Reliability Engineering and System Safety 94 (2009) 520–525

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Architectural constraints in IEC 61508: Do they have the intended effect?

Mary Ann Lundteigen *, Marvin Rausand

Department of Production and Quality Engineering, Norwegian University of Science and Technology, S. P. Andersens v. 5, NO 7491 Trondheim, Norway

ARTICLE INFO

Article history:
Received 19 November 2007
Received in revised form
19 May 2008
Accepted 14 June 2008
Available online 18 June 2008

Keywords:
Safety instrumented system
Hardware fault tolerance
Safe failure fraction
Systematic failure
Probability of failure on demand

ABSTRACT

The standards IEC 61508 and IEC 61511 employ architectural constraints to avoid that quantitative assessments alone are used to determine the hardware layout of safety instrumented systems (SIS). This article discusses the role of the architectural constraints, and particularly the safe failure fraction (SFF) as a design parameter to determine the hardware fault tolerance (HFT) and the redundancy level for SIS. The discussion is based on examples from the offshore oil and gas industry, but should be relevant for all applications of SIS. The article concludes that architectural constraints may be required to compensate for systematic failures, but the architectural constraints should not be determined based on the SFF. The SFF is considered to be an unnecessary concept.

1. Introduction

Safety instrumented systems (SIS) are important protection layers in the process industry. A SIS comprises input elements (e.g., pressure transmitters (PTs), gas detectors), logic solvers (e.g., relay based logic, programmable logic controllers), and final elements (e.g., valves, circuit breakers). A SIS is used to detect the onset of hazardous events (e.g., gas leakages, high pressures) and/or to mitigate their consequences to humans, the environment, and material assets. A simplified SIS is illustrated in Fig. 1, where a shutdown valve is installed to stop the flow in the pipeline when high pressure is detected by the PTs. The international standards IEC 61508 [1] and IEC 61511 [2] require that reliability targets for the SIS are defined and demonstrated. The reliability targets are assigned to each safety instrumented function (SIF) that is implemented into the SIS. The IEC standards use safety integrity level (SIL) as a measure for reliability.

Compliance to a SIL must be demonstrated by quantitative and qualitative assessments. The quantitative assessment includes estimating the SIS reliability. For a SIS operating on demand, which is often the case when the SIS is used as an independent protection layer in addition to the process control system, the *average* probability of failure on demand (PFD) is calculated [1,2]. The qualitative assessment verifies that all requirements related to work processes, tools, and procedures are fulfilled in each phase of the SIS life cycle.

The PFD does not cover all aspects that may cause SIS failure, and the calculated PFD may therefore indicate a better performance than will be experienced in the operating phase. Based on this argument, the IEC standards [1,2] have included a set of additional requirements to achieve a sufficiently robust architecture. These requirements are referred to as *architectural constraints*, and their intention is to have one (or more) additional channels that can activate the SIF in case of a fault within the SIS. The architectural constraints prevent SIS designers and system integrators from selecting architecture based on PFD calculations alone, and the requirements may therefore be seen as restrictions in the freedom to choose hardware architecture.

For each part of the SIS, the architectural constraints are expressed by the hardware fault tolerance (HFT), which again is determined by the type of the components (type A or B), the safe failure fraction (SFF), and the specified SIL. The SFF is the proportion of "safe" failures among all failures and the HFT expresses the number of faults that can be tolerated before a SIS is unable to perform the SIF. A "safe" failure is either a failure that is safe by design, or a dangerous failure that is immediately detected and corrected. The IEC standards [1,2] define a safe failure as a failure that does not have the potential to put the SIS in a hazardous or fail-to-function state. A dangerous failure is a failure that can prevent the SIS from performing a specific SIF, but when detected soon after its occurrence, for example, by online diagnostics, the failure is considered to be "safe" since the operators are notified and given the opportunity to implement compensating measures and necessary repairs. In some cases, the SIS may automatically respond to a dangerous detected failure as if it were a true demand, for example, causing shutdown of a process section or the whole plant.

* Corresponding author. Tel.: +47 73 59 7101; fax: +47 73 59 7117.
E-mail address: mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.06.003

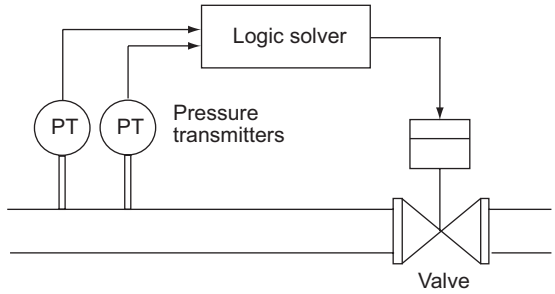

Fig. 1. Illustration of a SIS.

The architectural constraints are sometimes interpreted as a mistrust to the quantitative reliability analysis. Reliability experts frequently debate whether or not the architectural constraints are necessary, and if the SFF–HFT–SIL relationship is well-founded. It is particularly the suitability of the SFF that has been questioned [3–5].

