ELECTRONIC
VISION

On the concept of safety instrumented systems

Luis Efrén Barrero Páez[*]
Andrés Escobar Díaz[**]
Harold Vacca González[***]

submitted date: October 2013
received date: Noviembre 2013
accepted date: February 2014

Abstract

This paper presents a concrete definition of what a Safety Instrumented System (SIS) is. This involves important concepts such as risk, safety integrity level, SIL, life cycle and protection layer. The aim of this paper is to provide readers with a concise definition of SIS. To this end, the basic elements of a SIS are defined, the relationship of risk with a SIS is presented, layers of protection are defined in a industrial process, the implementation of a SIS is justified, and the correct methodology for the implementation of a SIS is obtained, namely Lifecycle. Finally, the paper describes a mathematical method for modeling and validating a particular SIS based on standards.

Key words

Safety Instrumented System, SIS, Risk, safety integrity level, SIL, Lifecycle, Protection layer

[*] B.Sc. In Electronic Engineering, Universidad Distrital Francisco José de Caldas, Bogotá (Colombia). M.Sc. In Engineering and MBA, Universidad de Los Andes (Colombia).Current position: Professor at Universidad San Buenaventura, (Colombia). E-mail: lui-barr@uniandes.edu.co.

[**] B.Sc. In Electronic Engineering, Universidad Distrital Francisco José de Caldas, Bogotá (Colombia). M.Sc. In Engineering and MBA, Universidad de Los Andes (Colombia). Current position: Professor at Universidad Distrital Francisco José de Caldas, Bogotá (Colombia). E-mail: aescobard@udistrital.edu.co

[***] B.Sc. In Mathematics, Universidad Distrital Francisco José de Caldas, Bogotá (Colombia). M.Sc. In applied mathematics, Universidad EAFIT (Colombia). Current position: Professor at Universidad Distrital Francisco José de Caldas, Bogotá (Colombia). E-mail: hvacca@udistrital.edu.co

1. Introduction

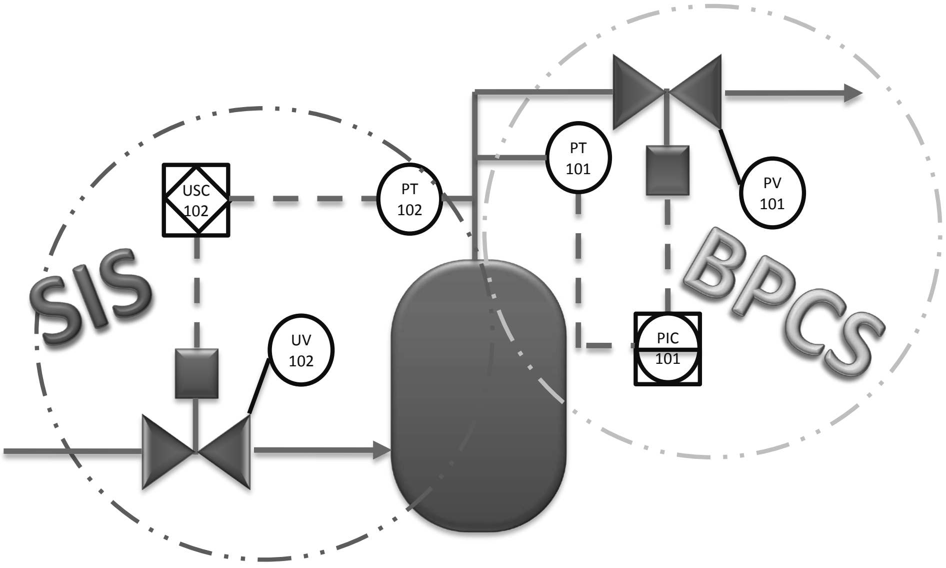
A Safety Instrumented System (SIS) is an engineering concept that redefines security structure in industrial processes. This concept involves a broader study of plants, processes, systems security, systems of measurement and control. A SIS arises from the need to handle dangerous conditions that emerge in plants, where the main purpose is to quantify and reduce the risk so as to take it to acceptable levels. The present paper is intended to define SIS and present the most relevant concepts related to it.

Section 2 of this paper presents the basic elements of a SIS. The third section shows how risk and SIS are related. Additionally, a presentation of the layers of protection is made. Section 4 explains the rationale behind the implementation of a SIS, the Section 5 illustrates the design methodology. Finally, the paper introduces the so called Lifecycle as well as the associated mathematical model.

