Can Functional Tests Be Replaced By Inspection After Demands?

Hui Jin
Department of Quality and Production Engineering
Norwegian University of Science and Technology
Trondheim, NO-7491, Norway
hui.jin@ntnu.no

Mary Ann Lundteigen, Professor
Department of Quality and Production Engineering
Norwegian University of Science and Technology
mary.a.lundteigen@ntnu.no

Marvin Rausand, Professor
Department of Quality and Production Engineering
Norwegian University of Science and Technology
marvin.rausand@ntnu.no

Prepared for Presentation at
American Institute of Chemical Engineers
2011 Spring Meeting
7th Global Congress on Process Safety
Chicago, Illinois
March 13-16, 2011

UNPUBLISHED

Can Functional Tests Be Replaced By Inspection After Demands?

Hui Jin
Department of Quality and Production Engineering
Norwegian University of Science and Technology
Trondheim, NO-7491, Norway
hui.jin@ntnu.no

Mary Ann Lundteigen, Professor
Department of Quality and Production Engineering
Norwegian University of Science and Technology
mary.a.lundteigen@ntnu.no

Marvin Rausand, Professor
Department of Quality and Production Engineering
Norwegian University of Science and Technology
marvin.rausand@ntnu.no

Keywords: Medium demand, Response to demands, PFD, Test coverage, Inspection

Abstract

Safety instrumented systems are used to reduce the risk of accidents in the process industry. To claim a certain risk reduction from such systems, it is necessary to perform reliability analyses, based on internationally accepted frameworks, such as IEC 61508 and IEC 61511. The main factors that influence the reliability are the failure rates of the components, the level of redundancy of hardware and software, and the frequency of periodic functional tests. The need for periodic functional testing has always been a challenge for the industry, as the tests often mandate a shorter or longer stop of the production. For those safety instrumented systems that must respond to rather frequent demands, the industry has started to ask if it is possible to replace some functional tests with thorough inspections after demands, and how information from responses to demands and the following inspections may be credited in the reliability analyses. This paper discusses the main characteristics of such a "testing strategy", and highlights some of the cautions, challenges, and conditions of use.

1. Introduction

Safety instrumented systems (SISs) are widely used as protection layers in the process industry, and a number of standards and guidelines have been published to assist the design, implementation, and follow-up of such systems. One of the most important standards is IEC 61508 [1], which outlines the key requirements in all phases of the SIS life-cycle. IEC 61508 is the basis for sector specific standards, such as IEC 61511, which applies to the process industry [2]. Both IEC 61508 and IEC 61511 have been adopted in many countries, for land-based process industry as well as for the offshore oil and gas industry. In the Unites States, IEC 61511 has been adopted with minor amendments and is referred to as ANSI/ISA 84.00.01-2004 [3].

IEC 61508 differentiates between two modes of operation, *low-demand* and *high/continuous-demand* mode of operation. In the recent edition of IEC 61508, different definitions are given to high-demand and continuous-demand mode, but throughout the rest of the standard, they are treated the same [1]. In IEC 61511, the corresponding modes are called demand mode and continuous mode of operation, but with the same interpretation as in IEC 61508 [2]. According to IEC 61508, a SIS is operated in a high/continuous-demand mode when the demand rate is greater than once per year (the test interval related criterion is removed in the recent edition of IEC 61508); otherwise it is operated in a low-demand mode [1].

The process industry employs the principle of having several independent layers of protection, in addition to the basic control system. Most SISs are therefore low-demand rather than high/continuous-demand and remain passive as long as the process is running normally. At the same time, the process industry has identified several other functions as safety-critical, and given requirements for their reliability in accordance with IEC 61508 and IEC 61511, even if the functions are needed for normal control as well as in response to hazardous events. Equipment used for well intervention and drilling operations, such as the blowout preventer (BOP) is, for example, used both during normal drilling operations and for isolation of the well in case of uncontrolled flow from the well. Such equipment is therefore operated in the high-demand mode, even if only a fraction of the demands are critical.

