“Double Jeopardy for $1000 Alex” - What It Is and How to Apply It

Donnie Carter, P.E.†, Jeffrey Miller, John T. Perez, P.E.†, William Wimberly, C.S.P.†
Cognascents Consulting Group, Inc.
1519 Vander Wilt Lane, Bldg. 4,
Katy, Texas 77449

† Presenter E-Mails: donniecarter57@gmail.com, john.perez@cognascents.com,
billy.wimberly@cognascents.com

Abstract

Process hazards analyses, such as Hazard and Operability studies (HAZOPs) and Layer of Protection Analyses (LOPAs), are structured, team-based exercises focused on hazard identification, risk assessment, and risk management. In order to manage the complexity associated with these analyses, recognized and generally accepted rules are imposed to manage and limit the review of hazard scenarios involving simultaneous failures. One of these rules has been dubbed “double jeopardy”.

Based on the authors experience via direct observation and review of PHA documentation, PHA teams continue to struggle to understand double jeopardy and how to effectively address simultaneous failures when applying PHA methodologies, such as HAZOP and LOPA. In addition, more widely accepted emergence and use of enabling conditions and conditional modifiers when developing hazard scenarios has blurred the legacy definition of double jeopardy.

In this paper, the authors provide an overview of double jeopardy along with specific PHA examples regarding credible as well as inappropriate applications of double jeopardy. They also present tools and recommendations to enhance PHA teams’ performances regarding the application of double jeopardy. More specifically, they address issues regarding latent failures (revealed vs. unrevealed conditions), concurrent incidence of failures, and independence of initiating events.

The target audience for this paper is anyone whose responsibilities include (1) leading within an organization that uses PHAs, (2) establishing PHA guidance documents, (3) applying PHA methodologies, and (4) reviewing PHA outputs and reports.

Introduction

“We do not need to analyze that scenario because it is double jeopardy. There is no way all of those initiating events will happen at the same time. Isn’t that double jeopardy?”

How many times have you heard these statements during a HAZOP? What did the team do? Who led the discussion and facilitated the final decision? Did the team have a clear understanding of the term “double jeopardy”? What is its derivation and original intent?

Based on incident investigations, some of the tragic and catastrophic events in the oil, gas, and chemical industries resulted from extremely unlikely combinations of initiating events (IEs) [7]. Events such as these are not typically assessed during a HAZOP or LOPA because these PHA methodologies are not designed for effective assessment of extremely unlikely scenarios. HAZOPs and LOPAs are structured, team-based exercises focused on hazard identification, risk assessment, and risk management [5]. In order to manage and temper the potential complexity of analysis for certain processes and unit operations, rules have been developed and utilized by PHA teams to focus assessment efforts on credible scenarios relative to extremely unlikely scenarios. Over time, double jeopardy has evolved into a HAZOP scenario-limiting convention, which some argue represents good engineering practice regarding HAZOP application and HAZOP limitations. Double jeopardy is often cited by teams as a reason not to assess certain scenarios stemming from multiple IEs even though the IEs may be dependent or result from a common cause.

When it comes to double jeopardy and HAZOP, the popular Jeopardy!® quiz show comes to mind where participants earn points by providing correct responses in the form of questions to answers presented in a grid of blue boxes. Each box is worth more points the lower it sits in each column. As PHA team members chime in with “Isn’t that double jeopardy?”, we often wonder as facilitators if they are asking us the question or if they are submitting their question as an answer for dismissal of the hazard scenario as non-credible and subsequent advancement to the next blue box (i.e. hazard scenario). The 25th anniversary of OSHA’s 1910.119 PSM mandate is just around the corner and we continue to struggle with double jeopardy’s role in hazard identification, risk assessment, and risk management.

Double Jeopardy Defined - Then and Now

Pre-PSM to 1997

Where did the term “double jeopardy” come from? According to direct inquiry of industry veterans, the term has been used since before the advent of PSM in 1992 so there is no definitive birthday of double jeopardy with respect to PSM. The 4th edition of the American Petroleum Institute’s (API) Recommended Practice (RP) 521: Guide for Pressure-Relieving and Depressuring Systems issued in 1997 included the following language in section 2.2 [1]:

“The causes of overpressure, including external fire, are considered to be unrelated if no process or mechanical or electrical linkages exist among them, or if the length of time that elapses between possible successive occurrences of these causes is sufficient to make their classification unrelated. The simultaneous occurrence of two or more conditions that could result in overpressure will not be postulated if the causes are unrelated.”

2003

In his book designed for PHA facilitators and participants, Nigel Hyatt [6] provided the following explicit definition:

"The chance that two (or more) unrelated events or incidents will occur at the same time. (It is important to note that two (or more) events or incidents arising from a common cause do not qualify). Specific double or multiple jeopardy events are frequently considered to be so rare that their consideration does not warrant further examination. [However non-specific multiple jeopardy events in general are not rare and frequently involve human error with multiple complex stages / interactions. Since their potential number are extremely high, although the probability of a specific multiple jeopardy event is extremely low, this makes non-specific (very-hard-to-predict) multiple jeopardy events fairly likely]."

<u>2014</u>

2014 was a significant year for double jeopardy as two influential organizations (CCPS and API) committed to additional explicit definitions of double jeopardy.

The language mentioned above from the 4th Edition of API RP 521 exists nearly verbatim in section 4.2.3 of what is now an API standard - API Standard 521: Pressure-relieving and Depressuring Systems (6th edition, January 2014) [2]. The title of sub-section 4.2.3 containing the language is "Double Jeopardy". Sub-section 4.2.3 explicitly states the following:

"The causes of overpressure are considered to be unrelated (i.e. independent) if no process or mechanical or electrical linkages exist among them or if the length of time that elapses between possible successive occurrences of these causes is sufficient to make their classification unrelated. The simultaneous occurrence of two or more unrelated causes of overpressure (also known as double or multiple jeopardy) is not a basis for design….This standard describes single jeopardy scenarios that should be considered as a basis for design."

