End-to-End Assurance

Author:

James Inge

Keywords:

Audit, assurance, end-to-end, governance, safety management.

Abstract:

In a recent change of Ministry of Defence policy, endorsed by the Second Permanent Under-Secretary and soon to be published in JSP 815 (ref. 1), the Department's Functional Safety Boards have been asked to take on a new remit: providing End-to-End assurance of safety. But what does this mean? And how will it affect day-to-day business in the Department? This paper describes the Ship Safety Board response to the End-to-End challenge.

Introduction

Governance is the business of governing an organisation: setting its goals, directing how they will be met and monitoring progress. Assurance is the feedback part of governance. It is the process that gives confidence that the policies set by senior managers are actually being carried out.

A large part of assurance is the normal management process of reporting risk, opportunity and performance information back up the line management chain. This can be considered "*bottom-up*" assurance, flowing vertically through the management hierarchy. Bottom-up assurance gives senior managers the confidence that their direction has flowed down to lower levels of the organisation by reporting the results back up the same communication path. By aggregating results at each organisational level, bottom-up assurance can achieve 100% coverage of the Department's business.

The disadvantage of the simple form of bottom-up assurance is that it can smack of "marking your own homework". Because assurance is reported by the people who are responsible for doing the work (also referred to as "*ensurance*"), it potentially suffers from a number of flaws. Problems may not be recognised and highlighted either due to groupthink[1], lack of experience in a particular area, or because people are less likely to notice their own mistakes. There may also be a temptation to filter bad news out of reports. For these reasons, independent assurance is often sought in business-critical areas such as safety. The higher the risk involved, the greater the level of independence that is required to give adequate assurance that the business is being appropriately managed.

The MOD has set up Functional Safety Boards (FSBs) to provide the Secretary of State, through 2nd PUS, with independent assurance about the level of safety performance and the effectiveness of safety management in every area of the Department. By supporting bottom-up assurance through techniques such as audits, the work of the FSBs has had some success in building confidence in the Department's processes, but this approach has its drawbacks.

Bottom-up assurance gives confidence that separate areas of the business are performing effectively, or in accordance with a standard. However, it does not give much confidence that different organisational units are working together to deliver the top-level outcomes desired by senior management. The introduction of the new offence of Corporate Manslaughter (ref. 2) has raised managers' awareness that safety must be managed effectively across the business, not just in isolated areas. Safety is an emergent property that is not a function of any one component of a system or organisation. It is the product of the interaction of many different components. End-to-End (E2E) assurance attempts to give confidence that the whole Department (and its suppliers) are working together.

[1] A process of reasoning or decision-making by a group, especially one characterized by uncritical acceptance or conformity to a perceived majority view.

End-to-End Assurance

The idea of End-to-End safety assurance comes from the concept of End-to-End logistics. E2E logistics is about ensuring that when the user in the field has a need for something (a capability, service or piece of equipment), everything necessary comes together efficiently and effectively to fulfil that need. This might mean supplying something from a catalogue, or it might mean developing an entirely new product. Either way, many different areas of the Department will need to work together to deliver the desired outcome.

E2E safety assurance is similar to E2E logistics, in that it is about giving confidence that all areas of MOD are working together to ensure the safety of front-line users and anyone else who could be affected by our activities. It is not focussed on checking whether each individual organisational unit is conforming to its own policies and requirements. Instead, it looks at whether the organisation as a whole is working effectively to deliver the required levels of safety.

The Ship Safety Board has chosen to define "*End-to-End*" as

"between the designer and the end user, across all lines of development, and including suitable feedback loops".

This definition was chosen to reflect the belief that clarity of communication between the designer of a system and its user (operator or maintainer) is vital to safety, and this extends across a number of supporting domains such as training and information systems. The communication needs to be two-way, so that issues are reported and addressed before they can accumulate and lead to problems which negate the designer's intent for a safe system. For brevity, "designer" and "user" are used in a broad sense. "Design" can include many levels of requirements capture and architectural design, while "use" can include maintenance, logistics, or other activities where people are exposed to risk.

