Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems

Yiliu Liu[1,*], Marvin Rausand[1]

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

Abstract

Some dangerous failures of safety-instrumented systems (SISs) are detected almost immediately by diagnostic self-testing as dangerous detected (DD) failures, whereas other dangerous failures can only be detected by proof-testing, and are therefore called dangerous undetected (DU) failures. Some items may 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 analyzes the effects of different testing strategies on the safety performance of a single channel of a SIS. The safety performance is analyzed by Petri nets and by approximation formulas and the results obtained by the two approaches are compared. It is shown that insert testing improves the safety performance of the channel, but the feasibility and cost of the strategy may be a hindrance to recommend insert testing.

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

[*]Corresponding author:
Email address: yiliu.liu@ntnu.no (Yiliu Liu)

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 [2, 3]. International standard [2] uses safety integrity, the probability of a SIS satisfactorily performing the specified safety instrumented function under all the stated conditions within a stated period of time as a performance measure.

A SIS has at least three subsystems: senor, logic solver and final element subsystems. A sensor subsystem (with one or more sensors) detects possible undesired event and send signals to the logic solver subsystem (with one or more logic solvers), which can interpret these signals and decides which actions should be taken. The final element subsystem also can have one more elements that take prescribed actions to prevent harm to plants, processes or machineries, namely, equipments under control (EUCs) [16]. Each subsystem may have one or more channels, which can independently perform a safety function.

In terms of safety integrity assessment of SISs, many researches have been carried out, e.g. for measuring the effects of system architectures [6, 14, 20], effects of testing strategies [11, 19], different demand modes and associated measures [1, 7, 9, 13], and varying modeling methods [2, 5]. More information about research achievements and directions of SISs can be found in [15, 16].

In literature, dangerous failures is regarded to occur once a SIS has no capability to response to a demand, which can be an event or a condition [16]. After such failures, the SIS will fall into a dangerous fault state. In fact, most modern SISs have built-in diagnostic self-testing capabilities that can detect many dangerous failures almost immediately such that a repair action can be initiated. These dangerous failures are called dangerous detected (DD) failures. It should be noted that diagnostic tests seldom discover all dangerous failures/faults, and the percentage of faults that can be revealed is called as diagnostic coverage (DC). 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 safety 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). The average probability of failure on demand (PFD_{avg}) in a (long) period is always used as the performance measure of a SIS/SIS subsystem/SIS channel [2, 3, 10].

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 EUC 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 total number of proof tests in a certain time period will increase. This means that the average length of the proof test interval will be reduced. Because the length of the proof test interval has a significant

influence on the unavailability of a SIS [17], 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, and to study the effects of these tests.

The remainder of the paper is organized as follows: Section 2 presents the possible follow-up test strategies of a single channel SIS after a DD-failure is revealed. Next, the modeling approach is briefly introduced, and 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. And then, general approximation formulas are proposed for more complex systems. Finally, section 6 presents conclusions and research perspectives.

2. Testing strategies induced by DD-failures

First, 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 I: Do not perform any insert proof test for DU-failures.
- Strategy II: Perform an insert proof test for DU-failures, while keeping the proof-testing schedule unchanged.
- Strategy III: Perform an insert proof test for DU-failures, and change the proof-testing schedule (by postponing the subsequent proof test).

To illustrate the difference between strategies II and III, consider a solenoid valve that is scheduled to be proof-tested each April and assume that a DD-failure occurs in September. If strategy II 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 III is applied, the next proof test is postponed till next September keeping the same interval between two proof tests.

We use the long-term average probability of failure on demand, $\mathrm{PFD}_{\mathrm{avg}}$, to measure the safety unavailability of the SIS. DU-failures are always the main contributor to the $\mathrm{PFD}_{\mathrm{avg}}$ because they may put the SIS in an unavailable state for a long time until a proof test is carried out. Fig. 1 illustrates possible shapes of the probability of failure on demand, $\mathrm{PFD}(t)$, as a function of the time t ,when test strategies II and III are applied, respectively.

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

3. Petri Net Analysis

Petri nets are used in this paper to model the different testing strategies. Petri nets have been adapted to SIS reliability analysis [5, 7, 16] especially for testing strategies of SISs [10, 12], and is also a recommended modeling approach in IEC 61508 [2] and ISO 12489 [8].

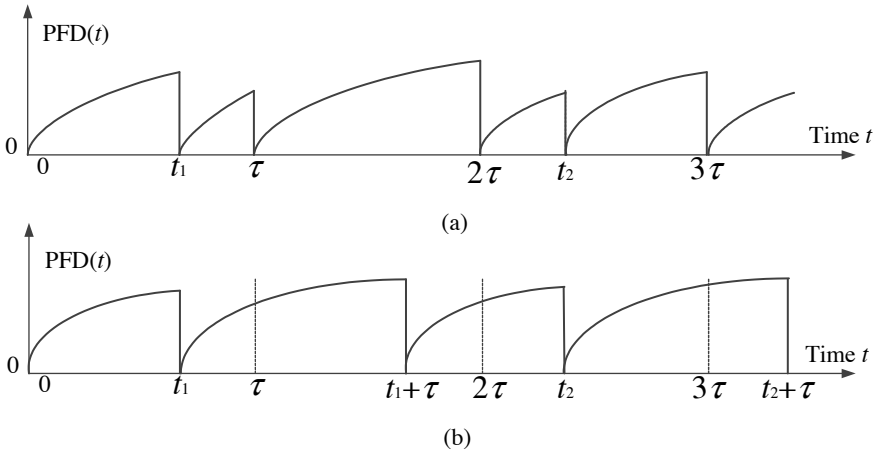

Figure 1: PFD for test strategies II (a) and III (b) as a function of time t, adopted from [12]