Additional clarification on double jeopardy is provided in section 4.2.4 in the same API standard:

"Latent failures should normally be considered as an existing condition and not as a cause of overpressure when assessing whether a scenario is single or double jeopardy."

The second explicit definition of double jeopardy provided in 2014 can be found in CCPS's book on enabling and conditional modifiers [4]:

"'double jeopardy' can be more precisely defined as the *concurrent incidence of two independent initiating events or other revealed failures*".

Both pressure relief design and process hazards analysis include a hazard identification step. Pressure relief design requires that credible overpressure scenarios be identified and HAZOPs require that IEs be defined before additional analysis is performed. The two exercises should arrive at the same result regarding what is credible and what is not with respect to double jeopardy. Inconsistencies in philosophy currently lead to inconsistencies across PHA documentation and pressure relief design bases. A HAZOP may call for overpressure protection while the pressure relief design basis does not address a specific overpressure scenario because double jeopardy is applied differently.

The definitions presented in this section are similar, but not identical. Clearly, double jeopardy has firm roots in the fields of pressure relief analysis and process hazards analysis. Although several organizations maintain standards regarding pressure relief analysis and PHAs, API and CCPS serve as two prominent standard-bearers in these fields. Oftentimes, the direction of the PHA team is influenced by the expertise in attendance. If the process engineer has deep pressure relief analysis experience, then double jeopardy is addressed in accordance with pressure relief design guidance. Double jeopardy is not explicitly addressed in CCPS's book on hazard evaluation procedures [5], which is the facet of PSM where double jeopardy continues to be misunderstood and misapplied. Careful examination of the components of double jeopardy will help the reader understand the complications associated with double jeopardy and, thereby, provide a framework to effectively apply double jeopardy. Effective application implies clarity, consistency, defensibility, and compatibility with good engineering practice.

Double Jeopardy Components

The initial goal for any hazard identification exercise is to determine whether a hazard scenario is credible or non-credible. Determination of a credible scenario during a PHA or pressure relief analysis must strike a delicate balance between under-developing scenarios resulting in missed significant risks and over-developing hazards resulting in significant time and expense for negligible benefit. Given the above definitions, credibility should be assessed using the following four criteria:

1. Independence of IEs;
2. Visibility of individual IEs;
3. Potential for concurrence of individual IEs; and
4. Combined initiating event likelihood (CIEL) tolerance.

Independence of IEs

If the initiating events for a potential hazard scenario are all dependent, then the hazard scenario is credible and should be assessed. Independence across IEs can be difficult to establish. Per API 521, IEs are independent as long as there are no process, mechanical, or electrical linkages between them [1, 2]. Criteria for independence should also include procedural or utility linkages. Some companies treat secondary IEs as enabling conditions. Enabling conditions can be traditional causes or safeguard failures [3].

Multiple IEs could fail the independence test either because of dependency (i.e. one IE directly or indirectly causes the second IE), or because of common cause failure. Common cause failures could result from normal or abnormal process conditions, partial or total failures in utility systems, BPCS component failures, human error, external events, or a combination of these. The examples presented later in this paper provide additional clarification regarding independence across normal and abnormal operating modes as well as control loop components.

Companies should provide guidance regarding independence of IEs. Guidance documentation should address simple instances of independence as well as complicated independence conditions, such as colocation, common design elements, partial power failure, partial instrument air failure, common I/O card failure, and selective MCC failure. Companies may choose a non-HAZOP methodology to assess hazard scenarios associated with complicated dependence conditions across multiple IEs.

It is easier to establish independence between procedural and non-procedural linkages than it is to identify independence between procedural linkages. For example, an operator inadvertently closing a manual valve associated with one processing unit and a BPCS failure within a different processing unit are typically independent IEs. An operator failing to open multiple valves (each located in a different location) may at first glance also seem like independent IEs; however, reading the relevant operating procedure reveals that instruction to open the multiple valves resides in a single step. Hence, omission of a single step by an inexperienced operator may result in multiple inadvertent valve positions, which does not meet the condition of independence.

Visibility of Initiating Event (Latent vs. Revealed)

After establishing whether all IEs are independent of each other or not, the next criterion to evaluate is visibility. Visibility in this context refers to the detectability of the IE. An IE is visible if it is announced or detected or revealed. For example, an operator may be alerted to an abnormal operating condition by way of an alarm. This abnormal operating condition is visible. An RO deemed safety-critical may have an associated inspection routine. Failure of this RO may be visible. BPCS failures may be visible or invisible depending on the failure mode. PHA teams should seek to understand the visibility of each IE. A check valve that is periodically tested for functionality and demonstrates a mean-time-between-failure (MTBF) significantly higher than the inspection interval may potentially be considered revealed. However, caution should be taken when relying on inspection to reveal failures as a process change may affect the MTBF, thereby changing an IE’s visibility.

An unrevealed or latent IE affords concurrence as there is no verification and confidence in its performance. Concurrence is credible for unrevealed or latent IEs. Determination of whether an IE is revealed or unrevealed should account for the likelihood of the IE as well as the time required to detect the IE. At this point in the double jeopardy evaluation, credibility depends on the number of revealed vs. unrevealed IEs. For a hazard scenario stemming from N number of IEs to be considered credible, then the number of unrevealed IEs must be ≥ N-1 (or revealed IEs must be ≤ 1). Note that the number of unrevealed IEs must be ≥ N-1 of independent IEs. A group of dependent IEs should be treated as a single IE when applying the above rationale.

