Incorporation of inherently safer design principles in process safety assurance: Association with risk assessment and use of risk-based approach

Ming Yang, Assistant Professor, Department of Chemical Engineering, School of Engineering, Nazarbayev University, Astana, Republic of Kazakhstan 010000

Inherently safer design (ISD) is a proactive approach in which hazards are eliminated or lessened so as to reduce risk with decreased reliance on engineered (add-on) safety devices and procedural measures. Four basic principles can lead to an inherently safer design – minimization, substitution, moderation and simplification. The main idea of this study is the application of all four principles to key areas of process safety management. Discussions are provided on how to link risk assessment with the implementation of ISD design principles in process safety management. A risk-based approach framework is also developed to support the selection of alternative ISD options. The ultimate objective is to provide a bridge between inherent safety principles and new strategies for process safety assurance. The motivation for this work stems from the gap that exists between accepted theory (the hierarchy of risk control measures) and industrial practice.

Keywords: inherently safer design, process safety, risk-based, risk assessment, and risk management.

1. Introduction

Process industry is currently faced with increasing requirements for implementing inherently safer design (ISD) considerations within their processes. ISD (inherently safer design) is the most effective manner in which to reduce industrial risk, and is characterized by a set of fundamental principles (Kletz and Amyotte, 2010). Currently available techniques for risk assessment and process safety assurance either do not explicitly consider inherent safety as an alternative for risk reduction measures, or, if they do, are so complex that their usefulness is extremely limited. Thus, there is a gap between accepted risk reduction theory and industrial practice. The objective of the current research is to address the narrowing of this gap in conjunction with process industry practitioners. The current research is therefore based on a clear need to develop techniques that incorporate the ISD philosophy in risk assessment methodologies to further reduce risk to people at a given facility and in the community, and to reduce risk to the natural environment. A critical feature of this study is to identify changes to the ISD methodology that will enhance acceptance of the overall approach by industry. To fulfill this task, this paper discusses the linkage between risk assessment and the implementation of ISD principles. A risk-based approach framework is also proposed to support the selection and implementation of ISD alternatives. The application of the proposed approach to real-world cases is being performed and will be demonstrated in Part II of the paper.

2. Process safety assurance and ISD

To assure process safety, a hierarchy of safety measures is used. In order of effectiveness, from most effective to least effective, the hierarchy consists of inherent safety, passive engineered safety, active engineered safety, and procedural safety. For the purposes of better understanding and further clarification, the definitions of the four safety measures as given in CCPS (2009) are captured here as follows:

- Inherent safety: Eliminating the hazard by using materials and process conditions that are non-hazardous; e.g., substituting water for a flammable solvent.
- Passive engineered safety: Minimizing the hazard through process and equipment design features that reduce either the frequency or consequence of the hazard without the active functioning of any device; e.g., providing a diked wall around a storage tank of flammable liquids.
- Active engineered safety: Using controls, alarms, safety instrumented systems, and mitigation systems to detect and respond to process deviation from normal operation; e.g., a pump that is shut off by a high-level switch in the downstream tank when the tank is 90% full. These systems are commonly referred to as engineering controls, although human intervention is also an active layer.
- Procedural safety: Using policies, operating procedures, training, administrative checks, emergency response, and other management approaches to prevent incidents, or to minimize the effects of an incident; e.g., hot work procedures and permits. These approaches are commonly referred to as administrative controls.

The ultimate difference between inherent safety and the other three hierarchy categories is that inherent safety seeks to eliminate a hazard at its source (as a foundational measure) as opposed to accepting the hazard and looking to prevent its occurrence or mitigate its effects (Amyotte and Eckhoff, 2010). Unlike the other controls for risk reduction, inherent safety is mainly applied to remove hazards in the design of a process. For better understanding, the four key principles of inherent safety are summarized as follows:

- Minimization: Use smaller quantities of hazardous materials when the use of such materials cannot be avoided or eliminated. Perform a hazardous procedure, as few times as possible when the procedure is unavoidable.
- Substitution: Replace a substance with a less hazardous material, or a processing route with one that does not involve hazardous material. Replace a hazardous procedure with one that is less hazardous.

- Moderation: Use hazardous materials in their least hazardous forms or identify processing options that involve less severe processing conditions.
- Simplification: Design processes, processing equipment, and procedures to eliminate opportunities for errors by eliminating excessive use of add-on safety features and protective devices.

3. Risk assessment and ISD in process life cycle

There are many opportunities to incorporate ISD principles into various aspects of risk assessment that can be applied in different phases of the process life cycle. Some examples of the opportunities are present below.

3.1 What-if Approach in conceptual phase

The principles of inherent safety can be incorporated into the What-if approach in the conceptual phase of the process life cycle. Use of inherent safety principles as 'mind triggers' in providing recommendations during a What-if analysis for each section of a process will help to ensure that the concepts of ISD are visible within the process. For example, assume a refrigerant has to be selected in the conceptual phase to provide cooling in a chemical process (CCPS, 2009). In this case, a possible What-if question corresponding to the substitution principle of ISD could be 'What if a flammable refrigerant is used instead of a non-flammable refrigerant?'.

