ABNORMAL SITUATION MANAGEMENT IN PROCESS CONTROL: DO WE HAVE IT UNDER CONTROL?

Raghu Raman, Kellogg Brown & Root, Sydney, Australia
Ian Cameron, University of Queensland, St Lucia, Queensland, Australia

ABSTRACT

Abnormal situation management (ASM) has been under increasing focus since the mid 1980s. There has been a significant amount of work done in many elements of ASM by researchers and control system vendors. Fault diagnosis, alarm system management and operator guidance systems have received both academic and industrial attention. However despite the developments, ASM is generally poorly practised in the process industries. Much of the actual practice places the onus on plant operators to respond effectively to abnormal conditions. This paper reviews the results of an industry questionnaire that sought to understand the current state of ASM in a range of chemical, oil, gas and base metal process facilities. It is clear that the technology developments are significantly ahead of application. There still remain key issues with regard to methods that effectively elicit root causes of abnormal conditions and the ability of operators to understand and respond to them. In the area of hazard identification the HAZOP procedure is routinely followed during the design phase to identify and deal with deviations, through alarms or interlocks. The causes of the deviation (failure modes) may or may not be fully identified and recorded in the HAZOP, and even if this occurs, not effectively communicated to the plant operator. The interviews with operators in various facilities have provided mixed results, with experienced operators confident of their abilities and inexperienced operators feeling threatened. Even if a trip occurs, without the knowledge of possible causes of the trip, re-starting the plant may not solve the abnormal situation. This paper explores just how effective are the current systems routinely used for ASM and raises the awareness towards an important but less focused area of process safety management.

1. INTRODUCTION

Poor abnormal situation management (ASM) or abnormal condition management (ACM) is considered to cost industry in the USA alone some $20 billion per year. This issue has been the focus of various programs in the USA via the ASM Consortium (Honeywell 2004) and the recently completed CHEM Project in the European Community (EC 2004). These initiatives have led to various software products such as Honeywell’s Experion or Gensym’s Optegrity (Gensym 2004) or toolboxes that link to current distributed control systems (DCS). Many of these tools rely on various levels of fault diagnosis technologies that include statistical analysis of process history data, the use of quantitative mathematical models or the use of qualitative approaches (Venkatasubramanian 2003a,b,c). Distributed control systems have become a standard feature in the control of process plants in the last 20 years. The DCS has enabled better control of the plant, design of complex alarm systems (exceedence of absolute limits, set point deviations, logic solving, trend monitoring etc), and design of interlocks where an alarm and operator response is considered inadequate.
The causes of a process deviation that result in an alarm or interlock activation are not always known in every situation. The process knowledge and experience of the operators has enabled management of many deviations. However, human error or inexperience can result in incorrect diagnosis, incorrect response and the sequence of events that follow, ultimately resulting in a runaway reaction, overpressuring or uncontrolled process, and loss of containment. How effective are the routine tools that seek to address this issue?

The Hazard and Operability study (HAZOP) is routinely used to evaluate the protective measures to cope with process deviations, especially for new plants at detailed design stage. What is not often carried out in a HAZOP is the identification and analysis of failure modes that initially cause the deviation. The causes are sometimes clustered into the category of ‘control loop failure’. Once the plant is commissioned and handed over by the design/constructor contractor to operations, the plant operator is left with the task of identifying the causes of a process alarm, so that appropriate response can be initiated. In the absence of documented failure modes specific to the process deviation in question, and operator awareness training on this, the operator may not be able to cope with the abnormal situation. Interviews with operators have provided mixed results, with experienced operators confident of their abilities and inexperienced operators feeling uncomfortable when interviewed. Even if a protection interlock is activated, without the knowledge of possible causes of the process deviation, re-starting the plant may not solve the abnormal situation, as the root cause may still be present. Should a loss of containment incident occur, the subsequent investigation, rather superficially, often attributes the incident to equipment failure and human error.

This paper highlights the gap that exists in the Safety Management System (SMS) with respect to ASM in Process Safety Management (PSM), with a view to raising awareness. Software tools available for ASM have not enjoyed widespread use in the industry, largely attributed to their complexity and cost. Some simpler approaches are suggested as a first step, that may be easier to implement.