The objectives of this article are to (i) provide more insight into the architectural constraints and how the HFT is determined from the type of components and the SFF, (ii) discuss and illustrate by case studies the non-intended effects of a high SFF, and (iii) decide whether or not SFF and HFT are useful concepts related to SIFs.

The article is organized as follows: The rationale for introducing the architectural constraints and for relating the architectural constraints to the SFF is discussed in Section 2. Whether or not a high SFF implies a high safety level is discussed in Section 3. The main characteristics and properties of the SFF are further analyzed and discussed in Section 4 based on two simple case studies. In Section 5, we discuss whether the concept of architectural constraints is really needed. In Section 6, we conclude and discuss the findings of the article and present some ideas for future work.

2. Hardware fault tolerance and safe failure fraction

The HFT gives restrictions to hardware architecture [6–8]. If HFT = 1 is specified, the selected configuration must tolerate one failure without affecting the SIF. Configurations that provide HFT = 1, are, for example, 1oo2, 2oo3, and 3oo4, where a *koon* system is functioning if at least k out of n components are functioning. The HFT needed to comply with a specified SIL is determined by the component type and the SFF.

SFF is a property of a component or component group. The IEC standards [1,2] define SFF as the proportion of "safe" failures among all component failures

$$\mathrm{SFF} = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \quad (1)$$

where λ_S is the rate of safe failures, λ_{DD} is the rate of dangerous detected (DD) failures, and λ_{DU} is the rate of dangerous undetected (DU) failures of a component.

An alternative representation of (1) is to express SFF as a conditional probability:

$$\mathrm{SFF} = \Pr(\text{The failure is "safe"} | \text{A component failure occurs}) \quad (2)$$

Hence, we may interpret SFF as a measure of the inherent safeness of a component, that is, to what extent the component responds in a safe way when a failure occurs.

The second parameter that is used to determine the HFT, is the component type. IEC 61508 [1] distinguishes between type A and type B components. A type A component is characterized by: (i) all failure modes are well defined, (ii) the behavior of the component under fault conditions is well known, and (iii) field data are dependable and able to confirm the failure rates that are claimed. The last criterion is often referred to as "proven in use." A type B component does not fulfill one or more of these criteria. IEC 61511 [2] uses a slightly different classification, and distinguishes between programmable electronic (PE) logic solvers on one side and non-PE-logic solvers/field devices on the other side. In practice, PE-logic solvers are classified as type B according to IEC 61508, while non-PE-logic solvers may fulfil the criteria for type A. Field devices may in some cases be type A and in other cases type B, depending on how many advanced (and programmable) features they have.

Table 1
SFF–HFT–SIL relationship in IEC 61508

SFF	0	1	2
HFT requirements (type A)			
<60%	SIL1	SIL2	SIL3
60–90%	SIL2	SIL3	SIL4
90–99%	SIL3	SIL4	SIL4
>99%	SIL3	SIL4	SIL4
HFT requirements (type B)			
<60%	–	SIL1	SIL2
60–90%	SIL1	SIL2	SIL3
90–99%	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

IEC 61508 [1] provides separate SFF–HFT–SIL relationships for type A and type B components, see Table 1. To our knowledge, the SFF–HFT–SIL relationship is not theoretically founded, but based on a previous concept of a diagnostic (DC)–HFT–SIL relationship [8]. In the table, the SFF is split into four intervals; below 60%, between 60% and 90%, between 90% and 99%, and above 99%. Similarly, IEC 61511 [2] suggests two separate tables, one table for non-PE-logic solvers/field devices and one table for PE-logic solvers, to reflect sector specific categories of components. The main differences between the approach taken in IEC 61508 and IEC 61511, are [3,9]:

- IEC 61511 does not treat SIL 4 systems; in this case the standard refers to IEC 61508.
- IEC 61511 does not give additional credit for SFF above 99%, whereas IEC 61508 does.
- In IEC 61511, the HFT table for non-PE-logic solvers/field devices is independent of the SFF. It is assumed that such devices, when built for safety applications, have SFF in the area of 60–90%. The HFT–SIL relationship proposed for non-PE-logic solvers/field devices corresponds to the HFT–SIL relationship for PE-logic solvers with SFF between 60% and 90%.
- IEC 61511 allows a reduction in HFT by one for non-PE-logic solvers/field devices if certain conditions, for example being proven in use, are met. Having fulfilled these conditions, the HFT–SIL relationship corresponds to the HFT–SIL relationship for type A components in IEC 61508, provided that the SFF is between 60% and 90%.
- IEC 61511 suggests increasing the HFT by one for non-PE-logic solvers/field devices, if the dominant failure mode is DU rather than safe or DD. In other words, if the SFF is below 50%, which may be the case for an "energize to trip" device, it is required to increase HFT by one. In this situation, IEC 61511 requires higher HFT than IEC 61508 for devices that fulfil the criteria of being type A and with SFF <60%.

It is therefore not a one-to-one relationship between the HFT tables in IEC 61508 and IEC 61511, but in most cases, we will end up with the same requirement for HFT for the same SFF and SIL.