MANAGING THE HUMAN ELEMENT IN MODERN SHIP DESIGN AND OPERATION

R V Pomeroy and B M Sherwood Jones Lloyd's Register of Shipping, London, UK

(Reproduced with the kind permission of the Royal Institution of Naval Architects from their Human Factors in Ship Design and Operation Conference, October 2002)

SUMMARY

The design and operation of ships has evolved and continues to develop, due to structural change in the industry and as a consequence of the introduction of new technologies and changes in manning. Lloyd's Register recognises the need for ship design to take account of the human element in order to ensure a reasonable level of marine safety. When considering marine safety it is necessary to consider both the human element and at the technical element in the broadest sense, not just the immediate causes of failures. Whilst this combined approach is taken in some incident analysis, whether after the event or as part of a proactive safety assessment, there is still a tendency to examine the human and the technical element independently of each other. An integrated socio-technical approach is required if full understanding is to be achieved. A simplistic technical approach tends to recommend local reactive solutions, such as the addition of more alarms, which may assist but will add complexity and the underlying cause may not be resolved.

The complexity of recent incidents with high-tech shipping is examined by event sequence analysis so that the real value of the present established hardware safeguards can be re-appraised. Accidents are necessarily a lagged (and unfortunate) source of data. There are many lessons to be learned from the experience of other sectors, to prevent the marine sector learning the same lessons the hard way. The Human Factors community has a technology transfer role to play here.

Much analysis of human error has been aimed at improving understanding, and its remedial value has not been fully exploited. The analysis presented examines how the various stakeholders might improve the barriers against incidents, what sort of approach (e.g. prescriptive, risk-driven, capability-driven) would be most appropriate, and the role that Classification Societies could play in supporting them, with emphasis on the work undertaken by Lloyd's Register.

AUTHORS' BIOGRAPHIES

Vaughan Pomeroy is responsible for the management of the research and development programme and the global naval business activities of Lloyd's Register. He joined Lloyd's Register in 1980 after working in the aircraft industry and with mechanical and electrical engineering consultants, initially to work on engineering research and specialist projects. He has held management positions within Lloyd's Register since 1987, successively responsible for machinery, pressure equipment and HQ engineering activities.

Brian Sherwood Jones is an independent Human Factors consultant who has supported Lloyd's Register's Human Factors activities for five years. After working in the aircraft industry, he worked at YARD Ltd and its successors for fourteen years, prior to setting up Process Contracting Ltd. three years ago. He has specialised in the Human Factors Integration of complex systems.

1. INTRODUCTION

The Human Element has long been recognised as important to marine safety. This recognition has led to developments in the approach to ship design and the introduction of classification Rules for key aspects such as for Integrated Bridge Systems (IBS), Habitability and the application of ergonomic principles to machinery control station arrangements. There have been similar developments in the last few years affecting manning and ship operation, including introduction of the International Safety Management (ISM) and major changes to the Standards for Certification and Training of Watchkeepers (STCW).

The work performed by Lloyd's Register to address the human element has been described previously [1]. This paper describes the direction of some of the work since that time. It continues the discussion of how technological innovations may increase the potential for accidents and some of the ways in which preventative measures may be put in place.

The NTSB Report on the grounding of the ROYAL MAJESTY [2] stated *"Thus, while human engineering is a known concept in the marine industry, there have not been any unifying efforts to integrate this concept into the marine engineering and manufacturing sector. Additionally, human engineering in the broader context of Human System Integration has been given little or no consideration. Consequently, the potential for error causing behavior related to these [automated] systems has not been adequately addressed by the marine industry"*.

This statement is a broadly accurate view of the industry and summarises the problem that Lloyd's Register has been addressing. An analysis of the ROYAL MAJESTY incident based on the factual evidence cited in the NTSB report [2] is presented as a vehicle to illustrate the issues to be resolved.

This incident was a major stimulus for recent changes to the Safety of Life at Sea (SOLAS) Regulations [3] that have been introduced for ships with extensive automation. Most of the major regulatory stakeholders (National Administrations, IMO, insurers, Classification Societies) have raised the profile of the human element, and appear set to maintain this profile for the foreseeable future. The importance of the human element to ship safety is not in dispute. Storey [4] stated that "80 per cent of accidents have nothing to do with the basic integrity of the ships themselves, but are down to human error." If we take a wider view of the human element, beyond the operational crew members, the impact is certainly higher than this oft-quoted value.

The operational context is changing. The seafarer population is changing in terms of background, culture and skill set. Crew complements are reducing. Ship and equipment design is changing, with increased adoption of computer-intensive technology. It is not obvious that these independent developments are compatible.

