THE ALARM SYSTEM FROM THE OPERATOR`S PERSPECTIVE

C T Mattiasson

Scanraff AB, Sweden

Introduction

Most (People in Control) would agree to the statement, that alarm systems of today, in general, do not work as well as required. It is of course in everybody's interest that they should. Operators, Management and Authorities, all want a system that really assists the operator in her/his work, when an upset occurs in the process. The operator because it would make his day easier, management because money is saved with shorter downtimes, and authorities because a more stable process operation with in the process industry, means less negative impact on the environment. So there is no conflict of interest, which is a good foundation to build on. In a number of incidents and accidents in recent years, the alarm system has been identified as a contributing factor to the escalation of events from upset to worse.

This paper will discuss the alarm system from the operators perspective. My background is in crude oil refining, so this paper is based on experience from alarm systems in refineries. However I do believe that what is stated herein will apply to most industries, at least in parts.

Design, Review, and Configuration of Alarm Systems

The alarm systems are designed for normal operation, and during normal operation the systems work quite well. But during upset conditions, even minor disturbances, the alarm system will generate a huge, unmanageable amount of alarms. The system is also configured for normal operation regarding alarm limits, alarm priorities and so forth. User influence at time of design is probably close to zero, and also during configuration end user considerations are not likely to be obtained. Eventually a review of the alarm system might be called for, and most likely now the operators will be more involved. Experienced operators can provide valuable information about process behavior during different process states, and

what they would like the alarm system to present to them, during normal and upset conditions Their knowledge will be of significant importance for a reviewing project.

If more and better tools for configuration were provided by the manufacturer, each site could have the alarm system customized to suit their specific desires. If these points of view were regarded, a more user friendly alarm system would be the result. It would, however, be more adequate if user input could be a possibility already at the time of design. Then less effort would be needed for reviewing and restructuring the alarm system. Users should have influence on the design of alarm systems Of course the manufacturer has no wish to develop a bad alarm system, they simply do not fully understand the end user needs. Much of the alarm system features is of no significant value to the operator. There is an engineering flavour to some of the features. Some functions may look good on paper, but without a good knowledge of the operators real needs, it is not likely that a good alarm system will be developed.

The reason for the manufacturers reluctance to involve users in the development is probably of a strategic and/or commercial nature. Understandably they would not like the competition to know in what direction their development efforts are going. But with good will and intentions from everybody involved, this should not be an issue. Hopefully in the future there will be much more co-operation user/manufacturer in this area.

Alarm Response Manual

Alarm response manuals are sometimes put forward as a big help for the operator during upset conditions. It is doubtful if that is so. All responses described in such a manual has to be absolutely correct, and since one alarm can have a number of responses, the effort to produce such a manual would be monumental. If there is only 1 response to an alarm, then maybe that response could be automated? Also keeping such a manual up to date would

consume considerable resources of the user staff, in an on-going fashion.

Over time such a manual might even drain operator knowledge, since they would turn to the manual instead of trusting their own skills and knowledge. Most of the required operator actions during an upset is time critical. It is not likely that using an Alarm Response Manual would be a practical way of working, when a large amount of alarms are calling for action. And finally, in general it is not lack of operator knowledge that causes operator errors during upsets, it is more often the information overflow, and the alarm flooding, that confuses the operator, or important alarms being missed because they are obscured by hundreds of other alarms, that might not even be relevant to the situation.

Operator Workload

During normal operation the operator workload is minimal, and other computer systems like expert systems, advanced control and so on are providing the operator support for optimizing and operating the plant in a safe manner. During upset conditions the situation is the reversed, the expert system is producing lots and lots of advise, advanced control is out of the picture, and the alarm system is more or less of no use in this situation.

Also, during upsets the readings from flow and level indicators might show unreliable, or even false values due to pressure and/or temperature drop in various process streams. When system-pressure and/or temperature drops, the hydrocarbon composition in process streams will change, but the alarm setpoints will remain those configured for normal operation. This the operator has to bear in mind.

An investigation at Scanraff showed that during normal operation the average number of operator actions per hour was **3.1** via the system (a random week). During upset conditions the average number of actions per hour increased to **52.8**. This is almost 1 action per minute via the system at upsets. To the system actions should be added conversations via radio and telephone and so forth. Now this is a full plate for the operator, and anything added will have a significant impact on the total efficiency and quality of the operator performance.

The operator has two kinds of workloads – a mental and a physical. The mental workload being things he must keep in mind, like controllers put in manual mode, control-valves that are blocked or bypassed, important alarms which must be checked regularly, and so on. The physical workload consists of actions taken via the DCS system, communication on radio and telephone, and discussions with engineers and supervisors. Therefore information presented to the operator must be of a manageable magnitude, otherwise the risk for mistakes increases.

