

Technical Standard

Date September 15, 2021

Ref. No MEIA0006

Page 1 (14)

Mondi AG.

Mondi Standard Harmonization

IMPLEMENTATION PROCEDURE FOR SAFETY RELATED SYSTEM (SRS)

Contents	1	General
	2	Hazard and Risk Analysis
	3	Overall Safety Requirements
	4	Description of the Technical Realisation
	5	Validation
	6	Operation and Maintenance
	7	Organisation and Responsibilities
	8	Documentation
	9	Summary
Appendices	I	Example of Hazard and Risk Analysis
	II	Example of SRS Specification Requirements
	III	SRS Documentation

Distribution

Mondi, AFRY

Orig.	15.09.2021 / SKO, AFRY	15.09.2021 / EP, AFRY	15.09.2021 / LCa, AFRY	15.09.2021 / LCa, AFRY	Original issue
Rev.	Date/Author	Date/Checked	Date/Approved	Date/Issued	Notes

ABBREVIATIONS

CAT	Configuration Acceptance Test
CE	Conformité Européenne, European conformity
DCS	Distributed Control System
e.g.	exempli gratia, for example
E/E/PE	electrical/electronic/programmable electronic
E/P	Environment and Property
etc.	et cetera, and other similar things
EU	European Union
FAT	Factory Acceptance Test
HART	Highway Addressable Remote Transducer
HAZOP	A hazard and operability study
I	Current
i.e.	id est, that is
IEC	International Electrotechnical Commission
MCC	Motor Control Cabinet
P&ID, PI diagram	Piping and Instrumentation diagram
PED	Pressure Equipment Directive
PFD _{avg}	Average Probability of Failure on Demand
SAT	Site Acceptance Test
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Related System
STO	Safety Torque Off
UPS	Uninterruptible Power Supply
VDC	Volts Direct Current

1 GENERAL

The purpose of this instruction is to specify to the Suppliers the general implementation procedure of the Safety Related Systems (SRS). Deviations from this instruction are permitted only by separate agreement.

This plan is premised on the IEC standard 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) and the IEC 61511 (Functional safety: Safety instrumented systems for the process industry sector).

Laws and regulations currently in force in the current country, especially:

250/2021 Sb. „Zákon o bezpečnosti práce v souvislosti s provozem vyhrazeným technických zařízení a o změně souvisejících zákonů“

NV 190/2022 Sb. „Nařízení vlády o vyhrazených technických elektrických zařízeních a požadavcích na zajištění jejich bezpečnosti“

NV 194/2022 Sb. „Nařízení vlády o požadavcích na odbornou způsobilost k výkonu činnosti na elektrických zařízeních a na odbornou způsobilost v elektrotechnice“

2 HAZARD AND RISK ANALYSIS

The Statute SEVESO II -directive relating to the industrial handling and storage of dangerous chemicals obliges the body engaged in such activities to draw up a special safety report concerning hazard assessment and management of certain plants in which dangerous chemicals are handled and stored. Further, directive 2014/68/EU on pressure equipment safety contains a requirement for the preparation of a hazard assessment and management.

If the delivery incorporates a plant or a part associated therewith referred to in SEVESO II or directive 2014/68/EU, the supplier of such a plan shall carry out a hazard assessment and management of the systems delivered by him. Necessary documents will include, but are not limited to risk evaluations (HAZOP analyses or other applicable problem analyses) covering e.g. source of danger, reasons for danger, possible consequences, as well as classification of dangers (safety integrity level). Also, a report of machine failure modes and failure probabilities shall be submitted to the purchaser.

The hazard and risk analysis have to be made and reported separately for each process. The analysis report is to be attached to the documentation for Safety Related System (see Appendix III)

The method for hazard and risk analysis and the form for the report are described in Appendix I.

3 OVERALL SAFETY REQUIREMENTS

When for a source of danger a safety integrity level is determined to be 1 or higher (i.e. SIL=> 1) the overall safety requirements and allocation of safety requirements will be specified.

The safety requirement specification will be presented clearly as a listing of the sources, which cause the safety functions in Safety Instrumented System (SIS), and the objects, which are controlled to the safety position by SIS. For each source the safety interlocking values of the relevant process variable will be specified. Please see Appendix II for an example of such a listing.

This detailed listing of the safety requirements will be attached to the documentation of the Safety Related System (see Appendix III).

In PI diagrams all the instrument loops and motor circuits that are connected to the SIS will be marked with Z.

If a loop or a circuit is connected to the SIS, the safety interlocks will be presented separately in the functional loop/circuit descriptions.

