NTNU
Norwegian University of
Science and Technology

Inhibits and Overrides

Applications Seen in a Safety Perspective

Anders Freddy Johansen

Master of Science in Engineering Cybernetics
Submission date: June 2011
Supervisor: Tor Engebret Onshus, ITK

Norwegian University of Science and Technology
Department of Engineering Cybernetics

NTNU – Trondheim
Norwegian University of
Science and Technology

Problem description

Premise:

Safety and Automation Systems (SAS) provide means that permit easy implementation and further use of inhibits and overrides during most operating conditions. These facilities may prove beneficial during many operating conditions but, at the same time, can impose serious threats against safe operation.

Objective:

A survey will be launched with the purpose of collecting information regarding usage of inhibits/overrides on some randomly selected installations. An in-depth analysis of the data will be executed in order to assess and present issues of:

- statistics; e.g. number of inhibits/overrides during different time intervals, duration, appearance of same tags, simultaneous inhibits/overrides of redundant functions, etc.
- comparison between installations/shift/personnel
- compliance with procedures/adequacy of procedures
- level of safety threats

Assignment given: January 10, 2011

Supervisor: Professor Tor Onshus

Abstract

The main purpose of this thesis has been to identify the general usage of the applications *inhibit* and *override* for a collection of installations operated by Statoil ASA. The applications are provided by a Safety and Automation System (SAS) that performs monitoring, control and safeguarding of the plant and its process. Logs that keep track of the SAS operator's actions and other facility-related events have been received from each installation, and regarded with respect to:

- the general evolvement and trend of the application usage
- instances of inhibits/overrides of long-term character
- redundant signals that are inhibited/overridden simultaneously
- critical time periods that exhibit high activity
- tags that are frequently involved in the application usage

The results that were obtained for each above-mentioned point made it possible to give a stetement of how the installations are controlled through utilization of the safety-impairing, but useful applications.

Preface

The process of producing a master's thesis is very complex and extensive. No less, it is also an interesting process characterized by growth in knowledge and self-confidence. When one realizes that one is capable of submitting a complete master's thesis, one grows as a person and experiences acknowledgement upon own abilities.

A part of the reason for why I became motivated for investigating the issue of safety in light of operator appearance, is the fact that accidents and disasters related to oil production units often tend to affect so many groups of people, in addition to harming animals and damaging nature. Especially, it was the oil spill taking place in the Gulf of Mexico (Deepwater Horizon, British Petroleum (BP)) that engaged me personally.

I wish to thank my supervisor Professor Tor Onshus at the Department of Engineering Cybernetics, Norwegian University of Science and Technology for his assistance during the period of writing.

I would also like to thank my co-supervisor in Statoil, Jan S. Austbø, for his advisory contributions.

Special thanks are given to the helpful Statoil employees Eivind B. Sandsmark, Henry Strøm, Hein Kolstø and Kjell A. Halvorsen for their efforts in obtaining experimental data from the various installations, and incidentally for their supportive work.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Earlier work

This thesis can be regarded as a continuation of [6], which is a paper that was conducted as a solution to a project assignment given in the fall semester of 2010. The problem that was addressed then is generally the same problem that shall be treated here, but there are some differences that are important to emphasize:

- All the previous work that was done in [6] was solely based on *one single* event log. Now, however, up to six event logs originating from six distinct oil production units are being considered in the analysis. This opens up for more valuable interpretation of the results, because of the now-existing comparison opportunities.

- Other, more orderly and descriptive methods have now been utilized in the presentation of the results, compared to earlier work. In addition, a completely new aspect of analysis is proposed; the weekly usage of inhibits/overrides is kept track of, hence making it possible to detect potential patterns/trends in the way the operators carry out realizations of the applications. Moreover, key statistical quantities related to these collected data are introduced.

Because the only available data at the time [6] was written were logs containing overviews of all the historical instances of inhibits and overrides, it (then) appeared natural to focus on individual cases of, for example, long-term incidents. It turns out that conclusions that are drawn exclusively on the basis of such kind of information, in the end can prove to be invalid. This is due to the lack of information concerning compensating measures or other initiatives taken by the operating crew in relation to every realization of an

impairing event. Because of this, it will no longer be drawn any "uncertain" conclusions, but instead emphasized to create an overall, general image of the situations at the different installations.

1.2 Motivation

It is widely known that manipulation of the control of a plant's production process through utilization of functionalities such as inhibit and override, may lead to potentially dangerous situations. Still, it is important for an operator to be in possession of the ability to apply such applications to certain signals if necessary, as shall be argued for in later sections. However, what is fundamental if the level of safety at an installation is reduced, is that the operator and other responsible personnel are aware of the weakenings and consequently deal with them.

The main motivational factor for carrying out a survey of the general usage of inhibits/ovrrides at different petroleum installations, is the knowledge that these applications have the capability of acting as a direct or indirect cause to an accident. The long-tail effects of such disasters usually involve massive environmental damage (including damage to the local wildlife), while the immediate response often is given in terms of loss of human lives and damage to equipment. If disastrous cases of inhibits/overrides were completely eliminated, several historical accidents could have been avoided. This shall be supported later through the demonstration of an example. The survey that has been done in this thesis will identify the general usage of the aforementioned applications, hence reflecting the characteristic evolvement of the various situations (based on the received logs). After having established familiarization with the results, Statoil will be able to address thoroughly processed data, allowing for follow-up activities on their initiative. Through possible revisions of operator procedures on the related field, the results may have impact on the daily operational activities at the installations.

1.3 Thesis outline

The dissertation has been conducted with the root objective that the topics shall be presented in a natural succession and order, in addition to provide the reader with a guiding line that can be followed through the entire thesis; from introduction through conclusion. It has also been emphasized to keep the reader within the frames of the work, so that no larger digressions steal

the focus of attention. The thesis does not assume that the reader possesses any great knowledge within the field of SAS and safety, hence sufficient reviews of theory will be made on the topic in advance of the presentation of the reuslts.

In Chapter 2, the required portion of theory is introduced, starting off by diving into the answer to how an SAS is structured and how it works; its constellation and functionality. In the same chapter, the core facilities *inhibit* and *override* will be explained very carefully, i.e. all the aspects related to their functionality and usage, risks and areas of application. This is then embraced by the presentation of standards and regulations associated with their signification in practice. In order to relate all of this to reality, it is provided an example of an actual accident as a consequence of improper application usage.

Chapter 3 presents an overview of the installations that have been included in the analysis, in addition to regarding some aspects related to the nature of the problem that had to be taken into consideration on beforehand of the examination of the data. In this chapter, also the methods that were used to solve the different sub-problems are explained, followed by the actual problem statement itself and presentation of the assumptions that were made.

Finally, in Chapter 4, the results of the analytical work are revealed together with their accompanying individual discussions, before it is all wrapped up by stating some concluding remarks about the findings (Chapter 5). For future work that is either based on this thesis' problem or results, some recommendations and suggestions to interesting aspects that may be taken into account are made, also in Chapter 5.

Chapter 2

Theory and background

This chapter goes through all the background theory that is necessary for the reader to be familiarized with in order to be capable of properly interpreting the results that will later be presented. It will be started off on a basic level by presenting what an SAS is and how it works, before it is narrowed down to address detailed theory related to the applications inhibit and override. First of all, acquaintance shall be made with the fundamental composition and structure of an SAS.

2.1 Safety and Automation System (SAS)

An SAS performs monitoring, logic control and safeguarding of an installation [1]. Roughly divided, an SAS consists of three types of elements; sensors, logic solvers and final control elements. Their composition is illustrated in Figure 2.1. A consideration of the following example will help a person who does not possess any significant background knowledge on the topic to gain some insight to how an SAS actually operates: a flow meter measures the immediate flow in a pipe and sends the information over to a microcontroller. The microcontroller proceeds by processing the received information and accordingly makes decisions on what should be done depending on the given value of the flow. After the solver has finished the comparison between immediate flow and stipulated flow limits, an output signal is generated on the basis of the outcome of the comparison, and sent to the valve governing the pipe flow. The servomechanism located on the valve (actuator) is activated, and the response action to the measured flow state is carried out through position adjustment of the specific valve.

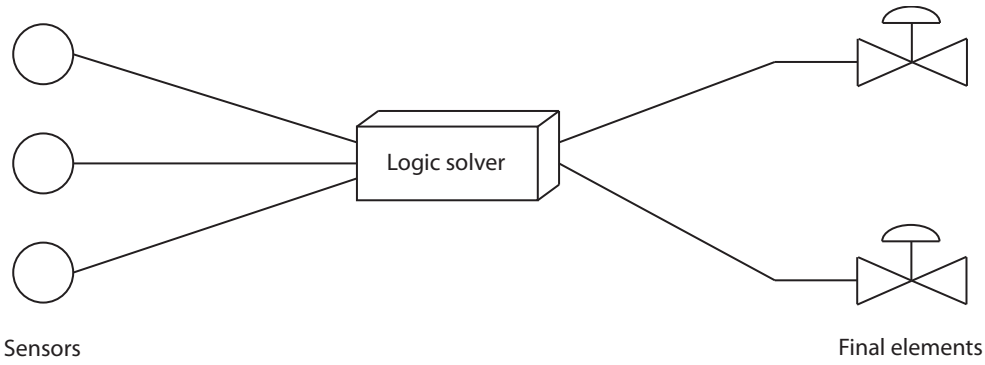

Figure 2.1: SAS composition.

As shall be seen later in this thesis, regulations and standards, design approaches, etc. that apply to development of Safety Instrumented Systems (SIS) are used on an equal footing in the development process of SASs. This is because the SIS can be said to be *part of* the SAS, hence both systems are subject to the same governing documents when it comes to safety level requirements. Also integrated in the SAS is the system responsible for controlling the plant process - the Process Control System (PCS). The approach where the SIS and the PCS are combined into one large system versus the other approach where they are separated, can be viewed in Figure 2.2. A PCS may be based on a bunch of different control strategies depending on the nature and characteristics of the particular process (internal dynamics), but some of the most popular and well-established methods within the field of process control can be listed without taking into account the process dynamics: optimal control (such as Model Predictive Control (MPC)), adaptive control (such as Certainty Equivalence Control (CEC)) and robust control (such as H_∞-control).

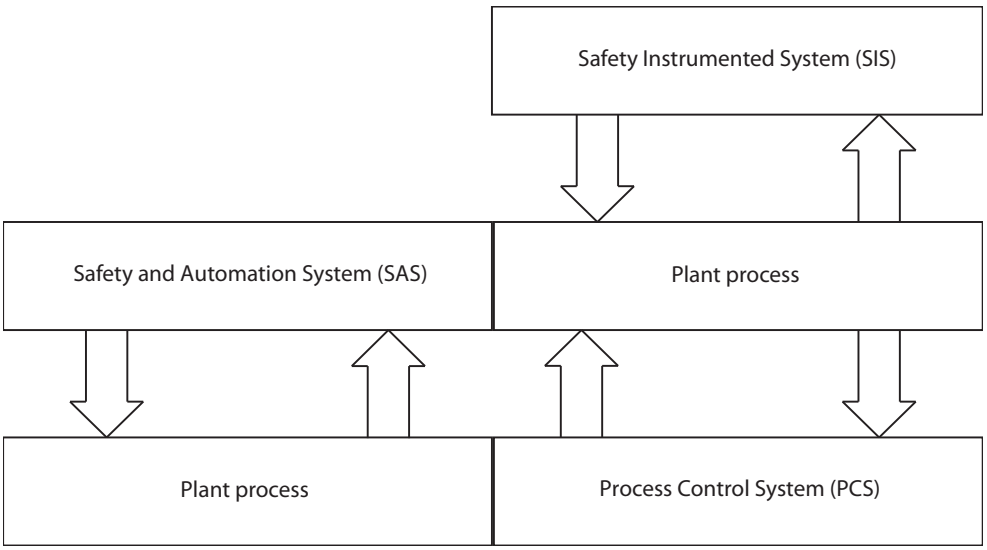

Figure 2.2: Alternative system architectures.

The merger of the two systems into a single, larger system, has brought with it both advantages and disadvantages on different levels of operation. Naturally, it is more practical for the operators to only have interference with one single operator station when operator action is demanded by the system or when the operator himself/herself wants to take some kind of action (for example to adjust a setpoint value), instead of being forced to make engagements through several stations which often have their own, individual Human Machine Interfaces (HMI). However, this beneficial aspect directly results in a major drawback that should be noted: due to the joint usage of hardware and software in the operator stations, a failure in either one of the two will affect both the PCS and SIS interface. In other words, the merger brings with it a common point of failure, hence less robust systems are especially vulnerable. This should be taken into consideration by the system designers in an early phase of the process.

The issue of independence between safety systems offshore has been studied closer by Hauge *et al.* in [7], and it is appropriate to reproduce some of the key findings that were made there. It was generally found that signals were sent from subordinate protection layers to their respective superior protection layers (e.g. signal flow from Process Shutdown Systems (PSD) to Emergency Shutdown Systems (ESD)). This practice shall ideally not occur since a risk for evolvement of failure-propagation from subordinate to superior layers will consequently arise, thus the main, fundamental purpose of the hierarchy division will be lost. Furthermore, it was in some cases seen

that safety-critical instrumented functions were implemented as a part of the PCS, and not as a part of the SIS. This is in conflict with an important demand for independence between control systems and safety systems made by The Petroleum Safety Authority Norway (PSA). This shall be debated more carefully in later sections that regard the topic of standards and regulations. There exists a large number of documents that make demands to all kinds of things related to SASs operation, and that are very important for institutions that are involved in the oil industry to comply with. Other findings concerning independence between the PCS and SIS were also made, for example that the two systems often shared communication network and other hardware, where heavy traffic from one of the two systems could lead to trouble for the other. However, the reader is referred to [7] for a more detailed overview.

2.2 Conceptual SAS topology

Norsk Sokkels Konkurranseposisjon's (NORSOK) standard I-002 presents a clear and conceptual SAS topology in one of its annexes (Annex C). It is intended as an informative annex, but the described way of arranging the overall system together seems to appeal to many system designers, and appears as the most common way of solving the SAS topology problem. The structure is presented in Figure 2.3, and will be reviewed in a step-by-step manner below. Incidentally, NORSOK is an organization that issues a set of standards which are administered through an organization named Standards Norway (SN), in order to assure adequate safety, value adding and cost effectiveness for the petroleum industry on Norwegian continental shelf.

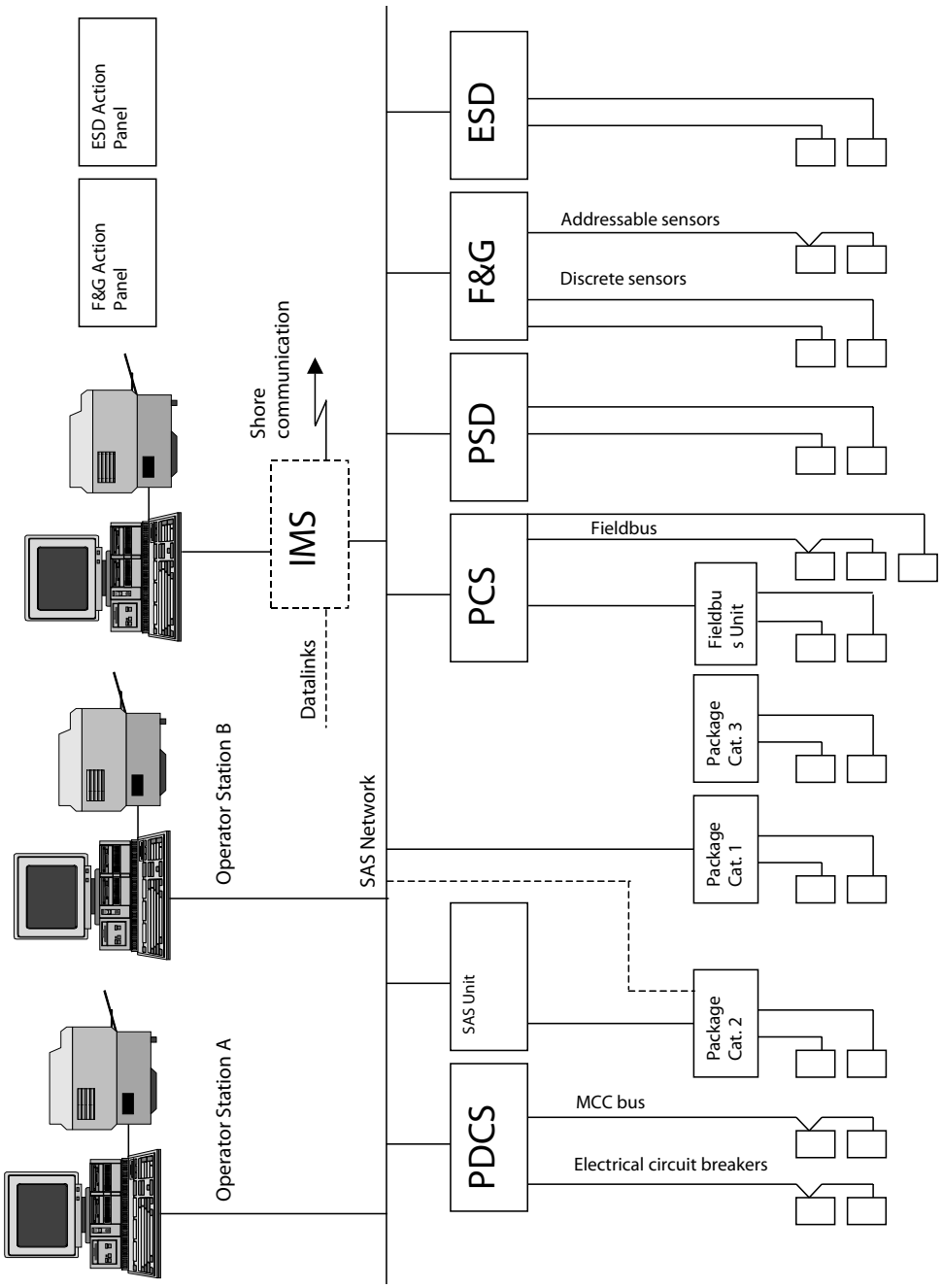

Figure 2.3: Conceptual SAS topology, as presented in [1].

