Chemical Hazard Engineering Fundamentals (CHEF) Q&A

Disclaimer:

Introduction

Hazards might be activities? Or its chemical-based hazards? Next week sessions cover Other Hazards which involve "energy related" hazards.

Are risks quantified or consequences like losses, business interruption, environmental clean-up, allow cost/benefit analysis for informed decisions? Estimates of consequence severity are highly uncertain and not very accurate. Utilizing a cost/benefit analysis can be done but may not be worthwhile.

Flammability Hazards

How does CHEF or RAST estimate the flash point of a mixture? CHEF and RAST use the lowest flash point of any component in a mixture which may be conservative representation of the mixture. RAST will also display an estimate based on the temperature where the estimated mixture vapor pressure divide by atmospheric pressure is the lower flammable limit. This technique is not very accurate as the liquid mixture may be very non-ideal and liquid or vapor composition may change with even small levels of evaporation.

Does CHEF or RAST have dust explosion calculation provision. If not, can you guide what tool can be used which could be as simple as CHEF or RAST? The method (Baker-Strehlow-Tang) we will share in the explosion module might be reasonably applied to dispersed solids (to give order of magnitude results) but this method is not validated for dust explosions. The explosion peak overpressure estimates in CHEF and RAST are based on a typical heat of combustion per volume (such as a stoichiometric vapor concentration of fuel or within the explosive range for dusts).

Is LEL & UEL applicable for dust? or we should consider MEC for dust? The Minimum Explosive Concentration is more appropriate for dusts than Lower Explosive Limit used for vapors and can often be determined experimentally. However, there are other variables for dust such as particle size making determining an accurate MEC often more difficult than an accurate LEL for vapor.

Formerly we used LEL (Lower Explosive Level), is more technical use LFL? These terms are often used interchangeably.

How do we know which NFPA standards are laws and which are recommended practice? In the US, some states or local building codes require RAGAGEP (Recognized and Generally Accepted Good Engineering Practices) be followed. The US Process Safety Management (PSM) requirements reference following RAGAGEP for equipment inspection and testing in PSM-covered processes. These are employer responsibilities and up to each company to resolve.

What is considered low and high MIE? Examples with ignitions sources we normally have inside the facilities? The MIE for many organic vapors is less than 1 mJ such that one would consider almost any ignition source could deliver. The MIE for dust ranges from less than 5 mJ to greater than 500 mJ. Often the ignition source is an electrostatic discharge which can range from 20 mJ for human static discharge to 1000 mJ for conical pile discharge to 3000 mJ for a spark. The energy from direct flame (fired equipment, combustion engines) or cutting and welding can be even higher.

About hybrid mixtures, the decrease of the MIE is due to the combination of a flam. liq. and comb. dust, or it could also be possible with non-combustible dust? The MIE for hybrid mixture typically is the result of the flammable vapor even for a non-combustible dust.

Toxicity Hazards

How to estimate ERPG-3 for substances that are not on the list? and for mixtures? I would normally work with a toxicologist if I could not find a value for ERPG, AEGL or TEEL to work from. I am not familiar enough or qualified to try to estimate a value from similar compounds. Once a value is known for each of the compounds in a mixture, we can use the correlation shared in the presentation to estimate a mixture value.

1000 ppm thresholds for toxic screening but recent incident in India with styrene leak (ERPG-3 1000 ppm) had multiple fatalities. So is it reasonable threshold? Any threshold values would depend on what your company determines and the “greater than 1000 ppm” is only an example criterion for screening. Styrene has an ERPG-3 of 1000 ppm, so I personally would not exclude it but it is not typically considered acutely toxic. It could be a valuable exercise to perform a simple toxic evaluation of the recent incident to see how the results compare to observations.

Have the LD and LC values used in CHEF and RAST been adjusted for humans? Yes. The values used in CHEF and RAST are derived from Probit Models or published ERPG or PAC values. These models are based on animal testing and extrapolated for differences in respiration rate, etc. in humans.

Is the ERPG term just for US or for Europe also? Emergency Response Planning Guidelines (ERPG) were developed by the American Industrial Hygiene Association (AIHA) but used globally. The AIHA periodically reviews these values and updates them as more information becomes available. Another commonly used criteria is the Acute Exposure Guidelines Limit (AEGL) developed by the US Environmental Protection Agency.

Reactivity Hazards

Any literature source to get the transfer coefficients (U) and activation energies (AE)? Heat transfer coefficient information is common from internet or literature searches. Activation Energy is more difficult to find other than literature for specific kinetic studies. A typical value is 25 to 30 kcal/gram mole and would represents approximately doubling of the reaction rate each 10 C increment.

What should be the temperature basis for storing reactive chemical? Ideally one would store a reactive chemical well below the temperature of no return. If that is not feasible, one would want a very large "time to maximum" rate (months or longer) such that the material is consumed in the manufacturing process long before significant decomposition (or other undesired reaction) takes place.

Should there be a safety margin applied to no return temperature for storing reactive chemical or just below it is fine? With many of the simple correlations shared, this is a high degree of uncertainty such that a safety margin is prudent. As the kinetic parameters (such as activation energy and rate constant) are more accurate, a lower safety factor such as 10 C may be appropriate.

How often do you see chemical reaction hazards arising from dusts alone? In addition to the flammability characteristics of dust, many solid materials are also unstable at elevated temperatures. Drying solids is a unit operation where them may be reaction hazards with dust alone.

You talked about the n-order of reactions. What's the significance of the order "n", apart from fitting the curve? The order of reaction is typically determined experimentally from the reaction rate as a function of reactant concentration. It may provide some indication of the reaction mechanism.

How do you design pressure vessel against vacuum condition? Vessels are often protected against vacuum conditions by a vacuum relief device. Vessels may be designed to contain full vacuum by the thickness of the metal used and fabrication technique such as reinforcing rings.

Other Hazards

How to account for Hydraulic Shock during PSV relief scenario. Pressure rise is more rapid then PSV can handle. This can be an issue if the pressure rise rate is very rapid such as for an internal deflagration or detonation. In some cases, a PSV or explosion panel may not be effective in protecting the equipment in very rapid pressure rise situations.

Is there a rule of thumb to apply for at which pressure a pressure vessel would fail (in relation to its design and/or test pressure)? As many regulatory or RAGAGEP safety factors for pressure vessels is approximately 3, assuming rupture could occur at 1.5 or 2 times the maximum allowable working pressure (MAWP) or the maximum pressure to which it is hydrostatically tested may be appropriate.

Water Hammer: Pmax is at the valve that closed or at the pump discharge? Where should I protect the system? The maximum pressure is generally at the terminal point (closed valve, etc.) in the direction of flow but there may be reflected pressure waves causing a high pressure at the initial point as well. One may want to consult a subject matter expert in fluid flow.

Will LNG Rapid Phase Transitions be considered as other hazards? Rapid Phase Transition (or extremely rapid – essentially explosive - vaporization of liquified gas) is certainly a hazard and related both the release pressure-volume energy and thermal energy.

Hydraulic Hammer: Also column separation after a closing valve and the shortly later resulting liquid flowing backwards creating a hammer may be an issue? Yes, similar to cavitation, the sudden downstream pressure drop from valve closure may induce vaporization followed by rapid condensation as pressure recovers.

Would it not be more safe to design a rupture disk to avoid such thing (Hydraulic Shock)? DIERS addresses hydraulic shock for reliefs of 2-phase flow.

Temperature increases, and thus pressure increases, from adiabatic compression of vapor in a line should also be considered in the hydraulic shock scenarios? Maybe, but the vapor temperature discharging a compressor is typically much higher than the inlet temperature (which is why discharge coolers are common). If the cooler fails, the pipeline may heat an undergo thermal stresses. The temperature may reach the autoignition temperature if the compressed material is flammable.

Experience and Historical Incidents

What are good references for historical incidents? The US Chemical Safety Board publishes results from major incident investigations that contain a tremendous amount of information (and often video reenactments of the event). There are also two books from CCPS: Incidents That Define Process Safety 1st Edition (2013) and More Incidents That Define Process Safety 1st Edition (2019).

Inherently Safer Design

Do you consider the fragile welding or rupture explosion door as a passive measure as well, and therefore you make take credit in the risk analysis? The CCPS Book Guidelines for Initiating Event and Independent Protection Layers in Layers of Protection Analysis page 202 notes "Frangible Roof on a Flat Bottom Tank" as a protection and if properly designed, the tank bottom is anchored, and tank foundation is in good condition suggests a probability of failure of demand of 0.01. This reference also notes "Explosion Panel on Process Equipment" on page 208 as a protection if properly designed, explosion routed to a safe location, and routinely inspected.

"Simplify" does not by itself meet the ISD definition of reducing or eliminating the underlying hazards. Why is it included as an ISD approach? Simplify should reduce the likelihood of human error and the likelihood of an incident. As you note, simplify does not truly reduce or eliminate a hazard as other ISD approaches.

Nearly every company I've worked with fails miserably to decommission old piping. How do you influence them to spend at a higher level to remove unused equip? How can one do a cost benefit analysis for getting business minded people to buy in an idea of inherent safety? This is somewhat a cultural issue similar to buying insurance. If decommissioned equipment is not removed, then hopefully it is well identified (painted unique color, etc.) and inspected to insure it remained disconnected and in a "safe" state.

Often ISD is applied to new designs only. Indeed, it's easier, but also for existing processes very beneficial. What is your experience for existing plants? I have had a few major ISD implementations for an existing facility. One was a process using a toxic intermediate and the process was modified to produce this material in situ (consuming it as it was produced rather than storing it). This required a significant capital investment to modify the equipment. In another, during startup of a new process, an undesired impurity was found. We modified the reaction to run at much lower temperature by adjusting the reactant and solvent concentrations while using the same equipment.

Would a passive barrier be considered ISD or would it be a safeguard or IPL? Does it get credit? If the passive barrier truly cannot fail, I credit the reduction in consequence severity (such as a dike or bund minimizing the surface area for pool evaporation, or venting through a tall stack to minimize ground elevation concentration) but include these barriers in the plant inspection program (dikes free of clutter, all cracks sealed, etc.) to make sure they are maintained.

Could ISD be skipped if a mature process is evaluated? Once the investment is made and the risk is managed to a tolerable level, I believe continued evaluation of ISD may not be productive.

Is a Pressure relief valve an active barrier? Yes. The upstream pressure is detected by a spring or other mechanical means which then opens the relief device.

Doesn't increasing the design pressure. actually increase the potential bursting vessel explosion hazard, since if the vessel does rupture, more energy is released? Higher design pressure is not always good. example: runaway reaction, at higher pressure of release will run at higher rate as temperature will be higher. Yes, the explosion energy is increased but the likelihood of failure is decreased. This is a good example that often risk or hazard analysis involves a "balance" rather than a single right or wrong answer.

ISD study or analysis has to be done at the start of process design -what are the methods by which we can study and say the design is safe? ISD evaluation is best early in the life cycle. I have seen "Checklist" used effectively, particularly within companies with significant design expertise. Within the business I worked in, we set up a formal review at the Conception life cycle stage to review chemistry, solvents, process conditions, etc. for ISD opportunities.

Hazard Evaluation Techniques

Are there good tools for doing PHAs? We use Excel. Very difficult to keep it from getting chaotic with all references etc. There is software available such as Leader, PHA-Pro, PHAWorks, etc. to help with documentation but I believe Excel can also work well. Keeping track of all the Initiating Causes and Consequences particularly across different Nodes can be a challenge.

Do you consider the failure of safeguards like valve in a car seal Program in wrong position, Loss of nitrogen to a flare (Valve failure), or sis valves fail? Do we consider the failure of the safeguarding? e.g. consider the failure of the SIS, then we have the action/recommendation to do the accurate loop test? Generally, failure of safeguards or protections are not Initiating Causes for the scenario they are designed to help mitigate. Three examples:

1. A PSV can be (and probably is) a safeguard for the overpressure scenario. However, it can fail open and as such become the initiating cause for a loss of containment scenario (not related to overpressure)
2. A check valve can be a safeguard for reverse flow, but can stick in the closed position becoming the initiating cause for the low flow deviation.

3. A SIF with a shutoff valve into a tank may be a safeguard for high level, but can fail closed becoming the initiating cause for low flow/high pressure

In Layers of Protection Analysis, if the Initiating Cause is extremely frequent (a special case or "high demand mode"), then one might consider the failure <u>frequency</u> of a protection (rather than its probability of failure on demand) to determine overall scenario frequency.

Has CHEF been validated/verified by CCPS member companies? If yes, are the names of the committee members published? CHEF uses correlations from the CCPS literature and other references. Often there are several methods available and one was selected for CHEF based on ease of use, simplifying assumptions, and comparison of results with more advanced techniques. There has not been a formal "validation" process by CCPS at this time.

Is RAST a substitute of a HazOp? RAST is not a HAZOP but includes the concepts of Nodes, Parameters and Deviations to generate a structured checklist of suggested scenarios based on user inputs to start from. It is not a complete list of scenarios and an evaluation team needs to also consider Parameter Deviations not included in the initial list, other Initiating Causes for the Loss Events noted, and interactions with other process Nodes. Also, HAZOP by its nature is performed by a team while it is possible (but not recommended) that evaluation using RAST be done by a single analyst.

Do you consider Deviations, Causes, Consequences and Safeguards outside of a Node while doing HAZOP study of a certain Node? Yes, the interactions with other Nodes need to be considered. One way of doing this is to consider only Initiating Causes associated with the Node being studied that may have Consequences in other Nodes ("local" cause and "global" consequence). In this way, a scenario with a Consequence associated with the Node being analyzed but not an Initiating Cause could be captured as "no local causes". This scenario would be captured when evaluating the Node in which the Initiating Cause occurs. One may also use an approach of "local" Loss Event and "global" Initiating Causes. The team needs to be consistent in the approached used to capture interactions between Nodes to ensure these are not missed.

What would be the key aspects of a good interaction between HAZOP and Fire Hazard or Fire risk assessments? HAZOP could identify situations or scenarios where fire could occur and capture fire protection safeguards. The physical location of process nodes where fire scenarios are identified my help to determine the most appropriate fire protection technique (fire monitors, water spray, fireproofing of structural members, etc.).

Is the library-based HazOp approach basically a "checklist"? We might categorize the library-based approached as a "checklist" but it is also a structured approach if based on process parameters with deviations that could lead to an incident.

