Controlling Human Performance Between Both Unplanned and Planned Tasks within Abnormal Operation Mode

William G. Bridges
Process Improvement Institute Inc. (PII)
1321 Waterside Lane, Knoxville, TN 37922 USA
wbridges@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2021 Spring Meeting and 17th Global Congress on Process Safety
Virtual
April 18 – 22, 2021

Controlling Human Performance Between Both Unplanned and Planned Tasks within Abnormal Operation Mode

William G. Bridges
Process Improvement Institute Inc. (PII)
wbridges@piii.com

Keywords: Operating procedures, SOP, troubleshooting, abnormal mode of operation, non-routine modes of operation

Abstract

There is confusion in terminology used in the chemical-related industry for the class of procedures commonly referred to as Abnormal Mode of Operation and Abnormal Situation Management. This paper provides a clear definition of each mode of operation and gives examples of how the human performance is controlled for each.

1. Normal – Either a continuous mode or a normal batch mode of operation.

2. Planned Non-routine (Non-Normal) – Startup, shutdown, are online maintenance are the main non-routine or non-normal modes of planned operation. But planned temporary procedures, with time limits, are also part of this mode.

3. Abnormal – These include those activities that are planned for and covered by generalized procedures or Trouble-shooting Guides, TSG, but this mode of operation also includes the class of activities that have not been foreseen and therefore do not have written, step-by-step procedures. Companies can and many times do have guides for how to make decisions during abnormal situations.

4. Emergency Operations – These are "planned and partially proceduralized." An emergency operating mode is a diminished or reduced operating plan.

5. Emergency Shutdown – These are "planned and fully proceduralized." Typically, a TSG or Temporary Procedure that fails to resolve the issue in time will go to this; or for some events such as

a sudden loss of containment, the operations team will go straight to one of these procedures.

6. Emergency Response – These are "planned and partially proceduralized" like Modes 4 or 5, but this mode focuses on the protection of people, assets, environment, given the release or other imminent harm is in play.

This paper provides a framework to ensure no mode of operation is overlooked and it will help sites understand what is needed to control risk during each mode of operation. Most of the paper and presentation focuses on Mode 3, Abnormal Mode of operation.

1. All Modes of Operation

There are many modes of operation of a continuous operating process or a batch process. Each mode of operation has unique challenges, but the successful control of each mode depends on controlling human error rates by controlling the 10 core human factors, discussed later in this paper. One good breakdown of the categories of operating modes is provided below:

1. Normal – This is either normal continuous mode of operation or normal batch mode / recipe operation. For a continuous plant, there are no step-by step operating procedures for normal mode, but rather there are general operation orders that dictate the production rates, special operation limitations for the day or week, and a list of triggers (deviations) that point the operators to step-by-step procedures (Abnormal but predicted mode of operation) if the process moves out of the quality bounds or approaches or crosses the safety bounds. Statistics for the past 30 years indicates that about 20% of major process safety accidents occur during normal mode of operation, and about 80% of these (16% of the total number of major process safety accidents) occur due to mechanical integrity failures such as corrosion, erosion, and failure of structural components. A few percentages of major accidents during this mode of operation occurs due to insufficient independent protection layers (IPLs) or inadequate control of the integrity of these IPLs. A few percentages of major accidents attributed to this mode of operation are failures to correctly handle an abnormal situation (see Mode 3 below).

2. Non-routine – These modes are "planned and proceduralized" and include startup, shutdown, and online maintenance as the three main types of non-routine mode of operation; but also planned Temporary procedures, with time limits, are part of these. All these modes have step-by-step instructions (similar to batch operating procedures and the hazards and even the potential accident scenarios can be well understood if the process hazard analysis (PHA) of these modes is performed correctly. Statistics for the past 30 years indicates that about 80% of major process safety accidents occur during these modes of operation. Lack of PHA of procedures for startup, shutdown, and online maintenance is the greatest weakness at most

chemical process plants, because without this PHA on non-routine modes of operation, the process is lacking the unique IPLs needed for these operating modes.

A fourth type of this class of procedure is "Response to failures using a Temporary procedure". Examples include how to run in bypass mode if the flow controller fails and you want to keep running in manual. Temporary procedures are different in that there is normally a "time at risk" consideration for setting a limit on the length of time that a process can be in this mode of operation.

3. Abnormal – Some consider abnormal procedures a sub-class underneath Non-routine operating procedures, but this is not best. Abnormal modes include some un-proceduralized activities, but the industry (and most sites) have guides for most of these abnormal situations, and most of these are triggered from deviations from Normal Procedures (Mode 1 above). Failures during handling of abnormal situations accounts for up to a few percent of the major process safety accidents. A further breakdown of this classification of abnormal mode of operation is possible:

    a. Response to upsets using a Trouble-shooting Guides (TSG) – These are "planned and proceduralized" for handling deviations from the operating window (these or normally triggered on an alarm); these may result in shutdown, safe park, or emergency shutdown (all of which are also proceduralized). One major difference between 3a TSGs and "planned" procedures in Mode 1 and 2 is that the "trouble" predicted in the TSG can occur under many conditions, and the developers rarely put step numbers, but instead organize the TSG into sections and further break the possible actions into "bulleted" steps, with no particular sequence. So, a TSG is planned, but not completely proceduralized as no one can predict whether the process will be ramping up, ramping down, or be in a steady state when the deviation alarm is triggered.

    The trigger for such a response is not always an alarm. The trigger could be a weather report, a flood warning, or some expected issues arising from upsets in supply or upsets in adjacent units.

    Since 1993, the authors have provided several definitive papers on TSGs and how these are developed and how these are documented and administered, the most recent of which is "*Best Practices for Writing Operating Procedures and Trouble-Shooting Guides* [Bridges & Tew, GCPS, 2017]"[6].

    It appears to PII that most of the failures in Mode 3, abnormal mode of operation, are due to weaknesses in brainstorming, developing, writing, practicing, and administering TSGs.

    There are also important limitations of time-constrained responses to TSGs. A key human factors concept reported from investigators at the US Chemical Safety Board (CSB) was humans have a hard time digesting

written information. We are pattern-based, not data-based. Mary Douglas wrote that we initially scan about 5 percent of what's in front of us[7]. We match this partial data scan against hundreds and thousands of stored memories, and do a FIRST-fit pattern match, not a BEST-fit pattern match. We "satisfize," we do not optimize. We make decisions very quickly based on partial data recognition. Handheld devices in the field have shown some improvement in this regard, as the information is available a step at a time and as visual information (like a GPS map in your vehicle) can be readily displayed as well.

b. Response to Unanticipated Events – This mode of operation is "not planned and not proceduralized" and therefore this mode of operation tends to worry management the most. In this mode of operation, we rely on experience, knowledge of the process & chemistry, and situational awareness to win the day. The FIRST occurrence of an unanticipated event is handled in PSM through an *Emergency MOC*, which is a way of saying "we'll figure this out immediately, make the best judgment of what to do, do it, and then later we will do the risk review of the change, and then finally we learn from this one event and proceduralize this scenario into a Temporary Procedure or TSG for the next time it comes up".

The US Nuclear Regulatory Commission (NRC) learned a painful lesson on this Mode of Operation decades ago during Three Mile Island accident, when operators were not given the latitude to make free flowing decisions, but instead were locked into a rigid set of TSGs and emergency response procedures. The aviation industry, governed in the US by the Federal Aviation Administration (FAA) learned about this mode of operation many decades ago, as the number of accidents due to Mode 1, Mode 2, and Mode 3a dropped dramatically, leaving only Mode 3b to deal with. The US NRC and US FAA are now focusing on helping operators (crews) recognize when they are in this mode and on providing the skills and thinking processes to handle this mode of operation.

4. Emergency Operations – These are "planned and partially proceduralized." In summary, an emergency operating mode is a diminished or reduced operating plan, and is normally controlled (at least in part) by a Temporary procedures.

5. Emergency Shutdown – These are "planned and fully proceduralized." Typically, a TSG or Temporary Procedure that fails to resolve the issue in time will go to this; or for some events such as a sudden loss of containment, the operations team will go straight to one of these procedures.

6. Emergency Response – These are "planned and partially proceduralized" similar to Modes 4 or 5, but this mode focuses on the protection of people, assets, environment, given the release or other imminent harm is in play.

2. Coverage of All Modes of Operation within US OSHA PSM and US EPA RMP regulations

The US OSHA regulation 29 CFR 1910.119 on process safety management (PSM) does mention most of the modes of operation listed above, and states that covered facilities should have procedures for each mode of operation, routine and non-routine. But the OSHA PSM regulation does not mention 3b mode of operation, *Response to Unanticipated Events.* Like the US NRC and US FAA before them, the process safety regulators (US OSHA and US Environmental Protection Agency [EPA]) initially assumed that all events could be predicted and therefore "planned for and proceduralized". But this is not completely possible, as the NRC and FAA found out.

Many in the chemical and related process industry recognize that chemical process are at least as complex as nuclear power plants and flying a passenger jet, and so there will be some events or situations that cannot be predicted. There are industry best practices on 3b mode of operation, some more than 40 years old, and there is a growing discipline for handling mode 3b events. And there is a depth of knowledge and experience in handling the other modes of "planned and proceduralized" 6 classes of activities of many decades, though best practices for developing and using TSGs are less than 3 decades old.

3. Coverage of All Modes of Operation within Process Safety Best Practices

Process safety was practiced in the chemical industry for decades before there were regulations on PSM. In fact, the US regulations on PSM are an outline of what the industry was already doing to control process safety, though candidly the US PSM regulations are only a skeleton of the best practices for controlling process safety; and this skeleton is missing many bones!

Many companies do a reasonable job of addressing risk during modes 1-6; and some do a great job. ***But many are still weak on Mode 3a, and most are weak on Mode 3b***. At the best companies, the goal is to shrink 3b types by converting them into 3a (as more of the 3b scenarios are learned), and also by eliminating many of these scenarios by targeted IPLs. But it is highly unlikely industry will learn to predict all events and so a TSG or Temporary Procedure will not be available and practiced (drilled) for some events; those remaining scenarios without procedures are **Mode 3b**.

As mentioned earlier, from statistics from the industry and from US OSHA, most major process accidents occur during Mode 2 and Mode 1. Figure 1 on the next page illustrates this distribution of when accidents happen. The entire category of Other is less than 5% of the number of major process safety accidents. There is not enough data to make a firm conclusion, but it is believed that in the chemical-related industry, less than 1% of the accidents are related to Mode 3b scenarios (unplanned and proceduralized response to an event). This may appear to be good news, but part of the reason the percentage is so small is because the number of losses due to the other modes of operation are all too high compared to the aviation industry and nuclear power industry. For the aviation industry, the fraction attributable to this 3b category is likely 20% or higher.

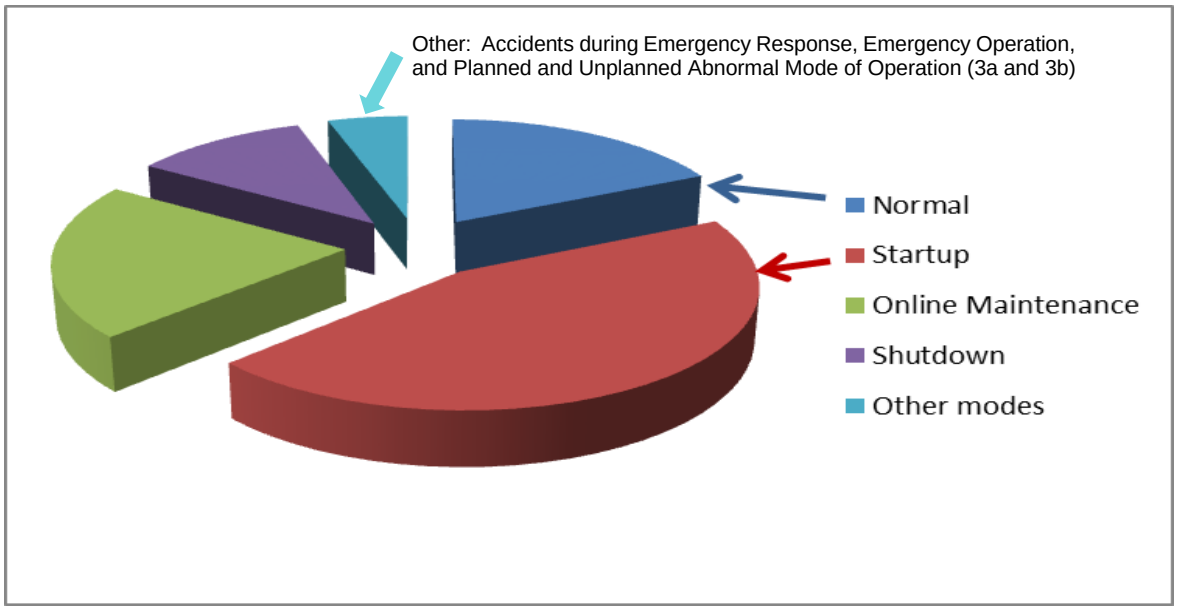

Figure 1: Distribution by Operating Mode of Major Process Safety Accidents[20]

Most of Mode 3 activities arise during deviations and failures during Mode 1 (normal operating mode) which directly take us to a Mode 3a or 3b activity (or directly to a Mode 4 or 5 activity). The best sites can and normally in fact do a great job of developing Mode 3a procedures with the associated plans and drill. Unfortunately, it appears most sites are not doing a good job in controlling Mode 2, 3b, or 4 activities. This is not because of (only) a lack of regulation… this is because of many factors.

PII (and likely others) provide courses on identifying procedures and developing procedures for Mode 2, Mode 3a, and Modes 4, 5, 6. And in PII's management of change (MOC) courses, how to plan for Emergency-MOC (Mode 3b activities) is covered. All of industry struggles with Mode 3b modes of operation. But fortunately, if Modes 2, 3a, 4, 5, are 6 are clearly planned and if there are sufficient IPLs in place for deviations from these procedures, which are predicted during PHA of the deviations from these procedures (which 80% of the industry is ***NOT*** doing), then the remaining number of Mode 3b scenarios becomes pretty small; about 1% of the major process safety accidents.

The more we learn and brainstorm and predict, the more Mode 2 and 3a procedures we will have, and the more the number of residual 3b scenarios (those that are unplanned and un-proceduralized) will shrink.

For Mode 3a scenarios, as mentioned earlier, the paper *Best Practices for Writing Operating Procedures and Trouble-Shooting Guides* [Bridges & Tew, GCPS, 2017][6] provides excellent guidance on planning for and writing the TSG for each predicted deviation. And further, the paper *LOPA and Human Reliability – Human Errors and Human IPLs (Updated)* [Bridges & Clark, GCPS, 2011][4] and the follow-on paper *Proven*

Approaches to Ensuring Operators Can Respond to Critical Process Deviations in Time (Human Response IPL) [Bridges, GCPS, 2017][5] show how the best companies implement effective systems to control accidents during Mode 3b. These three (3) latest papers build upon papers from 1995 until now on how to develop TSGs and approaches to get operators trained and drilled on responding to critical deviation alarms, and when to fallback to Mode 4 & 5 activities.

The next three pages provide examples of the procedure styles associated with Mode 2, 4, 5, 6 operations (Figure 2) and Mode 3a (TSGs) (Figure 3). Mode 1 does not have procedures but rather just has "shift orders" and "operator rounds and logs".

Section 5 of this paper provides focus on Mode 3b. But first, Section 4 will recap some key points related to human error probability for the other modes of operation. Again, the reader should review Appendix A for a listing of all human factors and multiplication factors in error rates, if the human factor is not optimized.

4. Aside: Human Error Probability for a Single Execution of a Rule-Based Task *(the Tasks is Planned and Proceduralized)*

To calculate the probability of human error (P_{HUMi}), the type of tasks must be defined and the baseline error rate for such a task needs to be established. Note that with excellent control of all of the human factors, a company can begin to approach the lower limits that have been observed for human error, but individual, specific human error probabilities may average about $P_{HUMi} = 0.01$. In some applications, such as maintaining SIL 2 and SIL 3 SIFs, $P_{HUMi} = 0.01$ is a large probability and it is critical in such applications to provide detection and correction for specific human errors.

Excellent control of all human factors means a robust design and implementation of management systems for each human factor are achieved with a high level of operational discipline. The first well-researched publication detailing potential lower limits of human error probability was by Alan Swain and H Guttmann (NUREG-1278, 1983)[8] and by others. However, many times, the limits they referenced get used out of context. The lower limits in NUREG-1278 assume excellent control of human factors, but such excellent control is rarely, if ever achieved. Additionally, some human errors listed by Swain and others were for a single error under highly controlled conditions, or on a "best day" instead of average error probability or rate over an average year of tasks. In general, PII has found it best to use the average error probabilities as discussed in the following section.

Figure 2: Example of Procedure that Follows Best Practice Rules for Operating Modes 2, 4, 5, 6

Unloading Monomer from Tanker to Storage

STEPS	DETAILS
1. Wear standard PPE, plus rubber gloves and full-face organic respirator.	Standard PPE includes hard hat, safety glasses with side shields, and steel-toe shoes.
2. Weigh in the tanker.	Record weight on GROSS line of form.
3. Check bill of lading.	... to verify correct type of material is in tanker.
4. Sign in tanker driver.	Driver must sign in as a visitor and be escorted at all times.
5. Take Certificate of Analysis to QC.	***CAUTION: To avoid contamination, DO NOT unload until you receive approval from QC.***
6. Spot tanker.	A) Direct driver to location. B) Verify brake is set. C) Chock the wheels on at least one side between the two rear axles. D) Ground the tanker (attach grounding strap to an unpainted metal surface).
7. Have the storage area operator make sure the storage tank can hold contents of tanker.	***WARNING:*** *Failure to perform this step can result in an overflow and spill of hazardous Monomer.* Perform **Tank Gauging Procedure (SOP-01-804)** or check the storage tank load cell readout. Storage tank operating limits are stenciled on the control panel.
8. Place 5-psig nitrogen pad on tanker.	A) Connect from local 5-psig nitrogen drop to aft bottom nitrogen connection on tanker. B) Open nitrogen supply valve. C) Then open valve at tanker.
9. Connect Monomer unloading hoses.	A) Verify hoses and gaskets are in good condition. (Hoses are normally stored on hose rack at unloading spot.) B) Connect from tanker to air pump. (Use aft bottom connection on tanker. Remove cap.) C) Connect from air pump to storage tank. (Connect to storage tank line labeled "from TW.")

Figure 3: Example of Trouble-Shooting Guide that Follows Best Practices for Operating Mode 3a

Trouble-Shooting Guide

Alarm or Indicator:	**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 spraying organic waste into the berm.		
Process Area:	FB&D Incinerator; Liquid Organic Liquid Feed	**Oper. Mode:**	Normal
Drawing #s:	D-400-PI-013		

IMMEDIATE ACTION (by system or by operator)

- DCS should shut down the organic feed pump (40-PM-18.445).
- From the DCS display, MAKE SURE the organic feed pump is shutdown.
- HAVE the field operator check for leaks near the organic feed pump.
- IF there is a large leak/release, THEN use the ESD switch to shutdown the unit and then follow/complete the shutdown and isolation procedure, OPS-ESD-117.
- IF there is a minor leak or no leak, THEN:
    - COMPLETE the rest of the trouble-shooting,
    - and DECIDE how to contain the leak for now,

DECIDE IF ALARM is REAL

- From the DCS, CHECK the pressure and feed tank level trends. IF the trends indicate the alarm if valid, THEN continue with finding the cause or fixing or bypassing the problem.

FINDING and FIXING the CAUSE

- CHECK valves upstream of the organic feed pump to see if any are closed too far, including checking ESD valves.
- CHECK, by feel with hand, if the heat tracing is on; IF Not, then TURN ON or open heat trace valves
- MAKE SURE nitrogen to the pump seal is at the normal operating pressure.
- CHECK if the line if plugged or frozen (skill)

Figure 3: Example of Trouble-Shooting Guide that Follows Best Practices (continued)

Trouble-Shooting Guide

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

- CHECK if the line if plugged or frozen (skill)
- CHECK if the level is actually low, use the Organic Feed Tank.
- IF the cause is low level in the feed tank, THEN resolve the problem if necessary based on cause that is found (skill)

FIX or BYPASS PROBLEM

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

END

Error Probability for Rule-Based Actions that are Not Time Dependent (Applies for Modes of operation 1 and 2 only):

Actions that do not have to be accomplished in a specific time frame to be effective are not time dependent; this is the case with Mode 1 and Mode 2 of operation. It should be obvious then that these do not include response to alarms, or similar actions with time limits (Mode 3 are highly time-dependent). Values listed below represent the lower limits for human error rates, assuming excellent control of human factors; these are expressed as the probability of making a mistake on any step:

- 1/100 – process industry; routine tasks performed 1/week to 1/day. This rate assumes excellent control of all human factors. Most places PII visits, the workers and managers and engineers believe this is achievable, but not yet achieved. {Actual data from the Savanah River Site indicated a Miscalibration error probability of 7.0E-3 and a Failure to Restore After Maintenance error probability of 5.1E-3 for an organization with excellent human factors control and data gathering (Table 1[9]). It is noted that these values could be rounded to 1/100. Organizations are cautioned to determine the actual data for human error rates in their own management systems before using human probabilities lower than 1/100.}
- 1/200 – pilots in the airline industry; routine tasks performed multiple times a day with excellent control of human factors. This average has been measured by a few clients in the airline industry, but for obvious reasons they do not like to report this statistic.
- 1/1000 – for a reflex (hard-wired) action, such as either proactive or minor corrective actions while driving a car, or very selective actions each day where your job depends on getting it right each time and where there are error recovery paths (such as clear visual cues) to correct the mistake. *This is about the rate of running a stop sign or stop light, given no one is in front of you at the intersection; the trouble is measuring this error rate, since you would have to recognize (after the fact) that you made the mistake.*

See Bridges and Collazo (GCPS, 2012)[10] for more details on this topic. Also see Appendix A.

Adjusting the lower limit rates to estimate a baseline rate at a site.

As mentioned earlier, the lower limit rates assume excellent control of human factors in the industry mentioned. Note that airline pilots have a lower error rate than what PII has measured in the process industry. This is due, in part, to the much tighter control by the airlines and regulators on factors such as fitness-for-duty (control of fatigue, control of substance abuse, etc.). Excellent control of human factors is not achieved in many organizations; therefore, the human error rates will be higher than the lower limit, perhaps much as much as 20 times higher. Table A1 in Appendix A provides adjustment factors for each human factor. These factors can be used to adjust the lower limit of error rate upward or downward as applicable, but the factors should not be applied independently. For instance, even in the worst situations, we have not seen an error rate for an initiating event or initial maintenance error higher than 1/5, although subsequent steps, given an initial error, can have an error rate approaching 1 due to coupling or dependency.

- 1/5 – highest error rates with poor control of human factors; this high rate is typically due to high fatigue or some other physiological or psychological stress (or combination). This is the upper limit of error rates observed with poor human factors and within the process industry. *The error rates in the Isomerization Unit the day of the accident at BP Texas City Refinery[11] were about this rate. The operators, maintenance staff and supervisors had been working about 30 days straight (no day off) on 12-hour shifts.*

For most applications, assume ***a baseline error rate of 0.02 (1/50) errors per step***, which is about average at the sites PII visited in the past 15 years. This value could be justified based on the fact that most chemical process sites do not control overtime during turnarounds and/or do not have a system for controlling verbal communication using radios and phones. In addition, for critical steps such as re-opening and car-sealing the block valves under a relief valve after the relief valve is returned from maintenance, the error probability is about 0.01 (1/100) to 0.04 (1/15)[12]; plus, the average probability of being in a "fail to function" state at time zero for a relief device is between 0.01 (1/100) and 0.02 (1/50) (Bukowski, 2007-2009)[13, 14, 15]. Both of these tasks have multiple

checks and have procedures (similar to what is done when servicing a SIF and when using bypasses for an SIF) and yet the observed human error probability remains between 0.01 and 0.02.

Error Probability for Response Actions that ARE Time Dependent (Applies for Operating Mode 3a) and that are Planned and Proceduralized.

This is the probability that the correct action will be completed within the time necessary, but after that time, the action will not help (so would be the same result as not doing the task). The probabilities listed below assume that there is a written TSG or similar procedure available to guide the action, and that there is a clear and unambiguous call for action, such as a loud alarm and light.

- 1 to 1/10 - if practiced/drilled once per year and there is not sufficient time to accomplish the response task. *It may get done in time on selected occasions, but you cannot count on there always being sufficient time available.*

- 1/10 - if practiced/drilled once per year and if there is always sufficient time, theoretically, to accomplish the response task. *This error rate assumes excellent human factors related to response actions.*

- 1/100 - if practiced/drilled once per week and there is sufficient time to accomplish response task. *This error rate assumes excellent human factors related to response actions.*

Standard rules (from LOPA) for Human Response to Critical Alarms

Typical rules for allowing credit for a human response to an alarm as an IPL, state that the alarm response be unique, independent, dependable, and auditable. More specifically:

- There must be a clear, unambiguous signal that an abnormal condition is present.
- The alarm cannot be generated from a component of the initiating event failure (i.e., credit cannot be taken for an alarm if failure of the measurement is a part of the initiating event)
- Distinct written procedures outlining required operator response to the alarm must be in place; these are normally in the format of a TSG.
- The response must be in the operator certification training program.
- The certification must have repetition, such as drill once a year, with measurement and recording of error rate and success rate of operators accomplishing the steps of the TSG within about ½ of the overall process safety time that is allocated to the "actual response to the alarm" response.
- There must be sufficient time (5 minutes for full response from the control room or 20 to 40 minutes if responding in the field/plant) to intervene after the alarm and before the consequence is manifested.

This level of rigor had a side-effect of minimizing the implementation of Human Response IPLs. Some believed this was a good thing, as their companies want to try to limit Human

Response IPLs to instances where an automated SIF was impractical or not possible. However, if implemented correctly, Human Response IPLs can be more effective than many other types of IPLs.

5. Controlling Human Error During Surprise Events – those situations we have Not Planned for and for which we do not have written procedures or guides

As a reminder Mode 3b is responding to unexpected events without TSGs or procedures. Currently, this mode of operation is commonly covered in the Emergency-MOC program. This might not be obvious to all process safety practitioners, but for a great many of us "emergency-MOC" is code for "we plan to work outside of the TSGs and other procedures because we are in uncharted territory… at least for now" … that is what most folks in the industry call Emergency-MOC. The risk review that is required for each MOC is performed after the change rather than before. All of us strive to eliminate the need for entering operating Mode 3b or we say we "strive to eliminate the need for emergency MOC," but no-one in any industry has accomplished this goal yet. Industry and regulators need to acknowledge that despite our best efforts, we simply CANNOT predict, plan, and proceduralize every possible event.

> ***Real World Example:*** Following the disaster at the Philips polyethylene plants in Pasadena, TX, in 1989, Phillips entered into a settlement agreement with US OSHA to follow all best practices in process safety, including all of the planned requirements in the OSHA PSM standard (still two years away from issuing as a regulation). To be proactive in a meeting with OSHA staff and plant staff, Phillips legal staff announced Emergency-MOCs would no longer be allowed at Phillips operations (meaning, the company will force a shutdown for every situation that has not been predicted and proceduralized, so as not to either have an involuntary MOC or try to make a better decision in the heat of the moment). Several attendees with many years of operations and process safety experience pushed back and stated that there will be a shutdown every few days to a week if this policy of no "emergency MOC" is implemented. The attorneys for Phillips insisted on the new policy. This is a real-intended stance. However, within 2 months, it was reversed and instead the company started to focus on eliminating as many "unplanned events" as possible by doing greatly improved PHAs of all modes of operation while proceduralizing (and training and drilling on) proper responses to all known deviations from the norm.

Key issues with Mode 3b situations: Because Mode 1, 2, 3a, 4, 5, and 6 operational situations are predicted/expected, they are proceduralized. Even in the case of a TSG — where the exact path and response is variable, based on information gleaned by the operator — the various paths have been thought through beforehand and documented. Thus, the responses to these tasks are developed by subject matter experts. There may be many different responses, and we use our best judgment to select one and use it. In other words, cause and effect are known, subject matter experts (SME) provide options, and then we

pick a good practice. When the need arises, we SENSE the need; Experts ANALYZE; the worker selects the best option and RESPONDs.

In the words of Steven Cutchen[23], each of these modes are Complicated in that they are not obvious but can be analyzed in a straight-forward fashion to establish the proper course of action.

Real World Examples:

- Making a cheesecake is Complicated. One SME may say use a box mix. Your grandmother, certainly an SME, may have her scratch recipe, and show you how the crust is supposed to feel when the moisture is correct.

- A debottleneck project is Complicated. Different contractors may propose different processes. You pick one, maybe not the cheapest.

In contrast to the above modes, operating Mode 3b situations are unanticipated and they are not proceduralized because they are unpredicted. Cause and effect are not discernible ahead of time and it may not even be possible to create a procedure after such a situation. This makes 3b situations extra Stressful and in the words of Steven Cutchen[23], Complex (i.e., situations in which we cannot accurately predict the outcome by traditional means).

Approaches to Handling Mode 3b Situation:

1. First, the company/site needs to optimize the human factors that govern all modes of operation, include 3b Mode. See Appendix A and the related papers on human factors at this conference[16, 17] and prior conferences[10, 18, 19]. This ensures that that contributing factors such as worker fatigue and verbal miscommunication on radios and phones will not exacerbate the already Complex and Stressful situation.

2. Teach your staff that the organization has made great efforts to predict all situations and have written plans in place for abnormal situations, and that any deviation from pre-planned approaches should follow the established MOC system, which ensures the hazards for a change or new situation is analyzed well before making the change. HOWEVER, also admit and stress that an unknown situation can occur and when it does, the workers (or selected staff) have the authority to:

    a. SHUT DOWN the process

    b. SAFE PARK the process, … or if deemed safer,

    c. CONTINUE TO OPERATE TEMPORARILY (emergency MOC territory) in a mode or method that is currently not documented.

    The site must clearly designate who has this authority for decision making during 3b Modes of operation.

3. Set Constraints and General Guidelines on when to force a shutdown to make that decision more comfortable in an unexpected, unpredicted situation. Note that it may seem best to immediately shut down anytime the process deviates into the unknown. But what if the staff believe a safe shutdown cannot be achieved? Or that following the approved shutdown procedures will not function well in this situation? Or that shutting down is less safe than switching to a unique way to operate temporarily? In such situations, taking away the flexibility to exercise initiative may cause more harm.

4. Brainstorm with those staff at the highest expertise level how to **experiment, test,** or **probe** for ways out of the situation, while maintaining options to fully and immediately shut the process or kill the reaction (last fallbacks). This can and should happen ahead of time using scenarios that had been unknown until a surprise happened. This can also be used in real time for a new unknown event. With each **experiment**, we **sense or perceive** what is working and what is not. Then we **respond** based on what we have learned and prepare for the next step or next probe or finally exit to a known procedure (exit the 3b mode of operation). Tabletop drills are similar in nature, but with those we normally have a known scenario to deal with. But the more times we exercise our minds on how to deal with the unknown situations, the better our real-time "probe and learn" becomes.

   During the true 3b scenario, the problem is changing, and the solution is emerging. We rely on our experiences and on our education and knowledge. To be most successful, we rely on the experiences of others as well. We collaborate. Staff can learn to approach new problems, using these steps.

   - We troubleshoot (if within the bounds of a TSG; a 3a situation)

   - When the need arises (3b situation), we EXPERIMENT within constraints and guidelines. We then SENSE the response to develop our learning. Finally, we RESPOND with our learning to inform the next PROBE.

   Real World Example:

   - Driving through East Tennessee you will go through many different terrains. The headlights reach 200 feet or so ahead. The precise circumstances of the drive make a procedure unworkable. Yet, the drive is made without difficulty. This is because of experience and the constant practice of making changes and sensing the response and learning what works and doesn't work.

   Real World Example Where Initiative was Used Out of Order:

   - A senior operator at a petrochemical plant in Saudi Arabia using newly developed chemistry for unique products ended up in a runaway reaction situation. The runaway was both unsafe (more unsafe than the operator likely realized) and a shutdown following the procedure was not quick enough and yet a trip of the reactor using the pre-design "big red button trip" would lead to days of cleanout of polymer buildup in the reactor. The worker did not probe

in this case, but instead forced a trip of the hydrogen feed control valve by putting a related controller in a mode that fooled one of the reactor isolation valves to close out-of-sequence (the operator did not have a remote close button for that specific isolation valve), which then cascaded to close all other isolation valves, but in a different sequence than designed. This stopped the unsafe runaway reaction while also preventing nearly all of the polymer build that would have otherwise resulted. This is technically not a 3b event, as the operations staff had "brainstormed and pre-planned" this approach to shutting the reactor down in a "better" way. The main issue in this example is that management and engineering staff were not receptive enough to New Ideas or possible improvements to the design unless such ideas came from a PHA team or Investigation team. So, in preparing for 3b events, each operation should work hard to listen to the plant staff and their ideas and to brainstorm with them on "better ways to make cheesecake." This will reduce the number of 3b scenarios and allow the company to make such improvements ahead of time.

What's Next:

Once a 3b event has occurred and you have learned the best approach, by all means try to proceduralize this in a step-by-step fashion, or in a guideline (TSG) fashion. If necessary and possible, develop a hardware or instrumented solution to the problem (as done in the last example above). The goal at most companies is to shrink the number of 3b types by converting them into 3a or 2 modes. For many Complex problems, having seen the event, it is now known and can be accommodated - designed around and proceduralized. But this can inadvertently create another problem. Other complex situations of 3b nature are inevitably on the way. Many of the remedy tasks cannot be proceduralized even after the fact. So, the structured approach listed above is necessary in most processes. And this concept, along with others, are missing from US PSM regulations and are not documented well in current guidelines from AIChE, API, AFPM, etc.

Note that Steve Cutchen, formerly of the US CSB, presented an excellent paper at the 16th GCPS, online, in August 2020, that described an approach labeled Safety-II[21]; this approach was started in Europe and is finding some acceptance there. This approach is like the one outlined above, and the author borrowed some of the phrasing for some of the points above from e-mail correspondence with Mr. Cutchen[7]. The reader is encouraged to research the Safety-II approach further.

6. Conclusions

The industry understands and controls the risk of accidents during all modes of operation; with a range of success from excellent control to not-so-good. One mode of operation has not gotten much attention – how to handle unplanned situations (unanticipated and un-proceduralized mode of operation). Most abnormal situations are "anticipated" and therefore planned for with hardware remedies or procedure-based remedies. If a site does an excellent job of predicting accident scenarios and controlling these, then what is left is less than 1% of major process safety accidents occurring from totally unforeseen causes.

This is good, since the chemical-related industry has not developed a standardized approach on how to handle the scenarios "they don't know about." Merely labeling them as black swan events and throwing our hands up when they occur is not best (after all, black swans are not really that rare in nature).

This paper laid out the background to understand what can be predicted and proceduralized, and also provides a framework for what to do with the scenarios we have not predicted.

We KNOW there will be unexpected and even unpredicted scenarios… that is but the first step in not being caught completely off guard. For these events, we need to develop "approaches for recognizing and handling" the unknown scenarios in a rational way. The industry needs more cohesion on such approaches.

7. References

1. Bridges, W., and Williams, T., *Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide within a Chemical Company*, International Conference and Workshop on Risk Analysis in Process Safety, October 21–24, 1997, Atlanta, GA, pp. 13–28. American Institute of Chemical Engineers. New York, NY. 1997.

2. Bridges, W., and Williams, T., Risk Acceptance Criteria and Risk Judgment Tools Applied Worldwide within a Chemical Company, International Conference and Workshop on Risk Analysis in Process Safety, October 21–24, 1997, Atlanta, GA, pp. 13–28. American Institute of Chemical Engineers. New York, NY. 1997.

3. Dowell, A., Layer of Protection Analysis: A New PHA Tool, After HAZOP, Before Fault Tree, International Conference and Workshop on Risk Analysis in Process Safety, October 21–24, 1997, Atlanta, GA, pp. 13–28. American Institute of Chemical Engineers. New York, NY. 1997.

4. Bridges, W., and Clark, T.,, *LOPA and Human Reliability – Human Errors and Human IPLs (Updated)*, 7th GCPS, AIChE, March 2011.

5. Bridges, W., *Proven Approaches to Ensuring Operators Can Respond to Critical Process Deviations in Time (Human Response IPL)*, 13th GCPS, AIChE, March 2017.

6. Bridges, W., and Tew, R., Best Practices for Writing Operating Procedures and Trouble-shooting Guides, 13th GCPS, AIChE, March 2017.

7. Cutchen, Steve "Re: I'll be making two presentations at the 2020 GCPS Virtual Conference - August 20." Message to William Bridges. 28 August 2020. E-Mail.

8. Swain, A. D., Guttmann, H. E., *The Human Reliability Handbook - with Emphasis on Nuclear Power Plant Applications*; NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Division of Facility Operations, 1983.

9. Savanah River PSV failure rate data *(see Reference 13, 14, 15)*

10. Bridges, W., and Collazo-Ramos, G., *Human Factors and their Optimization*, 8th GCPS, AIChE, April 2012

11. US Chemical Safety and Hazard Investigation Board (CSB), *Anatomy of a Disaster: Explosion at BP Texas City Refinery*, published 2006.

12. Dowell, A., and Bridges, W., *More Issues with LOPA - from the Originators*, 11th GCPS, AIChE, April 2015

13. Bukowski, Julia V. and Goble, William M., Villanova University, *Analysis of Pressure Relief Valve Proof Test Data*, Process Safety Progress, AICHE, March 2009.

14. Bukowski, Julia V. and Goble, William M., Villanova University, *Analysis of Pressure Relief Valve Proof Test Data: Findings and Implications*, 10th Plant Process Safety

15. Bukowski, Julia V., *Results of Statistical Analysis of Pressure Relief Valve Proof Test Data Designed to Validate a Mechanical Parts Failure Database*, Technical Report, September, exida, Sellersville, PA, 2007.

16. Bridges, W., and Rhodes, W., *Human Factors Missing from Process Safety Management (PSM) Systems*, 17th GCPS, AIChE, April 2021

17. Bridges, W., and Rhodes, W., *Human Factors Implementation – for Plant Workers*, 17th GCPS, AIChE, April 2021

18. Bridges, W., and Tew, R., *Human Factors Elements Missing from Process Safety Management (PSM)*, 6th GCPS, AIChE, March 2010

19. Bridges, W. and Rhodes, W., *Everything you need to Know about Human Reliability and Process Safety*, 17th GCPS, AIChE, March 2019

20. Bridges, W., *LOPA and Human Reliability – Human Errors and Human IPLs*, 6th GCPS, AIChE, March 2010

21. Cutchen, S., *Safety-II — Resilience In The Face Of Abnormal Operation*, 16th GCPS, AIChE, August 2020.

22. Gertman, D.; Blackman, H.; Marble, J.; Byers, J. and Smith, C.; *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005.

23. Cutchen, S., *Operational Discipline is not Follow the Procedure*, 16th GCPS, AIChE, August 2020.

Appendix A: Overview of Human Error and Human Factors

Experts typically quote that about 85% of accidents are caused by human error, though some say that except for natural disasters this figure is 100%. However, simply attributing these incidents to "human error" without evaluating the root cause implies that the errors are inevitable, unforeseeable, and uncontrollable. Nothing could be further from the truth.

Human errors are sometimes mistakenly called procedural errors. This is not true any more than saying all equipment errors are due to design errors. People make mistakes for many reasons, but PII estimates that only about 10% of accidents due to human errors in the workplace occur because of *personal* influences, such as emotional state, health, or carelessness; most human error is due to weaknesses in the control of human factors. Over the many decades of industry research and observation in the workplace on human error, industry has come to know that human error probability depends on many factors. These factors (described in more detail in *Human Factors Missing from PSM* [18]) include those shown below (note that the percentages shown below were developed by PII after analysis of more than 15,000 process safety, safety, and operational incidents):

- Procedure accuracy and clarity (the most cited root cause of accidents):
    - A procedure typically needs to be 95% or better accuracy to help reduce human error; humans tend to compensate for the remaining 5% inaccuracies in a written procedure.
    - A procedure must clearly convey the information and the procedure should be convenient to use.
    - Checklist features – These should be used and enforced either in the procedure or in a supplemental document.
- Training, knowledge, and skills
    - Employees should be selected with the necessary skills before being hired or assigned to a department.
    - Initial Training – There must be effective training. The initial training should be demonstration-based training on each proactive task and each reactive (e.g., response to alarm) task.
    - Ongoing validation of human action is needed and usually should be repeated (in either actual performance or in drills/practice) at least once per year. For human IPLs or safeguards, the action should be demonstrated to be “fast enough” as well.
    - Documentation – the human performance should be documented and retained to demonstrate the error rates chosen are valid.
- Fitness for Duty – Includes control of many sub-factors such as fatigue (a factor in a great many accidents), stress, illness and medications, and substance abuse.
- Workload management – Too little workload and the employee becomes bored (reducing alertness, increasing distractions), while too much overwhelms the employee (increasing stress, decreasing time per task); both cases can increase human error.
- Communication – Miscommunication (of an instruction or set of instructions or of the status of a process) is the second or third most common cause of human error in the workplace. There are proven management systems for controlling communication errors (such as repeat back, use of common jargon).
- Work environment – Factors to optimize include lighting, noise, temperature, humidity, ventilation, and distractions.

- Human System Interface – Factors to control include layout of equipment, displays, controls and their integration to displays, alarm nature and control of alarm overload, labeling, color-coding, error-proofing measures, etc.
- Task complexity – Complexity of a task or job is proportional to the (1) number of choices available for making a wrong selection of similar items (such as number of similar switches, number of similar valves, number of similar size and shaped cans), (2) number of parallel tasks that may distract the worker from the task at hand (leading to either an initiating event or failure of a protection layer), (3) number of individuals involved in the task, and (4) judgment or calculation/interpolation, if required. For most chemical process environments, task complexity is typically low (one action per step), but for response actions (human IPLs) there are almost always other tasks underway when the out-of-bounds reading occurs or the alarm is activated.

In addition to the human factors listed, other considerations for use of a human as an IPL include (1) time available to perform the action and (2) physical capability to perform the action safely.

Other papers provide much more detail on each human factor and the relative weighting of each.[10, 18, 19]

These human-error causes (human factors), which in turn result from other human errors, are all directly within management's control. When using human error data for controlling initiating events (IEs) and independent protection layers (IPLs), the site should ensure that the factors above are consistently controlled over the long-term and that they are controlled to the same degree during the mode of operation that the PHA, HAZOP, What-if, FMEA, or LOPA covers. For instance, if workers are fatigued following many extra hours of work in a two-week period leading up to restart of a process, then the human error rates can increase by a factor of 10 times or 20 times during startup.[4]

Human Factor Categories and Typical Impact of Each

To minimize human error, process safety systems should address the **Human Factors Categories** (see various US NRC and US DOE standards from 1980s and 1990s)[8, 22]. Table A1 on the next page lists the key human factor categories along with multiplication factors that poor human factors can have on the base human error rates.

Table A1. SUMMARY TABLE of 10 HUMAN FACTOR CATEGORIES

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[22]. 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 for Cognitive & Diagnosis Errors
Available Time (includes staffing Issues) – ***for responses only***	Inadequate time Barely adequate time (≈2/3 x nominal) Nominal time (1x what is expected) Extra time (at least 2x nominal and >20 min) Expansive time (> 4 x nominal and > 20 min)	P(failure)=100% 10 1 0.1 0.01
Stress/Stressors	Extreme (threat stress)	5
(includes staffing issues)	High (time pressures such as during a maintenance outage; issues at home, etc.)	2
	Nominal	1
Complexity & Task Design	Highly complex	5
	Moderately complex (requires more than one staff)	2
	Nominal	1
	Obvious diagnosis	0.2
Experience/Training	Low	10
	Nominal	1
	High	0.5
Procedures	Not available in the field as a reference, but should be	20
	Incomplete; missing this task or these steps	8
	Available and >90% accurate, but does not follow format rules (normal value for process industry)	3
	Good, 95% accurate, follows >90% of format rules	1
	Diagnostic/symptom oriented	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 (high fatigue level (>80 hr/wk or >20 hr/day, no day off in 7-day period; or illness, etc.)	20
	Highly degraded fitness (high fatigue such as >15 hr/day, illness, injury, etc.)	10
	Degraded Fitness (>12 hr day and >72 hr/wk)	5
	Slight fatigue (>8 hr per day; ***normal value for process*** industry)	2
	Nominal	1
Work Processes & Supervision	Poor	2
	Nominal	1
	Good	0.8
Work Environment	Extreme	5
	Good	1
Communication	No communication or system interference/damage	10
	No standard for verbal communication rules ***(normal*** value for process industry)	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 Section 4 of 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 procedures-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.