BEYOND LOPA: SAFETY INTEGRITY ASSESSMENT IN THE PHARMACEUTICAL SECTOR†

Alan G King, Hazard & Reliability Specialist, ABB Consulting, Billingham, Cleveland UK
David Hodgson, HSE Director, Shasun Pharma Solutions, Dudley, Cramlington, Northumberland, UK

This joint paper between Shasun Pharma Solutions and ABB outlines some of the challenges associated with hazardous batch process safety assessment and the benefits from carrying out a systematic study. Historically, Layer of Protection Analysis (LOPA) had been tried, but was found to be inadequate for the situation.

Shasun Pharma Solutions had relocated an exothermic batch reactor process to its site near Cramlington, Northumberland. In the relocation, a number of changes and improvements had been made to the process, so that the arrangements were not identical to those in the previous operating location. Therefore previous safety assessments were no longer applicable to the project. Dudley Northumberland is top tier COMAH site and Shasun had a legal obligation to ensure that the safeguards proposed reduced the individual risk of operating the new process to ALARP whilst also complying with the site's overall risk criteria.

In doing so, Layer of Protection Analysis was tried but the challenges presented by the process led to the rejection of this method by the company and a lack of confidence in the results by the regulator. The alternative approach as described in this paper, builds on some of the guidance from the post-Buncefield PSLG report, applies it to the batch processing pharmaceuticals sector, and couples it with a more flexible assessment technique.

This paper highlights the benefits of the approach used, and more importantly that it is applicable to all parts of the process sector, not just pharmaceuticals.

KEYWORDS: IEC 61511, IEC 61508, Functional Safety, Risk Reduction, Layer of Protection Analysis, LOPA, Pharmaceutical Sector, Hazard Analysis, Fault Tree Analysis (FTA)

BACKGROUND

Shasun Pharma Solutions are a custom service provider to the global pharmaceutical industry. Their site in the UK at Dudley, Northumberland provides specialist services in process development small scale manufacture for clinical trials, and full scale commercial manufacture of advanced intermediates and active pharmaceutical ingredients. It is a Top Tier COMAH[1] site and has a wide range of facilities. Its reactive chemistry capability includes Fluorination, Hydroxylamine handling, Organometallic, Friedel Craft and Carbonylation reactions. In addition, they have capability for handling bulk bromine, chlorine, hydrogen, ethylene oxide, and propylene oxide.

In 2009, the company site at Annan in Dumfriesshire was closed and a number of the processes were transferred to the Dudley site. One of these was a complex exothermic reactive process for a manufacture of a high value pharmaceutical intermediate. In the relocation, a number of changes and improvements were made to the process, so that the new arrangements were not identical to those in the previous operating location.

PROCESS OVERVIEW

The process forming the case study is a batch process. It has essentially three stages to it: (1) Batch make-up, (2) Reaction with catalyst addition and (3) Post reaction processing. During all three of these stages the process has a potential for exothermic reaction runaway and so control of temperature is very important.

The reactor vessel is a typical jacketed vessel with a motor driven agitator. An overview is shown in Figure 1. It has been simplified: not all sensors, valves or other features have been shown for clarity.

Figure 1 shows the reactor vessel together with the supporting heating and cooling arrangements. These allow the control of reactor temperature throughout the process. It will be noted that there are essentially four circulating flow loops (1) Primary Loop through the reactor jacket and Heat Exchanger EX1, (2) Secondary Loop between Heat Exchanger EX1 and Heat Exchanger EX2, (3) Tertiary Loop between Heat Exchanger EX2 and Heat Exchanger EX3, and (4) the steam flow input to Heat Exchanger EX3. The various control valves allow control of flow rates and temperatures in these loops.

The direct injection of cooling water to the reactor jacket is for temperature adjustment. The fire water injection provides emergency cooling as a protective measure. There

[1]COMAH = Control of Major Accident Hazards.