For example, if a hazard scenario stems from four IEs AND all IEs are deemed independent of each other, the hazard may or may not be credible. Credibility at this point in the evaluation depends on whether or not N-1 or more of the IEs are unrevealed. With three unrevealed IEs, this is a credible scenario and should be assessed. However, if two or more of the IEs are deemed revealed, then double jeopardy may apply and the scenario may be deemed non-credible.

Potential for Concurrence

After establishing whether all IEs are independent of each other AND whether the number of unrevealed IEs is $\geq$ N-1, the next criterion to evaluate is concurrence. Concurrent and simultaneous are not the same condition. Simultaneous is often interpreted as starting or happening at the exact same time. When applied literally, very few IEs occur simultaneously. On the other hand, concurrent means existing at the same time or running in parallel.

Although similar, the two words are very different with respect to double jeopardy definitions. Simultaneous allows for the dismissal of IEs that can exist concurrently, thereby, dismissing potential credible hazard scenarios. By considering concurrent IEs, hazard scenarios may be credible where one IE is associated with an unrevealed (latent) condition or abnormal operation and another IE is created by return to normal service activity.

Combined Initiating Event Likelihood (CIEL) Tolerance

Every hazard scenario is possible. But many processes have variable sets that make generation and assessment of every hazard scenario not practical given the confines of business. To limit the number of scenarios assessed during a hazard identification exercise, teams should apply criteria to determine which scenarios are credible. With respect to double jeopardy and overall credibility, the criteria already mentioned serve as a near-complete set. The final criterion is the combined IEL or CIEL. More specifically, for a scenario to merit analysis, the CIEL should not be less than an organization's preset lower CIEL tolerance and is the sum of all IELs regardless of visibility. Note that similar to the application of the visibility criterion a group of dependent IEs should be treated as a single IE when calculating the CIEL. The CIEL is a screening criterion and should not be used as the aggregate PHA IEL for the scenario ultimately assessed by the PHA team. The authors acknowledge the CIEL criterion as optional as some companies may not be comfortable in documenting preset CIEL tolerances. Risk acceptance criteria are sensitive pieces of information.

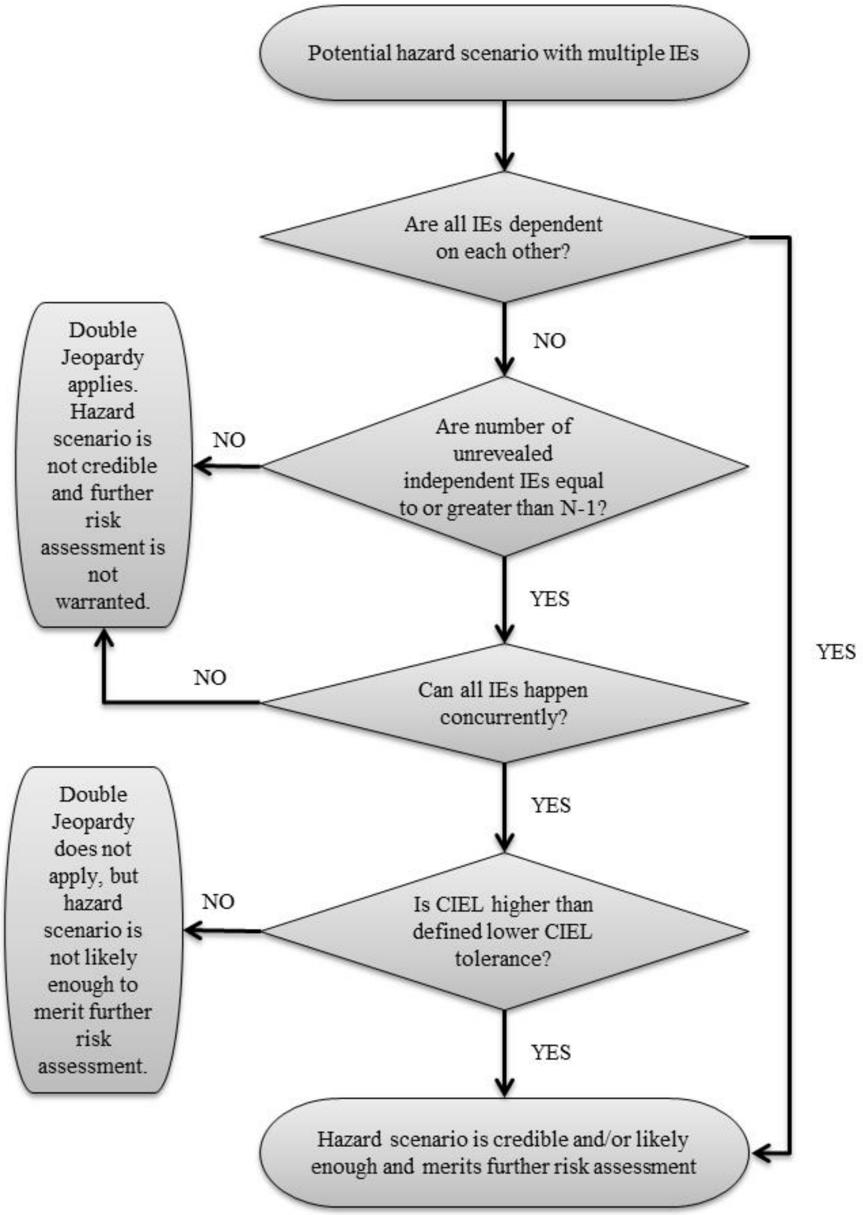
For example, the ACME Chemical Company has defined its lower CIEL tolerance at 1 x 10^{-5}. During a HAZOP, a scenario with a CIEL of 1 x 10^{-6} is developed. The scenario stems from understood, defined, and defensible IELs. The IEs are independent from each other. At least N-1 of the scenario's IEs are unrevealed. The condition of concurrence of all IEs is possible. However, the CIEL is lower than ACME's lower CIEL tolerance. Even though the hazard scenario meets all other criteria for credibility, its CIEL makes it extremely unlikely and impractical for assessment from a risk tolerance and business perspective. This does not mean that double jeopardy applies; it just means the scenario is not likely enough to merit further analysis.

