|  |  |
| --- | --- |
| cetlogo ***CHEMICAL ENGINEERING TRANSACTIONS***  ***VOL. xxx, 2025*** | A publication of  aidiclogo_grande |
| The Italian Association  of Chemical Engineering  Online at www.cetjournal.it |
| Guest Editors: Bruno Fabiano, Valerio Cozzani  Copyright © 2025, AIDIC Servizi S.r.l. **ISBN** 979-12-81206-xx-y; **ISSN** 2283-9216 | |

Human Error Probability in Responding to safety Alarms

Els Janssensa,\*, Dirk Roosendansb, Olivier Iddirb

aTotalEnergies SA, Anspachlaan 1, 1000 Brussels, Belgium

bTotalEnergies SA, 24 Cours Michelet, 92069 Paris La Défense, France

\*els.janssens@totalenergies.com

The human role is key to process safety and the control of risks, necessitating the inclusion and quantification of human actions as part of safety barriers. Incorporation of human action as a barrier component in risk analysis studies is recognized as an important, though often challenging aspect of the analysis. The non-consideration of human actions and interventions as safety barriers is a very conservative approach and could lead to unjustified expenditures to reduce risks by implementing additional hardware barriers or require more stringent performance levels on other barriers.

Existing methods for assessment of human error probability are, or very coarse (use of generic literature data, addressing only part of the human response loop), or very complex (for example SPAR-H, Petro HRA). A more pragmatic method for estimating the reliability of human response, addressing all components of the human response loop and their performance shaping factors, has therefore been developed. This method, called HEPIRA (Human Error Probability in Responding to safety Alarms), is a procedure for quantitative evaluation of the human error probability by operators in responding to critical process and fire & gas alarms, that intervene in the prevention or mitigation of a major accident scenario.

In HEPIRA, a qualitative review of 26 conditions allows to evaluate the performance of the measurement or detection system, the alarm visualization and observation and the effectiveness of event diagnostics, decision-making, as well as the execution of the required corrective action to stop the scenario from developing. These conditions have a varying level of criticality and their relevancy to the scenario depends on the complexity of the event and of the required corrective action. The application of the procedure results in a Probability of Failure on Demand ranging from 1 to 10-2.

* 1. Introduction

In industrial risk analysis studies, a safety barrier is a control measure or a grouping of control elements that on its own can prevent an initiating event developing into a loss of containment (prevention barrier) or can mitigate the consequences of an unwanted release of a hazardous substance or energy (protective barrier). A robust barrier must be amongst others effective, independent, and auditable. For safety instrumented barriers, it has been common practice in industry over the past decades to estimate the probability of failure as required by IEC 61511. For the barrier equipment, this probability mainly depends on the intrinsic reliability of the equipment (failure rate) and the functional test interval.

Including human actions as a possible safety barrier component is acknowledged as crucial, though it remains less standardized and often challenging. The role of humans in possible initiating events or within human-dependent protection layers is significant across process industries, and even more so during non-routine operations. Ignoring human actions and interventions as possible safety barriers is a highly conservative approach, potentially leading to unnecessary costs for additional hardware barriers or demanding higher performance levels from other barriers.

When focusing on process safety alarms requiring human intervention as a safety barrier, its composition can be described from a functional safety point of view, as presented in figure 1. A process deviation outside the normal operating window will activate an alarm in the process control room. This alarm indication can be visualized on the Human-Machine Interface for observation and consideration by a control room operator. This person, potentially assisted by multiple persons in the chain of command, needs to interpret and diagnose correctly the situation in the field to be able to decide and perform an effective corrective action to bring the installation back into a safe state (preventive barrier) or to mitigate the potential consequences following a loss of containment (protective barrier). The corrective action can have varying complexity, ranging from the activation of an instrumented function (e.g. pushing an Emergency Shutdown button) up to a more complex intervention in the field relying on multiple human and technical resources.

The effectiveness of human performance in responding to safety alarms may be affected by numerous organizational and personal factors but also by the environment in which humans are operating. According to Myers (2011), the human response loop should include the following items for human response to be effective:

* Written procedures specifying the required actions by operators in response to safety alarms.
* Clear communication that the task/action must be performed.
* The means to detect a problem (inputs), with clear indication, even in emergency situations, and simple to understand.
* The physical means of interaction with the process (e.g. a manual valve) under all reasonably expected conditions to prevent or alter undesirable consequences and defining what is to be done given the inputs.
* Regular training on how to perform the task (including documented drills/tests to guarantee that all intervening operators are capable).
* The provision and maintenance of needed resources (materials, tools, appropriate personal protective equipment) to execute the task.
* Sufficient time to observe the condition or alarm, to diagnose the problem and to analyze what should be done, and to correctly perform the task.
* The ability to verify whether the action/task was performed correctly.

