SAFETY CRITICAL OPERATIONS AND ACCIDENT BARRIERS

By Øyvind Kaasa
Hydro Corporate Research Centre,
Porsgrunn, Norway

Inhibition of an ESD/PSD subsystem, a fire&gas system including release deluge systems, actuation of fire dampers or electrically operated emergency systems, and/or overriding a interlock/keylock system requires special attention. The reason being that the risk and consequences if a temporary safety barrier fails, will increase if any of these safety barriers are out of service. Operations that require inhibition/ overriding this category of safety systems can be called Safety Critical Operations - SAFCO, implying such an operation carries a high risk. A plan for a SAFCO must take into account that the inherent plant safety level. It means that the safety level must be maintained through the whole operation, including the safety level for temporary safety barriers that include human factors. Accident stastistics point to human factors as a major accident cause in the process industry. Because a SAFCO normally requires the use of temporary safety barriers (TSB), that are either semiautomatic or 100% manual, the risk for TSB failure increases. In order to improve the failure rate for TSB's that include human factors, it is recommended to perform an analysis. For this purpose a method similar to a Safe Job Analysis is proposed for use when performing a SAFCO.

Introduction

The design of a process plant incorporates a number of safety barriers. Most of them function automatically. Some categories like ESD/PSD and interlock/key lock systems protect against incidents, i.e. prevent events that may cause accidents. Another important category is fire and gas systems that function as mitigating safety barriers. The reliability for almost all types of single safety barriers is considered insufficient, hence a second safety barrier as a back-up barrier is required. It could be a twin barrier, or it could be designed to operate as a logically different system. Engineering practice, and industry standards require two event barriers in parallel to ensure acceptable risk.

Background

Hazardous and operational analysis (HAZOP) is the most common method for identifying preventive safety barriers. When overriding/ inhibiting a safety barrier, the inherent safety of the plant must not be jeopardized. Hence a temporary safety barrier (TSB) is required. Temporary safety barrier normally contains one or several human factors and the risk for barrier failure increases. Experience has shown that the safety performance of plant personnel depends on a number of factors that vary between individuals depending on experience, education, etc. Human factors like stress level, job satisfaction, etc. are among other factors that determine the reliability of TSB that include human factors.

The common use of TSB signifies a need for a Best Practice guideline that addresses human factors and the risk for safety barrier failure in a systematic way when planning safety critical operations (SAFCO).

Analysing temporary safety barriers

Safe job analysis (SJA) or similar as required by the safety procedures for the plant, should be used when analysing safety critical operations This is to ensure that overriding/inhibiting safety barriers due to workover, maintenance, repair etc., does not have any adverse effect on the inherent safety integrity of the plant. The method will ensure that a temporary safety barrier (TSB) that includes human factor during a SAFCO, have

an equivalent reliability compared to the permanent safety barrier that is currently being overridden/inhibited. The proposed method includes an evaluation of the potential consequences in case of accident.

Safety critical operations

General

A Norsk Hydro chemical process plant has been analysed with respect to Safety critical operations (SAFCO). The operations can be divided into three subcategories depending on the type of safety barrier that requires inhibition or overriding:

1 Operations that require inhibition of a PSD/ ESD function
2 Operations that require inhibition of a fire & gas signal
3 Operations that require overriding an interlock or keylock system

Appendix A contains a summary of the safety barriers and how barriers work as part of process safety systems.

ESD/PSD functions

General

Replacing an automatic ESD/PSD with a temporary safety Barrier (TSB) incorporates normally the use of human factors, f.ex radio communication, reading instruments manually, releasing shutdown system manually, etc. If the incoming alarm signal is inhibited, the CCR operator will be prepared to actuate the ESD/PSD system as if the alarm signal was not inhibited. If the outgoing ESD/PSD function signal has been inhibited, an operator has to perform the safety function using a local manual safety button in case of an emergency situation. The CCR operator could also reset the ESD/PSD function to obtain the same result.

Plant observations

After a quick review of current practice with respect to inhibiting ESD/PSD signals, there are some observations with respect to temporary safety barriers that deserve to be highlighted.

Background

- Operators receive up-to-date information for all inhibited PSD/ESD signals at the start of every new shift.
- All signals being inhibited are approved by shift leader
- All signals being inhibited are written into the journal for inhibited ESD/PSD signals
- Instrument tag has yellow colour at the CCR panel when inhibited.

