Nijs Jan Duijm

Revision July 2012/
editorial corrections August 2013

Types of safety barriers

Within the (North Sea sector) offshore industry, the concept of “Safety Critical Elements” is used, which are defined according to [3]:

“"safety-critical elements" means such parts of an installation and such of its plant (including computer programmes), or any part thereof—
(a) the failure of which could cause or contribute substantially to; or
(b) a purpose of which is to prevent, or limit the effect of,
a major accident.”

With reference to this definition, the real “safety barriers” are covered by (b), while (a) refers to “primary-process systems”. Primary-process systems are the systems that are necessary to perform the primary process, i.e. to store (contain), transport, steer, control, etc., with the only aim to reach the business objective (a product or service). Failure of a (safety-critical) primary-process system is considered as a deviation, which will appear as an initial event in a safety-barrier diagram or bowtie. In this way, a primary-process system should not appear in a diagram as a barrier, but actually at the start (left-hand side) of the bowtie/diagram, as the initial deviation is the failure of (or threat to) the primary-process system. Realizing this, one should be careful about considering process containments (wall thickness) or basic process control system (BPCS) as barriers. This is quite in line with the considerations in LOPA ([4], chapter 6) about Independent Layers of Protection (IPL).

It should be understood that a (flawless) system can easily function without safety barriers, but not without the primary-process systems. These considerations may help to determine whether a system or action must be perceived as a safety barrier (defined as (b) above) or not.

The reason for distinguishing the safety barriers and safety critical primary process systems is that the primary process systems operate either continuously or very frequently (weekly, daily, ...) while interventions by safety barriers are rare (once a year or less). It is said that the primary process systems are running in "high demand" mode and safety barriers in “low-demand" mode. This has implications for an assessment of the probability of failure of the systems: primary process systems are "tested" every time they are used, and the human actions which are included in these systems are characterized by a high degree of routine. Safety-barrier reliability in contrast depends on the *planned tests* and *training based on imaginary and predictable events*.

The reason to pool safety barriers and safety critical primary process systems under a single designation (safety-critical elements) is that both are important for process safety, and the underlying tasks of management (safety management) to ensure that safety critical elements are in place and function are the

same namely that they must be maintained and that there is a need for procedures, training, sense of duty, good safety culture, etc.

"Level of Protection Analysis (LOPA)" ([4], Chapter 6) uses a similar separation between the primary process control (controlling to ensure that product meets product requirements) and measures that handle the process deviations that slip through the primary process control. LOPA attaches great importance to the subsequent barrier function being independent of the primary process systems and of each other - only then safety barriers can be perceived as "Independent Layers of Protection (IPL)."

For safety barriers it is also important that they are able to perform their barrier function. This means that they are able to perform the various phases of a defensive action. This defensive action consists of:

