Reliability Engineering and System Safety 95 (2010) 707–715

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Extension of ISA TR84.00.02 *PFD* equations to *KooN* architectures

Luiz Fernando Oliveira *, Rafael Nelson Abramovitch [1]

Det Norske Veritas, DNV Energy Solutions South America, Rua Sete de Setembro 111/19° andar – Centro 20050-006 – Rio de Janeiro – RJ, Brazil

ARTICLE INFO

Article history:
Received 5 August 2009
Received in revised form
31 December 2009
Accepted 17 January 2010
Available online 4 February 2010

Keywords:
Safety instrumented system
PFD equations
SIL verification
KooN architecture
Common-cause failure

ABSTRACT

Simplified equations for *PFD* evaluation of the most used architectures are given in ISA TR84.00.02-2002 document. This paper introduces a generalization of those equations for applications to any KooN architecture. The meaning of each individual term in the derived equations is explained. To strengthen their validity, several comparisons are made between their results and those of a numerical integration model for *PFD* assessment. The results show that the values obtained with the generalized equations are very close to those of the numerical model, even for highly redundant configurations. Comparisons are also made with the analytical equations given in IEC 61508. It is argued that the ISA equations are conceptually more consistent than those of IEC 61508 even though the numerical differences between the results are not significant in most practical cases. Overall, the results indicate that the generalized KooN *PFD* equations derived here may be applied to systems with higher redundancy, thus partly contradicting suggestions made in the above ISA reference that such equations should only be used for the simplest configurations. Some specific practical situations to which they cannot be applied are also pointed out.

1. Introduction

Merely ten years after the publication of ISA [1] and IEC [2,3] standards establishing functional safety requirements for Safety Instrumented Systems (SIS), their adoption has become practically universal in industrial sectors that require highly reliable protection systems. Not surprisingly, this has been mostly accelerated in the oil-and-gas industry, process plants, nuclear reactors, modern transportation systems, and large machinery.

At the core of the Safety Lifecycle approach adopted in those standards lays the processes for determining the required Safety Integrity Level (SIL) and for verifying compliance by system configurations used by SIS designers. For these purposes, aside from indicating the methods for determining the Required SIL, IEC 61508 Part 6 [4] also provides analytical equations for the quantitative evaluation of the Probability of Failure on Demand (*PFD*) of a few typical SIS architectures of widespread use in the industry: 1oo1, 1oo2, 1oo2D, 2oo2 and 2oo3. For the sake of simplicity, those equations are hereby referred to as “the IEC equations”. Even though the original Standard ISA-TR84.00.02 [1] did not include such equations, ISA published in 2002 a five-part technical report, whose second part [5] presents simplified analytical equations for the 1oo1, 1oo2, 1oo3, 2oo2, 2oo3 and 2oo4 configurations. Again for simplicity, those equations are hereby referred to as “the ISA equations”.

Frequently, SIS designers must select among several different configurations to meet a determined required SIL level. For that, a fundamental task is the evaluation of the *PFD* of each configuration. Both cited IEC and ISA Refs. [4,5], only provide equations for evaluating the *PFD* of the most frequently used configurations. From time to time, SIL analysts face situations where they need to evaluate the *PFD* of higher redundancy configurations. Neither of the two cited references gives equations for the *PFD* of a general *KooN* configuration[1]. Although there are several equations for evaluating the *PFD* of a *KooN* configuration in the open literature (see Smith [6]), the authors could not find any, which takes into account all the features considered in the standards equations — dangerous detected and undetected failure rates, safe failure rates, their respective MTTRs and common-cause factors. In addition, reference [4] does not show details of the derivation that led to the reported *PFD* equations, thus making their generalization to other SIL configurations a bit more difficult. Lastly, the equations in the two cited references are not equal, increasing the difficulties in fully grasping their logic.

In recent articles, Oliveira [7,8] showed how the *PFD* equations in IEC may be derived and generalized for *KooN* architectures.

* Corresponding author. Current address: DNV France, 69 Rue du Chevaleret, 75007 Paris France. Tel.: +33 60 9438064.
E-mail addresses: Luiz.Oliveira@dnv.com (L.F. Oliveira), Rafael.Nelson@petrobras.com.br (R.N. Abramovitch).

[1] Current address: PETROBRAS/E&P, Rua Chile, 65 – Centro, 20050-006, Rio de Janeiro, RJ. Tel.: 55 (21) 3722-7279.

[1] A *KooN* configuration is an SIS configuration where ‘*k*’ out of ‘*n*’ channels (or redundant components) must function for the safety function to be successfully performed.

0951-8320/$ - see front matter © 2010 Published by Elsevier Ltd.
doi:10.1016/j.ress.2010.01.006

Even though developed for the same purpose, the ISA equations in reference [5] were derived quite differently from those in IEC [4]. This paper develops a generalization of the simplified equations in ISA TR84.00.02-2002 Part 2 [5] for any *KooN* configuration. The underlying assumptions of the equations in Ref. [5] are maintained in the generalized equations here developed and the meaning of each term is explained. Exception is made to the systematic error term which is not included in this paper. Its inclusion would blur the comparison results for the various configurations since it would be basically the same for all of them. Furthermore they are not included in the IEC equations. Comparisons are made between the results from the equations in the two reference documents ([4,5]), showing that the ISA equations are conceptually more solid than those of IEC 61508. The latter, even though producing quantitative results similar to the former, when expanded reveal terms that lack any theoretical basis. They appear in some of the IEC equations due to assumptions made in their derivations. On the contrary, any single term in the ISA document [5] can be logically explained. For this reason, it is suggested here that the *PFD* equations given in Ref. [5] and their generalization presented in this paper be used in the new revision of IEC 61508 (excluding the systematic failure terms).