Recently, some manufacturers and oil companies have raised the question whether successful responses to demands, such as the non-critical demands in relation to well intervention equipment, may be credited as functional tests in reliability assessments of the safety functions [4]. So far, however, this issue has been given little attention and methods are therefore lacking. The aim of this paper is to clarify this issue and also to suggest ways to assess the reliability. More specifically, the objectives are to (i) discuss the possibility of taking credit from responses to demands in SIS reliability assessment for some specific situations, (ii) present PFD calculation formulas when responses to demands are considered, (iii) present ways to follow-up the SIS reliability when the credits from responses to demands are taken.

2. Reliability measures

A *demand* may be defined as an event or a condition that requires response by a safety related function that is performed by either a SIS or a non-SIS system. A system that uses the *same* type of components to perform safety as well as non-safety functions is exposed to a combination of (safety) critical demands and non-critical demands. In total, the demand rate may correspond to the high-demand mode, whereas the rate of the critical demands may fall in the low-demand mode. In order to avoid possible confusion and to cover systems responding to critical and non-critical demands, the expression, *safety related system* (SRS), is used in this paper. An SRS is further split into three subsystems [5]: (i) the input subsystem (e.g., sensors, transmitters), (ii) the logic solver subsystem (e.g., programmable logic controllers [PLC], relay logic systems), and (iii) the actuating subsystem (e.g., safety valves, circuit breakers). A subsystem may have one or more components. In the case of more than one component in a subsystem, the components usually work as a redundant configuration.

IEC 61508 and IEC 61511 suggest two different reliability measures for the two modes of operation: The average *probability of failure on demand* (PFD) for the low-demand mode and the average *probability of a dangerous failure per hour* (PFH) for the high-demand/continuous mode. IEC 61508 and IEC 61511 distinguish between four safety integrity levels (SILs), to each SIL, a certain PFD or PFH requirement range applies (IEC 61511 refers to IEC 61508 for the SIL 4 requirements).

When a demand for the SRS safety function occurs, the PFD is the average probability that the SRS fails to perform its safety function upon a demand. Depending on the placement of the SRS in the sequence of protection layers, the failure will have two different consequences: (i) if the SRS is the last protection layer, the failure will lead to an accident in the system. While (ii) if it is not the last protection layer, the failure will lead to a demand for the next layer. PFH is the frequency of demands for the next protection layer due to a SRS failure, or the accident frequency if the SRS is the ultimate protection layer.

The required PFD, corresponding to the required amount of risk reduction, may be determined from a hazard and risk analysis, supported by methods such as LOPA and risk graph, or by a simplified approach using, for example, the minimal SIL requirements suggested in the Norwegian guideline OLF 070 on the application of IEC 61508 and IEC 61511[6]. The required PFH is equal to or less than the acceptable frequency of a certain type of event or accident.

It is then up to the SRS manufacturer and system operator to compare the estimated reliability of each safety function with the required PFD or PFH. After the SRS has been installed, it is the responsibility of the end user to collect data, to make new reliability predictions, and make necessary improvements and adjustments to functional testing frequencies, to maintain the required PFD or PFH throughout the operational phase.

3. Classification of demands

Three categories of SRS modes of operation, instead of two as in IEC 61508, are proposed in this paper, see Table 1. In addition to low- and high/continuous-demand, a so-called *medium-demand* mode is introduced.

Table 1. IEC SIS category and proposed SRS category

IEC 61508 categorization	Low demand (<=once per year)	High/continuous demand (>once per year)	
Measure	PFD	PFH	
Proposed categorization	Low demand	Medium	High/continuous demand
Measure	PFD	PFD	PFH

The borderlines between medium-demand, low-demand, and high/continuous-demand are not explicitly defined, and will be influenced by application specific considerations. For example, in the subsea oil and gas industry, it may be reasonable to suggest the medium-demand mode as the demand rate in the range of once per year to once or twice per month. The PFD is suggested as

the reliability measure for an SRS in the medium-demand mode. In this demand mode, the PFH as a reliability measure will be too conservative [7].

The demands for the SRS can be (safety) critical or non-critical. This means that the total demand rate is the sum of critical demand rate and non-critical demand rate.

$$\lambda_{\mathrm{d}} = \lambda_{\mathrm{d}}^{\mathrm{crit}} + \lambda_{\mathrm{d}}^{\mathrm{non-crit}} \quad \text{[Eq.1]}$$

where λ_{d} is the total demand rate, $\lambda_{\mathrm{d}}^{\mathrm{crit}}$ is the critical demand rate, and $\lambda_{\mathrm{d}}^{\mathrm{non-crit}}$ is the non-critical demand rate.