3.2 RAM analysis in FEED (Front End Engineering Design) and detailed design phases

Reliability, availability and maintainability (RAM) analysis plays an important role in achieving an optimum performance in any design modification. ISD principles can be incorporated in RAM analysis to improve and predict the performance of the system in both FEED and detailed design phases of the process life cycle. For example, eliminating or minimizing in-process storage of chemicals can ensure better reliability of critical equipment. A lower amount of in-process stored chemicals can reduce the operation time, and improve reliability, availability and maintainability of these critical pieces of equipment. Necessary follow-up based on the results from the RAM analysis are required to avoid system failure or any process upset. Incorporating the moderation principle of ISD, for example, can lead to using lower pressures or temperatures if possible.

3.3 Safety critical elements in detailed design phase

Safety elements that are critical to use for preventing accidents or mitigating the effects of accidents, are called safety critical elements (SCEs). SCEs are classified as equipment, units, control devices, barriers, protocols, or systems whose failure could lead to a major accident. SCEs (e.g., critical alarms, critical interlocks, pressure relief and venting systems, fire detection and protection equipment, emergency isolation valves, etc.) have to be designed and installed in an inherently safer way. For example, safety systems can possibly be simplified by interfacing more components or equipment with a SCE. Using a shutdown switch for various process components or equipment, it could be possible to stop a process upset from propagating to a catastrophic failure.

3.4 HAZOP in detailed design and operations phases

The principles of inherent safety can be incorporated into the HAZOP approach to bring harmony to a system in case of process upsets and deviations. For example, the introduction of a catalyst with enhanced activity or selectivity, or of better mixing arrangements may facilitate the use of lower reaction temperatures or pressures (Marshall and Ruhemann, 2001). This example can be described as shown in Table 1 to identify ISD opportunities in the HAZOP approach.

4. The framework of risk-based approach

Varieties of ISD alternatives can be identified in different stages of process life cycle. Figures 1 and 2 present the proposed framework that can be used to screen out better ISD options. The following sections describe the main steps of this proposed approach.

4.1 Estimate the risk of base design

Life-cycle considerations play a vital role in implementing ISD changes and the best time to implement ISD alternatives is considered to be during early stages of process development and design. It is essential to make full use of available opportunities as early as possible (i.e., conceptual stage of the design) to minimize loss. Therefore prior to estimation of the risk, the design stage should be specified. This helps to understand the different attributes, design criteria and nature of the process.

A novel approach has been proposed to assess the risk of the base design based on damage factor (DF). This method eliminates the over-conservativeness of some existing index-based approaches, e.g., PIIS (Edwards and Lawrence, 1993), ISI (Heikkila, 1999), and SHE method (Killer et al., 2000). The following four basic process accident scenarios are considered in risk assessment:

- Vapor cloud explosions (VCE)

- Fires: pool fire, jet fire, fire ball, and flash fire
- Toxic gas release
- Toxic liquid release

Probability of occurrence can be calculated for each design unit using the bow-tie model (Figure 3) proposed by Rathnayaka et al. (2014).

Severity of damage due to fire

Heat flux is calculated as a function of the distance from the surface of the fire and plotted. Figure 4 gives an example of such graph. The heat flux from a certain distance from the fire is calculated from the product of actual surface emitting power, the view factor and the atmospheric transmissivity.

$$q' = SEP_{act} F_{view} \tau_a \tag{1}$$

Where *SEP_{act}* (W/m²) is the surface emitting power, F_{view} is the view factor, τ_a is the atmospheric transmissivity.

In Equation 1, F_{view} and τ_a are calculated as a function of the distance X (m) from the center of the fire. Since the effects of fire depend on the heat flux, the maximum heat flux of concern shall also be determined based on the damage level for which the risk is calculated. Table 1 can be used to define the maximum heat flux. Once the maximum heat flux is determined, the corresponding distance from the surface of fire (i.e., X_1 in Figure 4) is obtained. A maximum distance of concern (DC) is defined based on the considered facility and requirements of the management. The Damage Factor (DF) is defined as follows.

$$DF = \left\{ \begin{array}{ccc} \frac{X_1}{DC} & for & X_1 \le DC \\ 1 & for & X_1 > DC \end{array} \right\} \tag{2}$$

The severity index of damage due to fire (SI_{fire}) is quantified as a product of the damage level index (DLI) and the DF:

$$SI_{fire} = \text{DLI} \times \text{DF} \tag{3}$$

In Equation 3, the DF is interpreted as the percentage of distance/area (out of the defined maximum distance/area of concern) that may possibly be affected with a damage level given by the DLI. The following example is used to demonstrate how to obtain the SI_{fire}.

For illustrative purpose, assume that:

- 100% lethality in 1min and 1% lethality in 10s are the damage level of concern. (Table 1 indicates that the maximum heat flux is 37.5 kW/m^2).
- Figure 1 shows that X_1 associated with 37.5 kW/m^2 is 20 m.
- DC is 100 m.

Then the SI_{fire} is calculated as follows:
SI_{fire} = DLI × DF = 10 × (20/100) = 2

Severity index of damage due to VCE

For VCE scenarios, overpressure is calculated as a function of distance from the center of explosion and plotted. Figure 5 gives an example of such graph. Blast over pressure is obtained using the Baker-Strehlow-Tang method (Baker et al., 1996, Baker et al., 1998). Table 3 can be used to define the over pressure of concern (OPC) given the effects of explosion for different over pressures. Following the similar process as described in the previous section, the severity index of damage due to VCE (SI_{VCE}) is quantified using Equation 3.