For extremely high-consequence scenarios, a company may choose to fully evaluate the scenario despite its CIEL. Once again, companies desiring to adopt such an approach need to establish CIEL tolerance criteria for risk assessment teams. Lastly, for extremely high-consequence scenarios that ARE deemed double jeopardy, a company may still choose to fully evaluate the scenario.

Double Jeopardy Decision Tree

To aid the reader in application of the above criteria, the following decision tree has been developed based on the various definitions of double jeopardy against the above synthesis:

Chart 1. Double Jeopardy Decision Tree

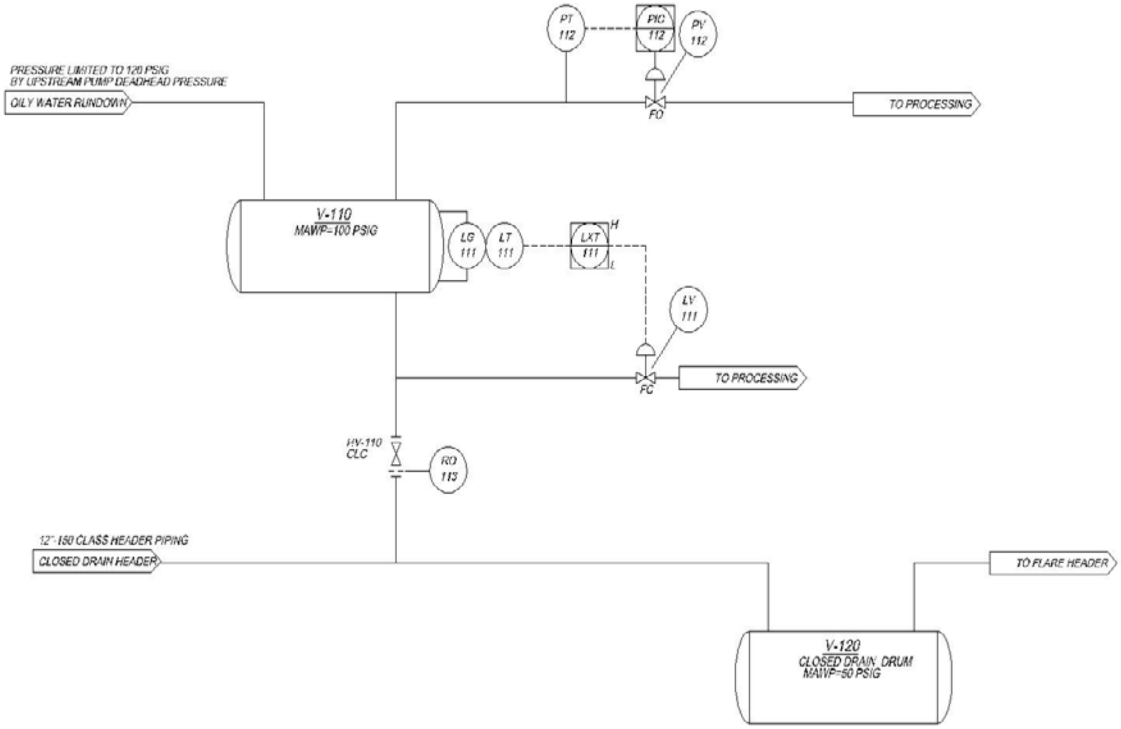

Potential hazard scenario with multiple IEs
Are all IEs dependent on each other?
NO
YES
Are number of unrevealed independent IEs equal to or greater than N-1?
NO
Double Jeopardy applies. Hazard scenario is not credible and further risk assessment is not warranted.
YES
Can all IEs happen concurrently?
NO
YES
Is CIEL higher than defined lower CIEL tolerance?
NO
Double Jeopardy does not apply, but hazard scenario is not likely enough to merit further risk assessment.
YES
Hazard scenario is credible and/or likely enough and merits further risk assessment

Application of the above decision tree assumes the starting point for double jeopardy assessment is a potential hazard scenario with multiple IEs with each having an understood, defined, and defensible IEL. Although not explicitly stated, the definitions provided by API and CCPS are easier applied when IEs have understood, well-defined, and defensible IELs. If any of the IEs associated with a potential double jeopardy scenario have hard-to-define likelihoods, then the scenario should not be assessed until all IELs are understood, defined, and defensible. Companies should provide IEL guidance to ensure consistency across quantitative hazard identification exercises. The authors acknowledge that HAZOP is a qualitative PHA methodology where numerical values for IELs are not always defined. However, HAZOPs often generate LOPA scenarios and consideration and definition of numerical IEL values should occur during the hazard scenario development effort in the HAZOP [8].

For example, external fire is considered a credible overpressure scenario per API 521 [1, 2]; however, it is difficult to assign a defensible likelihood to an external fire. External fire scenarios are assessed more effectively when they are developed as a consequence rather than an initiating event as the cause, time, and location are then brought into the analysis. Other examples of scenarios often assessed in HAZOP with hard-to-define IELs include leaks, ruptures, corrosion, and erosion.

