Studies in Systems, Decision and Control 255

Emil Pricop
Jaouhar Fattahi
Nitul Dutta
Mariam Ibrahim *Editors*

Recent Developments on Industrial Control Systems Resilience

Springer

Studies in Systems, Decision and Control

Volume 255

The series "Studies in Systems, Decision and Control" (SSDC) covers both new developments and advances, as well as the state of the art, in the various areas of broadly perceived systems, decision making and control–quickly, up to date and with a high quality. The intent is to cover the theory, applications, and perspectives on the state of the art and future developments relevant to systems, decision making, control, complex processes and related areas, as embedded in the fields of engineering, computer science, physics, economics, social and life sciences, as well as the paradigms and methodologies behind them. The series contains monographs, textbooks, lecture notes and edited volumes in systems, decision making and control spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

** Indexing: The books of this series are submitted to ISI, SCOPUS, DBLP, Ulrichs, MathSciNet, Current Mathematical Publications, Mathematical Reviews, Zentralblatt Math: MetaPress and Springerlink.

More information about this series at http://www.springer.com/series/13304

Emil Pricop · Jaouhar Fattahi · Nitul Dutta ·
Mariam Ibrahim
Editors

Recent Developments on Industrial Control Systems Resilience

Springer

Editors
Emil Pricop
Control Engineering, Computers
and Electronics Department
Petroleum-Gas University of Ploiesti
Ploiesti, Romania

Jaouhar Fattahi
Department of Computer Science
and Software Engineering
Laval University
Quebec City, QC, Canada

Nitul Dutta
Computer Engineering Department
Marwadi University
Rajkot, Gujarat, India

Mariam Ibrahim
Department of Mechatronics Engineering,
School of Applied Technical Sciences
German Jordanian University
Amman, Jordan

ISSN 2198-4182 ISSN 2198-4190 (electronic)
Studies in Systems, Decision and Control
ISBN 978-3-030-31327-2 ISBN 978-3-030-31328-9 (eBook)
https://doi.org/10.1007/978-3-030-31328-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedicated to our beloved families for supporting us all along.
Emil Pricop, Jaouhar Fattahi, Nitul Dutta and Mariam Ibrahim

Preface

Industrial control systems (ICS) have a critical place in the functioning and development of today's world. They are key components of every technical infrastructure around us, ranging from air conditioning in our homes and cars to the big factories, the energy production and distribution, the water distribution systems, and even the nuclear plants. The correct operation of the industrial control systems is essential for the functioning of our society, so they have to be designed to be resilient. This means that the ICS should be able to recover from various process faults and failures and to withstand emerging cyberattacks. These objectives can be achieved only by assuring both safety and security, being it physical or cybernetic. Also, a special interest is presented by predictive and preventive maintenance activities.

The main goal of the book is to collect valuable contributions of renowned researchers in the field of control engineering, Internet of Things, and cybersecurity. Some chapters are based on presentations and discussions that took place at the previous editions of the International Workshop on Systems Safety and Security (IWSSS, https://www.iwsss.org). The workshop, initiated in 2013, become a traditional annual scientific event in Romania. IWSSS is now a recognized venue for the exchange of experience and ideas in the field of systems safety, security, and resilience with the scope of stimulating joint work at a regional and international level.

The book comprises research based on theory, subsequent simulation and experimental results, numerous case studies, and practical implementations. Given the detailed discussion in the said context, the book offers profound insights on increasing the resilience of industrial control systems. Both fundamental and advanced topics are discussed, having the theoretical approaches sustained by practical examples.

The structure and chapters of the book are broadly grouped into core topics that address challenges related to safe operations of control systems, risk analysis and assessment, usage of attack graphs to evaluate and increase the resiliency of control systems, preventive maintenance, and malware detection and analysis. The resilience and cybersecurity of sensor networks and the Internet of Things devices, which are now an integral part of the various industrial control systems, are discussed in different chapters of the book.

Another notable contribution of this book is the inclusion of necessary and timely response to malicious attacks or hazardous situations. This topic will certainly help readers to decide the best approaches to handle such unwanted situations.

We believe, the contents of the book is essential readings for system engineers, researchers, and specialists. The topics discussed in the book are challenging and recent and we anticipate the book to represent a useful reference for all the professionals in the field of ICS resilience, safety, and security. Finally, the editors expect that this book will be a supportive auxiliary to undergraduate and graduate students, to academia and researchers trying to address security and safety issues related to the modern implementations of the industrial control systems.

Ploiesti, Romania — Dr. Emil Pricop
Quebec City, Canada — Dr. Jaouhar Fattahi
Rajkot, India — Dr. Nitul Dutta
Amman, Jordan — Dr. Mariam Ibrahim
August 2019

Contents

Editors and Contributors

About the Editors

Emil Pricop is currently with the Control Engineering, Computers and Electronics Department of the Petroleum-Gas University of Ploiesti, Romania. He holds the position of Senior Lecturer since 2018 and he is teaching Computer Networking, Software Engineering, and Human–Computer Interaction courses. He received his Ph.D. in Systems Engineering from Petroleum-Gas University of Ploiesti by defending in May 2017 the thesis with the title "Research regarding the security of control systems". His research interest is cybersecurity, focusing especially on industrial control systems security. Dr. Emil Pricop is co-editor of the book *Recent Advances in Systems Safety & Security (Springer, 2016)* and author or co-author of two national (Romanian) patents, five book chapters published in books edited by Springer, and over 30 papers in journals or international conferences. From 2013, Dr. Pricop is the initiator and chairman of International Workshop on Systems Safety and Security—IWSSS, a prestigious scientific event organized annually.