Severity index of damage due to toxic gas release

For a given release rate, the concentration of the toxic gas release is calculated as a function of the distance from the release point. The gas concentration can be obtained from the Gaussian dispersion model (EPA, 1995; Turner, 1994). Figure 6 gives an example of such graph. The height of the concentration of concern can be set as the average height of a person. A concentration limit is defined according to the threshold limit value (TLV). The DF is defined by the following equation:

$$DF = \left\{ \begin{array}{ccc} \frac{X_2 - X_1}{DC} & for & X_2 \le DC \\ \frac{DC - X_1}{DC} & for & X_2 > DC \end{array} \right\} \tag{4}$$

Where X_2 and X_1 are given in Figure 6.

Table 3 gives an example of the damage level index associated with different level of concentrations and exposure duration. Then the severity index of damage due to toxic gas release (SI_{TG}) can also be quantified using Equation 3.

Severity index of damage due to toxic liquid release

The damage is assessed based on the airborne quantity of the toxic substance. The total airborne quantity (AQ) of the toxic substance released is obtained through the addition of the fraction flashed from the liquid (AQ_f) and the fraction evaporated from the liquid pool surface (AQ_p). The Dow's Chemical Exposure Index Guide (AIChE Technical Manual, 1994) provides the following equations.

$$AQ_f = 5(F_v)L \qquad (5)$$

Where L is the liquid flow rate and Fv is the fraction of the liquid that will flash:

$$AQ_p = 9 \times 10^{-4}(A_p^{0.95})\frac{(MW)P_v}{T+273} \qquad (6)$$

Where A_p is the pool area, MW is the molecular weight, P_V is the vapor pressure of the liquid at the characteristic pool temperature and T is the characteristic pool temperature.

The airborne concentration is calculated as a function of distance from the point of release using Equation (7). Figure 7 gives an example of the airborne concentration-distance graph.

$$C = AQ \times (\frac{6651}{X})^2 \qquad (7)$$

Where C is the airborne concentration, X is the distance from the point of release, and $AQ = AQ_p + AQ_f$.
The concentration limits can be obtained from the Emergency Response Planning Guide (ERPG) values specified by the American Industrial Hygiene Association (AIHA) for specific chemicals (Emergency Response Planning Guidelines, 2015). Three categories of ERPG values (i.e., ERPG-1, ERPG-2, ERPG-3) have been defined by the AIHA based on the concentration levels where one may anticipate observing adverse effects. Assume that damage level index for concentration levels solely depends on the type of toxic gas released, indices for the 3 ERPG values. For instance for ERPG-1, we can assign an index of 3, ERPG-2 an index of 6 and ERPG-3 an index of 9. The severity index of damage due to toxic liquid release (SI_{LG}) can be quantified through the similar process as given in the previous section.

4.2 Identify the critical elements

The base design is checked for all relevant codes and standards using a perspective approach to ensure that all relevant codes and standards are complied with. Hazard identification method (e.g., Checklist, HAZOP, and FMEA) is carried out on each element of the base design to identify the critical elements (considering material, equipment and process conditions).

4.3 Implement the principles of ISD to generate alternate designs

The principles of ISD (i.e., minimization, substitution, moderation, and simplification) are implemented one-by-one to develop alternate designs. The applicability index of inherently safer design options can be obtained using the approach proposed by Rathnayaka et al. (2014).

4.4 Assess the risks of the alternate designs

The same index-based risk assessment approach is used to assess the risks of the alternate designs. For each design option, a risk reduction value is obtained by comparing the risks of base and alternate designs.

4.5 Identify the optimum design

Both the risk reduction and applicability indices are considered to identify the optimum design. Given equivalent weights to risk reduction and applicability, a design performance index value is computed as follows. A greater index value indicates a better design.

$$PI = \frac{1}{2} \times RR + \frac{1}{2} \times a \qquad (8)$$

Where RR is the risk reduction value, and a is the applicability index.

5 Conclusions

This brief paper has demonstrated various ways in which inherently safer design principles can be incorporated in a process safety management system, and proposed a framework to implement ISD principles and selection ISD options through risk-based approach. Key to the success of ISD implementation is its consideration at the earliest possible stages of the design life cycle. The application of the proposed approach to real-world case study is being conducted and will be reported in part II of the paper.

References

AIChE Technical Manual. (1994). Dow's Chemical Exposure Index Guide, first ed. Published by the American Institue of Chemical Engineers.

Amyotte P.R. and Eckhoff R.K. (2010). Dust Explosion Causation, Prevention and Mitigation: An Overview. Journal of Chemical Health and Safety, 17:15-28.

Baker, Q. A., Doolittle, C. M., Fitzgerald, G. A., and Tang, M. J. (1998). Recent developments in the Baker-Strehlow VCE analysis methodology. Process Safety Progress, 17(4), 297–301.

Baker, Q. A., Tang, M. J., Scheier, E. A., and Silva, G. J. (1996). Vapor cloud explosion analysis. Process Safety Progress, 15(2), 106–109.

Center for Chemical Process Safety (CCPS). (2009). Inherently Safer Chemical Processes: A Life Cycle Approach. New York, NY: Wiley.

Edwards, D. and Lawrence, D. (1993). Assessing the inherent safety of chemical process routes: is there a relation between plant costs and inherent safety? IChemE 71 (B), 252–258.