How do you address double work with PHA deviation "pressure high" and the relief design worst case checklist effort (e.g. according API scenarios)? I believe the relief design worst case scenarios are generally realistic PHA scenarios, so I don't view this a "double work". "Pressure High" is a very broad and common process upset and often related to other parameters such as “Temperature High leading to Pressure High”, or “Reaction High leading to Pressure High”, etc.

How to address endless discussions on what is credible or stacked scenario or double jeopardy? When the discussions are to clarify the scenario, it is normally helpful. However, when there are conflicting opinions, particularly on what is credible, I have found that a semi- or simplified quantitative estimate often helps. Often these estimates can be done by a team member “off-line” and report results back to the team. If sometimes find “double jeopardy” questions (two events occur in the same time frame) may be addressed by determining if one of the events could be a “unrevealed failure” or the events are actually related (not independent of each other). I also find that sometimes a scenario is too complex with multiple loss events for effective evaluation. Breaking these into smaller scenarios with only one Loss Event may help.

> For example: Overfill in Node 1 causes a flammable spill which ignites resulting in a pool fire that causes excessive heating to adjacent equipment (Node 2) which explodes sending projectiles which penetrates nearby equipment (Node 3) resulting in a hole with subsequent release of toxic material … could be broken into 3 *related* scenarios with one Loss Event each and the Initiating Cause being the Outcome of the scenario preceding it. (Scenario 1 – Overflow release causes a pool fire in the area. Scenario 2 – Fire in the Area causes excessive heat and rupture of equipment. Scenario 3 – Rupture of equipment causes projectiles to damage equipment resulting in a toxic release.)

This process obviously takes a lot of time. Are there time-estimating tools with node count and deviation count? The CCPS book <u>Guidelines for Hazard Evaluation Procedures</u> 3rd (2008) gives some guidance on the time required for various techniques. Time varies significant with the size and complexity of the process. For example: HAZOP of a “large process” may require 2 to 4 weeks of Preparation followed by 2 to 6 weeks for Evaluation followed by 2 to 6 weeks for Documentation (with Preparation and Documentation being essentially the Scribe and Team Leader and Evaluation including other team members). A Checklist evaluation of a “large process” may require 1 to 3 days Preparation, 3 to 5 days for Evaluation and 2 to 4 days for Documentation.

Some of the deviations can be combined. Like LOW and NO pressure. Is it a good idea to combine deviations in order to save time? If the deviations are truly the same, combining may be appropriate. Low Pressure meaning less than the normal operating pressure may be different from No Pressure which might be interpreted as Vacuum.

Is there a max time allowed between "red lining" and CAD of P&ID (per OSHA/ EPA, or as recommended by CCPS)? The maximum time is likely per company management of change policy or interpretation of regulatory requirements.

Are Failure of lines/leakages considered as cause for No Flow? They lead to loss of containment which is a different safety consequence in itself. Failure of lines can be considered a cause for no flow, low flow, or “other than” flow and (as you note) result in loss of containment scenarios. There may be other consequences of “no flow” that represent other scenarios. All of these should be considered.

For a line which has potential for Reverse flow, Is Passing of NRV considered as cause for Reverse Flow? Or is NRV considered as safeguard? An NRV or check valve is normally considered a safeguard. The situation leading to backflow such as failure of a pump where the downstream pressure (or hydraulic head) is higher than upstream pressure would be a potential Initiating Cause.

Whether Start-up and Shutdown need to be discussed as apart of Node or as a whole system separately? I typically consider different process steps (such as start-up or shutdown) as another Node involving the same process equipment. Design Intent and Operating Conditions (and sometimes chemical composition) are often different in different steps.

Is it recommended to include the evaluation of likelihood and severity before and after safeguards are discussed? Safeguard discussion can occur once the scenario has been defined. However, evaluation of risk (likelihood and severity) will be needed to determine the total risk reduction or total number of protections needed to meet a company's risk tolerance criteria.

Does a team spend time determining if the Probability of Failure of DCS control based upon PM or use of probability/severity tables from plant or industry used? Ideally the company has provided guidance for PFD if industry tables are not to be used. I believe these tables (such as in the CCPS book Guidelines for Initiating Events and Independent Protection Layers) are a good starting point.

How would you deal with companies hiding information in a HAZOP? How do you address people not forthcoming with design failures? Ideally the HAZOP leader would have access to Incident, Near Miss and other reports for the company and the specific facility. Reviewing these reports as part of the HAZOP preparation may help in asking appropriate questions during the review to flesh out some historical design or other issues.

Is it generally the responsibility of the facilitator to develop the design intent for all process nodes prior to the HAZOP? The facility may develop an initial draft of the Design Intent for the process Nodes but the team should review and update them as part of the review. This helps to get all team members focused on the Node being evaluated.

How do you risk rank extreme weather condition such as hurricane, flood etc.? What is reasonable probability (frequency) of this event? There is information from the National Weather Service regarding extreme weather and average number of lightning strikes per year for various locations. This may be a good starting point.

If there are many overpressure cases for a vessel and PSV is provided for governing case out of those. Can the same PSV be regarded as safeguard for all cases. I believe the same PSV can be a safeguard for multiple overpressure scenarios of the same equipment or node. However, the demand on this safeguard increases with each scenario, so the risk reduction credit or probability of failure on demand for a specific scenario may be reduced in a detailed risk analysis. For example, if there are 2 overpressure scenarios with the same overall scenario frequency, the demand is doubled and corresponding probability of failure on demand halved.

I don't understand cause by cause vs deviation by deviation. Why would you want to further develop a cause like seal leak (especially if there is no significant consequence)? These differences will be addressed in next week's presentation on HAZOP. I agree that if a Loss Event such as seal leak does not result in a significant consequence, there may be little value in identifying additional causes for the seal leak.

Do you do risk ranking and assessment as part of the HAZOP? I think relative risk ranking may help determine the scope of a HAZOP or which nodes to include.

Is it really important to consider drain and vent line for HAZOP? This can be a decision of the HAZOP leader. I normally only look at this scenario for highly hazardous materials.

Include special case node deviations like exceeding a reactive chemical temperature limit? Or is that just required PSI? Exceeding a critical temperature limit is a good scenario category to consider. The team would need to identify the Initiating Causes such as cooling system failure and consequence of a runaway reaction such as equipment rupture or relief system discharge.

For two pumps running in parallel (2x50%), when we consider pump failure as a cause, do we consider both pump failing at the same time? There is more than one way that this situation might be addressed. Having a second pump always running in parallel may be a safeguard for the pump failure scenario. Considering both pumps failing at the same time would depend if the pump failure is quickly detected (revealed) and the repair time to get the second pump back on line is small.

I see pump cavitation covered in no flow when it is really pressure. Any advice to get a team to cover deviations in the right place? Many parameter deviations are inter-related. Loss of Flow can lead to High Temperature which can cause High Pressure. In the end, it may not matter which parameter deviation initially led the team to consider the scenario.

Is it best for a team to cover all causes even if there are no safety consequences? i.e. several valves in a line or plugging all lead to the same consequence. It may be good to capture causes or groups of causes which result in little consequence of concern but not spend time evaluating them. This may help future teams understand why these were excluded from the study.

Where can I find a scenario library? Thanks. Some commercial PHA software contains libraries. A checklist of overpressure scenarios can be found in the National Fire Protection Agency (NFPA) literature. Also several companies develop a library of scenario for consideration.

Whether process shutdown shall be considered as consequence for asset loss or not? This depends on the agreed upon scope of the study. Does the study focus on Human and Environmental Harm only or does it include Business Interruption or Loss?

In flare node, loss of nitrogen to a flare is considered as a safeguard when there is a high temperature. Should valve fails on nitrogen to flare be included. There are many different types of flares. If, in the system you have, loss of nitrogen is truly a safeguard then it likely would not be the Initiating Cause for high temperature.

Hazard and Operability Study (HAZOP)

How to differentiate and decide between structured what-if (SWIFT) and HAZOP? We use SWIFT... Structured What IF Technique... how this is different from HAZOP? HAZOP is a form of structured What-If applied to each process Node. SWIFT is a systems-oriented technique. SWIFT was developed as an alternative to HAZOP in situations where HAZOP is not effective.

What about FMEA? Failure Modes and Effects Analysis is an excellent Hazard Evaluation technique particularly to help improve the reliability of equipment components and systems.

What's the trigger to move from HAZOP to HAZOP-LOPA? Is severity, likelihood, risk ranking always used with a what-if? I have never seen it without it. Each company may have specific protocols and requirements. Some companies incorporate a very simple risk analysis (often a simple risk matrix) in concert with Hazard Evaluations while others may want to see a more detailed risk analysis such as Layers of Protection Analysis. HAZOP and What-IF are very effective at identifying scenario Causes and Consequences. LOPA is very effective at evaluating the effectiveness of Protective Layers for scenarios. Many companies have the Hazard Evaluation team continue with the Risk Analysis. Other companies assign separate teams for Hazard Evaluation versus Risk Analysis.

Is RAST a type of a checklist? RAST is a structured checklist that uses concepts of process Nodes, Parameters and Deviations to develop a suggested list of scenarios to build upon.

Is bow-tie a hazard evaluation technique? Since bow-tie combines Fault Tree and Event Tree for a single Loss Event, it is an effective technique to look at scenario details.

How to handle Domino Effect? Is there a particular assessment method which is more suitable? Domino Effects often involve the interaction between process Nodes or continuation of a complex scenario with multiple Loss Events. It is often helpful to break up complex Domino Effects into smaller scenarios. For example, a Domino Effect may be overpressure of equipment which ruptures sending projectiles into an adjacent equipment items which is punctured causing a toxic release. This might be broken into two scenarios for evaluation; (1) overpressure of equipment which ruptures and creates projectiles and (2) projectiles puncture adjacent equipment resulting in a toxic release.

Is there a concise way to describe double jeopardy? I find it difficult to explain. Can you define double jeopardy using concepts of probability (like you do in LOPA)? There is a definition in the CCPS book Guidelines for Enabling Conditions and Conditional Modifiers Appendix A which is "the concurrent incidence of two independent initiating events or other revealed failures". It is based on the extremely low likelihood of two truly independent and revealed failures occurring at the same instant in time.

Is burner management mostly done by checklist? Many burner management systems have been well-studied such that checklist analysis may be an appropriate method.

Regarding Pool Fire how do you evaluate this initiating event? Other or High Temperature? Pool fire is more complex than a simple Cause-Consequence scenario. It is an example of Domino Effect in that we can have a spill from one Node that ignites creating a pool fire that causes excessive heat input to nearby equipment that may be in other process Nodes. I have had some success at breaking Pool Fire into multiple scenarios for each spill plus ignition that could occur within a specific region of the plant (often a diked area). I then estimate the frequency of each of these scenarios excluding mitigating safeguards as each represents one of several potential causes for pool fire induced heat input to equipment in this region. I then sum the frequency for each of the fire generating scenarios to obtain an overall frequency of pool fire in the region and use as an Initiating Event frequency for excessive heating of equipment in the region due to pool fire. This is essentially a simplified Fault Tree approach.

Can Human Factors and Facility Siting be a What If/Checklist or would you recommend another type method? Should Facility siting include a detailed study following NFPA guidance as well as a checklist? Any of the Hazard Evaluation techniques could be used, particularly for less complex systems. For siting studies, it may help to generate overpressure contours based on explosion scenarios from existing facilities in locating occupied buildings.

Is it typical to cover environmental scenarios in HAZOP? We typically only consider process safety events. This depends on what is decided as the scope of the study. It is often more difficult to quantify the consequence severity for environmental damage.

Any advice on the right size of a node? I have seen micro nodes and macro nodes that are not effective. If there are multiple similar equipment within a node, description of parameters and deviation become overly complex. For example, in evaluation of a distillation train, it may be easier for the team to use a specific column as a node and maybe even a reboiler or condenser as a separate node. Then it becomes less confusing for scenarios such as tube failure to ensure all are discussing the same tube (reboiler or condenser) or column level as to which column is being discussed. On the other hand, if the node is too small, the team may find the same scenario is repeated often.

Are going to explain about QRA technique further? The next several sessions will cover Consequence Analysis, Frequency Evaluation, and Layers of Protection Analysis – all parts of a more detailed Quantitative Risk Analysis. The methods covered are semi- or simplified quantitative.

Shouldn't Hazard evaluations and risk studies always be reviewed when process safety incidents happen? When a Process safety incident happens wouldn't be a good practice to always check the barriers of potential consequences been checked? Yes, reviewing completed hazard evaluation and risk studies will help determine what Management Systems were not effective (such as was Safeguard a poor design, not properly maintained, etc.).

Do we need to do HAZOP for Flare system as well? If the flare systems have been included in detailed Burner Management evaluations and reviews, one could question whether a HAZOP is needed.

Is fault tree or event tree a QRA tool. Yes. In addition to adding detail to potential hazard scenarios, Fault Tree and Event Tree are used in QRA to estimate frequencies, particularly if all events in a scenario sequence are not independent.

When are procedural reviews recommended? Procedure review is particularly beneficial for batch processing. In many batch processes, the procedures represent the Design Intent.

Flare system reverse flow may be an issue that needs to be addressed in every PHA. How does this affect local cause global consequence? What are your thoughts on local cause global consequence? This is always the best approach but there are a few cases that may span across several PHA's.
I often use an approach of local Loss Event – global Initiating Cause for situations such as this. In this case, one could evaluate propagation of the flame back to any interconnected equipment for Loss Events such as internal deflagration with rupture to the equipment being evaluated. Key is to ensure that evaluation of the scenario is not missed.

Development of Incident Scenarios

Do you study overfill causing over-pressure in case of liquid containing vessels? Yes, the overpressure is part of the event sequence. Typically, the overfill creates hydraulic pressure which may activate a relief device. One of the "Inherently Safer Design" concepts that may help is if the relief device set pressure is greater than pressure of any feed connected to the equipment – then the feed stops rather than activation of the relief device.

Do you list the ultimate (worst) Consequences ONLY or all the intermediate progression of consequences also? This may depend on the relationship of any intermediate consequences. For example: An overall scenario is that a leak of flammable ignites resulting in a pool fire which then exposes nearby equipment to heat input from the fire which then increases the temperature and pressure of the nearby equipment resulting in either rupture of activation of a relief device resulting in a toxic or flammable release … I often break these into multiple scenarios: Scenario 1 is the leak of flammable resulting in a pool fire. Scenario 2 is the heat input from pool fire leading to rupture of nearby equipment. Scenario 3 is the heat input from pool fire leading to activation of the relief device of the nearby equipment. (Scenario 2 and 3 are associated with a "node" being the nearby equipment.)

