Managing Double Jeopardy in Process Hazard Analysis

Allison De Man
ACM Automation Inc.
#700, 940 - 6th Avenue SW
Calgary, Alberta
ademan@acm.ca

Guillermo Pacanins
ACM Automation Inc.
#700, 940 - 6th Avenue SW
Calgary, Alberta
gpacanins@acm.ca

Abstract

Double jeopardy is a common process hazard analysis (PHA) term that is often misunderstood and misused. Identifying a PHA cause as a "double jeopardy cause" means that it does not need to be analyzed further, as typical PHA methodologies exclude double jeopardy causes from the analysis. Double jeopardy is defined as the concurrent incidence of two independent initiating events or other revealed failures (1). It is important to understand which multiple failure causes qualify as double jeopardy, and which causes are not considered as double jeopardy and therefore should be considered in the PHA. Many PHA participants are too quick to dismiss a cause because it appears to fall into the double jeopardy assumption. If these causes are wrongly dismissed, important hazardous scenarios may be missed and significant risk gap remains unidentified.

The majority of previous process incidents are the result of multiple failures as they involve a latent failure or are caused by a common mode of failure. It is crucial that multiple failure causes are carefully considered before being excluded from analysis. To make sure that all credible scenarios are identified, PHA participants need to clearly understand the concept of double jeopardy and when to apply it correctly.

Introduction

Process hazard analysis (PHA) studies such as hazard and operability studies (HAZOP) identify credible causes that lead to a process deviation and, in turn, can lead to a hazardous event with severe consequences. These causes are commonly referred to as "initiating events". Types and examples of initiating events can be found in Table 1. Once the initiating event has been identified, the resulting hazardous scenario is determined. The hazardous scenario is then risk ranked, or assessed, for severity and likelihood. Safeguards or independent layers of protection (IPLs) that can provide adequate risk mitigation, are then identified and recorded. If all IPLs fail or are not available during the occurrence of an initiating event the unwanted event may occur. If there are not enough safeguards in place to control the risk to an acceptable tolerable level then recommendations are identified to reduce the risk further.

Table 1. Types and Examples of Initiating Events

Initiating Event Type	**Example of Initiating Event**
Human Failure	Operations Error – Valve inadvertently left closed
Equipment Failure	Control Systems – Equipment failures (control valve)
External Event	Weather Phenomena – Tornado, hurricane, etc.

It is important for the HAZOP team to methodically identify, as much as possible, all the credible initiating events to ensure that the resulting hazardous scenarios include adequate safeguards or recommendations to reduce the risk to a tolerable level; however, a line has to be drawn when considering what is a credible initiating event and what is not. In the case of multiple failures scenarios, where two or more initiating events occur concurrently leading to a hazardous scenario, many combinations of failures can be conjured from the failures identified in the PHA. To analyze all these combinations of failures is a time-consuming exercise and not an efficient use of time in the HAZOP. Double jeopardy provides direction on when it is or isn't credible to address these multiple failure scenarios. Whether or not the multiple failure cases are deemed credible to address, each single initiating event failure must still be analyzed.

The term double jeopardy appeared as a legal term in the Fifth Amendment of the U.S. Constitution (1). Double jeopardy prevents a person from being tried in court twice for the same offense and be twice put in jeopardy of life or limb. Similarly, in the context of a PHA session the term double jeopardy prevents the analysis of two or more independent failures that occur concurrently; however, double jeopardy is incorrectly applied in many PHA studies. There are many multiple failure scenarios that must be considered and analyzed further to ensure adequate controls are place. There are a few key factors to consider before preventing concurrent initiating event failures from being analyzed in the PHA including:

1) Whether the multiple failure events are independent or dependent events. This includes considering failures which can lead to multiple concurrent failures such as the loss of power. These common failure modes can be difficult to identify, but give credibility to concurrent failure scenarios, as these failures can no longer be viewed as independent.

2) The estimated time duration that a failure exists before being detected and corrected. A cause cannot be neglected as double jeopardy if one of the failures is a latent failure, and therefore remains unrevealed long enough that the second failure could also occur resulting in the hazardous scenario. Similarly, even if a failure has been revealed, but the repair time is long enough that a second failure could occur during that time, the concurrent independent failure causes must be considered and analyzed in the PHA.

