Process Safety and Environmental Protection 117 (2018) 214–222

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Simultaneous evaluation of safety integrity's performance indicators with a generalized implementation of common cause failures

Mourad Chebila

Institute of Health and Safety, Batna 2 University, Algeria

ARTICLE INFO

Article history:
Received 15 February 2018
Received in revised form 26 April 2018
Accepted 27 April 2018
Available online 3 May 2018

Keywords:
Availability
Unconditional failure intensity
Common cause failures
KooN:G architectures

ABSTRACT

The average unavailability and the average unconditional failure intensity of safety-instrumented systems represent the main performance indicators of safety integrity. This paper employs an approach based on the exploitation of the availability expression to obtain both performance measures in a simultaneous and straightforward way for any KooN configuration. The implementation of such an approach is generalized to take into account the contribution of common cause failures using any parametric model. The validation of the obtained results is verified through their application using several architectures and using Beta Factor and Binomial Failure Rate models to handle such type of dependent events. Therefore, the contribution of this paper lies in proposing one single formula that can be used to estimate the two main safety integrity's performance indicators for any KooN architecture using any kind of common cause failures parametric model.

1. Introduction

As defined in the generic standard (IEC 61508, 2010) and in the process sector-specific standard (IEC 61511, 2016), functional safety aims to provide a framework that involves several phases and activities to cover the entire lifecycle of safety-instrumented systems (SIS) in purpose of ensuring their safety integrity and, therefore, establishing a satisfactory risk reduction management. An important constituent of such framework is the verification of the ability of SIS to fulfill their intended functions against several types of failures. This verification includes the quantification of the effects of random hardware failures to estimate two key performance indicators, which are: a) the average probability of dangerous failure on demand (PFD_{avg}) for low demand mode of operation, and b) the average frequency of a dangerous failure (PFH) for high demand and continuous modes of operation. Such estimation necessitates the consideration of several parameters, such as the architecture of the SIS as well as its subsystems, the dangerous failure rate of the various elements, the contribution of common cause failures (CCF), the diagnostic coverage of the diagnostic tests, the proof test interval, the mean time to restoration (MTTR), the mean repair time (MRT),. . .etc.

Examples of widely used reliability techniques to estimate PFD_{avg} and PFH include the reliability block diagrams, fault trees, Markov models, Petri nets. . ., which are profoundly studied in (IEC 61508, 2010; ISA-TR84.00.02-2002, 2002; Goble and Cheddie, 2005; Rausand, 2014) and applied to several specific aspects (Mkhida et al., 2014; Bukowski and Goble, 1995). More specifically, fault trees are broadly employed in reliability and probabilistic safety analyses with a traditionally recognized practical limitation associated with their manual application to the highly complex cases due to the massive amount of time and knowledge it requires. Several researches have been developed to overcome that drawback, such as (Szabó and Tárnái, 2000) where an automatic model generation algorithm is suggested based on the functional and hardware description of the system and a failure behavior description database. Additionally, computer-aided fault tree analyses are developed in (Khan and Abbasi, 2000; Ferdous et al., 2007, 2009) allowing the typical qualitative and quantitative treatment in addition to uncertainty and sensitivity analyses. Recently, a matrix-based approach is presented in (Roth et al., 2015) to automatically generate and evaluate fault trees. However, the comprehensive inclusion of CCF remains problematic because of its involvedness.

Because of their easiness and accuracy, the simplified equations have attracted a lot of attention from the committees of the international standards themselves as well as from a large number of researchers who have contributed to the development of several useful models.

E-mail address: m.chebila@univ-batna2.dz

https://doi.org/10.1016/j.psep.2018.04.019
0957-5820/

Nomenclature

BF	Beta factor
BFR	Binomial failure rate
CCF	Common cause failures
D	Dangerous
DD	Dangerous detected
DU	Dangerous undetected
KooN	K-out-of-N
MRT	Mean repair time
MTTR	Mean time to restoration
PFD	Probability of dangerous failure on demand
PFH	Frequency of a dangerous failure
SIS	Safety-instrumented system
A	Availability
avg	Average
$E()$	Integer part
ind	Independent
m	Number of the affected components
T_1	Proof tests interval
U	Unavailability
w	Unconditional failure intensity
β	Beta factor (CCF proportion using the beta factor model)
λ	Failure rate
μ_{DD}	Repair rate of DD failures
φ	Transformation operator

Yet, those models are based on the separate treatment of PFD_{avg} and PFH, and more notably, on the employment of the traditional Beta Factor (BF) model to handle the involvement of CCF events, which overrides their partial impact.

While, PFD_{avg} represents the average unavailability, PFH represents the average unconditional failure intensity (also known as failure frequency), which can be considered as the prime dependability measures of the repairable systems due to the significant amount of information they hold and their comprehensiveness of the other measures (e.g., mean down time and failure rate). Several contributions have been made to find and simplify the bridge that connects these two main attributes to facilitate their estimation at the system level. For instance, we mention (Buzacott, 1967, 1970), in which the system failure frequency is determined in terms of availability and some other importance measures by means of reliability block diagrams. Later, (Singh and Billinton, 1973; Singh, 1979; Nahman, 1981) employed cut-set based approaches to extract directly the failure frequency. Additionally, further enhancements have been realized in (Schneeweiss, 1981; Hayashi, 1991; Amari, 2000; Chang et al., 2004; Dutuit and Rauzy, 2005; Druault-Vicard and Tanguy, 2006), where several techniques have been applied using differential operators, variable inversion methods and importance factors.

Specifically, an interesting method is proposed in (Hayashi, 2006), which allows the direct transformation of the availability expression of a system into a matrix to calculate simultaneously the availability and the unconditional failure intensity within a reasonable computation time and without any additional parameters.

The main objective of this paper is to treat two main aspects. The first aspect is the implementation of such transformation method to estimate both performance indicators of safety integrity for any KooN architecture including the conventional parameters by only using the availability expression of the subsystem. The second aspect is the consideration of other CCF parametric models to estimate such indicators to overcome the shortcoming of the BF model. Subsequently, Section 2 is dedicated to the implementation of the discussed transformation method to estimate PFD_{avg} and PFH with and without considering CCF events, while the generalization of such application is handled in Section 3. Each case is validated by a numeric application to a variety of configurations. Lastly, some conclusions are discussed in Section 4.

2. Implementation

Availability is a key dependability attribute of the repairable systems, which is defined in (IEC 60050, 1999) as the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the external resources are provided. Analogously to most of the automated industrial systems, those devoted to safety are highly complex and comprising numerous components and structures. Among such structures, we find the KooN configuration, which requires the good operation of at least K components out of the existing N components. The availability of any KooN system $A^{KooN}(t)$, whose components are identical, can be written as a function of the availability of its constituents $A(t)$ as follows:

$$A^{KooN}(t) = \sum_{i=K}^{N} \binom{N}{i} A(t)^i (1 - A(t))^{N-i} \tag{1}$$

The proposed method in (Hayashi, 2006) employs the transformation operator "φ", which satisfies the following properties:

$$\phi(A_1 + A_2) = \phi(A_1) + \phi(A_2) \tag{2}$$