# Process hazard and risk analysis
# *Guideline*

**Comments on this report are gratefully received by**
**Johan Hedberg**
**at SP Swedish National Testing and Research Institute**
**mailto:johan.hedberg@sp.se**

## Summary

This report will try to describe the different steps that must be taken as part of the risk analysis.

Following main activities are identified:

- Defining the process and its Basic Process Control System (at this point no Safety Instrumented Functions (SIF:s) should be visible)
- Perform a process hazard analysis to identify if any further actions must be taken to reduce the risk.
- Identify those hazardous situations where it is appropriate to use a SIF to reduce the risk

The selection of SIL level for each identified SIF is described in a separate document called ***Process hazard and risk analysis Risk graph matrix.***

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

## TABLE OF CONTENTS

# 1 Introduction

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

## *1.1 Purpose*

In order to fulfil the requirements in the standard IEC 61511 a hazard and risk assessment shall be performed. Most companies develop their own format of the hazard and risk assessment. This document provides one possible example on how a hazard and risk assessment could be structured.

One of the first aspects that must be considered in the beginning of a new project is to identify potential hazards that could occur and decide how to handle these by for instance implementing so called Safety Instrumented Functions (SIF:s). The aim with this document is to try to describe the requirements concerning risk analysis in the standard.

## *1.2 References*

[1] IEC 61511-1 Functional safety- Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements
[2] IEC 61511-2 Functional safety- Safety instrumented systems for the process industry sector- Part 2: Guidelines for the application of IEC 61511-1
[3] IEC 61511-3 Functional safety- Safety instrumented systems for the process industry sector- Part 3: Guidance for the determination of the required safety integrity level

## *1.3 Scope*

This document covers the parts in IEC 61511 concerning process hazard and risk analysis.

The hazard and risk analysis (1) and the allocation of safety functions to protective layers (2) is the first two blocks in the safety life cycle according to IEC 61511-1. See figure 1.

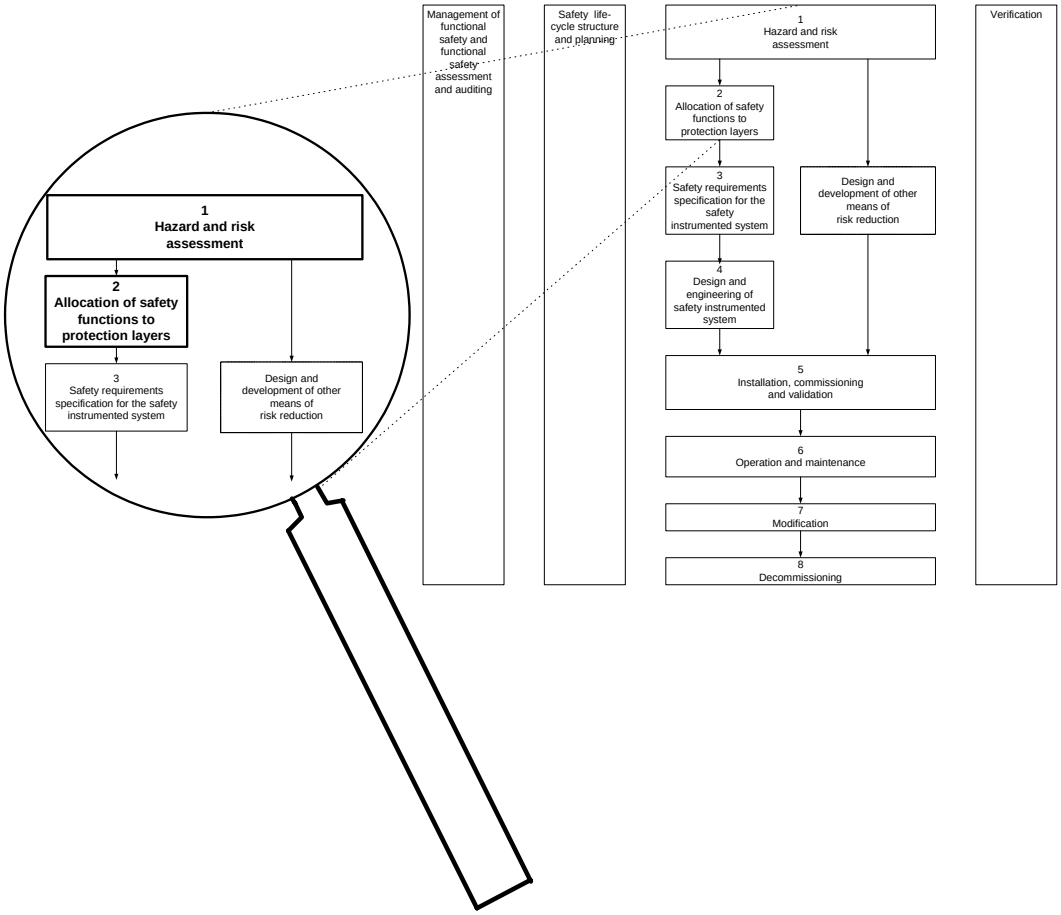



Figure 1. “Hazard and risk analysis” and “Allocation of safety functions to protection layers” life-cycle phases, IEC 61511-1:2003

## *1.4 Audience*

Persons involved in hazard and risk analysis.

