SINTEF REPORT

SINTEF Technology and Society
Safety and Reliability

Address: NO-7465 Trondheim, NORWAY
Location: S P Andersens veg 5 NO-7031 Trondheim
Telephone: +47 73 59 27 56
Fax: +47 73 59 28 96

Enterprise No.: NO 948 007 029 MVA

TITLE

Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase

AUTHOR(S)

Stein Hauge, Mary Ann Lundteigen

CLIENT(S)

PDS - multiclient

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
SINTEF A8788	Unrestricted	Håkon S. Mathisen, Kongsberg Maritime	
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
	978-82-14-04601-4	504091.12	38
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
PDS Report-SIS_follow_up_guideline_final_v01		Stein Hauge	Tor Onshus
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
	2008-12-01	Lars Bodsberg, Research Director	

ABSTRACT

This report includes guidelines for follow-up of Safety Instrumented Systems in the operating phase. The following main aspects are covered:

- A description of relevant SIS follow-up activities
- Planning and execution of these activities
- Establishing performance indicators and target values
- Failure reporting and classification
- Calculating updated failure rates
- Procedure for updating the length of the test intervals

The report summarises results from one of the activities of the PDS-BIP project "*Management and follow-up of SIS integrity*". This user initiated research project is sponsored by the Norwegian Research Council and the PDS forum participants.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Safety	Sikkerhet
GROUP 2	Operation	Drift
SELECTED BY AUTHOR	SIS follow-up	Oppfølging av SIS
	IEC 61508 / 61511	IEC 61508 / 61511

Foreword

The present report is the first revision of PDS[1] provided guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase. As more operational experience becomes available, the guideline may be updated.

The report has been prepared as part of the user initiated research project "*Management and follow-up of SIS integrity*". This project is sponsored by the Norwegian Research Council and the PDS forum participants. The work has mainly been carried out by SINTEF and does not necessarily express the view of all the PDS forum participants.

PDS Forum Participants in 2008

Oil Companies/Operators

- A/S Norske Shell
- BP Norge AS
- ConocoPhillips Norge
- Eni Norge AS
- Norsk Hydro ASA
- Talisman Energy Norge
- Teekay Petrojarl ASA
- StatoilHydro ASA
- TOTAL E&P NORGE AS

Control and Safety System Vendors

- ABB AS
- FMC Kongsberg Subsea AS
- Honeywell AS
- Kongsberg Maritime AS
- Bjørge Safety Systems AS
- Siemens AS
- Simtronics ASA

Engineering Companies and Consultants

- Aker Kværner Engineering & Technology
- Det Norske Veritas AS
- Lilleaker Consulting AS
- NEMKO AS
- Safetec Nordic AS
- Scandpower AS

Governmental bodies

- The Directorate for Civil Protection and Emergency Planning (Observer)
- The Norwegian Maritime Directorate (Observer)
- The Petroleum Safety Authority Norway (Observer)

[1] PDS stands for reliability of computer-based systems, and the PDS forum is a Norwegian initiative to gather industry and research institutes that work with reliability of SIS. For more information about PDS and the PDS forum please refer to: www.sintef.no/pds

TABLE OF CONTENTS

1 Introduction

1.1 Objective

The objective of this guideline is to describe work processes, activities and methods considered appropriate to ensure that the safety integrity level (SIL) of the safety instrumented systems (SIS) is maintained throughout the operational lifetime of the given installation. The main application area is the oil and gas industry, but the guideline may be relevant also for other industry sectors.

The main intention is to describe a practical approach towards implementing IEC 61508 / IEC 61511 in the operational phase of an installation, and to provide specific guidance on areas such as:

- relevant SIS follow-up activities
- planning and execution of these activities
- establishing performance indicators and target values
- failure reporting and classification
- how to calculate updated failure rates
- procedure for updating the length of the test intervals

The focus of this guideline is on the operational phase of an oil and gas installation. However, since premises for operation are introduced during preceding phases, some activities and documents relevant for design will also be described.

1.2 Abbreviations

Below is a list of abbreviations applied in this guideline:

ALARP	-	As Low as Reasonably Practical
ASR	-	Automatic Shutdown Report
BDV	-	Blowdown Valve
CCPS	-	Center for Chemical Process Safety
ESD	-	Emergency Shutdown (system)
F&G	-	Fire & Gas (system)
FMEA	-	Failure Mode and Effect Analysis
FMECA	-	Failure Mode, Effect and Criticality Analysis
FMEDA	-	Failure Mode, Effect and Diagnostic Analysis
FSA	-	Functional Safety Assessment
FF	-	Failure Fraction
HAZOP	-	Hazard and Operability study
IMS	-	Information Management System
MFS	-	Management of Functional Change
MoC	-	Management of Change
MTTF	-	Mean Time to Failure
O&M	-	Operation and Maintenance
PFD	-	Probability of Failure on Demand
P&ID	-	Process and Instrument Diagram

PSA	-	Petroleum Safety Authority (Norway)
SAR	-	Safety Analysis Report
SAS	-	Safety and Automation System
SIL	-	Safety Integrity Level
SIF	-	Safety Instrumented Function
SIS	-	Safety Instrumented System
SRS	-	Safety Requirement Specification

For a comprehensive list of definitions of relevant terms, reference is also made to ISO 14224 (2006) and ISO 20815 (2008).

2 Outline of SIS follow-up activities

The main activities associated with SIS/SIF in the operational phase are (IEC 1998; IEC 2003; OLF 2004; CCPS 2007):

- Operation
- Maintenance
- Monitoring
- Management of change

Key aspects of these activities are to
1. Detect, correct, and avoid introducing failures
2. Verify that assumptions, e.g., on operating and environmental conditions, made during design are still valid
3. Collect data to verify if the SIS meets the functional and safety integrity requirements, and
4. Take corrective actions if the actual performance deviates from the specified performance.

The relationships between these activities are shown in Figure 1.

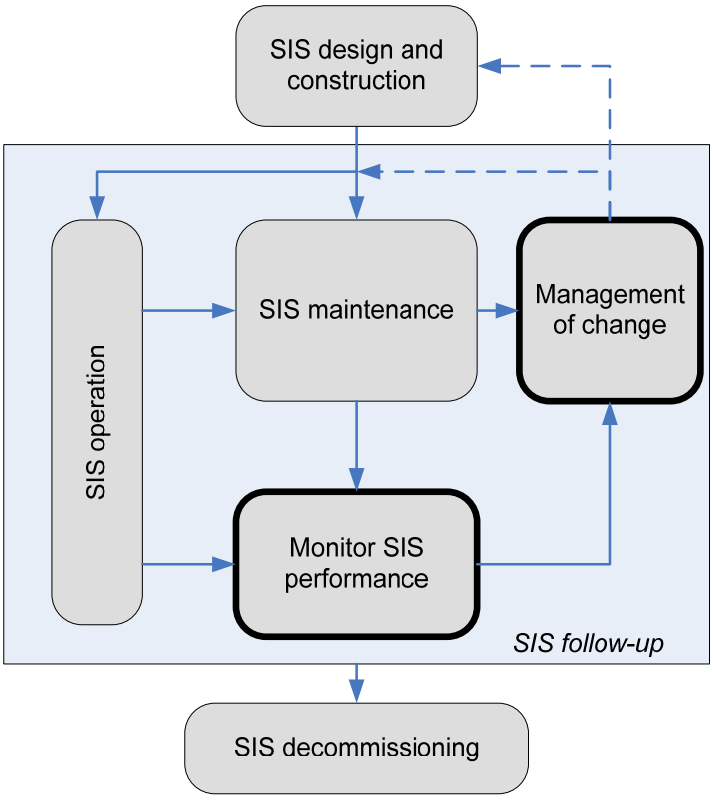

Figure 1 Main elements of SIS follow-up

SIS operation includes normal interaction with the SIS during operation; i.e. start-up and shutdown, execution of scheduled inspections, recording of identified failures, initiation of maintenance requests, implementation of compensating measures if the SIS is degraded or unavailable and setting, resetting and status tracking of bypasses. A bypass is an action taken to override, defeat, disable, or inhibit a SIF (CCPS 2007) and may be necessary to avoid process disturbances e.g. during testing.

SIS maintenance includes inspections, repair and overhaul, replacements and functional testing. Each activity may be split into preparation, execution, restoration, and failure recording. Maintenance may be initiated upon equipment failures (corrective maintenance), scheduled on a regular basis according to calendar time or operating hours (preventive maintenance), or initiated upon request from a condition monitoring system (condition based maintenance).

Monitoring includes establishment of performance indicators, performance indicator targets, and analysis of collected data to verify if the performance targets are met. The performance indicators must in some manner be related to the defined safety integrity level (SIL) for the safety instrumented functions (SIF).

Management of change addresses the follow-up of performance deviations and modification requests. For performance deviations, management of change means to analyse the underlying causes and make recommendations for how to proceed. For modification requests, management of change means to perform impact analysis, and determine if the modifications should be implemented, and if so, how the SIS is affected. Some performance deviations and modifications requests may be solved without having to modify the SIS hardware or software. Improving procedures, introducing more frequent testing and training of personnel are three such examples.

If modifications of the SIS hardware or software are necessary, IEC 61508 and IEC 61511 require a return to the appropriate design phase. In some cases, this means to go back to the hazards and risk analysis, and potentially specify new functional or safety integrity requirements. In other cases, it is sufficient to enter the detail design phase. Software modifications should always be treated as a SIS modification (CCPS 2007), and the implementation should follow the software development requirements in IEC 61508 (part 3) or IEC 61511 (section 12).

3 SIS documentation and premises for operation

3.1 Typical governing documents and document relationships

There will be several (hierarchical) layers of documentation relevant for the design and operation of safety instrumented systems on an oil and gas installation. For installations on the Norwegian continental shelf this will typically include:

- ***Joint regulations (Petroleum Safety Authority):***
  - Framework HSE: §9 Principles relating to risk reduction
  - Management: §1 Risk reduction, §2 Barriers
  - Facilities: §7 Safety functions
  - Activities: §44 Maintenance programme

- ***IEC61508:*** *"Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems"*

- ***IEC61511: "****Functional safety instrumented systems for the process industry sector"*

- ***OLF-070:*** *"Guidelines for the Application of IEC61508 and IEC61511 in the petroleum activities on the continental shelf"*

- ***Norsok standards:***
  - *NORSOK S-001 Technical safety*: The standard supplements the requirements in ISO 13702.
  - *NORSOK P-001 Process design*: The standard makes reference to the API RP 14C.
  - *NORSOK I-001 Field instrumentation*: The standard provides requirements for the selection of field sensors, hook-up details and documentation requirements.
  - *NORSOK I-002 Safety and automation systems (SAS)*
  - *NORSOK Z-016 Regularity management and reliability technology*: Has been further developed as a separate ISO standard (ISO 20815, 2008)

- ***General company governing documents:***
  - Company management philosophies
  - Company operation and maintenance philosophies
  - Company modification and MoC philosophies
  - Company guidelines for implementation and follow-up of SIS
  - Company performance standards and acceptance criteria

- ***Project/installation specific SIS documentation***

It should be noted that PSA refers to the IEC 61508 as a basis for SIS design and follow-up, and suggests the OLF 070 as one (out of possibly several) means to achieve compliance with this standard. The OLF 070 covers requirements from the IEC 61508 as well as the process sector specific standard IEC 61511.

