



SUOMEN SOODAKATTILAYHDISTYS
FINNISH RECOVERY BOILER COMMITTEE

Finnish Recovery Boiler Committee

**SAFETY INSTRUMENTATION
GUIDELINES FOR RECOVERY BOILERS**

Finnish Recovery Boiler Committee

Automation Work Group

15.1.2003

8.9.2008 Rev A



DISCLAIMER

By obtaining these guidelines, the user acknowledges and agrees to the terms of this disclaimer.

Finnish Recovery Boiler Committee is not responsible for the information, any errors or omissions, or for the results obtained from using this information. Use of this document shall be at user's sole risk. Such use shall constitute a release and agreement to defend and indemnify Finnish Recovery Boiler Committee from and against any liability, whatsoever in type or nature, in connection with such use, whether liability is asserted to arise in contract, negligence, strict liability or other theory of law.

The document is based on part on information not within Finnish Recovery Boiler's control. While the information provided in this document is believed to be accurate and reliable under the conditions and subject to the qualifications set above herein, Finnish Recovery Boiler Committee makes no representation or warranty, expressed or implied, as to the accuracy or completeness of the information provided in this document or any other representation or warranty whatsoever concerning this document. In no event will Finnish Recovery Boiler Committee or its affiliates thereof be liable to you or anyone else for any decision made or action taken in reliance on the information on this document or for any consequential, special or similar damages, even if advised of the possibility of such damages.



INTRODUCTION

The members of the Finnish Recovery Boiler Committee have desired a clear set of instructions about the implementation of the safety instrumentation for recovery boilers. This is due to a concern about safety and the variety of implementations between different manufacturing plants.

The first version of the guideline published in 2003 was revised in the autumn of 2009. In the revised guideline, the information that had become available by the autumn of 2008 was made use of. The new revision introduces the calibration of a risk graph for a recovery boiler, clarifies model interlocks and documentation needed as well as presents some theory about the verification of integrity levels with the help of a computational analysis.

It is not the intention of this document to force the manufacturers and users to employ similar equipment and control solutions or design the systems. This document is intended as a guide and checklist to provide the proper tools for promoting safety and long term unit availability. The document aims, with the help of principle model documents, to present an example solution, which can be used as a help for planning, design, manufacturing and use. Any laws, decrees and the instructions and guidelines by competent authorities should be observed and abided to

Our intent is to develop the document further, and for this reason we ask you to send any possible observations about faults, suggestions for improvements, and experiences to the secretariat of the Finnish Recovery Boiler Committee. Our contact details can be found on the web-pages of the committee. http://www.soodakattilayhdistys.fi/index_e.html

This document is translated into English. If the original Finnish text and its English language translation differ from each other, the original Finnish guideline applies.

Finnish Recovery Boiler Committee

Keijo Salmenoja
Chairman of the Board

Olli Ahava
Chairman of the Automation Work Group



Finnish Recovery Boiler Committee

SAFETY INSTRUMENTATION GUIDELINES FOR RECOVERY BOILERS



CONTENTS:

DISCLAIMER	1
INTRODUCTION.....	2
CONTENTS:.....	4
1 GENERAL	6
1.1 Sources	7
1.2 Concepts and definitions	7
2 PART 1.....	11
2.1 GENERAL	11
2.2 MANAGEMENT OF OPERATIONAL SAFETY	11
2.3 RISK ASSESSMENT	11
2.4 ORGANIZATION	12
2.4.1 Parties.....	12
2.4.2 Competency requirements.....	14
2.5 DOCUMENTATION.....	15
2.5.1 Definition phase.....	16
2.5.2 Planning and implementation phase	18
2.5.3 Testing documentation	20
2.5.4 Operation and maintenance phase	21
2.6 THE LOGIC SOLVER OF THE SAFETY INSTRUMENTED SYSTEM	22
2.6.1 The plan for a logic solver (hardware).....	23
2.6.2 The plan for the logic solver (software).....	23
2.7 FIELD EQUIPMENT	24
2.7.1 General	24
2.7.2 Measuring devices	25
2.7.3 Push buttons and switches.....	25
2.7.4 Valves.....	26
2.7.5 Pumps and fans	26
2.7.6 Motor valves	27
2.7.7 Safety switches	27
2.7.8 Voltage supply	27
2.8 FIELD DESIGN	27
2.8.1 Installation targets.....	27
2.8.2 Measurement points	27
2.8.3 Root valves and installation valves.....	28
2.8.4 Cabling	28
2.8.5 Markings.....	28
2.9 SAFETY LOCKING FOR THE RECOVERY BOILER	29
2.9.1 Boiler protection	29

2.9.2	Ventilation conditions for the burner	31
2.9.3	Furnace ventilated	33
2.9.4	Boiler burning permit for startup burners (furnace ready)	33
2.9.5	Burning permit for the startup burner	34
2.9.6	Boiler burning permit for load burners (furnace ready) (when required)	35
2.9.7	Burning permit for the load burner	35
2.9.8	The emergency-stop for auxiliary fuel	36
2.9.9	Feeding permit for diluted non condensable gases (DNCG)	37
2.9.10	Burning permit for concentrated non condensable gases (CNCG)	37
2.9.11	Start permit for liquor recycling	38
2.9.12	Liquor burning permit	39
2.9.13	Emergency-stop for liquor burning	39
2.9.14	Start permit for liquor ring wash up	40
2.9.15	Start permit for boiler floor wash up	41
2.9.16	Stopping of air fans	41
2.9.17	Quick stop	42
2.9.18	Rapid drain	44
2.10	TESTING	45
2.10.1	Factory acceptance testing	45
2.10.2	Commissioning testing and periodic testing	45
2.10.3	Testing of safety logic	46
2.10.4	Testing of field circuits	46
3	PART 2	48
3.1	GENERAL	48
3.1.1	General risk graph	48
3.1.2	Verification of the integrity level for safety instrumented systems	48
3.1.3	Interlock diagrams	48
3.1.4	Display images	49
3.1.5	Circuit design and wiring diagrams	49
3.1.6	Testing documents	49
3.1.7	Operation and maintenance guidelines	49

APPENDICES:

Appendix 1	Definition of the safety integrity level for a recovery boiler with the help of a risk graph
Appendix 2	Verification of integrity levels for safety instrumentation
Appendix 3	Examples of interlock diagrams
Appendix 4	Examples of logic solver
Appendix 5	Example of a loop wise functional description
Appendix 6	Examples of monitoring displays
Appendix 7	Principle models of loop and wiring diagrams
Appendix 8	Principle models of testing documents
Appendix 9	Principle guide for operation and maintenance
Appendix 10	Marking guidelines for safety related systems



1

GENERAL

This guideline applies to **Safety Instrumented Systems (SIS)** for recovery boilers.

The responsibility for this document is assumed by the Automation Work Group of the Finnish Recovery Boiler Committee. The first version of the guideline was completed in 2003.

The guideline was revised in 2008 on the instructions of the Automation Work Group of the Finnish Recovery Boiler Committee. The credits for the revision belong to Chairman Mauri Heikkinen Pöyry Forest Industry Oy and the members Sami Forsström Andritz Oy, Reijo Hukkanen Stora Enso Oyj, Mika Kaijanen Tukes, Raimo Koskinen Sunila Oy, Heikki Lappalainen Andritz Oy, Esa Palojärvi Metso Power Oy, Kauko Ylioinas BMS Kemi and Janne Peltonen Mipro Oy.

The guideline aims, with the help of principle model documents, to present an example solution, which can be used as a help for planning, design, manufacturing and use. Any laws, decrees and the instructions and guidelines by competent authorities should be observed and abided to.

The guideline has been carefully prepared, and, on drawing it up, the opinions of various interest groups (mills and equipment suppliers) about the structure and activities of SIS have been listened to. Also, the starting point has been that the equipment to be used complies with the requirements of the laws and degrees in effect in Finland and of the authorities responsible. The responsibility for the implementation of SIS belongs to the manufacturers of the equipment and those who implement its control system. It is the responsibility of the users or operators to ensure that SIS is employed correctly and with care and maintained in a similar way.

The guideline is aimed to comply with the EN-61508 and EN-61511 standards as far as applicable in respect to the definition of safety instrumentation, design, implementation, operation and maintenance. This applies to both the guideline concerning implementation as well as to the principle model documents.

This guideline is divided in two parts: Part 1 is the implementation guideline, and Part 2 contains the principle model documents related to the implementation. [KLTK's Safety instruction G10](#) (Finnish only), for example, presents general information about how to carry through a SIS project and about SIS's lifecycle. These matters are not repeated in this document. When the need has arisen, there is a reference to the instruction in question.



1.1 Sources

[EN 61508](#) (Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1-7).

[EN 61511](#) Functional safety: Safety Instrumented Systems for the process industry sector, parts 1-3.

[IEC 62061](#) Safety of machinery – Functional safety – Electrical, electronic and programmable electronic control systems.

[SFS-EN 50156](#) . Electrical equipment for furnaces and ancillary equipment, Parts 1-3

Asetus [vaarallisten](#) kemikaalien teollisesta käsittelystä ja varastoinnista 29.1.1999/59 (Decree on the Industrial Handling and Storage of Dangerous Chemicals, 29th January 1999/59) (In Finnish and Swedish only)

[Kauppa- ja teollisuusministeriön päätös painelaiteturvallisuudesta 8.10.1999/953](#). (The decision of the Ministry of Trade and Industry concerning the safety of pressure equipment) 8th October 1999/953) (In Finnish and Swedish only).

[97/23/EC Pressure Equipment Directive](#)

[98/37/EC Machinery Directive](#)

TUKES-julkaisu 4/2000, Opas kattilalaitoksen vaaranarvioinnin laatimiseksi (TUKES publication 4/2000. Guide for boiler plant risk assessment) (In Finnish only).

[Kattilalaitosten turvallisuuskomitea \(KLTK\) Suojeluohje G7 Soodakattilat 2000](#) (The Safety Committee for Boiler Plants (KLTK) Safety Instruction G7 Boiler plants 2000). (In Finnish only).

[TUKES-opas 2007, Turva-automaatio prosessiteollisuudessa](#). (TUKES guide 2007. Safety automation in process industries. (In Finnish only).

1.2 Concepts and definitions

Diagnostics is an operation performed by a safety related system or by some external system or a group of operations by which it is possible to discover a failure suffered by some system related to safety.

Diagnostic coverage (DC) reveals, in percentage terms, the portion of the dangerous faults in the system detected with the help of the diagnostic operations.

Self-diagnostics refers to operations used to discover failures. Utility programs in programmable safety devices are used to test the components of a programmable control unit or one of its channels (e.g., ROM) or the operations of operable modules (e.g., I/O modules).



Residual risk is the risk that still remains after some risk related safety systems have been implemented, in accordance with the risk reduction principles, for the process under control.

Acceptance is used to show, with the help of inspections and testing, that SIS, after its installation, complies with all the safety requirements set for it.

Target is a device or operation that SIS guides to a safe state if necessary.

Usability is the probability by which a planned functionality operates when required.

Operating system is the basic software for SIS.

The closed current principle means that a safety function remains in operation readiness with the help of constant auxiliary energy input and can function when the energy supply is interrupted.

Source signifies a measurement or operation, which either alone or together with another source can trigger a safety function, i.e., to lead the sources into a safe state.

The period between scheduled tests is the time period after which the safety related system will be regularly tested to discover the hidden faults that may have accumulated in the system during that period.

Basic process control system (BPCS) is an automation system which does not include safety related systems and is meant for the normal regulation and control of a recovery boiler plant.

Process safety time is the time period between an appearance of a dangerous fault in the control system and the moment when an accident will happen due to this dangerous fault if the safety function is not performed.

Risk refers to the combination of the probability of a certain dangerous event and of its consequence.

Risk analysis aims to systematically make use of available information to recognize hazards and to estimate the magnitude of risks that people or a population, property, or an environment is subjected to.

Risk assessment is a process that combines risk analysis with the assessment of the risk's significance.

E/E/PE is based on electric (E) and/or electronic (E) and/or programmable electronics (PE) technologies.

Protection means mechanical control by which the target to be controlled is lead to a safe state if the circumstances so demand. Protection functions regardless of possible interlocks or new controls. The functions of a safety related system are, typically, protections.



SIS means Safety Instrumented System and consists of sensors, logic solvers, final control elements (relays, valves, motors etc.) and the cabling between these.

SIS logic part (SISl) is that part of SIS that is connected to sensors and actuators. SRS is an acronym for Safety Related System and it consists of mechanical safety systems (e.g., safety valves) and of Safety Instrumented System (SIS).

Verification scrutinizes every work phase with practices of checking and acceptance that conform to a certified quality system.

Safe failure results, in a case of a failure of some device or system, in a safe state, or the failure does not affect the operation of safety functions.

Safety integrity describes the reliability of a safety function, i.e., that the safety function is realized when needed. Safety integrity combines the safety integrity of the equipment (equipment failure) as well as the systemic safety integrity (systematic errors in the system implementation).

Safety integrity level (SIL) is a discrete level to define the requirements of safety integrity of the safety functions for E/E/PE systems that are safety related. The safety integrity levels are graded from 1 to 4. Of these, 4 is the highest safety integrity.

Type acceptance is an inspection by a third party to ensure that a product, process or service that is appropriately identified complies with a certain standard or with detailed requirements.

Work flow principle ensures that a safety function is activated when the device receives an input of auxiliary energy.

Hazard is a possible source of damage or a situation enabling damage to occur.

Dangerous occurrence can give rise to damage.

Damage signifies a physical injury or health hazard or damage to property or environment.

Redundancy means performing the same function with two or more parallel devices or systems. In spite of their apparent independence, the different channels used to effect redundancy may run the risk of a common failure.

Fault or malfunction indicates an abnormal state, which might reduce the capability of a device or a system to perform a required safety function.

Failure means that a device or a system is no longer capable of performing a required safety function. Failures are either of a random nature (in devices) or systematic (in devices or programs).



Fault tolerance is the capability of a device or a system to continue performing the required safety function regardless of a failure. Fault tolerance in the implementation of safety functions is normally attained by employing redundancy or fail-safe structures.

Fault tolerance time is the period between the occurrence of a hazardous situation (caused by the process itself or by a device malfunction) and the point in time when the process behavior changes to a critical mode, the result of which is a dangerous event if there are no safety systems employed.

Common failure is a failure which causes a simultaneous failure in two or more channels that are performing a safety function in a multichannel system.



2 PART 1

2.1 GENERAL

The safety instrumentation of a recovery boiler is that part of the automation system that reduces risks by protecting the boiler from getting into a dangerous condition, or in a dangerous condition guides the boiler into a safe condition. The acronym SIS (Safety Instrumented System) is used for safety instrumentation. SIS includes the equipment and installations (for example, logic, cabling, and field and electric equipment) needed for the implementation of safety functions.

2.2 MANAGEMENT OF OPERATIONAL SAFETY

The management of the plant's operational safety is a part of the implementation of SIS. An essential part of SIS is documentation, which ensures that the assessment and maintenance of the safety level of safety systems is possible. During the duration of the entire undertaking, it must be kept in mind regarding the documentation, that one should be able to trace the systematic verification and acceptance of the integrity levels. Drawing up of an appropriate safety plan for the project guarantees that all the necessary actions to ensure safety will be done.

The lifecycle of SIS is divided into a definition phase, design and building phase, installation and verification phase, and operation and maintenance phase. The guideline based on IEC61508 presents, generally applied, the phases, responsibilities and documentation of the life cycle.

Verification must be applied at each work stage during the project, and the overall acceptance should take place at the final installation location before start-up.

2.3 RISK ASSESSMENT

Recovery boilers must be subjected to risk assessment, which includes a hazard and risk analysis and an evaluation of the significance of the risk. In evaluating the significance of the risk, one should consider different danger situations and their consequences, and then decide about the degree of tolerability that is acceptable. Risk reduction which is deemed necessary may consist of different SRSs and of external means to reduce risks (education, restricted movements, or other ways). SRS includes, in addition to SISs for E/E/PE, also SRSs for other technology such as safety valves, rupture disks etc.

It is useful to divide the hazard and risk analysis into two processes, so that the first process focuses on finding unrecognized hazards and the second on the evaluation of the risks discovered. By first concentrating solely on



detecting hazards will ensure that the end results in charting those hazards will be as good as possible.

The safety integrity level (SIL) by safety functions is to be defined based on the hazard and risk analysis. The most widespread method in the definition of the safety integrity level is risk graph in accordance with EN 61508 and 61511. The method is based on risk consideration, where the consequences of, exposure to, the possibility of the avoidance of a danger and its frequency of occurrence are observed when SIS is not being used. The risk graph and calibration suitable for recovery boilers are shown in Appendix 1 of Part 2. Calibration is shown separately for damage to persons, environment, materials, or property. The appendix also shows a model of a hazard and risk analysis form, in which hazards, the reasons for those hazards, their consequences, as well as the current preparation and extent (the required safety integrity level, SIS) are presented.

2.4 ORGANIZATION

The parties to the different phases in SIS project and their responsibilities must be defined in the beginning of the project. SIS's safety plan must present the tasks of the various parties, supply limitations (equipment, documents) and participation in tests and commissioning.

It is necessary to contact a permission authority or inspection office in good time and find out about the required assessment, inspection and permission procedures.

2.4.1 Parties

2.4.1.1 Operator

The end user (operator) is responsible for providing the chemical and process information and requirements specification that are essential for SIS. If the delivery of SIS is separate from the complete boiler system, the operator must assume the responsibility for the functionality and acceptance of the whole.

It is the operator's responsibility to ensure the maintenance, change management and periodic testing for the equipment in operation.

2.4.1.2 SIS supplier

The supplier of SIS must supply a system that meets the requirements specifications of the operator and complies with those of the law.



2.4.1.3 Boiler supplier

The boiler supplier is responsible for the equipment it delivers. If SIS is also included in the total delivery of the boiler, the supplier also takes the responsibility for its documentation, appropriateness, suitability and for the necessary inspections and acceptance procedures.

2.4.1.4 Assessor of SIS

An inspection office or a party that has no self-interests in the manufacturing and is competent can act as an assessor of SIS depending on the skill and competency. The operator or the supplier of the boiler selects a suitable assessor, but it is recommendable that, for the selection, there is communication with the authorities responsible for assessing compliance to the requirements - generally this is the inspection office.

The assessor inspects and verifies the application's operational safety and its compliance with the requirements. The assessor inspects the actions of each phase (definition, planning, implementation, operation and maintenance) of the lifecycle and information obtained from each of the phases. It is the task of the assessor to decide whether the aims of the applied standards and the requirements and procedures decreed have been complied with.

2.4.1.5 Inspection office

The tasks of the inspection office include the evaluation of the safety instrumented systems for pressure equipment, especially for integrated machinery and in periodic inspections. It is also the task of the inspection office to ensure the technical safety and reliability of the equipment being built and implemented and, after that, when it is being used.

2.4.1.6 Authority

Tukes (Safety Technology Authority) is the controlling authority in Finland for technical safety and reliability in its field. Its area of activity includes, among others, industrial handling of dangerous chemicals and pressure equipment and pressurized systems.

Tukes grants permits for plants involved in extensive industrial handling and storing of dangerous chemicals. Modifications and extensions which can be considered equal with building a new plant need a Tukes's permission.

In connection with the permit application or notification about a modification, the operator must present the plans regarding the principles and sufficiency of the implementation of SIS for the planned purpose and the inspection methods to be used during the system use.



2.4.2 Competency requirements

All the persons who deal with the operations of the SIS as a whole or of the lifecycles of software safety, including managerial tasks, should have the appropriate education, technical know-how, experience and competence which are related to their specific tasks.

The competence of the persons responsible for the planning, testing and commissioning of SIS must be indicated in the description of SIS. In addition, the documentation must contain information about the persons responsible. That information must show their education, competence and previous experience in SIS projects.

The following factors should be considered when considering the competence of these persons for their tasks.

- Appropriate technical knowledge suited to their application area
- Technical knowledge applicable to the technology in question (e.g., electrics, electronics, programmable electronics and software technology)
- Knowledge about the safety technology applicable to the technology in question
- Knowledge about legislation and safety regulations
- The consequences if the systems related to E/E/PE safety do not function
- The safety integrity levels of the systems related to the E/E/PE safety.
- The novelty of planning methods, structure or application
- Previous experience and its significance in relation to the particular tasks to be performed and the technology to be used
- The importance of competency in the particular tasks to be performed
- Courses taken that are related to the subject



2.5 DOCUMENTATION

Documentation must be made such that the matters are presented either in the same documentation or with clear references to other documents.

The table of contents could be made of, for example:

Definition phase

- Safety plan
- Hazard and risk analyses
 - Hazop analysis
 - Integrity level definitions
- SIS requirement definitions
- Evaluation report for the definition phase

Planning and implementation phase

- Functional specifications
- Safety locking diagrams
- SIS implementation description
- Field equipment guide and installation instructions
- Verification of integrity levels
 - Integrity level calculations and failure rate data
- I/O card and box layout for safety logic
- Plan for installation and commissioning
- SIS logic diagrams
- SIS program diagrams
- SIS displays
- Loop design and wiring diagrams
- Factory acceptance tests
 - FAT plan
 - FAT instruction
 - FAT test record
 - FAT test report
- Assessment report for the planning and implementation phase

Installation and acceptance phase

- SAT plan
- SAT instruction
- SAT records
- SAT acceptance report
- Assessment report for the installation and acceptance phase

Operation and maintenance phase

- Plan for operation and maintenance
- Plan for periodic testing
- Instructions for periodic testing



- Records for periodic testing
- Reports for periodic testing
- Assessment report for the operation and maintenance phase

2.5.1 Definition phase

The documents of the definition phase are drawn up in collaboration with the operator, with the persons responsible for the electrical design and instrumentation design and with the main equipment supplier.

2.5.1.1 Safety plan

The safety plan presents an implementation plan related to safety. It describes the process of a SIS project by stages and the methods by which safety is ensured. The focus is on quality assurance and matters related to the assessment of the appropriateness of the implementation.

The contents of the safety plan are, briefly:

1. Target

A short description of the target (plant)

2. Regulations, recommendations and standards to be applied

A list of laws, regulations, recommendations and standards to be followed in the definition, planning and implementation of the plants' SRSs.

3. Supply limitations

A short clarification about the planning and implementation supply limitations regarding the client, equipment supplier and SIS supplier.

4. Organization and responsibilities

The persons who are responsible for the definition, planning and implementation of SIS, tasks, responsibilities, supply limitations and competency (see 2.4.1).

5. Documentation

A short description about the documentation to be produced during the definition, planning and implementation of SRS.

6. Modification procedures

A description about how the management of possible changes is to be realized during the planning, testing, commissioning and maintenance phases.

