Alarm Management Strategies on Ships Bridges and Railway Control Rooms, A Comparison of Approaches and Solutions

Paul Traub - CCD Design and Ergonomics & Ralph Hudson - BMT Defence Services Limited

Key Words: Alarms, Alarm Management, Alarm Flooding and Human Factors Integration

Shipborne systems and railway control rooms share many similarities with respect to alarms. Historically, these operating environments have seldom taken full advantage of a systematic approach to alarm management. As a result, operators continue to complain of additional workload, stress, alarm flooding and masking caused by excessive numbers of unnecessary, spurious or repetitive alarms, leading to difficulties in identifying the true priority for an alarm. At a basic level alarms must identify the status of systems and indicate to the operator what needs to be done and the urgency of the failure. Current management of alarms and associated display technology does not adequately address this issue.

Traditional solutions to excessive alarms have advocated the use of automation and/or the delegation of an alarm to another person. This is not the panacea to alarm management and in some cases cause more problems than it can solve. For example, alarm suppression for non-critical alarms (with similar tonal qualities) can become an automated human response whereby the operator inadvertently suppresses critical alarms. Delegating alarms to other people (rather than eliminating the problem) can shift the problem elsewhere Ships normally perform a variety of tasks under a wide range of operating conditions, so a minor alarm in one operating state may be critical in another. Attempts to specify alarms more carefully can reduce the volume of unhelpful alarms but may also justify additional ones.

There are grounds for arguing that it is more realistic to help the operators prioritise the information they need rather than trying to filter out the alarms in the first place. This principle points to an ongoing need for much improvement in alarm management strategies, display presentation and novel display techniques.

This paper compares and contrasts alarm management approaches from rail and maritime sectors and seeks to distil best practice from both industries for application to robust, usable and pragmatic alarm management for these hazardous environments.

Introduction

Despite the ever increasing sophistication of modern automation systems, operators continue to report that they can be inundated with alarms that are unnecessary, redundant or generated in excessive numbers. Widespread attention to the issue across several industries has served only to re-emphasise the importance of alarm management whilst confirming that, in many cases, the problem still remains.

High numbers of alarms hinder thought processes and make it difficult for operators to respond effectively. Spurious and irrelevant alarms also distract operators from their tasks and can result in high priority alarms being ignored. This paper provides an assessment, focused mainly on the marine and rail industries, of why alarm management remains a challenge and advocates a

structured approach that helps resolve alarm management issues from the earliest stages of the design process.

Management of alarms is not helped by the continuing proliferation of differing terminologies across and within industries. The rail industry has both alarms and alerts and can have inconsistent definitions of alarm priorities. In the Royal Navy, alarms and warnings have separate definitions within the general term alert. This paper adopts a common civil marine practice and refers simply to 'alarms', leaving readers to associate different priorities of alarm with their own practices.

Aim

The aim of this paper is to compare progress and alarm management strategies in the rail and marine industries and to identify, in particular, how recent lessons in the rail industry can contribute to further improvements in the management of marine alarms.

The paper distils lessons of common interest and offers recommendations for robust and pragmatic alarm management within these potentially hazardous transport environments.

Context

Despite the sophistication of modern automation systems, and systems technology, alarms continue to be generated in unwelcome numbers. Significant investment in the aerospace world and specialised solutions in the process industries have illustrated the potential to make progress in managing alarms. However, the marine and rail industries have seldom attracted the same levels of funding and still face up to some underlying challenges:

- Modern control systems are often network based, highly integrated and may comprise several thousand parameters, many of which may be capable of generating alarms, particularly for major incidents. Some signalling centres, for example, have over 20 specific alarms, but when variants of the alarm are included amount to a potential of over 100 alarms that a signaller may receive.
- The trend towards lower manning levels continues and the associated increase in the level of automation does not necessarily reduce the number of alarms (under normal, abnormal and degraded modes), nor does it necessarily reduce the stress levels experienced for extreme or unusual incidents. Decision making aids can reduce but not eliminate the uncertainty and pressure in such situations.
- The more extreme failures, which in most environments will happen less than once a year, involve the interaction of multiple factors that few automation systems can resolve. At Ladbroke Grove [1], for example, the driver was able to over-ride the Automatic Warning System and pass the signal set at danger.
- Even if the automated response to an incident wins time for the operators to respond, (a hands-off strategy exploited effectively by the nuclear and process industries), the operators must still interpret (and in some cases prioritise) the alarms and other information presented to resolve a recovery path. Whether or not the initial response is hands-off, the marine or rail operators still have to identify a way ahead within a dynamic and unpredictable operating environment.