EXAMPLE 1: - Gas Blowby Through a Restriction Orifice (RO)

<u>Cause: Inadvertent Opening of a Locked Closed Valve</u>



<u>Consequence Developed by PHA Team</u>

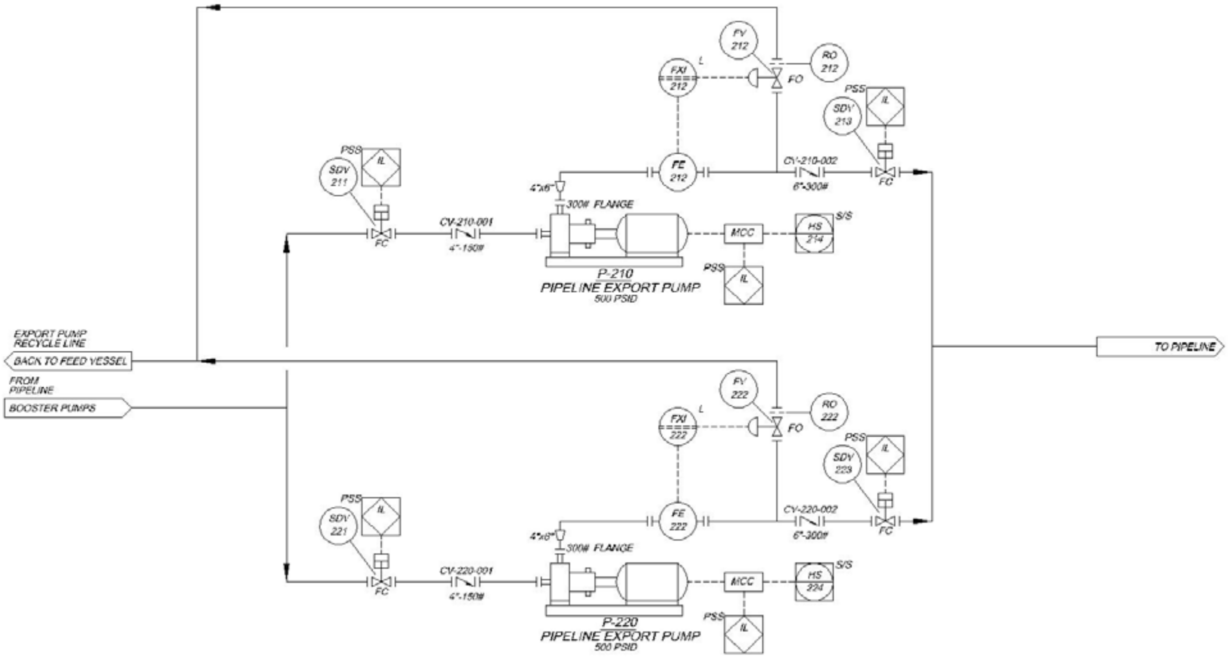
1. Inadvertent opening of HV-110 was considered, but no hazardous consequence of interest identified as RO-113 is designed to limit pressure to downstream piping and closed drain to less than the design pressure of the downstream system.

Outcome Using Double Jeopardy Decision Tree

Many PHA teams are tempted to say that inadvertent opening of HV-110 concurrent with failure of RO-113 is not credible. However, upon closer inspection, the RO may potentially be a source of latent failure. Often there is minimal maintenance or verification of the initial RO installation with no indication of failure until demand is made. Depending on the operating conditions and material selection, the RO may be eroded or corroded, or it may have been initially installed with the wrong diameter. The scenario would ideally be fully developed taking into account the likelihood of a failure or inappropriate installation of the RO. During a LOPA, while failure of a RO may be listed as an enabling condition, the authors' experience is that RO's and check valves are best developed as independent protection layers (IPLs). The list of IPLs may be developed easily after a risk assessment, affording the ability to ensure that the devices are incorporated into an appropriate maintenance routine or inspection regimen.

EXAMPLE 2 – Multiple Failures and Pump Failure

Cause: Failure of Pump P-210



Consequence Developed by PHA Team

1. Both pumps are normally operational. Potential to reverse flow back through failed pump P-210 due to simultaneous failure of pump, check valve, and local recycle loop considered but no consequence of interest as recycle line with restriction orifice is sized adequately to allow full reverse flow back to safe location.

