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. S, NO 7491 Trondheim, Norway

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.

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

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 leaks, 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.
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 koo n 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

\[
SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}}
\]  

(1)

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

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

\[
SFF = Pr(\text{The failure is “safe”}|\text{A component failure occurs})
\]  

(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. IEC61508 [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. IEC61511 [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 IEC61508, while non-PE-logic solvers may fulfill 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.

IEC61508 [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, IEC61511 [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 IEC61508 and IEC61511, are [3,9]:

- IEC61511 does not treat SIL 4 systems; in this case the standard refers to IEC61508.
- IEC61511 does not give additional credit for SFF above 99%, whereas IEC61508 does.
- In IEC61511, 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%.
- IEC61511 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 IEC61508, provided that the SFF is between 60% and 90%.
- IEC61511 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, IEC61511 requires higher HFT than IEC61508 for devices that fulfill the criteria of being type A and with SFF <60%.

It is therefore not a one-to-one relationship between the HFT tables in IEC61508 and IEC61511, but in most cases, we will end up with the same requirement for HFT for the same SFF and SIL.

---

Table 1

<table>
<thead>
<tr>
<th>HFT requirements (type A)</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60%</td>
<td>SIL1</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>60–90%</td>
<td>SIL2</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
<tr>
<td>90–99%</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL4</td>
</tr>
<tr>
<td>&gt; 99%</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HFT requirements (type B)</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60%</td>
<td>–</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>60–90%</td>
<td>SIL1</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>90–99%</td>
<td>SIL2</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
<tr>
<td>&gt; 99%</td>
<td>SIL3</td>
<td>SIL4</td>
<td>SIL4</td>
</tr>
</tbody>
</table>
In this article, we focus on the IEC 61508 approach, as this is adopted by many oil and gas companies and also by OLF-070 [10]. From Table 1, we note that:

- Components of type B require a higher HFT than components of type A, for the same SIL and SFF.
- The required HFT increases when the SFF decreases.
- The required HFT increases with increasing SIL.

For configurations of different types of components, for example, PTs and level transmitters, it is not possible to use the HFT tables directly, since the components may have different SFF. Instead, IEC 61508 [1] suggests that the achievable SIL is first determined for the individual components. A set of rules is then used to find the achievable SIL for the total configuration. These rules, which we refer to as merging rules, are further explained in [3].

3. Does high SFF indicate safe design?

As seen from Table 1, SFF is a crucial parameter when selecting hardware architecture as required by IEC 61508. Configurations based on components with SFF > 90% may require a lower HFT than for components with SFF of, for example, 75%. We may therefore deduce that components with high SFF are preferred to a similar components with low SFF. But does a high SFF indicate safe design?

Reliability experts, system integrators, and end users have questioned the suitability of SFF as an indicator of a safe design. Some concerns that have been raised, are:

- “Safe” failures are not always positive for safety. The SFF is based on the assumption that the SIS response to safe and DD-failures is safe, for the SIS as well as for the plant. However, the SIS response may sometimes induce new hazardous events [4,5]. Langeron et al. [11] argue that safe failures may evolve into dangerous failures, and therefore that the SFF is not an indicator of a safe design. A spurious closure of a shutdown valve may, for example, lead to water hammer effects that can deteriorate the valve and also affect a number of other components. Operators may lose confidence in the SIS if there are frequent alarms caused by “safe” SIS failures. There are several examples where operators have bypassed safety functions that have caused frequent alarms or process disturbances. In addition, human errors during repair and restoration of the SIS may introduce new failures.

- The SFF may credit unneeded hardware. The SFF gives credit to a high rate of “safe” failures, and for producers it is a business advantage to claim a high SFF. With a high SFF, components may be used in configurations with low HFT, which means lower cost for the customers. At present, the IEC standards [12] give little guidance to what type of safe failures to include in the SFF calculations. As a result, producers may use different approaches when calculating the SFF. Some include all types of safe failures, while others include only those failures that are relevant for the performance of the SIF (e.g., spurious operation failures). The PDS method [12] suggests that failures of non-critical components are omitted, which at least prevent these failures from being included with the purpose of increasing the SFF. This approach is supported by CCPS [6], which also poses additional constraints on the calculations by suggesting that only DD-failures that automatically lead to a safe state of the process are considered in the calculations.