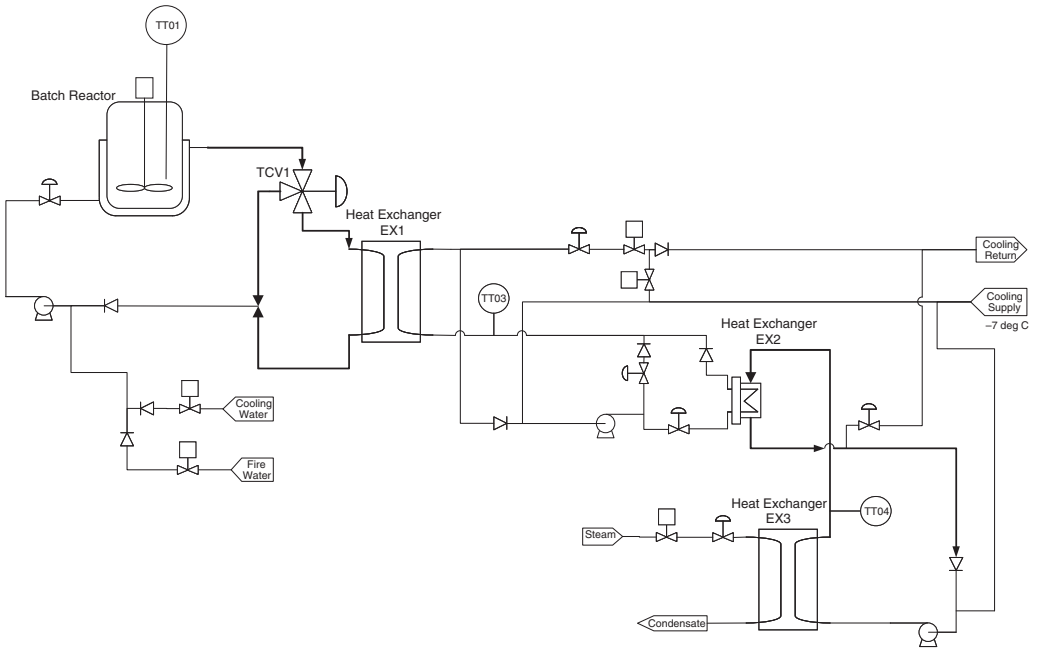

Figure 1. Simplified Process Overview

is also the feature to dump the contents of the reactor through the reactor bottom outlet (not shown in Figure 1) to a quench tank in the event of a reaction runaway.

During processing, the temperature of each of the circulating loops is controlled in order to provide the appropriate heating or cooling to the reactor. The overall arrangement installed at the Dudley site is different from the previous one at Annan, and so Shasun wanted a reassessment of the functional safety requirements for the process.

FUNCTIONAL SAFETY REQUIREMENTS

The international standards IEC 61508 [1] and IEC 61511 [2][2], together with the other sector standards that have been generated from IEC 61508, are seen today as representing current good practice in the management of functional instrumented protective measures across industry. Shasun, together with many other organisations in the global process industry sector, see the adoption of the principles within these standards as the way of demonstrating, to regulators and others, that appropriate risk management is in place.

These standards cover the whole of the safety lifecycle – from the initial concept through to operation and maintenance. Within the requirements in the early stages of the lifecycle, relating to Hazard and Risk Analysis, there is the need to review the hazardous event scenarios and to determine whether sufficient risk reduction has been put in place. This includes reviewing each scenario and determining an appropriate target performance for each safety instrumented function – most usually related to its probability of failure on demand – and described by a safety integrity level (SIL)[3]. This is the target performance needed for demonstration of effective management of risk.

The process of setting an appropriate target performance for a safety-instrumented function is commonly referred to as "SIL Determination". Methods for SIL Determination are illustrated by examples in Part 5 of IEC 61508 and Part 3 of IEC 61511. There are a variety of methods for SIL Determination illustrated in the standards; one of these methods is Layer of Protection Analysis (LOPA)[4].

LAYER OF PROTECTION ANALYSIS

Layer of Protection Analysis has been around for many years, and over the past 5 or so years, it has become what might be seen as the industry "Method of Choice" for SIL Determination. It was this method that was first used for the assessment of the necessary risk reduction for this batch reactor process. Shasun employed an independent chairman to lead the assessment sessions. However, in reviewing the Layer of Protection Analysis results Shasun realised that the challenges presented by the process were too complex for this approach to be effective and another approach was required. This decision was supported by the regulator.