Figure 1 gives a schematic overview of how the governing documents influence the project or plant specific documentation. As indicated in the figure, requirements to be followed up during SIS operation will result from regulations and standards, from general company governing documents as well as plant specific requirements laid down during design.

Plant specific requirements include assumptions and prerequisites stated in different engineering documentation. It is therefore paramount that all these premises are transferred to operations in a consistent and complete manner. This is further discussed in the next section.

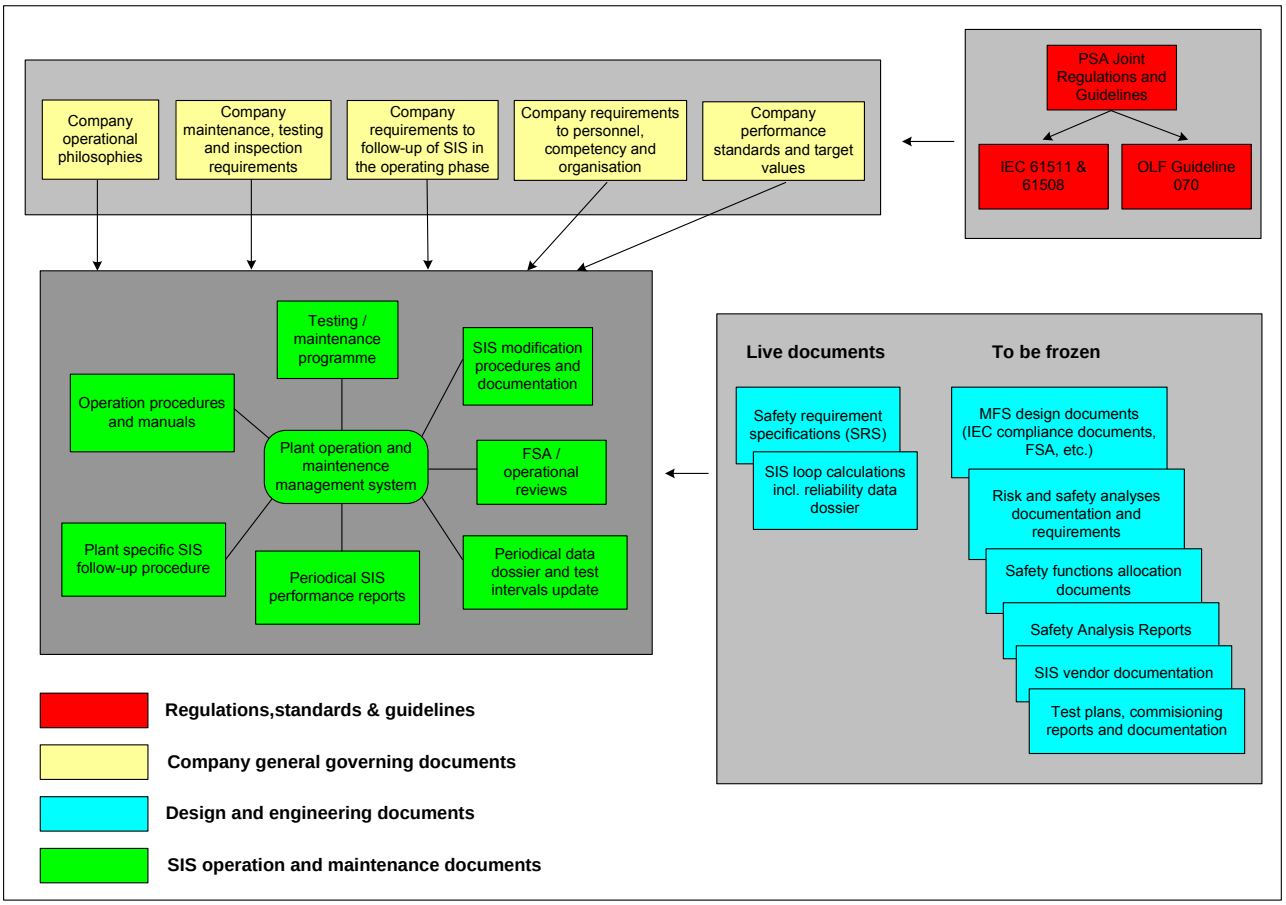

Figure 2 Possible document structure

3.2 Important premises from design

All SIS related requirements, assumptions and prerequisites from the design phase that may affect how the SIS is operated and maintained must be transferred to the applicable documents and responsible follow-up parties in a consistent and complete manner.

Below, some relevant documents are listed (ref. figure 1 above) together with a discussion of typical requirements and assumptions that can be found in these documents. An important activity will be to verify consistency between the different premises (and documents) from design in order to ensure that the "correct" requirements are being passed on to operations.

Hazards and risk analyses;
The main hazards and risk analysis document from the engineering phases will be the overall *Quantitative Risk Analysis (QRA)* for the plant / installation, the purpose of which is to assess the level of risk to people (and sometimes assets) from the planned operation of the installation. The QRA is normally initiated in the concept phase and updated throughout design (and also during operations). Although on a fairly overall level, the QRA will nevertheless include a number of assumptions related to the SIS which we may refer to as SIS performance requirements. Such assumptions may be:

- Reliability targets (PFD figures) for instrumented safety functions such as ESD, blowdown, F&G, ignition source isolation, firewater and if relevant ballast system functions and drilling BOP functions.
- Response times like e.g., signal transmission times for detectors/logic and response-/closure times for valves
- Criteria for accidental loads which the SIS shall withstand (e.g. explosion and fire loads – typically given in the Design Accidental Load Specification)
- Listing of critical ESVs with particular requirements concerning internal leakage rates
- Other assumptions that are made during the hazards and risk analysis which require particular SIS follow-up in the operational phase

Reliability targets, required response times and accidental loads are all parameters to be included in the SRS and are as such covered herein. It is necessary to ensure that there is consistency between assumptions made in the risk analysis and what is stated in the SRS. In case of discrepancies, these must be clarified and the need for updating the risk analysis, the SRS or both, must be considered.

Another important analysis activity in the engineering phase is the *HAZOP* studies. In these studies a number of assumptions and recommendations are made. Mostly these relate to process and SIS design (new sensor required, change set point, relocate instrument, etc.) and are implemented as mark ups on the P&IDs during design. However, the HAZOP studies also provide recommendations and requirements for operation, some of which may be related to SIS operation (e.g. bypasses during start-up, operator response upon a process deviation, etc.), and it is important to ensure that these recommendations are implemented in the relevant operational procedures.

Safety function allocation documentation;
The number and type of assumptions from the SIL allocation process will depend on the method used for establishing the SIL requirements. For example, when using the standard OLF 070 requirements directly, it is necessary to ensure that their underlying assumptions are implemented and followed up. These assumptions are mostly related to design aspects such as e.g. diagnostic coverage, fail-safe design and loop monitoring, but OLF 070 also includes assumptions related to failure rates, test intervals and complete safety loop testing which needs to be verified during operation.

When using risk graph and/or LOPA type of techniques for establishing the SIL requirements, such analyses will typically include a number of assumptions relevant for operational follow up. One assumption may be manual ESD activation by operators, another that a given process situation requires response from a number of systems, for example the process control system and a SIS. Project experiences and case studies have shown that LOPA on average tends to give somewhat lower SIL requirements than e.g. OLF 070, basically because alternative risk reducing measure and protection layers are taken into account when establishing the requirements. When credit is taken for alternative protection systems, it must be ensured that these systems' performance are in line with the assumptions and further that the systems are sufficiently independent. I.e. the premises for including the systems as separate protection layers must be fulfilled also during operation (e.g. by avoiding frequent bypasses and inhibits).

Safety Requirements Specifications;
The SRS contains the functional safety and safety integrity requirements for all the identified safety instrumented functions. The functional safety requirements describe what and how the SIS shall perform upon a process demand and under specified failure events. The safety integrity

requirements shall describe the reliability target and SIL level of each safety instrumented function.

OLF 070 recommends that the SRS is updated throughout the detail design. The SRS may, for example, be updated to highlight assumptions and requirements that result from subsequent lifecycle phases (e.g. from SAR reports), and which may affect SIS performance or strategies for operation and maintenance. If the SRS is updated, it is important to ensure that updated safety integrity requirements are verified by updating the relevant hazard and risk analyses. Updating of the SRS during the operational phase should be restricted to clarifications. Any modifications to the functional safety or safety integrity requirements require return to the appropriate lifecycle phases, for example the hazards and risk analysis.

Safety Analysis Reports (SAR) – compliance and verification reports;
The SAR is a report that documents that the safety instrumented functions comply with the specified SIL (and equipment reliability targets if these are given in addition). Safety Analysis Reports and other reports for estimation and verification of SIS integrity will include a large number of underlying assumptions. It is important that all such assumptions are identified and properly highlighted in the SAR (e.g. as a separate chapter), and classified according to how they affect operational and environmental conditions, operating procedures, maintenance procedures (including functional testing), and SIS performance. This may typically include assumptions concerning:

- functional test intervals and how the SIFs are to be tested;
- maximum allowable repair times for redundant equipment;
- demand rates;
- functions that are not to be inhibited or overridden (or only for limited time periods);
- manual operator intervention or activation of SIS functions;
- how an operational activity shall be carried out, e.g. the opening sequence for valves or the use of written checklists;
- response times, e.g. that a PAS function is sufficiently quick to prevent an overpressure situation.

It is sometimes seen that assumptions made in the SARs are in conflict with the requirements given in the SRS documents and/or the input given to the maintenance systems (e.g. the length of the test intervals in SAP). Again the importance of ensuring consistency between the various assumptions, requirements and documents should therefore be stressed.

Supplier SIL compliance documentation
For suppliers responsible for only a single element or part of a safety function, it is generally not considered necessary to prepare a complete SAR. Instead, they should submit a "SIL compliance document" that includes the following:

- *Documented compliance;* Reference to any verification of compliance to the IEC 61508 and/or IEC 61511 requirements regarding documented prior use as well as any 3rd party verifications of hardware and software design principles, applied tools, design and development procedures and work processes.
- *Failure mode description;* Description of the failure modes, and their related causes, preferably documented through a failure mode, effect, and consequence analysis (FMECA).
- *Failure classification;* A proposed classification of safe and dangerous failures, taking into account the particular application (e.g. the criticality of a failure of a pressure transmitter

that provides 20-4 mA signal will depend on what to define as the safe state for a specific application).