Shipping, like other industrial activities, is in transition between an approach to specification and regulation based on detailed prescriptive statements and an 'open-textured' approach based on goal-setting. The increasing adoption of system engineering approaches in a number of other sectors is in response to a similar trend. A related development on the commercial front in other sectors is the move away from hands-off procurement to supply chain management.

2. INCIDENT ANALYSIS

Lloyd's Register has analysed a number of incidents involving ships with complex automation, including the grounding of the cruise ship, ROYAL MAJESTY, which is used in the following paragraphs to illustrate the issues. The format used in these analyses has proved to be very useful when considering complex incidents with many apparently unrelated factors. The format used is broadly similar to other forms of influence diagrams, and is discussed at Annex 1 The complexity of the ROYAL MAJESTY incident is worthy of note. The NTSB report [2] provides 22 separate conclusions. The analysis here is, therefore, split into an overview and a number of subordinate diagrams.

Figure 1 shows the overview of the ROYAL MAJESTY grounding and the detail of

- near-term mitigation opportunities missed
- missed post-incident opportunities.

Several opportunities for avoiding the incident appear here. There did not seem to be a clear structure for passenger safety and incident management. Presumably responsibility for passenger safety is devolved, but this role is not closely connected to the bridge team.

Figure 2 shows the findings as regards design and build. In terms of system design, the lack of a system integration role led to a range of problems. The NTSB report called for an independent authority to oversee the management of total system integrity. However, from the nature of the problems encountered in system design either this activity or a system integration role working for the ship builder needs to be involved at a detail design level. The proper integration of electronics and automated system with the host platform is a difficult topic in a range of applications and warrants specific attention in automated ships.

The arrangements practised during the build and commissioning of ROYAL MAJESTY allowed for a mismatch between equipment design intent, crew qualifications and training and the ship operation. There is the possibility that new SOLAS V Regulations and the Safe Manning Certificate can be interpreted in a way that prevents such a mismatch. However, a more integrated socio-technical approach would provide a better chance of incident prevention for the longer term. For example, procedure development, documentation development and training definition ought to proceed in conjunction with system design and development.

Figure 3 shows one of the key aspects of the incident. Essentially, the crew lacked proper training in the operation of the bridge equipment and there was little in the way of management or cultural support.

Figure 4 characterises the shortfalls against the regulatory obligations in relation to training and design. Although the NTSB report provides a very thorough analysis in this and other areas, the recommendations appear to be highly focussed on the specific problems that led to the incident. For example, the items above apply to Integrated Bridge Systems as currently defined. However, the issues are fundamental and are, in reality, generic and should be applied to all onboard automation systems.

Figure 5 shows the issues relating to the dependence on automation and the lack of situation awareness. There were some aspects that could be considered to go beyond a lack of situation awareness and into the realms of a 'violation'.

3. MARINE TECHNOLOGY AND HUMAN ERROR

3.1 SKILL LEVELS

Apart from the changing skill patterns in ship operation mentioned above, there are changes in the operator community. Anecdotal evidence suggests that ship bridge crews are going through a similar change to that noted in aircraft cockpits. Older, but apparently more experienced, operators may not fully appreciate the capabilities and demands of the current technology but in an emergency would concentrate on the fundamentals of the situation. Conversely, younger, apparently less experienced operators would attempt to 'fix the computer' and not look out of the window.

