Challenges in Process Safety Assurance of a Hazardous Epoxidation

Stephen M Rowe, Managing Director, DEKRA Process Safety UK, Phi House, Southampton Science Park, Southampton, Hampshire, SO16 7NS

Keith V Middle, Principal Process Safety Specialist, DEKRA Process Safety UK, Phi House, Southampton Science Park, Southampton, Hampshire, SO16 7NS

Older, existing plant processes are not immune from a requirement to demonstrate that a safe system of work exists – indeed – they can often present the greatest risks as process safety knowledge and regulatory expectations evolve over time. This case study summarises the retrospective process to assure safety of an energetic epoxidation process following regulatory intervention action.

The process involves a number of hazardous materials (including hydrogen peroxide and performic acid) and process safety risks (including thermal stability and exothermic reaction). The paper focuses on the integration of various disciplines required to construct the safety case taking in to account reaction thermochemistry and kinetics, identification of hazardous scenarios, experimental quantification of the consequence of hazardous scenarios, layers of protection analysis, safety instrumented systems and relief system design - all of which are required to construct a sound safety case. Taken together - and with several changes to the plant/process - a tolerable residual risk can be demonstrated.

The study contains some nuance situations where wider lessons can be learnt by others - specifically in the areas of commonality of hazardous scenarios and risk, relief system design, the contribution of quench systems as a layer of protection, the vulnerability of certain safety measures, and ultimately in the cost of retrospectively assuring safety. The case study concludes with a reflection on the criticality of engagement of laboratory chemists in process safety, including an engineering contribution to the chemical development process. Overall, there are a large number of lessons to be learned by those developing new processes and those operating older processes.

KEYWORDS: reaction hazards, epoxidation, runaway, basis of safety, exothermic reaction safety

Introduction

Process safety knowledge and methodologies develop continuously over time and ensuring that legacy process safety assessments are regularly updated to reflect good practice in a current context is critically important. Deficiencies in process safety assurance are typically revealed in one of two ways:

- You work it out for yourself
  - reactively as a result of an incident; or
  - proactively via internal competence development
- Someone points it out to you
  - an external assessor – an auditor, external specialist consultant or a regulator

Proactive approaches are clearly favoured and encouraged. The consequence of a reactive approach can be a catastrophic event (with a range of collateral damages impacting the site and brand) or enhanced regulatory intervention. The latter scenario is uncomfortable, to say the least, as it puts pressure on the organisation to act under close scrutiny or face escalation of regulatory action through improvement notices to prohibition notices.

In the current case study, the regulator spotted deficiencies in several components of the safety case for a large scale, energetic, epoxidation process which had been operated by a company for over 50 years. The company engaged external expertise, together with growing their own internal competence, to close the gap to regulatory compliance and towards best practice. There were numerous issues which the company had to address around worst case scenario identification, layers of protection and risk quantification / estimation, and relief system design (fundamental sizing, vent stream treatment and mechanical design considerations (thrust force capability)).

Over a period of two years the company has diligently addressed each of the identified gaps but the cost accrued is an eye-watering £400k – and still climbing. Of course, over the 50 years the plant has operated there have been huge changes in the process, more stringent legislation, more educated and knowledgeable regulators, developments in understanding of process safety, and sophistication in the methods used to substantiate acceptable residual risk levels.

The primary purpose of this paper is to highlight the range of disciplines necessary to derive a safe system of work and the "inter-connectedness" of the different process safety activities involved. Deficiency in any discipline or activity has the potential to completely undermine the process - resulting in a false sense of security and generating an organisational cognitive bias that the safety is assured. This potential for cognitive bias should not be allowed to establish itself in an organisation amongst those involved in the process safety activities – a "chronic sense of unease" is ultimately a far more effective mindset. Key Learning Points (KLP's) are highlighted throughout the paper and summarised in the conclusion.

Details of the Epoxidation Process

Process Description

Vegetable oil is epoxidised using performic acid formed in-situ by the reaction of hydrogen peroxide and formic acid.

The process takes place in 22m^3 reactors as a semi-batch process with formic acid added over 120 minutes to a vegetable oil / solvent / hydrogen peroxide mixture at 65°C. On completion of the formic acid addition, further hydrogen peroxide is added to react with formic acid regenerated by the reaction (see Figure 1) and the batch allowed to react for a further 5 hours prior to cooling and downstream processing (no further reactive chemistry steps).

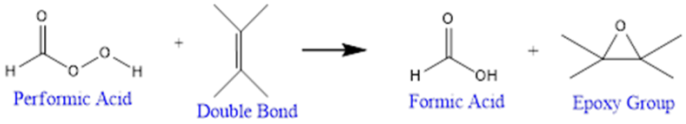

Figure 1. The Prileschajew Reaction for Epoxidation of Double Bonds

The local regulatory inspector suspected deficiencies in the process safety studies performed and engaged specialist inspector support to dig deeper. The regulator remained engaged with the operating company whilst improvements in process safety were planned and executed. This was the first, focused, regulatory intervention in the 50 year operation of the plant and process.

KLP 1: A golden rule in process safety is that the incident-free operation of a process over a number of years is not a suitable basis of safety. "We've been running this process for XX years and never had an incident; why do I need to do a hazard study now?" is inadmissible in court.

Despite having a good understanding of the process garnered across the 50 years of experience, competence in all areas of process safety is a requisite to be able to prove that risks are as low as reasonably practicable (ALARP). Any gaps in knowledge or deficiencies in processes are astutely detected by increasingly knowledgeable regulators.

