Reliability Engineering and System Safety 159 (2017) 206–213

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Using field feedback to estimate failure rates of safety-related systems

Florent Brissaud

RAMS industry (.eu), France

ARTICLE INFO

Keywords:
Functional safety
Safety-related systems
Safety integrity
Failure rate
Field feedback
Confidence intervals
Detected failures
Undetected failures
PFDavg
PFH
Uncertainties

ABSTRACT

The IEC 61508 and IEC 61511 functional safety standards encourage the use of field feedback to estimate the failure rates of safety-related systems, which is preferred than generic data. In some cases (if “Route 2_H” is adopted for the "hardware safety integrity constraints”), this is even a requirement. This paper presents how to estimate the failure rates from field feedback with confidence intervals, depending if the failures are detected on-line (called "detected failures", e.g. by automatic diagnostic tests) or only revealed by proof tests (called "undetected failures"). Examples show that for the same duration and number of failures observed, the estimated failure rates are basically higher for “undetected failures” because, in this case, the duration observed includes intervals of time where it is unknown that the elements have failed. This points out the need of using a proper approach for failure rates estimation, especially for failures that are not detected on-line. Then, this paper proposes an approach to use the estimated failure rates, with their uncertainties, for PFDavg and PFH assessment with upper confidence bounds, in accordance with IEC 61508 and IEC 61511 requirements. Examples finally show that the highest SIL that can be claimed for a safety function can be limited by the 90% upper confidence bound of PFDavg or PFH. The requirements of the IEC 61508 and IEC 61511 relating to the data collection and analysis should therefore be properly considered for the study of all safety-related systems.

1. Introduction to safety-related systems

Safety-related systems are designed to prevent hazardous events and/or to mitigate their effects. To this end, these systems implement safety functions. A safety function intends to achieve or maintain a safe state of equipment/system/installation, in respect to a specific hazardous event. In practise, safety-related systems are then used to reduce risks for making them tolerable.

Due to the critical role of safety-related systems for managing risks, “functional safety” standards have been developed. Notably, the IEC 61508 [1] provides a generic approach for all safety lifecycle activities of safety-related systems based on Electrical and/or Electronic and/or Programmable Electronic (E/E/PE) technology, from the concept to the decommissioning phase. Product and application sector standards have then been developed based on the IEC 61508, such as the IEC 61511 [2] for the Safety Instrumented Systems (SIS) used in the process industries. An SIS is a safety-related system composed of any combination of sensor(s), logic solver(s), and final element(s). The work described in this paper comes within the scope of these standards. However, the proposed results can be applied to any safety-related system (other than E/E/PE and SIS).

The “safety integrity” (cf. Section 2.1) of a safety-related system is affected by different kinds of dangerous[1] failures. First, a failure can be “systematic” (in hardware or software), that is, “related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors” [1] (ref. Part 4, Section 3.6.6) or “random” (in hardware), that is, “occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware” [1] (ref. Part 4, Section 3.6.5). Second, the failures can be detected on-line (e.g. by automatic diagnostic tests), and called “detected failures”, or undetected on-line but only revealed by proof tests (e.g. periodic test performed to detect hidden failures), and called “undetected failures”.

The purpose of this paper is to present how to estimate the rates of detected and undetected failures from field feedback, for safety-related systems. As claimed in the IEC 61508, “failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted” [1] (ref. Part 4, Section 3.6.5). Therefore, the scope of this paper is limited to random hardware failures.

Section 2 presents the functional safety requirements, as per IEC 61508 and IEC 61511, with regards to the safety integrity and to the requirements for the failure rates estimation from field feedback. Then, Section 3 presents how to estimate the failure rates from field feedback

[1] “Dangerous” means that the failure prevents the safety function from, or decrease its probability of, operating when required. According to the IEC 61508, only these failures are considered within the PFDavg or PFH (cf. Section 2.1).

http://dx.doi.org/10.1016/j.ress.2016.11.003
Received 30 May 2016; Received in revised form 30 September 2016; Accepted 12 November 2016
Available online 14 November 2016

with confidence intervals, considering both detected and undetected failures. An approach to use these estimated failure rates, with their uncertainties, for PFDavg and PFH (cf. Section 2.1) assessment with upper confidence bounds is finally proposed in Section 4.

2. Functional safety requirements

2.1. Safety integrity

The safety integrity is the ability of a safety-related system to perform the required safety function as and when required (i.e. its dependability with regards to the safety function). The safety integrity comprises hardware safety integrity (relating to random hardware failures, cf. Section 1) and systematic safety integrity (relating to systematic failures, cf. Section 1), which also includes the software safety integrity (when the systematic failures are attributable to software). However, the "systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can)" [1] (ref. Part 4, Section 3.5.6).

