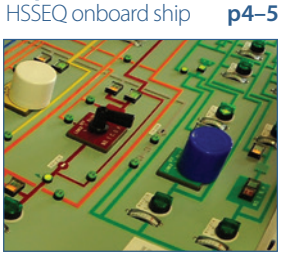
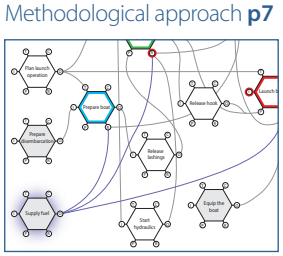
The International Maritime Human Element Bulletin

Issue No. 39 September 2015
ISSN 1747-5015

Alert!

It's all about Risk…





A Nautical Institute project

The Nautical Institute

sponsored by
The Lloyd's Register Foundation

Lloyd's Register Foundation

w: www.he-alert.org
e: editor@he-alert.org

Ivan put the final touches to his first Master's Standing Orders carefully leaving space at the end for the deck officers to each sign that they had read and understood them. Reading them through, he was pleased with his work. For so long it had been his role as a junior officer to read and sign such documents and now it was his turn to put his stamp on the way a ship, his ship, was going to be run.

He had carefully considered what aspects of good navigational practice he would include and, to help him, he had consulted the course manual he had received when he had undergone his most recent training: a course in Bridge Resource Management at the ship management company's own simulator training unit. The company ISM auditors would be impressed that he had cut and pasted key aspects of the training into his orders.

He had endured the training, which he had undertaken along with the junior officers with whom he was about to embark on his first voyage in command. It had gone well. The group had been carefully instructed in all aspects of good teamwork and, although they had found it difficult at first, the junior officers had learned to monitor his actions and orders and to speak up if they were concerned. For his part, despite finding it embarrassing and irritating, he had reacted well on the occasions that it had been pointed out that he was about to make an error. The team had passed with flying colours. That particular box had been ticked.

This, however, was different. This was not a simulator. In a short time he would really be taking his first command to sea. He was vastly more experienced than his officers and he was determined to stamp his authority from the start.

He picked up the Standing Orders and walked out of his cabin. Finding the Chief Mate talking with the Bosun he gave the Orders to him and told him to read and sign them and to make sure the 2nd and 3rd Mates did the same before departure. He then strolled to the bridge where he found the 2nd Mate working on the passage plan. Looking over his shoulder he noted that course lines had been drawn taking the vessel outside and well clear of a prominent local landmark - a small island complete with castle and lighthouse.

An alternative, more picturesque route, using a narrow inside channel was shorter. He told the officer to change the plan

An alternative, more picturesque route, using a narrow inside channel was shorter. He told the officer to change the plan. The 2nd Mate started to comment but, seeing the challenging look in the Master's face, he ate back his words. Walking back to his cabin Ivan thought to himself that this had been a good start. They would soon know exactly who was in charge!

A short time before departure Janez, the marine superintendent who was also the designated person for the ship, came on board to check that preparations for the voyage had been completed satisfactorily and to wish Ivan good luck with his first command. Among other documentation he looked at all the completed pre-departure checklists and read through the Master's Standing Orders.

He congratulated Ivan; everything appeared in order. He then accepted one of the two cans of beer, which Ivan had taken out from his fridge, and they both drank a toast to a successful voyage.

As Janez stood on the quayside watching the accommodation ladder being winched into its stowage position he was unaware that he would be speaking with Ivan again before the end of the day…

Introduction

David Squire, FNI FCMI

The Editor
Alert!
The Nautical Institute
202 Lambeth Road
London SE1 7LQ
United Kingdom

editor@he-alert.org

In **Alert!** Issue No. 26 we focussed on the essentials of an Integrated Management System and argued that there is a need for effective systems and processes and for health, safety, security, quality and environmental awareness to be combined with good working practices. In this Issue we are focussing on the management of Risk.

Since Issue No.26, we have seen a number of amendments to the ISM Code, one in particular introduced text changes to Section 6.2, which requires that the Company *should ensure that each ship is appropriately manned in order to encompass all aspects of maintaining safe operations on board.*

Manning issues (especially under-manning) can present a major risk; due regard should therefore be given to *The Principles of minimum safe manning*. In **Alert!** Issue No. 32, we offered some guidance on interpreting these Principles through the associated document *A Rough Guide to interpreting the Principles of Safe Manning*.

