CHEMICAL ENGINEERING TRANSACTIONS
VOL. 33, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Enrico Zio, Piero Baraldi

ISBN 978-88-95608-24-2; **ISSN** 1974-9791
DOI: 10.3303/CET1333063

Testing Strategies of Redundant Safety Instrumented Systems with Dangerous Detected Failures

Yiliu Liu

Department of Production and Quality Engineering, Norwegian University of Science and Technology, S.P. Andersens 5, Trondheim, Norway, 7491
yiliu.liu@ntnu.no

Proof testings are regularly conducted on safety instrumented systems (SISs) to reveal dangerous undetected (DU) failures so as to reduce process risks. Sometimes, self-diagnostic tests of SISs can find dangerous detected (DD) failures which will be fixed as soon as possible. If such detections of failures also activate further tests for all components in the SIS in order to discover hidden failures, the original functional test strategy will be adjusted. Three following test strategies for redundant SISs including parallel structures are discussed in this paper given that a DD failure has been found, and then models for these strategies are proposed based on Petri nets.

1. Introduction

Safety-instrumented systems (SISs) have been widely used in the process industry, so as to mitigate the risk associated with the operations of specified systems (Fanelli, 2012), which are referred as the equipment under control (EUC). Many SISs are only activated when a process demand occurs in the EUC, and as a result, some dangerous failures in SISs cannot be found until the systems are activated or tested. Modern SISs may conduct self-diagnostic testing during operation. Such testing can detect some dangerous failures immediately when they occur. The average period of unavailability of a SIS due to these dangerous detected (DD) failures is the mean down time (MDT) from the failure is detected until the function of the SIS is restored.

On the other hand, those dangerous failures not discovered with self-diagnostic testing are called dangerous undetected (DU) failures (Rausand, 2004), which should be revealed in a proof test and then fixed. Proof tests are always conducted at regular intervals, e.g. once per year, therefore the EUC is not protected by the SIS from the moment when a DU failure occurs until the subsequent proof test.

Redundant structures are often applied in SISs in order to achieve a high reliability. For example, if two shutdown valves are installed in a parallel structure as the actuating elements of a SIS (as a one-out-of-two structure, 1oo2), the flow can be stopped in emergency when any of them is able to close on demand. Given one valve has DU failure, the system is still functional if the other one can work well. The probability that both of the two items are in the failure state at the same time is much lower than that of DU failure occurring in one valve.

Both of two components in an 1oo2 system can have DD failures, and if a DD failure in one of components is detected, the system becomes an 1oo1 SIS during the repair, while the other component is assumed to perform safety instrumented function until the failed one is restored. After that, the maintenance team can select to conduct a proof test on this newly fixed component and check whether there is a hidden failure. And then, for another component, there are options available for the maintenance team: 1. Test the component for proof as soon as possible; 2. Test the component in the previously determined regular proof test.

Current studies on reliability of SISs always skip measuring the effects of the different strategies after a DD failure is found in a redundant structure. As a result, potential test strategies after DD failures need to be identified and modelled with proper methods, so as to measure their impacts on the reliability of SIS. In

Please cite this article as: Liu Y., 2013, Testing strategies of redundant safety instrumented systems with dangerous detected failures, Chemical Engineering Transactions, 33, 373-378 DOI: 10.3303/CET1333063

this paper, a 1oo2 SIS will be taken as an example of redundant structures and the test strategies after a DD failure is found in such a system will be studied.
The remainders of this article are organized as following: Test strategies for are identified in section 2. In section 3, several modelling methods are compared, and then models for different strategies are proposed in section 4. Conclusions and research perspectives occur at the end.

2. Test strategies

For an 1oo2 SIS, such as the two shutdown valves in a high integrity pressure protection system (HIPPS) for a pipeline as shown in Figure 1, two components in the system are normally tested one by one in proof tests.

