Proof testing of safety-instrumented systems: New testing strategy induced by dangerous detected failures

Yiliu Liu*, **Marvin Rausand**
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Abstract: Some dangerous failures of safety-instrumented systems (SISs) are detected almost immediately by diagnostic self-testing, whereas other dangerous failures can only be detected by proof-testing. The first type is called dangerous detected (DD) failures and the second type is called dangerous undetected (DU) failures. Proof tests are usually carried out at constant time intervals. DD-failures are repaired almost immediately whereas a DU-failure will persist until the item is proof-tested. Many items can have a DU- and a DD-failure at the same time. After the repair of a DD-failure is completed, the maintenance team has two options: to perform an "insert" proof test for DU-failure or not. If an insert proof test is performed, it is necessary to decide whether the next scheduled proof test should be postponed or performed at the scheduled time. This paper uses Petri nets to model the proof test strategies after DD-failures and to analyze the effects of the different strategies on the SIS performance. It is shown that insert proof tests reduce the unavailability of the system, whereas the adjustment (or not) of the test schedule does not have any significant long term effect.

Keywords: safety-instrumented system, proof test, dangerous detected-failure, dangerous undetected-failure

1. INTRODUCTION

Safety-instrumented systems (SISs) are widely used in many industries (e.g., process, nuclear, oil and gas industry) to prevent hazardous events and to mitigate the consequences of such events [1, 2]. A modern SIS has built-in facilities for diagnostic self-testing during operation. Such tests can detect many dangerous failures almost immediately such that a repair action can be initiated. These dangerous failures are called dangerous detected (DD) failures. On the other hand, dangerous failures that are not detected by diagnostic testing are called dangerous undetected (DU) failures and are only revealed in proof tests that are carried out at regular intervals (e.g., once per year).

The mean time from a DD-failure occurs until the function is restored, MTTR, is usually rather short (e.g., 5-8 hours), and DD-failures will therefore not be a main contributor to the unavailability of a SIS that is operated in low-demand mode (i.e., where demands for the safety function do not occur more often than once per year). For some channels, DD-failures can be repaired on-line, while the process is running as normal during the repair. In most cases, however, the process section has to be brought to a safe state (most often stopped) during the repair of the DD-failure. For some channels, DD- and DU-failures can be present at the same time and repairing a DD-failure does not guarantee that a DU-failure is not remaining in the channel. In some cases, it may be possible to proof-test for a DU-failure as part of the repair of the DD-failure.

Such proof tests can be regarded as "insert tests" between two scheduled tests, such that the number of proof tests in a certain time period will increase. This means that the average proof test interval will be reduced. Since the length of the proof test interval has a significant influence on the availability

* Corresponding author, yiliu.liu@ntnu.no

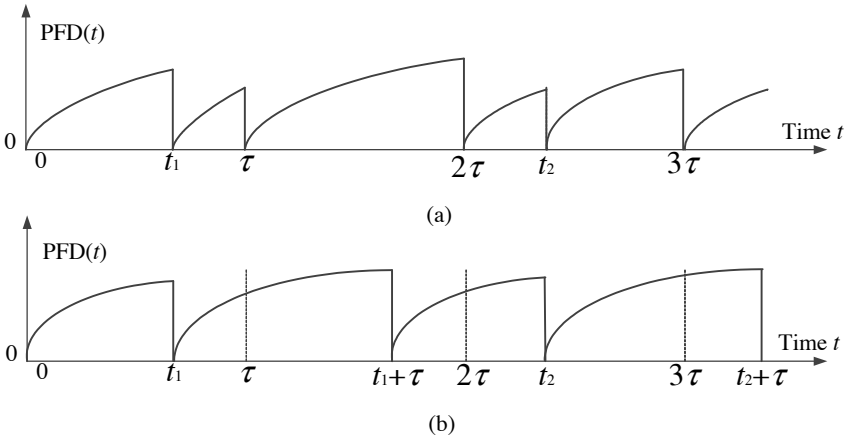

Figure 1: PFD for test strategies 2 (a) and 3 (b) as a function of time t

performance of a SIS [3], the new proof tests induced by DD-failures should also have influence. Thus, the objective of this paper is to model the relationship between such proof tests induced by DD-failures and SIS performance, as well to examine effects of these tests.

