Human Response IPLs and Human Error Prevention IPLs (beyond administrative controls)

William G. Bridges
Technical Director
Process Improvement Institute – part of Trinity Consultants
Knoxville, Tennessee, USA
wbridges@piii.com

Arthur M. (Art) Dowell, III, PE
Principal Engineer
Process Improvement Institute – part of Trinity Consultants
Houston, Texas, USA
adowell@piii.com

Matias Massello
Senior Process Safety Engineer
Process Improvement Institute – part of Trinity Consultants
La Plata, Argentina
mmassello@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2026 Spring Meeting and 22nd Global Congress on Process Safety
Houston, TX
April 12-16, 2026

HUMAN RESPONSE IPLS AND HUMAN ERROR PREVENTION IPLS (BEYOND ADMINISTRATIVE CONTROLS)

Main authors

William Bridges – Technical Director
Process Improvement Institute (PII) – part of Trinity Consultants
E-Mail: wbridges@piii.com

Art Dowell, III, PE – Principal Engineer/Senior Instructor
Process Improvement Institute (PII) – part of Trinity Consultants
E-mail: adowell@piii.com

Contributing author

Matias Massello – Senior Process Safety Engineer
Process Improvement Institute (PII) – part of Trinity Consultants
E-Mail: mmassello@piii.com

Abstract

There are many scenarios for which Layers of Protection Analysis (LOPA) may be difficult to apply. One such case is when a scenario is dominated by human error, and yet there does not appear to be a way to have one or more IPLs. This paper provides a list of human-error prevention IPLs to consider. Several case studies are provided, including an assessment of a task at a copper smelter that was addressed using LOPA, incorporating human-error-prevention IPLs that other sites may not have considered. It appears always possible to develop and install IPLs against high-human-error scenarios.

1. Fundamentals: Human Response to Critical Process Deviations

Humans response to an alarm or troublesome reading or sample result can be a great safeguard layer against major accidents because the human has the capability to diagnose false alarms and in other ways prevent a spurious shutdown of a process. Many organizations are reluctant to use human response as a protection layer because "humans are human" and make mistakes. Of course, instrumented systems fail as well. Nothing is perfect. The key to using human response as a layer of protection is to follow the general guidelines for qualifying a response as a Human Independent Protection Layer (IPL).

There are 5 steps to using a human to respond to a critical process deviation as a Human Response IPL:

1. Determine which parameter limits (announced by alarms or other triggers) should have a human response, and why a human response is best.
2. Ensure human response action meets the definition of an IPL
3. Develop a troubleshooting guide (general steps for the operators to take) for each response.
4. Perform initial training on each human response IPL.
5. Validate that human response success rates are high enough, including testing and periodic refresher training.

This paper explains the best practices we have found for each of these steps.

2. Step 1: Determination of which parameter limits should have a human response

The first step is to determine which parameter limits (announced by alarms or other triggers) should have a human response, and why a human response is best. This important first step is difficult for many organizations, either because they have a prejudice against using a human response as an IPL or because they do not trust their hazard evaluation teams to make such judgments. The CCPS book on LOPA (2001) [1] and the follow-on book, *Guidelines for Initiating Events and Independent Protection Layers*, CCPS (2015) [2], both allow the use of Human IPLs, and both give criteria on their use. Neither book tells how to determine if and when a Human IPL should be used, but both instead state that the PHA (HAZOP, What-If, etc.) is the setting for determining what layers of protection are appropriate, and if that fails, then LOPA itself allows the use of a Human IPL as one IPL in a scenario, but it is up to the LOPA analyst to determine that the Human IPL is the best selection from alternatives for risk reduction.

If qualitative methods such as HAZOP or What-If brainstorming are used to determine when a Human IPL is most appropriate, the team should follow the protocol outlined in Bridges & Dowell (2016) [3]. This approach provides a qualitative means of determining when safeguards (including human response safeguards) meet the definition of an IPL. Once determined, the Human IPL should be documented as such in the PHA analysis, as shown in Table 1.

Table 1. Example documentation of IPLs in a PHA (in this case HAZOP method) Analysis Table [3]

No.: 2 XXXX storage spheres xxx-T-XX A/B/C/D/E/F/G/H/I/J/K/L (1 of 12)					
#	**Dev.**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
2.1	High level	Too much flow to one sphere from XX Plant (through their pump; about 40 bar MDH)	High pressure (see 2.5)	High level SIF with level sensors voted 2oo2, to close inlet valve **IPL Type:** SIF SIL 1 Overflow thru pressure equalization line to other spheres (through normally open [NO] valve) **IPL Type:** Overflow	
		Misdirected flow - Liquid from xxx Plant(s) to spheres (see 1.4)	Overpressure of sphere not credible from high level, for normal operating pressure of the column (which is 1.75 MPa), unless all spheres are liquid filled and then thermal expansion of the liquid could overpressure the spheres	High level SIF with level sensors voted 2oo2, to close inlet valve **IPL Type:** SIF SIL 1 Overflow thru pressure equalization line to other spheres (through normally open [NO] valve) **IPL Type:** Overflow Spheres rated for 1.95MPa (19.5 Bar, approx) and the highest pressure possible from the column feeding the spheres is 1.75 MPa Level indication and high level alarm in DCS, used by operators to manually select which tank to fill **IPL Type:** Human IPL	
			Overflow into the equalization line will interfere with withdrawal from the column, but this is an operational upset only		
			Excessive pressure on inlet of high pressure liquid pumps, leading to excess load on pumps and trip of pumps on high pumps, causing trips of xxx, xxx, etc. - significant operability issue		
2.2	Low level	Failing to switch from the sphere with low level in time (based on level indication)	Low/no flow - Liquid from spheres through high pressure product pumps to the vaporizer (see 4.2)	Level indication and low level alarm, inspected each year, per government regulation **IPL Type:** Non-IPL. Not independent (part of the cause). 9 other spheres with possibly enough level to switch to Feeding from two spheres at all times, so unlikely for BOTH spheres to have low level at the same time Two level indication from SIS level transmitter, with low level alarm, with more than 60 min available to switch tanks (SIF driven alarm and response) **IPL Type:** Human IPL **Comment:** Possible IPL, if action of the operator is quick enough	Rec 4. Make sure the Human IPL of response to low level in all spheres and tanks is described in a trouble-shooting guide (like an SOP) and practiced once per year per unit operator. This will make this response a valid IPL.
			Low/no flow - Unqualified liquid from spheres back to Plant (see 6.2)		

3. Step 2: Ensuring Human Response action meets the definition of an IPL

The prior step should have already performed this check when determining whether a Human Response IPL is the best protection layer for the scenario. Regardless, before further efforts to ensure proper human response, the organization should ensure that all criteria for a human response IPL have been met. Per the *Guidelines for Initiating Events and Independent Protection Layers*, 2015 [2], this includes:

3.1. The Human IPL (and any associated alarm) must be truly independent of the other protection layers. That is, there must be no failure that can deactivate two or more protection layers.