- The growth in system functionality has not been matched by equivalent regulation of functions and their associated alarms and there remain widespread disparities in terminology and alarm management practice.

Rail Sector Issues

In the rail sector, alarm management has been heavily influenced by the Cullen Enquiry recommendations [1] into the accident at Ladbroke Grove. Prior to the Cullen Enquiry there were no formal requirements for the design of safety critical alarms within signalling control centres and it was often difficult for signallers to diagnose alarm information and respond rapidly to a Signal Passed At Danger (SPAD). Some alarms were routinely activated up to 60 times an hour and were not prioritised. On the trains themselves, drivers have several possible sources of alarms, including:

- Automatic Train Protection.
- Automatic Warning Systems.
- Drivers Reminder Appliance.
- Train Protection and Warning System.

Historically, accidents tended to be blamed on driver error, however unjustly. Signalling was, and often still is, controlled by small local signal boxes with few alarms. However, signalling is now migrating to larger Signalling Control Centres where there may be as many as 27 signallers on duty. Signallers will often have a greater area of control, a higher volume of rail traffic and a higher workload to deal with than their predecessors.

Today's signalling systems have collision avoidance systems akin to those used in Air Traffic Control. They tend to rely on a limited number of operator based safety critical functions which are supported by Solid State Interlocking to prevent the routing of trains on collision paths. Signalling centres have alarms associated with these functions as well as other alarms. Typical alarms (which also have variants within them) include:

- Signal Passed at Danger (SPAD).
- Track circuit failure.
- Axle counter failure.
- Tunnel flooding.
- Trip wire detection.
- Automatic Route Setting failure.
- Lamp filament failure.

With the exception of SPAD alarms, their prioritisation can vary and the temptation to make them all high priority must be avoided. They may simply indicate non-critical events or that systems are restoring themselves to normal. The advent of signalling control centres, with up to 30 workstations and over 100 audible alarms (when variants are included) has forced the rail industry to review its alarm management process and alarm specification.

Formal requirements to integrate human factors into the design of signalling control centres have been mandated for some time but there are now additional requirements for an 'Alarm Management Design Document' that establishes a structured approach for alarm management based on the following steps:

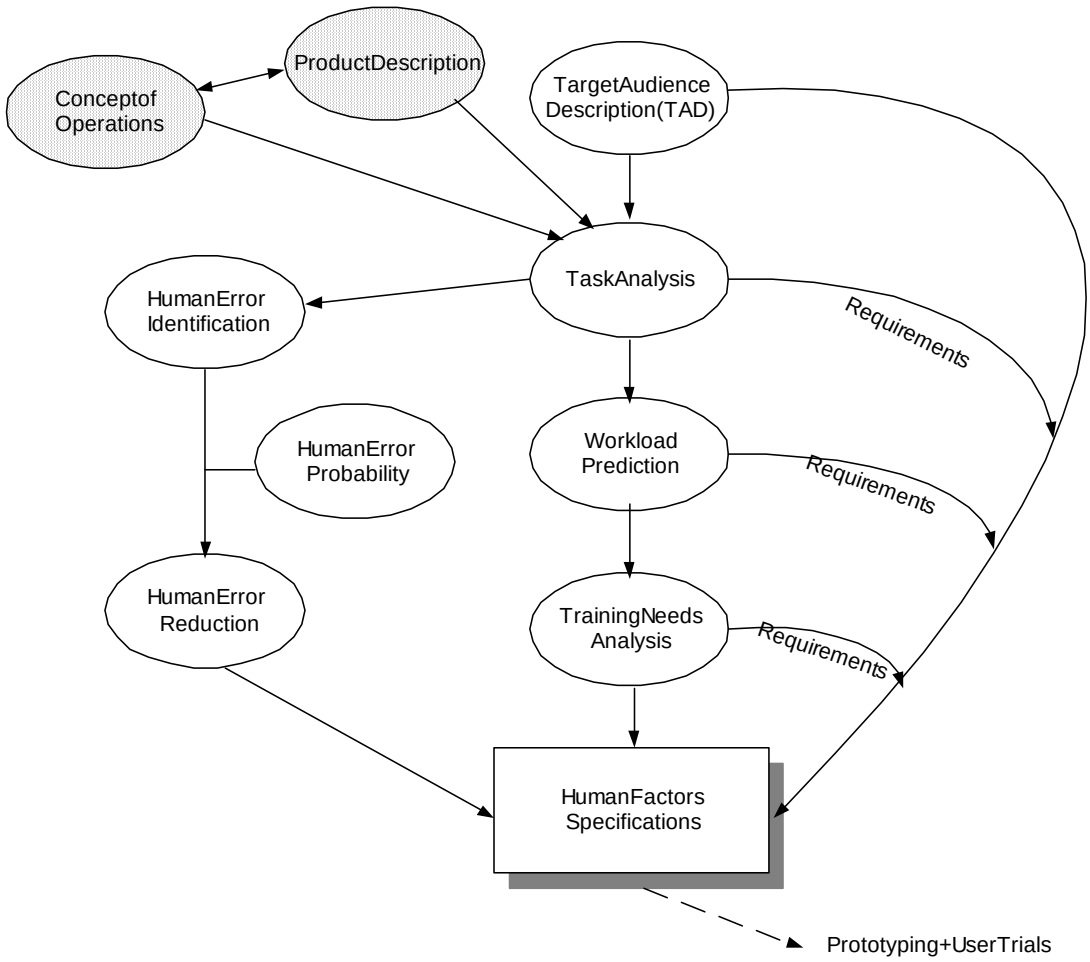
- Identify systems that can generate alarms.
- Consult with users to identify individual alarms that can be generated.
- Establish the intended recipient of each alarm, including an assessment of the associated maintenance and support processes.
- Prioritise alarm categories based upon their severity and consequences.
- Develop a concept for alarm management via the user interface.

These phases are broadly in alignment with those advocated by the Draft Network Rail Company Specification on Alerts Systems Design [2] with the addition of two further steps as follows:

- Test user interface concepts and alarm assumptions with representative signalers;
- If satisfactory continue to verify and test assumptions until implementation.

The associated human factors integration process is summarised at Figure 1.

Figure 1 Summary High Level HFI Design Process



The management of alarms in railway signalling centres is being made more robust by covering, as a minimum, the parameters at Table 2.

Table 1 Scope of Alarm Management Parameters for Railway Alarm Systems

Alarm Source	Alarm Class	Specific Alarms/Warning	How Generated	Recipient	Purpose	Priority Level	How Presented (Alarm)	Acknowledgement (Yes or NO)	False alarm rate issues	Proposed Mitigation

For this process to be successful, user involvement is paramount. Network Rail advocates that users contribute to the production of an alarm management plan and Her Majesty's Railway Inspectorate assesses the degree of user involvement in the process of eliciting design requirements for the safety case before accepting the resulting design.

Alarm management must therefore be addressed in a structured, systematic and auditable manner with full stakeholder involvement from the start.

Marine Sector Comparisons

For military and commercial vessels alike, significant progress has been made in recent years to both streamline and enhance the management of alarms. High levels of automation are available to enable lean manning levels and marine projects are, or should be, used to the challenge of matching the level of automation to operator tasking and providing an appropriate alarm management environment.

The suppliers of military Platform Management Systems (PMS) and the equivalent automation systems in the civil marine can take credit for improved exploitation of modern, windows based displays to provide the operators with the information they need in efficient formats. In common with the rail industry, however, there is scope to introduce a more structured approach to the incorporation of alarm management within the specification process as the operators still do not see the distinct improvement they have long called for.