Traditionally hazard identification methods could be complimented by checklist, not the other way around. Starting with a Check List could kill motivation keep looking. Yes, but also the team may be able to build upon the initial list through structured brainstorming (identify new parameters and deviations, then initiating causes, etc.). In addition, some techniques may be better suited for different process life cycle stages. For the exercise during the presentation, we ended up with 46 responses to finding applicable scenarios from the list and 40 responses to additional scenarios to consider not on the list within less than 5 minutes. Each technique has some disadvantages the team needs to be aware of and adjust for.

Do Mitigative safeguards reduce the severity of consequence or likelihood of consequence while calculating Risk? Mitigating Safeguards generally reduce the consequence magnitude as they take place after the Loss Event has occurred.

Some flammable materials could form toxic vapors on burning. How do we evaluate such scenarios? Yes, combustion products can be toxic but often we don't know what the combustion products are. If we know, the impact might be evaluated. If the fire is outdoors (such as a pool or jet fire), thermal gradients often result in significant plume rise such that ground level concentration may be relatively low. I often consider that each pool or jet fire may have started initially as a flash fire (and its associated impacts to nearby personnel) upon ignition. Then one could assess qualitatively if the consequence severity of the potential toxic impact is worse than the flash fire impact.

Do you do risk ranking and assessment as part of the HAZOP or LOPA? Evaluating risk (consequence magnitude times frequency) could be done qualitatively as part of HAZOP or more quantitatively as part of LOPA.

What about time at risk? Is that a conditional modifier? Time at risk is a conditional modifier as it impacts the consequence of leak and doesn't contribute to the loss event occurrence. Time at Risk is normally considered an Enabling Condition in that it acts with the Initiating Event. For example, if the scenario is caused by a frozen pipeline, then an Enabling Condition probability could be the fraction of time that the temperature is below the melting point of the pipeline material. Another example would be if a batch process must be in a certain step for the incident to occur and the Initiating Event could occur at any time, then the fraction of time in the specific step may be a "time at risk" enabling condition. See the CCPS book Guidelines for Enabling Conditions and Conditional Modifiers, Chapter 2 on pages 23 to 37.

Probability of ignition is defined as a conditional modifier by CCPS LOPA books. Yes, Conditional Modifier is the correct term. A point I was trying to make is that if the Outcome is flash fire or explosion, then ignition *must* occur for these outcome to be realized.

Sometimes a safeguard or action to prevent a consequence can cause another hazardous scenario. Shutdown of Ventilation system for example. How to account these? I sometimes view these as separate scenarios. A good example is activation of a pressure relief device. It prevents equipment rupture but often results in a loss of containment event (or different Incident Outcome) to evaluate.

This far I have not seen a jet fire as an outcome? Is that left out intentionally? Often a pool fire or jet fire initially begin as a flash fire (upon ignition of the flammable cloud). I normally evaluate the human harm from the flash fire but use pool or jet fire as a source of heat input to nearby equipment.

Can one modify the qualitative risk criteria in CHEF or RAST? CHEF does not contain specific risk criteria – only an aid to perform consequence estimates along with a scenario checklist and LOPA documentation form. RAST, however, does allow entry of the company's risk matrix or other "tolerable frequency" criteria.

Leakage due to corrosion is asset integrity issue and if this is a cause for hazard scenario then what's the preventive measure apart from preventive maintenance? True – the preventive measure is inspection and testing as part of a preventive maintenance program. For equipment containing highly hazardous material, one may want a more frequent inspection and testing program than for equipment containing less or non-hazardous materials. These types of scenarios are not commonly addressed in LOPA but often included a detailed Quantitative Risk Analysis. These are sometimes considered as "residual risk" cases resulting from chronic issues rather than an upset process conditions.

Source Models

Does this model consider time-dependent analysis to calculate the amount of material released? CHEF primarily estimates a maximum release rate, not a time-dependent simulation. It does not, for example, estimate lower release rate as the liquid head within equipment decreases over time.

Does CHEF tell you if the release is vapor, liquid, or both? or do you need to assess yourself? Yes, you will see the Physical State noted on the Source Model worksheet. CHEF compares the vapor pressure at the operating temperature to the operating pressure to determine if equipment contents are liquid or vapor. The user may "override" this estimate if desired.

Low pressure: release is in minutes. What is low pressure? CHEF and RAST allow one of two rupture "models" – use of instantaneous or puff dispersion models with an instantaneous release or emptying the entire equipment contents within a short time (often 10 minutes or less). If rupture of a low-pressure vessel involves the slow opening or tearing of the bottom seam, then release of the entire contents over a short time may be more reasonable. However, the estimated airborne rate is often nearly the same between these two approaches.

How to estimate hole size? Are there any rules for considering equivalent hole size? I have tried to look at a reasonable maximum hole size for a specific situation, but this is likely up to each company or business to determine a basis for consistency. As examples: For a gasket failure I have used the equivalent hole size to removing a section of gasket between two adjacent flange bolts and for a mechanical seal failure, I have looked at an equivalent hole diameter to the annular space between the shaft and bushing (a complete removal of the seal).

What is the difference between "hole size" and "short pipe flashing liquid"? Hole size represents the orifice equation and, for liquids, assumes no flashing occurs within the restricted flow path. Short pipe is based on sufficient length of the flow path such that equilibrium flashing is achieved. These two equations represent the extremes of flashing liquid flow as in the figure from CCPS, <u>Guidelines for Consequence Analysis of Chemical Releases</u> (1999) below.

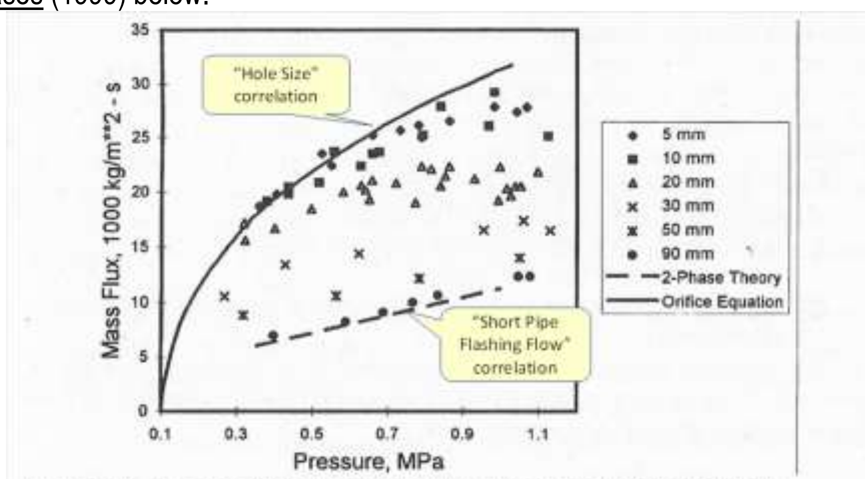

FIGURE 2.5. The mass flux from a flashing two-phase flow as a function of the upstream pressure. The data are plotted for various pipe lengths. The orifice equation predicts a maximum flow, while the two-phase model predicts a minimum flow. (Data from Fauske, 1985.)

What is the range of applicability for pool area equation? (is it valid for cryogenic pools?) Release of 1.23 kg /s without dike seems quite high - how does this corroborate with other models? CHEF and RAST spreadsheets assume a 1 cm liquid depth if a diked area is not specified similar to Dow's Chemical Exposure Index. There are more sophisticated pool spread correlations available in the literature, but minor surface irregularities can impact results (how flat and how smooth).

Have you published comparisons with other models? Most correlations are directly from the literature and generally accepted (such as an orifice correlation for hole size leaks). In other cases, I have made comparisons with other techniques, but none are published.

In your experience in using this worksheet tool for calculations during PHAs, which data were generally difficult to find and how did you manage to assume? Chemical properties (such as liquid heat capacity, liquid density, vapor pressure and heat of vaporization as a function of temperature) are sometimes difficult to attain, particularly in manufacture of specialty products. I have chemical property estimating and correlating routines I have used in these cases. For toxic or flammable properties, I often consult with a subject matter expert.

Could you update the units as used in the spreadsheet, capital often goes wrong? It should be: kg; kJ or kJoule; kW or kWatt. (kPa is used OK though :-) This is an ongoing activity as sometimes different abbreviations are common. With each update, I am trying to be more consistent between the various tools, manuals, and training slides.

Looks like as a minimum would be nice to have a button that imports chemicals from RAST since RAST has the ability to add user chemicals. In CHEF calculator, can we save our specific chemicals? What if the chemical is not listed in drop-down list? How could I add? In each of the CHEF worksheets, the chemical properties needed may be entered directly if the name is not listed such that the properties are automatically populated. Allowing user chemicals to be added to the listing may be a good feature to add but it does create significant complexity for a simple teaching aid. One could always “unhide” and “unprotect” the chemical list in your specific copy and add more chemicals (but you would need to remember to add these new chemicals each time a new version was downloaded).

Any warning that horizontal spray distance exits dike? No there is no warning as one needs to consider the elevation of the leak and leak trajectory compared to the height of the dike.

Why would the airborne quantity be affected by the presence of a dike? Pool evaporation rate is one of the primary terms in estimating the total airborne rate and impacted by the pool area. If a dike exists, the pool area is limited to the dike area.

How is the relief temperature evaluated for mechanical energy release (pump failure case)? In many cases, the relief temperature may be estimated as the boiling point at the relief device set pressure.

What is the effect / impact of flash fraction? The flash fraction represents the fraction of liquid release vaporized upon depressurization. It is a key contributor in estimating the total airborne rate.

Would be good to have a pull-down with different discharge coefficients to choose from. Currently only a square-edge orifice (Cd=0.61) and rounded entrance (Cd=1) are in the pull-down menu as these are most common. CHEF is intended as a quick and approximate answer. If more options are needed, an equivalent hole diameter may be entered to adjust for other discharge coefficients.

What is the inventory mass for this example? If not specified in the inputs, sufficient inventory for a one-hour release is assumed.

Where do you find the model used? The user selects which loss event release model to use based on the specific scenario being evaluated. There are four basic types – hole size, material balance, energy balance, or rupture.

Vapor Dispersions

What is the reference for the 18.75 seconds averaging time for flammables? The CCPS book Guidelines for Consequence Analysis of Chemical Releases pages109-110 or the CCPS book Guidelines for Chemical Process Quantitative Risk Analysis, 2nd pages 1399-140 discuss a factor to account for averaging time as $F_t = (t_a / t_{PG})^{0.2}$. The lower limit on this factor is approximately 0.5 and represents an instantaneous release. The Pasquill-Gifford averaging time, t_{PG}, is 600 seconds which implies an averaging time, t_a, of 18.75 seconds for a limiting factor, F_t, of 0.5.

Hard to believe recent styrene accident in India gave a dispersion of 5-6 km. It is much heavier than air and polymerize at elevated temperature. Could we try? As you state to share some examples by e-mail, could you also include info about the India event mentioned (rather than wait until last session)?

I plan to use this incident as a case study during the last week of the CHEF webinar. The vapor release rate was extremely high due to the runaway polymerization, but I do not believe a toxic concentration went as far as 5 to 6 km downwind. There is a tremendous amount of information that has been compiled to date. The India government has issued a preliminary report two weeks ago that may be updated as some details may not yet be clear. From what I have seen, an exothermic runaway polymerization was likely due to depletion of the inhibitor. The incident occurred during restart of the facility after being shut down more than 6 weeks due to the Covid-19 issues. There was a very high vent rate of styrene vapor due to the heat of polymerization creating a large vapor cloud. The wind direction at the time of the incident was toward the nearest residential area only 150 to 200 m from the release location. The report can be found at: https://greentribunal.gov.in/sites/default/files/news_updates/Report%20of%20the%20Joint%20Monitoring%20Committee%20in%20the%20O.%20A.%20No.%2073%20of%202020.pdf

Could you share more supporting references for the comment you made on slide 21: about most models been off by a factor of 2 or 3. [You only show 1 example]. Another example is an article "Comparison of Six Widely-Used Dense Gas Dispersion Models for Three Recent Chlorine Railcar Accidents" by Hanna, Dharmavaram, Zhang, Sykes, Witlox, Khajehnajafi, and Koslan (NATO Security through Science Series C: Environmental Security, January 2008). This study found that six commonly used software programs agreed to within a factor of 2 in the range of 0.1 to 100 km downwind for the three cases studied.

Are the charts going to be available? What about the video recording? As most information we are sharing is in the CHEF Manual (or will be distributed as worked examples), we do not plan to share the presentations. We are still looking into how best to share video recordings with participants.

Why is 3 m/s "typically" considered? Will a higher wind speed be more conservative? Generally lower wind speed is more conservative. The US EPA suggests using 1.5 F for worst case evaluation with an alternate case of 3 D. I have also seen 5 D used in screening studies. It would be up to each company to decide what best to use for screening purposes.

How do atmospheric temperature and humidity affect dispersion? Atmospheric temperature and humidity have some effect on dispersion (are used in evaluating the density of ambient air). Humidity was not considered in the simple models used in CHEF and RAST.

Why don't you use CCPS CA book (versus Crowl's)? The Britter-McQuaid dense gas model and Pasquill-Gifford neutrally buoyant models are described in the CCPS book Guidelines for Analysis of Chemical Releases pages 76 to 125. However, Crowl and Louvar, Chemical Process Safety, 3rd (in addition to description of the Britter-McQuaid and Pasquill-Gifford models) describe the transition from dense gas to neutrally buoyant on pages 219 to 225.

Can the tool model mixtures? If not, what is the best tool to use for mixtures? For these simple models, vapor density is the key variable and an equivalent molecular weight of a vapor mixture could be used. Note that these simple models do not incorporate deposition on surfaces or reactions with humidity in the air.

What is the reference for table on chart 40? There are several references for air exchange rate for typical houses and common ventilation requirements. Values depend upon age of the structure, climate (summer versus winter), house size, outdoor wind speed, and other factors. A report "Analysis of U.S. Residential Air Leakage Database", Lawrence Berkley National Laboratory Report 53367 (2003) provides a very detailed analysis of US houses. In this report, data ranged from roughly 0.1 to 3 with a median of 0.5 air changes per hour.

