Available online at www.sciencedirect.com
ScienceDirect
Journal of Loss Prevention in the Process Industries 20 (2007) 218–229
Journal of Loss Prevention in the process industries
www.elsevier.com/locate/jlp

Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing

Mary Ann Lundteigen*, Marvin Rausand

Department of Production and Quality Engineering, The Norwegian University of Science and Technology, 7491 Trondheim, Norway

Received 27 December 2006; received in revised form 9 March 2007; accepted 9 March 2007

Abstract

This paper presents a common cause failure (CCF) defense approach for safety instrumented systems (SIS) in the oil and gas industry. The SIS normally operates in the low demand mode, which means that regular testing and inspection are required to reveal SIS failures. The CCF defense approach comprises checklists and analytical tools which may be integrated with current approaches for function testing, inspection and follow-up. The paper focuses on how defense measures may be implemented to increase awareness of CCFs, to improve the ability to detect CCFs, and to avoid introducing new CCFs. The CCF defense approach may also be applicable for other industry sectors.
© 2007 Elsevier Ltd. All rights reserved.

Keywords: Common cause failures; Safety instrumented systems; Defense measures; Function testing; Inspection

1. Introduction

Safety instrumented systems (SIS) are used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment. A SIS generally consists of one or more input elements (e.g., sensors, transmitters), one or more logic solvers (e.g., programmable logic controllers [PLC], relay logic systems), and one or more final elements (e.g., safety valves, circuit breakers). The main parts of a SIS are illustrated in Fig. 1.

A SIS may perform several safety (instrumented) functions (SIF) and is sometimes referred to as a safety barrier or a protection layer (Sklet, 2006). Related SIFs may be combined into more comprehensive protection systems, like fire and gas detection systems and emergency shutdown systems.

The standards IEC 61508 (1998) and IEC 61511 (2003) are extensively used in the oil and gas industry, during all phases of the SIS life cycle. Both standards use safety integrity level (SIL) as a measure of SIS reliability. To enhance the reliability, redundancy is often introduced in the SIS architecture. Independence between safety barriers is achieved by combining diversity in design (e.g., by using diverse technology, diverse design and implementation approaches) with diversity in follow-up of SIS in the operational phase (e.g., by using different operation and maintenance procedures, scheduling or staff).

Common cause failures (CCF) are a serious threat to SIS reliability (Smith & Simpson, 2005; Summers & Raney, 1999; Edwards & Watson, 1979), and may lead to simultaneous failures of redundant components and safety barriers. IEC 61511 (2003) defines a CCF as *a failure which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to a system failure*. A channel is a single redundant path within a SIF, or alternatively a single SIF in case more than one SIF is required to obtain the necessary risk reduction.

Causes of potential CCFs may be introduced in design as well as in the operational phase. In the design phase, CCF causes may be a result of inadequate understanding of failure mechanisms and responses, improper selection of hardware components, and so forth. In the operational phase, CCF causes may, for example, be introduced because of improper testing, human errors during operation

*Corresponding author. Tel.: +47 73 59 7101; fax: +47 73 59 7117.
E-mail address: mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

0950-4230/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2007.03.007

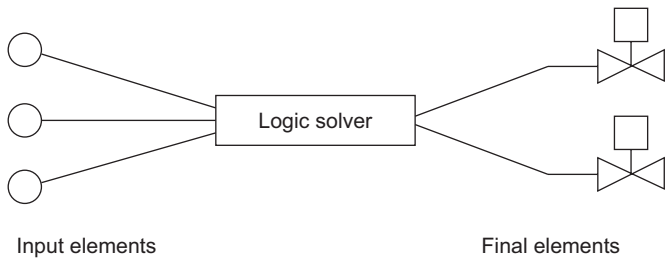

Fig. 1. Main parts of a safety instrumented system.

and maintenance, and environmental stresses outside the design envelope.

Many authors find it useful to split CCF causes into *root causes* and *coupling factors* (Parry, 1991; Paula, Campbell, & Rasmuson, 1991). A root cause is a basic cause of a component failure (e.g., a corrosive environment), while a coupling factor explains why several components are affected by the same root cause (e.g., inadequate material selection for several valves).

The nuclear industry is very concerned with CCFs, and is recording and analyzing CCF events (NUREG/CR-5460, 1990; NUREG/CR-5485, 1998; NEA, 2004, 2002, 2003, 2004). Several guidelines have been developed for qualitative and quantitative analysis of CCFs. The Nuclear Energy Agency (NEA) has initiated the International Common Cause Data Exchange (ICDE) project to encourage collection and analysis of data related to CCF events. Several analyses of CCF data that give insight into why CCFs occur have been published.

The oil and gas industry is mainly focusing on CCFs in the design phase of the SIS, while CCFs are given much less attention in the operational phase. The oil companies have systematically collected reliability data for more than 25 years through the OREDA project (Langseth, Haugen, & Sandtorv, 1998; Sandtorv, Hokstad, & Thompson, 1996). The data collection is based on maintenance reports from single item failures. This approach does not easily provide information about CCFs and the status related to CCFs is therefore not fully known. The Norwegian Petroleum Safety Authority (PSA) is, however, increasingly concerned with how new technology, standardization, and new operational concepts may reduce the independence between SIFs (Hauge et al., 2006).

Function testing and inspection are key activities for a SIS operating in the low demand mode. Low demand means that the SIS experiences few demands, typically less than once every year. Function testing and inspection are influencing the occurrence of CCFs in the operational phase because: (i) main types of CCFs can be identified and corrected through efficient testing and inspection procedures, and (ii) inadequate procedures and human errors may cause simultaneous failures of several components (Hirschberg, 1991; Johanson et al., 2003; Pyy, Laakso, & Reiman, 1997).

The objective of this paper is to propose a CCF defense approach which is able to improve the awareness to CCFs, prevent CCFs from being introduced during the execution of function tests and inspections, identify CCFs and CCF causes and select efficient defenses against future CCFs. The CCF defense approach is designed to be integrated with current practices related to execution and follow-up of function testing and inspection in the oil and gas industry. The CCF defense approach has been developed for SIS applications in the Norwegian oil and gas industry, but should be applicable also to other industry sectors.

The rest of the paper is organized as follows. In Section 2 we describe how CCFs currently are handled in the Norwegian oil and gas industry. Section 3 describes how diagnostic testing, function testing, and visual inspections may influence the occurrence of CCFs. In Section 4 we clarify and discuss the definition of a CCF and indicate how CCFs may be classified. The new CCF defense approach is described in Section 5. We conclude in Section 6 with a brief discussion of the proposed approach and give some recommendations for further work in Section 7.

2. The oil and gas industry's approach to CCFs

Recent SIS applications for the Norwegian oil and gas industry are built according to IEC 61508 (1998) and IEC 61511 (2003). The Norwegian Oil Industry Association (OLF) has developed a guideline on the practical application of IEC 61508 (1998) and IEC 61511 (2003) in the oil and gas industry, that is referred to as the OLF-070 (OLF-070, 2004) guideline. The standards and the guideline require that the effect of CCFs is taken into account in reliability calculations. IEC 61508 (1998) recommends using the β-factor model (e.g., see Rausand & Høyland, 2004), where β is the conditional probability of a CCF, when a failure has occurred. An extended version of the β-factor model, called the PDS method (Sintef, 2006), is frequently used in the Norwegian oil and gas industry.