The remainder of the paper is organized as follows: Section 2 presents the possible follow-up test strategies after a DD-failure is revealed. Next, the modeling approach is briefly introduced, and some Petri net models for different strategies are studied in section 3. The effects of different test strategies on the SIS availability performance are analyzed in section 4. Finally, section 5 presents conclusions and research perspectives.

2. TEST STRATEGIES INDUCED BY DD-FAILURES

In this paper, we study a simple SIS subsystem with only one channel. When a DD-failure in this system is detected, the maintenance team can repair the SIS channel in a short time, and then they have three options for testing the SIS for DU-failures:

- Strategy 1: Finish the work, but do not perform any insert proof test for DU-failures.
- Strategy 2: Perform an insert proof test for DU-failures, but keep the proof test schedule unchanged.
- Strategy 3: Perform an insert proof test for DU-failures, and change the proof test schedule (mostly postpone the subsequent proof test).

To illustrate the difference between strategies 2 and 3, consider a pressure safety valve that is scheduled to be proof-tested each April and assume that a DD-failure occurs in September. If strategy 2 is applied, a proof test for DU-failures is initiated immediately after having repaired the DD-failure, and the next proof test is still carried out the next April. If, on the other hand, strategy 3 is applied, the next proof test is postponed till next September keeping the same interval between two proof tests.

We use the probability of failure on demand (PFD) as measure for the safety performance of the SIS. DU-failures are always the main contributor to the PFD of a SIS because they may put the SIS in an unavailable state for a long time until a proof test is carried out. Fig. 1 briefly illustrates the changing trends of the PFD(t) as a function of the time t when test strategies 2 and 3 are applied, respectively.

In Fig. 1, $t_0, t_1, t_2, \ldots$, denote the times when DD-failures occur, and τ is the test interval. It is shown in Fig. 1(a) that the predefined proof test schedule is kept unchanged under strategy 2, and each proof test can reduce the value of PFD(t) to 0. Fig. 1(b) for strategy 3, illustrates that the time to the next proof test is re-counted after an insert test induced by a DD-failure.

3. MODELING TEST STRATEGIES

3.1. Modeling approach

In this paper, Petri nets are used to model the different test strategies. Petri nets have been adapted to SIS reliability analysis [4, 5] especially for test strategies of SISs [6, 7], and is also a recommended modeling approach in IEC 61508 [1].

The international standard IEC 62551 [8] defines the terminology of Petri nets in dependability analysis. There are two basic elements in such models, places (shown as circles in Fig. 2) and transitions (shown as bars) are connected with directed arcs. Tokens are illustrated as bullets to express the movable resources in the system and reside in the places. For each arc, a multiplicity is assigned to denote the token delivering capacity of the arc. The distribution of tokens in the places is regarded as a marking, and each marking represents a system state.

When all input places to a transition have at least as many tokens as the multiplicities of the associate arcs to the transition, the transition is enabled. And then, the transition can be fired to absorb the tokens in these places according to the multiplicities of the associate arcs. In this paper, timed Petri nets are applied, where a firing time (delay from enabled to fired) can be assigned to each transition. Such Petri nets have two types of transitions: immediate transitions (zero firing time, shown as thin bars) and timed transitions (shown as thick bars). In IEC 62551 [8], a blank bar is used to denote a transition with exponential firing time, and a filled thick bar is for the transition with constant firing time.

In addition, an inhibitor arc (shown as a small circle at the end of an arc) is sometimes used to prevent a transition from being enabled. Such a special arc enables its output transition when there is no token in the associate place. More details for Petri nets can be found in IEC 62551 [8].

3.2. Modeling test strategy 1

In the following subsections, three Petri net models are established to illustrate the three test strategies in section 2 after the occurrence of a DD-failure.