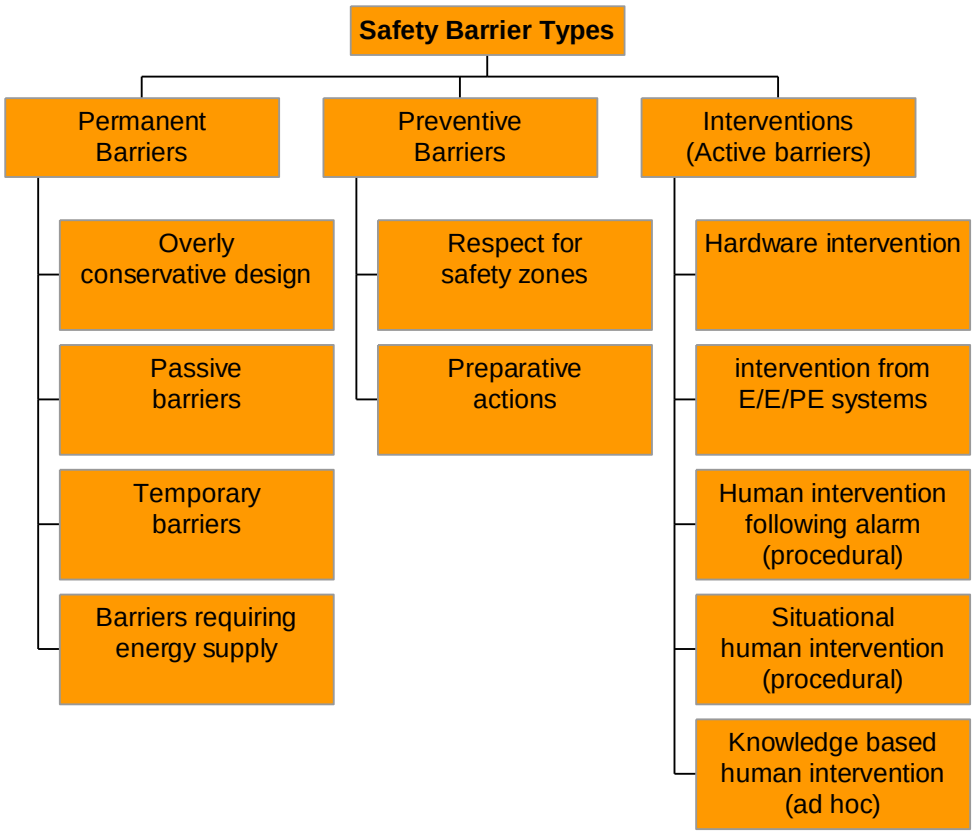
- to detect that there is a deviation
- to diagnose what the defensive action must be
- to perform the defensive action

(In LOPA this is called the "DDD" sequence: "Detect, Diagnose, Deflect")
A barrier is incomplete if one of these phases, especially to perform the action, is missing. An alarm is not a barrier if there is not an operator who performs the defensive action.

It is emphasized that it is the *actual response*, which constitutes the barrier. In the event of a human action is therefore the *action* itself, not the procedure describing the action ("paper is not a barrier"). But to define a desired action on a given situation by means of a procedure is the way safety managers can improve the likelihood that the desired action be performed when needed, i.e. the procedure (and the quality of the procedures), determine to a high degree the probability of success for a human response. To develop, maintain and train the procedure is an activity of *safety management*.

The following pages describe types of barriers. Safety barriers may be divided into three groups:

- Permanent barriers avert deviations or threats by means of their permanent physical presence, even before the deviation or the threat is materialized. Detection and diagnosis is thus not relevant for those.
- Preventive barriers include actions carried out independently of whether the deviation or threat is materialized. Detection and diagnosis is thus not relevant for those.
- Barriers conducting an intervention in the event of a deviation or threat. These barriers depend on a complete cycle of detection, diagnosis and action.



The safety-barrier types are described on the following pages in a uniform table format. The description includes a reference to safety management issues. The following safety-management issues are used, as defined in [1]:

- Risk analysis and selection of safety barriers
- Learning and management of change
- Manpower planning and availability
- Competence and suitability
- Commitment, compliance and conflict resolution
- Communication and coordination
- Procedures, rules, and goals
- Hard/software purchase, build, interface, install
- Hard/software inspection, maintenance, and replacement

The quality of the management issues that are marked red will affect the quality of the safety barrier (the likelihood that the barrier will be able to perform its barrier function as intended in case of a deviation). The management issues that are marked with a cross are considered to be of special importance. (These markings are derived from the ARAMIS project [1][2]).

For each barrier type a some examples and typical failure modes are included. Please note that the lists of failure modes are not exhaustive; failure modes depend on the individual barrier and the specific conditions, and failure mode identification should be performed systematically for each barrier.