The IPL (also applies to IE) includes the ENTIRE sub-system, including any root valves, impulse lines, and bypasses. The other IPLs cannot share any of these or other components (except for the mother board of the BPCS loops).

A device, system, or action is **not** independent of the initiating event and cannot be credited as an IPL for either approach if either of the following is true:

- Operator error is the initiating event, and the candidate IPL assumes that the same operator must act to mitigate the situation. Human error is equivalent to a system failure, and once a human has committed an error, it is unreasonable to expect the same operator to act correctly later in the sequence of events. This approach is justified because the error may be due to fatigue, illness, incapacity (drugs or alcohol), distraction, work overload, inexperience, faulty operating instructions, lack of knowledge, etc., that persist later when the action is required.

Examples where the Human IPL is not independent include

- Assuming that the same operator acts correctly after the operator error initiated the event.
- Alarms that are annunciated on the BPCS are not independent of the BPCS; if the BPCS is counted as an IPL, then such alarms cannot be counted as an IPL (again, see the exception discussed later).

3.2. The Human IPL is specifically designed (capable) to prevent or mitigate the consequences of a potentially hazardous event.

- Is the Human IPL valid for the mode of operation for the scenario (startup, shutdown, normal, batch, etc.)?
- Is the Human strong enough to perform the required action, such as closing a manual isolation valve?
- What are the maintenance/reliability practices and plant/company history for any related equipment that the Human must use to complete the desired action? How much likelihood reduction credit will you take for the alarm working?
- How good are the procedures and related training (and drills)? Were the operators trained in the specifics of how to respond to this alarm/indication? Are they tested often enough?

- Is the Human fast enough?

  Specific Criteria on Speed of Response versus Process Safety Time

  The criteria for setting the alarm level (that sets the time available for response) should be true before going to the effort of developing a procedure for response (before developing a troubleshooting guide explained in Section 6):

  The response is typically still possible, but it is time-dependent. The time available is called the process safety time (PST). The operator must complete the diagnosis, make the necessary change(s), and make sure they are out of harm's way by the end of the Maximum Allowable Response Time (MART) [4].

  We usually set an alarm or a pre-alarm to trigger this action. This is usually before the shutdown triggers (ESD occur automatically) or release points (PSV set points) are reached

  The Min and Max shown in a Troubleshooting Guide are not the absolute safety limits for a system, but are instead values that give us time to take action to prevent reaching the absolute limits.

  There is still time to prevent or avoid the final consequences that could occur if we reach the ultimate limits of the process. Usually, we want the MART to be ½ or less of the PST, and we want MART > 10 minutes for troubleshooting in the field/plant and MART > 5 min for troubleshooting only from the control room [5].

  See the PII database of IPL Datasheets for detailed criteria on qualifying a human IPL. Similar datasheets are also available in *Guidelines for Initiating Events and Independent Protection Layers*, CCPS (2015) [2].

3.3. The Human IPL must be maintained, tested, and validated periodically; it must be proven that the Human IPL can be relied upon to do what it was intended to do.

The IPL must be maintained and periodically proven or validated. The site must have data that supports the reliability factor. The frequency and test method must comply with best industry practices for such IPLs. Also, the site must maintain a database for each IPL that statistically supports the PFD stated. For a component or instrumentation IPL, this requires maintaining a statistical failure rate database that justifies the PFD listed for each IPL. For a human IPL, the site must maintain data from "drills" of the action of the worker that statistically demonstrates that the worker(s) can indeed implement the required action (of the IPL) within the time specified in the IPL, or else they must use another means of validation as discussed in Section 6 of this paper.

3.4. The Human IPL maintenance and validation must be *Audited*.

Auditing is required to ensure the validation, procedures, training, and resulting data are adequate. This is an administrative check. This auditing cycle is set frequently enough (typically 1 year for the first audit, then 5 years thereafter) to ensure that validation is carried out as planned and is sufficient to justify the IPL and its PFD.

4. Step 3: Developing a Troubleshooting Guide (TSG) for Each Response

TSGs are a special form of operating procedure. They are written for the actions we want the operators to take to recover from a process deviation, *before an emergency situation occurs*. They are called guides because rarely can we predict the process conditions at the time the action is required. Troubleshooting guides (and necessary training and drills) are required for any action considered a Human IPL. The Action Limit is what we show as the Min or Max in a troubleshooting guide. The action limit triggers the demand to use the troubleshooting guide.

If the unit has a good PHA/HAZOP, then it is best to extract information from the HAZOP (or What-If) analysis tables to start the development of each guide. (Table 2 shows examples of the conversion of HAZOP entries into TSG entries.) The guide is then finished with input from the process experts [6].

Table 2. Examples of Creating a TSG from a HAZOP Table

HAZOP Table Entry	Troubleshooting Guide Entry
Cause: *Bypass valve is open or passing*	Make sure the bypass is tightly closed
Safeguard: *Isolation valves for the vessel*	Isolate the vessel, if necessary
Safeguard: *Relief valve*	Make sure the relief valve block valves/relief path are open

The key categories of information needed in a troubleshooting guide are [6]:

- IMMEDIATE ACTION (by system or by operator)
- DECIDE IF ALARM IS REAL
- FINDING and FIXING the CAUSE
- FIX or BYPASS the PROBLEM

4.1. Optimal presentation of troubleshooting information

Ideally, troubleshooting information should be embedded in the basic process control system (DCS) so that operators can access it on demand with a single click or keypress. Using the DCS to display the steps for responding to alarms (troubleshooting) is becoming more the norm each year. For more than 15 years, many companies have been taking TSG information and embedding it in the DCS; operators can then access this reminder of the proper response with a single click on the human-machine interface (such as a mouse click). On the next page, ***see an example of the TSG that follows best practices*** [6].

Trouble-Shooting Guide

Alarm or other Trigger:	**PAL 4446 – Low Pressure Alarm for Suction of Organic Feed Pump 40-PM-18.445**

Action Limit	5 kPa		
Consequence:	Possible pump seal failure, releasing or sparying organic watse into the berm		
Process Area:	PB&D Incinerator; Liquid Organic Feed	**Oper. Mode:**	Normal
Drawings:	D-400-PI-013	**MART (minutes):**	21

Actions	Responsible
IMMEDIATE ACTION (by system or by operator)	
• DCS interlock should shut down organic feed pump (40-PM-18.445)	Operators
• From the DCS, MAKE SURE the organic feed pump is shut down	Operators
• HAVE the field operator check for leaks near the pump	Operators
• IF there is a large leak / release, THEN use the ESD switch to shut down the unit and follow/complete the shut down and isolation procedure, OPS-EP-232	Operators
• IF there is a minor leak or no leak, THEN: ○ COMPELTE the rest of the Trouble-Shooting Guide ○ And DECIDE hot to contain the leak ○ And Decide when to repair the leaking seal	Operators
DECIDE IF ALARM IS REAL	
• From the DCS, CHECK the pressure and feed tan level trends. IF the trends indicate the alarm is valid, THEN continue with finding the cause and fixing the caise or fixing or bypassing the problem.	Operators
FINDING and FIXING the CAUSE	
• CHECK valves upstream of the organic feed pump to see if any are closed too far, including checking the ESD valve.	Operators
• CHECK, by feel with hand, if the heat tracing is on. IF not, TURN ON heat tracing.	Operators
• MAKE SURE nitrogen to the pump seal is at the normal operating pressure.	Operators
• CHECK if the line is plugged or frozen (skill)	Operators
• CHECK if the line is actually low using the sight glass at the tank and opening/closing the valves on the taps to the tank	Operators
• IF the cause is low level in the feed tank, THEN resolve the problem if necessary based on the cause that is found (skill)	Operators
FIX or BYPASS PROBLEM	

Actions	Responsible
• IF necessary, SHUT DOWN the Unit to allow fixing the problem.	Operators
• FOLLOW the proper procedure to resolve problems (repair procedure, line clearing procedure, etc.)	Operators
• IF the desion is made to continue operation without all equipment in normal condition, THEN: ○ FOLLOW Temporary Operating mode, if there is a temporary procedure alread written for this possible problem/condition ○ FOLLOW MOC procedures to obtain apporval of any non-standard temporary operating procedure or mode	Operators
END	

Actions	Responsible

Date	Name	Errors found in procedure / Suggestions for improvement

Affiliate/Site/Plant	Owner	Number	Release Date	Next Revision
PII Chemical Plant	Sr Manager Operations	2020-521	2016 June 5	2021 June 5

Date	History of changes to this procedure
2016 June 5	Changed to EHSS critical procedure. Included hazard and risk assessment.
2011 June 5	New developed procedure

ATTACHMENTS

- **Related drawings, charts, etc.**
- **Background explanation**

Guidance

5. Step 4: Perform Initial Training on Each Human Response IPL

Now, each operator must be trained on the steps to take for each human response IPL. Each operator means all the shifts and all the operators who might need to respond to an alarm, AND all the backup operators who would need to cover vacancies for illness, training, or vacation.

6. Step 5: Validation that Human Response success rate is high enough

The failure rates and probabilities of failure on demand (PFDs) used in LOPA should be verified to ensure they are appropriate. Validation of the values used in risk analysis can follow any of the four

methods used for initially establishing failure rates. The validation method used for any particular value can differ from the original method used to determine a failure rate or probability of failure on demand.

As mentioned earlier, much of Section 6 was originally included in the *Guidelines for Initiating Events and Independent Protection Layers and Initiating Events, 2015* [2], but was subsequently cut before publication of the final book. This paper provides that useful information once again.

6.1. Validation approaches

The four *validation* methods are presented in increasing order of robustness. As the values used in a risk analysis increase with the reliability claimed, consideration should be given to using more robust validation methods. Site-specific data can be used to justify extending the reliability claimed for initiating events or independent protection layers beyond the values derived from generic data.

- **Expert Judgment.** It is often used as a validation method for all of the other methods of generating values for failure rates and probabilities of failure on demand. The critical evaluation of values derived from other methods by one or more experts is a means of validating the values used in a risk analysis.
- **Generic Data.** Validation by the use of generic data is through monitoring of any updates to the data used in an analysis along with other sources of generic data to ensure that improved values developed by industry sources do not invalidate the values originally selected. Validation by the use of generic data can be used for original values derived from expert judgment, generic sources, and predicted values. Normally, values for failure rates derived from analysis of site data are more accurate than any generic source, and generic source data would not be used to change the value derived from analysis of site data.
- **Predicted Reliability Values.** Can be used for validation when the original values were selected based on expert judgment or generic data, and predicted values become available. For example, a level transmitter might be assumed to fail once every 10 years based on expert judgment or generic data. If a predicted value of failure is later reported by the manufacturer for the particular level transmitter of one failure in six years based on calculations from component failure rates, the lower reliability may invalidate the LOPA based on the less conservative value.
- **Site-specific data.** The most robust means of validating the values used in LOPA is to collect and analyze failure rate data in the area being analyzed. Site-specific data can be used to validate failure rates developed from expert judgment, generic data, and predicted values. The validation process may support the values derived from the original method, show that the actual reliability of the systems is not as good as predicted by other methods, or reveal that the systems are more reliable than anticipated. When site-specific data reveals that systems are not as reliable as originally developed, steps can be taken to improve reliability or address potential deficiencies in risk management by implementing additional mitigating actions. In situations where the site-specific data reveals that the reliability of the systems in a particular

application is better than originally derived, the better values can be used in the design of future applications.

6.2. Choosing the Approach for Validation of Human IPLs

Figure 1 describes the decision-making necessary to choose Expert Judgment, Prediction/ Estimation, or Site-Specific Data approaches for validation.

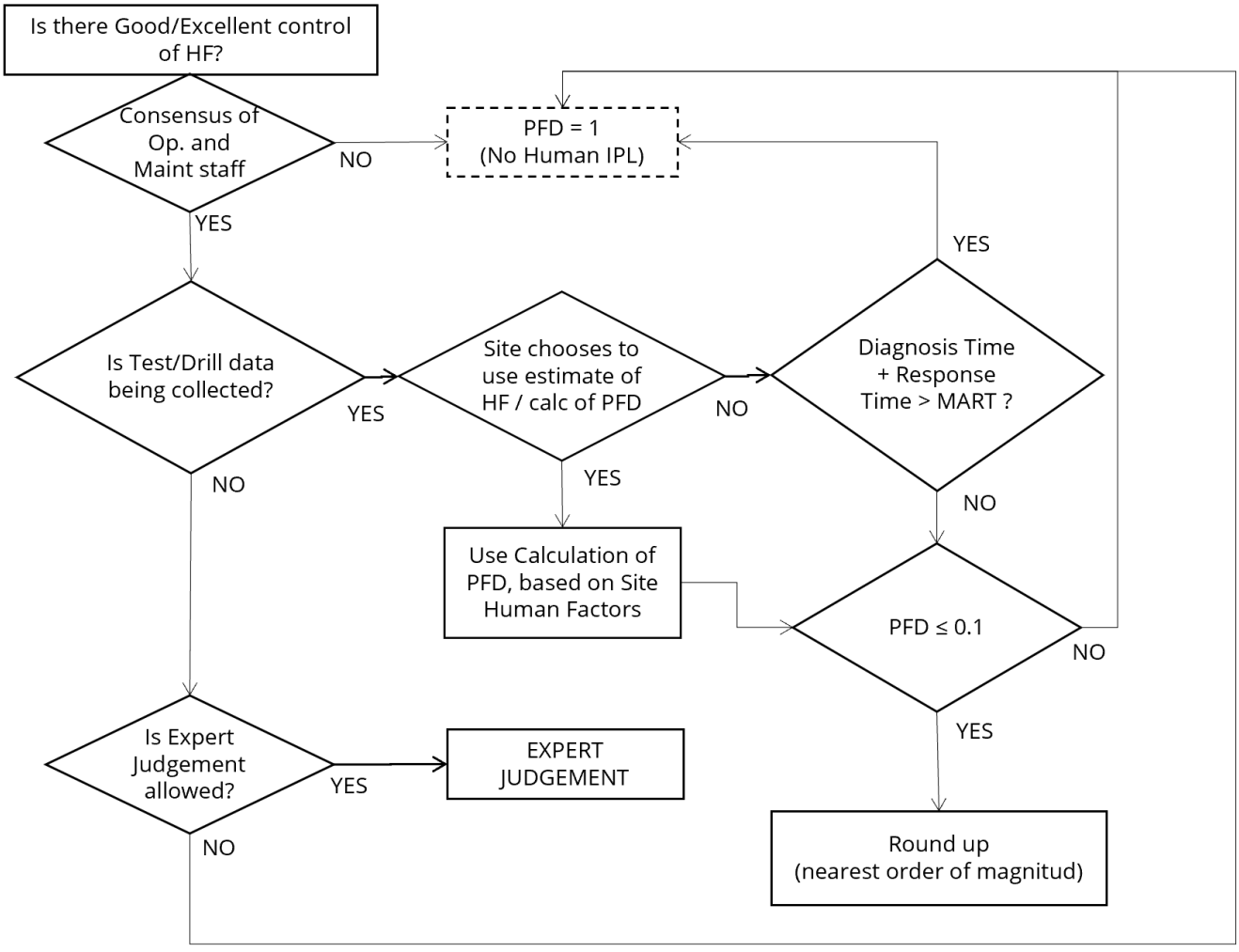

Figure 1. Example Decision Path for Validating Human Response IPL (Copyright PII, 2017 and 2026)

6.2.1. Determine if Validation by "Expert Judgment Only" Is Allowed

The questions in Table 3 are used in the initial screening process. If ALL are False, *then a PFD of 0.1 is valid without further calculation*. If ANY of the statements in Table 3 are true, then the validation

calculation approach (Section 6.2.2) or the Site-Specific Data (Section 6.2.3) must be applied to verify that the required reliability is achieved.

Table 3. Determine (Using Expert Judgment) if Validation by Predicted Data Is Required

#	Criteria	True	False
1	Based on consensus of expert opinion, the operator has less than 15 minutes to successfully detect, diagnose, and perform the required action		
2	Operator response is required without explicit criteria and response instructions		
3	Critical or emergency responses involve multiple people		
4	Response actions provide no feedback that they are effective		
		If any are True: Go through the Predicted Data method for validation of the PFD	**ALL False**: Use PFD = 0.1 (No further calculation needed. Expert Judgment is sufficient for validation.

Determine if the Expert Judgment Estimate of the Baseline Human IPL Time Is Less than MART

The time available is critical to the reliability of any response activity. A shortage of time leads to hurrying and increased stress. In addition, under these conditions, any errors that occur may not be correctable. Ultimately, the action must be accomplished within the MART.

For a human response IPL, MART is the time from when the sensed parameter reaches the set point (and then perhaps a few moments later the alarm sounds, if alarmed) to the point of no return where the corrective action can no longer prevent the incident. This value is determined from process dynamics independent of any hoped-for human response. It includes any time delay in alarm activation and any time for automated actions (initiated by the operator) to occur.

This example of validation by predicted data requires three different time elements versus MART (maximum time available to stop the event):

A. **Detection time.** Time from when the parameter of interest exceeds the "safety" limit until the deviation is noticed by the human.

- Detection and annunciation could be via a sensor and alarm, followed by sensory perception of the annunciation by the operator.
- Detection could be by the operator taking a sample to the lab and then subsequent analysis and reporting of results by the lab technician. The detection time in this case includes time between sampling (at least one cycle), plus the time to transport the sample, plus the time to wait for analysis and perform analysis, plus the time to report the results to the appropriate operating staff.
- Detection could be the operator noticing a problem during routine operator rounds, in which case, the time since the previous round is the major portion of the time consideration. So, for rounds every four hours, the detection time is greater than or equal to four hours; but note that it is best to rotate operators every round to enhance vigilance.

Use Expert Judgment for this estimate.

B. **Decision time** (time to decide what action to take; also called *diagnosis* time in HRA). The decision time was identified as a source of variability when people assessed the reliability of these activities. Consequently, the decision time is fixed within this validation method based upon the activity type. For purposes of alarms that a site would allow for LOPA, the decision time is normally less than one minute. But some HRA data developed for diagnosis time in control rooms (Swain, 1983 [8]) suggests that there is 90% chance the diagnosis will be correct if the worker in a nuclear power plant control room has at least 10 minutes to diagnose, and a 99% chance of correct diagnosis if they have 40 minutes. Because of these traditional values, the decision time is typically set at 10 minutes. However, for actions that require no or very little diagnosis or in simple process units, this value can reasonably be set to five minutes. Use Table 4.

C. **Response time** (time to complete all the alarm response activities). This is the time required to complete the tasks that will prevent the undesired event, as detailed in the alarm response procedure (e.g., after the procedure has been chosen as the correct course of action). Use Expert Judgment for this estimate. (For comparison, this is the time that is measured directly by testing/drills in validation using Site-specific data; see Section 6.2.3 for details.)

Estimate the task response time: Using solicitation of expert opinion (including at least two senior operators from the unit and one senior process engineer or equivalent), develop an Expert Judgment estimate of the time to complete the response activities, given that the diagnosis is performed correctly.

IF: Detection Time (including any delays in a related instrument system) + Decision time + Task response time > MART

THEN: The human response IPL is not valid using Expert Judgment Approach

Table 4. The Decision-Time Factor Assigned to the Different Activity Types

Activity type	Decision time
Unambiguous cue in a continuously staffed control room or similar staffing near an alarm annunciation location, with simple process and little or no diagnosis (with a decision tool, such as a troubleshooting guide).	5 min
Unambiguous cue in a continuously staffed control room or similar staffing near an alarm annunciation location, with complex process unit that requires diagnosis to deduce the failure cause and the proper action to take (with a decision tool, such as a troubleshooting guide).	10 min
Requires diagnosis of a novel fault situation (cannot be used for IPL in LOPA).	Beyond LOPA

If the total human IPL time is too great, then the site may:

- Decide to use other methods to validate the human response IPL
- Decide to redesign the human response IPL so that it can be done in less time than the MART.

- Decide to redesign the system to eliminate or reduce the risk.
- Decide to install or upgrade other types of IPLs (such as IPS, which are faster to respond) in lieu of the human response IPL not being available (because it is currently invalid).

6.2.2. Approach for Validation of PFD of HUMAN IPL using a combination of Generic Data and Predicted Data

The approach shown below is based largely on the methods described in SPAR-H (NUREG /CR 6883) [9], which is mainly a simplification of the much more complicated and detailed HRA methodology developed for the analysis of critical tasks (Swain, 1983) [8]. The approach starts with a baseline human error rate (0.0008 per year) is the lowest human error rate and then corrects that rank based on the multipliers related to good or bad human factors. See Table 5 for PII's method of how to estimate the PFD of a human response based on adjustment for human factors at the site and adjustment for the number of practices per operator per year (total practice is the combination of drills and actual responses to that same alarm by the same operator).

Table 5. Estimation of the PFD for Human Response IPL based on Basic Human Factors

Based in part on: Gertman, D.; et. al., *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005. PII has modified the list slightly to account for general industry data and terminology and to incorporate PII internal data.

Human Factor Category	Human Factor Issue/Level	Multiplier Error Rates
Available Time (includes staffing Issues) – ***for responses only***	Inadequate time	$P_{failuure}$=100%
	Barely adequate time (≈2/3 x nominal)	10
	Nominal time (1x what is expected)	1
	Extra time (> 2 x nominal and > 20 min)	0.5 to 0.1
Stress/Stressors (includes staffing issues)	Extreme stress (threat stress; unloading ship with crane non-stop for more than 2 hours, imminent hazard nearby)	5
	High stress (time pressures such as during a maintenance outage; issues at home...)	2
	Nominal	1
Complexity & Task Design	Highly complex task. Or very low complexity/boring task that requires 100% attention for more than 45 min.	5
	Moderately complex (requires more than one staff)	2
	Nominal	1
	Obvious diagnosis	0.2
Experience/ Training (practice rate is key))	Low experience relative to complexity of task; or poor/no training	10
	Nominal	1
	High	0.5
Procedures	Not available in the field as a reference, but should be. Or 75% accuracy or less ***(normal value for process industry)***	20
	Incomplete; missing this task or these steps; or < 85% accuracy	8
	Available and >90% accurate, but does not follow format rules	3
	Good, 95% accurate, follows >90% of format rules	1
Human-Machine Interface (includes tools)	Missing/Misleading (violates populational stereotype; including round valve handle is facing away from worker)	20
	Poor or hard to find the right device; in the head calc	10
	Some unclear labels or displays	2
	Good	1
Fitness for Duty	Unfit (extreme fatigue level at >80 hrs/wk, or >17 hr/day, no day off in 7-day period; or illness, legal intoxicated, etc.)	20
	Highly degraded fitness (high fatigue such as >15 hr/day or >72 hr/wk, or more than 4 consecutive shifts of 12 hours or more; illness, injury, legally barely intoxicated, etc.)	10
	Moderately Degraded Fitness (≥12 hr day or ≥ 60 hours/wk; but at least 1 day off [break] per week)	5
	Slight fatigue (more than 8 hr per day; up to 48 hrs per work week, but at least 1 day off [break] after 48 hours of work ***(normal value for process industry)***	2
	Nominal	1
Work Processes & Supervision	Poor	2
	Nominal	1
	Good	0.8
Work Environment	Extreme (in temp, humidity, noise, lighting, vibration, etc.)	5
	Good	1
Communication	Communication system/interference damaged; poor communication environment	10
	No standard for verbal communication rules ***(normal value for process industry); use this value if coordinated task for response***	3
	Well implemented and practiced standard	1

If all of these human error factors are controlled very well, then the optimized human error rates listed in this document are achievable. Alternatively, if one or more of these factors are compromised, the human error rate will increase by the values shown in this table. As an example, an individual whose fitness for duty rating is unfit due to the excessive work hours shown in the table will make errors at a rate 20 times greater than an individual whose fitness for duty is normal.

With excellent control of each of the human factors listed above, a company can begin to approach the lower limits that have been observed for human error. These lower limits are about:

- **1 mistake in 100 steps for most procedure-based tasks** (such as starting up a process unit), a little less for a routine (daily) task that becomes almost a reflex
- **1 in 10 chance or a little better for diagnosis and response to a critical alarm**

Excellent control requires superior design and implementation of management systems, which is enabled through a thorough understanding of these factors, as outlined below.

Simplifying assumptions

Not all inputs for a full HRA evaluation are likely to be readily available to the LOPA team or analyst. Some HRA inputs are often team or analyst judgments, which can lead to continued variability in results. For HRA inputs that could be reasonably held constant, human factors are set at the expected norm or standard. If the team or analyst feels that the human factors are not "up to standard" for the IPL (or related process unit) being validated, a recommendation for improvement for the specific human factor would be made, with validation contingent upon the plant or site implementing the recommendation.

It is ideal if all human factors (except practice) are set to 1 (no negative effect), but the analyst should use their judgment for the task, mode of operation, etc., for each human factor. **It is very rare for a site to have all human factors at a value of 1.**

As mentioned earlier, the approach shown below is based largely on the methods described in SPAR-H (NUREG/CR 6883) [9]. A somewhat similar calculation approach to human IPL validation has been used by Dow (Stack, 2010) [10]. but it does not allow correction of the estimate for poor human factors.

For a given human response IPL (triggered by an alarm or some other call for action), this validation approach consists of the following steps:

1. Estimate the time required for a successful response (which must be less than MART, as defined earlier). This is estimated from the following aspects of the response:
   A. Estimate the time for instrumentation or/or operator detection.
   B. Estimate the time for operator decision making (this is normally small compared to operator action).
   C. Estimate the time for operator action and verification

D. Fill in the appropriate factor in the *USED* column in Table 5 for the "Available Time" row at the table

2. Rate or scale the other Human Factors based on the descriptions in the columns. Fill in the appropriate factor in the *USED* column for each Human Factor.
3. Fill in the number of practices per year (PPY), which includes number of actual alarms responded to per year and number of times this alarm or a very similar alarm is drilled/practiced. The formula used to get to the right Practice Factor (PF), starting with a value of 0.0008 as the lowest baseline error rate possible, is:

$$PF = \left(\frac{250}{PPY}\right)^{0.6} + 0.4 \times \left(\frac{PPY}{1000}\right)^{2}$$

4. Calculate the overall human unreliability, which gives the PFD (normally 0.1) for the human IPL. If the number is > 0.1, then no PFD is allowed.

This PII method takes about 15 minutes to validate a PFD for one human IPL. This assumes the analysis is performed by a Subject Matter Expert (SME) who is trained in this method, is a human factors expert, and has access to the site data needed, which may, in turn, require solicitation of expert judgment (such as for the estimate of "time to respond"). Note that the time invested in validation by this method is comparable to validating one human IPL using Site-specific data, as presented in Section 6.2.3, which indicated that simply validating the actual responses to alarms (in drills) is likely the better approach.

6.2.3. Validation of Human IPLs by Site-Specific Data

A 0.1 PFD value for a human response indicates that the correct response occurs at least 9 out of 10 times (or no more than 1 wrong response for every 10 attempts). Most organizations will have identified many human responses involving a number of personnel as part of their LOPA studies. Some organizations believe that if they have a procedure and a training program in place, they can claim the PFD value of 0.1 for a Human IPL. This belief is no truer for a human IPL than it is for an active component-based IPL.

As required for all IPLs, a human IPL must be validated. The preferred approach to validation is direct measurement or testing of the human response (under controlled conditions or drills); but other methods of validation can include Expert Judgment, using data from other comparable settings (Generic Data method), and estimation of the PFD of human IPLs by mathematical modeling (Predicted Data method).

The next few pages present options for validating human IPLs using **site-specific data**. These include:

- 100% testing for each human responder and for each action to be taken.
- Sample plan testing of random combinations of human responders and actions.

One key focus of this paper is the discussion of practical means for collecting raw data in a plant setting to substantiate the site's error rates, especially for crediting a human IPL. The method for data collection covers the training requirements that should be met, proof drills for response to alarms, simulations and tests, frequency of proofs, and, of course, the effect of human factors on human error rates. *Actual plant data and tests are included in this paper to provide the reader with examples of how a simple data-collection and validation method can be set up within their companies*.

This section provides an example of the data needed for adequately counting the human in a LOPA (and other risk assessments) using Site-specific data for validation. One key focus of the section is the discussion of practical means for collecting raw data in a plant setting to substantiate site error rates, especially for crediting a human IPL. The method for data collection covers the training requirements that should be met, proof drills for response to alarms, simulations and tests, frequency of proofs, and, of course, the effect of human factors on human error rates. *Actual plant data and tests are included in this* section *to provide the reader with some examples of how a simple data collection and validation method can be set up within their companies*.

If a site has a robust system for reporting and investigating near-misses, it can be used to identify site-specific data on human errors (including both IEs and failures of human IPLs). Obtaining high near-miss reporting rates is covered in other research and papers (Bridges 2008, 2012, etc.) [11]. Note that the ratio of near-misses to loss events likely needs to be higher than 15 to provide sufficient data for validation using near-miss data alone.

Another way to collect site-specific data on error rates is to measure them through tests or drills of the action, and, for human IPLs discussed later, the results may need to be adjusted to account for the actual stress levels of the response. This practice is not commonplace in the chemical industry, but the US Nuclear Regulatory Commission (NRC) requires, under 10 CFR 55.45 and 55.59 [12], that all power plant operators be tested once per year on abnormal procedures. This testing is mostly related to humans involved as IPLs. 10 CFR 55.45 and 55.59 also allude to the possibility of using a test of a representative sample of human responses, but we address this option later in this section .

Example: Using Tests/Drills (Site-Specific Data Collection) to Validate Human Response IPLs
Until now, the actual effort to collect such data has not been well documented in the literature, though many chemical companies, refineries, and nuclear power plants do, in fact, validate human response using this method. Recent research (Bridges, 2010 and 2011) [13] [11] by three chemical companies documented the effort required to validate human response IPLs using Site-specific data. The following is an excerpt of the research results.

Validation Setup: A simple test was used to measure the response to an alarm condition. The test was not meant to measure the probability of detection of the alarm, but rather to measure the time required and the success in determining and executing the proper response to critical alarms as part of human IPLs. Two chemical plants belonging to large organizations (one in Malaysia and one in the USA) performed the test.

The test involved having multiple operators in one unit of one plant/site (one per company) respond to critical process alarms. These alarms were related to human IPLs. The actual response and time of response were measured, but essentially the tests were set up as a "pass or fail" – in other words, the tests were to determine if the operators were able to respond as desired/expected, within the allotted MART.

To run each test, the plants printed a data card (the size of an index card) and handed it to an operator chosen at random. Below (Figure 2) is an example of such an index card.

Human IPL Validation Test/Drill		
Response Task:	Max. Allowable Resp. Time (MART)	Response Time:
LAH for Tank 105	*15 minutes*	5:20 minutes
Date of Test:	Time/Shift:	Employee Number:
1/23/10	07:35/A	23122
	Pass/Fail: Pass	

Figure 2. Example of a card used to administer the validation of a single human IPL

Note that the card contains an estimate of the MART – as defined earlier in this appendix and elsewhere in this guide; this is the time an operator has to perform the task once the alarm is received until it is too late to take any further action. The time it took to print and hand out the index card was minimal.

Validating/Testing: A human response IPL "failed" if the operator could not perform the required action to prevent the hypothetical outcome within the MART (defined earlier). The person administering the test timed the operator's response and recorded the results. (Again, note that these tests did not validate the probability of an operator failing to detect an alarm.) Each test took 10-15 minutes to administer and less than one minute to record the data. The validation was performed by multiple operators on multiple shifts. The tests were administered by a shift supervisor, a shift engineer, or, in some cases, a process safety coordinator. It is likely that another operator could administer most proof tests (validations), and site management could audit a percentage of the tests to help ensure against bias. If the operators test each other, then the time to administer a test is likely not significant enough to measure, since they must be there, regardless of their other duties. The total time for the test varied, but the two sites that performed the test considered the time to administer the test to be minimal; the greatest effort was simply for someone other than the operator to be there to "independently" measure the operator's response time (i.e., time to administer the test).

For the most part, the tests came with little warning and occurred on all shifts. Several critical alarms were tested using various operators, all randomly selected. (It is anticipated that, unless a sample plan is used, each operator will perform roughly one response related to each human IPL each year.) The time to respond was recorded on the index card.

Based on such raw data, the site was able to (1) evaluate the degree to which they were controlling human factors for the units, (2) identify which human responses qualify as IPLs, and (3) validate that the response is accurate enough and quick enough to qualify for the PFD used as the credit for the IPL (which for LOPA, the PFD is limited to a value of 0.1).

Table 6 provides a sample of the site-specific data for several similar human IPLs from the three sites (one in Malaysia, one in Canada, and one in the USA). For the Malaysia and Canada sites, the data were from the same operating area, comprising multiple operators across four rotating shifts of eight hours each. For the USA site, the shift was 12 hours.

All the IPLs passed (all operators performed each action correctly within the allotted time) during these tests/drills. The labor to perform the test took less than 15 minutes per test (including documentation time). After the initial resistance at each site to performing the test, the subsequent tests were not resisted and in fact the operations staff embraced the testing/drills since they saw many side benefits from the test/drills, including the re-enforcement of "what to do" with all parties involved (the person doing the test, the person recording the test, and the other operators who noticed the test in progress). Lead operators and supervisors administered the test; very little training or coaching was needed to ensure the drills were done properly.

Table 6. Site-specific validation of Human Response IPLs*

IPL #	Company	Response Task	Num. Tests	Avg. Response Time	MART	Failures	Avg. PFD	LOPA PFD
1	A	ABP: High temp in Generator	6	2.3	10	0	0	0.1
2	A	ABP: Loss of acid flow to Generator	12	2.2	10	0	0	0.1
1	B	Low seal gas pressure to turboexchanger bearings	5	5.7	15	0	0	0.1
2	B	High lube oil temp – XX Compressor	5	6.3	30	0	0	0.1
3	B	Low-level emergency alarm – Steam drum	5	4.9	15	0	0	0.1
4	B	High-high lube oil temp – YY Compressor	5	6.1	30	0	0	0.1
1	C	High level on Ammonia Absorber Column	10	5.1	15	0	0	0.1
2	C	Low temp alarm on Ammonia Compressor discharge	10	4.9	15	0	0	0.1
3	C	Low level in CO2 Compressor KO Drum	10	7.0	15	0	0	0.1
4	C	High level in HP Carbamate Condenser	10	6.1	15	0	0	0.1
5	C	High pressure in HP Carbamate Condenser	10	5.0	15	0	0	0.1
6	C	High pressure on Steam Controller to Rectifying Column heater	10	5.4	15	0	0	0.1

* Data provided by 3 companies (in USA, Canada and Malaysia)

All three sites believe it is possible to use a sampling of human error for similarly qualified humans doing similar response or proactive tasks. (This is because the responses for all IPLs were the same when the same operator acts on different alarms or when different operators act on the same alarms.) A sample plan of perhaps only 5% to 10% of the number of human-task pairs may be necessary to have a valid statistic for human error for a "type of action." Sampling is valid for human actions because of how the mind processes information and how humans take the necessary actions for similar situations. Obviously, sampling can greatly reduce the measurement and documentation burden for validating human error rates. If sampling is used, the sites suggest that:

- The site should first screen which responses can be grouped together into general types of response IPLs. Then a lesser percentage will need an individual validation drill.
- Perhaps do just one or two drills per shift per group per year for the simpler ones on some periodic basis; that gives a chance to test feasibility (make sure valves are not locked, make sure valve wrench or other tools are available, etc.).

Human performance sampling is discussed in detail in the parent paper on this topic [13] [14].

ADJUSTMENT for STRESS: As mentioned, these data (as with all drills) are collected during a simulation of a call for action. In a real event, *the stress to perform the task correctly would increase the average error rate*. NRC estimates (Gertman, 2005) [9] that the stress for this type of pre-emergency response action (versus emergency response and evacuation) will likely not be "extreme," but it will be "high," in which case a conservative estimate is that error rates would double from the test/drill case. It is likely not possible to get a drill that accurately mimics the stress of a real alarm event, so there will likely always be a need to adjust data to account for increased errors due to stress. It is likely more appropriate to double the observed error rates (observed PFDs) rather than doubling the observed response time. But in either case, the IPL data collected above must still "pass" when adjusted for stress for an IPL to be validated using Site-specific data.

7. Human Error Prevention IPLs (beyond administrative controls)

Once an organization optimizes human factors, it must recognize that human errors will still occur – albeit at a lower frequency and likely with a smaller adverse impact than before. Therefore, when the consequences of a human error are unacceptably high, the organization should implement solutions to further reduce the residual risk. These solutions can be designed either to prevent the error or to compensate for it, but they must be independent of the human error-initiating **event**.

Bridges and Rhodes [15] have compiled the following list of the best remedies for human error for these situations.

- **Captive Key.** Applied to the valve handle hub. PFD = 0.01. Requires placing one component, such as a valve or door, into an open or closed position before releasing the key needed to move another component into a potentially unsafe position. Can be used to make a sequence of steps for certain tasks difficult or impossible to skip or perform in the wrong order.

  - *Special consideration:* only one person at the site should have access to the machine that produces keys; only this person should be authorized to replace a key; copying of keys should not be tolerated and should be strictly enforced.

- **Limit switches on valve position.** Ensures that valves are in the correct position, potentially depending on mode or compared to another valve. The concept is similar to a captive key, but the control is by limit switches instead. The switch would trigger a shutdown or otherwise prevent misalignment. PFD = 0.1 to 0.01, with 0.01 requiring strenuous maintenance practices for switches that are not typical in many plants.
  - Typical limit switches are used for many permissives and mode change interlocks. Maintenance practices and control strategies must be well established to bring the probability of jumpering, knifing, or otherwise defeating a limit switch to a very low probability.
  - Some manual valves can be modified to have feedback/indication (though these are harder to keep working), giving the ability to verify if systems are isolated from the DCS panel.
  - Not as robust as captive key systems.
- **Mechanically coupled valves.** 2 valves that are hydraulically, pneumatically, or mechanically/physically linked. PFD = 0.1 to 0.01, with 0.01 requiring feedback/ indication on both valves.
  - Typically used to ensure that the mode switch will be successful, such as when backwashing filters or entering regeneration mode for driers, i.e., preventing only one of two valves from operating.
  - Special consideration: Limit switches are still needed to verify position, as these valves are difficult to maintain due to their more complex drive or pneumatic systems (can't operate on output alone).
- **Instrumented Permissive.** Such as an interlock/permissive to verify the pressure is within the correct range before allowing an XV to open. An example is where pressurization with a gas is supposed to be done manually before opening a valve for a cryogenic liquid to enter the system, given that the materials of construction experience brittle fracture potential at the temperature (boiling point) of the flashing liquid. PFD = 0.1 to 0.01, depending on configuration as a SIL 1 or SIL 2 preventive SIF.
- **Hand-held device with bar code reader**. To verify that the user has been to each device in the right sequence. PFD = 1 to 0.1 but could be stronger if tied back to the BPCS, which would then have the computer, not the computer operator, watching the activity to confirm a critical step is performed.
- **RF tags and matching of a pair.** Like Captive Key in concept, but for hose connections, and perhaps other situations. PFD = 0.01.
- **Unique connections.** Unique size, coupling type, thread pattern, etc., to reduce the chance of a wrong connection. PFD = 0.01.

- **Spring closing lever valves.** A manual valve that the human must hold open by use of the lever handle (typically), that will automatically close when the lever is released. Also called a dead-man valve. PFD = 0.1 to 0.01 (but usually PFD = 0.1 maximum). Such arrangements are applicable to small valves to prevent leaving a valve unattended, such as during manual draining or loading. Can be defeated by tying the handle in the open position.
- **Swing elbow.** The elbow and associated piping are designed so that the process can only be lined up in one direction at a time. PFD = 0.001. This arrangement works well for switching to process modes, such as regeneration of desiccant driers or catalytic reactor beds with very hot air or steam, but when the normal flow alignment is to a hydrocarbon process.
- **Unique SIF to compensate for, rather than prevent, Human Error.** PFD = 0.1 to 0.001. The example provided earlier was for an instrumented permissive. This remedy to compensate for a unique human error scenario includes installing SIFs to shut down a process or block or vent a line, such as to eliminate an overpressure scenario that is too large for the current pressure relief system (the scenario is a larger flow than any practical PSV or rupture disk system can handle).
- **Increase PSV size for a scenario unique to startup or online maintenance.** As needed, to achieve the full value of the PFD for the PSV configuration.
- **Upgrade materials.** Account for scenarios not considered in the original design by upgrading materials sufficiently that the consequences of human error are no longer possible, thereby reducing the likelihood by 2 to 4 orders of magnitude. See the "recommendation" in the Instrumented Permissive for one such example.
- **Change the design of at-risk components/systems.** Design out the need for components at risk or change to a different strategy for certain unit processes. This is an inherently safer approach, and it can include some of the design considerations mentioned above.

Each organization will want to develop such a list with examples, including (1) when to use each remedy, (2) what value of risk reduction is gained, (3) how to quickly estimate the cost of the remedy, and (4) an example or two of the remedy to help with clarification.

Table 7. Human Error Prevention alternatives

Safeguard/Remedy alternatives	RRF	Cost (k$)
Captive Key	100	0.5 to 1
Proximity Limit Switches (both ends are hardwired)	10 - 100	0.5
Mechanically coupled valves	10 - 100	
Instrumented permissive	10 - 100	
Bar Code – w/o procedure embedded; combined with interlocks	3 - 10	0.1
Bar Code – with procedure embedded; combined with interlocks	3 - 10	0.3
RFID (radio frequency identification; the reader is hardwired)	100	5

Safeguard/Remedy alternatives	RRF	Cost (k$)
Unique connections	100	
Spring-loaded dead-man valves	10 – 100	0.2 - 1
Swing elbow	1000	
Change to inherently safe design	1000	TBD

8. Conclusion

This paper presents a 5-step process for setting up and maintaining human response to critical process deviations.

1. Determine which parameter limits (announced by alarms or other triggers) should have a human response, and why a human response is best.
2. Ensure human response action meets the definition of an IPL
3. Develop a troubleshooting guide (general steps for the operators to take) for each response.
4. Perform initial training on each human response IPL.
5. Validate that human response success rates are high enough, including testing and periodic refresher training.

The paper also list many human-error prevention features (engineered features).

9. Acronyms

CM: Conditional Modifier
CS: Conditional Severities
EE: Enabling Event
HRA: Human Reliability Analysis
IEF: Initiating Event Frequency
IPL: Independent Protection Layer
IPS: Instrumented Protective System
ITPM: Inspection, Test, Preventive Management
LOPA: Layers Of Protection Analysis
MART: Maximum Allowable Response Time
PF: Practice Factor
PFD: Probability of Failure on Demand
PHA: Process Hazards Analysis
PPY: Practice Per Year
PSM: Process Safety Management
PSV: Relief Valve / Pressure Safety Valve
RRF: Risk Reduction Factor, =1/PFD

SOP: Standard Operating Procedure
TSG: Trouble-Shooting Guide

10. References

[1] CCPS/AIChE, Layers of Protection Analysis (LOPA), Wiley, 2001.

[2] CCPS/AIChE, Guidelines for Independent Protection Layers and Initiating Events in Layer, Wiley, 2012.

[3] W. Bridges and A. Dowell, "Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP - or - Why it is not necessary to "Boldly go beyond HAZOP and LOPA"," in *AIChE/CCPS 12th Global Congress on Process Safety*, Houston, TX, 2016.

[4] W. Bridges, "LOPA and Human Reliability – Human Errors and Human IPLs," in *AIChE/CCPS 6th Global Congress on Process Safety*, San Antonio, 2010.

[5] Process Improvement Institute, "Online database of IPLs and IEs," [Online]. Available: (pending).

[6] W. Bridges and R. Tew, "Best Practices for Writing Operating Procedures and Trouble-Shooting Guide," in *AIChE/CCPS 13th Global Congress on Process Safety*, San Antonio, TX, 2017.

[7] CCPS/AIChE, Guidelines for Chemical Process Quantitative Risk Analysis, Wiley, 2000.

[8] A. Swain and H. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278)," 1983.

[9] D. Gertman, H. Blackman, J. Marble, J. Byers and C. Smith, *The SPAR-H Human Reliability Analysis Method (NUREG/CR-6883),* Washington DC: U.S. Nuclear Regulatory Commission, 2005.

[10] R. Stack and P. Delanoy, "Evaluating Human Response to An Alarm for LOPA or Safety Studies," in *AIChE/CCPS 6th Global Congress on Process Safety*, San Antonio, 2010.

[11] W. Bridges, "Gains from getting Near Misses reported," in *AIChE/CCPS 19th Global Congress on Process Safety*, Houston, TX, 2023.

[12] US Nuclear Regulatory Commission, *Training requirements for nuclear power plant operators - 10CFR55.45 and 10CFR55.59.*

[13] W. Bridges and T. Clark, "LOPA and Human Reliability - Human Errors and Human IPLs (Updated)," in *AIChE/CCPS 7th Global Congress on Process Safety*, Chicago, IL, 2011.

[14] W. Bridges, "Proven Approaches to Ensuring Operators Can Respond to Critical Process Deviations in Time (Human Response IPL)," in *AIChE/CCPS 13th Global Congress on Process Safety*, San Antonio, TX, 2017.

[15] W. Bridges and W. Rhodes, "Human Factors Elements missing from Process Safety Management (PSM) Systems," in *AIChE/CCPS 17th Global Congress on Process Safety*, 2021.

[16] CCPS/AIChE, Guidelines for Risk Based Process Safety, Wiley, 2007.

[17] R. Walpole and et. al., Probability & Statistics for Engineers & Scientists, 8th ed., Prentice Hall, 2006.

[18] US Department of Defense, *Military Standard: Sampling Procedures and Tables for Inspection by Attributes (MIL-STD-105E),* 1996.

[19] CCPS/AIChE, Guidelines for Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis, Wiley, 2014.