ALARM PERFORMANCE IMPROVEMENT DURING ABNORMAL SITUATIONS

Peter Andow
Honeywell Hi-Spec Solutions, Southampton, UK

The process industries are continually facing new challenges to increase throughput, improve safety, reduce emissions and reduce costs. Competitive pressures have increased substantially, partly due to low oil prices.

In many plants there is minimal scope for further improvements due to changes in operating conditions or plant throughput. By contrast, there are still substantial improvements possible from improved handling of "abnormal situations". The Abnormal Situation Management Consortium has identified alarm systems as a key area for performance improvement. This paper examines the improvements that may be gained by improvements in the performance of alarm systems.

Topics covered include:

- The Abnormal Situation Management Consortium
- The role of alarm systems in reducing the frequency and impact of abnormal situations.
- Means for improvement of alarm systems.

THE ABNORMAL SITUATION MANAGEMENT CONSORTIUM

The Alarm Management Task Force (AMTF) was formed from 25 customer representatives in 1990. The AMTF was concerned with alarm system problems common to all vendor distributed control systems. The AMTF team recognised that the alarm system was central to the problem of handling abnormal situations - but that many other factors are also relevant. The ASM ^{TM} (Abnormal Situation Management ^{TM}) Consortium was originally formed in 1994 by Honeywell and the major US oil refining companies (Amoco, BP, Chevron, Exxon, Mobil, Shell and Texaco) arising from the activities of the Alarm Management Task Force.

Other companies have since joined the consortium, including chemical (Nova, Celanese and Union Carbide), training companies (Technology Training Systems) and control building design (Brad Adams Walker). Three University Affiliates (Ohio State, Purdue and Toronto) also joined. Bullemer[2] gives more information on Consortium activities.

Abnormal Situations can be caused by:

- Changes to plant operating conditions that may be intentional or due to operating errors;
- Failures occurring in the plant or its control systems, such as deterioration of heat exchanger performance;
- Environmental events such as severe weather;
- Mechanical damage - such as that caused by pipe failure or vehicle collision.

The consortium's activities were considerably wider than those of the Alarm Management Task Force, since the consortium had recognised that difficulties in Alarm Management were only the most obvious symptoms of problems elsewhere in the plant and/or the wider organisation.

For example:

- Management Culture: Some companies operate a "no blame" culture whilst other companies make life very difficult for an operator who makes a "mistake" – particularly when this results in unnecessary lost production.
- Safety Culture: Some companies spend considerable efforts on Hazard Identification and Analysis to reduce both the frequency and consequences of abnormal situations. Other companies spend much less time on such activities.
- Operating Procedures: Many companies spend considerable time and effort in development of elaborate operating procedures for use when problems occur but, in practice, these procedures are often not used during abnormal situations. A variety of explanations are given for this:
    - There is insufficient time to locate the appropriate procedure;
    - There is insufficient time to read and understand the procedure when required;
    - The procedure had not been kept up to date as plant changes occurred;
    - The procedure was thought to be erroneous or inapplicable to a particular situation – perhaps because the operator had experienced difficulties with other procedures.
- Training: Some companies give much more training than other companies. Some companies rely heavily on "on the job" training - which isn't very effective for handling abnormal situations - whilst other companies will give special attention to diagnostic training.
- Human Factors: Some companies are much more pro-active than others in ensuring that the Plant Environment, the Control Room Environment, the Console Design etc. are appropriate for avoiding and/or handling abnormal situations.
- Team Organisation: Some companies organise their operating teams so that co-operation between team members both inside and outside the control room is more effective. This can be particularly useful during abnormal situations.
- Communications: Some companies focus strongly on ensuring good communications between all concerned.
- Maintenance Practices: The quality of maintenance practices and procedures varies widely. Poor practices have caused or otherwise impacted many incidents.

The list above is not intended to be exhaustive – but it does illustrate that many "performance shaping factors" can impact the management of abnormal situations.

There was also recognition within the consortium that "prevention is much better than cure" – it is much better to avoid an incident altogether than to be skilled at dealing with it in real time.

HANDLING ABNORMAL SITUATIONS

There are 3 stages in handling an abnormal situation:

- Detection
- Diagnosis
- Correction

DETECTION

Early detection is important – because fault consequences will often be less severe and the time for corrective action is longer. The Alarm System design is critical for early detection. The most obvious approach to reducing detection time is to operate with tighter alarm limits – and many companies have tried that approach. Unfortunately this also leads to many spurious alarms (sometimes called "false positives") – alarms that are due to noise rather than any genuine problem. The real requirement is to get early detection and a low number of spurious alarms. Current industrial systems are prone to "alarm floods". The EEMUA Guidelines [1] provide guidance on alarm system design.

