PRACTICAL PROCESS SAFETY MANAGEMENT IN CHEMICAL MANUFACTURING

Andrew H K Fowler[1,*], Ian Walker[2] and Richard Wall[3]
[1]HFL Risk Services Ltd, Denton, Manchester, M34 3SU
[2,3]Nufarm Ltd, Wyke, Bradford, BD12 9EJ
* Corresponding author

Process safety management (PSM) has been highlighted as a factor in recent major incidents, notably, BP Texas City and Buncefield. PSM requires an organisation to consistently perform in the following areas: defining acceptable operating envelopes for all critical components of a process; maintaining the process conditions within these envelopes; understanding the impact of excursions; maintaining and testing equipment and preventative and protective devices; rigorous compliance with procedures; and professional management of change processes. Essentially PSM is ensuring the reality of plant operations and maintenance is the same as the design intent throughout the life cycle of the process. Preventative actions have an ongoing impact on system performance. The efficacy of the measures may have been determined during the design phase (the 'intent'), but the ongoing maintenance and operation of these measures (to ensure their effectiveness) need also to be of sufficient integrity (the 'reality') at all times.

Nufarm at Wyke operate a Basis of Safety approach, which builds on Process Hazard Reviews, Chemical Reaction Hazard Assessments and other Hazard Identification techniques, and essentially identifies those items (instruments, operations etc.) that are critical to ensure the reactor systems remain within the safe operating envelope at all times.

This paper illustrates the approach by considering systematically two of the main safety instrumented systems used on typical reactor systems – temperature and flow, and provides options for reducing potential errors in both maintenance and operations. The output of the approach will be described including how the results have been incorporated into the training of operators and maintenance staff; and in the written operating procedures and written maintenance, testing and inspection procedures used on site.

INTRODUCTION

Process safety management has been highlighted as a factor in recent major incidents, notably, BP Texas City (BP, 2005) and Buncefield (MAIB, 2008). Process safety management requires an organisation to consistently perform in the following areas:

- Defining acceptable operating envelopes for all critical components of the process.
- Maintaining the process conditions within these envelopes.
- Understanding the impact of excursions.
- Maintaining and testing equipment and preventative and protective devices.
- Rigorous compliance to procedures.
- Professional management of change processes.

The application of the principles of good process safety management is essentially to apply the management practices to ensure that all processes are controlled and managed at all times. It is therefore focussed on safety critical elements only.

Essentially it is making the reality of plant operations and maintenance the same as the design intent all of the time. It is getting it right first time and ensuring that it is always right. Preventative actions have an ongoing impact on system performance. The efficacy of measures may have been determined during the design and build stages (the 'intent'), but the ongoing maintenance and operation of these measures (to ensure their effectiveness) need also to be of sufficient integrity (the 'reality') at all times.

There are some key stages to this approach which are:

- Identify the safety critical elements – these may be hardware or software (instrument trips, operating instructions etc.).
- Make the critical elements special – make them recognisable as critical – so it is clear and unambiguous that a particular piece of plant/equipment, or a particular operation is critical to safety.
- Communicate to all relevant personnel why the safety critical elements are special – requiring adherence to specific procedures etc. – why the job must be done right every time.

METHODOLOGY USED AT NUFARM, WYKE

Nufarm Ltd at the Wyke site in Bradford have developed a suite of Basis of Safety procedures including the Engineering Basis of Safety; Control Engineering Basis of Safety; Mechanical Basis of Safety; and Operations Basis of Safety. These bases of safety build upon the current Process Hazard Reviews, Chemical Reaction Hazard Assessments and Hazard Identification procedures, which of course, require the reaction systems to be designed and installed to good practice guidance as a minimum.

The Basis of Safety approach adopted uses essentially fault tree analysis but in a simplified way using descriptors rather than numerical values for likelihood, because the primary aim of the approach is as a communication tool; allowing operating and maintenance personnel to understand the efficacy of risk reduction measures installed on reactor systems, rather than for use by risk practitioners. Hence the output of the approach is incorporated in the training of operators and maintenance staff; and in the written operating procedures and written maintenance, testing and inspection procedures.

However the site at Wyke is a top tier COMAH[3] site, so the approach developed has been implicitly linked to the Nufarm risk matrix which is calibrated to published HSE criteria as justification that the approach adopted is fit for purpose.

The Basis of Safety approach is only adopted on site for certain processes where the consequences of the event have been considered, under worst case conditions, to result in either Fatal or Critical consequences. The definitions of these consequences are identical to those used in the Nufarm risk matrix, namely:

- Fatal – 1–5 deaths on site; many injuries; off-site injuries; airbourne hazards, on and off site resulting in injuries; toxic liquid released off site.
- Critical – Major accident/occurrence as defined by COMAH or RIDDOR; few people requiring hospital treatment off site; release that would require notification to EA; toxic gas alarm activated; COMAH siren activated.