The IEC standards have few specific requirements related to CCFs in the operational phase, and this may be a reason why CCFs are not given much attention in this phase. Another reason may be that there is a general lack of knowledge on how CCFs affect operation and maintenance, since CCFs are not recorded and analyzed. There is no guidance in OREDA (2002) on how to collect data on CCFs, even though CCFs are mentioned in connection with fire and gas detectors. ISO 14224 (2006) recognizes the importance of sector specific CCF data for SIL analysis, and suggests that CCF data are derived from analysis of single failures rather than being recorded directly. Currently, however, data related to CCFs are not collected.

IEC 61508 (1998), part 6, Humphreys (1987), and Smith and Simpson (2005) provide checklists that can be used to determine an application specific β value, while the PDS method suggests generic β values for various SIS components. The generic values are based on previous estimates combined with expert judgments, and may not reflect the

plant specific conditions. The checklists are not always sensitive to single improvements, and a new or improved defense tactic in the operational phase may therefore not lead to a reduction of the estimated β-factor.

To save money and ease operation and maintenance, the technical solutions become more and more standardized. The same type of PLCs is, for example, used in several SIS applications. This standardization may reduce the independence between SIS applications (Hauge et al., 2006). New operational concepts, like remote monitoring and control, may introduce additional risks (Johnsen, Lundteigen, Fartun, & Monsen, 2005; Sintef, 2003). Sintef, the Norwegian research organization, has recently carried out two studies that analyze CCFs and the level of independence in typical SIS applications on oil and gas installations (Hauge, Hokstad, Herrera, Onshus, & Langseth, 2004; Hauge et al., 2006). The first study was initiated by SIS vendors, system integrators and end users participating in a network on the application of the PDS method in Norway. The second study was initiated by Hydro, the Norwegian oil company. Unfortunately, there has, so far, not been any follow-up of these studies.

3. Diagnostic testing, function testing and visual inspection

Diagnostic testing, function testing, and visual inspections are important means to verify that the SIS is able to perform its safety functions and to reveal any failures that may impede the SIS from functioning on demand. Failures that may prevent the SIS from functioning on demand are referred to as *dangerous* failures by IEC 61508 (1998) and IEC 61511 (2003).

Diagnostic testing is online means to detect deviations, degradations and discrepancies, and is usually performed by dedicated software and hardware, implemented inherently in the components (e.g., watchdogs) or added to the SIS configuration (e.g., read-back of status signals from field elements for comparison with output signals set by the PLC). Failures detected by diagnostic testing are called *dangerous detected* failures in IEC 61511 (2003). The diagnostic software and hardware usually do not test the complete SIF, but give alarm upon various abnormalities (e.g., drift, exceeded cycle time, and communication error) on component level. Diagnostic alarms that share the same cause may indicate the presence of a CCF.

Function testing and visual inspections are offline means to detect SIS failures and are performed at regular intervals. The objective of function testing is to confirm the correct functionality and to reveal undetected failures that may impede the SIS from functioning on demand. Visual inspection looks for observable deterioration and unauthorized modifications. Failures revealed by function testing and inspection are called *dangerous undetected* failures in IEC 61511 (2003). The interval between function tests (or inspections) has a direct influence on the SIF's probability of failure on demand.

In most cases, function testing and inspection are executed manually. However, new technology has been developed for automated testing, for example, partial stroke testing of valves (Lundteigen & Rausand, 2007; Summers & Zachary, 2000). In the future it is expected that new oil and gas installations may be built for more extensive use of automated testing and inspection, but for the current oil and gas installations (that may stay in operation for another two decades) it is not realistic to expect major changes in the function testing and inspection strategies.

This paper focuses on current approaches to function testing, and how defense measures may be implemented to increase awareness of CCFs, to improve the ability to detect CCFs, and to avoid introducing new CCFs.

Function testing and inspection generally comprise the following six tasks:

(1) *Scheduling*: Today, function testing and inspections are scheduled automatically by the maintenance management system. At a predefined time, the function test or inspection is submitted as a work package that includes the test or inspection procedure.
(2) *Preparation*, *execution*, *and restoration*:
   (a) *Preparation*: Before the test or inspection is executed, it is required to do certain preparations; to obtain work permits, find the necessary documentation, to coordinate with other involved disciplines and, in some cases, to perform a job safety analysis. Job safety analysis is commonly used in the oil and gas industry to prepare for critical and complex work activities with a potentially high risk to humans, equipment or the environment. A function test or inspection does not always require a job safety analysis. This depends on the complexity of the work, and the total amount of ongoing activities in the same area.
   (b) *Execution*: The prescribed steps in the test or inspection procedure are executed, including setting necessary overrides and inhibits.
   (c) *Restoration*: After the test or inspection is completed, the affected components are put back into operation in a safe and adequate manner. This may involve opening/closing of isolation valves, following interlock procedures, resetting solenoids and valves and removing inhibits and overrides.
(3) *Failure reporting*: Deviations and failures are reported through the maintenance management system by the personnel executing the function test or inspection. Failures and deviations may be recorded as free text, as numerical values (e.g., pressure readings) or by using pre-defined classification systems of failure causes, detection method, and failure effects.
(4) *Failure analysis*: The purpose of the failure analysis is to assess the SIS performance and compare with the target performance (SIL requirements). The SIS performance in the operational phase is usually derived from the

number of dangerous failures detected during a function test, inspection, and real demands. To ensure that the quality of the recorded data is adequate, it is often necessary to reassess the initial failure classification and review the free text descriptions. Performance monitoring has also been done prior to the introduction of the IEC 61508 (1998) and the IEC 61511 (2003). On the Norwegian continental shelf, it has, for several years, been required to report the status of safety barriers. The main difference between the previous approach and the IEC 61508 (1998)/IEC 61511 (2003) requirements, is the focus on the performance of safety functions rather than on safety components.

(5) *Implementation*: It is necessary to prepare and implement corrective means related to the recorded failures. It is expected that failures detected by diagnostic testing, function testing, and inspection are corrected immediately to reduce the unavailability of the SIF. In cases where failures are not possible to correct immediately, compensating measures must be implemented.

(6) *Validation and continuous improvements*: At regular intervals, it is necessary to review current work practices and procedures and to analyze how they comply with the overall objective of SIS follow-up, which is to maintain the SIS performance during operation and maintenance. It may be relevant to review the extent of overdue tests, the adequacy of the failure classification system and the failure reporting procedures, SIF performance versus SIL targets, quality and scope of proof test execution (HSE, 2002). Any deviations or deficiencies should be captured and used to improve SIS follow-up.

