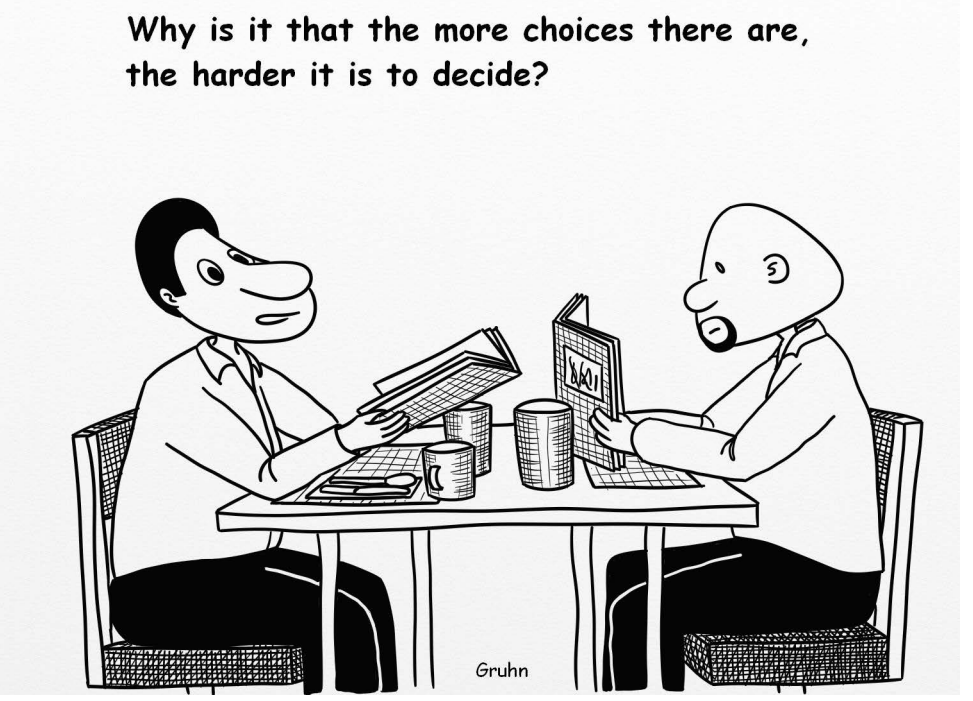
Simon Lucchini, CFSE, MIEAust, CPEng

Simon Lucchini received Bachelor's degrees in both electrical engineering and science from Sydney University, Australia, and he is a Charted 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



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

What Is a Safety Instrumented System?

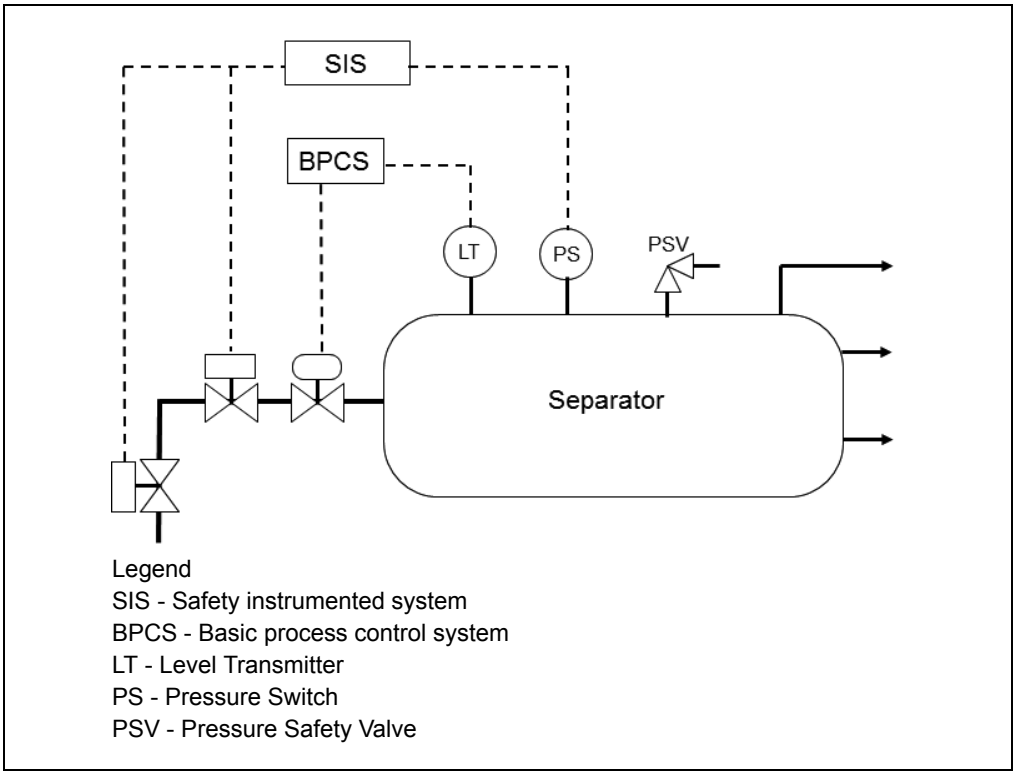


Figure 1-1. Control Function and Safety Function

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-