We also now have the ILO *Guidelines for implementing the occupational safety and health provisions of the Maritime Labour Convention* which offers a more comprehensive approach to risk management than that current under the ISM Code.

In the context of security, the ISPS Code covers the general aspects of security aboard ship and in ports, but it does not embrace the relatively new risk of cyber-attack, which can have an effect on the human-system aspects of risks.

However, the Round Table of international shipping associations are developing Industry guidelines – for which drafting work is still in progress – to provide advice to ship owners and operators on how to minimize the risk of a cyber-attack through user access management, and how to protect on board systems, develop contingency plans and manage incidents if they occur.

This is the last but one Alert! bulletin. Issue No. 40 - the final Issue - will serve as a *wrap up* edition, which will be published on 1 January 2016 in pdf format; we are investigating funding for the printing of this final Issue. We are also exploring the possibility of publishing a compilation of Issues 1 to 40.

Reports & Studies

Maritime cybersecurity using ISPS and ISM codes

Alejandro Gómez Bermejo

In this article Alejandro Gómez Bermejo presents some ideas to incorporate maritime cybersecurity policies, procedures and controls in vessel operations using the ISS and ISM Codes

Downloadable from:
www.he-alert.org/docs/published/he01335

Vessel Cybersecurity Risk Analysis

Alejandro Gómez Bermejo

In this article, Alejandro Gómez Bermejo introduces vessel cybersecurity risk analysis and show an example of its application to the Information and Communications Technology (ICT) assets in the Integrated Bridge System of a vessel.

Downloadable from:
www.he-alert.org/docs/published/he01340

Back numbers of Issues 1 to 38 of the **Alert!** bulletins and associated centrespread features can be downloaded from
http://www.he-alert.org/en/all-issues.cfm

Bound editions of Issues 1 to 12 and 13 to 21 can be purchased From the Nautical Institute Publications Shop at:
http://www.nautinst.org/en/shop/

The Alert! videos offer a unique insight into the importance of the human element in shipping and its impact on maritime safety. Each video corresponds to one of the Alert! Bulletins, and can be downloaded from:
http://www.he-alert.org/en/videos.cfm

Join us on the following sites

https://facebook.com/thenauticalinstitute

https://twitter.com/NauticalInst

LinkedIn http://www.linkedin.com/groups/Nautical-Institute-1107227

YouTube http://www.youtube.com/TheNauticalInstitute

Big Data: Harnessing it to improve Risk Management

Warwick Norman, Chief Executive Officer, RightShip
www.rightship.com

The maritime industry – not renowned for its willingness to proactively embrace change - is now seeing both the benefit and necessity of employing big data to enhance commercial opportunities, and also improve the safety and sustainability of the industry and those that work within it.

These opportunities also bring unprecedented challenges. Previously, the relative lack of connectivity of various data sources has provided some sort of protection; however the modern-day *internet of things* has changed this. Organisations need to understand and mitigate the risk they face within their operating environment, ensuring effective precautions and responses are in place should they fall prey to cyber attack.

At RightShip we clearly recognise the commercial advantages of big data, having spent the last two years upgrading our online risk management platform to a multi-million dollar predictive analytics tool.

The ability to instantly and meaningfully analyse multiple, massive data feeds into a simple risk assessment tool means that real-time analysis will better target substandard maritime performance. The benefits to our clients are huge.

Our business is based on receiving incoming data, running it through complex internal processes, and distributing the results to clients through a secure online platform. Systems and procedures that protect this process are vital, and we achieve this by being certified to ISO/IEC 27001 *Information Security Management* which provides a systematic approach to managing information to ensure it remains secure.

The aim of all of this is to ensure communication security, protection of client information (in and out) and business continuity.

Communications Security & Information Protection

A full-time Marine Assurance Coordinator is employed to ensure that requirements to ISO/IEC 27001 are applicable to our people, processes and IT systems. This involves control of information (how people access the system), classification of information (differentiated access levels for individuals), ongoing information security education for all staff, the use of licensed and trackable software, and an asset management process.

Users of our risk management platform require authentication, which is achieved through a cryptographic protocol developed by AuthO.