In this example, it is assumed that the total system is equipped with two operator stations (A and B, respectively), as well as an Information Management System (IMS) station. The IMS is used exclusively for presentation of information and storage of event data [1]. It should not be possible to take actions upon any process control or safeguarding equipment through the IMS interface. Nevertheless, it will have the same access rights (in terms of reading access, not writing) as the operator stations due to the shared SAS network. It will also be possible to pass on the collected information further into an onshore location as demonstrated by the drawing.

Connected to the SAS network are multiple subsystems which can be controlled individually from the operator stations or from action panels. Two of the most critical parts of the safety system, the Fire & Gas System (F&G) and Emergency Shutdown System (ESD), are typically provided the action panels. The main mission of the ESD is to prevent abnormal conditions at the facility to escalate into major hazards. When an hazardous situation first has taken place, the ESD shall also limit the extent of damage. The F&G shall continuously monitor for the presence of gasses that may be toxic or lead to fire/explosion, in addition to monitoring for actual fires, so that the personnel have the opportunity to be alerted in advance of a potential dangerous event [8]. This is achieved by using addressable discrete sensors, as shown in the figure. The advantage addressable sensors have over non-addressable sensors is that the firefighters are able to find out exactly where the abnormal fire/gas situation is evolving, as each sensor is assigned a unique address. Additionally, if the sensor is analog, the quantity of fire or gas will be known as well.

Moreover, it can be seen that the Process Shutdown System (PSD) and Process Control System (PCS) are hooked up to the SAS network. The PSD's main task is to monitor and safeguard the core of the production process and consequently take action if abnormal conditions are detected. If the situation gets bad enough, the ESD may invoke the PSD to shut down the whole or parts of the process. Next in line is the PCS which is controlling the plant process to behave according to operator specifications, so that desired process outcomes are obtained. Fieldbus is typically used in the communication between the PCS and the belonging network of controllers. This is a type of communication network that has a number of advantages, but explaining these in detail is outside the scope of this thesis. The reader is referred to [9] for more information on the topic of automation networks.

Another important part of the overall facility control system is the Power

Distribution Control System (PDCS) which controls and monitors the electric power generation and distribution network supplying the facility [1]. It is critical to achieve a well-behaved control of both frequency and amplitude of the power that goes out to the site apparatus, since incorrectly supplied instruments may be damaged. To ensure that this is not happening, electrical circuit breakers are installed as a part of the package acting as a barrier against the danger. The circuit breakers will break the electrical circuit so that plant apparatus is not supplied with current containing spikes or other damaging phenomena. Also communicating with the PDCS is the Motor Control Center (MCC). This is a center which masters the many electric motors that are spread around the entire installation.

2.3 The life-cycle of a safety-related system

International Electrotechnical Commission's (IEC) standard IEC 61508 presents a technical framework for the developmental process of a safety-related system in terms of an overall safety life-cycle. The life-cycle describes "the life" of a safety system from birth to death, and contains 16 individual phases. The model is so well-established in the industry that it is worth taking a deeper dive into the thoughts that lie behind its existence. It is intuitive and easy to understand, and has been used frequently by system developers as a guideline since the time it was first published. IEC 61508 is a reputable and well-known international standard together with its close related IEC 61511, which shall be considered in a later section. It is a generic standard, which means that it is applicable to all Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems, regardless of application.

In general, IEC is a non-profit-making organization that releases international standards in relation to electrotechnologic devices and systems. These standards often serve as a basis for further national standards that are generated inside each country. In Norway, The Norwegian Oil Industry Association (OLF) publishes the document OLF-070 which is a guideline to how to use and implement IEC 61508 and IEC 61511 on petroleum installations on Norwegian continental shelf. This can be read more about in Appendix B. The overall safety life-cycle that have been spoken of above is reproduced in Figure 2.4. Each of the phases will be explained in more detail beneath the figure.

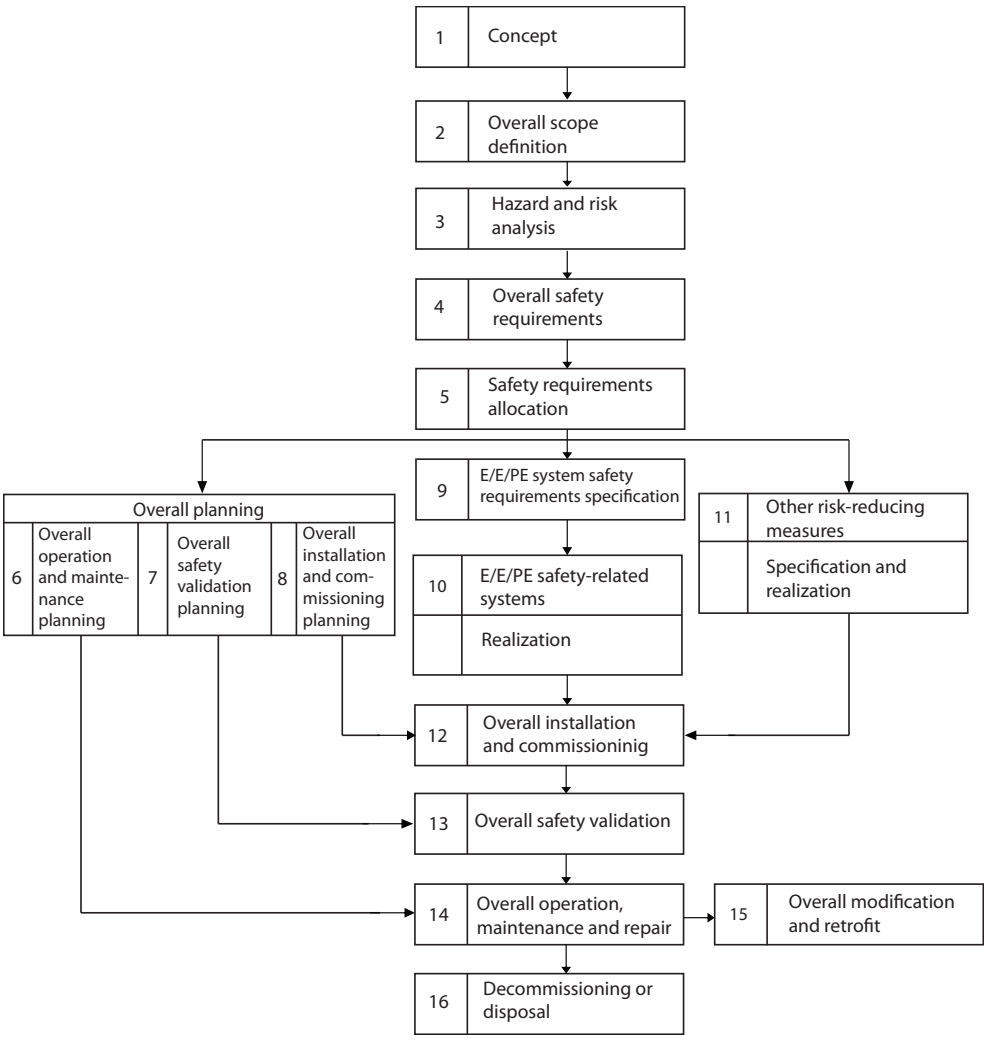

Figure 2.4: The overall safety life-cycle, as presented in [2].

It is very important to obtain a sufficient level of understanding with respect to the Equipment Under Control (EUC) and its environment. This is the scope of phase one in the cycle. The EUC is basically all the equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities [2]. In other words, all the parts that are included in the overall system. When this is completed, the standard suggests that the developers define the overall scope of the safety-related system, something that can be done by determining where to place the boundary that separates the EUC from the EUC control system. The EUC control system bases its outputs on inputs from the plant process and relevant setpoints, and aims to control the available EUC such that the total system attains a

desirable behavior. Then, maybe the most critical phase of them all follows; hazard and risk analysis. During this phase, all possible hazards that may arise from consecutive event sequences are to be determined, together with the EUC risks associated with them. Obviously, this is a complex process, but it is very important that nothing is left to chance and that all possible operating conditions/circumstances are incorporated in the analysis.

When the safety-related system's development team has given an account of all the practicable unsafe outcomes in the system, they can carry on the process by developing requirement specifications for the overall system, and accordingly assign/allocate Safety Functions (SF) to each and every one of them. This is phase four and five, respectively. When the first five phases are successfully carried through with by the team, the analysis part of the design process is over. Henceforth, the issues of planning, realization and operation are considered. This involves planning and development of procedures that address operation and maintenance (phase six), validation (phase seven) and installation and commissioning (phase eight). It is important that this work is done very carefully, as procedures that are precise and easy to interpret can save the responsible company for time and trouble (and thus costs).

When this is done on an holistic basis, the attention can be paid to the E/E/PE part of the safety-related system (referred to as the SIS/SAS in this thesis). Phase nine concentrates on defining a Safety Requirement Specification (SRS) in terms of the already defined SFs for the SAS, while Phase 10 is concerning the actual realization of the SAS so that the requirements and demands to the system are fulfilled. If it turns out that the SAS is not sufficient (but only necessary) in order to meet the specified requirements, other risk-reducing measures must be considered as well to fill in for the gaps. This is done in Phase 11.

Furthermore, the physical installation, commissioning, and then validation and daily operation follow. All of these activities are done according to procedures developed in the earlier phases, and are treated in Phase 12, 13 and 14 respectively. If the buyers are satisfied with the existing distributor, they can request a retrofit. This requires parts of the hardware and/or software to be replaced and renewed. This is, of course, assuming that upgrades are available on the market. Often, a reason for a company to carry out a retrofit is that the authorities that verify the systems - the classification societies - require new features or safety measures in their verification procedures. At the end of an SAS life, decommissioning is eventually carried out and it can again be started at phase one in the life-cycle if a new safety-related system

is to be developed (of course making use of the knowledge that was gained during the developmental process of the earlier SASs).

Something else that must be considered during system design, and which also is a term presented in IEC 61508, is Safety Integrity Level (SIL). This is a statistical measure of the safety-related system's capability of carrying out a safegurading action on demand from the process [2]. In Figure 2.5, the four levels of safety integrity are presented, where a function holding a level of safety integrity four is approved for maximum safety and SIL 1 represents the lowest level of safety. The SIL concept is used, among others, by the authoroties to specify their requirements for safety related to various safety functions distributed for different purposes around the facility. For certain safety functions a higher probability for that the corresponding safeguarding action will be carried out on process demand may be required, for example in the case of process shutdown due to the scenario of abnormal pressure conditions in a tank, for example. For other, less critical functions, a SIL of 1 may be adequate/sufficient. If the above-mentioned guideline OLF-070 is complied with during system design, a minimum level of safety integrity will be provided for the overall system. In some cases, it may have a reassuring effect to dedicate a safety function a higher SIL than what is required by the authorities. However, often it is necessary to just meet the minimum requirements in order to minimize costs.

Safety Integrity Level	Low Demand Mode of Operation (Pr. of failure to perform its safety functions on demand)	Continuous/High-demand Mode of Operation (Pr. of dangerous failure per hour)
4	>= 10^{-5} to 10^{-4}	>= 10^{-9} to 10^{-8}
3	>= 10^{-4} to 10^{-3}	>= 10^{-8} to 10^{-7}
2	>= 10^{-3} to 10^{-2}	>= 10^{-7} to 10^{-6}
1	>= 10^{-2} to 10^{-1}	>= 10^{-6} to 10^{-5}

Figure 2.5: SIL table, as given in [2].

2.3.1 IEC 61511's role in the cycle

While IEC 61508 is a standard concerning safety-related systems in general, IEC 61511 is a more specific standard which exclusively concentrates on the SIS's role in the safety hierarchy. Simply, it can be said that it is a process sector implementation of IEC 61508. Exactly like its "parental standard", also this standard exhibits a safety life-cycle in order to spread its message and guide SIS developers on their way in developing an SIS whose measures

are in accordance with given safety regulations. Besides that the life-cycle-focus of IEC 61508 is on the overall system and that the life-cycle-focus of IEC 61511 is on the SIS, the two life-cycles are approximately identical, thus a reconstruction of the latter will not be presented in this section. By just imagining that the one presented in Figure 2.4 also applies to the evolutionary process of an SIS, a parallel can be drawn intuitively.

The standard makes explicit demands to the specification, design, installation, operation and maintenance phases of the SIS through clauses that are stated sequentially in the document. The goal is to achieve that the plant process, at any time, finds itself in a safe state. The term *safe state* is defined to be a state of the process when safety is achieved [10]. And again, *safety* is exactly freedom from unacceptable risk [10]. Many of these expressions are intuitive to understand and do not actually need any further explanation. Notwithstanding, they are all explained and defined in a thorough fashion in the standards that speak of them in order to avoid misunderstandings. It should also be stressed that the expressions may have different meanings in different contexts (e.g. a definition of an expression in IEC 61508 may differ from the definition of the same expression in IEC 61511).

2.4 Explanation of the applications

To rule out the possibility for misunderstandings, it is important to provide the reader with clear and unambiguous definitions of the concepts that are being discussed. In the following sections, perhaps the two most cited terms in this thesis are being thoroughly explained.

2.4.1 Inhibit

Inhibit is an application provided by the SAS which the operator can make use of in cases where it is desirable to make the system logic independent of an input signal. This implies that the value of the relevant input signal is not taken into consideration when the logic solver processes the received information and is about to decide what should be done as a reaction to the process state/condition. This again leads to that the corrsponding safeguarding action that normally should have been carried out in such a situation, fails to appear. Consider the following scenario: a sensor located somewhere on the installation measures a pressure. The logic solver will perform an evaluation of the pressure measurement and check whether it is exceeding an upper bound of what is acceptable for safety purposes, or not. Accordingly,

the corresponding safeguarding action should be to ease/relieve the pressure, if the result of the evaluation is that the situation may appear as impending. Consequently, an inhibition of the sensor input signal will prevent the pressure-relief from being carried out. In some of the literature, inhibit is also referred to as blocking, as for example in [1]. Hereupon is the definition that will be used throughout this thesis:

***Inhibit**, or **blocking**, means to disable a safeguarding function, but allowing associated alarm annunciation as well as manual/automatic control. Inhibit, or blocking, applies to both individual action alarms[1] and input signals effecting safeguarding and disabling functions.* [1]

2.4.2 Override

Override is another application provided by the SAS which the operator can make use of in cases where it is desirable to make an output signal independent of the system logic. This assumes, however, that the output signal is given an external value so that the terminal device (final control element) has a command/an instruction to act in accordance with at any time, in order to not receive empty messages. The external value that is fed into the apparatus varies on request from the operator or other management personnel, which in turn depends on the purpose of the override. By making use of the example given above in the inhibit section, the effect of an override can be explained easily; consider that the final control element whose role is to relieve the pressure in the case of overpressure consists of a valve, and that the signal leading to this valve has been overridden. The consequence of this will be that the control mechanism which is controlling the motion of the valve (actuator), not obeys any command coming from the logic solver, but instead only listens to predefined operator instructions. This is the importance of carrying out an override, and the applications to both inhibit and override will be presented in the succeeding sections. It shall be emphasized that when the term "application" is used, it can refer to either the applications inhibit/override, or their area of application, i.e. the actual interpretative meaning of the word. This will, however, be possible to understand out from the context which the word is placed in. As before, NORSOK provide us with a concise definition:

***Override** means to set the output signal to a predefined state, independent*

[1] An individual action alarm is an alarm feature in the SAS intended for automatic control and safeguarding actions. This type of alarms includes blocking facilities, in contrast to warning alarms [1].

of changes in logic states. [1]

A visualization of the functionality of the above-mentioned applications is shown in Figure 2.6 below.

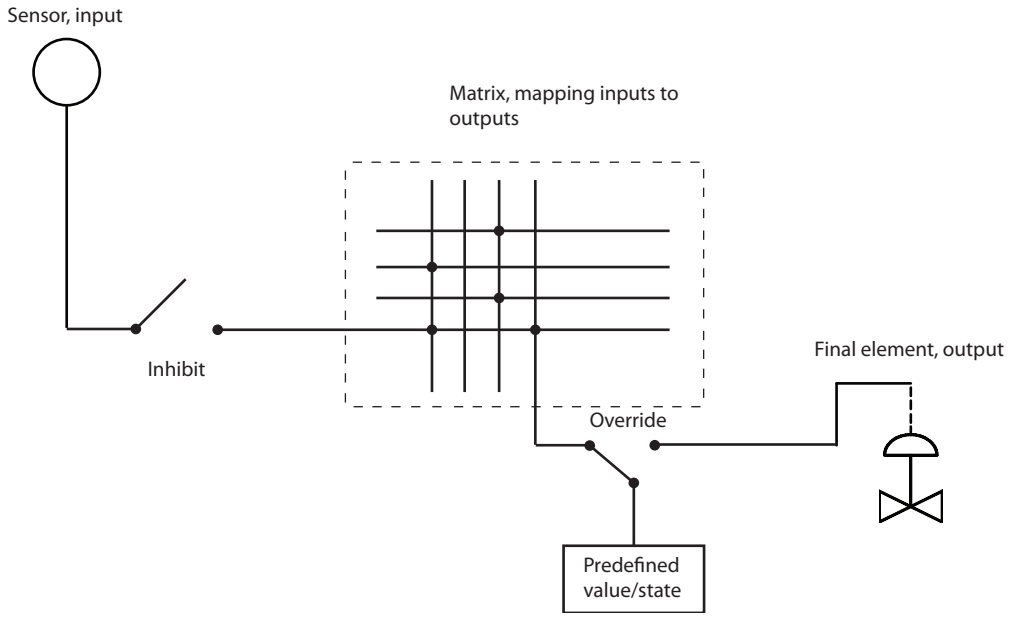

Figure 2.6: Inhibit and override, inspired by figure presented in [3].

2.5 Areas of application

There are several areas of application related to the functionalities of inhibit and override, such as maintenence work, testing and shutdown prevention. The ones that are most used in practice and regarded as the "most common" ways of utilizing the facilites will be presented in the following sections.