What is the reference for equation in chart 38? The equation is from a simple material balance assuming a constant volumetric rate of air ingress and exit from a building.

$V_B\, dC = V\,(C_{Outdoor} - C)\, dt$ *where V is vent rate and V_B is building volume*

$\int dC / (C_{Outdoor} - C) = (V / V_B) \int dt = VR \int dt$ *where VR is air exchange rate*

$\ln ((C_{Outdoor} - C) / (C_{Outdoor} - 0)) = - VR\,(t - 0)$

and $\mathbf{C / C_{Outdoor} = 1 - e^{-VR\,t}}$

Does the dilution from relief devices also affect toxic effects? Yes, the initial dilution from Jet Mixing that is typical for relief devices reduces the concentration within a short distance such that atmospheric dissipation begins with a lower concentration.

After getting the distance at equation 37, should it be corrected by a factor of 2? The factor of 2 is a correction on the overall distribution coefficient for a short averaging time used in estimating flammable *concentration* at a distance. Since our example was addressing a toxic outcome the factor of 2 would not be applied.

Would 3600s used for as average timing for calculating ERPG? One could use an averaging time of 3600 seconds to obtain a one-hour *average* concentration to account for an ERPG being a one-hour exposure duration. I have seldom seen this done.

Classes A to F for atmospheric stability refer to PASQILL classes. Yes, these refer to the Pasquill (often noted as Pasquill-Gifford) stability classifications.

CHEF allow us to modify the air conditions. How to show "dispersion detailed"? As shared in the presentation, the wind speed, atmospheric stability class, and surface roughness category may be changed upon using the "Show Correlation Details" macro button to unhide these columns.

Explosion Models

Does CHEF and RAST address BLEVE? CHEF and RAST approach the energy associated with equipment rupture where liquid flashing occurs as a BLEVE even if the temperature at rupture is less than the critical superheat limit (normally greater than 0.8 to 0.9 of the critical.) The chemical properties in CHEF and RAST do not utilize an equation of state such that the critical temperature is not known. CHEF and RAST use an equivalent volume which includes vapor formed by the flashing liquid as discussed in R. Prugh, Quantitative Evaluation of "Bleve" Hazards, J. of Fire Prot. Egr., 3 (1991).

How and from where 15 ft. between PES and adjacent equipment is derived? This value is merely to give an idea for the distance needed for the flame front to decelerate in the absence of obstacles. We are not attempting to share specifics on how to identify congested or confined areas within a facility into Potential Explosion Sites (PES). Identifying specific congested and confined regions greatly improves accuracy but is difficult to evaluate. This is one of the reasons for the simplification of using the entire cloud volume as a single PES in CHEF.

Difference between flash fire vs vapor cloud explosion? How we can justify the credibility of flash fire over explosion as part of the congestion factor takes into account? Although both involve a moving flame front, flash fire does not produce a significant blast wave and damaging overpressure. So, if a flammable cloud ignites, a flash fire may engulf personnel in the flame front. If the flame front accelerates to create a vapor cloud explosion, there is additional damage from the blast overpressure.

What is the nature of explosion? Is it volume increase in very short time due to physical phase change or chemical reaction releasing large amount of gases? The pressure from combustion comes from the sudden increase in vapor volume both due to increase in moles of gas produced relative to the moles of reactants and (usually more importantly) the sudden heating of the vapor by the heat of combustion.

What is considered LONG duration or impulse? Assuming a long Impulse is conservative and simplifies the evaluation such that only blast overpressure is used for the estimate of damage.

Please comment on use of NFPA-921 overpressure consequence VS BDL from pressure and impulse curves. *Are there any guidelines for overpressure levels and their impacts? Are they part of CHEF manual? How would you define the application of this software: for indicative purposes or ...?* Building Damage Level from pressure and impulse curves are more accurate but more complex to evaluate. The CHEF and RAST spreadsheets (and concepts presented within CHEF) are intended to provide quick and approximate estimates to help Hazard Identification and Risk Analysis study teams better understand the consequence severity for scenarios being considered. A condensed table of blast impacts versus overpressure from NFPA-921 may be found in the CHEF Manual on page 129. The CCPS book, Guidelines for Consequence Analysis of Chemical Releases (1999) has good table of damage versus overpressure on page 138.

What is early explosion and late explosion? Is it clearly defined? Early versus late typically refers to when ignition occurs. Late ignition would be when the vapor cloud has reached its maximum size with a maximum of fuel available.

What is Class I dust? What is the reference which provide burning velocity of dusts? As noted in the flammability hazards presentation, a deflagration index is used for dusts to describe how rapidly the pressure rises during combustion. A Class I dust represents a relatively slow pressure rise rate similar to a low fundamental burning velocity (or "fuel reactivity") for vapors.

How accurate are these graphed models are as compared to real world explosions? Are they always conservative or there are exceptions? How to know which model to use? These models are generally an empirical correlation to actual explosion data. The challenge is proper categorization of the correlating parameters (such as fuel reactivity, obstacle density, and level of confinement). The TNT equivalent was developed in the 1960s and commonly used. It is reasonable for vessel rupture and some energetic chemical reactions such as detonation. The Baker-Strehlow-Tang is more appropriate for combustion related explosions such as Building Explosion or Vapor Cloud Explosions.

For dust explosion, should we consider VCE? Since a dust is not vapor, we normally refer to this as a dust explosion but may want to use the Baker-Strehlow-Tang (BST) approach to estimated blast overpressure versus distance.

Why not use TNO model? The TNO model is similar to the BST approach but the explosion efficiency is based on 10 source strengths. It is sometimes more difficult to determine which source strength to use than determining Mach Numbers in the BST model.

For dust explosion such as sulfur, does the Explosion tab from the CHEF Calculation Aid suitable as well? The dust deflagration index often depends on particle size, so it may be useful to know the deflagration index for the specific dust being evaluated. As a first approximation, I might consider a Class II dust as similar to a fuel reactivity of "medium" but there is little data to support this.

What guidance/book advocate use of BST for internal explosion in equipment? Also, for dust explosion scenario? The CCPS book Guidelines for Consequence Analysis of Chemical Releases (1999) notes the issues in determining explosion efficiency using the TNT equivalency model for vapor cloud explosions. This book also notes that the TNO and BST models were specifically developed on the basis of deflagrative combustion. API-752 also provides guidance that the TNT equivalency model is not appropriate for vapor cloud explosions.

During the first webinar you said that you will show how to model dust explosions using BST, I would like to request if you could include explanation in email? But if you consider CHEF aid for a dust explosion. What Chemical Name to consider as there is no solid in the list? What model do I select if I wanted to look at the overpressure of a dust collector exploding indoors? Most commonly, we are interested in Dust Explosions within a Building or Confined Space within equipment (such as a dust collector). By selecting the "Building or Head Space Explosion" option on the Explosions worksheet of the CHEF Calculation Aid, one only needs to enter the fuel reactivity, building volume and level of congestion to estimate blast overpressure – a Chemical name is not needed to find these properties. This estimate uses the Baker-Strehlow-Tang model which has not been validated for dust explosion.

To simulate an excessive natural gas flow distinguishing flame in boiler scenario, should we use TNT or BST model in chef aid? I normally break up a boiler into two separate equipment items for evaluation – the combustion unit and the heat exchanger. I use BST for evaluating explosion within the combustion chamber and TNT for estimating rupture blast overpressure of the heat exchanger.

Why to take middle point of LEL distance while calculating maximum impacted distance? Why not some other location? The most conservative simplification would be to assume the epicenter as the furthest edge of the flammable cloud from the release location. However, since assuming the entire vapor cloud volume as a Potential Explosion Site is conservative, the center of the cloud was selected as the epicenter as being more realistic.

Detonation or over Mach 1 is pressure wave compression of vapors ahead of wave to over auto ignition temp....right? I believe detonation or greater than Mach 1 is indicating acceleration of the flame from to greater than the speed of sound within the unreacted fuel-air mixture rather than related to auto ignition.

Impact Estimation

What is an appropriate level of concern to evaluate onsite toxic impact? ERPG has an assumption of exposure time for 1 hour, which is too conservative. An equivalent, or dose-adjusted, ERPG may be a reasonable level of concern for injuries onsite. As you note, ERPG is specific to a one-hour exposure. In the Toxicity Hazards presentation, a method for determining a concentration representing the same dose at different exposure duration was shared.

Are the impact levels versus fire heat radiations, overpressure, flash fire specifically available in CHEF manual? So, companies commonly set an overpressure, %toxic lethality, etc. as criteria for a certain consequence (fatalities, etc.)? There are examples for screening criteria in the CHEF Manual similar to what was shared in the Impact Estimation presentation. The "level of concern" should be decided by a business or company for consistency among evaluation teams. There are currently no specific industry standards and CCPS does not endorse any specific values.

But how to determine the Radiation intensity in a quantitative way (kW/m^2) in a scenario description? SDS? Have the Chef Aid the possibility to calculate the thermal radiation in case of pool fire or jet fire? I did not include an estimate of pool fire in CHEF but have an estimate of distance to severe thermal burns from a fireball. The CCPS book <u>Guidelines for Consequence Analysis of Chemical Releases</u> (1999) contains a method for estimating thermal radiation from pool fires on pages 210-223. (A simplified version of this method assuming typical properties of hydrocarbons in the RAST tool Pool Fire Frequency worksheet.) A key is estimated of radiation (thermal radiation) intensity at a receptor some distance from the radiation source.

What are effects of higher than normal Oxygen levels. For example: if oxygen is released from an oxygen generator or storage during an event. One issue with high oxygen content is that combustible materials will burn more energetically in oxygen than air creating a more severe flammability hazard. The flammable limits may also be broader than with air.

How to reasonably estimate oxygen rich impact to personnel? what concentration may lead to severe injury? How to assess the consequence of LOC of oxygen? I believe the short duration symptoms of too much oxygen are often minimal but can include headache, sleepiness or confusion. There may also be increased coughing and shortness of breath as the airways and lungs become irritated. It may be prudent to consult a medical specialist for more information.

In Vapor Cloud Explosion outcome threshold, values in the manual are 10 times higher than in presentation. Which is the right one? Wouldn't you consider release/time for a de minimis vapor cloud release rather than just the total amount released? How do we know if vapor cloud will result in flash fire (with no overpressure) or VCE (with overpressure)? A minimum release rate may be an indication of cloud size similar to using a small mass of released vapor. I believe either could be used. Using a de minimis value for a flammable release is not indicating that explosion cann*ot* occur but merely that, at some small value of explosion energy, the blast wave is not sufficient to cause much damage or human harm beyond that of a flash fire. 100 kg released mass was shared as an example criterion in the presentation (although

1000 kg was used as an example in the CHEF manual). This is a judgment call and up to the business or company to select a value or merely assume all flammable releases could be a potential vapor cloud explosion.

How could the trajectory of projectiles be estimated? In the January Tarragona runaway reactor cover reaching 2-3 km distance from the site. There is a simple maximum fragment range correlation in the CCPS book Guidelines for Consequence Analysis of Chemical Releases (1999) on page 170 that is used in RAST. It is range in m = 120 $w^{1/3}$ where w is the TNT equivalent in kg. Other estimation techniques are described in the same reference on pages 166 to 173 which incorporate the specific mass and shape of the projectile for greater accuracy.

Should the damage from flash fire estimated by distance to cloud center or distance to LEL? Are flash fires not considered credible per API 752 guidance? Flash fire maximum impact to people safety on injuries and no fatalities? As noted in the Impact Assessment presentation, a simple technique is to consider all personnel within the "flash fire" zone to be severely impacted (potential fatalities) while those beyond this zone to not be impacted at all. The effect or impact zone is estimated as a "pie shaped" area using the radial distance from the release point. If the radial distance is small such that only a small fraction of body area (less than 25%) would receive 2nd or 3rd degree burns, than injury may more appropriate than fatality as a consequence. Since the duration of a flash fire is very short (seconds), there may be little damage to equipment although the subsequent jet or pool fire may cause greater damage.

Can there be situation where person is outside flash fire impact area but still within pool fire or jet fire impact area? Generally, the maximum distance to a fraction of the lower flammable limit is somewhat greater than the flame distance of a resulting "steady state" jet or pool fire. For example, when igniting an outdoor gas grill, the "flash" upon ignition after leaving the gas flowing for a period of time extends beyond the "steady state" distance of the flame from the burner nozzle.

Please, don't neglect Effects/RiskCurves for CA/QRA! I only included what I thought were more commonly used Consequence Analysis / Quantitative Risk Analysis software in the pooling question, not a comprehensive list. Indeed, RiskCurves is also fairly common.

How do LD_{01}, LD_{50}, ERPG-3 values correlate? How to calculate? This was covered in the Toxicity Hazards presentation. Ideally, we would have company accepted probit models for inhalation toxicity. We suggested that a multiple of ERPG-3 concentration may be a reasonable surrogate where probit models do not exist. During the presentation, I shared a graph of concentration/ERPG-3 versus lethality for various published probit models. It was noted that 1 to 2 times ERPG-3 may be a reasonable surrogate for 1% lethality and 3 to 5 times ERPG-3 may be a reasonable surrogate for 50% lethality at a one-hour exposure.

Why use ERPG rather than AEGL? There are more chemicals with ERPG than AEGL established.

For hazard distance discussion- the population density is considered excluded from the equation while determining consequences? If it is intended to *not* use specific reference to human harm in categorizing consequence severity, severity may be categorized by hazard distance with a greater hazard distance being a higher severity. The specific values would need to be established by a company or business for consistency. For example, a company may decide to use a specific distance to 0.5 LFL concentration as a semi-quantitative criterion for a specific severity level rather than estimate the number of people severely burned.

Knowing the uncertainty of wind direction how can we use the on-site outcome as presented? One simplifying assumption that may not have been stressed enough in the presentation is a wind direction toward the highest population (such as directly toward occupied buildings). If the on-site personnel are truly located randomly throughout the production area, then direction is less important. However, when evaluation of personnel "in the immediate area", one should consider outdoor work areas that are located within the toxic vapor cloud distance.

