FIT FOR PURPOSE? QUESTIONS ABOUT ALARM SYSTEM DESIGN FROM THEORY AND PRACTICE

by Dr Steven Shorrock

Most safety-critical environments – nuclear power control rooms, flight decks and operating theatres – have one critical system feature in common: alarms. The ATC ops room, by comparison, has few. But this will not always be the case. More complexity, increasing automation, and future changes in ATM, will mean more alarms – something that CNS colleagues have experienced for over a decade.

QF32 and the alarm avalanche

4th November 2010.
Just four minutes after take off, climbing through 7,000ft from Singapore Changi Airport, an explosion occurred in one of the engines of QF32, a Qantas Airbus A380. Debris tore through the wing and fuselage, resulting in structural and systems damage. The crew tried to sort through a flood of computer-generated cockpit alerts on the electronic centralised aircraft monitor (ECAM), which monitors aircraft functions, produces messages detailing failures, and lists procedures to undertake to correct the problem. They crew recalled an "avalanche" of (sometimes contradictory) warnings relating to engines, hydraulic systems, flight controls, landing gear controls, and brake systems.

David Evans, a Senior Check Captain at Qantas with 32 years of experience and 17,000hrs of flight time, was in an observer's seat during the incident. Interviewed afterwards, he said *"We had a number of checklists to deal with and 43 ECAM messages in the first 60 seconds after the explosion and probably another ten after that. So it was nearly a two-hour process to go through those items and action each one (or not action them) depending on what the circumstances were"* (Robinson, 8 December 2010). The Pilot in Command, Captain Richard de Crespigny (15,000hrs) wrote, *"The explosion followed by the frenetic and confusing alerts had put us in a flurry of activity, but Matt* [Matt Hicks, First Officer, 11,000hrs] *and I kept our focus on our assigned tasks while I notified air traffic control … 'PAN PAN PAN, Qantas 32, engine failure, maintaining 7400 and current heading'"… "We had to deal with continual alarms sounding, a sea of red lights and seemingly never-ending ECAM checklists. We were all in a state of disbelief that this could actually be happening."* (21 July, 2012). Subsequently, Captain de Crespigny stated, *"At the point of maximum stress, the cockpit displays didn't make a whole lot of sense"* (Pasztor, 27 June, 2013).

Rewind to 1979

Over thirty years prior to QF32, the Three Mile Island (TMI) partial nuclear meltdown in 1979 was perhaps the first major illustration of the alarm problem. The Report of the President's Commission on the accident stated, *"During the first few minutes of the accident, more than 100 alarms went off, and there was no system for suppressing the unimportant signals so that operators could concentrate on the significant alarms. Information was not presented in a clear and sufficiently understandable form; for example, although the pressure and temperature within the reactor coolant system were shown, there was no direct indication that the combination of pressure and temperature meant that the cooling water was turning into steam. Overall, little attention had been paid to the interaction between human beings and machines under the rapidly changing and confusing circumstances of an accident"* (p. 11). A shift supervisor testified that there had never been fewer than 52 alarms lit in the control room. The computer printer registering alarms was running more than 2 hours behind the events. Similar to de Crespigny's remark above, the TMI control room operator Craig Faust recalled for the Commission his reaction to the incessant alarms: *"I would have liked to have thrown away the alarm panel. It wasn't giving us any useful information".* The accident triggered a flurry of human factors/ergonomics (HF/E) activity.

Many other accidents have featured alarm handling since then, including the Texaco explosion and fires (Milford Haven, UK, 1994) and the Channel Tunnel fire (1996). In the UK, official investigations have found significant deficiencies in alarm handling (see Health and Safety Executive, 2000). Alarm flooding, poorly prioritised

alarms and 'clumsy automation' have prevented users from detecting important alarms, understanding the system state, and reacting in a directed and timely manner. While alarm systems are one of the most essential and important interfaces between human operators and safety-related processes, they can also be one of the most problematic.