All communications between client browsers and our server is encrypted using SSL, which ensures that all data remains private and integral.

Business Continuity

Cloud computing conjures up images of something that comes out of the sky; however the reality is quite different. Systems are generated by physical hardware that is housed inside buildings, connected by networking cable – and so online security also necessitates security of the physical environment of our servers, ensuring protection against external and environmental threats such as fire and floods.

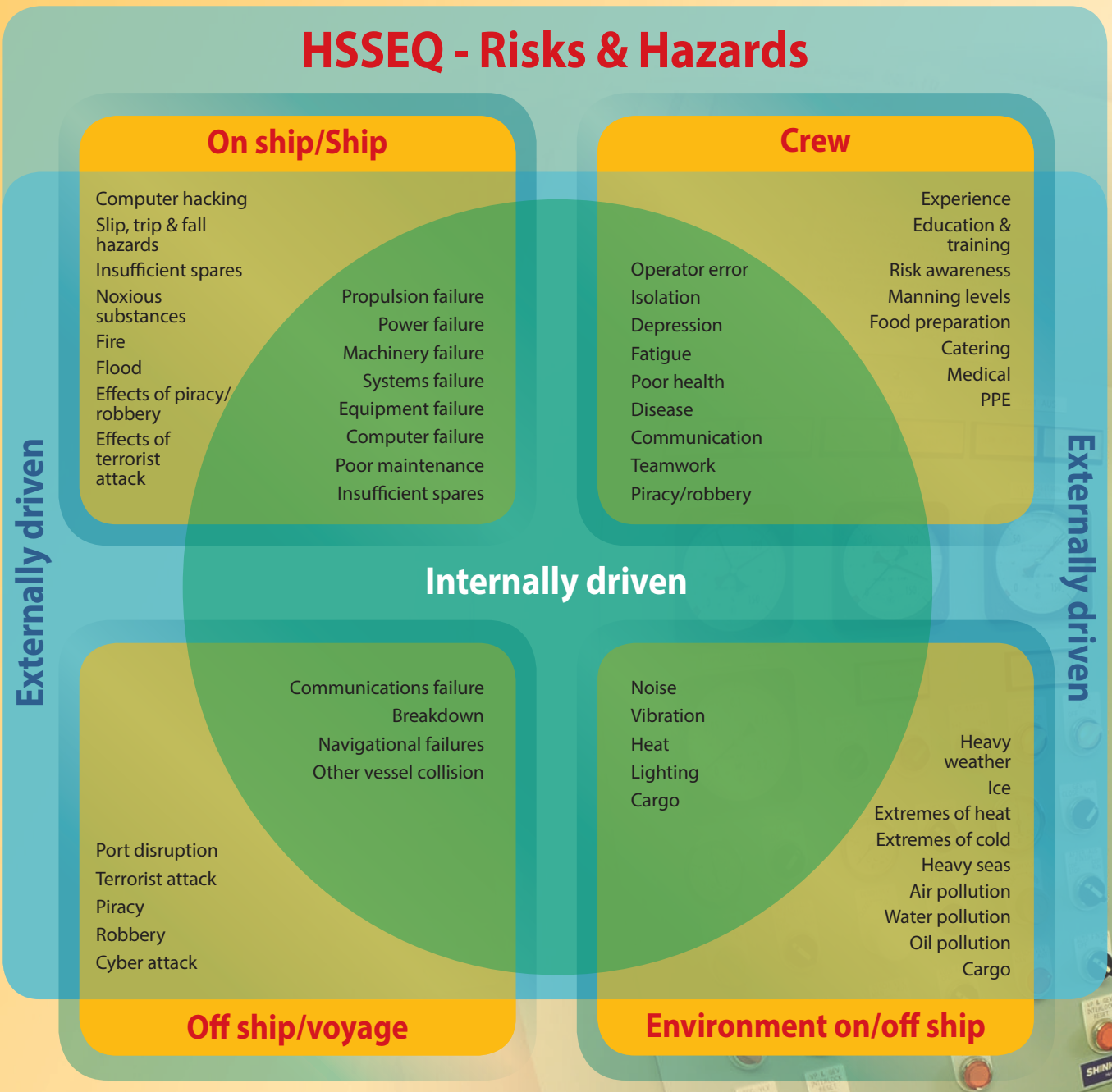
Likewise, physical access to the RightShip offices and the disparate locations of the some 38 servers that are used requires authorised electronic security passes – sometimes in multiple formats. Data is backed up frequently, mirrored and moved to separate servers, which in turn are also backed up frequently.