To fulfil its role, E2E assurance must look at all relevant activities and processes, wherever they are carried out. It needs to include all lines of development[2] and all relevant areas of the MOD, and may extend to our external suppliers. For equipment and platforms, it must consider all stages of the CADMID project lifecycle (Concept, Assessment, Demonstration, Manufacture, In-service and Disposal). However, it must also consider projects that are not managed through the formal CADMID cycle (such as organisational changes), and non-project activities, such as day-to-day management or the procurement and supply of commodities.

The MOD has a complex organisational structure that has evolved to deal with the challenges of both supporting operations and efficiently acquiring equipment and hence is not necessarily optimised for efficient management of safety. The structure results in a large number of internal organisational interfaces, so a large part of E2E assurance needs to be focussed on checking that these interfaces are working.

The Ship Safety Board End-to-End Assurance Model

The SSB has to answer the question "Is MOD shipping being managed safely?" The letter of delegation to its Chairman requires it to report assurance of this. A single "maritime safety management system" does not exist explicitly, but is in effect a federation of safety management systems operated by the various organisational pillars. This means that there was no obvious standard that the SSB could use as a yardstick. The Board therefore needed to generate a framework or model against which it could assess the overall effectiveness of ship safety, without imposing an additional layer of management which could confuse lines of accountability.

[2] Training, Equipment, Personnel, Information, Concepts & Doctrine, Organisation, Infrastructure and Logistics.

In developing an appropriate model, a number of sources relevant to the management of high-hazard activities were examined. Among these were the Health & Safety Executive (HSE) publication "Successful Health & Safety Management" (HSG 65), the International Maritime Organisation (IMO) International Safety Management (ISM) Code and the Licence conditions applied to the management of UK Nuclear facilities (refs. 3, 4 and 5).

HSG 65 lays great emphasis on the design and implementation of effective "*risk control systems*" (RCSs). The purpose of such control systems is to make sure that appropriate workplace precautions are implemented and kept in place. HSG 65 gives examples of possible RCSs associated with inputs, processes, and outputs from an organisation.

The concept of risk control systems working as defensive layers against major accidents is developed in another HSE publication, HSG 254, produced jointly with the Chemical Industries Association. This refers to James Reason's "Swiss Cheese Model", postulating that "(major) accidents result when a series of failings within several critical risk control systems materialise concurrently". The path of an accident sequence from the occurrence of a hazard to a harmful event is blocked by a stack of cheese slices representing the scope of each RCS. Holes in the cheese represent defects in the RCS or gaps in coverage. Most trajectories between a hazard and the occurrence of harm are blocked by at least one RCS, but where the holes in each layer align, there is no defence and an accident may occur. HSG 254 focuses on developing proactive and reactive indicators to monitor the RCS performance (ref. 6).

The ISM Code was introduced by the IMO in 1998 in the aftermath of a number of accidents in which poor safety management was a factor, notably the *Herald of Free Enterprise* ferry disaster in 1987. It focuses on a number of aspects of safety management which are not covered by the traditional emphasis on material safety. Among these are:

- Conduct of shipboard operations in accordance with documented procedure
- Emergency preparedness
- Reporting/analysis of non-conformities, accidents and hazardous occurrences
- Maintenance of the ship and equipment
- Control of documentation and data
- Verification, review and evaluation
- Certification

Many of these themes correspond closely to Licence conditions employed by the HSE Nuclear Installations Inspectorate as the basis of the regulation of nuclear facilities. These license conditions do not relieve the licensee of the responsibility for safety. They are non-prescriptive and set goals that the licensee is responsible for meeting, amongst other things by applying detailed safety standards and safe procedures for the facility. The arrangements, which a licensee develops to meet the requirements of the licence conditions, constitute elements of a nuclear safety management system. Both the general goal-setting tone of licence conditions and the particular emphasis on management of change were drawn from to develop the Ship Safety Board's subsequent safety model.

Using the sources outlined above and recognising the existence of a number of significant elements of risk control already in place in the MOD, a model was constructed based on existing organisationally-based (vertical) safety management systems forming a matrix with eleven cross-cutting 'risk control systems', as shown in Figure 1. This is termed the End-to-End Safety Model.