References

[1] Guldenmund, Frank; Hale, Andrew; Goossens, Louis; Betten, Jeroen; Duijm, Nijs Jan, The development of an audit technique to assess the quality of safety barrier management, Journal of Hazardous Materials, Vol.130 Issue.3, 234-241, 2006, ISSN: 03043894, DOI: 10.1016/j.jhazmat.2005.07.011

[2] Duijm, Nijs Jan; Goossens, Louis; Quantifying the influence of safety management on the reliability of safety barriers, Journal of Hazardous Materials, Issue Vol.130 Issue.3, 284-292, 2006, ISSN 03043894, DOI 10.1016/j.jhazmat.2005.07.014

[3] The Offshore Installations and Wells (Design and Construction, etc.) Regulations 1996, Statutory Instrument 1996 No. 913, UK Government, ISBN 011054451X, TSO Customer Services, http://www.opsi.gov.uk/si/si1996/Uksi_19960913_en_1.htm#tcon (Regulation 26)

[4] CCPS/AIChE, Layer of Protection Analysis, Simplified Process Risk Assessment, AIChE, 2001, New York, ISBN 0-8169-0811-7

Title	**EXCESSIVELY CONSERVATIVE DESIGN AND MECHANICAL REDUNDANCY**
Detection	Not relevant
Diagnose	Not relevant
Action	Hardware: Resilience and redundancy withstanding physical forces
Description	"Excessively conservative" means that the relevant characteristics of equipment (e.g. wall thickness) are at least a factor two more than what would be required using state-of-the-art or traditional standards used for that process. Redundancy means that under normal conditions forces are transmitted through multiple independent paths and each path has the capacity to perform the desired function alone. Evaluation of redundancy must consider whether the redundant systems can be affected simultaneously by an accident or deviation (independence). Redundancy that requires an active shift to another system must be perceived as an intervention (i.e. an active barrier).
Examples	Over-dimensioned wall thickness, fitted with double steering cables or rods, fitted with double electrical connections.
Failure mechanisms	Material failure or installation errors, in particular following maintenance; slow degradation; process conditions that exceed even so the material strength, in particular following changes in process conditions; simultaneous (common cause) failure of redundant systems.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
X							X	

<table>
<tr><td>Title</td><td>PERMANENT PASSIVE BARRIER</td></tr>
<tr><td>Detection</td><td>Not relevant</td></tr>
<tr><td>Diagnose</td><td>Not relevant</td></tr>
<tr><td>Action</td><td>Hardware: Strength or capacity to handle the deviation or threat.</td></tr>
<tr><td>Description</td><td>Passive Barriers are elements in a system that are constantly present (i.e. they do not need to be activated), and that are installed with the only reason to avoid or limit hazardous situations (i.e. the installation can in principle operate without those barriers).</td></tr>
<tr><td>Examples</td><td>Tank bunds, dyke, fire protection, drainage sump, fence, lightning conductors, collision barrier, edge protection, hardware protection against body parts entering hazard zones.</td></tr>
<tr><td>Failure mechanisms</td><td>Lacking strength or capacity, construction error, slow degradation, human error causing flaws (e.g. open rain-water drains in tank bunds), removed (e.g. protection) or not installed or not re-installed after maintenance.</td></tr>
<tr><td>Relevant management factors</td><td>
<table>
<tr><td>Risk analysis and selection of safety barriers</td><td>Learning and management of change</td><td>Manpower planning and</td><td>Competence and suitability</td><td>Commitment, compliance and conflict resolution</td><td>Communication and coordination</td><td>Procedures, rules, and goals</td><td>Hard/software purchase, build, interface, install</td><td>Hard/software inspection, maintenance, and replacement</td></tr>
<tr><td></td><td>X</td><td></td><td></td><td></td><td></td><td></td><td>X</td><td></td></tr>
</table>
</td></tr>
</table>