Emergency Response Planning GuidelinesTM. (n.d.). Retrieved January 10, 2016, from https://www.aiha.org/get-involved/AIHAGuidelineFoundation/EmergencyResponsePlanningGuidelines/Pages/default.aspx

Environmental Protection Agency. (1995). EPA–454/B–95–003a (User's Guide for the Industrial Source Complex ISC3 Dispersion models, Volume I). Research Triangle Park, North Carolina, 27111.

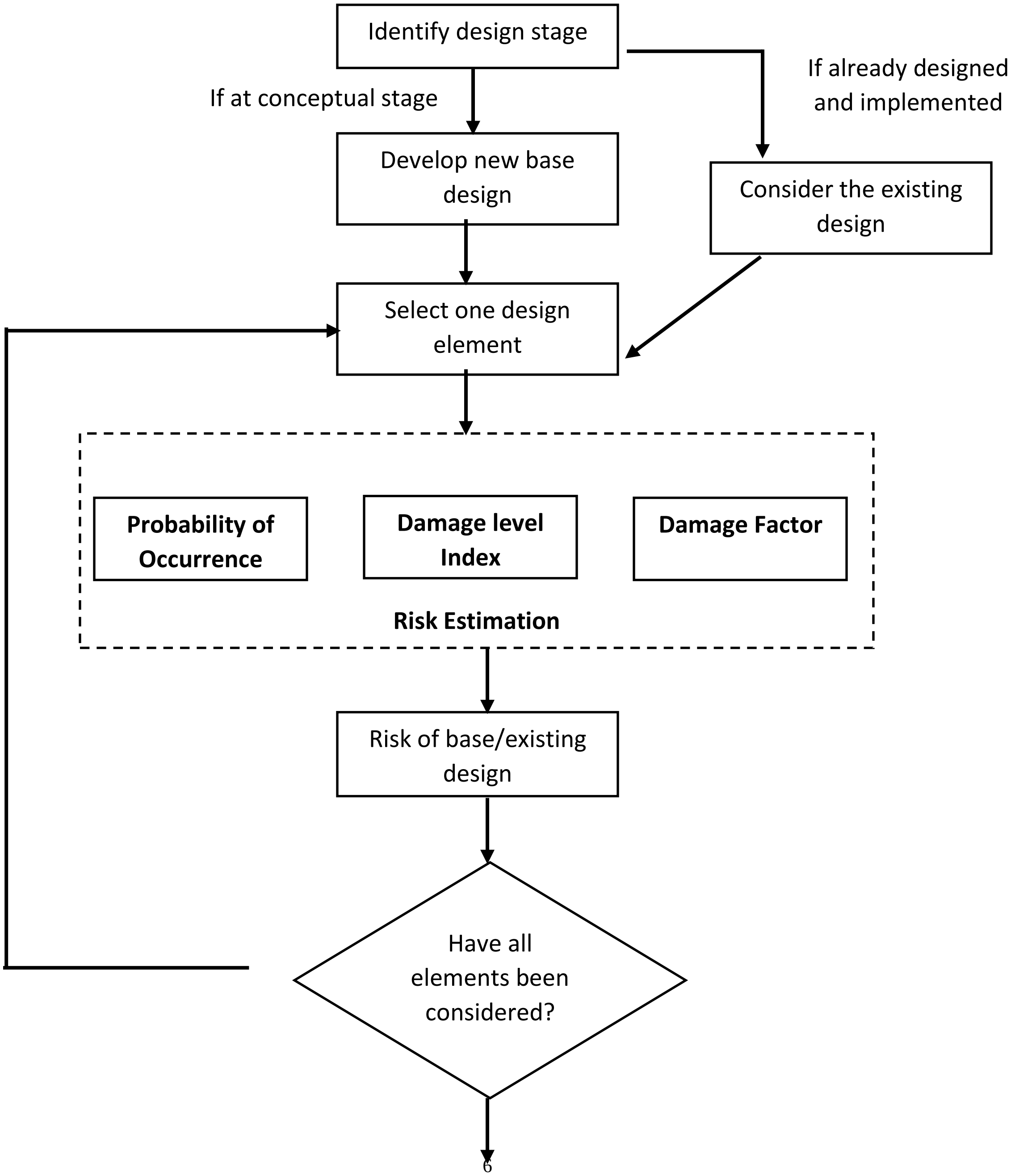
Heikkila, A.-M. (1999). Inherent safety in process plant design: An index-based approach (D.Sc.Tech.). Teknillinen Korkeakoulu (Helsinki) (Finland), Finland. Retrieved December 20th 2015 from http://search.proquest.com.qe2a-proxy.mun.ca/docview/304579749?pq-origsite=summon

Kletz T. and Amyotte P. (2010). Process Plants: A Handbook for Inherently Safer Design. Second Edition. New York, NY: CRC Press.

Koller, G., Fischer, U., & Hungerbühler, K. (2000). Assessing Safety, Health, and Environmental Impact Early during Process Development. Industrial & Engineering Chemistry Research, 39, 960–972.

Marshall V. and Ruhemann S. (2001). Fundamentals of Process Safety. Warwickshire, UK: Institution of Chemical Engineers.

Rathnayaka, S., Khan, F., & Amyotte, P. (2014). Risk-based process plant design considering inherent safety. Safety Science, 70, 438–464.