- Sometimes the SFF is only calculated for parts of the components. IEC 61508 [1] covers electrical, electronic, and PE components, and as a result, producers may sometimes calculate SFF for this part of the component, and assume that the mechanical part is functioning perfectly. In this case, the SFF may not reflect the performance of the component as a whole [13].

- If the PFD is affected by uncertain reliability data, then so is the calculated SFF. The architectural constraints are meant to compensate for the uncertainty in the PFD estimate. However, if the reliability data that are used to find the PFD are uncertain, the data used to calculate the SFF are usually even more uncertain. Experience from the OREDA project has clearly shown that safe failures get less attention than dangerous failures in the data collection [14].

Despite these concerns, it is sometimes claimed that the SFF is “good for safety”, since safe failures and DD-failures that lead to activation of final elements may act as functional tests. However, the reliability gain from this additional testing may be counteracted by the reliability loss due to stress during spurious activations.

4. SFF characteristics

The characteristics of the SFF become more clear if we rewrite Eq. (1), such that

\[
SFF = \frac{\lambda_S}{\lambda_{tot}} + DC \frac{\lambda_D}{\lambda_{tot}}
\]  

(3)

where \(\lambda_{tot} = \lambda_S + \lambda_{DD} + \lambda_{DU}\), \(\lambda_D = \lambda_{DD} + \lambda_{DU}\), and DC the diagnostic coverage (of dangerous failures) defined by DC = \(\lambda_{DD}/(\lambda_{DD} + \lambda_{DU})\).

From Eq. (3), some characteristics of the SFF become evident:

(1) Two components with the same total failure rate and the same SFF do not necessarily have the same properties. One component may have a higher rate of safe failures (compared to the total failure rate) than the other, while the the other component has a higher DC.

(2) The SFF is a relative number and components with the same SFF–DC relationship may therefore have quite different properties. A component with a high rate of safe failures and a high total failure rate, may have the same SFF as another component with lower failure rates.

As a result, the SFF does not necessarily indicate whether or not a component has a safe design. If a high SFF is obtained by a high rate of safe- and/or DD-failures, these failures may create a higher rate of hazardous events, as indicated in Section 2. The ambiguity of the SFF is further illustrated in two case studies.

4.1. Case studies

Two case studies have been designed to illustrate that:

(i) the SFF may have ambiguous effects on safety and production availability;

(ii) the SFF may favor unsafe design of components.

**Case study I: SFF versus safety and production availability.** In this case study, we study how the various properties of a single component can affect safety and production availability. The following component properties are used to illustrate the effects:

- the initial failure rates for safe and dangerous failures are equal to \(1 \times 10^{-6}\) failures per hour;

- the probability of a component to be in a functional state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.

- the probability of a component to be in a dangerous state is 0.05.

- the probability of a component to be in an unknown state is 0.05.

- the probability of a component to be in a safe state is 0.95.
The tree structure in Fig. 2 shows how the SFF, the safety, and the production availability are affected by high and low values of λ₀, λ₀, and DC, respectively. We assume that the production availability is influenced by the spurious trip rate (STR) of the component. For a single component, the STR is given by [15,16]

$$STR \approx \lambda_{SO} + \lambda_{DD}$$

where λ₀ is the rate of spurious operation failures [15]. In this case study, we assume that all safe failures give a spurious operation, such that λ₀ = λ₀. In addition, we assume that the system is configured such that a trip occurs when a DD-failure is detected [15,16], but other operating philosophies may also be selected [12,15,16].

It is further assumed that safety is measured by the average PFD, which for a single component is [17]

$$PFD \approx (1 - DC) \times \frac{\lambda_{DD} \tau}{2} = \frac{\lambda_{DD} \tau}{2}$$

where τ is the functional test interval. The formula is valid when the component is restored to an “as good as new” condition after each functional test, the test and repair times are negligible compared to the length of the functional test interval, and when safe- and DD-failures are detected immediately and restored within a short time compared to the functional test interval. The PFD is seen to decrease when the dangerous failure rate decreases and/or when the DC increases. Eq. (5) does not take into account any potential, secondary effects on safety from safe- and DD-failures.

The SFF is calculated from Eq. (1). With the suggested input data, the SFF is either below 60% or above 90%. In Fig. 2, an SFF below 60% is marked as low (L) and above 90% as high (H). We assume that 1 × 10⁻³ is the PFD target for the component, and classify an average PFD below this target as positive for safety (+), and above this target as negative for safety (−). Similarly, we assume that a high rate of safe failures and/or a high rate of DD-failures corresponds to a high STR which is negative for the production availability (−). With the given input data, this means that an STR above 9.1 × 10⁻⁶ failures per hour is considered as negative for the production availability, and an STR below this rate is considered as positive.