2.5.1 Inhibit

The inhibit functionality is utilized in situations related to process operation, but occasionally it is also applied for test purposes. A case of the latter area of application is presetned in [11] through an Operational Sequence Diagram (OSD), proposing a method for how to perform tests on Pressure Transmitters (PT). It is suggested a procedure where the operator starts off the routine by setting an inhibit flag on the PT tag in the SAS. This inhibition is carried out through an instrument technician who isolates the PT, hence

making it independent from other parts included in the control of the plant process. Furthermore, a calibration is carried out in order to achieve measurement reliability. The next step is to make the PT subject to a changing pressure environment so that alarms in the system are triggered. The test is considered as successful if alarms go off at respective alarm limits. This kind of testing is actually possible to perform without having any stop in production. This is a direct consequence of the inhibit's functionality, that is to make the system logic independent from the incoming sensor signal, so that the related final control element is not invoked despite of the critical change in pressure. If this is done correctly, process shutdown commands are avoided.

The need for the inhibit property also arises in the daily operational management of a plant. While the purpose of using the application in a test context is to check whether sensor equipment is working or not, the intent of using it in an operational context is to prevent safeguarding actions from taking place as consequences of abnormal process conditions. This may be of interest to the operator if his/her inhibit intervention results in that plant production is maintained and shutdown actions are avoided. This will, however, require that the operator, or other administrative personnel, have conducted a risk analysis (the thoroughness of the assessment depends on the situation) of the outcome, so that the plant safety is not reduced significantly due to the inhibit action. If the result of the assessment is that the initiative does not have the potential of putting humans, environment or equipment in danger, the action may be realized. To tie this up against a real operational scenario, the following example can be considered: a sensor is broadcasting an incorrect measurement value, which is very unfavorable seen from a process control perspective. The measurements will propagate their path further to the logic solver and final control elements, hence it may seem appropriate to inhibit the signal so that ill-behaved process evolvement is avoided. Moreover, there exists evidence that the functionality has been abused in order to avoid process shutdown, despite the fact that this had been the safest thing to go through with. A practical example which demonstrates how the facilites can be related to an actual situation of process control is addressable in Appendix A.

2.5.2 Override

Primarily, the override facility is used under four different settings; during operation, for maintenance purposes, in test situations and in the start-up phase of a process. During maintenance work, advantage can be gained with

respect to safety by overriding the final control element which is to be repaired or serviced, in the way that the apparatus cannot constitute any harm to the servicing crew while work is ongoing. Neither is it preferable to have an ill-behaving final control element which is interfering with process control or plant safeguarding. A maintenance override gives the operator an opportunity to make the element independent from system logic.

Normally, certain output signals are required to be overriden during the initialization phase of a process in order to "get the wheels going" and make a start-up feasible [5]. The reason for this is that currently existing input signals do not satisfy the logic's conditions to enable start-up operations, so this must be done artificially and forced by the operator. Shutdown functions must be blocked so that shutdown is not demanded during start-up [12]. The functionality of start-up overrides shall, according to [10], be validated so that conditions related to such a critical situation can be shown and documented to be safe. Moreover, start-up criteria should be specified in procedures that are available for the operator. A hazard preventive measure would be to automatically disable start-up overrides after a certain time limit so they are not present in the system beyond time periods of necessity. For overrides that are set to indefinite time intervals (and are not reset automatically), a good practice is to remind the operator of the overrides that are alive in the system by providing recurrent alarms [12].

If a final control element needs to be tested for its operational purpose, the item can be set subject to an override. This can only be done in cases where enforcement of the final control element value does not affect the process negatively or sets up dangerous situations, such as closing of pressure-valves that do not lead to pressure build-up/accumulation, etc. In situations where, for example, start-up of a pump on command from operator will have bad influence on the process control, other approaches must be undertaken for the execution of the test event. Actually, the most useful aspect related to overrides seen in a test context, is to check whether the logic device returns the correct value on the output, given a set of inputs. This can most easily be explained through a short example; given the condition that a thermometer measurement that exceeds 100°C shall trigger a shutdown action of the whole plant. If it is of interest to simply verify that correct output value is set by the logic, but to avoid the overall shutdown command, the thermometer can be exposed to artificial heating, given that the Emergency Shutdown Valves (ESV) are overridden to be placed in an open position. It is only necessary to verify that they (in reality) would have been closing in the case of an emergency situation. Just like before, full production is main-

tained under test conditions, which obviously is of great economic advantage.

Last, but not least, the application that is directed for operational purposes shall be discussed. Imposing an override action on an element makes it possible to overrule any shutdown action that may originate from critical state conditions detected on the inputs. This can be of great use when safety limits are considered to be too strict, or when strange system behavior leads to inconsequent and ambiguous shutdown demands. The operator then has the ability to prevent shutdowns considered as "unnecessary", until the problem is resolved. It also serves as a tool for making it realizable to push production limits towards upper production bounds, so that earnings are maximized. However, this is a two-sided phenomenon because of the danger that is often related to such an action. It is precisely the related aspect of danger that will be thoroughly discussed in the next following section.

2.6 Risk-related aspects

The risk associated with an override depends on the number of overrides that are alive in the system simultaneously, in addition to the length of the time period the override is held active. It may be, in some cases, that the cumulative risk of having multiple overrides applied to one single (coinciding) process unit, constitutes a greater danger than the sum of the individual risks associated with each and every one of them [5]. This is an aspect that must be taken into account before a work permit is issued for the area. A work permit is a safety regulatory measure which ensures that the workers are capable of carrying out their specific job tasks in a safe manner [13].

Although the SASs installed on facilities today mostly provide a log feature that is keeping track of live inhibits and overrides present in the system, handwritten logbooks placed in the Central Control Room (CCR) are still in use. This shall also be supported later, as one of the installations included in this thesis' survey only recorded overrides by the use of pen and paper. Otherwise, handwritten logbooks can be necessary because the computerized safety system does not have the ability to capture all types of overrides that are possible to implement. These are typically overrides that are carried out manually and by hardwiring, such as placing a jumper between two contact surfaces so that the signal travels in circuit outside the element. Those that are not registered electronically must be recorded on paper. Since this process depends on human factors and abilities (i.e. requires that the operator remembers to log the event every time), it introduces a potential source of

error of human character, which is often the type of error that is most crucial for an accident to take place.

To minimize the risk for human errors to occur, checks of logbook up againts the actual plant situation should be done regularly, and several parties should be involved in the verification [5]. In Table 2.1, a proposition of the parties that should be involved in the verification process is made, together with some corresponding time intervals of how often the check should take place. An inspection arrangement should be initiated by the operations manager at every interchange in shift, so that operators are up to date on the situation each time they go on duty. Furthermore, it is proposed that the site manager is involved in the override control on a weekly basis, while the technical/engineering manager within the company is engaged monthly.

Table 2.1: Verification table of overrides, based on the one presented in [5].

	Control room operator	Operations manager	Site manager	Technical authority
Every shift	Yes	Yes		
Weekly			Yes	
Monthly				Yes

Another measure of preventive character is to undertake a risk analysis of any action that may lead to an impairment of the overall installation safety. Of course, this has to be done before the relevant action is carried out in order to have any effect. The thouroughness of the assessment will vary, depending on the nature of the impairing act. For start-up overrides, an assessment may even be unnecessary, unless active overrides are already present in the same, coinciding part of the process location [5]. This does not, however, apply to start-up and shutdown of the plant in general. During these activities, large variations in pressure, temperature and other process states will take place, thus a larger risk for having occurances of process instability during these highly-dynamical phases is more likely than during normal steady-state operation [14].

One of the most dangerous aspects related to having inhibits, overrides and/or bypasses alive in the system, is the risk for that the plant process is evolving in such a way that the missing feature (which was ”removed” as

a consequence of the impairing action) suddenly should be needed; that a process demand is made while the specific SAS functionality is temporarily unavailable [15]. This unfavourable aspect stems from the fact that if a Safety Instrumented Function (SIF) is disabled by operator, the part of the process that is placed under protection by the disabled SIF will still continue to serve its purpose, that is to participate in the overall production process. This results in that the plant is regarded as "available". However, the production is carried through without the normal safeguarding environment, so the SAS is considered as "unavailable". If fundamental, critical SIFs were disabled and a function call from the process is made, it is conceivable that dangerous situations may arise [16].

It is important that operators and other people that are in contact with the applications get extensive experience so they can build up self-confidence when it comes to governing the process and the SAS in general. This can be explained by using a well-known term within the discipline of psychology, saying that they gain a "sense of coherence" for their work [17], i.e.:

- they find their work-related activities meaningful
- they understand the logic behind their actions, i.e. they understand the consecutive result of the observed outputs logically based on the imposed input values
- they perceive their job as manageable

Although it may often appear to third-party individuals that the technical elements of the process control are making up "the big differences" in the overall picture, it is important to not neglect the human factors that actually play an important role in the operation of a plant. The mind of the operator tends to be reflected in the way of governing the SAS. This is why the above-mentioned points are included in this section and considered as fundamental, despite that they are actually embraced by a field that is as diverse as psychology.

Furthermore, a phenomenon that is proven to be provoked by frequent application usage is something that is called *systematic failure*. A systematic failure is, according to IEC 61511, a failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. In particular, it can be said that this type of failure is associated with improper setting and resetting of inhibits/overrides

[15]. As it can be understood from the definition, it can represent a very comprehensive process to actually eliminate and rule out the possibility for systematic failures to be introduced in the system. However, these failures can be revealed by the operator if he/she executes a deterministic pattern or sequence of actions, hence making it possible to identify in exactly which succession the events are triggered. A diagram can therefore be put together after all the possible combinations have been examined. In future operation, the pitfalls may be avoided by regarding the action-reaction diagram and perfrom operational executions thereafter.

2.7 Relevant standards and regulations

In this section, regulations and standardizations that directly affect the operator's behavior in terms of utilizing the facilities inhibit and override will be regarded. As shall be seen, the regulations issued by The Petroleum Safety Authority Norway (PSA) have been emphasized in particular, since these are representing the Norwegian authorities' requirements for petroleum operations. However, there also exist plenty other regulatory literature associated with the topic, but taken into account that it is difficult to actually say anything about the operators' actions with respect to compliance with these, it is not seen as suitable for the purpose to write innumerable pages on the topic. For that reason, the aspects considered as most significant are incorporated herein.

2.7.1 Central PSA regulations

The Petroleum Safety Authority Norway (PSA) is a governing organization that issues a set of regulations to ensure that petroleum activities carried out on Norwegian continental shelf are evolving safely, that is with respect to people, environment and material assets. The five regulations that have been published by the authority are called The Framework Regulations, The Management Regulations, The Facilities Regulations, The Activities Regulations and The Technical and Operational Regulations. Because the facilities of main interest in this thesis, inhibit and override, are *managed* by the SAS operator, The Management Regulations will be of the most interesting character in this context, also because these regulations are the only regulations in the collection of regulations that make specific demands on the consequences of the application usage.

PSA Management Regulations

It is interesting to interpret Section 5 in The Management Regulations which deals with barriers, in light of Section 2 which addresses the question about responsibility for the actions that are carried out at the facility. Section 2 further refers to Section 7 in The Framework Regulations which states that:

"The operator and others participating in the activities are responsible pursuant to these regulations. The responsible party shall ensure compliance with requirements stipulated in the health, safety and environment legislation. The operator shall ensure that everyone who carries out work on its behalf, either personally, through employees, contractors or subcontractors, complies with requirements stipulated in the health, safety and environment legislation." [18]

The operator is, in other words, responsible for that the operation of the petroleum activity progresses in accordance with the stipulated regulations. The term "operator" is explicitly defined to be "anyone executing on behalf of the licensee the day to day management of the petroleum activities", which in principle refers to the petroleum facility's general manager [18]. It may be useful to have this clause about responsibility distribution in mind when the focus is moved over to the highly relevant aspects of the regulations.

Because of a recent revision of the regulations, Section 5 is a merger of what were Section 1 and 2 in earlier versions. Chapter 2 in the regulations is regarding the management of risk on the facility. In relation with this, the following demand (among many others) is made by PSA concerning barriers in the system:

"The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life." [19]

In order to have the competence to discuss the meaning of this statement, the term *barrier* must be defined. The meaning of the expression is not explicitly specified in the regulations, but it can be understood and interpreted as synonymous with the term *safety function*, i.e. SIF in an SAS context [20]. For academic purposes, there does also exist a rigorous definition that can be found in [21]:

*A **barrier** is a measure which reduces the probability of realizing a hazard's*

potential for harm and which reduces its consequence. [21]

It should be stressed that barriers may be physical elements (materials, protective devices, shields, segregation, etc.) or non-physical measures (procedures, inspection, training, drills, etc.) set in to protect the installation [21]. SIFs that are implemented an realized through an SAS may loose their functionality if the operator affects them by the use of, for example, inhibit or override. If such impairing events take place, something must be done to maintain the level of plant safety, i.e. to preserve the barrier that was present in the first place. Furthermore, the regulation states what to do if a barrier-weakening has already happened:

"Personnel shall be aware of which barriers are not functioning or have been impaired. The responsible party shall implement the necessary measure to remedy or compensate for missing or impaired barriers." [19]

It is quite easy to understand what Section 5 in the regulations is actually demanding. In brief, it can be concluded that an SF shall maintain its role within the SAS throughout the SAS's operational lifetime, hence compensating measures must be implemented when actions of an impairing character are carried out by the operator. Naturally, it is not told explicitly what to do in order to compensate for the debilitations in each individual case, as this will depend on a bunch of parameters (e.g. installation, situation, etc.). However, this shall be specified in the procedures regarding operational activities and maintenance of the safety system, referring the reader to Section 16.2.2 in IEC 61511, which has been spoken of earlier. This will save the operators and managers for much confusion and disagreement during the implementational phase of the compensating measures.

On the other side, if it is not specified in the procedures exactly what measures that are to be implemented in order to re-gain safety balance, a general technical approach will be needed. Serving as an alternative to this is the model presented in Figure 2.7, which is represented in terms of a flowchart. It is based on theory introduced in [14] and the figure therein.

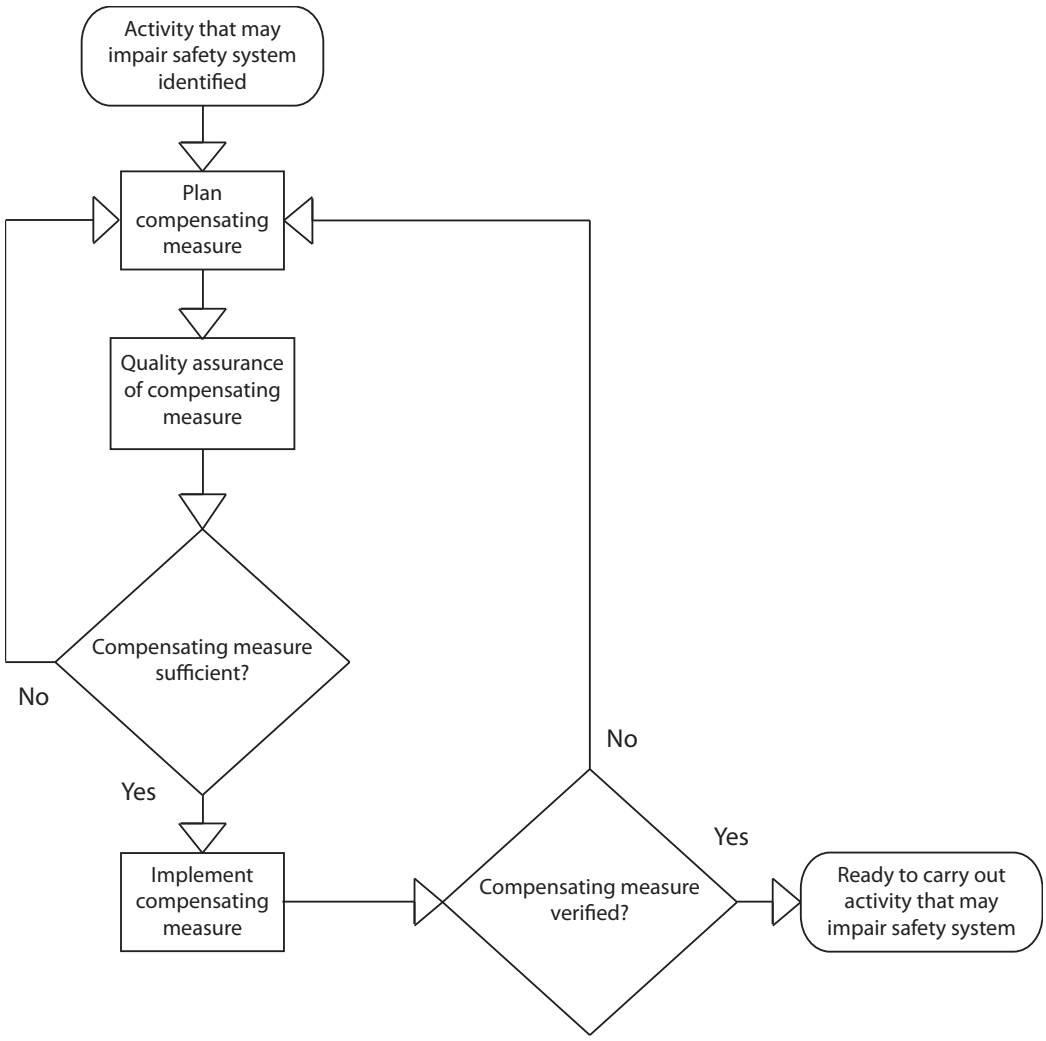

Figure 2.7: Procedure for implementing compensating measures.

Considering the chart from a top-down perspective; once an activity that may undermine function(s) in the safety system is detected and identified, or planned executed in the near future, planning concerning what kind of measures that should be implemented to compensate for the reduced functionality should be initiated. It is important to undergo this phase *in advance* of the realization of the impairing act. Moreover, quality assurance must be performed before a decision can be made regarding the sufficiency of the proposed measures. If it turns out that the measures are not sufficient to balance for the weakened functionality in the system, more efficient measures must be considered. If the measures are adequately met and proven to be solid enough, progression towards the next phase (where the actual realization of

the actions are taking place) can be made.