2. Elements of a SIS

A SIS consists of the following instruments: sensors, controls and actuators, which are used in order to make the plant reach specific safety standards (a safety state) whenever the operating conditions of the plant lead to hazardous environments or to certain risk. A SIS is recommended to be separated from the Basic Process Control System (BPCS). This condition allows separating features for process requirements and safety, and also facilitates the diagnosis and maintenance for each of the systems (see Fig 1). BPCS is an active system that meets regulatory tasks of the process. A SIS is passive and is intended for long periods of time without taking any action, but it must be prepared to act whenever necessary. For these reasons, such a system should be monitored and maintained regularly.

Figure 1. SIS vs BPCS



Source: [1].

3. Risk

A SIS has three basic elements, namely a processing system, actuators and sensors. This set of elements defines the safety integrity level (SIL) (see Figure 2). SIL is associated with a probability of dangerous failure of the system, and it can be determined after conducting a risk analysis. Risk is a measurement of the likelihood and severity of an event, in this case unwanted. These measurements address questions like: what are the consequences of the event? How frequent the event might be?

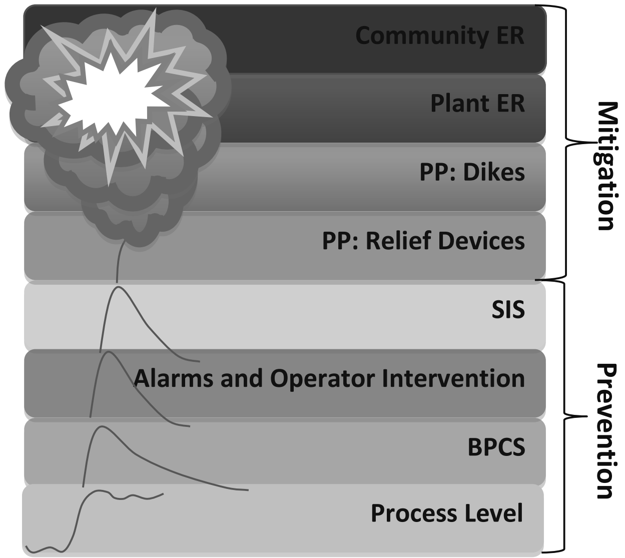
Figure 2. Safety Integrity Level (SIL)

Safety Integrity Level	Probability of dangerous failure	Risk reduction factor
SIL 4	0.0001-0.00001	100000 to 10000
SIL 3	0.001-0.0001	10000 to 1000
SIL 2	0.01-0.001	1000 to 100
SIL 1	0.1-0.01	100 to 10

Source: own elaboration

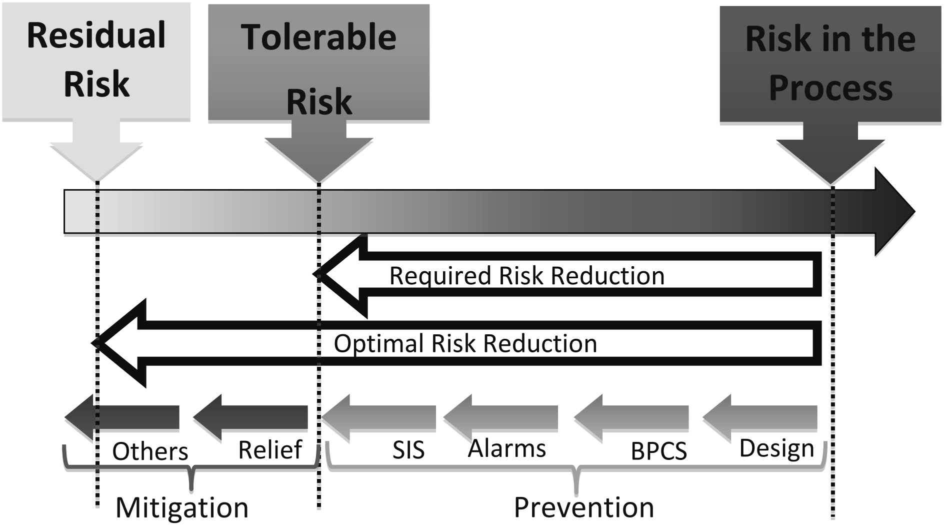
The risk in an industrial process decreases by implementing protective layers (Figures 3 and 4). All process or plants involve a risk. Companies are responsible for determining their acceptable levels of risk. Protective layers are divided according to two aspects: prevention and mitigation. When certain hazardous conditions are associated to a process, prevention layers lead the process to normal condition. Mitigation layers only act when a disaster has already occurred, and so are intended to try to reduce its impact.