7. Testing, inspection, survey, acceptance and auditing methods

A short description about the testing, inspection, survey, acceptance and auditing procedures to be used during the project.



8. Training plan

A short description about the training on safety functions and about SIS training for the operational personnel.

9. Schedule

The main issues, documents and different inspections for the definition, planning and implementation of SIS are defined in the schedule.

2.5.1.2 Hazard and risk analysis

Generally, it is the main equipment supplier who draws up the hazard and risk analysis, which is then examined together with the operator. The document should consider dangers associated with recovery boilers and assess the related risks and risk reduction methods.

There are two stages for the hazard and risk analysis:

Stage 1 (HAZOP or similar)

In stage 1, a hazard assessment is made for a plant/equipment/device by using, for example anomaly examination (HAZOP Hazard and Operability Study) or a similar analysis method.

In the assessment the actions to reduce risks are defined with SIS or by other risk reduction methods (e.g., rupture disks, safety valves).

Stage 2 (SIL definition)

In stage 2, an assessment is made, based on the report of stage 1, about the risks associated with hazards and about risk reduction methods. Safety integrity levels (SIL) for the safety functions to be implemented in SIS are also defined. Risk assessment focuses on personal risks, but also serious environmental harm, material damage and production losses may be assessed.

Appendix 1 in Part 2 shows in more detail the implementation and documentation of the hazard and risk analysis for a recovery boiler.

The necessary parts of hazard and risk analyses must be updated if in the planning and acceptance stages:

- decisions are made, which can change the grounds of the decisions made in stages 1 and 2
- new hazard situations come up



2.5.1.3 SIS requirement specification (safety functions implemented by SIS)

The requirement specification for SIS are normally provided by the main equipment supplier. The requirements definition is based on the hazard and risk analysis, and it must contain the functional requirements of total safety for the SIS equipment and for SIS safety functions (descriptions of safety functions) and their integrity level requirements. The level of safety must be defined for each recognized hazard.

The requirement specification discusses the requirements expected from the operations and reliability of safety functions, verification of compliance with the requirements, as well as preparation for hazardous situations, their prevention, limitation of consequences etc.

The requirement specification must be completed before the definition of SIS's logic part and its procurement.

2.5.1.4 Safety interlock diagrams

Interlock diagrams are designed by the main supplier. In the safety interlock diagrams all the safety functions presented in the requirements definition are shown unambiguously. Correct device positions are used and the interlock values for process variables are shown as accurate number values. The interlock diagrams should be completed before programming starts.

2.5.1.5 Field equipment guide and installation instructions

The field equipment guide and installation instructions show the field equipment solutions to be used in the project for the planning and design of instrumentation and electrification. The instructions must also give instructions about installations and markings.

2.5.2 Planning and implementation phase

The documentation for the planning and implementation phase presents the part of the SIS documentation that is created when a SIS is designed and completed in accordance with the definition phase.

2.5.2.1 Description of SIS implementation

The description of SIS implementation shows the part of the safety instrumented system and the part of the field equipment. The description of the logic solver is created by the supplier of the safety instrumented system. The description of the field equipment and installation is created by the designer of the electrical and instrumentation plan supplementing the part done by the supplier of the safety instrumented system, or a separate implementation description is drawn up by that designer.



A selection of the principles to be used in the implementation of SRS is made in the SIS's implementation plans. The description must indicate the equipment used and their behavior in possible equipment break-downs as well as the necessary program blockings to prevent outsiders from changing calibration or parameters.

When selecting the implementation principles, attention should be paid to the SIS's periodic tests and testing interval. One should note that it should be possible to organize a considerable portion of the periodic tests to be conducted during the normal operation of the plant and in connection with its shutdown as well as with its startup.

2.5.2.2 Verification of integrity levels

Verification of integrity levels is part of the implementation description. In verification, the attainability of safety integrity for safety functions must be shown, in accordance with the hazard and risk analysis and the requirement specification. Verification must be performed by examining separately the sufficiency of the device architecture and the probability of an equipment failure due to a fault. This should be based either on the reliability data (failure rate, failure rates due to dangerous faults, and diagnostics) related to the field equipment and logic solver or, if these values are missing, on other estimations and experience. The verification of integrity levels is explained in more detail in Appendix 2 of Section 2.

Integrity level calculations are the task for the supplier of the safety instrumented system. These calculations are based on the reliability data (failure rates, failure rates due to dangerous faults, and diagnostics itself) obtained from the designer of the field sections (electrification and instrumentation).

2.5.2.3 The safety instrumented system's layout for cabinets, boards and I/O.

The safety instrumented system's layout for cabinets, cards and I/O is designed by the system's supplier. The layouts must also show any possible spare cards.

2.5.2.4 The plan for installation and commissioning

The plan for installation and deployment consists of several documents from different areas. The complete document is produced by the end client, who collects documents from the different areas of interest to be used in the planning of deployment. The client also draws up a detailed schedule about the stages of deployment and the duties and responsibilities for each party.

The plan for the installation and commissioning of the logic solver, electrification as well as of instrumentation is to be accomplished by the designers of the areas of interest in question.



2.5.2.5 SIS program diagrams

The programming for the SIS's logic solver is the responsibility of the system's supplier. The program must have such documentation that it can be understood without the presence of the program author.

2.5.2.6 SIS displays

SIS displays are shown either on SIS's own terminals or in the normal process control system.

2.5.2.7 Loop and wiring diagrams

The text "RELATED TO INTERLOCKS" must be affixed to the loop and wiring diagrams of the field equipment that is to be connected to the safety instrumented system. The loop and wiring diagrams are made by the designer in that area.

2.5.3 Testing documentation

Testing (FAT factory acceptance testing, SAT site acceptance testing, and periodic testing) documentation includes a testing plan, testing instructions, testing records, and a testing report.

2.5.3.1 Testing plan

The testing plan includes the target of testing, testing organization, conditions for testing, documentation needed in testing, testing equipment, testing methods, testing acceptance criteria, instructions for creating a testing report, as well as the report distribution.

2.5.3.2 Testing instructions

Accurate testing instructions based on tests are made. The instructions explain the preparations for each testing stage, and instruct on how to simulate the sources and how to realize possible temporary connections between the channels. They also explain the interlocks (objects) for each testing stage. Different equipment combinations (1/2, 2/3) must be tested separately and presented in the testing instructions.

The aim of the testing instructions is to guide the testing to such an accuracy that it is possible, afterwards, trace the testing process.



2.5.3.3 Testing records

The testing records must be prepared beforehand in line with the testing instructions and in such a way that the operations realized and the interlocks occurring can be witnessed and the locking limits can be written down.

2.5.3.4 Testing report

The testing report is prepared at the end of testing. The report states the testing target, date, and participants and includes a mention about the test acceptance and the signatures and their clarifications of all the participants. In addition, the modifications and additions made on the definition and testing material are recorded in the report. If the repair, modification and addition operations cannot be tested with the testing under way, it should be recorded when the deficiencies will be tested.

The end client or the supplier of the safety instrumented system is responsible for creating the testing plan, instructions and the testing records.

2.5.4 Operation and maintenance phase

2.5.4.1 The plan for operation and maintenance

A plan for the operation and maintenance of the safety instrumented system must be made. This plan should tell about the target of the plan and the persons responsible for it, and contain an explanation about SIS's documentation, an introduction of the operating and maintenance personnel to SIS, the plant's general safety instructions, guidance to periodic testing, and instructions for maintenance and modification procedures (permissions, acceptances, documentation etc.). The plan is drawn up by the end client together with the supplier of the safety instrumented system.



2.6

THE LOGIC SOLVER OF THE SAFETY INSTRUMENTED SYSTEM

The logic solver (SIS₁) of the safety instrumented system must be independent of the basic process control system. It can, nevertheless, be connected to the basic process control system through, for example, bus-connections or hardwiring. A separate SIS unit means a separate logic or a (integrated) logic that has been built with separate control system components and contains only the operations meant for safety protections. It should be kept in mind that the logic solvers and the components must be certified for the purpose intended.

SIS₁ is implemented in accordance with the defined highest integrated safety level based on the hazard and risk analysis. Even though the above mentioned logic solvers, as single-channeled, had been accepted at the safety integrity level 3 (SIL3), SIS₁ when connected with a recovery boiler, for the sake of usability, must be built in such a way that the processors can be changed during the operation. Similarly, redundant I/O's for the input and output cards must be located in such a way that the failure of an individual card cannot result in the deterioration of the usability or safety of the plant.

The measurements of the circuits related to SIS are wired first to SIS₁, from where the measurement data for indications, reporting, control and for similar needs is lead to the process control system either directly through a bus, through an I/I transformer or with additional outputs from SIS₁

Connection of safety related regulation and control circuits to SIS is realized with a separate control from SIS₁, with which the final control element (valve, damper, fan, pump etc.) can be brought to a safe state at the so-called "hard wire" independently of the basic process control system. Regulation and control operations which do not have safety requirements are implemented in the basic process control system.

Controlling motor valves and motors related to motor centers to a safe state is implemented with the help of safety relays which are located to the safety logic.

When necessary, to attain the required integrity level, a separate additional control target is needed. This will further reduce the risk associated with the possible non-functioning of the control target in question. This means, in the case of the primary air fan for example, that in addition of the safety control for the fan's motor, the safety logic also guides the air flow control dampers to a safe position.



2.6.1 The plan for a logic solver (hardware)

The logic in its equipment container is installed in the SIS cabinet. Also the incoming and outgoing cables from the field are placed there. The required isolators and relays are also located in the same cabinet or in a distribution frame to be positioned on the side of the cabinet. Redundant input and output signals are located on different boards in such a way that as high as possible degree of usability is achieved (for example, measurements with the selection principle 2 out of 3).

A separate marking is attached to the cabinets, frames, cards and channels that are connected with SIS, to indicate that the equipment belongs to the safety related circuits. The cross-connection to the signals related to SIS is done by red wiring to distinguish it from the signals going to the basic process control system.

The markings of SIS and the circuits related to it must comply with the Report 9/2000, Rev A “Marking recommendation for safety related systems” issued by the Finnish Recovery Boiler Committee. Report is presented in Appendix 10.

Voltage feed to the logic solver is arranged from a voltage source that is equipped with a screening transformer. In addition to this, a standby voltage feed must be arranged for the logic solver (and through it to the field equipment) in case of interruptions and faults in the main voltage feed. The standby voltage feed must connect automatically and without an interruption once the main supply has ceased functioning. The standby supply is accomplished with UPS equipment and a set of direct current batteries. The standby voltage supply must be able to feed the system at least 45 minutes (normal rapid drain and safety time period). An alarm for the operator must be connected to the condition monitoring of both the main feed and the standby supply.

2.6.2 The plan for the logic solver (software)

The documentation must include own interlock diagrams for the SIS circuits' operations and unambiguous verbal descriptions as well as the basic circuit arrangement which shows the whole circuit on a single document from the source to the object (trip limits, operation, I/Os, connections to other parts) (see Section 2, Appendices 3, 4 and 5).

Separate displays about the SIS safety functions are created for the interface to the safety logic or that to the basic process control system (see Section 2, Appendix 6). These give information about measurement data, binary state data, and, in addition to controls, also about the state of the measuring instruments and about controlled objects under final state monitoring.

Its own alarm pages, in which the SIS alarms can be put into their own category, must be made for SIS in the basic process control system. Apart



from the SIS functions, information is needed also about sensor and signal faults in the field equipment. A notification or an alarm text with a time stamp attached (for example in 100 ms intervals) must be generated when SIS is triggered. The system must be able to tell the basic reason for the triggering of SIS. Similarly, the alarms must be able to monitor the deviations of redundant measurement signals (for example, if the deviation is more than 10%).

SIS programs must be protected with a password or by other means in such a way that any modification of the programs by outsiders is prevented.

2.7 FIELD EQUIPMENT

2.7.1 General

The field equipment, in the case of a recovery boiler, does not need a separate SIS which would have its own field equipment and logic solver; for this it is sufficient to use equipment that is normally used in the basic process control. Nevertheless, it should be noted that the signal data from measuring instruments, control switches, limit switches or other sources is first brought to SIS, from where the signal can be further taken to the basic process control system to be utilized there.

Similarly, no separate valves are installed only for the SIS's controls. The necessary closing and opening operations are realized using the process control valves. This, however, presupposes that the required integrity level is achieved.

The higher the requirement for a safety function's integrity level, the more independent and reliable should the equipment for SIS be.

In addition, in the case of field equipment, it is necessary to pay attention to the redundancy and reliability requirements as demanded by the safety integrity levels (SIL) and usability.

When specifying the field equipment one must also pay attention to the possibility of periodic testing during operation.

The safety of SIS as a whole (sensors – logic solver – actuators) should be checked with the help of a computational analysis, to ensure that the integrity level defined with the help of the risk analysis is achieved with the selected structural solution for the safety instrumented system. To be able to conduct a computational analysis in order to ensure the adequacy of the operational safety for the entire SIS, one should demand, for all the field equipment selected, an approval for safety related systems and its probability of failure values in accordance with the EN-61508 standard. There is an example of the computational analysis in Appendix 2 of Section 2.



2.7.2 Measuring devices

The measuring devices should be analog 2-wire transmitters with high quality self-diagnostics. The transmitters should be, primarily, certified transmitters meant for safety use. When using normal transmitters, the measurements should be realized using the 2/3 comparison principle to achieve as high usability as possible.

When using the safety transmitters with a higher quality self-diagnostics (the best solution), a higher integrity level and usability is achieved using two transmitters and 1/2D principle. There are two separate signals, the measuring signal and the diagnostics signal, that can be obtained using safety transmitters. The diagnostics signal gives information about the state of the transmitter. It is not necessary to guide the plant into a safe state due to the failure of one transmitter. The responsibility for that is transferred to the other transmitter alone, and the operator is alerted to the failure condition. The failed transmitter must be replaced within a set time period.

In addition to the protective interlocking caused by the process interlock limit, the failure of the transmitter, as well as that of the cable, must trigger a safety interlocking function. All pressure and level measurements related to the recovery boiler's SIS are to be realized by pressure and pressure difference transmitters. The transmitters must block programming and be adjusted with approved calibrated devices. Redundant measurements must be calibrated in the same range.

The compensation of the measurement signals in safety related circuits must be realized in connection with air volume measurements. However, this is not necessary in drum level measurements, where a raw signal should be used as the tripping signal primarily. The reason for this is that compensations increase SIS's circuits, different calculation methods and algorithms complicate the clarity of the whole and the significance of compensations in measurements is not that great. Compensation calculations in SIS must be done in such a way that the compensation signals are included in SIS. If the same compensation signal is used for compensating several measurement signals, the safety of that solution must be justified.

2.7.3 Push buttons and switches

Main ESD, rapid drain and emergency-stop push buttons must be of the mushroom shape, red in color and equipped with a sufficient number of poles. The buttons must lock when pressed in. The interlock caused by the emergency-stop buttons is acknowledged with a separate acknowledgement button located in the control room. The buttons on the field must be marked in such a way that it is clear what effect the use of the button will have and that the button can be seen clearly from a distance of at least 10 meters.



Limit switches must be of such type and connected in such a way that the so-called circuit opening connection principle is realized. The switches may be either inductive (2-wire) or mechanic with self-cleaning contacts.

2.7.4 Valves

The valves connected with the controls of SIS must be equipped with spring return actuated devices. The driving direction of the actuator must be selected in such a way that the spring force guides the valve to a safe state while the pressure air leaves the actuator.

The guidance to a safe state is realized with a solenoid valve, which is installed linking it to the actuator. The solenoid valve when de-energized lets the pressure out of the actuator, and the spring forces the valve to a safe state. It should not be possible to manually control the solenoid valves.

A solenoid valve is installed between the positioner of the control valves and the actuator. In an interlock situation, the solenoid valve uses a spring to force the control valve to a safe position in accordance with the interlock instructions.

"Spring closes" actuators are used as fire valves and ESD valves while "spring opens" actuators are used as ventilation/pressurization valves. Fire valves and ESD valves must comply with the requirements of the medium.

Feed water valves (stop valves), main steam valves, blow down valves, start-up valves, attemperation valves, rapid drain valves, drum level reducing valves, sootblowing valves and main inlet header rapid drain are traditionally electrically driven and equipped with a secured auxiliary supply.

2.7.5 Pumps and fans

The motor outputs used are standard outputs (no different colored internal wirings or different colored terminal blocks).

The running state of pumps and fans are obtained, with the help of closing auxiliary contacts, from motor contactors at the motor centre or, alternatively, from the frequency converter using the contact data at SIL 1 and in addition, for example, from the voltage or current monitoring or from some process measuring value starting from SIL2 integrity level.

Any possible seizing-up of a main output contactor is taken care of by oversizing the contractor. The dimensions of the contractors comply with the IEC60947-2 coordination class 2, AC3, (Simocode trigger class 10), so that ICS (measured breaking capacity for an extreme short circuit) is sufficiently high.



2.7.6 Motor valves

Auxiliary relays for SIS controls are added to the motor valves' outputs. The relays used are auxiliary relays approved for safety and are, depending on the application, in parallel (start) or in series (stop).

The temperature control and torque limits for motor valves are bypassed in connection with the protective interlocking of SIS.

2.7.7 Safety switches

Both the motors and the motor valves are equipped with normal safety switches.

2.7.8 Voltage supply

For field equipment that require a 230 V external supply, the voltage feed must be wired from a UPS secured network. The network must be designed in such a way that it can keep the system running for 45 minutes.

The main supply for motor valves and for other safety related actuators must be arranged from a secured centre (e.g., diesel or by other means).

2.8 FIELD DESIGN

2.8.1 Installation targets

The installation targets must be designed and installed in such a way that tests can be performed without dismantling the installations.

2.8.2 Measurement points

In measurements related to SIS, the basic principle is that each measurement has its own process measurement connection.

A separate pumping connection point must be included in the measurement points of the measurement transmitters for commissioning tests and for periodic testing. Pumping can be arranged, for example, through a 5/2 installation valve.



2.8.3 Root valves and installation valves

Both the root valves and the installation valves must be lockable, or the handles and hand wheels must be removed so that outsiders cannot change the valve positions. Clear indicators about the open/closed position must be installed in the valves once the handles and hand wheels have been removed.

2.8.4 Cabling

Measurements and controls connected with SIS can be realized using individual or multicore cabling. For analog signals protected cables are used.

SIS's redundant measurement signals are transferred to the SIS's logic solver through different cables and preferably through different routes. If multicore cables are used in the installations, separate multicore cables that are exclusively reserved for SIS are used for signals connected with SIS.

There is not enough experience yet about field bus solutions to be able to recommend them for the transfer of measurement and control data in SIS.

2.8.5 Markings

Field equipment, root and installation valves, process measurement points and cabling must be distinguished by a different marking (red) from the rest of the field equipment (See Appendix 10).



2.9 SAFETY LOCKING FOR THE RECOVERY BOILER

It should be kept in mind that safety functions must always be based on the hazard and risk analysis made for the recovery boiler. Also, when assessing the significance of the risks, the integrity level must be defined. This has not been discussed in connection with the lockings presented below.

To achieve a adequate safety level, the work group ended up with the following model lockings.

2.9.1 Boiler protection

Purpose:

Boiler protection means all the necessary actions, from the viewpoint of safety, to prevent damage to the boiler. Boiler protection consists of several process values and device states for the boiler. These are defined values and states. When the boiler protection conditions have been complied with, the boiler can be start-up and firing can continue.

Sources:

Main ESD button

- The main ESD button pressed in the control room

Steam drum level

- The drum level is below the lower limit (dry boiling guard)
3 pressure measurements
 - with 2/3 selection
- The drum level is above the upper limit (wet boiling guard)
3 pressure measurements
 - with 2/3 selection

Primary air

- The amount of primary air below the lower limit
2/3 selection, for example, of the following conditions:
 - the fan is not running
 - The amount of primary air below the lower limit
 - the pressure of the air ring below the lower limit

Secondary air

- The amount of secondary air below the lower limit
2/3 selection, for example, of the following conditions:
 - the fan is not running
 - the amount of secondary air below the lower limit
 - the pressure of the air ring below the lower limit

Furnace pressure

- The pressure of the furnace above the upper limit
3 pressure measurements
 - with 2/3 selection



Flue gas outlet

- The Flue gas outlet closed (at least one gas outlet must be open)
- The Flue outlet open signal is compiled from the fan's running data and from open limit switch signal of the input and output dampers.
 - the fan is not running
Using the 2/3 selection about the fan's rotating speed data, electric drives on - data, and the vacuum pressure measurement after the electrostatic precipitator
 - the rotating speed of the fan below the lower limit
 - the fan is not running
 - the vacuum pressure of the channel above the lower limit
 - the income channel damper away from the open limit
3 limit switches
 - 2/3 selection
 - the output channel damper away from the open limit
3 limit switches
 - 2/3 selection

Control air (when required)

- the pressure of the control air below the lower limit
3 pressure measurements
 - 2/3 selection

The O₂ content of the flue gas (when required)

- The content of O₂ in the flue gas is below the minimum limit
3 oxygen measurements
 - 2/3 selection

Objects:

Liquor burning

- liquor burning permit removed
 - liquor feeding pumps stop
 - liquor feeder valves close

Burning of auxiliary fuel

- burning permits for auxiliary fuel systems are removed
 - the burners' quick-closing valves close
- starting permits for auxiliary fuel systems are removed
 - the ignition gas valve closes

Burning of diluted non condensable gases (DNCG)

- the feeding permit for DNCG is removed
 - the feeder valves for DNCG close down
 - DNCG are lead to a stack or to a spare burning place

Concentrated non condensable gases (CNCG)

- the feeding permit for CNCG is removed
 - the feeder valves for CNCG close down
 - CNCG are lead to a chimney or to a spare burning place
 - the feeder valves for the auxiliary fuel of CNCG close down

Blow gas from the dissolver (when required)

- The dissolver's blow gas valves to the boiler close down
- The dissolvers blow gas valves to the chimney / roof open



The boiler's lower airs

- The boiler's lower airs stop
 - fans stop
 - dampers close

The boiler's upper airs

- The upper airs of the boiler are left running

Furnace ventilated

- The furnace ventilated signal removed

2.9.2 Ventilation conditions for the burner

Purpose

Burner ventilation is an operation in which the burner is ventilated in order to ignite the auxiliary fuel. At the start of the ventilation the boiler protection must be in condition so that the first burner can be started after the ventilation. Ventilation conditions are made up of many of the burner's process values and device states which must be at certain values and states.