Last but not least, the requirement for independence between safety barriers must not be forgotten. As most of the other demands that have been presented, this is also stated in Section 5 of The Management Regulations, and is reproduced in the paragraph below:

"Where more than one barrier is necessary, there shall be sufficient independence between barriers." [19]

One of the main reasons for insisting on sufficient independence between barriers, is to try to rule out the possibility for introducing common cause failures in the system. IEC 61511's definition clearly reads that:

*A **common cause failure** is 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.* [10]

The definition is very wide and universal in its wording, but can be unambiguously interpreted to mean that a common cause failure is capable of bringing down multiple protection layers or barriers/safety functions if striking the system, when it is spoken of in relation with an SAS. A field of research is to try to overcome the chance for introducing such failures in safety systems, and spesifically the reader is referred to [11] if more detailed theory on the topic is wanted. There, among other things, it is proposed a method for function testing which may be helpful when dealing with common cause failures in an SAS.

2.8 BP Texas City refinery disaster

The number of accidents due to improper process control and poor attitude towards safety systems continues to grow as the 21^{st} century evolves. On March 23, 2005, BP Texas City refinery, which at that time was America's third largest refinery, suffered a major accident as a consequence of that flammable gas was ignited. This, in turn, resulted in multiple explosions and fire over a large process area. In total, 15 workers were killed and 170 people injured. In retrospect, there is a lot to learn from the accident, since it has been subject to extensive analysis by U.S. authorities. The following facts that will be presented are based on U.S. Chemical Safety and Hazard Investigation Board's (CSB) animation video of the incident at BP's refinery

in Texas City, Texas, USA. The setup of the overall process at the refinery is shown in Figure 2.8, and the reader is encouraged to address this drawing frequently during the description of the course of events.

It all started with the preparation of an isomerization unit which is playing a key role in the process of distillation. This means that highly flammable liquid hydrocarbons are fed into the unit, since the purpose of the distillation is to separate the different fluids from each other. The "light" parts of the liquid evaporates at an earlier stage than the heavier components, and are later cooled down higher up in the distillation column. At some point the feeding of hydrocarbons into the column was initiated. During normal operation, the liquid level in the tower should not exceed more than approximately 6,5 ft. However, the sensor installed in the isomerization unit was not able to measure liquid level any higher than 10 ft., so beyond this point it was impossible to have any idea about the level in the tank.

As the hydrocarbon-feed made progress with time, a level high-alarm was activated. The operator and workers acknowledged the alarm, but the feeding was not stopped for that reason. The initial start-up phase of an isomerization unit requires that the liquid level of hydrocarbons is higher than in the case of normal operation. This is because the start-up phase of a process differs from the rest of the operational phases (cf. start-up overrides). A second alarm functioning as a redundant alarm to the first should later had gone off, indicating that the level was still high and rising. This alarm, however, failed to appear. When the first part of the start-up phase was finished, the liquid level in the bottom of the tower was 13 ft. (found in later calculations, since the sensor was not capable of measuring higher levels than 10 ft.).

The work that was resumed a few hours later involved circulation of the liquid which was already in the system, in addition to further filling into the tower. However, despite that it was specified in the start-up procedures that the valve controlling the liquid flow out of the tower shall be set in an open position at this stage of the process, it was left closed, hence the liquid level only continued to grow. When, in addition, the heating process of the liquid began, an alarm indicating that the tank was witnessing an overpressure soon went off. At this point, the actual level of hydrocarbons was 138 ft., while the level transmitter inside the tank was broadcasting a level of 10 ft. and falling, due to equipment malfunctioning.

Some of the heating elements were moderated after the alarm went off, but the pressure-relief valves which normally should be triggered to open as a

safeguarding reaction to the high-pressure alarm, did not react. This led to that a field worker manually had to open another valve leading to the blowdown drum in order to ease the pressure. A blowdown drum serves the purpose as pressure reliever for the gas that evaporates from the liquid hydrocarbon heating and causes the high pressure. The gas enters the drum and later the atmosphere.

Eventually, the workers reacted to the situation by opening a valve that transported the liquid in the bottom of the distillation column to external storage tanks. Normally, this would have improved the conditions inside the tank, but due to extremely high temperature, the liquid began to boil inside the tower, causing the contents to expand and consequently overflow into the piping. This, in turn, led to an enormous pressure on the automatic pressure-relief valves which finally responded to open and cause the liquid to flow further into the blowdown drum.

At some ponint, there was supposed to go off an alarm indicating a high contents level of liquid in the drum, but also this failed to appear. This caused the highly flammable liquid hydrocarbons to overflow the drum and burst into the atmosphere. Probably, according to [22], it was a car running idle in the nearby area which ignited the substance and caused the series of explosions and fires.

This terrible incident could have been avoided if the safety at the facility had been of a higher quality, for example if a flare system was installed instead of a blowdown drum. The flare system would have burnt off the flammable gases and, at an earlier stage, alerted the crew of what was about to happen. Moreover, the disaster demonstrates how important it is for workers to possess a high level of understanding and process insight, seeing that the episode could have been revoked if a worker had detected the critical conditions.

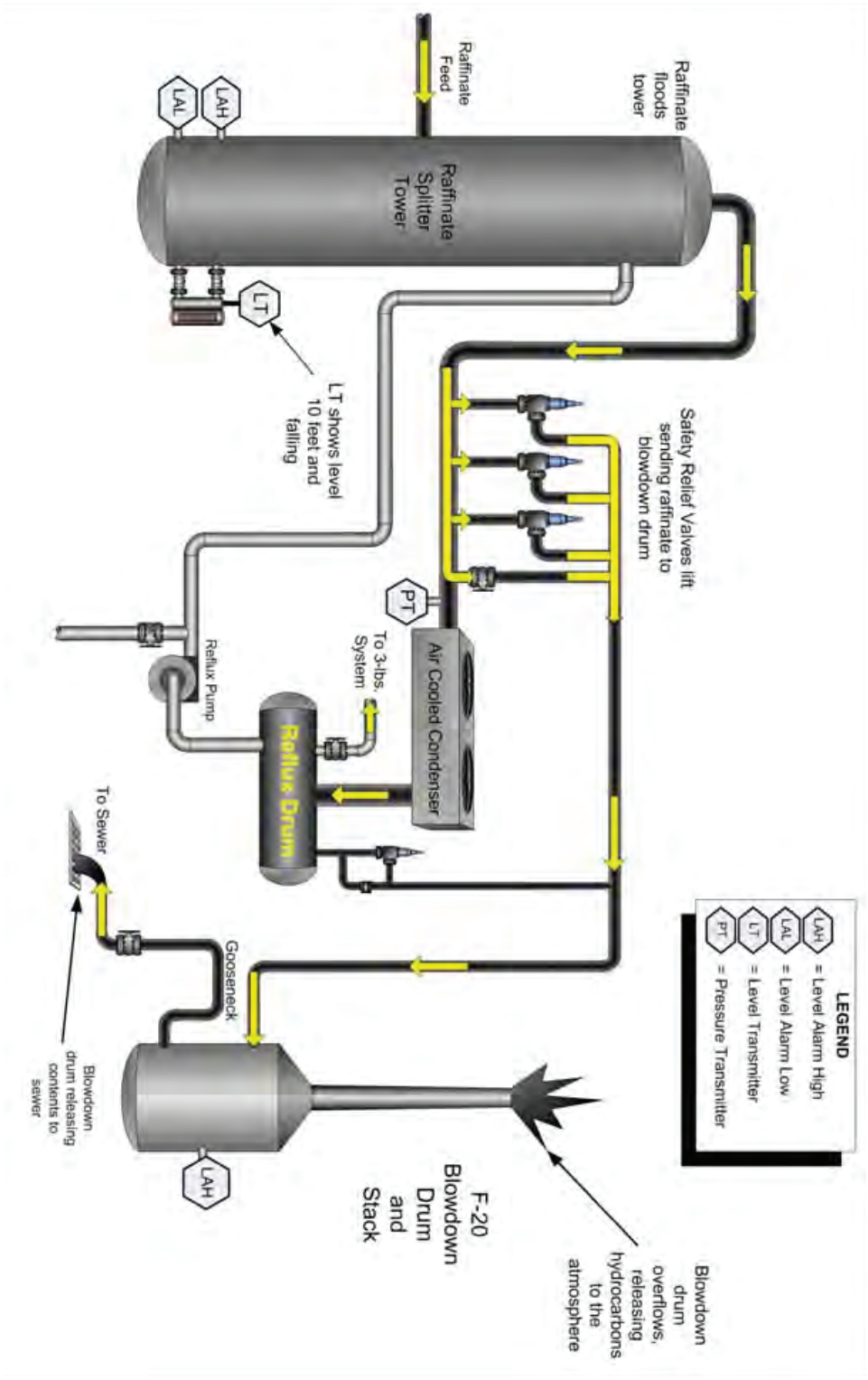

Figure 2.8: BP Texas City process constellation, as given in [4].

Chapter 3

Problem considerations and methods

In a study like this, it is important to give an account of which conditions the work is been based on and what kind of assumptions that are made, so that traceability is obtained. This makes it possible for a third party to reconduct the analysis and check whether their results are in compliance with the ones presented here (and vice versa). First, an overview of the installations that have been included in the study will be presented. Thereafter, the different types of data sets will be introduced together with some provided explanation regarding the nature of each and every one of them. The chapter is rounded off by giving a detailed problem statement followed by a proposition of characteristic methods and approaches that were used.

3.1 Installation log overview

Table 3.1 presents an overview of all the installations included in the study. The table systematically shows the installation identification terms that will be used throughout the thesis when the individual facilities are being addressed (identity), the time period of provided log data (log period), and whether the received information contains knowledge about inhibits, overrides or even all general events that have taken place during the entire test period (inh., ov. and all, respectively). Due to anonymity reasons, the installations will be referred to as "Installation A", "Installation B" etc., rather than their real names. This was complied with on request from the collaborating partner (Statoil ASA).

The advantage of having access to the complete event log instead of only

being restricted to the inhibit/override log, is the possibility to backtrack past events in relation to instances of, for example, concentrated bursts of overrides. By doing this, process shutdowns and other extensive activities may be detected by observing other general commands made on behalf of the operator in the time-neighborhood of an event. However, it was only possible to obtain complete logs from Installation D and E. It will not be done any further investigation of related activities other than inhibit and override, as the required workload associated with the applications proved to be sufficient.

A significant aspect to take note of, and which can be read directly from the table, is the lack of a log associated with overrides at Installation F. It was only possible to obtain a log that dispalyed all the cases of inhibits that had taken place during the test period. This is due to the fact that the overrides are only kept track of and recorded on paper in the CCR. Furthermore, the range of the log period for this installation is very short compared to the others. This makes the related results less rigorous, but they do yet provide a good short-term image of the overall situation. This is the only onshore installation included in the survey, so perhaps more information from this would have provided a stronger basis for comparison purposes relative to the other offshore facilities.

Table 3.1: Installations included in the survey, $Y = Yes$ and $N = No$.

Identity	Log period	Inh.	Ov.	All
A	Oct. 2008 - Nov. 2010	Y	Y	N
B	Aug. 2008 - Nov. 2010	Y	Y	N
C	Oct. 2008 - Nov. 2010	Y	Y	N
D	Nov. 2007 - Jan. 2011	Y	Y	Y
E	Jul. 2007 - Jan. 2011	Y	Y	Y
F	Jan. 2011 - Mar. 2011	Y	N	N

3.2 Preparation of the data sets

The received data sets from the different installations required each a certain amount of pre-processing and re-arrangement before any useful knowledge could be extracted. However, the amount of pre-processing that was required from each installation varied greatly. All the received information from Installation A, B and C were actually proposed in a ”plug and play” fashion, meaning that no preparatory work was necessary to go through with before

starting up the analytical part of the work. However, the logs originating from Installation D and E required a tremendous amount of preparational work in advance of the analysis. This was solely due to the file format of the log files; the received history of events at Installation D and E consisted of 92 and 115 separate .txt files in total, respectively. Since neither Notepad (which is the default program of choice when opening .txt files on Windows computers) nor Microsoft Word provides any good environment when working with large data sets, it appeared natural to import the files to Microsoft Excel instead. Generally speaking, Excel is the program of preference when operations on large amounts of data are to be made. The program offers the user an enormous library of functions that are executable on historical data, and that give well-arranged results.

The import process turned out to be not so trivial and straightforward as first expected. During the transformation, the dates were totally misconstructed leading to interchanges between the year-part and the day-part in the date format. In addition, the program misunderstood the sectioning of the columns so that the date often ended up as an event description, making the results meaningless. This could, however, be corrected for manually. The process was time-consuming but necessary in order to proceed to the next level where, among other things, the data had to be sorted by time and date so that the events appeared in chronological order.

3.3 Problem statement

The main objective of this thesis is to perform analysis (of various character) of event data collected from a handful of SASs governing different production facilities operated by Statoil ASA. There are only events that have the potential to weaken the safety level of a facility that shall be considered in this survey, in other words, special emphasis is put on the operator-based interference with the applications inhibit and override. From experience, it is widely known that accidents related to oil-producing installations often are accidents of an extensive character, where especially wildlife and nature are vulnerable groups (and people if, for example, explosion is involved). A disaster that took place shortly in advance of this thesis writing is the well-known Deepwater Horizon scandal where large amounts of oil was spilled into the Gulf of Mexico and reached continental coasts far away. The responsible party was the British company BP. However, the outcomes of the analysis will hopefully help to shed light on the issue of safety in association with the operator-related application interference, and thereby contribute to increase

the awareness upon the consequences of impairing functions that are realized in the system.

In order to be capable of saying anything about the daily-basis operation of the different installations, the logs originating from each and every one of the facilities are being regarded with respect to a bunch of analytical aspects. In particular, it will be interesting to:

- look at the evolvement of the usage of inhibits/overrides over time; to perform a trend survey
- examine the difference in the utilization of the applications between different shifts, personnel and day/night periods
- perform a comparative study of the different installations, focusing on key statistical quantities
- reveal tags that repeatedly tend to show up in the overview
- investigate signals that appear as blocked/overridden for longer periods of time
- address redundant elements that appear to be "taken out of operation" synchronously

Beyond this, it will be difficult to evaluate the events in light of existing standards and regulations. This is simply because information regarding compensating measures and other risk-preventive initiatives implemented by the personnel at the respective facilities, was not possible to procure. In other words, it is impossible to verify whether an operator action is carried out in compliance with procedures, etc.

Another thing worth mentioning here, is that the focus of this study has been to identify and get an idea of the *general* application usage at the installations, rather than emphasizing individual events. Paying too much attention to single events may undermine "the big picture", in addition to that conclusions drawn based on such events can be uncertain or erroneous. This is primarily because of the lack of insight to information, as named earlier. For example, if a signal (according to the log) has been inhibited or overridden for an unusual long period of time, it may be the case that a new signal has taken over the original functionality possessed by the old one (without the ability for a third party to discover this), and that the old one is deleted. Or, the case may be that the signal is completely disabled due to

an alternative arrangement that has been put into place. However, it shall be concentrated on actually detecting the cases that stand out in terms of the above-mentioned points, regardless of the lack in ability to address the causes of the events, so that they later in time may be investigated further on initiative from the company.

3.4 Data representation

Figure 3.1 below presents how the logs are put together by the SASs at the different installations, and how they are represented in Excel. It does actually show more than just this, namely all the "types of events" that have been considered to represent either inhibit or override at the respective facilities, which means that these (and only these) event types are included in the study of this thesis. Because the installations are governed by SASs distributed by different vendors, the events do not completely coincide with each other. Despite this, it was eventually agreed (after having consulted with the responsible contact persons) that the instances that are shown in the figure are the events that correspond to the well-established definitions of inhibit and override.

It shall be noted that Figure 3.1 does not completely reflect the truth with respect to the different log appearances. The representations in Excel are a bit more complex than what is shown here, hence it is only presented "a stripped version" of the truth. The truth is that there exist a few more columns of information, but that these do not provide any useful information when it comes to the survey of this thesis. For this reason, they have been omitted.

Time	EventText	Name1	Description
19.09.2010 21:00:29	Overbroing på	GP-3001A-DP	OX
19.09.2010 21:19:21	Overbroing av	GP-3001A-DP	OX
22.10.2010 09:32:28	Utkobling på	LALL-20057	CD2004
22.10.2010 09:36:59	Utkobling av	LALL-20057	CD2004

(a) Installation A, B and C

Tag Name	Tag Description	Command	Value	Date	Time
W-62-XY___102M	VANNTÖMMING KO TANK	Overbro	På	06.10.2008	14:35:43.405
W-62-XY___102M	VANNTÖMMING KO TANK	Overbro	Av	06.10.2008	14:46:27.400
G-43-LT___007M	NAS VÄSKEUTSKILLER	Höyutk.	På	06.03.2010	10:06:08.218
G-43-LT___007M	NAS VÄSKEUTSKILLER	Höyutk.	Av	06.03.2010	10:06:24.208
G-25-LT___020M	EKSP INNL VÄSKEUTSK	Lavutk.	På	19.12.2009	08:24:26.068
G-25-LT___020M	EKSP INNL VÄSKEUTSK	Lavutk.	Av	19.12.2009	20:37:42.090
G-79-ES___150M	PAS 3.00 FRA NAS	Utkoblet	På	27.08.2007	13:15:57.672
G-79-ES___150M	PAS 3.00 FRA NAS	Utkoblet	Av	27.08.2007	13:16:03.667

(b) Installation D and E

Timestamp	Tag	Tag Description	Area	Message	Value
02.01.2011 08:40:24	20LS5046 03	HELLNING 3 TIL 1 VF-A	PCDA	BLOKKERING HH	BLOKRT
02.01.2011 09:40:19	20LS5046 03	HELLNING 3 TIL 1 VF-A	PCDA	BLOKKERING HH	NORMAL

(c) Installation F

Figure 3.1: Data representation of the different logs.

Obviously, the first three installations (A, B and C) provide the logs that are of a character which makes them the simplest to interpret. Insofar as the log originating from Installation F, this is also true. These representations are well-arranged and trivial to extract useful information from. The EventText column in Figure 3.1(a) tells whether an action is an inhibit action (Utkobling på/av) or an override action (Overbroing på/av), while in Figure 3.1(c) this can be discovered by looking at the Value column; the activation of an inhibit is represented by BLOKRT and a deactivation by NORMAL. When it comes to Installation D and E given by Figure 3.1(b), there were several candidates jumping on the borderline to be regarded as inhibits/overrides. This was because the interpretation of the various operations were somewhat vague and difficult to obtain. But, after consultation with competent personnel, it became clear that all the attributes contained within the Command field were event instances that for certain were in compliance with the definitions.