Layer of Protection Analysis can be a highly effective SIL Determination tool for simple scenarios as illustrated in Figure 2.

[2]IEC 61511 is the Process Sector standard derived from the generic standard IEC 61508 on instrumented Functional Safety.

[3]There are four safety integrity levels defined in the standards IEC 61508 and IEC 61511. SIL 1 is the lowest performance level and SIL 4 the highest.

[4]See Reference [4].

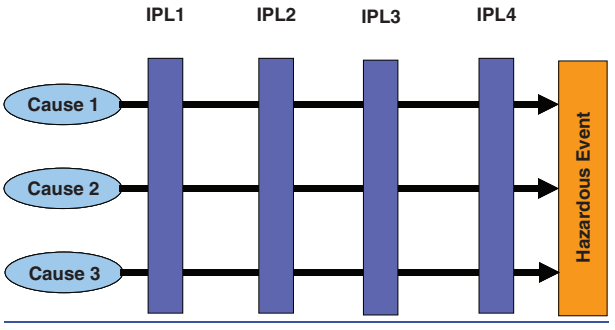

Figure 2. Illustration of Simple Scenario

In this type of simple scenario, Layer of Protection Analysis assumes that each initiating cause has been identified and that all the protection layers (IPLs) are effective protection measures for any of the initiating causes. It also assumes that there is complete independence between each of the protection layers. However, when the situation is more complex such as that illustrated in Figure 3 where some of the protection layers apply only to some of the initiating causes, it represents much more of a challenge for the analysis team and the person chairing the team.

This type of situation also brings into question whether Layer of Protection Analysis is the appropriate method to choose, especially if some of the "independent" protection layers are not fully independent and actually share equipment. Layer of Protection Analysis is generally seen as a very easy and straightforward method, at least in terms of its concepts. As a result, it has often invited its use in situations where the complexity is beyond what it can easily handle and where those using it cannot see its limitations.

In the analysis of the batch reaction system described above, the level of complexity was not fully appreciated and Layer of Protection Analysis was used. The analysis did not explore the separate phases of the batch process and the initiating cause failures associated with each phase. Whilst there was some consideration of what protective measures applied to which causes, the Layer of Protection Analysis did not fully appreciate the nature of the design and made assumptions about independence that were not actually valid. The most blatant of these related to two instrumented protection layers claimed in the Layer of Protection Analysis. Each of these layers in the Layer of Protection Analysis was assigned a failure probability of 0.002 which is towards the better end of the SIL 2 range. Overall, the combination of these two instrumented layers was being assumed to provide a failure probability of 4×10^{-6}, better even than the best performance provided by SIL 4[5].

On closer inspection, it was clear that whilst these two "layers" had different valves as the final elements, they actually shared the same logic solver and also shared the same set of temperature sensors – hardly justification for claiming independence or even indeed that there were two layers and certainly nothing to justify the level of performance claimed in the Layer of Protection Analysis.

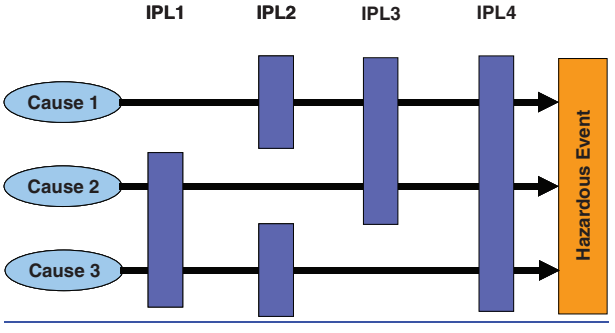

Figure 3. Illustration of a More Complex Scenario

HAZARD ANALYSIS

Shasun therefore decided to seek a hazard analysis approach for assessing the risk reduction requirements on this process. Hazard analysis had previously been used for the process at the Annan site and they now wanted to use a similar approach for the Dudley installation.