4 DESCRIPTION OF THE TECHNICAL REALISATION

4.1 General

In the process industries the hazard and risk analysis (e.g. using a risk graph) normally leads to the requirement to lower risk, e.g. SIL => 1. However, it is very rare that SIL of 4 is encountered in the process industries; this highest level would require more than one safety related system to be built.

If the hazard and risk analysis leads to SIL of 1, 2 or 3, then the risk is considered to be too high and it must be reduced (see Appendix I). A common approach to reduce the risk is to build a separate Safety Instrumented System (SIS) which includes sources (sensors, switches etc.), safety logic and objects (valves, pumps etc.).

According to the standards IEC 61508 and IEC 61511 the SIS must in each case be designed to correspond to the SIL reached in the hazard and risk analysis.

When verifying the integrity level for a protection built within SIS, the adequacy of the device architecture as well as the mathematical probability of failure due to hardware failure has to be considered separately. 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 standards require that the average probability of dangerous failure to perform its design function on demand (PFDavg) will be calculated for the chosen Safety Instrumented Function (SIF). This calculation is to be based on the failure frequencies of all the components (i.e. sources, safety logic and objects). This value must correspond to the SIL in question.

The calculated PFDavg value is based on the dangerous failure frequencies of the various components; however, these frequency values are for most field devices still imperfect. Thus, assumptions need to be made which, in turn, reduce the reliability of the evaluation of the adequacy of SIS.

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.

Examples and practical experiences, however, provide guidelines for the reduction of the risk for each SIL:

- SIL 1 requires e.g. one certified and reliable transmitter, one certified logic and one certified valve
- SIL 2 requires e.g. two certified and reliable transmitters (using the principle of “1 out of 2”), one certified logic and one certified valve with two certified solenoid valves.
- SIL 3 requires e.g. three certified and reliable transmitters (using the principle of “2 out of 3”), one certified logic and one certified valve with two certified solenoid valves. It should be noted that the principle of “2 out of 3” increases also the usability of the plant.

To increase the usability of the plant in case of SIL 1 and SIL 2 two channels in the safety logic (including two separate outputs) are used.

4.2 Safety Instrumented System

The Safety Instrumented System (sensors – safety logic – actuators) will be designed so that the safety requirements of the safety integrity level will be fulfilled by each component of the system.

The field devices used for the normal process control can be used for SIS. However, the signals of the sources (the measurements, limit switches, hand switches etc.) will be connected first to the safety logic (and only then to DCS). SIS has to be independent from DCS.

4.2.1 Safety logic

The safety functions will be realized with the programmable safety logic, which is certified for the use in the safety applications according to IEC standards 61508 and 61511.

The safety logic will be a separate unit, which can be connected to the process control system e.g. via bus or hard wiring. This separation can be realised by a totally separate logic (e.g. Hima, Siemens and Pilz). The safety logic could be also integrated with DCS if agreed with Purchaser and as long as the system is certified for the use in safety applications.

Hardware SRS functions, such as relays, must be avoided.

The system should be designed so that should avoid using additional external hardware, everything should be handled internally in the Safety controller.

4.2.2 Certificates and manuals

The safety logic has to be certified to the highest safety integrity level (SIL) that the process requires according to the risk analysis and the subsequent safety requirements. The certificates and manuals will be delivered by the supplier two weeks before the first evaluation of the documentation for the definition of the safety requirements.

The certificates and manuals will be attached to the documentation for the Safety Instrumented System; see Appendix III.

4.2.3 Measurement and control principles

The analogue transmitters (pressure, temperature, flow etc.) will be used instead of the binary switches to measure relevant process variables. The signals will be 4-20mA.

The binary signals (limit switches, position switches etc.) will be connected to the safety logic using Fail to Safe principle.

In case of SIL > 1 redundant measurements (1 out of 2 or 2 out of 3) will be used and there is deviation (of over 10 %) of the measurement values will be alarmed. All device or cable failures will be handled separately and alarmed. If the measurement is used both in the safety functions and in normal process operations (in DCS) the measurement signal will always be connected directly to the safety logic and only then to DCS (e.g. via a bus).

4.2.4 Diagnostic of the safety logic

It is recommended to design the safety logic with self-diagnostic and redundancy. This means redundancy of the safety logic controller. The controllers will be compared and any differences will be alarmed.

Alarm displays will be made for the safety loops; indicating relevant process alarms, field device and signal faults. Alarm texts will be formed for safety functions of the SIS. Also, sources for the SIS interlocks will be clearly presented.

4.2.5 Software

The safety functions shall be built totally in SIS, not partly in DCS, for example the compensation calculation.