Figure 3. Protective layers, ER: Emergency Response, PP: Physical Protection



Source: [2].

Figure 4. Decreased Risk



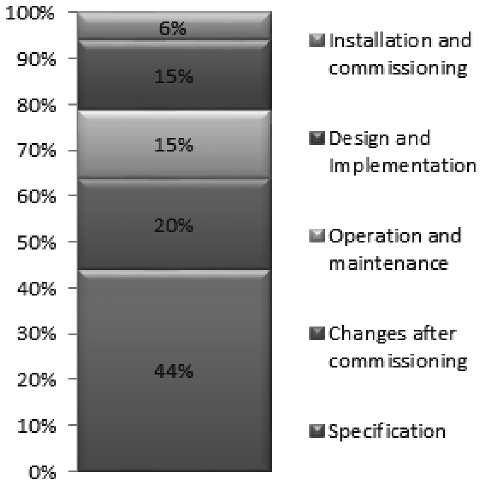
Source: [3].

In this context, SIL establishes a probability of failure, determined through risk analysis for a system with a SIS. In the ISA S84.01 standard SIL is defined as a set of discrete levels of security based on the probability of dangerous failure of a given system (Figure 4). In practice, for implementation, SIL systems 1 and 2 are actually achievable; SIL systems 3 and 4 are difficult or impossible to achieve due to the small failure probabilities. Thus, a SIS helps to reduce risk and therefore represents a layer of prevention within an industrial process.

4. The rationale behind SIS

There are various reasons to justify the existence of SIS, [4]. For example, the oil industry lost nearly $2 trillion by accident in the early 90's [5]. In other words, not having a SIS is more expensive than acquiring a new one. The actual causes of accidents are attributed, in 44% of the cases, to a bad design and poor specifications made in systems; on the other hand, 20% is attributed to changes that are not recorded after the start of a process (Figure 5).

Figure 5. Cause of accident



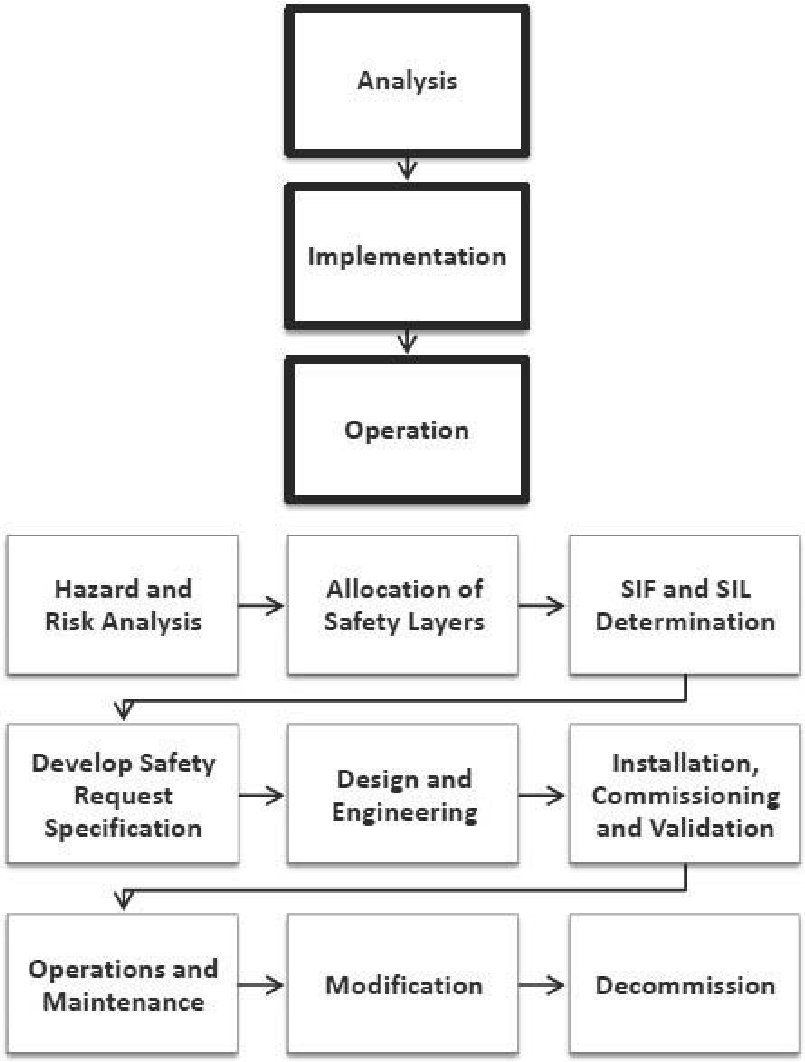
Source: [6].