The international standard IEC 62551 [4] defines the terminology of Petri nets in dependability analysis. Places (shown as circles in Fig. 2) and transitions (shown as bars) are two basic elements, which 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 change the distribution of tokens in places. A firing time (delay from enabled to fired) can be assigned to each transition. In IEC 62551 [4], a thin bar is used to represent an immediate transition (zero firing time), a blank bar is for 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 [4].

Petri net models in IEC 61508 [2] have in addition predicates and assertions, which are defined in [2] and [18] as

- a predicate (identified by "?" or "??") is a formula to control the enabling condition of a transition;
- an assertion (identified by "!" or "!!") is a formula used to update one variable when the transition is fired.

Such interpretations are also helpful in some ordinary Petri net, and may make the model more compact and understandable.

3.1. Testing strategy I

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

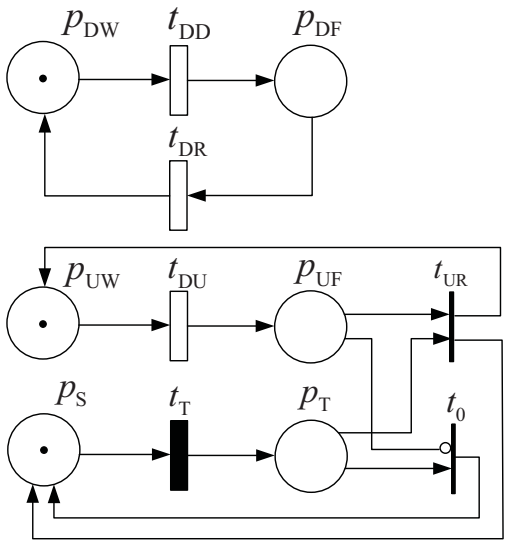

Figure 2: Petri net model for test strategy I

Fig. 2 shows the Petri net model for test strategy I. 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}. The occurrence of a DU-failure is modeled in the same way with p_{UW}, t_{UW} and p_{UF}. Both t_{DD} and t_{DU} are blank, meaning that the failure times are exponentially distributed. In addition, an exponentially distributed transition t_{DR} is used to model 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_{UR} and t_0 express the two situations in a proof test. If a DU-failure in the SIS is revealed, t_{UR} can be fired; otherwise, t_0 can be fired. The inhibitor here is for enabling t_2 when there is no token in p_{UF}. No matter whether t_{UR} or t_0 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. It should be noted that both t_{UR} and t_0 are immediate transitions, ignoring the testing/repair time, since they are much shorter than the testing interval.

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 movement of tokens between p_{DW} and p_{DF} has no influence on other tokens.

It is also possible to model the operation with a Petri net with predicates and assertions (as shown in Fig. 3). Places and transitions have the same meaning as those in Fig. 2. The description "?DU=0" means that a necessary firing condition of t_{DU} is the value of variable DU is equal to 0. And the assertion "!DU=DU+1" means that after the firing of t_{DU}, the value of the variable DU is added with 1.

For the transition t_{UR}, its predicate is "?T=1", meaning that a proof test is carried out. In fact the two firing conditions of this transition are represented by the weight of its input arc in the figure and the predicate respectively. While in case no DU-failure occurs, t_0 is fired with the predicate "?DU=0". It can be found that with predicates and assertions, the functions of inhibitors of Fig. 2

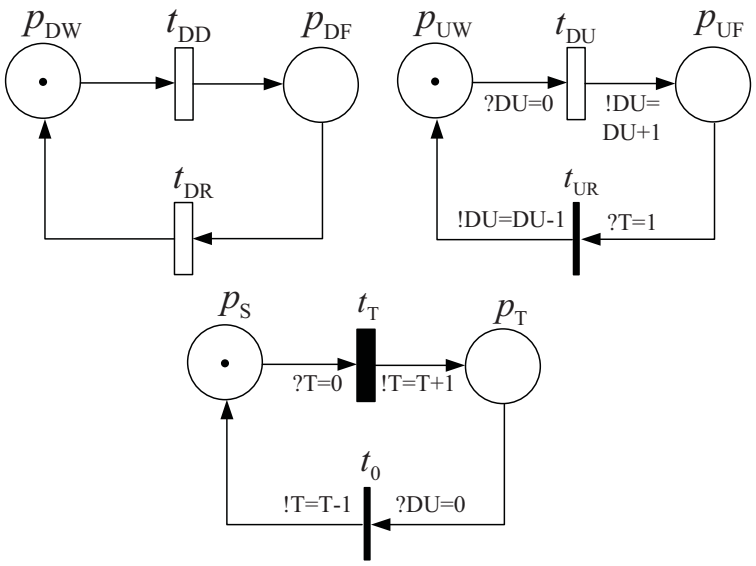

Figure 3: Petri net model for test strategy I with predicates and assertions

can be identically realized in Fig. 3.