KLP 2: Regulators, particularly specialist inspectors, are increasingly knowledgeable in process safety – often with leading edge knowledge. Operating companies must be confident that their process safety studies are able to withstand scrutiny – either through provision of internal competence, using external specialists or a combination of both.

Primary Process Safety Risks of the Process

The principal hazards of the process include:

- a highly exothermic main reaction, and hence the process is arranged as a semi-batch operation,
- potential exothermic decomposition of the hydrogen peroxide which generates gas and is exothermic,
- detonable mixture concentrations. Owing to the process raw materials (primarily formic acid and hydrogen peroxide) there is a combination of concentrations that could lead to a shock-sensitive detonable mixture. This risk is mitigated by control of concentrations outside of the detonable concentration range,
- flammability risk associated with process materials and
- oxidation / spontaneous combustion propensity of vegetable oil when finely divided (for example, when absorbed by vessel and pipe lagging).

In the early years of the process operation, considerable investigation was directed to understanding and avoiding the potential for a detonable mixture (3rd point, above); far less study was undertaken on the first two hazards.

The failure scenario study highlighted certain specific cases which required more detailed consideration as to their consequences and likelihood; it is these that were examined in the Layer of Protection Analysis (LOPA), simulation (adiabatic calorimetry) and vent sizing work. The balance of this paper focuses on the process undertaken to assure that runaway reaction risks were ALARP and met the company's own residual risk criteria.

KLP 3: A safe system of work is required to protect against all foreseeable risks

Assuring Safety against Runaway Reactions

Strategic Assessment Process

Whilst more prescriptive methods can be reliably applied to dealing with flammability risks, runaway reaction risk assessment tends to be a less prescriptive field. However, a structured methodology must be applied within an organisation to ensure that such risks are assessed in a systematic and reliable way. The starting point of runaway reaction risk assessment should not be the point of scale-up where Chemical Engineers take ownership of process safety. Decisions made in development by chemists, essentially dictate the level of hazard of the process – leaving engineers to handle risk reduction. A simplistic lifecycle assessment methodology is illustrated in Figure 2 – starting at the chemical route selection stage. Educating development chemists in process safety is critical in ensuring that developed processes present as low an intrinsic hazard as possible.

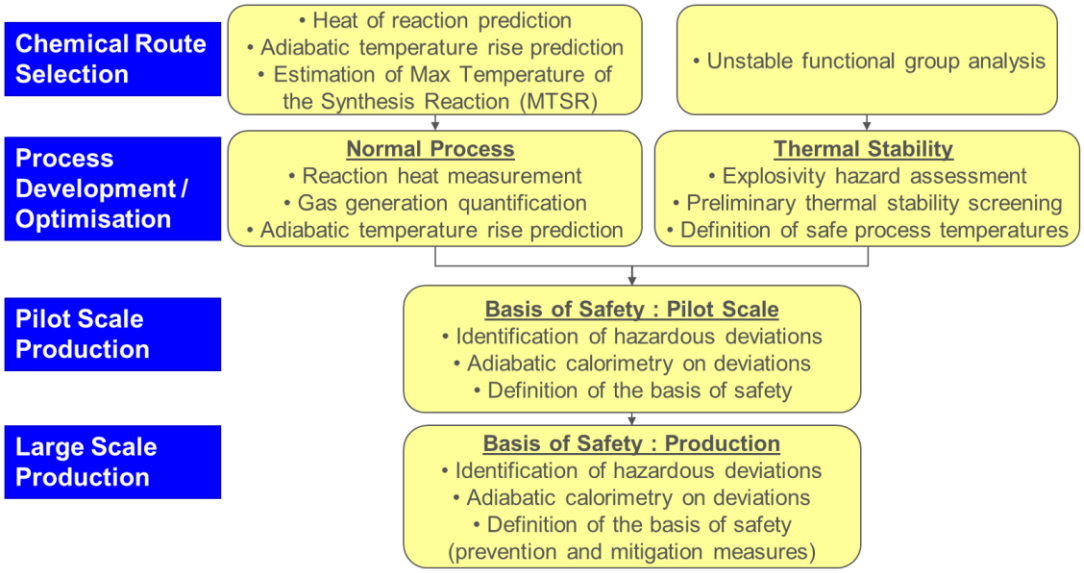

Figure 2. Systematic Assessment of Runaway Reaction Hazards

For existing and legacy processes, a first step in assessment is to ensure that the process is adequately characterised (thermodynamics, kinetics and thermal stability well understood). This represents important data to take through to the identification of hazardous deviations (Process Hazard Analysis (PHA)) and enables better and more informed decisions to be taken when considering the consequences of identified deviations. In the current study, reaction calorimetry and thermal stability information on intermediate mixtures was collected to backfill knowledge prior to repeating the PHA.

KLP 4: A systematic assessment process should be engrained in the process development and process operation lifecycle. Process Safety must be considered from the start of the development journey. For retrospective process assessments, missing characterisation data should be backfilled to optimise the effectiveness of decisions made when considering consequences in the PHA process.