For an SRS operating in the medium-demand mode, different combinations of critical demand rate and non-critical demand rate may be distinguished:

1. Critical demands are dominating; non-critical demands are rare
2. Non-critical demands are dominating; critical demands are rare
3. The rates of critical demands and non-critical demands are comparable

This paper focuses on combination 2, where the total demand rate is in the medium demand mode range and the critical demand rate is in the low demand mode range. One example is the pipe RAM preventer in a BOP system that is used to hang-off drill pipes during drilling and to stop flow is case of an uncontrolled flow. Since the critical demands, that matters with respect to safety, are in the low-demand mode, the PFD is used as reliability measure.

SRSs operating in the medium-demand mode with combination 1 or combination 3 can been studied with a similar approach, but this is not done in this paper.

4. Demands as test opportunity

An SRS may suffer from both *dangerous detected* (DD) failures and *dangerous undetected* (DU) failures. Periodic functional testing is used to reveal DU-failures, while diagnostic testing is used to reveal DD-failures. In the medium-demand mode, we assume that, upon detection of a DD-failure, the *equipment under control* (EUC) [1] is taken to a safe state immediately. The contribution from DD-failures to the PFD is therefore negligible compared to DU-failures. Thus only DU-failures are considered in the paper.

Functional tests may improve the SRS reliability in two ways. First, a functional test with positive result (no failure) confirms the functionality of the SRS at the time of testing. Second, a functional test with negative result (with failure) reveals the unavailability of the SRS (components) before the next demand. When it is followed by a repair action, the reliability of the SRS is improved.

For SRSs operating in a low-demand mode, the benefit of functional tests is easily justified given the possibility of revealing a DU-failure before the next demand. In the high/continuous-demand mode, however, it may be impossible to perform regular functional testing at the frequency that is adequate to prevent an accident. However, it is still important to note that functional testing is

needed to reveal DU-failures in redundant configurations. In the medium-demand mode, where the SRS responds to frequent, but non-critical demands, it is reasonable to compare the credit from this type of "random'' testing with the periodic functional tests.

A challenge with functional testing is its interference with the production. Operation of actuating devices often leads to production stops and may imply significant costs. The industry is therefore seeking for means to make functional testing more efficient. Exploiting the information gained from responses to demands may be one of the means to complement the functional testing strategy.

The response to a non-critical demand that is followed up by a thorough inspection may have a similar effect on the SRS reliability as a functional test. A successful response to a demand resembles a functional test with a positive result, and confirms the functionality. A failed response to a demand resembles a functional test with negative result. It reveals the DU-failure, and relevant repair actions may be initiated, but sometimes with additional cost.

4.1 Differences in functional test and demand characteristics

Even with the similarity between periodic functional testing and responses to (non-critical) demands (followed up by inspections), there are some significant differences that need to be considered in SRS reliability assessment.

Costs
A functional test is pre-scheduled, and the necessary equipment and resources are allocated in advance. The costs in relation to functional tests are mainly dependent on the loss of production, the resources needed to perform the test and necessary repair. The costs of the inspection after non-critical demands depend on the same factors except for most of the production loss is inevitable regardless of if an inspection is performed or not. In addition, there may be extra cost to mobilize the personnel and relevant equipment due to that the inspections cannot be planned. The total costs of inspection may increase due to the more frequent execution of non-critical demands (compared to functional testing). It may therefore be necessary to build SRSs that can automatically verify the status of all components after an activation of a system functional.

Note: Costs related to critical demands may be significant, and depend on the degree of damage caused by an SRS failure. For example, a failure to shut down upon high separator pressure will not lead to any large damage, if secondary means of protection, such as opening of pressure relief valves, is successfully achieved (assuming adequate flare capacity). For comparison, a failure of the blowout preventer (BOP) may result in fatality as well as environmental damage, such as the Deepwater Horizon accident in 2010 in the Gulf of Mexico, and the resulting costs are huge. The cost issue in relation to critical demands is, along with the safety issue, one of the reasons why taking credit from critical demands should be much more careful than taking credit from non-critical demands in SRS reliability analysis. The credit from critical demand is not considered in this paper.