4. Definition and classification of CCFs

4.1. The main attributes of CCFs

There is no generally accepted definition of CCF. This means that people in different industry sectors may have different opinions of what a CCF is. Smith and Watson (1980) review nine different definitions of CCF and suggest that a definition must encompass the following six attributes: (1) the components affected are unable to perform as required, (2) multiple failures exist within (but not limited to) redundant configurations, (3) the failures are "first in line" type of failures and not the result of cascading failures, (4) the failures occur within a defined critical time interval (e.g., the time a plane is in the air during a flight), (5) the failures are due to a single underlying defect or a physical phenomenon (the common cause of failures), and (6) the effect of failures must lead to some major disabling of the system's ability to perform as required.

All these attributes are reflected in the CCF definition that is used by the nuclear power industry (NEA, 2004). Concerning attribute (4), the ICDE project defines the critical time interval to be the time between two consecutive inspections. IEC 61508 (1998) and IEC 61511 (2003) do not include the critical time aspect in their definition of CCF. It is, however, natural to restrict the analysis to dependent failures occurring within the same function test interval. All critical failures should, at least in principle, be identified and corrected as part of the function test and repair action. A failure in the next interval will therefore be a single failure, even if it is dependent on a (corrected) failure in the previous interval. To clarify when dependent failures are defined as CCF during failure analysis, the following attributes may be applied: (1) the CCF event comprises multiple (complete) failures of two or more redundant components or two or more SIFs due to a shared cause, (2) the multiple failures occur within the same inspection or function test interval, and (3) the CCF event leads to failure of a single SIF or loss of several SIFs.

4.2. Classification of CCF attributes

Failure classification systems may be used to identify potential failures and to structure both causes and effects. Some authors distinguish between pre-operational and operational failure causes (Humphreys & Jenkins, 1991; Watson & Edwards, 1979), some use the concept of root causes and coupling factors, where the root causes may be further split into trigger events, conditioning events and proximate causes (Parry, 1991; Mosleh et al., 1994). Here, a proximate cause is a readily identifiable cause of failure, a conditioning event is a condition that predisposes the component to failure, and a triggering event is an event that initiates the transition to the failed state. The nuclear power industry has established classification systems for CCF causes and differentiate between various types of root causes and coupling factors (NEA, 2004; NUREG/CR-5460, 1990; NUREG/CR-5485, 1998). One such classification system is shown in Table 1. The operational failure causes proposed by, for example, by Humphreys and Jenkins (1991), overlap quite well with the coupling factors.

In many cases, CCF analysis is often limited to dependent failures within a single SIF since the reliability is estimated for each SIF separately. Cooper, Lofgren, Samanta, and Wong (1993) have introduced common failure mechanisms as an alternative concept to CCFs, to ensure that also CCFs affecting different SIFs are identified and followed up. A common failure mechanism comprises failures that share failure mechanisms, design or function, and time of occurrence. Failures that are classified with common failure mechanisms do therefore share the same coupling factors.

CCF causes are often identical to the systematic failure causes. Systematic failures are in IEC 61508 (1998) and IEC 61511 (2003) defined as failures that are due to design,

implementation or operational related errors. The IEC standards suggest, as a general rule, not to quantify systematic failures. However, some systematic failures are quantified through the modeling of CCFs.

It may be convenient to distinguish between classification systems for failure reporting and classification systems for in-depth failure analysis. For failure reporting it is important that the taxonomy is intuitive and easy to understand, giving an initial and rough classification. For failure analysis one may add more detailed taxonomy, as suggested in OREDA (2002).

5. New CCF defense approach

In this section, we describe a new CCF defense approach which may be integrated with current approaches for function testing, inspection and follow-up. The new approach focuses on the following key aspects: (1) to avoid introducing CCFs during function testing and inspection, (2) to identify CCFs and CCF causes based on failure reports, and (3) to use the insight of failure causes to select efficient means to defend against future CCFs. The approach may be integrated into existing function testing and inspection related work processes, and has been designed to avoid any significant additional workload on plant workers. The approach builds on experience from the nuclear power industry (Hellstrøm, Johanson, & Bento, 2004; Hirschberg, 1991; Johanson et al., 2003; Parry, 1991; Paula et al., 1991; NUREG/CR-5460, 1990), the process industry (Summers & Raney, 1999), the oil and gas industry (Hauge et al., 2004, 2006) and own experience from maintaining SIS on oil and gas installations.

The CCF defense approach follows the main tasks of function testing and inspection that are described in Section 3 and illustrated in Fig. 2. The six activities are based on checklists and analytical methods like operational sequence diagrams (OSD), influence diagrams and cause-defense matrices.

Table 1
ICDE classification of common causes (NEA, 2004)

Classification of root causes	Classification of coupling factors
State of other components	Same/similar hardware
Design, manufacture or construction inadequacy	Hardware design
Human actions	System design
Maintenance	Hardware quality deficiency
Internal to component	Same/similar operational conditions
Procedure inadequacy	Maintenance/test schedule
Abnormal environmental stress	Maintenance/test procedure
Other	Maintenance/test staff
	Operation procedure
	Operation staff
	Same/similar environmental exposure
	Internal
	External
	Other

5.1. Task 1: ensure that necessary improvements are captured when scheduling

Scheduling of function test and inspection procedures is usually performed automatically and with predefined intervals by the maintenance management system. During the scheduling process, a work package is created specifying the type of resources, estimated number of hours needed to perform the work and the test procedure to be used. An important defense against CCFs is to ensure that any corrections and improvements to the test procedure are captured when new function test or inspection work packages are created.

5.2. Task 2: avoid introducing CCFs during preparation, execution, and restoration

Experience shows that CCFs are often introduced during maintenance due to human errors, erroneous procedures and deficient work processes (Hellstrøm et al., 2004; Pyy et al., 1997). Human errors may be deliberate actions (e.g., carelessness due to inappropriate understanding of the

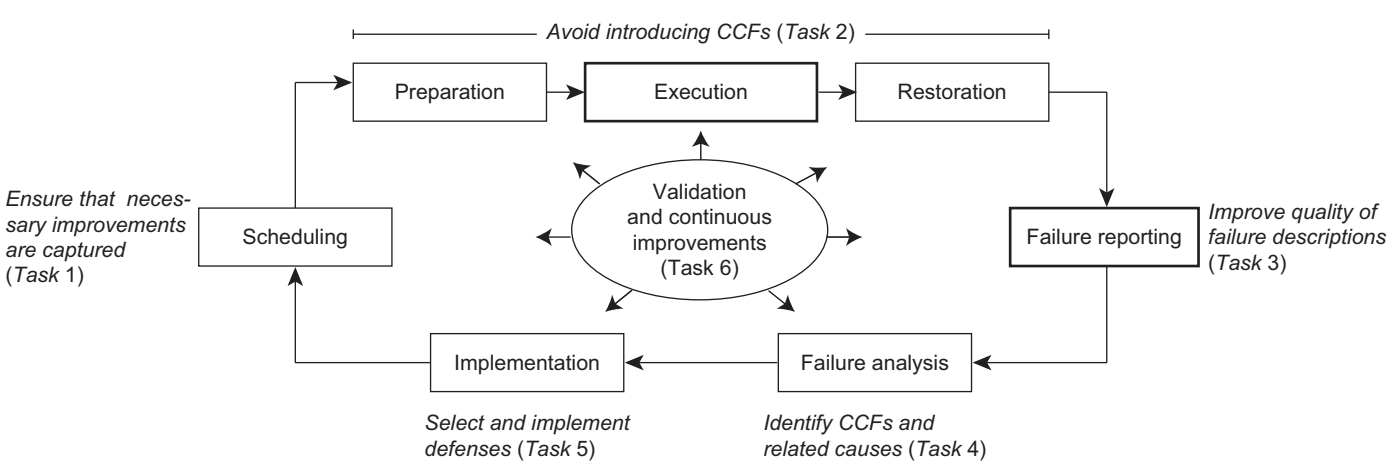

Fig. 2. Main concepts of the CCF defense approach.

risks involved), accidental omission (e.g., forgetting parts of the instructions or leaving components inadvertently inoperative), or inadequate execution of the prescribed instructions (e.g., improper adjustments, miscalibration of equipment, improper bypassing). Deficient work processes may lack adequate coordination between maintenance disciplines, be based on deficient procedures or inadequate selection of tools.