Process Thermochemistry

The process involves multiple potential exothermic reactions. Reaction calorimetry using the Mettler Toledo RC1e system [ref. Mettler] on the desired reaction indicated that the epoxidation stage has a heat of reaction of -230 to -250 $kJ.mol^{-1}$ whilst undesired reactions also offered considerable heat release potential (decomposition of hydrogen peroxide and performic acid have heats of reaction of -98 $kJ.mol^{-1}$ and -352 $kJ.mol^{-1}$, respectively). In context, the desired reaction had a potential adiabatic temperature rise of 330 K; this would substantially exceed the reaction vessel's design temperature and its design pressure. In addition to the exothermic nature of the reaction, additional risks associated with the process were:

- the generation of permanent gas during the second stage peroxide addition, and
- non-instantaneous kinetics. Idealised semi-batch processes would offer instantaneous kinetics such that reaction will occur "on contact", providing direct control over heat release through control of the feed and feed rate. In the epoxidation, accumulation of unreacted thermally sensitive material occurred throughout the additions, with the maximum level of accumulation equating to 51% immediately after the second peroxide addition.

Figure 3 illustrates the reaction calorimetry profile for the process, clearly illustrating both the gas generation and accumulation of reactants (and hence heat release).

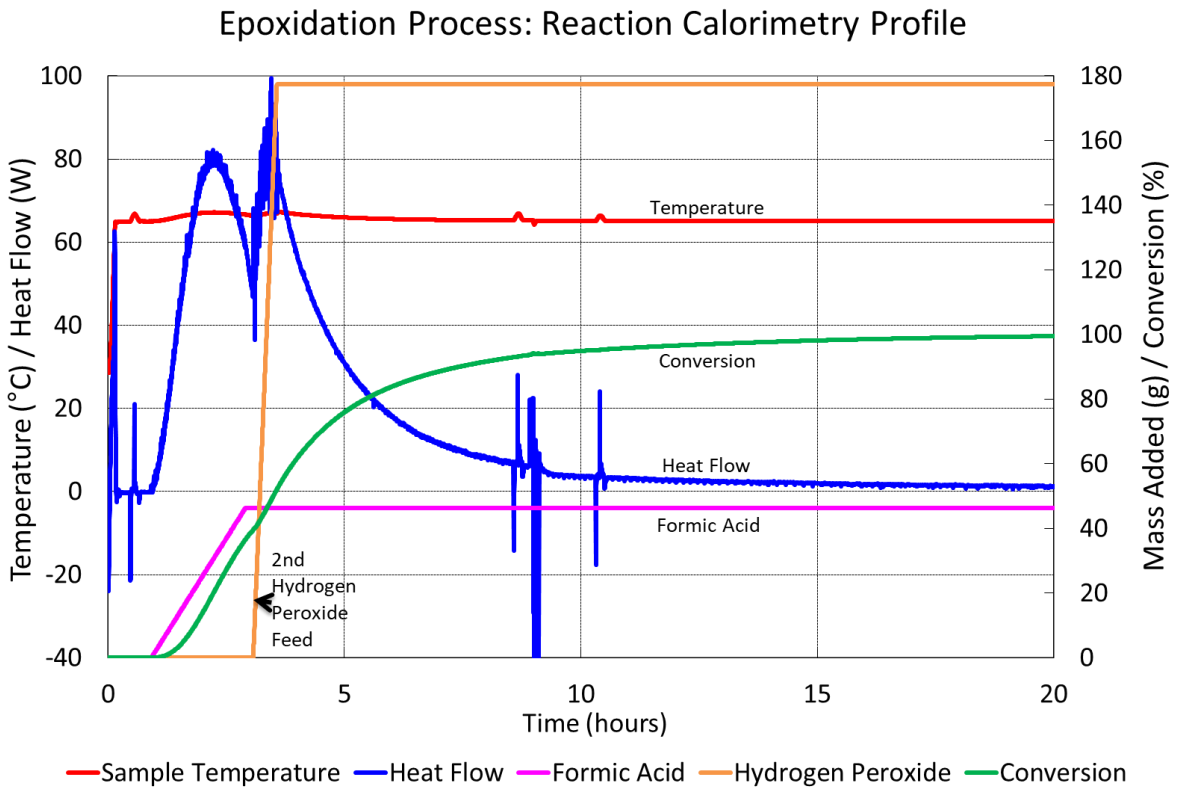

Figure 3. Reaction Calorimetry Profile for the Epoxidation Process under Normal Conditions

The high heat of reaction, resulting in a high calculated potential adiabatic temperature rise, indicates the high hazard potential of the process but the kinetics of the reaction under uncontrolled conditions dictates the time available for any corrective action and the size required for any relief system.

KLP 5: While chemists focus on thermodynamics, engineers focus on kinetics – because kinetics drive vent size, and the prospect of taking any other corrective action. Regulators increasingly seek kinetic data when inspecting multi-product plant to ensure worst case reactions are known. Comparing heats of reaction provides a basis for hazard analysis but not risk assessment.

Thermal Stability

In the case of many industrial runaway reaction incidents, the desired chemical reaction is ultimately not responsible for the incident. Frequently, instability of the mixture causes secondary or side reaction. For this reason, characterisation of runaway reaction risk requires an understanding of both the thermodynamics and kinetics of the desired reaction (with gas generation measurement) AND thermal stability assessment for all stages of the process; thus measures can be taken to prevent limiting safe thresholds from being exceeded. An adiabatic calorimetry test was performed on the epoxidation mixture (after completion of reaction following the second peroxide charge) using an Accelerating Rate Calorimeter (ARC) [ref. Thermal Hazard Technology] . Figure 4 shows the resulting thermogram and indicates initiation of a large and violent secondary reaction from 270°C. When corrected for the thermal mass of the test equipment, this indicates a T_{D24} value of 238°C (T_{D24} is the temperature from which the reaction takes 24 hours from initiation to reach its maximum rate of decomposition. It is often considered to be a “maximum safe handling temperature” or “onset temperature”).