Jaouhar Fattahi is currently working with Defence Research and Development Canada (DRDC) at the Valcartier Research Centre as a defence scientist. He is also an adjunct professor with Laval University, Quebec City, Canada. He obtained his Ph.D. on the security of cryptographic protocols from Laval University in October 2015. He completed his postdoctoral fellowship at the Canadian Armed Forces Research Centre in the field of cybersecurity. He has also been a computer engineer since 1995. Dr. Jaouhar Fattahi is the author of *The Theory of Witness-Functions* for verifying security of cryptographic protocols. He now specializes in reverse engineering and machine and deep learning applied to security and cybersecurity. He is an IEEE member.

Nitul Dutta is a professor in the Computer Engineering Department, Faculty of Engineering (FoE), Marwadi University, Rajkot, Gujarat, since 2014. He has a total experience of 20 years. He received B.E. degree in Computer Science and

Engineering from Jorhat Engineering College, Assam (1995), and M. Tech. degree in Information Technology from Tezpur University, Assam (2002). He completed Ph.D. (Engineering) degree in the field of Mobile IPv6 at Jadavpur University (2013) and published 15 Journal and 30 conference papers. He has completed two AICTE sponsored research projects of worth Rs. 25 Lakhs (approx.) (Rs. Twenty-Five Lakhs only). His current research interests are wireless communication, mobility management in IPv6-based network, cognitive radio networks, and cybersecurity.

Mariam Ibrahim received her Bachelor's degree in Electrical and Computer Engineering from the Hashemite University, Jordan, in 2008, and M.S. in Mechatronics Engineering from Al-Balqa Applied University, Jordan, in 2011, and the Ph.D. in Electrical Engineering from Iowa State University, USA, in 2016. She was a lab supervisor with EE department at the Hashemite University (2008–2011). She joined the German Jordanian University (2011) as an RA, where she got a scholarship to pursue her Ph.D. studies; she is currently an assistant professor at GJU. Her research interests include discrete-event systems, stochastic systems, power systems, communication networks, healthcare systems, together with their control and resiliency analysis, and system model-based verification/attack graph generation using AADL. She is a member of Iowa Section IEEE Control Systems Society Technical Chapter. She serves as a scientific reviewer in the international scientific committee of the International Workshop on Systems Safety and Security—IWSSS since 2017, journal of *IET Cyber-Physical Systems: Theory & Application, 2018*, and *IEEE Network Magazine, 2018*.

Contributors

Qays Al-Hindawi Department of Mechatronics Eng, Faculty of Applied Technical Sciences, German Jordanian University, Amman, Jordan

Ahmad Alsheikh Department of Mechatronics Eng, Faculty of Applied Technical Sciences, German Jordanian University, Amman, Jordan

Horia Andrei SM-IEEE, Bucharest, Romania;
Doctoral School of Engineering Sciences, University Valahia Targoviste, Targoviste, Romania

Paul Cristian Andrei Department of Electrical Engineering, University Politehnica Bucharest, Bucharest, Romania

Alina-Simona Băieşu Automatic Control, Computers and Electronics Department, Petroleum-Gas University of Ploiesti, Ploiesti, Romania

Tomáš Bajtoš Faculty of Science, Institute of Computer Science, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

Radoslav Benko Faculty of Law Institute of International Law and European Law, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

Krishna Delvadia Chhotubhai Gopalbhai Patel Institute of Technology, Bardoli, Gujarat, India

Viktor M. Denisov "Flagman Geo" Ltd., Saint-Petersburg, Russia

Viorel Dumitru National Institute of Materials Physics, Magurele, Romania

Nirali Dutiya Department of Computer Engineering, Faculty of PG Studies, MEF Group of Institutions (MEFGI), Rajkot, India

Nitul Dutta Computer Engineering Department, MEF Group of Institutions, Rajkot, Gujarat, India

Marian Gaiceanu Department of Control Systems and Electrical Engineering, Dunarea de Jos University of Galati, Galati, Romania

Theodora Gaiceanu Gheorghe Asachi Technical University of Iasi, Iasi, Romania

Mariam Ibrahim Department of Mechatronics Eng, Faculty of Applied Technical Sciences, German Jordanian University, Amman, Jordan

Octavian Ionescu National Institute for Research and Development in Microtechnologies, IMT Bucharest, Bucharest, Romania

Nilesh Jadav Department of Computer Engineering, Faculty of PG Studies, MEF Group of Institutions (MEFGI), Rajkot, India

Dhara Joshi Department of Computer Engineering, Faculty of PG Studies, MEF Group of Institutions (MEFGI), Rajkot, India

Xinxin Lou Bielefeld University, Bielefeld, Germany

Ioan Marinescu Doctoral School of Engineering Sciences, University Valahia Targoviste, Targoviste, Romania

Terézia Mézešová Faculty of Science, Institute of Computer Science, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

Stefan Pircalabu Cyberswarm Inc., San Mateo, CA, USA

Emil Pricop Petroleum-Gas University of Ploiesti, Ploiesti, Romania

Gabriel Rădulescu Control Engineering, Computers and Electronics Department, Petroleum-Gas University of Ploieşti, Ploieşti, Romania

Laura Rózenfeldová Faculty of Law, Department of Commercial Law and Business Law, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

Pavol Sokol Faculty of Science, Institute of Computer Science, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

Vasile Solcanu Dunarea de Jos University of Galati, Galati, Romania

Marilena Stanculescu Department of Electrical Engineering, University Politehnica Bucharest, Bucharest, Romania

Kajal Tanchak Computer Engineering Department, MEF Group of Institutions, Rajkot, Gujarat, India

Asmaa Tellabi University Siegen, Siegen, Germany

Andrey V. Timofeev LLP "EqualiZoom", Astana, Kazakhstan

Safety Instrumented Systems Analysis

Alina-Simona Băieșu

Abstract Operating most industrial processes, especially those in the oil and gas industry, involves an inherent risk due to the presence of dangerous/flammable substances. Therefore, using Safety Instrumented Systems (SIS) is mandatory. These systems are especially designed to protect personnel, equipment and environment by reducing the likelihood of an unwanted event to appear by reducing the severity of its impact. This chapter presents a comprehensive *Introduction* in the field of Safety Instrumented Systems, then the most important feature of a SIS is presented, *Safety Integrity Level of a Safety Instrumented System* and some *Practical Aspects Regarding Safety Instrumented Systems* are outlined. The chapter ends with some considerations regarding *IT Enabled Safety Systems*.