Alarm suppression is an example of a well established technique that could be applied more effectively by earlier attention within the project life cycle. Automatic or manual inhibits are used to over-ride alarms that would otherwise be generated by routine events such as the deliberate shutting down of a generator. If the inhibits to be applied are not identified by the operator in good time, or if a limited alarm suppression capability is specified in the first place, ships will enter service with a source of unnecessary alarms that may be difficult or time consuming to inhibit once at sea.

As recognized in the rail industry, the prioritisation of alarms into clearly defined bands could be further improved. There is a trend to replace the use of two alarm levels ('alarm' and 'warning' in the Royal Navy) with 3 levels (such as the 'warnings', 'cautions' and 'advisory' alarm levels of military aviation), allowing the top level to be reserved for critical alarms, the second for alarms that justify fast operator intervention to pre-empt a critical situation and the third for alarms for which a slower response can be justified. By no means a new issue, there is clearly scope to achieve useful standardisation across marine and rail transport sectors.

However much progress is made in these areas, it still remains difficult for operators to identify what is most important to them and to subsequently track and monitor related events. In particular, the definition of alarms and their presentation to the operators should identify where

normally minor alarms can have major consequences. Highly automated protection can lead operators into a false sense of security (complacency caused by undue trust in the automation), tempting the assumption that all major problems are covered by the automation. There is scope to help operators identify the indirect implications of an alarm by flagging them as having particular significance. Similarly, more flexible navigation within the automation system would allow operators to cross-check related indications without the need for special decision aids.

It is important to select carefully the information made available to the operators. Modern systems with embedded control generate large amounts of data, both for the manufacturer's own use and for the control and monitoring needs of the ship's plant. If too many parameters are monitored, the operators will be swamped with unnecessary indications and alarms. If too little information with respect to alarms is imparted to the operator, the manufacturer may reject liability for major equipment failure on the grounds that more comprehensive monitoring could have pre-empted the associated fault.

Selection of the appropriate data for alarm monitoring is also an important part of the wider integration process. Modern systems with embedded control systems can be expected to operate reliably and efficiently but there is no guarantee that interaction with other systems will not lead to unacceptable failure modes. The associated hazard and failure mode analysis that should identify such problems must also inform the alarm specification process so that operators cannot be left unaware of incompatible operation between otherwise healthy systems.

Another factor which points to a need for further improvement is the need for efficient recovery after a significant plant failure. In general, modern automation systems incorporate high levels of plant protection. For example, the automatic response to an electrical fault will cause breakers to trip in milli-seconds. The plant will usually be brought to a safe state without operator intervention. Unfortunately, it is the recovery process that may take some considerable time and a vessel with tugs standing by pays a heavy price for unscheduled delays. The operators, however, are often left with hundreds of alarms to filter, interpret and then address after a major failure, making it difficult to identify the original cause of the problem and then focus on the key information that will enable them to recover normal operation. Any provision within the automation system for the efficient filtering out of irrelevant information and for improved links between alarms and recovery related information should therefore be actively considered.

Automation and Alarm Management

Lower manning levels, higher levels of automation and more capable alarm management are all intimately linked, as exemplified by modern integrated bridges. Although they have a range of navigational decision aids, support systems and "smart automation" to help them on the bridge, mariners are exposed to an increasing diversity of supervisory and decision making tasks. Their attention is often divided between primary navigation displays and secondary tasks such as engine and cargo functions. Automated collision avoidance systems are able to monitor increased numbers of vessels and reduce the computational load on the bridge watchkeepers but also demand more interpretive skills and deeper technical knowledge of the support systems provided.

Precisely the same parallels exist in the rail sector. Signallers must assist in not only routing of trains, but timetabling, liaison and management of the railway with other stakeholders (such as freight and passenger trains, and trackworkers). They also have a plethora of other systems to monitor and respond to that have safety and performance related tasks associated with them.

Where automation is unsatisfactory in any industry, this is often because it is specified without the careful consideration of human capabilities and limitations. The addition of each automated

system further increases the number of sub-systems that a human operator must monitor and that could potentially fail. For example the addition of a single automated system can result in the need for the operator to monitor:

- The automated function itself.
- The status and health of the automated system.
- The automatic or manual selection of operating modes and configurations.