In CNS/ATM, alarms are currently most prevalent in system control. Typically, an integrated, centralised control and monitoring system (CMS) is used to monitor and control engineering systems within an ATC centre. Engineers monitor alarms from dedicated workstations, and remedy faults either remotely (via software) or locally. The tasks of a system controller currently have little overlap with air traffic controllers, but with increases in automation, the line between the functions will begin to fade. The complexity and criticality of systems will mean that we all need to pay more attention to the HF/E needs of CNS, and also to the alarms that are likely to migrate to the ATM environment.

Alarm design 101

The purpose of alarms is to direct the user's attention towards significant aspects of the operation or equipment that require timely attention. Much has been written on good practice for alarm management. The Engineering Equipment and Materials Users Association (EEMUA) (1999) summarise the characteristics of a good alarm as follows:

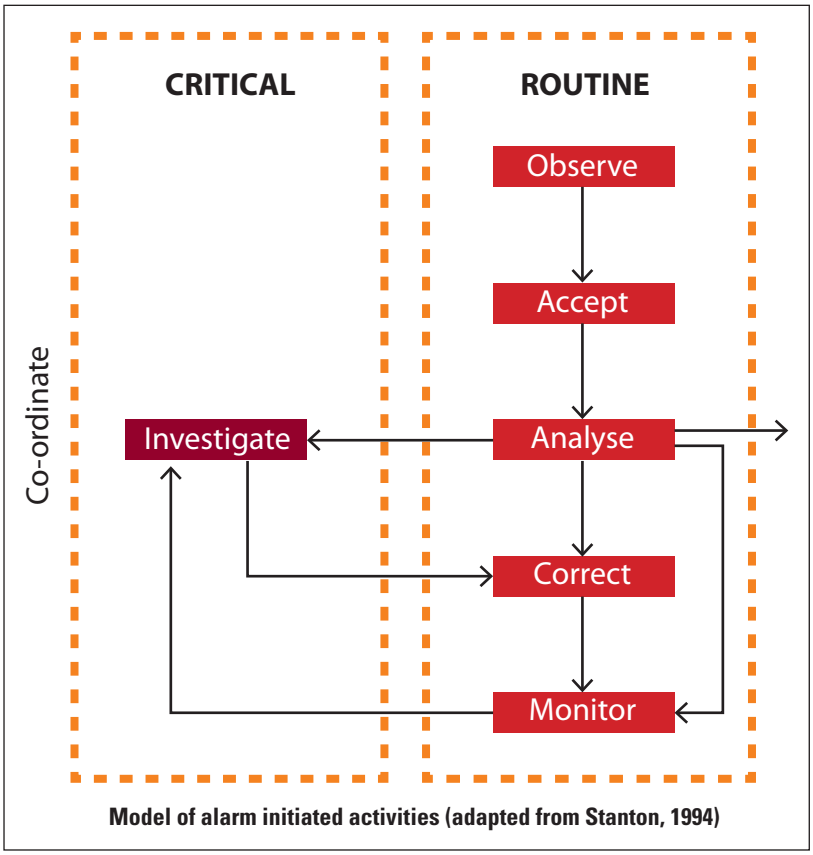
- **Relevant** – not spurious or of low operational value.
- **Unique** – not duplicating another alarm.
- **Timely** – not long before any response is required or too late to do anything.
- **Prioritised** – indicating the importance that the operator deals with the problem.
- **Understandable** – having a message that is clear and easy to understand.
- **Diagnostic** – identifying the problem that has occurred.
- **Advisory** – indicative of the action to be taken.
- **Focusing** – drawing attention to the most important issues.

These characteristics are not always evident in alarm systems. Even when individual alarms may seem 'well-designed' they may not work in the context of the system as a whole and the user's activity.