Keywords Safety instrumented systems · Risk analysis · IT enabled safety systems

1 Introduction

This paragraph outlines general aspects regarding the Safety Instrumented Systems (SIS) and their goal by presenting examples of such systems used in the industrial practice.

It also presents the evolution of the current in use standards that regulates the design, implementation and operation of SIS, focusing on IEC 61508 and IEC 61511 standards. The delimitation between the Control Systems (CS) and Safety Instrumented Systems (SIS) it is also highlighted by marking the major differences between the two types of automated systems.

A.-S. Băieșu (✉)
Automatic Control, Computers and Electronics Department, Petroleum-Gas University of Ploiesti, Ploiesti, Romania
e-mail: agutu@upg-ploiesti.ro

E. Pricop et al. (eds.), *Recent Developments on Industrial Control Systems Resilience*, Studies in Systems, Decision and Control 255,
https://doi.org/10.1007/978-3-030-31328-9_1

1.1 Safety Instrumented Systems General Aspects

A Safety Instrumented System (SIS) aims to bring the process to a safe state when the normal operating conditions are violated, for reasons of safety and protection [1]. Therefore, the role of a SIS is to monitor potential hazardous conditions and to mitigate the consequences in case of an unwanted dangerous event appearance.

A SIS is a set of sensors, logic solvers and actuators [2].

A SIS does not improve production or efficiency but helps to reduce economic losses by reducing risks [1].

The structure of a SIS is presented in Fig. 1.

The sensors are used to measure process parameters (temperature, pressure, flow, etc.) and to use their measures to determine whether an equipment or process is in a safe or unsafe state. The sensors can be of various types, from simple pneumatic or electrical switches to intelligent sensors with diagnosis. These sensors are dedicated to SIS and use communication channels and power supplies, different from those of control system sensors.

The logic solvers have the role of establishing what decision should be made based on the information received from sensors. Typically, the logic solver is a Programmable Logic Controller (PLC) that receives as inputs the signals from sensors, runs a particular program according to these values in order to prevent possible dangerous situations and sends output control variables to actuators.

The actuators carry out the actions from the logic solver. Usually the actuators are two-way valves (opened/closed), pneumatically operated.

All SIS components must be designed so that they can safely isolate the process in the event of a hazardous situation [3].

In the following, a SIS example is presented to highlight its role, structure and operation [4].

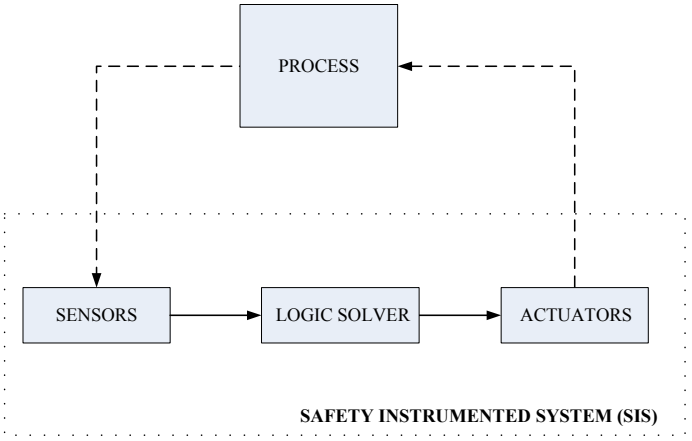

Fig. 1 A safety instrumented system (SIS) structure

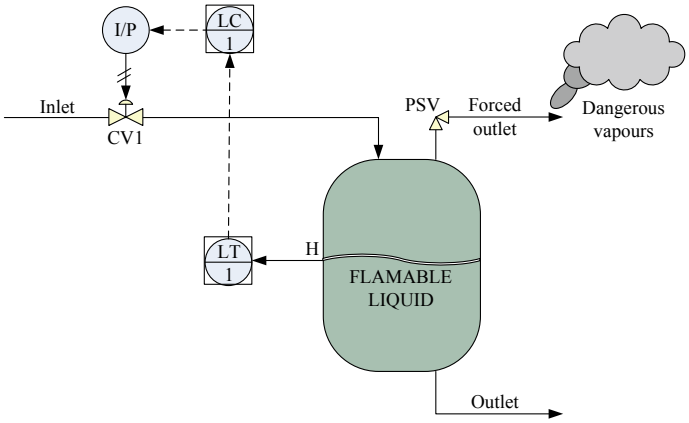

Fig. 2 A flammable liquid level control system: LC1—level controller, LT1—level transducer, I/P—electro/pneumatic converter, CV1—control valve, PSV—overPressure Safety Valve, H—liquid level

Figure 2 presents a vessel in which a flammable liquid is stored. A typical control loop must maintain the level (H) at 50%. An unwanted dangerous event can occur if the control loop fails for some reason and the vessel becomes full. The vessel has an overPressure Safety Valve (PSV) which evacuates the liquid out of vessel, but it will form a dangerous cloud of vapours [5].

Situations that can cause the control loop malfunction are:

- the Control Valve (CV1) cannot be operated;
- the Level Transducer (LT1) is faulty;
- the Level Controller (LC1) is manually operated and the Control Valve (CV1) is opened.

To prevent a possible damage, in the event of Control System (CS) malfunction, a Safety Instrumented System (SIS), as in Fig. 3, can be used. The CS equipment are marked with 1 and the equipment from SIS structure, with 2.