If operator skills, tasking, workload and quality of life are not addressed early in the design process, operators may find that their specified role is limited to monitoring the automation and only intervening when it fails. Without the skills or experience to address the failure, automation induced operator errors will occur. Even if such a pitfall is avoided, a high standard of training is essential as operators must understand both the automation itself and the underlying principles of the plant. Sooner or later, operators will find themselves operating the plant under emergency conditions when the automation has failed. It is exactly at these peaks of operator workload that cascades of unhelpful alarms will occur.

It is relatively easy to reduce the physical and mental workload of operators under normal conditions but it is more difficult to ensure that automation ensures an acceptable workload and enhances overall ship safety under the full range of failure conditions. It is not yet fully understood how to minimise the serious peaks in workload and associated stress when the automation is suddenly degraded. However, when automation is used as mitigation it must be matched to the tasks required of the operator under all normal, abnormal and degraded modes of operation.

Human-automation interaction requires a human to make a judgment in parallel with an automated system, and then to perceive, consider, accept or reject the automated output as appropriate. A couple of rail incidents provide useful examples of automation induced failures:

Notre Dame de Lorette (Line 12), Paris, France (30 August 2000) – A southbound train was derailed and overturned on a tight curve at the entry to Notre Dame de Lorette station injuring 24 people. The first car of the train skidded into the station and overturned, stopping 1 metre short of a stationary train in the opposite platform. The train was being manually driven due to a failure of the automatic piloting system and the cause of the accident was put down to driver error brought about by the lack of familiarity with manual operation.

Shady Grove Passenger Station (January 6th, 1995) -A collision between a Washington Metropolitan Area Transit Authority Train with a standing freight train at Shady Grove Passenger Station in Maryland was attributed to the automation. In the moving train, braking was an automated function and the driver had no direct manual control over the braking force applied. The accident occurred during icy weather for which the automatic braking system was not correctly programmed. The driver was killed and the damage to property was estimated at over 2 million dollars.

Although seldom appreciated directly, at the heart of any automation strategy is the need to strike the correct balance between trusting the system to fulfill its purpose and knowing when not to trust it. Mistrust (interference) and over-trust (complacency) of safety critical automated systems have been causes of numerous human error induced accidents in high hazard industries. Some illustrative examples are provided in the following table.

Table 2 Alarm and Automation Design Issues

Alarm and Automation Issue	Rail Specific Example	Marine Specific Example
Nuisance Communications	Multiple messages and tones for the recovery of non-critical systems.	Limited alarm suppression.
Excessive False Alarm rates	Track circuit alarms going off during possessions (when the railway is closed to traffic)	Ineffective alarm 'hysteresis' bands for rough seas.
Effect of increased monitoring load attributable to use of automation	Restoration of Axle Counters providing additional alarms during an automated process. Alarms activate whether or not the automatic system itself is in service. .	Heating, Ventilation and Air Conditioning (HVAC) plants tend to generate high numbers of alarms because of their distributed configuration.
Effect of component proliferation and system complexity caused by automation	Up to 8 alarm variants in relation to failures, recovery and status of an automated system	Daggri 2005-Master and Mate did not make full use of the integrated bridge system because they were unfamiliar with its features and therefore its capabilities and options [3]
Trust (overtrust and mistrust) of automation and the impact on human error	Not really applicable to signalling but has occurred with train drivers. For example, drivers canceling the Automatic Warning System when the next signal is red. Failure of Automatic Route Setting, resulting in sudden peaks in signaller workload	Royal Majesty 1995, Grounding caused by the watch officers over-reliance on the automation features of the integrated bridge system [4]
Safety implications of different automation modes	During handbacks of possessions, some alarms may be disabled. Handover process is very robust to address the automation issue	Crown Princess misalignment between auto-pilot and steering system.

Table 3 demonstrates that automation is never a panacea in either rail or maritime sectors. A human centred design process will ensure that scenario analysis is used to check the operators' expectancies as well as their intended tasking. Potential changeovers from supervisory to manual operating modes must be addressed if the alarm management is to help rather than hinder the process.