Title	**PERMANENT BARRIER: ENERGIZED**
Detection	The effect does not depend on the detection of a deviation, but the barrier needs to be active or working.
Diagnose	Not relevant
Action	Hardware: capacity to perform the barrier function
Description	These barriers are constantly present, but need energy to work. If activation is required upon certain conditions, consider classification as temporary barrier.
Examples	Forced ventilation, active corrosion prevention, continuous circulation of material to avoid e.g. hot spots or separation, continuous inerting of systems, pilot flames, continuous addition of inhibitors.
Failure mechanisms	Not turned on/not activated, lacking capacity, lacking energy supply or material (gas) supply.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
	X				X		X	

Title	**TEMPORARY BARRIER (PASSIVE OR ENERGIZED)**
Detection	The effect does not depend on the detection of a deviation, but the barrier need to be present or working.
Diagnose	Not relevant
Action	Hardware: Strength or capacity to handle the deviation or threat.
Description	Barriers temporary put in place or temporary used, depending on a temporary situation (such as maintenance or repair works) or within a specific time spans or locations. Installation and use depends to a high degree on routines, procedures and rules.
Examples	Barriers around repair work, blind flanges over open pipes, spades in pipes, inhibitors in substances, personal protection equipment (PPE: e.g. hard hats, safety goggles, safety clothing, safety gloves), clothes and shoes to avoid static electricity, fixed safety belt (as in a plane), earthing of tanks during (un)loading, mechanical lock-out systems
Failure mechanisms	Not put in place, not donned (PPE), not appropriate for the hazard (chemicals, heat, pressure), wrongly mounted.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
		X				X		X

Title	**RESPECT SAFETY ZONES AND WARNINGS**
Detection	Detection relates to warnings and signs, not to detection of deviations (passive barrier as regards to deviations).
Diagnose	Not relevant
Action	Behaviour: To respect markings and warning signs: refrain from entering danger zones and refrain from manipulating marked parts of installations.
Description	Symbols, markings and warning signs (passive, i.e. not alarms) request to perform or refrain from certain behaviour. Implies in general refraining from certain actions (not touching, not operating, not entering, not smoking). Respecting danger zones prevents people from getting hurt when deviations occur (mitigating barrier). Awareness of valves closing off dangerous substances may prevent erroneous operation. Note that the barrier consists of the behaviour itself, not the signalling. Note that marking components such as valves in order to support correct operation is part of a management obligation to provide a sufficiently good human-machine interface and work place rather than a safety barrier.
Examples	Not entering danger zones (e.g. at cranes or robot stations, open containers, rotating machinery) , refrain from operating valves, avoid contact with hot parts, respecting smoking prohibitions, obeying speed limits.
Failure mechanisms	Not respecting signs and markings, lacking signs, unclear signs, and conflicts with work tasks.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
X				X		X		

Title	**PREVENTIVE PROCEDURAL ACTION**
Detection	Detection concerns attention to situations where the preventive action is required according to procedure, the deviation or threat is not detected.
Diagnose	Not relevant
Action	Behaviour or hardware: To follow rules and procedures which apply to the situation at hand or (activate) automated sequencing through steps in a process.
Description	The activity is performed as part of a procedure for some operation or step in a process in order to prevent dangerous situations, even when the dangerous situation not necessarily is present. There may be overlap with "Temporary barrier" (e.g. making a ground connection and leaving it in place during the (un)loading), but this barrier type focuses on actions performed prior to the hazardous activity, i.e. detached in time.
Examples	Venting of closed spaces before entering, venting/emptying hoses before detachment, earthing tankers before (un)loading to prevent static electricity, inerting vessels or reactors before taking into use.
Failure mechanisms	Not executing the action, incomplete or faulty execution.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
X				X		X		

Title	**HARDWARE INTERVENTION**
Detection	Hardware
Diagnose	Hardware
Action	Hardware
Description	Barriers that by means of direct mechanical-physical principles both detect the deviation and perform the necessary action.
Examples	Pressure relief valves, bursting disks, sprinkler heads, explosion relief hatches, blocking mechanism in modern safety belts in cars
Failure mechanisms	Insufficient capacity (too small, too slow), wrong set point, blocked (including piping towards the barrier), stuck or other mechanical defects.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
X								X