From the point of view of a cost-benefit analysis, the cost of implementing a SIS is much lower than losing human lives, causing damage to the environment, paying liability costs, reducing production, or doing harm to equipment, infrastructure and ultimately to the image of a company.

5. Life cycle

Finally, the implementation of a SIS must follow various steps, namely the lifecycle design [7] (Figure 6). If the methodology is followed, it guarantees that: SIS Reduces costs, increases process safety, ensures compliance with regulations and provides an example of good engineering practice. The methodology has three stages: Analysis, Implementation and Operation. These stages describe the activities necessary for the completion of a SIS; from conception to the complete deployment of the system.

Figure 6. Life cycle of a SIS


Analysis
Implementation
Operation
Hazard and Risk Analysis
Allocation of Safety Layers
SIF and SIL Determination
Develop Safety Request Specification
Design and Engineering
Installation, Commissioning and Validation
Operations and Maintenance
Modification
Decommission

Source: [5].

6. Mathematical Model

To the best of our knowledge, very few works exist in the literature that address control algorithm development and validation for **SIS** based on a mathematical method.

Recently, [8] described a mathematical method for modeling and validating SIS based on IEC standards. Such an approach considered diagnosis and treatment for each safety instrumented function (SIF) including hazard and operability (HAZOP) studies on the equipment or system under control. For modeling critical-fault diagnosis, Bayesian networks (BN) and Behavioral Petri nets (BPN) are suggested. For modeling critical-fault treatment, interpreted Petri nets (PN) are suggested, since this approach is based on the behavior of dynamic systems, as oriented by occurrence of discrete events, according to discrete event dynamic systems (DEDS). Additionally, coordination modeling is used to link each treatment model to a corresponding diagnostic model. Also, for these coordination models, interpreted Petri nets are suggested. The mathematical model generated will allow the validation of the control algorithm by providing a computational resource that ensures compliance with the SIL specifications according to IEC 61508. Finally, these models can be translated into any language defined by IEC 61131-3, in accordance to standard IEC 61511 (IEC, 2003a), and implemented using Safety Programmable Logic Controllers (PLC), as a layer of risk reduction separated from Basic Process Control Systems (BPCS).

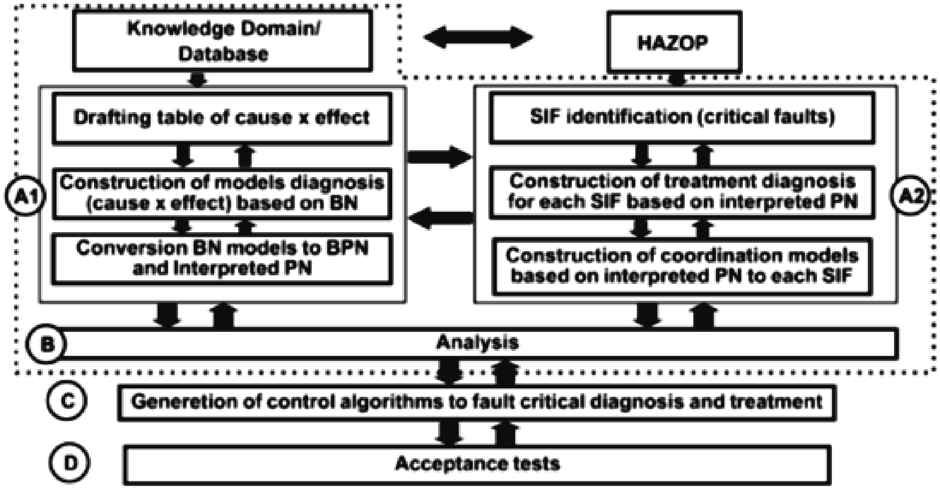
First, a Bayesian network is a structure that graphically models relationships of probabilistic dependence of cause-effect, considering a group of variables. The BN provides a method of reasoning used to represent partial beliefs under conditions of uncertainty. The construction of a structured Bayesian Network can be accomplished from either a database obtained from a process, or from domain knowledge. In the last decade, many Bayesian-network structured-learning algorithms have been developed. These algorithms generally fall into two groups, namely search- & scoring-based algorithms and dependency analysis-based algorithms.