Outcome Using Double Jeopardy Decision Tree

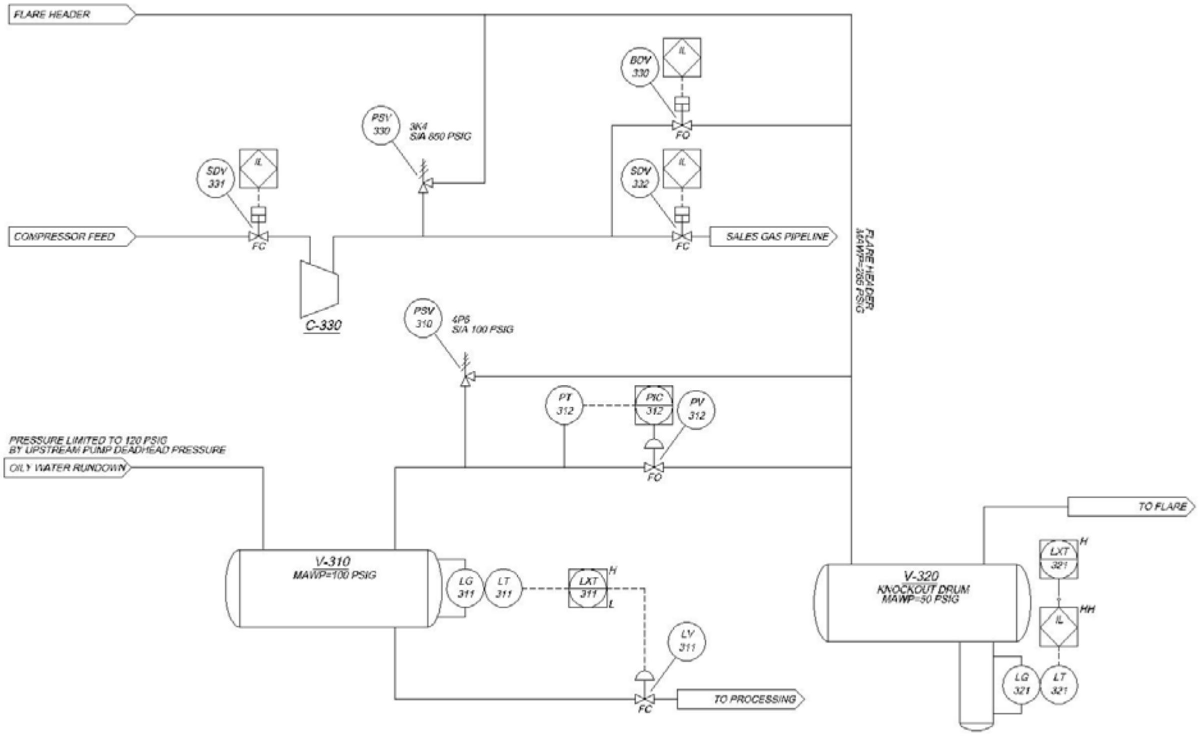
Failure of the check valve, recycle loop, and pump failure are correctly depicted as independent events by the team. However, this scenario has three independent initiating events

(N=3), two of which may be considered unrevealed. The recycle line (which in this case is a local instrumented loop with no DCS visibility) and the check valve (known reliability, but inadequate inspection frequency) are both considered unrevealed failures. Since the number of unrevealed failures (all of which may occur concurrently) is ≥ N-1, the scenario should be progressed along the tree.

All of the initiating events in the example are each assumed to have IELs of 1 x 10^{-1}. This would result in a CIEL of 1 x 10^{-3}. Since the CIEL is greater than the threshold (assuming a 1 x 10^{-5} threshold), this case would be considered a credible event. The consequence ideally would be developed as the potential reverse flow from the pipeline through Pump P-210 with overpressure of the upstream 150 class piping.

EXAMPLE 3: Concurrent Events in Different Operating Units

Cause: LV-311 Fails Closed with Subsequent Blowdown



Scenario Developed by PHA Team

LV-311 on the oily water separator fails closed with potential to overfill V-310 and the flare system. The upstream pressure is limited to 120 psig by the upstream pump's maximum deadhead pressure. Concurrently, BDV-320 opens in response to an upset in the gas compression unit or is inadvertently opened. This leads to relief of high pressure gas into the liquid-filled flare system, and subsequent overpressure or mechanical failure of the flare system or oily water separator. The HAZOP team deemed the two IEs to be double jeopardy and the scenario to be not credible as the IEs occur in two different units.

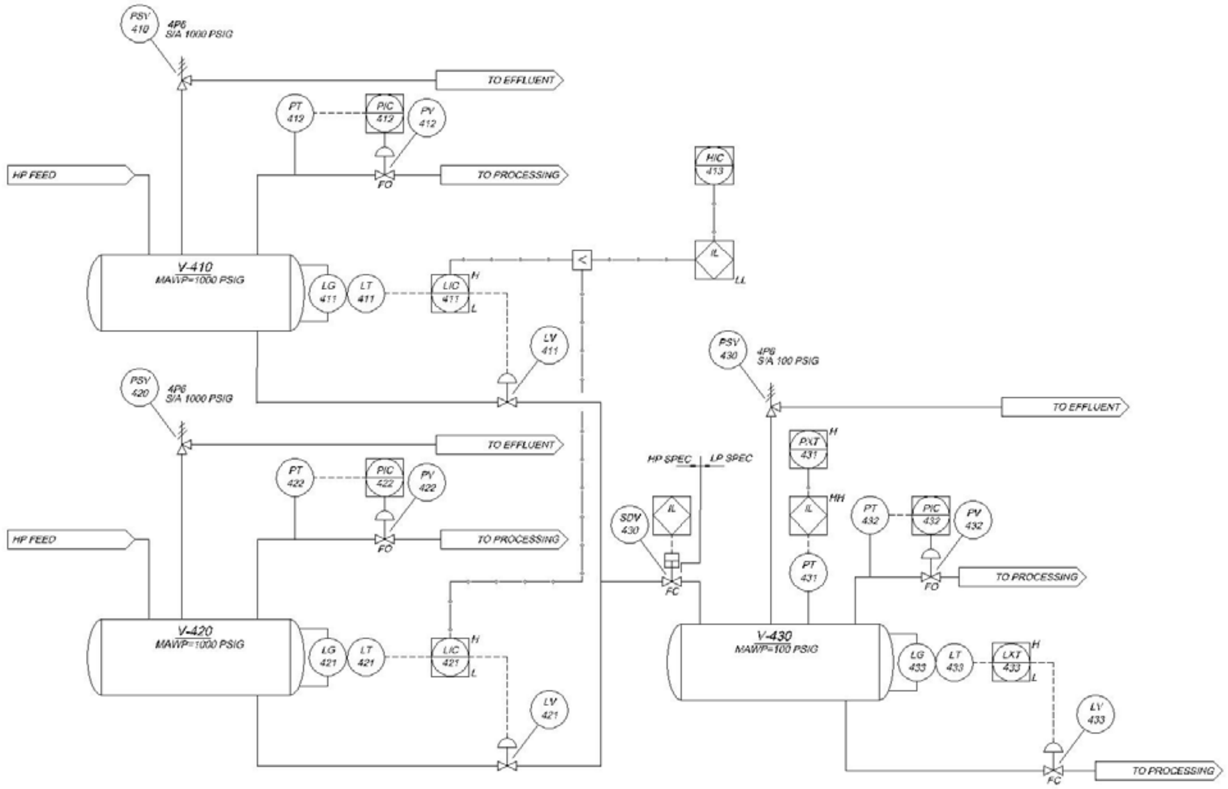
Outcome Using Double Jeopardy Decision Tree