BIMBO, ICS, INTERTANKO and Intercargo have recently announced that they are jointly developing standards and guidelines to address the major cyber security issues faced by the shipping industry. A strategic, coordinated and ongoing effort is needed to protect the industry and its individual players who wish to maintain either the business as usual approach, or develop an operational advantage in this era of rapid technological change.

Just like physical and asset security, shipping operators will have to find tailored solutions to cyber security that protect their organisational information and complement their operating environment.

Organisations need to understand and mitigate the risk they face within their operating environment, ensuring effective precautions and responses are in place should they fall prey to cyber attack

The human element and human-system aspects of risks



There are a growing number of codes and standards and guidelines related to different aspects of maritime Health Safety, Security, Environmental and Quality (HSSEQ) management, including:

- ISM Code (Safety & Environmental Protection)
- Guidelines for implementing the occupational safety and health provisions of the Maritime Labour Convention, 2006
- ISPS Code (Security)
- ISO 9001 (Quality)
- ISO 31000:2009 (Risk Management)

The core of these is Risk Management, for which ISO 31000:2009 provides generic guidelines. When managing risk it is important to consider the human element.

This centrespread focuses on the human element and human-system aspects of risks in the context of total HSSEQ onboard ship. See also: *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000* published by the Institute of Risk Management (IRM) - https://www.theirm.org/media/886062/ISO3100_doc.pdf

in the context of total HSSEQ onboard ship

Alert!

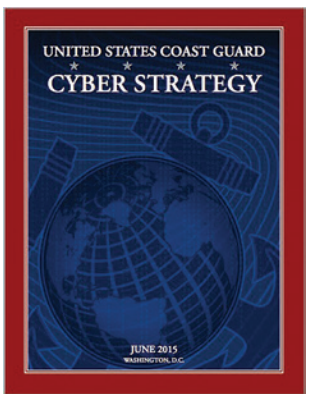
The Process

Issue No.26
A human-centred approach to HSEQ

http://www.he-alert.org/filemanager/root/site_assets/centrespreads/centrespread_26.pdf

Cyber: It's about Operational Risk Management

Rear Admiral Paul Thomas, United States Coast Guard, Assistant Commandant for Prevention Policy



Defending cyberspace is about ensuring the confidentiality, integrity and availability of internal networks and systems

The recently released U.S. Coast Guard Cyber Strategy (http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf) is one of a family of strategies that will help drive the service's planning, operations and acquisitions into the next decades. The Cyber Strategy is notable for several reasons, not the least of which is the title. The U.S. Coast Guard has developed a Cyber Strategy; not a Cyber Security Strategy. That is because for the Coast Guard, like most modern organizations, cyber today is about how we operate; how we sense, communicate, direct, control, manage and execute operations and support functions. Cyber security – protecting against attacks or unauthorized access - is just one aspect of how we manage cyber risks and make the most of cyber technologies. Cyber enabled operations require comprehensive cyber operational risk management similar to the management of physical safety, security and environmental risks.

Coast Guard Cyber Strategy

The Coast Guard Cyber Strategy describes three strategic priorities which form the basis for mutually supporting, interdependent lines of effort that must be undertaken simultaneously to achieve the strategic intent. They are: Defend Cyberspace; Enable Operations; and Protect Infrastructure. These same or very similar three top level priorities are applicable to any organization that wants to operate in, and manage the risks of, cyberspace. Defending cyberspace is about ensuring the confidentiality, integrity and availability of internal networks and systems to carry out critical business or mission execution functions. Enabling operations is about leveraging a diverse set of cyber capabilities, and safe, secure networks and systems, to conduct effective, efficient operations. Protecting infrastructure is externally focused. In the case of private sector entities this includes ensuring business partners, supply chains, and connections to customers and other stakeholders are secure.