The SIS elements are symbolized using the ANSI/ISA 5.1 Specific Standard [6].

The SIS from Fig. 3 operation can be described as follows: the level transducer LZT2 has the role of detecting the vessel maximum liquid level (Hmax) and when this happens, the logic solver, for example a PLC, stops the vessel feeding through the UZV2 Safety Valve. Basically, the logic solver acts on the electromagnetic valve UZY2 that stops the air supply of UZV2, the air being ventilated outwards. The UZV2 will remain closed until all faults are removed. When the liquid level reaches a normal value, the operator can reset the UZV2 valve state, using HS2 (Human reSet) and the normal operation can continue.

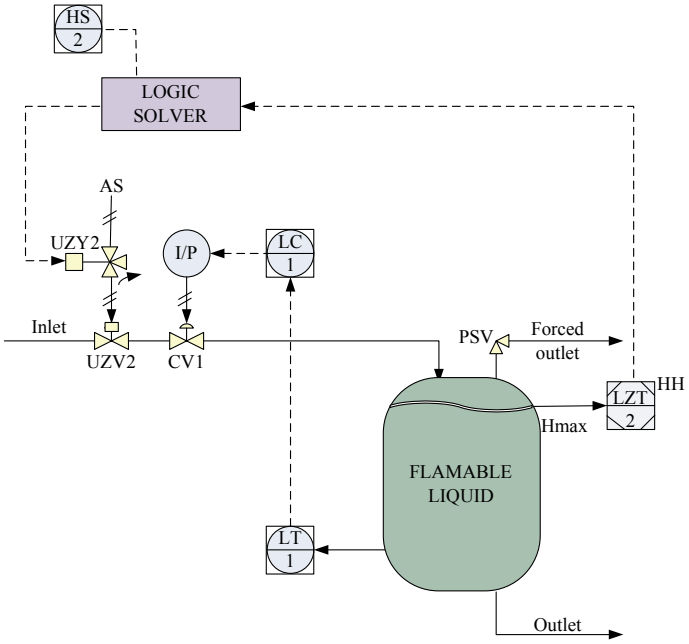

Fig. 3 Liquid level control system and safety instrumented system: LC1—level controller, LT1—level transducer, LZT2—high level transducer, UZV2 safety valve, I/P—electro/pneumatic converter, CV1—control valve, PSV—overPressure Safety Valve, UZY2—electromagnetic valve, AS—air supply, HS2—Human reSet, HH—high level alarm (High High), Hmax—high level

1.2 Safety Instrumented System Standards

The Safety Instrumented Systems (SIS) are receiving attention in the industrial sector due to the increasing environmental pressure in order to reduce the gas emissions and to get the most environmentally friendly products, but also because of the many accidents that occurred in different installations, through time.

Until the ‘80s, the industrial process safety issue was left to the decision of the various companies, who based on their own experience developed set of rules regarding SIS design and use. Subsequently, these sets of rules have been integrated into international standards and government regulations that require companies to comply with certain procedures.

IEC 61508 Standard

The IEC 61508 standard was developed by IEC (International Electrotechnical Commission) and covers a wide range of fields of activity and a multitude of SIS-associated equipment [7].

The standard applies for all steps which a SIS passes through from specification, design, operation, use, decommissioning and covers all the constituent parts of the SIS: sensors, logic solvers and actuators.

IEC 61508 standard has 7 parts [4]:

- Part 1, (December, 1998) presents some general specifications;
- Part 2, (May, 2000) presents the requirements for programmable electrical/electronic systems;
- Part 3, (December, 1998) presents requirements for software components;
- Part 4, (December, 1998) presents definitions, abbreviations and terminology to ensure a certain consistency;
- Part 5, (December, 1998) presents examples for determining the Safety Integrity Level (SIL);
- Part 6, (April, 2000) provides the appliance guide of Parts 2 and 3;
- Part 7, (March, 2000) presents a brief presentation of the techniques and methods relevant for Parts 2 and 3.

The most important part of IEC 61508 is the life cycle model of a SIS, shown in Fig. 4.

IEC 61511 Standard
IEC 61511 includes additional guidance for determining the Safety Integrity Level (SIL) to be imposed by the design team at the beginning of the SIS design phase and is structured in 3 parts [8]:

- Part 1, provides definitions, hardware and software requirements;
- Part 2, provides the appliance guide of Part 1;
- Part 3, provides guidance for determining the SIL.

The IEC 61511 standard is dedicated to the end user whose task is to design and operate the SIS in an industrial plant. The requirements are those imposed by IEC 61508, but modified to fit to practical situations from an industrial plant. 61511 standard does not cover the design and implementation of equipment used in safety applications, such PLCs, which remains standardized by IEC 61508.

1.3 Safety Instrumented Systems Versus Control Systems

A fundamental question is whether the Safety Instrumented Systems (SIS) and Control Systems (CS) systems should be combined or a clear delimitation between these two should be established.

According ANSI/ISA 84.01 [9], *Separation between control systems and safety instrumented systems reduces the probability that at some point in time either control and safety functions to be inactive, or some modifications to the control systems will lead to changes in the functionality of the safety systems. Therefore, it is generally necessary to separate the control systems from the safety instrumented systems*.

Several basic differences between the two types of systems support the idea that control and safety should be separated. Control operations are active, dynamic, and performance-oriented. Safety operations are passive.