KLP 6: Isothermal calorimetry measurements only tell half the thermal story necessary to understand the safety of a chemical process. Understanding thermal stability is a further essential ingredient in understanding process risk.

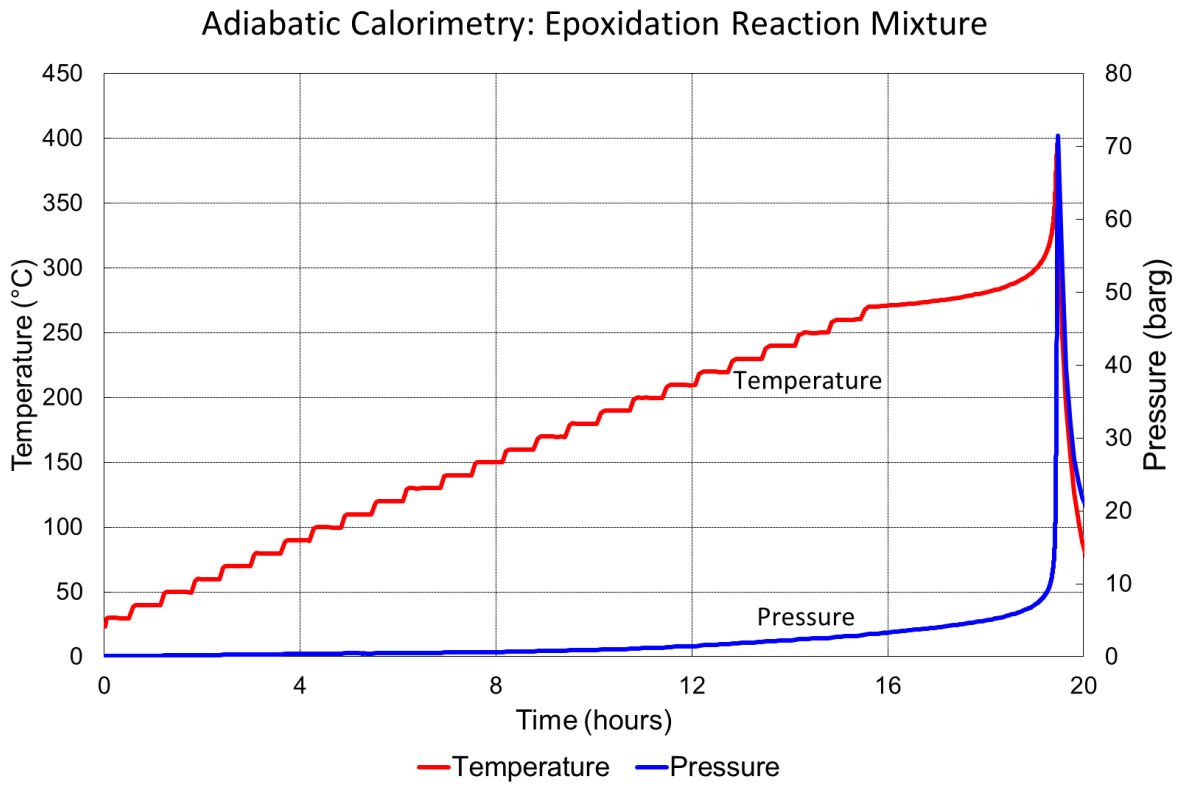

Figure 4. Adiabatic Calorimetry on the Epoxidation Reaction Mixture

Identifying Hazardous Scenarios

As with all elements of the safety assurance process, a reliable and robust PHA is essential in identifying potentially hazardous scenarios requiring prevention or protection. During the structured review of process hazards of the epoxidation process, a number of scenarios were identified where there was a possibility of developing a hazardous consequence. Of these cases, the ones considered of most concern were subject to laboratory investigation to quantify the magnitude of the consequences (using adiabatic calorimetry to directly simulate plant scale heat loss conditions). However, it was clear that there were significant safeguards already in place, so the risk (likelihood) of manifestation of these consequences requires evaluation. Previous work conducted during the site COMAH submission had addressed major releases using Fault Tree Analysis (FTA) and Quantified Risk Analysis (QRA) techniques.

In the current study, Layer of Protection Analysis (LOPA) was employed to study the schedule of specific hazards derived during the process hazards review. Thus the LOPA was a key element in the overall approach of identifying the potential hazards, quantifying the magnitude of the consequences, evaluating the likelihood bearing in mind the integrity of the safeguards, and therefore deciding upon the tolerability of the residual risk. The rigorous and evidence-based nature of the LOPA studies provided confidence in the outcome, limiting assumptions and cognitive bias, by design. The LOPA approach was facilitated by an independent process safety specialist thereby further reducing scope for corporate cognitive bias. The conduct of the LOPA by / with a diverse team (from operators to plant managers) also reinforces the concept that each layer of protection has a finite integrity. All process safety engineers know this, but it is even more critical that plant personnel do - such that their reliance on safeguards is tempered with an understanding of both their importance and their limited reliability.

KLP 7: Hazardous scenarios must be rigorously identified – avoiding assumptions and corporate cognitive bias. The process of performing the LOPA also educates all stakeholders that all safeguards are not equal, with some having a finite (and in some cases very limited) reliability, some having a minor contribution to the overall protection, and others having a high importance.