Cyber Operations in the Marine Transportation System (MTS)

The MTS is increasingly reliant on a complex, globally connected system of cyber technology to control ordering, scheduling, routing, tracking, directing and paying for cargo movements around the world. Automated systems also control physical functions and ensure that safety, security and environmental standards are met. In many the most complex, high consequence operations, such as ultra-deep water drilling, machines talk to machines to make decisions and direct actions faster than humanly possible; they are the reason why these cutting edge operations can occur. A failure of these cyber systems, from accident or deliberate intent, could have tremendous consequences for human life, the environment, property, and the global energy and supply chain. Cyber is how we operate the MTS today; and as such operational risk management is inherently cyber risk management.

It is not just about hackers and attackers

Media reports of high profile cyber system breaches are common, and there is no doubt that nation states, cyber criminals and hacktivists will continue to target cyber systems, including data and control systems in the MTS. These targeted attacks are only a portion of the risk. Cyber accidents, such as the unintentional introduction of malware, the improper application of a software patch, or other misuse by well-intentioned employees, customers or contractors can have equally debilitating and physical consequences. In fact we have seen failures of critical safety and environmental systems that resulted from cyber accidents.

It is not just an IT issue

Thinking about cyber as simply an IT issue is akin to thinking about the safe operation of a ship as simply a main propulsion issue. Cyber is operational. It touches on every aspect of how we design, construct, operate and maintain ships and port facilities, and how we train and equip the people who operate them. Identifying cyber risks and implementing the most effective and efficient solutions requires operators, engineers, IT, emergency management, and other personnel. This is cyber risk management.

It is not a brave new world

The cyber revolution is creating new opportunities in the MTS – and new risks and vulnerabilities. The good news is that the marine industry knows how to handle risk – they do it on every watch and shift. Cyber and cyber risk management is not a brave new world for the MTS; it is the next step in the technological evolution of the MTS. When we moved from sail to steam propulsion as a new operational construct, we introduced new operational risk management measures, including design, construction and maintenance standards for boilers and, for the first time, shipboard engineers. As we grow our reliance on cyber systems we must similarly introduce the appropriate risk management measures. Safety culture extends into cyberspace, and Safety and Operational Management Systems should address training, operations and maintenance of critical cyber systems that reduce vulnerability to both cyber accidents and cyber attacks.

A methodological approach to the management of risk and safety

Nippin Anand, Principal Surveyor, Safety Management Systems Specialist, DNV GL- Maritime

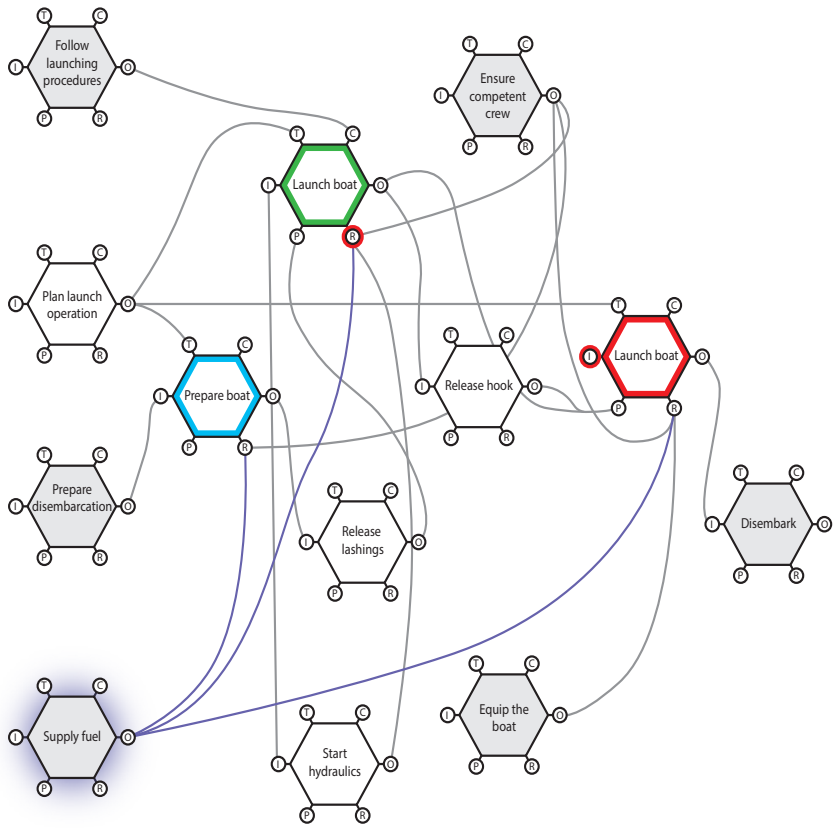
Organisations don't make safety. Organisations exist to make profits and safety is a necessary evil that needs to be overcome in the face of finite resources, limited knowledge, conflicting goals and intense competition. A seafarer could either spend all day working a job in accordance with all available procedures and instructions or opt for a reasonably acceptable job in limited time to the best of his or her experience and ability.