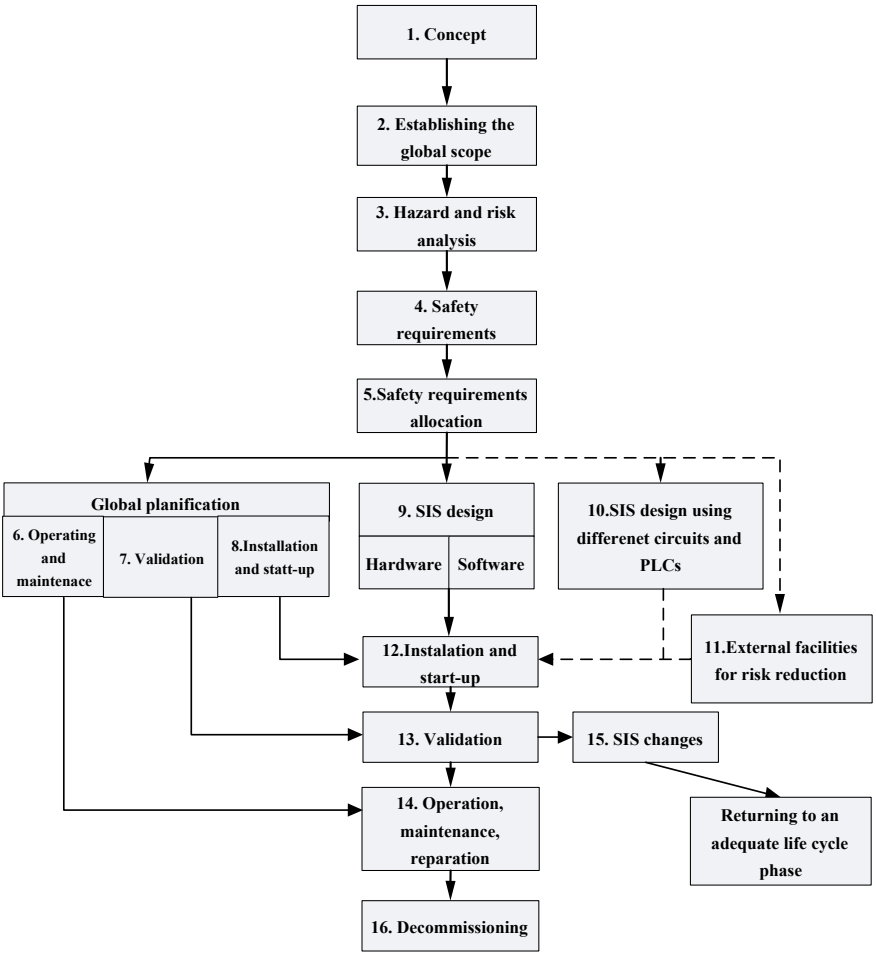

Fig. 4 Safety life cycle model according to IEC 61508 [7]

CSs act actively to maintain or change process conditions, helping to achieve the best performance of the process. They are often used to force the process to its limits, in order to obtain the required performance. They were not built to provide safety.

Since control system operation is continuous, it does not incorporate error diagnostics routines. A CS either work or not. There are no hidden defects. In these systems, operating errors are visible.

CSs are usually flexible and allow easy operation in the sense that, for example, operators can modify certain parameters or exclude certain part of the control system. This aspect has to be avoided in case of the safety systems.

Safety Instrumented Systems (SIS) are exactly the opposite of Control Systems (CS). They work only at certain times, their action must be restricted, and they must be reliable and act instantly when necessary. An example is the overPressure Safety

Valve (PSV) from Figs. 2 and 3, which must be closed as long as the pressure is below a certain value and opened when the pressure reaches a certain high limit. If the pressure never touches this limit, the valve should never open. Likewise, it may happen that this valve if stays closed for a long time, when a problem appears and must be opened, it cannot be opened. Therefore, these systems can hide defects that are not directly observed.

Because the SIS components stay for a long time in standby mode, it may not work if they must be put into operation. As such, these systems should be tested or should include techniques that provide the possibility of self-testing.

Safety instrumented systems are designed to involve human intervention as low as possible. The operator interacts with the control system. If it fails, the next step is to pass it on manually and the operator must act directly on the process. If this intervention also fails to make the necessary corrections, the last line of defence, the SIS, should work automatically and independently. The only human interference allowed is the start-up or maintenance of certain parts of the system.

2 Safety Integrity Level of a Safety Instrumented System

This paragraph describes the main methods for determining the Safety Integrity Level (SIL), which is the most important feature of a SIS.

The IEC 61508 standard defines four levels of SIL, marked with SIL1, SIL2, SIL3 and SIL4. SIL 4 denotes the highest level of safety integrity and SIL 1, the smallest. The Safety Integrity Level of a SIS can be expressed in terms of Probability of Failure on Demand (PFD) for systems/functions that operate with a low demand rate or in terms of Probability of dangerous failure Per Hour (PFH) for systems/functions that operate with a high demand rate or continuously.

There are several methods and tools for determining SIL, developed by different companies and organizations in order to provide support for assessing the process's risk and turning it into something palpable that has a certain meaning that is the required SIL level.

These methods can be grouped into four main categories: quantitative and semi-quantitative methods (e.g. LOPA—Layer of Protection Analysis), qualitative (e.g. risk matrix, risk graph) and semi-qualitative methods (e.g. calibrated risk graph).

A system risk is a function of the frequency of an unwanted dangerous event and the severity of the consequences of that event/hazard. Risk can influence personnel, production, environment etc. [10].

$$\text{RISK} = \text{FREQUENCY} \times \text{HAZARD CONSEQUENCE}$$

According to [5], hazard is an inherent feature of a system/process that has the potential to cause damage to individuals, processes or the environment.

In the case of chemical processes, hazard is the combination of a hazardous material, an operating environment with problems and some unplanned events that can cause accidents.

Depending on how the Risk Reduction Factor (RRF) is expressed, quantitatively or qualitatively, what is the scope and purpose of the risk analysis a particular type of method is chosen. Although the method used is a qualitative one, a number always quantifies the determined SIL (SIL1, SIL2, SIL3 or SIL 4).

The SIL level is a measure of the performance of the safety system and not a direct measure of process risk. The higher the risk of a process is, the higher the safety level will be and the number that follows the SIL increases as value.