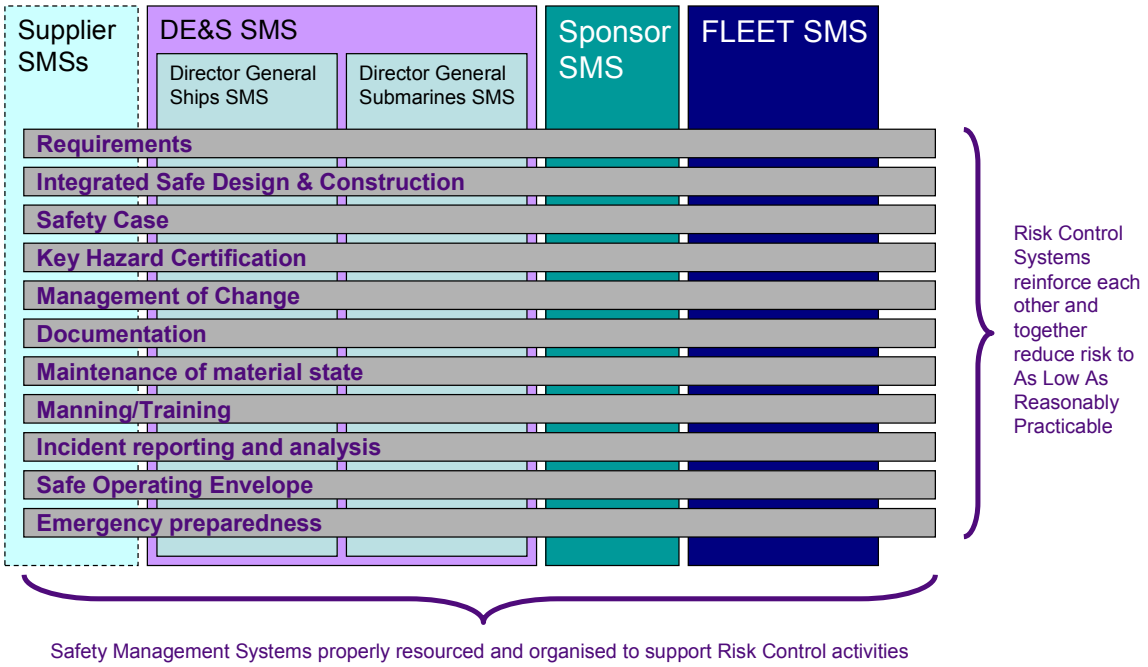

Figure 1 — The End-to-End Safety Model

The twelve risk control systems (eleven cross-cutting systems, supporting and supported by the organisational safety management systems), have a large degree of overlap in scope. This is intentional: multiple layers are required in the Swiss Cheese model to give confidence that faults in one RCS will be covered by another. However, the overlap does allow debate over the choice of definition for each RCS. There is also overlap with other engineering and project-management systems that are not purely focussed on safety, e.g. quality, reliability. The selection used by the SSB tries to reflect the guidance mentioned above and the current practice within MOD. It was recognised that many of the necessary processes were already in place, but often informally or in a piecemeal manner and not usually designed holistically. The role of the Ship Safety Board (policy, assurance and regulation) was not to tackle this directly, but to put in place a framework to illustrate what "good" looks like, and to progressively seek measurement and improvement.

Accordingly, for each RCS, a basic framework was developed setting out:

- the Scope of the RCS – what it had been chosen to cover
- the generic Risk that it was intended to mitigate
- the Goals to be achieved – what "good" looks like

As an illustration, Figure 2 shows the Scope, Risk, and Goals for the Safe Operating Envelope RCS.

Risk Control System: Safe Operating Envelope

Scope: The scope of this RCS covers the processes for defining and promulgating conditions and limits for safe operation of ships and systems and then for ensuring that these are understood and adhered to, with adequate on board oversight. Scope also extends to the arrangements for risk assessment and approval for waivers for operation outside the normal envelope.

Risk of inadequate control in this area: Unauthorised operation of systems outside designed conditions and limits, as a result of either lack of knowledge or deliberate violation, leads to safety risk.