Strategy for Addressing Alarms in Rail and Maritime Sectors

From the alarm management perspective, this paper argues that automation should not be a blunt instrument that makes matters worse. A structured and focused approach to alarm management will integrate the human element into its core process and is likely to incorporate the representative and proven elements of the strategy below:

1. Identify scenarios and human tasks (task analysis) in relation to alarms (including normal, abnormal and degraded modes of operation).
2. Identify each alarm source – take user advice to identify the alarms required.
3. Assign alarm prioritisation levels based on severity and consequences, then refine with user consultation.
4. Produce an alarm functional model.
5. Establish the intended recipient of each alarm (and associated maintenance and support processes).
6. Develop a concept of how alerts will be incorporated into the user interface. Consider display formats that reflect operator thought processes as well as system architectures.
7. Assess if decision aides or smart automation can assist with alarm management.
8. Conduct a rigorous assessment of whether proposed decision aids will be effective for the anticipated modes of operation.
9. Test user interface concepts with the users themselves.
10. Conduct human workload assessments for parallel tasks.
11. If satisfactory, continue to verify and test assumptions until implementation.

Stage 6 is one of the key steps as it will ultimately define the requirements for managing alarms.

The process of implementing effective alarm management is not a simplistic task and should be conducted by a team that brings together the expertise of those that understand the system constraints, human factors specialists and the operators themselves. The process must be human centric and is generally referred to as Human Factors Integration.

The Potential for More Advanced Design

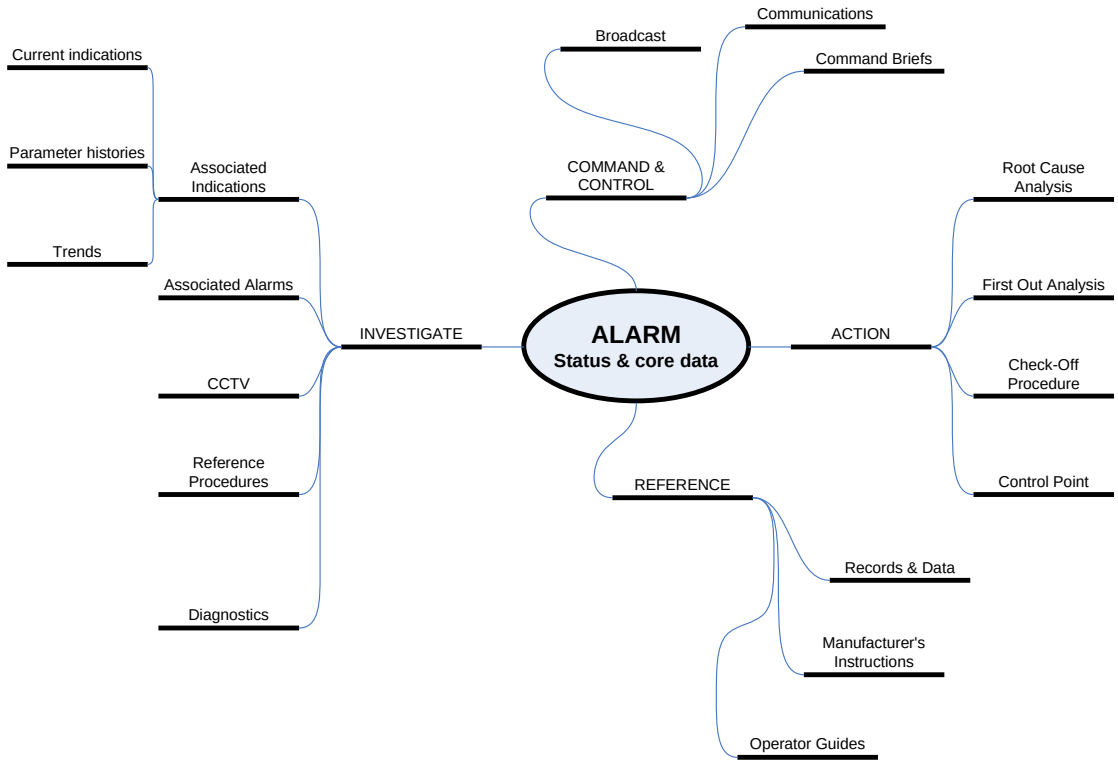


Figure 2 Alarm Response Options for the Operator

Figure 2 identifies some of the key responses that an operator may be expected to make in response to an alarm and that might influence the configuration of a dedicated alarm display. This is akin to a human factors task analysis and in effect is a human centered design process that has elicited alarm design requirements. The central ellipse represents the data that applies to any alarm, such as current value, set level and time of activation. The operators would expect to have immediate access to this information from the relevant alarm icon or menu, whatever type of display page is on view when the alarm is generated.