According to the IEC 61508 and IEC 61511, the safety integrities are arranged in Safety Integrity Levels (SIL), from SIL 1 (for the lowest integrity level) to SIL 4 (for the highest integrity level). Based on the hazard and risk analysis, the allocation phase (among the other activities defined in the safety lifecycle) aims at defining a target failure measure and an associated SIL for each safety function to be carried out by the safety-related system. Depending on the mode of operation of the safety function, the failure measure is specified in terms of:

- the average probability of a dangerous failure on demand of the safety function (PFDavg), if the safety function is only performed on demand and the frequency of demands is no greater than one per year (i.e. low demand mode); or
- the average frequency of a dangerous failure of the safety function [per hour] (PFH), if the safety function is only performed on demand and the frequency of demands is greater than one per year (i.e. high demand mode) or if the safety function retains the equipment/system/installation in a safe state as part of normal operation (i.e. continuous mode).

If the target failure measure[2] is PFDavg $< 10^{-x}$ (for a low demand mode), then the associated SIL is x (with x=1, …, 4); if the target failure measure is PFH $< 10^{-(x+4)}$ (for a high demand or continuous mode), then the associated SIL is x (with x=1, …, 4).

The SIL, with the target failure measure, are part of the safety requirements specification (among other requirements, notably those relating to the safety function). Then, the realisation/design phase aims at creating a safety related-system that meet these specified safety requirements. Notably, the quantification of the effect of random hardware failures consists in estimating the achieved PFDavg or PFH, which shall be below the target failure measure. The next subsection refers to the hardware safety integrity requirements, taking part of the realisation/design phase, that concern the failure rates estimation from field feedback.

2.2. Requirements for failure rates estimation from field feedback

It is stated in the IEC 61508 that [1] (ref. Part 2, Section 7.4.4):

> "the highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes (to be implemented at system or subsystem level):
>
> – Route 1_H based on hardware fault tolerance and safe failure fraction concepts; or,
> – Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels."

The "safe failure fraction" (SFF) is used by Route 1 $_H$ (cf. [1], Part 4, Section 3.6.15, for the definition of the SFF). However, the SFF has been questioned several times [3,4]. Basically, "the use of the SFF as a safety criteria is a lack of discernment" notably because "the SFF can be artificially increased just by adding (or overestimating) safe failures" [5]. Therefore, "Route 2_H shall be preferred than Route 1_H as far as possible" [5]. Regarding the IEC 61511, the SFF is not applicable since the second edition of the standard (published in February 2016) and the "requirements for hardware fault tolerance" derive from Route 2_H of the IEC 61508.

The description of Route 2_H is not within the scope of the present paper (cf. [1], Part 2, Section 7.4.4.3, for the description of Route 2_H). However, regarding the failure rates estimation from field feedback, a dedicated requirement is defined [1] (ref. Part 2, Section 7.4.4.3.3):

"If Route 2_H is selected, then the reliability data used when quantifying the effect of random hardware failures shall be:

a) based on field feedback for elements in use in a similar application and environment; and,
b) based on data collected in accordance with international standards (e.g., IEC 60300-3-2 or ISO 14224:); and,
c) evaluated according to:
  i) the amount of field feedback; and,
  ii) the exercise of expert judgement; and where needed,
  iii) the undertaking of specific tests;

in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

In addition, it is stated (regardless of Route 1_H or 2_H) that [1] (ref. Part 2, Section 7.4.9.5):

"The estimated failure rates, due to random hardware failures, for elements can be determined either

a) by a failure modes and effects analysis of the design using element failure data from a recognised industry source; or
b) from experience of the previous use of the element in a similar environment.

NOTE 1 Any failure rate data used should have a confidence level of at least 70%. (…).

NOTE 2 If site-specific failure data are available then this is preferred. If this is not the case then generic data may have to be used."

The IEC 61511 is a bit less prescriptive but based on the same philosophy.

Therefore, the IEC 61508 and IEC 61511 encourage the use of field feedback to estimate the failure rates (under reasonable conditions), which is preferred than generic data (such as PDS Data Handbook [6] or OREDA [7], especially if the elements are not in use in a similar application and environment). If Route 2_H (from IEC 61508) is adopted (and therefore not using the controversial SFF), this is even a requirement. Moreover, the failure rates should be estimated with confidence intervals. These estimations are the purpose of Section 3.

Finally, the IEC 61508 also specifies that [1] (ref. Part 2, Section 7.4.4.3.3):

"If route 2_H is selected, then the reliability data uncertainties shall be taken into account" for PFDavg or PFH assessment and, "the system shall be improved until there is a confidence greater than 90% that the target failure measure is achieved".

The same requirement is given by the IEC 61511 [2] (ref. Part 1, Section 11.9.4), but independently of Route 2_H and the level of

[2] In some practise, a target SIL is chosen *a priori* and the target failure measure is defined *a posteriori* such as the following requirement is met.