This article raises a number of questions for consideration in the design of alarm systems, framed in a model of alarm-handling activity. The questions may help in the development of an alarm philosophy (one of the first steps in alarm management), or in discussion of an existing system. The principles were originally derived from evaluations of two different control and monitoring systems for two ATC centres (see Shorrock et al, 2001). These evaluations used an exhaustive HMI guidelines database (MacKendrick, 1998; Shorrock, et al. 2001). The guidelines that were relevant to alarm handling, and put into context by the evaluations, were extracted and grouped to help form preliminary principles. In parallel, a model of alarm-initiated activities (Stanton, 1994) was used to group and form the final set of principles. The resultant principles are included in this article as questions for consideration, structured around six alarm-handling activities (Observe, Accept, Analyse, Investigate, Correct, and Monitor). This is illustrated and outlined below.

Understanding alarm initiated activities

Observation is the detection of an abnormal condition or state within the system (i.e., a raised alarm). At this stage, care must be taken to ensure that coding methods (colour and flash/blink, in particular) support alarm monitoring and searching. Excessive use of highly saturated colours and blinking can de-sensitise the user and reduce the attention-getting value of alarms. Any use of auditory alarms should further support observation without causing frustration due to the need to accept alarms in order to silence the auditory alert, which can change the 'alarm handling' task to an 'alarm silencing' task.



Model of alarm initiated activities (adapted from Stanton, 1994)

DR STEVEN **SHORROCK**

is Project Leader, Safety Development at EUROCONTROL and the European Safety Culture Programme Leader. He is a Registered Ergonomist and a Chartered Psychologist with a background in practice and research in safety-critical industries. Steve is also Adjunct Senior Lecturer at the University of New South Wales, School of Aviation.

Acceptance is the act of acknowledging the receipt and awareness of an alarm. At this stage, user acceptance should be reflected in other elements of the system that is providing alarm information. Alarm systems should aim to reduce user workload to manageable levels; excessive demands for acknowledgement increase workload and unwanted interactions. For instance, careful consideration is required to determine whether cleared alarms really need to be acknowledged. Group acknowledgement of several alarms (e.g. via using 'click-and-drag' or a Shift key) may lead to unrelated alarms being masked in a block of related alarms. Single acknowledgement of each alarm, however, can increase workload and frustration, and an efficiency-thoroughness trade-off can lead to alarms being acknowledged unintentionally as task demands increase. It can be preferable be to allow acknowledgement for alarms for the same system.

Analysis is the assessment of the alarm within the task and system context, leading to the prioritisation of that alarm. Alarm lists can be problematic, but, if properly designed, they can support the user's preference for serial fault or issue management. Effective prioritisation of alarm list entries can help users at this stage. Single 'all alarm' lists can make it difficult to handle alarms by shifting the processing debt to the user. However, a limited number of separate alarm lists (e.g., by system, function, priority, acknowledgement, etc.) can help users to decide whether to ignore, monitor, correct or investigate the alarm.

Investigation is any activity that aims to discover the underlying factors order to deal with the fault or problem. At this stage, system schematics or other such diagrams can be helpful. Coding techniques (e.g., group, colour, shape) again need to be considered fully to ensure that they support this stage without detracting from their usefulness elsewhere. Displays of system performance need to be designed carefully in terms of information presentation, ease of update, etc.

Correction is the application of the results of the previous stages to address the problem(s) identified by the alarm(s). At this stage, the HMI must allow timely and error-tolerant command entry, if the fault can be fixed remotely. For instance, any command windows should be easily called-up, user memory demands for commands should be minimised, help or instructions should be clear, upper and lower case characters should be treated equivalently, and positive feedback should be presented to show command acceptance.

Monitoring is the assessment of the outcome of the Correction stage. At this stage, the HMI (including schematics, alarm clears, performance data and message/event logs) needs to be designed to reduce memory demand and the possibility of interpretation problems (e.g., the 'confirmation bias').

Additionally, in multiple-user systems, co-ordination between operators is required to work collaboratively to attend to system problems. This may involve delegating authority for specific issues to colleagues, or co-ordinating efforts for problems that permeate several different parts of the overall system.

The design questions for each stage of alarm handling are shown in the table. In most cases, questions are applicable primarily in one stage of alarm handling, but also have a bearing on other stages, depending on the system in question. The questions are therefore shown in terms of their primary relevance within the model, but may be considered against other stages.