Observations

- No specific procedures for defining a temporary accident barrier in case of inhibiting ESD/PSD-alarm signals.
- No specific system for evaluating risk for barrier failure, and consequences in case the temporary safety barrier fails.

Analysis of temporary safety barriers (TSB)

When starting an analysis of temporary safety barriers before inhibiting an ESD/PSD system, relevant documents included procedures should be available. The analysis should focus on:

- which part of the ESD/PSD system requires inhibiting
- which part of the TSB includes human factors
- risk for TSB failure
- consequences of TSB failure
- compensating efforts because of TSB
- description of back-up safety barrier in case TSB failure

Documents and procedures

When inhibiting a safety barrier because of a SAFCO, the following information should be available when performing an analysis:

- Safety shutdown diagram or similar
  Contains information about system and equipment shutdown logic.
- Process & Instrumentation Drawing (P&ID)
  Contains piping and instrument information.
- Hazop analysis
  Contains information about safety barriers.

Question list
In the process of reviewing safety barriers the signal loop and the corresponding process system connected to the PSD/ESD signal should be identified as well as temporary safety barrier and the human factors involved. For analysing purposes, PSD signals can be divided incoming PSD signals to CCR and actuating shutdown signals (outgoing PSD signals from CCR). ESD signals are treated for analysing purposes as outgoing signals from CCR only. The reason being that incoming signals to CCR that initiate a ESD signal would be either a F&G signal or a PSD signal.

Incoming PSD/ESD signals
When an alarm for any reason is inhibited, the following questions should be asked by the plant operator/technician that has requested inhibition of the PSD alarm. The answers should be discussed with the shift leader/assisting shift leader/CCR operator:

PSD/ESD situation:
- What type of alarm requires inhibiting? How is the alarm normally received in CCR?
- Is there another independent safety barrier in addition to the alarm being inhibited?
- Which PSD/ESD protection system is the alarm designed to activate normally?

Post-PSD/ESD situation with a TSB in place:
- How can the TSB be described?
- What is the estimated time delay for the TSB compared to an automatic alarm?
- What are the human factors/links required to make the TSB functioning?
- What can be done to minimize the human factors of the TSB?
- What can happen if the TSB fails? Worst case? Consequences to people, environment, equipment, production?

Inhibiting outgoing PSD/ESD signals
Analyses of a TSB that is meant to be a substitute for PSD/ESD function in case of emergency requires special attention because of the time element.

Questions to be asked before inhibiting
- How long time is available for checking out alarms?
- Who has the final say before the manual/semiautomatic TSB is actuated?
- How long time is required to actuate the TSB in case of emergency?

Post PSD/ESD situation with a TSB in place
- How can the TSB be described?
- What is the estimated time delay for the TSB compared to an automatic actuation of the ESD/PSD signal?
- What will it take to make the TSB functioning with acceptable reliability?
- What can be done to minimize the human factors included in the TSB?
- What can happen if the TSB fails? Worst case? Consequences to people, environment, production equipment, production output?

Resetting a safety barrier
There is always a risk that a TSB is not reset properly when a maintenance job, etc. is completed. Therefore the analysis should include some questions about resetting:
- When can the inhibiting status of the safety barrier be removed? Criteria?
- Human factors are involved?
- What are the risk for resetting the safety barrier incorrectly when the SAFCO is completed
- What can happen if the safety barrier is not reset correctly? Worst case? Consequences to people, environment, equipment, production?

Summary of analysis
- List the human factors that have the greatest risk for failure
- List compensating actions.

Fire & gas signals

General
In ref. /1/ an analysis of eight cases of "hot" work that has resulted in serious accidents, has been reported. The conclusion contains four lessons to be learned:

#1 Beware of fugitive or hidden fuels
#2 Filling a vessel with an inert gas does not mean that fuel or oxygen is absent
#3 Both fuel and Oxygen concentration can vary with time and position.
#4 Use multiple safeguards.

In this report lesson #4 - the use of multiple safeguards or safety barriers is analysed to ensure the reliability of barriers.

It is common to inhibit fire & gas detectors when performing "hot" work because of the potential for:

a) igniting flammable/explosive materials located in the vicinity of the work place, or
b) igniting gas that has been released by accident in the vicinity due to circumstances other than the "hot" work itself such as equipment failure or operational factors.

Typical precautions that are taken to prevent an event/incident:

- Sufficient distance to flammable material
- A flame proof division between the ignition source and the flammable material.
- A fire guard equipped with a gas detector. The duty of the fire guard is twofold: alarm CCR and applying a fire extinguishers and/or trigger the deluge system.

