# Chapter 4.
# Testing and Maintenance

Mary Ann Lundteigen  Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

**NTNU – Trondheim**
Norwegian University of
Science and Technology

# Learning Objectives

The main learning objectives associated with these slides are to:

- Introduce different types of testing of safety instrumented systems (SIS)
- Relate testing to reliability of SIS
- Discuss some underlying assumptions associated with repair of failures

The slides include topics from Chapter 4 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

# Outline of Presentation

# Definition of Testing and Maintenance

Suitable definitions aimed to use in relation to SIS are:

☞ Testing: Execution of a function of a system, subsystem, or channel to confirm that the function can be performed according to the requirements stated in the safety requirement specification (SRS).

☞ Maintenance: The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state which it can perform a required function (IEC 191-07-01).

# Why Important?

Testing and maintenance are of particular importance for SIS:

- Some SISs are dormant (passive) while in normal operation, and the ability to function must be checked from time to time.
- The state of each redundant channels may not necessarily be confirmed in relation to demands
- We want to perserve the assumptions about constant failure rates, meaning that the SIS components should always be in their useful life period (and replaced before entering the wear-out phase)

The main strategy for testing and maintenance of SIS has been preventive and calendar-based. It is now a trend to replace this strategy with condition-based, where possible. This would impact how we calculate PFD and PFH.

# Procedures

Testing and maintenance procedures:

- Describes how and when the tests and carry out the maintenance.
- Give guidance on how to report different types of failures, so that they are linked to the correct lists for further analyses and treatment
- Procedures give often reference to the equpiment *safety (or operation) manual*, which will give more specific details about methods, constraints, and tools.

# Several Types of Tests

In relation to a SIS, we may distinguish between the following types of tests *in the operational phase*:

- Proof tests
- Function test
- Diagnostic tests
- Partial proof tests
- Staggered tests

The tests are discussed in more detail in the following.

# Proof Ttest

☞ Proof test: A carefully planned periodic test, which is designed to reveal all DU faults of each channel in a safety loop.

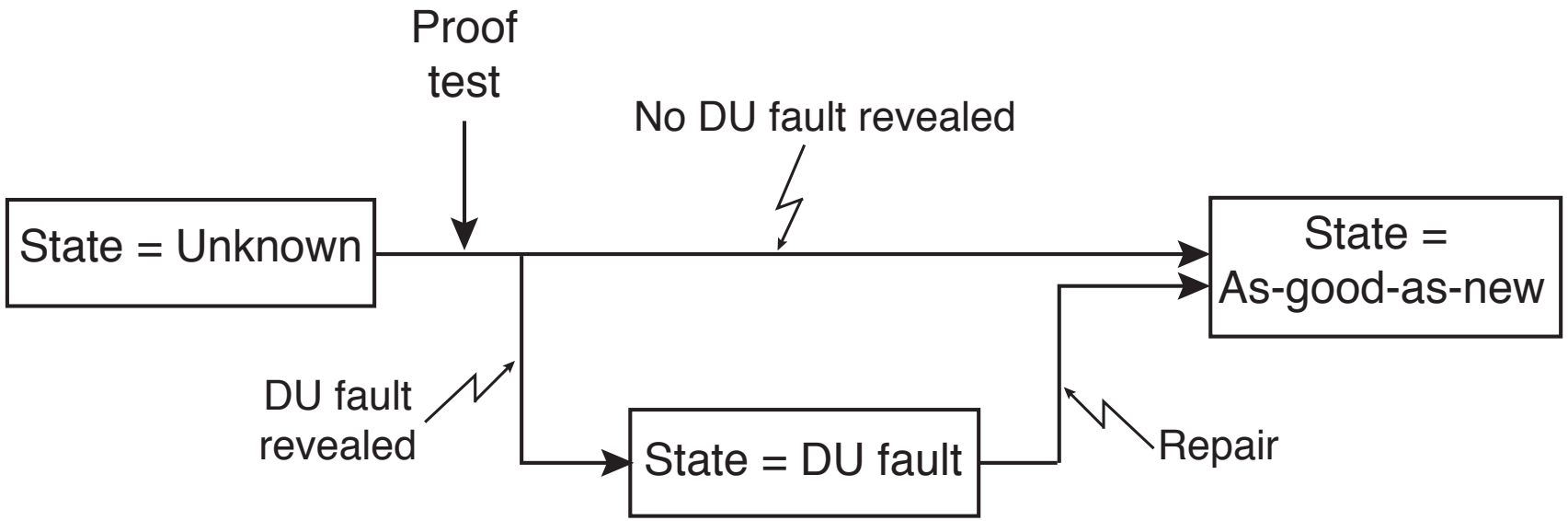
A proof test will be carried out according to a specified *proof test interval*, determined with basis in regulatory requirements, manufacturer's recommendations, and reliability analyses.