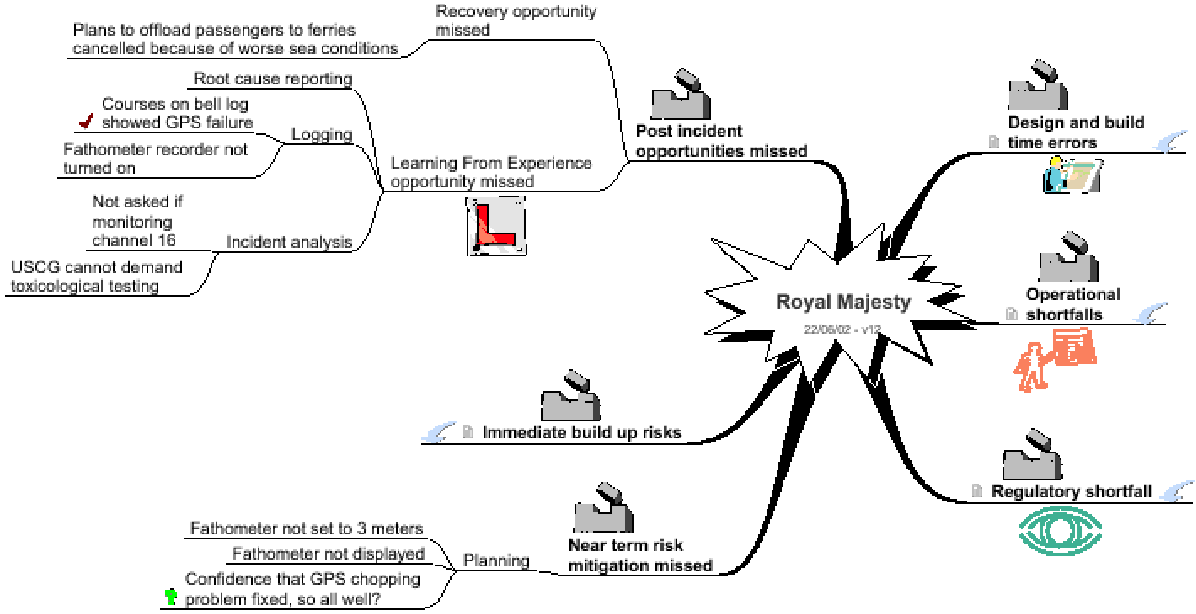

Figure 1: Overview

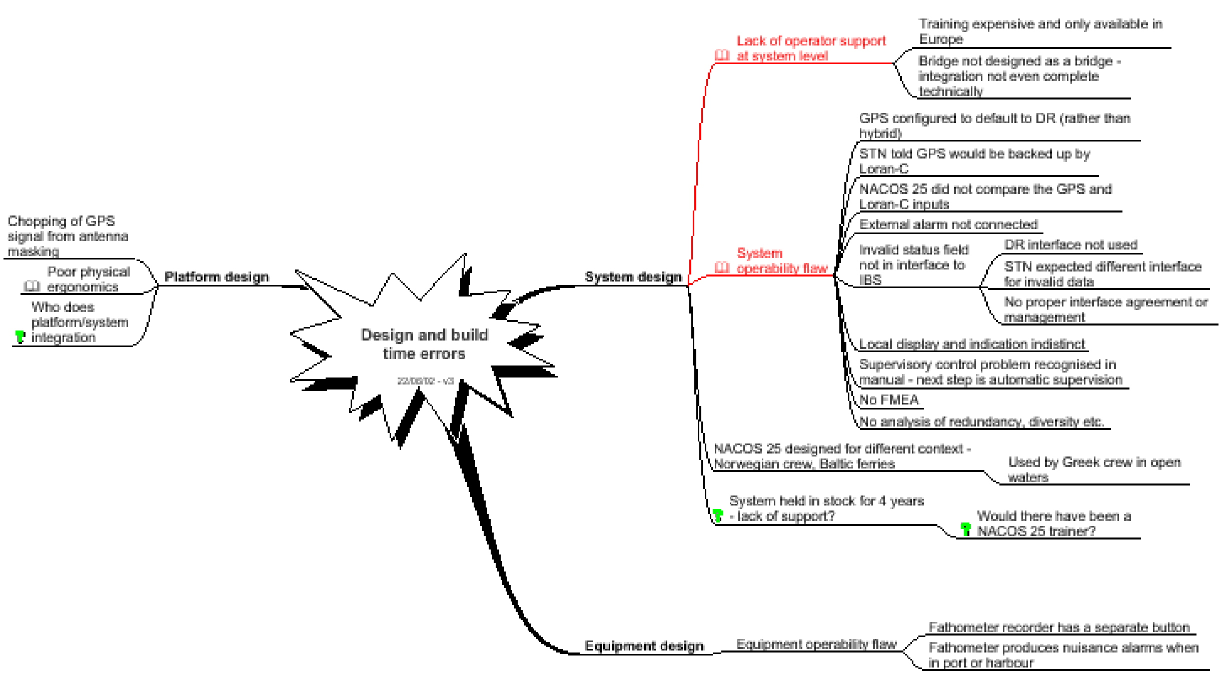

Figure 2: Design and build time errors

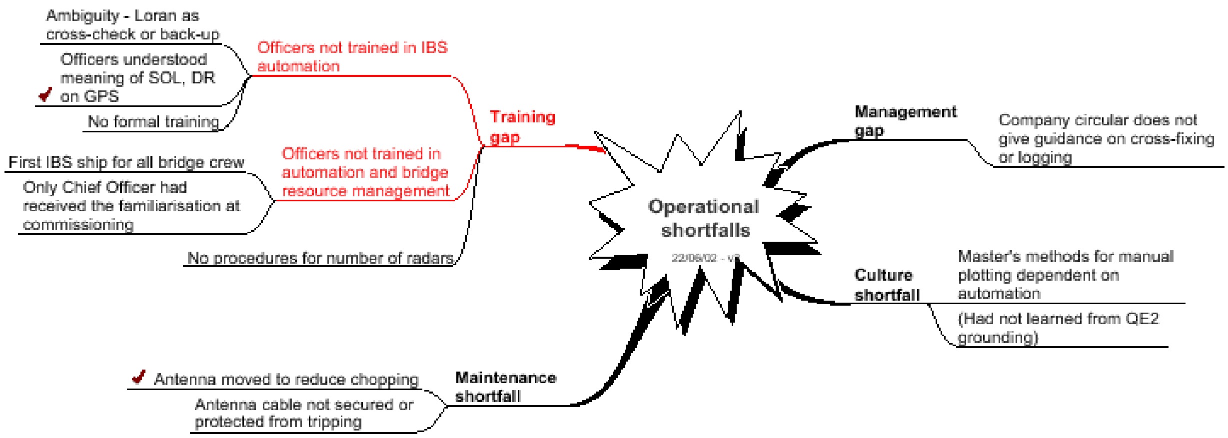

Figure 3: Operational shortfalls

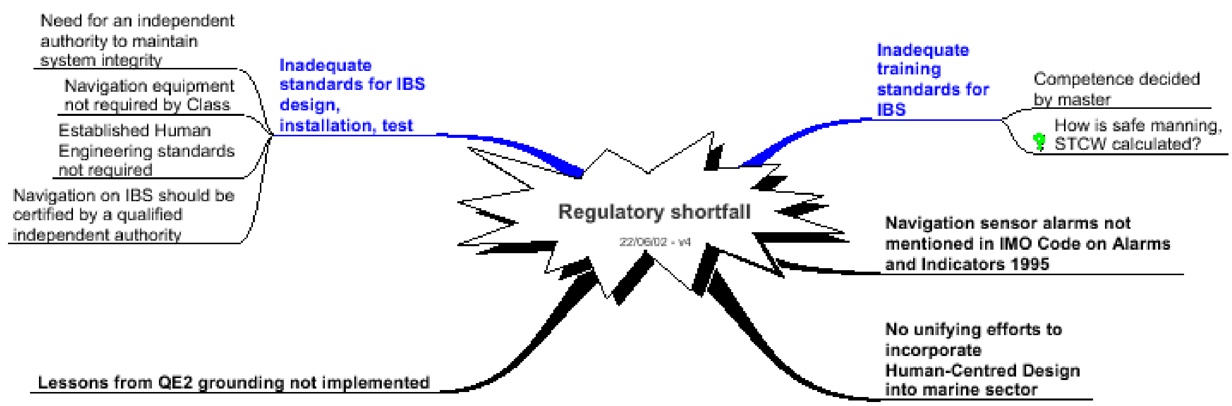

Figure 4: Regulatory shortfall

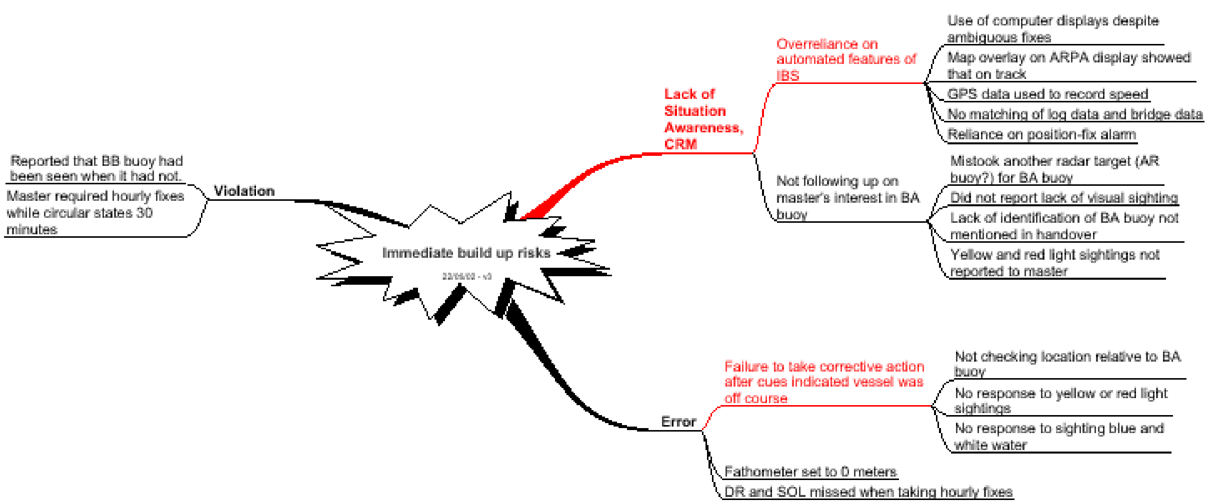

Figure 5: Immediate build up risks

There are, also, changes in other agencies that have a significant role in assuring maritime safety. The surveyor and auditor population is changing. The design community is now under greater time pressure than ever, also with much more automation, and anecdotal evidence suggests that more obvious mistakes are getting through the system and being delivered to the operators.