Fig. 2 shows the Petri net model for test strategy 1. In this model, a DD-failure occurs when the token in p_{DW} is removed by the transition t_{DD} and deposited to p_{DF}. In the same way, the places p_{UW}, t_{UW} and p_{UF} are used to denote the occurrence of a DU-failure. Both t_{DD} and t_{DU} are blank, which means that the failure times are exponentially distributed. In addition, exponentially distributed transition t_{DR} is used to denote the repair times of the SIS from the fault state due to DD-failures, respectively.

Proof tests are reflected by firing t_{T} and depositing a token to p_{T}. The filled bar shows that proof tests are carried out at constant intervals.

Transitions t_1 and t_2 express the two situations in a proof test. If a DU-failure in the SIS is revealed, t_1 can be fired; otherwise, t_2 can be fired. The inhibitor here is for enabling t_2 when there is no token in p_{UF}. No matter whether t_1 or t_2 is fired, a token can be deposited to p_{S}, meaning that the test is finished and the test resources are restored and ready for the next proof test. In this figure, both t_1 and t_2 have exponential distributed firing times, reflecting the assumption that the time required to perform a proof

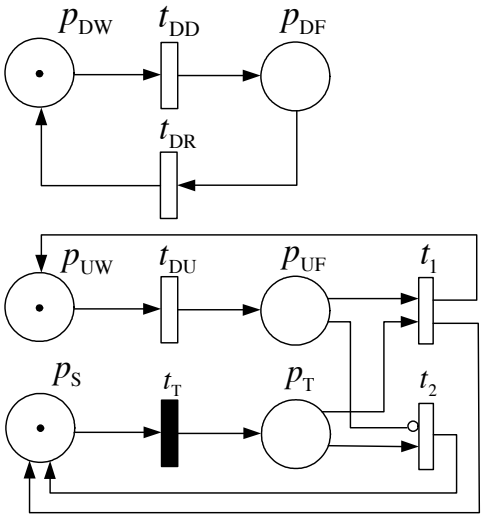

Figure 2: Model for test strategy 1

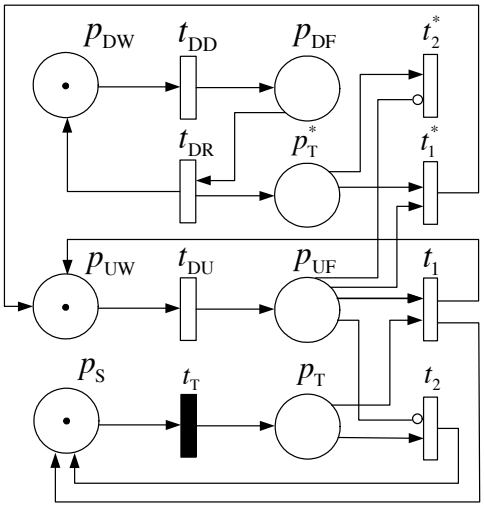

Figure 3: Model for test strategy 2

test is exponentially distributed. In fact, the firing time of t_1 includes the time for the proof test and for the repair of the DU-failure.

It should be noted that the part describing the DD-failure is separate from the parts describing the DU-failure and the proof test in this model. The moving of tokens between p_{DW} and p_{DF} has no influence on other tokens, since maintenance does not do anything except for repairing the DD-failure in strategy 1.

3.3. Modeling test strategy 2

Test strategy 2 is modeled in Fig. 3 by adding one place and two transitions to the model for strategy 1. When t_{DR} is fired in this model, a token is released to p_{DW} and another token can enter p_T^* to initiate a proof test for DU-failure. The functions of t_1^* and t_2^* are similar with those of t_1 or t_2, in absorbing the token in p_T^* to complete the test. In the case where a token resides in p_{UF}, it will be absorbed by t_1^*. Thereafter, a token is released to p_{UW}, such that a DU-failure is revealed by the proof test induced by

