Reliability Engineering and System Safety 150 (2016) 160–170

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

PFD$_{avg}$ generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models

Fares Innal*, Mary Ann Lundteigen, Yiliu Liu, Anne Barros

Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Article history:
Received 28 August 2015
Received in revised form
21 January 2016
Accepted 28 January 2016
Available online 6 February 2016

Keywords:
Safety instrumented system (SIS)
Partial testing
KooN configuration
PFD$_{avg}$
Multi-phase Markov models

ABSTRACT

IEC 61508 is a standard on design and operation of safety-instrumented systems (SISs) which has been adapted by many national regulations as the recommended way to achieve high-reliability systems. Many decisions about the design of SIS rely on the results from reliability assessments. It is therefore important that the reliability assessments are able to capture key properties of the system, such as the consideration of regular partial and full proof tests. IEC 61508 has proposed analytical formulas for commonly used architectures. Unfortunately, these formulas do not explicitly include the contribution of partial tests and consequently their use is mainly restricted to full proof tests. In addition, the already existing formulas dealing with partial tests disregard the different repair times. The aim of this paper is to (i) extend the PFD$_{avg}$ formulas given in IEC 61508 by including partial tests impact and, (ii) investigate their consistency based on multi-phase Markov models related to 1oo1 and 1oo2 architectures and (iii) to establish new generalized formulations in light of the results related to the investigation process, which account for the different repair times. Different comparisons are performed throughout the paper in order to validate the set of the derived formulations.

1. Introduction

Safety instrumented systems (SISs) play a vital role in the protection of people, environment and assets from hazardous events generated within technical systems, and in their interaction with the environment. IEC 61508 [1] has been developed as a performance-oriented standard, with the aim to frame the design and operation of SIS so that the necessary risk reduction is achieved. Safety integrity level (SIL) has been introduced as the overall performance measure and is a way to translate the necessary risk reduction into technical (i.e. hardware and software) requirements and process requirements concerning design, operation, and maintenance. IEC 61508 specifies two probabilistic measures to SIL on the basis of how often the SIS is required to respond to hazardous events: the average probability of dangerous failure on demand (*PFD*$_{avg}$) and the probability of dangerous failure per hour (*PFH*). The first measure is used for low-demand mode and applies when the SIS needs to respond on the average every year or less. The latter measure applies when the SIS is operated in the high-demand mode, where the demands occur more often than once every year on the average, and in the continuous mode, when the safety functions of the SIS is a normal part of the operation of the protected system. The *PFH* measure is out the scope of this paper and therefore will not be discussed further.

The quantification of the *PFD*$_{avg}$ considers several parameters: system configuration or architecture (*K-out-of-N*, in the following shortened to *KooN*), failure rates, proof test intervals, repair and restoration times, and common cause failures (CCFs). IEC 61508 distinguishes between four SILs, and a target range of *PFD*$_{avg}$ is allocated to each of these. If the calculated *PFD*$_{avg}$ is above the target range of a specified SIL requirement, it is necessary to evaluate how the reliability can be improved. The main strategies to enhance reliability are to either improve the inherent reliability (i.e., by introducing more reliable components), add more redundancy, or carry out regular proof testing more often. It may be remarked that the latter strategy has some possible negative effects. Higher operational costs may follow from more frequent planned maintenance and production stops. The overall risk level may also increase due to more abruption of normal operation. For some equipment it is possible to complement regular proof (i.e., complete) testing by partial testing, such as for shutdown valves [2–5]. Partial stroke testing of valves means to operate the valve just partially, for example by 20% from the normal position, so that failures related to sticking of valves or delayed operation may be detected [5]. Partial testing may be introduced to improve safety (by complementing existing proof testing regime with partial testing) or reduce costs (by compensating an extension of proof test intervals with partial testing) [5,6].

* Corresponding author. Tel.: +47 73597102.
E-mail addresses: innal.fares@ntnu.no, innal.fares@hotmail.fr (F. Innal).

http://dx.doi.org/10.1016/j.ress.2016.01.022
0951-8320/© 2016 Elsevier Ltd. All rights reserved.

IEC 61508 has proposed analytical formulas for PFD_{avg} that are tailor-made for selected configurations. Unfortunately, the standard does not provide underlying assumptions that are needed to generalize for *KooN* systems, but generalizations are proposed by others in several papers and industry guidelines [7–11]. The most challenging facet of the generalized formulas is their restricted application area. Most analytical formulas assume, for example, that the tests are perfect, even if this assumption is seldom valid. Imperfect test conditions are more close to reality, and relate to practical limitations about how the test is carried out and that test conditions are different from demand conditions. Partial testing is a special case, where the scope of the test is limited in order to overcome other challenges, such as disturbing the production [5]. Summers and Zachary [3] shows how partial tests can be accounted for when calculating PFD_{avg}, but only for 1oo1 architecture. Oliveira [6] was the first to generalize the PFD_{avg} for *KooN* systems subject to partial testing with basis in IEC 61508. Brissaud et al. [12] developed first exact formulas for PFD_{avg} for *KooN* systems, considering both periodic and non-periodic partial tests. Approximations for these formulas are provided in Brissaud et al. [13]. Jin and Rausand [14] presented exact and approximate generalized expressions for PFD_{avg}, and may be regarded as an extension of [12] and [13] with the inclusion of common cause failures (CCFs). Chebila and Innal [15] have made an additional extension, by also considering the effect of dangerous detected (DD) failures. It is worth noticing that the common drawback of the already existing formulas is the non consideration of repair times, which are neglected compared to proof and partial tests intervals.