3.2 SUPERVISORY CONTROL

In a number of ways, shipping is responding to the issue of extensive automation later than other sectors. For example, the process industries responded to earlier incidents such as Flixborough and Three Mile Island. It may be possible, therefore to learn from experience in other sectors. Incidents, such as ROYAL MAJESTY, illustrate the problems of 'supervisory control' [5] where the operator has less to do but has more to monitor. Adding automated monitoring, such as smart alarm systems, can be useful but brings other problems and ironies of automation [6]. There is now a considerable literature and body of experience [e.g. 7] that addresses the problems of automated systems, notably the problems of 'clumsy automation' that is 'strong, silent and difficult to direct' [8].

In the examination of incident analysis by LR, there have been a number of instances where technical solutions have been proposed to human-system problems, typically introducing more alarms. There is a very real risk that this approach will not produce the benefits that are expected by the proposers and that it leads to entering Woods' cycle of error [8], shown in Figure 6.

"Attributing system failures to human operators generates demands for more rules, automation, and policing. But these actions do not significantly reduce the number of latent failures in the system. Because overt failures are rare, a quiet period follows institution of these new policies, convincing administrators that the changes have been effective. When a new overt failure occurs, it seems to be unique and unconnected to prior failures (except in the label human error), and the cycle repeats. With each pass through the cycle, more rules, policies and sanctions make the system more complicated, conflicted, and brittle, increasing the opportunities for latent failures to contribute to disasters."

It is important that solutions go beyond the specifics of an incident, and do not make systems more brittle. We should be wary of any proposal to 'introduce a new alarm channel' as a solution.

Although the classification society Rules address machinery alarms, and the new SOLAS V Regulations address bridge alarms, there is more that can be done during design and operation to improve the presentation of status information, to support diagnosis and corrective action and to deal with nuisance alarms.

3.3 USER AS INTEGRATOR

It has been observed [1] that the operational safety culture, the working environment and the design/development process are interconnected. Courteney [9] has pointed out that the human pilot forms the interface between many different parts of the aviation system, such as selection, training, licensing standards, flight deck design, flight time limitations, air traffic control, and operating procedures.

"If different parts of the system are not entirely compatible, this interface becomes strained, and may fail. This failure is known as 'pilot error' or, more recently, a 'human factors' issue. In general, the individual parts of the aviation system receive a great deal of attention, in terms of both management and regulation. The interfaces between them receive rather less, because they are difficult to quantify and have no clear ownership. Achievement of highly compatible interfaces may require individual areas to expand the boundaries of their task beyond its current definition. Ensuring the adequacy of the interface to the pilot, and through him, the interface to other areas, may not necessarily be defined as a program task in civil aircraft development."

There are many similarities here with the marine industry. For example, the present arrangements for definition of STCW and Safe Manning Certificates, and their links to equipment Type Approval include long time delays, and a more integrated approach is required.

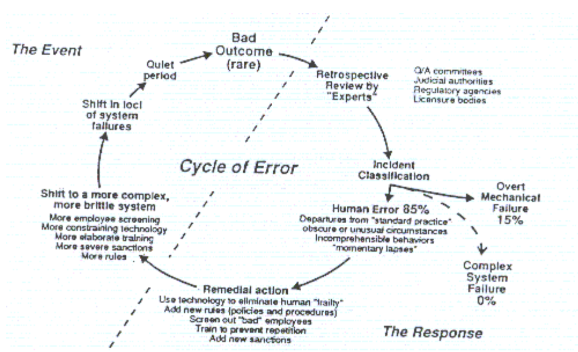

Figure 6 - Cycle of error

The increasing commercial pressures on each part of the marine industry will make interfaces between them less compatible without external influence e.g. from regulation. The need for an integration role (other than by the user) is recognised, but it is unlikely to happen on its own.