# Proof Test

The main purpose of a proof test is to reveal *all* DU failures, but this is not always possible. We may therefore distinguish between:

- **Full proof test**: A proof test where it is planned to reveal all DU failures are revealed. This is an ideal, but often unrealistic situation. Nevertheless, we often assume that a proof test is full (perfect) in reliability assessments.
- **Imperfect /partial proof test**: A proof test where not all DU failures are revealed, due to planned restrictions in test scope (partial test) or constraints about the test due to test conditions and/or inadequacies in how the test is carried out (imperfect test).

# The Proof Test Process



# Practical Implementation

A proof test is often split into sub-tests of practical reasons. For example, at regular intervals there may be campaigns to test all pressure transmitters at the facility, or to function test all emergency shutdown valves to check closure and response times.

A proof test procedure will give the specific details about the test to be carried out, including

- Preparation and isolation necessary to carry out the test
- Functionality to be tested (for example alarm functions, individual signals, voting, response to specified fault conditions, such as power failure)
- Tools and equipment needed in relation to the test
- Restoration of the item, to ensure that it is properly put back into operation

# Impact of Proof Test for Production/Operation

Many safety functions will, when executed, stop the production, either directly by closing valves, or indirectly by isolating power to equipment.

- Testing of input elements (sensor), including its tie-in to the logic solver, may be carried out without disturbing the operation, as long as redundant input elements are available, or compensating measures are implemented.
- Testing of final elements (valves, breakers) is more challenging, as the complete functionality may interact directly with the operation
- Temporary stops of production may cause problems, both operational and also safety-wise

It is often a motivation to extend intervals between proof tests to avoid these operational challenges, as long as the safety is not compromised.

# Imperfect Proof Test

There are many reasons why a proof test is not full (or perfect).

- The test procedure may be deficient, or the test tool inadequate, leaving failures unrevealed.
- It is not safe or practical to test under the same conditions as demands. Who would like to test fire detectors on-board an offshore facility by initiating a fire?
- Faults may be introduced in a proof test, due to the stresses involved, but also due to errors made while executing the test, the repair, or in the restoration.

The imperfectness of a proof test may be modeled by the *proof test coverage*.

# Proof Test Coverage

☞ Proof test coverage (PTC): The conditional probability that a DU fault will be revealed in a proof test, given that the fault is present when initiating the proof test.

Some attributes of PTC:

- The PTC will be from 0-100%.
- A full (perfect) proof test has a PTC of 100%
- An imperfect proof test will have a PTC < 100%

The manufacturers may suggest a PTC of their equipment, but this value may need to be verified against the actual test conditions.

# Mean Test Time and Mean Repair Time

Mean test time (MTT):

- The mean time (spent) to perform the proof test. It covers the time from where the item is unable to carry out its function due to the test, and to the point in time it has been put into operation again.

Mean repair time (MRT):

- The mean time (required) to repair a failure found during a proof test. It covers the time from where the fault was revealed and until the item has been repaired and restored to a functioning state.

# Function Test

- The terms “function test” and “functional test” are often used with the same meaning as a proof test
- Yet, some make a point that a function test can in some cases be a test of the overall functionality of the SIF, and that the state of each redundant channel is not confirmed..