The human interface and the alarm system must be designed in such a way that they do not add to the operator workload. During upsets the working situation for the operator is such, that she/he should not be forced to work with the interface itself, e.g. browsing between displays unnecessarily, opening/closing windows etc. Everything should be designed in such a way that information needed is easy accessible for the operator. The most used interactions should be designed so that only 1 keystroke is needed to, e.g. call up a display. Everything that add to operator workload must be carefully considered, so that nothing is created unnecessarily. The description of the alarms in the alarm list should be clear, so that it does not add to the mental workload, and should not leave any room for interpretation or misunderstanding.

Operator Performance

What is the operator`s task? The answer is depending on the process mode at the time for the question. During normal operation it is to optimize, pushing towards constraints with a minimum of product quality giveaway. When a minor upset occur, her/his job is to bring the process back to normal operation. During a major upset she/he is expected to bring the process to the nearest safe state, and if disaster threatens, shut it down, and try to limit the consequences.

To meet these expectations the operator must be provided with the tools necessary to carry out her/his duties to the best possible standard.

The quality and amount of information and alarms that are presented to the operator have a direct impact on her/his performance. It is therefore important that information and alarms presented are relevant to the current operating situation. This is not the case with today's alarm systems. While the process is dynamic, the alarm system is static. The operator adjusts to the situation, and deal with it to the best of his capacity. The alarm system is static, and important alarms are difficult to locate in the alarm list, because alarms are

coming and going to the list, and therefore the alarm list is constantly repacked. Each time the operator looks at it, it has changed. An alarm that he wants to keep an eye on for some reason, might suddenly be gone from the list, and when this happens the operator does not know if the alarm has returned, or if it is on the next page of the list, so he has to browse through the list. This is consuming valuable time, time that would be better spent on recovery work with the process. A lot of time also has to be spent on acknowledging alarms. But if nothing else, at least this will stop the flashing in the displays, and silence horns and buzzers.

Real Life Example: Compressor Trip

A compressor trip is a very unpleasant event. It cannot be considered to be a major upset, but the result is production loss, and a lot of work for the operators. Hereafter follows a evaluation of a compressor trip.
The consequences of a trip of this compressor is that the heater will shut down, and so will the feed-pump. This is done by the safety system. So alarms that are meaningful to the operator in this situation are confirmation of heater shutdown and feed-pump shutdown, and the reason for the compressor trip.

-392 alarms generated for the entire event
-1 alarm every 2 seconds the first minute
-254 alarms the first hour
-Operator acknowledged alarms 204 times
-1 alarm was triggered 118 times
-9 alarms were triggered more than 10 times
-Operator took 79 actions
-Theoretical minimum of actions were 39
-Event lasted 1.5 hours

It is obvious that the alarm system considered this to be 392 separate events, while to the operator this was one event, a compressor trip. Consequences of the compressor trip is that the safety system will shut down the heater, and take out the feed. The operator is fully aware of this, but the alarm system is not, so there is no compatibility operator/alarm system. The operator is capable of adapting to the situation, and so should the alarm system be. As it is today, the operator has to spend time and effort to analyze what has happened by searching the overfilled alarm list before he can take corrective actions.
Also the chattering alarm (sample flow to a sulphur analyzer, triggered 118 times), should

have been noticed by the alarm system and disabled, since it was obviously not relevant at this time.
An in-depth analysis of this event showed that a reasonable number of alarms would have been in the neighborhood of 75 – 80. Some of these would have been alarms confirming that the safety system worked as intended, and others urging the operator to take appropriate action. If the alarm system had worked in this manner, a considerable amount of time would have been saved, and consequently the downtime would have been shorter. An alarm system that adapts to the situation in the same manner as the operator, would also decrease the stress that the operator is exposed to in situations like this. If there had been fewer alarms for this event, she/he could more easily have seen what had happened, and she/he could have started recovery actions sooner, and feedback from system on the actions taken would shortly have been visible in the alarm list, as the process would recover from the event.

Benchmarking

For the reason of creating a standard for alarm systems, and a way to measure system design and performance, the following metrics are an attempt to do so.. Much of this work has been done within Honeywell Users Group; Operator Interface Workshop.
Listed hereafter is a number of metrics, that the group has agreed on to be valuable, when analyzing an alarm system.