The software documentation of the safety logic will be separate from the normal DCS software documentation. If that is not possible, the safety logic part will be marked clearly in the software documentation, e.g. other colour, separate line thickness or line type. Any unauthorized changes or modifications to the software will be prevented by the use of a password.

The trip limits should be set in DCS systems so that it trips in DCS earlier than in the safety system, to only trip via the safety system in the event that the DCS controller is not active.

Each safety circuit must be displayed in operator environment, with full information from safety controller and DCS controller incl. trip limits, time for last trip, total number of trips.

In DCS systems, logic must be implemented in order to be able to initiate and test run the security functions.

The Safety system should only handle discrete signals such as AI, AO, DI and DO, no functional objects should be included into the Safety application software.

It is recommended to design the software in the most basic way with “AND”, “OR” timers and limit switches.

The SIS logic supplier shall hand over the last version of the program to Purchaser for the control of the modification management. SIS software programming need to be implement according to IEC 61508 and 61511.

4.3 Field equipment

All field equipment must be certified for the use in safety applications. Pressure and temperature will be measured with 2-wire HART transmitters. Any unauthorized changes or modifications of the transmitter calibration will be prevented, e.g. by the use of a password.

The redundant transmitters must have the same calibration.

4.3.1 Instrument Equipment

4.3.1.1 Pressure and differential pressure transmitters

The pressure and differential pressure transmitters will be installed directly to the process pipes or the transmitters with capillaries will be used. If the isolation or manifold valve has to be used, the opening and closing of the valve will be prevented by locking of the valve.

If the compensation calculations are needed all relevant signals will be connected to the safety logic and the compensation will be made in the safety logic.

4.3.1.2 Temperature measurements

Pt100 sensors with transmitters in the junction box will be used for temperature measurements.

4.3.1.3 Valves

Both on/off and control valves that are connected to the safety logic will be equipped with the spring return actuator; the spring moving the valve to the required safety position.

For on/off valves the control of the solenoid valve will be controlled by the output from SIS. In the safety position of the valve the solenoid valve is de-energized. When SIL = or > 2, the two solenoid valves will be used. Both limits of on/off valve need to be connected to the SIS.

For the control valves a solenoid valve will be added between the positioner and actuator; thus the spring will force the valve to the required safety position. When SIL = or > 2, the two solenoid valves will be used. The solenoid valve will be controlled by the safety logic.

4.3.1.4 Limit switches

The limit switches will be chosen and connected to the safety logic using Fail to Safe principle. The switches can be either inductive (2-wire) or mechanical with the self-cleaning contacts.

4.3.1.5 Solenoid valves

In the safety systems the solenoid valves have to be of the spring return type and without the hand operation possibility. The control power of the solenoid valves will be 24 VDC. When SIL = or > 2, the two solenoid valves will be used.

4.3.2 Electrical Equipment

4.3.2.1 MCC's

The contactors in MCCs connected to the safety logic will be dimensioned so that $I=I_n/0.6$.

The running status of the motors will be hardwired to SIS, if running status is a part of safety interlocking or safety function in SIS.

To stop Direct-On-Line motors, certified auxiliary relays will be used (one relay in SIL 1 and SIL 2, two relay in SIL 3). The connection will be made so that the control voltage for MCC is cut off when the relays are de-energised.

To stop Variable-Frequency Drive motors, certified auxiliary relays will be used (one relay in SIL 1, two relay in SIL 2 and SIL 3). The connection will be made so that the Safe Torque Off (STO) is disabling energy off when the relays are de-energised.

4.3.2.2 Motor valves

Motor valves which are part of Safety Instrumented Function, will be hardwired to SIS.

The thermal switches and torque limits of the motor valves will be bypassed in the safety functions. The safety functions of the motor valves will be realised by duplicating the auxiliary contacts in MCC.

4.3.2.3 Auxiliary relays

The auxiliary relays relating to the safety control of the valves and motors must be installed in the same rack as the safety logic.

Certified relays must be used in all safety controls.

4.3.2.4 Safety switches

Both the motors and motor valves will be equipped with the normal safety switches by the equipment. Special cases will be handled separately.

4.3.2.5 Emergency stop push button

The emergency stop push buttons have to be of "mushroom" type and red in colour. The push buttons are to lock in down position and the reset is possible only with the use of a key. The key released emergency stop push button is only recommended, not mandatory and to be decided case by case. The field-mounted push buttons will be marked so, that they are readable from 10 m.

Emergency stop push button shall be wired to the SIS and each emergency stop button shall be individual signals. Each emergency stop push button shall be implemented by two contacts and two input channels in SIS.

4.3.2.6 Power supply

The instrument equipment which need external power supply will be connected to the UPS.