Events with consequences more severe than these definitions require a full quantified risk analysis and assessment to be undertaken. Similarly, for those events with consequences that are less than Critical, proportionality would suggest only a qualitative assessment is required. The methodology therefore used is semi-quantitative in its intent, but because of how it is used within the site, numerical values are not presented, but transposed into descriptors.

Unlike the more traditional fault tree analysis, where frequencies/probabilities are assigned to each fault condition or sub-tree, with Boolean algebra being used to determine the frequency of the top event; the Nufarm approach again uses Boolean algebra but aims to reduce the top event to a value of Implausible (10^{-5} per year or less) or Most improbable (10^{-4} to 10^{-5} per year). So in effect, the event is considered a certainty without any measures, and the risk reduction installed reduces the likelihood by 4–5 orders of magnitude.

This is very similar to Layers of Protection Analysis (AIChemE, 1993) (LOPA) where the target risk figure is chosen against a specific consequence. As for LOPA only independent measures are considered. The ranges of values assigned to the measures have been cross-checked against recognised sources of failure and reliability information, and are used by leaders of the study in the analysis.

The benefits of this approach include:

- Easily understood by operating and maintenance personnel.
- Indicates the extent to risk reduction by each individual measure and hence allows sensitivity to the outcome to be determined easily.
- Order of magnitude approach allows avoidance of determination of reliable generic failure data – although checks are in place to ensure values used are appropriate.
- Allows the focus on the risk reduction measures rather than a number.
- System only considers layers of prevention. Reduction of risk by mitigation measures and/or other conditional modifiers does not form part of the analysis ie the preference of the approach is to avoid the event rather than let the event occur and then reduce the risk. This means that the approach used is pessimistic.
- Once the target value is reached, other potential measures are considered along with a simple cost benefit analysis to determine if the risks are ALARP.

The Basis of Safety approach adopted at Nufarm, Wyke is considered fit for purpose, in that it offers:

- A clear approach for incorporating operating and maintenance personnel in the analysis
- A clear indication of the risk reduction measures necessary to prevent a given event – the efficacy of which are transposed into operating instructions, and maintenance, testing and inspection procedures
- An indication that the number and type of risk reduction measures installed is sufficient
- Is pessimistic because mitigation measures and conditional modifiers are not used
- The approach can be the starting point for ALARP considerations
- The approach is calibrated both to HSE's published criteria and the corporate risk matrix.

The key to the approach is that it considers the full life cycle of the system. For example, the design intent of a reactor system may be to isolate the reactant feed if a given temperature is reached to prevent the possibility of an exothermic runaway. To ensure sufficient integrity of the temperature trip loop, a SIL 1 instrument loop (sensor – logic solver – isolating valve) may have been installed. This SIL level implies a particular level of risk reduction, but what the Basis of Safety approach adopted at Wyke does is also identify the other means by which the integrity of the safety system can be defeated. Many of these failures have occurred throughout the operational life of the processes installed on site. For example, if the temperature sensor is calibrated incorrectly; the wrong sensor is replaced; the thermocouple is not present in the fluid – all these errors could significantly undermine the criticality of the instrument loop resulting in the design intent being lost.

Table 1. Measures for ensuring integrity of temperature control

Issue	Potential causes	Potential measures	Justification
		Temperature	
Temperature probe must be in fluid	Temperature probe removed and not replaced	Temperature loop should not be linked out on removal, so preventing operation of reactor system with trip removed.	Critical instrument loops should not be linked out unless under robust management of change procedure.
		PTW sign-off and handover. PTW should make it clear that trip is critical. Supervisor must inspect installation before closing permit.	Adherence to PTW handover procedures for critical trip.
		Clear and unambiguous indication at trip location on reactor that trip is removed.	Indicates to all personnel that trip is not present and that reactor system should not be operated (unless robust management of change procedure in operation).
	Incorrect probe replaced	Clear and unambiguous tags on both instrument and its location on reactor.	Reduction in potential for human error. Tags indicate criticality of instrument loop and correct location.
		Tags could have type and range included. Type and range to be included on instrument test procedure/checklist and on PTW.	Cross check for both instrument fitter and for plant supervisor when signing off permit to work.
	Temperature probe too short	Ensure length required is stated on test procedure/checklist. Could also be recorded on instrument and location tags.	Reduction in potential for human error. Tags indicate criticality of instrument loop and correct location etc.
		Require 2 man check and signatures required on logsheet.	Cross check
	Position of temperature probe	Minimum liquid level determined during process design, recorded on system information dossier and probe installed accordingly – checked during commissioning.	Commissioning carried out by dedicated process team.
		Liquid minimum levels to be considered as part of management of change procedures for reactor systems.	Clear and unambiguous indication that temperature is critical and dependent on liquid level.
		Liquid minimum level should always be above any heating/cooling internal coils (where fitted).	Basic process design
		Install temperature probe in Bottom Run Off valve (if installed).	Temperature probe at lowest possible location. Check needed to ensure agitation is efficient at this location to prevent solids settling out etc.
	No oil in thermowell (if required)	Ensure requirement for thermowell oil (type and quantity) is stated on instrument procedure/checklist.	Efficacy of temperature measurement reliant on provision and correct type of oil being present.
		Replace oil (type and quantity) at intervals in accordance with suppliers information, or at each test interval.	Since quantities are likely to be small, may be better to replace at each test interval rather than according to suppliers interval which may be every 2–5 years – potential for oil change interval to be missed. Equipment will be necessary to be provided to enable oil replacement (small siphon pump etc.)