QF32 and you

The QF32 crew were overwhelmed at every stage of the model of alarm initiated activities described above. But their experience, competence and ingenuity meant that they were able to take control of the aircraft, not by getting caught up in an alarm flood, but by focusing on what was working. They had to take the initiative and adjust their performance in a way that was never previously imagined, as alerts became unusable. Sometimes, system complexity makes it near-impossible to imagine some forms of emergent system behaviour. When he was asked if he had any recommendations for Qantas or Airbus concerning training for ECAM messages in the simulator, David Evans responded, *"We tried to recreate it in the sim and we can't! I think it was just such an extraordinary day"* (Robinson, 8 December 2010). Our inability to specify systems perfectly, or to train for every single eventuality, is one reason why we need highly competent people in control. But the goal is well-designed systems supporting highly competent people, not highly competent people working around systems that fail to meet their needs.

Will alarms ever be as critical in CNS/ATM as they are in the cockpit or control room? It's hard to say, but one thing is for sure, ATM will see more alarms, and CNS is already well on the road. With regard to the issues that have been known for over 30 years in other industries, prevention is better than cure. As the experts in your work, you need to be involved in the design of alarm systems from the beginning, and at every stage. And remember that, fundamentally, human factors/ergonomics is about design, not accidents. So demand competent HF/E design expertise, and a user-centred design process. Understanding the nature of alarm handling, and the associated design issues, can help you – the field expert – to be a more informed user, helping to bring about the best systems to support your work.

References

- de Crespigny, R. (July 21, 2012). This is your captain speaking. *The Australian*. EEMUA (1999). *Alarm Systems: A Guide to Design, Management and Procurement*. EEMUA Publication No. 191. The Engineering Equipment and Materials Users Association: London.
- Health and Safety Executive (2000). *Better Alarm Handling*. HSE Information Sheet - Chemicals Sheet No. 6. March, 2000. See http://www.hse.gov.uk/humanfactors/topics/alarm-management.htm
- Kemeny, J.G. (Chairman) (1979). *President's Commission on the Accident at Three Mile Island*. Washington DC.
- MacKendrick, H. (1998). *Development of a Human Machine Interface (HMI) Guidelines Database for Air Traffic Control Centres*. R & D Report 9822. National Air Traffic Services Ltd.: London.
- Pasztor, A. (June 27, 2013). How Pilot Brought In Crippled Superjumbo. *The Wall Street Journal*.
- Robinson, R. (8 December 2010). EXCLUSIVE - Qantas QF32 flight from the cockpit. Royal Aeronautical Society. http://bit.ly/1LjECi1
- Shorrock, S.T., MacKendrick, H. and Hook, M., Cummings, C. and Lamoureux, T. (2001). The development of human factors guidelines with automation support. *Proceedings of People in Control: An International Conference on Human Interfaces in Control Rooms*, Cockpits and Command Centres, UMIST, Manchester, UK: 18 - 21 June 2001.
- Shorrock, S.T. and Scaife, R. (2001). Evaluation of an alarm management system for an ATC Centre. In D. Harris (Ed.) *Engineering Psychology and Cognitive Ergonomics: Volume Five - Aerospace and Transportation Systems.* Aldershot: Ashgate, UK.
- Shorrock, S.T., Scaife, R. and Cousins, A. (2002). Model-based principles for human-centred alarm systems from theory and practice. Proceedings of the *21st European Annual Conference on Human Decision Making and Control*, 15th and 16th July 2002, The Senate Room, University of Glasgow.
- Stanton, N. (1994). Alarm initiated activities. In N. Stanton (Ed.), *Human Factors in Alarm Design*. Taylor and Francis: London, pp. 93-118.

FIT FOR PURPOSE? **QUESTIONS TO ASK ABOUT ALARM SYSTEM DESIGN**

This checklist may help to inform an alarm philosophy or an informal exploration of an alarm system from the viewpoint of user activity. It should be possible to answer 'Yes' to most questions that are applicable. The questions may be useful in discussions involving users, designers and other relevant stakeholders.