4.4 Installation, marking and cabling of the field equipment

4.4.1 Installation

4.4.1.1 Process connections

Each SIS connected measurement must have its own process connection.

4.4.1.2 Isolation and manifold valves

Both the isolation valves and manifolds will be equipped with the locks.

For the SAT or periodic tests the pressure and differential pressure transmitter will be equipped with either a separate valve or a “pumping” connection to the isolation and manifold valve. The “pumping” can be also made to using the 5/2 manifold.

4.4.1.3 Installation standards and hook-ups

In general, the installation of the equipment connected to SIS will be done according to the normal field equipment standards and hook-ups. No separate installation documentation for the SIS connected equipment will be made.

The installations will be designed and made so that the tests can be made without removing the transmitters, measuring lines or cables. However, the installation of the temperature sensors will be designed so that the sensors can be moved to a heater for the test.

4.4.1.4 Field boxes

The cabling of the SIS connected signals will be done via separate field boxes connected directly to SIS. The field boxes which are used for the SRS signals will be equipped with the separate terminal strips with red colour (or another colour defined for SIS in the Mill specific standard) markings.

If it is economically more feasible the SIS signal cables may be pulled directly to the safety logic.

4.4.2 Marking

To highlight the equipment connected to the SIS (sensors, transmitters, switches, valves, MCC's, motors, safety switches etc.) as well as the related isolation valves, process connections and cablings they must be marked with the red name plates (or another colour defined for SIS in the Mill specific standard).

4.4.3 Cabling and cross connection wiring

Shielded cables will be used for the SIS signals.

The redundant signals will be cabled via separate routes if possible. If the multi-core cables are used for SIS signals no “normal” signals are allowed in the same cable.

5 VALIDATION

The SIS will be validated during the project in four separate phases;

- 1) Specification
- 2) Engineering and FAT
- 3) Implementation and validation

4) Operation and maintenance

After the start-up the SIS will be tested periodically according to the procedures presented in operation and maintenance plan.

The purchaser, suppliers, designers, authorities and also possible the insurance company ought to participate in all tests. The test reports have to be signed after each test by the person in charge of SIS testing.

5.1 **Factory acceptance test (FAT)**

In a factory acceptance test the SIS will be tested separately from the normal DCS program test.

For FAT a test plan will be prepared. It will contain the object of the plan, the test organization, the requirements of the test, the documentation, the test equipment, the approval procedure of the tests and the instruction for the test report.

In the test instruction the preparations for the test, all simulations, calculation the values for the interlocks and the safety functions for the objects (valves, motors etc.) will be described.

5.1.1 **Configuration acceptance test (CAT)**

In CAT the process interlocks (field equipment) and also the safety logic will be tested. The process interlocks will be tested by simulating the process value; the value will be compared to the calculated mA-value of the interlocking limit. Also, the interlocks for the cable and the sensor faults will be tested. In the safety logic test the card, bus and power supply faults will be tested.

In the test report the sources, interlocking limits for process values, the objects and the safety positions for the objects will be presented. During the test the interlocking limits where the SIS is triggered and the safety positions of the objects (valve closed, motor stopped etc.) will be marked.

5.1.2 **Modification management**

After the Configuration Acceptance Test (CAT) any modification shall not be allowed, without separate modification procedure. If SAT team has to make a modification during SAT, End-user will be notified. All modifications shall be consulted with End-user and modification team. SAT team leader will take care of all documenting updates.

5.2 **Overall safety validation**

The overall safety validation will be made, like FAT, separate from the normal DCS test. This phase is also often called Site Acceptance Test (SAT).

A test plan will be prepared. It will contain the object of the plan, the test organization, the requirements of the test, the documentation, the test equipment, the approval procedure of the tests and the instruction for the test report.

The interlocking limits of the pressure and temperature transmitters will be tested with the pressure and temperature calibration equipment so, that in the test situation the process conditions are similar to the normal process conditions. Note that the test equipment must have calibration certificates.

The valves and motors are in normal operation during the test, so that the safety function of the valves can be seen as a movement to the safety position. The motors will be tested so that the safety switches are opened and the safety function will be observed in the control contactor.

Test reports similar to those of FAT will be prepared. The SAT includes also the field equipment and the cabling will be tested.

5.3 Periodic test

During the normal operation and maintenance of the plant the SIS will be tested periodically according to the certificates of the safety logic and the field equipment. The periodic tests are similar to overall safety validation and in tests the similar test reports can be used. In the test the field loops (the sources and the objects) will be tested 100% every time but the safety logic can be tested randomly only partly. Periodic testing is implemented by the end-user.