Much work has been done in this area recently by the ASM Consortium using "State Estimators". Results to date are encouraging. The approach used:

- A set of State Estimators that provide a complete description of the process state;
- An infrastructure that combines and presents notifications to the plant operators.

This approach is being tested in field tests on 3 different customer sites. The State Estimators include 4 different technologies:

- Multivariate Statistics;
- Qualitative Trend Analysis;
- Neural Net Clustering;
- Sensor Validation.

The tests are showing an accuracy of 70 - 80%. This is encouraging although it is recognised that a higher accuracy will be required for widespread plant usage.

DIAGNOSIS

Diagnosis is usually the most difficult part of the Detection-Diagnosis-Correction sequence. Even "simple" faults can be difficult for an operator to diagnose if the fault has not been seen before.

Diagnostic Training is the most obvious way to increase the proportion of faults that are familiar to the operator. The operator then uses pattern recognition to identify the fault. Care must be taken to avoid mistaking one fault for another that has similar symptoms but may have a quite different cause.

Many companies have also attempted to build diagnostic support systems – see separate discussion below.

CORRECTION
In some cases (particularly where severe damage occurs and/or major releases of toxic material occur) corrective action may be limited to consequence-mitigation rather than anything to "correct" the fault. But in many other cases, corrective action will be relatively straight-forward once a fault has been correctly diagnosed.

DIAGNOSTIC SYSTEMS TECHNOLOGY

Many companies have attempted to build computer-based diagnostic systems for use in process plants. Many research projects have also focused on the same problem.

The literature contains papers as far back as the mid-1960's on the use of computer-based diagnostic systems in chemical and nuclear power plants. The basic diagnostic problems have not changed at all in the 30 years that have passed since then – but the computer hardware and software available for building such systems has changed in ways that could hardly have been imagined by the writers of those early papers.

It is clear that a computer can be programmed easily to associate a "pattern" of symptoms with a fault. In spite of this, it has proved to be very difficult (in practice) to create robust and reliable diagnostic systems.

A wide variety of techniques and technologies have been tried including:

- Boolean logic;
- Probabilistic calculations (including fuzzy logic);
- Directed graphs;
- Fault trees;
- Cause-consequence analyses;
- Knowledge-based systems;
- Neural networks.

In spite of all this work there is no established or proven methodology. In the author's opinion, this is because the practical problems of creating, using and maintaining the underlying Failure Models have been consistently under-estimated.

The ASM Consortium has designed and evaluated a diagnostic system called AEGIS. This system uses State Estimators for early detection and then supports the operator through the diagnosis and correction stages. Experience with AEGIS has been very positive but many challenges remain before systems like AEGIS can be used routinely.

THE ROLE OF ALARM SYSTEMS

Alarms systems are a key element of abnormal situation management – probably the most important element. Some observations on the vast majority of (but not all) alarm systems:

- Alarm systems have grown from (typically) a few hundred alarms to many hundreds or thousands of alarms on most plants during the last 20 years.
- Many systems show excessively-high alarm rates – often an alarm every few minutes even during "normal" operation.
- Some plants average more than one alarm per minute.

- Many plants suffer from “alarm floods” during abnormal situations. The rate of alarms reported in accident reports is excessive – examples like “40 alarms in the first minute” are not unusual.
- Many alarm systems are poorly maintained. Alarm limits etc. are often inappropriate for current operating conditions and may not have been reviewed since plant start-up.
- New alarms are often added, particularly in the early life of a plant. Alarms are rarely deleted.
- Many alarms are poorly and inconsistently prioritised.
- It is often observed that alarms do not result in any operator action. Why are “alarms” like this needed?

The above list is not exhaustive!

ALARM SYSTEM IMPROVEMENT

Alarm systems have rarely been designed to the same standards as other plant systems. They can be much improved with application of common sense and solid engineering.