Sources

Main ESD button

- Main ESD button not pressed in the control room

Primary air

- The amount of primary air above the lower limit
2/3 selection, for example, of the following conditions:
 - the fan is running
 - the amount of primary air over the minimum
 - the pressure of the air ring above the lower limit

Secondary air

- The amount of secondary air above the lower limit
2/3 selection, for example, of the following conditions:
 - the fan is running
 - the amount of secondary air above the minimum
 - the pressure of the air ring above the lower limit

Furnace pressure

- The pressure of the furnace below the upper limit
3 pressure measurements
 - with 2/3 selection

Flue gas outlet

- The Flue-gas-outlet-closed (at least one gas outlet must be open)
 - The Flue outlet open signal is compiled from the fan's running data and the input and output data related to open dampers.
 - the fan is running
- Using the 2/3 selection about the fan's rotating speed data, electric drives on - data, and the vacuum pressure measurement after the electrostatic precipitator
- the rotating speed of the fan above the lower limit
 - the fan is running
 - the vacuum pressure of the channel below the lower limit



- the input channel damper on the open limit
3 limit switches
 - 2/3 selection
- the output channel damper on the open limit
3 limit switches
 - 2/3 selection

Control air

- the pressure of the control air above the lower limit
3 pressure measurements
 - 2/3 selection

The emergency-stop for auxiliary fuel

- The emergency-stop button for auxiliary fuel not pressed

The emergency-stop for liquor burning

- The emergency-stop button for the liquor burner not pressed

The liquor lines to the boiler

- All liquor lines to the boiler closed

Isolation of diluted non condensable gases in the furnace

- The isolation valves for DNCG closed

Isolation of concentrated non condensable gases in the furnace

- The isolation valves for CNCG closed and ventilation valve opens

Fuel lines for auxiliary fuel burners

- The quick closing valves for the auxiliary fuel burner closed

The furnace ventilated

- Permitted time after the ventilation of the furnace exceeded

Objects

Furnace ventilation

- The ventilation permit for the furnace still valid

Implementation

The tripping condition “do not ventilate the boiler” is implemented in SIS. Monitoring related to the ventilation and ignition readiness is implemented in SIS.

The monitoring of the boiler ventilation is implemented in SIS. The safety logic controls that, after the ventilation order, the quantity of air has reached the required level and that the ventilation takes the time required. The time and the quantity of air needed for ventilation must be confirmed with the supplier of the boiler to ensure that the required quantity of air goes through the boiler.



2.9.3 Furnace ventilated

Purpose:

After the boiler has been ventilated for the required time, 'furnace ventilated' precondition signal arrives, which means that the permit for the firing of the first burner has been obtained. The ventilated signal is not needed when the liquor fire data is in effect in the furnace or when one of the burners is in operation.

Sources

Boiler protection

- Boiler protection in good condition

The emergency-stop for auxiliary fuel

- The emergency-stop button for auxiliary fuel not pressed

Ventilated time

- Furnace ventilated time below permitted

Liquor lines to the boiler

- All firing liquor lines to the boiler closed

Auxiliary fuel burners in operation

- No auxiliary fuel burner in operation

Burner ignition attempts

- Fewer than 2 attempts to ignite a burner with oil or fewer than 1 by gas

Targets

Furnace ventilation

- Furnace ventilated signal still valid

Implementation:

The tripping conditions (do not ignite the boiler) are implemented in SIS. Monitoring of operations related to ventilation and ignition preparedness is implemented in SIS₁. These monitoring processes include:

- Fire in the boiler signal creation
- Counting of ignition attempts

The counting of ignition attempts is implemented in SIS. A single ignition consists of a ignition order and the opening of the quick closing valve of the burner in question (the closing-limit signal – off). Two ignition attempts with oil are permitted, after which the ventilation of the boiler have to be repeated before any further ignition attempts.

2.9.4 Boiler burning permit for start-up burners (furnace ready)

Purpose

The boiler burning permit for the startup burners ensures that the boiler condition is such that the startup burner can be set to work.



Sources

Ventilation of the furnace

- Furnace ventilated

OR

Liquor firing

- Liquor firing in operation
- Liquor flow to the boiler above the lower limit, and
- The amount of steam from the boiler above the lower limit

OR

Auxiliary fuel burners

- At least one auxiliary fuel burner in operation

Objects

Furnace burning permit for the startup burners in effect

2.9.5 Burning permit for the start-up burner

Purpose

The burning permit for the startup burner ensures that both the furnace and the burner are in a state in which the burner can be started and that the process and state information related to both the auxiliary fuel to be burned and to other intermediate agents needed is correct.

Sources

Boiler protection

- Boiler protection in good condition

The emergency-stop for auxiliary fuel

- The emergency-stop button for auxiliary fuel not pressed

Combustion air

- The pressure of the combustion air above the lower limit

The pressure of auxiliary fuel

- The pressure of auxiliary fuel above the lower limit and below the upper limit

The temperature of auxiliary fuel

- The temperature of auxiliary fuel above the lower limit

Burners' control air pressure

- The burners' control air pressure above the lower limit

The pressure of the dispersing agent intermediary

- The pressure of the selected dispersing agent intermediary above the lower limit (oil firing)

Boiler burning permit for the start-up burners

- Boiler burning permit for the start-up burners in effect

Burner in place

- Burner in the burning place signal in effect

Air damper open

- Air damper in open limit

Flame control

- Flame exists (after a certain time from the ignition)



Objects

Burning permit for the start-up burner

- Burning permit for the start-up burners in effect

2.9.6 **Boiler burning permit for load burners (furnace ready) (when required)**

Purpose

The boiler burning permit for load burners ensures that the boiler conditions are such that the load burner can be started up.

Sources

Liquor firing

- Liquor firing in operation
 - Liquor flow to the boiler above the lower limit, and
 - The amount of steam from the boiler above the lower limit

OR

Start-up burners

- At least the required number of auxiliary fuel start-up burners in operation

Objects

Furnace burning permit for load burners in effect

2.9.7 **Burning permit for the load burner**

Purpose

The burning permit for load burners ensures that the furnace and the burner are in a state in which the burner can be started and that the process and state information related to both the auxiliary fuel to be burned and to other intermediate agents needed is correct.

Sources

Boiler protection

- Boiler protection in good condition

The emergency-stop for auxiliary fuel

- The emergency-stop button for auxiliary fuel not pressed

Furnace burning permit for load burners in effect (when required)

- Liquor burning in operation - on

OR

- A sufficient number of start-up burners on

Combustion air

- The pressure of the combustion air above the lower limit

The pressure of auxiliary fuel

- The pressure of auxiliary fuel above the lower limit and below the upper limit

The temperature of auxiliary fuel

- The temperature of auxiliary fuel above the lower limit



Burners' control air pressure (when required)

- The burners' control air pressure above the lower limit

The pressure of the dispersing agent intermediary

- The pressure of the selected dispersing agent intermediary above the lower limit (oil firing)

Load burner in place

- Load burner in burning place signal in effect

Combustion air flow (when required)

- The flow of the combustion air above the lower limit

The proportion of combustion air and fuel (when required)

- The proportion of combustion air and fuel correct

The pressure of auxiliary fuel at the burner

- The pressure of auxiliary fuel at the burner above the lower limit

Flame control

- Flame exists (after a certain time from the ignition)

Objects

Burning permit for the load burner

- Burning permit for the load burner in effect

2.9.8 The emergency-stop for auxiliary fuel

Purpose

The purpose of the emergency-stop buttons for the auxiliary fuel burners is to stop the auxiliary fuel burners and shut the feeding line valves as well as open the ventilation/pressurization valves in case of a possible disturbance such as fire.

Sources

Main ESD button

- Main ESD button pressed

Emergency-stop buttons

- Emergency-stop button pressed in the control room
- Emergency-stop buttons pressed in the field along the passages
- Emergency-stop buttons pressed in the burner control cabinets

Objects

Fire stop valves for the burner's auxiliary fuel

- Fire stop valves for the auxiliary fuel close

Auxiliary fuel burners

- Quick-closing valves for the auxiliary fuel burners close
 - Start-up burners
 - load burners

Ignition gas feed for the burners

- The burners' quick-closing valves for the ignition gas close

Start-up permit for the burners

- The burners' ignition gas valves close



Burner ventilation

- The ventilation of the burner is interrupted and the “furnace ventilated” signal disappears

Implementation:

Emergency-stop buttons must be equipped with opening contacts (circuit-opening connection principle).

Pressing the emergency-stop buttons in the control room or along the passages closes all fire stop valves and the burners’ quick-closing valves either directly through the effect of the outputs of the safety logic or through the outputs of the basic process control system which are wired through relays controlled by the safety logic.

Pressing the emergency-stop buttons in the burner control cabinets closes the feeder valve and, when required, opens the ventilation valve at the burner concerned as well as closes the quick-closing fuel valves at the burner.

2.9.9 Feeding permit for diluted non condensable gases (DNCG)

Purpose

The feeding permit for DNCG ensures that the boiler is in a state in which DNCG can be safely fed into boiler and that the gases burn properly.

Sources

Boiler protection

- Boiler protection in good condition

The amount of steam in the flow (if required)

- The amount of steam in the boiler is above the minimum limit

The level of the odorous gas condensate pocket (when required)

- The level of the odorous gas condensate pocket is below the maximum limit

Odorous gas content (when needed)

- Content is below the minimum limit

Objects

Feeding permit for DNCG

- The feeding permit for DNCG is in effect
 - DNCG to burn valve not locked
 - The collection valves not locked

2.9.10 Burning permit for concentrated non condensable gases (CNCG)

Purpose

The feeding permit for CNCG ensures that the boiler is in a state in which CNCG gases can be safely fed into boiler and that the gases burn properly.



Sources

Boiler protection

- Boiler protection in good condition

Liquor fire signal to the CNCG feed

- Liquor firing in operation
 - Liquor flow to the boiler above the lower limit, and
 - The amount of steam from the boiler above the lower limit

Auxiliary firing in operation, oil/gas or methanol (when required)

- Auxiliary firing in operation

The pressure of the combustion air in the burner

- The pressure of the combustion air above the lower limit

The pressure of the burner's CNCG line

- The pressure of the stink gas line above the minimum and below the maximum

Condensate tank level

- Condensate tank level below the upper limit

The surface of the water lock tank

- The surface of the water lock tank above the lower limit and below the upper limit

Drop separator surface

- The drop separator level below the upper limit

Explosion plates in the stink gas line

- Explosion plates unbroken

Objects

Burning permit for CNCG

- Burning permit for concentrated stink gases in effect
 - CNCG to burn valves and ventilation valve not locked

2.9.11 Start permit for liquor recycling

Purpose

In connection with liquor firing, it is important that the liquor to be burnt does not enter the boiler in concentrations that are too low and that the state of the boiler is such that the liquor fed to the boiler burns and thus does not cause any melt water explosion hazard.

Sources

Liquor feeding valves

- All feeding valves for liquor nozzles closed

Liquor nozzles / Safety gates

- All liquor nozzles away from the boiler
- All safety gates closed

Main ESD

- Main ESD button not pressed

Emergency-stop for liquor burning

- The emergency-stop button for liquor burning not pressed



Objects

Start permit for liquor recycling

- Start permit for liquor recycling in effect
 - liquor pumps not locked
 - Liquor On/Off valves not locked

2.9.12 Liquor burning permit

Purpose

The liquor burning permit ensures that the boiler is in a state where liquor can be safely fed in and that the liquor burns properly. The aim is to prevent the entrance of wash water to the furnace at any stage.

Sources

Boiler protection

- Boiler protection in good condition

Emergency-stop for liquor burning

- The emergency-stop button for liquor firing not pressed

Liquor solids %

- Liquor solids % and/or its density above the lower limit
 - with 2/3 selection

Steam drum pressure (when required)

- Steam drum pressure above the lower limit of the liquor firing limit
 - 2/3 selection

Auxiliary fuel burners in operation

- Adequate number of auxiliary fuel burners in operation

OR

Liquor fire signal still valid

- Liquor flow above the lower limit
- The amount of steam above the lower limit

Wash up for the liquor lines

- Wash up for the liquor lines not selected
- Wash pipe piece not in place
- Hand valve closed

Objects

Liquor firing permit

- Liquor firing permit in effect
- Liquor pumps not locked
- Liquor On/Off valves/control valves not locked

2.9.13 Emergency-stop for liquor burning

Purpose

The purpose of the emergency-stop buttons for liquor burning is to stop liquor burning in case of a possible disturbance, e.g., a broken pipe or fire.



Sources

Main ESD button

- Main ESD button pressed

Emergency-stop buttons

- Emergency-stop button pressed in the control room
- A wall-specific emergency-stop button in the field at the liquor feeding levels pressed

Objects

Liquor feeding valves for the boiler

- Liquor feeding valves close

Liquor feeding and recycling pumps

- Liquor feeding and recycling pumps stop

Liquor recycling valves

- Liquor recycling valves close

Implementation

Emergency-stop buttons must be equipped with opening contacts (circuit-opening connection principle).

Pressing an Emergency-stop button in the control room closes all liquor feeding and recycling valves either directly through the effect of the outputs of the safety logic or through the outputs of the basic process control system which are wired through relays controlled by the safety logic. A wall-specific Emergency-stop button only closes the liquor feeding valve of the wall in question.

2.9.14 Start permit for liquor ring wash up

Purpose

Wash up means, in the first place, washing the liquor feeding lines into a collection tank and, in the second, washing up the nozzle lines and nozzles. The aim is to prevent the entrance of wash water to the furnace at any stage.

Sources

Liquor feeding valves

- All feeding valves for liquor nozzles closed

Liquor nozzles / Safety gates

- All liquor nozzles away from the boiler
- All safety gates closed

Objects

Wash up start permit

- Wash up start permit in effect
 - Liquor pumps not locked
 - Water valves not locked
 -



2.9.15 Start permit for boiler floor wash up

Purpose

The purpose of the start permit for boiler floor wash up is to prevent the entry of wash water to a boiler that is too hot.

Sources

Boiler-specific definitions

Objects

Start permit for floor wash up

- Wash up start permit in effect
 - Water supply pump not locked
 - Water valves not locked

2.9.16 Stopping of air fans

Purpose:

Stopping the air fans when the flue gas outlets are closing prevents the entry of flue gases to the boiler room and high excess pressure in the boiler.

Sources:

- The flue gas outlet closed (at least one flue outlet must be open)
- The flue open signal is compiled from the fan's operation data and the input and output channel data related to open dampers.
 - the fan is not running
 - Using the 2/3 selection regarding the fan's rotating speed data, electric drives on data, and the vacuum pressure measurement after the electrostatic precipitator
 - the rotating speed of the fan below the lower limit
 - the fan is not running
 - the vacuum pressure of the channel above the lower limit
- the income channel damper away from the open limit
 - 3 limit switches
 - 2/3 selection
- the output channel damper away from the open limit
 - 3 limit switches
 - 2/3 selection

Objects

The boiler's lower airs

- The boiler's lower air stops
 - fans stop
 - dampers close

The boiler's upper airs

- The boiler's upper airs stop
 - fans stop
 - dampers close



2.9.17 Quick stop

Purpose:

The purpose of the quick stop is to immediately stop the burning of liquor and the stack by switching off the fuel feed and air supply to the lower part of the furnace. The quick stop is initiated from the control room using the main ESD button.

Source:

Main ESD button in the control room

- The main ESD button has been pressed

Objects

Alarms

- Voice alarms and alarms lights are activated

The feed of liquor

- The liquor pumps stop
- The fire On/Off valves of the liquor feed close
- The feed valves of the liquor close

The auxiliary fuel burners

- The quick-closing valves of the auxiliary fuel burners close

The auxiliary fuel feed

- The fire shut-off valves of the auxiliary fuel feed close

The feed of ignition gas to the burners

- The quick-closing valves of the ignition gas feed to the burners close

The diluted non condensable gases (DNCG)

- The feed valves of DNCG close
- The DNCG are lead to the chimney or to the spare burning place

The concentrated non condensable gases (CNCG)

- The feed valves of CNCG close
- The gasses are lead to the chimney or to the spare burning place

The gasses of the dissolver (when required)

- The gas valves of the dissolver to the boiler close
- The gas valves leading from the dissolver to the chimney / roof open

The air feeds

- The primary air feed to the furnace is prevented
 - the primary air fan stops
 - the primary air damper closes
- The secondary air feed to the furnace is switched to the quick stop position
 - the damper of the secondary air feed is switched to the quick stop position
- The tertiary air feed to the furnace is switched to the quick stop position
 - the closing plate of the tertiary air feed is switched to the quick stop position

The electrostatic precipitators

- The electrostatic precipitators are switched off



Sooting

- Sooting is stopped and the soot fans driven from the furnace
- The sooting steam valves close

Ash and salt conveyors

- Ash and salt transporters stop

Wait / consideration time for rapid drain is started

- The wait / consideration time (3 min) for rapid drain is started

It will be jointly decided during the boiler risk assessment whether or not boiler bottling will also be automatically performed during a quick stop, in which case:

Water and steam valves

- Feed water pumps stop
- Feed water valves close
- The automatic start of the feed water turbine pump is prevented
- Attenuation water valves close
- Main steam valves close
- Start-up closing valve opens
- Start-up control valve opens 20%

Implementation:

The main ESD button must be equipped with opening contacts (circuit-opening connection principle).

The quick-closing valves of the auxiliary fuel lines are closed and if needed, the ventilation valves are opened using the safety instrumented system by switching the control signals of the logic part to de-energized. The quick closing valves and the ventilation valves switch to the safety state through spring actuators.

Burner control itself is not necessarily a part of the SIS, but the burn control logic is given permission to burn from the SIS.

The switching of the fire valves, feed valves, air dampers, motor valves, pumps, air fans etc. to a safe state is implemented either through direct switches in the logic part or through separate relays that are controlled from the safety logic (SIS)



2.9.18 Rapid drain

Purpose:

The purpose of the rapid drain is to prevent water from getting in contact with the melt. Once quick stop has been triggered, a rapid drain can be started at discretion using a switch in the control room.

Source:

The rapid drain button

- The rapid drain button has been pressed

Objects:

- Feed water pumps stop
- Feed water valves close
- The automatic start of the feed water turbine pump is prevented
- The steam cooling water line valves close
- Main steam valves close
- The start-up close valve closes
- The start-up control valve closes

After a set time (3 min) from the quick stop

- The rapid drain valves open

Implementation:

The rapid drain button must be equipped with closing contacts (circuit-closing connection principle).

The safety logic controls separate closing relays that force the valves into the safe position. During safety control the moment limits and the temperature switch of the motor valves must be bypassed.

Releasing the rapid drain button stops the drain, causing the rapid drain valves to close.

All fast purge valves are tested line by line at regular intervals during use by closing the hand valve located after the rapid drain valves. Testing is done valve by valve on the monitor of the control room or locally. Testing can proceed once testing has been chosen on the monitor and the hand valve is closed.

The testing of the rapid drain valves can also be done in the basic automation system. After testing the hand valves must be in the opened position. Testing will be logged. Any faults or inadequacies will be corrected immediately.

There must be an alarm or for instance a red signal light on the emergency stop panel for a closed hand valve.



2.10 TESTING

The SIS acceptance phase includes factory testing (FAT) and deployment testing (SAT), which are primarily used to verify that all safety functions work as they should. Unlike other parts of the normal control system, the SIS is subject to periodic testing at regular intervals in addition to the aforementioned testing. The length of the intervals depends on the acceptance requirements of the various parts of the system. Any periodic testing that requires stoppage should, where possible, be aligned with other inspections (pressure equipment, chemicals, etc.) or other known times of stoppage.

As much of the periodic testing as possible should be executed during normal use and/or the boiler's startup and shutdown phases. This should be taken into account when planning periodic testing.

Field instruments normally require more frequent testing than is expected of the safety logics (Hima, Siemens, Honeywell, etc.). The selected devices and installations of field instruments should thus factor for both ease of testing and the possibility for runtime testing.

A dual-channel SIS installation should always include the possibility of testing the channels separately. Each separate channel must be able to complete the necessary safety controls in their entirety.

Any simulators used for testing must have up-to-date calibration logs that meet official national standards.

For each of the aforementioned tests, it is important to establish a test plan and test instructions, and to enter executed tests into both a log and a detailed test report that is signed by all participants.

2.10.1 Factory acceptance testing

In factory acceptance testing (FAT) the emphasis is on program testing. Field equipment can be simulated by different means, for example, by wiring the sources to switch and light boards to speed up the testing.

The important thing is that all the sources and source combinations (2/3 measurement selections and other logical combinations) are examined and that the computational mA values for interlocking limits are carefully scrutinized.

2.10.2 Commissioning testing and periodic testing

When testing the commissioning of the whole (SAT) and in periodic testing, it is recommended that the source signal simulations for field equipment are performed in a manner that is as real as possible. This means that pressure signals and pressure difference signals are simulated by pumping, temperature signals by warming, press buttons and limit switches



by real devices, and that running data is obtained from real data (the prevention of accidental start in case of a rotating apparatus must be taken into account). The real objects are also observed and identified in the field, valves by their movements, stopped motors by the contactors, by relay movements etc.

The tests of each testing phase are divided into two stages: safety logic tests and field circuit tests.

2.10.3 Testing of safety logic

In the preparatory stages of each testing, it should be ensured that the reason why the safety object goes into a safe state is due specifically to the operation of a safety interlock and not, for example, of a normal process interlock.

For FAT testing, the system supplier draws up a safety logic related testing plan which covers all the system's fault and error situations that can be tested, taking into account also the redundancy in the different parts of the system. Moreover, the supplier draws up a checkup list about the system assembly, configuration and programming in accordance with the requirements of the manufacturer's operation instructions. The functionality of different diagnostic alarms must be verified to make it possible to derive a full benefit from the system's high diagnostics level.

In safety logics that are equipped with doubled processors, the stopping of one of the pair must be tested.

Fault testing of safety logic should include disconnections of cards, isolation of different connections and interruptions of voltage supply. These procedures are also applied in factory acceptance testing (FAT) so that the faults hidden by redundancies can also be revealed. When testing the whole (SAT) and in periodic tests during operation, however, the operating system inspection is not complete. Only some of the cards, connections and voltage interruptions are inspected according to the plan.

2.10.4 Testing of field circuits

In field testing for individual measurement transmitters, in addition to the testing of normal safety limits, also possible signal fault and transmitter failures must be taken into account. Depending on how a signal fault or transmitter failure is arranged in the transmitters, the safety logic must be constructed in such a way that the faults are discovered and the safety functions are implemented.

When testing the field circuits, one should be careful to ensure to that the real interlocking value for a safety limit and the objects observed safe states are recorded.



In 2/3 of the optional measurements the testings should be arranged so that the measurements would be dealt with individually and in 1/3 the safety alarms and fault alarms would be identified and trippings in pairs would be identified.

