Proceeding Paper

Multiobjective Optimization of the Performance of Safety Systems †

Boukrouma Houcem Eddine [1,*] , **Bendib Riad** [2] , **Zennir Youcef** [2] and **Mechhoud El-Arkam** [2]

1 Research Laboratory on Surface and Interface Physics and Chemistry LRPCSI,
Université 20 Août 1955 Skikda, Skikda 21000, Algeria
2 Automatic Laboratory of Skikda, Université 20 Août 1955 Skikda, Skikda 21000, Algeria
* Correspondence: hd.boukrouma@univ-skikda.dz
† Presented at the 2nd International Conference on Computational Engineering and Intelligent Systems, Online, 18–20 November 2022.

Abstract: The activation of the safety-instrumented systems in industrial processes is carried out after the occurrence of specific deviations (dangerous situations) from normal operation (normal situations), but in some cases, the safety-instrumented systems are activated in the absence of deviations or requests; these are the unwanted activations. The system chosen in this study is a system with high-pressure gas and inflammable gas, and it is protected by a firefighting system that prevents any kind of accident in order to protect humans, systems, and the environment. The activation of the emergency shutdown system causes stoppage of the whole system by closing the input and output valves. This paper presents the optimization of the voting redundancies of safety-instrumented systems by a multiobjective genetic algorithm. The objectives to optimize are the average probability of dangerous failure on demand, which represents the system safety integrity, and the spurious trip rate, which presents the activation of a safety function without the presence of a demand.

Keywords: optimize; vote; redundancy; safety instrumented system; emergency shutdown system; genetic algorithm

1. Introduction

In most real-world problems, several goals must be satisfied simultaneously in order to obtain an optimal solution. The search for the best compromise between availability and costs (operational and life cycle) is at the heart of the industry's concerns.

A firefighting system or FF is a system that is used in hazardous areas to prevent situations that could have catastrophic effects economically, environmentally, or operationally. They are designed to minimize the consequences of emergencies, such as injury to personnel or damage to equipment [1]. In this context, the firefighting system not only serves to protect the installation in case of deviation, but also to protect the people in the vicinity.

This study was devoted to the optimization of the performances of FF of a combined cycle power system by the minimization of the rate of spurious trip (STR) as well as the probability failure on demand (PFD). This is done by acting on the vote of the architecture (KooN) of this system.

2. Abbreviation

CCF	Common cause failure	Avg	average
β	Factor for quantification of C	ESD	Emergency shutdown
βD = βDD	β for dangerous detected (DD) failures	FE	Final Element
βSD	β for safe detected (SD) failures	KooN	K out of N
βSU	β for safe undetected (SU) failures	LS	Logic Solver
λD	Dangerous failure rate	MRTS	Mean repair time for SU failures
λDD	Dangerous detected failure rate	MTTRSD	Mean time to restoration for SD failures
λDU	Dangerous undetected failure rate	S	Sensors
λS	Safe failure rate	SD	Safe Detected Failures
λSD	Safe detected failure rate	SIF	Safety Instrumented Function
λSU	Safe undetected failure rate	SIS	Safety Instrumented System
λDind	Dangerous detected independent failure rate	STR(KooN)	STR for KooN architecture
λSind	Safe detected independent failure rate	STR	Spurious trip rate
		SU	Safe Undetected Failures
		T1	Interval between tests

3. Identify the System

The gas turbine-based power plant is characterized by its relatively low capital cost compared with the steam power plant. One of the technologies adopted nowadays for efficiency improvement is the combined cycle. Combined cycle technology is now well established and offers superior efficiency to any of the competing gas turbine-based systems that are likely to be available in the medium term for large-scale power generation applications. A combined-cycle power system (Figure 1) typically uses a gas turbine to drive an electrical generator, and recovers waste heat from the turbine exhaust to generate steam. The steam from waste heat is run through a steam turbine to provide supplemental electricity [2]. The overall electrical efficiency of a combined-cycle power system is typically in the range of 50–60%—a substantial improvement over the efficiency of a simple, open-cycle application of approximately 33%.
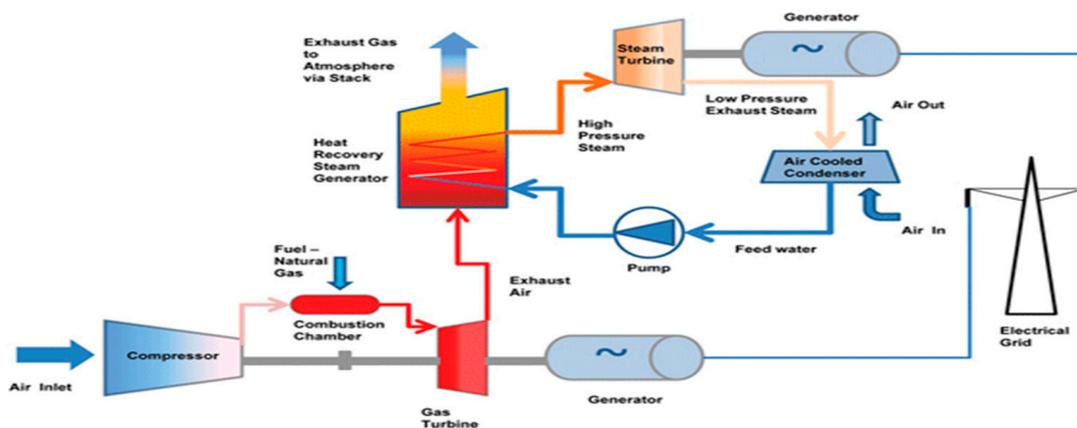

Figure 1. Block diagram of combined cycle power plan.

4. Firefighting System

The function of fire protection system is to provide safety (in terms of lives) from fire hazards and to provide protection (in terms of property) from fire hazards. Additionally,

the fire protection system must be able to provide early fire warnings and fire suppression. Fire protection systems are designed in accordance with the requirements of NFPA and other standards [3].

The FF system contains three subsystem sensors that send the data from the site or the machine equipped with these sensors to the logic solver that treats the output of sensors and makes the decision regarding the intervention of the extinguishing system (Table 1).

Table 1. Elements constituting the FF system with the presentation of the architecture (KooN type) of each of these elements.

Elements	Architecture
Sensors	1oo3
Logic solver	1oo3
Extinguishing system	1oo3

In addition to failures on demand that affect the availability of the system when we need its safety action, the FF system can be activated in the absence of deviations by false signals from its sensors, an incorrect decision of the logic solver, an incorrect action of the logic unit, or an unwanted action. This activation is characterized by a spurious activation rate.

5. The Problem to Be Optimized

The firefighting system serves not only to protect the installation in case of deviation but also to protect the man in the surroundings and ensure the generation of energy necessary for many facilities. This system starts since the date (test phase) of their putting into service of the untimely activations of the FF system without the presence of a real demand of the installation, and this causes the shutdown of the entire installation, the loss of production, and loss of time to resume the work.

The optimization of FF performances will allow a reduction in the frequency of failures of this system and a reduction in the unwanted activations of this system to avoid such problems as the loss of production and wasted production time.

6. Classification of Firefighting Failures

Some failures of safety systems can lead to dangerous situations, and others can lead to false activations (but without any danger), so the failures of our safety system (FF) can be classified according to their effects in two categories [4].

(1) Dangerous failures: A failure that has the potential to put the safety-related system in a dangerous state or prevent a safety function from operating when required (demand mode). For these reasons, it is expressed with the probability of failure on demand (PFD). PFD is a measure of the effectiveness of a safety function. It expresses the likelihood that the safety function does not work when required to.

(2) Safe failures or spurious activations: These are failures that do not have the potential to put the safety-related system in a dangerous state or make it unable to perform its function [5].

The term "activation" indicates that there is some transition from one state to another and the term "spurious" indicates that the causes of the triggering are false, incorrect, and unreal [1].

Spurious activations of firefighting system can cause partial or complete shutdowns of the facilities, so it is necessary to reduce its occurrence to

(1) avoid production losses due to shutdowns, and
(2) avoid the risks that may appear during the restart phase.

The spurious activation rate or spurious trip rate is defined as the average number of spurious activations of a safety function per unit of time [6].

7. Redundancy of Systems

In order to reduce the probability that a safety system does not fulfill its security function at the moment it is requested, a solution consists of redundant (totally or partially) certain elements constituting that system (sensors, logic unit, terminal elements, and even transmission means). Note that the redundancy can be realized with identical materials or with different technologies.

A redundancy of 1ooN is the best to ensure the safety function, but it influences negatively the rate of spurious activations because with this architecture it is enough of one element to activate spuriously to cause the activation of all the system [7].

The optimization of the spurious activations and failure on demand will allow us to minimize the number of spurious activations, minimize the lost time to restart the system and the costs of stopping production, and minimize the dangerous situation in which the safety activity is required.

A problem such as this is very complicated, but we can solve it with analytical methods; in fact, the use of metaheuristic methods such as the genetic algorithm (GA) is the best way to solve this problem.

8. Optimization (STR) and PFD

The STR and PDF of a well-defined safety function provided by a given SIS is determined by calculating and combining the same variables of its three subsystems (S, LS, and FE). This can be expressed by the following general formula:

$$〚PFD〛\_avg = 〚PFD〛\_avg (S) + 〚PFD〛\_avg (LS) + 〚PFD〛\_avg (FE).$$

$$STRavgSIS = STRavg (S) + STRavg (LS) + STRavg (FE).$$

Obviously, each of these three subsystems is represented by a KooN architecture [2]. Reference [3] explains the formula of STR(KooN) and PDF (KooN):

$$PFDmoy (KooN) = A_N^{N-K+1} \lambda_{Dind}^{N-K+1} \prod_{i=1}^{N-K+1} MDT_{i001} + \beta \lambda DU \left(\frac{T1}{2} + MRT\right) + \beta D \lambda DD \, MTTR.$$

$$STR(KooN) = A_N^K \lambda_{Sind}^K \prod_{i=1}^{K-1} MDTS_{i001} + \beta \lambda SU + \beta D \lambda SD. \tag{1}$$

with

$$A_N^{N-K+1} = \frac{N!}{(K-1)!}$$

$$\lambda D = \lambda DD + \lambda DU$$

$$\lambda Dind = (1 - \beta) \lambda DU + (1 - \beta D) \lambda DD$$

$$\lambda S = \lambda SD + \lambda SU$$

$$\lambda Sind = (1 - \beta SU) \times \lambda SU + (1 - \beta SD) \lambda SD$$

$$〚MDT〛\_i001 = \lambda DU/\lambda D(T1/2 + MRT) + \lambda DD/\lambda D.MTTR \tag{2}$$

$$〚MDTS〛\_i001 = \lambda SU/\lambda S(T1/2 + MRTS) + \lambda SD/\lambda S.MTTRS. \tag{3}$$

We act on the voting of each subsystem because the system is in the production phase, which means we cannot modify the number of elements (N), so we can only act on the voting (KooN) of each subsystem sensor subsystem, logic solver subsystem, and final element subsystem. Multiobjective optimization is an area of multiple criteria decision making that is concerned with mathematical optimization problems involving more than one objective function to be optimized simultaneously. In our study, the objectives we try to optimize are the PFD and the STR of an emergency shutdown system.

9. Genetic Algorithm

A genetic algorithm is a search heuristic that is inspired by Charles Darwin's theory of natural evolution. This algorithm reflects the process of natural selection by which the fittest individuals are selected for reproduction in order to produce offspring of the next generation. All of this has been done via the following steps of the GA [8].

Notion of Natural Selection

The process of natural selection starts with the selection of fittest individuals from a population. They produce offspring which inherit the characteristics of the parents and will be added to the next generation. If parents have better fitness, their offspring will be better than parents and have a better chance of survival. This process keeps on iterating, and, at the end, a generation with the fittest individuals will be found. This notion can be applied for a search problem. We consider a set of solutions for a problem and select the best set [9].

At first, the coding to be used must be defined. Then, by using a random process, an initial population of strings is created. Next, a set of operators is used to take this initial population to generate successive populations, which hopefully improve with time. The main operators of the genetic algorithms are reproduction, crossover, and mutation.

Reproduction is a process based on the objective function (fitness function) of each string. This objective function identifies how good a string is. Thus, strings with higher fitness value have a larger probability of contributing offspring to the next generation.

Crossover is a process by which members of the last population are mated at random in the mating pool. A pair of offspring is generated, combining elements from two parents (members), which hopefully have improved fitness values. Mutation is the occasional (with small probability) random alteration of the value of a string position. In fact, mutation is a random-walk process through the coded parameter space. Its purpose is to ensure that important information contained within strings is not lost prematurely.

10. Results and Discussion

In order to facilitate the use of genetic algorithms, their execution is now fully supported by the fully supported by the Optimization Toolbox of the MATLAB environment. The gene code represented in Table 2.

Table 2. The gene of the code used in the GA.

K_S	$T1_S$	K_{LS}	$T1_{LS}$	K_{FE}	$T1_{FE}$

The variables in our code are the voting KooN of the sensors and logic solver but the final elements are two valves working together when the logic solver send a signal of closing so the voting of the final element is 2oo2. Moreover, the other variable is the T1 of each element of the FF system.

After executing the GA to optimize the STR of the ESD based on choosing the best voting and the best time between periodic tests, the results of the optimization can be presented, as in Table 3 [10].

Table 3. Results of the optimization the STR of FF system.

Variables			Objective Functions	
K1 (Sensors)	K2 (UL)	K3 (Extg Sys)	PFDavg	STR
2	2	2	0.00878	1.0257×10^{-5}
2	1	1	0.00855	3.5591×10^{-5}
2	1	2	0.00863	3.5516×10^{-5}

To get a PFD = 0.00878 and STR = 1.0257×10^{-5}, the best voting for the sensors is 2oo3 with a voting of logic solver 2oo3—the same voting for the extinguishing system. To get a PFD = 0.00855 and STR = 3.5591×10^{-5}, the best voting for sensors is 2oo3. For the logic solver, 1oo3 is the same for the extinguishing system and to get PFD = 0.00863. To get an STR = 3.5516×10^{-5}, the best voting for sensors is 2oo3, and for the logic solver 1oo3 and 2oo3 are the best voting for the extinguishing system.

11. Conclusions

As a conclusion to our work, it should be noted that spurious activation must be taken into consideration in the performance evaluation of instrumented safety systems due to the important economic losses caused by this type of failure.

For the optimization of the performance of a safety system, the use of genetic algorithms is a powerful tool to help in the decision-making process for the choice of an adequate architecture.

The GA still has some limitations, such as the coding step, which requires time and good knowledge of the system; in addition it relies on hazards in its operations.

That is why integrating machine learning will be more useful in solving optimization problems to provide methods of optimization with a higher, intelligent rate.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fatima, M.; Assia, H.; Habib, H. Commande d'un système éolien basé sur une MADA. *IJSET* **2019**, *11*, 9–14.
2. *Design and Operation of Heat Exchangers and Their Networks*; Roetzel, W.; Luo, X.; Chen, D. (Eds.) Elsevier: Amsterdam, The Netherlands, 2020; ISBN 978-0-12-817894-2.
3. Combined Cycle Manual by Hyundai. 2020. Available online: https://www.hyundai.com/content/dam/hyundai/in/en/data/connect-to-service/owners-manual/kona.pdf (accessed on 1 November 2022).
4. *Standard IEC 16508*; Functional Safety of Safety-Related Electrical/Electronic/Programmable Electronic Systems. International Electrotechnical Commission: Geneva, Switzerland, 2000; Parts 1 to 7.
5. Lundteigen, M.A.; Rausand, M. *Spurious Activation of Safety Instrumented Systems in the Oil and Gas Industry: Basic Concepts and Formulas*; Elsevier: Amsterdam, The Netherlands, 2007.
6. Bae, J.-H.; Shin, S.-C.; Park, B.-C.; Kim, S.-Y. Design optimization of ESD (Emergency shutdown) System for offshore process based on reliability analysis. In Proceedings of the 2016 International Conference on Design Engineering and Science (ICDES 2016), Kuala Lumpur, Malaysia, 27–29 February 2016.
7. Thuy, L.; Adjadj, A.; Chaumette, S.; Bouchet, S.; de Dianous, V. Performance Evaluation of Engineered Safety Barriers. 2008. Available online: https://www.mementodumaire.net/wp-content/uploads/2012/03/Omega_10_Evaluation_BTS_v2_0908_web.pdf (accessed on 1 November 2022).
8. Innal, F.; Dutuit, Y.; Chebila, M. Reliability Engineering and System Safety: Safety and operational integrity evaluation and design optimization of safety instrumented systems. *Reliab. Eng. Syst. Saf.* **2015**, *134*, 32–50. [CrossRef]
9. Barros, D.B. Natural Selection as a Mechanism. *Philos. Sci.* **2008**, *75*, 306–322. [CrossRef]
10. *MATLAB 2017 Software*; MathWorks, Inc.: Natick, MA, USA, 2017.