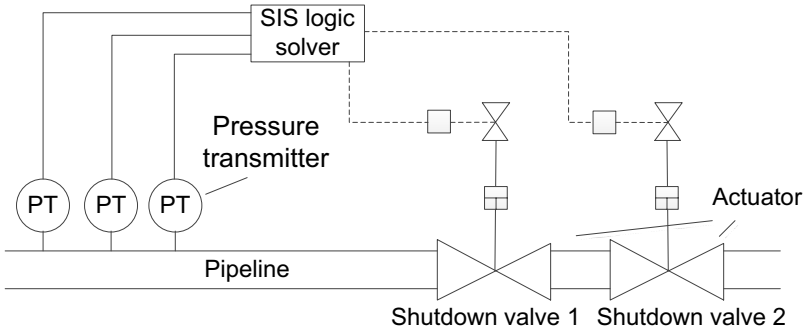

Figure 1: A high integrity pressure protection system

If a DD failure occurs in one valve, the maintenance team can fix the DD failure and have a proof test on the valve, and then they can decide whether or not to conduct a proof test on another valve. The decision should be made based on the working conditions and available maintenance resources.
Given a proof test is conducted on the valve without DD failure, it can be regarded as an ''insert proof test'' between two regular proof tests. In this context, since such a test also can guarantee all hidden failures in the tested valve are found, it is necessary to measure whether the original proof test schedule needs to be adjusted. For example, if proof tests are initially planned to conduct at each September 1st, and the regular test interval is one year. When there is an ''insert proof test'' at June 1st, the maintenance should decide the next date of proof test is September 1st or June 1st next year.
Therefore, there are three main strategies possible to be adopted by the SIS operators given a DD failure occurs in one of two parallel components:

- Strategy 1: Do not test another component until the subsequently regular proof test (Keep the current test strategy unchanged).
- Strategy 2: Test another component, and keep the current proof test schedule unchanged.
- Strategy 3: Test another component, and change the proof test schedule (mostly postpone the subsequent proof test).

In all these three strategies, the subsequent proof test will cover both of the two components.
In fact, there are some other possible test strategies in different operating conditions, e.g. when a DD failure is found in valve 1, fix it and test valve 1 while skip valve 2. In the subsequently regular proof test, only valve 2 will be tested. Such a strategy may be applicable for SISs where two components are installed very far from each other. But in this paper, only common situations are taken into consideration, one valve is assumed able to be tested immediately after the test on the other one is finished.

3. Modelling methods

In terms of SIS modelling and reliability assessment, some methods have been developed. The approximation formulas suggested by the IEC standard (IEC 61508, 2009) have been widely used in process industries, and PDS handbook also provides similar methods for Norwegian oil and gas industry (Hauge et al., 2010). Such formulas are easy to use, but they are not able to measure dynamic (time-dependent) behaviours associated with a SIS.
State-based approaches, such as Markov methods, are more suitable for systems with dynamic behaviours (Liu and Rausand, 2011). However, it is difficult, if not impossible, to identify all states of the SIS given that proof tests are triggered upon opportunities so as to make analysis in a Markov model. Another state-based method, Petri net (PN), may be a better alternative. Liu et al. (2012) have compared

PN and Markov method, and conclude PN models have advantages in the flexibility and completeness of SIS modelling. In this paper, PN will be adopted to model different test strategies.

In simple, PN is a graphical and mathematical modeling tool to describe a system. A PN may be regarded as a 5-tuple, PN = (P, T, F,W, M), where:

$P = \{p_1, p_2, \ldots, p_m\}$ is a finite set of places,

$T = \{t_1, t_2, \ldots, t_n\}$ is a finite set of transitions,

$F \subseteq \{P \times T\} \cup \{T \times P\}$ is a set of arcs,

$W: F \rightarrow \{1, 2, 3, \ldots\}$ is a multiplicity function of an arc,

$M : P \rightarrow \{0, 1, 2, 3, \ldots\}$ is a marking.

As David and Allen describe in their book (2004), the two basic elements of PN, places (shown as circles) and transitions (shown as bars) are connected with directed arcs. For each arc, a multiplicity is assigned. Tokens are illustrated as bullets and assigned to the places. The distribution of tokens in the places of a PN is called marking, and each marking represents a system state.

In addition, sometimes an inhibitor arc (shown as a small circle at the end of an arc) is used to prevent a transition from being enabled. A firing time can be assigned to each transition, such that a PN can have two types of transitions: immediate transitions (0 firing time, shown as thin bars) and timed transitions (shown as thick bars). More details about PN can be found in IEC 62551.

4. Models of proof test strategies

Before modeling, some assumptions in this paper should be mentioned:

- DU-failures in different components occur independently from each other;
- A component has at most one type of failure (DU/DD) at a specific moment;
- Repairs can restore the failed components to a fully functioning state.