A diagram of a diagram

Description automatically generated

*Figure 1: Structure of a safety barrier composed of process safety alarm(s) and human actions*

* 1. Literature Review

A literature study was conducted to find existing Human Reliability Analysis methods that can be used during Process Hazard Analysis for a founded estimation of the reliability of the human response loop.

Several methods in literature suggest the use of generic values for quantifying human error probability in responding to safety alarms. As illustrated in tables 1 and 2, probabilities of failure on demand reported in literature vary from 10-2 to 1. These data however do not reflect the specific circumstances in which humans have to operate and are usually limited to the ability to perform correct diagnostics of a situation and take the right decisions accordingly. They only cover a part of the alarm response loop shown in figure 1. Important aspects such as the quality of the measurement system, the quality of alarm visualization and observation, and the nature of required corrective actions, all affecting the effectiveness of human response, are usually not addressed.

Table 1: Simplified technique for estimating operator response (Marzal E., Sharpf E., 2001)

|  |  |
| --- | --- |
| Event description | PFD |
| Normal operator response  For an operator to respond normally to a dangerous situation, the following criteria should be true:   * There exist ample indications that there is a condition requiring a shutdown * The operator has been trained in proper response * The operator has ample time (W> 20 minutes) to perform the shutdown   The operator is always monitoring the process (relieved for breaks). | 0.1 |
| Drilled response  All the conditions for a normal operator intervention are satisfied, and a “drilled response” program is in place at the facility. Drilled response exists when written procedures, which are exactly followed, are drilled or repeatedly trained by the operations staff. The drilled set of shutdowns forms a small fraction of all alarms when response is so highly practiced that its implementation is automatic. This condition is rarely achieved in most process plants. | 0.01 |
| Response unlikely  All conditions for a normal response intervention probability have not been satisfied. | 1.0 |

Table 2: Probabilities of Failure on Demand for human actions or response (CCPS, 2007)

|  |  |  |
| --- | --- | --- |
| Time available after alarm (or initial observation) | Conditions  (assuming adequate documentation, training and testing   procedures) | PFD |
| Any response time | The operator action is complicated, e.g. large number of alarms generated by initiating cause or the required response is not documented in a written procedure, or the operator is not trained on the written procedure. | 1.0 |
| < 10 min | The operator must troubleshoot to determine what the appropriate response is. | 1.0 |
| 2 - 10 min | The response is drilled and practiced (also known as a “never deviate response). If the alarm is received, the operator must execute the safe state action without delay. The alarm is independent of the BPCS. | 10-1 |
| ≥ 10 min | The operator response does not require troubleshooting or investigation prior to action. The alarm may be implemented in the BPCS or be independent of the BPCS[3] | 10-1 |
| ≥ 40 min | The operator response requires minor troubleshooting or investigation prior to action. The alarm may be implemented in the BPCS or be independent of the BPCS[3] | 10-1 |
| 24 hrs | Multiple operators can take action. Alarm should be automatically repeated at an interval necessary to ensure that each shift is notified of the process condition. Minor troubleshooting may be performed prior to action. The alarm is independent of the BPCS. | 10-2 |

An advanced method is the SPAR-H Human Reliability Analysis method (Gertman, 2005), developed by the U.S. Nuclear Regulatory Commission. This method allows to estimate the human error probabilities associated with operator and crew actions and decisions in response to initiating events at commercial U.S. nuclear power plants. The method decomposes HEPs into diagnose and action failures. It accounts for the context associated with human failure events (HFEs) by using performance-shaping factors (PSFs) and dependency assignment to adjust a base-case HEP using a beta distribution for uncertainty analysis.

The Petro-HRA method (Institute for Energy Technology, 2017) has been derived from the SPAR-H method, adjusting it to post-initiating events in the petroleum industry. Nonetheless, its application also requires a high level of expertise in the assessment of performance shaping factors.

As a conclusion, the existing methods for assessment of human error probability are or very coarse (use of generic literature data, addressing only part of the human response loop) or very complex (for example SPAR-H, Petro HRA).