(*Continued*)

Table 1. Continued

Issue	Potential causes	Potential measures	Justification
		Provide instructions on how to deal with removal of aged oil or charred material.	Temperature probes may be difficult to remove if oil has charred. Procedure to deal with this occurrence needs to be developed.
Temperature probe must read correct temperature of fluid.	Instrument incorrectly calibrated	On bench calibration: Clear written test procedures and checklists. Human error significantly reduced if one fitter carries out calibration with second fitter recording results – then repeated fully by fitters changing positions.	If calibration is a two-man job then error is reduced significantly. However, may be too resource intensive. Probably only required for highest critical systems.
		On bench calibration: Provision of test fluids covering full range of temperature required eg water 0–100°C; sand baths for higher temperatures etc. Use of certified and validated standards under laboratory conditions.	Link to quality procedures.
		Operator checks during reaction. If boiling, output of thermocouple should read boiling point of mixture – ensure present on SOPs. Check, ambient temperature is output when reactor is at ambient conditions. Develop acceptable limits and build into SOPs and batch logsheets.	Important checks that will pick up drift or error on instruments each batch, rather than waiting for test intervals.
		On-line calibration: Sensor not removed but signals injected. For example, 4 mA = 10°C; 20 mA = 110°C. Calibration curve of temperature vs mA required.	Bench calibration is considered higher integrity than signal injection calibration. However mode of calibration can be related to test intervals. If temperature loop requires testing every six months but reactor shutdown for maintenance occurs yearly, then do bench calibration when reactor is down for maintenance and signal injection calibration at other times.
		On-line calibration: Clear written test procedures and checklists. Human error significantly reduced if one fitter carries out calibration with second fitter recording results – then repeated fully by fitters changing positions.	If calibration is a two-man job then error is reduced significantly. Probably only required for highest critical systems.
		Provide two independent temperature probes on each reactor with continuous monitoring between both sensors.	Allows automated continuous checking on temperature value. Higher integrity solution especially if both probes are not removed together – will allow check on reinstallation. Better if both probes have dissimilar locations ie one on baffles, the other in BRO valve line.

		If two temperature probes cannot be accommodated, because of lack of available ports, install Duplex instrument. Duplex probes have two thermocouples present in single thermowell and can have same integrity (i.e. SIL 1) as a single instrument.	
Temperature trip must operate at correct temperature and have the correct executive action.	Incorrect trip setting	Ensure trip setting present on test procedures/checklists and action required (specific valves closed/opened)	As for calibration above
	Incorrect trip relay chosen	Ensure correct relay is specified in test procedures/checklists. If trip is SIL 1 then safety relay orm approved relay with relevant performance data is required.	Criticality needs to be recognised.
	Inappropriate fail safe mode installed	Design specification from process safety protocols need to clearly and unambiguously define fail safe mode.	Basic process design.
		Instrument procedure/checklists need to be developed for testing of fail safe mode.	Must check that if any part of the instrument loop fails (sensor – logic solver – relay – valve) the loop fails safe.
	Incorrect or incomplete trip action	All valves on the loop require instantaneous monitoring to ensure all actions are performed. This will require personnel to be present at each valve location with appropriate communication between all personnel.	All trip actions must be seen to have operated at the same time.
	Trips not tested on re-installation of any part of the instrument loop.	Trip actions must be carried out on-line – they cannot be fully tested off-line or on the bench.	Clear unambiguous testing protocols/procedures need to be developed.
	Trip setting altered to allow test, but not reset to correct value.	Clear unambiguous testing protocols and instructions with supervisory monitoring to ensure trip setting chosen is correct.	Need to recognise criticality to ensure job is done correctly every time.
		Sensors are now available with a trip action test button. Pressing this button activates the trip action at the same reliability as actually activating the trip at a required temperature.	No need to alter trip settings.
	System not functioning ie no power supply; no electrical continuity.	Should be a clear indication that the system is live and functioning.	Better if a light is lit if OK, which goes out if loop is faulty. If opposite then blown bulb would not be fail safe.
		Ensure loops of cable are provided to ensure flexibility and lack of strain when removing/replacing.	Good process design and technician competence.