- *Failure data;* Failure rate estimates (for each failure mode) including estimated SFF, with reference to sources and main assumptions
- *Additional reliability parameters;* Other important reliability parameters such as diagnostic coverage factor and assumed functional test coverage together with a specification of the assumptions under which the figures are derived.
- *Operation and maintenance;* Requirements and recommendations related to operation, maintenance and functional testing.
- *Conditions of use;* Constraints related to response times, closure times and other parameters relevant for the SIS performance. In addition, a short assessment from the supplier on important constraints that may apply due to the specific operating and environmental conditions.

It is important to check whether the vendor assumptions and recommendations are in line with requirements in the SRS and in the maintenance systems, and upon deviations to clarify underlying causes and whether these are acceptable.

The SIL compliance document for an individual SIS component, for example a particular type of pressure transmitters or a specific valve type, may be included as attachments to the overall SAR analysis of the SIF. Any classification of safe and dangerous failures proposed by a SIS supplier, should be verified, and if necessary, modified in the SAR.

4 Planning and execution of activities

4.1 General

This chapter describes how to prepare for and execute SIS follow-up in the operation phase. Key aspects of SIS follow up are to monitor and maintain adequate SIS performance throughout operation. The required SIS performance is given by the functional safety and safety integrity requirements. The preparation starts in the design phase, while the execution covers the phases of operation, maintenance, and modifications.

4.2 Preparing for SIS follow-up

Parallel to the SIS design and implementation, it is necessary to start preparing for SIS follow-up (i.e. Phase 6 of the IEC 61508 lifecycle). The preparations may include (but are not limited to):

- Nomination of persons / department to be responsible for SIS follow-up during operation
- Identification of design related documentation that must be kept updated during operation of the SIS.
- Development of overall procedures for SIS follow-up that describes activities, responsibilities and methods related to SIS operation, maintenance, performance monitoring, and modifications, see Figure 3.
- Identification of competence and training needs, see section 4.6.

4.3 SIS follow-up procedure

A plant specific SIS follow-up procedure should be developed. The SIS follow-up procedure may include the following main sections:

- Description of the main SIS follow-up activities, as illustrated in Figure 3
- Roles and responsibilities
- Competence requirements
- Reference to all SIS follow-up related procedures

For each follow-up activity it must be clearly defined who is responsible and what persons or departments that should be involved or informed. Some activities may be executed on a regular basis, for example once every 3rd month or annually, while others may be performed in connection with certain events, like e.g. a SIS failure. In cases where one or more 3rd parties are involved in SIS follow-up, it is especially important to ensure proper allocation and implementation of responsibilities and work processes.

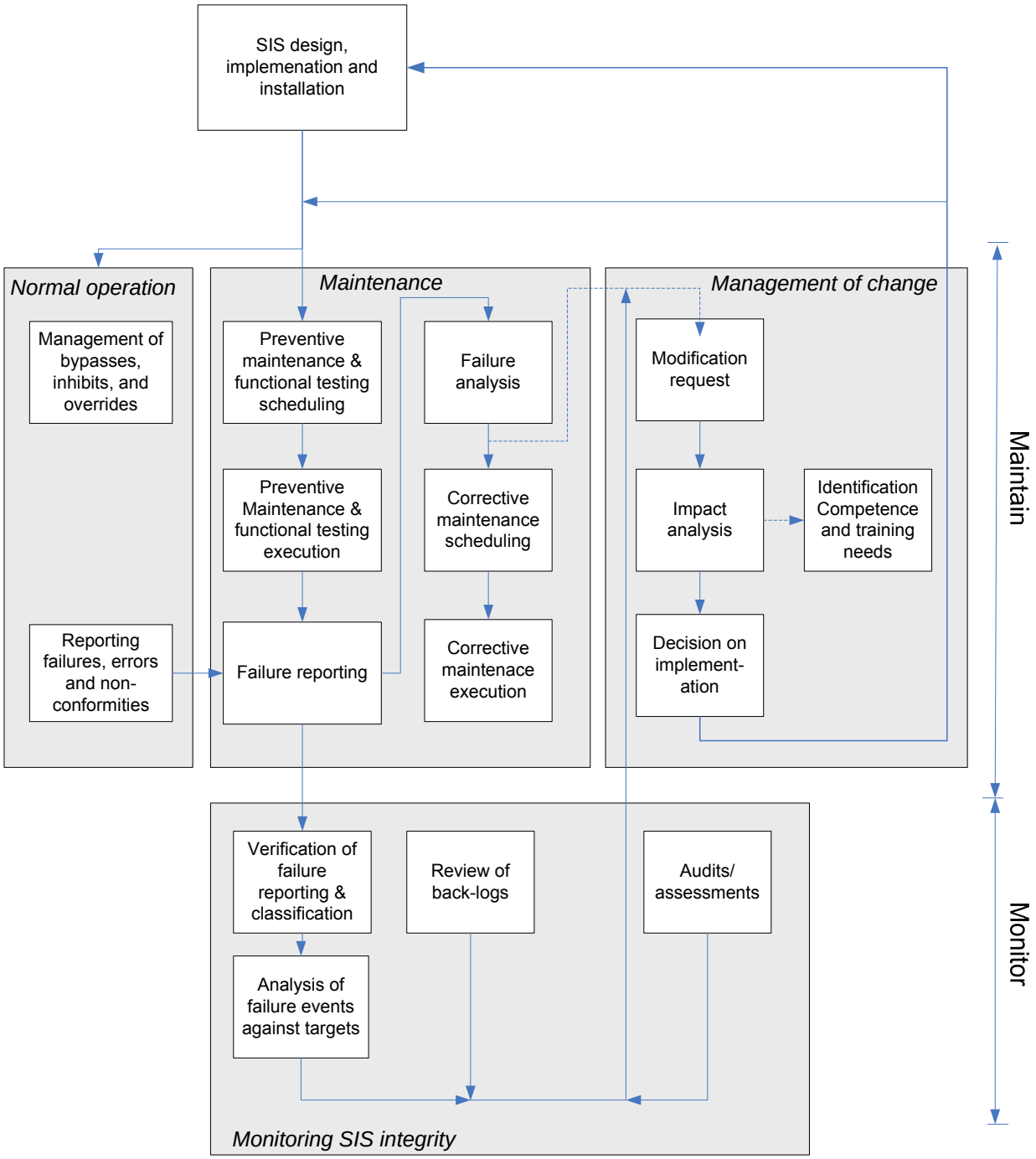

Figure 3 Illustration of SIS follow-up activities

A summary table describing relevant SIS follow-up activities is presented in Appendix A.

4.4 Activities to maintain integrity

In this section, some more details are provided on the SIS activities related to maintaining the SIS integrity.

4.4.1 Management of bypasses, inhibits, and overrides

Bypasses, inhibits, and overrides are sometimes necessary in relation with maintenance activities or start-up. However, the use of such means should be strictly controlled. One reason is that

systematic failures may be introduced due to improper setting or resetting. In addition, a hazardous situation may occur upon a process demand while the SIS is temporarily unavailable.

Procedures for use of bypasses, inhibits, and overrides should describe:

- Provisions for use
- The instructions needed for setting, suspension and verification of suspension
- Precautions that should be taken to avoid introducing systematic failures
- Logging of status on bypasses, inhibits, and overrides
- Routines for how the status on bypasses, inhibits, and overrides are communicated from one shift to the next.

4.4.2 Response to SIS failures

Procedures must be established that describe necessary actions in the event of a SIS failure. The procedure must specify that:

- All failures are to be recorded;
- Compensating measures must be evaluated and implemented until the failure has been repaired;
- PSA activity regulations require dangerous detected failures to be corrected immediately. If repair for some reason is delayed, it is important to identify and implement compensating measures.

4.4.3 Recording and analysis of SIS failures

The SIS failures should be recorded through the maintenance system, and clearly allow for distinction between failures that are detected during normal operation, by diagnostic alarms, or during a function test or a real demand. The purpose of this distinction is to be able to classify safe and dangerous (detected and undetected) failures. Additional information should also be requested on the failure causes, to improve the subsequent failure analysis and repair actions. A procedure on how to classify failures, and what additional information to include on e.g., failure causes should be developed, and referenced or included in the relevant operation, maintenance and function testing procedures.

4.4.4 Regular inspection, maintenance and function testing

The SIS shall be regularly tested and inspected according to what is described in the SRS and laid down in the maintenance system. When the reliability of the SIS is estimated, it is often assumed that functional testing is perfect, i.e.:

1. All dangerous failures that are not detected during normal operation are revealed during a function test, and
2. The SIS components, if failed or found degraded, are restored to an as good as new condition.

These assumptions are however difficult to fully comply with in the operation phase, because:

- A function test may never be able to fully represent a real process demand. Testing with a real gas leakage, fire or overpressure would themselves create new hazardous situations.
- During a function test there is always a possibility that new failures are introduced due to e.g., incorrect calibration and incorrect restoration of tested equipment.

Consequently, in order to minimise these effects it is important that functional testing as good as possible resembles a real demand and that the entire safety function is included in the test. Often tests are performed on part of the function at a time (e.g. a pressure transmitter). In such case it is important that only the components that are actually included are credited as tested and further

that the components inhibited or omitted from the test are covered by separate testing programmes.

Further, it is important to define how maintenance is performed to maintain the "as good as new condition", and how to avoid introducing new failures during repair and restoration.

4.4.5 SIS Modifications

Handling of SIS modifications is sometimes referred to as *Management of Change* (MoC). A SIS modification may be changes to hardware, software, and/or procedures and work practises with a potential effect on the SIS' ability to perform as intended. A MoC procedure should address:

- Criteria for when a modification shall be initiated. Examples are deviations from specified (functional safety or safety integrity) performance, operation outside the operating and environmental conditions specified during SIS design (e.g. increased process temperature), high number of false alarms or diagnostic alarms that lead to stress on control room operators, expansions of the process plant, etc.;
- A method for analysing the impact of modifications, for the SIS, for other systems, and whether it affects the independence between protection layers. The impact analysis should identify new hazards that may arise from new firmware or new security threats;
- What type of documentation that must be updated as part of the modification(s), for example drawings, equipment description sheets, and operation and maintenance procedures;
- Which safety lifecycle phase to return to for implementation of the modification(s).
- What persons or departments that have the authority to approve SIS modifications, and what persons and departments that must be involved;
- Any new competence and training needs;

In addition access security procedures must be available to assure that only authorised personnel can access the SIS hardware and software and that only approved changes are made to the SIS.

4.5 Monitoring SIS performance

Monitoring the SIS performance involves:

- To compare the recorded SIS performance with the specified performance targets that are described in the SRS.
- To compare assumptions that are made during design with the conditions under which the SIS is operated and maintained.
- To assess how well procedures and work practises contribute to avoidance of and control with systematic failures.