Hazard Analysis (see Reference [3]) has been around for a large number years, since the 1970s (see Reference [6]), and has proved its capability to tackle complex scenarios. The key stages are (1) reviewing the hazardous event scenario to be clear about the undesired consequence, (2) using a demand tree as a systematic means of identifying all the relevant initiating causes, and (3) creating an individual fault tree for each initiating cause, (4) linking all the individual fault trees together to describe the overall scenario, and (5) quantifying the fault tree to determine the frequency of the hazardous event. In doing this, initial assumptions will be made regarding the target performance of the various safety instrumented functions involved in the overall scenario as risk reduction measures. The assumptions are then revised depending on the frequency for the hazardous event and how that compares with the company criteria for the severity of the event in question.

DEVELOPING DEMAND TREES

The use of demand trees as a systematic means of identifying initiating causes has been around for many years, but has not been particularly widely appreciated. However, in recent years following the Buncefield Incident in 2005, the PSLG[6] Final Report[7] describes in Annex 3: "Demand tree methodology for systematic identification of initiating causes". It is this methodology that has been used for the analysis described in this paper.

The diagram in Figure 4 shows the overall demand tree; this was the initial split for the analysis. Each of the

[5]SIL 4 has a PFDavg range:$<1 \times 10^{-4}$ to 1×10^{-5}.
[6]PSLG = Process Safety Leadership Group.
[7]See Reference [7].

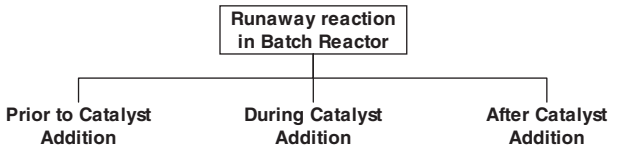

Figure 4. Overall Demand Tree

phases identified as having potential for a runaway reaction were then assessed further.

Further analysis of the three phases generated three additional demand trees. Figure 5 shows the detailed demand tree for the "During Catalyst Addition Phase". This shows the process features that were identified by the assessment team as capable of leading to a runaway reaction during this phase of the process. One of the key aspects to be recognised when generating a demand tree is that all protective or other risk reduction measures are ignored. This means that the demand tree has a focus solely on the failures that can trigger the hazardous event occurring. This has the benefit of simplifying the thinking process and allowing those involved to set aside the distraction of risk reduction features, knowing that those features will be included in the analysis in a systematic manner at the next stage.

It should be noted that for this paper the actual equipment item tag numbers have been removed from the diagram in Figure 5; the inclusion of tag numbers is vital for identification of pumps, control loops, vessels etc. This is both for clarity at the time of conducting the analysis and for later reference.

INDIVIDUAL FAULT TREES

For each initiating causal failure identified by the analysis team, an individual fault tree was developed to show the protective measures that would have to be in a failed state to allow that initiating causal failure to generate a runaway reaction.

There are two important features to note in Figure 6. The first is that the initiating cause is described by frequency, as is the output of the last "AND" gate. By contrast, the measures that contribute to risk reduction are described by probability. In Figure 6, the frequency lines are green and the probability lines are a dashed line in yellow. The second feature to note is that the inclusion of the probability that 'Probability that batch is in preparation or catalyst addition is in progress' is only valid if, as in this case, the temperature control is checked to be working properly prior to the beginning of each batch.

SAFETY INSTRUMENTED FUNCTIONS

When creating such an individual fault tree, it is important to define clearly the safety instrumented function that is being included in the analysis. In this case, the safety instrumented function has been designated Function "(B)" in the analysis. The details of the function are best described by a small sketch, as in Figure 7. This will help anyone designing the function or verifying that it has the necessary performance.

One of the really significant benefits of this approach is that each specific safety instrumented function or function variation can be included. One of the problems with the Layer of Protection Analysis was that this particular function was considered as two functions protecting against this initiating cause: (a) one operating the firewater valve and (b) one