Recommended defenses should be applied by the field technicians, and comprise means to improve self-checking, improve work planning and preparation, improve the operability readiness control, increase the respect to procedures, and verify adequate training of personnel (Hellstrøm et al., 2004). During execution of the tasks it is required to maintain a high awareness to CCF causes.

Separate checklists are suggested for the three tasks: preparation, execution, and restoration. Often, similar components (e.g., pressure transmitters) within the same area are tested simultaneously. In this case, the preparation checklist may be applied once, while the execution and restoration checklist must be repeated for each component tested or inspected.

Checklist for preparation:

(1) Have potential human errors during execution and restoration been identified and discussed?
(2) Have human error incidents been experienced during previous execution?
(3) Have compensating measures been identified and implemented to avoid human errors?
(4) Are the personnel executing the test familiar with the testing and calibration tools?
(5) Are the calibration tools calibrated?
(6) Does the procedure have known deficiencies, like ambiguous instructions?
(7) Does the procedure describe necessary steps to safely restore the SIS?

Checklist for execution:

(1) Are the components operated within the specified environmental and operating conditions? (E.g., within the specified temperature or pressure range, humidity constraints, vibration constraints, flow composition, and so on.)
(2) Are the components protected against damage from nearby work activities?
(3) Are process connections free from plugging and (if relevant) heat-traced?
(4) Are all field SIS components (constituting the safety function being tested) labeled?
(5) Are additional components that are operated during SIS function testing and inspection sufficiently labeled?

Checklist for restoration:

(1) Has the physical restoration (e.g., isolation valves and bypasses) been verified (e.g, by a colleague)?
(2) Have all suspensions of inhibits and overrides been verified and communicated?
(3) Are any remaining inhibits, overrides or bypasses logged, and compensating measures identified and implemented?
(4) Has the safety function been verified before start-up?

Any question given an answer "no" indicates a deviation (or a potential cause) that may lead to a CCF. Deviations should therefore be discussed and compensating measures or corrections implemented.

5.3. Task 3: improve the quality of failure reporting

The maintenance management systems that are currently used in the oil and gas industry are not suited for direct recording of CCFs. CFFs have to be identified from the recorded single failure events. The nuclear industry applies a similar approach (Hirschberg, 1991). Unfortunately, the failure classification systems used for failure reporting have ambiguous taxonomy that may be interpreted differently by different persons. In addition, the failure classes are incomplete and insufficient to use for further in-depth analysis of failure causes. It is therefore necessary to record free text descriptions of failure causes, effects and detection methods in order to verify the initial failure classification and provide necessary information to decide whether or not a CCF has occurred.

Analysis of CCFs is not the only reason for using extra time on failure descriptions. Databases like OREDA (2002) also require access to more in-depth descriptions of failure causes and effects. Any deficient information may be difficult to collect at a later stage since the involved personnel may (due to offshore work schedules) be off for three or four weeks at a time.

A set of questions has been proposed for use by field technicians during failure recording, and may be added as default text in the input field for free-text description. The questions enable a more complete description of failures and failure causes.

Checklist questions for failure reporting:

(1) How was the failure discovered or observed? (Incidental, by diagnostics, during function testing, inspection or repair, upon a demand or by review/audit.)
(2) What is believed to be the cause(s) of failure? (Several possible explanations may be included.)
(3) What was the effect of the failure on the safety function? (Loss of complete function, degraded, none.)
(4) Was the component tested or inspected differently than described in the test or inspection procedure, and why was the approach different?
(5) Has the component been overexposed (operational or by environmental stresses), and if so, what may be the related causes?
(6) Have—to your knowledge—similar failures been experienced previously?

5.4. Task 4: identify CCFs through failure analysis

Failure analysis of recorded failures is usually performed by system or equipment responsible engineers. It is proposed to use failure reports generated by the maintenance management system to identify CCFs. This is in line with ISO 14224 (2006) and what is also done in the nuclear power industry (Hirschberg, 1991). The nuclear power plants have for several years collected and shared CCF data, through, for example, the ICDE project. Our main objective is to identify CCFs for the purpose of selecting appropriate and plant specific defenses. In light of ISO 14224 (2006), it may be required also to develop procedures and systems for collecting and sharing data on CCFs.

The starting point for the failure analysis is the failure reports and supplementary failure descriptions (free text) in the maintenance management system. It is suggested to identify CCFs through a four step process: (1) review the failure descriptions and verify (and if necessary correct) the initial failure classification, (2) perform an initial screening that captures failures that (a) have similar design or physical location, (b) share failure causes, (c) have been discovered within the same test or inspection interval, and (d) the failure causes are not random (as defined by IEC 61508, 1998 and IEC 61511, 2003), (3) perform a root cause and coupling factor analysis by using influence diagrams, and (4) list the root cause and coupling factors in a cause-defense matrix as shown in Table 2. Whereas corrective work packages are generated automatically when single failures are registered in the maintenance management system, step 1–step 4 must be performed as additional activities.

Step 1 is necessary for validating single failures as well as CFF causes and effects to ensure appropriate follow-up. Step 2 raises attention to failures that have common failure mechanisms, and that have not been detected by diagnostics. If failures detected by diagnostics are not repaired within a prescribed time, or if the same type of dangerous detected failures occurs rather frequently, they should be included in the analyses as well.

In step 3, it is proposed to identify the root causes and coupling factors by using a root cause and coupling factor analysis diagram. The main objective is to get more insight into the CCF causes, and thereby have a well-prepared basis for selecting suitable defenses. The analysis should be performed by a group of relevant personnel, rather than by individuals, and may include plant workers as well as engineers. A separate diagram may be constructed for each CCF identified in step 2. The root cause and coupling factor diagram may start with a description of the CCF, including the failure mode and the components having caused the failure, as shown in Fig. 3. The failure mode is the non-fulfillment of the required SIS performance. From there, the root cause and coupling factor diagram is drawn from right to left through iterative asking for underlying failure causes.

The CCF causes are always a result of a root cause and a coupling factor, indicated by an "and" gate in Fig. 3. In some cases it may, however, be difficult to determine the root causes (due to inadequate failure descriptions). In this case, one may focus on the coupling factors and still find adequate defenses against future CCFs. The analysis stops when no further insight into failure causes is available.