To determine the effect area of a toxic release, hence check if the release goes to a safe location. What value of toxic level do you see as safe? ERPG-3 value? There may be differences in interpreting "safe" so this would be a business or company decision. ERPG-3 is defined as a concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing or developing life-threatening health effects. This concentration may be interpreted as "safe" from life-threatening health effects for a one-time situation, particularly for on-site personnel who are likely not infants, elderly, infirmed, etc.

A 2nd edition of the CCPS book "Guidelines for Evaluating Process Plant Buildings for External Explosions and Fires" (with Toxics added) was published in 2012. The reference to occupant vulnerability versus overpressure was not included in the more recent edition as more accurate (but more complex) correlations are now available.

So how far off in toxic impact are you in simply using 5X ERPG3 as the fatality indicator and simply tracking the dispersion extent and known population maps? As noted in the presentation, this approach may be reasonable for on-site inhalation toxic estimation (using 5 times ERPG-3 as a surrogate for 50% lethality from a one-hour exposure). An off-site population may be beyond the distance to 5 times ERPG-3 concentration, so evaluation of lower concentration and lower lethality at further distance (such as the "integration method") would be better.

Likelihood Evaluation

For probability of ignition: Why did you chose to use HSE approach instead of the CCPS book? The approach in the HSE report shown uses a distribution of generic ignition sources such that the larger the flammable cloud footprint (or greater the release rate), the more likely ignition will be. This approach is essentially based on the likelihood of a flammable cloud reaching a generic ignition source. In RAST, the "Ease of Ignition" is also taken into account. Categories for Ease of Ignition are described in Larry G. Britton, "Assessing Probability of Ignition (POI) of Gases and Vapors with Deflagration Potential", Neolytica Inc, March 10th, 2005. Pyrophoric materials are assumed to always ignition (POI=1) independent of release quantity while materials such as ammonia or methylene chloride are categorized as "Low" Ease of Ignition likely needing a very strong ignition source. This approach is intended to represent engineering judgment and has not been validated with experimental data.

The CCPS book Guidelines for Determining the Probability of Ignition of a Released Flammable Mass (2014), describes the ignition probability of known ignition sources *once the flammable cloud has reached the source*. What was described in the presentation is that if a known ignition source is within the distance to the lower flammable limit from the release location – use values described in the CCPS book (generally higher than 0.1 which I noted might be rounded to 1 if using "order of magnitude" values). If there is not a known ignition source within the flammable cloud, use an approach similar to the HSE report rather than assume no ignition occurs.

How to justify the right scenario need to be apply enabling event or time at risk factor? This is often challenging. The CCPS book, Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis (2014) provides guidance on this. I find that "Time at Risk" is the most common Enabling Condition. Essentially the event sequence could only occur if the Enabling Condition were true. Examples may be a specific step of a batch sequence where a hazardous material were being used or a requirement for an unusually low (or high) ambient temperature. I believe the most common misapplication of Time at Risk involves unrevealed (or latent) failures. For example: one would not normally apply an Enabling Condition probability for an Initiating Event of transfer hose failure. The failure of a transfer hose may be caused by damage when not in use and only discovered during material transfer.

How come Both Bulb Burn out Probability of failure is 0.05/year it should be unit less? On the light bulb failure what was the equation used to get .05/year frequency? Note that either bulb can fail over the same time interval. If Bulb 1 fails at 0.5/year and is not repaired for 0.1 year, the probability the bulb is out, P = 0.5/year x 0.1 year = 0.05. While this occurs, what if the other bulb also fails? Bulb 2 fails = 0.5/year x Bulb 1 failed probability (0.05) = 0.025/year. There is another failure case which needs to be considered: What if Bulb 2 fails first and then Bulb 1 fails? This would be described as follows: Bulb 1 fails (0.5/year x Bulb 2 already failed probability (0.05) = 0.025/year (case 2 for both bulbs out). You must add together each of these cases to get 0.05/yr.

Could you expand little more your recommendation for use more sophisticated software for estimating frequencies below 1E-4? CCPS LOPA book doesn't mention limit. I shared a very simplified Fault Tree approach that did not incorporate common cause failures (or a beta factor when performing a more detailed Fault Tree analysis). So, when estimating very-low failure frequencies (such as 10^{-4}/year or maybe higher if power reliability is unusually low or there are other factors which may fail multiple systems simultaneously), common cause failures need to be included or the failure frequency will be under-estimated.

Could you provide the full reference for the HSE document mentioned on slide 12? The specific graphical depiction on Slide 12 came from John Spouge (DNV Consulting), "New Generic Leak Frequencies for Process Equipment", Process Safety Progress Vol.24, (2005). A similar depiction is found in Failure Frequency Guidance Process Equipment Leak Frequency Data for Use in QRA, DNV (2013).

Isn't MTTB failure is MTTF +MTTR'? I am not familiar with MTTB. I had described Mean Time Between Failure (MTBF) as 1 / Average Failure Rate and is also the sum of the time period of operation and time period for repair. I should have written the PFD for revealed failures as merely the Mean Time to Repair, MTTR, divided by MTBF as the time to repair is already included in the Mean Time between Failures.

What was your approach to "adjusting" the failure data for corrosives? Was there a limit on how much adjustment (1 or more orders of magnitude)? Fortunately, I had company data on failure frequency and was able to make some adjustment based on the chemical service and corrosion rate of the specific material of construction.

How does "Probability of Exposure" is defined? A better term would be Probability of Personnel Presence which is a Conditional Modifier related to the fraction of time people are likely to be within an effect or impact zone.

It looks like you are combining enabling conditions and conditional modifiers into the term "enabling condition", correct? I have been trying to keep these terms separate as they have different definitions. An Enabling Condition as a condition that does not cause the scenario but must be present or true for the scenario to proceed to a loss event. A Conditional Modifier is generally used when risk criteria endpoints are expressed in impact terms (e.g., fatalities) instead of in primary loss event terms (e.g., release, vessel rupture). They both, however, are probabilities that impact the overall frequency of a scenario. *I sometimes mistakenly refer to probability of ignition (POI) as an Enabling Condition when describing a scenario with flammable outcome such as flash fire or vapor cloud explosion (as it must occur for the event sequence to happen), however POI is actually a Conditional Modifier.*

Do companies create/assemble a common database of frequencies etc. for consistency? or does each PHA leader use their own references and judgement? Ideally a company will adopt a standard set of frequencies to use in Risk Analysis for consistency across evaluation teams.

For a Fault Tree, does the top event consider the probability of injury? If the top event used in the Fault Tree is an injury, then one could estimate the overall probability of injury from all causes.

Are there generic event trees (like for pool fire) that we can adapt to our real installation? The CCPS Book, Layer of Protection Analysis (2001) on page 71 gives a typical frequency of 0.1 to 0.01 for small external fires (aggregate causes) and 0.01 to 0.001 for large external fires (aggregate causes). I believe these are good values to start with. However, when using these generic values, we don't know the specific causes and would not be able to utilize protective layers that prevent the fire from occurring (only mitigating protections could be used). I shared a simple Fault Tree approach for estimating pool fire frequency from multiple causes to allow the evaluation team in applying preventive protections to the highest frequency causes to manage the risk.

Simmons model gave higher ignition probabilities than the other models. Could you please open a bit why it is so? From the HSE Research Report 226, it was noted that the Simmons model (1974) is wholly based on incidents involving spills of LNG or LPG related to US transportation incidents and may not reflect the densities and types of ignition sources found at manufacturing sites storing flammable gases.

What's the reference for the "bathtub curve" shown in slide 6? The "bathtub curve" is a graphical depiction of the Weibull distribution commonly used in reliability literature. The specific diagram on Slide 6 was adopted from Crowl and Louvar, Chemical Process Safety, 3rd (2011) on page 551.

Does the duration of the start-up of a plant can be a time factor if the cause of the scenario can only occur during the start (example: failure to ignite a burner)? This may be an Enabling Condition (as Time at Risk being a fraction of time in the start-up condition) or possibly described within the Initiating Event such as ignitor failure probability times the number of light-offs per year to obtain the failure frequency.

Do protective layers can really have safe outcome? Isn't there always some negative outcomes? Generally, a preventive protective layer brings the operation within the control limits or a safe shut-down state before the loss event occurs – a "safe" outcome (other than potential loss of production). A mitigating protective layer may reduce the magnitude of the consequence. An example of a potentially negative outcome might be associated with activation of a pressure relief device. This protective layer prevents destructive overpressure to equipment but may result in a more controlled release to the atmosphere (which is why I sometimes consider a pressure relief device as a mitigating protection where a release to atmosphere may be less severe than a release associated with rupture of the equipment).

How does CHEF help in LOPA? CHEF describes some of the concepts and methods that might be used in Layers of Protection Analysis. During our CHEF Webinar we discussed development of scenarios, estimation of "worst" consequences and frequency to obtain risk, and categorizing risk in development of a risk matrix to determine the number of risk reduction credits or protective layers needed to achieve a company's tolerable frequency.

Human failure on demand for IPL: Is this recommended to use a human as a protective function and if so, how high can we go 0.1, 0.01, 0.001, 0.0001? Can a human be used as an IPL if procedures are safety critical with second set of eyes used? Human error is a common Initiating Event and some companies do not allow an Administrative Procedure as protection layer. I generally do not believe that the same person performing the procedure that failed resulting in an Initiating Event should be credited to properly execute an administrative procedure used as a protection layer. The CCPS book Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis (2015) on page 256 lists consideration for using Human Response to an Abnormal Condition (with PFD of 0.1) as a protection layer. These conditions include having sufficient time to respond and complete required actions, having a written step-by-step procedure to follow, the person is well-trained, and the person is not put into a dangerous situation to accomplish the required action. This reference also lists conditions for using Human Response to an Abnormal Condition with Multiple Indicators and > 24 hours to Accomplish the Required Actions (with PFD of 0.01) as a protection layer.

Time at risk; for the classic unload scenario, can we use a system check to allow its use and also credit the system check in the LOPA? This may be "double counting" a risk reduction credit. I mentioned that failure of a material transfer hose is often an "unrevealed" failure (the hose may have been damaged when not in use) and a time at risk enabling condition probability would not apply. However, if a pressure check or leak check prior to each use was implemented, any failure of the hose would need to occur during the fraction of time for the transfer operation. The lessor of either a Time at Risk enabling condition probability or credit for Human Response to an Abnormal Condition administrative procedure PFD may be appropriate but not both.

Risk Analysis and Risk Assessment

Since CHEFs estimates human harm quantitative, is it considered a QRA? The methods described in CHEF would not typically be adequate for it to be considered a detailed Quantitative Risk Analysis (QRA). In detailed QRA, human harm (and environmental damage and business loss) is quantified, there is often many cases of the same scenario to evaluate different wind directions, wind speeds, atmospheric stability, night-time population location versus day-time or weekends, etc.

Are all risk matrices based on "order of magnitude"? A risk matrix can be defined by the company in quantitative or qualitative categories. Many risk matrices are intended to be "order of magnitude" to match "order of magnitude" risk reduction factors.

If you have an ineffective & unmaintained (mitigating) barrier, the inherent risk does not change, correct? A more appropriate term may be that the "unmitigated" risk does not change which is the risk with no protective layers applied.

Recognizing that it's not a barrier, how do you represent "probits" on a Bow-Tie? A probit model allows representation of a normal or Gaussian distribution. In the Toxicity Hazards and Impact Assessment modules, we discussed using a probit model to relate dose (concentration times exposure duration) of a toxic material to likelihood of fatality. This is not a protection or safeguard but merely a means to quantify the scenario consequence and would not be a barrier represented on a bow-tie diagram.

For a Bow-Tie analysis, is it recommendable to simplify the consequences, using the worst scenario? or evaluate different scenarios to show different barriers? How to justify the effectiveness whether the mitigative safeguard could be taken as credit of consequence reduction. I have used the Bow-Tie technique to show the inter-relationship of scenarios involving the same loss event. I treat each cause-consequence pair as a separate scenario. In this way we can show that preventive protections may apply to more than one scenario but that mitigating protections often relate to only one outcome. (For example, a high-level interlock which shuts off all feeds to an equipment item might apply to several Initiating Events to an Overflow loss event. However, a mitigating protection to shut off the ventilation to an occupied building in the event of an outdoor toxic release from the same overflow loss event protects building occupants but not personnel located outdoors.)

If we take credit of IPL for reducing the Severity than how in LOPA you will take credit in reducing the frequency? are you going to reduce TMEL? Risk is the product of consequence severity times frequency. Credit for an Independent Protection Layer is essentially the same in Layers of Protection Analysis for mitigating (often a reduction in severity magnitude) or preventive (often a reduction in frequency). A risk reduction credit is typically one order of magnitude lower value of risk (or sometimes one category lower of either severity or frequency of the risk matrix).

Are there differences between European QRA and American QRA? Is it possible to be risk-based acceptable, but not compliant with regulation? Some countries require Quantitative Risk Assessment (QRA) for facilities handling hazardous materials and may even provide criteria by which the analysis is to be done. Also, some companies require QRA for very-high risk processes and may prescribe criteria or protocols to follow. Each company or country's requirements may be different.

Can you explain cost-benefit analysis for risk reduction additional measures? A quantitative cost-benefit analysis is difficult as it requires placing a numerical value on human life. This exercise is analogous to purchasing insurance. The Health and Safety Executive (HSE) provides some limited guidance for cost-benefit analysis relative to ALARP (as low as reasonably practicable) requirements. I believe this analysis is best when used to compare risk reduction options on a relative basis to find the lowest cost options.

Is the pyramid on slide 13 from a CCPS Book? Slide 13 is not from a publication but merely a depiction of how a company might establish guidance (or requirements) for what level of risk analysis is needed.

How many simplified quantitative risk analyses could a refinery unit have? The number and/or scope for risk analysis would depend on the specific company or country requirements. Quantitative risk analysis may be acceptable for lower risk units reserving semi-quantitative or detailed quantitative analysis for high risk operations.

Is the chart on slide 25 for a single event (1 cause-consequence pair)? Typically, a Risk Matrix would be used at the single scenario level. The categories should be established that a single scenario frequency for a specific consequence severity is well below a company's cumulative risk tolerance criteria (sometime referred to as an "FN" curve).