2. WHAT IS AN ABNORMAL SITUATION?

An abnormal situation is one where a process variable (flow, pressure, temperature, concentration, level etc) goes outside its operating envelope and, if not brought under control by appropriate response, may escalate to an emergency situation (e.g. loss of containment). Even if a loss of containment does not occur, the equipment is subject to conditions outside its design limits, and its mechanical integrity is undermined.

In the hierarchy of managing process safety in plant design and operation, three distinct activities are undertaken during the design and operational phases:

1. Hazard and Operability Study (HAZOP): This is undertaken during detailed design to address process deviations that may occur, and identify the required response, hardware or procedural, or both.

2. Safety Management System (SMS): This is developed prior to plant commissioning and covers safe systems of work, procedures, and training of
personnel. The training is expected to provide process knowledge for the operator and tools to diagnose the causes of process deviations should they occur, and appropriate response.

3. Emergency Response Plan (ERP): This is integral to the SMS and addresses response measures to possible plant emergencies, with main focus on loss of containment emergencies that may lead to fire, explosion, toxic exposure or environmental impairment.

Each of the above steps is a safety barrier to an escalating abnormal situation.

- HAZOP helps to identify potential abnormal situations and develops appropriate alarms or interlocks, and provides input to operating procedures.

- The SMS addresses how the abnormal situation can be diagnosed and managed, through descriptions in the operating manual (HAZOP information transferred to this manual) and operator training. If the abnormal situation is not managed correctly, it could escalate into an emergency.

- The emergency response plan (ERP) is designed to respond to an emergency which has occurred, ASM failure being one of the contributors to the emergency.

Thus, effective ASM prevents an emergency from occurring and ERP helps to bring the emergency under control. The hierarchical relationship is shown in Figure 1.

While the HAZOP and ERP feature strongly in PSM, the ASM component of the SMS has received relatively less attention, the SMS focusing more on systems of work and related training, and maintaining safety critical systems integrity.

3. SOME EXAMPLES OF ASM FAILURE

The following examples illustrate how effective ASM could have prevented the emergencies and serious outcomes. The examples span a wide range of facilities, showing the common causes in all of them.
Three Mile Island Unit 2 nuclear plant - USA
The ingress of moisture into the instrumentation system started it all, with feedwater pumps to secondary cooling circuit shutdown. A sequence of events followed (steam turbine trip, emergency feedwater pump failure due to blocked isolation). The rest is history…

The system was designed to shut down safely, if no interference from operators occurred. The diagnosis problem was that operators didn’t recognize the initial cause that shutdown the feedwater pumps nor the fact that isolation valves, that should have been open, were in fact closed. This was only discovered 8 minutes into the accident and that was just too late to avert the events that followed (Perrow 1999).

If a set of failure modes for critical alarms were available to the operator, the failure could have been diagnosed correctly. Further, the system had been designed to shutdown safely if no action was taken. It is the operator’s interference following wrong diagnosis that accelerated the problem. An important part of ASM should be that interlocks cannot be overridden unless the one can be reasonably certain of the diagnosis.

Esso Longford Gas Plant - Australia
Gas Plant 1 used refrigerated lean oil to extract LPG in an absorber, leaving the vessel as “rich” oil. This oil is heated through several heat exchangers before distillation to remove LPG. Lean oil is recirculated back to the absorber.

A larger than normal flow of gas had occurred in the plant. The condensate level control was on manual by-pass because of a control loop problem. Condensate continued to build in the absorber, finally going into the rich oil stream. Lean oil flow was interrupted and so very cold liquid passed through the heaters dropping the temperature well below design. Feed to the plant was stopped but the unit was not depressurized. Finally pumps on the warm lean oil feed were restarted. This caused an embrittlement fracture in the exchanger and loss of containment. Fire and explosion followed.

The operators did not diagnose the problem of overflowing condensate nor did they understand the potential failure mode of embrittled steel (Hopkins 2000). This awareness embrittlement as a failure mode alone may not have solved the problem, unless the operator is given tools for such diagnosis, e.g. low temperature alarm or permissive interlock for re-start. This incident also reveals that ASM alone cannot prevent incidents unless there are alarms to identify an ASM. This places extra pressure on the HAZOP process.