Identify design stage
If at conceptual stage
If already designed and implemented
Develop new base design
Consider the existing design
Select one design element
Probability of Occurrence
Damage level Index
Damage Factor
Risk Estimation
Risk of base/existing design
Have all elements been considered?

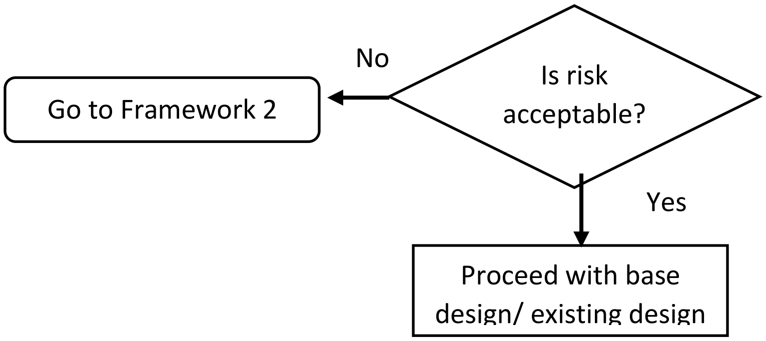
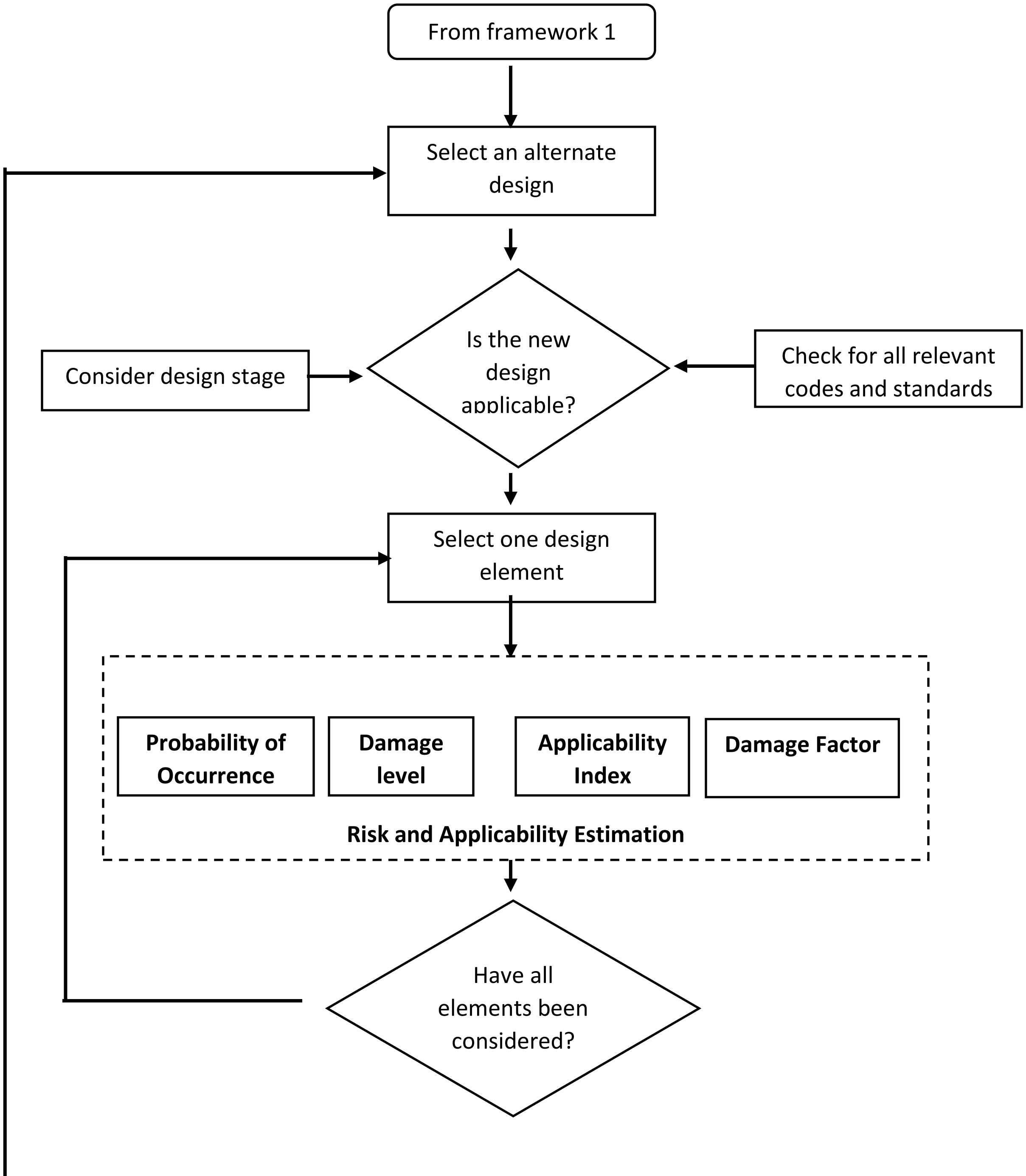


Figure 1 Risk assessment of the base design


From framework 1
Select an alternate design
Consider design stage
Is the new design applicable?
Check for all relevant codes and standards
Select one design element
Probability of Occurrence
Damage level
Applicability Index
Damage Factor
Risk and Applicability Estimation
Have all elements been considered?