The diagram may also be used pro-actively, to identify failure causes that may lead to CCFs in the near future. In this case, one may extend the diagram with analysis of other relevant SIS components that may lead to loss of the safety function, as illustrated in Fig. 3 by dashed arrows and nodes. Relevant components may, in this context, mean redundant components. To identify potential failure causes, one may use a simple checklist of typical failure causes, for example the one shown in Table 1.

The application of the checklist may be illustrated for a pressure transmitter in a pipeline. A pressure transmitter performs the following subfunctions; to sense the pipeline pressure, convert the pressure reading to an analogue signal and transmit the pressure reading to the logic solver. Failure of one of the subfunctions leads to failure of the pressure transmitter. The root causes and coupling factors may be analyzed for each subfunction failure. The root causes of sensing failures may, for example,

Table 2
Simplified cause-defense matrix

CCF	Root cause	Coupling factor	Defense alternatives	R	C	Impact (H/L)	Cost (H/M/L)
Failure of ESD valves	Solenoid stuck due to pollution in hydraulic supply	Same design	Implement regular quality check of hydraulics	√	√	M	L
		Hook-up to same hydraulic supply	Installing filters in hydraulic supply	√		H	M
			Replacing existing solenoids with new and more robust ones				

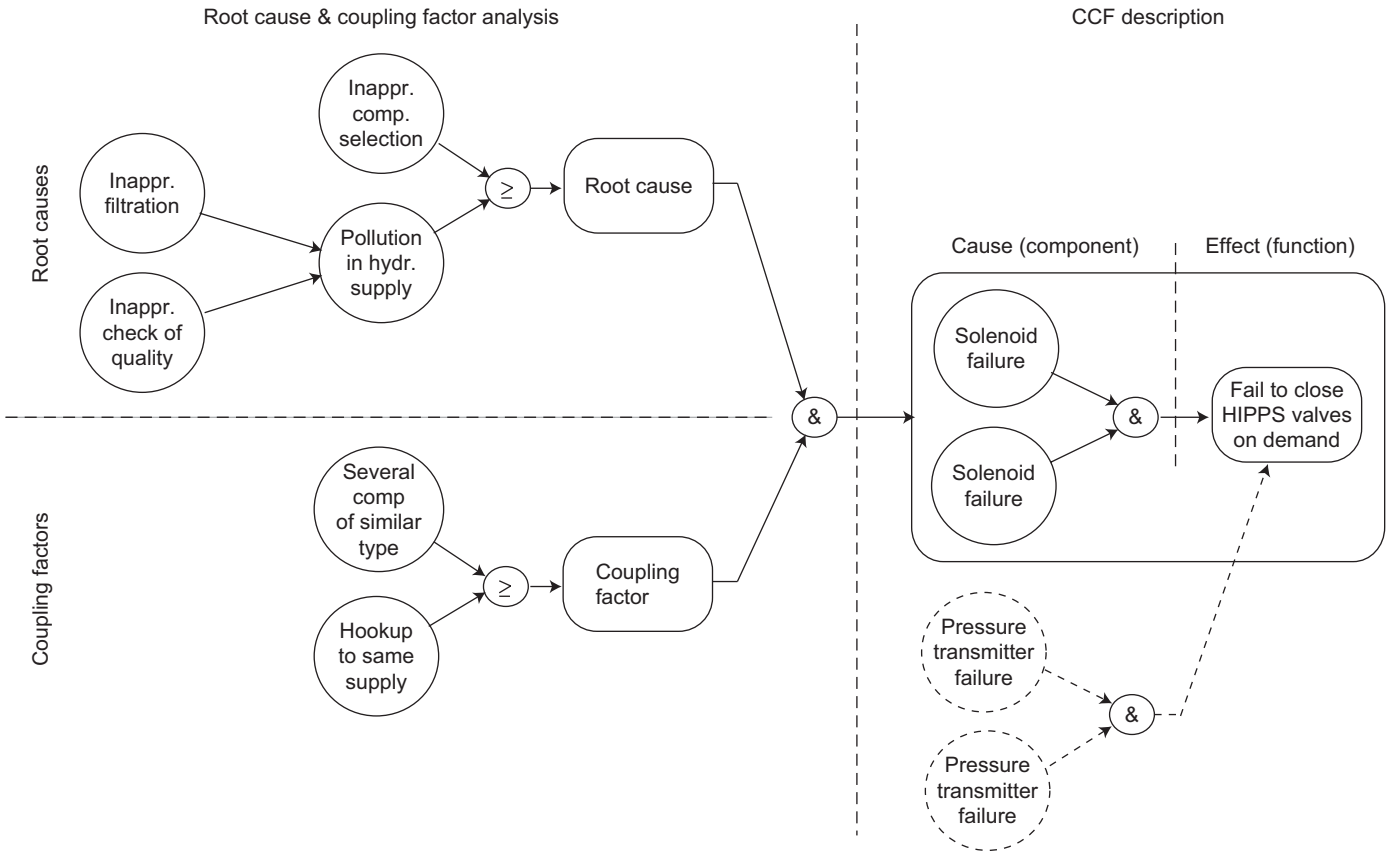

Fig. 3. Root cause and coupling factor analysis diagram.

be construction inadequacy (e.g., too small dimension of pressure sensing line) or human actions (e.g., leaving the transmitter isolated). Several pressure transmitters may fail simultaneously because the same inappropriate design is selected for all components, or they are tested using the same deficient procedure. This failure analysis process may be continued for all components and their related subfunctions.

The main results from the analysis, which are the root causes and the coupling factors, may be listed in a simplified cause-defense matrix, as illustrated in Table 2.

5.5. Task 5: implement defense measures

Implementation of CCF defense measures is important to prevent future occurrences of similar failures. In the nuclear industry, cause-defense matrices are used for detailed assessment of defenses (NUREG/CR-5460, 1990; Paula et al., 1991). In the cause-defense matrices, a set of predefined defenses are considered for each root cause and coupling factor. Several types of defenses are covered, like design related improvements, procedure related improvements, and physical barriers. The expected impact of all defense alternatives are evaluated, and used to rank their efficiency. In the nuclear power industry, the impact analysis is also used to estimate the rate of occurrence of CCFs, as input to the reliability models (e.g., see Mosleh, Parry, & Zikria, 1994). In the proposed CCF defense approach, it is recommended to apply a simplified cause-defence matrix, where simplified means that impact analysis is limited to a smaller selection of defense options.

The CCF defense approach applies the simplified cause-defense matrix in combination with a set of generic defense options, see Tables 2 and 3. The generic defense options have been adapted from NUREG/CR-5460 (1990) and Parry (1991). This list may be used in group discussions to suggest application specific defenses. The defense strategies "new procedure" and "improved quality control" may, for example, be used to derive the more specific defense strategy "regular quality checks of hydraulics".

It should be noted that the list of generic defense options does not include staggering of staff and staggered testing, even if these measures defend against CCFs (Summers & Raney, 1999). Offshore oil and gas installations are often scarcely manned, and staggered testing may be unrealistic to implement. In addition, it may be more complex to coordinate and more time consuming. However, in other applications staggered testing and staggering of staff may be relevant and should then be added to the list.