Usually, the qualitative methods are used in the design phase of the SIS and the quantitative methods are used more in the SIL verification and validation phases.

2.1 Quantitative Methods

For systems with a low demand ratio, after determining the risk level, the next step is to determine, using (1), the Risk Reduction Factor (RRF) required to meet the tolerable risk level. This is achieved by dividing the number of times per year when a SIF function fail to function to the number of demands per year. The result is the acceptable number of times when a SIF may not operate at a demand per year, named the Probability of Failure on Demand (PFD) [8].

The Risk Reduction Factor (RRF), in frequency, is given by [11]:

$$RRF = \frac{F_{np}}{F_t}, \tag{1}$$

where F_{np} is the frequency of the risk without protection and F_t is the tolerable risk frequency.

The Probability of Failure on Demand (PFD) is:

$$PFD = \frac{1}{RRF} = \frac{F_t}{F_{np}}. \tag{2}$$

Further, SIL is determined using Table 1.

The Probability of Failure on Demand, PFD of a Safety Instrumented System (SIS) is obtained by summing the PFD for transducers (ZT), logic solvers (PLCs) and actuators (UZ) [3]:

$$PFD_{SSP} = PFD_{ZT} + PFD_{PLC} + PFD_{UZ}. \tag{3}$$

Also, PFD for transducers (PFD_{ZT}) is obtained by summing PFD for sensors and adapters:

Table 1 Safety integrity level and required values for the instrumented system performance in case of low demand rate system [7]

Safety integrity level, SIL	Probability of failure on demand, PFD	Availability, 1-PFD (%)	Risk reduction factor, RRF = 1/PFD
4	10^{-4} to 10^{-5}	99.99–99.999	10^4 to 10^5
3	10^{-3} to 10^{-4}	99.9–99.99	10^3 to 10^4
2	10^{-2} to 10^{-3}	99–99.9	10^2 to 10^3
1	10^{-1} to 10^{-2}	90–99	10^1 to 10^2

Table 2 Safety integrity levels (SIL) and required values for the safety system performance in case of a high demand rate/continuous operation systems [7]

Safety integrity level, SIL	Probability of failures per hour, PFH	Mean time to failure, MTTF
4	10^{-9} to 10^{-8}	10^4 to 10^5
3	10^{-8} to 10^{-7}	10^3 to 10^4
2	10^{-7} to 10^{-6}	10^2 to 10^3
1	10^{-6} to 10^{-5}	10^1 to 10^2

$$PFD_{ZT} = PFD_{adaptor} + PFD_{sensor}, \tag{4}$$

and the PFD for actuators (PFD_{UZ}) is obtained by summing the PFD for electromagnetic valve UZY and the safety valve UZV:

$$PFD_{UZ} = PFD_{UZT} + PFD_{UZV}. \tag{5}$$

For systems with a high demand ratio or continuous operation, the Safety Integrity Level (SIL) is determined using the Probability of a hazardous Failure per Hour (PFH) or the Mean Time To Failure indicator (MTTF), according to Table 2.

The two measures (PFD and PFH) of the SIS performance are related, the dependence between them being expressed through equation [12]:

$$PFD = \frac{T}{2} \cdot PFH = \frac{T}{2 \cdot MTTF}. \tag{6}$$

PFD is the Probability of Failure on Demand, T represents the test or replacement interval, PFH Probability of a dangerous Failure per Hour and MTTF is the Mean Time To Failure.

2.2 Risk Matrix

The risk matrix is one of the most popular method for determining the Safety Integrity Level (SIL), due to its simplicity. The risk matrix takes into account the frequency and severity of an unwanted event, based on a classification of the risk parameters.

The frequency of an event to occur can be quantified in terms such Small (S), Medium (M), High (H) or any other suggestive terms, Table 3.

Consequences and its severity can be quantified based on various risk factors such personnel, environment, production, equipment, capital, etc.

Table 4 provides an example of the severity of risk values, associated with personnel, environment and production.

Table 3 Risk frequency values [13]

Level	Frequency	Qualitative interpretation
3	High (H)	An unwanted event may occur more than once in the predicted life time of the plant
2	Medium (M)	An unwanted event can occur once in the predicted life time of the plant
1	Small (S)	An unwanted event may appear with a low probability over the predicted life time of the plant

Table 4 Example of severity values/risk consequences [13]

Level	Severity/consequences	Personnel	Environment	Production/equipment
III	Catastrophic (C)	More fatalities	Escapes of dangerous substances outside the plant perimeter	Losses greater than $1,500,000
II	Serious (S)	Single death or injuries requiring recovery time	Releases of non-hazardous substances outside the perimeter of the plant or leakage of dangerous substances into the perimeter of the plant	Losses between 100,000 $ and 1,500,000 $
I	MINor (MIN)	Injured that requires medical treatment or first aid	Releases of hazardous substances to a restricted area of the plant perimeter or without leakage	Losses up to $100,000

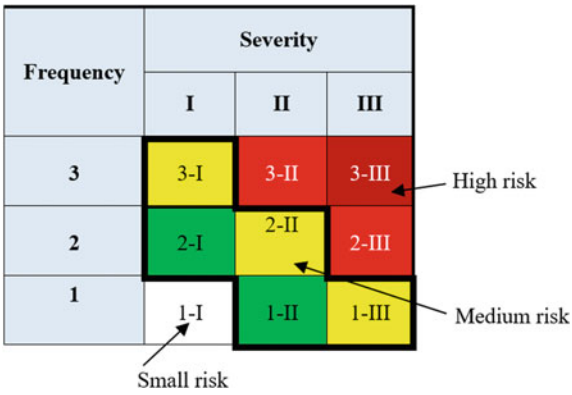

Fig. 5 Global risk (risk matrix)

According to Table 4, the consequences may be MINOR (MIN), SERIOUS (S) or Catastrophic (C), according to severity level. Categories can be selected either qualitatively or quantitatively by attaching some economic figures, deaths, etc.