Goals to be achieved:

- Safe operating envelope clearly defined
- Conditions and limits communicated to all personnel responsible for complying
- Adequate on board supervision of operation within approved limits
- Reporting/review mechanism for any breach of limits
- Defined process for risk-assessing/approving essential operation outside envelope

Figure 2 — Summary of the Safe Operating Envelope Risk Control System

If all the goals for each risk control system were being substantially met, and evidence of this existed, then it is asserted that the Ship Safety Board would be in a sound position to give assurance that MOD Shipping was being safely managed. This argument can be put forward in goal-structuring form (ref. 7), as shown in Figure 3. A high-level diagram like this allows any weaknesses in control systems to be illustrated in the context of the whole MOD safety system (e.g. by using traffic-light colouring in the boxes to represent the performance of each RCS). It also shows the continuing importance of the areas which work well to be shown. If necessary, the structure can be expanded to show the detailed supporting arguments and evidence.

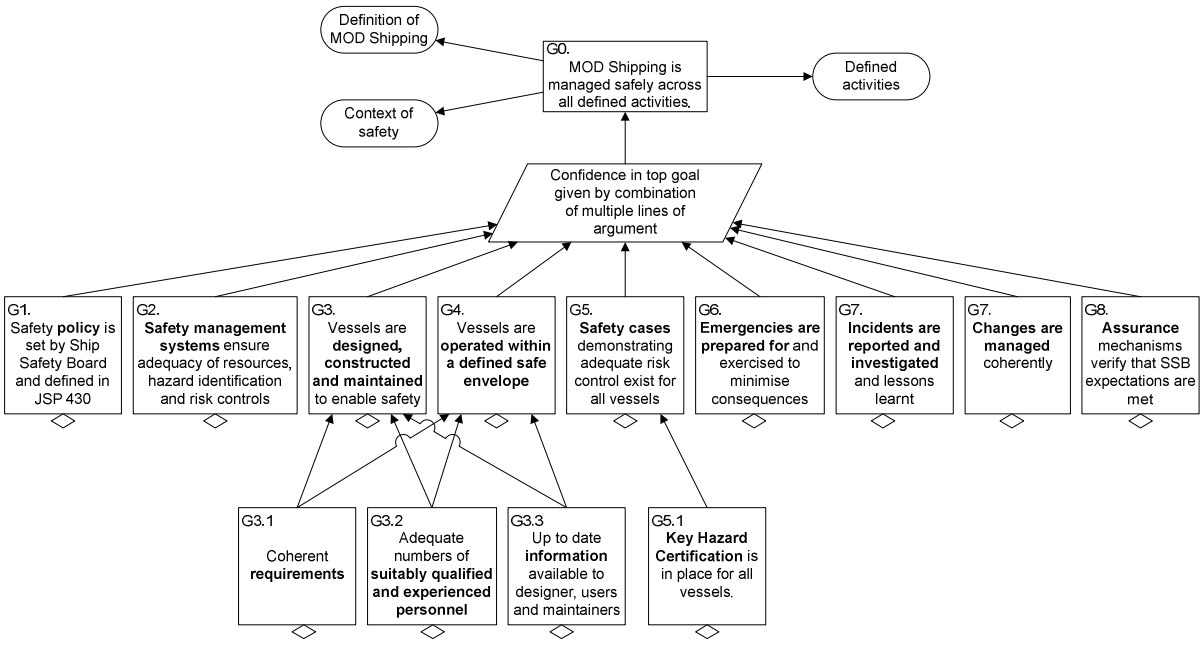

Figure 3 — Goal Structure for Safety of MOD Shipping

End-to-End Assurance Reviews

Traditional audits normally involve asking a series of questions to examine whether a system complies with a prescribed standard or policy. End-to-End Assurance Reviews take a more holistic approach, by looking at how effectively the organisation works together to meet its goals.

The aim of an E2E Assurance Review is to examine the practical working of an area of end-to-end risk control in order to provide both assurance of the extent to which it is functioning effectively in reducing safety risk, and also constructive and practical recommendations to improve effectiveness. The process for undertaking this is being developed but is based on the following principles:

- Reviews will be of the overall effectiveness of a process in reducing risk, not of specific organisations.
- Audit skills and techniques will be used in undertaking reviews, but use of the term 'audit' will be avoided.
- The programme of reviews will be tailored as a result of consultation with stakeholders and the SSB on priorities relating to perceived risks and weaknesses.
- Each review will be tailored to address known or perceived weaknesses.
- Reviews will seek to improve the E2E model by validating the RCS scope and goals.
- Recommendations made by reviews will be subject to a consultation process so that they stand maximum chance of implementation (Better to have an 80% solution with full buy-in, rather than a 100% solution with no buy-in).