Design Metrics

-Number of control-loops per operator
-Number of configured alarms per operator
-Number of Analogue Inputs
-Number of Digital Inputs

Performance Metrics

-Average number of operator actions/hour, normal operation
-Number of operator actions, first hour, upset conditions
-Average alarm rate/hour, normal operation
-Number of alarms the first minute, upset conditions
-Number of alarms the first 10 minutes, upset conditions.
-Average number of standing alarms
-Average number of shelved alarms

-Average spread of alarms (%) each priority, normal operation, (Emergency, High, Low)
-Spread of alarms (%) each priority, upset conditions, (Emergency, High, Low)
-Spread of priorities (% of each) for all configured alarms, (Emergency, High, Low)

These metrics can of course be discussed, but they do originate from a wide spread of industries, and countries. Honeywell Users Group have identified these metrics from work by 11 different companies in 9 countries. Remaining work is to establish values or target values for each metric. It is essential that some metrics for alarm systems are developed, so that a (hopefully) international standard for measuring alarm system design and performance can be established. This would be beneficial for all parties involved. For this to happen, it is necessary for some sort of standardization commission or equal to take action. If true benchmarking figures are available, companies can compare themselves to these figures, and then quite easily see how their own system is doing, something like a Solomon-study for alarm systems.

System Features

Some features for alarm management comes with the system; different priorities, disable/inhibit, sorting in different ways, freeze the alarm list, and a few more. However, these functions are merely cosmetic, and does not improve the alarm system behavior during upsets a whole lot, some might even be a bit risky to use; like sorting by priority. If only Emergency are showed on the list (by the sorting function), many alarms will be obscured, and if not dealt with in due time, they may de facto become Emergency, and might cause the situation to escalate to worse instead of coming back to normal. Another disadvantage with these functions are that the operator has to invoke them himself. This means that he will have to do work with the alarm system, while his attention is needed by the process. It will distract him from his most pressing duties at a time when it is very important that his full attention is dedicated the process.

Future Design of Alarm Systems

It seems like a new approach to alarm system design is needed. Companies, organizations, projects, and other groups are today working with the alarm system all over the globe, so the manufacturers do have a window of opportunity to obtain valuable input from these groups.

Software applications for improving alarm system performance can be bought from third party's, and consultants provide their services for a certain fee. This is costly, and time and resource consuming, and are also patchwork, like fixing up an airplane with wires and tape.

In the future the alarms will reflect the state of the process, and the alarm list will in fact be a prioritized action list. The system will automatically adapt to the process state, and the operator will not be presented with alarms that are not relevant to the current operating state. The system will inform the operator of the situation, maybe like this:

---COMPRESSOR TRIP---
---SAFETY SYSTEM ACTIVATED---
---CONFIRMED HEATER SHUT DOWN---
---CONFIRMED FEED PUMP SHUT DOWN---
First out: High-High level, suction drum
nnnnnnnnnnnnn
nnnnnnnnnnnnn
nnnnnnnnnnnnn
nnnnnnnnnnnnn

This can be done if the alarm system more resembles the process, e.g. the process has sections like Feed Section, Heater Section, Reactor Section, Stripper Section, Product Section, and so on. The alarm system can be designed in a similar way, so that when disturbances occur in the process, that very same alarm "module" for that part of the process will be activated. Now, when the alarm system knows this, alarms that are secondary alarms, caused by the initial disturbance, will not be triggered. The number of alarms are hereby reduced, and alarms triggered are relevant to the situation.

Maybe some way to graphically present what the consequences will be, if an alarm is not dealt with in due time could be created, a sort of consequence mapping, possibly together with some indication of the time available before the consequence is a fact.

By adding dynamics to the system, like suppressing secondary alarms and so forth, a big improvement of the alarm system can be achieved. But it is important that this is done by configuration, and not by user written programs or similar. Programs need to be updated, while the system parameters (like alarm limits, and alarm priorities) are automatically updated. If a program should not

be updated, the consequences could be severe.

In the future alarm systems there will be a much clearer relation between the actions the operator must take to bring the process back to normal, and the alarms that are presented on the screens.

What is stated here about the future development of alarm systems might be some sort of wishful thinking, but if effort is put in to this subject by end users, and system developers, for certain, a new and better alarm system will be a reality.

Maybe some interaction between all the different groups, authorities, manufacturers and academia, that are currently working in this area, together could come up with a common goal for such an effort, and develop an entirely new approach to alarm systems.

Since there are so many engaged in this line of work, there is obviously a great need for something better. I also believe that there is a lot of knowledge gathered in these groups, so some sort of information exchange could prove beneficial for all.

Such a venture should also involve operators, since they are the primary victims of today's alarm systems.