Verification of design assumptions versus real operating conditions and avoidance and control of systematic failures may be incorporated in already existing verification and audit activities that the company performs for safety related systems, or can be performed as separate reviews, for example through functional safety assessment (FSA) performed in operation.

Practical follow-up of SIS performance and how to verify that SIL requirements are met during operation are further discussed in chapter 6.

4.6 Competency requirements

It is important that competence needs are specified for all SIS follow-up activities. Key issues important for *all* persons involved in SIS follow-up, are to:

- Understand the purpose and functional requirements of the SIS;
- Understand the hazards against which the SIS is protecting;
- Be aware of operational and environmental constraints under which the SIS must operate;
- Be aware of what "as good as new" means for different SIS components, and what actions that must be taken to restore the equipment to this condition;
- Be familiar with procedures for failure recording and classification.

For personnel that are involved with *SIS monitoring*, ref. chapter 2, it is important to have additional knowledge related to:

- Basic concepts used in reliability assessments, including failure classification, failure rates, probability of failure on demand (PFD) and common cause failures (CCFs);
- Basic principles for calculating the PFD from a reliability block diagram and techniques to analyse failure modes and effects (FMEA, FMECA and FMEDA);
- Governing rules and relevant standards, like e.g. Petroleum Safety Authority regulations, IEC 61508 / 61511 and the OLF 070 guideline;
- All SIS related documentation, i.e. the safety requirement specification, design documentation that must be kept updated, and operation and maintenance procedures including SIS related company specific procedures and guidelines;
- Conditions that apply for the SIS to remain (sufficiently) independent from other systems (protection layers).

5 Verification of SIL requirements during operation

This chapter goes into some more details on how to verify that the SIL requirements are being met during operation. In particular it is discussed how to establish target values and performance indicators for monitoring SIS performance, how to collect relevant follow-up parameters and how to verify that the integrity target values are being fulfilled.

5.1 Prerequisites

Prior to operation it is assumed that SIL requirements have been allocated to the instrumented safety functions and that appropriate test intervals have been set so as to fulfil the given SIL requirements.

It is also assumed that for each group of comparable components, such as ESD valves or gas detectors, the number of (tagged) items on the plant is known.

5.2 Establishing performance indicators and target values

The purpose of this section is to describe a basis for establishing safety integrity performance indicators and target values against which these indicators can be measured.

5.2.1 Some definitions

Below some of the terms used in this section is defined.

Integrity performance indicator: measure of the *experienced* safety integrity of a SIS component, such as e.g. a gas detector or an ESD valve. Typically, this may be the number of experienced safety critical failures for a further defined population of components.

Note: A *safety critical failure* is a failure that prevents the component to perform its safety function, i.e. to bring the process to a predefined safe state. E.g. for a blowdown valve a safety critical failure may be defined as “the valve does not open on signal within specified time”.

Integrity target value: measure of the maximum *acceptable* number of safety critical failures for a defined population of components. For example this may be the acceptable failure fraction times the number of individuals in the population.

Failure fraction (FF): the number of failures, x, divided by the corresponding number of tests and/or activations, n

5.2.2 Basis for selected indicators and target values

Basically, our main intention is to verify that the *experienced* (or measured) safety integrity of the SIS is acceptable as compared to the premises laid down in the design of the installation, here represented by the SIL requirements.

In order to do this, we need to establish a *connection* between the assumptions and requirements from design and the integrity performance indicators that are to be followed up during operation.

Registration and counting of safety critical failures, or Dangerous Undetected (DU) failures in IEC terminology, is an already established practice for many operators. It is therefore attractive to use the number of DU failures as an *integrity performance indicator*. The associated *integrity*

target value can be calculated from the generic DU failure rate, since in design this parameter is used to show that the *predicted* PFD meets the *required* PFD. For a population of n identical components, the expected number of DU failures during a time period t can be approximated by[2]:

$$E(X) = n \cdot t \cdot \lambda_{DU} = t_n \cdot \lambda_{DU}$$

Here, E(X) is the expected number of DU failures, λ_{DU} the assumed failure rate from design, and t_n is the total (accumulated) time in operation. Note that we here assume that each of the n components must be activated at least once during the observation period t.

Hence, by recording the number of DU failures for the n components during the same observation time t, and comparing this number with E(X), we get an indication of how "good" the components perform. As seen the E(X) is directly linked to the λ_{DU} from design which has been used to verify that the SIL requirements are fulfilled. Therefore, if the number of experienced DU failures is below E(X), we will assume that the actual failure rate (experienced so far) is lower than the failure rate that was assumed in the design phase. Also note that the E(X) expression is here independent of the number of activations or tests. This is advantageous since for a sample of components with different testing/activation frequency a common target values can be applied.

Consequently, we propose to use E(X) as the integrity target value and number of experienced DU failures as the integrity performance indicator.

Some Norwegian oil companies have used the *failure fraction (FF)* as a performance indicator for SIS related components. The FF is, for a given population and a given time period, defined as *the number of failures divided by the corresponding number of tests and/or activation,* and has an interpretation similar to the PFD. By nature, the FF will therefore depend on the length of the test interval; i.e., more failures are expected for components that are tested seldom than if they are tested more frequently. In practice, the oil companies have often used a fixed FF target for each group of similar components, without taking into account how often the components are tested. Furthermore, similar components may perform safety functions that have different SIL requirements, for example, some pressure transmitters may be used for process shutdown functions while others may be used for emergency shutdown functions. Finally, to estimate the FF, the exact number of activations for the entire population must be known. Keeping track of all such activations for an entire population of components is however often a practical challenge. Great care should therefore be taken if using the FF or PFD as performance indicators.

Example calculation

On a given plant there are 500 smoke detectors with an assumed failure rate from design of $\lambda_{DU} = 1.0 \cdot 10^{-6}$ per hour. During a period of one year the expected number of experienced failures for the sample of 500 smoke detectors will then be:

$$E(X) = n \cdot t \cdot \lambda_{DU} = 500 \cdot 8760 \text{ hours} \cdot 1.0 \cdot 10^{-6} / \text{hours} \approx 4$$

Hence the expected number of failures during one year of operation will be approximately 4, which can then be used as an annual target value for the smoke detector population. It should be

[2] It is here assumed that the failure rate λ_{DU} is exponentially distributed. Since DU failures are not revealed until an actual demand or a test, the expression for E(X) will be an approximation. We have disregarded the possibility of a component being unavailable for parts of the observation period (and thereby ignored the possibility of more than one failure within the observation period). However, given the high MTTFs of the equipment under consideration, the error margin of the approximated E(X) will be within 1-2%, which for practical purposes is sufficiently exact.

noted that when using an annual target value it is assumed that the detectors are tested at least once a year. If the smoke detectors are tested 2 times or 4 times per year, the same target value can be applied. However, if the detectors are tested only every second year, then a target value of 8 failures *per two years* in a sample of 500 flame detectors should apply.

5.2.3 Comparison with the integrity target values

For each group of comparable components the number of tagged items in the component group and the assumed failure rates from design are used to establish the integrity target values. An example of how this may appear for some selected equipment is given below.

Table 1 Example of performance target values for selected equipment

Description of equipment class	**No of tagged items**	**Target values** (max no of DU failures)	**Comments / notes**
ESD valves – ESV	98	2 per year	Based on an assumed λ_{DU} for ESVs of $2.9 \cdot 10^{-6}$ per hour Assumed proof test interval: 12 months
Blowdown valves - BDV	35	1 per year	Based on an average assumed λ_{DU} for BDVs of $2.9 \cdot 10^{-6}$ per hour Assumed proof test interval: 12 months
Circuit breakers – electrical isolation	150	2 per two year	Based on an average assumed λ_{DU} for circuit breakers of $0.6 \cdot 10^{-6}$ per hour Assumed proof test interval: 24 months
Gas detectors	636	6 per year	Average assumed λ_{DU} for gas detectors of $1.0 \cdot 10^{-6}$ per hour Assumed proof test interval: 12 months

The actual number of DU failures registered for a specified type of equipment (for example ESD valves or gas detectors) shall then be compared with the given target criteria. For the purpose of comparison, the following general guidelines may apply:

- If the number of registered failures is "*on target*" then the situation is considered acceptable but the possibility of removing the failure cause should anyhow be considered (ALARP principle).
- The ALARP principle also applies if the number of registered failures is *below the target* value, however the situation is acceptable and less frequent proof testing may in some cases be considered (see section 6.3)
- If experienced number of failures is above target, a failure cause analysis should be performed and compensating measures to reduce the number of future failures must be considered, including the need for more frequent proof testing (see section 6.3)

The latter case, i.e. more failures than expected has occurred, is of special importance. This indicates a situation where the failure rate assumed during design may be too optimistic, and as a consequence the SIL requirements may not be fulfilled.

5.3 Information sources – collection of SIS follow-up parameters

A major challenge related to SIS follow-up is the variety of sources from where the relevant parameters shall be collected. Information about SIS failures, demands and inhibits/overrides will be provided from different operation and maintenance activities and systems. Figure 4 shows *an example* of the most important SIS follow-up parameters and the sources from where information about these parameters will typically be collected.