To increase the credibility of the generalized equations derived in this paper, a comparison is made with corresponding results from a numerical model, which solves the problem by numerical integration of the time-dependent system unavailability (*PFD*) function built from the logical combination of individual component unavailability functions. This numerical model, developed by the authors [9], follows closely the computational procedures used in FRANTIC software [10] developed by the Nuclear Regulatory Commission of the United States in the 80's and 90's. A similar model has been recently published [11]. The results of the comparisons throughout this paper demonstrate that the values obtained with the generalized equations here developed are very close to the values attained with the numerical model, even for systems with a high redundancy level.

The ISA technical report [5] suggests that the simplified equations be used only for systems mentioned in the report (1oo1, 1oo2, 1oo3, 2oo2, 2oo3 and 2oo4 configurations) and that, for more complex and redundant systems, Markov and fault tree methods should be used instead. This paper shows that the simplified analytical equations may be applied also to high-redundancy systems.

This paper is structured in nine sections, as follows. After this brief introductory section, the terminology is presented in Section 2. The ISA equations [5], without common-cause failure (CCF) terms, are analyzed in Section 3. In Section 4 a *PFD* equation is proposed for any *KooN* architecture without contributions from CCFs. In Section 5 the CCF contributions are added to the generalized *KooN PFD* equation. In Section 6 a brief conceptual comparison between the ISA and the IEC equations is presented. Section 7 presents *PFD* results for some typical *KooN* systems, comparing results from the IEC, ISA, and the generalized equations proposed in this paper among themselves and with those obtained with the numerical model. The main limitations of the analytical equations for *PFD* evaluation are indicated in Section 8 and the final comments are presented in Section 9.

2. Terminology

The key variables used in the mathematical expressions in this paper are presented in Table 1. As far as possible, the definitions and representations in IEC 61508, Part 6 [4] were kept.

Table 1
Abbreviations and nomenclature.

C_k^n	Number of combinations of size "*k*" from a set with "*n*" elements
DC_D	Dangerous Diagnostic Coverage Coefficient
DC_S	Safe Diagnostic Coverage Coefficient
HFT	Hardware Fault Tolerance
KooN	"*k*" out of "*n*" configuration (or architecture)
MTTR	Mean Time to Restoration
PFD	Probability of Failure on Demand (of a component, a channel, a system)
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T_1	Proof-test interval
β	Beta Factor for dangerous undetected failures
β_D	Beta Factor for dangerous detected failures
λ	Total failure rate (dangerous failure rate+safe failure rate)
λ_D	Dangerous failure rate
λ_{DD}	Dangerous detected failure rate
λ_{DU}	Dangerous undetected failure rate
λ_S	Safe failure rate
λ_{SD}	Safe detected failure rate
λ_{SU}	Safe undetected failure rate

3. The ISA equations without contributions from common cause failures

IEC 61508 [4] presented analytical equations for evaluating the *PFD* of the most commonly utilized architectures: 1oo1, 1oo2, 1oo2D, 2oo2 and 2oo3. Recently, it has been shown by Oliveira [7,8] that those equations may be deduced by an approach that expresses the *PFD* as the product of a single average failure mode frequency, multiplied by the average time that the system remains in the failed state. The failure frequency is obtained considering the total dangerous failure rate (sum of undetected and detected dangerous failure rates). The average time in the failed state can be obtained from the mean time in the dangerous undetected failure mode, and the mean time to repair the detected dangerous failures.

Similarly, Part 2 of the ISA 2002 technical report [5] also presents simplified analytical equations for 1oo1, 1oo2, 1oo3, 2oo2, 2oo3 and 2oo4 architectures, which show a few differences in relation to the IEC 61508 equations [4]. Ref. [5] shows that the equations were deduced as the sum of the contributions to the *PFD* deriving from the various possible combinations of dangerous failure modes, detected and undetected, resulting in the smallest amount of failures capable of causing system failure, for each system architecture, disregarding some terms that only bring minor contributions. For a *KooN* system, the 'smallest amount' of failures capable of causing system failure is $n-k+1$. This encompasses any combination of modes of failure that render the safety system unavailable on demand.

After examining equations from both standards, a clear difference in philosophy is noticed when calculating the probability of failure on demand. IEC 61508 [4] considers that dangerous detected failures ('*DD*') in a channel will take the channel to a failed state and it will remain in this state until the component is repaired. Thus the plant would continue to operate, during the channel restoration time, resulting in a contribution from detected dangerous failures to the probability of system failure on demand.

Differently from IEC, in the ISA equations [5] it is assumed that if a safety system composed of a single channel would suffer a dangerous detected failure, the system will cause the plant to go into a safe shutdown, bringing the system to a safe state. Thus, the contribution from dangerous detected failures (*DD*) is absent in the *PFD* equation for the 1oo1 architecture. An analysis of the ISA equations for the other architectures shown in Tables 2–4 below,