By joining the values of the two properties, the frequency and severity of the risk, the risk matrix is obtained (Fig. 5).

If the identified risk is high, then changes are recommended. If the identified risk is medium, it is necessary to add additional safety levels. If the identified risk is low, no changes or additions of protection levels are required.

Given that, if each risk matrix cell has an associated SIL level, then the process of determining the SIL level is simple [13].

Figure 6 shows a typical modified risk matrix chart for determining the SIL level.

Severity-minor consequence (I), low frequency (1) leads to unnecessary SIL. This means that the risk is considered tolerable.

Severity-minor consequence (I), average frequency leads (2) to a low SIL level, while catastrophic consequence, high frequency leads to a high SIL level. In case of a SIL 3 or SIL 4 required level, additional studies should be conducted as a single SIF may not provide sufficient risk reduction [14].

Fig. 6 The modified risk matrix for determining the SIL level

Frequency	Severity		
	I	II	III
3	SIL 2	SIL 3	SIL 4
2	SIL 1	SIL 2	SIL 3
1	No SIL	SIL 1	SIL 2

Sometimes, due to the assessments that need to be made, the result may be unrealistic. Therefore, it is recommended to use other tools and methods in conjunction with this method in order to improve the quality of the determination [8].

The risk matrix has two dimensions, the frequency and severity of an event. Sometimes, in practical applications, there is also added a third dimension that takes into account additional safety levels, resulting the risk matrix of safety and protection levels.

2.3 Risk Graph

The method of determining the Safety Integrity Level (SIL) using the risk graph is based on the methods written in the German publication DIN 19250 [15].

Table 5 lists the risk parameters classification suggested in IEC 61511.

The risk graph method is a qualitative method that takes into account the consequence and frequency of a dangerous event, but also the likelihood that the personnel could avoid the danger [14].

For the Consequence parameter (C), in relation to personnel's risk, four categories of consequences are suggested, ranging from minor injury to multiple deaths. C1 is the least severe category. In general, the consequences are measured by the degree of injuries of individuals but also by environmental or financial measures [8].

Occupancy Frequency (F) shows the fraction of time in which the hazardous area is occupied by personnel. F2 shows a higher risk than F1 because the area is occupied more frequently. Usually, in accordance with IEC 61511, F1 can be selected if the hazardous area is occupied less than about 10% of the time.

Table 5 Risk parameters classification according to IEC 61511

Risk parameter	Notation	Classification
Consequence (C)	C_1	Minor injuries
	C_2	Serious injury of one or more persons
	C_3	Death of one person
	C_4	Catastrophic effect. Many deaths
Occupation frequency of the affected area (F)	F_1	Rare to frequent (<0.1)
	F_2	Frequent to continuous (>0.1)
The probability of avoiding the consequences (P)	P_1	Possible in certain conditions (>90%)
	P_2	Almost impossible (<10%)
The probability of occurrence of an unwanted event (A)	A_1	Very unlikely to appear (F < 0.01/year)
	A_2	It is unlikely that an unwanted event will appear (F > 0.01/year)
	A_3	Relatively large probability that an unwanted event to appear (F > 0.1/year)

The possibility of personnel to avoiding the danger is incorporated into parameter P. This parameter shows which methods must be identified by personnel in order to escape the danger. Additionally, the rate of development of the dangerous event is taken into account. Two categories are suggested, P1 and P2, P2 indicating the highest risk. In order to select P1, a list of statements must be validated. Such lists of statements are suggested in IEC 61511.

The final parameter is the probability of occurrence (A), which is the frequency of the occurrence of an unwanted event without SIF (Safety Instrumented Function).

Figure 7 is a typical chart of personnel risk. Similar graphs can be obtained for the risk associated with equipment, production losses or environmental impact.

The path from left to right is determined by the selected risk parameter values. The selected result, the occupancy frequency and the probability of avoidance leads to a certain output line, O. The output line leads to three values of the parameter A. Choosing the parameter A is the last step in determining the SIL level. Choosing a higher A parameter results in a higher SIL level [14].

If the probable consequence is assessed to be serious injury to one or more persons, C2 is selected. If the area could be exposed to personnel rarely to more frequent, F1 is chosen. It is possible that under certain conditions the unwanted events can be avoided, which means that parameter P1 should be chosen. The combination of these risk parameters leads to the O2 output line. Considering a high probability that an unwanted event to occur, A3 is selected. According to Fig. 7, SIL 1 is required.

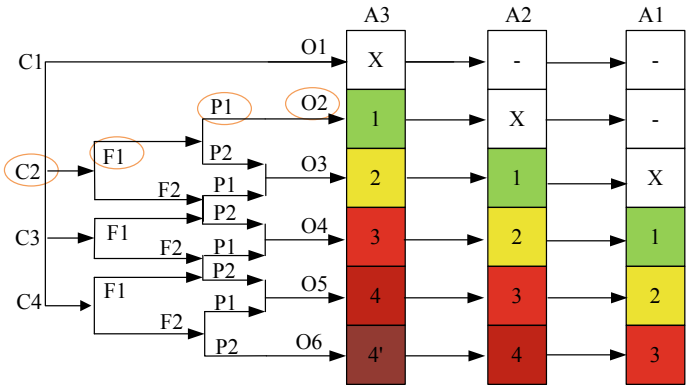

Fig. 7 Risk graph: C—consequences (C1—minor injuries, C2—serious injuries, C3—one death, C4—more deaths); F—frequency (F1—rare to frequent, F2—frequent to continuous); P—probability of avoidance (P1—sometimes possible, P2—almost impossible); A—appearance probability (A1—very small, A2—small, A3—relatively high); X—SIS is not necessary, 1, 2, 3, 4—safety integrity level, SIL, 4′—one SIS is not enough

3 Practical Aspects Regarding Safety Instrumented Systems

This paragraph outlines some general aspects regarding SIS implementation by listing the main requirements of the components, the available implementation technologies and ways to connect them.