For the epoxidation process, the credible failure scenarios retained and subjected to LOPA were:

1. Cooling Failure at the End of Peroxide Feed
2. Cooling Failure, Coincident with Hydrogen Peroxide or Formic Acid Overcharge
3. Cooling Failure, Coincident with Low Reaction Temperature
4. Agitator Failure Leading to Reactant Accumulation and inadequate Heat Transfer

5. Late First Peroxide Addition after Formic Acid Charging
6. External Fire Leading to Runaway of Peroxide Decomposition
7. Extended Hold Period with & without Epoxidation Inhibitor
8. High Temperature
9. Early Drop from Reactor and Cooling Failure in receiver

For each potentially hazardous scenario, LOPA sought to:

- quantify the magnitude of the consequences,
- evaluate the likelihood (bearing in mind the provision, integrity and independence of the safeguards), and therefore
- decide upon the tolerability of the residual risk
    - Risk tolerability < 1 onsite fatality every 10^6 years.
    - *Note: Tolerability criteria are chosen by the company and should be at least as good as the HSE guidance.*

Figure 5 indicates the mathematical evaluation of likelihood given the presence of multiple Independent Protection Layers [ref. Gowland].

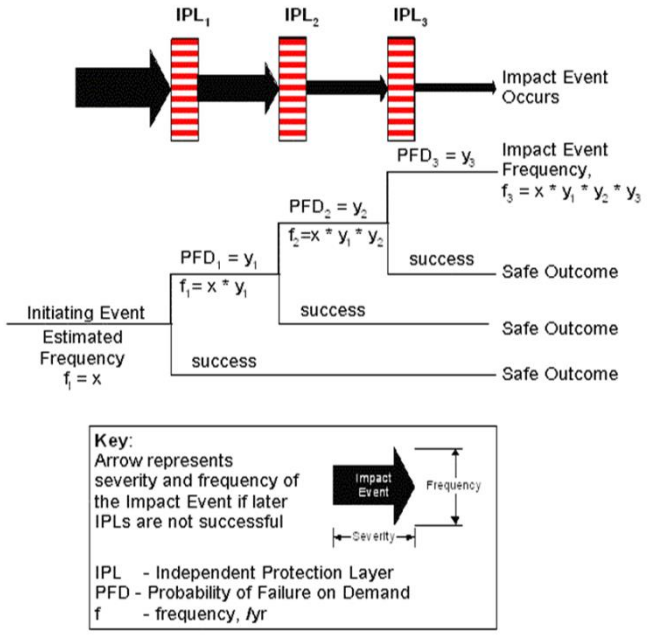

Figure 5. Evaluation of Event Frequency for multiple Independent Protection Layers

Scenario Consequence Evaluation

Risk is the product of likelihood and consequence. Evaluation of consequence should avoid optimistic outcome biases and, as far as possible, be based on quantitative information. While modelling techniques such as PHAST [ref. PHAST] can be used for flammable atmosphere risks, simulation models for runaway reactions are inherently more difficult to construct given the very wide range of physical property and kinetic data required. Adiabatic Calorimetry offers an empirical solution for evaluation of consequence in terms of pressure, temperature and time evolution, with different test protocols designed to simulate each failure scenario of interest. This technique was applied to each of the credible scenarios using the Vent Sizing Package (VSP II) [ref. Fauske] calorimeter. The data from simulation of scenario 1 is illustrated on Figure 6. The very high temperatures and pressures developed by the reaction would be more than capable of rupturing the 22 m3 reactor in the absence of an effective pressure relief system or other mitigation measure. With two operators supervising the process and present in the vicinity of the reactor, it is highly likely that two fatalities would result if the scenario were to occur.

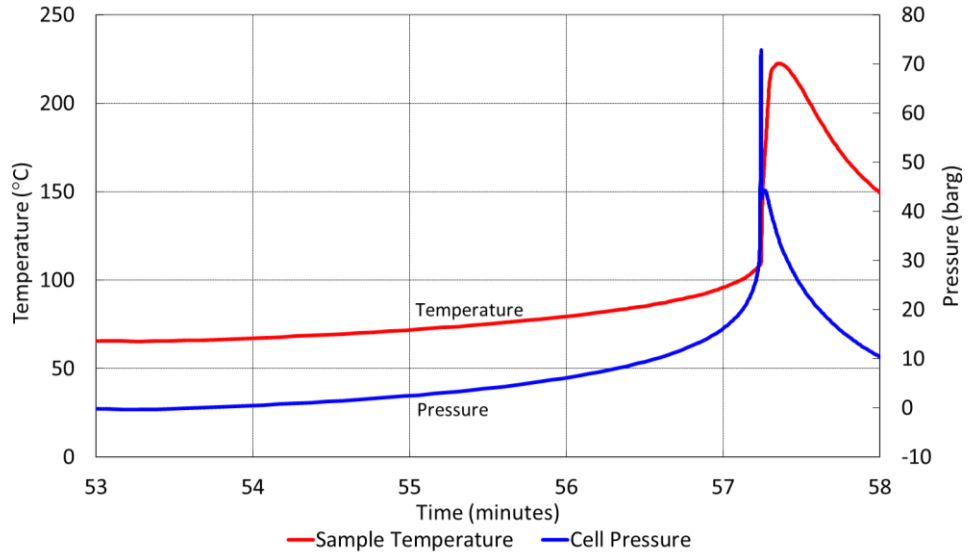

Figure 6. Adiabatic Calorimetry Simulation of Scenario 1 (Cooling Failure at end of Peroxide Feed)

Layers of Protection and Tolerable Risk

For each scenario, the LOPA sought to identify all possible initiating causes (and sum the likelihoods) and then look at the effectiveness (risk reduction factor) for each independent protection layer in use.