3.4 ROLE OF REGULATOR

Human variability and adaptability make detailed prescription particularly difficult for areas affected by the human element. For situations where there is any significant change in the manning, technology or type of operation, there are major difficulties with producing detailed prescriptive design specifications. Any solution of manning, documentation and procedures, user interface design and platform design can only be judged as correct against a context of use. The specification of fitness for purpose for the human element cannot be generic. Fortunately, the capability that is required to ensure delivery of systems with Quality In Use [10] is available. The principles to be followed in design, development and operation are known [11]. The means to deliver a process and principles based solution that can take account of context of use exist [12].

However, present approach to statutory regulation and within the Rules of classification societies, which form an essential part of the overall safety regulatory process, are prescriptive. In a prescriptive approach, the owner and regulator need to understand requirements decomposition at all levels (e.g. from ship operation to equipment part numbers). The owner retains both business and technical risks. In return, he retains control over all aspects of the job. This can simplify the specification of implementations that are sub-optimal for the project in hand, but which enable a more optimised solution at the level of the client business. For example, the equipment may not be the best for this particular contract, but it is the equipment being used on other contracts and this choice simplifies support. The job of the supplier is relatively straightforward. Suppliers have evolved a skill base, culture and costing strategy based on straightforward compliance with specific requirements. For monitoring and acceptance in a contractual or regulatory setting, the prescriptive approach has the advantage that inspection is largely at the lowest implementation level, and comprises a series of simple checks. This may be a long series of checks. The disadvantages arise because the specification is inevitably imperfect. Areas subject to rapid operational or technological change also suffer severely from this approach.

A goal-setting approach to procurement offers benefits to situations with an informed purchaser and an intelligent supplier. Similar benefits accrue to a situation with an informed regulator and an intelligent supplier or operator. The prospective owner specifies what he wants at the level of his business, in high-level ship operation terms. He retains the business risk. The supply chain translates this specification into something that is designed and delivered. The supplier retains the technical risks of implementation. Given an intelligent supply chain, this approach enables each level of supply to optimise the solution in its own area of expertise. The aim is that the client does no more work than is necessary, carries no more risk than is necessary and the suppliers are given maximum opportunity to innovate (gain market share) or to take profit. Appropriately supported, this approach minimises the information exchanges as requirements and implementation evolve.

The disadvantages of this approach are:

- There is the risk that a non-intelligent supplier is selected for some part of the supply chain.
- There is the risk that the high-level requirement is misunderstood because of its abstract nature.
- In some markets, the number of intelligent suppliers may be very limited, restricting the client's ability to run a competition, with an inevitable increase in price.
- The ability of the client to monitor progress of the implementation may be limited.

There are mitigations for all of the above disadvantages, but they represent deterrents to adoption for much of the marine sector, posing an obstacle to broad adoption of Human System Integration. Similar obstacles have been found in the aviation sector [9].

A simplified practical example of the strengths and weaknesses for a limited area of Human Factors is given in Annex 2. Examples of goals and prescriptive requirements relating to the new SOLAS V Regulation 15 'Principles relating to bridge design, design and arrangement of navigational systems and equipment and bridge procedures' [3] follow, in approximate order of abstraction:

- Principle requiring an effective interface between the various agencies.

The Regulation addresses designers, manufacturers and shipowners with respect to the bridge design and layout. However, the responsibility for ensuring correct bridge procedures are adopted lies with the Master.

- Requirements to achieve Quality In Use.

Facilitating the tasks to be performed by the bridge team and the pilot in making full appraisal of the situation and in navigating the ship safely under all operational conditions.
Promoting effective and safe bridge resource management.
Allowing for expeditious, continuous and effective information processing and decision-making by the bridge team and the pilot.

- Linking Quality In Use with design intent.

Minimising the risk of human error and detecting such error if it occurs, through monitoring and alarm systems, in time for the bridge team and the pilot to take appropriate action.

Enabling the bridge team and the pilot to have convenient and continuous access to essential information, which is presented in a clear and unambiguous manner, using standardised symbols and coding systems for controls and displays.

- Design principles (still requiring interpretation for the context of use).

Indicating the operational status of automated functions and integrated components, systems and/or sub-systems. It should be possible from this place to operate the ship safely, in particular when a fast sequence of actions is required.

- Design principles requiring limited interpretation of the context of use.

The height of the lower edge of the front windows should allow a forward view over the bow for a person in a sitting position at the workstation for navigating and manoeuvring and the workstation for monitoring.
The console should be dimensioned and configured so that all relevant controls can be reached from a sitting position.

- Prescriptive design requirements that can be checked with no specific reference to the context of use.

There should be a field of vision around the vessel of 360° obtained by an observer moving within the confines of the wheelhouse.

Achieving the successful interfaces between the various agencies will represent a significant step forward. It will be necessary to find ways of demonstrating that the higher level principles are met. It will not be sufficient to assume that by meeting the various prescriptive design requirements, the higher level principles will be met.