The performance of a SIS depends on each element from its structure (sensor, logic solver or actuator), so a special attention must be given starting from the stage of choosing the type of each sensor and actuator to be used, to the implementation of the logic solver phase or to the way that these parts are interconnected.

The field devices that are parts of the Safety Instrumented Systems (SIS) must be selected and installed to meet the performance requirements expressed through the Safety Integrity Level (SIL), for each SIF (Safety Instrumented Function).

Any SIS associated field device must be separate and independent of those of the control system. With few exceptions, sharing equipment with the control system can cause procedural and maintenance problems.

In order to achieve the necessary independence, the following components should be separated from the control system [16]:

- the field sensors, safety and electromagnetic valves, pulse lines;
- wires, panels and junction boxes;
- voltage sources.

If the SIS signals are to be sent to the control system for comparison, the signals between the two systems should be isolated (using optical insulators) to prevent that one single failure affecting both systems.

The SIS field devices should be fail safe. In most cases, this means that the devices are normally energized. De-energizing or losing power will initiate the unit/plant shutdown.

Systems where the shutdown function is activated in the case of alarms are used to reduce false errors due to power failures.

Only tested technologies should be used in safety applications.

When installing sensors, the following general requirements must be considered [17]:

- contacts must be normally closed and normally energized;
- sensors must be directly connected to the logic system;
- smart transducers are more commonly used for SIS due to improved diagnostics facilities and rigorous reliability. When using such transducers, procedures should be established to ensure that they cannot be left in forced outputs;
- the contacts of the electric circuit should be hermetically sealed for greater reliability;
- the SIS associated field sensors should be differentiated in a certain way by the sensors of the control system by a single tag, numbering or colour;
- when using redundant sensors, a discrepancy alarm should be provided to indicate the failure of a single sensor.

In case of flow measurement, although diaphragm transducers are primarily used in most safety applications, the vortex and magnetic flow transducers can offer some advantages such ease of installation and improved performance.

In the case of temperature sensors, the main failure mode of thermocouples is burning; therefore, detection and alarm systems should be used.

In the case of pressure sensors, the main precautions to be taken are when selecting the range and that the condensate accumulation will not cause calibration problems.

Level transducers with air blowers and nitrogen purge have proven to be reliable, requiring low maintenance.

When installing actuators, they should be set to maintain their status after a shut-down function, until manual reset. They should be allowed to return to their normal state only if the variables that generated the stop have returned to their normal operating values.

The following aspects should be considered when selecting the actuators:

– closing/opening speed;
– leaks;
– fire resistance;
– suitability/compatibility of the material;
– diagnostic requirements;
– the safety of the valve;
– the need for a position indicator or limiter;
– on-line maintenance capacity.

The bypass valves must be considered for each safety valve that fails in the closed state. Limiters can be used to initiate an alarm if a bypass valve is opened.

Generally, safety valves should be dedicated to safety applications and separate from the control valves.

Electromagnetic valves have a low reliability and therefore can be one of the most critical (weaker) components in the whole system. A common cause of the failure is burning the coil causing a false stop. It is important to use a tap like to withstand high temperatures, including heat generated by its own coil, heat generated by furnaces, exposure to sunlight, etc. Double ball valves or redundant valves can also be used.

24 V powered electromagnetic valves seem to be more reliable due to low energy consumption and low heat output.

When installing a field equipment, consideration should be given to issues related to:

– environment (temperature, vibration, shock, corrosion, humidity etc.);
– on-line testing, if necessary;
– maintenance requirements;
– accessibility;
– local indication;
– protection against frost, if required.

Common wiring defects include grounding, noise and induced voltages.

General recommendations to minimize connection issues:

– each field device must have its own set of connections to the logic system;
– it is not recommended to connect multiple discrete inputs to a single input channel of a logic system, in order to reduce the number of wires and the expenses related to the input modules. A disadvantage of such an arrangement is that it will be much more difficult to troubleshoot and diagnose problems.
– it is also not advisable to connect a single logic solver output to multiple valves;
– each input and output field variable must be limited to the electric current; This can be done either as an integral part of the input/output modules of the logic element or by using external fuses;
– SIS wiring and junction boxes must be delimited from all other instruments and/or wiring of the control system;
– all equipment, wires etc. must be clearly labelled.

4 IT Enabled Safety Systems

Information Technology (IT) is a technology that has the fastest rate of development and application in all areas of different industrial fields and requires adequate protection in order to provide high security. The goal of the safety analysis for an IT system is to identify the main threats, vulnerabilities and safety features in order to protect the information stored electronically with implications regarding data integrity, availability and confidentiality [18].

As the complexity of different type of projects increased, the advances in information technology and data acquisition equipment and tools, offered the possibility to significantly increase the ability to store, retrieve, transmit and manipulate data and information during the entire steps of a project, Fig. 8. A precise real-time control of the equipment, materials, construction methods and work environment is needed in order to ensure the safety risk prevention and emergency response [19].

IT can reduce the errors rate in three ways: by preventing the main errors, by offering a rapid response after an unwanted dangerous event has occurred and by tracking and providing feedback about that event. The main methods for preventing errors and dangerous events appearance are based on tools that can improve communication, make information more accessible, assist with calculations, perform real time checks, provide monitoring and decision support.

In order to minimize losses, it is necessary to use risk management and risk assessment concepts regarding the area of the information technology [20].

The IT enabled systems risk management consists of analysis, planning, implementation, control and monitoring of implemented measurements. Using risk management the risk level is identified and measures to reduce risk are taken in order to maintain the risk on an acceptable level.

The IT enabled systems security modules are grouped into generic aspects (organization, personnel and data backup policy), infrastructure (buildings, server room