Figure 7 illustrates the LOPA summary for Scenario 1.

Runaway Reaction
LOPA of Scenario 1 (Example)

Event Description

Failure of the cooling water supply at a point in the process sequence immediately after the second hydrogen peroxide charge, leading to runaway reaction, vessel over-pressurisation and its rupture, resulting in the fatality of two operators.

Initiating Causes and Likelihood

○ Cooling pump failure	1.3 x 10^{-3} / y
○ Electrical failure	0.1 / y
○ Control failure closes cooling supply	0.1 / y
○ Agitator failure	5.6 x 10^{-2} / y
○ Cooling water pipe rupture	negligible
○ **Total initiation likelihood**	**0.26 / y**

Protection Layers in Place

○ General process design*	2.0 x 10^{-1}
○ SIL compliant quench system	4.5 x 10^{-2}
○ Evacuation in emergency	1.0 x 10^{-1}
○ Adequately sized relief system**	1.0 x 10^{-2}
○ **Mitigated event likelihood**	2.3 x 10^{-6} / y (with relief)

* 1750 batches per year / risk period is 1 h per batch in 8760 h / y (1750 / 8760 = 0.2)

** CCPS "Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis", 2015, offers risk reduction factor of 100 for an adequately sized relief system

Conclusion: Risk is As Low as Reasonably Practicable (ALARP) **if relief system is shown to be effective**. *(NOTE: Risk is the sum of all scenarios, not just this scenario)*

Figure 7. Summary of the LOPA Calculation for Failure Scenario 1

Each initiating cause is evaluated rigorously using evidence wherever possible. For example, the case of cooling pump failure rate has been determined through the following logic:

- Cooling water is supplied by a cooling tower remote from the plant. There are 3 pumps, although 1 pump has sufficient duty for the reactor; 2 pumps are always running with 1 pump on standby via an auto-changeover arrangement. Previous work has judged that the frequency of a pump failure due to mechanical reasons would typically be 1 in 6.7 years; however with the operating protocol, loss of a single pump would not be sufficient to invoke a runaway. As all 3 pumps are cycled on a 3 month basis, there is an effective 3 monthly test period; thus failure of the two running pumps together can be assessed as the failure frequency of one pump (0.15/yr) AND the probability that the second pump will fail (0.5 x 0.15 x 3/12), so an overall failure rate of 0.0028/yr. But complete cooling failure also requires that the auto-changeover to the standby pump will fail, or that that pump has already failed. The probability that a well-designed and maintained control system will fail is limited to 0.1 as a non-SIL system, whilst the probability that the pump will be non-functional is as calculated above (0.5 x 0.15 x 3/12), thus an overall probability that the standby pump is not available is 0.12. Additionally, common cause elements must

be considered and a factor of 5% can be shown to be reasonable for the pumps. Combining these results indicates that the frequency at which all pumps will fail due to mechanical or other individual aspects is 0.0013/yr (1 in 785 years). There is limited site experience against which this value can be compared, but the cooling pumps have been in place for 6 years and no failures have occurred (thus site data for 18 operating years).

The sum of all initiating cause frequencies provides the overall initiation likelihood, thus a similar assessment is required for each of the other causes.

Similarly for safeguards, each (independent) protection layer is evaluated rigorously to determine their probability of failure on demand. Looking at examples from the epoxidation reactor:

- Time at risk.
  - The plant processes 1750 batches per year and the "at risk" period is 2 hour per batch (this is the period when the accumulation is sufficiently high to cause a runaway that could exceed the vessel design pressure). In a full year, the probability of failure occurring while the process is in the "at risk" period is 1750 h (1750 batches x 2 hr at risk per batch) / 8760 h per year = 0.4.
- Evacuation in emergency
  - Standard procedures require evacuation of the production building in the event of an emergency condition (e.g. high temperature alarms and activation of the quench). Such an action would be effective at eliminating fatality, and owing to personnel training the reliability of this action is considered good – a credit of 0.1 is taken.

The plant operates a quench system, triggered by high temperature, as a protection layer. However, adiabatic simulation of the quench (Figure 8) clearly demonstrates that although the quench slows the reaction down, it does not prevent re-acceleration to hazardous conditions.