Each plant specific defense is evaluated with respect to protection impact (the ability to protect against future occurrences) and cost impact. The protection impact is evaluated qualitatively, as either high (H) or low (L), an approach which is also used in the more extensive cause-

Table 3
Generic defense options

Administrative control	Improved preparation Improved coordination Improved responsibilities Improved feedback of experience Improved safety culture Improved training Improved quality control
Documentation	Improved drawings Improved functional description
Procedures	New procedure Improved procedure text (clarification, added scope or information) Improved quality control of restoration Improved test tools and calibration
Monitoring and surveillance	New alarm or alert. Implementation must follow IEC 61508 (1998)/61511 (2003) New condition or logic sequence
Physical barriers	Improved physical support or fastening Improved physical protection
Hardware or software modifications of SIS	Modifications requiring design changes. Redesign following IEC 61508 (1998)/61511 (2003)

defense matrices for the nuclear industry (but with other symbols). The cost impact may be evaluated qualitatively (high (H), medium (M) or low (L)) or quantitatively (based on a cost estimate). If the costs are considered quantitatively, the cost impact may include design and installation costs or the life cycle costs. For each selected defense, it should be indicated if the root cause (R), the coupling factor (C) or both are affected. The information may be useful for assessing the estimated impact on reliability parameters, for example, the β-factor (in case the β-factor model is selected) or the dangerous failure rate. At the current stage, the CCF defense approach does not recommend how the reliability parameters should be updated.

5.6. Task 6: validation and continuous improvements

Systematic failures that may lead to CCFs, are not always captures through execution and follow-up of function testing and inspection. According to Summers and Raney (1999), the most critical cause of CCFs during SIS design and implementation is an erroneous or incomplete safety requirement specification. If, for example, an inadequate fire protection is specified, the detectors may fail to detect a real fire. The similar argument may be relevant for the operational phase; if the work processes, procedures, tools and competence are inappropriate for avoidance, identification and follow-up of CCFs, they may not provide the intended protection against CCFs. Validating all work tasks at regular intervals with respect to how they comply with the new approach may capture weaknesses and lead to continuous improvement. It may also be relevant to evaluate the effect of implemented defenses, either qualitatively or quantitatively.

The CCF defense approach suggests two new validation activities: (1) task analysis of function testing and inspection execution, and (2) use of a new validation checklist. The task analysis is suitable for capturing the causes of human interaction failures (Kirwan & Ainsworth, 1992), and the selected approach builds on operational sequence diagrams OSD as illustrated in Fig. 4. One may choose to concentrate on those work processes that are related to SIS components where CCFs or CCF causes have been experienced. The new validation checklist builds on the SIS life cycle checklists proposed by Summers and Raney (1999). Many oil and gas companies perform regular audits of, for example, SIS follow-up and performance. Some of the questions suggested for the validation checklist may therefore be covered by existing audit procedures.

Checklist questions for validation:

(1) Are requirements for the safety function covered by the function test or inspection procedure(s)?
(2) Are all disciplines involved in SIS testing, inspection, maintenance and follow-up familiar with the concept of CCFs?
(3) Are dangerous undetected failure modes known and sufficiently catered for in the function test and inspection procedures?
(4) Are the test limitations (compared to the real demand conditions) known?
(5) Are all redundant channels of the safety function covered by the function test or inspection procedures?
(6) Are failures introduced during function testing and inspection captured, analyzed and used to improve the associated procedures?
(7) Are failures detected upon real demands analyzed to verify that they would have been detected during a function test or inspection?
(8) Are changes in operating or environmental conditions captured and analyzed for necessary modifications to the SIS or related procedures?
(9) Are the calibration and test tools suitable and maintained according to the vendor recommendations?
(10) Are personnel using the calibration and test tools familiar with their application?
(11) Are procedure deficiencies communicated to the responsible persons and followed up?
(12) Are the diagnostic alarms followed up within the specified mean time to restoration?
(13) Are CCF systematically identified and analyzed, and defenses implemented to prevent their recurrence?

Questions given the answer "no" indicate a potential weakness in the defense against CCFs, and should be discussed to determine corrective actions.

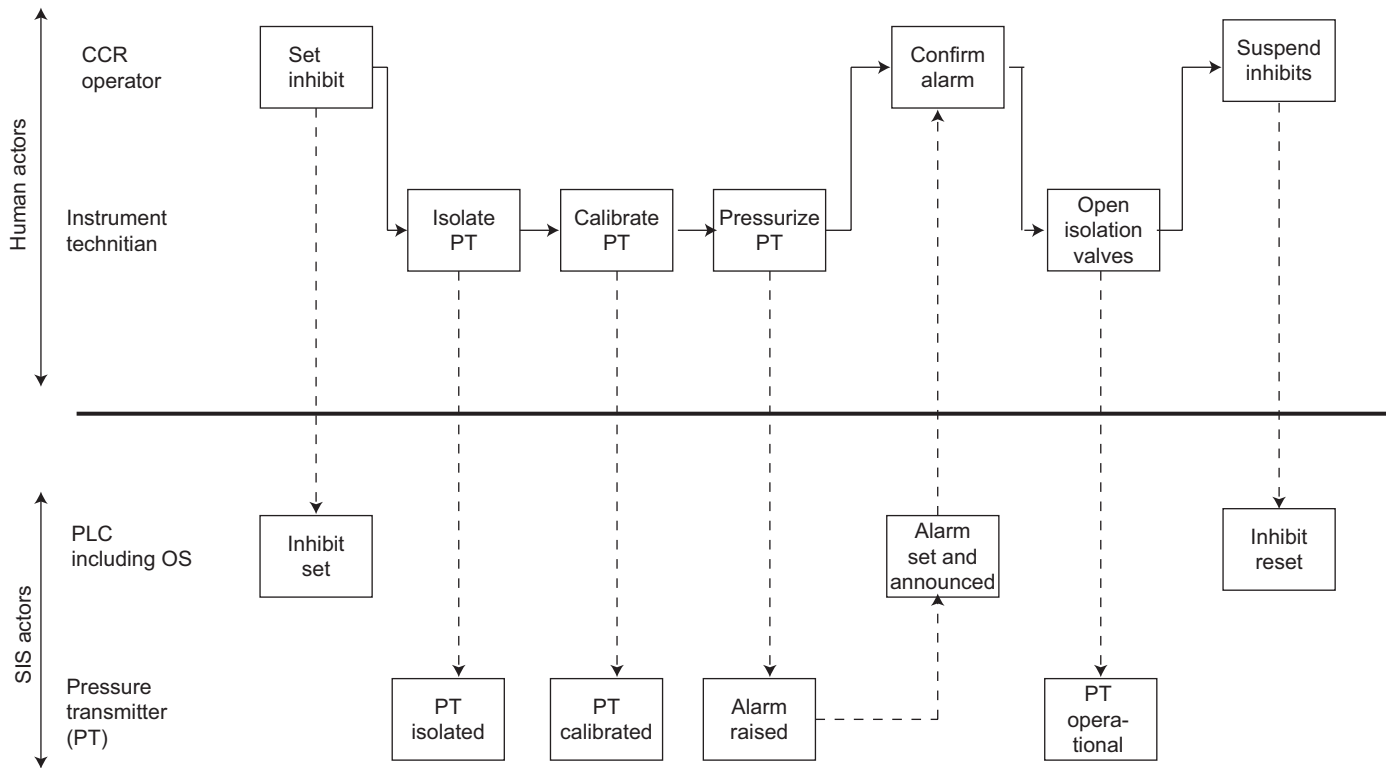

Fig. 4. OSD for function testing of pressure transmitters.