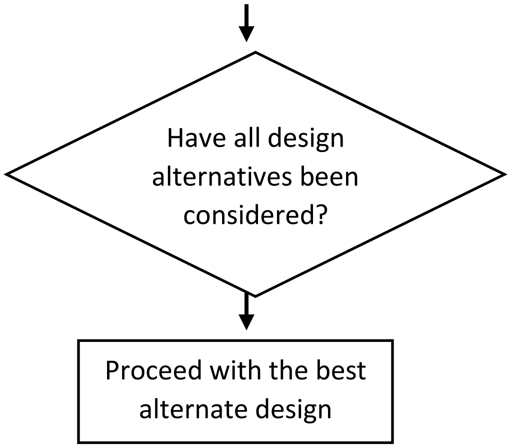

Have all design alternatives been considered?
Proceed with the best alternate design

Figure 2 Risk assessment of the alternate inherently safer design options

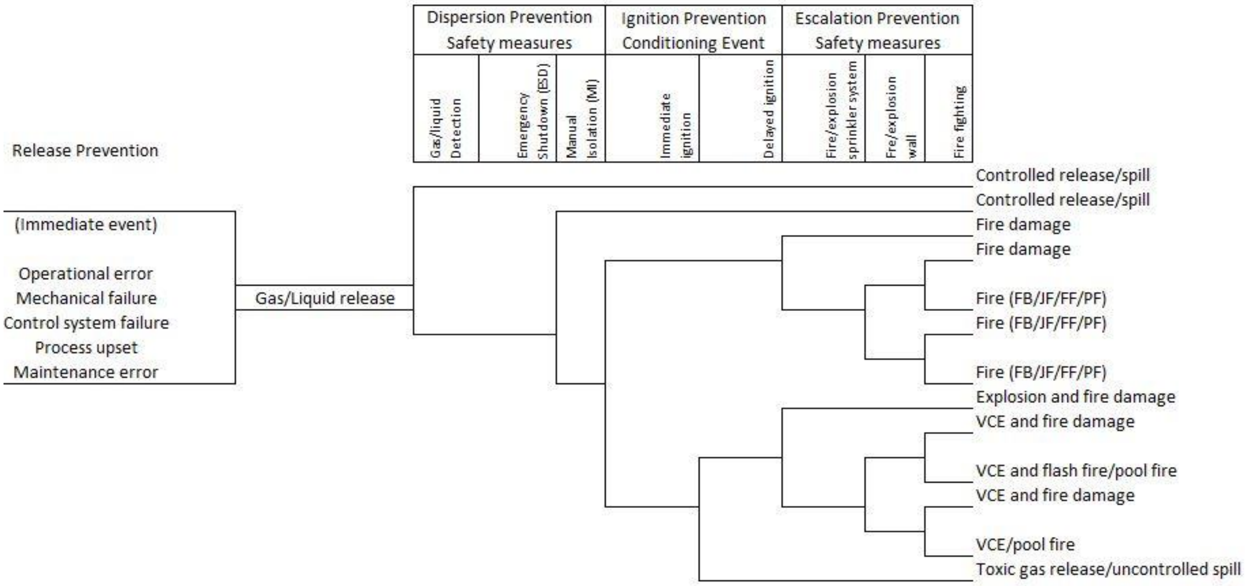
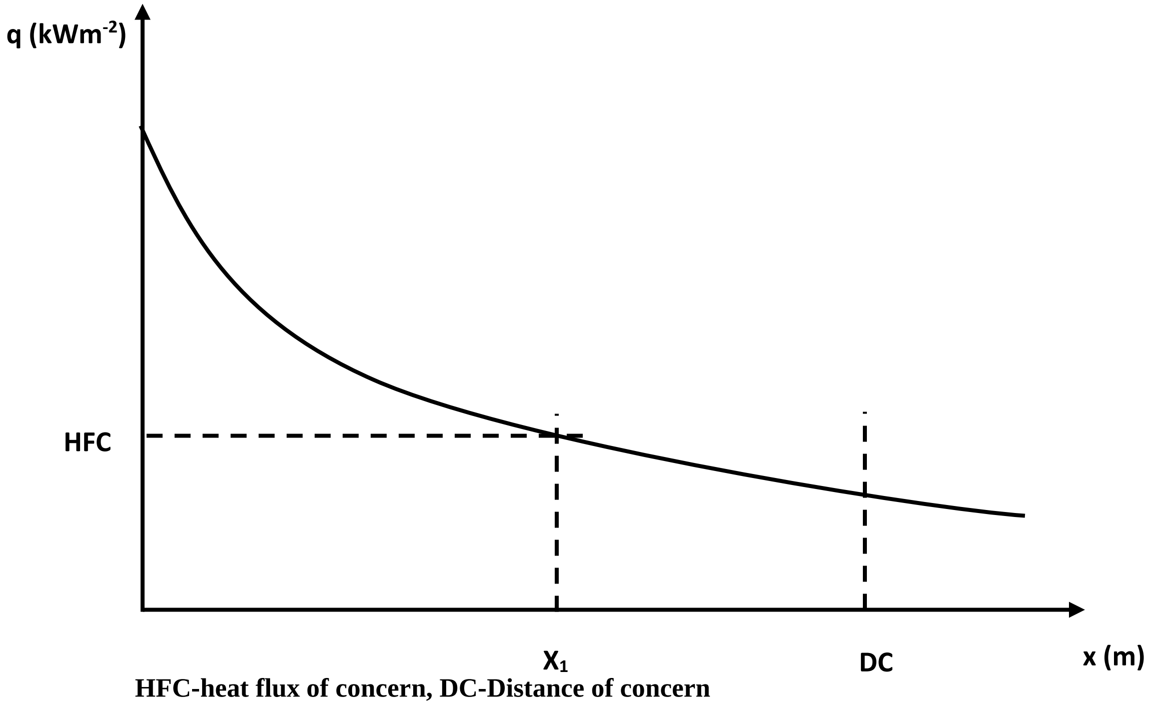
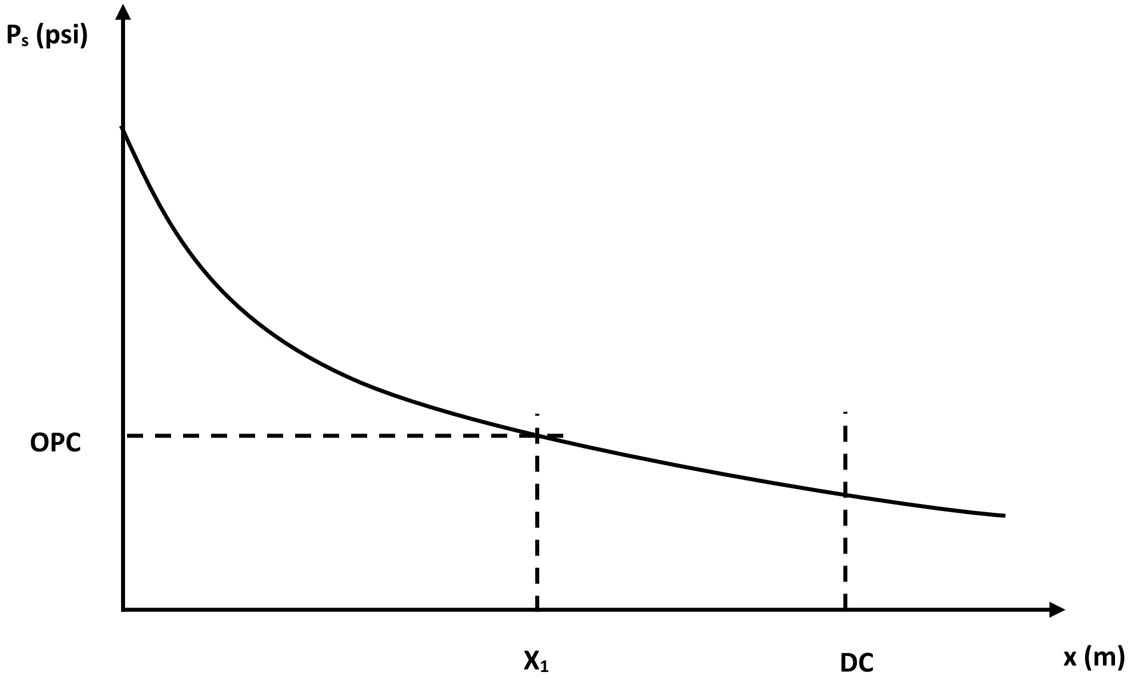