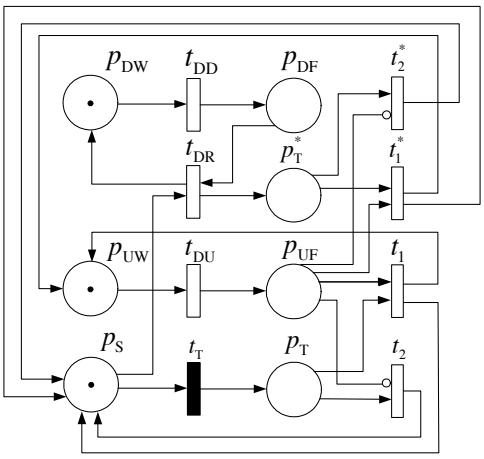

Figure 4: Model for test strategy 3

the DD-failure and repaired.

There is no relation between DD-failure part and the scheduled proof test part in this model. Even if there is an insert proof test, the transition t_T is still fired at the scheduled time.

3.4. Modeling test strategy 3

The model in Fig. 4 for test strategy 3 has no new place or transition compared with the model in Fig. 3, but some arcs are involved to relate DD-failures and scheduled proof tests. In Fig. 4, t_{DR} is fired by absorbing the token in p_S. When one of the transitions, t_1^* and t_2^* is fired, a token can come back to p_S. In other words, when performing the insert proof test in the model, the enabling condition of t_T is stopped. Such a change implies that once there is a proof test induced by a DD-failure, the resource for scheduled testing will be used, and the time counting process for the next proof test is re-initiated.

It should also be noted that such a model ignores the probability that a DD-failure and the scheduled proof test take place at the same time. This assumption has little influence on the following analyses since this probability is very low.

4. EFFECTS ON SIS PERFORMANCE

In the analysis of the influences of the three test strategies on SIS performance, the following assumptions are made:

- DU- and DD-failures occur independent of each other;
- The occurrences of DU- and DD-failures have constant failure rates;
- The system can have both DU-and DD-failures at a specific moment;
- Only one maintenance team is available for testing and repair of the SIS;
- A failed system can be restored to a fully functioning state (i.e., without any failure);
- The test and repair times are exponentially distributed.

The average, long term PFD (or PFD_{avg}) is used in this section as the measure to analyze the effects of different test strategies on the performance of a SIS. PFD_{avg} is determined by the contributions from DD- and DU-failures, and for all the three test strategies, PFD_{avg} can be calculated as:

$$\text{PFD}_{\text{avg}} = \Pr(\mathbf{m}(p_{\text{DF}}) = 1) + \Pr(\mathbf{m}(p_{\text{UF}}) = 1) - \Pr(\mathbf{m}(p_{\text{DF}}) = 1) \cdot \Pr(\mathbf{m}(p_{\text{UF}}) = 1) \quad (1)$$

where $\Pr(\mathbf{m}(p_{\text{DF}}) = 1)$ denotes the long term sojourn probability of the model where place p_{DF} holds one token, such that the SIS is unavailable due to a DD-failure. Similarly, $\Pr(\mathbf{m}(p_{\text{UF}}) = 1)$ is equal to the unavailability of the SIS due to a DU-failure.

Since DD- and DU failures are independent from each other, both $\Pr(\mathbf{m}(p_{\text{DF}}) = 1)$ and $\Pr(\mathbf{m}(p_{\text{UF}}) = 1)$ involve the probability of simultaneous DD- and DU-failures, and thus when we calculate PFD_{avg}, the probability $\Pr[(\mathbf{m}(p_{\text{DF}}) = 1) \cap (\mathbf{m}(p_{\text{UF}}) = 1)]$ should be subtracted to remove this overlap. Of course, for highly reliable SISs, $\Pr[(\mathbf{m}(p_{\text{DF}}) = 1) \cap (\mathbf{m}(p_{\text{UF}}) = 1)]$ is very small and without a significant influence on the calculated result.