Randomness

Unlike functional tests, the demands are usually random events. Non-critical demands for the pipe RAM preventer for mud control during drilling operations is one such example. The occurrence of demands may be modeled as a stochastic process. The characteristic of the process depends on the situation, but with no particular trend in the occurrence of demands, a homogeneous Poisson process (HPP) may be an adequate model.

Note: Demands may in some cases be nearly deterministic events. The pipe RAM in the BOP may also be used to hang-off drill pipes regularly. This type of event occurs at rather regular points in time. For modeling of demands, one must consider if both random and deterministic (non-critical) demands are present and if they reveal the same failure modes.

Pro-activeness

A functional test is a proactive action in terms of risk reduction. Responses to non-critical demands will have a pro-active effect as well, i.e., that the DU-failures are revealed before the next critical demand.

A response to a critical demand is, on the other hand, not a “pro-active” action in terms of risk reduction, even if the successful response may prevent a demand for the next protection layer.

“Test coverage”
For the purpose of reliability analyses, it is often assumed that a functional test has 100 % coverage, meaning that all DU-failures are revealed during the test. The realism of this assumption is sometimes debated, and some methods have introduced new parameters that account for the type of DU-failures that are not revealed by the test [8]. To achieve 100 % test coverage would require that the functional tests are performed under critical demand conditions. This is, of course, not what we would like to do in practice, for example to release hydrocarbon gas into an area to verify the performance of the gas detectors.

The “test coverage” in relation to non-critical demands may vary depending on (i) the failure modes that are covered in the activation upon non-critical demands, and (ii) whether the states of all components are verified (either by the activation or the subsequent inspection) in case of redundancy. The former issue may be exemplified by the BOP example: When the BOP pipe RAM preventer is used for hang-off of a drill pipe, it is not able to reveal the failure mode “leakage through the RAM’’. The latter issue may be exemplified by a set of gas detectors working as a 2-out-of-3 (2oo3) logic. When the detectors successfully signal a gas leakage, it is not possible to known whether all three detectors detected the leakage, or only two of them, without doing any additional effort.

4.2 Taking characteristics into account in the PFD

In the PFD calculation, we usually account for the following factors (see also Figure 1): DU-failure rates, system architecture, functional test interval, and the fraction of DU-failures that are common cause failures (CCFs). DD-failures, repair rate, and test time may also be added if they are expected to influence the PFD.

In this paper, we also include the factors that may be important when non-critical demands are included in the PFD calculation. Based on the discussions in Section 4.1, these factors are:

- Non-critical demand rate
- Coverage of failure modes
- Inspections strategy

The coverage of the failure modes, i.e., the fraction of failure modes that may be revealed during a response to a demand, the inspection strategy, together with the system architecture determine what is in Section 4 referred to as the "test coverage".

