Reliability Engineering and System Safety 134 (2015) 32–50

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Safety and operational integrity evaluation and design optimization of safety instrumented systems

Fares Innal [a,*,1], Yves Dutuit [b], Mourad Chebila [a]

[a] Batna University, IHSI-LRPI, avenue Chahid Mohamed Boukhlouf, 05000 Batna, Algeria
[b] TOTAL Professeurs Associés, 38, rue du Prieuré, 33170 Gradignan, France

ARTICLE INFO

Article history:
Received 15 September 2013
Received in revised form
26 September 2014
Accepted 2 October 2014
Available online 13 October 2014

Keywords:
Safety instrumented system (SIS)
KooN architectures
Safety integrity
Operational integrity
SIS optimization
Genetic algorithms (GA)

ABSTRACT

The control of risks generated by modern industrial facilities could not be guaranteed without the use of safety instrumented systems (SIS). The failure of SIS to achieve their assigned functions could result in huge consequences with respect to both (i) the safety of the monitored system (relating to the SIS safety integrity) as well as (ii) its production availability due to false trips (relating to the SIS operational integrity). Furthermore, these two aspects are usually antagonistic. Therefore, the assurance of this double performance comes first by a thoughtful design of SIS. In that case, the aim of this paper is twofold. First, it focuses on the establishment of generic analytical formulations allowing the assessment of the SIS performance regarding safety integrity and operational integrity. Second, it deals with SIS architecture design optimization. The optimization problem is firstly addressed by a preliminary search for a balance between the above two quantities relying on the analysis of the structure of *KooN* architectures. Then, a more general and suitable approach based on genetic algorithms is proposed, where several performance indicators and the costs of purchase and maintenance are expected to be considered simultaneously. This general approach is illustrated through an application example.

1. Introduction

Since the publication of the IEC 61508 standard devoted to functional safety [1] and its related sector based standards, such as the IEC 61511 for process safety [2], the interest in using certified safety instrumented systems (SIS) has considerably increased. These systems are usually the first layer of protection called upon to control potentially hazardous deviations of the monitored process, i.e. the equipment under control (EUC), and therefore to put it in a safe state. In general, a SIS is made up of the following three subsystems:

S (sensor): this is made up of a set of input elements (sensors, detectors, transmitters, etc.) which monitor the evolution of the parameters representing the process behaviour (temperature, pressure, flow, level, etc.). If at least one of these parameters exceeds a threshold level and remains there, this deviation constitutes the demand or solicitation emanating from the EUC.

LS (logic solver): includes a set of logic elements (e.g. Programmable Logic Controller or PLC) that collect information from the *S* subsystem and carries out the decision making process that may eventually end by activating the third subsystem.

FE (final element): this subsystem acts directly (emergency shutdown valves) or indirectly (solenoid valves, alarms) on the process in order to neutralize its deviation by generally putting it in a safe state, within a specified time which must be identified for each safety function.

The quantitative (probabilistic) evaluation of SIS performance is a paramount step for their validation as specified in the IEC 61508 standard. This validation is none other than the assurance that they can properly perform their assigned safety functions. The ability of SIS to meet a given safety target (tolerable risk level) is called "safety integrity", which is measured differently depending on the SIS modes of operation:

– Average probability of failure on demand (PFD_{avg}) for the "low demand" mode. This mode is typical for safety systems which are activated only on exceeding a threshold value (process upset).
– Probability of dangerous failure per hour (*PFH*) for the "high or continuous demand" mode. This mode of operation is typical of

Abbreviations: BPCS, basic process control system; CCF, common cause failures; DC, diagnostic coverage; EUC, equipment under control; FE, final element subsystem; GA, genetic algorithm; IEC, International Electrotechnical Commission; KooN, K out-of N; LOPA, layer of protection analysis; LS, logic solver subsystem; MDT, mean down time; MOP, multi-objective optimization problem; MRT, mean repair time; MT, mission time; MTTR, mean time to restoration; PFD, probability of failure on demand; PFH, probability of failure per hour; PFS, probability of failing safely; S, sensors subsystem; SIL, safety integrity level; SIS, safety instrumented system; STR, spurious trip rate; SOP, single-objective optimization problem

* Corresponding author. Tel.: +213 669290488.
E-mail address: innal.fares@hotmail.fr (F. Innal).
[1] Present address: Cité El Annabet, Béni-Béchir, Skikda 21000, Algeria.