As seen from Fig. 2, a high SFF often has a positive effect on safety, but in some cases, when a high SFF has been derived from high failure rates, the safety may suffer. A high SFF may be both positive and negative for production availability, depending on the magnitude of the rates of safe- and DD-failures. From this simple example, it is evident that the SFF has ambiguous effects on safety and production availability.

Case study II: SFF versus safe design. The unintended effects of the SFF become even more evident if we take the producer’s perspective and decide to improve the SFF of a certain type of component. In this case study, the producer may choose between the following strategies:

(1) The component is redesigned so that internal sub-component failures lead to a safe, rather than a dangerous component failure. In many cases, reduction of the rate of dangerous failures corresponds to a comparable increase in the rate of spurious operation failures (e.g., by installing a spring return so that the specified safe position upon loss of power).

(2) The component is designed with more reliable sub-components, so that the rates of safe as well as dangerous failures decrease (e.g., by improving a valve actuator with more robust spring materials and better protection against leakage).

(3) The component is redesigned with less reliable sub-components so that the rate of spurious operations increases, while we assume that the rate of dangerous failures remains unchanged (e.g., by reducing the seal quality of a fail-safe valve actuator such that we get more frequent hydraulic leakages).

(4) The producer adds new hardware and software to the current design to detect a fraction of the previously undetectable dangerous failures, such that the DC increases (e.g., by adding an online sonic leak detection system to a valve).

(5) The component is redesigned to make it less vulnerable to spurious operation. We may assume a lower rate of spurious operation, while the rate of dangerous failures remain unchanged (e.g., by improving a valve actuator so that less frequent leakages may be expected).

In Table 2, the effects of these five design changes are shown with respect to “good engineering practice” and SFF. Good engineering practice may be considered as design in accordance with relevant standards and regulations with the purpose of preventing hazardous events [18]. For components used in a SIS application, good engineering practice is a means to ensure safe and reliable components.

The case study shows that some improvements that are in accordance with good engineering practice, for example, cases 2 and 5, have no, or a negative effect on the SFF. This means that the SFF does not encourage such design changes. The case study also shows that modifications leading to a worse design, for example, as shown in case 3, is given credit through a higher SFF. For cases 1 and 4, the SFF responds as expected, that is, the SFF increases when the improvements are in line with good engineering practice.

One may question if there is a logical reasoning behind the relationship between SFF and HFT. HFT is a measure of the robustness against component failures, that is, the ability of the SIF to be activated in the presence of dangerous failures in one or more channels. Linking safe failures to architecture robustness does not seem reasonable, since the safe failures do not have the potential to prevent the SIF from performing its function. In fact,
the safe failures may cause the SIF to be activated when this is not intended. Thus, we may claim that there is no well-founded reason for reducing the HFT if the high SFF is based on a high fraction of safe failures.

5. Do we need the architectural constraints at all?

The rationale for introducing the architectural constraints is to “achieve a sufficiently robust architecture, taking into account the level of subsystem complexity” [1,2]. The underlying concern is that quantitative assessments alone may underestimate the reliability, and as a result, lead to selection of unsafe architectures. The IEC standards [1,2] assume that the reliability increases with increasing HFT. But does the architectural constraints lead to more reliable architectures?

One immediate effect of increasing the HFT is that the STR increases [15]. As mentioned in Section 3, more frequent spurious trips may have a negative effect on safety, due to the secondary effects from process disturbances, like stress on affected physical components as well as on the personnel. The correlation between HFT and reliability improvements may be further questioned in cases where:

- The SIF is likely to fail due to common cause failures (CCF) rather than independent failures. Higher HFT makes the SIF less vulnerable to independent (random) dangerous failures. However, if redundant components share the same or similar design principles, follow-up, or are exposed to same operational and environmental conditions, one may experience that two or more components fail simultaneously. These CCFs [19–21] will reduce the reliability benefit from increasing the HFT.
- The reliability model is incomplete. HFT is considered for those components that have been identified to have an effect on the SIS’s ability to perform the SIF and, consequently, are included in the reliability model. If the SIS is complex, have complex interactions with other systems, or if we have not put enough effort into understanding the complete SIF loop, we may fail to capture all relevant components. If some of these unidentified components alone may cause failure of the SIF, a higher HFT of the identified components may not lead to a more reliable system.