For the periodic tests a test plan will be prepared. It will contain the object of the plan, the test organization, the requirements of the test, the documentation, the test equipment, the approval procedure of the tests and the instruction and distribution for the test report. As the periodic test will be made, for example, only every two years, the test plan must be so exact that the test organization can see what kind of arrangements have to be made before tests and how the tests will be made.

6 OPERATION AND MAINTENANCE

All normal maintenance works of the logic and field equipment (checking of the calibration, changing of the field device, changing of the card etc.) do not require a test or documentation according to safety standard IEC 61508. These works can be realised like the maintenance works for normal equipment.

All additions, modification of the cabling, cross connection and software in the loops that are connected to the SIS will need to be handled like the implementation of SRS. Thus, this kind of additions and modifications will be tested according to the test plans and appropriate test reports will be prepared. Functional Safety Manager's (FSM) permit is required to do the modifications in SIS and FSM also makes the decisions, which changes (replacing similar device) can be made without the authorities.

The following items will be handled in the operation and maintenance plan for SIS; the object of the plan, responsible people, documentations, training, specifications of the requirements, periodic tests and reports, maintenance and changing instructions, Log for SIS and service instructions. The suppliers of the SIS are responsible to develop together with the purchaser the operation and maintenance plan for SIS. The operation and maintenance plan is to be attached to the documentation for Safety Instrumented System (see Appendix III).

7 ORGANISATION AND RESPONSIBILITIES

7.1 Project

The people who participate in the engineering and implementation of the Safety Instrumented System have to have adequate competence with regard to the functional safety systems. The organization will be named in the project. The people who

participate in the engineering of the Safety Instrumented System can be for example as follows:

- The person from Purchaser is who represents end-user in the project. Person in charge is Mr. P P.
- The person from Designer, who represents main designer in the project. Person in charge is Mr. D D.
- The person from Supplier, who represents the designer and supplier of the Safety Related System. Person in charge is Mr Z Z.
- The person from Supplier, who represents the main equipment supplier and bearer of the operating permission during the project for the plants and the designer and the supplier of the field instrumentation and electrification for SRS. Person in charge is Mr. S S.
- The person from Supplier, who represents the main equipment supplier and bearer of the operating permission during the project for the department 1. Person in charge is Mr. S S.
- The person from Supplier, who represents the main equipment supplier and bearer of the operating permission during the project for the department 2. Person in charge is Mr S S.

7.2 Operation and maintenance organization

The mill organization for the operation and maintenance of the SIS after the project will be named later if not exist.

8 DOCUMENTATION

The separate documentation will be made for the Safety Instrumented System (SIS). The table of the contents for the documentation of SIS is presented in Appendix III.

The documentation of SIS need to be accurate, easy to understand and suit for purpose. Documentation shall be traceable and available all lifetime of SIS.

9 SUMMARY

With respect to the Safety Related System and Safety Instrumented System the standards IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety related systems) and IEC 61511 (Functional safety - Safety instrumented systems for the process industry sector) shall be followed. A summary that contains also safety evaluation and specification for the overall safety requirements is presented in the following page.

Safety lifecycle phase (Applied IEC 61508) *)		Partici- pants	Respon- sibility	Objectives	Documentation
1	Concept	SU	SU	To determine the process and the equipment	Clarification of the process and equipment
2	Overall scope definition	SU, PU, SSU	SU	To determine the scope of SIS	Clarification of the scope of systems included in SIS
3	Hazard and risk analysis	PU, SU, DE,	SU	To determine the hazards and hazardous events and their risk	Hazard and risk reports
4	Overall safety requirements	PU, SU, DE, SSU	SU	To determine the overall safety requirements, inc. their safety integrity levels (SILs)	Inspection reports Specification for the overall safety requirements
5	Overall safety requirements allocation	PU, SU, DE, SSU	SU	Determine the risk reduction necessary for each intolerable risk	Safety interlocking diagrams Functional descriptions
6	Overall design, implementation, operation and maintenance planning	PU, DE, SSU	SU	To develop a plan for design, validation, installation and implementation of the Safety Instrumented Systems (SIS)	Safety Plan Operation and maintenance plan within SU's scope of delivery.
7	Overall safety validation planning	PU, DE, SSU	SU	To develop a plan to facilitate the overall safety validation of the Safety Instrumented Systems	Validation plan (SIS)
8	Overall installation and commissioning planning	PU, DE, SSU	SU	To develop a plan for the installation and commissioning of Safety Instrumented Systems	Installation and commissioning plan within SU's scope of delivery.
9	E/E/PE safety requirement specification	PU, SU, DE, SSU	PU/DE	To define safety requirements to E/E/PE system in right terms to achieve required SIL	Specification of SIS requirements
10	Realisation: SIS	PU, SU, DE, SSU	SSU/SU	To realize Safety Instrumented Systems according to plans	Description of technical realisation (SSU). Loop drawings (SU). Program diagrams (SSU). Checking of the overall safety requirements (SU).
11	Overall installation and commissioning	PU, SU, SSU, AU	SSU	To install and commission Safety Instrumented Systems according to safety plan	Included in: Testing protocol SAT Validation report SAT
12	Overall safety validation	PU, SU, DE, AU SSU, AU	SU/SSU	To validate that the Safety Instrumented Systems meet the safety requirements	Testing protocol FAT (SSU) Validation report FAT (AU). Testing protocol SAT (SSU) Validation report SAT (AU)
13	Overall operation and maintenance validation	PU, SU, DE, SSU, AU	SU	To validate that operation and maintenance are going according to plan	Validation report. Note (5).