Observe	Yes	No	N/A
1. Is the purpose and relevance of each alarm clear to the user?			
2. Do alarms signal the need for action?			
3. Are alarms presented in chronological order, and recorded in a log (e.g. time stamped) in the same order?			
4. Are alarms relevant and worthy of attention in all the operating conditions and equipment states?			
5. Can alarms be detected rapidly in all operating (including environmental) conditions?			
6. Is it possible to distinguish alarms immediately (i.e., different alarms, different operators, alarm priority)?			
7. Is the rate at which alarm lists are populated manageable by the user(s)?			
8. Do auditory alarms contain enough information for observation and initial analysis, and no more?			
9. Are alarms designed to avoid annoyance or startle?			
10. Does an indication of the alarm remain until the user is aware of the condition?			
11. Does the user have control over automatically updated information, so that information important to them at any specific time does not disappear from view?			
12. Is it possible to switch off an auditory alarm independent of acceptance, while ensuring that it repeats after an appropriate period if the problem is not resolved?			
13. Is failure of an element of the alarm system made obvious to the user?			
Accept			
14. Has the number of alarms that require acceptance been reduced as far as is practicable?			
15. Is multiple selection of alarm entries in alarm lists designed to avoid unintended selection?			
16. Is it possible to view the first unaccepted alarm with a minimum of action?			
17. In multi-user systems, is only one user able to accept and/or clear alarms displayed at multiple workstations?			
18. Is it only possible to accept an alarm from where sufficient alarm information is available?			
19. Is it possible to accept alarms with a minimum of action (e.g., double click), from the alarm list or mimic?			
20. Is alarm acceptance reflected by a change on the visual display (e.g. visual marker and the cancellation of attention-getting mechanisms), which prevails until the system state changes?			
Analyse			
21. Does alarm presentation, including conspicuity, reflect alarm priority with respect to the severity of consequences of delay in recognising the problem?			
22. When the number of alarms is large, is there a means to filter the alarm display by appropriate means (e.g. sub-system or priority)?			
23. Are users able to suppress or shelve certain alarms according to system mode and state, and see which alarms have been suppressed or shelved? Are there *means to document the reason for suppression or shelving?			
24. Are users prevented from changing alarm priorities?			
25. Does the highest priority signal always over-ride, automatically?			
26. Is the coding strategy (colour, shape, blinking/flashing, etc) the same for all display elements?			
27. Are users given the means to recall the position of a particular alarm (e.g. periodic divider lines)?			
28. Is alarm information (terms, abbreviations, message structure, etc) familiar to users and consistent when applied to alarm lists, mimics and message/event logs?			
29. Is the number of coding techniques at the required minimum? (Dual coding [e.g., symbols and colours] may be needed to indicate alarm status and improve analysis.)			
30. Can alarm information be read easily from the normal operating position?			
Investigate			
31. Is relevant information (e.g. operational status, equipment setting and reference) available with a minimum of action?			
32. Is information on the likely cause of an alarm available?			
33. Is a usable graphical display concerning a displayed alarm available with a single action?			
34. When multiple display elements are used, are individual elements visible (not obscured)?			
35. Are visual mimics spatially and logically arranged to reflect functional or naturally occurring relationships?			
36. Is navigation between screens, windows, etc, quick and easy, requiring a minimum of user action?			
Correct			
37. Does every alarm have a defined response and provide guidance or indication of what response is required?			
38. If two alarms for the same system have the same response, has consideration been be given to grouping them?			
39. Is it possible to view status information during fault correction?			
40. Are cautions used for operations that might have detrimental effects?			
41. Is alarm clearance indicated on the visual display, both for accepted and unaccepted alarms?			
42. Are local controls positioned within reach of the normal operating position?			
Monitor			
43. Is the outcome of the Correction stage clear to the user? (A number of questions primarily associated with observation become relevant to monitoring.)			
Co-ordinate			
44. Are shared displays available to show the location of operators in system, areas of responsibility, etc?			