4. CONCLUSIONS

Incidents attributed to 'human error' in modern shipping (and other incidents) result from the failure of multiple barriers. The prevention of incidents depends upon the strengthening of these safeguards. There is no 'silver bullet' to enable the broader context of Human System Integration to be addressed by the marine industry. The implications of this are as follows:

- Progress depends upon resources that can be used as part of mainstream activity and do not depend upon scarce expertise for their application.
- Consideration of the human element must become part of the mainstream rather than a specialist discipline.
- Tools for dealing with the human element must be usable by auditors and surveyors, though training will still be required as well.
- Whilst there is a role for specialist Human Factors consultancy, the key role for specialists is as tool builders, developing and providing the tool set for application by surveyors, designers, operators and installers.

There is a great deal of work to do on a number of fronts. The scale of change required is considerable. For such change to be absorbed by the industry, a 'drip-feed' approach is necessary. Effective prevention needs coverage of the total marine operation rather than an exclusive focus on ships.

As discussed previously [1], the human element does not lend itself to detailed prescriptive approaches. The transition to goal-setting approaches is unlikely to be rapid or uniform. It appears likely that both approaches are likely to run in parallel for some time. Typically complex systems and goal-setting are likely to be compatible, as are simple shipboard systems and the established prescriptive approach.

To meet the challenge of integrating the human element into ship design and operation, Lloyd’s Register is taking the results of its extensive research and development programme in human factors and incorporating these into goal-setting approaches and extending the application of prescriptive approaches in the Rules to cover the modern and future application of complex systems. Alongside the Rule developments, approaches are being developed that will be consistent with the delivery of support for human factors input into a wide variety of situations by non-specialists of different disciplines. By these approaches it is considered that the greatest impact can be made, thereby maximising the safety gain.

5. ACKNOWLEDGEMENTS

The authors wish to thank the General Committee of Lloyd's Register of Shipping for permission to publish this paper. The views expressed are those of the authors and do not necessarily represent the policy of Lloyd's Register of Shipping.

6. REFERENCES

1. POMEROY, R.V., TOMLINSON, C.M., 'A Systems Approach to Integrating the Human Element into Marine Engineering Systems', in 'Human Factors in Ship Design and Operation', RINA International Conference, London, Sept 2000.
2. NTSB 'Grounding of the Panamanian Passenger Ship ROYAL MAJESTY on Rose and Crown Shoal near Nantucket, Massachusetts, June 10, 1995'. NTSB PB97-916401, Marine Accident Report NTSB/MAR-97/01, 1997.
3. MCA, 'Safety of Navigation, Implementing SOLAS Chapter V', 2002.
4. STOREY, M., article in Fairplay, March 14 p4, 2002.

5. SHERIDAN, T.B., JOHANNSEN, G., (Eds.) 'Monitoring behavior and supervisory control' NY, Plenum Press, 1976.
6. BAINBRIDGE, L., 'Ironies of Automation', in Rasmussen, J., Duncan, K., Leplat, J. (Eds.), 'New Technology and Human Error' Wiley, ISBN 0 471 91044 9, 1987.
7. WOODS, D.D., JOHANNESEN, L.J., COOK, R.I., SARTER, N.B., 'Behind Human Error: Cognitive Systems, Computers, and Hindsight' CSERIAC SOAR 94-01, 1994.
8. COOK, R., WOODS, D., 'Operating at the Sharp End: The Complexity of Human Error'. In Bogner, M.S., ed., 'Human Error in Medicine', Hillsdale, NJ: Lawrence Erlbaum, pp 255-310. [ISBN 0-8058-1385-3], 1994.
9. COURTENEY, H.Y., 'Practising What We Preach', Proceedings of the First International Conference on Engineering Psychology and Cognitive Ergonomics, 1996.
10. ISO PAS 'A specification for the process assessment of human-system issues', in press.
11. ISO TR 18529:2000 'Ergonomics of human system interaction - Human-centred lifecycle process descriptions'.
12. ISO 17894 xxx ATOMOS
13. JOHNSON, C.W., 'Reasons for the failure of incident reporting in the healthcare and rail industries' in Redmill, F., Anderson, T., 'Components of System Safety'. Proceedings of the Tenth Safety-Critical Systems Symposium, Southampton, UK, 2002. Springer-Verlag, London ISBN 1-85233-561-0, 2002.
14. HUDSON, P., REASON, J., WAGENAAR, W., BENTLEY, P., PRIMROSE, M., & VISSER, J. 'Tripod Delta: Proactive approach to enhanced safety'. Journal of Petroleum Technology, 1994 46: 58-62.