http://dx.doi.org/10.1016/j.ress.2014.10.001
0951-8320/

Nomenclature

A_n^k	number of arrangements of size k from a set with n elements
C_n^k	number of combinations of size k from a set with n elements
C_P	purchase cost
C_P^{SIS}	SIS purchase cost
C_P^{max}	maximum allowed SIS purchase cost
C_T	proof tests cost
C_T^{SIS}	SIS proof tests cost
C_T^{max}	maximum allowed SIS proof tests cost
I_{Bi}	ith component Birnbaum importance factor
DC	diagnostic coverage for dangerous failures
DC_S	diagnostic coverage for safe failures
MDT_{KooN}	mean down time for $KooN$ architecture due to independent dangerous failures
MDT_{sd}	mean down time consecutive to a shutdown
$MDTS_{1ooi}$	mean down time for 1ooi architecture due to independent safe failures
$MTTR$	mean time to restoration for DD failures
$MTTR_S$	mean time to restoration for SD failures
MRT	mean repair time for DU failures
MRT_S	mean repair time for SU failures
PFD_{avg}	average probability of failure on demand
PFD_{avg}^{SIS}	SIS average PFD
PFD_{avg}^{max}	maximum allowed value for PFD_{avg}^{SIS}
PFD_{KooN}	PFD for $KooN$ architecture
PFD_{KooN}^{ind}	independent PFD for $KooN$ architecture
PFD_{KooN}^{CCF}	dependent PFD for $KooN$ architecture (CCF contribution)
PFH_{SIS}	SIS probability of dangerous failure per hour (average)
PFH_{max}	maximum allowed value for PFH_{SIS}
PFH_{KooN}	PFH for $KooN$ architecture
PFH_{KooN}^{ind}	independent PFH for $KooN$ architecture
PFH_{KooN}^{CCF}	dependent PFH for $KooN$ architecture (CCF contribution)
PFS_{avg}	average probability of failing safely
PFS_{KooN}	PFS for $KooN$ architecture
PFS_{KooN}^{ind}	independent PFS for $KooN$ architecture
PFS_{KooN}^{CCF}	dependent PFS for $KooN$ architecture (CCF contribution)
STR_{SIS}	SIS spurious trip rate (average)
STR_{max}	maximum allowed value for STR_{SIS}
STR_{KooN}	STR for $KooN$ architecture
STR_{KooN}^{ind}	independent STR for $KooN$ architecture
STR_{KooN}^{CCF}	dependent STR for $KooN$ architecture (CCF contribution)
STR_{KooN}^{DDind}	STR for $KooN$ architecture due to independent DD failures
STR_{KooN}^{DD}	STR for $KooN$ architecture due to DD failures
T_1	proof tests interval
w_{acc}	average accident frequency
w_i	ith component failure frequency
w_{IE}	initiation event frequency
w_S	system unconditional failure intensity (failure frequency)
w_t	tolerable frequency
x_i	ith decision variable
β	CCF proportion (β factor)
$\beta_{DU}(=\beta)$	β for dangerous undetected (DU) failures
$\beta_{DD}(=\beta_D)$	β for dangerous detected (DD) failures
β_{SD}	β for safe detected (SD) failures
β_{SU}	β for safe undetected (SU) failures
λ_D	dangerous failure rate
λ_{Dind}	independent dangerous failure rate
λ_{DCCF}	dependent dangerous failure rate (CCF)
λ_{DD}	DD failure rate
λ_{DDind}	independent DD failure rate
λ_{DDCCF}	dependent DD failure rate
λ_{DU}	DU failure rate
λ_{DUind}	independent DU failure rate
λ_{DUCCF}	dependent DU failure rate
λ_S	safe failure rate
λ_{Sind}	independent safe failure rate
λ_{SCCF}	dependent safe failure rate (CCF)
λ_{SD}	SD failure rate
λ_{SDind}	independent SD failure rate
λ_{SDCCF}	dependent SD failure rate
λ_{SU}	SU failure rate
λ_{SUind}	independent SU failure rate
λ_{SUCCF}	dependent SU failure rate

safety systems that have a permanent or regular operation (e.g. the basic process control system: BPCS).

Regarding the *PFH* concept, the first named authors of this paper have shown that it is the average failure frequency of the SIS. Also, they have conducted a detailed discussion on the aforementioned modes of operation [3,4].

In order to specify the requirements for a given SIS regarding the safety target, the IEC 61508 standard adopts the concept of safety integrity level (SIL) which is therefore a measure of the confidence with which the SIS can be expected to perform its intended safety function [5]. Table 1 shows the relationship between the above probabilistic performance (PFD_{avg} or PFH) and the SIL concept.

In addition to the requirements specified in the IEC 61508 standard, aiming to meet safety objectives (safety integrity), it is necessary to take into account any perturbation due to SIS failures on the nominal operation of the EUC (even though it is safe). These disturbances are usually caused by nuisance tripping (false trip, spurious trip, spurious activation) of the SIS which result in production loss and thus are economically prejudicial, and potentially dangerous [6]. For instance see Ref. [7] for a detailed definition and discussion of terms and concepts related to spurious activation of a

Table 1
Safety integrity levels (SIL) according to PFD_{avg} and PFH.

SIL	PFD_{avg}	PFH (h^{-1})
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$