It is the operator that must decide how to respond to the alarm. Some alarms may require immediate action and, particularly for critical alarms, there may be mandatory procedures to follow. The use of an advanced display would allow operators to follow a direct link to the appropriate procedure or check-off list. This would allow rapid diagnostics of the alarm source and the associated operator actions required. There could also be a link to a system page containing the controls most likely to be needed for the response.

If the automation system within the advanced display has a synchronized clock reference to time stamp each event at source, operators will be able to identify events in their true order of occurrence. Multiple breaker trips, for example, need to be resolved to within a few milli-seconds to identify the original, or 'first out', tripping event.

Finally, there could be direct link to decision aids associated with the anticipated need for operators to act quickly. Such a decision aid might provide 'root cause analysis' that senses the changes of state within the system and applies logic to offer, in priority order, the most likely causes. Historically, such decision aids have often offered poor value for money in the marine industry because significant effort is needed to analyse the many combinations of trips that may occur across the operating modes a ship's plant will undergo at sea and in harbour. In some cases, there may be too many variables for decision aids to be able to solve the problem at all. Operators, in any case, seldom call for such support, preferring to be given the relevant, uncluttered information they need to make their own decisions.

For many alarms, the operator response to the alarm need not involve direct action. Investigation of the cause of the alarm may be appropriate, either to make the operator fully aware of the situation or to eliminate options before taking action. A single smoke detector alarm, for example, will be examined before direct fire suppression is initiated. In determining the appropriateness of the design a human task analysis should be undertaken.

To help the operators conduct the relevant investigation, the alarm can be linked to information such as associated plant indications, related alarms, CCTV monitors and diagnostics. This information should be elicited from operators themselves. In a modern automation system, the history and trends for each parameter should be readily available and a well configured alarm display would allow the operators to focus immediately on those that relate to the alarm of interest.

The design of the advanced display could aid operator performance by offering 'reference' links that would give the operators easy reference to background data, supporting documentation and other information that would help them resolve the situation.

Conclusion

In both the maritime and rail sectors there is scope to enhance alarm management processes by the more structured incorporation of human factors from the early stages of the design process.

Situations will continue to arise that generate large numbers of alarms and operators must be given the support and tools they need to apply their skills and judgement under all operational conditions.

Effective human factors integration will ensure that the initial design process develops requirements incorporating the concept of operations, tasking and associated skill levels. These requirements develop further and support a robust audit trail for human related design decisions when workload, human error and training needs are accounted for.

The marine industry can learn from recent investigations within the rail industry and build on some of the latest progress in HFI methods and standards. The challenges common to both the rail and marine industries can be addressed without excessive levels of expenditure if structured design processes, active user involvement, constructive HCI solutions and a receptiveness to industry wide standardisation are brought together.

REFERENCES

[1] The Ladbroke Grove Rail Enquiry, Part 1 Report, The Right Honourable Lord Cullen PC, HSE Books, 2001
[2] Network Rail Company Specification, Alerts Systems Design, Draft01 March 2003 EPGN/3-2B (Guidelines for the Design of Railtrack User Interface Displays), Part 2A, October 2002
[3] National Transportation Safety Board. (1997*). Marine accident report-Grounding of the Panamanian passenger ship* Royal Majesty *on Rose and Crown Shoal near Nantucket, Massachusetts*, June 10, 1995 (NTSB/MAR97/01). Washington DC.
[4] Report on the investigation of the contact made by UK registered Ro-Ro ferry Daggri with the breakwater Ulsta, Shetland Islands, 30th July, 2004, MAIB Report 6/2005, April 2005