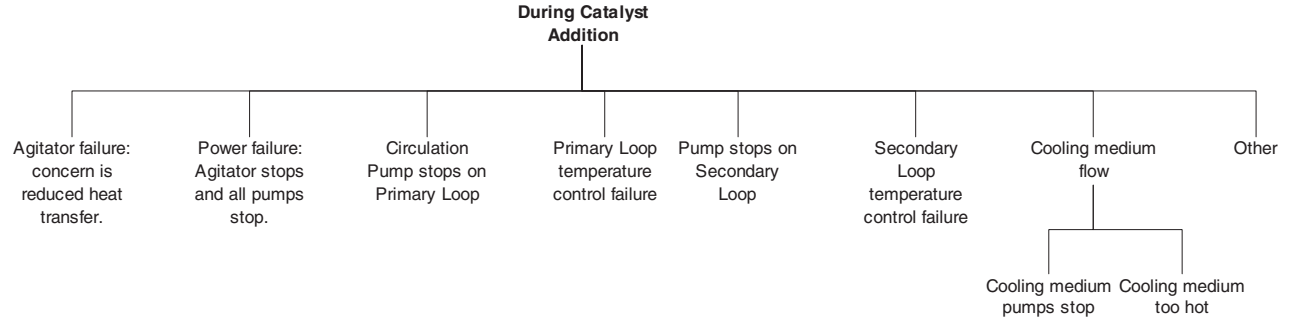

Figure 5. Demand Tree for During Catalyst Addition

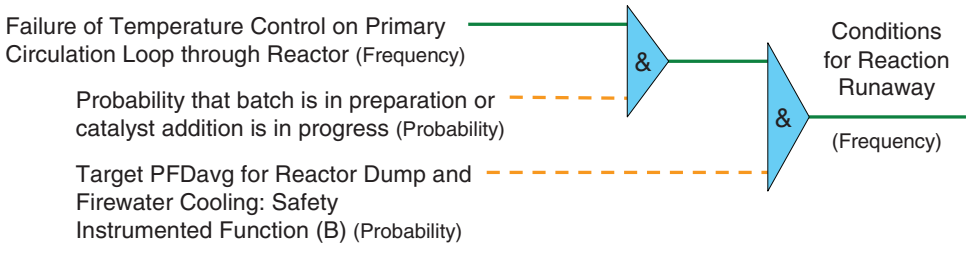

Figure 6. Individual Fault Tree

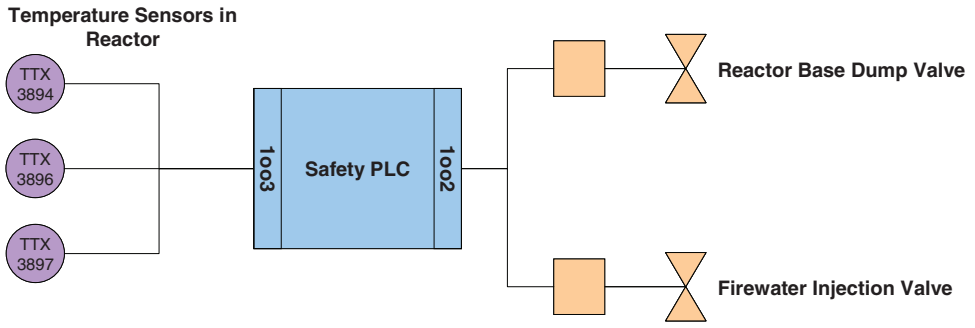

Figure 7. Safety Instrumented Function (B)

operating the dump valve. The analysis erroneously overlooked or ignored the problem that the two functions used the same set of temperature sensors. Indeed the LOPA actually claimed a performance of SIL 2 for each of these "functions" and was therefore claiming an overall performance equivalent to the SIL 4 range for the two together.

For some of the other initiating causes, where the firewater injection would not be sufficient to prevent runaway from occurring, the safety instrumented function only has one output channel available. This is shown in Figure 8.

The instrumented protection design also featured some hardwired relay based logic protecting against overtemperature from the steam heating. It monitors the temperature of the tertiary loop circulation and if that rises above the set point, it closes a block valve in the steam feed line.

Thus, each complete safety instrumented function is included as and where it is appropriate. It is really clear for the person reviewing the analysis exactly what functionality is being used for what part of the analysis for risk reduction.

REACTOR BASE VALVE

It was also clear that the reactor base valve played a key role in the instrumented protection. Due to the batch nature of the process, the correct operation of this valve could be tested before each batch. However, it was also realised that it would be used at the end of each batch to discharge the product and so it would be on average one day from when the valve was last shown to be working properly. Thus, the probability of this valve not functioning, when needed as part of an instrumented safety function, would be very small indeed. The PFDavg for the whole of safety instrumented function (A) would meet the requirements for the best performance end of the SIL 2 range.