When drawing up tripping limits based on analog measurements, it should be remembered that a deviation caused by a possible hysteresis should be taken into account downward and that the tripping limit is not to be exceeded at any stage. This applies in cases where the tripping source is the process measurement's upper limit.

The starting point for the testings is always that, for example, in the case of boiler protection, it is simulated initially as being in a good condition. The tripping of the boiler protection will be caused by the signal pairs under testing either by using mA simulators (FAT testing) or by pumping in the field (commissioning and periodic tests). In the same way, the transmitters' signal and transmitter faults must be inspected in pairs, taking into account all the possibilities.



3 PART 2

3.1 GENERAL

This part presents model documents connected with the SIS lifecycle. There may be plant-specific digressions from the model documents. For example, there are two different ways to present logic diagrams and, in addition or as an alternative to these, there are also verbal descriptions with which these diagrams can be supplemented.

3.1.1 General risk graph

Appendix 1 shows, with the help of a risk graph, the safety integrity level definition for a recovery boiler. The definition is based on the risk graph diagram which complies with the SFS-IEC 61508 standard. The calibration of the diagram was adjusted to make it suitable for the definition of the integrity levels for personal, environmental, property and shut down damage in connection with the recovery boiler. The appendix also has a model of the hazard and risk analysis form and shows how to fill it out.

3.1.2 Verification of the integrity level for safety instrumented systems

Appendix 2 presents the methods for verifying the integrity level (the required risk reduction) achieved by safety instrumented system.

The appendix employs mathematics based on failure probabilities. The values of different safety protection factors are added up, and the conclusion is that the overall probability of failure on demand (PFD) of the protective equipment comes up to the required integrity level.

The appendix also has formulae from Appendix B of the IEC 61508-6 standard. When applying the formulae, attention should be paid to the assumptions and limitations discussed in the standard. The formulae presented are not suitable for calculations of diverse channels.

3.1.3 Interlock diagrams

In interlock diagrams, a format similar to that in Appendix 3 can be used. Either the safety interlocks and basic control process lockings are presented in the same diagram, in which case the SIS interlocks are shown with two parallel lines, one continuous and the other one broken, or they are shown in their own diagram.

Appendix 4 shows SIS basic circuit models designed with the 1/2 principle. These illustrate the functional structure of the entire SIS circuit from the sources to the logic solver and further on to the objects. The diagrams detail the sources, I/Os, auxiliary relays, dependencies to the basic process control system and the objects to control.



An example of a verbalized SIS circuit operation is shown in Appendix 5.

3.1.4 Display images

Appendix 6 consists of examples of display images related to the recovery boiler's safety interlock operations.

3.1.5 Circuit design and wiring diagrams

Model diagrams of the loop and wiring diagrams are shown in Appendix 7.

3.1.6 Testing documents

Appendix 8 shows the SIS model documents for factory acceptance testing (FAT) and periodic testing. Periodic testing documents can be adapted for the use as commissioning testing documents.

3.1.7 Operation and maintenance guidelines

Appendix 9 shows the principle model for an operation and maintenance plan. It gives details about the persons responsible for SIS, maintenance of the documentation, training, requirement definitions, and about exceptional situations.

The appendix also contains a model guide for SIS modification procedures in case a need arises for them. Such a guide should give the instructions about who has the authority to order application, wiring, device, and testing modifications as well as about the reporting of the modifications. In cases where the modifications change requirements definitions or are otherwise considerable, the whole safety lifecycle must be looked over thoroughly, starting from the hazard and risk analysis.



SUMMARY

The members of the Finnish Recovery Boiler Committee have inquired for a clear set of guidelines about the implementation of safety instrumentation for recovery boilers. This is due to a concern about safety and the variety of implementations between different manufacturing plants.

The enforcement of the SFS-IEC 61508 reference standard as the Finnish national standard has forced the manufacturing plants in all their processes related to functional safety to refer to that standard and use its methods. This, in turn, has created confusion about implementations and handling of functional safety.

The guideline aims to inform on hardware solutions, both about the selection as well as installation, and thus give the practitioner as clear a picture as possible about the implementation. The document cannot take a position on whether the selected hardware solutions, as far as the measurements and controls are concerned, comply with the integrity level required in each particular case. This matter will be brought to the fore in the future development of the document, once failure probability values that are more reliable have been obtained from the equipment manufacturers in the future. This will allow quantitative (computational) examination of integrity levels for different equipment solutions.

The aim of this document is to present a clear example with the help of guidelines and principle model documents, to clarify and standardize the practice in the future. The interlocks that the work group listed as candidates to be included in SIS are example interlocks from implemented boiler projects. The definition of final safety interlocks should always be based on a hazard and risk analysis, which should take into account, in a case-specific manner, the equipment and process solutions as well as environmental factors such as location, movement and unfamiliar equipment at the plant.

The carrying thought behind the model documents is that the practitioner should have as good a starting point as possible to implement the required documents. The objective is that the example documents and instructions, by their clarity and consistency, would enable efficiency of operation and maintenance in the activities during operation and in periodic testings.

The recovery boiler is subject to many different guidelines and instructions. The implementation and operation of safety instrumentation has required its own guideline to increase its clarity and unity to a decent level. Even at its first stage, the guideline has received an enthusiastic and encouraging welcome from different quarters, among them many competent authorities. The feedback obtained has been very useful in the subsequent scrutiny of the guideline. The work group would like to get feedback in the future also from the practitioners to update and further develop the guideline.

APPENDIX 1

RISK GRAPH

Definition of the safety integrity level for a recovery boiler with the help of a risk graph



1 GENERAL

1.1 Hazard and risk analysis

The purpose of the hazard and risk analysis is to chart and define the hazards related to the operation of a recovery boiler and to define the magnitude of the risks caused by them. The general objective is that the analysis deals separately with personal, environmental, material and shut down hazards.

The authors of the analysis, however, make their decision case by case about whether to deal with the material and shut down hazards in addition to personal and environmental hazards, which according to the general standards and regulations must be dealt with. See EN61508 and EN61511.

A common way to proceed in the Hazard and risk analysis is to start by charting the hazards. An example of this is the Potential Problem Analysis (POA). The charting of hazards continues with the help of hazard recognition methods, the best-known of which is the HAZOP method. HAZOP is based on the examination of the reasons and consequences of the deviations in processes. After the hazards have been recognized, they are categorized, and non-tolerable hazards are then brought to a tolerable level.

Dangers, reasons for those dangers, their consequences, as well as the current preparation and the extent of the risk are presented in an analysis form of which there is a model as an appendix. The management of the hazards must be recorded in the form and in relation to the subprocesses of the boiler. This ensures readability and also that any possible later examination, modifications and additions can be done easily.

The magnitude of the risk (the required risk reduction) related to the risks that can be protected against with safety instrumentation, are defined with the help of the risk graph, which is presented in the following pages. The parameters of the risk graph used in the definition are shown separately for different hazards (personal, environment, material and shut down hazards).

1.2 The factors of the hazard and risk analysis

The persons who participate in the authoring of the hazard and risk analysis, must know, among other things, the operation of the boiler (operations supervisor), measurements, different subprocesses, chemicals to be employed, and the boiler's electrics, instrumentation, control and mechanics.

The leader of the analysis must be cognizant with the analysis method and also adequately know the process to be dealt with.

1.3 Documentation

One must ensure that all the documents that are necessary for dealing with the matter are up-to-date and available, in order that the identification of hazards became as successful as possible (the plant's layout drawings, PI charts, process descriptions, etc.).



1.4 Hazard management

When dealing with hazard items in the hazard analysis, at least the following matters listed below must be considered. The list can be used as a checklist, though only possible real hazards need to be recorded.

Process hazards / Process deviations:

- water access to the furnace
- high / low temperature
- high / low pressure
- high / low level
- flow deviations (no flow, large flow, backflow)
- fire
- explosion
- leak
- failure (for example, DCS, critical measurement, valve)
- mechanical damage
- interruption in the auxiliary energy supply
- human errors
- startup / shutdown
- shut down / maintenance
- others

Hazard factors related to the working environment of the equipment and machines

- moving machine parts
- crushing
- entanglement
- trapping
- hazards due to high pressure gas or liquid spray
- electrical hazards
- hazards due to temperature (e.g. hot surfaces, for example)
- noise
- radiation
- touching or breathing of harmful substances
- biological or microbiological hazards
- disregard to ergonomic principles
- unexpected startup
- human errors
- falling or thrown parts
- slipping, stumbling or falling of person
- hazards associated with lifting
- others

1.5 Classification of damage

The authors of the analysis (the owner of the plant) can decide case by case whether to classify the material and shut down hazards as risks related to safety or whether they should be dealt with as so-called device protections, in which case the markings would



follow the normal practice and the protection circuits would also no come under the periodic testing programs the way safety instrumentation does.

2 RISK GRAPH

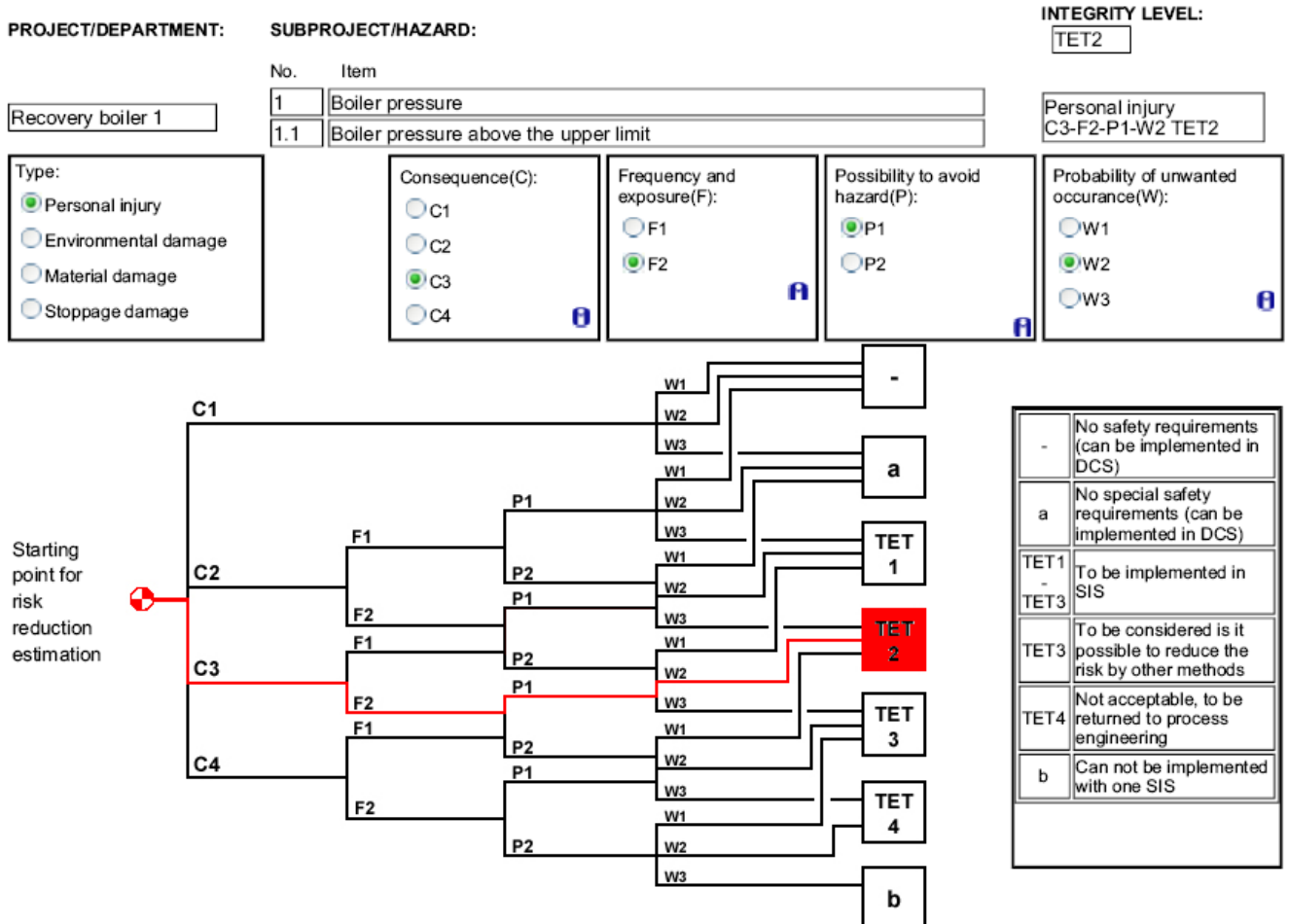


Figure 1. Risk graph



2.1 Integrity levels and the calibration of the parameters in risk graphs

2.1.1 Risk graph parameters

2.1.1.1 Consequence parameter, C

Personal safety

Consequence parameter C is divided in four levels: C1, C2, C3 and C4. In risk assessment, the result parameter is defined according to the table below:

Consequence parameter	Calibration	For example
C1	Minor injury done	Small wound, bruise or mild burn. No sickness leave
C2	Disablement or sickness, no permanent effect on working capacity	Results in, for example, a medical examination and sickness leave
C3	Death or serious injuries	Disablement
C4	Death of several people	

Environmental safety

Consequence parameter	Calibration	For example
C1	No damage, hazard or harm to residents nearby No negative publicity	- Slight smell inconvenience - Mild and concentrated stink gas conduction to the chimney for a short duration only - Small amount of alkaline liquor to the channel
C2	Slight environmental contamination that can be fixed. Slight contaminant emission to the environment	- Smell inconvenience - Concentrated stink gas conduction to the chimney for a longer duration - Alkaline liquor to the channel - Emission which requires an emission notification to be made
C3	Considerable contaminant emission extending outside the plant area and exceeding the permitted limit for the environment	- A large scale alkaline liquor or other emission which causes the destruction of the bacterial strain in the biological purifying plant
C4	Catastrophic emission outside the plant area	Serious contamination of the ground, ground water or waterway - Serious destruction of plant or animal life nearby

Material safety



When estimating the parameter for material damages, equipment damage and repair work, costs are taken into account.

Consequence parameter	Calibration	For example
C1	<50 000 Eur	Replacement of the fan motor
C2	0,05 - 1 M Eur	- Tube leak, - Breakdown of a combustible air fan
C3	1 - 5 M Eur	Stink gas thud
C4	>5 M Eur	Smelt water explosion

Shut down safety

When assessing the result parameter of shut down damages, other plants shut down damages must be considered also.

Consequence parameter	Calibration	For example
C1	<8h	Interruption in liquor firing
C2	8h – 1 wk	- Tube leak, - Breakdown of a combustible air fan
C3	1 wk – 2 mth	Stink gas thud
C4	>2 mth	Smelt water explosion

2.1.1.2 Frequence and exposure time risk parameter F

Personal safety

Stay parameter	Calibration	For example
F1	The hazard centered on a limited area, and movement around the area is irregular	Electrostatic precipitator area, cylinder level
F2	The hazard centers on the entire boiler room or levels where movement is commonplace	Liquor feeding level, burner level and lowest level

Environmental, material and shut down safety

Environmental, material and shut down risks are not time dependent, for which reason the parameter that is always used is F2.

2.1.1.3 Possibility to avoid hazard parameter P

The hazard avoidance parameter, P, describes the possibility to avoid an event in a situation where there is no electric safety function or when it is not operational.



Timewise, the area of influence of parameter P is between the safety function and the hazardous event.

To discover a non-functionality of the protection, there must be an alarm that is not dependent on safety instrumentation, and the non-functionality of the protection must be detectable from process variables and/or state information.

Personal safety

Possibility to avoid a hazard	Calibration	For example
P1	<ul style="list-style-type: none">- Possible in certain circumstances- The operator has a sufficient time to act- The persons in the area have the possibility to move to a safe area	<ul style="list-style-type: none">- The hazard can be spotted and avoided in time- Discovered with measurements and alarms- Shutting up of different combustibles, fast stop
P2	Otherwise, select P2	

Environmental, material and shut down safety

The procedures employed, in case of parameter P for hazard avoidance probability, are the same for environmental, material and shut down safety risks.

Possibility to avoid a hazard	Calibration	For example
P1	<ul style="list-style-type: none">- Possible in certain circumstances- The operator has a sufficient time to act	<ul style="list-style-type: none">- The hazard can be spotted and avoided in time- Discovered with measurements and alarms- Emission of green liquor or other combustibles to the channel- Closure, fast stop
P2	Otherwise, select P2	

2.1.1.4 Probability of the unwanted occurrence W

Probability of the unwanted occurrence parameter, W, describes the appearance probability of a hazard when protection by safety instrumentation is not taken into account. When estimating the probability of an event, the effect of other means to reduce risks is also considered.

Other risk reduction means include, for example:

- - planning, design
- - normal basic process control interlocks, controls, etc.
- - safety valves
- - rupture disks
- - explosion relief panels
- - gas and fire detectors
- - training, instructions, etc.



Personal, environmental, material and shut down safety

The procedures employed, in case of parameter P for hazard existence probability, are the same for personal, environmental, material and shut down safety risks.

Probability of the unwanted occurrence parameter	Calibration	For example
W1	Very small (occurrence interval more than 33 years)	Occurrence of damage not probable in this plant under the present practice
W2	Small (occurrence interval 3 – 33 years)	Damage has occurred in a comparable plant elsewhere and there is a reason to believe that it can happen in this plant within the next 3 – 33 years
W3	Probable (occurrence interval 4mth – 3 years)	It is probable that damage will occur in this plant during the next 3 years

With the help of the occurrence intervals above, a generally tolerable individual risk level can be achieved.

2.2 Hazard and risk analysis form

The front page of the form is to be filled out with the details of the plant and the project, the system being analyzed, the drawings used (e.g., PI diagrams), the participants in the analysis, the date, place and possible observations, which later on must be attended to, for example, if the analysis proves inadequate for some reason.

Real hazard situations should be entered in the **Hazard** section. This applies, for example, to excessive pressure in the boiler. All possible hazards due to hazard situations that can cause at least personal or environmental hazards are recorded. The work group decides whether to record also possible material and shut down hazards.

All possible reasons that can cause the hazard to be dealt with or start a possible chain of events that leads to the hazard in question should be entered in the **Hazard causes** section.

In the **Consequences** section, first the cause-specific general consequences are entered and, under that, the damage-specific consequences for personal, environmental, material and shut down damages. Their possible magnitude is also estimated here.

The **Current Protection (without SRS)** section is used to record all possible preparation, whether mechanical or electrical, handled by instruction or by education, that can affect the possible occurrence of damage.

The **Risk (without SRS)** section records the parameter path (e.g., C3-F2-P1-W2) obtained from the risk graph's estimation of the magnitude of the risk reduction requirement and the risk reduction requirement itself (-, a, SIL1 – SIL4 or b). See Figure 1 of the risk graph.

The **SRS/Actions/Comments** section is used to enter the work group's proposals about possible safety operations in SRS and other possibly needed additional clarifications.

Hazard and risk analysis form

Annex 1

SAFETY INSTRUMENTATION
GUIDELINES FOR RECOVERY BOILERS
Hazard and risk analysis form

	HAZARD	HAZARD CAUSES	CONSEQUENCES -Personal damage -Environmental damage -Material damage -Shut down damage	CURRENT PROTECTION (without SIS)	RISK (without SIS)	SIS/ACTIONS COMMENTS
1. BOILER WATER SYSTEM						
1.1	Steam drum level too low	- a big leak in the furnace	- boiling dry - pipe damage - melt water explosion	- level measurement (2/3) - local water glasses 2 pcs + camera - instructions for operation and maintenance	Person: C4-F2-P2-W1 SIL3 Environment: -C2-F2-P2-W1 SIL1 Material: -C4-F2-P2-W1 SIL3 Shut down: -C4-F2-P2-W1 SIL3	Periodic test inspections and strength measurements for boiler pipes. Tripping from a low level 2/3 react (LI-7312, -13, -22)
1.2	Steam drum level too low	- a leak in the boiler	- boiling dry - pipe damage - <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> melt water explosion hazard	- periodic test inspections and strength measurements for boiler pipes - level measurements (2/3) - <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> local water glasses 2 pcs + camera - difference measurement for the water feed and amount of steam causing an alarm <input type="checkbox"/> <input type="checkbox"/> - instructions for operation and maintenance - periodic test inspections and strength measurements for boiler pipes	Person: C4-F2-P1-W1 SIL2 Environment: -C2-F2-P1-W1 a Material: C1-F2-P2-W2 - Shut down: -C2-F2-P1-W2 SIL1	SIL2 implemented Tripping from a low level 2/3 react (LI-7312, -13, -22) - closing of the auxiliary fuel burners - ventilation discarded - liquor firing stopped - feeding of DNCG stopped

SAFETY INSTRUMENTATION
GUIDELINES FOR RECOVERY BOILERS
Hazard and risk analysis form

	HAZARD	HAZARD CAUSES	CONSEQUENCES -Personal damage -Environmental damage -Material damage -Shut down damage	CURRENT PROTECTION (without SIS)	RISK (without SIS)	SIS/ACTIONS COMMENTS
1.3	Steam drum level too low	- feed water flow prevented	- boiling dry - pipe damage - melt water explosion hazard	□□□□- level measurements (2/3) - □ local water glasses 2 pcs + camera - □ instructions for operation and maintenance - feed water flow measurement	Person: C4-F2-P1-W1 SIL2 Environment: - C2-F2-P1-W1 a Material: C1-F2-P2-W1 - Shut down: C2-F2-P1-W2 SIL1	SIL2 implemented Tripping from a low level 2/3 react (LI-7312, -13, -22) - closing of the auxiliary fuel burners - ventilation discarded - liquor firing stopped - feeding of DNCG stopped
1.4	Steam drum level too low	- a sudden increase in pressure	- the surface of the cylinder falls momentarily	- level measurements (2/3) - local water glasses 2 pcs + camera - instructions for operation and maintenance	Person: C1 - Environment: -C1 - Material: C1 -Shut down: C	No safety requirement

APPENDIX 2

VERIFICATION OF INTEGRITY LEVELS FOR SAFETY INSTRUMENTATION



1 GENERAL

When verifying the integrity level for a protection built within SIS, one must consider separately the adequacy of the device architecture as well as the mathematical probability of failure due to hardware failure. The examination of both the device architecture as well as that of the probability of failure must be conducted for each of the protection's structural part (subsystems) separately. The interlocks that are built for the safety instrumentation consist mainly of the source part or normally transmitters, of safety logic, and of the object part or normally valves and motors (see Figure 1).