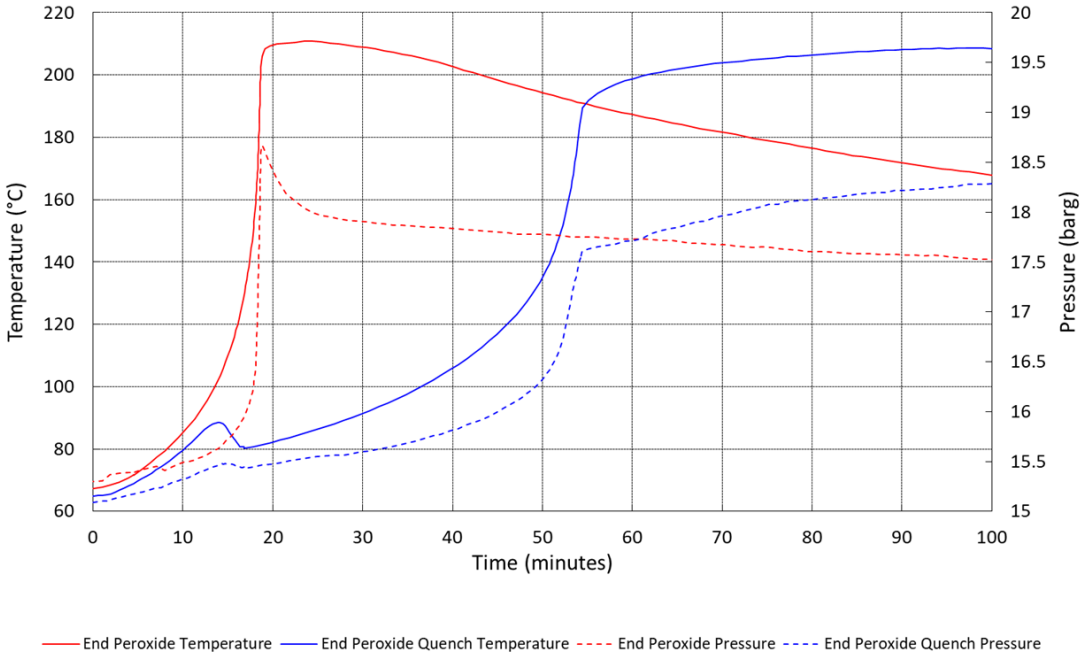

Figure 8. Adiabatic Simulation of a Scenario 1 with and without Emergency Water Quench Injection

Thus, the quench, as a safeguard, is ineffective in arresting a runaway reaction but it does moderate the consequences.

KLP 8: Physical water quench does not stop a reaction. Reaction continues but at lower rate (buys time) and to lower (but possibly still hazardous) peak conditions. Safeguards don't just need to operate, they must be fully effective in removing the hazard.

Cold water quench addition was retained as a safeguard. The quench is initiated automatically by a hardwired high temperature interlock at 90°C (SIL 1) or manually by the operator. Laboratory work (as in Figure 8) has indicated that quench activation in response to a worst case second peroxide addition runaway is not able to eliminate the runaway; but it does delay the consequences by 30 – 40 minutes, although it would be more effective at other stages of the cycle. The delay to the runaway will allow potential corrective action and provide additional time for plant evacuation. The quench activation is SIL compliant; previous FTA work has evaluated the PFD, taking into account potential for an empty quench tank and failure of the hardwired injection system at 0.045.

The relief device is also a safeguard – if adequately sized. For the epoxidation reactor, the existing relief system was initially shown to be inadequate to cope with the severity of most severe runaway reaction. A mechanical engineering review of the reactor subsequently allowed re-rating of the vessel design pressure which, together with changes to the relief system dimensions and routing, enabled the new relief arrangements to be adequate to mitigate a runaway and hence credit to be taken as an independent layer of protection. However, even so, this is also not a safeguard with absolute reliability [ref. CCPS, 2015], and a PFD value must be included. Relying on a relief system alone is therefore unlikely to be effective in meeting residual risk criteria.

KLP 9: Just because the vessel has a vent, does not mean it is adequate

KLP 10: CCPS "Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis", 2015, suggests a risk reduction factor of 100 for an adequately sized relief system.

The mitigated event likelihood is the product of each protection layer PFD. In the case of scenario 1, the mitigated event likelihood is 2.1×10^{-6} / year (with an effective relief system).

This rigorous LOPA approach is applied to each credible scenario and the sum of the individual values is the overall event likelihood, as summarised in Table 1 for the epoxidation reaction [ref. PSLG, 2009].

Number	Scenario	Intermediate Event Likelihood (per year)
1	Cooling Failure at the End of Peroxide Feed	2.1×10^{-6}
2	Cooling Failure, Coincident with Hydrogen Peroxide or Formic Acid Overcharge	1.7×10^{-7}
3	Cooling Failure, Coincident with Low Reaction Temperature	4.7×10^{-8}
4	Agitator Failure Leading to Reactant Accumulation and inadequate Heat Transfer	2.3×10^{-7}
5	Late First Peroxide Addition after Formic Acid Charging	Negligible
6	External Fire Leading to Runaway of Peroxide Decomposition	1.4×10^{-8}
7	Extended Hold Period with & without Epoxidation Inhibitor	-
8	High Temperature	1.7×10^{-9}
1-8 Total	**Total risk level for reactor**	**2.6×10^{-6}**

Table 1. Summary of Event Likelihood for all Credible Scenarios

Relief System Design Considerations

As alluded to previously, the provision of an adequately sized relief system is a reliable safeguard (albeit, not sufficiently reliable alone). However, there are a number of challenges posed by the epoxidation reaction which need to be considered in the relief system design.

- Multi-phase flow – the reaction is rapid in the venting period with a high probability of two-phase flow. DIERS relief system design methods [ref. Etchells, 1998, Fisher, 1992] for two-phase flow must be applied, using the appropriate calculation for the system – tempered, hybrid or non-tempered / gassy).
- Relief containment – numerous large scale runaway incidents highlight that vessels undergoing two-phase flow will be substantially emptied during the relief process. An adequately sized catch / dump tank system should be considered to permit liquid and vapour / gas separation and minimise the environmental release of the liquid portion, with the need for further treatment of the vent stream being determined by the nature of the released material. The siting of such a potentially large vessel requires consideration early in the design process since locating it in an existing plant or a fixed new design can pose problems relating to line routing.
- Mechanical Forces – for a rapid release of two-phase material through a large diameter vent, the thrust forces exerted by the flow can be substantial. The relief system must therefore be adequately designed and supported to resist deformation by the high velocity / high density flow. In the present case, the design of the vent routing was influenced by the strength limitation of the building structure to resist these forces.

