SECTION D: PROCESS HAZARD ANALYSIS/ACTION ITEMS AND SAFEGUARD PROTECTION ANALYSIS

D.1 PROCESS HAZARD ANALYSIS

ISO Section 450-8.016(d) and RISO Chapter 6.43.090(d) require Stationary Sources to conduct a process hazard analysis (PHA) on each covered process at their Stationary Source. The PHA and PHA revalidations should be conducted in conformance with Sections 5100.2 and 5110.4 of the CalARP program regulations, whichever is applicable, and Section 7.3 of the *Contra Costa County CalARP Program Guidance Document,* except in assessing whether seismic events must be considered. The Stationary Source must complete recommended actions from PHA's and PHA revalidations within one year from completing the PHA. If a process shutdown is required, the recommended actions must be completed during the first regularly scheduled turnaround of the applicable process subsequent to the 1-year completion time frame. With the exception of Security and Vulnerability Assessments, other studies and analyses related to the PHA (external events such as seismic, facility siting for a process unit, and other studies such as evaluations for latent conditions, human factors, inherently safer systems, etc.), are subject to the same 1-year completion time frame for any action items/recommendations developed as a result of these studies or analyses, unless a turnaround is required. Stationary Sources must send Contra Costa Health Hazardous Materials Program (CCHHMP) a request for extension prior to the due date for any PHA action items (including other studies and analyses related to the PHA) that cannot be addressed within 1 year and a turnaround is not required. Note: This chapter is intended to work with Section B Chapter 4 and Section H in this guidance.

As part of an external events analysis of PHAs, the risks from seismic events must be evaluated (i.e., a seismic assessment must be conducted) if the covered process (as defined in ISO Section 450-8.014(a) and RISO Chapter 6.43.090(b)) contains a regulated substance (as defined in Section 5050.3(ss) of the CalARP program regulations) and the distance to the nearest public receptor for a worst-case release scenario[1] is within the distance to the toxic or flammable endpoint (i.e., Program 3 covered process).[2] The seismic assessment should be conducted in accordance with Section 7.3.4 and Appendix B of the *Contra Costa County CalARP Program Guidance Document.* In addition, CCHHMP recommends that a post-seismic event facility inspection protocol be established and implemented that would require the inspection of the structural integrity of the equipment after a significant seismic event in the area. Documentation of such inspection should be maintained for the PHA team to review.

Additionally, County Ordinance Code Chapter 450-8, Section 450-8.016(j) requires the following for PHAs.

D.1.1 PHA PROGRAM REQUIREMENTS

Each stationary source must develop a PHA program that meets all the requirements in the regulation. The PHA study must be appropriate to the complexity of each process for all processes covered by the regulation. A PHA is a method for identifying, evaluating, and controlling existing or potential hazards associated with each process and is an integral and core element of any prevention program. The stationary source may use several different techniques listed in section D.1.2 for conducting a PHA; however, the technique selected must be appropriate to the complexity of the process and well-suited for determining and evaluating the hazards of each process. It should be noted that CalARP regulations require that stationary sources work with CCHHMP in selecting and using the appropriate PHA methodology.

PHAs must be revalidated at least every 5 years.

All process hazard analyses shall be performed by a team with expertise in engineering and process operations, and the team shall include at least one employee who has experience and knowledge specific to the process being evaluated. Also, one member of the team must be knowledgeable in the specific PHA methodology being used.

ISO Section 450.016(b)(1)(A) and RISO Section 6.43.090(b) requires that human factors be included in the process hazard analysis process, which is described in Sections B.4 and D 1.4.

ISO Section 450.016(a)(3)(B) and RISO Section 6.43.090(a)(3) requires the stationary source to consult with employees and their representative on the conduct and development of the process hazard analysis program.

D.1.2 PHA METHODS

A PHA is a qualitative approach for identifying existing or potential hazards, generating credible accident scenarios and their consequences, evaluating the severity and consequences of those hazards, and listing existing safeguards. The PHA method chosen must be appropriate for the complexity of the process. The methodologies are the following:

1. **What-If**: a brainstorming approach in which a team familiar with the process asks questions about possible deviations from the standard design, operating procedures, maintenance or equipment failures within the process. These questions are usually worded as "What if" questions. For example, "What if the pump fails?"

2. **Checklist**: a list that contains information on specific items of process design, construction, maintenance, and operation (such as process covered by standards, codes, and industry practices) and provides a means for standardized evaluation of plant hazards. Checklists can be generated using existing industry standards; however, they must be tailored to fit your specific process. This method may be more appropriate for simple processes with limited change (ex. aboveground storage tanks).

3. **What-If/Checklist**: a technique that combines the systematic approach of the checklist with the brainstorming approach of a "What-If" analysis.

4. **Hazard and Operability Study (HAZOP)**: a study conducted by a team that systematically identifies hazards and operability problems by searching for deviations from

the design intent of each section or node of the process. The team considers the causes and consequences of these deviations to generate potential hazards, generate credible accident scenarios and their related consequences, and list existing safeguards. The team then considers possible risk reduction alternatives.

5. **Failure Mode and Effects Analysis (FMEA)**: a qualitative approach of tabulating system/plant equipment, their failure modes, and each failure mode's effect on the system/plant. A failure mode is a description of how equipment fails. The consequences of these failures are analyzed to identify each failure's potential hazards, generate credible accident scenarios and their consequences, list existing safeguards, and generate possible risk reduction alternatives.

6. **Fault Tree Analysis (FTA)**: a deductive technique that focuses on one particular accident or final event and provides a method for determining the causes of the event. The fault tree is a graphic model that displays the various combinations of equipment failures and faults that can result in the final event. The probability of each event can be calculated using the estimated probabilities of each event path leading to the final event.

Other PHA methods recognized by engineering organizations or governmental agencies may also be used. The ISO and RISO regulations require that stationary sources work with CCHHMP in selecting and using the appropriate PHA methodology. Consult with CCHHMP regarding PHA methods chosen for analysis. Regardless of which method is chosen, the ISO and RISO regulations require at least one person on the PHA team who is qualified and trained in the methodology. Training on such methodologies is available from several professional organizations and private companies.

It should be noted that it may be beneficial to supplement one PHA methodology with another method to provide a robust analysis of the process. It is typical for the HAZOP method to be augmented with the checklist method and utilize checklists to analyze specific hazards.

D.1.3 FACILITY SITING

During the PHA, regardless of the PHA methodology used, facility siting must be addressed. Many facilities utilize a checklist to address this requirement. Facility siting is the spatial relationship between process hazards, the presence of people in the area, including control rooms and occupied buildings, the location of equipment, including the accessibility of equipment for maintenance and operators; and the location of PPE and emergency response equipment. The facility siting evaluation should also consider the availability and accessibility of emergency response equipment along with the suitability of evacuation routes during an emergency. There are standards for placement and construction of occupied buildings (permanent and temporary) depending on the blast and toxic release potential. The 2005 BP Texas City accident fatalities brought into focus the catastrophic result of incomplete consideration in the placement of temporary trailers in process areas. API has published guidance for permanent (RP 752) and portable buildings (RP 753), and tents (RP 756). Pressure reliefs and de-pressurizing systems should be located in accordance with API-RP 521. The facility should review electrical area classification maps to ensure equipment is suitable for the area classification established following *NFPA 497*, *API RP500*, or *API RP505.*

According to the API recommended practices, each site should conduct a separate standalone comprehensive facility siting study. This study will review the stationary source as a whole with an evaluation of the hazards from the process streams, temperatures/pressures, and congestion of the process area in relation to the location of structures that house personnel. Each PHA should review this study as part of addressing facility siting. If the site utilizes this approach, more global facility siting issues can be addressed from the recommendations of a more comprehensive study. This type of study is completed every five years.

D.1.4 HUMAN FACTORS

During the PHA, regardless of the PHA methodology used, human factors must be addressed. Many facilities utilize a checklist to address this requirement. Attachment A: Latent Conditions Checklist, contains human factors related questions that may be used to evaluate human factors during the PHA. The use of a Latent Conditions Checklist is further described in Section B.4. The consideration of human factors is to evaluate machines, operations, and the work environment to match human capabilities, limitations, and needs. It is the environmental, organizational, job factors, human and individual characteristics that influence human behavior at work. The PHA setting serves to assess situations or conditions that can affect the work environment's health and safety. It is important to note that humans may be called upon to address an adverse situation by correcting or mitigating a hazard and may exacerbate the situation if the process controls, procedures, analyses, etc., do not properly take the human factors element into account consideration. Recognizing and understanding individuals' performance is necessary to adequately assess the potential risk of the process under study.

D.1.5 EXTERNAL EVENTS

During the PHA, regardless of the PHA methodology used, external events, including seismic events, must be addressed. Many facilities utilize a checklist to address this requirement. Other types of external events should also be examined if the stationary source is in an area subject to that type of event, including but not limited to tornadoes, high winds, tsunami, or floods. The facility could use FEMA national risk index to identify natural hazards. The process should be examined to determine if it would withstand these natural events while maintaining primary containment of the highly hazardous material. The potential impacts of lightning strikes and power failures should also be considered. The potential for terrorist attacks or sabotage from internal or external sources; is more appropriately evaluated in a Security Vulnerability Analysis (SVA).

If vehicles (including rail accidents) could impact the process, it should be examined for the consequences of such impacts. Fires adjacent to the process should also be evaluated. For example, if there is a propane tank and an ammonia tank in close proximity to each other, the impact of the fire at the propane tank could impact the ammonia tank. This analysis would include evaluating potential flame impingement.

A site may choose to perform a separate standalone seismic study of a process that is conducted every 5 years. If this is the case, the PHA team should review this study during the PHA.

D.1.6 COMPLETION OF RECOMMENDED ACTION ITEMS

Stationary Sources must document the decision made to implement or not implement all process hazard analysis recommended action items and the results of recommendations for additional study. This documentation must include the justification for not implementing any recommended actions. Federal OSHA provided guidance for justifiably declining recommendations from incident investigations in the September 1994, OSHA Instruction CPL 2-2.45A CH-1. These criteria have since been applied to recommendations formulated during PHA's. CCHHMP encourages Stationary Sources to consider the impact on surrounding communities when declining recommendations.

- The analysis upon which the recommendation is based contains material factual errors
- The recommendation is not necessary to protect the health and safety of the employer's own employees, or the employees of contractors
- An alternative measure would provide a sufficient level of protection
- The recommendation is infeasible

Cal/OSHA issued the following clarification in Part 4 of the June 1994 Process Safety Management Guidelines. "…Cal/OSHA's intent is that an employer is required to implement the teams' findings and recommendations except to the extent that an employer can document that an alternative will be at least as effective or efficient in addressing the safety concerns that are the subject of those findings and recommendations".

The Stationary Source must complete the recommended actions selected for implementation, including those formulated during PHA, as follows:

- All actions not requiring a process shutdown must be completed within one year after completion of the PHA unless the Stationary Source demonstrates to the satisfaction of CCHHMP that within one year is infeasible
- All actions requiring a process shutdown shall be completed during the first regularly scheduled turnaround of the applicable process subsequent to one year after submittal of the Safety Plan or after completion of the PHA unless the Stationary Source demonstrates to the satisfaction of CCHHMP that such a schedule is infeasible
- Stationary Sources must send CCHHMP a request for extension (e.g., PHA variance request) before PHA actions (including other studies and analysis related to the PHA) become overdue when they cannot be addressed within 1 year and a turnaround is not applicable. Stationary Sources should send CCHHMP the request

for extension at least 30 days prior to the due date for PHA action items (including other studies and analyses related to the PHA) that cannot be addressed within 1 year and a turnaround is not required.

Examples of situations where the schedule may be infeasible include procuring customized equipment requiring a long lead time for fabrication and delivery, complex projects requiring significant front-end engineering, facilities that require substantial time to construct or implementing a recommended action that requires the application of a local air district permit to construct or county land use permit and its requirements (a CEQA analysis may be conducted.) The Stationary Source must demonstrate that they initiated the land use permit process in a timely manner.

The Stationary Source must retain documentation of closure and any associated justification of actions identified by the process hazard analysis. CCHHMP interprets "actions" to include, but not be limited to, all recommendations made for changes to physical equipment and procedures and additional studies and information. Actions related to operating procedures should be completed as soon as practicable. The Stationary Source must also retain documentation of communication to operating, maintenance, and other employees whose work assignments are in the process and who may be affected by the recommendations or actions.

D.2 SECURITY AND VULNERABILITY ASSESSMENT

Also, as part of PHAs, and as required in Section 450-8.016(g), Stationary Sources are required to complete a Security and Vulnerability Assessment (SVA) as defined in Section 7.3.4 of the *Contra Costa County CalARP Program Guidance Document*, by June 30, 2007, and at least once every five years after the initial assessment, or as prescribed by federal regulation. For Stationary Sources that are not regulated or required by the Department of Home Land Security (DHS) under the Chemical Facilities Anti-Terrorism Standards (CFATS) or Maritime Transportation Safety Act (MTSA), is required to perform an SVA or revalidations at least every five years per the ISO, the SVA shall include:

- SVA methodology; consult with CCHHMP if using any methodology not listed in this section;
- Intent to perform a 5-year SVA revalidation and description of the method used to perform a revalidation;
- Indication of what mechanism is in place to track and ensure that recommendations are addressed;
- Indication of the criteria for rejecting recommendations; and
- Documentation for assuring that recommendations are properly addressed.

The following SVA assessment methodologies are acceptable to CCHHMP:

- American Institute of Chemical Engineers Center for Chemical Process Safety: Guidelines For Analyzing And Managing The Security Vulnerabilities Of Fixed Chemical Sites;
- Department of Justice – Sandia Labs: Chemical Facility Vulnerability Assessment Methodology;
- Department of Justice – Sandia Labs: Risk Assessment Methodology for Water Systems (RAM-W);
- Synthetic Organic Chemical Manufacturers Association, Inc. (SOCMA): Manual on Chemical Site Security Vulnerability Analysis Methodology and Model;
- Air Products: APCI Security Vulnerability Assessment;
- BASF Security Vulnerability Assessment (SVA) Methodology & Enhanced Security Implementation Management;
- ExxonMobil: Chemical Facilities Safeguards and Security Risk Assessment Methodology;
- Georgia Pacific: Security and Vulnerability Assessment;
- American Petroleum Institute/National Petroleum Refiners Association Security Vulnerability Assessment method. [Contra Costa CalARP Guidance Document Appendix I]; and
- The workshop sponsored by the Water Environment Federation that covers 'Vulnerability Assessment and Security Planning for Medium Drinking Water Utilities' that includes training on how to apply the EPA approved software titled 'VSAT' for developing an SVA for a medium size water treatment plant.

For those Stationary Sources that are required to submit their SVA to the DHS, the responsibility will remain as Federal regulatory oversight. CCHHMP will not include the audit questionnaire for this subject as part of the CalARP/ISO/RISO safety audit. However, as described in section E.7, the Safety Plan shall include a discussion of the SVA performed and the process for resolution of identified issues. Preparation and submittal of DHS Chemical Security Assessment Tool TOP-Screen does not constitute an SVA or an SVA revalidation.

D.3 SAFEGUARD PROTECTION ANALYSIS (SPA)

Each stationary source must develop a Safeguard Protection Analysis (SPA) program that meets all the requirements in the regulation. The regulation requires a Layer of Protection Analysis (LOPA) or an alternative type of analysis approved by the department that uses a quantitative, qualitative, or equivalent semi-quantitative method to determine the effectiveness of existing safeguards and safeguards recommended in a PHA to reduce the probability and/or severity of a catastrophic release. The safeguard protection analysis may be a standalone analysis or incorporated within a PHA.

A SPA is a simplified risk calculation that focuses on reducing the PHA scenario frequency. A SPA can be completed using a variety of techniques. Semi-quantitative techniques typically provide semi-quantified event frequencies, while the consequence severity is rated qualitatively. LOPA is called out in the regulation and is one of the more widely known SPA techniques. If the Stationary Source decides to use a different semi-quantitative technique, the alternative should be demonstrated to be equally effective and approved by CCHHMP prior to implementation. Quantitative techniques, e.g., Quantitative Risk Assessments (QRA), are also acceptable for meeting the SPA requirement.

All safeguard protection analyses must be performed by a team with expertise in engineering and process operations. The team must include at least one employee who has experience and knowledge specific to the safeguards and one member who is knowledgeable about the specific safeguard protection analysis method used.

D.3.1 LOPA

One of the published and widely-used semi-quantitative process risk assessment tools used to determine the effectiveness of the existing engineering and administrative controls (often referred to as safeguards) is the Layer of Protection Analysis (LOPA) methodology. The method uses an order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of IPLs to approximate the risk of a scenario. Risk reductions are proportional to the probability of failure on demand (PFD) and rounded to an order of magnitude. LOPA's rule-based approach in evaluating safeguards makes it more consistent than the qualitative PHA process. However, LOPA is limited to a single cause-consequence pair as a scenario. It is not a comprehensive assessment of all the possible outcomes in an event tree or quantitative analysis. Therefore, it is important to precisely identify the initiating event that led to the undesirable scenario in the PHA. There are times when there are multiple initiating events resulting in the same outcome. It should also be noted that not all initiating events are suitable for analysis by LOPA. If the team identifies that the initiating cause is not suitable for LOPA analysis, another method should be used.

Initiating Event is the beginning of a sequence of events leading to the consequence of concern. An initiating event may be a device failure, system failure, external event, or wrong action (or inaction). The likelihood of occurrence of an initiating event is called *Initiating Event Frequency (IEF)*.

Conditional Modifiers are risk reduction factors that may be justifiably applied to an event likelihood when certain conditions are met. Conditional Modifiers are used to assess the probability that the potential consequence will occur. Some LOPA practices focus on the loss of containment events (i.e., release to the atmosphere), while others focus on the overall endpoint impact (e.g., fatalities). Conditional modifiers are only applicable when the risk is being assessed for the overall endpoint impact. If the stationary source uses Conditional Modifiers during LOPA, then your program should specify when they can be used and if there is a limit on the number of Conditional Modifiers that may be applied during the analysis. The intent of the SPA is to reduce the likelihood of major incidents, so the LOPA should seek to reduce the potential for loss of containment. Conditional modifiers may include the following:

- Probability of a hazardous atmosphere

- Probability of ignition or initiation
- Probability of explosion
- Probability of personnel presence
- Probability of injury or fatality
- Probability of equipment damage or other financial impact

Alternatively, the stationary source may perform the best-estimate of the overall impact while risk ranking and not have to apply conditional modifiers. For example, rather than conservatively assuming that flammable release scenarios will ignite 100% of the time when risk ranking, the stationary source may use CCPS's *Guidelines for Determining the Probability Ignition of a Released Flammable Mass* or a similar process to achieve the best-estimate during the initial risk ranking. Under no circumstances should conditional modifiers be used when the conditions have already been accounted for in the risk criteria.

Conditional modifiers and IPLs are both risk reduction factors, expressed as probabilities, which apply to a specific scenario. IPLs are safeguards that react to or act to control the initiating event. The risk reduction from an IPL is accounted for after any conditional modifiers are applied. Conditional modifiers do not respond to an initiating event but consider the probability that the process is vulnerable to impact when the incident sequence propagates. If the stationary source uses conditional modifiers, they must have supporting evidence that the condition exists to substantiate the risk reduction of the conditional modifier. This means the assumptions must be based on 'hard' data and not rely on expert judgment or experience. Conditional modifiers must be periodically audited to ensure the conditions are valid.

Enabling Conditions are operating conditions that are necessary for an initiating cause to propagate into a hazardous event. Enabling conditions do not independently cause the incident but must be present or active for it to proceed. An example is where the process plant has to be in a specific and often transient state of operation in order for the process deviation to realize the consequence of concern. Most LOPA scenarios are deviations from normal, steady state operation, and so enabling conditions would generally not be used for those scenarios. Enabling conditions may include weather extremes, in which the initiating event scenario can occur "only" under specific conditions. For example, a pipe burst due to water freezing can only occur at specific times of the year. For more information, CCPS has developed *Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis.*

D.3.2 OTHER TECHNIQUES

LOPA is also not an adequate methodology when the frequency of the Initiating Event (IE) is not understood or IPL values are not understood. In these instances, alternative quantitative analysis may be required. There may also be instances when the risk reduction achieved by the LOPA process requires immediate action. This generally occurs during startup and shutdowns because many of the instrumented IPL's are disabled or bypassed. This means that the IPL's during abnormal operations are more reliant on "human-based" IPLs, which may not be independent. Under LOPA rules, the amount of risk reduction credit is limited when they are not independent. This scenario may also be evaluated using quantitative techniques to better understand the hazards. This guide recognizes the QRA as an acceptable SPA method for instances previously described and as follows:

1. The frequency of Initiating Event is not understood
2. IPL and associated values not fully understood
3. Residual risk profile requires immediate action

If the scenario cannot be evaluated using LOPA or QRA techniques, the stationary source should consult with CCHHMP to determine an acceptable method.

D.3.3 SAFEGUARDS AND INDEPENDENT PROTECTION LAYERS (IPL)

Safeguards subject to the SPA rules must be an IPL, which means they are independent from the initiating event and each other. They also need to be effective and auditable. IPL can be a device, a system, or a series of actions that prevent the scenario from proceeding to the undesirable consequence. An IPL can be preventive as well as mitigative. Preventive layers are IPLs that act to prevent the scenario from occurring, such as Operator actions and Safety Instrumented Systems (SIS). Mitigative IPLs reduce the severity of the consequence after it has occurred. Examples of a mitigative IPLs would be tank dikes or fire suppression systems. Below is a partial list of the different types of IPLs:

- **Passive IPLs** - "continuous demand" devices that do not require the **detection** of the initiating event or action by any **person** to reduce the consequence or likelihood of the incident. Characteristically these devices offer high reliability but limited protection. Examples include tank dikes, underground drainage systems, and fireproofing.

- **Active IPLs** - can be either "continuous demand," "high-demand," or "low-demand," which require the **detection** of an *incipient incident* followed by the **activation** of the device. The *active IPL* will prevent an incident from developing or mitigate its consequences**.** Examples of these include SIS, Relief Valves, Basic Process Control Systems (BPCS), Safety Controls, Alarms (with response actions), and Interlocks (SCAI). Note that any BPCS claimed as a safeguard cannot be related to a BPCS that is an initiating cause of the scenario.

- **Safety Instrumented Systems (SIS)** - instrumented IPLs designed in accordance with ANSI/ISA 84.00.01/IEC 61511 and follow the principles in the Technical Reference. An SIS system is a subset of the Active IPLS listed above.

- **Human-Based IPLs** - involve detecting the incipient incident followed by the Operator(s) performing a series of actions or activating devices to prevent the scenario from occurring.

- **Legacy IPLs** - SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance of standards (e.g., ANSI/ISA-84.01-1996). The owner/operator must demonstrate that the equipment is designed, maintained, inspected, tested, and is operating in a safe manner.

NOTE: While all IPLs are safeguards, not all safeguards are IPLs. The Stationary Source may list other safeguards in the SPA; however, they may not take credit for risk reduction unless they are an IPL. The PHA does not require safeguards to be independent of each other; therefore, there will be more safeguards claimed in a PHA than a SPA.

D.3.4 INDEPENDENT PROTECTION LAYER CHARATERISTICS

Independent: The basic premise for independence is that the IPL will function as designed and will not be affected by the initiating event or the failure of another IPL. Secondly, the actuation of the IPL should not be dependent on other devices or systems. Lastly, the SPA methodology should account for common cause failure as this would prohibit the safeguard from acting as an IPL.

Effective (Functionality, Integrity, and Reliability): The IPL must be effective to stop the initiating event from progressing (preventive) or to significantly reduce the consequence of the scenario (mitigative). The IPL must be valid for the mode of operation being analyzed (e.g., startup, shutdown, normal). Note: Often, interlocks are bypassed during portions of startups and shutdowns. They cannot be claimed as safeguards if they are bypassed when a scenario is proposed to occur.

The IPL must be able to actuate, or actions must be executed with sufficient time to prevent the consequence of concern from occurring. The Stationary Source should ensure that the IPL is *timely* by identifying the appropriate IPL Response Time (IRT) and the Process Lag Time (PLT). The IRT for human-based IPL should consider the time for the alarm system to annunciate and the time for the Operator to detect, diagnose, and execute the response steps, followed by the time it takes the process to return the desired process conditions.

When using human-based IPL, the Stationary Source must assess the *human error rate in order* to determine the appropriate IPL probability of failure on demand (PFD). Factors that should be considered are procedure accuracy, procedure clarity, training, operator knowledge, operator skill, fitness for duty (including fatigue), workload management, communication protocols, work environment conditions (e.g., lighting, noise, temperature, access), Human Machine Interface clarity, and job complexity. The CCPS has generally agreed that human response to an abnormal condition within sufficient response time has a PFD of $1.0 - 1 \times 10^{-1}$.

The *integrity* of the IPL is its ability to dependably achieve the required risk reduction against the consequence of concern. For the IPL to be dependable, it must be available when needed and perform as specified within a relatively short period of time. The ability to reveal an IPL failure and correct the failure immediately increases the overall availability of the system to respond. The Stationary Source should have established methods for detecting failures in the IPLs. Failures that are not revealed by diagnostics or by the Operator during normal operation should be detectable by proof testing. These should be corrected as defined by an asset integrity plan.

The *reliability* of the IPL is its ability to perform its function under stated conditions for a specific time period. The concept of reliability is that the IPL will operate as required when required. Moreover, the required reliability is impacted by the expected demand rate on the IPL. There are three demand modes for IPLs, Low Demand Mode, High Demand Mode, and Continuous mode. Low Demand Mode is when the IPL is expected to be challenged less than once per year, whereas high demand mode is expected to be challenged more than once per year. In contrast, the continuous mode failure of the IPL leads to the propagation of the event. Note: it is typical for a safeguard to be included in a maintenance program in order to be claimed as an independent safeguard or IPL.

Auditability: The Stationary Source shall maintain documentation for the life of the IPL to provide evidence that the IPL conforms to the expectations of the original design. Documentation generally includes inspection procedures, validation, and proof testing. Verifying a human-based IPL includes periodic review of procedures, training records for operators, and the actual response time to alarms.

[1] As specified in California Code of Regulations, Title 19, Chapter 4.5, Section 2750.3
[2] As specified in California Code of Regulations, Title 19, Chapter 4.5, Section 2750.2(a)