3.5 Methods and approaches

The cumulative amount of working hours spent on the total problem is strongly dependent on the different approaches used to attack the smaller sub-problems. This section presents the methods that were used in the different parts of the analysis, in addition to provide some important information about the problem itself. Some of the analytical procedures are more sophisticated than others, but none are particularly complicated, seeing that the methods considered as being the most favorable for the different purposes were actually based on a brute force mentality.

3.5.1 Detection of long-term inhibits/overrides

First of all, it should be pointed out that *long-term* in the context of this thesis, is defined to be an event that lasts for at least one month. Such an absolute lower limit was necessary to establish in order to avoid confusion coming up in the middle of the survey. The limit of one month allowed for a certain tolerance without being too strict or slack, making it an appropriate limit for the long-term intent.

There were not many alternatives to choose from in terms of examination methods when detection of long-term inhibits/overrides was on the agenda. The only option was simply to look at the timestamp for the activation of an event, for then to scroll and recover the same signal and its deactivation further down in the log (unless the signal was kept restrained throughout the

entire period). However, a way to ease the work a little was to sort the events with respect to time, from oldest to newest, and then to continue the sorting by tag number. The consequence of this were events arranged in chronological order, sorted into blocks of different tag numbers, which was making the process a little less cumbersome than it initially was. Regardless of this modification, the task was still the most time-consuming of them all. Even so, it was an important part of the overall problem to actually go through with and complete, since the results from the analysis gave a measure of "how usual" it was to inhibit/override input/output signals at the different installations.

3.5.2 Redundant inhibits/overrides

It turned out that identifying tags representing redundant elements in the event log was not equally easy as expected. After consulting with the contact persons and supervisor/professor, it was ascertained that, in many cases, knowledge about the individual system and its structure in general were assumptions for being able to say anything about redundant elements. However, during this conversation, it was also established that tags that only differed by one letter, for example the two tags GP-63472A and GP-63472B, with high probability could be regarded as redundant elements. These two tags typically represent pump signals, where the first tag belongs to a primary pump, and the second one is representing a backup pump (to the first one). The backup pump is supposed to take over the work for the primary pump if it suffers a pressure drop or other similar impairments. This requires that the backup unit's state is defined to be in *stand-by*, which can be controlled manually or automatically by the operator through the SAS.

The logs were examined for redundant tags by the procedure of first sorting the events by time and date, then by tag number. This lead to that the tags of interest (the redundant tags) appeared sequentially, making them easily surveyable. To accordingly check for simultaneousness, the time stamps for their inhibit/override activation and deactivation were considered. For Installation A, B, C and F, this method worked very well. Installation D and E, however, displayed a completely different approach in terms of tag number dedication. It proved to be impossible to detect whether two (or three) elements were redundant by just considering the tag number, leading to that this sub-problem's analysis was omitted for these installations. It was also later claimed by the responsible contact person for the installations that these did not have any redundant elements other than, for example, that a tank is provided with two level transmitters whereupon one of them is connected to

the process safety system and the other one to the process control system. This, however, is not considered as redundancy in the term's correct sense.

3.5.3 Shift and personnel

Changes in shifts and personnel take place at fixed times, and particularly for installations offshore there are tight arrangements for this. For the onshore facility (Installation F), however, the whole situation is coordinated quite differently. It is more convenient to treat such an installation as a normal workplace and thus implement the shift/personnel scheme thereafter. It could be attested that the structure of working hours compared to the rest of the installations participating in the study, was indeed very complicated. A surveillance of this pattern would have demanded that a large amount of aspects had to be taken into consideration, which is the reason for why the analysis of this installation was not carried out.

For all the other installations which are located offshore, the model is very simple; interchanges in shifts are made at 07:00 and 19:00 each day. In addition to this, a new operator crew is transported to the oil rig every second Tuesday, so that each personnel constellation is out on the rig for two weeks, followed by four weeks of absence. The approach used when examining the differences in inhibit/override usage between distinct personnel, was actually to perform a trend analysis of the past events. This trend analysis aimed at creating an overall picture of the general operator control situation at the different installations. Through the results coming out of the assessment, it was also possible to extract useful information regarding critical periods and intervals. The peaks that were showing up in the constructed plots would then correspond to weeks of operation where many interventions from the operator were made.

The technique has for its object to sort the events by time, and then to count the group of events that showed up within the relevant week. It is important to emphasize that the counting started from 07:00 the first Tuesday appearing in the log, and continued throughout 07:00 the next Tuesday. This kept on in a similar fashion until all the individual weeks were covered, making two such weeks an equivalent to the time an arbitrary personnel constellation was at work on the rig. Besides this, it was generated general, descriptive statistical quantities based on the samples that were made, by utilizing one of Microsoft Excel's built-in data analysis tool.

3.5.4 Appearance of same tags in the overview

Since some of the signals are more involved than others in the daily operator-related control of a plant process, it is of interest to identify and list up the ones that stand out the most. This may help the managers to detect the location of the exact sensor/final control element on an installation that needs service, or where measures must be implemented in order to improve the situation. To keep track of these cases, the history was sorted by tag number. By manually running through every tag and record the total number of appearances, a list could finally be produced (which in turn could be sorted internally) and presented.

3.5.5 General comments on comparison and methods

In the predecessor of this thesis (ref. [6]), only information coming from Installation C was subject to analysis. All the presented results in the paper were generated based on events in the log confirming that the inhibits/overrides were written to separate inhibit/override logs. In the survey of this thesis, however, the results will be based on events appearing in the log as signals which are sent out internally from the system modules, confirming that inhibit/override bits have been physically set in the modules. Since the analysis of Installation A and B were done solely based on these signals, Installation C was re-analyzed with respect to the same types of signals in order to gain an equal grounding to use for comparison purposes. This introduced new results which deviated from the ones presented in the previous paper. However, the deviations are very small since the two distinct logs shall in theory be identical, but due to technical issues related to each individual system, they are not exactly (but almost). It is also important to emphasize that the work done earlier is not erroneous, just an alternative approach with a different basis.

In general, it is known that interesting findings can be made if different entities within a similar group are set up against each other and compared at different levels. There is reason to believe that this is the case in the study of this thesis as well, so comparison of the results related to the different installations have been emphasized heavily. In [6], a similar study as the one in this thesis was made, but only with SAS information provided from *one* installation. Solely based on the (isolated) results presented there, it was not trivial to create any comprehensive picture of the overall operator control situation at the facility. Now, when several installations are participating in the survey, it is possible to regard the results relative to each other, hence

making it feasable to draw conclusions based on the noticeable differences.

Although comparison provides a great advantage when interpreting results, it is also important to mention that the initiative of setting the different quantities up against each other and achieve a 1:1 comparison relationship is not always possible. This drawback is due to the fact that the different installations are equipped with SASs distributed by different vendors, introducing discrepancy in SIF interpretation. This is because the different vendors have their own way of designing the SASs, leading to dissimilar SAS setup and configuration. However, after having ascertained that the actual interpretations of inhibit and override were identified and recognized in each system, it was possible to perform adequate and meaningful comparisons to a great extent after all.

For all the following results, the analysis is based on the complete event log that is provided from each installation, except for the trend analysis results. Here, it was decided to look at each isolated family of installations by themselves, from a shared starting point in time to another shared endpoint. This gave very good opportunities to compare the internal family results directly. The criterion that must be met for a collection of installations to be considered as a *family*, is that all the installations included in the group are governed by a SAS with the same setup and configuration (from the same vendor). In the case of this thesis, this is actually equivalent with stating that all installations within the same family must be members of the same oil field, i.e. located close to each other and utilizing hydrocarbons from a coinciding collection of oil wells.

Chapter 4

Results and discussion

In this chapter, all the results that were obtained for the smaller sub-problems will be presented sequentially, together with their provided discussions. The chapter is composed as follows; first, the results of the trend and statistical analysis will be proposed, followed by a presentation of frequently involved signals. Afterwards, the situations related to the long-term instances will be addressed, and finally all the observed cases of simultaneously inhibited/overridden signals will be made available.

4.1 Trends and statistics

Based on the knowledge that any change in shift is carried out either 07:00 in the morning or 19:00 in the evening for all the five installations included in this section's survey, the trend analysis was realized in accordance with the corresponding procedure described earlier. As the figures will show, the first family of installations (Installation A, B and C) was analyzed with respect to data originating from the two-year period October 21, 2008 through November 02, 2010, while the second family (Installation D and E) was regarded over the three-year interval November 13, 2007 - December 28, 2010.

4.1.1 Inhibits

Installation A, B and C

Since the number of inhibits varied greatly from week to week, a plot of the actual data would appear as very "noisy" with large amplitude variations and peaks, and no clear information would have been possible to extract at first glance. However, if the actual weekly data is passed through a low-pass filter, it may be possible to determine the general evolvement of the curves

and perhaps say something about the trend. A solution to this was found by considering the *moving average* of the actual data rather than the actual data themself. The moving average gives an indication of a curve's further path, and can be used as a tool in forecasting. The aspect of forecasting, however, will not be emphasized here. What will be focused on more, is the moving average's ability to function as a smoothing application which makes it easier to assess the general trend under less-dynamical conditions.

The method requires that it is defined a window length that shall be kept constant throughout the whole experiment. This is an important assumption for methods that implement the moving horizon scheme. When this quantity is defined, the first sample can be obtained by averaging over the first n points of the data set, where n is the window length. Mathematically, this is described by $\text{SMA}_1 = \frac{1}{n}\sum_{i=1}^{n} x_i$, where x_i is the ith point of the data set and SMA_1 is the first Simple Moving Average (SMA) sample [23]. Moreover, the kth SMA sample can be found by applying the formula $\text{SMA}_k = \frac{1}{n}\sum_{i=k}^{k+n} x_i$. In total, there will be $N - n$ SMA samples, where N is the number of points in the data set. This is also the reason for the delayed start of the curves in Figure 4.1. The figure shows moving averages of the weekly inhibit activity at Installation A, B and C over an horizon of 12 weeks. The period length of 12 weeks gave good smoothing properties while still preserving the curves' characteristic dynamics.

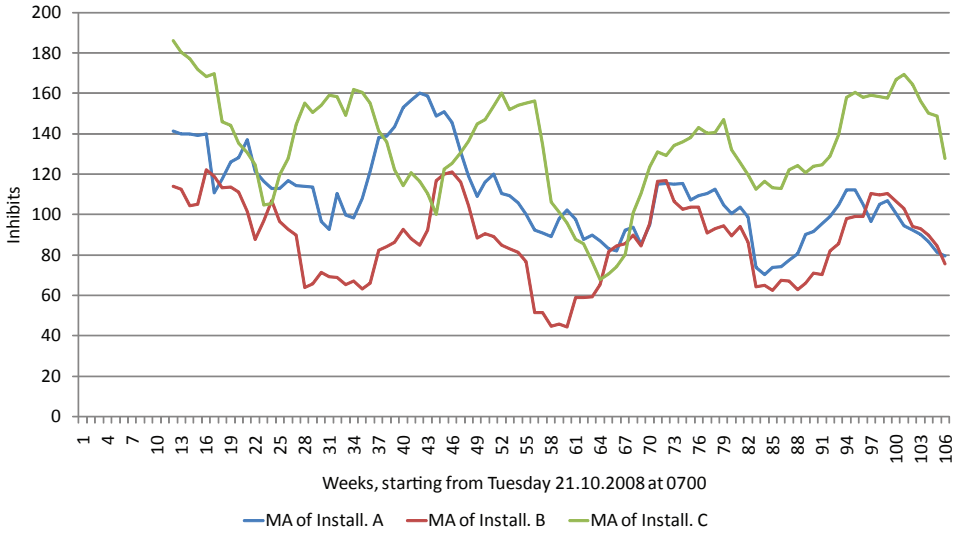

Figure 4.1: Moving average of inhibit involvement; A, B and C.

Perhaps the most obvious thing to take note of from the figure, is the strong correlation between the curves. The attitude towards carrying out inhibits at one installation seems to depend on the activity taking place at other installations within the family. Basically, this should not be very surprising, because all the installations are producing oil from the same oil field. What this mean, is that there may be "invisible" dependencies between the oil wells that could have been seen if a mathematical model of the coupled system was regarded. Particularly remarkable is the clear correlation between the inhibit activity at Installation A and B, where the two curves almost appear as identical with just a phase shift separating them. This is of course not the case, but only an interesting observation that is worth mentioning. When it comes to Installation C, the dependency does only "show up" in the latter half part of the curve.

Another fascinating discovery is the fact that if linear trend lines are plotted for each curve, all the lines have negative corresponding slopes. This can be interpreted in the way that the trends for carrying out blockings on signals are generally declining for each installation, which indicates progress in the a positive direction. The degree of decrease, however, varies a lot between the installations. The reason for why the trend lines are not drawn into Figure 4.1, is because of the over-complexity it would have caused, making it harder to pull out other critical information. This is why there has been allocated space for a separate plot of "the most successful facility"; Installation A. The result is presented in Figure 4.2.

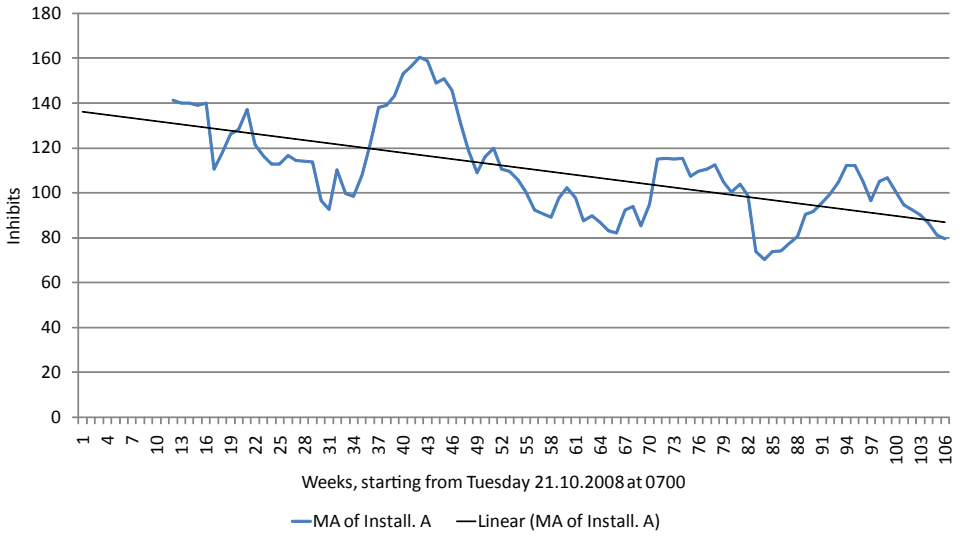

Figure 4.2: Moving average of inhibit involvement; A.

Without significant effort, it is possible to reveal that the overall inhibit activity at Installation C is higher than at the other two facilities. There are two possible explanations for why this is the case; either (1) the size of Installation C is bigger (measured by the amount of I/Os), or (2) the attitude towards carrying out inhibits at Installation C is more relaxed seen from an operator point of view. The peaks of the curves cannot be mapped directly in a 1:1 relationship with the personnel that possesses the highest ratio of inhibits. This is due to the adopted approach of moving averages that was applied to the data. However, to end up at the stage of the above-presented result, all the instances of inhibits had to be count - every week. The outcome of this was in turn used to generate some classical descriptive statistics related to the characteristic weekly usage. Microsoft Excel's add-in feature Analysis ToolPak proved very useful for this matter, since the data sets were well-arranged and organized orderly in an Excel workbook. Table 4.1 below presents an overview of the major key statistics associated with the actual data. The following statistical terms are explained in the readings [24] and [23], which were used to re-gain understanding of the statistical concepts.

Table 4.1: Descriptive statistics related to the weekly inhibit usage.

(a)

Installation A	
Mean	108,9
Standard error	6,9
Median	92,5
Mode	55
Standard deviation	71,3
Sample variance	5082,8
Kurtosis	5,1
Skewness	1,9
Range	442
Minimum	0
Maximum	442
Sum	11540
Count	106
Confidence level 95,0%	13,7

(b)

Installation B	
Mean	88,5
Standard error	6,3
Median	72
Mode	0
Standard deviation	65,3
Sample variance	4265,0
Kurtosis	3,0
Skewness	1,6
Range	332
Minimum	0
Maximum	332
Sum	9386
Count	106
Confidence level 95,0%	12,6

(c)

Installation C	
Mean	135,5
Standard error	7,1
Median	117,3
Mode	97,5
Standard deviation	73,6
Sample variance	5413,5
Kurtosis	0,4
Skewness	0,9
Range	337
Minimum	0
Maximum	337
Sum	14365
Count	106
Confidence level 95,0%	14,2

The purpose here is not to thoroughly discuss each and every one of the table entries above, but rather to highlight and comment the variables that are most interesting and perhaps differs a lot from the other installations. Most of the quantities are well-known, but a few of them may need a short explanation. Kurtosis is an introduced statistical quantity with the intention

of measuring the "heavyness" or "peakedness" of the tail of a probability distribution or data set. The highly positive kurtosis of Installation A reflects the fact that the major part of the inhibits were undertaken in the earlier phase of the time interval; it actually indicates that the trend of the curve is declining, as mentioned earlier.

The mean (or expected value) shows that the highest number of inhibits an arbitrary week during the period of investigation can be expected to be observed at Installation C. Moreover, the smallest dispersion from the mean, the standard deviation, can be anticipated at Installation B, which demonstrates that the distribution is more "even" or "uniform" there than at the other facilities. The sample variance is simply the standard deviation squared. The count is measured to be 106 for all the installations, indicating that the period of study ranges over 106 weeks.