The efficiency of the diagnostic test for a SIS is measured by the diagnostic coverage (DC), which is the fraction of the rate of dangerous failures that are revealed by the diagnostic testing relative to the rate of all dangerous failures. Suppose that the total dangerous (D) failure rate of a SIS is 2×10^{-5} per hour, and DC is 0.9. Thus, the rate of DD-failures (λ_{DD}) is $0.9 \times 2 \times 10^{-5} = 1.8 \times 10^{-5}$ per hour, whereas the rate of DU-failures (λ_{DU}) is $(1 - \text{DC}) \times 2 \times 10^{-5} = 2 \times 10^{-6}$ per hour. In this case, we can regard the scheduled test interval (τ) as 1 year (8760 hour), and all test and repair rates as 0.125 per hour (meaning that the average time of testing and repair is 8 hours). Therefore, the transition rates of $t_{\text{DR}}, t_{\text{UR}}, t_1, t_2, t_1^*$, and t_2^* are 0.125 in all the three models. Here, the testing and potential repair processes are partly simplified: Repair time is included in the test duration. Since such time is rather short compared with the test interval, the simplification has little impact on the calculations.

The firing time of t_{T} in the model in Fig. 3 is set to be 8752 hours, which is equal to the test interval minus the average test time. While the corresponding firing time t_{T} in Fig. 4 is 8744 (8760-8-8) hours, since the maintenance resource is used in the test for DD-failures and then in the testing for DU-failures. If these transitions are approximated as exponential distributed ones, the firing rate also should be determined in the consideration of testing and repair time.

Monte Carlo simulations for the three models in Fig. 2-4 are carried out by using the software GRIF.[1] The results are shown in Table 1.

Table 1: PFD_{avg} of the SIS under different test strategies

	Strategy 1	Strategy 2	Strategy 3
$\text{PFD}_{\text{avg(DD)}}$	1.4389×10^{-4}	1.4403×10^{-4}	1.4455×10^{-4}
$\text{PFD}_{\text{avg(DU)}}$	8.6930×10^{-3}	8.0501×10^{-3}	8.0511×10^{-3}
PFD_{avg}	8.8356×10^{-3}	8.1930×10^{-3}	8.1945×10^{-3}

Strategies 2 and 3 change the proof test schedules since the maintenance team performs follow-up actions induced DD-failures, and thus the rates of DD-failures can be simply assumed to influence the effects of test strategies 2 and 3. In order to measure this effects, we check four DD-failure rates from 2×10^{-5} to 2×10^{-4} per hour, while keeping the DU-failure rate at 2×10^{-6} per hour. The corresponding DCs vary from 0.91 to 0.99.

[1] `http://grif-workshop.com`

In Table 2, we only present the PFD_{avg} values due to the DU-failures, because they are the dominant parts of the unavailability of the SIS.

Table 2: PFD_{avg} of the SIS with different DD-failure rates

	$PFD_{avg(DU)}$		
λ_{DD}	Strategy 1	Strategy 2	Strategy 3
2×10^{-5}	8.6995×10^{-3}	7.9740×10^{-4}	7.9792×10^{-3}
6×10^{-5}	8.6970×10^{-3}	6.8910×10^{-3}	6.8792×10^{-3}
1×10^{-4}	8.6902×10^{-3}	6.0541×10^{-3}	6.0513×10^{-3}
2×10^{-4}	8.6937×10^{-3}	4.6436×10^{-3}	4.6440×10^{-3}

The results illustrate the reduction of $PFD_{avg(DU)}$ obtained by using test strategies 2 and 3. Since DD-failures have no relation with proof testing, the values of $PFD_{avg(DU)}$ have a constant level. Meanwhile, with test strategies 2 and 3, $PFD_{avg(DU)}$ decreases with more frequent DD-failures and the follow-up proof testing for DU-failures.