Plant observations

Some of the standard safety barriers at the plant require manual operation to function as intended in the design. Hence these systems are exposed to an increased risk for a system failure due to at least one human factor.

- In case of a fire the deluge system will normally be released manually from the CCR. It can also be started locally by the fire guard or an operator.
- When CCR receives a fire alarm, the CCR operator has to find the information about the location of the fire in a 10 pages long list hanging on the wall in the CCR. An option could be to have the location of the fire displayed directly on a plant overview in the CCR panel together with a corresponding identification code for the deluge system that will be released.
- Operation of fire dampers requires manual assistance. (Perhaps with the exception of some minor systems.)
- Plant view video cameras requires manual assistance to capture a view of a fire and gas emergency at a specific location
- Because emergency air to the CCR is not part of Honeywell control system, it has to be started manually.
- Environmental gas detectors give alarm only. Manual follow-up actions are required.

These observations should be analysed in order to understand how the human factor and the risk for failure can be reduced to a minimum.

Analysis of temporary safety barriers

When starting an analysis of temporary safety barriers before a fire and gas system will be inhibited, relevant documents including procedures are required. The analysis should focus on:

- which part of the F&G system that requires inhibiting
- which part of the temporary safety barrier that includes human factors
- risk for failure
- compensating efforts because of the use of human factors included in the TSB

Documents and procedures

In order to analyse a SAFCO that includes inhibiting a F&G signal due "hot" work or other type of operations, the following documentation contains important and relevant information:

- Procedures for performing "hot" work.
- Safety shutdown diagram or similar
  Contains information about system and equipment shutdown logic.
- Process & Instrumentation Drawing (P&ID)
  Contains piping and instrument information.
- Fire & gas matrix (FGM)
  FGM contains information about tags and F&G loops.

Question list
For analysing purposes, F&G signals can be divided into alarms (incoming signals to CCR) and release signals that actuates equipment shutdown and deluge systems (mitigating systems).

F&G incoming signals (alarms)
In the addition to the questions listed above for incoming PSD signals, the following questions should be asked in case of a gas leakage in the vicinity of "hot" work location:
- Which human factors/links are involved in limiting the danger for gas ignition?
- Is it likely that any of these human factors/links will fail in a worst case situation?
- What can be done to minimize the human factors?
- How long time will it take to remove the danger for gas ignition?

Actuating F&G protection systems:
- Can the alarm of the incident (smoke, gas release, open fire) be blocked or be missing due to human factors?
- Which situations can generate an alarm?
- What human factors/links are required to trigger the fire extinguishing system for a specific area and/or shutdown of equipment as required?
- What happens if any of these human factors/links fail in a worst case situation?
- Any actions required to minimize the human factor as part of the mitigating safety barriers?

Interlock systems or key locked valves
General
Interlock systems are designed to ensure operation of specific valves in a specified sequence to prevent hazardous process condition. Physical locking of valves in an open or closed position is another method with the same objective.

Case study - starting up a cracker
Before starting up a cracker, the cracker must be filled with Nitrogen. An interlock system is installed to ensure that the CCR operator can not open the valve for supplying fuel gas to the cracker if the N_2 pressure is not constant for a certain minimum time period. In some cases operational needs require overriding the fuel gas interlock system. According to procedures the following steps must be taken to ensure that the cracker contains no air before starting up:
1 Perform a SJA.
2 Measure manually the atmosphere in the cracker with two different ex-meters at several high and low positions. All ex.meters are calibrated once a week.
3 Override the Nitrogen concentration signal from the cracker
4 Open the fuel gas supply valve
5 Start burners according to procedures

Note that two different ex.meters are used because using only one could mean faulty measurements. To reset the Nitrogen pressure signal, general procedures for resetting interlock systems apply.

The interlock system at the plant has the same procedures with respect to overriding as the PSD/ESD system has for inhibition, i.e. the journal for inhibiting PSD/ESD that is kept in the CCR, contains also information about interlock systems that have been overridden. The procedures for key lock system describes a more decentralized system, and the key cabinet is not located in the CCR.

Analysis of temporary safety barriers
Hazardous process situations where the interlock/key lock system is out of service, require a TSB. In general similar analysis as proposed for F&G and PSD/ESD systems above, should be applied for interlock/key lock systems.