The installations have all in common that they are witnessing at least one week where no inhibits were undertaken, hence the entry of minimum= 0. The range is equal to the maximum number of interventions from operator during a week, and the highest activity can be found at Installation A in the period November 18, 2008 - November 25, 2008. Here, it was carried out 442 cases of inhibit interventions. It should be reminded that "interventions" incorporates both activations and deactivations of the application. There are also cases where the operator performs an activation/a deactivation of the function multiple times, sequentially, with just seconds in between each action, or that the signal is broadcast several times due to unknown reasons. This aspect, however, is not accounted for in the analysis in order to avoid highly complex results.

Other basic quantities are *mode* and *median*. These say something about the value that appears the most frequently and the central value in a data sequence, respectively. Furthermore, by regarding the total amount of inhibits made during the entire test period, Installation C represents the facility with the most occurences with a number of 14 365, or 135,5 on average per week (which is the mean).

The standard error of the mean can simply be found by calculating $\sigma_m = \frac{\sigma}{\sqrt{n}}$, where σ is the standard deviation and n is the number of samples (the count). There is also presented a confidence interval corresponding to a confidence level of 95%, which assumes that the samples are normally distributed, or Gaussian. The intervals are not proposed explicitly, but can easily be found

by computing $\mu \pm z_{0,95}\sigma_m$, where $z_{0,95}$ is found by standard normal table lookup and μ is the mean.

Installation D and E

In, respectively, Figure 4.3 and Table 4.2 below, the results of the identical analysis which was carried out on the weekly inhibit data of Installation D and E, are introduced. Perhaps the most remarkable thing about the evolvement is the great difference in the utilization of the blocking facility in the earlier weeks of the test period. At this point in time, the activity at Installation E appears as, by far, much higher than the activity at Installation D. Which can be seen from the entries of the table that are representing the total amount of interventions taken place during the whole period, this is also the case when all the weeks of operation are accumulated together. Indeed, there are certain individual weeks that are functioning as major contributors to increasing the overall average, but the trend is generally that there are, especially during the first 60 weeks of the moving average, realized many more inhibits at Installation E than at D, before the pattern apparently flattens out and levels with the one of the other graph. Despite of this image, it is Installation D that possesses the week in which the most interventions were made; Week 89 with a count of 369 interventions.

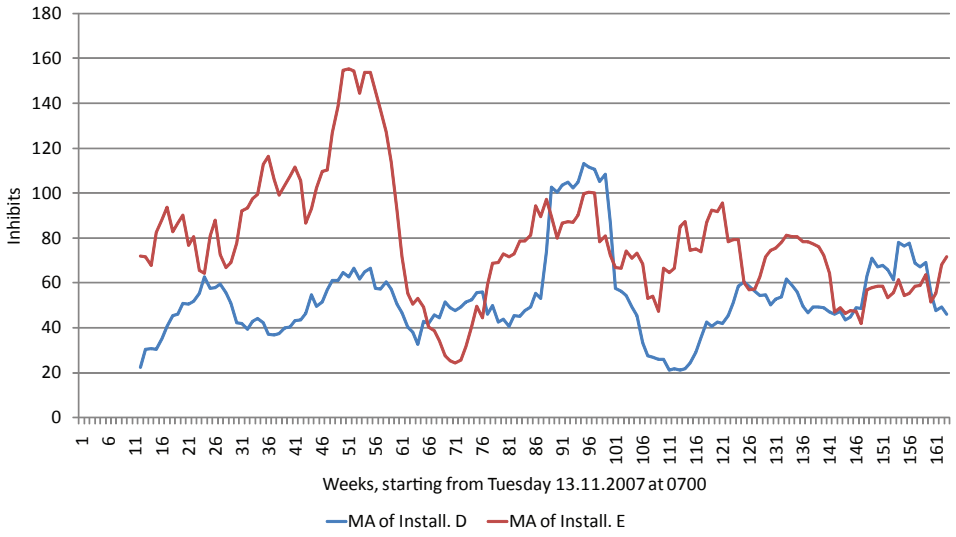

Figure 4.3: Moving average of inhibit involvement; D and E.

There is no longer any correlation to take notice of, neither any significant pattern that indicates any decline or increase in trend (besides the aforementioned situation at Installation E which will have a descending effect on a

plotted trend line), in contrast to the other installations presented earlier. The underlying causes to the clearly observable peaks at the week intervals 89-99 and 50-56 at Installation D and E, respectively, are in fact distinct. When the focus is turned back on the Excel worksheet where also the actual data are stored, it is trivial to detect that the direct cause to the peak period of Installation D is an abnormally high level of activity that takes place during the weeks 88/89 (with corresponding 272/369 inhibit interventions). However, the peak of Installation E stems from a critical period during the Weeks 44-50, where an extraordinary large amount of operator interferences were made.

Table 4.2: Descriptive statistics related to the weekly inhibit usage.

(a)

Installation D	
Mean	51,9
Standard error	3,8
Median	39
Mode	22
Standard deviation	48,9
Sample variance	2388,9
Kurtosis	13,4
Skewness	2,9
Range	369
Minimum	0
Maximum	369
Sum	8453
Count	163
Confidence level 95,0%	7,6

(b)

Installation E	
Mean	77,5
Standard error	5,2
Median	56
Mode	22
Standard deviation	66,5
Sample variance	4417,5
Kurtosis	0,4
Skewness	1,2
Range	265
Minimum	0
Maximum	265
Sum	12639
Count	163
Confidence level 95,0%	10,3

When the installations have been compared within their home families, it can be dedicated a few words to how the situation appears between the families. This is done best by considering the tables of statistics, and primarily the entry related to the mean; obviously, it can be expected a significant higher number of blockings during an arbitrary week of operation at one of the installations contained within the first family, than the second. Moreover, the usage of blockings in the second family of installations appears as more smooth and uniform (without taking into account the exceptional case in the start-phase of Installation E). This is also reflected by the standard deviation which states that the fluctuation around the mean is generally higher for the first family than for the second.

4.1.2 Overrides

Installation D and E

On an equal footing with the inhibits, the overrides were counted on a week-to-week basis, making it possible to reconstruct the operator actions at each installation in a plot. In this case, however, equally good results by utilizing the approach of moving averages were not possible to obtain. This was due to the scattered existence of override incidents compared to the inhibits. A moving average would have given a distorted impression of the actual situation, hence justifying the alternative solution of plotting the actual data in a bar diagram. A presentation of the conditions related to the override usage at Installation D and E will first be given, followed by the results that were obtained for Installation A, B and C. For the former case, the collected data are sketched in Figure 4.4, while the generated statistics are presented in Table 4.3.

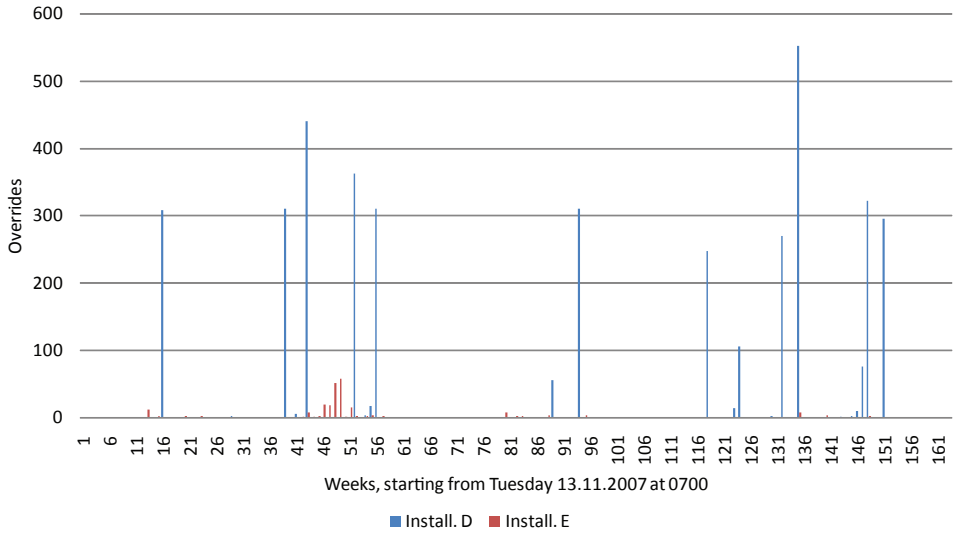

Figure 4.4: Weekly override activity at Installation D and E.

The chart primarily expresses the huge difference between the two facilities in the ways of perfoming plant control through the utilization of overrides. By assuming that already one override has been realized during an operational week at Installation D, the probability for that more than hundred others also have been carried out within the same week, is very high. This is worth dedicating a wondering thought; why is this the case? It has been impossible to obtain a good answer to this question, so it is recommended to investigate this further by competent people with sufficient insight into the

plant management. The information that is provided at this point in time is insufficient in order to draw any conclusion about this. This is why, as stated earlier, it is viewed as more important to present the situations as they actually appear based on the received logs, as this cannot be misinterpreted.

Another remarkable aspect is the overall small amount of overrides at Installation E. It is interesting to think of that it is actually legitimate to conclude that the ratio of the total amount of overrides at Installation D versus Installation E is 17, especially when the two facilities that have been considered belong to the same family of installations. Obviously, there is something fundamentally different in the approach of performing plant operation. It is not of particular interest to address the tables of statistics any further here, since the bar diagram speaks for itself.

Table 4.3: Descriptive statistics related to the weekly override usage.

(a)

Installation D	
Mean	24,7
Standard error	6,9
Median	0
Mode	0
Standard deviation	88,2
Sample variance	7779,9
Kurtosis	14,5
Skewness	3,8
Range	552
Minimum	0
Maximum	552
Sum	4025
Count	163
Confidence level 95,0%	13,6

(b)

Installation E	
Mean	1,5
Standard error	0,5
Median	0
Mode	0
Standard deviation	6,6
Sample variance	43,3
Kurtosis	53,3
Skewness	7,0
Range	58
Minimum	0
Maximum	58
Sum	237
Count	163
Confidence level 95,0%	1,0

Installation A, B and C

When the other family of installations is considered, it is easy to discover that the conditions regarding override interventions at the three facilities are not equally dramatic compared to the case above. The visualization of the results is presented in Figure 4.5, while the key statistics related to them are given in Table 4.4. Very rarely, it occurs a large number of overrides within one single week of operation. When this is said, there are still a few

weeks that are related to high activity; Week 44 at Installation C is the (by far) most hectic period - a total of 63 override interventions were realized. Furthermore, it is pointed out that Week 6, 46 and 70 are instances of busy periods at Installation C. The most eventful periods at Installation A are the weeks which are assigned the numbers 31, 48, 80 and 98. The period where the majority of the overrides were carried out at Installation B, were the Weeks 24 and 29. It is interesting to observe how the override actions are correlated between Installation A and B, with special regard to the peaks at Weeks 79/80 and 97/98.

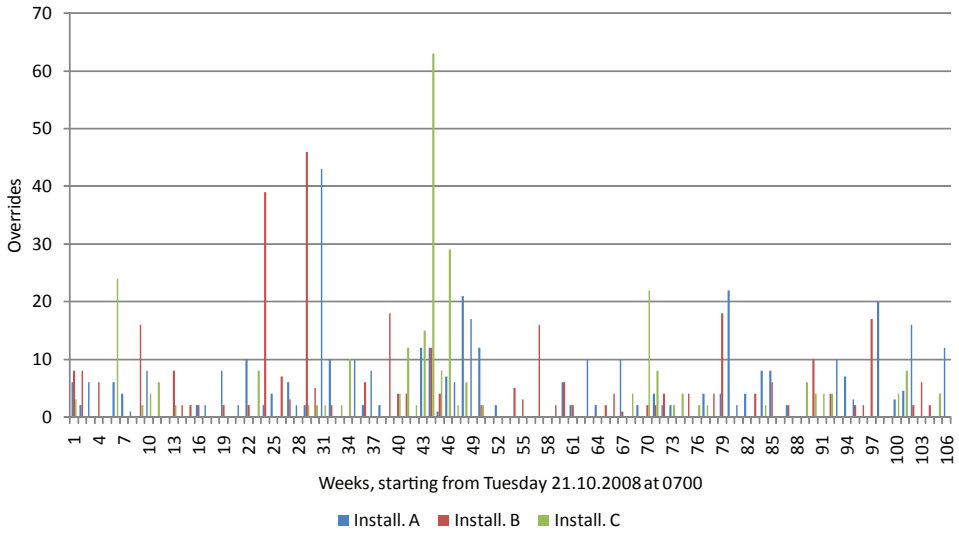

Figure 4.5: Weekly override activity at Installation A, B and C.

It cannot be said that there is something fundamentally different in the way of controlling the installations through the usage of overrides on the basis of the plot above and the tables below. However, if the two families are again set up against each other, it can be concluded that the application usage schemes for the two families are in fact so different that they are nearly incomparable; Installation D exhibits an abnormally high utilization during certain weeks, Installation E exhibits a noticeable low amount of overrides during an arbitrary week, while the installations contained within the first family display a less dynamical and ”more stable” practice of the override feature.

Table 4.4: Descriptive statistics related to the weekly override usage.

(a)

Installation A	
Mean	3,8
Standard error	0,6
Median	2
Mode	0
Standard deviation	6,3
Sample variance	39,7
Kurtosis	14,2
Skewness	3,1
Range	43
Minimum	0
Maximum	43
Sum	408
Count	106
Confidence level 95,0%	1,2

(b)

Installation B	
Mean	3,2
Standard error	0,7
Median	0
Mode	0
Standard deviation	6,9
Sample variance	47,1
Kurtosis	20,6
Skewness	4,1
Range	46
Minimum	0
Maximum	46
Sum	340
Count	106
Confidence level 95,0%	1,3

(c)

Installation C	
Mean	2,7
Standard error	0,7
Median	0
Mode	0
Standard deviation	7,6
Sample variance	58,2
Kurtosis	38,7
Skewness	5,6
Range	63
Minimum	0
Maximum	63
Sum	290
Count	106
Confidence level 95,0%	1,5

4.1.3 Other comments on trend tendencies

Another interesting finding that was made during the survey of this seciton, is that the operator activity with respect to activation and deactivation of

inhibits tend to increase in the time-neighbourhood of shift interchanging. This indicates that the operators, as individuals, are having preferences in terms of what kind of signals they want to keep blocked when they are in charge of the SAS. The tendency is generally that some occurences of blockings that have been made at an early stage of the shift, are being annulled just before a different crew is taking over the control. Then, when the new operator is in place, other tags are being subject to the same pattern. This may imply that there is no clear, congruent instruction which exclusively is being met during operation.

A different pattern can be observed when regarding the activity at day versus night. Without going into any details, it can confidently be said that the major part of events concerning plant process operation are taking place during daytime. This is actually no surprise; the daylight is providing visibility, hence making every job task easier to perform. Furthermore, there are presumably more workers on duty at day than at night, making it possible to attain a higher rate of production at daytime.

4.2 Frequently involved tags

Some signals are more involved in blockings/overrides than others, and the primary interest in this part of the study is to act as a watchdog for these "vulnerable" signals. It is not desirable that signals are exposed to these impairments more often than necessary, thus it is not preferable that an operator performs active process control through regulation of information flow between logic solver and sensor/final control element. Furthermore, it will be useful to observe which groups of signals that stand out at the respective installations, i.e. whether it (for example) seems to be a collection of temperature tags that tops the list of "the most busy tags", or a group of level signals. It will also be of significance to notice if the operator involvement pattern tends to vary among the facilities. Once again, it is stressed that the analysis aims at providing the reader with an overall (general) picture of the situations rather than reflecting the more detailed, event-specific image.

4.2.1 Inhibits

As each inhibit/override is implemented and realized in the system, the event pops up in the total overview in addition to being recorded in separate inhibit/override logs. All these cases of events were counted and stored in a worksheet so they could be visualized through diagrams. Because the time

scales of the logs originating from the different installations varied widely, a solution to the presentation problem had to be found. It was concluded that the best way to propose the results so that the possibility for comparison was not completely ruled out, was to divide the total amount of interventions related to each tag by the number of weeks with provided log data, so that the quantity "number of interventions per week, on average" was obtained. The quantity represents the frecuency of occurences in an orderly way and has the corresponding denomination $\frac{intervention(s)}{week}$. This can be attested by the y-axes of the sub-figures included in Figure 4.6. More specifically, the figure shows the three most frequently inhibited signals at each installation. Due to excessive space requirements, there was not room for presenting more than three characteristic signals related to each installation.

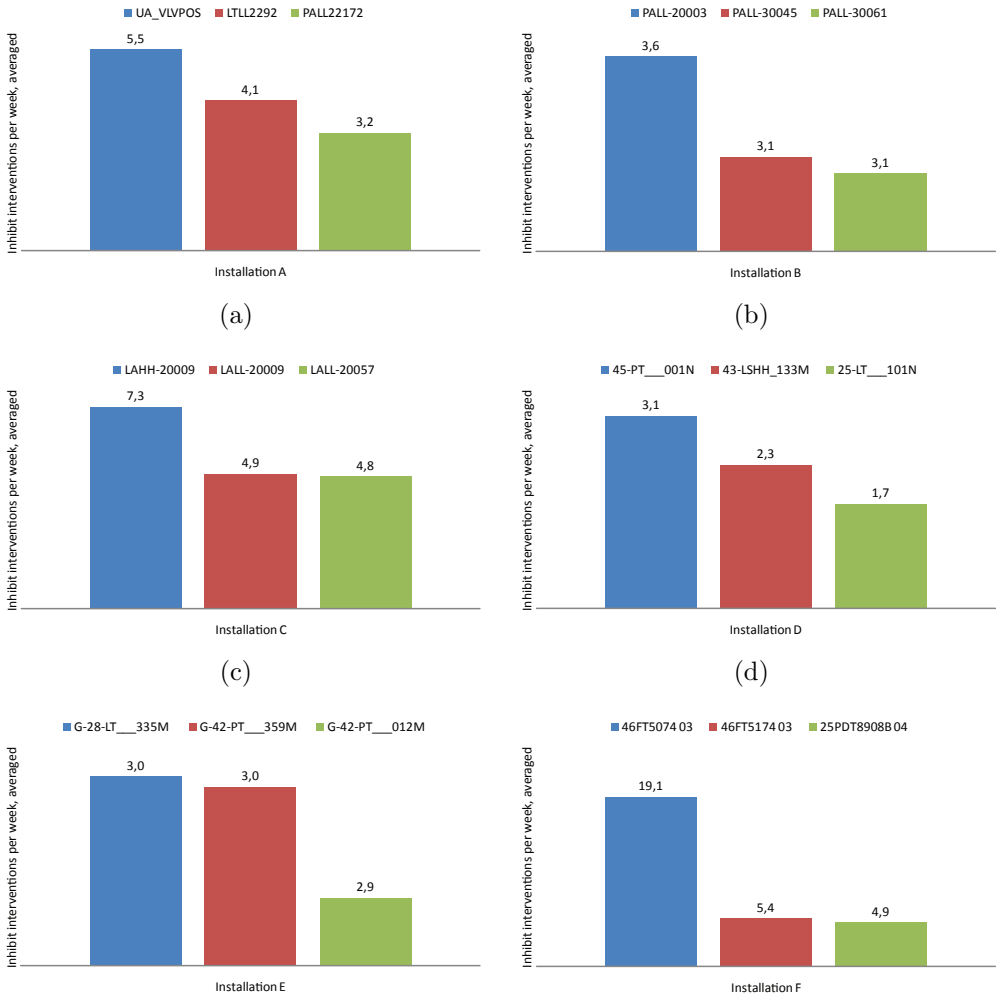

Figure 4.6: Top three most frequently inhibited signals.