The two IEs appear to be independent; however, upon closer inspection, the two IEs can be shown as having a dependency that the HAZOP team did not identify. In this example, the relatively simple LT-321 interlock on the flare knockout drum shuts down all units feeding into the flare system. This in turn initiates depressurization of the compression unit. The compressor blowdown could occur with a liquid-filled flare relief header; hence, there is potential to overpressure the flare header or oily water separator or to damage the flare piping due to a liquid slug. In this case, although blowdown initiation is designed to serve as a safeguard, it is dependent and attributable to the failure of the level controller LXT-311. Thus, this is a credible scenario that should be further evaluated in the HAZOP.

Modern facilities often rely on complex safety instrumented responses, thereby prescribing multiple actions for any individual trip of a safeguard. These safeguards should be developed for full functionality and response. In this example, the blowdown of the facility concurrent to a liquid-filled flare system is not double jeopardy; in fact, it is designed to perform exactly that function. This example illustrates how secondary consequences may be dismissed as double jeopardy or escalation when in fact they are attributable to a set of dependent IEs.

EXAMPLE 4: Two High Pressure Separators Feeding a Low Pressure Separator

Cause: Failure of Two LVs



Scenario Developed by PHA Team

The HAZOP team correctly identifies two initiating events that could lead to gas blowby and subsequent overpressurization of V-430 via LV-411 or LV-421 failing open. The team evaluates the PT-431/SDV-430 SIF and PSV-430 on the separator for the scenarios and determines that no additional protection is required.

Outcome Using Double Jeopardy Decision Tree

Should the HAZOP team also consider a scenario where LV-421 and LV-411 fail open concurrently or would such a scenario be double jeopardy and therefore not credible? To make this determination, the team will need to consider a number of questions, including the following:

1. Are there any process conditions, either normal or abnormal operating conditions, which could cause both LVs to fail open concurrently? For example, do the inlet streams contain any solids (e.g. sand or wax) that could cause the LICs to incorrectly read the liquid level as high? A further question is do the inlet separators receive input from the same source?
2. Can one level control valve failing open or sticking in the open position be a latent or revealed failure? If latent, then failure of the LV may not be detected until the second LV fails.
3. What is the failure mode of the two LVs? If the valves have been designed as fail open or fail last position, then loss of utilities, instrument air, hydraulics, or electrical power could result in both valves failing open concurrently. In determining the failure mode, the team should consider all of the components that comprise the level control loop, not just the valve actuators. For example, it is not unusual for a level control loop to be designed as fail last position on loss of input signal to the BPCS processor even though the LV is designated fail closed.
4. Are the LVs controlled using a common logic solver? If yes, are there any logic solver failures that could inadvertently drive both LVs open?
5. Are there other common components in the level control valve loops that could cause both LVs to fail open concurrently, such as a common I/O card used for both LICs or both LVs?
6. Are there any operating procedures or practices that would lead to an operator inputting the incorrect set point for both LICs?

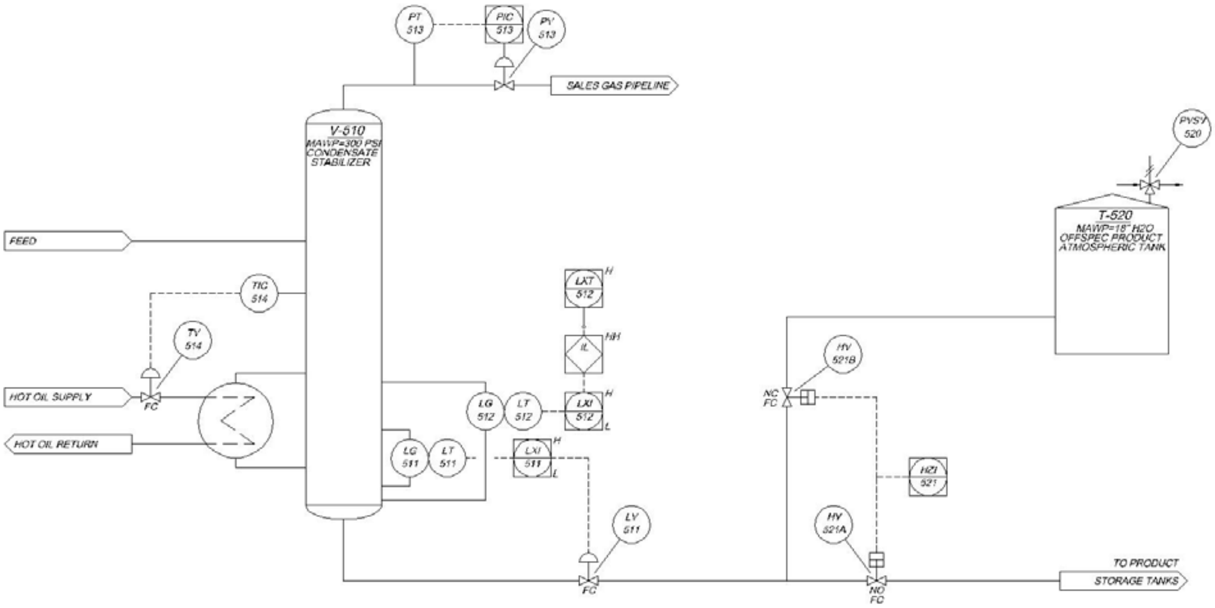
If the HAZOP team determines that LV-411 and LV-421 concurrently failing open is a credible scenario, then the adequacy of PT-431/SDV-430 SIF and PSV should be re-evaluated. Specifically, the team should evaluate the response time of the PT-431/SDV-430 SIF, the capacity of the PSV and associated vent/flare system, and the performance standards of any other safeguards identified.