Second, the PN, considered as a tool that allows a graphical and mathematical description of the system, is a communication tool among people related with the project, interpretation and clear identification of the states and actions. PN can represent processes with synchronism, concurrency, causality, conflict, and those that share resources and normal situations in productive systems (PS). The mathematical support of PN is useful for performing the formal tests of the dynamic properties of the system. This is especially useful in applications in which security is a relevant factor.

Third, a BPN is an ordinary PN with an additional OR-transition intended to model fault propagation among multiple paths by considering a set of observations about a process. BPN is a type of PN that models a diagnostic process since no cyclic process has to be represented. In this context, the process of a Bayesian network (BN) can be represented through a BPN. If two effects are independent of a cause based on database, then an OR-transition is considered, but if the two effects are dependent (i.e. both effects take place when a cause is present), then the AND transition is considered.

Figure 7 shows the mathematical method for modeling and validating control algorithms for SIS design based on BN, BPN and PN, [8].

Figure 7. Mathematical method for critical fault diagnosis and treatment in SIS design


Knowledge Domain/ Database
HAZOP
Drafting table of cause x effect
SIF identification (critical faults)
A1
Construction of models diagnosis (cause x effect) based on BN
Construction of treatment diagnosis for each SIF based on interpreted PN
A2
Conversion BN models to BPN and Interpreted PN
Construction of coordination models based on interpreted PN to each SIF
B
Analysis
C
Generetion of control algorithms to fault critical diagnosis and treatment
D
Acceptance tests

Source: [8]

The method defines four steps, namely (A) modeling, (B) analysis, (C) generation of control algorithms and (D) acceptance tests. The modeling step is divided into two complementary stages: (A1) critical fault diagnosis and (A2) critical fault treatment and coordination. Step (B) (i.e. analysis) is performed to both verify if some PN properties for critical fault diagnosis, treatment and coordination integrated models are met, and validate integrated models in compliance with specifications. Liveness, safety, conservativeness and reachability properties should be verified for SIS applications. Step (C) (i.e. generation of control algorithms) is performed to convert verified models into a language recommended by standard IEC 61131-3 (IEC, 2003b) and accepted by IEC 61511 (IEC, 2003a) for implementation in a Safety PLC. Finally, Step (D) (i.e. acceptance tests) is performed in accordance to IEC 61511 in order to validate whether a control algorithm for each SIF complies with the specifications.

7. Conclusions

This document provided specific and general concepts, terms, relevance and methodologies associated to a SIS. This paper will motivate readers to get involved and deepen their understanding of these topics, especially when addressing control-algorithm development and validation for SIS based on mathematical models for the study of these systems.

Reference

[1] K. J. Mitchell , P. Hereña, T. M, *“Safety Instrumented Systems Engineering Handbook”*, 2010.

[2] D. Hatch T., "*Intech, Operatorsonalert, ISA*", 2009.

[3] Standard IEC 61511. 2003.

[4] P. Ghrun, H.L. Cheddie, *“Safety Instrumented Systems. DesignAnalysis, and Justification”*, 2005..

[5] Oil & Gas Journal. 2001.

[6] “Out of control: Why control systems go wrong and how to prevent failure”, UK HSE, Página 31.

[7] ISA84,IEC61508, IEC61511.

[8] R. Squillante, D. dos Santos Filho, L. A. Riascos, F. Junqueira, P. Miyagi, "*Mathematical method for modeling and validating of safety instrumented system designed according to IEC61508 and IEC 61511*". Available in: http://www.abcm.org.br/pt/wp-content/symposiumseries/SSM_Vol5/Section_II_Control_Systems/24332.pdf.