* 1. Pragmatic Method for Human Safety Barrier Reliability Estimation

To be easily deployed in risk analysis, a pragmatic method addressing all components of the human response loop is needed for assessment of human error probability. For this purpose, HEPIRA was developed in TotalEnergies. HEPIRA is a procedure for quantitative evaluation of the human error probability by operators in responding to process and fire & gas alarms, as part of a safety barrier. The procedure was not designed to address other situations in which human response plays an important role (e.g. errors during maintenance activities or execution of normal operating procedures). HEPIRA encompasses all aspects of the human response loop, as illustrated in Figure 1.

A diagram of a process flow

Description automatically generated

*Figure 2: Scope of the HEPIRA evaluation method, represented on a scenario bowtie*

HEPIRA covers as well preventive process safety alarms, as fire & gas alarms intervening as a protective barrier after the loss of containment has occurred (see figure 2). The procedure is composed of a checklist of 26 conditions (see table 5) covering the 5 components of a human response loop, namely:

1. the quality of the measurement system,
2. the quality of the alarm visualization and observation (HMI),
3. the effectiveness of event diagnostics,
4. the effectiveness of decision-making,
5. the effectiveness of corrective action.

A mapping was conducted of the 26 conditions with the factors included in the Petro-HRA method. All the factors included in the Petro-HRA method, as well as in (Myers, 2011) are covered by 1 or more of the 26 said conditions. Depending on the complexity of the situation that triggers the alarm and depending on whether the corrective action is carried out from the control room or must be executed in the field, the method makes a distinction in 4 case types, illustrated in table 3. Each case corresponds to a subset of the 26 conditions. For certain cases, some conditions are not relevant. A criticality level was also attributed to each of the 26 conditions, using the definitions in table 4 below.

Table 3: Cases in HEPIRA

|  |  |  |
| --- | --- | --- |
| Case number | Event triggering the alarm | Action in the field |
| 1 | Simple and easy to understand  (situation that doesn’t involve multiple alarms and/or troubleshooting and does not cause a high-stress situation) | Not required |
| 2 | Required |
| 3 | Not easy to understand  (involving multiple alarms and/or requiring troubleshooting and causing a high-stress situation) | Not required |
| 4 | Required |

Table 4: Criticality levels of HEPIRA conditions

Increasing error probability

|  |  |
| --- | --- |
| Criticality | Description |
| Critical (C) | This condition is a must. When a critical condition is not complied with, no credit can be given for human response to the alarm. |
| Major (M) | This condition has a major impact on the effectiveness of human response. |
| Important (I) | This condition has a high impact on the effectiveness of human response. |
| Significant (S) | This condition might affect the effectiveness of human response significantly. |

Table 5 summarizes the 26 conditions of the HEPIRA method for qualitative review of the reliability of the human response loop, including the relevancy of the conditions for each of the 4 case types and their criticality.

Table 5: HEPIRA’s conditions for reliability evaluation of the Human Response loop with indication of case applicability and criticality

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Condition | **Case number à** | **1** | **2** | **3** | **4** |
| 1.1 | The alarm system (sensors) is robust and independent from the BPCS? | S | S | S | S |
| 1.2 | The alarm system is integrated in the BPCS but the initiating event is linked to a different controller on BPCS and the alarm system is independent of other protection layers to manage the event? | C | C | C | C |
| 1.3 | A quality HAZOP study is available including the evaluation of adequacy & appropriate location of sensors/alarms? | C | C | C | C |
| 1.4 | There is a high quality and formalized Management of Change process covering changes in instrumentation (hardware, settings)? | I | I | I | I |
| 1.5 | The measurement system is reliable (not exposed to frequent false alarms) and aligned with operational goals (fit for purpose)? | I | I | I | I |
| 1.6 | There is a dedicated program for testing and maintenance of critical alarms? | M | M | M | M |
| 2.1 | The alarm system and control room layout are adequately and ergonomically designed using good industry practices? | S | S | S | S |
| 2.2 | Operators are periodically (re)trained in understanding and working with the alarm system? | M | M | M | M |
| 2.3 | There is a high-quality process for managing bypassing of alarms and for management of modifications pertaining to the alarm visualization (hardware, settings)? | M | M | M | M |
| 2.4 | Qualified operators are continuously present in the control room? | C | C | C | C |
| 2.5 | The configuration of the alarm system (noise, light, vibration level) and the organization of the alarm management (fatigue, distraction) allows for rapid observation of this alarm? | M | M | M | M |
| 3.1 | Operators have extensive knowledge of the process and are trained individually and collectively to react adequately to this process deviation? | M | M | M | M |
| 3.2 | If the event is triggered by error of an operator, the diagnostics following the alarm are performed by a different operator? | NR | NR | C | C |
| 3.3 | If the event is triggered by error of an operator and the diagnostics need to be performed by the same operator, will he be able to correctly interpret, diagnose and recover the situation? | C | C | NR | NR |
| 3.4 | There is an Alarm Management/Prioritization System or a decision aid system to treat complex situations and to guide operators? | NR | NR | M | M |
| 3.5 | Operators are trained in using the Alarm Management System? | NR | NR | M | M |
| 3.6 | The physical environment allows rapid diagnostics (fatigue, noise, light, vibration, distraction)? | M | M | M | M |
| 4.1 | The chain of command is well defined, communicated and understood? | I | I | I | I |
| 4.2 | The physical environment allows rapid decision-making (fatigue, noise, light, vibration, distraction…)? | I | I | I | I |
| 4.3 | There is time and the possibility to discuss the situation with other operators/supervisors/managers to take appropriate action? | NR | NR | M | M |
| 5.1 | The Process Safety Time is fully defined and understood and is at least twice the time needed for effective intervention and longer than 2 minutes? | C | C | C | C |
| 5.2 | The Process Safety Time is very long (hours)? | S | S | S | S |
| 5.3 | There is sufficient time to discuss the intervention strategy with others? | NR | I | NR | I |
| 5.4 | There are sufficient resources (people, systems) to manage the situation in the field? | NR | C | NR | C |
| 5.5 | There is a dedicated program for testing and maintenance of systems (access, intervention) needed to manage the situation in the field? | NR | I | NR | I |
| 5.6 | The corrective action or the conditions under which these actions need to be performed are: simple, moderately complicated or complex? | NR | S | NR | S |