## Example

In the oil and gas industry, the same shutdown valve may get a signal from both the emergency shutdown system (ESD) and the process shutdown system (PSD) via separate solenoid valves. It is not always straight forward to determine if both solenoid valves responded, or just one of them. Sometimes, a delay is implemented in the PSD logic to separate the signals, but this is not always a welcomed solution.

# Partial Proof Test

☞ Partial proof test: A carefully planned periodic test, which is designed to reveal some specific DU faults without any significant disturbance of the EUC.

In relation to this type of test, we may introduce

- Partial proof test coverage, which is the percentage (%) of DU faults that can be revealed by a partial proof test.
- Partial proof test interval, which is the planned time between partial proof tests.

# Imperfect Versus Partial Proof Test

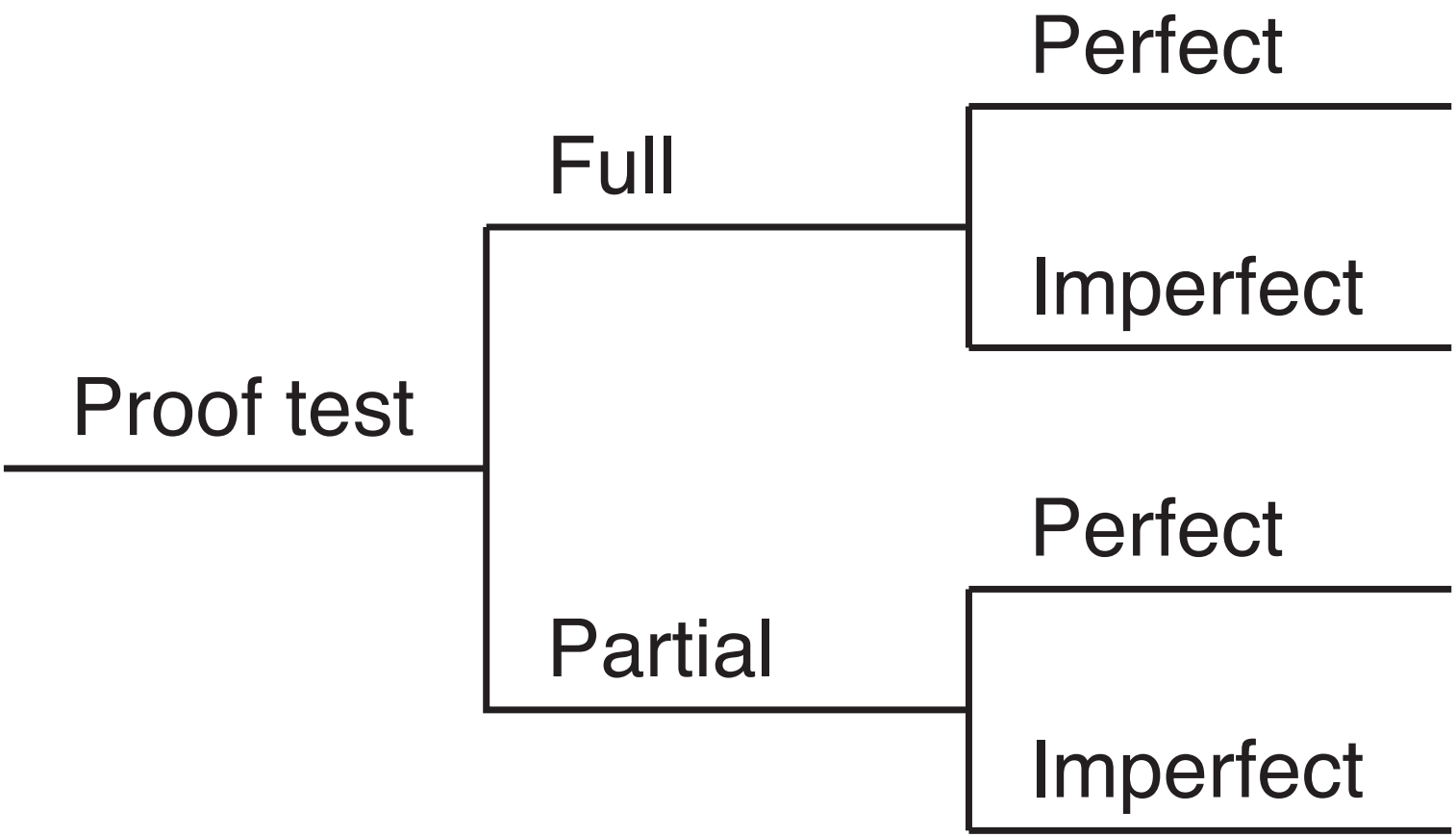
In the textbook, it is made a distinction in the meaning of an imperfect proof test and a partial proof test:

- An imperfect proof test relates impact of different conditions during a real demand and the test. These inadequacies and differences may desired or undesired.

- A partial proof test relates to the planned scope of the test. A partial test is designed to reveal certain failure modes, often with the aim to avoid disturbance of operation of production while the test is ongoing.

The tests are discussed in more detail in the following.

# Imperfect versus partial proof test



# Diagnostic Tests

A certain fraction of dangerous and safe failures may be detected by diagnostic tests.

☞ Diagnostic test: An automatic partial test that uses built-in self-test features to detect faults.

In response to detected safe or dangerous fault (DD), the item or system may either (or both):

- Raise an alarm in the control room, to notify operators about the fault and the need for corrective actions
- Initiate an immediate action to bring the EUC to a safe state

# Diagnostic Test Coverage

A certain fraction of dangerous and safe failures is often defined as diagnostic coverage (DC). Here, we place the focus on the DC of dangerous failures, $DC_D$.

☞ $DC_D$: The conditional probability that a dangerous fault is detected by the diagnostic test, given that a dangerous (D) fault is present when the diagnostic test is initiated.

The $DC_D$ may be calculated as:

$$CD_D = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DU} + \lambda_{DD}}$$

# DC categories

IEC 61508-2 classifies DC into four categories:

| Category | DC interval |
|---|---|
| 1 | 0%-60% |
| 2 | 60%-90% |
| 3 | 90%-99% |
| 4 | $\geq$ 99% |

# Related Terms

In relation to diagnostic tests, it is useful to introduce the following terms:

- Diagnostic test frequency, which is the regular interval of executing the diagnostic test.
  - Diagnostic tests may run more or less frequently, and IEC 61508 specifies that the detection plus restoration must be less than the process safety time to be credited in e.g., the calculation of the safe failure fraction (SFF)
  - An indication what is regarded as a suitable diagnostic test interval is indicated in relation to the methodology for determining the beta factor in IEC 61508-6. Here, the credit of diagnostic test is reduced if the diagnostic test interval is greater than 2 days, and increased if it is less than 2 hours
- Mean time to restoration (MTTR), which is the time to detect the fault plus the time needed to repair and fully restore the item to a functioning state.

# Staggered Tests

It is often assumed that redundant channels are tested simultaneously. In practice, the test is often sequential, but the time between each test is negligible.

An alternative testing strategy to simultaneous testing of redundant channels, is *staggered testing*

☞ Staggered test: A test where where two redundant channels are tested with the same proof test interval, but at different point in time.

- The main purpose of staggered testing is to reduce dependency due to the test itself
- Some find staggered testing to be of more academic interest than a practical testing strategy

# Pros and Cons of Testing Strategies

| Test method | Pros | Cons |
|---|---|---|
| Simultaneous test | Time efficient, as resources have already been allocated | Unprotected while the test is ongoing |
| Sequential test | Partial protection | More time consuming |
| Staggered test | Partial protection. Improved reliability (in theory, due to reduced dependency from the test itself) | More time consuming, and difficult to manage with respect to planning and scheduling |

# Classification of Tests

Manual versus automatic tests:

- Proof tests (full, partial, and staggered) are often manual or manually initiated
- Diagnostic tests are usually automatic

Online versus offline tests:

- Diagnostic tests are often online
- Proof tests may be online or offline tests