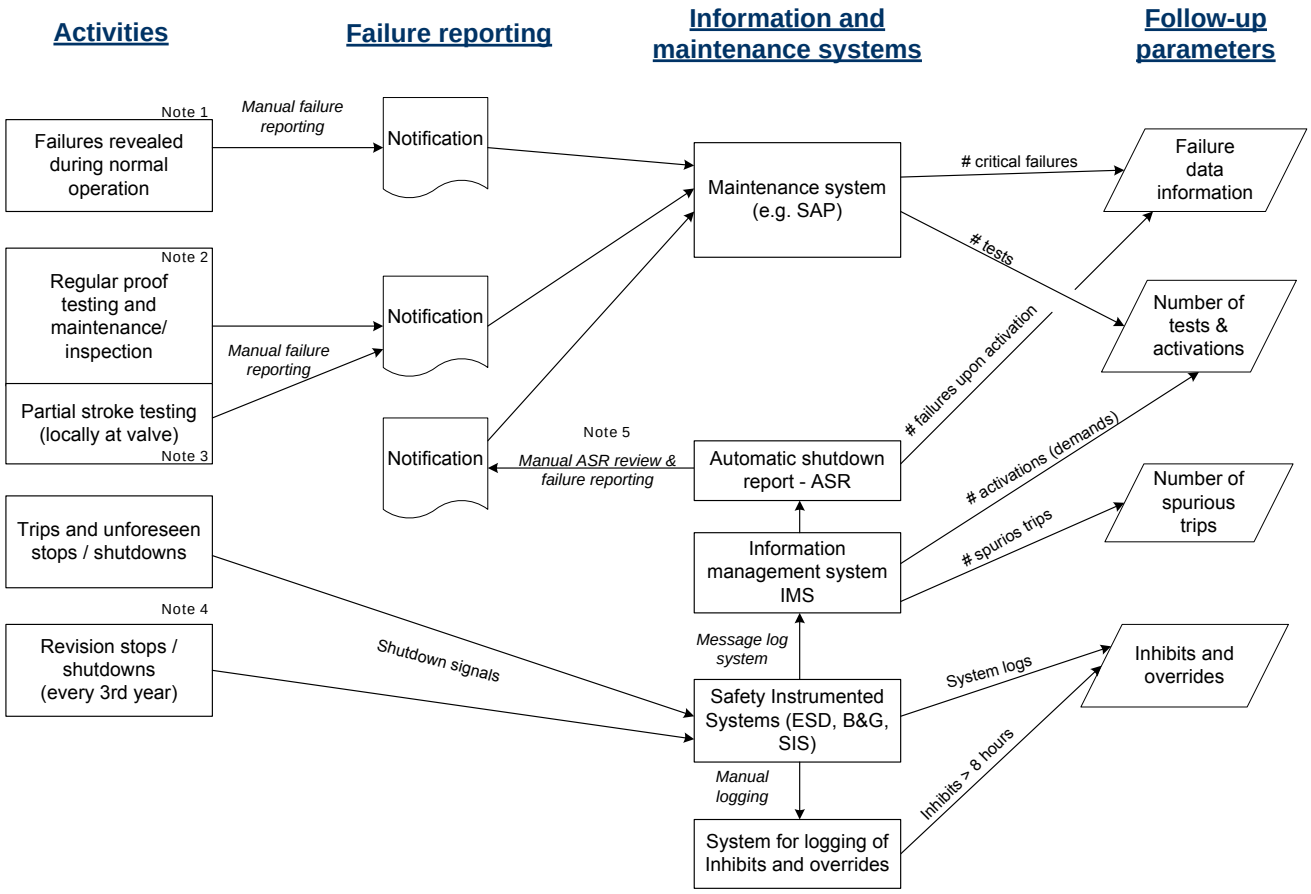

Figure 4 Information sources and information flow

Notes/comments to the figure:

1. A SIS failure may be revealed during normal operation, e.g. when a shutdown valve for some reason needs to be closed during operation, but is stuck. A notification will then be prepared in the maintenance system in case of a failure.
2. During functional testing of the SIS the results from the tests are registered, and a modification shall be prepared in case of a component failure.
3. Partial Stroke Testing (PST) may be performed regularly for selected valves such as ESD valves. If, during PST it is revealed that e.g. the valve will not leave its starting position, then a notification will be prepared.
4. When a planned (e.g. revision stops) and/or an unplanned shutdown occur, selected input elements (causes), logics and final elements (effects) are activated, thus creating events in the message log system. Typically if an Information Management System (IMS) is available, the events are imported into the IMS which again generates an automatic shutdown report (ASR) indicating which final elements have operated successfully or have failed to perform their intended function. Also, the IMS can be used to keep track of spurious trips as well as number of activations.
5. Normally the automatic shutdown report (ASR) only indicates whether a component has been successfully activated or not (e.g. if a valve has closed). Hence, the ASR report must normally be gone

through manually, reported failures must be investigated and a notification must be prepared in case of a critical failure.

It should be noted that the above illustration is just an example of possible information sources and how different SIS parameters may be collected. The actual system implementation on each specific plant will obviously determine the details.

5.4 Registration and classification of SIS failures

For the purpose of being able to follow-up and verify the SIL requirements it is paramount that critical SIS failures revealed during operation and maintenance are properly registered and classified.

All failures of SIS components discovered in the operational phase, e.g. during testing, during normal operation or upon a demand must therefore be registered by preparing a notification in the maintenance system.

It is essential that maintenance personnel performing failure reporting are properly trained and motivated in order to ensure high quality notifications. This will simplify later failure classification and makes it possible to verify whether SIS performance is in line with the target values. In particular it is important:

- To give an as detailed as possible description of the failure in the free text field in the maintenance system;
- To correctly specify the failure mode (e.g. a shutdown valve fails to close);
- To correctly specify the detection method for the failure (e.g. during functional testing, self-diagnostics, during normal operation, etc.);
- If possible specify the failure cause (e.g. corrosion, hydrate formation, human error, etc.).

For a comprehensive description of a standardised basis for collection of reliability and maintenance data, reference is made to ISO 14224 (2006).

6 Updating failure rates and test intervals based on operational experience

Based on plant operational experience with the SIS, updated failure rates that incorporates the new information should be estimated periodically, say *every third year.* This is especially important when a higher number of dangerous undetected (DU) failures than expected have been experienced since this indicates that the quantitative SIL requirements may not be fulfilled.

If SIL loop calculations are available from design, the updated failure rates can then be used as input to these models. In this manner it is possible to verify, on a safety function level, whether the SIL requirements are fulfilled during operation. For some of the equipment types which are few in number and/or have very low failure rates (such as e.g. logic solver), no or little failures can be expected during a three years period, or even during the lifetime of a plant. For such units, recalculating the failure rates may not be feasible or even desirable.

If operational experience proves that the equipment is significantly more or less reliable than what was assumed in the design phase, extending or reducing the length of the test interval may also be considered. Changing the functional test interval is however a major decision which needs to be substantiated by confident quantitative as well as qualitative arguments.

The purpose of this chapter is twofold:

1. To describe a ”preferred method” for update of the dangerous undetected failure rate λ_{DU} based on operational experience as well as a priori knowledge related to the failure rate from design

2. To describe a “preferred method” for update of the proof test interval for the component group under consideration

In addition to the methods described, a number of example calculations are given to illustrate their application.

This chapter includes some formulas and statistical details which may not attract the interest of all readers. Therefore an Excel spreadsheet model has been developed in order to simplify the calculations both for update of the failures rate as well as the test intervals.

6.1 Updating failure rates

6.1.1 Process for updating failure rates

The proposed procedure for updating the failure rates is illustrated below.

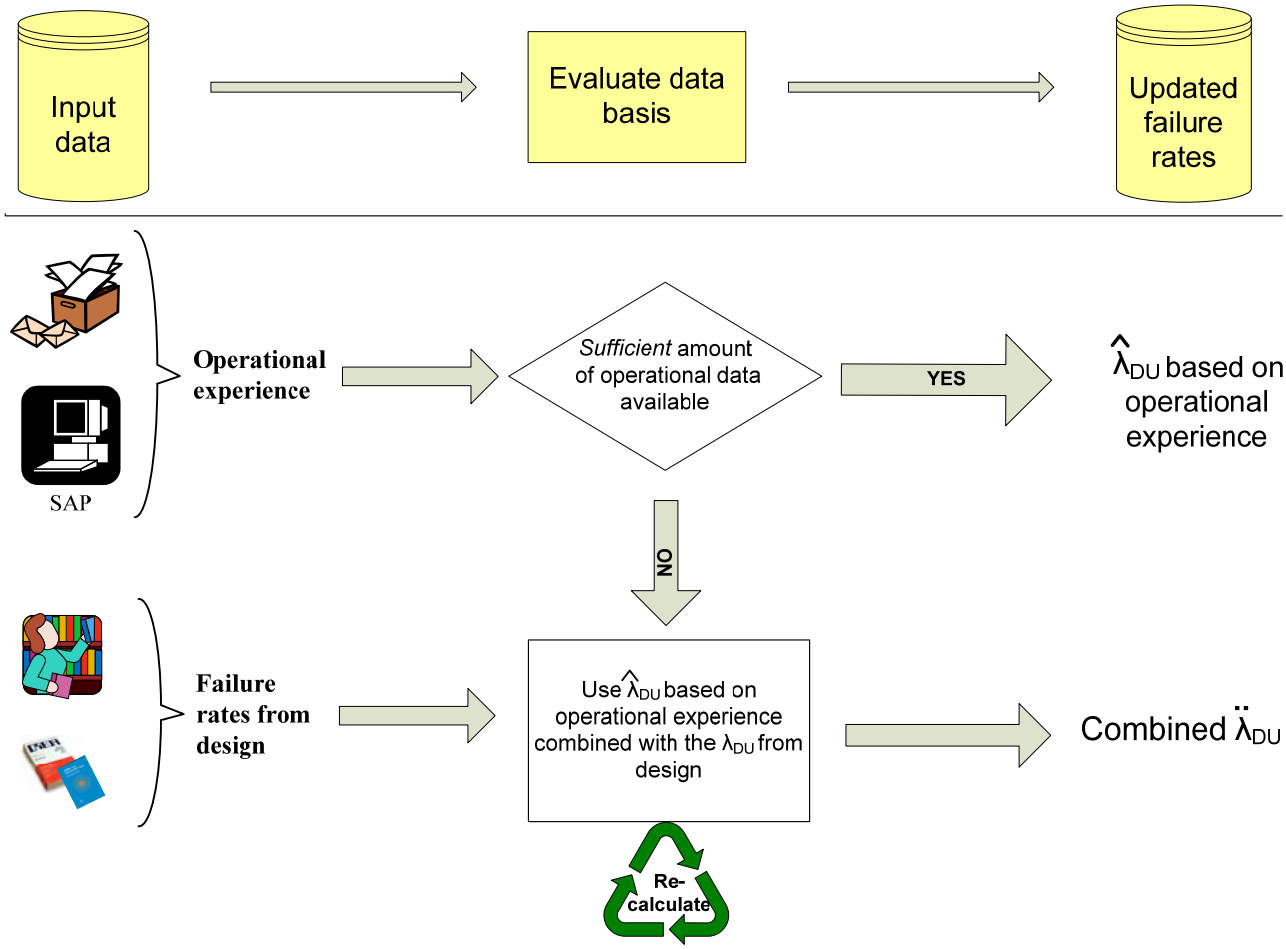

Figure 5 Process for updating the failure rate based on operational experience

If sufficient operational data is available (as further discussed in section 6.1.2) it will be possible to derive at an updated failure rate $\hat{\lambda}_{DU}$ with sufficient confidence. Hence, in this case it will not be (strictly) required to apply the original λ_{DU} from design when calculating the new updated failure rate.

If insufficient operational experience is available, as is often the case, it will be necessary to combine the (limited) operational data with the a priori estimate of the failure rate λ_{DU}. This in order to avoid that "coincidences" combined with limited aggregated time in operation makes the new failure rate estimates fluctuate (i.e. being too sensitive).

When using the original failure rate λ_{DU} from design it will be necessary to specify some kind of confidence (uncertainty) in the original failure rate estimate. This in order to decide how much weight shall be given to the original failure rate estimate as compared to the weight of the experienced failure rate. Alternatively, if the mentioned Excel program is being used, it will be possible to let the program select an "appropriate" value for the uncertainty. This may be relevant if the user only have an estimate of the mean λ_{DU} but no additional information on the uncertainty (as is often the case).