2 HARDWARE STRUCTURES

In safety instrumented systems, the functional protections are built of different device structures, so that a single field device, for example, at the source side is replaced by several field devices. This provides additional security for safety operations and in certain structures also more usability for the plant. The most common device structures are:

1/1 structure (1oo1, 1 –out-of-1)

- one component (e.g., measurement), SIS is activated by the component demand or failure

1/2 structure (1oo2, 1 –out-of-2)

- two components connected parallel, SIS is activated by a separate demand or failure from each component

2/2 structure (2oo2, 2 –out-of-2)

- two components connected parallel, SIS is activated by a simultaneously occurring demand or failure from both of the components. Thus, a failure of only one of the components does not activate SIS.

2/3 structure (2oo3, 2 –out-of-3)

- three components are connected parallel, SIS is activated by a simultaneously occurring demand or failure of two of the components. Thus, a failure of only one of the components does not activate SIS.

3 FAILURES

3.1 Dangerous and safe failures

Components' failure modes can be divided into safe and dangerous failures. The classification of the failure modes is based on the examination of the system state after the failure.

Dangerous failure refers to a situation, where a safety related system is prevented from responding to a potentially dangerous situation. Dangerous failures may be caused by, for example, an incorrect system definition, systematic or random equipment failures, a programming or human error or changes that have taken place in the system's operating environment.



A failure in a safety related system can lead to an accident if SIS does not correctly function in that exigency. The mathematical failure probability examination due to hardware failures is based on dangerous failures in practice.

In the case of a safe failure, the system incorrectly interprets the process to be in a dangerous state and thus often performs a shutdown for the failed system.

3.2 Undetected and detected failures

To anticipate failures, it is of the utmost importance that the system or the operator notices a possible failure situation. Based on this, failures can be further classified into undetected and detected failures.

A detected failure is a failure which can be discovered with the internal system diagnostics or in connection with normal operations, for example, from the control room. An undetected failure refers to a situation in which the system experiences a failure but the failure remains unnoticed. Undetected failures are normally found in periodic testing.

4 EXAMINATION OF HARDWARE ARCHITECTURE

In the examination of hardware architecture, hardware fault tolerance and safe failure fraction are brought under inspection. The examination of hardware architecture brings added demands to the complexity of the hardware in some cases where a higher SIL could theoretically be achieved if the mathematical examination approach only were used in the examination.

Table 1 shows the permissible hardware safety integrity according to the fault tolerance of the hardware and safe failure fraction of a device for so-called simple devices. Simple devices are assumed to be devices whose

- all failure modes are known
- behavior in a fault situation can be completely defined
- failure rate track record for detected and undetected dangerous failures is sufficiently well known to be regarded as reliable failure information based on practice.

Table 1. Permissible hardware safety integrity for so-called simple devices

Safe failure fraction	Hardware fault tolerance N		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - 90 %	SIL2	SIL3	SIL4
90 % - 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4



Table 2 shows the permissible hardware safety integrity according to the fault tolerance of the hardware and safe failure fraction of a device for other than so-called simple devices.

Table 2. Permissible hardware safety integrity for other than so-called simple devices

Safe failure fraction	Hardware fault tolerance N		
	0	1	2
< 60 %	not permissible	SIL1	SIL2
60 % - 90 %	SIL1	SIL2	SIL3
90 % - 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

In the tables, fault tolerance N means that N+1 faults can result in losing the safety function. In different hardware architecture examinations it is important to consider, e.g., the safe failure fraction for process measurement transmitters. Once that is, for example, between 60-90 %, SIL1 can be achieved with a single transmitter. Employing two transmitters of the same transmitter type, SIL2 can be achieved. Here we need to assume that the quality requirements for the hardware, software and the project to be implemented are of SIL2 level.

If the components have not been given their safe failure fraction (SFF), these can be calculated with the equation:

$$SFF = (\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_D)$$

where

λ_S = combined safe failures probability

λ_{DD} = the probability of dangerous failures detected by diagnostics

λ_S = combined dangerous failures probability

5

FAILURE PROBABILITY EXAMINATION

In the integrity level verification, each part of the protection is examined separately or, in normal situations, the source (e.g., a transmitter), the logic, and the target (e.g., valve). See Figure 1. In failure probability examination the average probability of failure on demand (PFD_{AVG}) is calculated, once the exigent condition appears, for the protection built in SIS as a whole by adding up the failure probabilities for the different part factors (source, logic, target) as follows:

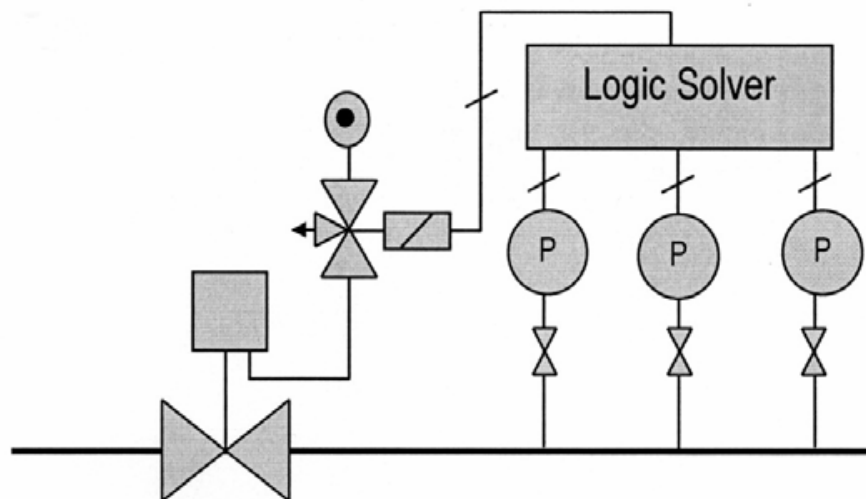


Figure 1. Example basic structure for safety instrumented system

$$PFD_{AVG} = PFD_{SENSOR} + PFD_{LOG} + PFD_{ACTUATOR}$$

where:

- PFD_{AVG} is the average failure probability for the SIS safety function when an exigent situation occurs
- PFD_{SENSOR} is the failure probability of a sensor (e.g., transmitter) or an input connection unit when an exigent situation occurs
- PFD_{LOG} is the failure probability of the logic solver when an exigent situation occurs
- $PFD_{ACTUATOR}$ is the failure probability of an output connection unit or actuator (e.g., valve) when an exigent situation occurs.

5.1

Integrity levels and the probability of dangerous failure

Table 3 shows the correspondence between the integrity levels (SIL) and the average probability of dangerous failure on demand (PFD) as well as the achieved risk reduction. The data on the table is based on PFD values for a small number of demands, which means that the safety function demand is less than once a year or at most twice during the interval between periodic testing.

For example, in SIL2 the average probability for the total number of failures should be between 10^{-2} - 10^{-3} . The risk reduction will then be of 100 – 1000 magnitude.

Table 3. Correspondence between the SIL and the PFD

Integrity level (SIL)	Average probability failure on demand (PFD)	Risk reduction	
4	$\geq 10^{-5}$ $< 10^{-4}$	> 10000	≤ 100000
3	$\geq 10^{-4}$ $< 10^{-3}$	> 1000	≤ 10000
2	$\geq 10^{-3}$ $< 10^{-2}$	> 100	≤ 1000
1	$\geq 10^{-2}$ $< 10^{-1}$	> 10	≤ 100



5.2 PFD formulae for hardware structures

The formulae are from Appendix B of the IEC 61508-6 standard.

Note: When applying the formulae, attention must be paid to the assumptions and limitations expressed in the standard. The formulae presented are not suitable for calculations of diverse channels.

Table 4 explains the parameters for the formulae employed:

Table 4. Abbreviations for the PFD formula

MTTR (h)	Mean time to repair (hours)
TI (h)	Periodic testing interval (hours)
PFD _G	The average probability of failure on demand for a device
PFD _{sys}	The average probability of failure on demand for safety functions
λ_D (1/h)	The probability of dangerous failure (per hour)
λ_{DD}	The probability of detected dangerous failures (per hour)
λ_{DU}	The probability of undetected dangerous failures (per hour)
β_D	The fraction of the detected dangerous failures that have a common origin
β	The fraction of the undetected dangerous failures that have a common origin
t_{CE}	Device's mean equivalent down time (h)
t_{GE}	System's mean equivalent down time (h)

Structure 1001

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

$$PFD_{\text{SENSOR}} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

where

$$t_{CE} = (\lambda_{DU} / \lambda_D) ((T_1 / 2) + MTTR) + (\lambda_{DD} / \lambda_D) MTTR, \text{ thus}$$

$$PFD_{\text{SENSOR}} = \lambda_{DU} (T_1 / 2 + MTTR) + \lambda_{DD} MTTR$$

Structure 1002

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

$$PFD_{\text{SENSOR}} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU}) t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (T_1 / 2 + MTTR)$$

where

$$t_{CE} = \text{as in structure 1001}$$

$$t_{GE} = (\lambda_{DU} / \lambda_D) ((T_1 / 3) + MTTR) + (\lambda_{DD} / \lambda_D) MTTR$$



Structure 2oo2

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

$$PFD_{\text{SENSOR}} = 2(\lambda_{DU} + \lambda_{DD}) t_{CE}$$

where

t_{CE} = as in structure 1oo1

Structure 2oo3

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

$$PFD_{\text{SENSOR}} = 6((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (T_1 / 2 + MTTR)$$

where

t_{CE} = as in structure 1oo1

t_{GE} = as in structure 1oo2



5.3 PFD calculation examples for different device structures

Table 5 shows some obtained PFD values for different device structures using the formulae presented above. The calculation example uses a pressure transmitter whose:

- $\lambda_D = 3,3E-07$ 1/h
- $\lambda_{DD} = 1,2E-07$ 1/h, of which
- $\lambda_{DU} = 2,1E-07$ 1/h
- $\beta = 2\%$
- $\beta_D = 1\%$

In the calculation, the value of MTTR is 8 h and the periodic testing interval (TI) 3 years.

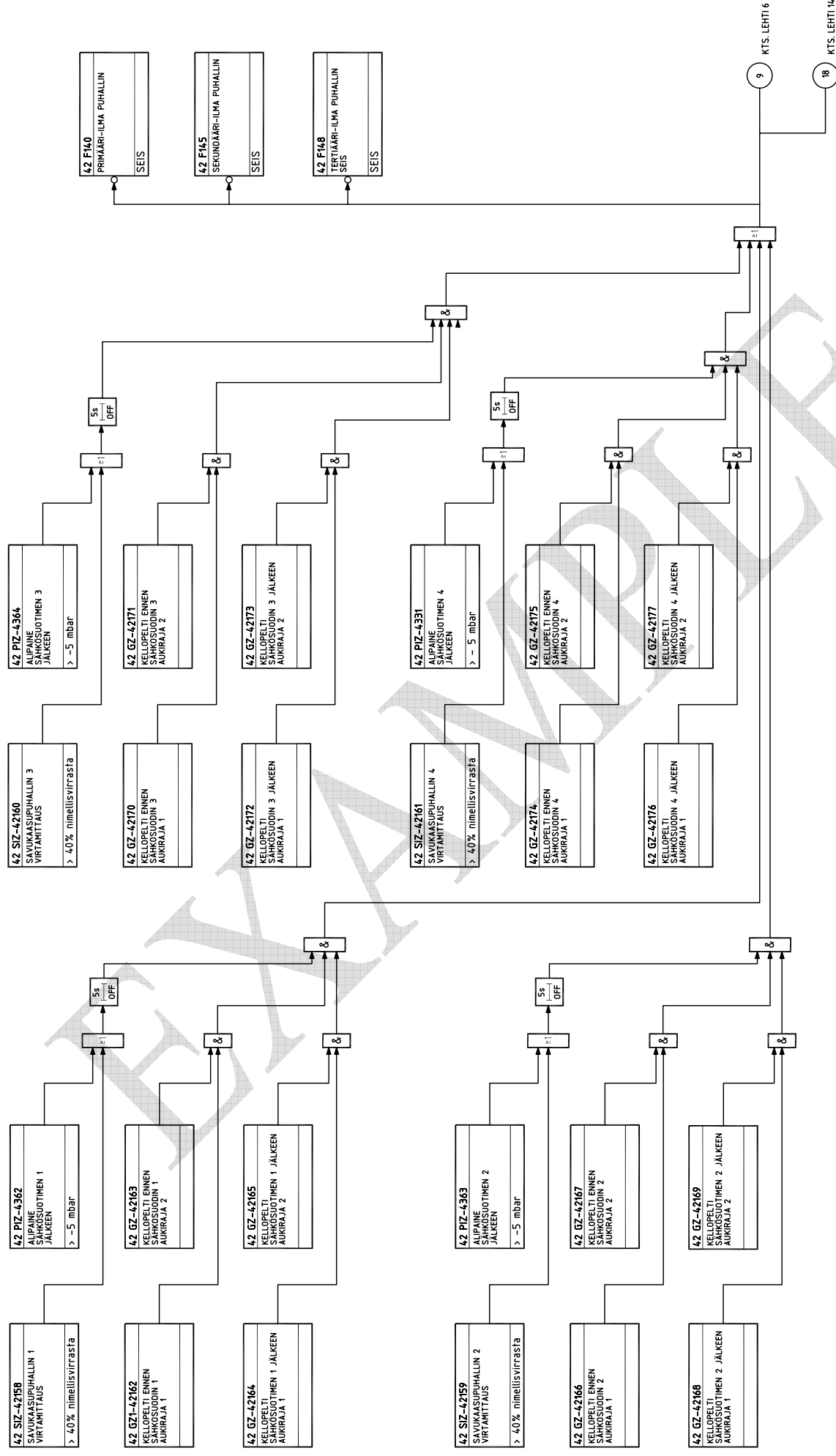
Table 5. PFD calculation example

Rakenne	MTTR (h)	TI (h)	PFD _G	λ _D (1/h)	λ _{DD}	λ _{DU}	β _D	β		
Painelähetin 1001 -> venttiili kiinni										
Anturi	3051T	1001	8	26280	2,8E-03	3,3E-07	1,2E-07	2,1E-07	0,01	0,02
Logiikkaosa	F6217	1001	8	26280	1,5E-05	2,4E-07	2,4E-07	9,6E-10	0,01	0,02
Logiikkaosa	H51q-HS	1001	8	87600	1,7E-04	9,3E-07	9,2E-07	3,6E-09	0,01	0,02
Logiikkaosa	F3330	1001	8	26280	9,5E-06	1,2E-07	1,2E-07	6,5E-10	0,01	0,02
Toimilaite	M1 + EJ	1001	8	26280	6,9E-03	1,8E-06	1,2E-06	5,3E-07	0,01	0,02
				PFD _{sys}	9,9E-03	SIL 2				
Paine-erolähetin 1002 -> venttiili kiinni										
Anturi	3051T	1002	8	26280	6,7E-05	3,3E-07	1,2E-07	2,1E-07	0,01	0,02
Logiikkaosa	F6217	1002	8	26280	2,7E-07	2,4E-07	2,4E-07	9,6E-10	0,01	0,02
Logiikkaosa	H51q-HS	1001	8	87600	1,7E-04	9,3E-07	9,2E-07	3,6E-09	0,01	0,02
Logiikkaosa	F3330	1001	8	26280	9,5E-06	1,2E-07	1,2E-07	6,5E-10	0,01	0,02
Toimilaite	M1 + EJ	1001	8	26280	6,9E-03	1,8E-06	1,2E-06	5,3E-07	0,01	0,02
				PFD _{sys}	7,2E-03	SIL 2				
Paine-erolähetin 2002 -> venttiili kiinni										
Anturi	3051T	2002	8	26280	5,6E-03	3,3E-07	1,2E-07	2,1E-07	0,01	0,02
Logiikkaosa	F6217	2002	8	26280	2,9E-05	2,4E-07	2,4E-07	9,6E-10	0,01	0,02
Logiikkaosa	H51q-HS	1001	8	87600	1,7E-04	9,3E-07	9,2E-07	3,6E-09	0,01	0,02
Logiikkaosa	F3330	1001	8	26280	9,5E-06	1,2E-07	1,2E-07	6,5E-10	0,01	0,02
Toimilaite	M1 + EJ	1001	8	26280	6,9E-03	1,8E-06	1,2E-06	5,3E-07	0,01	0,02
				PFD _{sys}	1,3E-02	SIL 1				
Painelähetin 2003 -> venttiili kiinni										
Anturi	3051T	2003	8	26280	8,7E-05	3,3E-07	1,2E-07	2,1E-07	0,01	0,02
Logiikkaosa	F6217	2003	8	26280	2,7E-07	2,4E-07	2,4E-07	9,6E-10	0,01	0,02
Logiikkaosa	2 * H51q-HS	1001	8	87600	3,7E-04	2,1E-06	2,1E-06	8,1E-09	0,01	0,02
Logiikkaosa	F3330	1001	8	26280	9,5E-06	1,2E-07	1,2E-07	6,5E-10	0,01	0,02
Toimilaite	L12 + BJ	1001	8	26280	5,0E-03	1,3E-06	8,9E-07	3,8E-07	0,01	0,02
				PFD _{sys}	5,5E-03	SIL 2				


APPENDIX 3

INTERLOCK DIAGRAMS

Examples of implemented interlock diagrams



Toimittaja/no.		Toim.pilr.no.		Pvm.		Pir. nimi		Laji		Sovellus		Laitteipaikka	
Ank.no.				Suunn.				Keskus				Laitte	
				Tark.		Osasto		No.				Laitte	
				Hyv.		Tekn.kok.		No.				Rev.	


PÖYRY

SODAKATTILA,
 TURVA-AUTOMAATIO
 SAVUKAASUTIE AUKI

APPENDIX 4

BASIC DIAGRAMS

Examples of a logic solver (1/2 principle)

Muutos Muutos			Muutos Muutos			Muutos Muutos			LIITE 4 16A0913-E0044 2(2)		
									PERUSAUTOMAATIOJÄRJESTELMÄ		
									B0		
									JÄNNITTEEN SYÖTTÖ INVENTTERI		
KANAVA A			<div>TLJ-LOGIIKKA</div>						B0		
KANAVA B			<div>TLJ-LOGIIKKA</div>								
									LIPEÄN PSV1 (SULKEUTUU)		
									LIPEÄN PSV2 (SULKEUTUU)		
									LIPEÄN SYÖTTÖPUMPPU (PYSÄHTYY)		
Toimittaja/ no.			Pvm.			Piiir. nimi			Laji		
Ark. no.			Suunn.			SOODAKATTILAN TLJ LOGIIKKAAVIO LIPEÄN POLTON VALVONTA			Sovellus		
			Tark.						Keskus		
			Hyv.						Piiir. no.		
									Lähtö		
									Rev.		

APPENDIX 5

PRINCIPLE FUNCTIONAL DESCRIPTION

Example of a loop wise functional description



93HS0001 FIRE VALVE FOR NATURAL GAS:

Use:

It functions as a fire valve for natural gas

Operation:

The valve is opened and closed by the operator.
The circuit is connected to safety interlocks. Pressing the Main ESD button or the emergency-stop button closes the valve through SRS.

Alarms: Interlocks:

Safety interlocks:

Interlocks close the valve 93HV0001 when:

Main ESD button 93XZ0001 is pressed in the control room. Emergency-stop button 93XZ0002 is pressed in the control room.

Emergency-stop button 93XZ0003 is pressed at the burner level.

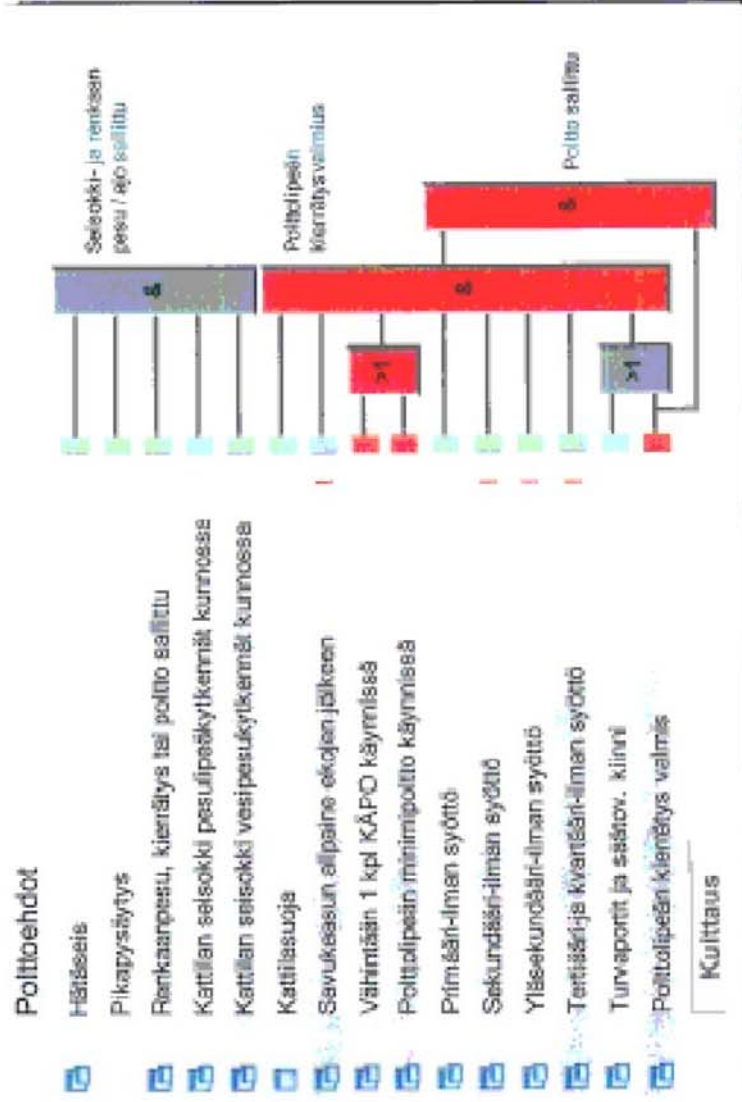
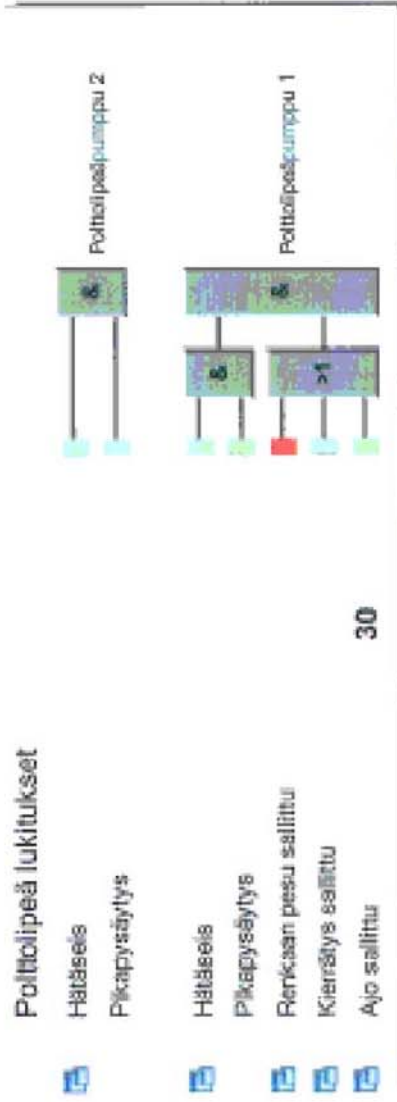
Emergency-stop button 93XZ0004 is pressed at the melt channel level.