Documents and procedures
In order to analyse a SAFCO that requires overriding a interlock/key lock signal, the following documentation contains important and relevant information:
- Procedures for overriding an interlock/key lock system.
- Procedures for the actual operation that requires overriding a interlock/key lock system.

- Process & Instrumentation Drawing (P&ID)
  Contains piping and instrument information.
- Key lock/interlock matrix if available
  Contains information where these systems are located and how they function

Note that a number of operations requiring overriding a interlock/key lock system, do not have procedures, i.e. for this type of operations a SJA analysis should be required. Especially when it can be categorized as a safety critical operation (SAFCO)

Question list
Refer to question lists for PSD and F&G for an analysis that can adapted when analysing an interlock or a key lock system that has to be overridden.

References
/1/*Lessons learned from fires, flash fires, and explosions involving hot work*. R.A. Ogle and A.R. Carpenter, Process Safety Progress Vol.20, no 2, June 2001

Appendices

Appendix A

Definitions

Accident. A sudden, unintended work-related event that results in injury, and/or business interruption, and/or damage to property, the environment or a third party.
Near-miss. A sudden, unintended work-related event with no consequences that , under different circumstances, could have become an accident.
Incident is a collective term including accidents and near-misses.
Event is a collective term to describe a situation that develops into an incident

Process safety
Safety barriers (typical)
There are several barrier levels involved if a safety critical operation causes an incident such as a leakage of hydrocarbon due to high level in a tank. The fluid subsequently ignites and the accident escalates into a and explosion and a fire:

Before any leakage, these signals are initiated:

Level 1 Process alarm (high level alarm)
Level 2 Event barrier (high level shutdown) and tank is depressurized
Level 3 PSV opens
After both preventive safety barriers fail and tank starts leaking:
Level 4 Active Mitigating barrier
Level 5 Passive Mitigating barrier
Level 3 Personal protection equipment (pseudo barrier in a strict definition of barriers)

Process alarm
In a HAZOP analysis a process alarm is not considered a safety barrier. It is only a warning that tells CCR operator about an irregular process condition. It does not initiate any changes in the process conditions

Typical process alarms are: Pah/pal, tah/tal, lah/lal

Event barrier
Barriers preventing accidents from taking place, i.e. they will ensure that abnormal process situations are brought and kept under control automatically. Note that a preventing safety barrier consists of an incoming signal, a logic control unit and an outgoing signal that initiates some type of action.

Typical event barriers are:
PSD/ESD, PSV, interlock and key lock systems.

Personal protection equipment
Personal protection equipment is mentioned only to have a complete list

Typical personal protection equipment are:
Helmet, gloves, flameproof clothing, breathing apparatus, etc.

Active mitigating (consequence reducing) barriers
Active mitigating (consequence reducing) barriers are designed to bring an incident under control with minimum damage. It means saving personnel from accidents, reducing damage to the environment ,

third party and/or production equipment, and minimum production loss.

Typical examples are:
Fire & gas detectors, fire water, deluge, sprinklers, fire dampers, door shutters, shutdown switches for electrical equipment, etc.

Passive mitigating (consequence reducing) barriers
Passive mitigating (consequence reducing) barriers have the same purpose as active mitigating (consequence reducing) barriers, but they are not part of the PSD/ESD/F&G systems.

Typical passive mitigating (consequence reducing) barriers are:
Fire walls, escape routes, pipe insulation, fire seals in hazardous drain systems, etc.

Appendix B

Form being used for approval of the inhibition of ESD/PSD, Fire & Gas, or overriding key lock/interlock systems

1	Fabrikk	Anleggsdel/Forbruker	Tag/Kurs-nr.
2	Inngrep ❑ Overbroing ❑ Undertrykking av alarm ❑ Annet Beskrivelse: ❑ disable ❑ inhibit ❑ endret alarmgrense		
3	Begrunnelse		
4	Konsekvenser		
5	Iverksatte tiltak - alarmgrense endret fra/til ❑ SJA utført Antatt tidspunkt for fjerning av inngrep: Dato: Kl.		

6	Overbroing/Inngrep	Dato	Klokkeslett	Signatur	Skift eller avdeling
	Godkjent				
	Lagt inn				
	Avstengt mot prosess				
	Forlenget godkjenning til				
	Forlenget godkjenning til				
	Forlenget godkjenning til				
	Forlenget godkjenning til				

7	Beskrivelse/Dokumenthenvisning

8	Oppheving	Dato	Klokkeslett	Signatur
	Godkjent			
	Fjernet			
	Avstenging mot prosess fjernet			