Since PN is very flexible modeling method, models proposed in the following subsections are not the only ways for modeling the corresponding test strategies

4.1 Strategy 1

The model for the strategy where test is not performed on the component without DD failure is illustrated as in Figure 2.

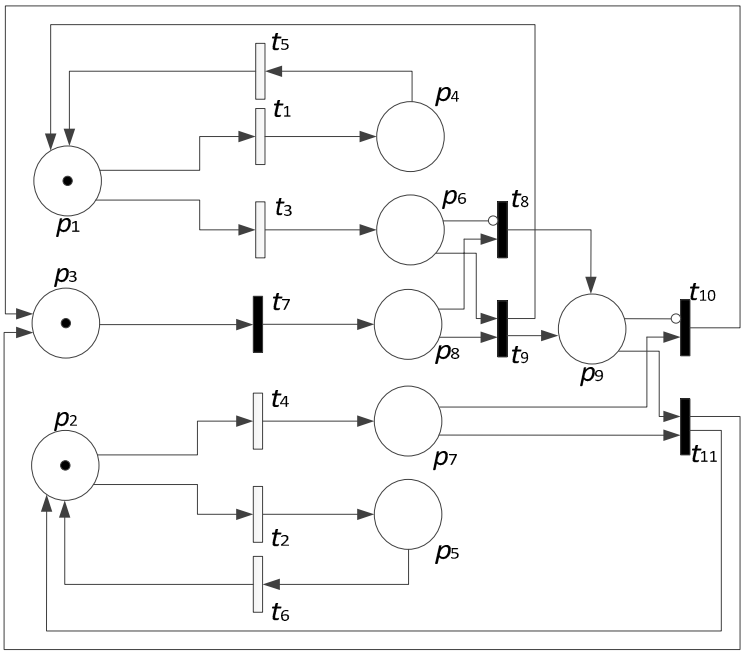

Figure 2: A PN model for strategy 1

In this model, blank bars, such as t_1 and t_3, are used to denote transitions with the transition time (the duration from the moment a transition is enable to it is fired) of exponential distribution, and filled bars, such as t_7, denote transitions with deterministic transition time. IEC 62551 has defined symbols for

transitions with different distributions of firing time. It can be found that failures and restorations are assumed to follow exponential distribution in this model, and test intervals are deterministic.
When the token in p_1 is absorbed by t_1 due to DD failure, the enabling condition of t_3 is not satisfied any more until a token comes back to p_1. It implies that the component is totally restored when t_5 is fired, in terms of both DD and DU failures.
Places denoting DD failures are separate from ones associated with tests in Figure 2, therefore DD failures have no influence on test strategies.

4.2 Strategy 2
In strategy 2, a DD failure in one component can trigger a proof test on the other one, so the model in Figure 2 should be adjusted as in Figure 3.

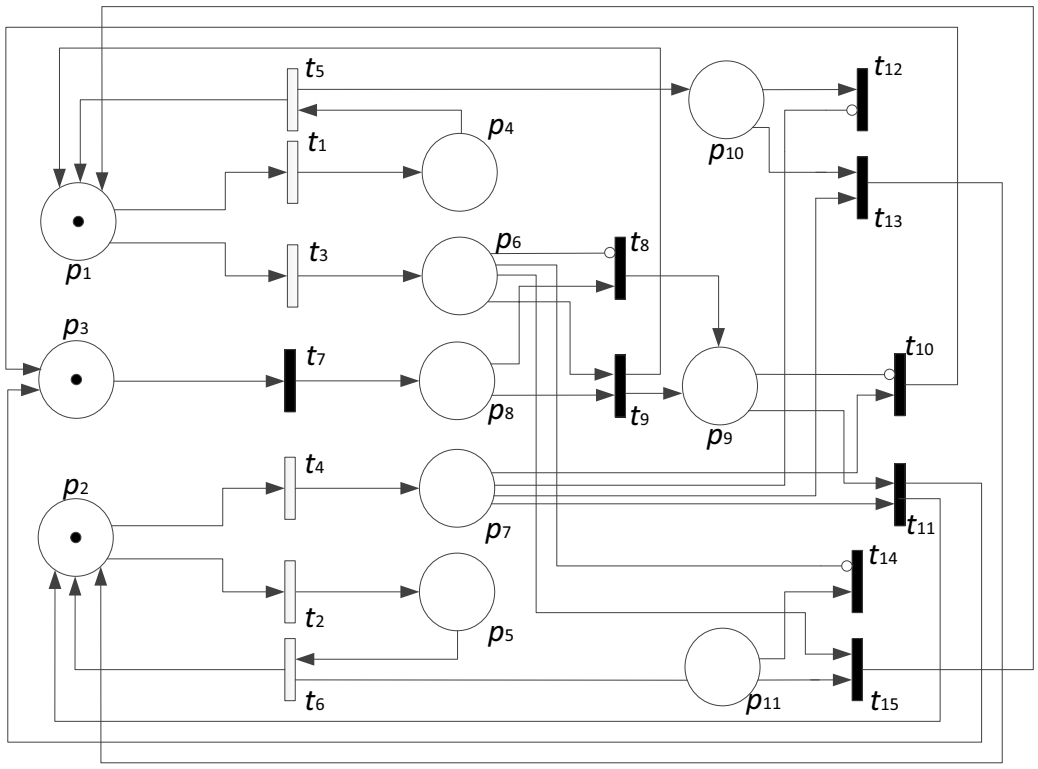

Figure 3: A PN model for strategy 2

Two places p_{10} and p_{11} are added in the updated model. When a DD failure is detected in valve 1, a restoration is initiated by firing t_5, and then releasing one token in p_{10} while another token in p_1. Such a change of tokens means the failed valve is repaired and the maintenance team is ready to fulfil another task (token fallen in p_{10} denotes the team).
Places p_{10} and p_7 are related with transitions t_{12} and t_{13}. It is known a token staying in p_7 means a DU failure in valve 2, thus if there is a DU failure, t_{13} in the model is enabled. And then, the tokens in p_7 and p_{10} will be removed by t_{13}, meaning the insert test is conducted, and the failure is revealed and fixed. On the other hand, if no token is in p_7, the team cannot find a failure in valve 2. They finish the test, and in the model, the token in p_{10} will be absorbed by t_{12} with the inhibitor arc.
For the DD failure in valve 2, it also can trigger a test on valve 1, modelled in the same way shown in Figure 3.
In such a model, the part of regular proof test is not impacted by the newly adding places and transitions, thus the initial testing strategy will keep unchanged.

4.3 Strategy 3
In strategy 3, a DD failure in one of valves can trigger the test on the other. In addition, the next proof test will be postponed so as to save costs associated with tests, since the insert proof test have revealed all hidden failures. The model for strategy 3 is shown in Figure 4.

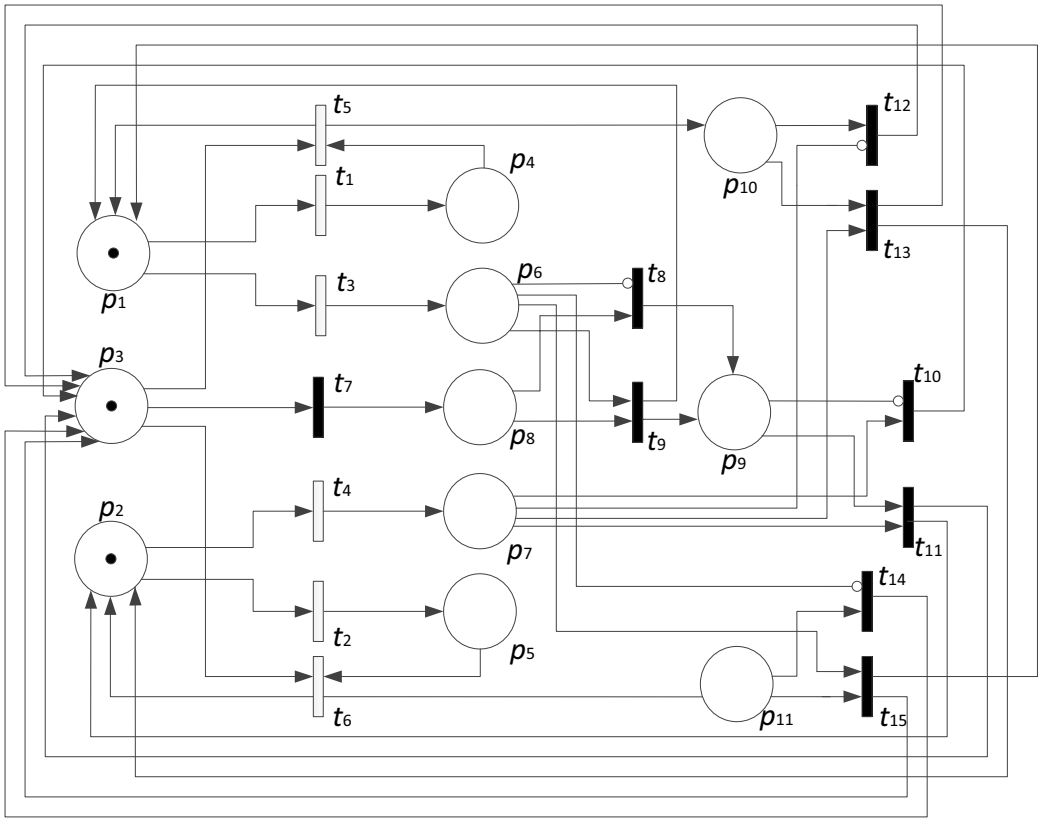

Figure 4: A PN model for strategy 3

Two output arcs from p_3 are added in the model in Figure 3. Such additions can help t_5 to remove the token in p_3 when it is fired. And then the firing of t_7 is stopped, meaning the initial proof test schedule is changed.

After the firing of t_{12} or t_{13}, one token can return to p_3, the enabling condition of t_7 can be satisfied again, and its firing time starts from the moment the token falls in the place. Such a model illustrates that the regular test resource will be shared by the insert test, and both of two types of proof tests can find the hidden failures in components.

4.4 Reliability Assessment

Reliability assessment is not the focus of this paper, but some clues can be provided. The results of the assessment can be used to compare these strategies.

When measuring the reliability of the SIS, the probability that both place p_1 and p_2 have no token can be used to calculate the average unavailability. In such a method, both DD and DU failures are contributors of the unavailability.

5. Conclusions and research perspectives

Three models based on Petri nets are proposed in this article, for simulating different test strategies for a redundant SIS when a DD failure is found in one of two components. Such models reveal the differences in behaviours of maintenance team with various test strategies, and will be helpful to measure their effects on the reliability of the SIS. Monte Carlo simulation can be adopted in the assessment. On the other hand, numerical method may be also helpful given that all deterministic transitions should be approximated as transitions with exponential distribution.

Models in this paper can be further compacted and streamlined so as to increase their readability. Such a modelling method seems more complex than the one where one place hold two tokens, but it is able to model behaviours of two different components. A colour Petri net (CPN) method can be used to reduce the sizes of models. More details about CPN can be found in the book of David and Allen (2004).

For future researches, reliability assessment for the SIS should be well conducted based on models in this paper, in order to compare these testing strategies. It is not hard to find that with strategy 2, a higher

reliability of the SIS can be expected, but how much improvement is still in question. If the cost related with the testing operations is noticeable, it may be necessary to make a balance between the reliability improvement and its price.
Models for more complex systems and test strategies are also wanted in deeper studies. SISs with 1oo3, 2oo3, 2oo4 structures should be modelled, and staggering testing methods also should be taken into consideration.
Last but not least, common cause failures (CCFs) are very important factors of the reliability of a SIS with a redundant structure. Such kind of failures should be involved in future modelling.

References

Bukowski J., 2006, Incorporating process demand into models for assessment of safety system performance, in Proceedings of RAM' 06 Symposium. 571-581, Alexandria, VI, USA.

David R., Alla H., 2004, Discrete, Continuous, and Hybrid Petri Nets. Springer, Heidelberg, Germany.

Fanelli P., 2012, Safety and environmental standards for fuel storage sites: How to enhance the safety integrity of an overfill protection system for flammable fuel storage tanks, Chemical Engineering Transactions, 26, 435-440.

Hauge S., Lundteigen M. A., Hokstad P., Håbrekke S., 2010, Reliability Prediction Method for Safety Instrumented Systems. SINTEF, Trondheim, Norway.

IEC 61508, 2009, Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Part 1-7, International Electrotechnical Commission, Geneva, Switzerland.

IEC 62551, 2012, Analysis techniques for dependability: Petri net techniques, International Electrotechnical Commission, Geneva, Switzerland.

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.

Rausand M., 2011. Risk Assessment: Theory, Methods, and Applications. Wiley, Hoboken, NJ, USA.