However, this single valve would have what is termed a Hardware Fault Tolerance (HFT) of Zero – any failure of the valve to operate would prevent the function from operating. This means that it would not initially meet the requirements of IEC 61511-1 for final elements which looks for a hardware fault tolerance of 1 for SIL 2 operation. IEC 61511-1 does however permit the reduction of the hardware fault tolerance requirement for SIL 2 from 1 down to 0, if the requirements in the standard for what is called "Prior Use" can be demonstrated. Shasun have a substantial number of reactors and reactor base valves with years of operating experience. This allowed such a demonstration to be put together and support the use of the single reactor base valve for the SIL 2 safety function.

OUTCOME

Overall, each of the individual fault trees – one for each initiating cause – together with the appropriate risk reduction measures feeding into the triangular "AND" gates (as in Figure 6) are then combined by linking their outputs with a large rectangular shaped "OR" gate to the right. By doing this, it is possible to see which of the contributions are contributing most to the overall frequency of the hazardous event and to make decisions as to whether there is a need to consider additional risk reduction and also where

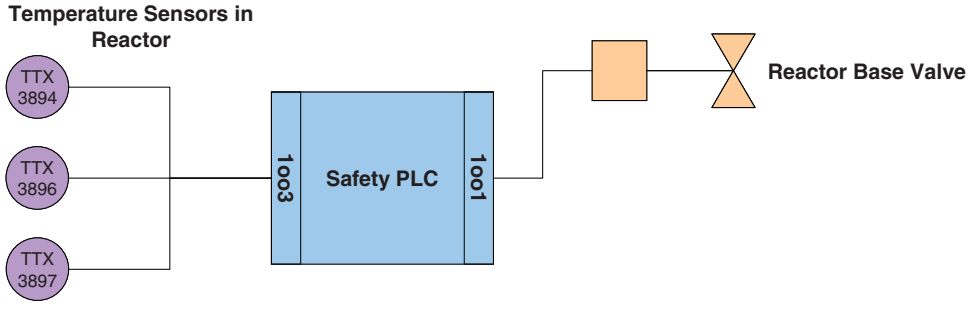

Figure 8. Safety Instrumented Function (A)

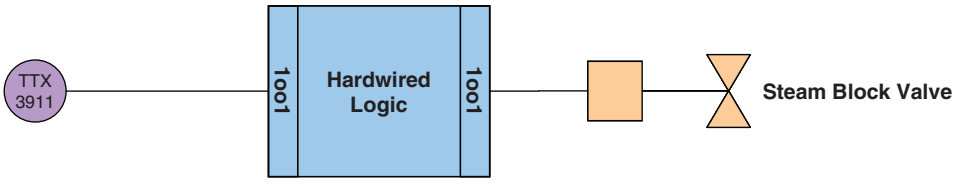

Figure 9. Safety Instrumented Function (C)

to target it to achieve the most risk reduction overall – see Figure 10. Note: the purpose of Figure 10 is to show the overall shape of the fault tree; it has been deliberately softened to obscure anything that might be considered commercially sensitive detail.

The fault tree also allowed the assessment of risk of fatality to the most exposed individual. In this case study, the analysis used a hypothetical person who was defined as a process operator solely engaged with the process being considered. This allowed comparison with published guidance on risk and the risk criteria used by Shasun.

BENEFITS

The type of fault tree described above provides the capability for SIL Assessment and the incorporation of a number of different Safety Instrumented Functions that contribute to the risk reduction for a specific scenario. As such it is far more flexible than Layer of Protection Analysis. It also benefits from providing a highly pictorial representation of the overall situation and how the risk reduction is being applied. This has been commented on by regulatory authorities as providing a very clear demonstration of the scenario and how the risks associated with it are being managed. Indeed, the legal responsibility under the COMAH regulations is for a demonstration of risk management, to show how it is being achieved.