3.2. Testing strategy II

Strategy II can also be modeled by a Petri net with predicates and assertions, as illustrated in Fig. 4.

The impact of DD-failures can be modeled with introducing a variable DD. Initially, there is no DD failure present and the value of DD is 0. When a DD-failure occurs, the value of DD becomes 1, and when the DD-failure has been repaired, the value of DD returns to 0. The value DD is also a predicate of t_{UR}, such that when a DU-failure is present, transition t_{UR} can be fired either by a proof test or a DD-failure.

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

3.3. Testing strategy III

The model for testing strategy III can follow Fig. 4 while building a relation between the proof test and the test activated by a DD-failure as in Fig. 5. A predicate "?T=0" is added to the transition t_{DD}, and it also has a new assertion as "!T=T+1". Such controlling sentences are used to assign the resource of proof-testing to the tests activated by a DD-failure, while removing the probability that DD-failure and proof test occur at the same time. Then the testing resource can be allocated back to proof-testing with the assertion t_{DR} as "!T=T-1".

In other words, once a DD-failure occurs, the firing condition of t_T is stopped. The time counting process for the next proof test is not re-initiated until the insert test is finished.

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.

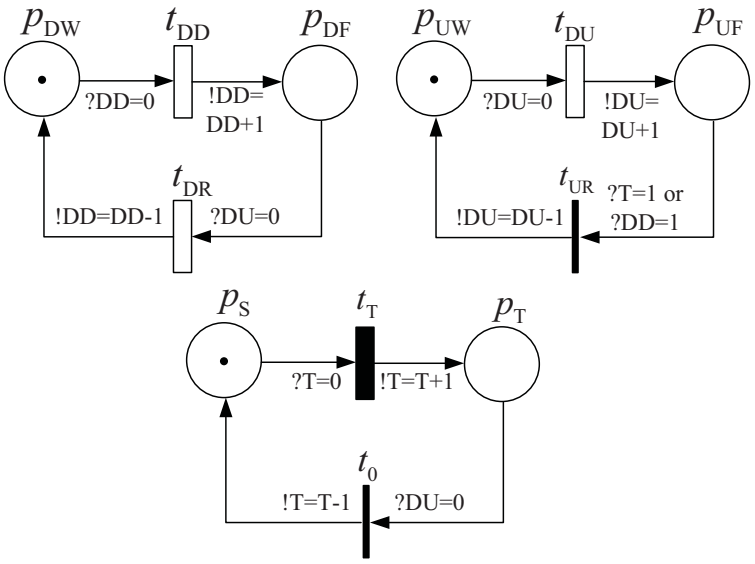

Figure 4: Model for test strategy II

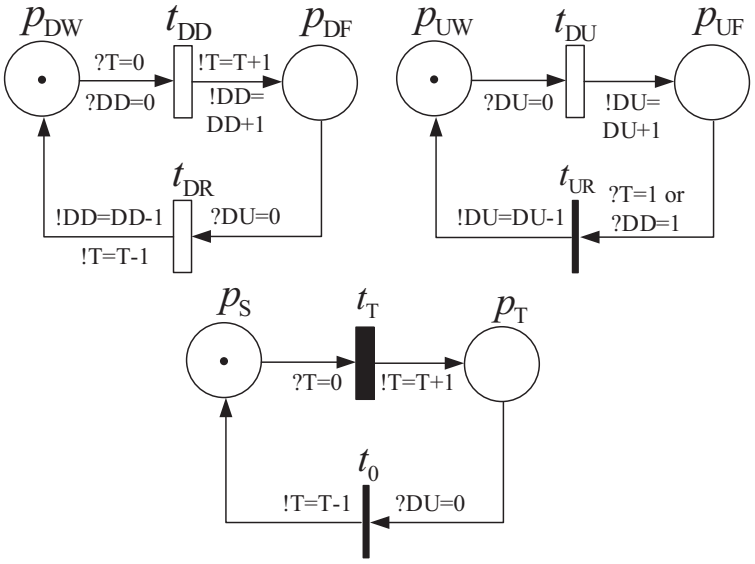

Figure 5: Model for test strategy III

3.4. Input data and assumptions

The formulas derived in the rest of the paper are illustrated by numerical examples. The examples are based on the following data and assumptions:

- DU- and DD-failures occur independent of each other.
- A DU-failure and a DD-failure can be present at the same time.
- The dangerous undetected (DU) failure rate of the channel is $\lambda_{DU} = 2 \cdot 10^{-6}$ per hour.
- The initial dangerous detected (DD) failure rate is $\lambda_{DD} = 2 \cdot 10^{-5}$ per hour. To illustrate the effects of DD-failures, selected values of the DD-failure rate λ_{DD} between $2 \cdot 10^{-5}$ and $2 \cdot 10^{-4}$ per hour are studied. The corresponding DC-values are hence between 0.90 and 0.99.
- The mean repair time of a DD-failure is MTTR = 8 hours. The repair time of a DD-failure also includes the time required to carry out an insert test for DU-failure and, if necessary, to repair this failure. The safety function of the channel is regarded to be lost during the MTTR.
- All failures are detected and repaired during the insert test, and after an insert test, the channel is as-good-as-new.
- The mean time required to proof-test and, if necessary, restore/repair a DU-failure is ignorable compared with the proof test interval. The channel is as-good-as-new after the proof test.
- The scheduled proof-testing interval is $\tau_1 = 8\,760$ hours (i.e., one year). This is the time from a proof test is initiated until the subsequent proof test is initiated.