Based on this, several questions arise:

i. At which point is it acceptable to say that sufficient operational experience is available?

ii. How shall the uncertainty for the initial estimate be specified and what rules/limitations need to "lay implicit" when this is done by an average/standard user?

iii. What formula(s) shall be used to calculate the new updated $\hat{\lambda}_{DU}$ (or $\ddot{\lambda}_{DU}$) ?

iv. And what rules and formulas shall be applied in order to calculate the new updated test intervals?

6.1.2 What is sufficient operational experience?

A well known fact is that plant specific conditions in large influence the performance of the safety systems and hence the experienced failure rates. Therefore, there are good arguments for using mainly plant operational data whenever this is statistically justifiable.

For some equipment types like e.g. fire- and gas detectors there will be a significant amount of experience data available already after some years of operation due to the high number of installed units. E.g. for a plant with 500 smoke detectors, the aggregated operational time per year will be more than 4 million hours.

A possible "cut off point" for using only operational data, may be when the confidence in the $\hat{\lambda}_{DU}$ based solely on operational experience equals the confidence in the λ_{DU} from design, i.e.:

> *When the statistical confidence in $\hat{\lambda}_{DU}$ is comparable to the confidence in the design failure rate λ_{DU} then it is justifiable to apply only operational experience.*

So when/how will this typically occur?

Looking at some representative figures for SIS equipment (detectors, sensors and valves) from OREDA® we see that:

- Typically the upper 95% percentile in the confidence interval[3] for the critical failure modes will be in the order of 2-3 times the mean value

  We therefore state that for cases where the upper 95% percentile of the $\hat{\lambda}_{DU}$ based on operational experience is approximately 3 times the mean value or lower, we may use the $\hat{\lambda}_{DU}$ value solely.

How many operational hours do we need for this to occur? By trying different values we find that:

> *"When the product of the accumulated operational hours times the number of failures exceeds some $3 \cdot 10^6$ hours, then the above condition is normally fulfilled.*

---

[3] In statistical terms, a confidence interval is an interval estimate of some population parameter. Instead of only specifying a single value (typically the mean of the failure rate), an interval likely to include the parameter is given. How likely the interval is to contain the parameter is determined by the confidence level. E.g. a 90% confidence interval for λ_{DU} may be given by: [$0.1 \cdot 10^{-6}$ per hour, $5 \cdot 10^{-6}$ per hour]. This means that we are 90% confident that the failure rate will lie within this interval. Further we are 95% sure that the λ_{DU} is less than $5 \cdot 10^{-6}$ per hour which is denoted the upper 95% percentile (i.e. the interval is "symmetric" and there is a corresponding 95% likelihood that the failure rate will be bigger than $0.1 \cdot 10^{-6}$ per hour).

It should be noted that in case of only one experienced failure, the above condition will strictly speaking not be fulfilled (the ratio will be closer to 5). However, in case of only one failure, the allowed operational time must exceed as much as $3 \cdot 10^6$ hours, which is considered sufficient to rely solely on operational experience.

For cases where zero (0) failures have occurred, special considerations must be made; In case of:

1. A very low original failure rate, the additional operational information has (so far) confirmed this and there is no evidence to alter the original assumption.
2. Opposite, in case of a very high original failure rate estimate, the fact that no failures have occurred during the observation period indicates that the original failure rate estimate may be too high.

Consequently, when having observed zero failures during operation, it will in any case be necessary to apply the original failure rate λ_{DU} in the update process.

6.1.3 Specifying the uncertainty for the initial failure rate estimate

The uncertainty of the initial λ_{DU} will here be specified by giving an additional conservative failure rate estimate, here denoted $\lambda_{DU\text{-}CE}$. The bigger the difference between the original failure rate λ_{DU} and the conservative failure rate estimate $\lambda_{DU\text{-}CE}$, the larger the uncertainty (i.e. the smaller the confidence is in the original estimate).

When specifying the uncertainty, i.e. the conservative failure rate estimate $\lambda_{DU\text{-}CE}$, some "conditions" needs to be pointed out:

a. If the user of the method shall give in the uncertainty estimate himself/herself, it should be possible to find the values in some handbook (e.g. in the updated PDS data handbook, 2009 version).

b. If an all too optimistic (low) or too pessimistic (high) initial failure rate has been specified, it is important that this estimate is "corrected" as quickly as possible if operational experience proves otherwise.

c. It the user of the method has no prior knowledge related to the uncertainty, some "default" choice of the conservative $\lambda_{DU\text{-}CE}$ should be given. In the mentioned Excel spreadsheet model the program itself will be able to select an appropriate value of $\lambda_{DU\text{-}CE}$ if the user does not have this information.

These aspects and how to specify the $\lambda_{DU\text{-}CE}$ are further discussed in section 6.2.2 where we present formulas for combining operational experience with the original failure rate estimate.

6.2 Calculating updated failure rates

6.2.1 Applying operational experience only

For the case with sufficient accumulated operational time to rely solely on this experience, calculating a new failure rate estimate is relatively straightforward and the new failure rate estimate $\widehat{\lambda}_{DU}$ is given by:

$$\hat{\lambda}_{DU} = \frac{\text{Number of failures}}{\text{Aggregated time in service}} = \frac{x}{n \cdot t} = \frac{x}{t_n}$$

Where

n = number of components in the population of comparable components
x = number of observed/registered DU failures during observation period
t = observation period
t_n = total aggregated time in operation (= t·n if all components have been in operation)

As discussed in section 6.1.2 this estimate can be used when the product of the accumulated operational time times the number of failures (i.e. $t_n \cdot x$) exceed $3 \cdot 10^6$ hours.

Example calculation:
Assume that there are 35 blowdown valves on a given plant. The assumed failure rate from design $\lambda_{DU} = 2.9 \cdot 10^{-6}$ per hour. During 3 years of observation one critical DU failure has occurred. The total observation period will be $3 \cdot 8760 \cdot 35 = 9.2 \cdot 10^5$ hours

An estimate for the new updated failure rate, based on this operational experience, will then be:

$$\hat{\lambda}_{DU} = \frac{\text{Number of failures}}{\text{Aggregated time in service}} = \frac{1}{9.2 \cdot 10^5} = 1.1 \cdot 10^{-6} \text{ per hour}$$

A 90% *confidence interval* for this failure rate is given by (ref. section 6.3.2 for how to estimate this):

$[5.6 \cdot 10^{-8}$ / time, $5.2 \cdot 10^{-6}$ / hour]

I.e. a relatively wide confidence interval since the total aggregated operational time is limited. Hence, in this case it is recommended to combine the operational experience with the failure rate estimate from design as shown in the next section.

6.2.2 Combining operational experience with original failure rate estimate

For the case with insufficient accumulated operational time we need to combine the original failure rate estimate with the new operational data. An important question then becomes: *how much trust do we want to put in the original estimate of λ_{DU}?*

From OREDA® data we find that roughly speaking the absolute value of the standard deviation for the critical failure modes is often comparable to the mean value itself[4]. However, always taking the conservative failure rate estimate as $2 \cdot \lambda_{DU}$ may give some undesirable consequences and will also impede the user from specifying a value. This is further discussed below.

Assume that we have defined n, x, t and t_n as above. In addition to the failure rate λ_{DU} from design we also need to define $\lambda_{DU\text{-}CE}$ which is the conservative estimate of the failure rate. The following alternatives for giving the $\lambda_{DU\text{-}CE}$ are foreseen:

- The user of the method specifies a conservative estimate for the failure rate, or

[4] This also implies that a conservative estimate for the original λ_{DU} can be taken as $2 \cdot \lambda_{DU}$

- The $\lambda_{DU\text{-}CE}$ is taken as $2 \cdot \lambda_{DU}$
- If either of the above are *less than* $5 \cdot 10^{-7}$ per hour, then $5 \cdot 10^{-7}$ per hour is anyway taken as the $\lambda_{DU\text{-}CE}$

I.e. $\lambda_{DU\text{-}CE}$ is chosen as:

$$\lambda_{DU-CE} = \max\left\{\text{user specified value}, 2 \cdot \lambda_{DU}, 5 \cdot 10^{-7}\right\}$$

Note that here a lower limit of $5 \cdot 10^{-7}$ per hour has been specified for the $\lambda_{DU\text{-}CE}$. This to avoid that very low failure rates and corresponding low estimates for $\lambda_{DU\text{-}CE}$ totally outweighs the operational experience[5]. Another way of putting this will be to say that we never believe a conservative estimate for the dangerous undetected failure rate (in the field) for any piece of field equipment to be better than $5 \cdot 10^{-7}$ per hour (based on e.g. generic data from OREDA / PDS).

We now define the uncertainty parameters α and γ as follows (see e.g. Vatn, 2006):

$$\alpha = \lambda_{DU} \Big/ \left[\lambda_{DU-CE} - \lambda_{DU}\right]^2$$

$$\gamma = \alpha \cdot \lambda_{DU}$$

In order to obtain an updated failure rate estimate based on operational experience combined with the a priori failure rate estimate λ_{DU} (and the $\lambda_{DU\text{-}CE}$) we now get the following formula:

$$\ddot{\lambda}_{DU} = \frac{\gamma + x}{\alpha + t_n}$$

As discussed earlier in this chapter the formulas to calculate α, γ and $\ddot{\lambda}_{DU}$ have been implemented in an Excel spreadsheet model and the calculations can therefore be performed automatically. As discussed above it will be optional whether to specify the $\lambda_{DU\text{-}CE}$ or letting the program choose an appropriate value.

Example calculation:
Again consider the example with 35 blowdown valves, an assumed failure rate from design $\lambda_{DU} = 2.9 \cdot 10^{-6}$ per hour and 3 years of observation with only one critical DU failure. The total observation period is then $3 \cdot 8760 \cdot 35 = 9.2 \cdot 10^5$ hours

Further assume that $\lambda_{DU\text{-}CE}$ is taken as $2 \cdot \lambda_{DU}$, i.e. $5.8 \cdot 10^{-6}$ per hour.

α og γ are then given as $3.5 \cdot 10^5$ and 1 respectively.

An estimate for the new updated failure rate will then be:

$$\ddot{\lambda}_{DU} = \frac{\gamma + x}{\alpha + t_n} = \frac{1+1}{3.5 \cdot 10^5 + 9.2 \cdot 10^5} = 1.6 \cdot 10^{-6} \text{ per hour}$$

[5] For example if a failure rate λ_{DU} of 10^{-8} per hour has been assumed in design and the corresponding $\lambda_{DU\text{-}CE}$ is taken as $2 \cdot 10^{-8}$ per hour, then some 10.000 years of aggregated time in service is needed before the operational experience gets an equal weight as the original estimate.