If only DU-failures are taken into account, PFD_{avg} is often approximated as (e.g., in [4])

$$PFD_{avg(DU)} \approx \frac{\lambda_{DU}\tau}{2} \tag{2}$$

The idea behind the formula is that the unavailability of the SIS is the DU-failure rate multiplied by the mean time until the DU-failure is revealed ($\tau/2$). This can also be formulated as the DU-failure rate divided by the mean revealing rate of the DU-failure (i.e., $2/\tau$). Results of PFD_{avg} based on such an approximation is close to those by the model under test strategy 1, where DD-failures do not induce more tests for DU-failures. However, two types of proof tests exist under test strategy 2. With the same philosophy as used to develop Eq. 2, the unavailability of the SIS due to DU-failures also can be approximated as the DU-failure rate divided by the mean revealing rate of the DU-failure.

$$PFD_{avg(DU)} \approx \frac{\lambda_{DU}}{\frac{2}{\tau} + \lambda_{DD}} = \frac{\lambda_{DU}\tau}{2 + \lambda_{DD}\tau} \tag{3}$$

Based on Eq. 3, it can be found that if the rate of DD-failure is high, the reduction of PFD_{avg} with test strategy 2 is more obvious. The data in Table 2 shows the same trend.

Test strategies 2 and 3 have approximately the same effects on the SIS performance. Even if the two strategies after some few DD-failures result in different PFD profiles, their average, long term PFD are very close. When the rate of DD-failures is low compared with the scheduled test frequency, the number of proof tests induced by DD-failures is very low, and the influence of postponing one proof test is therefore low. If the rate of DD-failures is relatively high (e.g., equal or higher than the scheduled test interval), the two strategies are still similar because the changed proof test schedule will often be changed again by another DD-failure before the next proof test. For example, when the rate of DD-failure is high enough, a DD-failure often occurs between two scheduled proof tests, and thus the next scheduled proof test may be postponed again and again. PFD_{avg} due to DU-failures under test strategy 3 can therefore be approximated by Eq. 3.

The managerial implications based on the findings include: Proof testing for DU-failures induced by DD-failures can improve the performance of a SIS, especially when DD-failures occur rather

frequently. After the insert tests, it is not important for the long term SIS performance whether the original proof test schedule is changed or not. Selection of test strategies 2 or 3 should involve other factors in consideration, such as the cost of each proof test, and cost due to the adjustment of the testing schedule.

5. CONCLUSION

This paper studies follow-up activities after a DD-failure has been detected. Insert proof testings to reveal DU-failures are found to be able to reduce the unavailability of the SIS, especially when DD-failures occur frequently. Based on the presented Petri net models, the average values of the PFD_{avg} of the SIS in the long term are similar no matter if the original proof test schedule is changed or not. Such findings are helpful for operators to select their appropriate strategies on the basis of the requirements for safety and cost.

Studies of SISs with more complex structures are needed to verify the conclusion of this study, since only the simplest one-out-of-one system is considered here. Common cause failures (CCFs) are always dominanting factors for the unavailability of complex SISs with redundancies, and thus it is necessary to consider such kind failures in prospective studies. In addition, since the sizes of Petri net models in this paper will greatly increase when involving more elements in the system, suitable modeling methods should also be developed.

References

[1] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7.* Geneva: International Electrotechnical Commission, 2010.

[2] IEC 61511, *Functional safety: safety instrumented systems for the process industry sector, part 1-3*. Geneva: International Electrotechnical Commission, 2003.

[3] M. Rausand and A. Høyland, *System reliability theory; models, statistical Methods, and applications*. Hoboken, NJ.: Wiley, 2nd ed., 2004.

[4] M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications*. Hoboken, NJ: Wiley, 2014.

[5] ISO/TR 12489, *Petroleum, petrochemical and natural gas industries – reliability modeling and calculation of safetyt systems*. Geneva: International Organization for Standardization, 2013.

[6] Y. Liu and M. Rausand, "Reliability effects of test strategies on safety-instrumented systems in different demand modes," *Reliability Engineering & System Safety*, vol. 119, pp. 235–243, 2013.

[7] Y. Liu, "Optimal staggered testing strategies for heterogeneously redundant safety systems," *Reliability Engineering & System Safety*, vol. 126, pp. 65–71, 2014.

[8] IEC 62551, *Analysis techniques for dependability Petri net techniques*. Geneva: International Electrotechnical Commission, 2012.