6. Discussion

The proposed CCF defense approach is based on a set of checklists and is supported by influence diagrams, task analyses, and simplified cause-defense matrices. The oil and gas industry is familiar with checklists that are used to initiate discussions on focus areas and identify deviations from regulations and engineering standards. One example is the crisis intervention and operability analysis (CRIOP) methodology that uses checklists to verify the design of offshore control centers (Johnsen et al., 2004).

Several important features related to the development of efficient checklists are discussed by Summers and Raney (1999), Summers, Raney, and Dejmek (1999), and Walker (1997). The questions must be relevant (so that they provide information on factors that are relevant to CCFs), complete (cover all relevant aspects of CCFs), specific (so that the attainable response is obtained), repeatable (so that the user gives the same answer when the question is repeated under similar circumstances) and reproducible (meaning that different users give the same answer under similar circumstances).

The CCF defense approach recommends that analyses of root causes and coupling factors are based on influence diagrams. Influence diagrams are suitable for qualitative as well as quantitative analyses (e.g., see Jensen, 2001). Methods like fault tree analysis, the modified FMEA analysis tool (Childs & Mosleh, 1999) and the failure classification sheets used in the nuclear power industry (Mosleh et al., 1994) may also be applied. Influence diagrams are, however, preferred since they give a simple illustration that is easy to grasp by practitioners. Cooper et al. (1993) recommend to skip the analysis of root causes, and rather focus on common failure mechanisms (which captures coupling factors). Their argument is that failure descriptions often lack sufficient information to determine the root causes, that the root causes may be interpreted differently by different people, and that the root causes are not as relevant for selecting efficient defenses against CCFs as the common failure mechanisms. In our approach, we have maintained the attention to defense tactics against root causes. However, if adequate failure descriptions are not available, one may limit the attention to the coupling factors.

A simplified cause-defense matrix has been selected rather than the more extensive version used in the nuclear power industry (Paula, 1990). To perform very detailed analysis of defense measures and their impact may not be realistic in the oil and gas industry that (at the current stage) does not use this information to estimate the CCF failure rates.

Task analysis may be used to verify that all relevant CCF causes are catered for in the checklists and procedures (e.g., see Davoudian, Wu, & Apostolakis, 1994). Task analysis is a method where the sequence of tasks, the role of the various actors and their way of communicating are analyzed. There are several approaches to task analysis (e.g., see Hendrick & Benner, 1987; Kirwan & Ainsworth, 1992). The concept of OSD has been selected for the CCF defense approach, since it is an intuitive way of visualizing

the communication between various actors, both humans and technology. The OSD is organized similar to a sequential timed events plotting (STEP), an approach that has proved to be efficient in similar applications (Sintef, 1998, 2003).

The current version of the CCF defense approach does not relate the efficiency of defenses to the reliability parameters. Several approaches may be considered for future extensions. One alternative is to wait and see if the failure reports indicate a reduced failure rate. Another alternative is to take credit for the expected effect, by estimating a new failure rate or a new β-factor. However, it may be difficult to determine if the reduction is due to a certain defense measure or to other factors. The failure rate may be updated following the approach, for example, by Vatn (2006) or Sintef (2006). To update the β-factor, the PDS method (Sintef, 2006), the betaplus method Smith and Simpson (2005), IEC 61508 (1998) β-factor checklists or the checklists developed by Humphreys (1987) may be applied.

Other effects from using the CCF defense approach that may be difficult to measure quantitatively is the increased awareness to the causes and effects of CCFs. Increased awareness may improve the detection of CCFs during execution and follow-up of function testing and inspection, and give more attention to how human interaction related failures may be avoided. The importance of maintaining independence between safety functions and redundant components may also be more evident to all actors working with SIS operation, maintenance, and follow-up.

7. Conclusions and ideas for further work

The CCF defense approach presents a practical implementation of defenses during the operational phase of oil and gas installations. It builds on generic and recognized methodologies combined with related research results and experience from other industry sectors. To our knowledge, a similar approach has not been developed, and may therefore be a valuable contribution for SIS follow-up. The approach has yet not been tested in real applications, but this type of testing will be performed and reported later.

A main limitation of the current version of the CCF defense approach is the lack of quantitative means to indicate any trends in the status of CCF defenses in the operational phase. This is therefore an important area for future research. There are several other ideas for further work. One obvious issue is to test the checklists and tools in the oil and gas industry, and analyze feedback for further improvements of the methodology. Another area is to consider alternative analytical techniques, for example, for analyzing the root causes and coupling factors. The recommendation by ISO 14224 (2006) to collect data on CCFs may also represent a challenge for the oil and gas industry data, and it may be important to develop common approaches to classification of CCFs. A last issue is to analyze new operational concepts and technology and how they may introduce new CCF causes. In the future, one may expect extensive use of automated function testing and new ways of human interaction that may introduce new stresses to technology as well as to humans and organizations.

Acknowledgments

We would like to acknowledge the RAMS group at the Department of Production and Quality Engineering at NTNU for valuable comments during development of this paper. We would also like to thank the anonymous referees for suggestions to improve the presentation of the paper.

References

Childs, J. A., & Mosleh, A. (1999). A modified FMEA tool to use in identifying and addressing common cause failure risks in industry. In *Annual reliability and maintainability symposium*, Washington, DC.

Cooper, S. E., Lofgren, E. V., Samanta, P. K., & Wong, S.-M. (1993). Dependent failure analysis of NPP data bases. *Nuclear Engineering and Design*, *142*, 137–153.

Davoudian, K., Wu, J.-S., & Apostolakis, G. (1994). Incorporating organizational factors into risk assessment through the analysis of work processes. *Reliability Engineering and System Safety*, *45*(1–2), 85–105.

Edwards, G. T., & Watson, I. A. (1979). *A study of common-mode failures*. Technical Report, UKAEA-SRD- R 146.

Hauge, S., Hokstad, P. R., Herrera, I., Onshus, T., & Langseth, H. (2004). *The impact of common cause failures in safety systems*. Technical Report STF38 F04410 (restricted), Sintef, Trondheim, Norway.

Hauge, S., Onshus, T., Øien, K., Grøtan, T. O., Holmstrøm, S., & Lundteigen, M. A. (2006) *Uavhengighet av sikkerhetssystemer offshore—status og utfordringer*. Technical Report STF50 A06011, SINTEF, Trondheim, Norway (in Norwegian).