To ensure temperature control as design intent, the following must occur:

- The temperature probe must be in the fluid at all times
- The temperature probe must fail safe in the required manner (high temperature trips should fail high; low temperature interlocks should fail low)
- The temperature probe must have the required range and be correctly calibrated
- The temperature trip must execute the correct required action

The Basis of Safety approach essentially identifies those items (instruments, operations etc.) that are critical to ensure the reaction systems remain within the safe operating envelope at all times. The Basis of Safety also builds on the other assessments carried out during the design phase of a process. What the approach does is consider how the efficacy of these safety critical items can be assured throughout the life cycle of the process.

This study considered systematically the five main safety instrumented systems used on typical reactor systems – temperature, pressure, flow, level and agitation, and provided options for reducing potential errors in both maintenance and operation based on professional judgement and consideration of best practice.

The results from the study are illustrated in Tables 1 and 2 for temperature and flow and offer numerous methods to increase the integrity of the systems used on reactor systems.

CONCLUSIONS

The method adopted at the Nufarm site at Wyke, Bradford is considered a good example of good process safety management in action. The basic philosophy is to ensure that safety critical items are identified and that throughout the life cycle the design intent or risk reduction achieved is maintained accordingly. This requires that all relevant personnel are aware that certain items (whether they are safe operating procedures; maintenance instructions or items of hardware) are critical or special. This then clearly indicates to all involved that to maintain safety (the design intent) the job must be carried out correctly each and every time.

Safety critical instruments can be made recognisable as 'special' in several ways: they can be painted in a specific colour or the tags can be specifically coloured; the safety relays could be grouped together into one specific instrument cabinet with a means of opening the cabinet that is different to the other cabinets; multi-core cabling could be used only for non-safety critical items; safety critical instrument lines could be drawn in different colours on P&IDs, etc.

There are also other management type issues that could be adopted, perhaps by corporate rules, to indicate the special nature of critical instrument loops. For example, should safety critical instrument loops ever be linked out? Should the rule be that if a safety critical loop is faulty that the plant should not be operated? Should maintenance, testing and calibration of safety instrumented loops only be carried out by fully competent instrument fitters – the use of apprentices alone should not be

Table 2. Measures for ensuring integrity of flow control

Issue	Potential causes	Potential measures	Justification
		Flow	
Incorrect flow control	Orifice plate missing or not replaced following maintenance	Orifice plates highlighted as critical in maintenance procedures, tagged with size and flow duty etc.	Ensures criticality of orifice plates is clear and unambiguous
		Use of orifice pipe rather than plate	If orifice removed the space cannot simply be nipped up between flanges
	Orifice plate blocked	Orifice plates/pipes to be checked and cleaned during shutdown sessions or more frequently if known how quickly blockages occur	Present on critical items checklist
	Orifice increased in size due to corrosion/erosion	Orifice plates/pipes to be checked and cleaned during shutdown sessions or more frequently if known how quickly blockages occur	Present on critical items checklist
	Orifice plate in wrong location	If pressure regulator on air driven pump is altered, flow will alter if orifice is downstream of pump. In such cases better to install orifice in air supply to pump	General process design
		Upstream electrical pump must be replaced with like for like, otherwise flow regime may alter	General process design

allowed. What additional controls are placed on contractors working on safety critical elements?

Safety critical steps in safe operating procedures can be made special by highlighting those instructions that must be carried out according to the instructions every time by the use of coloured or bold type. It is also good practice to insert the reason why the particular step is critical.

The key points are that the design intent must be assured at all times. So the intent must be clear and unambiguous – not only how often a loop should be checked/tested, but what should be looked for, how the job should be done, and what standard is acceptable. All appropriate personnel should be made clear of the critical plant/processes and why it is important that the job (maintenance, operations etc.) must be done right every time – short cuts and discretion should be avoided for safety critical jobs.

REFERENCES

1. AIChemE, 1993, Guidelines for Safe Automation of Chemical Processes ISBN 0-8169-0554-1.
2. BP, 2005, Fatal Accident Investigation Report, Isomerisation Unit Explosion Final Report, BP Texas City, www.bp.com/liveassets/bp_internet/us/bp_us_english/STAGING/local_assets/downloads/t/final_report.pdf
3. MAIB, 2008, The Buncefield Incident 11th Dec 2005, Final Report of the Major Incident Investigation Board, ISBN 978 0 7176 6270 8.
4. Statutory Instrument, 1999, No 743 The Control of Major Accident Hazards Regulations 1999 (COMAH).