Piper Alpha Oil Platform
The initial explosion from a condensate leak resulted in a fire causing gas riser rupture, producing a massive fire ball engulfing the platform, in 22 minutes after the initial explosion. Despite the fire, other connected platforms continued to export their oil to Piper Alpha believing that the Piper Alpha crew would quickly bring the incident under control. This simply fed the fire on Piper Alpha.
The causes of the incident were so complex that a simple ASM alone could not have prevented it. However, the diagnosis of other platform personnel that the Piper Alpha crew would handle the fire incident was incorrect, and continuing to feed Pipe Alpha with gas resulted in the massive escalation following the riser failure. The ASM did not address platform interface issues adequately.

**Explosion within Reactor**
An oxychlorination plant produced 1-2 dichloroethane by reacting a mixture of ethylene, hydrogen chloride and air in a catalytic fluid bed. The waste heat boiler tube bundle inside the reactor was used as a heater for reactor startup. The low temperature reactor trip, ensuring a minimum operating temperature to prevent air/ethylene explosion, was overridden during startup.

A reactor trip occurred during startup. By the time the cause of the trip was investigated and the reactor was re-started, it had cooled to below acceptable temperature. The senior operator was away from the site for a short duration, giving charge to the relief operator, who attempted to re-start the reactor. As soon ethylene was admitted, there was a loud explosion. Tonnes of catalyst spewed out of the rupture disc over a wide area.

The causes of the incident were (a) inexperience of relief operator (b) dependency on a single experienced operator who was not there (c) the inability to diagnose the cause of the initial trip quickly, and (d) not recognising the minimum temperature required for startup. Later, the override on the low temperature trip was removed.

**Anhydrous Ammonia Release**
A large petrochemical facility has an ammonia plant and other downstream plants (800m away) that used the anhydrous ammonia. A buffer storage tank near the downstream plant was periodically filled manually. The day tank was fitted with a local level gauge, a level transmitter signal to the central control room. A level alarm high (LAH), and an independent high high level alarm (LAHH) are provided, to alarm in the control room. The tank filling procedure was for the field operator to inform the control room operator, open a manual valve to transfer ammonia to the day tank, and close the valve when desired level is reached, as seen on the local gauge. Should LAH sound in the control room, the procedure was for the control room operator to contact the field operator by radio and ask the transfer to be stopped.

On one occasion, the local level gauge had failed and the tank was overfilled. LAH sounded in the control room. The control room operator contacted the field operator according to procedure. The field operator ignored this and trusted the local gauge. LAHH sounded, but this time the control room operator did not take any action on the grounds that he had already done so for the previous alarm. Approximately 12 tonnes of anhydrous ammonia liquid escape through the atmospheric pressure safety valve. Fortunately there were no fatalities.

The ASM problems in this case were: (a) there was no established protocol of authority - can the field operator ignore an instruction from the control room? (b) Failure of the field operator to recognise that the level indicator could have failed, even when alerted. The design itself was flawed in that there were no interlocks to stop the fill. Incorrect diagnosis and ineffective communication added to the problem.
Fuel Tank Overflow and Fire
A large storage tank containing flammable liquid was being filled but the operators did not know that the level indication and the safety alarm systems had failed. They did not monitor the filling operation closely because they believed that the tank still had plenty of capacity remaining. The tank overflowed and the strong odour was detected by a security guard who reported it to the control room. Two operators responded by driving a truck to the area to investigate. Within minutes, there was a loud explosion and fire. It is believed that their truck provided the ignition source that caused the initial deflagration and ensuing fires.

Here is an example of an abnormal situation and an unrevealed failure, difficult to detect without adequate instrumentation. It is the incorrect response of driving into a flammable vapour cloud caused the major emergency (CCPS 2004).

The above examples clearly illustrate that:
(a) correct diagnostic tools are required for the operator, both instrumented systems and documentation and
(b) correct operator response
are critical in preventing an abnormal situation escalating into a major accident event, and the latter escalating into a disaster. They confirm the earlier findings by Nimmo (1995) that ASM has 3 principal sources:
- Work or people context factors (~40%)
- Equipment factors (~40%)
- Process factors (~20%)
The ability to address these comprehensively is still the challenge of ASM systems.