Safety lifecycle phase (Applied IEC 61508) *)		Partici- pants	Respon- sibility	Objectives	Documentation
14	Overall operation, maintenance and repair	PU	PU	To maintain safety	Log.
15	Overall modification and retrofit	PU	PU	Verification	Request Report (impact) Log
16	Decommissioning or disposal	PU	PU	Verification	Report (impact) Log

Explanations: PU = Purchaser, SU = Equipment supplier, SSU = Safety Instrumented System supplier, DE = Designer, IN = Insurance company, AU = Authorities, PED = Pressure Equipment Directive*) Numbering refers to the lifecycle presented in IEC 61508

Common rules and notes:

1. All documentation made by SU, AU, DE, SSU will be delivered to PU.
2. All safety lifecycle phases need to be verified.
3. Verification and inspection reports made by AU are included in SU's scope of delivery.
4. Requirements of local pressure equipment requirements have to be followed.
5. First inspection/periodic test have to be executed according the operation and maintenance plan before the acceptance of the process delivery.



Appendix I

**Mondi AG.
Mondi Standard Harmonization**

EXAMPLE OF HAZARD AND RISK ANALYSIS

1 OBJECTIVES

The objective of a hazard and risk analysis is to identify and indicate the hazardous events associated with the plant or its systems and equipment. Regarding the sources of danger, a target level will be determined for risk reduction, and the adequacy of the achieved risk reduction and preparedness for hazardous events will also be estimated.

2 DEFINITION OF THE SYSTEM TO BE ANALYSED

The systems and the functions to be analysed will be specified. The process areas and functions that will be excluded will also be specified. In addition, it will be agreed which functions should be examined during the analyses of other processes or by other specialists.

Example of the boundaries of the risk analysis:

The analysis has been limited to the internal functions and structures of the plant and includes the measures related to normal operation and maintenance.

The following will be left out from the analysis:

- All repairs and modifications (before they are carried out a separate study is needed, including analysis of hazards, preparation of instructions and work permit practice to be followed)
- External hazards and dangers beyond the control of the plant's operating personnel (e.g. exceptional natural forces or vandalism)

3 SELECTION OF ANALYSIS METHODS

A working group will be selected. The group should be sufficiently competent to carry out the hazard analysis and to identify hazardous events. The group should also be familiar with the methods used for risk analysis and have a thorough knowledge of the subject under consideration. The expertise of the working group should be specified and recorded.

The principles of implementation will be determined and the schedule will be agreed on.

The minimum documents and information required for the analysis will be defined to provide proper conditions for successful identification of hazards (plant layout drawings, PI drawings, process descriptions, etc.)

4 DESCRIPTION OF HAZARDOUS EVENTS

The working group will list system-specific potential sources of danger, reasons for danger and consequences. This should be done for each system separately using the attached form. First of all, potential personal injuries will be assessed, and if necessary, significant dangers and risks to the environment and property should be estimated. The identified hazardous events will be classified according to the description given in section 7.

5 RISK REDUCTION METHODS

Risk reduction methods shall be described by risk for other than the electrical safety related system.

Considering normal plant operations, attention should be paid to the exposure to hazardous situations and to the possibility for advance warning of hazardous situations, limiting the area and other methods that could be used to prevent a hazard to occur.

6 CLASSIFICATION METHOD

The calibration of the risk graph applicable to the system in question will be confirmed. The calibration shall be in accordance with generally approved conditions and apply to the entire plant. See for an example.

7 CLASSIFICATION OF DANGERS CAUSING PERSONAL INJURIES

Classification will be made at least for those identified risks that may cause serious personal injuries. The classification shall follow the scale based on the calibration agreed on in advance to produce comparable results. The hazard and risk analysis is done assuming that no SIS was fitted.