# 2 Definitions and abbreviations

**basic process control system (BPCS)**
system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1 (3.2.3 in IEC 61511-1)

**fault**
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (3.2.21 in IEC 61511-1)

**failure**
termination of the ability of a functional unit to perform a required function (3.2.20 in IEC 61511-1)

**error**
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition (3.2.18 in IEC 61511-1)

**hazard**
potential source of harm (3.2.31 in IEC 61511-1)

**hazardous situation**
circumstance in which a person is exposed to hazard(s) (3.1.3 in IEC 61508-4)

**hazardous event**
hazardous situation which results in harm (3.1.4 in IEC 61508-4)

**harm**
physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment (3.2.30 in IEC 61511-1)

**instrument**
apparatus used in performing an action (typically found in instrumented systems) (3.2.38 in IEC 61511-1)
NOTE Instrumented systems in the process sector are typically composed of sensors (for example, pressure, flow, temperature transmitters), logic solvers or control systems (for example, programmable controllers, distributed control systems), and final elements (for example, control valves). In special cases, instrumented systems can be safety instrumented systems (see 3.2.72 in IEC 61511-1).

**process risk**
risk arising from the process conditions caused by abnormal events (including BPCS malfunction)
NOTE 1 The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety). (3.2.54 in IEC 61511-1)

**safety instrumented function (SIF)**
safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function (3.2.71 in IEC 61511-1)

# 3 Description of the basic process control system

Before the hazard and risk assessment should be started it is important that it exists an adequate description of the process and its associated basic process control system (BPCS). This description should not include any safety measures as the focus of the process hazard and risk analysis will be to determine whether these are necessary or not.

When a hazard and risk assessment should be performed on an existing process including the control system it may be difficult to decide out which parts that should be included in the description as many safety features are already included in the existing system.

It is always easier when a new process control system should be designed. In this case aspects of safety measures are not considered before the process hazard and risk assessment is started.

This conceptual description of the process and its associated BPCS will provide input to the hazard and risk assessment.

# 4 Process hazard and risk analysis

An example of a process hazard and risk analysis form is described in appendix 1 of this report. It is important to emphasize that this is only **one** example on how to structure the hazard and risk assessment and it is the responsibility of each individual company to perform the process hazard and risk analysis in an appropriate way. The aim with this form is to try to include aspects related to the risk analysis described in IEC 61511.

This chapter describes the aspects that are included in the process hazard analysis form. The headings used below are the same as you find on the form. The information provided is aimed to facilitate the use of the form.

**Phase:**
During the life cycle of the process plant it will pass through a number of different phases. Below follows examples of a number of different phases:

- start-up
- normal operation
- shutdown
- maintenance
- manual intervention
- loading
- process upset
- emergency shutdown

It is important that the process hazard analysis considers all phases of the process plant in order to be able to identify all hazardous events that could occur.

**No:**
This is only a consecutive number.

**Mode:**
Informs about in which mode the process is running for a certain life cycle phase. For instance in the phase called *normal operation* following modes could for instance exist:

- start-up
- normal running
- stop

For less complex systems it could be more efficient to remove the **Mode** column from the form and combine the **Mode** column with the **Phase** column.

**Hazard:**
In IEC 61511-1 *hazard* is defined as *potential source of harm*. Below follows some examples of hazards:

- Combustible substance
- Explosive substances
- Toxic fumes
- Substances kept at high pressure in a containment (for instance a tank)
- Objects or material with a high or low temperature
- Radiation from heat sources
- Ionising radiation source
- Energy release during decomposition of a substance

The hazards described above are examples on hazards and when a company performs a process hazard analysis it is important that all relevant hazards are considered.

One way to identify hazards could be to investigate which kind of hazardous events that have occurred earlier in the process plant.

**Hazardous events:**
In IEC 61511-1 *hazardous event* is defined as *hazardous situation which results in harm*. Each identified hazard could give a number of different hazardous events. For each identified hazardous event it should also be described which factors that did contribute to it

As an example the hazard *Combustible substance* could give the following hazardous events:

- Pool fire outside a tank, due to leakage, when an ignition source is present
- Flash fire inside a tank when an ignition source is present

Factors that could contribute to the leakage in the tank could for instance be:
Bad connection joint

- Gasket damage
- Tube damage
- Pipe damage

**Sequence of events leading to the hazardous event:**
A certain hazardous event could occur depending on many different sequences of events. It is important to go through all sequences that could give a certain hazardous event to find out which of these sequences that have got the highest frequencies. One commonly used technique to find out the frequency for each hazardous event is called LOPA (Layers Of Protection Analysis).