Figure 3 The bow-tie model (Rathnayaka et al., 2014)



HFC-heat flux of concern, DC-Distance of concern

Figure 4 Heat flux-distance graph



OPC – Over pressure of concern

Figure 5 Overpressure- distance graph

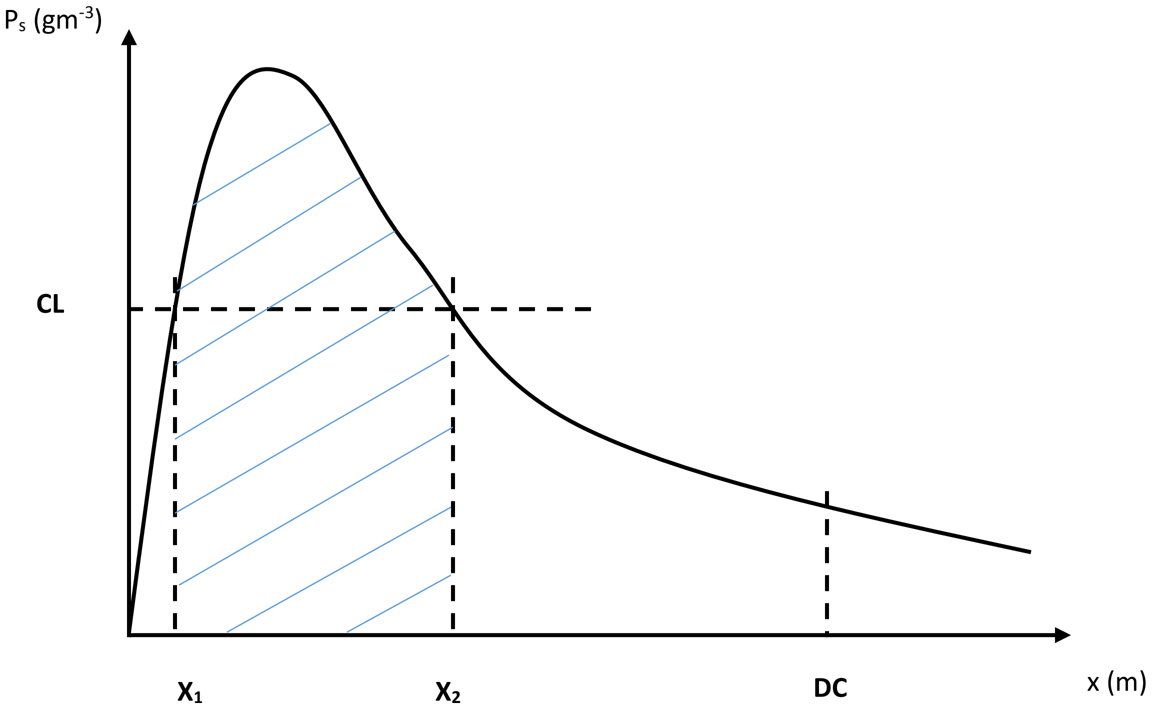
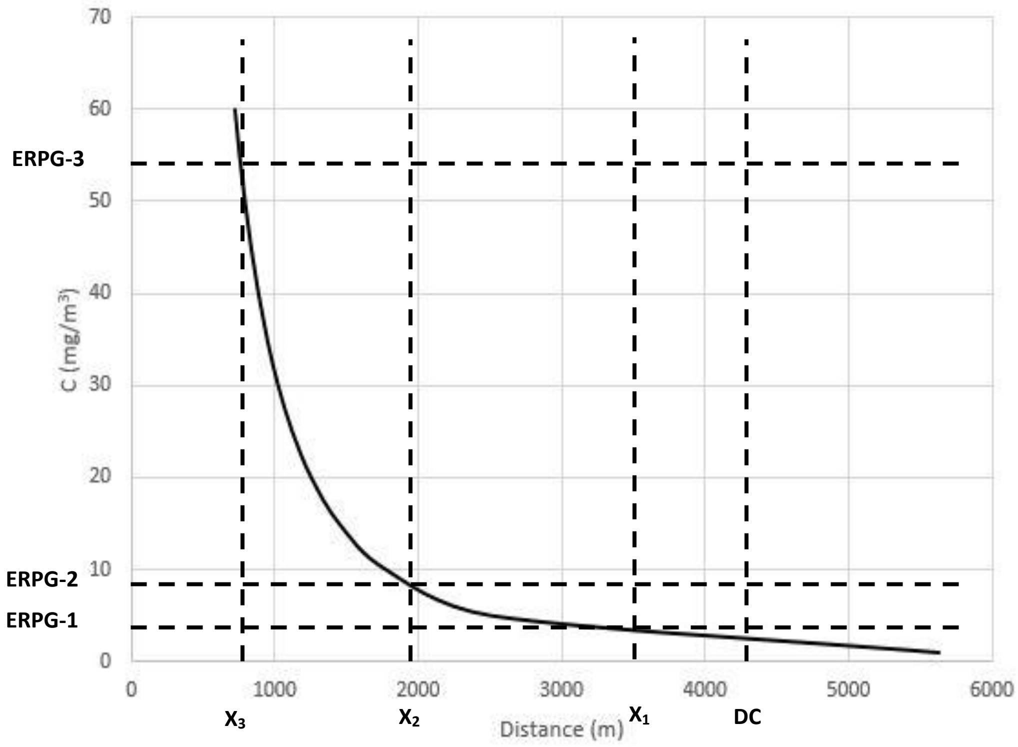


Figure 6 Concentration-distance graph (toxic gas)



Where X_i is the corresponding hazard distance for the ERPG value considered.

Figure 7 Concentration-distance graph (toxic liquid)

Table 1 ISD opportunities in HAZOP analysis.

Item in HAZOP Approach	Parameter in HAZOP Approach	Deviation	ISD Opportunity
Process chemistry and conditions	Pressure and temperature	Higher pressure and higher temperature	Moderation by introducing a catalyst to ensure lower reaction temperature or pressure, and better mixing.
	Mixing rate	Inadequate mixing	

Table 2 Heat flux and associated damage levels

Heat flux (kWm^{-2})	Effects on materials	Damage level index	Effects on humans	Damage level index
150-200	1st degree damage for iron	10-9	100% lethality	10
20-80	2nd degree damage for iron	8-7	100% lethality	10
37.5	Equipment damage	6-5	100% lethality in 1 min 1% lethality in 10s	10
25	Minimum intensity for ignition of wood in prolonged exposure	4-3	100% lethality in 1 min Serious injuries in 10s	9-8
12.5	Minimum intensity for ignition and melting of plastic tubes	2-1	1% lethality in 1 min 1st degree burns in 10s	4-7
4	-	0	No lethality 2nd degree burns probable Pain after exposure of 20s	1-3
1.6	-	0	Acceptable limit for prolonged exposure	0

Table 3 Vapor cloud explosion and associated damage level

Overpressure (psi)	Effects	Damage level index
>20	Heavy built concrete buildings severely damaged or demolished	10
10	Reinforced concrete buildings severely damaged or demolished Most people are killed	9
5	Buildings collapse, injuries universal, widespread fatalities	8-6
3	Residential structures collapse Serious injuries common, fatalities may occur	5-3
1	Window glass shatter Light injuries may occur	2-1