Hellstrøm, P., Johanson, G., & Bento, J.-P. (2004). Dependency defence—How to protect against dependent failures. In *PSAM 7/ESREL*, Berlin, Berlin: Springer.

Hendrick, K., & Benner, L. (1987). *Investigating accidents with STEP*. New York: Marcel Dekker.

Hirschberg, S. (1991). Experiences from dependent failure analysis in nordic countries. *Reliability Engineering and System Safety*, *34*(3), 355–388.

HSE (2002). *Principles for proof testing of safety instrumented systems in the chemical industry* (*prepared by ABB Ltd for the HSE*). Technical Report 428/2002, Health and Safety Executive.

Humphreys, P., & Jenkins, A. M. (1991). Dependent failures developments. *Reliability Engineering and System Safety*, *34*(3), 417–427.

Humphreys, R. A. (1987). Assigning a numerical value to the beta factor common cause evaluation. In *Reliability'87: Proceedings of the sixth conference*, (pp. 2C/5/1–2C/5/8), Birmingham, UK.

IEC 61508. (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Part 1: General requirements. International Electrotechnical Commission, Geneva, 1998.

IEC 61511 (2003). *Functional safety—safety instrumented systems for the process industry*. Part 1: Framework, definitions, system, hardware and software requirements. International Electrotechnical Commission, Geneva, 2003.

ISO 14224 (2006). *Petroleum, petrochemical and natural gas industries—collection and exchange of reliability and maintenance data for equipment*. International Standardization Organization, Geneva, 2006.

Jensen, F. V. (2001). *Bayesian networks and decision graphs*. New York: Springer.

Johanson, G., Hellstrøm, P., Mankamo, T., Bento, J. P., Knochenhauer, M., & Pörn, K. (2003). *Dependency defence and dependency analysis guidance—Volume 2: Appendix 3-18 How to analyse and protect against dependent failures. Summary report of the Nordic Working group on Common Cause Failure Analysis*. Swedish Nuclear Inspectorate (SKI).

Johnsen, S. O., Bjørkli, C., Steiro, T., Fartum, F., Haukenes, H., Ramberg, J., et al. (2004). *CRIOP: A scenario method for crisis intervention and operability analysis*. Technical Report STF38 A03424, Sintef, Trondheim, Norway.

Johnsen, S. O., Lundteigen, M. A., Fartun, H., & Monsen, J. (2005). Identification and reduction of risk in remote operations of offshore oil and gas installations. In *ESREL'05* (pp. 957–964). Balkema.

Kirwan, B., & Ainsworth, L. K. (1992). *A guide to task analysis*. London: Taylor & Francis.

Langseth, H., Haugen, K., & Sandtorv, H. A. (1998). Analysis of OREDA data for maintenance optimisation. *Reliability Engineering and System Safety*, *60*(2), 103–110.

Lundteigen, M. A., & Rausand, M. (2007). The effect of partial stroke testing on the reliability of safety valves. In *ESREL'07*, Stavanger, Norway.

Mosleh, A., Parry, G. W., & Zikria, A. F. (1994). An approach to the analysis of common cause failure data for plant-specific application. *Nuclear Engineering and Design*, *150*(1), 25–47.

NEA (2004). *ICDE Project Report: Collection and analysis of common-cause failure of emergency diesel generators*. Number NEA/CSNI/R(2000)20. Nuclear Energy Agency.

NEA (2002). *ICDE Project Report: Collection and analysis of common-cause failures of safety and relief valves*. Number NEA/CSNI/R(2002)19. Nuclear Energy Agency.

NEA (2003). *ICDE Project Report: Collection and analysis of common-cause failures of check valves*. Number NEA/CSNI/R(2003)15. Nuclear Energy Agency.

NEA (2004). *International common-cause failure data exchange*. ICDE general coding guideline – technical note. Number NEA/CSNI/R(2004)4. Nuclear Energy Agency.

NUREG/CR-5460 (1990). *A cause-defense approach to the understanding and analysis of common cause failures*. Nuclear Regulatory Commission, Washington, DC.

NUREG/CR-5485 (1998). *Guidelines on modeling common-cause failures in probabilistic risk assessment*. Nuclear Regulatory Commission, Washington, DC.

OLF-070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. The Norwegian Oil Industry Association.

OREDA (2002). *OREDA reliability data*. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, (4th ed.).

Parry, G. W. (1991). Common cause failure analysis: a critique and some suggestions. *Reliability Engineering and System Safety*, *34*, 309–326.

Paula, H. M. (1990). Data base features that are needed to support common-cause failure analysis and prevention. An analyst's perspective. *Nuclear Safety*, *31*(2), 159–173.

Paula, H. M., Campbell, D. J., & Rasmuson, D. M. (1991). Qualitative cause-defense matrices; engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering and System Safety*, *34*(3), 389–415.

Pyy, P., Laakso, K., & Reiman, L. (1997). *A study of human errors related to NPP maintenance activities*. IEEE Sixth annual human factors meeting (pp. 12–23).

Rausand, M., & Høyland, A. (2004). *System reliability theory; models, statistical methods and applications* (2nd ed.). New York: Wiley.

Sandtorv, H. A., Hokstad, P. R., & Thompson, D. W. (1996). Practical experiences with a data collection project: The OREDA project. *Reliability Engineering and System Safety*, *51*(2), 159–167.

Sintef (1998). *Methods for safety analysis in railway systems*. Technical Report STF48 A98426, Sintef, Trondheim, Norway.

Sintef (2003). *Morgendagens HMS-analyser for vurdering av tekniske og organisatoriske endringer*. Technical Report STF38 A02423, Sintef, Trondheim, Norway (in Norwegian).

Sintef (2006). *Reliability prediction methods for safety instrumented systems—PDS method handbook*. SINTEF, Trondheim, Norway.

Sklet, S. (2006). Safety barriers: Definition classification and performance. *Journal of Loss Prevention in the Process Industries*, *19*(5), 494–506.

Smith, A. M., & Watson, I. A. (1980). Common cause failures—a dilemma in perspective. *Reliability Engineering*, *1*(2), 127–142.

Smith, D. J., & Simpson, K. G. L. (2005). *Functional safety—A straightforward guide to applying the IEC 61508 and related standards*. Burlington, UK: Elsevier.

Summers, A. E., & Raney, G. (1999). Common cause and common sense, designing failure out of your safety instrumented system (SIS). *ISA Transactions*, *38*, 291–299.

Summers, A., & Zachary, B. (2000). Partial-stroke testing of block valves. *Control Engineering*, *47*(12), 87–89.

Summers, A. E., Raney, G., & Dejmek, K. A. (1999). Safeguard safety instrumented systems. *Chemical Engineering Progress*, *95*(11), 85–90.

Vatn, J. (2006). Procedures for updating test intervals based on experience data. In *ESReDa Conference*, Trondheim, Norway.

Walker, A. J. (1997). Quality management applied to the development of a national checklist for ISO 9001 audits for software. In *Proceedings of the IEEE international software engineering standards symposium*, Walnut Creek, USA. IEEE.

Watson, I. A., & Edwards, G. T. (1979). Common-mode failures in redundancy systems. *Nuclear Technology*, *46*(2), 183–191.