Risk is defined as a combination of the probability of occurrence of injury and the severity of it. Typically, in the process sector, risk is a function of the following four parameters:

- the consequence of the hazardous situation (**C**);
- the occupancy (probability that the exposed area is occupied) (**F**);
- the probability of avoiding the hazardous situation (**P**);
- the demand rate (number of times per year that the hazardous situation would occur in the absence of the SIS) (**W**).

The risk graph (figure 1) can be used to determine the risk-related safety integrity level (**SIL**), which equals the need for risk reduction.

Any significant risks and effects on the environment and property (E/P) affect the classification by increasing the demand for the safety integrity level. The cases of environmental damage in which the terms of the environmental permit are clearly exceeded as a result of damage shall be marked on the form. Regarding property damage, only the cases in which the value of the damage exceeds EUR 2 million are recorded. (It is assumed that the plant has a sufficient insurance policy to cover losses caused by the interruptions in operation.)

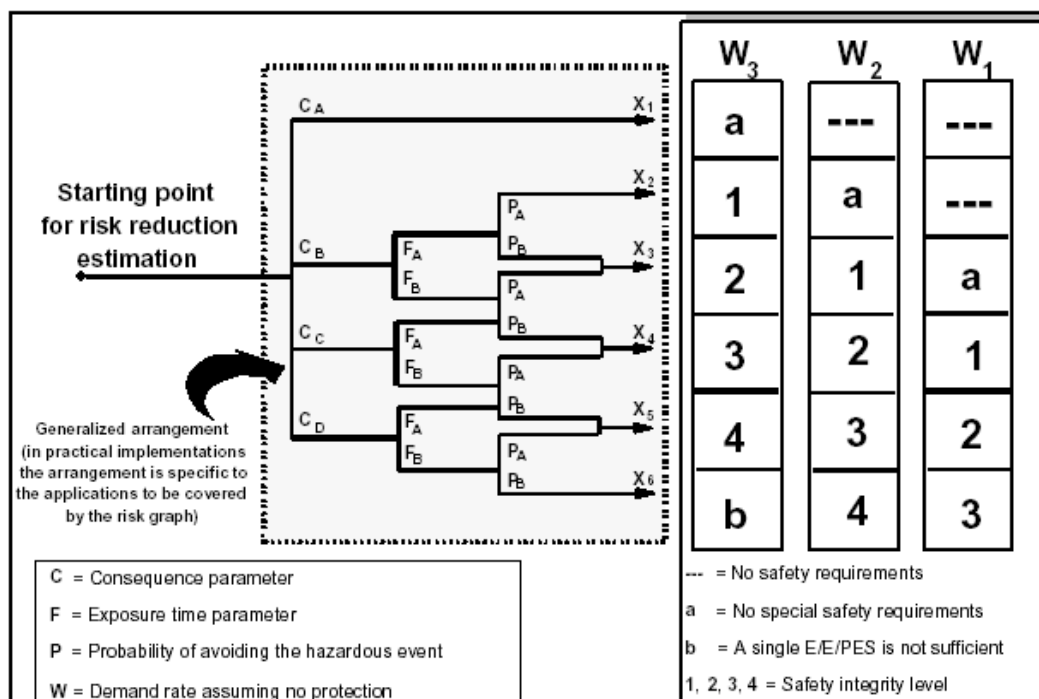


Figure 1 - Risk graph: general scheme (IEC 61511-3 annex D). Note. Values are to determine as shown in example tables Appendices I and II.

8 VERIFICATION OF RISK REDUCTION

The division of risk reduction into different Safety Instrumented Systems (SIS):

- External risk reduction methods (user's manuals, work permits, access control, etc.)
- SIS's of other technology (e.g. traditional safety valves, ...)
- Electrical SIS (E/E/PE)

9 VERIFICATION OF SUFFICIENCY OF RISK REDUCTION

The safety equipment supplier will verify that the safety equipment meets all the requirements set for this equipment (e.g. CE, PED).

The supplier of the electrical SIS will verify the total reliability of the SRS using probability calculation. The calculation must take into account the control system of the SIS, the configuration (1oo2, 2oo3 ...) of field circuits function by function and the field devices, as well as the wiring and cabling.

10 FURTHER PROCESSING AND RE-ASSESSMENT

Data in the areas that need further processing or reassessment of hazardous situations will be specified the Note column of Example.

For example:

The analysis cannot be completed unless required documents or sufficient expertise is available.

Further processing is needed, especially; in those cases where according to the classification a higher than expected safety integrity level is required ($SIL \geq 3$).

These cases must be added to the data of the process area to be analysed and their further processing must be ensured.