As compared to the failure rate based solely on operational experience (i.e. $1.1 \cdot 10^{-6}$ per hour, ref section 6.2.1), we see that this combined estimate is somewhat "slower" with respect to adjusting to the operational experience (due to the weighting of the original failure rate estimate).

6.3 Updating the test intervals

6.3.1 Introduction / background

Having calculated the new updated failure rate estimates, an interesting case will often be to consider the length of the test interval – i.e. to consider whether the present testing frequency is appropriate when taking credit for the additional information gathered through operational experience.

If operational experience proves that the equipment is significantly more or less reliable than what was assumed in the design phase, there may be room for changing the test interval.

When considering a change of the test interval this will generally be most relevant for components with a significant amount of operational experience, either based on a high number of installed items and/or several years of operation.

First we therefore consider a method where only operational experience is applied.

6.3.2 Simple approach based on halving or doubling of the test interval

When using operational information as part of a decision to change the functional test interval, it is important to ensure a sufficient degree of confidence in the underlying quantitative estimates. I.e. changing the functional test interval is a decision which needs to be substantiated by extensive quantitative as well as qualitative arguments. We will therefore argue for a rather conservative approach for changing the functional test intervals.

A conservative approach is further supported by the fact that functional test intervals often are changed in large steps rather than in small steps. The oil companies usually perform testing and maintenance in batches, and testing that requires process shutdown is often performed during scheduled revision stops, for example once every year. Typical functional test intervals are 3 months, 6 months, 12 months, 24 months, or in some cases 36 months. For practical purposes, it is therefore often a question of whether or not the functional test interval may be doubled or halved.

First we define the following parameters (mostly the same as in the previous sections):

n	=	number of components in the population of comparable components
x	=	number of observed/registered DU failures during observation period
t	=	observation period
t_n	=	total aggregated time in operation ($t \cdot n$ if all components have been in operation)
τ	=	length of original functional test interval
λ_{DU}	=	the (originally) assumed rate of dangerous undetected failures
$\hat{\lambda}_{DU}$	=	updated λ_{DU} based on operational experience only

First we calculate the dangerous undetected failure rate, $\hat{\lambda}_{DU}$, similar as in section 6.2.1, i.e.:

$$\hat{\lambda}_{DU} = \frac{\text{Number of failures}}{\text{Aggregated time in service}} = \frac{x}{n \cdot t} = \frac{x}{t_n}$$

As discussed above, a high degree of confidence in the quantitative estimates is desirable. Therefore we next establish a 90% confidence interval for $\hat{\lambda}_{DU}$, and use this interval as part of the decision criterion as to whether the functional test interval can be extended or shortened. The upper and lower value of the 90% confidence interval may be calculated by (Rausand & Høyland 2004):

$$\left(\frac{1}{2t_n} z_{0.95,\,2x} \;,\; \frac{1}{2t_n} z_{0.05,\,2(x+1)} \right)$$

Here t_n and x are defined as above, and $z_{0.95,\nu}$ and $z_{0.05,\nu}$ denote the upper 95% and 5% percentiles, respectively, of the χ^2-distribution with ν degrees of freedom. Values for the different percentiles in the χ^2-distribution can be found from tables or they can be calculated using standard functions in Excel. If no DU failures have been experienced during the observation time, we may use the single sided lower 90% confidence limit (see below).

Having estimated the 90% confidence interval, we propose the following set of main rules for changing the functional test interval:

1. *If $\hat{\lambda}_{DU}$ is less than half the λ_{DU} and the entire estimated 90% interval for the $\hat{\lambda}_{DU}$ is below λ_{DU}, then the functional test interval can be considered doubled (e.g. from once every year to every second year)*

2. *If $\hat{\lambda}_{DU}$ is more than twice the λ_{DU} and the entire estimated 90% interval for the $\hat{\lambda}_{DU}$ is above λ_{DU}, then the functional test interval must be halved (e.g. from once every year to every six months)*

This can be further illustrated by the following figure.

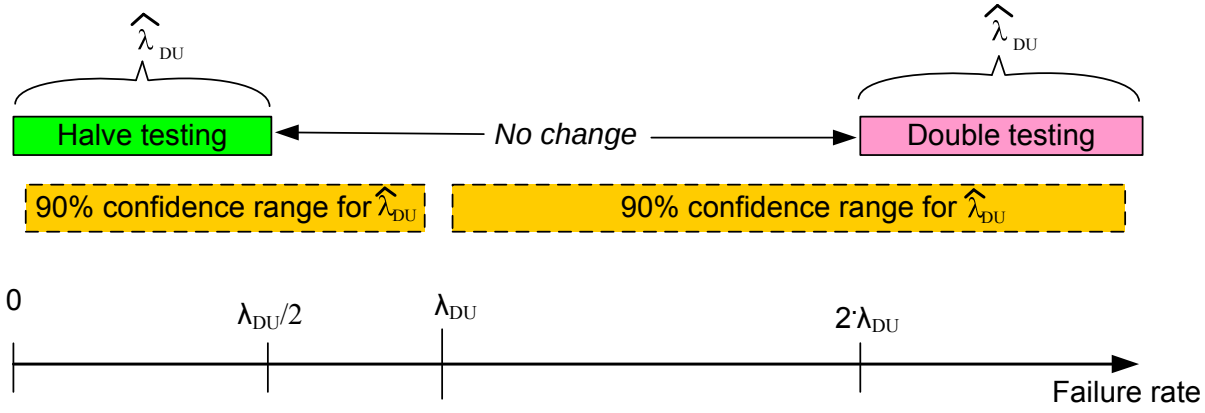

Figure 6 Illustration of rule set for changing the test interval

As seen, a relatively conservative approach has been chosen, i.e. before recommending a change of the test interval a high confidence is required in order to conclude that the experienced failure rate significantly deviates from the failure rate assumed in design.

Additional considerations and discussion
Below, some additional considerations are made concerning how this method shall be applied in practice.

- If no/zero failures are observed within the observation period t (i.e. x = 0), then a one-sided 90% confidence interval for $\hat{\lambda}_{DU}$ can be established, given by: $\left(0 , \frac{1}{2t_n} Z_{0.10,\,2}\right)$. If this entire confidence interval is below the original λ_{DU} then the test interval can be considered increased.

- The failure information shall be applied cumulatively throughout time. I.e. all information from previous years of operation (i.e. from start of observation) shall be taken into consideration. E.g. when having four years of operation, then all information from these four years shall be taken into consideration unless equipment has been redesigned and/or introduced during the period (in which case only the relevant operational period must be applied).

- It is implicitly assumed that the initial test interval is established based on the original λ_{DU}. The comparison shall therefore always be done against this value (and the test interval may have to be changed back again). E.g. if for some piece of equipment the test interval has been changed from 1 year to every second year, and one suddenly starts to experience a lot of failures in year 3 and 4, then it may become necessary to "go back" to the original test interval of 1 year.

- When collecting failure information, it must be remembered that various start-up problems may cause a high(er) number of initial failures, e.g. due to inherent quality problems, failures during installation or commissioning. For topside equipment a required "burn-in phase" should therefore be allowed for, thereby removing the "children's deceases".

- The method is conservative in the sense that a lot of information is required before the "strict" rule set can be fulfilled. On the other hand; the more aggregated operational time available, the more components in the population and therefore the more interesting to actually change the test interval. E.g. if one is considering 30 blowdown valves versus 500 gas detectors it will probably be much more savings related to reduced testing of the detectors.

- The method is probably not cost optimal, but is considered as a fairly simple and straightforward way of supporting a decision to change the test interval for selected cases where the number of components are high and the aggregated time in service therefore accumulate quickly.

It should be strongly pointed out that when considering to increase (or reduce) the test interval, this should not be based on quantitative considerations only. See section 6.4 for a more thorough discussion of this.

Example calculation:
An interesting case for evaluating the length of the test intervals will be fire and gas detectors since the volume is large and thereby the gain of reduced testing will be significant. We will therefore consider an example with 800 smoke detectors which have been in operation for two years.

The smoke detectors are assumed to have a failure rate from design of $\lambda_{DU} = 0.8 \cdot 10^{-6}$ per hour. There are 800 such detectors and the expected number of failures during <u>*two years*</u> of operation can then be calculated as:

$$E(X) = \text{Expected \# of failures in population} = \lambda_{DU} \cdot n \cdot t = 0.8 \cdot 10^{-6} \cdot 800 \cdot 2 \cdot 8760 \approx 11 \text{ failures}$$

Let us now assume that over a period of two years, only 2 DU failures have been registered for the population of smoke detectors. Here the registered number of failures is far below the target value (of 11 failures for two years or some 5 failures annually) and as discussed in section 5.2.3 less frequent proof testing may be considered. The new estimated $\hat{\lambda}_{DU}$ will be:

$$\hat{\lambda}_{DU} = \frac{\text{Number of failures}}{\text{Aggregated time in service}} = \frac{2}{800 \cdot 2 \cdot 8760} = 0.14 \cdot 10^{-6} \text{ per hour}$$

The 90% confidence interval is then given by:

$$\left(\frac{1}{2t_n} Z_{0.95,\,2x} \,,\, \frac{1}{2t_n} Z_{0.05,\,2(x+1)} \right) = \left(\frac{1}{2 \cdot 800 \cdot 17520} Z_{0.95,4} \,,\, \frac{1}{2 \cdot 800 \cdot 17520} Z_{0.05,6} \right) = \left(0.025 \cdot 10^{-6} \,,\, 0.45 \cdot 10^{-6} \right)$$

Where the $Z_{0.95,\,4}$ and $Z_{0.05,\,6}$ percentiles can be found from tables (or from Excel), to be 0.71 and 12.59 respectively.

As seen, the new estimated $\hat{\lambda}_{DU}$ is more than a factor five less than the originally assumed λ_{DU} and the entire 90% confidence for the $\hat{\lambda}_{DU}$ is below the original λ_{DU}. Hence, based on the proposed rule set, <u>the test interval can be considered doubled for this case</u>.

6.3.3 A more flexible approach to changing the test intervals

The above method is restricted to either halve or double the test interval. There may however be situations where a more limited change of the test interval can be relevant. E.g. if the original test interval is 6 months and the operational experience does not allow doubling of the test interval, it may still be feasible to increase the test interval to 9 months.

Below, a procedure for changing the test interval in a more flexible way is described:

1. The following restrictions and assumptions apply:
   a. The test interval can never be more than doubled or halved (max allowable change). This assumption is made to ensure some conservatism in how much the functional test interval may be altered.
   b. The maximum allowed length of the test interval shall be 36 months. 36 months interval corresponds to the longest interval between revision stops for oil and gas installations at the Norwegian Continental shelf, and we assume that the functional

status of all safety critical equipment should be verified with no longer intervals than this.

c. The "allowed" test intervals to be suggested by the program will be on a discrete scale as follows; 1 month, 3 months, 6 months, 9 months, 12 months, 18 months, 24 months, 36 months.
d. It is implicitly assumed that the original test interval τ is based on the original assumed failure rate λ_{DU} and is selected so as to fulfil the relevant SIL requirements.