Are risk-graphs applied in QRA's? It seems that individual risk doesn't take into account the environment of the plant. It is really a risk assessment? Risk Graphs are merely a means for sharing or communicating risk analysis results. As described, risk may be displayed as "individual risk" contours near the plant site (risk to an individual at a specific location from all scenarios) or as cumulative frequency of all scenarios versus fatality for "societal risk". The graph or display should ideally be consistent with the company or country requirements (such as maintain risk to an individual located at the plant boundary less than a specific value or societal risk below specific "FN Curve").

How do you see an approach if we just estimate the consequences and use always a frequent likelihood when doing Fire Hazard Assessment? NFPA 551 contains guidance for evaluation of fire risk assessments. I believe it may be grossly conservative to assume a high frequency for all scenarios such that the risk is merely defined by the consequence severity. A key issue often evaluated in a Fire Hazard Assessment involves managing the firefighting water so that nearby waterways do not become contaminated. How would this compare with property damage and potential loss of life scenarios?

Would the 3 regions of the pyramid correspond to the 3 regions of the risk matrix i.e. if the risk is red, then we would need the detailed QRA? The intent was that the colors on the risk matrix related to categories of risk (high, moderate, and low) but unfortunately, we did not show the legend for the different colors of the risk matrix. These could also relate to the risk being acceptable, unacceptable, and tolerable with some level of approval.

What is the scale to be used for consequence & frequency? 1 to 5 for each (e.g. 5x5)? Each company may decide the number of categories for consequence severity and frequency to be used. I have seen 5 categories commonly used to relate Consequence Severity as: minor injury, major injury, potential fatality, several fatalities, and many fatalities. The most I have seen used is 7 categories of consequence severity and least is 3 categories.

Why does the matrix is reversed comparing to the diagram? The risk matrix can be oriented several ways. The depiction shared on slides 24 and 25 show high risk (high frequency, high consequence) at the bottom left such as we have done in the Risk Analysis Screening Tool (RAST) where others I have seen place highest risk at the top-right of the matrix. Often when using an "order of magnitude" approach, the negative $\log_{10}$ of the frequency is often used as a frequency factor, so the orientation shared would be from low frequency factor on the left to high frequency factor to the right.

Could you recommend a free Fault tree or Bow-Tie software? I am not a subject matter expert in this area and have not worked with most of the software available to make recommendations. I have tried Fault Tree Plus (Isograph) and BowTieXP (GCE) in the past.

Should you include in enabling factors conformance with PSM elements or RAGAGEP (Recognized and Generally Accepted Good Engineering Practices) standards as credit or debit? Generally, conformance with PSM elements and/or RAGAGEP standards are not considered enabling factors or safeguards. The failure frequency data available is typically where PSM elements and/or RAGAGEP are in place. However, extraordinary practices might be considered. For example, both PSM and RAGAGEP would require a testing and inspection program to be in place as a minimum requirement. However, if a testing and inspection program that far exceeds the minimum requirement were implemented, that might be considered a protective layer (for example: following design and inspection for lethal service per ASME might be considered a protective layer for an asset integrity scenario).

Is the Risk Matrix semi-qualitative approach more conservative than the LOPA and QRA? Can a company just use a risk matrix? The semi-quantitative or simplified approaches use simplifying assumptions and are generally (not always) more conservative than a detail QRA. Often the high cost of additional protective layers may be reduced with a more detailed analysis (where it might be demonstrated that fewer protective layers needed to meet a risk tolerance criteria).

Layers of Protection Analysis

Is there a limit (a maximum number) of IPL that could be considered independent? e.g. If you have more than 10, can you ensure they are truly independent? At some point, common cause failures become an important term to include, so I would expect above 3-4 protective layers there may be issues with the assumption of truly independent. Failure of the logic solver is a common cause for failure for the IPLs that use it. Even to achieve 3-4 protective layers may require multiple logic solvers to be used to achieve the reliability needed.

When using SIS as an IPL in a LOPA, should you use the "order of magnitude" credit or the actual calculated credit from the SIL calculations? If using only order of magnitude in the analysis, rounding the “credit” for a SIL-1 SIS to 0.1 is appropriate. If you are using factors more precise than order of magnitude for Probability of Ignition, Time at Risk or considering the higher demand for the same IPLS used in related scenarios, then a convenient way to compensate is by using the “design” or actual calculated SIL calculations rather than add an addition protection. For example, if you estimate a probability of ignition of 0.2, then using a PFD for a SIL-1 protection of 0.05 (rather than 0.1) may show that the scenario frequency meets the tolerable frequency without adding another protective layer.

CHEF uses "population density" for estimating consequence. Does that already include "Probability of Personnel Presence"? or it should be adjusted during LOPA. The population density is based on a random distribution of people throughout the facility (person could be anywhere within the facility at any time). By multiplying population density times the impact area, the result is the number of people who could be impacted based on this random distribution. If the resulting number of people is a fraction, this represents the likelihood of a single fatality. If once uses a single fatality as the Consequence, then the product of population density times impact area would represent the “Probability of Personnel Presence”. If a company chooses to consider <0.1 likelihood of fatality as a surrogate for Severe Injury, then a Probability of Personnel Presence would not be used as this would already be accounted for in the Consequence severity of Severe Injury.

Is there a limit on how to use time at risk? e.g. would it be acceptable to be exposed to a very-high risk, just because it happened during a very-short time? I am not aware of a specific numerical limit for Time at Risk, but the CCPS book Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis describes situations where Time at Risk should not be used. This enabling condition is not normally used with unrevealed failures (such as a transfer hose may already be in a failed state before it is used). It is also not typically applied to continuous operations where hazards are constant over time or procedure-based operations involving human performance errors in execution of a stepwise procedure.

When determining a probability (enabling event or IPL), is there a method to perform a sensibility analysis to evaluate the level of confidence in that value? Most failure probability information is based on historical data. As with many estimates within Process Risk Analysis, the uncertainty is high and the statistical confidence level may be relatively low.

Do calculation on chart 36 works for when we are NOT using order of magnitude? The LOPA documentation from slide number 36 (found in the CCPS book Layers of Protection Analysis (2001) and in the CHEF Calculation Aid) will accept values not rounded to the nearest order of magnitude (such as 0.02 or 0.5).

Your definition of LOPA is different to the one included on CCPS Books. Why? The characteristics of LOPA shared in the presentation come from the CCPS book Layers of Protection Analysis (2001). A more precise definition is found in the CCPS glossary as: "An approach that analyzes one incident scenario (cause-consequence pair) at a time, using predefined values for the initiating event frequency, independent protection layer failure probabilities, and consequence severity, in order to compare a scenario risk estimate to risk criteria for determining where additional risk reduction or more detailed analysis is needed. Scenarios are identified elsewhere, typically using a scenario-based hazard evaluation procedure such as a HAZOP Study."

We use Risk = Consequence X Frequency as criteria for including a scenario in LOPA study. Does that seem most logical? Layers of Protection Analysis is fairly detailed and complex. It may not be appropriate for very-low consequence or very-low risk scenarios. If the worst consequence is for example an objectionable odor, some companies may not require a risk analysis of this level of detail.

Do we take credit or risk reduction for our enabling condition and the initiating event in our analysis? For example, regulator failure and human failure. Enabling conditions are not necessarily common in LOPA scenarios and need to be independent of the Initiating Event. For your example of Regulator Failure and Human Failure – if the regulator could already be in a failed state that is only discovered upon the failure of proper execution a procedure, then an enabling condition probability would not apply.

Can the ignition source estimate tool from CCPS be available to participants? I believe this comes with purchase of the CCPS book Guidelines for Determining the Probability of Ignition of a Released Flammable Mass, (2014).

When using order-of-magnitude only, is there a value to try to estimate ignition probability with more than 1 significant figure? Order-of-magnitude is less than one significant figure. For example: <0.01 to 0.1 or 0.02 or 0.05 would all be rounded to 0.1 as the nearest order of magnitude.

During the presentation you mentioned procedures as IPLs. CCPS Book specifically list procedures are not usually considered IPLs. Which interpretation is correct? Both CCPS books Layers of Protection Analysis (2001) and Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis (2014) describe conditions where Human Action IPLs can be effective. These Human Actions include execution of procedures. To consider as an IPL, there must be an unambiguous cue that there is an abnormal process condition, there must be sufficient time for the operator to diagnose the situation and execute the corrective action, there are clear procedures, personnel are trained, the corrective action should not place personnel in a dangerous situation, etc.

Should we consider a leak due to cavitation? We would have a leak when the material is introduced into the system. Ideally cavitation does not occur under normal operating conditions (not always present) or there may be a design issue needing to be addressed. Cavitation is not a common Initiating Event but a situation caused by a potential initiating event, such as insufficient liquid level at the pump suction. Cavitation left unresolved may lead to seal failure and loss of containment.

LOPA is used for SIL Determination, is consequence-based scenario build or SIF-based scenario? LOPA is used to determine the number of protections needed to bring the scenario to a tolerable frequency based on your company's risk criteria.

When does a passive IPL be so effective to functionally eliminate the scenario? Like remote drainage. This situation is similar to Inherently Safer Design. Protective Layers usually have some probability of failure and are not sufficiently reliable to truly eliminate a scenario. A remote drainage situation might be reducing the frequency of pool fire scenario in the immediate area. However, the dike needs to free of debris for proper drainage to occur so it is not so reliable to eliminate the scenario.

Would you consider passive IPLs as consequence-reducing or frequency-reducing protection? For passive IPL as dike, could it reduce the consequence, saying, limiting the pool fire? or it can only reduce the frequency but the consequence is a big fire? Any IPLs could be Frequency Reducing (such as Preventive IPLs) or Consequence Reducing (such as Mitigating IPLs). For example, a Pressure Relief Device is often considered a passive protection to reduce the frequency of high overpressure. A dike might be considered a passive IPLs with regards to reducing the consequence severity of environmental damage from a spill.

How many BPCS-Loops do you consider independent if these are part of the same BPCS-system? This depends on the logic solver reliability. The CCPS book Layers of Protection Analysis (2001) notes that not more than two BPCS Loops should normally be considered for the same scenario (including the Initiating Event if it is failure of a BPCS Loop) unless the logic solver has been certified to a higher level of reliability.

Bow-Tie could be used to diagram a LOPA? Bow-Tie shows the relationship of all causes for a loss event to the left and all outcome with consequence to the right. I approach each cause-consequence pair as a separate scenario – so Bow-Tie shows the relationship between related scenarios. One can also show all protections for these related scenarios on a Bow-Tie.

Does the type of initiating events from the CCPS ·Initiating Events and Independent Protection Layers are similar to the ones in quantitative Risk analysis? The CCPS book Guidelines for Chemical Process Quantitative Risk Analysis, 2nd (2000) does not address specific Initiating Events from process upsets. The CCPS book Initiating Events and Independent Protection Layers in Layer of Protection Analysis (2015) provides many examples with recommended failure frequency.

Do you have a reference for the statement on slide 8 "The most common screening method is based on consequence"? I don't have a literature reference, merely an observation. Companies often have design and operational requirements that address that address some risk (such as requiring an inert atmosphere when handling flammable liquids or requiring some form of dead-head protection for pumps). In these cases, Layers of Protection Analysis may not add value unless the consequence or risk was higher.

If a batch operation needs cooling for 1 hour per day x 6 batches or 6 hours per day with unrevealed cooling not aligned or operator error how can Time At Risk be used. If I understand the question, failure of the cooling system would be unrevealed but the scenario could only occur during the cooling step. If there was implemented a reliable check of the cooling system before each use (cool the batch a few degrees before allowing the system to enter the hazardous step), then we would know failure needs to occur during the 6 hour/24 hours per day or 0.25 fraction of time. Without a check of the cooling system, the failure could occur at any time so a time at risk probability may not be appropriate.

What's the criteria for determining an internal explosion to destroy a vessel? Is it 4 times of MAWP? Could I assume an internal explosion always rupture a vessel? Many recent design codes in the US or Europe use a factor of approximately 1/3 to 1/4 times the estimated burst pressure or tensile strength for the MAWP. Since there can be corrosion or other factors over time, I often use 2 times the MAWP as a "minimum" burst pressure for pressure vessels. This multiple of MAWP may be lower for API tanks. When estimating the energy released upon rupture, I sometimes use 4 times MAWP but assume 50 of this energy goes to the blast wave.

Could you please elaborate a bit on about the second onion layer (Manage-Process Safety Systems)? It is an "extra" layer to the historical LOPA Onion diagram to represent that the Management Systems must be functioning properly for any safeguard protective layer to work. The reference is: J Kline and BK Vaughen, Process Safety – Key Concepts and Practical Approaches, CRC Press, Boca Rotan FL (2017)

Doesn't ALARP include summing residual risk for all consequence and adding more IPLs if residual exceeds a number. This may not be specific to ALARP. When developing a Risk Matrix, the tolerable frequency for a scenario should be less than the company's risk criteria. Often a company's criteria are based on cumulative risk and a facility may have multiple scenarios of the same of worse consequence. (For example: If a company's risk tolerance is 1×10^{-4} per year for a single fatality incident, then the *single scenario* risk matrix would likely incorporate 1×10^{-5} or 1×10^{-6} per year for a single fatality scenario as there may be many scenarios with a single fatality consequence to be summed for the corporate criteria (including residual failures).

Do we need to calculate a response time for a human to perform the task to take credit for the "average human"? I typically do try to make an estimate of the total time between an alarm and completion of the required action for a protective layer. The CCPS book Layers of Protection Analysis notes in the examples on page 103 a 10 to 40 minutes response time and simple well-documented action for a Probability of Failure on Demand of 0.1. I believe this gives some idea of the time needed for a reliable execution of a procedure.

Procedures and Human Performance

Is sabotage taken into account under human error? Sabotage is a Process Safety consideration, particularly for access to facilities or access to process control systems. However, Layer of Protection Analysis may not be suitable to evaluate scenarios involving sabotage.

When is the best time to complete a procedural PHA (nonroutine, su/sd, or other)? I believe that a procedural PHA (very-high level) can be started during the early design phase of a facility, but likely not completed until procedures are fully developed prior to start-up. At an early design stage, one can consider alarm set points and the required response time for a procedure in evaluating normal fill levels or design pressures.

On chart 33 of the previous presentation, it shows a limitation for human response to BPCS (by IEC) does it mean we can't exceed that value even after an HRA? I believe the 10 to 40 minutes response times noted in the examples from slide 33 of the Layers of Protection Analysis presentation represent a good starting point. The response time needed depends on the complexity of the procedure, staffing levels, etc. such that a Human Reliability Assessment (HRA) may be used to justify a better response time value.