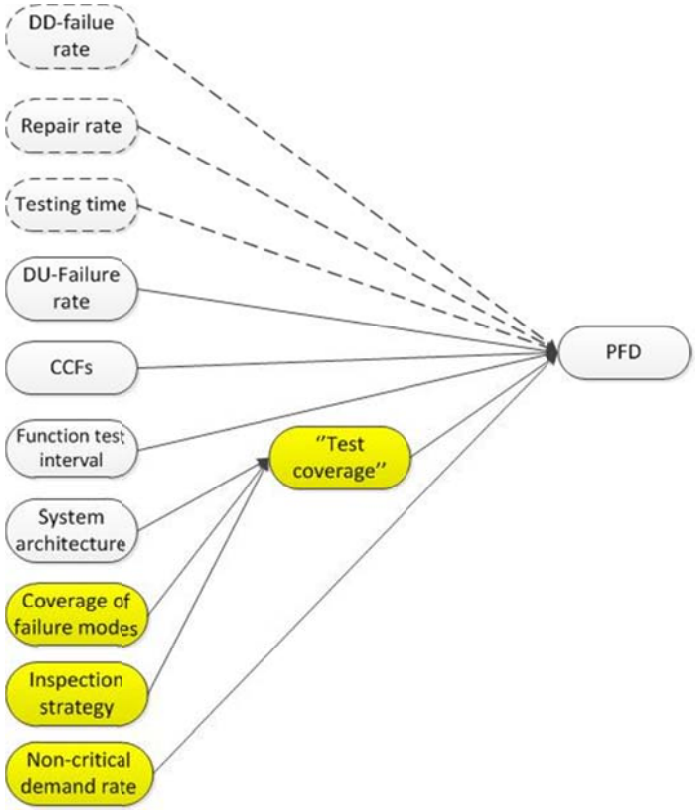

Figure 1. Influencing factors of PFD

5. Reliability modeling of demands as test opportunity

The PFD of the whole SRS can be obtained from the PFD of the subsystems. To calculate the PFD of a subsystem based on the factors in Figure 1 requires some additional detailing of the underlying assumptions. In this paper, these may be summarized as follows:

1. Non-critical demands occur according to an HPP with intensity (demand rate), $\lambda_{\mathrm{d}}^{\mathrm{non-crit}}$, within the medium-demand mode range. The impact on the SRS reliability from critical demands is assumed to be negligible compared to non-critical demands, since non-critical demands are dominating as assumed in Section 3.

2. All components have identical and constant failure rate, but it may be relevant to use the approach in ISO 13849 to account for the additional stress from frequent operations.
3. Functional testing is performed with frequency f_{FT}, where $f_{\mathrm{FT}} \ll \lambda_d$.
4. Each response to a non-critical demand (successful or failed) is followed by a thorough inspection, where the main purpose is to verify the state of all redundant components.
5. Upon detection of a failure, the EUC is taken to a safe state and the failed components are repaired immediately (This assumption means that the active repair time can be disregarded in the PFD quantification).
6. The inspection time and the following time to restore the system are negligible (might not be realistic for some systems).
7. The components are assumed to be independent, i.e., no possibility of CCFs.

Since the non-critical demands may not cover all failure modes, we introduce a ratio θ that

$$\theta = \frac{\lambda_{\mathrm{DU}}^{\mathrm{d}}}{\lambda_{\mathrm{DU}}} \quad \text{[Eq.2]}$$

where $\lambda_{\mathrm{DU}}^{\mathrm{d}}$ is the rate of failures with modes that can be revealed by non-critical demands, and λ_{DU} is the total component DU-failure rate. When all failure modes can be revealed by non-critical demands, then $\theta = 1$.

Taking credit from responses to non-critical demands is similar to using *partial stoke testing* (PST) to verify the state of valves. According to [9], the total PFD can be calculated as the sum of the PFD contribution from PST and the PFD contribution from functional testing. Therefore, a similar approach is used for response to non-critical demands. The PFD of a subsystem is approximately the sum of the PFD contribution from the responses to demands ($\mathrm{PFD_d}$) and the average PFD contribution from functional testing ($\mathrm{PFD_{FT}}$).

$$\mathrm{PFD} \approx \mathrm{PFD_d} + \mathrm{PFD_{FT}} \quad \text{[Eq.3]}$$

In order to calculate $\mathrm{PFD_d}$, two scenarios are differentiated according to whether or not the states of every component can be verified by the response to demands with respect to the failure modes that are covered by the demands.

1. **Scenario 1**: The states of every component in the subsystem can be verified by the responses to demands and the following inspections. The situation in this scenario may be that (i) the subsystem is functioning as a NooN logic or (ii) the inspection after demands can verify the state of every component.

2. **Scenario 2**: The states of all components in the subsystem cannot be verified by the responses to demands and the following inspections. The situation in this scenario may be that the subsystem is function as a MooN logic, where $\mathrm{M} < N$ and the inspection after demands cannot verify the state of every component.

For scenario 2, the voting logic of the subsystem may be changed after a demand due to the degraded operation, but this is not further investigated in this paper. We only consider scenario 1 where the PFD_d can be calculated as, (see also Figure 3):

$$\mathrm{PFD_d} = \int_0^\infty \mathrm{f\,(t)} \frac{1}{t} \int_0^t (1 - \mathrm{R(u)}) \mathrm{du\,dt} \quad \text{[Eq.4]}$$

where $f(t)$ is the probability density function of the time to a non-critical demand, $R(u)$ is the reliability function of the subsystem in question, and t is the time to a non-critical demand.