Such assumptions are used for both approximation formulas and analysis based on Petri nets.

It also should be noted that the assumption of the ignorable test/repair time can be not valid when DD-failures occur too often. If the frequency of DD-failure is very high, the times of tests/repairs can become noticeable in comparison with testing interval, such that their contribution to unavailability of a SIS cannot be skipped. But in this article, we do not consider such extreme situations. As shown in the following example, DD-failure rate is up to 2×10^{-4}, meaning that testing interval even involving insert tests is still much longer than test/repair time. In addition, costs factors in proof and insert tests are also skipped in this article.

3.5. Probability of failure on demand

The PFD_{avg} of the channel is determined by the contributions from DD- and DU-failures, and for all the three testing strategies, PFD_{avg} can be calculated as:

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

where $\Pr(\mathbf{m}(p_{DF}) = 1)$ denotes the average unavailability of the channel due to a DD-failure (i.e., the long term average probability that place p_{DF} holds one token). Similarly, $\Pr(\mathbf{m}(p_{UF}) = 1)$

is equal to the average unavailability of the channel due to a DU-failure. Both $\Pr(\mathbf{m}(p_{\mathrm{DF}}) = 1)$ and $\Pr(\mathbf{m}(p_{\mathrm{UF}}) = 1)$ involve the probability of simultaneous DD- and DU-failures, such that when calculating $\mathrm{PFD}_{\mathrm{avg}}$, the probability $\Pr\left[(\mathbf{m}(p_{\mathrm{DF}}) = 1) \cap (\mathbf{m}(p_{\mathrm{UF}}) = 1)\right]$ must be subtracted to remove this overlap. For highly reliable channels, however, the probability of simultaneous DD- and DU-failures is negligible.

The efficiency of the diagnostic testing for a channel 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.

3.6. Monte Carlo simulation

The $\mathrm{PFD}_{\mathrm{avg}}$ for the single channel for each of the three test strategies is determined by Monte Carlo simulations using the GRIF software.[1] The simulation is based on Petri net models with predicates and assertions (see Figs. 3 and 4). Results are obtained by simulating a period of 87 600 hours (10 years) one million times. The initial value of the DD-failure rate, $\lambda_{\mathrm{DD}} = 2 \cdot 10^{-5}$ per hour is used in the simulations. Table 1 presents the obtained total $\mathrm{PFD}_{\mathrm{avg}}$ and the contributions from DD-failures [$\mathrm{PFD}_{\mathrm{avg(DD)}}$] and DU-failures [$\mathrm{PFD}_{\mathrm{avg(DU)}}$] for each test strategy. It is seen that the contribution from DD-failures is small compared to the contribution from DU-failures.

Table 1: $\mathrm{PFD}_{\mathrm{avg}}$ of a single channel for three different test strategies

	Strategy I	Strategy II	Strategy III
$\mathrm{PFD}_{\mathrm{avg(DD)}}$	$0.16 \cdot 10^{-3}$	$0.16 \cdot 10^{-3}$	$0.16 \cdot 10^{-3}$
$\mathrm{PFD}_{\mathrm{avg(DU)}}$	$8.70 \cdot 10^{-3}$	$8.21 \cdot 10^{-3}$	$8.30 \cdot 10^{-3}$
$\mathrm{PFD}_{\mathrm{avg}}$	$8.86 \cdot 10^{-3}$	$8.37 \cdot 10^{-3}$	$8.46 \cdot 10^{-3}$

The effect of test stategies II and III are not very significant in Table 1. The PFD of the best strategy (II) is only 5.5% lower than the PFD of strategy I. The probability of a DD-failure in a test interval is $1 - e^{-\lambda_{\mathrm{DD}}\tau} \approx 0.16$, meaning than less than one out of six test intervals will experience a DD-failure and an insert test.

3.7. Varying rates of DD-failures

With strategies II and III, the channel is proof-tested after each DD-failure, and the rate of DD-failures, λ_{DD}, therefore influences the contribution $\mathrm{PFD}_{\mathrm{avg(DU)}}$ from DU-failures. To examine this effects, we consider four different DD-failure rates from $2 \cdot 10^{-5}$ to $2 \cdot 10^{-4}$ per hour, while keeping the DU-failure rate at $2 \cdot 10^{-6}$ per hour. The other parameters are kept the same in all the simulations. Table 2 presents the contribution $\mathrm{PFD}_{\mathrm{avg(DU)}}$ due to DU-failures obtained with the GRIF software.