ANNEX 1 - INCIDENT ANALYSIS FORMAT

Where the report e.g. [2] highlighted something as being a cause, this is identified in red. Contributory factors are identified in blue. Where there are questions outstanding from the reading of the report, these are identified. There are a number of instances where correct mitigation action had been taken. These are identified with a tick.

The approach taken to the incident analysis has the following characteristics:

- It assumes multiple causes;
- It takes an event tree approach, where successive 'barriers' to an incident have been breached;
- It attempts to get to a level of root cause analysis that means that the systemic failures can be identified;
- Although Johnson [13] warns of the dangers of classification errors, it was decided to attempt a standard structure for attributing causes. It is believed that attributing causes to enabling systems through the life cycle is likely to be less obviously misleading than the types of coding scheme described by Johnson.
- It is aimed at identifying potential preventative measures rather than in-depth analysis of causes. Although words such as 'shortfall' and 'error' are used, there is no attempt to assign blame. The interest is in understanding, but principally in corrective action at a systemic level.
- A 'mind map' approach has been used to present the analysis in a condensed form with readily available tools.

The incident analysis format adopted in the work at LR bears many similarities to accepted methods such as TRIPOD [14], event trees and fault trees. The reasons for adopting this particular format were:

- It draws out the multi-agent nature of accident causation and identifies the main groups of agents through the life cycle.
- It enables cause and contributory factors to be related to models of good practice such as ATOMOS [12] (rather than models of failure such as Generic Failure Types) and thereby supports the assimilation of preventative measures.
- This particular incident analysis activity does not need to identify the specific causal sequences or logic, enabling the use of simpler diagrams. It is recognised that this format may not suit all phases of incident analysis.

ANNEX 2 - EXAMPLES OF DIFFERENT APPROACHES TO REGULATION

This annex presents different approaches (in Table 1 below) to specification (of alarms) and summarises the implications for assessing compliance, and the strengths and weaknesses of each approach.

Type of requirement	***Example for alarms***	***Guidance to surveyor***	***Implications for assessment of compliance***	***Strengths, weaknesses***
High level specification of Product	The presentation of alarms and indicators should be clear, unambiguous and consistent.	(partial) The alarm message clearly identifies the condition that has occurred.	Trip some items of equipment, read the alarm message and check that the message identifies the condition.	Very difficult to create other than simple conditions. Example would involve extensive test programme. Requires in-depth knowledge by surveyor of the plant and of how message would be interpreted by crew in operational conditions.
Detailed specification of Product	Alarms shall provide specific information.	Each alarm entry in the alarm list should show: the alarm state marker (unaccepted, accepted, standing, clear, reset); the alarm priority marker; the alarm message; time and date.	Check alarm list on checklist.	Easy to do. Potentially many items to check. Probably low impact on safety.
High level specification of Performance	Timeliness. Sufficient warning.	Adequate time should be allowed for the operator to carry out his defined response.	Cause surprise failures under high workload (or high fatigue) conditions, time response, and check safety of ship, plant, personnel.	Very difficult to create representative conditions or adequate sample.
Detailed specification of Performance	No excess standing alarms. No alarm cascades, grouping of alarms.	There shall be no more than 10 standing alarms (+ 30 shelved alarms) in the alarm list when running main engine(s) and auxiliaries alongside. There shall be less than 20, and preferably less than 10 alarms in the 10 minutes following a major machinery disturbance.	Surveyor checks plant state, counts number of alarms in list. Records findings in checklist. Compatible with approach to mainstream surveys. Surveyor trips a major piece of machinery (or arranges for it to be tripped) having checked that it is safe to do so, and then counts the number of alarms in the ECR and on the bridge in the next 10 minutes.	Easy to do, measures an accepted indicator, but ought to be tailored to design and manning of ship.
High level specification of process	The supplier shall follow a user-centred design methodology The operator shall operate and maintain an alarm improvement strategy.	The supplier shall follow the principles of human-centred design and the design process specified in ISO 13407. (principles and process descriptions supplied) The operator shall appoint someone responsible for managing the alarm system. There is senior management commitment. Standards are set. The system is reviewed.	Inspection of records concerning: demonstration of usability; user involvement in design; development of design standards; analysis of context of use. OR Assessment of processes using ISO TR 18529. Review of process documentation; management Terms of Reference; evidence of review and change management.	Allows for new technology, addresses safety issues, but requires examination of design/development activity rather than the ship and its systems. Generally compatible with an ISM audit in approach. Tackles important safety aspect. Addresses a design topic from a management point of view.