3) The consequence severity of the concurrent independent failures. There are cases where the consequence of the concurrent independent failures is more severe than the single independent failure cases. Even though, the likelihood of concurrent independent failure is less, the high severity can result in a risk that may need additional mitigation above what is present for the independent failures.

Independence of Initiating Events

Trying to brainstorm every combination of failures in a HAZOP is not a productive use of HAZOP time, especially if those failures are independent failures. An independent failure means that when one failure occurs it does not influence the occurrence of the second failure and vice versa. If one event occurring affects the probability of independent occurrence of the second event then these two events are not considered to be independent. To calculate the approximate probability of occurrence of concurrent multiple independent failures, the probability of each independent failure is multiplied as shown in Figure 1 (2). The multiplication of independent failures results in a low probability of concurrent occurrence. This probability of occurrence can reach a low enough value that it is deemed not credible, and therefore not worth analyzing in the HAZOP. Any combination of independent initiating events are considered to be double jeopardy, and further analysis in the PHA is not required; whether those failures are human, external, or equipment.

Probability of Failure of A = 10^{-2}/year
Probability of Failure of B = 10^{-2}/year

When A and B are independent failures, an approximation of the probability of occurring concurrently is

$P(A \text{ and } B) = P(A) \times P(B) = 10^{-2} \times 10^{-2} = 10^{-4}$/year

Figure 1. Approximation of the Probability of Concurrent Multiple Independent Failures

Independence is a huge factor for determining the credibility of a scenario in HAZOPs and must be verified and validated. For instance, if there is a potential failure elsewhere in the system that can lead to a multiple event failure, that failure event needs to be considered. These failures are commonly a deviation of intended operating mode; abnormal or break-down operating mode and include failures such as the loss of utilities. These failures provide a link of dependency between two initiating event system failures. This need to capture common mode deviation failures in the HAZOP showcases the importance of analyzing abnormal deviations such as loss of utilities and start-up/shutdown operating modes in the HAZOP. Analysis of loss of utilities - such as power, instrument air, water, etc. - facilitates the identification of failures that can lead to multiple initiating events scenarios. Additionally, the analysis of start-up/shutdown operating modes can also identify common cause initiating events such as operational errors leading to the incorrect orientation of multiple valves. Identification of abnormal operating mode initiating events is important to allow analysis of the impact that these multiple scenarios can have on the system.

Revealed or Unrevealed Failures

Whether a single failure is revealed or detected shortly after the failure occurs or remains unrevealed for some duration of time affects whether a multiple failure scenario can be classified as double jeopardy. If the failure remains unrevealed for long enough that a second failure also occurs, then double jeopardy is not applicable to this multiple failure scenario and it needs to be considered in the PHA. These unrevealed failures are typically referred to as latent failures. Latent failures do not have an immediate effect on the system when the failure occurs, otherwise that failure would likely be noticed. Examples of latent failures include a normally opened control valve that fails in the open position, as that failure would not be detected until that valve is needed to close on demand. Depending on the control operation of that valve it may not be called upon to close for weeks or months at a time. This latent unrevealed initiating event failure, along with another independent initiating event failure, could lead to a hazardous multiple event scenarios.

If two independent initiating events were found to credibly occur concurrently (e.g. one initiating event was unrevealed) then the probability of occurrence of each event would be added to determine the probability of occurrence of the multiple failure case. This addition of credible concurrent independent failures can be shown in Figure 2. This scenario is still very probable to occur and the concurrent failure should therefore be considered in the HAZOP.

Probability of Failure of A = 10^{-2}/year
Probability of Failure of B = 10^{-2}/year

When A and B are independent failures, but one failure is unrevealed the probability of occurring concurrently is

P(A and B)= P(A) + P(B) = 10^{-2} + 10^{-2}= 2x10^{-2}/year

Figure 2. Probability of Credible Concurrent Independent Multiple Failures

The analysis of multiple concurrent failures can also be applicable if the repair time for a revealed failure is long enough that a second failure could occur during that time. The time required for detecting, diagnosing and correcting the failure needs to be considered when determining the failure duration. Long durations of corrective action for a failure, along with the occurrence of another independent failure, can result in a credible multiple failure scenarios that need to be considered in the PHA study.