There always is a balance between efficiency and thoroughness in undertaking any job. So what appears as an unsafe act or rule violation on the surface is merely an adjustment required to get work done. But occasionally when adjusting and improvising, a worker may also get injured. Whilst improvisations and adjustments leading to everyday success are difficult to measure (or even notice), safety gets easily measured based on negative outcomes. Success and failure are equivalent and often matters of hindsight, outcome and judgment (of selected few).

Furthermore, minor improvisations and adjustments in complex socio-technical systems (i.e. systems comprising of humans working with technology for example ships, planes, hospitals, power plants etc.) may emerge in the form of major consequences. In a resource constrained world with systems being pushed to their limits this is not difficult to imagine. As Aristotle once said, the sum is greater than the parts. Finally human and technological functions in socio-technical systems may resonate in complex ways to generate unintended outcomes. For instance applying an incorrect helm in confined waters would have far serious implications for vessel safety than in open waters. Adjustments, equivalence, emergence and resonance are vital aspects of socio-technical systems.

Given that high risk facilities operate as complex socio-technical systems, it follows that the management of risk and safety requires a systems approach. One such methodological approach that has gained increased popularity in recent years particularly in high risk industries is Functional Resonance Analysis Method (FRAM). The practical application of the model is vast and generic. It includes management of everyday operations, management of change, system design, safety management, risk assessment, and monitoring of system performance. A unique strength of the model is that it could be applied for both risk management (forecasting) and accident investigations (regression).

The actual FRAM model aims to provide an overview of functional interactions and critical



interdependencies within the system (see figure). Each function consists of an input, output, control, resource, time and precondition. The overall aim is to understand how minor adjustments may become a source of significant performance variability in the system and lead to unintended outcomes (accidents).

The model aims to understand performance variability simply by examining how workers do their job (and not what the procedures may dictate). In so doing, the subtle details of workplace culture and the values and perceptions of workers can come to light.

Human error as we all know too well is the cause behind 90% of the accidents. But if for every one thousand successes there is one accident then what is the reason for 999 successes? Surely credit cannot be assigned to diligent rule following or robust technical designs – not at least in our industry! In a resource constrained world, adjustments and adaptability (or seamanship as we know it) are fundamental to understanding why things go right. By examining what normally goes right we would know why things sometimes can go wrong, and find constructive ways of controlling variability and improving performance. FRAM offers a structured method and conceptual framework.

Given that high risk facilities operate as complex socio-technical systems, it follows that the management of risk and safety requires a systems approach

For further information on how to build a FRAM model go to: http://functionalresonance.com/how-to-build-a-fram-model/index.html

Compliance with the ISM Code and the Maritime Labour Convention 2006

Robert Brindle, Lead Specialist Investigations, Lloyd's Register Marine

Compliance with international conventions might seem to be something taken for granted but it may surprise many people how often a ship receives a deficiency or is detained through non-compliance with international convention requirements.

At Port State Control (PSC) inspections there is an increasing trend for deficiencies to be raised in two particular areas – the ISM Code and the Maritime Labour Convention, 2006.

Ship owners and managers develop a Safety Management System for use within the Company but that system is only as good as the people who implement it. Deficiencies raised at PSC inspections, perhaps related to lack of maintenance, that might in the past have been given a Deficiency Action Code 30 (vessel detained) are being recorded as Deficiency Action Code 17 (rectify before departure) and marked ISM related. The detainable deficiency will typically record that a safety management audit by the Administration is required before departure and that the deficiencies raised are effective evidence of a serious failure, or lack of effectiveness, of implementation of the ISM Code.