Improvement typically requires a multi-phase approach:

- Collect static alarm configuration data and dynamic performance data (“alarm journals”).
- Review the data examining alarm frequency, the most common alarms, time to respond etc. Part of this task can be done using analysis tools by specialists who do not know the particular plant, but final conclusions can only be made by experienced staff familiar with the plant and it’s operations.
- Develop an alarm philosophy that is consistent with plant needs, DCS facilities available and human operator capability.
- Redesign the alarm system using the alarm philosophy. Redesign must involve engineering and operations staff. The result of this process is that a significant number of the existing alarms will be removed – often as much as 50%. In some cases, the plant displays will also be redesigned to further improve operator effectiveness.
- Produce an alarm manual that clearly identifies:
    - Alarm identification data (tag, message etc.).
    - Alarm configuration.
    - Causes of the alarm.
    - Operator response required.
    - Consequences if the alarm is not acted upon.
- Use the alarm manual to train all plant operators.
- Monitor the new system regularly – it needs maintenance.

IMPROVED ALARM SYSTEM PERFORMANCE

NORMAL OPERATION

The net result of careful redesign is improved performance. A reasonable target is that a panel operator would typically only handle a few alarms in an hour of normal operation. In some cases, it is possible to achieve a “black panel” where no alarms are active!

ABNORMAL SITUATIONS
During unexpected abnormal situations (i.e during a major disturbance or equipment failure) performance will also be improved. Alarm floods may still occur but will be less severe – with perhaps 60% fewer alarms. A significant factor here is that any alarms that do occur will at least have clearly-identified responses.

REAL-TIME ALARM HANDLING

Further improvements in performance require changes in the dynamic alarm system. A number of approaches are possible:

- Escalation of alarm priority as the incident progresses.
- Suppression of low-priority alarms when multiple higher-priority alarms are active.
- "Grouping" of alarms that are similar (e.g. multiple thermocouples in a reactor bed).
- Suppression of consequential alarms following trips.
- "Shelving" of "standing alarms" caused by instrument failures or unusual plant conditions.

These techniques can reduce the alarm rate considerably – to the point where the panel operator can use the alarm system to effectively respond to abnormal situations.

The benefits of improved performance are:

- Increased production due to less plant trips.
- Increased conformance with product quality targets.
- Decreased accident rates.
- Decreased emission rates.

These benefits all make a direct impact on business profitability.

ADVANCED APPLICATIONS

The improvements described above are limited to the alarm system and process displays. Other improvements are possible:

- State Estimators can be used to give early warning of plant failures. The benefit here is that early detection can improve the options for operator action as well as the "thinking time" available. Much current research is aimed at this area.
- Diagnostic systems can also be used to recognise fault patterns and assist the operator in recovery. The AEGIS system (mentioned above) is an example.

It must be stressed that "Advanced Applications" are unlikely to be of great benefit unless the "foundation" of the basic plant alarm system is first improved.

AN EXAMPLE APPLICATION

The AEGIS prototype system used as an example and "test bed" application. A plant model was constructed based on an FCCU operated by one of the Consortium member companies. The AEGIS design is based on 6 components:

- A State Estimator (What is our current status?)
- A Goal Setter (What's the next best thing to do?)
- A Planner (How can we do it?)
- An Executor (Make sure it is done properly.)
- A communicator (Make sure everyone is in the loop.)
- A Monitor (Learn from experience.)

The plant model was constructed and failure models identified from operating experience. Simulation was then used to test the prototype. The prototype system was found to be capable of handling all of the failure scenarios. Demonstrations of the diagnostic behaviour were given to all Consortium members. A team of operators from a similar plant was also asked to review the results. The operators were very positive.

CONCLUSIONS AND PROSPECTS FOR THE FUTURE

It is clear that there are substantial benefits to be obtained from better handling of abnormal situations. It is also clear from the literature that there are substantial challenges that must be overcome if we are to build robust and reliable operator support systems. Alarm systems are the central focus for operator support during abnormal situations. The ASM Consortium had its roots in the Alarm Management Task Force and has done much work in this area. The ASM Consortium has recognised many other “performance-shaping” factors but there are still key improvements that are expected in the Alarm Systems area:

- Alarm systems are a key element in the management of abnormal situations. Many current alarm systems are of poor quality.
- Many alarm systems can be substantially improved so that “alarms” are real and “alarm floods” are significantly reduced or eliminated.
- The use of State Estimators for early detection will be a key factor in increasing the time available for diagnosis and correction. Much work is being done in this area both inside and outside of the Consortium. The technology is encouraging and is advancing.
- Automated diagnostic systems will be used in more complex plants. These systems will require substantial investments in failure modelling.

TRADEMARKS

REFERENCES

1. Anonymous, 1999, Alarm Systems - A Guide to Design, Management and Procurement, EEMUA Publication N. 191.
2. Bullemer, P., Cochran, T., Harp, S., and Miller, C., 1999, Collaborative Decision Support for Operations Personnel, Proc. Interkama ISA Conference.