Incipient failures can be considered in the same way as latent unrevealed failures; incipient failures are also not considered double jeopardy when occurring concurrently with another initiating event. Incipient failures are the result of imperfections in the condition or state of an item that will degrade over a relative long period of time resulting in a critical equipment initiating event failure if continuous monitoring and corrective maintenance action is not taken (3). Incipient failures such as corrosion and flange leaking occur over a long period of time, and therefore have a relatively low probability of occurrence. Even though the probability of an incipient failure occurring concurrently with another initiating event is relatively low, the resulting consequence severity may be so severe that the scenario must be considered for analysis in the PHA.

Consequence Severity

As previously mentioned, the probability of occurrence of two concurrent independent initiating events is typically very low (rare event approximation); however, there can be cases where even though the probability of occurrence is extremely low (incipient failures) the severity of the multiple failure hazardous event can be so severe that the resulting risk level may require analysis in the PHA. This is especially important in scenarios where the resulting concurrent failure can have a more severe outcome than each independent event failure.

It is also often assumed that the safeguards put in place to protect against one independent failure should also help to mitigate against the concurrent failure of two independent events. However, there can be cases where the safeguards are found to be inadequate to mitigate against the multiple concurrent failure scenario because of the increased severity and resulting risk level. Additionally, there can be instances where certain safeguards can be deemed unnecessary for the lower severity independent failure case and not listed as mitigation safeguards. These safeguards would then be missed when identifying critical safeguards if the high severity scenario that they are required to protect

against were not analyzed. This underestimation of the risk of a scenario is also an issue if these high risk scenarios are being addressed in additional studies such as Layer of Protection Analysis (LOPA) or Qualitative Risk Assessment (QRA). Neglecting to analyze high severity multiple concurrent failure scenarios can leave an unacceptable level of risk that lacks adequate risk control.

What events are not considered "Double Jeopardy"?

Chain reaction events, knock-on events, failure of safeguards or IPLs, existence or non-existence of conditional modifiers or enablers are not double jeopardy events in a PHA analysis. Examples of these events can be found in Table 2.

Chain reaction events, also called cascade or sequential events, are not double jeopardy events. Chain reaction events are the result of one failure triggering another failure; these failures occur sequentially one after another. Typically chain reaction events are included in the hazard development mechanism as the root initiating event leads to the resulting hazardous consequence scenario.

During the HAZOP session the team may identify multiple failure scenarios that involve an initiating event failure along with the failure of a safeguard. The occurrence of an initiating event along with the lack of response of a safeguard(s) is already taken into consideration when developing the hazardous event scenario, as the hazardous scenario only occurs if the safeguard(s) fails. This leads to the importance of independence, diversity, separation, reliability, and availability in safeguard selection. One needs to be certain that the listed safeguards will provide the required control when called upon to prevent the consequence, or protect the system from damage.

Knock-on events are events that occur as the result of failure events in other process units, or adjacent process areas of the same facility. Knock-on events can include impacts from fire, explosion, loss of containment, etc., resulting from a hazardous scenario occurring in another area or process unit. Analyzing the impacts of knock-on events occurring concurrently with an initiating event are not considered to be double jeopardy. Concerns around the location of adjacent units and their potential impacts should be discussed in siting studies, or addressed as a siting concern during the PHA study itself.

The existence or non-existence of conditional modifiers and enablers along with an initiating event failure are not considered to be double jeopardy as these conditional effects do not initiate a hazardous scenario by themselves. Enabling conditions are similar to latent conditions in that they usually occur before the initiating event, but don't lead to a hazardous scenario themselves (2). Conditional enablers do, however, make scenarios possible as they are a contributing cause/factor that leads to the hazardous event. The qualitative probability of existence or non-existence of conditional modifiers is included in the scenario risk ranking assessment. Conditional modifiers affect the probability of the consequence (e.g. fatality) instead of reducing the probability of occurrence of the hazardous event (e.g. vessel rupture) (1). An example of a conditional modifier is the probability that a person would be in the area, and therefore be impacted, when the hazardous event occurs. An example of a conditional

enabler, is the presence of an ignition source, where the hazardous event will only occur if that ignition source is present to enable the scenario.

Table 2. Examples of failures that are not double jeopardy

Failure Type	Example
Chain reaction	Control valve failure creating vacuum and pump failure
Safeguard/IPL Failure	Blockage of a PSV
Knock-on events	Fire in an adjacent unit
Conditional modifier	Probability that a person would be in the hazardous area
Conditional enabler	Presence of an ignition source

What Events are considered Double Jeopardy?