Are permissive to detect human error IPL for unmitigated or mitigated risk. Typically, unmitigated risk represents the consequence times frequency with no protective layers. So a human performance protective layer

Is Human Reliability (Human Factors) done as part of LOPA (to modify/define PFD)? (if yes, how). Or as part of HAZOP (identify initiating events)? Normally HAZOP is qualitative where Human Reliability Assessment is a more detailed and somewhat quantitative evaluation to determine the probability of failure on demand (or 1 – reliability) of a procedure to be credited as a protective layer. It could be used for determining Initiating Event frequency but I don't personally see that very often.

What's the reference for table on chart 28? The reference for the LOPA document table shown on slide 28 of the Layers of Protection presentation is the CCPS book Layers of Protection Analysis (2001) page 50.

How can a human and procedure be validated for high consequence scenario OR are they not allowed generally? A human performance protection layers could be used (if appropriate) for any consequence severity, not only high-risk. For example, human response to an alarm involves a procedure to take the documented action.

How do we average the human probability based on experience of employees? Experience specific to the procedure being evaluated is a key input for estimating human reliability. The more times a procedure is executed (practiced or tested) by a person, the more likely the next execution will be done properly.

Why is it called "skill-based slip" in the example of driving through a STOP sign? This is an analogy where the car driver as an operator. The "procedure" to stop for a stop sign is well-practiced, well-documented, a test on this procedure is required obtain a driver's license.

Can you send the reference slide at the end of the presentation to us in the responses to questions? There were several references for this presentation and time did not allow sharing in detail:

OGP Report 434-5 Human Factors in QRA (2005)

CCPS, Human Factors Methods for Improving Performance in the Process Industries, John Wiley and Sons, (2007), Hoboken, NJ USA

CCPS, Guidelines for Writing Effective Operating and Maintenance Procedures, John Wiley and Sons, (1996), Hoboken, NJ USA

Reason, Human Error, Cambridge University Press (1990)

Procedure based initiating event. Can you take a time at risk if say hooking up a tank car once a month, less than 10% of time? This depends on if the hose failure is unrevealed. If the hose has failed when not in use such as run over by a fork truck or not stored properly, than time at risk may not apply. However, if a leak check is performed prior to each use, then one could use the lesser of check procedure probability of failure or time at risk. We would know that the hose could only fail during the time window of use.

Preventive Protection Layers

Should IPL also have independent utility (electricity, CW, Instrument air, etc.)? Should utility PFD's be included in the system PFD? The reliability of utilities needs to be considered in the overall reliability or probability of failure on demand (PFD) for protection layers. One also needs to consider if the utility is likely to fail as part of the scenario. In a pool fire situation, the fire may create excessive heat for equipment and damage utilities in the area. The design of most fire protection system (sprinklers, area water spray, fire monitors, etc.) normally includes back-up power (such as a diesel generator) to the fire water pumps (and, in some cases, a back-up water supply). If the final element is designed to "fail safe", the loss of power or instrument air may result in a "false trip" of a protective layer (unnecessary shut down) rather than failure of the protection upon demand.

What are general procedures for Proof Testing? Does it make a difference if you test all the elements of a SIS at the same time or at a different time (with same or different testing frequencies)? Is Partial Valve Stroke test considered as proof test? and does PVST get any credit in SIL calculations? Can you please help me understand partial loop proof test v/s full loop proof test? The purpose of a Partial Valve Stroke Test is to limit the frequency or test interval for a full stroke test in SIL calculations, particularly for facilities desiring several years between maintenance shutdown. Valve failures are modeled in two parts: those failures that can be tested using the partial stroke (such as a stuck valve) and those failures that can only be tested using a full stroke test. It is best to consult an automation subject matter expert for procedure details.

What is the place of fault detection systems (e.g. watch dog in a PLC) in a SIS? A watch dog merely keeps track of how long it takes to execute control calculations. If calculations require too much time, it is an indication that the logic solver has failed (or crashed) and the program is halted.

SIL Calculation: Would you include any of the SIF interface points with Humans (i.e. Root valves, SIF bypasses, etc.)? I think it could be a significant number. As noted in the presentation, for Human Response to Alarm, both the reliability of the instrumented alarm and the reliability of the procedure that defines the corrective actions are needed to determine the overall integrity level of the protection. If there is more than one cause to initiate the sequence of events (for example: failure of a control valve or inadvertent opening of a manual by-pass valve), I often consider these a two separate scenarios in the risk analysis to minimize complexity.

Usually the Emergency Shut Down (ESD) system has several SIFs with a common Logic Solver, if there are 2 SIFs that prevent same scenario sequence, are they considered Independent? If there is no relationship between the Initiating Event or the two Safety Instrumented Functions (sensors or final elements), they might be considered independent. For example: if high temperature shuts off the feed to a reactor AND high pressure (a separate independent sensor) shuts off the feed to the reactor, separate shut off valves would generally be needed to be considered independent. Also, the logic solver would need sufficient reliability to meet the combined SIL level of the two safety instrumented functions.

How many ways are there to trip an electric pump or compressor. This is in order to provide IPL for tripping this equipment. An interlock to stop an electric pump or compressor would typically disconnect the electrical power supply (such as opening the main contacts of the motor starter). An instrument subject matter expert may be able to provide greater detail.

Is a SIL-4 system appropriate to use for chemical industry? I have never used (or designed) a SIL-4 system. Finding a logic solver capable of SIL-4 may be much more difficult than designing two SIL-2 protective layers (possibly with two logic solvers).

I have noticed that NFPA is now designating Burner Management Systems must comply with SIL 2 instrumentation. Does Risk Assessment ask for calcs to be done? I would consider that SIL-2 integrity should be demonstrated to meet NFPA guidance. This may involve redundant gas shut off valves and high integrity (or multiple) flame detectors.

If a car seal is used on a bypass do you fail the human to not have installed the car seal...seems circular reference if you use the car seal as the safeguard? Please give an example of a physical locking mechanism. A lock with key similar to that used for lock-out tag-out would be a simple type of locking mechanism. A car seal may be sufficient to prevent inadvertent opening or closing of a valve but less effective than a lock with key. The lock or car seal would often be part of a procedure for a second person reviewing the action before proceeding.

When designing a new SIS, for example SIL-1. Do you design for 0.1, 0.01 or 0.05 PFD? This was actually the polling question used during the Preventive Safeguard presentation. Most answered using the simple order-of-magnitude SIL value such as 0.1 or 0.01. Many companies using only order of magnitude values assume that situations requiring slightly higher reliability are offset by systems where the actual reliability is better than credited. I noted that if there are two (or more) related scenarios using the same protective layer, the demand is actually the sum of each scenario PFD that can be accounted for by designing a slightly more reliable SIS. For example: if there are two scenarios using the same SIS where we want to credit as 0.1 in each scenario, we can design the SIS for 0.05 to account for twice the demand.

Could a human be used for RRF of 3-4 magnitude; seems too high? I would agree that a risk reduction factor of 3 to 4 seems beyond what would be reasonable for human reliability. Generally, I would think that using a risk reduction factor of 1 for human performance would be rare unless there were additional people involved. It is often difficult to catch one's own mistake. The CCPS book <u>Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis</u> (2015) allows a PFD of 0.01 (or risk reduction factor of 2) for "Human response to an abnormal condition with multiple indicators and/or sensors, and the operator has > 24 hours to accomplish the required response action". I also believe that the alarm annunciation should reoccur frequently rather than merely be acknowledged once if corrective actions are not yet completed.

Please discuss LOPAa vs LOPAb and requirements to use LOPAb? LOPA approach A and approach B are described in the CCPS book <u>Layers of Protection Analysis</u> (2001) pages 83 to 88. Approach A is conservative since it allows only one IPL for a single Basic Process Control System (BPCS) that must be independent of the Initiating Event. This approach eliminates many common cause failures affecting the IPL reliability. Approach B allows more than one IPL within the same BPCS or one IPL plus an BPCS failure Initiating Event that is independent of the IPL. This approach (approach B) assumes the BPCS logic solver is much more reliable than sensors or final elements. This CCPS book also notes that international standard IEC 61511 states that the risk reduction factor for all protections in the BPCS is limited to 1. So, if additional risk reduction is used, the analyst should provide an evaluation to support the use of higher risk reduction factors.

Can you give examples of Common Cause Failures for a SIF other than Power supply failure? If multiple instruments are mounted on the same nozzle of a tank, then plugging of that nozzle would represent a common cause failure (or may indicate that the protections are not fully independent). Similarly, failure of instrument air supply may impact multiple instruments and be a common cause failure.

Must check valves be subject to an annual test of function to take a 0.1 credit? The CCPS book Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis (2015) does not specifically mention a one-year inspection frequency but notes for a generic 0.1 Probability of Failure on Demand, “testing or replacement interval is set based on the results of the manufacturer’s recommendation and history of previous inspections” and “testing in situ or off-line may be conducted by providing back pressure sufficient to monitor for leakage”.

Can you pile several independent SIS to improve SIL of a trip system? One may not need to “pile” entire SIS loops but add multiple sensors and/or multiple final elements to improve the Safety Integrity Level. Often the logic solver is not the limiting factor in the overall reliability of the protection layer.

How to estimate risk reduction with mitigative systems- passive and active? If a dike is in place, do you evaluate the loss event with/without a dike? If you do it with a dike, do you use count the dike as an IPL (and reduce risk w/PFD)? Do you recommend reducing the severity in the raw risk before prevention/ protection or do you use the dike as a passive safeguard with no risk reduction? Estimation of risk reduction may depend on the specific outcome of the scenario being evaluated. If the scenario involves a spill with environmental impact such as the contamination of ground water, then using the generic 0.01 Probability of Failure on Demand may be an appropriate risk reduction factor versus an unconfined spill for this passive protection layer (as an effective dike or bund would completely eliminate the ground water contamination). For a liquid spill creating a flammable or toxic cloud, one would normally estimate the consequences using the confined surface area for evaporation to determine the reduced or mitigated consequence. In this case involving spill evaporation, the consequence determined from evaporation of the confined surface area is typically not two orders of magnitude lower than an unconfined spill (such that a risk reduction of 0.01 would not be appropriate).

I think it is important to emphasize that passive safeguards do have to be maintained or they may be found to be ineffective when needed. Yes, all protective layers need to be inspected and maintained. For example, the CCPS book Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis (2015) notes for Dikes berms, and bunds receiving a Probability of Failure on Demand of 0.01 should have “visual inspection to confirm the integrity of the containment system” and “mechanical/civil inspections are conducted at an appropriate frequency” among other considerations.

Mitigating Protection Layers

What PFD would you give to two PRV in parallel? Can a relief device be used for 0.001 PFD? The CCPS book Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis

(2015) notes for Dual spring-operated pressure relief devices that an overall Probability of Failure on Demand 0.001 if no isolation valves are present or 0.01 if a single valve could isolate one of the PRVs. There are other considerations described in this book. I have seen 0.0001 used if it is ensured that there is no common cause potential (each valve is connected to a separate nozzle on the tank and each is sized to fully mitigate the scenario independent of the other, etc.).

PSVs being ultimate layer of protection. Do you have to have control system to prevent the overpressure? Can have only the PSV to prevent the overpressure? The Pressure Safety Valve cannot be the means for pressure control but is designed to respond only to abnormal pressure conditions. The system would typically have some other system to manage the normal operating pressure such as a breather vent, a system of pressure regulators, or a pressure control loop.

Is there an industry accepted definition of what does "venting to a safe location" is? For PRF, and other devices would please comment on some requirements for a good safe location discharge? I am not aware of a universally accepted definition of "safe location" for the discharge of a pressure relief device. I believe that concentration at locations where personnel could be present be estimated to ensure it is less than a company specific concentration of concern (for example less than a fraction of the lower flammable limit for flammability hazards). If there is potential for exposure to a dangerous concentration, then venting to an effluent treatment device such as a flare, scrubber, incinerator, etc. rather than directly to atmosphere should be considered.

Can electrically classified equipment be considered as Independent protection layer? What would be their PFD? Typically release of flammable material into an electrically classified area is accounted for in the Probability of Ignition rather than consider a protective layer. I have seen electrical classification noted as a safeguard but not as a protective layer.

Foam deluge systems could also be used as a mitigation system to decrease evaporation, even if there is not yet a fire. Yes, something that floats on the surface of a spilled liquid helps to minimize evaporation rate. I have seen plastic (or other material compatible with the spill) balls in the spill containment area used for this type of application as well.

DIERS has a memo on fire protection and design but API 521 does not take credit for fire protection from deluge, how would you include fire prevention? NFPA and API address "credits" for drainage, water spray and fireproof insulation differently. NFPA 30 uses Environmental Credit Factors applied to a base correlation for maximum heat flux for fire exposure. API 521 uses different base maximum heat flux correlations for systems with adequate drainage and firefighting capability versus systems without adequate drainage and firefighting capability rather than a system of "credits". For risk analysis, I have typically used NFPA 30 correlation for storage or low-pressure tanks and API 521 correlations for pressure vessels. I normally do not take a credit for probability of failure on demand (PFD) for drainage, water spray and fireproof insulation but estimate the consequence from the appropriate maximum heat flux (per NFPA or API) divided by the heat of vaporization to obtain the required release rate.

Hypotheticals? Especially toxic release that might require shelter in place. Shelter in place locations should be maintained such that there are no penetrations (openings) that could allow infiltration of outside air, all doors and windows are closed, ventilation systems are quickly such down, etc. for potentially toxic releases. I have often been concerned about how long it takes to ensure all doors and windows are closed and all ventilation systems shut down during hypotheticals compared to how long it takes for a potential toxic release from nearby spill locations to reach the building (distance divided by wind speed).

Can we assign a lower failure probability (PFD) using two different operating methods (PRV and rupture disk in parallel) than one method (2 PRVs in parallel)? The CCPS book Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis (2015) uses the same PFD for a safety valve as a rupture disk and so I would not see why there would be a lower PFD for using a disk and valve in parallel compared to two disks or two valves.

Can monitoring performance of your system testing actually decrease the PFD based on proven in service. If so examples of required documentation? If there is sufficient company or plant historical data to show an increased mean time between failures compared to the standard tables, then possibly a decrease in failure probability (PFD) for risk analysis might be justified. One needs to be cautious when using historical data in that any safeguards or protections that exist may be incorporated into the failure frequency data.