As a function of the criticality of these 26 conditions, a quantitative evaluation of the probability of failure on demand for a safety barrier consisting of an alarm and the corresponding human response loop can be made.

The rule set for the attribution of the PFD, is simplified in the event tree in figure 3. The detailed decision tree considering every of the 26 conditions to yield an appropriate PFD is not reproduced in this paper. The HEPIRA method will result in one of the following discrete PFD values: 1, 0.33, 0.1, 0.03, 0.01. It should be noted that the value of 0.01 is highly constrained and requires, amongst other things, independence between the alarm system and the BPCS.

A green rectangular object with a white background

Description automatically generatedA diagram with blue lines

Description automatically generated

Conditions

1.1 to 1.6

Conditions

4.1 to 4.3

Conditions

5.1 to 5.6

Conditions

3.1 to 3.6

Conditions

2.1 to 2.5

*Figure 3: Event tree for assessment of human performance in responding to safety alarms*

* 1. Conclusions

A pragmatic approach was developed in TotalEnergies for evaluation of the reliability of the response of operators in control rooms responding to process alarms. This method (called HEPIRA) holds the middle between methods encountered in literature that are, or oversimplified (e.g. use of generic data), or too complex to be used by non-experts in human error probability assessment.

An important benefit of the HEPIRA method lies in raising the awareness of operationals on the influence of performance shaping factors as for example process safety time, human-machine interfacing and clarity of safety critical operating procedures on the reliability of human response loops. It enables the identification of opportunities to reduce operator error and the harmonization of human safety barrier reliability assessment in parallel with the fundamental concepts of functional safety. The outcome of HEPIRA was benchmarked against existing methods (INERIS - Omega 20, 2009) and good agreement was observed.

**Nomenclature**

BPCS – Basic Process Control System PFD – Probability of Failure on Demand

HEP – Human Error Probability NR – Not Relevant

References

Bye A., Laumann K., Taylor C., et al., 2017, The Petro-HRA guideline, Institute for Energy Technology, Report IFE/HR/E-2017/001.

Center for Chemical Process Safety, 2007, Guidelines for Safe and Reliable Instrumented Protective Systems, John Wiley & Sons, Inc.

France INERIS, 2009, Omega 20, Approach for evaluating Human Safety Barriers, [www.ineris.fr/fr/omega-20-approach-evaluating-human-safety-barriers-0](http://www.ineris.fr/fr/omega-20-approach-evaluating-human-safety-barriers-0) accessed 01.10.2024.

Gertman D.I., Blackman H.S., Marble J.L., Byers J.C., Smith C.L., 2005, The SPAR-H Human Reliability Analysis Method, US Nuclear Regulatory Commission, NUREG/CR-6883.

Marzal E., Sharpf E., 2001, Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis, Research Triangle Park, The Instrumentation, Systems and Automation Society.

Myers P., 2011, Layer of Protection Analysis – Quantifying Human Performance in Initiating Events and Independent Protection Layers, 14th annual symposium of Mary Kay O’Connor Process Safety Center.