Double jeopardy is applicable for two separate independent and concurrent initiating events leading to a process deviation from the intended design. As long as the initiating events are independent, revealed, have a low probability of concurrent occurrence, and do not result in an extremely high consequence severity, they do not need to be considered concurrently as an initiating event in the PHA analysis.

Double Jeopardy Case Study

On August 28, 2008, an explosion at a Bayer CropScience pesticide manufacturing facility in West Virginia killed two workers and injured eight others. The explosion was the result of a runaway chemical reaction inside a pressure treater vessel, that over pressurized and ultimately exploded the vessel (4). The vessel was abruptly brought back into service after a lengthy maintenance period even though maintenance was not concluded on the system. The first initiating event occurred during the start-up mode, a high concentration of methomyl-containing solvent was sent to the treater (a combination of human errors led to this event). The second initiating event was the failure to pre-fill the treater with clean solvent. These two initiating events were independent (although both the result of human errors in sequence). The concurrent occurrence of these two independent initiating events, along with the failure or inadequacy of the safeguards present, lead to the runaway reaction and resulting explosion. The two initiating events appear to fall under the double jeopardy assumption, and therefore would not have been analyzed in the PHA session; however, if all modes of operation had been discussed during the PHA session, concerns around the start-up mode and credible concurrent failures may have been identified. If the credible concurrent start-up mode initiating events had been identified, adequate safeguards may have been in place to prevent this hazardous scenario.

Contribution of Root causes

Major accidents generally involve more than one cause. More commonly, half a dozen root and contributing causes were identified as playing a part in the occurrence of the major accident (5). In PHA studies only the causes and initiating events at the physical process level are identified. This means that

double jeopardy is only credible for causes at that process level. This is of concern, as many of the root causes that lead to these hazardous events are found at the process safety management (PSM) level. These roots causes can include elements such as inadequate training and inadequate maintenance and integrity programs. These PSM root causes can influence the independent concurrent multiple failure cases. Unfortunately, the PHA is not the place to discuss or identify the presence of management organizational, PSM, issues. This goes to show that no matter how detailed or meticulous the PHA itself is, there still can be underlying organizational PSM issues that can affect the physical root cause of a major incident. Process hazard analysis is vulnerable to organizational PSM issues; research and development is being conducted today to identify the relationship between the safety emergent properties of physical and organizational safety management safety systems (6) (7).

Conclusions

It is important that careful consideration goes into determining if two or more initiating events can be considered as double jeopardy or not. If these initiating events are wrongly dismissed, important hazardous scenarios may be missed and a high risk gap could remain unidentified. The following questions should be asked in the PHA session when multiple initiating event failures are brought up, to determine if double jeopardy can be applied.

- Are the initiating events independent or is there a common cause failure mode that could lead to both initiating events occurring?
- Are the failures revealed failures? Would you know if one of the failures occurred, or could one failure be a latent failure that remains undetected?
- Is the resulting consequence severity of the concurrent independent failures high enough to be considered an extreme risk?

If the initiating event failures are independent (of very low probability), revealed, and do not result in a high consequence severity, then the concurrent initiating event failures are considered to be double jeopardy and do not need to be analyzed further in the qualitative PHA.

References

1. **Center for Chemical Process Safety.** *Appendix A: Simultaneous Failures and "Double Jeopardy", in Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis.* Hoboken, NJ, USA : John Wiley & Sons, Inc., 2013.

2. *Treatment of Multiple Failures in Process Hazard Analysis.* **Baybutt, Paul.** 2013, AIChE, pp. 361-364.

3. **API STD 689.** *Collection and Exchange of Reliability and Maintenance Data for Equipment, First Edition.* July 2007.

4. **US Chemical Safety Board.** *Investigation Report: Pesticide Chemical Runaway Reaction Pressure Vessel Explosion, at Bayer CropScience, LP, Institute, WV, on August 28, 2008.* January 2011. Report No. 2008-08-I-WV.

5. *Oversights and Omissions in Process Hazard Analyses: Lessons Learned from CSB Investigations.* **Kaszniak, Mark.** 264-269, s.l. : Process Safety Progress, 2010, Vol. 29.

6. *Risk Management in a Dynamic Society: A modelling Problem.* **Rasmussen, Jens.** s.l. : Safety Science, 1997, Vol. 27 No. 2/3.

7. **Leveson, Nancy G.** *Engineering a Safer World.* s.l. : The MIT Press, 2012.