11

CHANGES IN RISK REDUCTION AND SUGGESTIONS FOR IMPROVEMENT

Any changes in the process and associated safety equipment shall be considered so as to avoid hazardous situations.

As soon as the changes have been made, the hazardous situations and related risk reduction must be reassessed.

[illegible]

Calibration of the General Purpose Risk Graph, Example

Risk parameter		Classification	Comments
Consequence (C)	C _A	Minor injuries of a person (Light injury to persons)	1 The classification system has been developed to deal with injury and death to people. (This classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or asset damage.) 2 For the interpretation of CA , CB, CC and CD, the consequences of the accident and normal healing shall be taken into account
	C _B	Serious / permanent injury to one or more persons; death to one person	
	C _C	Two persons die	
	C _D	Death to several persons) (Catastrophic effect, very many people killed)	
Occupancy (F) This is calculated by determining the length of time the area exposed to the hazard is occupied during a normal working period. NOTE - If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected. NOTE - It is only appropriate to use F _A where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up	F _A	Rare to more often exposure in the hazardous zone. Occupancy less than 10 %	3 See comment 1 above
	F _B	Frequent to permanent exposure in the hazardous zone	
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	P _A	Adopted if all conditions in column 4 are satisfied	4 P _A should only be selected if all the following are true: □□facilities are provided to alert the operator that the SIS has failed □□independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area □□the time between the operator being alerted and a hazardous event occurring exceeds 1 hour or is definitely sufficient for the necessary actions
	P _B	Adopted if all the conditions are not satisfied	
Demand rate (W) without safety instrumented function under consideration. To determine the demand rate it is necessary to consider all sources of failure that can lead to one hazardous event. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designed and maintained according to IEC 61511, is limited to below the performance ranges associated with SIL1.	W ₁	Demand rate less than 0,03 per year (<1/30a)	5 The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SRS 6 If the demand rate is very high (e.g., 10 per year) the SIL has to be determined by another method or the risk graph recalibrated. Then the operation mode is high demand or continuous (IEC 61511□1, Clause 3.1.48.2).
	W ₂	Demand rate between 0,3 and 0,03 per year	
	W ₃	Demand rate between 3 and 0,3 per year For demand rates higher than 3 per year higher integrity shall be needed	
Any significant risks and effects on the environment or property (E/P) affect the classification by increasing the demand for the safety integrity level.	E	In environmental damage the cases in which the terms of the environmental permit are clearly exceeded as a result of damage shall be marked on the form.	(It is assumed that the plant has a sufficient insurance policy to cover losses caused by the interruptions in operation.)
	P	Regarding property damage, only damage cases the value of which exceeds EUR 2 million are recorded.	
NOTE This is an example to illustrate the application of the principles for the design of risk graphs. Risk graphs for particular applications and particular hazards will need to be agreed with those involved, taking into account tolerable risk (see IEC 61511-3 Clauses D.1 to D.6.)			



Appendix II

**Mondi AG.
Mondi Standard Harmonization**

EXAMPLE OF SRS SPECIFICATION REQUIREMENTS

[illegible]



Appendix III

**Mondi AG.
Mondi Standard Harmonization**

SRS DOCUMENTATION

TABLE OF CONTENTS

A. SPECIFICATION

- 1 Implementation plan for safety instrumented system
- 2 Hazard and risk reports
- 3 SIL determination and Safety Requirement Specification
- 4 Inspection report (specification material)

B. ENGINEERING AND IMPLEMENTATION

- 1 Safety interlocking diagrams
- 2 Functional descriptions/diagrams electrical and instrument loops
- 3 Description of technical realisation
- 4 Safety integrity level calculations (checking of overall safety)
- 5 Cabinet and I/O lay-out drawings
- 6 Connection drawings
- 7 Application software programs (diagrams) and displays
- 8 Loop and wiring drawings
- 9 Certificates (SIL level)
- 10 Manuals for logic and field devices

C. SIS APPLICATION PROGRAMS

- 1 Logic diagrams
- 2 Programs
- 3 Displays

D. FACTORY ACCEPTANCE TEST

- 1 FAT Plan
- 2 FAT Instruction
- 3 FAT Protocol
- 4 FAT Report
- 5 Inspection report (Engineering and FAT)

E. IMPLEMENTATION AND VALIDATION

- 1 SAT Plan
- 2 SAT Instruction
- 3 SAT Protocol
- 4 SAT Report
- 5 Inspection report (Implementation and validation)

F. OPERATION AND MAINTENANCE

- 1 Operation and maintenance instructions
- 2 Periodic test Plan
- 3 Periodic test Instruction
- 4 Periodic test Protocol
- 5 Periodic test Report
- 6 Inspection report (Operation and maintenance)