Emergency-stop button 93XZ0005 is pressed by the auxiliary burners on the roof.


Data to other circuits:

APPENDIX 6

EXAMPLES OF MONITORING DISPLAYS

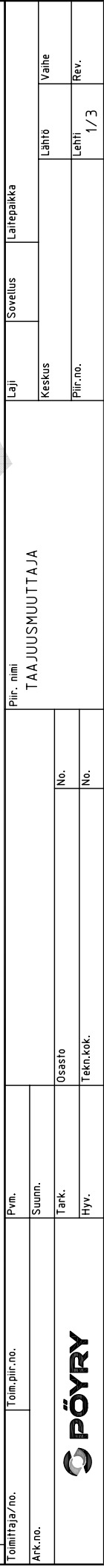


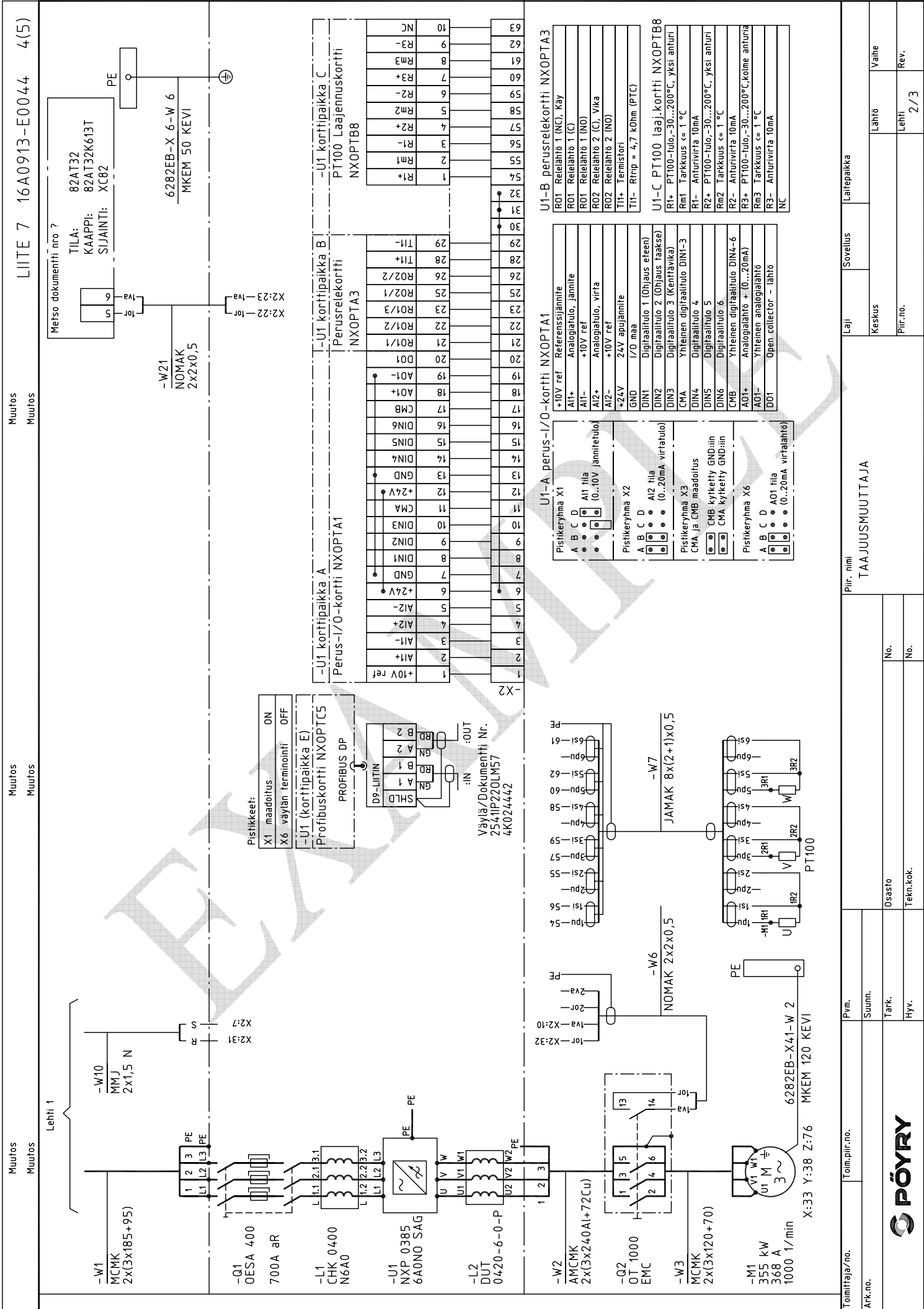
Toimitaja/no.		Toim.piiir.no.		Pvm.		Piir. nimi		Laittepaikka	
Ark.no.				Suunn.		LIPEÄNPOLTTO		Laji	
								Keskus	
				Tark.				Lähtö	
				Hyv.				Piir.no.	
				Tehn.kok.				Lehti	
								Rev.	

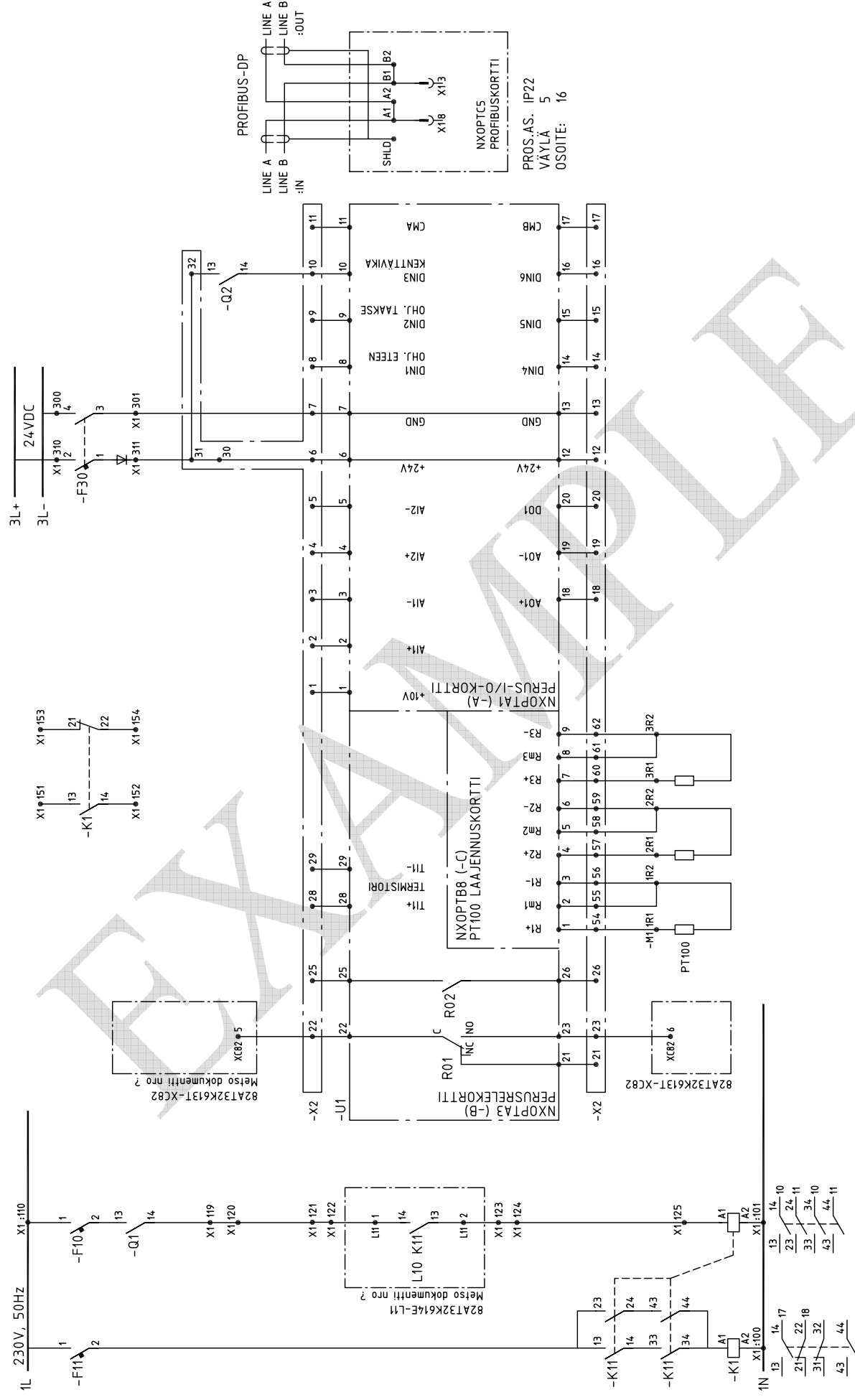
Muutos Muutos		Muutos Muutos		Muutos Muutos		LIITE 6 16A0913-E0044 2(2)			
Savukaasutie auki									
Savukaasupuhallin 1		6282716501							
Savukaasu sähkösuotimelta 1		82PCZ-44634	-3099 Pa	<	-500 Pa				
Kellopeti 1 auki 1		82GZ-44631		>1					
Kellopeti 1 auki 2		82GZ-44632		>1					
Kellopeti 4 auki 1		82GZ-44639							
Kellopeti 4 auki 2		82GZ-44640							
Savukaasupuhallin 2		6282716502							
Savukaasu sähkösuotimelta 2		82PCZ-44624	-4412 Pa	<	-500 Pa				
Kellopeti 2 auki 1		82GZ-44621		>1					
Kellopeti 2 auki 2		82GZ-44622		>1					
Kellopeti 5 auki 1		82GZ-44629							
Kellopeti 5 auki 2		82GZ-44630							
Savukaasupuhallin 3		6282716503							
Savukaasu sähkösuotimelta 3		82PCZ-44613	426 Pa	<	-500 Pa				
Kellopeti 3 auki 1		82GZ-44610		>1					
Kellopeti 3 auki 2		82GZ-44611		>1					
Kellopeti 6 auki 1		82GZ-44619							
Kellopeti 6 auki 2		82GZ-44620							
Toimittaja/no.		Pvm.		Pir. nimi		Laji	Sovelus	Laittepaikka	
Ark.no.		Suunn.		SAVUTIEAUKI		Keskus		Lähtö	
		Tark.				Pir.no.		Lehti	
		Hyv.						Rev.	
		Tekn.kok.							
		No.							
		No.							
									

APPENDIX 7

PRINCIPLE MODELS OF LOOP AND WIRING DIAGRAMS







		Pvm.	Pilir. nimi						Laji	Sovellus	Laitepaikka
Ark.no.	Toim.piliri.no.	Suunn.	TAAJUUSMUUTTAJA						Keskus		Vaihe
		Tark.									
		Hyv.							Pilir.no.		Rev.
											3 / 3

APPENDIX 8

PRINCIPLE MODELS OF TESTING DOCUMENTS

- Testing instruction, FAT testing, 8A**
- Testing record, FAT testing, 8B**
- Testing report, FAT testing, 8C**
- Testing instruction, periodic testing, 8D**
- Testing record, periodic testing, 8E**
- Testing report, periodic testing, 8F**



TESTING INSTRUCTION, FAT TESTING

Recovery Boiler Ltd

SRS PROJECT

EXAMPLE

RECOVERY BOILER

A TESTING OF THE FIELD CIRCUITS

1 FAST STOP

1.1 Preparations

- 1.1.1 Ensure that the process is simulated in such a way that it can be tested.
- 1.1.2 Using the simulating connectors, put the Main ESD button to an OK state in both A and B channels.
- 1.1.3 Prevent programmable interlocks and mark the changes in the logbook.
- 1.1.4 Control valves 93HV0001, 93HV0002, 93HV0003, 93HV0004, 93FV0005, 93FV0006, 93HV0007 and 93HV0008 to an open state and valves 93HV0009, and 93HV0010 to a closed state and start pumps 930001 and 930002 and pumps 930003 and 930004.

1.2 Main ESD 93XZ0001.Z1 (Channel A)

- 1.2.1 Simulate the Main ESD button 93XZ0001 by opening the switch in channel A and record the acknowledgement for channel A.
- 1.2.2 Verify that the interlocks function with light and sound alarms (card output switches off), with the boiler protection (tripped, LED turns off), valves 93HV0001, 93HV0002, 93HV0003, 93HV0004, 93FV0005, 93FV0006, 93HV0007 and 93HV0008 (close) and 93HV0009 and 93HV0010 (open) and pumps 930001 and 930002 (stop) and pumps 930003 and 930004 (stop). Also verify that the startup, load and odorous gas burners are turned off (auxiliary relays disengage).
- 1.2.3 Acknowledge, on the testing record, that the objects interlocks function on channel A.
- 1.2.4 Turn the simulation switch to an OK state on channel A.

1.3 Main ESD 93XZ0001.Z2 (Channel B)

- 1.3.1 Do the preparations as in 1.1.
- 1.3.2 Simulate the Main ESD button 93XZ0001 by opening the switch in channel B and record the acknowledgement for channel B.
- 1.3.3 Verify that the interlocks function with light and sound alarms (card output switches off), with the boiler protection (tripped, LED turns off), valves 93HV0001, 93HV0002, 93HV0003, 93HV0004, 93FV0005, 93FV0006, 93HV0007 and 93HV0008 (close) and 93HV0009 and 93HV0010 (open) and pumps 930001 and 930002 (stop) and pumps 930003 and 930004 (stop).
- 1.3.4 Also verify that the startup, load and stink gas burners are turned off (auxiliary relay disengages).
- 1.3.5 Acknowledge, on the testing record, that the objects interlocks function on channel B.
- 1.3.6 Turn the simulation switch to an OK state on channel B.



TESTING INSTRUCTION, FAT TESTING

1.4 Finalization

- 1.4.1 If you do not test other interlock circuits at the same time, reset the circuits' programmable interlocks and acknowledge the repairs done on the logbook.

2 BOILER PROTECTION (PRESENTED ONLY PARTIALLY)

2.1 Preparations

- 2.1.1 Ensure that the process is simulated in such a way that it can be tested.
2.1.2 Prevent programmable interlocks and control valves 93HV0007, 93HV0008 to an open state and start pumps 930003 and 930004.

2.2 Boiler pressure below 25mbar (Channel A) Transmitters 93PT0001 and 93PT0002

- 2.2.1 On channel B, simulate the limit value data of pressure transmitters 93PT0001, 0002 and 0003 to a good state and in such a way that channel B does not receive the limit exceeded information.
- 2.2.2 Bring the boiler protection to an OK state as follows:
- Flue open
 - simulate valves 93GZ0001.01 and 02 in an open position and fan 930005 to an operating state (one flue open)
 - Primary air fan
 - simulate the primary air fan into an operating state
 - Secondary air fan
 - simulate the secondary air fan into an operating state
 - Steam drum surface ok
 - use potentiometers to simulate, from the terminal blocks to two steam drum level measuring loops, those values that are between the wet and dry boiling limits.
 - Instrument – air measuring circuit ok
 - use potentiometers to simulate, from the terminal blocks to two instrument-air measuring loops, those values that are over the tripping limit.
- 2.2.3 Increase “pressure” 93PT0001 with a simulator, at the same time observing, on the display, the slow increase of the pressure over the tripping limit (above 12 mA).
- 2.2.4 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.2.5 Decrease the “pressure” back below the tripping limit.
- 2.2.6 Increase “pressure” 93PT0002 with a simulator, at the same time observing, on the display, the slow increase of the pressure over the tripping limit (above 12mA).
- 2.2.7 Verify the alarm “Safety limit exceeded on the loop” and “No boiler protection tripped”.
- 2.2.8 Increase also “pressure” 93PT0001 with a simulator, at the same time observing, on the display, the slow increase of the pressure over the tripping limit (above 12mA).
- 2.2.9 Verify that interlocks function with the boiler protection (trips), and that the startup, load and odorous gas burners stop (auxiliary relays disengage), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop).
- 2.2.10 Acknowledge, on the testing record, that the objects interlocks function on channel A.



TESTING INSTRUCTION, FAT TESTING

- 2.2.11 Decrease, with simulators, the “pressures” from both measurements below the tripping limits.

2.3 Broken signal operations

- 2.3.1 Break the measurement signal loop at transmitter 93PT0001 by disconnecting the simulator cable.
- 2.3.2 Verify the alarm “Signal fault on the loop and no safety interlocks”.
- 2.3.3 Reconnect the signal cable.
- 2.3.4 Break the measurement signal loop at transmitter 93PT0002 by disconnecting the simulator cable.
- 2.3.5 Verify the alarm “Signal fault on the loop and no safety interlocks”.
- 2.3.6 Break the measurement signal loop also at transmitter 93PT0001.
- 2.3.7 Verify that interlocks function with the boiler protection (trips), and that the startup, load and odorous gas burners stop (auxiliary relays disengage), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop).
- 2.3.8 Acknowledge, on the testing record, that the objects interlocks function on channel A.
- 2.3.9 Reconnect the simulators to the loops.

2.4 Boiler pressure below 25mbar (Channel B) Transmitters 93PT0001 and 93PT0002

- 2.4.1 On channel A, simulate the limit value data of pressure transmitters 93PT0001, 0002 and 0003 to a good state and in such a way that channel A does not receive the limit exceeded information.
- 2.4.2 Bring the boiler protection to an OK state as follows:
- Flue open
 - simulate valves 93GZ0001.01 and 02 in an open position and fan 930005 to an operating state (one flue open)
 - Primary air fan
 - simulate the primary air fan into an operating state
 - Secondary air fan
 - simulate the secondary air fan into an operating state
 - Steam drum surface ok
 - use potentiometers to simulate, from the terminal blocks to two steam drum level measuring loops, those values that are between the wet and dry boiling limits.
 - Instrument – air measuring loop ok
 - use potentiometers to simulate, from the terminal blocks to two instrument-air measuring loops, those values that are over the tripping limit.
- 2.4.3 Increase “pressure” 93PT0001 with a simulator, at the same time observing, on the display, the slow increase of the pressure over the tripping limit (above 12 mA).
- 2.4.4 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.4.5 Decrease the “pressure” back below the tripping limit.
- 2.4.6 Increase “pressure” 93PT0002 with a simulator, at the same time observing, on the display, the slow increase of the pressure over the tripping limit (above 12mA).
- 2.4.7 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.4.8 Increase also “pressure” 93PT0001 with a simulator, at the same time observing, on the display, the slow increase of the pressure over the tripping limit (above 12mA).



TESTING INSTRUCTION, FAT TESTING

- 2.4.9 Verify that interlocks function with the boiler protection (trips), and that the startup, load and stink gas burners stop (auxiliary relays disengage), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop).
- 2.4.10 Acknowledge, on the testing record, that the objects interlocks function on channel B.
- 2.4.11 Decrease, with simulators, the “pressures” from both measurements below the tripping limits.

2.5 Broken signal operations

- 2.5.1 Break the measurement signal loop at transmitter 93PT0001 by disconnecting the simulator cable.
- 2.5.2 Verify the alarm “Signal fault on the loop and no safety interlocks”.
- 2.5.3 Reconnect the signal cable.
- 2.5.4 Break the measurement signal loop at transmitter 93PT0002 by disconnecting the simulator cable.
- 2.5.5 Verify the alarm “Signal fault on the loop and no safety interlocks”.
- 2.5.6 Break the measurement signal loop also at transmitter 93PT0001.
- 2.5.7 Verify that interlocks function with the boiler protection (trips), and that the startup, load and stink gas burners stop (auxiliary relays disengage), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop).
- 2.5.8 Acknowledge, on the testing record, that the objects interlocks function on channel B.
- 2.5.9 Reconnect the simulators to the loops.

Repeat the same testing also for measurements 93PT0002 and 93PT0003 as well as 93PT0001 and 93PT0003.