2. Calculate the $\ddot{\lambda}_{DU}$ similar as in section 6.2.2

3. Calculate the ratio between: $\lambda_{DU} / \ddot{\lambda}_{DU}$. This ratio indicates the fractional change in failure rate and thus the "allowed" change of test interval.

4. The (first iteration) updated test interval can now be calculated as: $\ddot{\tau} = (\lambda_{DU} / \ddot{\lambda}_{DU}) \cdot \tau$

5. If the new proposed test interval $\ddot{\tau}$ *is larger than* τ:
   a. The new test interval $\ddot{\tau}$ shall now be rounded *down* to the first allowed test interval (ref. point 1a. - 1c. above)
   b. If this proposed test interval is double of the original test interval, then in addition the test for $\hat{\lambda}_{DU}$ shall be fulfilled (ref. section 6.3.2). If not fulfilled, then the new test interval shall again be rounded *down* to the next allowed test interval (ref. point 1c. above)

6. If the new proposed test interval $\ddot{\tau}$ *is smaller than* τ:
   a. The new test interval $\ddot{\tau}$ shall now be rounded *up* to the first allowed test interval (ref. point 1a. - 1c. above)
   b. If this proposed test interval is half of the original test interval, then in addition the test for $\hat{\lambda}_{DU}$ shall be fulfilled (ref. section 6.3.2). If not fulfilled, then the new test interval shall again be rounded *up* to the next allowed test interval (ref. point 1c. above)

As seen, there is a built-in conservativeness in the proposed procedure for changing the test interval. If the new proposed test interval $\ddot{\tau}$ differs from the original τ, the new test interval will always be rounded *towards* the original interval. Also, in order to allow for a doubling or halving of the test interval, the additional criteria from section 6.3.2 must be fulfilled. In practice this implies that a significant amount of operational experience needs to be available to support a decision of halving or doubling the test interval.

Note that the formulas to calculate the required parameters as discussed above have been implemented in an Excel spreadsheet model and the calculations can therefore be performed easily in this program.

Example calculation 1:
Again consider the example with the 35 blowdown valves from section 6.2.2; one critical DU failure during 3 years of operation, $\lambda_{DU} = 2.9 \cdot 10^{-6}$ per hour, $\lambda_{DU\text{-}CE} = 5.8 \cdot 10^{-6}$ per hour, $t_n = 9.2 \cdot 10^5$ hours and the updated failure rate was calculated as $\ddot{\lambda}_{DU} = 1.6 \cdot 10^{-6}$ per hour. Furthermore it is assumed that the blowdown valves originally are tested every 12th month.

We then enter step 4. in the above procedure and calculate the (first iteration) updated test interval as:

$$\ddot{\tau} = (\lambda_{DU} / \ddot{\lambda}_{DU}) \cdot \tau = \frac{2.9 \cdot 10^{-6}}{1.6 \cdot 10^{-6}} \cdot 12 \text{ months} \approx 22 \text{ months}$$

Going on to step 5a, we see that the new test interval shall be rounded *down* to the first allowed test interval. This is 18 months (ref. point 1c.) and hence the new proposed test interval becomes 18 months.

Example calculation 2:
Now consider the same blowdown valve example and the same parameters as above, but assume that zero (0) failures have occurred during the three years period.

Using the formula from section 6.2.2, the new updated failure rate estimate is then:

$$\ddot{\lambda}_{DU} = \frac{\gamma + x}{\alpha + t_n} = \frac{1 + 0}{3.5 \cdot 10^5 + 9.2 \cdot 10^5} = 8 \cdot 10^{-7} \text{ per hour}$$

Now, entering step 4. in the procedure, the (first iteration) updated test interval becomes:

$$\ddot{\tau} = (\lambda_{DU} / \ddot{\lambda}_{DU}) \cdot \tau = \frac{2.9 \cdot 10^{-6}}{8 \cdot 10^{-7}} \cdot 12 \text{ months} \approx 43 \text{ months}$$

Going on to step 5a, we see that this exceeds the maximum allowable change of test interval (i.e. a doubling from 12 to 24 months). Therefore the new test interval is set to 24 months.

This leads on to step 5b where we additionally shall perform the test for $\hat{\lambda}_{DU}$ as described in section 6.3.2. The one sided 90% confidence interval for $\hat{\lambda}_{DU}$ with zero registered failures can be estimated to: [0, $2.5 \cdot 10^{-6}$ / hour]. Since the upper limit of this interval is below the assumed λ_{DU} from design (being $2.9 \cdot 10^{-6}$ per hour), a doubling of the test interval is allowed and the proposed new test interval becomes 24 months.

6.4 Additional qualitative aspects to consider when changing the test interval

Changing the test interval should not rely on quantitative considerations alone. It is also necessary to consider qualitative factors like:

- *Quality of and confidence in the collected failure data information:* Have all relevant failures been recorded and are they correctly classified as dangerous or safe failures?
- *Relevance of collected data – new equipment:* Have data been collected for the presently installed equipment, or has some equipment been replaced with another make/type during the collection period?
- *Quality of testing:* How is the quality of functional testing? Are all potential DU failures revealed by the current practices, tools, and procedures?
- *The number of operational hours:* Are the amount of operational experience underlying a decision to reduce or increase the length of the test interval sufficient? This is, however, implicitly taken care of by the confidence interval calculations.

- *Type of failures experienced:* Similar components may be subject to the same identifiable failure cause, e.g., failure of several pressure transmitters due to a repeated calibration error or valves failing due to excessive sand production. We are then faced with examples of systematic failures which also have the potential to introduce common cause failures. In such cases, rather than increasing the frequency of functional testing, a root cause analysis should be performed so that corrective means can be identified and implemented for the components in question.
- *The benefit and practicalities of changing the test interval:* Are there any practical implications that may influence the savings/gain of changing the functional test interval? Many installations are run on low or no permanent manning and maintenance is performed on a "campaign" basis. Hence, the test intervals must in practice often be adapted to such a testing regime.
- *Vendor recommendations:* What does the vendor recommend with respect to frequency of testing? When deviating from this and particularly when testing less frequent than what is recommended, the motivation behind the vendor recommendation may need to be further assessed.
- *Secondary effects of the functional test intervals*: Is the assumption of a constant failure rate still valid when the functional test interval is extended, or is it likely that the component may reach the wear out period before next functional test? Are there any other foreseen secondary effects by extending the functional test intervals, e.g., build-up of materials in valve seat or cavity for normally opened valves? Or may more functional testing introduce new failures, due to additional wear or human errors?

The aspects above may be included in a checklist. Based on an evaluation of these aspects, one may find that a change in the functional test interval is not recommended or should be postponed until more insight is gained on failure causes or more data has been collected.

7 References

"*A new approach for follow-up of safety instrumented systems in the oil and gas industry*", S. Hauge and M.A. Lundteigen, Esrel 2008

"*Procedures for updating test intervals based on experience data*", J. Vatn, ESREDA seminar on "Reliability of Safety-Critical Systems", 2006

"*System reliability theory*", Rausand and Høyland, Wiley 2004

"Guidelines for Safe and Reliable Instrumented Protective Systems, CCPS 2007, Wiley & Sons

IEC 61508: Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems, part 1-7, Edition 1.0 (various dates).

IEC 61511: Functional safety - safety instrumented systems for the process industry sector, part 1-3, 2003

Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry, OLF guideline 070, 2004

ISO 14224: Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment. Second edition, ISO 2006

ISO 20815: Petroleum, petrochemical and natural gas industries – Production assurance and reliability management. First edition, ISO 2008

Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2006 Edition, SINTEF Report STF50 A06031

Reliability Data for Safety Instrumented Systems - PDS Data Handbook, 2006 Edition, SINTEF Report STF50 A06030:

Appendix A: Table of follow-up activities and responsibilities

In the below table a brief description of important SIS follow-up activities are given. It is also indicated how often the activities may be performed and responsible person/department. Obviously this needs to be adapted to the particular plant under consideration and are therefore meant as guidance only.

Table 2 SIS follow-up activities, frequency and responsibilities

When to perform	Description of SIS follow-up activities	Responsible position
Continuous O&M activities	SIS operation during normal conditions and in degraded mode, including • Reporting of safety critical failures revealed during activities other than testing • Logging of inhibits and overrides • Compensating measures • Logging of equipment out of service	Production / operation
	SIS maintenance, testing and inspection according to maintenance programme and test procedures, including • Reporting of safety critical failures • Reporting of other failures • Repair and replacement of defect components	Maintenance
As required / upon demand	Day to day SIS follow-up activities, including assistance to O&M on SIS related questions.	SIS system responsible
	Identify and evaluate the need for SIS modifications based on reported failures, deficiencies and non-conformities, process changes, etc. Initiate necessary modification activities according to procedures and initiate studies and analyses as required SIS Management during study and modification Update of SIS documentation including SRS if required.	Technical support / SIS system responsible / Technical safety / Automation
	Perform SIS audits and verifications as required	SIS system responsible
	After a shutdown / SIS activation go through IMS/ASR reports, identify possible safety critical failures revealed and if relevant prepare maintenance notifications.	SIS system responsible
Every 3rd month	Go through and verify that maintenance notifications and failure reports for safety critical equipment are of sufficient quality to perform failure classification. If required, modify and supplement the notifications.	SIS system responsible
	By spot-check verify that SIS operation and maintenance is performed according to procedures.	SIS system responsible

When to perform	Description of SIS follow-up activities	Responsible position
Every 3rd month	Go through maintenance back-log and initiate necessary actions as required.	Maintenance
Annually	Extract relevant failure reports maintenance system, etc. Perform failure classification, evaluate number of DU failures for each equipment type and compare with plant target values. If necessary introduce compensating measures, analyse failure causes and/or consider length of test interval.	SIS system responsible with assistance from technical safety and automation
	From IMS, system logs etc.; estimate other relevant SIS follow-up parameters such as spurious trip rates, actual demand rates, number of inhibits/overrides, etc.	SIS system responsible with assistance from technical safety and automation
	Prepare annual SIS performance summary report. Identify any recommended changes / modifications to SIS design or procedures due to performance deviations or integrity degradation.	SIS system responsible with assistance from technical safety and automation
	Prior to revision stop prepare a "stop-plan" describing how the planned shutdown shall be optimally utilised with respect to data collection and test results.	SIS system responsible with assistance from technical safety and automation
Every 3rd year	Recalculate failure rates, update data dossier and verify whether SIL requirements for safety functions are fulfilled.	SIS system responsible with assistance from technical safety and automation
	Consider the requirement and possibility for updating of test intervals.	SIS system responsible with assistance from technical safety and automation