Title	**AUTOMATED INTERVENTION/SAFETY INSTRUMENTED SYSTEM (SIS)**
Detection	Hardware
Diagnose	Hardware/software
Action	Hardware
Description	Automated intervention by a system of electrical/electronic/programmable electronic (E/E/EP) components, that on the basis of input from sensors is able to determine what intervention needs to be made, and activates actuators (like powered valves) to perform this intervention. In order for an automated system to be considered to be an independent safety barrier (independent protection layer) the components that make up the automated system should not be part of the basic process control system (BPCS).
Examples	Emergency shutdown system (ESD), emergency blowdown system, airbag in a car.
Failure mechanisms	Component failure (sensors, electronic circuits and actuators), software failure, design failure, common cause failure
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
X								X

Title	**HUMAN INTERVENTION FOLLOWING ALARM**
Detection	Hardware/software
Diagnose	Behaviour according to clear procedures (”Skill & Rule based”)
Action	Behaviour according to clear procedures (”Skill & Rule based”) (may include activation of powered components)
Description	Actions of operators in response to clear instrument signals or alarms. There will be clear instructions describing the actions that are required to respond to the each of the alarms. The sensors, transmitters and actuators are part of the barrier system. In order for the alarm system to be considered to be an independent safety barrier (independent protection layer) the components that make up the alarm system should not be part of the basic process control system (BPCS).
Examples	Manual shutdown or adjustment, evacuation, calling fire brigade on alarm, close/open (correct) valve
Failure mechanisms	Failure of sensors, transmitters or software, flaws in instructions, wrong intervention, operator not present.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
	X	X		X			X	

Title	**SITUATIONAL HUMAN INTERVENTION (PROCEDURAL)**
Detection	Human observation and interpretation
Diagnose	Behaviour according to clear procedures (”Skill & Rule based”)
Action	Behaviour according to clear procedures (”Skill & Rule based”)
Description	The hazardous situation is detected by human observation of (a combination) factors in accordance with clear rules and procedures. There are no clear alarms, the hazardous situation needs to be derived from a combination of inputs. Instrument failure can both be considered to be a part of the initiating deviation (a dangerous failure in the sense that a deviation does not show up) or as part of the barrier failure. This barrier also includes actions of supervisors supervising other operator’s tasks.
Examples	To adjust hardware set-points, to warn others for action or evacuation, to disconnect tanks, hoses or pipes, to avoid escalation protection equipment with foam or fire-fighting water.
Failure mechanisms	Failure of instruments or software, flaws in instruction, lack of attention, wrong intervention.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
X			X	X		X		

Title	**KNOWLEDGE-BASED HUMAN INTERVENTION (AD HOC)**
Detection	Human observation and interpretation.
Diagnose	Behaviour on the basis of knowledge and reasoning (”Knowledge based”)
Action	Behaviour
Description	Intervention that requires a continuous knowledge-based assessment of the situation (e.g. during a rescue operation) and/or requires detailed analysis in cases where no procedures or rules apply. *This barrier type is provided for sake of completeness. Apart from use as a mitigating barrier (emergency response) at the far right-hand side of the diagram or bow-tie, prevention of foreseeable conditions should be dealt with by premeditated actions, supported by procedures, i.e. “Rule and Skill-based” barriers.*
Examples	Fire-fighting, emergency response, to (re)gain control over a complex system (such as a nuclear reactor) and bring it to a safe condition.
Failure mechanisms	Wrong assessment and diagnosis, inadequate intervention, intervention too late, too early.
Relevant management factors	

Risk analysis and selection of safety barriers	Learning and management of change	Manpower planning and availability	Competence and suitability	Commitment, compliance and conflict resolution	Communication and coordination	Procedures, rules, and goals	Hard/software purchase, build, interface, install	Hard/software inspection, maintenance, and replacement
		X	X		X			