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
1. FAST STOP								
93XZ0001.Z1	Button, control room				Light alarm			
	Pressed	<i>Pressed</i>	A		-starts functioning	<i>Relay checked</i>	<i>MTe</i>	
					Sound alarm			
			A		-starts functioning	<i>Relay checked</i>	<i>MTe</i>	
					Boiler protection			
			A		-activates	<i>LED off</i>	<i>MTe</i>	
					FUEL VALVES			
				93HV0001	Fire valve for natural gas			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0002	Fire valve for oil			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0003	Methanol gate			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0004	NCG gate			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0005	Primary air slide			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0006	Primary air slide			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0007	Stop valve for firing liquor 1			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0008	Stop valve for firing liquor 1			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	

Tester in charge:

Signature Name clarification

COMMENTS

Tester in charge:

Signature Name clarification

APPENDIX 8 B
EXAMPLE
FAT TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
				93HV0009	Ventilation of natural gas			
			A		-opens	Relay disengaged	MTe	
				93HV0010	NCG to stack			
			A		-opens	Relay disengaged	MTe	
					BURNERS			
					Startup burners			
			A		-stop	Relay disengaged	MTe	
					Load burners			
			A		-stop	Relay disengaged	MTe	
					NCG burners			
			A		-stop	Relay disengaged	MTe	
					FANS			
				930001	Primary fan			
			A		-stops	Relay disengaged	MTe	
				930002	DNCG fan			
			A		-stops	Relay disengaged	MTe	
					PUMPS			
				930003	firing liquor pump 1			
			A		-stops	Relay disengaged	MTe	
				930004	firing liquor pump 2			
			A		-stops	Relay disengaged	MTe	

Tester in charge:

Signature Name clarification

APPENDIX 8 B
EXAMPLE
FAT TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93XZ0001.Z2	Button, control room				Light alarm			
	Pressed	<i>Pressed</i>	B		-starts functioning	<i>Relay checked</i>	<i>MTe</i>	
					Sound alarm			
			B		-starts functioning	<i>Relay checked</i>	<i>MTe</i>	
					Boiler protection			
			B		-activates	<i>LED off</i>	<i>MTe</i>	
					FUEL VALVES			
				93HV0001	Fire valve for natural gas			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0002	Fire valve for oil			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0003	Methanol gate			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0004	NCG gate			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0005	Primary air slide			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0006	Primary air slide			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0007	Stop valve for firing liquor 1			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0008	Stop valve for firing liquor 1			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0009	Main steam valve			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0010	Main steam valve bypass			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	

Tester in charge:

Signature Name clarification

APPENDIX 8 B
EXAMPLE
FAT TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
				93HV0009	Ventilation of natural gas			
			B		-opens	Relay disengaged	MTe	
				93HV0010	NCG to stack			
			B		-opens	Relay disengaged	MTe	
					BURNERS			
					Startup burners			
			B		-stop	Relay disengaged	MTe	
					Load burners			
			B		-stop	Relay disengaged	MTe	
					NCG burners			
			B		-stop	Relay disengaged	MTe	
					FANS			
				930001	Primary fan			
			B		-stops	Relay disengaged	MTe	
				930002	DNCG fan			
			B		-stops	Relay disengaged	MTe	
					PUMPS			
				930003	firing liquor pump 1			
			B		-stops	Relay disengaged	MTe	
				930004	firing liquor pump 2			
			B		-stops	Relay disengaged	MTe	

Tester in charge:

Signature Name clarification

APPENDIX 8 B
EXAMPLE
FAT TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
1. BOILER PRESSURE								
FURNACE PRESSURE								
93PI0001	Furnace pressure							
	-pressure above 25.0 mbar	12,0 mA	A		1/3 alarm activated			25 mbar = 12.0 mA
93PI0001	Furnace pressure				BOILER PROTECTION			
	-pressure above 25.0 mbar	12,1 mA	A		-activates	Activated	MTe	
93PI003	Simulated to a OK-state	OK						
					BURNERS			
					Startup burners			
			A		-stop	Relay disengaged	MTe	
					Load burners			
			A		-stop	Relay disengaged	MTe	
					NCG burners			
			A		-stop	Relay disengaged	MTe	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			A		-closes	Relay disengaged	MTe	
				93HV0008	Fast stop valve for feeding liquor			
			A		-closes	Relay disengaged	MTe	
					PUMPS			
				930003	firing liquor pump 1			
			A		-stops	Relay disengaged	MTe	
				930004	firing liquor pump 2			
			A		-stops	Relay disengaged	MTe	

Tester in charge:

Signature Name clarification

APPENDIX 8 B
EXAMPLE
FAT TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93PI0001	Furnace pressure							
	-signal broken	<i>Broken</i>	A		1/3 alarm activated			
93PI0001	Furnace pressure				BOILER PROTECTION			
	-signal broken	<i>Broken</i>	A		-activates	<i>Activated</i>	<i>MTe</i>	
93PI003	Simulated to a OK-state	<i>OK</i>						
					BURNERS			
					Startup burners			
			A		-stop	<i>Relay disengaged</i>	<i>MTe</i>	
					Load burners			
			A		-stop	<i>Relay disengaged</i>	<i>MTe</i>	
					NCG burners			
			A		-stop	<i>Relay disengaged</i>	<i>MTe</i>	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0008	Fast stop valve for feeding liquor			
			A		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
					PUMPS			
				930003	firing liquor pump 1			
			A		-stops	<i>Relay disengaged</i>	<i>MTe</i>	
				930004	firing liquor pump 2			
			A		-stops	<i>Relay disengaged</i>	<i>MTe</i>	

Tester in charge:

Signature Name clarification

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93PI0001	Furnace pressure							
	-pressure above 25.0 mbar	12,03 mA	B		1/3 alarm activated			25 mbar = 12.0 mA
93PI0001	Furnace pressure				BOILER PROTECTION			
	-pressure above 25.0 mbar	12,05 mA	B		-activates	Activated	MTe	
93PI003	Simulated to a OK-state	OK						
					BURNERS			
					Startup burners			
			B		-stop	Relay disengaged	MTe	
					Load burners			
			B		-stop	Relay disengaged	MTe	
					NCG burners			
			B		-stop	Relay disengaged	MTe	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			B		-closes	Relay disengaged	MTe	
				93HV0008	Fast stop valve for feeding liquor			
			B		-closes	Relay disengaged	MTe	
					PUMPS			
				930003	firing liquor pump 1			
			B		-stops	Relay disengaged	MTe	
				930004	firing liquor pump 2			
			B		-stops	Relay disengaged	MTe	

Tester in charge:

Signature Name clarification

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93PI0001	Furnace pressure							
	-signal broken	<i>Broken</i>	B		1/3 alarm activated			
93PI0001	Furnace pressure				BOILER PROTECTION			
	-signal broken	<i>Broken</i>	B		-activates	<i>Activated</i>	<i>MTe</i>	
93PI003	Simulated to a OK-state	<i>OK</i>						
					BURNERS			
					Startup burners			
			B		-stop	<i>Relay disengaged</i>	<i>MTe</i>	
					Load burners			
			B		-stop	<i>Relay disengaged</i>	<i>MTe</i>	
					NCG burners			
			B		-stop	<i>Relay disengaged</i>	<i>MTe</i>	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
				93HV0008	Fast stop valve for feeding liquor			
			B		-closes	<i>Relay disengaged</i>	<i>MTe</i>	
					PUMPS			
				930003	firing liquor pump 1			
			B		-stops	<i>Relay disengaged</i>	<i>MTe</i>	
				930004	firing liquor pump 2			
			B		-stops	<i>Relay disengaged</i>	<i>MTe</i>	

Tester in charge:

Signature Name clarification



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

SIS PROJECT

MODEL

FACTORY ACCEPTANCE TEST REPORT ON SAFETY INTERLOCKS (SIS) OF A RECOVERY BOILER

1 TARGET

A safety instrumented system for a recovery boiler (SIS)

2 TIME AND PLACE

01-02.01.2005

Recovery Boiler Ltd

3 PARTICIPANTS

N. N.

Plant operator

N. N.

Person responsible for the plant's SIS

N. N.

Automation installer

N. N.

Main designer

Inspection office/ Y. Y.

Inspector

4 TESTING METHODS

The testing was conducted in accordance with the testing plan and testing instructions.

5 TESTING ACCEPTANCE

On the basis of the testing, we state that the interlocks that form a part of the safety related system for the section function correctly and safely. Therefore, the testing can be accepted.

The testing summary in Annex 1 presents some alarm deficiencies as well as some parts that were left untested.



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

Recovery Boiler Ltd

Plant operator

Person in charge of SIS

Recovery Boiler Ltd

Recovery Boiler Ltd

Inspector

Main designer

APPENDICES

1. Testing summary



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

SIS PROJECT

ANNEX 1

MODEL SUMMARY OF THE FACTORY ACCEPTANCE TEST (FAT) FOR A RECOVERY BOILER'S SAFETY INTERLOCKS (SIS)

1 TESTING ARRANGEMENTS

1.1 Safety system

The system as a whole was installed and connected.

Hardware:

- the system was energized and switched on.

Software:

- the programs had been loaded on the system, and, for individual loops, the normal process control procedures at the process stations had been tested beforehand.

Documentation:

- the following documentation was used in testing: SIS connection diagrams, SIS operation descriptions, SIS display images, loop diagrams and wiring diagrams as well as I/O and hardware layout drawings, testing instructions and testing records.

Testing equipment:

- Measurement channels had been wired to a separate potentiometer board, with which the simulation of individual measurements was easy to implement. During measurement simulations, the measuring loops were connected to mA measuring instruments, which allowed the measurement of accurate mA signals. The measurements were performed by a Beamex MIC 10 calibrator. The calibration certificates for the measuring instruments are in Appendix 6.

2 TESTING

In the testing, the process interlocks at the process station for all targets (valves and motors) were removed, to ensure that SIS operations were the reason for the valves and motors to get to a safe state.

The testing was performed in a straightforward manner, by following the testing instructions, which had been made beforehand and where the testing was divided into possible interlock failures and field equipment and process faults.

The field equipment and process faults were tested in full. (the emergency-stop switch as well as each process measurement value of the boiler protection were simulated and tested for each channel).



TESTING INSTRUCTION, ANNUAL TESTING

In addition to the functioning of the interlocks, alarm signals and interlock indications on SIS displays were examined. Appended there is also a copy of the page of the alarm printer and a display page both related to tripping situations.

3 COMMENTS ON TESTING

3.1 Testing of the safety system

The testing was performed according to the plan. The programs and the system functioned well. Some observations related to the testing:

- A signal fault did not trigger measurement 93PI0001 to send a loop-specific alarm. It was a programming fault, which was then repaired, and a retesting took place.
- System alarms were generally missing. These alarms had not yet been created for the system. The alarms are tested during the commissioning testing.

4 DOCUMENTATION

The testing plan can be found in the testing folder's interleaf Section 1. Functioning of the sources as well as that of interlocks is marked in the testing record (interleaf 4). The same interleaf divider holds the printouts of the alarm pages for the interlock functions. The final safety interlock connection diagrams for the recovery boiler, SIS display images, program diagrams related to interlocks as well as the hardware layout images are in the same folder.



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

SRS PROJECT

EXAMPLE

RECOVERY BOILER

A TESTING OF THE FIELD LOOPS

1 Fast stop

1.1 Preparations

- 1.1.1 Ensure that the process is in such a state that it can be tested.
- 1.1.2 Shut hand valves 1000 (natural gas), 1001 (oil), 1002 (methanol), 1010, 1011, 1012 and 1013 (liquor for firing).
- 1.1.3 Remove the main fuses from fans 930001 (Primary fan), 930002 (Fan for DNCG) as well as from pumps 930003 (Firing liquor pump1), and 930004 (Firing liquor pump 2).
- 1.1.4 Change the connection to main ESD button 93XZ0001-Z2 (channel B) with terminal blocks 93CR11.12 AX1:1-3, so that 1 and 2 connect together.
- 1.1.5 Prevent programmable interlocks and mark the changes in the logbook.
- 1.1.6 Control valves 93HV0001, 93HV0002, 93HV0003, 93HV0004, 93FV0005, 93FV0006, 93HV0007 and 93HV0008 to an open state and valves 93HV0009, and 93HV0010 to a closed state and start fans 930001 and 930002 and pumps 930003 and 930004.

1.2 Main ESD button 93XZ0001.Z1 (Channel A)

- 1.2.1 In the control room, press main ESD button 93XZ0001 in and acknowledge for channel A in the records.
- 1.2.2 Verify that interlocking takes place for light and sound alarms (activate), boiler burner (trips, LED goes off), valves 93HV0001, 93HV0002, 93HV0003, 93HV0004, 93FV0005, 93FV0006, 93HV0007 and 93HV0008 (close) and 93HV0009 and 93HV0010 (open) and fans 930001 and 930002 (stop) and pumps 930003 and 930004 (stop).

Also verify that the startup, load and odorous gas burners become turned off when cutting the 230V control voltage by relays in the burner control cabinet 93CR05.10.

- 1.2.3 Acknowledge, on the testing record, that the objects interlocks function on channel A.
- 1.2.4 Lift the main ESD button back to the upper position.
- 1.2.5 Change the connection to main ESD button 93XZ0001.Z2 (channel B) back as it was.



TESTING INSTRUCTION, ANNUAL TESTING

1.3 Main ESD button 93XZ0001.Z2 (Channel B)

- 1.3.1 Change the connection to main ESD button 93XZ0001.Z1 (channel A) with terminal blocks 93CR11.08 AX1:1-3, so that 3 and 4 are brought together.
- 1.3.2 Do the other preparations as in 1.1.
- 1.3.3 In the control room, press main ESD button 93XZ0001 in and acknowledge for channel B in the records.
- 1.3.4 Verify that interlocking takes place for light and sound alarms (activate), boiler burner (trips, LED goes off), valves 93HV0001, 93HV0002, 93HV0003, 93HV0004, 93FV0005, 93FV0006, 93HV0007 and 93HV0008 (close) and 93HV0009 and 93HV0010 (open) and fans 930001 and 930002 (stop) and pumps 930003 and 930004 (stop). Also verify that the startup, load and odorous gas burners become turned off when cutting the 230V control voltage by relays in the burner control cabinet 93CR05.10.
- 1.3.5 Acknowledge, on the testing record, that the objects interlocks function on channel B.
- 1.3.6 Lift the main ESD button back to the upper position.
- 1.3.7 Change the connection to main ESD button 93XZ0001.Z2 (channel A) back as it was

1.4 Finalization

- 1.4.1 If you do not test other interlock loops at the same time, reset the loops' programmable interlocks and acknowledge the repairs done on the logbook.

2 BOILER PROTECTION (PRESENTED ONLY PARTIALLY)

2.1 Preparations

- 2.1.1 Ensure that the process is in such a state that it can be tested.
- 2.1.2 Shut hand valves 1010, 1011, 1012 and 1013 (liquor for firing).
- 2.1.3 Remove the main fuses from fans 930001 (Primary air fan), 930008 (Secondary air fan), 930005 (Flue gas fan 1), 930006 (Flue gas fan 2) and 930007 (Flue gas fan 3) as well as pumps 930003 (Firing liquor pump 1) and 930004 (Firing liquor pump 2).
- 2.1.4 Prevent programmable interlocks and control valves 93HV0007, 93HV0008 to an open state and smoke dampers 93GZ0001.01, 93GZ0001.02, 93GZ0002.01, 93GZ0002.02, 93GZ0003.01 and 93GZ0003.02 to a closed state and stop fans 930005, 930006 and 930007

2.2 Boiler pressure below 25mbar (Channel A) Transmitters 93PT0001 and 93PT0002

- 2.2.1 On channel B, simulate the limit value data of pressure transmitters 93PT0001, 0002 and 0003 to a good state in such a way that the B channel does not receive the limit exceeded information.
- 2.2.2 Bring the boiler protection to an OK state as follows:
 - Flue open



TESTING INSTRUCTION, ANNUAL TESTING

- open dampers 93GZ0001.01 and 02 and start fan 930005 (one flue open)
 - Primary air fan
 - start the primary air fan
 - Secondary air fan
 - start the secondary air fan
 - Steam drum surface ok
 - simulate, from the terminal blocks to two steam drum surface measuring loops, values that are between the wet and dry boiling limits.
 - Instrument-air pressure
 - ensure that the pressure in the network is above 3,5 bar. If not, simulate, from the terminal blocks to two instrument-air measuring loops, values that are over 3,5 bar.
- 2.2.3 Lift the pressure by pumping with transmitter 93PT0001. At the same time observe, on the display terminal, the slow increase in the pressure above the tripping limit (above 25 mbar).
- 2.2.4 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.2.5 Decrease the pressure back below 25 mbars.
- 2.2.6 Lift the pressure by pumping from transmitter 93PT0002. At the same time observe, on the display terminal, the slow increase in the pressure above the tripping limit (above 25 mbar).
- 2.2.7 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.2.8 Increase also pressure from transmitter 93PT0001, at the same time observing, on the display terminal, the slow increase of the pressure over the tripping limit (above 25mbar).
- 2.2.9 Verify that interlocks function with the boiler protection (trips), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop) and that the startup, load and stink gas burners stop (the relays in the burner control cabinet disengage).
- 2.2.10 Acknowledge, on the testing record, that the objects interlocks function on channel A.
- 2.2.11 Decrease the pressures from both measurements below the tripping limits.
- 2.3 Broken signal operations**
 - 2.3.1 Break the measurement signal loop at transmitter 93PT0001 by disconnecting the signal cable.
 - 2.3.2 Verify the alarm “Signal fault on the loop and no safety interlocks”.
 - 2.3.3 Reconnect the signal cable.
 - 2.3.4 Break the measurement signal loop at transmitter 93PT0002 by disconnecting the signal cable.
 - 2.3.5 Verify the alarm “Signal fault on the loop and no safety interlocks”.
 - 2.3.6 Break the measurement signal loop also at transmitter 93PT0001.
 - 2.3.7 Verify that interlocks function with the boiler protection (trips), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop) and that the startup, load and stink gas burners stop (the relays in the burner control cabinet disengage).
 - 2.3.8 Acknowledge, on the testing record, that the objects interlocks function on channel A.
 - 2.3.9 Reconnect the signal cables with the transmitters.



TESTING INSTRUCTION, ANNUAL TESTING

2.4 Boiler pressure below 25mbar (Channel B)

Transmitters 93PT0001 and 93PT0002

- 2.4.1 On channel A, simulate the limit value data of pressure transmitters 93PT0001, 0002 and 0003 to a good state in such a way that the A channel does not receive the limit exceeded information.
- 2.4.2 Bring the boiler protection to an OK state as follows:
- Flue open
 - open dampers 93GZ0001.01 and 02 and start fan 930005 (one flue open)
 - Primary air fan
 - start the primary air fan
 - Secondary air fan
 - start the secondary air fan
 - Steam drum surface ok
 - simulate, from terminal blocks to two steam drum surface measuring loops, values that are between the wet and dry boiling limits.
 - Instrument-air pressure
 - ensure that the pressure in the network is above 3,5 bars. If not, simulate, from the terminal blocks to two instrument-air measuring loops, values that are over 3,5 bar.
- 2.4.3 Lift the pressure by pumping from transmitter 93PT0001. At the same time observe, on the display terminal, the slow increase in the pressure above the tripping limit (above 25 mbar).
- 2.4.4 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.4.5 Decrease the pressure back below 25 mbars.
- 2.4.6 Lift the pressure by pumping from transmitter 93PT0002. At the same time observe, on the display terminal, the slow increase in the pressure above the tripping limit (above 25 mbar).
- 2.4.7 Verify the alarm “Safety limit exceeded on the loop and no boiler protection tripped”.
- 2.4.8 Increase also pressure from transmitter 93PT0001, at the same time observing, on the display terminal, the slow increase of the pressure over the tripping limit (above 25mbar).
- 2.4.9 Verify that interlocks function with the boiler protection (trips), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop) and that the startup, load and stink gas burners stop (the relays in the burner control cabinet disengage).
- 2.4.10 Acknowledge, on the testing record, that the objects interlocks function on channel B.
- 2.4.11 Decrease the pressures from both measurements below the tripping limits.

2.5 Broken signal operations

- 2.5.1 Break the measurement signal loop at transmitter 93PT0001 by disconnecting the signal cable.
- 2.5.2 Verify the alarm “Signal fault on the loop and no safety interlocks”.
- 2.5.3 Reconnect the signal cable.
- 2.5.4 Break the measurement signal loop at transmitter 93PT0002 by disconnecting the signal cable.
- 2.5.5 Verify the alarm “Signal fault on the loop and no safety interlocks”.
- 2.5.6 Break the measurement signal loop also at transmitter 93PT0001.



TESTING INSTRUCTION, ANNUAL TESTING

- 2.5.7 Verify that interlocks function with the boiler protection (trips), with valves 93HV0003 and 93HV0004 (close) as well as with pumps 930003 and 930004 (stop) and that the startup, load and sink gas burners stop (the relays in the burner control cabinet disengage).
- 2.5.8 Acknowledge, on the testing record, that the objects interlocks function on channel B.
- 2.5.9 Reconnect the signal cables with the transmitters.

Repeat the same testing also for measurements 93PT0002 and 93PT0003 as well as 93PT0001 and 93PT0003.

EXAMPLE

APPENDIX 8 E
EXAMPLE
ANNUAL TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
1. FAST STOP								
93XZ0001.Z1	Button, control room				Light alarm			
	Pressed	<i>Pressed</i>	A		-starts functioning	<i>Functioned</i>	<i>MTa</i>	
					Sound alarm			
			A		-starts functioning	<i>Functioned</i>	<i>MTa</i>	
					Boiler protection			
			A		-activates	<i>Activated</i>	<i>MTa</i>	
					FUEL VALVES			
				93HV0001	Fire valve for natural gas			
			A		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0002	Fire valve for oil			
			A		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0003	Methanol gate			
			A		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0004	NCG gate			
			A		-closes		<i>MTa</i>	Not tested
				93HV0005	Primary air slide			
			A		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0006	Primary air slide			
			A		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0007	Stop valve for firing liquor 1			
			A		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0008	Stop valve for firing liquor 1			
			A		-closes	<i>Closed</i>	<i>MTa</i>	

Tester in charge:

Signature Name clarification

APPENDIX 8 E
EXAMPLE
ANNUAL TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
				93HV0009	Ventilation of natural gas			
			A		-opens	<i>Opened</i>	<i>MTa</i>	
				93HV0010	NCG to stack			
			A		-opens	<i>Opened</i>	<i>MTa</i>	
					BURNERS			
					Startup burners			
			A		-stop	<i>Stopped</i>	<i>MTa</i>	
					Load burners			
			A		-stop	<i>Stopped</i>	<i>MTa</i>	
					NCG burners			
			A		-stop	<i>Stopped</i>	<i>MTa</i>	
					FANS			
				930001	Primary fan			
			A		-stops	<i>Stopped</i>	<i>MTa</i>	
				930002	DNCG fan			
			A		-stops	<i>Stopped</i>	<i>MTa</i>	
					PUMPS			
				930003	firing liquor pump 1			
			A		-stops	<i>Stopped</i>	<i>MTa</i>	
				930004	firing liquor pump 2			
			A		-stops	<i>Stopped</i>	<i>MTa</i>	

Tester in charge:

Signature Name clarification

APPENDIX 8 E
EXAMPLE
ANNUAL TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93XZ0001.Z2	Button, control room				Light alarm			
	Pressed	<i>Pressed</i>	B		-starts functioning	<i>Functioned</i>	<i>MTa</i>	
					Sound alarm			
			B		-starts functioning	<i>Functioned</i>	<i>MTa</i>	
					Boiler protection			
			B		-activates	<i>Activated</i>	<i>MTa</i>	
					FUEL VALVES			
				93HV0001	Fire valve for natural gas			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0002	Fire valve for oil			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0003	Methanol gate			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0004	NCG gate			
			B		-closes		<i>MTa</i>	Not tested
				93HV0005	Primary air slide			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0006	Primary air slide			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0007	Stop valve for firing liquor 1			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0008	Stop valve for firing liquor 1			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0009	Ventilation of natural gas			
			B		-opens	<i>Opened</i>	<i>MTa</i>	

Tester in charge:

Signature Name clarification

APPENDIX 8 E
EXAMPLE
ANNUAL TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
				93HV0010	NCG to stack			
			B		-opens	Opened	MTa	
					BURNERS			
					Startup burners			
			B		-stop	Stopped	MTa	
					Load burners			
			B		-stop	Stopped	MTa	
					NCG burners			
			B		-stop	Stopped	MTa	
					FANS			
				930001	Primary fan			
			B		-stops	Stopped	MTa	
				930002	DNCG fan			
			B		-stops	Stopped	MTa	
					PUMPS			
				930003	firing liquor pump 1			
			B		-stops	Stopped	MTa	
				930004	firing liquor pump 2			
			B		-stops	Stopped	MTa	

Tester in charge:

Signature Name clarification

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
1. BOILER PRESSURE								
FURNACE PRESSURE								
93PI0001	Furnace pressure							
	-pressure above 25.0 mbar	25,1 mbar	A		1/3 alarm activated			
93PI0001	Furnace pressure				BOILER PROTECTION			
	-pressure above 25.0 mbar	25,0 mbar	A		-activated	Activated	MTa	
93PI003	Simulated to a OK-state	OK						
					BURNERS			
					Startup burners			
			A		-stop	Stopped	MTa	
					Load burners			
			A		-stop	Stopped	MTa	
					NCG burners			
			A		-stop	Stopped	MTa	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			A		-closes	Closed	MTa	
				93HV0008	Fast stop valve for feeding liquor			
			A		-closes	Closed	MTa	
					PUMPS			
				930003	firing liquor pump 1			
			A		-stops	Stopped	MTa	
				930004	firing liquor pump 2			
			A		-stops	Stopped	MTa	

Tester in charge:

Signature Name clarification

APPENDIX 8 E
EXAMPLE
ANNUAL TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93PI0001	Furnace pressure							
	-signal broken	Broken	A		1/3 alarm activated			
93PI0001	Furnace pressure				BOILER PROTECTION			
	-signal broken	Broken	A		-activates	Activated	MTa	
93PI003	Simulated to a OK-state	OK						
					BURNERS			
					Startup burners			
			A		-stop	Stopped	MTa	
					Load burners			
			A		-stop	Stopped	MTa	
					NCG burners			
			A		-stop	Stopped	MTa	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			A		-closes	Closed	MTa	
				93HV0008	Fast stop valve for feeding liquor			
			A		-closes	Closed	MTa	
					PUMPS			
				930003	firing liquor pump 1			
			A		-stops	Stopped	MTa	
				930004	firing liquor pump 2			
			A		-stops	Stopped	MTa	

Tester in charge:

Signature Name clarification

APPENDIX 8 E
EXAMPLE
ANNUAL TESTING RECORD

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93PI0001	Furnace pressure							
	-pressure above 25.0 mbar	25,05 mbar	B		1/3 alarm activated			
93PI0001	Furnace pressure				BOILER PROTECTION			
	-pressure above 25.0 mbar	25,04 mbar	B		-activates	Activated	MTa	
93PI003	Simulated to a OK-state	OK						
					BURNERS			
					Startup burners			
			B		-stop	Stopped	MTa	
					Load burners			
			B		-stop	Stopped	MTa	
					NCG burners			
			B		-stop	Stopped	MTa	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			B		-closes	Closed	MTa	
				93HV0008	Fast stop valve for feeding liquor			
			B		-closes	Closed	MTa	
					PUMPS			
				930003	firing liquor pump 1			
			B		-stops	Stopped	MTa	
				930004	firing liquor pump 2			
			B		-stops	Stopped	MTa	

Tester in charge:

Signature Name clarification

SOURCE	NAME	VERIFIED	CHANNEL	TARGET	NAME	VERIFIED	ACK	COMMENTS
93PI0001	Furnace pressure							
	-signal broken	<i>Broken</i>	B		1/3 alarm activated			
93PI0001	Furnace pressure				BOILER PROTECTION			
	-signal broken	<i>Broken</i>	B		-activates	<i>Activated</i>	<i>MTa</i>	
93PI003	Simulated to a OK-state	<i>OK</i>						
					BURNERS			
					Startup burners			
			B		-stop	<i>Stopped</i>	<i>MTa</i>	
					Load burners			
			B		-stop	<i>Stopped</i>	<i>MTa</i>	
					NCG burners			
			B		-stop	<i>Stopped</i>	<i>MTa</i>	
					LIQUOR FEEDING VALVE			
				93HV0007	Fast stop valve for feeding liquor			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
				93HV0008	Fast stop valve for feeding liquor			
			B		-closes	<i>Closed</i>	<i>MTa</i>	
					PUMPS			
				930003	firing liquor pump 1			
			B		-stops	<i>Stopped</i>	<i>MTa</i>	
				930004	firing liquor pump 2			
			B		-stops	<i>Stopped</i>	<i>MTa</i>	

Tester in charge:

Signature Name clarification



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

SIS PROJECT

MODEL

MODEL PERIODIC TESTING REPORT ON THE SAFETY INTERLOCKS (SIS) OF A RECOVERY BOILER

1 TARGET

A safety instrumented system for a recovery boiler (SIS)

2 TIME AND PLACE

01-02.01.2005

Recovery Boiler Ltd

3 PARTICIPANTS

N. N.

Plant operator

N. N.

Person responsible for the plant's SIS

N. N.

Automation installer

N. N.

Electric installer

Inspection office/Y. Y.

Inspector (part time)

4 TESTING METHODS

The testing was conducted in accordance with the testing plan and testing instructions.

5 TESTING ACCEPTANCE

On the basis of the testing, we state that the interlocks that form a part of the safety instrumented system for the section function correctly and safely. Therefore, the testing can be accepted.

The testing summary in Annex 1 presents some alarm deficiencies as well as some parts that were left untested.



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

Recovery Boiler Ltd

Plant operator

Person in charge of SIS

Recovery Boiler Ltd

Recovery Boiler Ltd

Automation installer

Electric installer

Recovery Boiler Ltd

Inspector

APPENDICES

1. Testing summary



TESTING INSTRUCTION, ANNUAL TESTING

Recovery Boiler Ltd

SIS PROJECT

ANNEX 1

PERIODIC TESTING REPORT ON THE SAFETY INTERLOCKS (SIS) OF THE RECOVERY BOILER

SUMMARIZING MODEL

1 TESTING ARRANGEMENTS

1.1 Safety system

The system as a whole was in operation.

Before the testing was started, the central unit cards in the safety system's logic part were replaced with new ones. In this way, also new cards can be tested during periodic testing.

Documentation

- the following documentation was used in testing: SIS connection diagrams, SIS operation descriptions, SIS display images, loop diagrams and wiring diagrams as well as I/O and hardware layout drawings, testing instructions and testing records.

2 TESTING

The test objects in the field testing regarded as belonging to so-called SIS were

- -Fast stop
- -Rapid drain
- -Boiler protection (from several field variables)
- -Emergency-stop (the control room of the recovery boiler, in field 3 pcs)

All the trippings were arranged in such a manner that the tripping in question affects at a time only the SIS's channel (A or B) to be tested. The testing instructions explain how to block each tripping signal away from the channel that is not to be tested.

Analog measurements (sources in the boiler protection part) were simulated in accordance with real process conditions: a calibration pump was used to pump the necessary pressure to the pressure and surface transmitters for creating the SIS tripping limit there. The required activity from the 2/3 operations was generated by always pumping two transmitters to the same state. In this way the whole loop from the transmitter to the safety system could be tested. The calibration certificates for the equipment used in the testing are in the testing folder at tab 9 interleaf.

The valves were in the test in normal operation mode and their movements to a safe state were verified on a monitor and on the field.



TESTING INSTRUCTION, ANNUAL TESTING

The safety switches of the motors were turned to 0 position and the main fuses were removed. That the motors were stopped by interlocks was verified by contractors.

In the testing, the process interlocks at the process station for all targets (valves and motors) were removed, to ensure that SIS operations were the reason for the valves and motors to get to a safe state.

The testing was performed in a straightforward manner, by following the testing instructions, which had been made beforehand and where the testing was divided into possible interlock failures and field equipment and process faults.

The field equipment and process faults were tested in full.

(the emergency-stop switch as well as each process measurement value of the boiler protection were simulated and tested for each channel).

The fault testing for safety interlocks was not done in full, because that had already been performed to completion with the factory acceptance test (FAT). Only some sporadic tests were undertaken. The following fault cases were tested:

- -I/O card no. 5 was removed from frame 0
- -I/O card no. 7 was removed from frame 1
- -the supply of electricity was cut for frame 0
- -expansion bus no. 5 was removed from frame 1
- -frame 1 was removed from the field connection
- -process station 60 was stopped

In addition to the functioning of the interlocks, alarm signals and interlock indications on SIS displays were examined. Appended there is also a copy of the page of the alarm printer and a display page both related to tripping situations.

3 COMMENTS ON TESTING

3.1 Testing of the safety system

The testing was performed according to the plan. The programs and the system functioned well. Some observations related to the testing:

- For some reason, part of the markings of the field equipment and cabling had come loose. The markings were attached by the client during testing.
- On pressing the 93XZ0015 Emergency-switch (B channel), valve 93HV0007 started closing slowly, resulting in a wrong-limit alarm. It was noticed that the air pipes by the valve were bent in some places and slowed down the movement of pressure air in the piping system. The pipes were straightened and the valve's closing time became normal. The client will replace the air tubes during the next stoppage.

APPENDIX 9

PRINCIPLE GUIDE FOR OPERATION AND MAINTENANCE

Plan for operation and maintenance, 9A

Guide for modification procedures, 9B



PLAN FOR OPERATION AND MAINTENANCE

Recovery Boiler Ltd

SIS PROJECT

MODEL

PLAN FOR OPERATION AND MAINTENANCE

HISTORY

The first version was written on 15th January 2003.

1 PLAN TARGET

This recommendation applies to the operation and maintenance of a Safety Related System (SRS) for recovery boilers of Recovery Boilers Ltd.

2 PERSONS IN CHARGE

The person responsible for the safety of the recovery boiler is the operations supervisor.

The responsibility for the maintenance of automation and SIS belongs to the plant's automation maintenance where the person in charge for SIS is the automation master for the recovery boiler.

3 DOCUMENTATION

The entire documentation related to SIS has been collected in section-specific folders, which can be found with the day master, in the archive, in the automation configuration space for the liquor line or with the SIS person in charge.

The operation and maintenance instructions are kept in the SIS documentation folder. The plant's SIS person in charge has the master documentation (clause 2). That person is also responsible for updating the folder and for its distribution to the parties involved.

4 TRAINING

4.1 Training plan

The head operator of the plant and its SIS person in charge draw up a plan of continuous training for the operation and maintenance personnel. The plan pays attention to:

- the training of the technical personnel on fault diagnostics and repair as well as on testing of the system
- the training of the operation personnel
- the introduction of SIS to those unfamiliar with it



PLAN FOR OPERATION AND MAINTENANCE

- a separate retraining of the personnel when the need arises, for example, during the periodic testing or other changes

4.2 Training register

A register is being maintained on training and competency. All the training events are entered to the training register that is maintained by the personnel administration. These events include participation in training events organized by an equipment supplier or a client.

5 REQUIREMENTS DEFINITIONS

5.1 Routine activities

The daily duties of the maintenance personnel in relation to the operation and maintenance of SIS are the following:

- Tidiness of the areas
- Prevention of entry from outsiders to the areas concerned (own key for the areas of electrical and automation equipment and processes)
- Keeping the SIS cabinet doors closed
- Updating of the SIS document folders
- Monitoring of air quality in SIS areas (temperature, pressure difference, moisture)
- Keeping the alarm lists under observation and responding to repeated alarms
- Observing the state of installations during factory visits and initiating preventive actions against hazard conditions possibly caused by temporary placing of foreign objects at the plant.

5.2 Operation instructions

The operation and maintenance instructions for different processing situations are presented in process-specific operation instructions, which include the operations before startup, during startup, running, and shutdown and the actions during a stoppage.

The operation instructions also show the SIS related loops that are in the section and their operation.

The instructions also discuss possible faults/failures and how to remove them, thus trying to prevent a hazardous state or decrease the consequences of the hazard.

5.3 Periodic testing and records

Due to the nature of processes and the structure of SIS, in which all SIS's field and system devices form part of the process control equipment, all field and system devices are under constant operation and being supervised. For example, if one of the connections for duplicated limit information breaks, the limit signal disappears and causes thus the tripping of interlocks and the process shutdown. In measurements based



PLAN FOR OPERATION AND MAINTENANCE

on the 2/3 principle, one can be temporarily removed for calibration or maintenance, but the remaining transmitters then operate as if part of an 1/2 arrangement.

The portion of undetected faults based on the above is small in normal process run situations. It is regarded as reasonable to schedule periodic testing in 18 - 24 - 26 intervals depending on the hardware structure.

The periodic testing plan, the testing instructions and records for periodic testing are in the SIS periodic testing folder. The records drawn up during testing must also be included in that folder.

The periodic testing plan discusses the wherewithal (organization, documentation, testing equipment) for testing, how the tests are run, error correction, test acceptance, report formulation etc.

The testing instructions present, for each loop, the preparations for testing, necessary changes in connections to enable loop-specific testing, tripping instructions for the sources and instructions for record keeping.

5.4 Maintenance and modification

All maintenance operations for field and system equipment (calibration checkup, transmitter change, card replacement etc.) are regarded as maintenance. These do not require SIS compliant acceptance if the devices and limits remain unmodified. Comparable new devices of different types require the SIS compliant acceptance.

Modification operations, on the other hand, include all changes in loops within the domain of SIS (loop additions, changes in cabling, cross-connections and applications). These must always be dealt with in accordance with the acceptance plan and inspection records must be kept of them.

It is the operation supervisor who has the power to give a permit for modifications. The supervisor also can decide which modifications are small, in which case they can be done independently, and which modifications require the use of the authorized assessment method.

The person responsible for the implementation of the modifications regarding SIS and for the competency of the persons involved in those modifications is the person in charge for SIS mentioned in Item 2. That person can decide whether to do the modification with the plant's own resources or whether to ask help from the personnel of the equipment supplier or from other competent outside sources (In accordance with the Guide for modification procedures).

Tuning modifications for transmitters equipped with a so-called safety plate (a normal marking with a red background) must be done with consideration, and the modification must be entered in the SIS documentation.

Transmitters connected to SIS - if lockable either by their transmitter box or installation valve - must be kept locked.



PLAN FOR OPERATION AND MAINTENANCE

The Guide for modification procedures can be found in the SIS documentation folder in its operation and maintenance instructions section. The instructions explain the procedures to be followed for modifications:

- Maintenance of the requirement specifications
- Contacts to authorities and/or assessors
- Maintenance of SIS safety definitions
- Maintenance of implementation plans
- Implementation design and documentation
- Verifications of the modification
- Modification reports

5.5 Operation and maintenance log book

No separate SIS log book is kept. All SIS events – trippings, failures, faults, testing, modifications, etc. - are entered in a shift's event log book.

Shift managers and operators enter SIS related events due to faults, failures or trippings into the shift's event log immediately after the fault, failure or tripping took place.

The operations supervisor must keep track of the events in the log book. If it is found that some fault or hazard situation repeats, measures must be taken to eliminate the problem. These measures can include personnel training, a change in the requirements definitions, a modification in the SIS safety definitions or implementation, replacement or addition of field equipment, etc.

If there is a need for a modification, the operations supervisor creates a change management form, of which a copy is delivered to the person in charge of SIS.

In all these cases the modification procedures of Item 5.4 should be complied with.

5.6 Maintenance instructions

The SIS logic solver does not normally require other maintenance apart from the periodic testing. Possible maintenance instructions are defined in the equipment supplier's instructions.

The maintenance instructions for field equipment that are related to SIS are kept in the documentation folders. Calibration and condition inspections take place during periodic testing.



PLAN FOR OPERATION AND MAINTENANCE

6 EXCEPTIONAL SITUATIONS

In case of a failure in SIS (for example, a faulty card) processes cannot be run. No separate contingency bypasses have been built for testing or maintenance in case of a SIS failure. An exception to this, however, are the 2/3 measurement principles for analog measurements, where one transmitter can be removed, for example, for maintenance. When there is a SIS failure, the SIS related parts of the process are interrupted.

The maintenance personnel repair the faults that appear, in accordance with the operation and maintenance instructions. If necessary, a representative of the equipment manufacturer is invited there.

Following a failure, testing or maintenance, the process startup is performed in accordance with the operation instructions as in the case of a normal startup.

EXAMPLE



GUIDE FOR MODIFICATION PROCEDURES

Recovery Boiler Ltd

SIS PROJECT

MODEL

GUIDE FOR SIS MODIFICATION PROCEDURES

HISTORY

The first version was written on 15th January 2003.

1 OBJECT OF THE INSTRUCTIONS

This recommendation applies to Safety Related Systems (SRS) for recovery boilers by Recovery Boilers Ltd.

2 GENERAL

All maintenance operations for field and system equipment (calibration checkup, transmitter change, card replacement etc.) are regarded as maintenance. These do not require SIS compliant testing if the devices and limits remain unchanged. Comparable new devices of different types require the SIS compliant testing.

Modification operations, on the other hand, include all changes in loops within the domain of SIS (loop additions, changes in cabling, cross-connections, internal wiring and programs). These must always be dealt with in accordance with the testing plan and entered into testing records.

3 MAINTENANCE OF REQUIREMENT SPECIFICATIONS

The person responsible for the SIS requirement specifications, for their changes and for the maintenance, while the boiler mentioned above is in operation, is the person in charge for SIS. That person can give a permit for modifications and decide which modifications are small, in which case they can be done independently, and which modifications require the use of the authorized assessment method. For example, changes in tripping limits and in the user interface can be interpreted as small modifications. Modifications that are more significant include, for example, removals and additions of safety inputs.

4 MAINTENANCE OF IMPLEMENTATION PLANS

Before a modification is realized, it is designed and planned in the modification plans that are in the SIS modification folder. The person responsible for all the operation time maintenance of the SIS's implementation plans is the person in charge of SIS.

The modification should not noticeably change the overall reliability of SIS. Moreover, the modifications must be planned in accordance with the SIL principles such as:



GUIDE FOR MODIFICATION PROCEDURES

- 2 channel structure, 1/2 or 2/3 tripping
- closed-circuit current principle
- single fault in SIS must not prevent the protection from operating when required
- protection must function regardless process stations

When planning a modification, attention must be paid on that the alarms and protection controls should enable the tracking and clarification of tripping signals and facilitate also fault detection.

5 IMPLEMENTATION CHANGES AND DOCUMENTATION

Only a person who is sufficiently knowledgeable in the relevant systems area is allowed to make changes in SIS software and wiring. The person in charge for SIS assumes the responsibility for the competence of the persons involved. It is recommended that the responsibility for the maintenance of the system's software is limited to 2-3 persons, each of whom takes the responsibility for the maintenance of program or other documentation.

Software modifications are kept in the folder for the management of the recovery boiler's configuration state modifications. The operations supervisor is provided with a copy of the modifications.

5.1 Application modifications

A password and a username are needed for signing in to the planning system.

The modifications in line with the implementation plans are prepared on the desktop to the modules from the file system.

The modified and checked up module is left on the desktop to wait for a suitable stoppage. In case it takes a longer time for a stoppage, a backup copy of the desktop should be made.

It must always be confirmed that a command gets through. The front indicator lights of a card confirm its startup.

Do not update the cards when the process is active, because updating momentarily resets the outputs and thus stops the related parts of the process.

5.2 Wiring modifications

The modifications in line with the implementation plans are drawn up for the diagrams of internal wiring loops on the field and in SIS.

Wiring modifications/additions are realized according to the stoppage work list. To avoid short circuiting problems, connected channels are disconnected for the time the work takes.

Do not perform wiring modifications while the process is active, because possible connection problems during the modification work, when new connections are added,



GUIDE FOR MODIFICATION PROCEDURES

can cause the tripping of SIS for the process in question or the relevant parts of the process can get into an abnormal state

5.3 Field equipment modifications

Replacing a field device with a same type of a device is not a modification if the new device has the same calibration as the old one. On the other hand, to replace a field device with one of a different type, to add a new one or to change one's location is modification work, which must be planned and have approved by the person in charge of SIS or by the plant's operations supervisor or, if needed, by a competent authority.

Before a replacement with or addition of a new type of a device, it is necessary to ensure that the device's authorizations designate it as suitable for safety loops.

When installing field devices, one must follow the installation methods and markings corresponding to the implementation plans presented in the SIS description.

6 MODIFICATION TESTING

Modifications/additions are tested in accordance with a testing plan drawn up, modification by modification, by the person in charge for SIS and approved by the plant's operations supervisor. To ensure testing that is independent of the implementation, in addition to the implementation planner, at least one person with a sufficient competence, e.g., the person in charge for SIS, must accompany the testing procedures.

The plan should present the personnel participating in the testing; how to test the functions of a module loaded after a change in the software or wiring modifications or changes in field devices; the acceptance criteria for the tests; and how to document the testing.

After the tests have been completed, the person in charge for SIS updates the related documents in different places in the SIS folder. When necessary, the modifications must be updated also to periodic testing documents and to operations and maintenance instructions.

7 REPORTING ON MODIFICATIONS

The tested modification/addition is reported to the person in charge of SIS, who gathers together all the documentation related to the modification and reports further on to the operation supervisor of the plant. The supervisor approves the modification as having been performed and tested, enters its details in the SIS operation and maintenance log book (if exists), and updates and distributes the bulletin in accordance with the instructions.

If necessary, the plant's operations supervisor reports to the authorities about the modification.

APPENDIX 10

MARKING RECOMMENDATION FOR SAFETY RELATED SYSTEMS



EXAMPLE

Finnish Recovery Boiler Committee

**MARKING RECOMMENDATION FOR SAFETY
INSTRUMENTED SYSTEMS**

19.10.2000

**Report 9/2000
Rev. A**



1 GENERAL

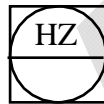
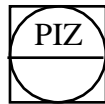
The members of the Finnish Recovery Boiler Committee have felt the need to standardize the marking of the loops and devices in relation to safety instrumented systems (SIS) for recovery boilers. This recommendation aims to standardize the markings of SIS loops used in manufacturing and in planning and design.

2 MARKING RECOMMENDATION FOR LOOPS OF SAFETY INSTRUMENTED SYSTEMS (SIS)

2.1 PI diagram

Those loops which have protection (safety) interlocks (e.g., a valve or something comparable that has been defined as needing interlocks or a measurement that gives locking limit information) are supplied with an additional letter, Z.

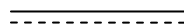
E.g: PIZ, HSZ, PICZ, etc.



2.2 Interlock, control and loop diagram

In interlock and control diagrams signals are marked by drawing a dashed line by the side of a normal line.

For example:



In cross-connection documents these wiring signals are marked with letter Z across the line.

For example: ————— Z —————

The figures carry a legend: z line = red cross-connection wire

2.3 Wiring

The cross-connection wiring for devices with safety interlocks is made with an orange red wire.

2.4 Device plates and markings

The plates of the interlocked devices in field containers are of orange red color. Those field boxes which contain only loops with interlocks are also equipped with an orange red box plate.

Field devices connected with safety interlocks are equipped with normal field equipment plates which are fixed on base plates that are bigger in size and colored orange red. An orange frame is thus shown around the normal plate, which has a text 'Safety Interlocking'.

Example: Under the device plate (yellow) of the firing liquor input valve there is an orange red safety interlocking plate installed.