4. INDUSTRY SURVEY ON ASM PRACTICE
A survey of 23 process facilities operated by 10 major corporations in Australia was carried out to evaluate how these plants managed abnormal situations in the facility. These facilities covered petroleum refineries, petrochemical plants, chemical plants, oil and gas storage facilities and mineral processing facilities. A survey questionnaire of 30 simple questions was prepared. Some organisations provided multiple responses, both from the management and from the operators.

4.1 The survey
The questionnaire was mainly directed towards the people factors in ASM. An abridged summary of questions are provided below:

- Age of facility and average experience of operators
- Frequency of review of written operating procedures
- Whether there is a register of critical operating parameters and acceptable operating limits
- Procedure for management of change, type of safety review conducted, operator participation in these reviews, and average number of changes made per year
- How is AS currently identified, root causes identified and situation managed (alarms, interlocks, operator experience, technical support, operating manual, interactive screen based systems, expert system software tools)
• Control room ergonomics, operating philosophy, formal human error analysis and management
• Teamwork and communication
• Whether incidents and near misses occur in these facilities, with current ASM practice

4.2 The outcomes

The major outcomes of the survey were:

1. In nearly all cases the facility was more than 20 years old
2. 70% of facilities were classified as Major Hazard Facilities (MHFs) with 80% of those being continuous chemical operations and the remainder oil and gas facilities
3. Average experience of all operators was in the 10-20 years range
4. In less than 50% of the industries, procedures had been reviewed and updated within the last 2 years. In others, the review interval has been 2-5 years.
5. All facilities had registers of critical operating parameters and change management procedures with ASM incidents being captured in corporate systems
6. In the previous 5 years about 50% of the facilities had carried out more than 20 plant or procedure changes and in conducting those changes, HAZOP was used in more than 80% of cases. There was no use of FMEA techniques. Operator participation occurred in 80% of the facilities during these reviews. Storage facilities tended use safety reviews rather than HAZOPs.
7. In about 80% of cases, operational changes were communicated to operators using work instructions and formal training
8. It was reported that almost 100% of facilities had definitions of abnormal situations (AS) and that process alarms were the universal indicator of those situations. Operational experience was nominated in 90% of cases as another important indicator and in nearly all cases process control occurred from a VDU-console.
9. The operating manual was used in 100% of situations to help identify the cause of the AS and engineers were consulted in 80% of those cases
10. It was clear that in a majority of situations the operator was not aware of the consequences of incorrect response to the AS and that there was a unanimous claim across all facilities that “near misses” had occurred because of incorrect responses.
11. In less than 15% of the facilities operators had built-in screen displays of causes and responses to alarms and interlocks.
12. Only 30% of those surveyed stated that the operators had adequate time to diagnose and respond to abnormal situations.
13. Only in 1 case had a formal facility study been undertaken to address human error evaluation. In every facility no formal training of operators had taken place to help recognize and reduce human error.
14. In 90% of the facilities, control room ergonomics were considered satisfactory
15. In almost all cases, safety was considered a priority over production, as an operating philosophy
16. All expressed the view that the operators worked effectively to assist one another in ASM conditions and that in 30% of cases the level of communication with engineers needed improvement.

4.3 Summary of key findings

The key findings were:

1. Despite the availability of ASM systems, there is not a wide application base of these systems. Most process operations do not employ them as routine tools.
2. ASM systems currently practised rely on procedures and operating manuals. These often do not provide the basis for effective ASM
3. The operator requires deeper knowledge and training even if there are intelligent systems available and used.
4. HAZOP, despite its wide appeal and use, requires complementary hazard identification methods to ensure that failure modes are adequately captured as part of the root cause analysis of process deviations.

5. CAUSES OF GAPS IN ASM

Nimmo (1995) lists a number of causes for inadequate management of abnormal situations that have escalated into accidents. The following is a summary of Nimmo’s findings and the findings of the present industry survey.

HAZOP stage:

1. Causes of process deviations not fully identified in the HAZOP. There is a need to identify failure modes rather than recording ‘control loop failure’.
2. Many HAZOPs of new plants at design stage do not have operations involvement.
3. HAZOPs organised by the EPC contractor during the project phase focus mainly on design, with less emphasis on operation.
4. Inadequate alarms for operator to identify and respond to deviations. This can result in unrevealed failures, identified only after it has escalated, e.g. the tank overflow incident.