As an example the hazardous event *Eruption of a tank due to high pressure* could for instance be reach by the following sequences of events:

- Too high flow of liquid into the tank caused by a fully opened inlet valve
- Too low (reduced) discharge flow of liquid from the tank resulting from a constantly closed outlet valve
- Chemical reaction inside the tank leading to a rapid volume expansion and increased pressure

**Determination of requirements for risk reduction:**
This part of the process hazard and risk analysis form estimates the consequence and frequency of each identified hazardous event.

The estimation of consequences is split into the following five categories:
H=Health
E=Environment
I=Image
P=Property
L=Loss of production

All these aspects are important to consider in the estimation of consequences and of course will that above category with the highest consequence level give the overall requirement on risk reduction.

Each of these five consequence categories are divided into five different levels
1=Small
2=Slight
3=Large
4=Very large
5=”Disastrous”
**It is important to point out that it is the responsibility of each individual company to, by themselves, define more in detail each consequence level!**

Also the frequencies could be divided into five different levels:
1= Once in 1000 years
2= Once in 100-1000 years
3= Once in 10-100 years
4= Once in 1-10 years
5= More often than once a year
**This is only an example of how frequencies could be divided into different levels.**
**It is important to point out that it is the responsibility of each individual company to, by themselves, define more in detail each frequency level!**

The consequence- and frequency numbers are placed in a 5 by 5 matrix and depending on how this matrix is calibrated it will inform about when additional risk reduction is necessary or not.
**It is important to point out that it is the responsibility of each individual company to, by themselves, calibrate the matrix!**

**Safety measures required (Yes/No)?**
If the risk estimation has given that no additional safety measures are required it will not be necessary to fill in the rest of this form (the columns to the right of this one)

If the risk estimation has given that additional safety measures are required the complete form must be filled in.

To keep up the efficiency during the initial process hazard and risk analysis one possibility could be to only fill in the first part of this form and exclude the rest of the columns. These columns could be filled in at a later stage for those hazardous events where additional safety measures are required.

**Is it possible to reduce or remove the hazard?**
This column informs about the possibility to reduce or completely remove the hazard.

For some hazardous situations it may be possible to reduce or remove the hazard but in some situations it will not be possible because the hazard itself is part of the main process. As an example some kind of *Combustible substance* could be an important part in a process and in that case it will not be possible to remove thi hazard.

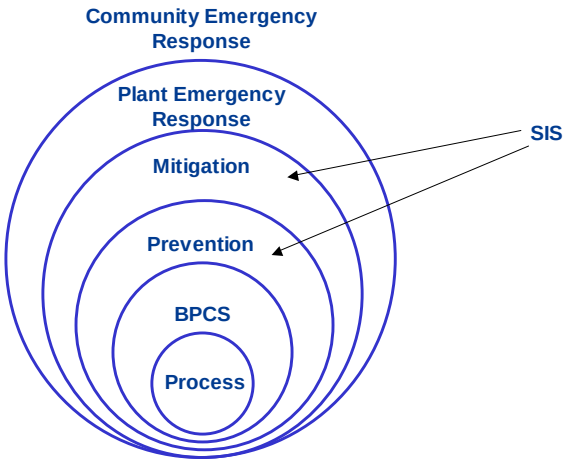
**Is it possible to interrupt the hazardous sequence?**
In some situations it could be possible to interrupt the hazardous sequence and in that way avoid that a hazardous event occurs.

**Safety function partly/completely realised by other technology or/and external risk reduction facilities:**
This column includes safety functions that are not based on electrical/electronic and programmable electronics. This could for instance be

**Safety instrumented function (SIF):**
In those cases where it is necessary to use a SIF this column gives a description of the SIF, in effect what is the aim with the safety instrumented function:

Examples on different SIF:s:
Opening of a safety valve when the temperature increases a certain level (prevention layer)
Opening of a safety valve when the pressure reaches a certain level (prevention layer)
Automatic start of a fire-extinguishing system when a fire is detected (mitigation layer)

Safety instrumented functions (SIF:s) are used in the mitigation layer and prevention layer as defined in IEC 61511-1.




**Comments:**
In this column it is possible to add additional information and comments.

# Appendix1 Process hazard and risk analysis form

## Process hazard and risk analysis form

**Phase:**

| No: | Mode: | Hazard: | Hazardous event: | Sequence of events leading to the hazardous event: | Detemination of requirements for risk reduction: | | | | | | Safety measures required (Yes/No)? | Is it possible to reduce or remove the hazard? | Is it possible to interrupt the hazardous sequence? | Safety function partly/ completely realised by other technology or/and external risk reduction facilities: | Safety instrumented function (SIF): | Comments: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Consequence | | | | | Freq. | | | | | | |
| | | | | | H | E | I | P | L | | | | | | | |
| 1 | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | |