CONDITIONAL MODIFIERS AND ENABLING EVENTS – SHOULD YOU EVER TRUST THEM?

William Bridges
Process Improvement Institute, part of Trinity Consultants
Tennessee, USA
wbridges@piii.com

Art Dowell, III
Process Improvement Institute, part of Trinity Consultants
Texas, USA
adowell@piii.com

Matias Massello
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

CONDITIONAL MODIFIER AND ENABLING EVENTS - SHOULD YOU EVER TRUST THEM?

Main author

William Bridges – Technical Director
Process Improvement Institute (PII) – part of Trinity Consulting
e-mail: wbridges@piii.com / william.bridges@trinityconsultants.com

Art Dowell – Principal Engineer/Instructor
Process Improvement Institute (PII) – part of Trinity Consulting
e-mail: adowell@piii.com / art.dowell@trinityconsultants.com

Contributing author

Matias Massello –Process Safety Engineer
Process Improvement Institute (PII) – part of Trinity Consulting
e-mail: mmassello@piii.com / matias.massello@trinityconsultants.com

Abstract

The originators of LOPA have always been reluctant to use conditional modifiers (CM), enabling conditions (EC) in LOPA. This is not from lack of experience in LOPA or CM or EC. The hesitation to use these factors is because unlike Independent Protection Layers (IPLs) and Initiating Events (IEs), these extra risk reduction factors cannot be periodically validated and because changes that affect these factors are usually not managed/recognized. Also, many of the factors are not presented with the proper rules to avoid errors. The authors share their experience on when using such factors is appropriate and what the limits of risk reduction are.

Introduction

Layer of Protection Analysis is a simplified form of quantitative risk analysis that uses order-of-magnitude categories for initiating event frequency, consequence severity and probability of failure of independent protection layers (IPLs) to analyze and assess the risk of one or more incident scenarios. LOPA can be useful in the process development, process design, operational, maintenance, modification and decommissioning life cycle phases.

LOPA was developed to help answer questions such as:

- What layers of protection are needed to meet our risk goals?
- How much risk reduction does each layer provide or need to provide?

LOPA can help answer these questions with less time and effort than a full quantitative risk analysis (QRA), although there are instances when use of a complete QRA may be warranted. LOPA is an order-of-magnitude type of quantitative method that builds on qualitative hazard evaluations such as HAZOP Studies. By analyzing selected scenarios in detail, effective application of LOPA can be used to determine whether the risk posed by each analyzed scenario has been reduced to meet a specified risk goal. However, if the analyst or team can make a reasonable risk decision using only qualitative methods, then LOPA may not be warranted. Qualitative hazard evaluation methods such as HAZOP Studies are intended to identify a comprehensive set of incident scenarios and qualitatively analyze those scenarios for the adequacy of safeguards. LOPA is generally used to analyze a subset of incident scenarios.

At times, simple order-of-magnitude LOPAs can be expanded with greater rigor by implementing aspects of a more complete QRA. The use of enabling conditions and conditional modifiers falls into this realm.

An independent protection layer (IPL) is a device, system, or action that is capable of keeping a scenario from proceeding to the undesired loss event, independent of the initiating event or the action of any other layer of protection associated with the scenario. A preventive safeguard meets the requirements of being an IPL when it is designed and managed to achieve the following seven core attributes:

- *Independent* - the performance of a protection layer not being affected by the initiating event or by the actions of other protection layers.
- *Functional* - capable of operating successfully in response to a specific abnormal condition.
- *Integrity* - the risk reduction that can reasonably be expected given the protection layer's design and management.
- *Reliable* - assurance that a protection layer will operate as intended under stated conditions for a specified time period.

- *Validated, maintained, and audited* - implementing, maintaining and verifying information, documents, and procedures that demonstrate the adequacy of and adherence to the design, inspection, maintenance, testing, and operation practices used to achieve the other core attributes
- *Access security* - the use of administrative controls and physical means to reduce the potential for unintentional or unauthorized changes.
- *Management of change* - the formal process used to review, document, and approve modifications that are not replacements in kind, prior to implementation of the modifications.

Clearly, an IPL can be relied upon to provide the associated risk reduction factor. In contrast, enabling conditions and conditional modifiers cannot be relied upon in many instances, as they are not controlled well by management of change and they are not periodically maintained and tested.

Definition and defining characteristics

An **Enabling Condition** (**EC**) is a condition that makes the beginning of a scenario possible. An enabling condition is neither a failure nor a protection layer. It consists of an operation or condition that does not directly cause the scenario, but that must be present or active for the scenario to proceed to a loss event. Note that mitigating factors, such as the probability of personnel presence or of emergency evacuation, are *conditional modifiers* and not enabling conditions. The term *enabling event* is sometimes used for *enabling condition.* The term *enabling condition* is preferred, since enabling conditions are not generally events but rather conditional states.

CAUTION: If taking EC credit for an at-risk time fraction such as a process being in a certain step or making a certain product, the analyst should ask the following question: If the initiating condition occurs when the process is NOT at risk, will the failure be detected before the process next enters the at-risk phase? If the answer is *yes,* the failure will be detected, and an enabling condition probability may be appropriate. If the answer is *no,* then it may be erroneous to consider this an enabling condition, since the failure would only be detected when the consequence of concern occurs. (In this case, it may be an initiating event and not an enabling condition.

One general type of enabling conditions involves the concept of **time at risk.** Time at risk is when an incident sequence may only be realized a certain fraction of the time when conditions are right for the event sequence to progress to a loss event. An underlying assumption for time-at-risk enabling conditions is that *only revealed failures can act as initiating events during time-at-risk conditions.* A *revealed failure* is one that may be immediately or almost immediately apparent through an alarm or indicator system. For example, a primary feed pump failing off during continuous operation of a process would be rapidly apparent by its effects on process parameters when the feed flow is lost.

A **conditional modifier** (**CM**) is one of several possible probabilities included in scenario risk calculations when risk criteria endpoints are expressed in impact terms (e.g., fatalities) instead of in primary loss event terms (e.g., release, vessel rupture). Conditional modifiers include, but are not necessarily limited to probability of a vessel rupture (versus the pressure reached for a scenario) and probability of personnel presence (given the mode of operation, or time available to respond to a process parameter alarm)

Probability of environmental impact would also be a possible conditional modifier. If used, it could follow the same general approaches as probability of injury or fatality and/or probability of equipment damage or other financial impact.

ECs and CMs cannot be relied upon to the same assurance as IPLs, as they are not controlled well by management of change and they are not periodically maintained and tested or validated. The authors, and others recommend NOT using ECs and CMs in LOPA.

CCPS textbook, Guidelines for Enabling Condtions and Condition Modifiers in LOPA

This textbook was proposal around 2010 as a CCPS project. The originators of LOPA, William Bridges and Art Dowell, III, discouraged the use of ECs & CMs because these risk reduction were so often applied wrongly, reducing the risk estimate wrongly. They recommended against development and publication, but many Technical Steering Committee members were using such factors and therefore believed they needed the book. The originators of LOPA recommended that those companies drop the use of ECs & CMs and only rely on features or actions that could be proven in the field or tested, such as improvements to the initiation events (IEF reduction) or improvements of additions of IPLs; along with changing the company's risk tolerance limit to 10^{-4}/yr for multiple fatality or 10^{-3}/yr for a single fatality. The orginators were overruled. William Bridges decided to the join the book writing committee as a contributor, but his main contribution was inserting warnings in the textbook on misuses of specific ECs & CMs. The authors of this paper (the originators) still recommend against wholesale use of ECs & CMs; we only use selected ECs & CMs in selected situations where the specifc EC or CM can be validated in the field. The breakout text boxes in this paper are such warnings that have been extracted from the textbook.

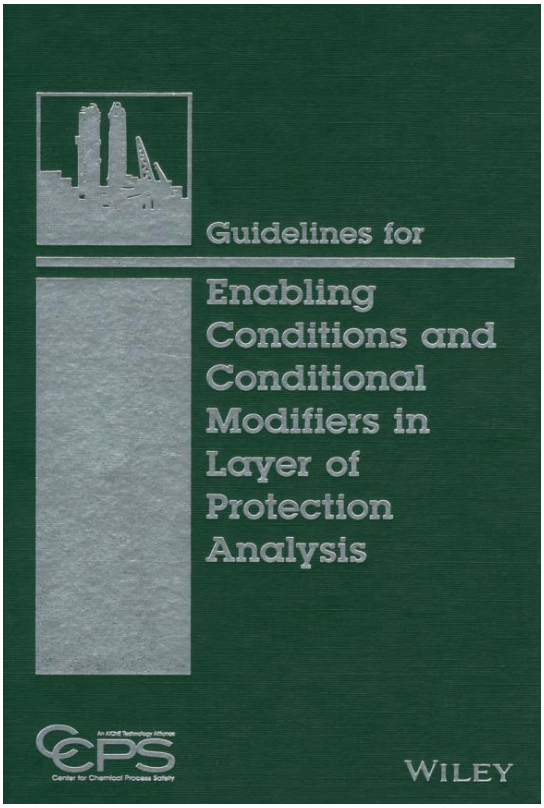

Figure 1. Guidelines for Enabling Conditions and Condition Modifiers in LOPA book cover

Conditional Modifiers (CMs)

This section presents the different types of CMs (Table 1) that are described in this paper, along with a brief description of what each CM is and the challenges for their appropriate use.

Table 1. Types of Conditional Modifiers (CM)

Abbreviation	Conditional Modifier
P_{vr}	Probability of vessel rupture
P_i	Probability of ignition or explosion
P_p	Probability of personnel presence
P_f	Probability of personnel fatality or injury
P_{ha}	Probability of hazardous atmosphere
P_{sd}	Probability of structural damage (from blast, etc.)

LOPA originators (and their organizations) used consequence severity categories based on human harm (e.g., fatality) or property damage (e.g., $MM) or estimates of environmental damage or fines from regulators for environmental harm. Usually, the consequence severity statement includes the EC or CM, so using the reduction factors for the EC or CM would be double-counting. But some companies preferred to use conditional modifiers (CM) to make the description of the scenario clearer. Depending on the endpoint of severity that a company is using, conditional modifiers were needed to account for (1) the probability of vessel rupture (versus the maximum pressure reached in a scenario), (2) the probability of ignition for a flammable release, P_i, (3) the probability of one or more persons present in the danger zone for toxic release or a fire, P_p, and (4) the probability of fatality, P_f, given ignition and given the person(s) is present. (From the perspective of the organization, omitting these conditional probabilities would overestimate the risk.)

When the conditional modifiers P_i, P_p, and P_f are part of the LOPA system, their use should be constrained by the organization's LOPA guidance to ensure consistency. Table 2 to Table 5 provide recommended guidance used by the authors that is reasonably consistent with CCPS guidelines [1], [2], [3].

The originators of LOPA avoid the use of **ECs & CMs** typically by developing consequence severity categories based on the amount of release from a loss of containment and the condition of the release (e.g., below or above the boiling point or above the design pressure of the vessel). These consequence severity categories inherently include the conditional modifiers of P_{vr}, P_i, P_p, and P_f. For LOPA, using P_{vr}, P_i, P_p, and P_f would underestimate the risk. In such cases, some analysts have incorrectly used ECs and CMs (in the worst case to simply force the calculation to meet the risk tolerance criteria for the consequence severity category, even though the ECs and CMs do not legitimately apply.

Probability of Vessel Rupture (P_{vr})

This CM was not addressed specifically in the CCPS CM/EC book, but instead there was a similar concept in the original LOPA book, in an Appendix, where the Consequence was modified based on the multiples over design pressure for the scenario. But this is more correctly stated as a CM with a probability reduction factor based on the multiple of the design pressure that is possible for the scenario, given that all safeguards and IPLs fail.

The probability of a pressure vessel rupture depends on several factors, including the material properties, design standards, safety factors, operating conditions, temperature, and the extent of overpressure relative to the design pressure. There is no universal formula that directly correlates the percentage of overpressure to rupture probability, as it varies by vessel design, material, and all of the factors above.

Key Concepts

1. *Design Pressure (DP)*: The maximum pressure a vessel is designed to withstand safely, incorporating safety factors. Typically, the vessel will have onset of plastic deformation at ambient temperature at 2.5 to 4 times the design pressure, depending on the code, e.g., ASME Boiler and Pressure Vessel

Code, but the vessel is more likely to fail in the 2 to 2.5 DP range due to defects in the metal plate and welds.

2. *Maximum allowable working pressure (MAWP)*: The pressure the vessel can safely handle, given the actual thickness of the metal plate used to fabricate the vessel to meet the design pressure that is specified. Usually a few % above DP.
3. *Maximum allowable working temperature*: Since metals lose strength with increasing temperature, the operating temperature range, and the temperature reached during a PHA scenario (excursion) are critical as that weakens the metal and also adds defects to the metal for various reasons including temperature cycles (stress cycles) and graphitization (for carbon steel) that combine to lead to creep cracks.
4. *Overpressure*: The pressure exceeding the design pressure expressed as a percentage (e.g., 10% overpressure means 1.1 times the design pressure).
5. *Rupture*: A catastrophic failure where the vessel cannot contain the pressure, leading to a breach or explosion. This depends on the material's ultimate tensile strength (UTS), metal fatigue, corrosion, stress concentrations from defects, etc.
6. *Probability of Failure*: This is often modeled using probabilistic methods, such as those based on structural reliability analysis, which account for uncertainties in material strength, manufacturing defects, cycling-induced defects, and operating conditions.

General Trends

- *Low Overpressure (0–10% above design pressure)*: The probability of rupture is typically very low because safety factors are built into the design. For example, ASME codes often require vessels to withstand pressures significantly above the design pressure without yielding. The probability of failure might be on the order of 10^{-6} to 10^{-4} (extremely low) for well-maintained vessels.
- *Moderate Overpressure (10–50% above design pressure)*: The probability increases as the pressure approaches or exceeds the yield strength of the material. For example, at 20–30% overpressure, the probability of rupture could rise to 10^{-3} to 10^{-2}, depending on the material and inspection history. However, instrumentation and flange gaskets may leak. **The authors and others consider pressure excursions to 50% overpressure to cause a consequence of a leak, but not a rupture.**
- *High Overpressure (50–100% or more above design pressure):* The probability of rupture becomes significant, potentially reaching 10%, as the pressure approaches the ultimate tensile strength or critical flaw limits. Brittle materials may fail abruptly, while ductile materials may deform before rupture. When the temperature approaches the MAWT (Maximum Allowable Working Temperature), the concern increases.

- *Very High Overpressure (>100% or more above design pressure):* The probability of rupture becomes significant, potentially reaching 10–100%, as the pressure approaches the ultimate tensile strength or critical flaw/ defect limits, resulting in the steel shell or welds failing. Brittle materials (from defects) may fail abruptly, while ductile materials may deform before rupture. When the temperature approaches the MAWT, the concern is doubled!

Conclusion

It is unlikely to have vessel or piping rupture below 1.5 times the DP, so the authors use a probability of rupture of 0 (RRF greater than 10,000). For DP between 1.5- and 2-times DP, the authors consider that the combination of material defects in the plate and welds, together with the higher stress, will lead to a 5 to 10% chance of rupture, so we use a P_{vr} of 1 usually, but occasionally we will use 0.1 (10%). For DP > 2 times the DP, the authors consider the combination of material defects in the plate and welds, together with the higher stress of the pressure in the vessel, will lead to > 10% chance of rupture, so we use a P_{vr} of 1 (100% chance) (so no risk reduction factor) in all cases (for all clients).

Table 2 lists the values of P_{vr} used by some clients (NOT by the authors) along with those values that the that will use when necessary.

Table 2. Probability of Vessel Rupture (P_{vr})

Overpressure range	Some Clients of the Authors		The Authors Recommendation	
	Pressure Vessels	Piping	Pressure Vessels	Piping
1 – 1.5x DP	0	0	**0**	**0**
>1.5 – 2 x DP	1E-2	0	**1E-1 or 1**	**0**
>2- 3 x DP	1E-1	1	**1**	**1**
>3 x DP	1	1	**1**	**1**

Probability of Ignition (*Pi*)

Probability of ignition is the likelihood that a flammable atmosphere, dust cloud, combustible mist, or reactive material will actually ignite or initiate after a loss of containment or abnormal condition.

A key issue is understanding the release's propagation. Note that the pressure increase in the scenario may be due to a temperature rise, which causes more flammable vapor than would be expected from a release at normal operating conditions. We must consider:

1. How much flammable vapor is generated from the release?
2. How far can the flammable vapor flow?
3. Can the flammable vapor reach the ignition sources?

The authors normally include the probability of ignition, probability of presence, and probability of fatality with the selection of the consequence severity, because P_i, P_p, and P_f cannot be validated, assured, or measured with respect to the accident scenario that is being modelled. Also, the probability that the client (LOPA analyst) is misusing this probability and grossly underestimating the risk is far greater than the error in selecting the appropriate severity.

With that said, the authors have modified some rules for the use of P_i to lower the likelihood major errors in LOPA; see Table 3. [4], [5]

Table 3. Probability of ignition (P_i)

Situation	P_i	Comments
Consequence includes breaking of equipment due to high pressure, high temperature, crevice corrosion, or metal fatigue	1	Assumes electrical equipment associated with pressurized equipment will break, thereby providing an ignition source
Consequence includes breaking of equipment due to steady-state corrosion or erosion, or else overflow with no breakage, with release of flammable only within a C1D1 area	0.01	If liquid release can flow outside of the C1D1, such as if a dike fails, then this value is changed to 1, and the dike is included with a PFD of 0.01, if the other criteria of dike IPL are met. If the release is vapor or gas, the P_i is set to 1.0 unless consequence models have estimated that the vapor/gas cannot be in the flammable range in C1D1 area.
Consequence includes breaking of equipment due to steady-state corrosion or erosion, or else overflow with no breakage, with release of flammable only within a C1D2 area	0.1	If liquid release can flow outside of the C1D2, such as if a dike fails, then this value is changed to 1, and the dike is included with a PFD of 0.01, if the other criteria of dike IPL are met. If vapor release can flow outside of the C1D2, then this value is changed to 1.
Consequence includes overflow of flammable liquid within 50 ft of road or access alley that is commonly used	1	
Consequence includes overflow of combustible liquid, below boiling point within 50 ft of road or access alley that is commonly used	0.01	
If the site does not have excellent control of changes to maintain (or to avoid defeat of) an ignition classification	1	
For LOPA, dikes are not counted as an IPL if the release is above the boiling point of the flammable liquid.	1	

The authors recommend to never allow the use of probability of ignition as a risk reduction factor within LOPA

Probability of ignition estimates lower than 1.0 have proven wrong for some catastrophic scenarios. "Ignition sources are free, supplied by nature," paraphrased from Trevor Kletz. For example, no flammables were present when the hot work permit was issued for welding, but operating conditions changed, releasing flammable material to the location of welding sparks.

Probability of Personnel Presence

P_p (Probability of Personnel Presence) is a CM that relates to the fraction of time people are likely to be within the affected area when a fire/explosion or a release of toxic material occurs. [3] This is the most misused CM.

With that said, the authors have rules for use of P_p to lower the likelihood of major errors in LOPA; see Table 4. [4] [5]

Table 4. Probability of Person Present (P_p)

Situation	P_p	Comments
If human error is the cause of the initiating event	1	
If the operator's response to BPCS or SIF alarms is to go to the area of the scenario, and they have more than 30 seconds to get to the process area	1	
Scenario occurs while workers are known to be nearby, such as during a step-by-step process (such as batch, unloading, startup tasks)	1	
Initiating event is a **random, unannounced event (there are no alarms to draw the workers into the area)** such as release due to corrosion or erosion or metal fatigue; use one of cases below:		Calculated from average time in the area of ALL workers (operations and maintenance)
• Structure/area normally occupied	1	
• Structure/area occasionally occupied (less than 8 hr/day)	1	
• Remote facility or exclusion area (less than 1 hr/day)	0.1	
• If the site does not have excellent control of changes affecting normal P_p, or if the fraction of time in area is > 0.3 then use a factor of 1	1	0.3 is the mid-point of the log base 10 between 0.1 and 1 (so midway through an order of magnitude on a risk matrix).

The authors recommend to never allow the use of probability of presence as a risk reduction factor

P_p estimates lower than 1 have normally proven wrong for actual catastrophic scenarios. In many cases, the initiating event is one or more people who are present in the danger zone. In at least one incident,

personnel present at shift change who were troubleshooting a problem included two shifts for each of the following disciplines: operator, mechanic, operating foreman, maintenance foreman, engineer – yet a typical LOPA would not likely estimate that many people present.

Probability of fatality (P_f)

P_f (probability of fatality) is the "conditional" probability that, given a person is within the effect area (impact zone) and that the hazardous condition exists (such as presence of released toxic substance or presence of a flammable gas or vapor and an ignition of same) as determined in the preceding section, a serious injury or fatality would actually result. This conditional modifier cannot be determined independently of the probability of personnel presence, since it will depend on the endpoint chosen to calculate the effect area. [3] P_f estimates lower than 1 have proven wrong in many catastrophic scenarios. Some organizations do not use P_f as it is believed that this probability is sometimes a matter of chance and they do not want the calculated risk to be reduced.

The authors (the originators of LOPA) always include P_i and P_f within the selection of the severity, because this has proven to give less chance of underestimating the risk of a scenario. The authors do not use P_i and P_f in LOPA, but Table 5 provides some typical factors used in the industry.

The authors recommend against using probability of fatality as a risk reduction factor in LOPA

Table 5. Probability of Fatality, *Pf*, (given person present in a fire/explosion or a release of toxic material) for LOPA

Situation	P_f	Comments
For fire or toxic release and person is in a protected area, given P_p and P_i and Consequence Severity (S) and IEF are independently estimated from P_f	0.1	Protected area must be specifically designed to protect against the scenario.
For fire or toxic release and person is outside of protected area, given P_p and P_i and Consequence Severity (S) and IEF are independently estimated from P_f	0.5	*Pf* for flash fire is usually 1.0; for jet fire or pool fire, escape may be possible, hence 0.5.
For explosion and person is in protected area, given P_p and P_i and Consequence Severity (S) and IEF are independently estimated from P_f	0.1	Protected area must be specifically designed to protect against the scenario.
For explosion and person is outside of protected area, given P_p and P_i and Consequence Severity (S) and IEF are independently estimated from P_f	1	

Enabling Conditions (EC)

As mentioned at the start of the paper, an EC is a condition that makes the beginning of a scenario possible. An enabling condition is neither a failure nor a protection layer. The most common EC is the fractional time at risk estimate.

Time at Risk Fraction (P_t or TAR)

Time at risk (TAR) is the fraction of time an incident sequence may be realized when conditions are right for the sequence to progress to a loss event. An underlying assumption for time-at-risk enabling conditions is that *only revealed failures can act as initiating events during time-at-risk conditions.* A *revealed failure* is one that may be immediately or almost immediately apparent through an alarm or indicator system. For example, a primary feed pump failing off during continuous process operation would be rapidly apparent from its effects on process parameters when feed flow is lost.

The example below illustrates the dangerous misuse of P_t. In an eight-hour batch reaction, loss of cooling can cause a runaway reaction only during a critical two-hour period. LOPA analysts can be tempted to calculate a time-at-risk enabling condition by the following equation:

$$TAR = \frac{\#\ of\ batches}{year} \times \frac{2h\ Time\ At\ Risk}{8760\ h/year} \qquad \text{[Eq. 1]}$$

DO NOT USE THIS EQUATION

An implicit assumption in this equation is that all the failures that can cause loss of cooling occur only during the critical two-hour time period when the runaway reaction can occur on loss of cooling. In reality, for a typical cooling water supply system, the causes of loss of cooling can be viewed as loss of water flow or high temperature of the cooling water, as shown in Table 6.

Table 6. Typical Causes of Loss of Cooling

Loss of Cooling Water Flow	High Temperature of Cooling Water
Cooling water pump tripped	Cooling tower fan tripped
Water flow control loop failed to low flow	High thermal load on cooling tower
Manual block valve closed or throttled	High ambient temperature (above design)
Line plugged	
Low level in cooling tower	

Equipment failures that lead to loss of cooling can occur randomly during the time-at-risk interval, or during the time-**not**-at-risk phase. If the operators do not know the status of the cooling water before they enter the critical time-at-risk phase, they will find out when the runaway reaction occurs! Using time-at-risk without knowledge of the status of the enabling condition system can drastically underestimate the actual risk and give a false sense of confidence.

In order to use time-at-risk, it is essential to confirm that the cooling water system is operating correctly and has not failed before starting the critical time-at-risk phase. Some facilities have a cooling water supply pressure indicator with a low alarm and a cooling water supply temperature indicator with a high alarm to alert the operators to potential failures of the cooling water. Operator response to alarm procedures should be available and should include prohibitions against starting the critical time-at-risk phase of the reaction.

Table 7 shows some rules to estimate the Initiating Event Frequency (IEF).

Table 7. Probability of Time at Risk fraction

Situation	IEF to use instead of using a discrete P_t	Comments
If Human Error is the Initiating Event	Use the probability of human error as the IEF	
If two Initiating Events must occur	Use failure rate as the IEF of the scenario	Use the IEF of the 2nd Initiating Event
If the demand on the first IPL is more than twice the test frequency of that IPL	Ignore the first IEF and use the IEF of the first IPL as the replacement IEF	The original IE is dropped from the scenario, and the new IE uses the steady state failure rate (new IEF) of the IPL that is the first one triggered (because of the high demand of that IPL)

Human Limitations Leading to Improper Use of CMs and ECs

Overconfidence bias and the Dunning-Kruger effect

Overconfidence bias occurs when individuals overestimate the accuracy of their judgments or the correctness of their decisions. This cognitive bias is pervasive and affects all humans, regardless of expertise or experience. A clear example of this bias is that most people believe that they are better drivers than the average person (which is mathematically impossible). The bias often leads to excessive risk-taking and poor decision-making because people believe they are less likely to make mistakes than they actually are.

A related phenomenon is the **Dunning-Kruger Effect**, which describes how individuals with lower competence in a domain tend to overestimate their abilities, while highly competent individuals may underestimate theirs. This mismatch arises because those with limited knowledge lack the metacognitive ability to recognize their own shortcomings, making them appear the most overconfident. [6]

Overconfidence has contributed to several historical disasters, including:

- **The sinking of the Titanic** – Designers and operators believed the ship was "unsinkable," leading to insufficient lifeboats and complacency in safety measures.
- **The Challenger space shuttle tragedy** – Decision-makers underestimated the risk posed by O-ring failures during a low-temperature launch despite engineers' warnings.
- **Titan submersible implosion:** OceanGate's experimental submersible, Titan, imploded in 2023 near the Titanic wreck during a routine dive. Despite engineers and industry experts publicly expressing safety concerns, OceanGate management proceeded with presumptive confidence in its carbon-fiber hull, a decision reflecting overconfidence in judgment and underappreciation of failure risks.

These examples illustrate how overconfidence can amplify systemic risks, especially in high-stakes environments like engineering and process safety. Recognizing and mitigating this bias is essential for sound risk management and decision-making.

An important facet of overconfidence bias is what Sánchez and Dunning (2018) [7] call the **"Beginner's Bubble".** Contrary to the classic notion of "unconscious incompetence", novices do not start out overconfident; initially, they are cautious and realistic about their abilities. However, after only a few experiences (often in tasks involving probabilistic reasoning), their confidence rises sharply, far outpacing their actual performance. This surge occurs because beginners quickly form their own theories about how to succeed, many of which are flawed, and they stop processing feedback effectively. While their performance improves gradually, confidence tends to stabilize or even decline slowly, creating an early bubble of overconfidence that can be dangerous in safety-critical contexts.

In a PHA/LOPA environment, most, if not all, team members are within the "Beginner's bubble" (little knowledge + high confidence) in regard to consequence modelling, failure rates, and probabilistic estimation

Human limitations in evaluating complex scenarios

Humans are inherently limited in their ability to accurately assess scenarios involving numerous variables and interdependencies. Cognitive psychology and decision science have shown that our brains rely on **heuristics** (mental shortcuts) to simplify complex problems. While these shortcuts are useful for everyday decisions, they introduce systematic biases and errors when applied to high-stakes, multi-variable environments such as process safety.

One key limitation is **bounded rationality**, a concept introduced by Herbert Simon, which states that humans cannot process all available information due to constraints in time, cognitive capacity, and attention. Instead, we satisfice by choosing an option that seems "good enough" rather than optimal.

Another challenge is **cognitive overload**. When faced with dozens of interacting variables, humans struggle to maintain an accurate mental model. Research shows that working memory can only hold about 4–7 items at once, making it nearly impossible to intuitively grasp complex probabilistic relationships. This limitation fosters reliance on simplifying assumptions, which can distort risk estimates.

In PHA/LOPA, the accident scenarios discussed involve lots of variables which also have a significant degree of uncertainty: Failure rate, type of failure, safeguards reliability, pressure at which a pipe/vessel ruptures, rupture point, type of rupture, potential shrapnel, ignition sources and probabilities, personnel presence, emergency response, time of day, weather, etc.

Comments on Accuracy

Many companies believe that risk calculations using LOPA (or QRA) are accurate. But the factors (PFDs, IEFs, etc.) are not accurately known for a site. The "*Guidelines for Process Equipment Reliability Data*" (PERD) [8] describes the difference between plant-specific data and generic data as well as the difference between confidence and tolerance:

> "The ideal situation when performing a CPQRA is to have sufficient plant-specific data for each piece of equipment. However, there are many variables in the process, maintenance practices, and data collection that can fluctuate throughout a study period and have a major influence on the results: intensified preventive maintenance can lower and eliminate failures; changes in process conditions may severely exacerbate fouling tendencies or corrosion rates; equipment may be upgraded and even replaced during the study extending operating life; many failures may have been missed; many failures may be wrongly recorded such as a reported pump failure when the push button was really at fault. Since populations and operating time are limited in most plant studies and the number of failures may be heavily biased by the variations noted, plant-specific failure rates may lack statistical confidence.
>
> Confidence that the calculated failure rate is a good estimate of the true rate can be increased by lengthening the study or sample time. Adding another population of the same equipment under the identical circumstances to the original population will reduce uncertainties and increase confidence in the calculated failure rates.
>
> Plant-specific data are frequently unavailable or are low in their level of confidence. Further, this source of data cannot provide information on equipment not in use at the plant, nor can it do more than suggest how plant equipment might behave under different circumstances. Since

> data collection is very difficult, using shared or generic data is one way of resolving these problems without the expense of extensive data collection systems. Frequently, the only way to gather sufficient data for a CPQRA (Chemical Process Quantitative Risk Analysis) is to build a data set using inputs from other plants within the company or from other available resources. Generic data provide less specific and less detailed data, but can draw upon a much larger equipment population, representing more exposure time, and present a much more realistic data than that limited to a single plant."

Any specific factor used in LOPA risk calculations usually has a range of **plus and minus an order of magnitude** (**a factor of 10**). Table 8 and Table 9 show some IEF and PFD as examples, indicating the lower and upper limits of the 90% confidence interval. [8] [9]

Table 8. Failure rate (mean and 90% confidence interval lower/upper limits) per year of different equipment

Item	Failure mode	Lower	Mean	Upper	Source*
Pressure sensor	Degraded	1.8E-4	4.6E-2	1.8E-1	OREDA
Solenoid valve	Spurious operation	9.5E-4	3.6E-3	8.6E-3	PERD
Flame detector	Catastrophic	4.6E-4	3.8E+0	1.5E+1	PERD
ESD/PSD Valve	Spurious operation	8.8E-5	3.7E-2	1.5E-1	OREDA

* Sources show the data per 10^6 hours instead of per year

Table 9. PFD (mean and 90% confidence interval lower/upper limits) of different equipment

Item	Failure mode	Lower	Mean	Upper	Source
Check valve	Fails to close	2.9E-4	2.2E-3	6.7E-3	PERD
PSV (Spring loaded)	Fails to open on demand	1.3E-4	5.2E-3	2.3E-2	PERD
Solenoid valve	No change in position on demand	3.4E-4	2.8E-3	1.0E-2	PERD
Motor driven pump	Fails to start on demand	1.9E-3	1.9E-2	6.0E-2	PERD

In most cases, it seems we have no significant digit, but rather have a significant order of magnitude, which may be best expressed (if rounded up) as $10^{-X\pm Y}$. Then what if the range is broader; say: 0.01 to 0.0001 with a mean and median of 0.001. How is that expressed? 0.001 ± a multiplication factor of 10? So, again here only the single digit of the exponent is significant in the expression of the data: $10^{-3\pm1}$. **Enabling Conditions and Conditional Modifier Probabilities also have significant uncertainty ranges.**

From our experience, uncertainty in probabilistic risk assessments tends to grow as residual risk decreases. This occurs because extremely low-probability events lack sufficient real-world data for meaningful comparison or validation. Figure 2 (on the next page) illustrates how the uncertainty of the risk value is likely to increase as the calculated risk drops lower and lower to the 10^{-6} per year range. Note that each oval is an illustration of the plus/minus 2 sigma uncertainty of both the consequence value and the frequency value and any step in a quantitative risk assessment for a specific scenario, including risk assessments using LOPA. This is the more proper presentation of the results, especially since a risk matrix

is a log-log (base 10) plot of risk assessment results. There is no need to illustrate any finer gradation than the approximate order of magnitude since the data estimates with uncertainty included only supports an expression of: $\mathbf{P = 10^{-X\pm1}}$.

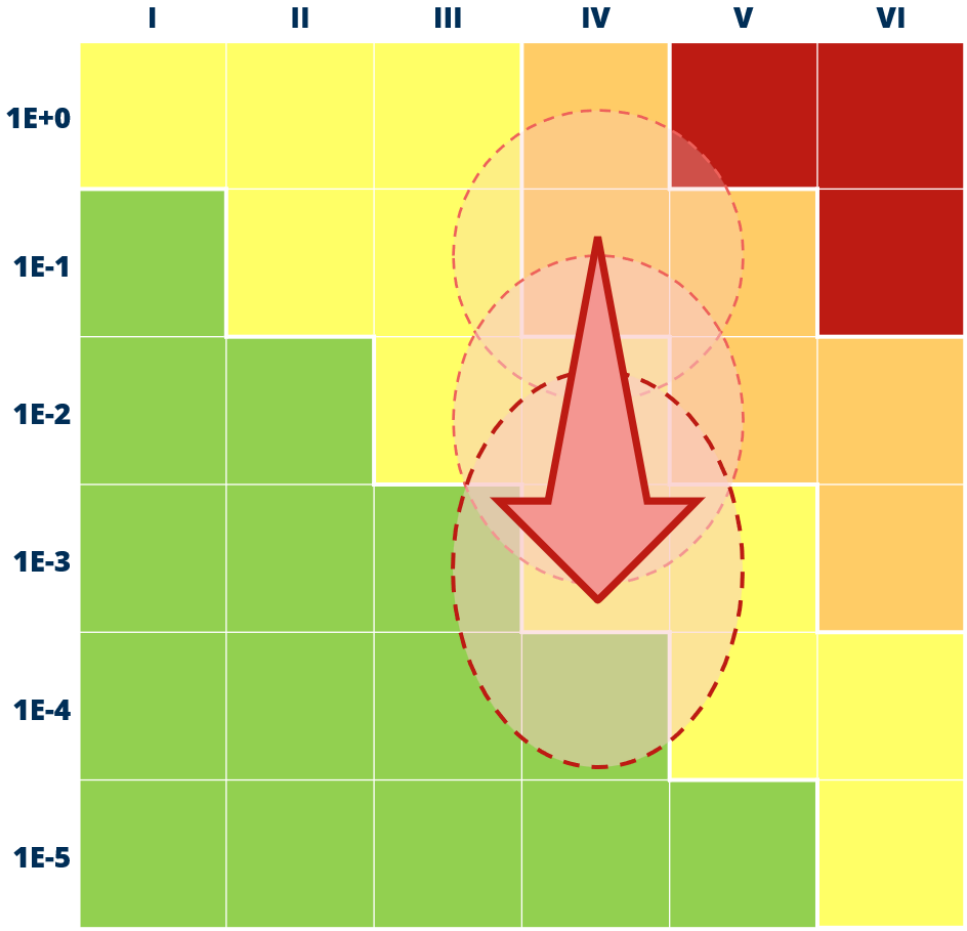

Figure 2. Residual Calculated Risk, showing growing uncertainty in the results (risk) as the risk drops lower (courtesy of Process Improvement Institute) [10]

We cannot prove how much the uncertainty grows, but if risk analysts were off by 3 orders of magnitude in the past in the 10^{-6} range of probability per year; it is likely that the chemical industry is off by 2 orders of magnitude in the range of 10^{-4} per year. Hence, we believe that $P = 10^{-X\pm1}$ is an appropriate representation of the results of each estimate and each calculation result for quantitative risk assessments, including LOPA. Further, since the data has so much uncertainty and since our overall industry has still limited experience with accident scenario risk prediction, we believe a risk calculation of less than 10^{-4} per year is meaningless and not supportable, as it is very likely that common-cause errors of the common humans in operations and maintenance departments will outweigh all other risk factors in the range of 10^{-4} per year and less, as shown in the study of the risk estimates in the nuclear power industry, mentioned above.

When multiplying numbers, the result should be rounded to the same number of significant figures as the input number with the fewest significant figures, reflecting the error/uncertainty from the least precise measurement. Hence, the uncertainty of any LOPA is never better than +/- an order of magnitude, and that is true only if the analysis is limited to valid IEs and valid IPLs (if ECs and CMs are avoided.)

General comments on EC/CM Validation

Most companies are aware that IPLs and IEs must be validated, and records must be kept and audited. This issue also has been a huge problem in the past +20 years of LOPA implementation and is one of the problems addressed in *Guidelines for Initiating Events and Independent Protection Layers,* 2015 [2]. Currently, even if following industry advice, it means nothing if your own test data shows the IPL or IE value is worse than what we specified in the LOPA. For instance, what if you follow industry advice for PSV maintenance and testing, but then your own records indicate that every time you pull a couple of specific PSVs, they are compromised in some way? Obviously, you have a problem with these specific PSVs and, therefore, using them as IPLs (or using the PFD value you hoped for) is not valid.

On the other hand, **most companies are not aware that ECs and CMs must also be validated, and records must be kept and audited**. But we have not yet found any operating company that truly manages potential changes to ECs and CMs or that validates or proves these are valid on a sufficiently routine basis. This is why most operating companies prohibit the use of ECs and CMs.

Our experience with about 200 clients suggests that usually the companies that use ECs and CMs have set their risk reduction targets too low (often impossibly low). Table 10 summarizes our observations:

Table 10. Risk Tolerance Criteria versus Use of ECs and CMs

	Consequence Categories		
	Single fatality Loss of ~10MM USD Offsite injury	**Multiple fatalities Loss of ~100MM USD Offsite fatality**	**Use of ECs and CMs**
Risk Tolerance Criteria for final mitigated likelihood of scenario (per year)	1E-3	1E-4	None used; none allowed; LOPA and risk judgement are straightforward; all risk factors can be validated; almost no SIL 3 SIFs are allowed; there may be some MooN relief valve configurations due to the limits of how large a PSV can be.
	1E-4	1E-5	CMs are used for about half of the scenarios, although almost no ECs are used. Occasionally, have used SIL 3 SIFs. Note that these CMs, EC, and SIL 3 SIFs cannot be validated to achieve the credited risk reduction factor
	1E-5	1E-6	Heavy use of CMs and ECs required. Many uses of SIL 3 SIFs and MooN relief valve configurations needed. Note that these CMs, EC, and SIL 3 SIFs cannot be validated to achieve the credited risk reduction factor

Case study

For one large client of the authors, we reviewed the use of ECs and CMs on about 200 LOPA scenarios. They were using these factors because that was the only approach to reach a tolerable risk level of 10^{-5}/year for a single fatality and 10^{-6}/yr for scenarios with multiple fatalities. Of course, not all ECs and CMs categories were used in all scenarios. P_{vr} and P_P were the most commonly used, but P_t was also used many times. After a review by the authors staff and the PHA team members regarding the uses of these CMs and EC versus the best practices stated in this paper, we concluded the following:

- P_{vr} was used incorrectly by the client roughly 90% of the time.
- P_p was used incorrectly by the client roughly 90% of the time.
- P_t was used incorrectly by the client, essentially 100% of the time that TAR was used.

Based on this feedback, the client is revising the rules for the use of ECs and CMs and adjusting the risk targets to be more realistic.

Conclusion

Setting proper rules for use by a PHA team is superior to using ECs and CMs that are complicated to understand and nearly impossible to prove the risk reduction values that are claimed. We suggest teaching the rules for P_{vr} and P_p in this paper to PHA team leaders and avoiding ECs and CMs in general. It is wiser

to change the risk matrices (or other descriptors of the risk tolerance criteria) to eliminate even the temptation to use ECs and CMs.

Acronyms

CM: Conditional Modifier
CS: Conditional Severities
EC: Enabling Condition (same as Enabling Event)
EE: Enabling Event (same as Enabling Condition)
IEF: Initiating Event Frequency
IPL: Independent Protection Layer
ITPM: Inspection, Test, Preventative Management
LOPA: Layers Of Protection Analysis
P_f: Probability of fatality/injury
P_i: Probability of ignition
P_p: Probability of personnel presence
P_{SD}: Probability of structural damage
P_t: Probability of Time At Risk
P_{vr}: Probability of vessel rupture
PFD: Probability of Failure on Demand
PHA: Process Hazards Analysis
PSM: Process Safety Management
PSV: Relief Valve / Pressure Safety Valve

References

[1] CCPS/AIChE, Layer of Protection Analysis, simplified process risk assessment, Wiley, 2001.

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

[3] CCPS/AIChE, Guidelines for Enabling Conditions and Conditional Modifiers, Wiley, 2014.

[4] W. Bridges and A. M. Dowell, "Key issues with implementing LOPA - Perspective from the Originators of LOPA," in *AIChE/CCPS 11th Global Congress on Process Safety*, Austin, TX, 2015.

[5] W. Bridges and A. M. Dowell, "More issues with LOPA - from the Originators," in *AIChE/CCPS 17th Global Congress on Process Safety*, 2021.

[6] J. Kruger and D. Dunning, "Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments," *Journal of Personality and Social Psuchology,* 2000.

[7] C. Sanchez and D. Dunning, "Overconfidence among begginers: Is a little learning a dangerous thing?," *Journal of Personality and Social Psychology,* vol. 114, 2018.

[8] CCPS, Guidelines for Process Equipment Reliability Data, Wiley, 1989.

[9] SINTEF Industrial Management, OREDA - Offshore Reliability Data Handbook, OREDA Participants, 2002.

[10] W. Bridges and A. M. Dowell, "Key issues after 30 years of implementing LOPA - from the Originators of LOPA," in *AIChE/CCPS 22nd Global Congress on Process Safety*, Houston, 2026.