An additional concern when increasing the HFT is that we add complexity and potentially new vulnerabilities to the SIS. As a result, we may experience that the reliability is reduced rather than increased by raising the HFT.

One argument that may support a higher HFT, at least at first glance, is the potential for systematic failures. Systematic failures are safe and dangerous failures caused by design errors, implementation errors, installation errors, and operation and maintenance related errors. Systematic failures also embrace software failures, and failures that are due to the selection of inappropriate hardware for the current environmental conditions. The IEC standards [1,2] recommend that systematic failures are omitted in the PFD calculations, since they do not have the same predictable characteristics as random hardware failures. HFT can therefore be a means to compensate for systematic failures. Operational experience indicates that a significant fraction of SIS failures are systematic rather than random hardware failures [1,2,12,17]. Some reliability databases, like OREDA [14], therefore include systematic failures in their failure rate predictions. Other reliability databases cover only random hardware failures. This is, for example, the case for MIL-HDBK-217F [22], where the data come from controlled laboratory testing.

The robustness against systematic failures from raising the HFT may not be as high as expected. First of all, the systematic failures may be safe as well as dangerous, which means that the frequency of process disturbances increases with increasing HFT. Secondly, the causes of systematic failures often share the properties of CCF causes [20], and a systematic failure is therefore likely to affect several components rather than a single component. As discussed above, a higher HFT has a limited effect on the reliability of the SIF if a considerable fraction of the failures are due to CCFs.

6. Discussion and further work

According to the IEC standards [1,2], the SIS hardware architecture must be selected so that (i) the calculated reliability meets the specified SIL, and (ii) the HFT is according to the architectural constraints. In some cases, the architectural constraints call for higher HFT than is necessary based on the reliability calculations. End users and system integrators have therefore questioned the need for architectural constraints, and whether architectural constraints lead to safer design. Their concern has been addressed and discussed in this article.

The architectural constraints specify a minimum HFT for each subsystem (input elements, logic solver, final elements) based on the SIL target, the component type, and the SFF. The IEC standards use the SFF as a measure of inherent safeness of components, and allow lower HFT for configurations of components with high SFF. This article has critically examined the properties of the SFF in two case studies, and investigated if a high SFF necessarily leads to a safe design. Based on the case studies, we conclude that:

- The SFF is not an adequate indicator of a component’s reliability properties. Two components with the same SFF may have quite different characteristics with respect to rate of spurious operations, rate of dangerous failures, and DC.
- A high SFF does not always indicate a safe component, in the same way as a low SFF is not always synonymous with an unsafe component. The SFF may give credit (in terms of increased SFF) to unsafe designs as well as punishment (in terms of unchanged or decreased SFF) for safe designs.

We have argued that reliability models and reliability data may fail to capture all failures of a SIF. One example is that reliability calculations often omit the contribution from systematic failures.
In fact, IEC 61508 suggests that these failures should not be included in reliability calculations, and argue for other means to identify and prevent such failures, for example, use of checklists. The increasing use of PE-logic solvers and smart field devices, will inevitably lead to more failures with systematic causes, introduced during design, construction, and sometimes also during operation, maintenance, and modifications. Adding more HFT to such functions may increase the robustness against systematic failures, but will also increase the system complexity.

A project has recently been initiated to study the relationship between the SFF and the PFD, using Markov methods [23]. It may be useful to explore the results from this project, to gain more insight into the effects of high and low SFF.

More research should be devoted to treat systematic failures in reliability assessments. New methods to predict and analyze systematic failures should be developed. A first steps in this development has been taken by the PDS project [12]. In a new method, the contribution from software failures represents a major challenge. Hardware functions are increasingly being replaced by software implemented functions, to allow new and more flexible technical solutions and to save costs. The cost of writing software code once is lower than the cost of having hardware in all systems. As mainly hardware components are catered for in reliability calculations, it is a need to clarify how the contribution from systematic failures may affect the reliability of SIS.

As a supplement to the architectural constraints, we believe that more attention should be directed to the construction of reliability models, and the system and functional analyses on which the models are based. With more complex features of SIS components it is important to analyze the functionality of each SIS component, rather than assuming a certain behavior, and also to take into account their interactions. Such a qualitative analysis gives two benefits: improved reliability models and improved insight into the SIS functionality.

Acknowledgments

We would like to thank the reviewers of this article for well-considered and useful inputs and comments.

References