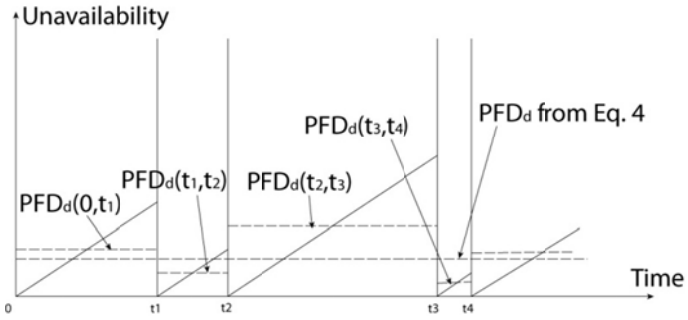

Figure 3. PFD_d calculated from Eq.4

The PFD can also be approximated as the average unavailability each time the SRS is demanded. This is equal to the expected PFD_d when a non-critical demand occurs, see Figure 4. If, for example, demands occur at times t_1, t_2 and t_3 with probabilities P_1, P_2 and P_3, respectively, the $\mathrm{PFD_d} = \sum_{i=1}^{3} \mathrm{PFD_d}(t_i) P_i$. To include all the possible times a demand may occur, the PFD_d is given in Eq.5.

$$\mathrm{PFD_d} = \int_0^\infty \mathrm{f\,(t)} (1 - \mathrm{R(t)})\,\mathrm{dt} \quad \text{[Eq.5]}$$

where the notation is the same as in Eq.4.

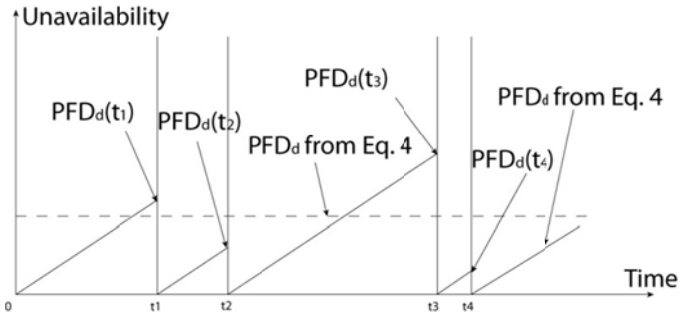

Figure 4. PFD_d calculated from Eq.5

Comparing the results from Eq.4 and Eq.5, it is seen that Eq.5 gives a more conservative result. The uncertainty of the PFD_d calculated by the approach in this paper may be higher than for the conventional approach due to the randomness of the "tests" and the "test coverage" of the

demands. To compensate for this increased uncertainty, we recommend using Eq. 5 rather than Eq. 4.

5.1 Single component subsystem

For a subsystem with a single component, the average PFD of the subsystem can, according to Eq. 3 and Eq. 5, be calculated as

$$\mathrm{PFD} \approx \mathrm{PFD_d} + \mathrm{PFD_{FT}} = \int_0^{\infty} \lambda_{\mathrm{d}}^{\mathrm{non-crit}} \mathrm{e}^{-\lambda_{\mathrm{d}}^{\mathrm{non-crit}} \mathrm{t}} \left(1 - \mathrm{e}^{-\theta \lambda_{\mathrm{DU}} \mathrm{t}}\right) \mathrm{dt} + \frac{(1-\theta)\lambda_{\mathrm{DU}}}{2 f_{\mathrm{FT}}} = 1 - \frac{\lambda_{\mathrm{d}}^{\mathrm{non-crit}}}{\lambda_{\mathrm{d}}^{\mathrm{non-crit}} + \theta \lambda_{\mathrm{DU}}} + \frac{(1-\theta)\lambda_{\mathrm{DU}}}{2 f_{\mathrm{FT}}} \quad \text{[Eq.6]}$$

NOTE: A condition of using Eqs. 3 and 6 is that the functional test frequency is significantly lower than the non-critical demand rate, as what has been stated in assumption 3.

When all failure modes can be revealed by demands, $\theta = 1$, thus

$$\mathrm{PFD} \approx 1 - \frac{\lambda_{\mathrm{d}}^{\mathrm{non-crit}}}{\lambda_{\mathrm{d}}^{\mathrm{non-crit}} + \theta \lambda_{\mathrm{DU}}} = \mathrm{PFD_d} = \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{d}}^{\mathrm{non-crit}}} = \lambda_{\mathrm{DU}} * \mathrm{MTBD} \quad \text{[Eq.7]}$$

where MTBD is the *mean time between demands*.