Table 2 illustrates the reductions of $\mathrm{PFD}_{\mathrm{avg(DU)}}$ obtained by using the test strategies II and III. It is found that $\mathrm{PFD}_{\mathrm{avg(DU)}}$ decreases with more frequent DD-failures and follow-up proof-testing for DU-failures.

[1] A software developed by TOTAL for system analysis, more information can be found at `http://grif-workshop.com`

Table 2: $PFD_{avg(DU)}$ for a single channel with different DD-failure rates

	$PFD_{avg(DU)}$		
λ_{DD} (per hour)	Strategy I	Strategy II	Strategy III
$2 \cdot 10^{-5}$	$8.70 \cdot 10^{-3}$	$8.21 \cdot 10^{-3}$	$8.30 \cdot 10^{-3}$
$6 \cdot 10^{-5}$	$8.70 \cdot 10^{-3}$	$7.39 \cdot 10^{-3}$	$7.83 \cdot 10^{-3}$
$1 \cdot 10^{-4}$	$8.70 \cdot 10^{-3}$	$6.61 \cdot 10^{-3}$	$7.30 \cdot 10^{-3}$
$2 \cdot 10^{-4}$	$8.70 \cdot 10^{-3}$	$5.27 \cdot 10^{-3}$	$6.19 \cdot 10^{-3}$

4. Approximation Formulas for PFD_{avg}

Approximation formulas for PFD_{avg} for the three testing strategies are developed in this section. To make it easier to follow our arguments, we have simplified the formulas. The results are therefore not fully correct, but close enough for most practical purposes. The formulas are exemplified by the same input data and the same assumptions as for the simulations based on Petri nets by the GRIF software. We also compare the results with the results obtained by the GRIF software. When developing the approximation formulas, it is assumed that the probability of two or more DU-failures in the same proof test interval is negligible. With the given input data, this probability is approximately $1.5 \cdot 10^{-4}$.

4.1. PFD_{avg} due to DD-failures

Both DD- and DU-failures may cause dangerous downtime of the channel. The downtime associated with DU-failures is, however, different from the downtime associated with DD-failures. A DU-failure is undetected and the safety function of the channel may be unavailable over a long time without our knowledge. We believe that the equipment under control is protected by the channel, while it is in fact unprotected. DD-failures, on the other hand, are detected almost immediately and the safety function is usually unavailable during a short time interval while the DD-failure is repaired. During this downtime, we know that the safety function of the channel is unavailable and may therefore take safety precautions.

The occurrence of DD-failures and the associated downtime are the same for all the three testing strategies. Each time a DD-failure occurs, it is repaired and the mean repair time is MTTR. For all the three strategies, the PFD-contribution from DD-failures is

$$PFD_{avg(DD)} = \lambda_{DD}\,MTTR \tag{2}$$

Whether or not the PFD-contribution from DD-failures should be taken into account depends on the operational strategy and the configuration of the SIS.

4.2. Strategy I

For strategy I, with no insert tests after DD-failures, the contribution to the average PFD from DU-failures, $\mathrm{PFD}^{(\mathrm{I})}_{\mathrm{avg(DU)}}$, is given by (e.g., see page 199 in [16])

$$\mathrm{PFD}^{(\mathrm{I})}_{\mathrm{avg(DU)}} = 1 - \frac{1}{\lambda_{\mathrm{DU}}\tau}\left(1 - e^{-\lambda_{\mathrm{DD}}\tau}\right) \approx \frac{\lambda_{\mathrm{DU}}\tau}{2} \tag{3}$$

The approximation in (3) is always conservative and is considered to be adequate when $\lambda_{\mathrm{DU}}\tau$ is small, e.g., less than $5 \cdot 10^{-2}$ (with our data, $\lambda_{\mathrm{DU}}\tau = 1.75 \cdot 10^{-2}$ and the error is less than 0.6% of the correct value).

Assume that a DU-failure has occurred in a test interval $(0, \tau)$. Because the DU-failure is undetectable, it is not known exactly when the failure occurred. But given that the DU-failure is assumed to occur with an exponential distribution, the time of its occurrence is uniformly distributed over $(0, \tau)$. The mean time of occurrence of the DU-failure is therefore $\tau/2$. The channel will not be able to perform its safety function during the rest of the proof test interval and the mean (dangerous) downtime (MDT) associated with the DU-failure is therefore $\tau/2$ (e.g., see [16]).

Eq. (3) can therefore be written

$$\mathrm{PFD}^{(\mathrm{I})}_{\mathrm{avg(DU)}} \approx \lambda_{\mathrm{DU}} \cdot \mathrm{MDT}^{(\mathrm{I})}_{\mathrm{DU}} \tag{4}$$

Eq. (4) is a general approximation formula for the $\mathrm{PFD}_{\mathrm{avg}}$ due to DU-failures [2, 16] and is used in the rest of this paper.

4.3. Strategy II

With strategy II, the channel is tested for DU-failures and, if necessary, repaired as part of the repair of DD-failures. This means that the channel is as-good-as-new each time a DD-failure has been repaired.

Because all the proof test intervals have the same stochastic properties, we may restrict our attention to the first interval $(0, \tau)$. Assume that a DU-failure has occurred in $(0, \tau)$ and let X be the time of the occurrence of the DU-failure. Because we disregard the possibility of more than one DU-failure in the interval, X is uniformly distributed over $(0, \tau)$. The probability density of X is $f_X(x) = 1/\tau$ for $0 < x \leq \tau$.