In order to overcome this limitation, the objective of this paper is to provide a new PFD_{avg} formulation that takes into account these repair times. For this end, first, a generalization for PFD_{avg} formulas including the contribution of partial testing is developed based on the IEC 61508 formulas scheme. Secondly, a consistency check of that generalization is carried out relying on multi-phase Markov models approximated by classical Markov models. The use of Markov models allows to accurately study the different failure sequences. Precisely, the analytical formulas for 1oo1 and 1oo2 systems have been developed from their respective approximated Markov models and compared with the proposed generalized formulas. The results show that the generalization based on the IEC 61508 scheme is formally wrong. Finally, new PFD_{avg} formulas for *KooN* systems have been derived on the basis of the study of failure sequences leading to system failure, with support from the results obtained from the consistency check process. More precisely, the formulas derivation relies on the quantification of the mean sojourn time related to each failure sequence. The summation of the contribution of the different failure sequences results in the new PFD_{avg} generalization. The followed approach makes it easier to consider the repair times and to distinguish between those attached to failures detected by either partial or proof tests.

The remaining part of this paper is organized as follows. Section 2 introduces parameters and assumptions that are commonly used in formulas for PFD_{avg}. The generalization for PFD_{avg} with basis on IEC 61508 is given in Section 3. In Section 4, 1oo1 and 1oo2 systems are deeply investigated and checked against this first generalization. In Section 5, new generalized and accurate formulas for PFD_{avg} are derived and the results they give are compared against those induced by the first generalization and those obtained from multi-phase Markov models. A second comparison is achieved with respect to the already existing formulas in the literature. Finally, some concluding remarks and future researches are given in Section 6.

2. SIS, Failure and repair times terminology

2.1. SIS definition

A typical SIS consists of three subsystems: sensors (transmitters, detectors), logic solver (API, PLC) and final elements (shutdown valves, pumps, circuit breakers). The sensor subsystem measures physical parameters of the protected system (temperature, pressure, level, etc.). The logic solver subsystem makes appropriate decisions, by comparing the measurements with given thresholds. The decision may be to operate final elements subsystem, to either bring or maintain the system in a safe state.

Specific subsystems are used to carry out specific safety instrumented functions (SIFs). A SIS may carry out one or more SIFs. Each subsystem may be considered as a *KooN* system, where *K* out of *N* identical items must function for the subsystem to function. That is, the failure of $N–K+1$ items results in the failure of the subsystem.

2.2. IEC 61508 failure taxonomy

IEC 61508 defines three modes of operation of a SIS: low-demand, high demand and continuous demand. In the low demand mode, it is assumed that a SIF is demanded less or equal to once per year, otherwise the SIF is said to be in high or continuous demand. A SIS will normally have only low-demand or only high-demand or continuous demand, and seldom a mixture.

The IEC 61508 suggests PFD_{avg} as a suitable reliability measure for low-demand systems. Its quantification is made on the basis of random hardware failures, characterized by a constant failure rate λ. Not all failures are equally important and relevant for the quantification. Dangerous (D) failures (with the associated failure rate λ_{D}) are important and therefore included, as they may prevent or seriously impair the ability of the SIF to function. Safe (S) failures (λ_S) that do not have this effect are not important in this context, but may be considered in relation to other performance measures such as the spurious trip rate [10,16]. The D failures are further split into dangerous detected (DD) failures (λ_{DD}) and dangerous undetected (DU) failures (λ_{DU}). DD failures are announced immediately by diagnostics and restored within a mean time to restoration (*MTTR*) that is normally short. The fraction of DD failures among all D failures is referred to as the diagnostic coverage (DC), and is mainly a property of the diagnostic features of the items.

Considering the previous descriptions, the dangerous failures rate is specified by the following relation:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} = DC \bullet \lambda_D + (1 - DC) \bullet \lambda_D \tag{1}$$

The *DU* failures are more critical, as the failures remain hidden until the next scheduled proof (or in some cases partial) test. Once detected, a DU failure is restored within a mean repair time denoted *MRT*.

Proof test coverage denotes the fraction of DU failures that can be revealed during a proof test. Most analytical formulas assume that (*i*) the proof tests are perfect, meaning that the proof tests coverage = 1, (*ii*) that the test duration is negligible (= 0), and (*iii*) that the repair is perfect so an “as good as new” condition is achieved for the failed item(s). These assumptions allow to assume that the PFD_{avg} calculated for one proof test interval applies also for all future intervals.

2.3. Inclusion of partial tests

Partial tests are introduced to reveal a certain fraction of *DU* failures. This means that the DU failure rate is split into two parts: failures detected by partial tests (λ_{PT}) and the remaining failures that still hidden until the next full or complete test (λ_{FT}). In this paper, partial tests are assumed to be periodically distributed over the proof test interval (T_1): carried out each period equals to $T_{PT}= T_1/m$. Their