Since Installation A, B and C are installations belonging to the same family, it would be obvious to believe that the difference between their way of practicing inhibits is not very large. However, if their correspondig figures are considered, this hypothesis is both correct and erroneous at the same time; the tags coming in as 1^{st}, 2^{nd} and 3^{rd} place in the overviews do all appear with the approximately same frequency compared to each other, except for LAHH-20009 which turns out to be quite superior. In addition to this, it is fascinating to observe that there are only pressure-related signals represented in the plot of Installation B, while at Installation C there are only level-related signals. This may indicate that there exist distinct thoughts

related to the application usage between the different installation's personnel, and that it is reason to believe that these thoughts are reflected through their daily operation. It is not a part of the task to draw any conclusions about this issue, since the base of information and results is too weak for this. In any case, it is interesting to dedicate the topic some thoughts and philosophize over some of the differences that are showing up. However, the most important thing is to let the numbers speak for themselves. Regardless of this, there should exist one common guideline that describes, step by step, what should be done if the need for the application arises.

Another remarkable aspect with the figure, is that the onshore facility (Installation F) exhibits a superior domination over the others; the tag 46FT5074 03 has a weekly average of $19,1 \frac{interventions}{week}$. This is beyond what any other installation can display, hence the "reward" for including such an installation in the study as well, begins to emerge. It should be recalled that the provided log time period only spans the first three months in the year of 2011, in contrast to the other logs coming from the rest of the installations which are covering up to several years of events. However, because the history can attest that the tag is being interfered with and engaged very often and at regular time intervals, the possibility for that this is just accidental within a small time interval, can nearly be eliminated. Since the number of appearances of this tag in the overview differs so much from the signals coming in as 2^{nd} and 3^{rd} place at the same installation, one can assume that there are problems with the element itself or the signal being transmitted from it, that is root to the frequent operator intervention. Incidentally, the affected signal is related to an outlet of a pump which is member of a pump network providing a second-order level of redundancy. The situation at Installation D and E shall not be discussed in any large extent, since there were no noticeable outcomes here. The operator behavior at the two installations seems quite similar, and both pressure and level transmitter tags are incorporated in the rankings.

4.2.2 Overrides

Figure 4.7 portrays the results of the same analysis which was done for the overrides. It is clear that there are some cases also here that stand out from the rest of the group. The first thing that comes to mind is the large difference between the amount of overrides applied to the top signal of Installation C compared to all the others, included the signals for the installations within the same family. The high frequency of the appearances of this signal was also discovered in an earlier work, so for more detailed information on this

the reader is referred to [6]. Beyond this, it can generally be said that interference with the override application on selected signals within family one, generally is higher than for family two, where the utilization of overrides is less widespread and frequent. It must not be forgotten that it was found earlier (from the descriptive statistics of the overrides) that it occured approximately 17 times more overrides at Installation D than at E during the entire test period. The fact that the frequency related to each signal is quite equal between the two, is just witnessing that Installation D involves a much wider constellation of signals in the overall override process.

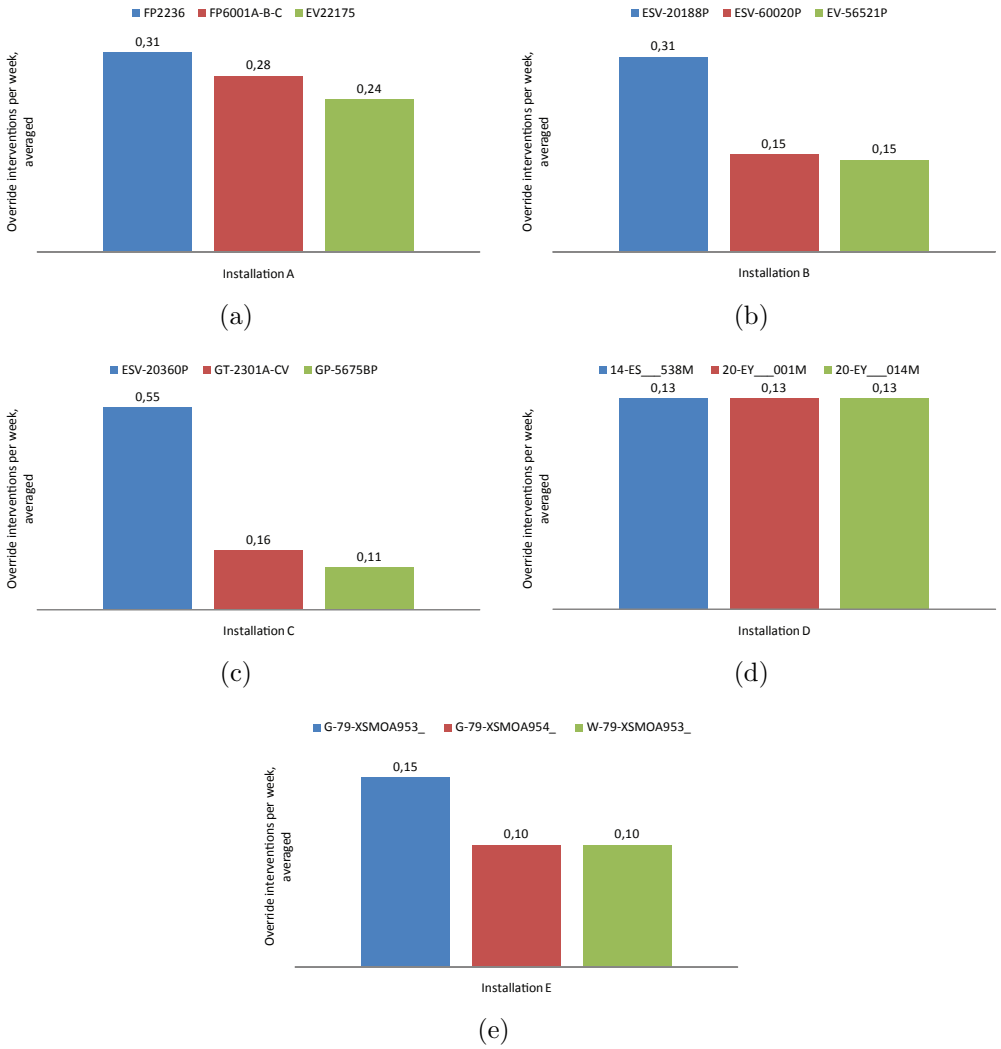

Figure 4.7: Top three most frequently overridden signals.

It is also useful to address the distinction in types of tags that are overridden

most frequently at the different facilities. Because of vaguenesses or total lack of tag description, this is not always feasible. For Installation B and D there are only ESD-related signals which are represented in the diagram. These are typically actions taken by the operator in order to prevent a shutdown event so that production is maintained. At Installation C, it is also an ESD-related signal at the top, followed by two shutdown signals to an unknown element and a pump, respectively.

4.3 Long-term instances of the applications

Since the method that was used to reveal long-term events is based on examining the logs with the human eye, the guarantee for that all existing cases are found, vanishes. The majority of the instances, however, will still be discovered with high probability, since this section's study (especially) was devoted high accuracy and thoroughness. For consistency and practical reasons, the quantities describing the results in this section will be given in "interventions per week, on average", as in the previous section. From an overall perspective, it was observed many cases of long-term events (inhibits/overrides that lasted for more than one month), thus a list of each and every one of them would not have functioned as a descriptive source of information. No general indication of the situations could have been extracted from this, in addition to that the reader would have experienced such an approach as overwhelming. Every single long-term event is, however, addressable in the Excel worksheet that was used to store the acquired information, and which the histograms that follow are based on.

4.3.1 Inhibits

Before moving on to discuss the results, it is once again emphasized that an intervention is either an activation or a deactivation of an operation. This means that the number of activations is approximately the number of interventions divided by two. This philosophy does also imply that an SF that gets disabled and never gets enabled back, only is counted as one intervention, while an SF that is subject to both a deactivation and a reactivation is counted as two interventions. Figure 4.8 proposes the results that were found in the counting of long-term inhibit interventions for each installation.

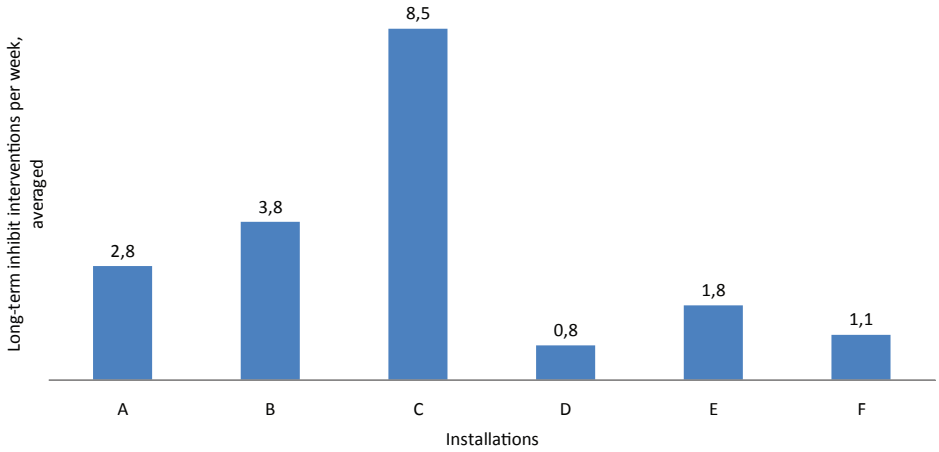

Figure 4.8: Overview of long-term inhibit instances.

As noted earlier in the theoretical part of the thesis, the risk associated with an impairing operator action increases dramatically in line with the time the impairing event is alive. When the above results are interpreted in light of this statement, the fact that the greatest danger related to long-term inhibits can be found in the operation of Installation C, can easily be established. There are more than twice as many occurences of long-term interventions here than at Installation B, which represents "the second worst facility" in terms of long-term inhibits. Obviously, the first family of installations stands particularly out in a negative way. Also included in the results are signals that have been blocked and later phased out and deleted from the system, where perhaps new signals (with new tag numbers) have replaced the former. There is no overview available of the signals this apply to, and it is just a small percentage of the signals that are subject to a replacement, hence this aspect is not important to take into account when interpreting the results. On average, the operators at Installation E intervene with one more long-term instance of the blocking function compared to Installation D during an operational week, which is not an appreciable difference (nor a particularly high number). This also applies to Installation F, where the operators seem to be good at avoiding long-term instances of inhibits.

4.3.2 Overrides

In general, it is realized a lot more inhibits than overrides during the operational time of an installation. The explanation to this is that the need to prevent shutdown actions does not arise with an equally high frequency as the need for making the logic independent from certain sensor input signals,

in addition to the fact that an override possesses the potential of exerting a greater danger than an inhibit. This is due to the fact that the last and crucial element in the chain of information flow (the final control element) which is the only element with the ability to affect the existing process state, is restrained in its action. Despite this, it is actually carried out many more long-term overrides than inhibits at Installation D, which can be seen from Figure 4.9. This is an alarming observation and a very exceptional situation compared to the others. The situation at Installation C is also completely reversed, but this time in a positive way; from being the installation that possesses the highest number of long-term instances of blockings, it is now a facility that exhibits an excellent practice in terms of nearly not realizing any long-term overrides at all (just 0,03 per week).

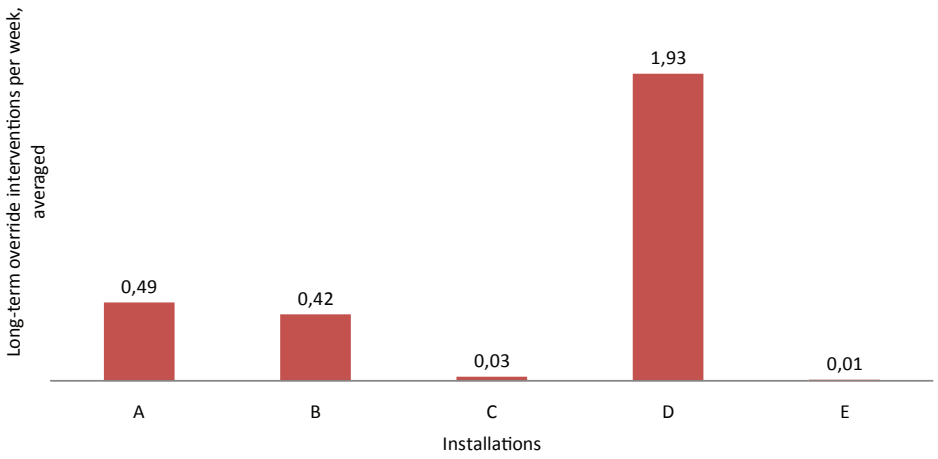

Figure 4.9: Overview of long-term override instances.

From the descriptive statistical quantities (and incidentally from the plot) related to overrides previously presented in the section about trends and statistics, it was seen that the total amount of overrides carried out at Installation D compared to E, was huge. This leads to that the results presented in this section should not surprise anyone in particular, since they actually are a direct outcome of the aforementioned; it is easy to understand that the relationship between overrides in general and long-term overrides is highly correlated - if many overrides are realized at a plant, it is more likely that there are realized a certain amount of long-term overrides as well, in contrast to the situation at an installation where there are carried out nearly zero overrides. Nevertheless, it is not good practice, nor an excuse for a facility to have so many long-term cases alive during daily operation, even though

the amount of overrides is high. It is obviously the application usage in general that should be considered to get the numbers down, since the long-term situation consequently will be improved if improvements are made towards the everyday, ordinary usage. Beyond this, there shall be given credit to the operators governing the SASs at Installation C and E that set a good example for the others.

4.4 Redundant inhibits/overrides

It is related a considerable amount of danger to blocking of redundant sensor signals and overriding of redundant control elements. It is important to be aware of that not all divisions of a plant (or its process) are provided with redundancy, but only selected, often critical areas. This makes it even more important to not pull these elements out of operation synchronously. The resulting situation would have been that none of the scheduled elements had been able to respond to any process request showing up on-demand, which potentially can lead to hazardous events.

Again, it is emphasized that it was not possible to verify 100% whether the following results correspond to cases of redundancy or not, but that it can be considered as "most likely" that this is true, taken into account the signals' appearance and naming. Assuming that the given cases actually are redundant, the collaborating company (Statoil ASA) has the opportunity to investigate the findings further. The main objective of this sub-problem's analysis is not to draw any definitive conclusions, because there exists an element of uncertainty in the base data. However, the objective is rather to propose the cases that may be interpreted as redundant, and that have been observed in the log. Since none of the installations displayed any huge interference with redundant inhibits/overrides, it was actually possible to present the complete collection of findings in tables, something that was not appropriate to direct for the long-term case.

4.4.1 Overrides

Table 4.5 offers an overview of all the detected cases of (possibly) redundant output signals that have been overridden simultaneously. The reason for that single tags like FP5008A-B and FP6001A-B-C are also included in the table, is because it is taken into account that such signals have the potential of being connected to more than one element, i.e. A and B for the former, and A, B and C for the latter. The table specifies how many overlapping intervals

of the tags that have been observed, in addition to stating the duration of the longest coinciding "inoperative" period. As explained earlier, Installation A, B, C and F are the installations regarded in this analysis. Among these, override history is provided for the first three, so the table reflects the override situation at the Facilities A, B and C.

Table 4.5: Simultaneously overridden redundant signals.

(a)

Installation A		
Identification	Overlapping intervals	Longest duration
FP5008A-B	1	9 sec
FP6001A-B-C	15	3 days
SD_RC_A-B_CSP	1	1 year +
SD_RC_A-B_CSV	2	24 days

(b)

Installation B		
Identification	Overlapping intervals	Longest duration
EV-53001A-BP	1	3 days
GP-2001A_B	2	7 sec
GP-2002A_B	6	18 min
GP-2005A_B	1	6 sec
GP-5614AP GP-5614BP	1	53 min
GP-5631AP GP-5631BP	2	1 h 50 min
GP-5803A-BP	1	50 min
GT-2301A-CV GT-2301B-CV	1	4 h

(c)

Installation C		
Identification	Overlapping intervals	Longest duration
GP-2505A-BP	1	3 sec
GP-5650A-BP	2	6 sec
GP-5676AP GP-5676BP	1	27 sec
GT-2301A.CV GT-2301B.CV	1	9 h
GT-2301A-CV GT-2301B-CV	1	9 h

The outcomes shall only be commented on briefly and not discussed in any greater extent, because of the uncertainty that is associated with them. Installation A holds the lowest number of involved redundant signals (only four

in total), but yet it possesses the definitely longest period of override duration among all, here represented by 1 year +. This means that the tag was observed to be overridden for one year, until the log ended. However, there are only observed single tags in this log, which is in contrast to the other two production units included in the table. Installation B and C exhibits a two-level redundancy scheme on, for example, some of their pumps which are addressed by the tag prefix GP. Incidentally, it can be seen that their corresponding overlapping intervals are of a very short-term character, which is reassuring and positive.

4.4.2 Inhibits

To familiarize with the results related to the identical study carried out for the inhibit application, it is referred to Table 4.6 and 4.7. It was not room for containing all the results in one large table (consisting of sub-tables) as above, so they were distributed in two. There were not found any cases of synchronously blocked redundant signals in the log of Installation B, hence the table entries consistently filled with NULL. Moreover, it can be seen that Installation C and F can be accounted for the highest number of involved redundant tags, and that, among these, Installation F surprises (negatively) by having "managed to" perform so many redundant inhibits in such a short time (3 months of provided log). There are even found cases of third-order redundancies on some of the level and pressure transmitters (LT and PT, respectively). It can also be observed that the last two cases in Table 4.6 are referred to as COMPLICATED. The reason for this is simply that it was very difficult to ascertain the number of occurences of simultaneous redundant overrides that were undertaken for these particular tags, and their corresponding duration. At the risk of providing incorrect information, these quantities are not specified.

Table 4.6: Simultaneously inhibited redundant signals.

(a)

Installation A		
Identification	Overlapping intervals	Longest duration
PAHH61543A PAHH61543B	25	8 days

(b)

Installation B		
Identification	Overlapping intervals	Longest duration
NULL	NULL	NULL

(c)

Installation C		
Identification	Overlapping intervals	Longest duration
LAHH-57031A LAHH-57031B	8	4 h
LAHH-57041A LAHH-57041B	25	9 h
LALL-57031A LALL-57031B	20	4 months +
LALL-57041A LALL-57041B	45	20 days
PAHH-24134A PAHH-24134B	1	30 min
PAHH-56873A PAHH-56873B	1	6 h
PAHH-56878A PAHH-56878B	1	4 min
PAHH-56890B PAHH-56890C	1	2 min
PAHH-60017A PAHH-60017B	1	1 day
PALL-56866A PALL-56866C	6	1,5 months
PALL-56873A PALL-56873B	COMPLICATED	COMPLICATED
PALL-56878A PALL-56878B	COMPLICATED	COMPLICATED

Table 4.7: Simultaneously inhibited redundant signals.

Installation F		
Identification	Overlapping intervals	Longest duration
29LT4074A 03 29LT4074B 03 29LT4074C 03	2	20 min
29LT5035A 03 29LT5035B 03	1	3 days
29LT5074A 03 29LT5074B 03 29LT5074C 03	3	3 days
29PT5086A 03 29PT5086B 03 29PT5086C 03	2	30 min
29PT8528A 03 29PT8528B 03 29PT8528C 03	2	20 min
40FT5004A 04 40FT5004B 04	1	5 min
46LT8641A/B 03	2	4 h
46LT8641A/B 04	2	4 h

Chapter 5

Conclusion and recommendations

5.1 Conclusion

Based on the received event logs consisting of variable lengths, it can with great confidence be stated that there are carried out more inhibits at the first family of installations (Installation A, B and C) than at family number two (Installation D and E) during normal plant operation. However, when this is said, the diagrams indicate a falling trend for all the facilities within the first family, which is a positive evolvement of the application usage. Another fascinating aspect is that Installation E seems to exhibit a critical period at an early stage of the test period, where an unusual large amount of inhibits were undertaken during, in particular, the weeks of 44 through 50 (relative the time scale that was constructed internally).

When it comes to the concluding remarks about the overall picture of overrides, it shall be emphasized that the way of controlling Installation D versus E in terms of override utilization, turned out to be fundamentally dissimilar. It was conducted as many as 17 times more overrides during the entire period of study at the former facility compared to the latter. In the meantime, the answer to this mystery is unknown, and the reason may never be revealed unless further investigation is provoked. Moreover, it was seen that the operator activity at daytime is higher than at night, and the activity around shift interchanges is also generally higher than during other operational time.

After having all the different tag overviews examined, it was feasible to conclude that both PT and LT tags were the tags which showed up the most in

relation with the inhibit application. Similarly for the overrides, there were typically ESVs and pumps that were affected and had the highest ratio of appearances in the log. Especially, Installation C possesses a shutdown signal that stands particularly out when measuring the inhibit occurences by number of interventions per week, averaged. This is incidentally the same signal that also was found in the analysis of the predecessor of this thesis (ref. [6]). When only considering the offshore facilities and comparing within the collection of these, the most frequently inhibited signal can be found at Installation C, as well. However, the onshore facility, Installation F, stands for the most remarkable outcome of this sub-study; the signal that possesses the highest ratio of appearances in the inhibit log can be found here. The corresponding tag was interfered with 19,1 times per week, compared to 7,3 which is representing the value of the second most frequently inhibited signal of them all.

In the analysis concerning long-term cases of blockings and overrides, there were made some quite interesting discoveries; family *one* of installations tends to realize a lot more long-term inhibits than the rest of the facilities. Again, Installation C is characterized as "the worst" facility of them all, with over twice as many occurences of long-lasting inhibits (at least one month of duration) compared to Installation B, which is the second worst facility. But, however, the situation is completely changed when the focus is moved over to the study of long-term overrides. Here, Installation C exhibits an outstanding practice, while Installation D is "the big bad wolf". This is in fact very fascinating, since Installation E, which is included in the same family as Installation D, does not carry out any long-term instances of overrides at all, so to speak.

Simultaneous cases of inhibits/overrides of redundant elements were more or less just listed as proposals or suggestions due to the uncertainty related to the results which made it impossible to draw any definite conclusions. Because of the lack in informative material, it was not possible to state whether an event in the log represented a redundant element or not. For this reason, concluding remarks about this topic shall be omitted.

5.2 Recommendations for further work

In this study, it has been necessary to completely and solely rely on the events appearing in the logs, which of course is not an optimal solution. To be able to make comments on the compensating measures that have been implemented in the different situations, and whether an operator action that

has taken place is in accordance with standards/regulations, and if the action is actually considered necessary to go through with under the given circumstances, it requires that more comprehensive monitoring of the operators/CCR is applied. However, this will also demand greater resources and perhaps that the survey is conducted on an oil rig, or something similar. Below, it is given some definite suggestions to what can be done:

- get access to internal Problem and Improvement (P&I) documents so that well-known operational problems can be mapped to individual, critical situations reflected in the log
- address the constellation and direction of flow of the different processes at the different installations, utilizing Piping and Instrumentation Diagrams (P&ID) to gain process insight
- make oneself personally acquainted with how things evolve in the CCR and how the staff are working, i.e. to interfere with the SAS and the equipment that is used and to see how the staff approaches their duties in practice

Appendices

Appendix A

A practical example

It is reasonable to claim that a practical control problem in the process industries, and especially in the petroleum industry, is to drive the pressure in a tank filled with gas to a desired setpoint-pressure decided by a superior controller (perhaps by the use of an MPC scheme) or by an operator. A possible solution to this problem is to use the basic principle of feedback control. Such a classical feedback structure is shown in Figure A.1. This is a simple structure where the reference values[1] of the controlled variables, which enter the summation sign from the left on the figure, are compared with the actual measurements of the corresponding states[2] in the plant process [25]. The measured values are subtracted from the setpoint values, and the error terms are fed into a controller algorithm which decides the magnitudes of the control signals that are to be applied to the corresponding final control element actuators. The system continues this dynamic behaviour until the closed-loop equilibrium is achieved, i.e. the reference values are equal to the measured values. Furthermore, if it can be assumed that the closed-loop system exploits a controller strategy that makes operation at the (linearized) system's equilibrium points Globally Asymptotically Stable (GAS), convergence towards the reference values can be guaranteed [26].

[1] A state's reference value is the desired output value of the state.

[2] Often, it is not possible to trivially/directly measure the values of the states that are to be controlled. In that case, a state estimator can be used.

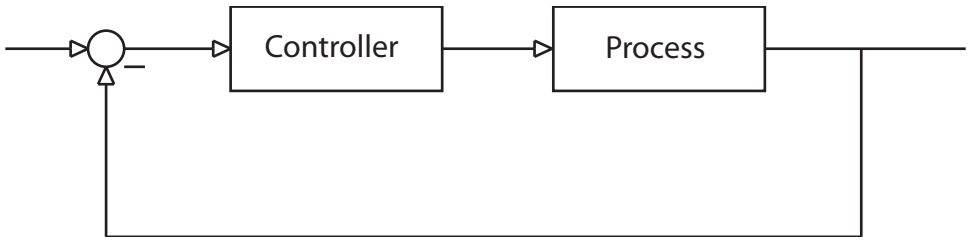

Figure A.1: Classical feedback structure as known from the literature.

The problem is visualized in Figure A.2 under the same conditions it was proposed in the text above. Additionally, the possibility for that the tank may contain flammable gas is held open, as it goes out from the figure. Clearly, the feedback philosophy has been implemented, and the controller is provided with a measurement of the pressure in the tank which is obtained from a manometer. The value of the control signal, which is to be sent to the servomechanism of the controllable valve, is based on the error between the pressure measurement and the given setpoint. There are many alternatives when it comes to the choice of controller strategies, depending on what kind of properties the person in charge wants the closed-loop system to possess. This will, however, not be discussed any further due to its irrelevance with respect to problem description.

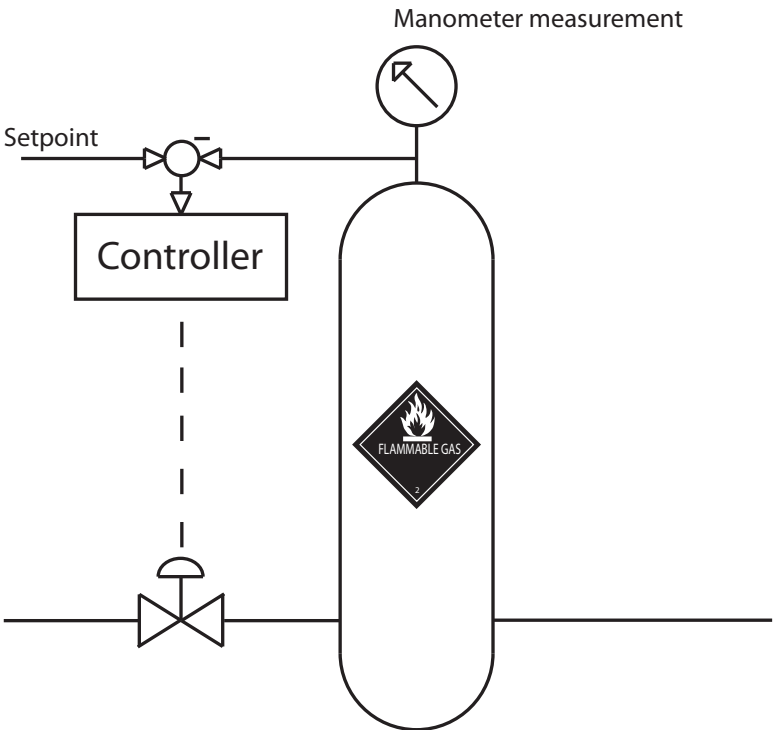

Figure A.2: Representation of the closed-loop system.

After having built up the problem and made a presentation of it, the purpose of this example will be to demonstrate and comment on how the applications inhibit and override will affect the the process behavior in general. By recalling that the inhibit functionality is applied to an input signal, and that the override is applicable to output signals, there will be no doubt about the following statements:

- an inhibit directed towards the signal leading from the manometer measurement to the controller/logic solver will be equivalent to not include the actual tank pressure values in the calculation of the control signal
- an override directed towards the signal leading from the controller/logic solver to the pressure control valve will be equivalent to not take the computed control signal into account when controlling the pressure in the tank. Accordingly, this does also neglect (indirectly) the actual measured values coming from the manometer.

It can easily be imagined that improper usage related to the applications may lead to pressure build-up and potentially dangerous situations. Changes in process states (gas pressure, temperature, etc.) may happen faster than

assumed, and the risk for explosion and fire will consequently be within the scope of realistic consequences.

Appendix B

Application of IEC 61508/61511

In some cases, formal standards such as IEC 61508 and IEC 61511 can be found hard and confusing to interpret. This may be because of the academic language that is used, or because it is not definitively stated in each and every case what should be done to meet the different requirements. With the intent of making it easier to implement the above-mentioned standards in practice, The Norwegian Oil Industry Association (OLF) has issued a guideline which helps the user to construct an SAS that shall meet the minimum requirements for SIL. In this appendix, the most relevant aspects concerning the operator usage of the facilities inhibit and override in the guideline will be presented, referring to [27].

One of the demands, is that all the inhibits/overrides/bypasses (impairing actions, basically) shall be notified to the operators located in the control room, usually through canalization of the SAS and the HMI that is supported there. Furthermore, it is proposed that the facilities are provided with some kind of password protection, so that arbitrary persons are not able to access the critical functions of the system. It is also suggested that the override functionality should be considered to completely be eliminated for safety functions characterized by an SIL of 3 or higher. As in some of the other standards, this guideline also considers it appropriate to limit the time an override shall be permitted to be alive in the system (including test overrides), depending on the SIL class. "Watchdog timers" can be employed for this purpose to rule out the possibility for forgetting overrides that have been realized in the past.

The guideline emphasizes that functional tests, or proof tests, are preferred

to be carried out as integral tests. This means that the complete SAS loop which the relevant element is part of is tested, even if the functionality of, for example, a sensor or final control element is the only verification objective of the test. Tests of shutdown valves are suggested to be scheduled at points in time when process shutdown is planned on beforehand (regardless of the testing), in addition to execution at regular time intervals. Beyond this, the issue about compensating measures is devoted an own section, but since this has already been discussed adequately, no further comments will be made here.

In Appendix G of OLF-070 it is, inter alia, expressed that IEC 61508/61511 require that the Critical Action Panel (CAP) shall provide a global mechanism that makes it possible to disable all inhibits/overrides that are currently active in the system. An CAP is typically an extension and part of the total SAS interface which is usually placed in the location environment of the operator stations, making it easily accessible. Other requirements in the guideline that have not been mentioned here, are either considered as irrelevant or have already been discussed previously in the main contents of the thesis.

Bibliography

[1] NORSOK I-002, "Safety and Automation System (SAS)," Rev. 2, May 2001. Norsk sokkels konkurranseposisjon.

[2] IEC 61508 (all parts), "Functional safety of electrical/electronic/programmable electronic safety-related systems," 2nd Edition, 2010. International Electrotechnical Commission.

[3] Tor Onshus, *Instrumenteringssystemer*. 5. utgave, januar 2011.

[4] CSB, "Final Investigation Report on BP Texas City Refinery Explosion and Fire," March 2007. U.S. Chemical Safety and Hazard Investigation Board.

[5] NCOE, "Overview and Guidance on the Management of Overrides," Newcastle Chambers of Engineering, Technical Note: 015.

[6] Anders F. Johansen, "Inhibits and Overrides - Applications seen in a safety perspective," December 2010. Project work.

[7] Stein Hauge, Stig Ole Johnsen, Tor Onshus, "Uavhengighet av sikkerhetssystemer offshore," 2009. Petroleumstilsynet.

[8] NORSOK S-001, "Technical safety," 4th Edition, February 2008. Norsk sokkels konkurranseposisjon.

[9] Dick Caro, *Automation Network Selection: A Reference Manual*. ISA: The Instrumentation, Systems, and Automation Society, 2nd Rev. Edition, 2009.

[10] IEC 61511 (all parts), "Functional safety - Safety instrumented systems for the process industry sector," 1st Edition, 2004. International Electrotechnical Commission.

[11] Mary Ann Lundteigen and Marvin Rausand, "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," May 2007. Department of Production and Quality Engineering, The Norwegian University of Science and Technology.

[12] Statoil ASA, "Override concept," Internal document.

[13] OLF Guideline 088, "Recommended Guidelines for Common model for Work Permits (WP)," September Rev. 2, 2003. The Norwegian Oil Industry Association.

[14] StatoilHydro ASA, "Tiltak ved svekkelser i sikkerhetsfunksjoner," Internal document.

[15] Stein Hauge, Mary Ann Lundteigen, "Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase," 2008. PDS - multiclient.

[16] Paul Gruhn, "The evaluation of safety instrumented systems - tools to peer past the hype," *ISA Transactions*, vol. 35, 1996.

[17] Geir A. Espnes and Geir Smedslund, "Helsepsykologi," 2. utgave, 2009. Gyldendal akademisk.

[18] PSA, "The Framework Regulations," Regulations after January 1, 2011. Petroleum Safety Authorithy Norway.

[19] PSA, "The Management Regulations," Regulations after January 1, 2011. Petroleum Safety Authorithy Norway.

[20] PSA, "Risk level in the Norwegian petroleum activities," Rev. 12, 2010. Petroleum Safety Authorithy Norway.

[21] ISO 17776, "Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment," 1st Edition, 2000. International Organization for Standardization.

[22] CSB, "Safety Video: Explosion at BP Refinery," 2007. U.S. Chemical Safety and Hazard Investigation Board, `http://www.youtube.com/watch?v=c9JY3eT4cdM&feature=player_detailpage`.

[23] Jerry M. Mendel, *Lessons in Estimation Theory for Signal Processing, Communications, and Control*. Prentice Hall, 2nd Edition, 1995.

[24] Ronald E. Walpole, Sharon L. Myers, Raymond H. Myers and Keying Ye, *Probability and Statistics for Engineers and Scientists*. Prentice Hall, 9th Edition, 2011.

[25] Jens G. Balchen, Trond Andresen, Bjarne A. Foss, *Reguleringsteknikk*. Tapir, 5. Utgave, 2003.

[26] Hassan K. Khalil, *Nonlinear Systems*. Prentice Hall, 3rd Edition, 2001.

[27] OLF Guideline 070, "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry," October Rev. 2, 2004. The Norwegian Oil Industry Association.

[28] J. M. Maciejowski, *Predictive Control with Constraints*. Prentice Hall, 1st Edition, 2001.

[29] StatoilHydro ASA, "Tiltak ved overbroinger, utkoblinger eller andre svekkelser av sikkerhetssystem," Internal document.

[30] YA-710, "Prinsipper for utforming av alarmsystemer," February 2001. Oljedirektoratet.

[31] Marvin Rausand, "Chapter 10 Reliability of Safety Systems," April 2004. Department of Production and Quality Engineering, The Norwegian University of Science and Technology, `http://www.ntnu.no/ross/srt/slides/chapt10.pdf`.