Given that a DU-failure occurs at x, and it will remain undetected until the proof test at time τ, unless a DD-failure occurs in the interval (x, τ) and the DU-failure is detected and repaired as part of the repair of the DD-failure. The downtime of the DU-failure is therefore the minimum of $\tau - x$ and the time until a DD-failure. The mean downtime is therefore [16]

$$\mathrm{MDT}^{(\mathrm{II})}_{\mathrm{DU}}(x) \approx \int_0^{\tau-x} e^{-\lambda_{\mathrm{DD}}u}\, du = \frac{1}{\lambda_{\mathrm{DD}}}\left(1 - e^{-\lambda_{\mathrm{DD}}(\tau-x)}\right) \tag{5}$$

The mean downtime related to a random DU-failure can be calculated on the basis of the

expected occurrence time of the DU-failure, and so

$$\begin{aligned} \mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{II})} &= E\left[\mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{II})}(X)\right] = \int_0^{\tau} \mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{II})}(x) f_X(x)\, dx \\ &= \frac{1}{\lambda_{\mathrm{DD}}}\left[1 - \frac{1}{\lambda_{\mathrm{DD}}\tau}\left(1 - e^{-\lambda_{\mathrm{DD}}\tau}\right)\right] \end{aligned} \tag{6}$$

The corresponding average PFD is calculated according to mean downtime similarly with eq. (4) as

$$\mathrm{PFD}_{\mathrm{avg(DU)}}^{(\mathrm{II})} \approx \lambda_{\mathrm{DU}} \cdot \mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{II})} \tag{7}$$

The results obtained by using eq. (7) are presented in Table 3 and compared with the results obtained by simulating the Petri net model by the GRIF software. The results obtained by the approximation formulas are seen to be very close to the results obtained by the GRIF software. A reason for obtaining slightly higher values by the approximation formulas is that we have used conservative approximations when we developed the formulas.

Table 3: $\mathrm{PFD}_{\mathrm{avg(DU)}}$ for a single channel with different DD-failure rates and with test strategy II

	$\mathrm{PFD}_{\mathrm{avg(DU)}}$	
λ_{DD} (per hour)	Petri net	Approx. formula
$2 \cdot 10^{-5}$	$8.21 \cdot 10^{-3}$	$8.26 \cdot 10^{-3}$
$6 \cdot 10^{-5}$	$7.39 \cdot 10^{-3}$	$7.40 \cdot 10^{-3}$
$1 \cdot 10^{-4}$	$6.61 \cdot 10^{-3}$	$6.67 \cdot 10^{-3}$
$2 \cdot 10^{-4}$	$5.27 \cdot 10^{-3}$	$5.28 \cdot 10^{-3}$

4.4. Strategy III

The main difference between strategy II and strategy III is that with strategy III, the time to the next proof test is reset after each DD-failure. When the channel is repaired (either as part of a proof test or an insert test), the channel is as-good-as-new and the time to the next test is equal to the minimum of τ and the time to a DD-failure. The length Y of the test interval is therefore a random variable with probability density

$$f_Y(y) = \begin{cases} \lambda_{\mathrm{DD}} e^{-\lambda_{\mathrm{DD}} y} & \text{for } 0 < y < \tau \\ e^{-\lambda_{\mathrm{DD}}\tau} & \text{for } y = \tau \end{cases}$$

The mean length of a test interval is

$$E(Y) = \int_0^{\tau} e^{-\lambda_{\mathrm{DD}} u}\, du = \frac{1}{\lambda_{\mathrm{DD}}}\left(1 - e^{-\lambda_{\mathrm{DD}}\tau}\right) \tag{8}$$

Because a test interval is restarted after each DD-failure, no DD-failure can occur within the test interval. All the test intervals have the same stochastic properties and we can therefore restrict

our attention to a specific interval that is started at time $t = 0$. Assume that a DU-failure is observed in the test (proof test or insert test) at time y. As for strategy II, the conditional occurrence time X of the DU-failure is uniformly distributed over $(0, y)$. The occurrence of the DU-failure is not observable, but we denote the occurrence time x. The downtime associated with the DU-failure is $y - x$ and the mean downtime is $\mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(y) = y/2$, i.e., the conditional mean downtime when the length of the test interval, in which the DU-failure occurred, is y.