It is worthwhile to observe that the lack of effective implementation of the ISM Code is not necessarily caused by a lack of action on the part of the ship's crew. A safety management system applies to the company as a complete entity, both ship and shore based, and it may well be that the deficiencies raised at PSC inspections are due to a failure by the company to order spare parts in a timely manner or to provide the required resources to ensure that maintenance is carried out on board.

The entry into force of the Maritime Labour Convention, 2006 (MLC) has provided further challenges to companies and ships with respect to compliance. Article V of the MLC dealing with implementation and enforcement responsibilities is very important because it establishes the principle of no more favourable treatment. This means that ships entering a port in a State where MLC has entered into force and flying the flag of a State that has not ratified MLC shall receive no more favourable treatment than ships flying the flag of any State that has ratified the Convention. States where MLC has entered into force are now able inspect any ship against the requirements of the MLC at a Port State inspection.

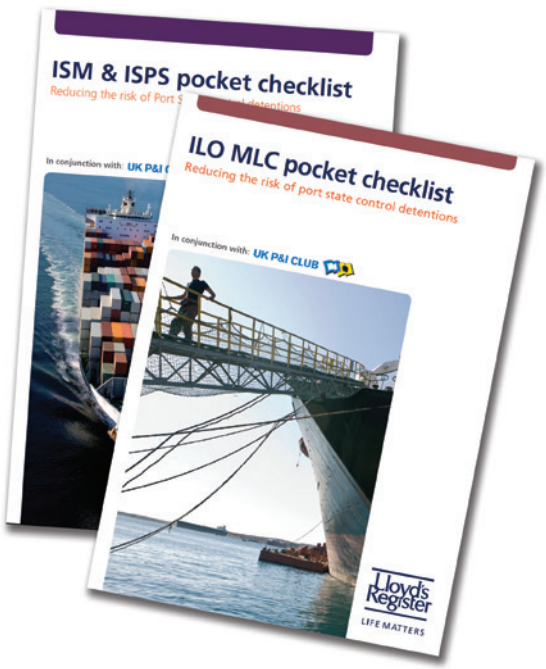
Many companies operating ships that fly the flag of a State that has not ratified the MLC do already request inspection of their ships against the requirements of the Maritime Labour Convention on a voluntary basis.

The difficulty for companies and ships crews is that shipboard compliance against the requirements of both the ISM Code and MLC will only be checked by the Flag Administration, or the Recognised Organisation on their behalf, at intervals of between 2 and 3 years. Therefore it is the responsibility of the ships' crew to ensure ongoing compliance on board.

So we come back to people and people can be fallible despite the best of intentions. However there is help out there. Lloyd's Register and the UK P & I Club, for example, have collaborated for a number of years in the production of a series of Pocket Checklists and these provide a wealth of information for masters and ships' officers to help prepare for PSC inspections, particularly with respect to ensuring compliance with the ISM Code and MLC.

The Pocket Checklists, which are available in hard copy or as an App for iPhone, iPad or Android devices, detail areas that PSC officers will want to inspect and identify requirements to allow masters and ship's officers to self-check compliance prior to arrival at a port.

To download the pocket checklists go to: http://www.webstore.lr.org/category/20-checklists.aspx



This bulletin is distributed and promoted with the kind support of:
Global Maritime Education & Training Association (GlobalMET); International Federation of Shipmasters' Associations (IFSMA); International Institute of Marine Surveying (IIMS); Institute of Marine Engineering, Science and Technology (IMarEST); International Maritime Pilots' Association (IMPA); NewsLink; Royal Institute of Navigation (RIN); Royal Institution of Naval Architects (RINA)

Alert!
The International Maritime Human Element Bulletin

Editor: David Squire, FNI

Published by the Nautical Institute, the world's leading international professional body for qualified mariners

www.nautinst.org
Membership info: sec@nautinst.org

Cover story: Captain Nick Beer, FNI

Centrespread & masthead image: Danny Cornelissen
www.portpictures.nl +31625555172

Printing: Indigo Press +44 (0)23 8023 1196

Website: Pixl8
www.pixl8.co.uk/ +44 (0)845 260 0726

Design & artwork production by:
Jacamar (UK) Ltd: www.jacamar.co.uk