Clear indication of the key contributors to the overall level of risk is important when deciding on the procedures that need to be put in place and the aspects that those procedures need to cover. This will include the testing requirements for the safety instrumented functions – what to test and when to test.

CONCLUSIONS

Whilst LOPA has its place as a SIL Determination method, it is important to be able to recognise when the situation faced is more complex, and a different approach should be selected. This paper has highlighted the principles behind the hazard analysis approach used in this case study, and indicates the benefits that result from it. Hazard Analysis using demand trees and fault trees has a long history of use in the process industry and is a well recognised and accepted means of

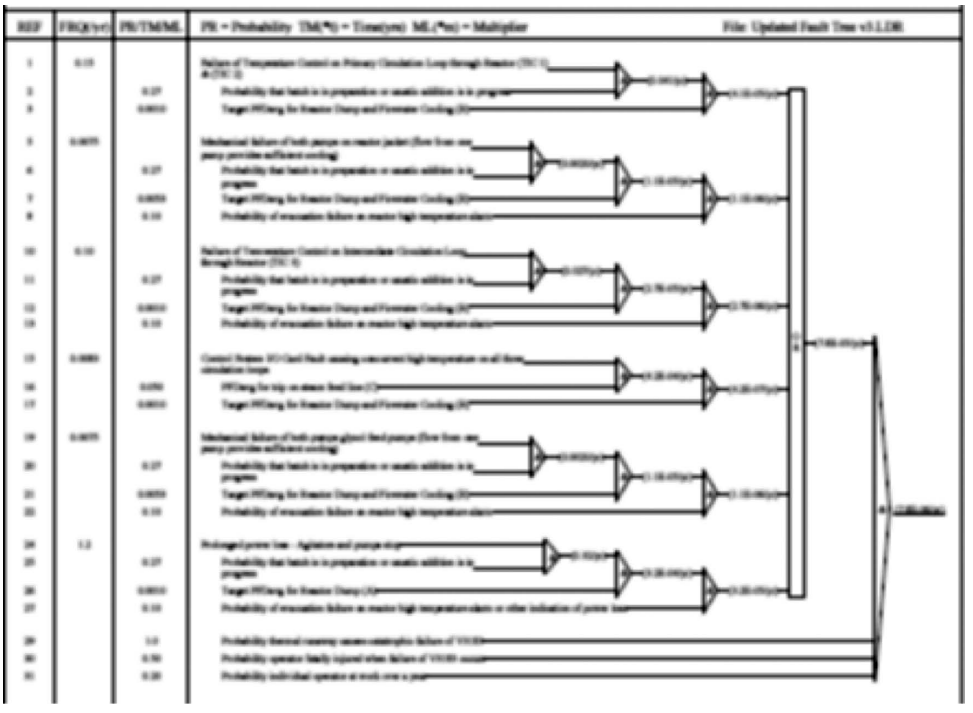

Figure 10. Overall Fault Tree

assessing the overall hazardous event frequency. Hazard Analysis offers significantly more flexibility compared with Layer of Protection Analysis and helps the competent analyst to avoid some of the pitfalls that are common with LOPA. It allows the demonstration of the risk reduction achieved with the various safety instrumented functions and should additional risk reduction be required, it allows the cost effective targeting of any additional measures.

REFERENCES

1. IEC 61508: "Functional safety of electrical/electronic/ programmable electronic safety-related systems", International Electrotechnical Commission, Geneva, Edition 1, 1998 & 2000, also Edition 2, 2010.
2. IEC 61511: "Functional safety – Safety instrumented systems for the process industry sector", International Electrotechnical Commission, Geneva, 2003.
3. "HAZOP and HAZAN", Trevor Kletz, Institution of Chemical Engineers; 4th Edition, 2006.
4. "Layer of Protection Analysis – Simplified Process Risk Assessment", CCPS 2001.
5. "Guidelines for Chemical Process Quantitative Risk Analysis" Second Edition CCPS 2000.
6. "Thirty Years of Quantifying Hazards", J T Illidge, M L Preston, A G King, IChemE Hazards XIV Symposium, Manchester, 1998.
7. "Safety and environmental standards for fuel storage sites", Process Safety Leadership Group, Final report, HSE, 2009. ISBN 9780717663866.