When we know that a DU-failure occurred at time x, we also know that a DD-failure did not occur in the interval $(0, x)$. Because of the memoryless property, the time to the next DD-failure is measured from time x. The time till the next test is therefore the minimum of $\tau - x$ and the time until a DD-failure. The conditional mean downtime associated to the DU-failure at time x is therefore calculated according to eq. 8 as

$$\mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(x, y) = \frac{1}{\lambda_{\mathrm{DD}}}\left(1 - e^{-\lambda_{\mathrm{DD}}(\tau - x)}\right) \tag{9}$$

The mean downtime (conditional on y, but not on x) is

$$\begin{aligned}\mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(y) &= \int_0^y \mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(x, y) f_X(x)\, dx = \int_0^y \mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(x, y) \cdot \frac{1}{y}\, dx \\ &= \frac{1}{\lambda_{\mathrm{DD}}} - \frac{e^{-\lambda_{\mathrm{DD}}\tau}}{\lambda_{\mathrm{DD}}^2 y}\left(e^{\lambda_{\mathrm{DD}} y} - 1\right)\end{aligned} \tag{10}$$

Because of the uniform distribution, the conditional mean occurrence time of the DU-failure (given y) is in the middle of the test interval and on the average, the mean time until the DU-failure, must be equal to the mean downtime, that is

$$E(X \mid y) = \mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(y)$$

This means that we can determine y and thereby the MDT related to the DU-failure by solving

$$\frac{y}{2} = \frac{1}{\lambda_{\mathrm{DD}}} - \frac{e^{-\lambda_{\mathrm{DD}}\tau}}{\lambda_{\mathrm{DD}}^2 y}\left(e^{\lambda_{\mathrm{DD}} y} - 1\right) \tag{11}$$

The solution is not very easy to be organized as a simple formula, so we used a computer to find y from eq. (11). The mean downtime is $\mathrm{MDT}_{\mathrm{DU}}^{(\mathrm{III})}(y) = y/2$ and the results of $\mathrm{PFD}_{\mathrm{avg}}$ are given in Table 4. The results obtained by the approximation formulas are seen to be somewhat higher than the results obtained by using the GRIF software, but still acceptable for most practical purposes.

5. Number of Tests with the Three Strategies

Testing for DU-failures induced by DD-failures can improve the performance of a channel, especially when the diagnostic coverage is high (e.g., DC > 90%). In the following, the number of tests for DU-failures with the three strategies are calculated for a interval $(0, m\tau)$, where m is an integer.

Table 4: $\text{PFD}_{\text{avg(DU)}}$ for a single channel with different DD-failure rates and with test strategy III

	$\text{PFD}_{\text{avg(DU)}}$	
λ_{DD} (per hour)	GRIF software	Approx. formula
$2 \cdot 10^{-5}$	$8.30 \cdot 10^{-3}$	$8.50 \cdot 10^{-3}$
$6 \cdot 10^{-5}$	$7.83 \cdot 10^{-3}$	$8.02 \cdot 10^{-3}$
$1 \cdot 10^{-4}$	$7.30 \cdot 10^{-3}$	$7.56 \cdot 10^{-3}$
$2 \cdot 10^{-4}$	$6.19 \cdot 10^{-3}$	$6.44 \cdot 10^{-3}$

1. For strategy I, the scheduled proof tests are the only tests for DU-failures. During $(0, m\tau)$, the number, $N_I^{(\text{PT})}(0, m\tau)$, of proof tests is

$$N_I^{(\text{PT})}(0, m\tau) = m \tag{12}$$

2. For strategy II, all the m scheduled proof tests are carried out. In addition, insert tests for DU-failures are carried out after each DD-failure. The mean number $N_{II}^{(\text{IT})}(0, m\tau)$ of insert tests during a period $m\tau$ is given by

$$N_{II}^{(\text{IT})}(0, m\tau) = \lambda_{\text{DD}} \left(m\tau - N_{II}^{(\text{IT})}(0, m\tau)\text{MTTR} \right)$$

because each time a DD-failure occurs, the channel is inoperable during the repair time of the DU-failure and the associated insert test. This gives

$$N_{II}^{(\text{IT})}(0, m\tau) = \frac{m\lambda_{\text{DD}}\tau}{1 + \text{MTTR}\lambda_{\text{DD}}} \tag{13}$$

The total mean number of tests for DU-failures with strategy II is therefore

$$N_{II}^{(\text{T})}(0, m\tau) = N_{II}^{(\text{PT})}(0, m\tau) + N_{II}^{(\text{IT})}(0, m\tau) = m + \frac{m\lambda_{\text{DD}}\tau}{1 + \text{MTTR}\lambda_{\text{DD}}} \tag{14}$$

3. For strategy III, proof tests are only carried out when the time since the previous DD-failure or proof test is at least τ. The time to the next test for DU-failure is therefore the minimum of the time to the next DD-failure and τ. The mean time between tests (MTBT) for DU-failures (i.e., proof tests or insert tests) is therefore (e.g., see [17])

$$\text{MTBT}(\tau) = \int_0^\tau e^{-\lambda_{\text{DD}} t}\, dt = \frac{1}{\lambda_{\text{DD}}} \left(1 - e^{-\lambda_{\text{DD}}\tau} \right) \tag{15}$$

The total mean number , $N_{III}^{(\text{T})}(0, m\tau)$ of tests for DU-failures with this strategy is

$$N_{III}^{(\text{T})}(0, m\tau) = \frac{m\tau - N_{III}^{(\text{T})}(0, m\tau)\text{MTTR}}{\text{MTBT}(\tau)}$$

This gives

$$N_{III}^{(\mathrm{T})}(0, m\tau) = \frac{m\tau}{\mathrm{MTBT}(\tau) + \mathrm{MTTR}} \tag{16}$$