KLP 11: Designing a relief system is way more complicated than just sizing a hole correctly!

Summary of Key Learning Points

1. "We've been running this process for XX years and never had an incident, why do we need to study it now?" is not a valid basis of safety.
2. Regulators are increasingly knowledgeable in process safety – operating companies must be confident that their process safety studies are able to withstand detailed scrutiny – either through provision of internal competence or using external specialists
3. A safe system of work is required to protect against all foreseeable risks
4. A systematic assessment process should be engrained in the process development and process operation life-cycle. Process safety must be considered from the start of the development journey, and for retrospective process assessments, missing characterisation data should be backfilled to provide a full understanding of behaviour during process deviations.
5. Kinetics drive vent size and/or the time required to complete other protection measures (heats of reaction alone are not enough).
6. Isothermal calorimetry AND thermal stability are needed to understand overall thermal risk.
7. Hazardous scenarios must be rigorously identified – avoiding assumptions and cognitive bias; and the value, limitations and integrity of safeguards must be fully understood
8. Physical quenching does not stop reactions – but it does slow them down. Safeguards don't just need to operate, they must be fully effective in removing the hazard.
9. Just because the vessel has a vent, does not mean it is adequate!
10. Typically, an adequately sized relief system represents a risk reduction factor of only 100.
11. Designing a relief system is way more complicated than just sizing a hole correctly!

Conclusions and Final Thoughts

A simple request by a regulating authority to demonstrate that the basis of safety for an established process with nearly 50 years of operating experience, revealed a need for an extensive investigation into many aspects of its chemistry, engineering and operation. A structured in-depth programme of study was necessary to gather sufficient evidence to satisfy all concerned that the process was safe to continue production.

The epoxidation process was known to be potentially hazardous from the perspective of being able to form detonable mixtures and consequently considerable work had previously been undertaken to ensure this risk was practically eliminated. Whilst the earlier work was thorough, this was not the only hazard inherent in the process and other severe risks had not been recognised and therefore received considerably less scrutiny. To ensure a valid basis of safety, all potential hazards from all potential failure scenarios, need to be mastered and a company must not be lulled into believing that by eliminating the highest profile issue, any other hazards would most likely be tolerated. In fact, a sound assessment routine requires that all issues are sought and addressed and often this will need an iterative approach, reducing the residual risk of the highest potential hazard before moving on to each of the others in turn, tackling consequence, magnitude, and likelihood of occurrence progressively. Individual assessment of each hazard is a key part of this process, fully questioning the engineering and integrity of all proposed safeguards and plant operations. As this case study demonstrates, to achieve an acceptably low residual risk in the case of a severe runaway reaction, it will probably be necessary to utilise a variety of measures, including a correctly designed and engineered emergency pressure relief vent system, SIL rated instrumentation for critical interlocks, robust and tested operating procedures to handle emergencies; all applied to a process whose safe operating envelope has been rigorously defined with extensive study. Therefore the creation of a satisfactory basis of safety for this process required the close collaboration of plant and laboratory chemists, safety specialists, process, mechanical, and instrumentation engineers, and operations personnel, making use of robust experimental data and conducting detailed calculations – a highly qualified and dedicated team.

Acknowledgements

The operating company who have granted permission for this paper to be published are thanked for enabling others to learn from their experience.

References

CCPS, 2015, "Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis", ISBN 978-0-470-34385-2

Etchells, J. & Wilday, J., 1998, "Workbook for Chemical Reactor Relief System Sizing", Contract Research Report 136/1998, HSE Books, 0 7176 1389 5

Fauske & Associates, VSP2, (https://www.fauske.com/chemical-industrial/adiabatic-calorimetry-relief-system-design)

Fisher, H.G. et al, 1992, “Emergency Relief System Design using DIERS Technology – The Design Institute for Emergency Relief Systems DIERS) Project Manual”, AIChE, ISBN 0-8169-0568-1

Gowland, R., “How Layer of Protection Analysis practice in UK is affected after the guidance drawn up after the Buncefield accident”, European Process Safety Centre

Mettler Toledo, “RC1 Reaction Calorimeter”, (https://www.mt.com/au/en/home/products/L1_AutochemProducts/Reaction-Calorimeters-RC1-HFCal/RC1mx-Reaction-Calorimeter.html)

PHAST, DNV GL AS. Phast 8.1, (https://www.dnvgl.com/services/process-hazard-analysis-software-phast-1675)

Process and HSE Engineering- A Professional Blog for HSE, Process and Safety Engineer, “LOPA – Layer of Protection Analysis”, Wordpress.com, (https://hseengineer.wordpress.com/lopa-layer-of-protection-analysis/)

Process Safety Leadership Group (PSLG), 2009, “Safety and environmental standards for fuel storage sites – Appendix 2: Guidance on the application of layer of protection analysis (LOPA) to the overflow of an atmospheric tank”, HSE Books ISBN 978 0 7176 6386 6

Thermal Hazard Technology, “Accelerating Rate Calorimeter”, (http://www.thermalhazardtechnology.com/products/accelerating+rate+calorimeter)