Operations Phase:

5. Absence of a clear understanding of what an abnormal situation is, and its consequences in the event of an incorrect response. Hazards of incorrect response not highlighted in process knowledge communication to the workforce.
6. Absence of clear procedures for dealing with abnormal situations (as opposed to emergencies)
7. Inadequate time available for the operator to mount the correct response. This is a design deficiency, as this should have been identified at the hazard identification stage, and designed using layer of protection analysis.
8. HAZOP documentation rarely revisited after the design phase, whereas there is much useful information on response to deviations that could be brought into the operating manual.
9. Significant role of human errors - incorrect response to AS
10. Control room ergonomics contributing to human error (this problem has been largely overcome in modern plants, and upgrades to older plants)
11. Incorrect operating philosophy - the attitude that there should be no production interruption, whereas it may be safer to shut down, or let the installed safety instrumented system (SIS) initiate a shut down, as a response to an abnormal situation. This may not be a significant factor as almost all the surveyed companies have a philosophy of emphasizing safety over production.
12. Loss of organisational memory - information from earlier minor incidents is lost. How often we have seen the question asked - “what did we do when this alarm came up last time …?”
13. Change of personnel. Much depends on operator’s knowledge and experience, and when changes to personnel occur, and therefore their knowledge is lost to the organisation. Perron and Friedlander (1996) and Philley (2002) argue the case for including organisational changes such as downsizing in management of change for safety, and list a number of human factors contributing to accidents caused by organisational changes.
14. Inadequate teamwork and ineffective communication. 30% of those surveyed said that this area needs improvement.
15. Even in MHF facilities where operator participation is mandatory in the Safety Case development process, ASM gets only a cursory review. The “correct” response to AS by operator is implicitly assumed in most cases.

6. METHODS TO IMPROVE ASM

There are ASM systems available but not widely used in the industry. Their use is likely to be driven by considerations of cost and more importantly the expertise within companies to actually implement effective systems that require integration of real-time data analysis, extraction of trends and relating root cause analysis to comprehensive HAZOP/FMEA studies through expert system technology and related approaches.

Some actions can still be taken to improve the effectiveness of ASM that are less complex to implement.

1. Training of personnel in the hierarchy of process safety management and the importance of ASM as a tool to prevent process deviations turning into process emergencies.
2. Operator participation in HAZOP whenever possible, especially as part of management of change in operating plants. Rotating the operator in HAZOP sessions and involving the operator specific to the area being reviewed.
3. Identification of failure modes of process deviations in the HAZOP, ensuring that safeguards address all failure modes, and identifying appropriate operator response. This may lengthen the HAZOP process, but if operators are present, provides for an implicit training tool as well.
4. Training of operator in identification of failure modes for process deviations by using a focused FMEA technique.
5. Improved operating manual. Capturing AS response from HAZOP documentation into the operating manual.
6. Including the changes in personnel and hence loss of process knowledge and experience as part of management of change, especially in evaluating the competency of replacement personnel.

7. SUMMARY

An industry survey has indicated that there is a gap in the effectiveness of SMS, in the area of ASM. Ill-managed, an abnormal situation may escalate into a major emergency. Despite the availability of ASM systems, they have not found widespread application.

The causes of ineffective ASM have been identified. These can be sourced back to not identifying failure modes of deviations in the HAZOP, lack of transfer of HAZOP generated information into operating manual, critical dependence on operator’s knowledge and experience, lack of awareness of ASM’s critical importance in the hierarchy of PSM, and ineffective use of tools available.

As plants age, the dependence on the experience of the operators becomes more and more critical. As personnel change, a new generation needs to be trained with what information is still left in the organisation’s memory. Where ASM relies on operator and engineer intervention this is particularly crucial. It also applies to modern ASM tools. The industry survey clearly indicated the areas of inadequacy.

The industry survey has indicated that only 20% of those surveyed use such information to assist the operator. Since technical help from the engineer is sought for ASM in about 90% of those surveyed, a screen-based interactive expert system can help to provide this assistance in the first instance, especially as engineering help may not be available 24 hours a day.

8. REFERENCES

Gensym, 2004 (Ian, please fill in reference)
Perrow, C., 1999, Normal Accidents: Living with High-Risk Technologies, Princeton University Press, USA

ACKNOWLEDGEMENTS
The authors wish to thank the organisations who participated in the survey and provided valuable insight into current industry practice.