The mean number of DD-failures (and insert tests) is not influenced by the test strategy, and thus it is possible to use eq. (13) again here to calculate $N_{III}^{\mathrm{IT}}(0, m\tau)$. And then, the mean number of proof tests with strategy III is equal to the number of total tests minus the number of insert tests:

$$\begin{aligned} N_{III}^{(\mathrm{PT})}(0, m\tau) &= N_{III}^{(\mathrm{T})}(0, m\tau) - \frac{m\lambda_{\mathrm{DD}}\tau}{1 + \mathrm{MTTR}\lambda_{\mathrm{DD}}} \\ &= \frac{m\tau}{\mathrm{MTBT}(\tau) + \mathrm{MTTR}} - \frac{m\lambda_{\mathrm{DD}}\tau}{1 + \mathrm{MTTR}\lambda_{\mathrm{DD}}} \end{aligned} \tag{17}$$

Table 5 presents the mean number of proof tests and insert tests for strategies II and III with the data in the case example, over a period of length 10τ (i.e., ten years) .

Table 5: Average test numbers in ten years

λ_{DD} (per hour)	Strategy II		Strategy III	
	PT	IT	PT	IT
$2 \cdot 10^{-5}$	10	1.75	9.13	1.75
$6 \cdot 10^{-5}$	10	5.25	7.59	5.25
$1 \cdot 10^{-4}$	10	8.75	6.24	8.75
$2 \cdot 10^{-4}$	10	17.49	3.67	17.49

6. Summary and research perspectives

This paper has studied follow-up activities after a DD-failure has been detected in a SIS channel. Insert proof tests to reveal DU-failures are found to be able to reduce the PFD of the channel, especially when DD-failures occur frequently. Petri net models with predicates and assertions have been developed to assess the PFD and the PFD has been quantified for tree testing strategies and for different values of the DD-failure rate. Approximation formulas have been developed for the three testing strategies and compared with the results obtained by the Petri nets models. Strategy II is found to give the lowest PFD, but leads a rather high number of tests. Strategy III also gives an improved PFD, but this strategy may in practice be expensive to manage.

The main reason that approximation formulas have been developed is that we believe that the user can get far more insight into the problem by studying the approximation formulas than by obtaining the results by simulation. Another benefit is that the approximation formulas can be evaluated without any dedicated software. A standard spreadsheet program is sufficient.

The current paper is restricted to a single channel of a SIS and it is assumed that all tests perfect tests, in the sense that all failures are detected and that the channel is repaired to an as-good-as-new condition. This assumption may not always be realistic and the authors are working

with an extension of the paper where the insert tests are imperfect tests with a less than perfect test coverage.

Studies of more complex SISs with several identical or non-identical channels are on-going and will be reported in the future.

Acknowledgment

Dr. Fares Innal has given helpful guidance on using the GRIF simulation software.

References

[1] Bukowski, J., 2006. Incorporating process demand into models for assessment of safety system performance. In: Poceedings of RAM' 06 Symposium. Alexandria, VI, USA.

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

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

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

[5] Innal, F., 2008. Contribution to modelling safety instrumented systems and to assessing their performance critical analysis of IEC 61508 standard. Ph.D. thesis, University of Bordeaux.

[6] Innal, F., Dutuit, Y., Chebila, M., 2015. Safety and operational integrity evaluation and design optimization of safety instrumented systems. Reliability Engineering & System Safety 134, 32–50.

[7] Innal, F., Dutuit, Y., Rauzy, A., Signoret, J. P., 2010. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. In: Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. Vol. 224. pp. 75–86.

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

[9] Jin, H., Lundteigen, M. A., Rausand, M., 2011. Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation. Reliability Engineering & System safety 96 (3), 365–373.

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

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

[12] Liu, Y., Rausand, M., 2014. Proof testing of safety-instrumented systems: New testing strategy induced by dangerous detected failures. In: 12th Probabilistic Safety Assessment & Management Conference (PSAM 12). Honolulu, HI.

[13] Liu, Y. L., Rausand, M., 2011. Reliability assessment of safety instrumented systems subject to different demand modes. Journal of Loss Prevention in the Process Industries 24 (1), 49–56.

[14] Lundteigen, M. A., Rausand, M., 2009. Architectural constraints in IEC 61508: Do they have the intended effect? Reliability Engineering & System Safety 94 (2), 520–525.

[15] Lundteigen, M. A., Rausand, M., 2010. Reliability of safety instrumented systems: Where to direct future research? Process Safety Progress 29 (4), 372–379.

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

[17] Rausand, M., Høyland, A., 2004. System Reliability Theory; Models, Statistical Methods, and Applications, 2nd Edition. Wiley, Hoboken, NJ.

[18] Signoret, J.-P., Dutuit, Y., Cacheux, P.-J., Folleau, C., Thomas, P., 2013. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering & System Safety 113, 61–75.

[19] Torres-Echeverria, A. C., Martorell, S., Thompson, H. A., 2009. Modelling and optimization of proof testing policies for safety instrumented systems. Reliability Engineering & System safety 94 (4), 838–854.

[20] Torres-Echeverria, A. C., Martorell, S., Thompson, H. A., MAY 2011. Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing. Reliability Engineering & System Safety 96 (5), 545–563.