If the HAZOP team determines that the IEs are independent, then the IE visibility criteria should be applied. Can one LV failing open or sticking in the open position be a latent failure? This could occur if the LV fails stationary with minimal changes in the feed rate or composition or if the downstream system is capable of absorbing significant rate fluctuations. If latent, then failure of the LV may not be detected until the second LV fails. For this case, N-1=1, which is equal to the number of unrevealed IEs. Assuming failure of one LV is latent; the visibility criterion would indicate that this scenario should be considered further as concurrence is available.

Assuming that latent failure of the LV is possible and both high pressure trains are in operation at the same time, concurrent failure of both LVs is credible. The final criterion to consider is the CIEL. A typical level control loop failure rate is 1 x 10^{-1}. However, in accordance with earlier guidance that a group of dependent IEs should be treated as a single IE when calculating the CIEL, this scenario's CIEL should be 1 x 10^{-1} and not 1 x 10^{-2}. The CIEL is greater than the assumed preset CIEL criteria of 1 x 10^{-5}.

EXAMPLE 5: Overpressure of Offspec Tank

Cause: LV Failure During Abnormal Condition



Scenario Developed by PHA Team

1. HV-521A closed and HV-521B open, routing flow to the offspec tank. The team notes that overfilling may result in the potential overpressure of the Offspec Tank T-520. The team determines that the PVSV-520 is adequately sized to prevent the overpressurization of the offspec tank during this operation.
2. LV-511 fails open resulting in gas blowby and overpressurization of the product storage tanks. The team determines that the combination of the LXI-512 and PSVs on the downstream product storage tanks are adequate protection against the potential overpressurization of the product storage tanks.

Outcome Using Double Jeopardy Decision Tree

The team did not consider that failure of LV-511 could occur during the abnormal operating condition of flowing product to the offspec tank, resulting in gas blowby to and potential overpressure of the offspec tank. Application of the Double Jeopardy Decision Tree might determine that contaminants in the offspec condensate or abnormal process conditions could also result in LV-511 inadvertently opening. Assuming the two IEs are independent, applying the remaining decision tree criteria would lead to this scenario being deemed credible, not double jeopardy.

Conclusion

Double jeopardy and its role within engineering design and risk assessment have evolved over the last three decades from informal rules of thumb to explicit definitions in good engineering practice. Nonetheless, PSM practitioners continue to struggle with clear, consistent, and defensible application of double jeopardy, which subsequently introduces inconsistencies across the various hazard identification exercises associated with PSM activities (e.g. pressure relief design and PHAs).

The authors posit the following four criteria as key to determining the credibility of hazard scenarios stemming from multiple IEs:

1. Independence of individual IEs;
2. Visibility of individual IEs;
3. Potential for concurrence of individual IEs; and
4. Combined initiating event likelihood (CIEL) tolerance.

These four criteria have been incorporated into the Double Jeopardy Decision Tree presented in this paper. The decision tree can be used as a tool by anyone trying to determine the credibility of a hazard scenario, such as process engineers performing pressure relief analysis or participants on a HAZOP team.

While it may not be practical due to corporate environments to assess all possible hazard scenarios, the lives of those we serve are worth the time and energy to determine which hazard scenarios stemming from multiple IEs are credible and likely enough to occur. Claiming double jeopardy can be an easy and quick way out of assessing a credible hazard scenario. However, when claiming double jeopardy, it is best to do so from a position of confidence using a consistent and defensible process compatible with good engineering practice rather than using half-hearted questions as answers.

References

1. American Petroleum Institute, API RP 521: Guide for Pressure-Relieving and Depressuring Systems, 4th Edition. API Publishing Services, Washington, D.C., 1997.

2. American Petroleum Institute, API Standard 521: Pressure-relieving and Depressuring Systems, 6th Edition. API Publishing Services, Washington, D.C., 2014.
3. Baybutt, P., *Treatment of Multiple Failures in Process Hazard Analysis*. Process Safety Progress, 2013. 32(4): p. 361-364.
4. Center for Chemical Process Safety / American Institute of Chemical Engineers, Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis. Center for Chemical Process Safety / American Institute of Chemical Engineers, New York, NY, 2014.
5. Center for Chemical Process Safety / American Institute of Chemical Engineers, Guidelines for Hazard Evaluation Procedures, 3rd Edition. Center for Chemical Process Safety / American Institute of Chemical Engineers, New York, NY, 2008.
6. Hyatt, N., Guidelines for Process Hazards Analysis, Hazards Identification & Risk Analysis, 1st Edition. Dyadem Press, Ontario, Canada, 2003.
7. Ireland, J. R., Scott, J. H., and Stratton, W. R., *Three Mile Island and Multiple Failure Accidents*. Los Alamos Science, Summer/Fall 1981. 3: p. 74-91.
8. Perez, J. T., Baum, D., Faulk, N., *Improved Integration of LOPA with HAZOP Analyses*. Presented at 2009 Global Congress on Process Safety, American Institute of Chemical Engineers, Center for Chemical Process Safety.