If we assume that the non-critical demands can reveal all failure modes and that the state of every component can be verified, we may conclude that functional testing gives no added value to the reliability unless they are performed very frequently (which in many cases is impractical).

5.2 Multiple components subsystem

For a subsystem with redundancy, an example is used to illustrate how the PFD can be calculated. Considering a subsystem of three pressure transmitters working as a 2oo3 configuration, it is assumed that the pressure transmitters are needed for a particular type of operation, for example for mud control during drilling operations, to raise an alarm upon a specified pressure setting. The same transmitters are also needed in the execution of a shutdown function. It is further assumed that the non-critical demands (i.e., when exceeding the pressure set point) on average occur 4 times per year ($\lambda_{\mathrm{d}}^{\mathrm{non-crit}} = 4.57 \times 10^{-4}$ per hour).

The failure rate of each transmitter is set to 5×10^{-6} per hour, and we assume that no periodic functional testing is scheduled. This strategy mandates that the state of each transmitter is confirmed by inspection after each non-critical demand. We further assume that the non-critical demands can reveal all failure modes, that the inspection after a demand can verify all component states, $\theta = 1$, and that the time needed to perform inspection and maintenance is negligible. If a transmitter failure is revealed by diagnostics, repair is initiated immediately and the contribution from DD failures may be neglected. Common cause failures (CCFs) are not considered in this example, but may easily be added using e.g., the standard beta factor model.

According to Eqs. 3 and 5, the PFD for this 2oo3 configuration subsystem is [10]

$$\text{PFD} = \int_0^{\infty} \lambda_{\text{d}}^{\text{non-crit}} \text{e}^{-\lambda_{\text{d}}^{\text{non-crit}} \text{t}} (1 - 3e^{-2\lambda_{\text{DU}} t} + 2e^{-3\lambda_{\text{DU}} t})\, \text{dt} = 1 - \frac{3\lambda_{\text{d}}^{\text{non-crit}}}{\lambda_{\text{d}}^{\text{non-crit}} + 2\lambda_{\text{DU}}} + \frac{2\lambda_{\text{d}}^{\text{non-crit}}}{\lambda_{\text{d}} + 3\lambda_{\text{DU}}}$$

[Eq.8]

By inserting the non-critical demand rate and failure rate in Eq.13, we obtain $\text{PFD} = 6.8 \times 10^{-4}$.

6. Follow-up in the operational phase

IEC 61508 and IEC 61511 require the reliability of SRSs is maintained throughout the whole operational life. All factors that influence the reliability, such as the number of recorded failures and the time between periodic (and, as suggested in this paper, random) tests must therefore be monitored, analyzed, and used as basis for making decisions about reliability. For low demand systems, the approach suggested by Lundteigen and Hauge [11] may be used.

The approach advocated in this paper mandates monitoring of non-critical demands. New (experienced) demand rates and PFD need to be compared with the assumptions and calculations that were made in the design phase. A stepwise approach may be as follows:

1. Record the number of non-critical demands and the total operation time.
2. Estimate the actual demand rate as well as the actual PFD by the recorded operational information.
3. Compare the actual PFD and the predicted PFD.
4. If the actual PFD is greater than the predicted PFD, introduce measures (e.g., additional functional tests) to improve the SRS reliability and proceed to 5, otherwise stop.
5. Make a new PFD estimation with the actual demand rate and new measures.
6. Compare the new PFD estimation and the predicted PFD.
7. If the new PFD estimation is greater than the predicted PFD, introduce more measures, then proceed to 5 again, otherwise stop.

This procedure may be performed with a certain interval (e.g., once per year) to maintain the due SRS reliability.

In the daily follow-up of SRSs, we must avoid too long time between tests. With too long time since the last response to a non-critical demand, it may be necessary to perform a functional test to not compromise the reliability requirement. We may introduce the maximum allowed time between demands/tests, t_{max}. If this time is reached, we perform a functional test to make sure the time between demands/tests is not greater than the maximum allowed time between demand/tests, thus the PFD does not exceed a certain value. The t_{max} may be the mean time between demands, but it can also be argued that it is a value within a specified confidence interval.