Can you take emergency response credits for the public based on green zones, etc.? Generally, not in Layers of Protection Analysis as it is difficult to ensure the public is familiar with appropriate emergency procedures and adequately trained.

Does CCPS offer a Management System questionnaire for culture assessment? Yes. See Appendix F in the book Essential Practices for Creating, Strengthening, and Sustaining Process Safety Culture (2018).

Will the PFOD book 2015 be updated soon? Currently, there are no plans for a 2nd edition to the CCPS book Guidelines for Initiating Event and Independent Protection Layers in Layer of Protection Analysis (2015). If your company is a member of CCPS, please discuss this idea with your company's CCPS Technical Steering Committee (TSC) representative. Each TSC is encouraged to propose ideas (plural) for potential projects. I would recommend ensuring that your proposal clearly describes why there is an urgent need (you noted "soon") for an update. Are these needs significant due to improved understanding of PFD (or PFOD)? Are there significant advances in PFD-related (determining?) technologies or significant new PFD data on other equipment not noted in the first edition (from experience)? All proposed next-edition book projects then proceed through the TSC voting process within the first two quarters of *each year* with the proposals being voted on and then potentially becoming projects *for the following year*. It's not a speedy process, but it is effective when working with groups of volunteers who have full-time jobs to begin with.

How do you use Mitigating layers in LOPA? How do you use order of magnitude reduction for a mitigating layer? Does complete drainage of flammable give a credit or eliminate fire case entirely? Determining how to credit a mitigation protective layer is challenging. If mitigation completely removes the consequence (or impact) when functioning properly, then a probability of failure on demand (PFD) is an appropriate means to apply the credit. If drainage of a flammable liquid to a remote impoundment location will completely remove any fire heat input to the equipment being evaluated, then a PFD based obstruction to drainage (such as dirt, debris, ice build-up, etc. within the drainage path) and other considerations is appropriate. The CCPS book Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis (2015) suggests a PFD of 0.01 in this case. If, however, the liquid does not drain to a sufficient distance for *complete* removal of radiant heat from the fire (which is often the case), then I estimate the consequence severity from the reduced heat input with no PFD credit and use the more conservative of the two results (potential obstruction of sufficient distance and closer, but reduced, heat impact).

Is there a CCPS reference (other than CHEF manual) where "time-scaled ERPG" is defined? Does AIHA recommends time adjustments for ERPG values? The “time-scaled” or “dose-adjusted” values are merely from the definition of dose. There are many references dose relationship including Crowl and Louvar, Chemical Process Safety, 3rd (2011) and CCPS, Guidelines for Chemical Process Quantitative Risk Analysis, 2nd (2000). Dose = C^n t where C is concentration, n is an exponent derived from experimental data, and t is exposure duration. ERPG-3 is defined as a response (maximum concentration below which nearly all individuals could be exposed *without experiencing life-threatening health effects*) for a one-hour duration. From this definition of dose, we can estimate the concentration at which we would expect the same response for a different exposure duration. For example: if the 60-minute ERPG-3 is 100 ppm by volume and the exponent n=2, then the time-scaled or dose-adjusted ERPG-3 for a 15-minute exposure is $\text{ERPG-3}_{15\text{-minute}} = (60 \text{ minute} / 15 \text{ minute})^{1/2}\ \text{ERPG-3}_{60\text{-minute}} = 200$ ppm by volume.

CAI and Arnel Confined Space Explosion Case Study

Is reasonable to justify more than 3 or 4 IPLs are really independent? In other words, is 1E-7 realistic? Risk tolerance of 1E-7 is very conservative, is it not? Wouldn't installing a vapor vent on the tanks that vent to a safe location eliminate the building explosion scenario? It is a challenge to have 3 to 4 protective layers that are truly independent. It may require more than one logic solver. A tolerable frequency of 10^{-6} to 10^{-7} per year for a single scenario may be reasonable for the potential of multiple offside fatalities. This will depend on a company’s risk criteria (risk matrix). A point we tried to make was that if many protective layers would be needed to meet the risk criteria, one might consider re-design options. In this specific scenario, venting of flammable vapors within a building is very bad practice. Modifying the design to seal and vent outdoors may have eliminated the scenario.

If RV failed (PFD = 0.01), the result would be a vessel burst, right? So how can ventilation help? The scenario was not a failure relief valve but that these mix tanks were essentially open to the building. The mix tank had a loose-fitting cover over the top opening to keep out debris which was not sufficient to prevent vapors from escaping into the building.

Can you show how you use the CCPS book to reach the conclusion for the probability of ignition? What is the Hazardous Area Classification of this case? A table from page 50 of the CCPS book Guidelines for Determining the Probability of Ignition of a Released Flammable Mass (2014) was shared during the Layers of Protection Analysis presentation. This reference lists area sources for low to medium density process area (outdoors) of 0.1 to 0.15. The book also notes that indoor ignition may be a highly probability than outdoor and suggests multiplying the outdoor probability by 1.5 to 2. This would give a probability of 0.15 to 0.3 which I “rounded” to the nearest order of magnitude for the example. The area electrical classification was not mentioned in the CSB report.

BST uses congestion AND confinement to estimate the scaled pressure and distance. You chose medium congestion, but what confinement did you use? The curves shown in the presentation were based on 2 to 2.5 D confinement. The building walls fail at relatively low overpressure allowing the explosion to propagate radially (x and y directions), hence this level of confinement was used.

Why did you choose medium congestion? The building contained mix tanks and other obstacles (piping, work platforms, etc.). The equipment density was assumed that one could walk through the area fairly easily but not completely unobstructed. The CHEF presentation on Explosion contained some guidance for selecting congestion. From the ISB Incident Report it did not seem so congested that "high" would seem appropriate.

What was source of vulnerability curve? The "data points" for the graph shared in the presentation came from CCPS Guidelines for Evaluating Process Plant Buildings for External Explosions and Fires (1996) page 62. There is a more recent edition of this book but the vulnerability information was not included as there are more recent correlations based on a greater number of building structural types and incorporating blast impulse in addition to overpressure.

I'm still confused about the difference between enabling conditions and conditional modifiers, could you give some examples to help understand? This was covered to some extent in the Layers of Protection Analysis presentation. The CCPS glossary defines Enabling Condition as "a condition that is not a failure, error or a protection layer but makes it possible for an incident sequence to proceed to a consequence of concern. It consists of a condition or operating phase that does not directly cause the scenario, but that must be present or active in order for the scenario to proceed to a loss event; expressed as a dimensionless probability." One of the most common Enabling Conditions is Time at Risk if the Loss Event can only occur during a specific period of time such as during a specific step of a batch process.

The CCPS glossary defines Conditional Modifier as "one of several possible probabilities included in scenario risk calculations, generally 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 limited to: probability of a hazardous atmosphere, probability of ignition, probability of explosion, probability of personnel presence, probability of injury or fatality, and probability of equipment damage or other financial impact." There is a CCPS book Guidelines for Enabling Conditions and Conditional Modifiers (2014) with more information on this.

What is the process for adding chemicals to the tool so the information can be reused? Can CCPS add chemicals to the list and update the Chef tool? I understand that since CHEF can't take mixture for modelling that's why heptane is considered for modeling. but is it not becoming conservative in some sense? Why only Heptane is considered? In the example shared today (CAI and Arnel Building Explosion), the CSB report did not provide an actual recipe only a list of the material involved. As the flash point, boiling point, and mass release to reach the lower flammable limit were nearly the same for each of the primary solvents, we used heptane for the screening evaluation. The results for propyl alcohol is nearly identical so we did not share it. In our earlier presentation on Chemical Hazards, we shared some techniques for estimating mixture flash point and other properties. As the chemical properties are inputs in the CHEF Calculation Aid, they can be entered by either selecting a chemical or entering the property values directly. In this way, the user may estimate the mixture properties and enter the appropriate values or merely perform the consequence analysis with multiple times with single chemicals and select the "worst".

How can ventilation and RV help for the same scenario? The potential protective layer captured under "Relief Device" is to seal the tank and vent outdoors to other safe location. This change in design might even be considered an Inherently Safer Design such that the building explosion caused by excessive heating a vaporization of contents would not occur. However, it would depend on how the solid materials are added. If there is a potential for this seal-vent system to fail, then considering it a protection layer with estimated failure probability is appropriate (versus eliminating the scenario). This example is for illustration only.

LG Polymers Runaway Reaction Case Study

You pointed some design failures. Would a HIRA catch those? One of the principles of HazOp is that the process is safe to operate with the current design, right? I believe that an effective Management of Change program should have caught some of the design failures. Typically, an HIRA should be done as part of the Management of Change to ensure that new hazards are not introduced. The HIRA technique for this could include HAZOP or other techniques noted in our earlier presentation on Hazard Evaluation Techniques.

If the polymer ppm was measured in the tank every other day, why was no action taken on the day when the ppm shot up from 48 to 400? I don't believe the operations personnel appreciated the implications of this rapid increase in polymer formation. It was interpreted as a quality issue and not necessarily an early warning for a runaway reaction.

Is there a single place where I can find the charts and Q&A shared by email? We plan to update the CHEF Manual to ensure all the information in the presentations we shared is included. We may also develop a list of key questions and/or worked examples as an appendix to the manual.

What are the limitations of the reactivity screening tool? What kinetic knowledge would you recommend to have BEFORE using the tool? It is very difficult to "guess" reaction kinetics. Reactive Chemicals test data is a good place to start in understanding the thermal stability and chemical compatibility. From our polling question it appeared that roughly 50% of the participants noted have Reactivity Chemicals testing capability within their company. There are contract laboratories available for those small companies without testing capabilities. I have often asked for a simple Differential Screening Calorimetry test to determine heat of reaction and obtain some idea for reaction rate versus temperature. From there, it is easier to request more detailed testing (such as Accelerating Rate Calorimetry, Vent Sizing Package experiment or other) to address specific scenarios.

Where can we find the High Power Committee Report? The summary report can be found at: https://www.ap.gov.in/wp-content/uploads/2020/07/The-High-Power-Commitee-Report.pdf

Why an airborne rate of 525 kg/sec? A vent rate of 525 kg/sec was estimated from the reaction kinetics as what would be needed to balance the polymerization heat rate at the relief conditions of 0.1 bar and 148 C under adiabatic conditions (worst case conditions). It is what might have been used in a Risk Analysis and might provide the basis for relief design. Fortunately, some of the actions taken during the incident (such as addition of water, addition of a high temperature reaction inhibitor) and the thermal gradient within the tank such that only the top portion was likely reacting at the maximum rate mitigated the vent rate to a much lower value.

Styrene is usually stored under inert gas with sufficient oxygen levels (3-8%). Had this aspect been evaluated during the investigation? Some companies are comfortable addressing internal deflagration hazard in storing flammable liquids by managing ignition sources while others manage the oxygen content. Maintaining the oxygen in the vapor space in the range noted is common and was discussed in the presentation on Flammability Hazards.

Are you planning to use the results of the polls for any kind of study? (If yes, shouldn't you ask the participants if they agree/allow it?) We have used results of polling questions to decide what to share in the presentation. We don't plan to share the polling results externally.

Is the M5 tank also have the same (1) dip pipe arrangement as M6, OR (2) a floating return pipe arrangement? I believe that the High Power Committee report noted that m5 is a newer tank and has more temperature measurements. I am not sure about the dip pipe arrangement.

On slide 30, but I thought at the end it has more than 60 MT of styrene vaporized. Is this so? The slide later said 800 MT was vaporized. The 60 MT vaporized in the SuperChems kinetic model was that which occurred before vessel rupture in the simulation. The 800 MT was estimated based on only venting occurring without rupture.

For modelling of such an event, it's important to know the how much monomer is involved in the reaction. Any suggestions how to get these data? In the screening evaluation, it was assumed that all monomer in the tank (1830 MT) was involved and that the tank was at a uniform temperature throughout. It is a starting point and represents a "worse case".

In what condition to use LOPA? LOPA would be used if we were performing a Risk Analysis rather than an Incident Investigation. LOPA would be based on anticipating a hazard scenario and implementing protections before an incident occurs.

How to estimate impact of oxygen concentration on inhibitor depletion? The table on Slide 14 indicated a reduced induction time with lower oxygen concentration. For example: at 85 F and styrene saturated with air, the shelf life was shown to be roughly 6 months. If only 3 pm dissolved oxygen the shelf life is only 10 to 15 days. This information was from Americas Styrenics LLC, "Safe Handling and Storage of Styrene Monomer" (2016).

I think 525 kg/s is over-estimated. For one hour, this would be already 1890 MT is vaporized. Or some misunderstanding? Yes, venting would only last for 25 minutes at this high vapor rate until the styrene was essentially completely polymerized.

Was a HAZOP study in place for this case? The report noted that no risk assessment had been done, so I assume that a HAZOP was not in place.

Would a recirculation line suffice for proper tank mixing (vs the float mixing system)? Modification to the tank resulted in the inlet and outlet of the recirculating system being on the same side and near the bottom of the tank. This was such a large tank that this arrangement contributed to the poor mixing and thermal gradient which contributed to the runaway reaction. (Note that it was estimated that the top of the tank was 18 C warmer than the bottom of the tank.)

Were the inhibitor and polymer levels being monitored during the downtime? Were the tanks re-circulated during the extended downtime? Both inhibitor and polymer levels were monitored. The tank was recirculated at well but due to the modification of six months prior, the tank was not well mixed.

Is 10% vulnerability about the same as 10% lethality. What is the best reference for overpressure in typical construction to vulnerability/lethality? Fatalities primarily occur due to blunt force trauma when portions of the building collapses upon the occupants. Vulnerability and lethality are being used interchangeably.

LOPA is not used for every scenario? only for high consequence? This would depend on the company's requirement or protocol for risk analysis. LOPA involves considerable time/effort and is often reserved for the more severe consequences or higher risk scenarios.

Where can we find all Q&A, documents and records if we have registered late (after first sessions)? These were sent by email to those registered at the time. We will check into resending to those who request it and provide an email address.

So the most significant impact was toxic. There was no relief effluent treatment for the undersized relief system? There was not effluent treatment associated with the m5 storage tank. I believe operations personnel believed fire was the greater hazard and focused most attention to this possible outcome. Had this release ignited resulting in a flash fire or vapor cloud explosion, the consequence severity may have been worse.