A more detailed discussion of SRS follow-up is not made in this paper, but it is certainly a further research field.

7. Concluding remarks

In this paper, the possibility of using information from responses to demands in SRS reliability assessment is investigated. The conditions under which demands may be treated as functional tests and credited in PFD calculation are discussed. The study has been focused on SRSs operating in the so-called medium-demand mode, particularly when the SRS is subject to critical demand with a low-demand rate and non-critical demands with a medium-demand rate. By considering only the non-critical demands, PFD calculation formulas are established.

The paper has been written in response to a question raised by the SRS manufacturers: Can responses to demands and inspections (to some extent) replace the functional tests. Despite the effort made in this paper to give new insights into this topic, there are several questions that remain unsolved. Some examples include:

- More insights into the pros and cons of using responses to demands as tests are needed, and they should be founded on industry cases beyond those considered in this paper.
- With more reliance on demand rate to quantify the PFD, follows the need for a systematic recording of non-critical demands. Even if IEC 61508 and IEC 61511 point at the need to monitor the (critical) demand rate for the purpose of validating the assumptions under which the SIL requirements have been founded, the authors have seen little evidence that such a practice has been implemented.
- The paper points at the need for inspections after each response to a non-critical demand. In practice, this is time consuming and effort is needed to ensure that the confirmation about all component states is automatically collected by the SRS.
- The paper has not addressed the possibility of taking spurious activation into account in the PFD calculation, even if such responses may also replace (to some extent) the need to perform functional tests. The issue has been discussed by a few authors [12]. However, this is a premature field, and cautions should be taken to avoid a design that credit frequent spurious activations as a means to achieve high reliability.
- New quantification approaches give new requirements to the follow-up of SRSs in the operational phase. A brief approach has been indicated in this paper, but more research and case studies are needed before implemented by the industry.

The approach does not cover all requirements needed to comply with a SIL requirement: Quantifying PFD (or PFH) is just one step out of many that are needed to comply with a SIL requirement. Manufacturers also need to build systems that fulfill the requirements for architecture constraints and systematic safety integrity. End users must demonstrate that all the necessary conditions and assumptions that affect operation and maintenance are maintained throughout the SRS lifecycle.

It is the authors' opinion that more research is needed before an industry practice may be suggested for the topic of this paper and some of the other identified issues.

8. References

[1] IEC61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, Geneva, 2010.

[2] IEC61511, “Functional safety - safety instrumented systems for the process industry,” International Electrotechnical Commission, Geneva, 2003.

[3] ANSI/ISA 84.00.01: 2004 (IEC61511 Mod), Application of safety instrumented systems for the process industries, ISA, Raleigh, NC, USA, 2004.

[4] O. Olamilehin, “Fault tree analysis applied to SIL,” Master thesis, NTNU, Trondheim 2010.

[5] M. A. Lundteigen and M. Rausand, “Spurious activation of safety instrumented systems in oil and gas industry: Basic concepts and formulas,” *Reliability engineering and system safety*, Volume 93, p. 1208-1217, 2008.

[6] OLF-070, “Application of IEC 61508 and IEC61511 in the Norwegian petroleum industry,” The Norwegian oil industry association, Stavanger, Norway, 2004.

[7] H. Jin, M. A. Lundteigen and M. Rausand, “Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation,” *Reliab Eng Syst Safety* (2010), doi:10.1016/j.ress.2010.11.007

[8] PDS method handbook, “Reliability prediction method for safety instrumented systems,” SINTEF, Trondheim, Norway, 2010.

[9] M. A. Lundteigen and M. Rausand, “Partial stroke testing of process shutdown valves: How to determine the test coverage,” *Journal of Loss Prevention in the Process Industrie*s, Volume 21, 2008.

[10] M. Rausand and A. Høyland, *System reliability theory: Models, statistical methods and applications (2nd. ed.)*, Wiley, New York, USA, 2004.

[11] M. A. Lundteigen and S. Hauge, “Management of safety integrity in the operational phase,” *Inside functional safety*, Issue 1, 2010.

[12] E. Munkeby, “Effect of safe failures on the reliability of safety instrumented system,” Master thesis, NTNU, Trondheim 2008.