As these reviews are carried out, it can be expected that the underlying model will be developed and refined. Senior managers may take a view on which areas are more, or less, useful in giving them confidence that their responsibilities are being adequately discharged. Future accidents may reveal other areas which are not being adequately addressed, leading to refinements of the model.

An E2E Assurance Review has been carried out on the performance of the Incident Reporting and Analysis RCS. This included an initial review of policy and instructions, to survey what documented processes exist for following up accidents and incidents, then a review of how incidents reported by a representative selection of ships had been followed up in practice.

The policy survey identified various different reporting systems, catering for different types of incident and different customer groups, but with a significant degree of overlap between some of the systems. While the individual systems seem to function reasonably well, staff may lack awareness of the variety of different systems, and few of the systems are optimised to contribute to improvements in safety. The review has highlighted potential improvements in how data is distributed that could improve its utility, and resource issues that are limiting the potential for exploiting the data. The full results of the review will be published separately.

While carrying out the assurance review on incident reporting and analysis, it was noted that the review activity itself had a positive safety benefit, aside from any recommendations it might make. By asking questions, it prompted all involved to get a better understanding of how their work fits in with the rest of the Department and to think about how they could contribute more effectively.

Other Applications of the End-to-End Safety Model

As well as specific reviews, the End-to-End safety model is beginning to be used to structure the duty holder reports presented to the Ship Safety Board's six-monthly meetings. In some business areas it is also being used to help generate performance metrics. By highlighting the goals to be achieved by risk control systems, the model helps staff identify metrics that are relevant to their own area of business and are also good indicators of the overall safety management effectiveness of the organisation.

By promulgating the end-to-end safety model, awareness of the various risk control systems is beginning to be raised across the MOD Shipping community. This should be beneficial by showing staff in different areas what they need to achieve together and where they can contribute. Eventually this could lead to the foundation of a unified maritime safety management system. However, the SSB will set high-level goals rather than attempting to find a one-size-fits-all policy at the detailed working level. The Board has adopted the philosophy that process design should be driven by the particular problems posed by MOD Shipping.

Conclusions

End-to-end Reviews provide a method of gaining assurance of the effectiveness of safety management across the whole scope of an activity within a large enterprise, rather than across many activities within a small organisational unit. They do this by defining goals to show what good performance should look like in the systems used to control the risk posed by the activity, then looking for evidence to show how well the goals are being met. Because this goal-based approach is not specific to the particular processes used in any given business area, it can be applied across the boundaries between organisational units.

While end-to-end reviews of a single risk control system may be less representative of the enterprise as a whole than an audit of a sample of organisational units, it is believed that better assurance will be provided within the scope of that review. This is because there is a clear link between the review's scope, the risks that need to be controlled and the goals set for the systems that control them.

Having developed the methodology for assurance of the safety of MOD Shipping, it must now be further tested in practice to determine whether it provides the level of assurance desired by the Ship Safety Board and other senior managers.

Acronyms

CADMID	Concept, Assessment, Demonstration, Manufacture, In-service and Disposal
E2E	End-to-End
FSB	Functional Safety Board
HSE	Health and Safety Executive
IMO	International Maritime Organisation
ISM	International Safety Management
JSP	Joint Service Publication
MOD	Ministry of Defence
PUS	Permanent Under-Secretary
RCS	Risk Control System
SSB	Ship Safety Board

References

1. Ministry of Defence, Joint Service Publication 815 – Defence Safety and Environmental Management, JSP 815, London: MOD, October 2006.
2. Corporate Manslaughter and Corporate Homicide Act 2007. c.19.
3. Health and Safety Executive, Successful Health and Safety Management, HSG 65, 2nd ed. (amended). Sudbury: HSE Books, 2000 (2003). ISBN 0-7176-1276-7.
4. International Maritime Organisation, International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code), Resolution A.741(18) adopted 4 Nov 1993. London: International Maritime Organisation, 1993 (amended 2000, 2004). Available at http://www.imo.org/HumanElement/mainframe.asp?topic_id=182
5. Health and Safety Executive, Nuclear Site Licence Conditions, Health and Safety Executive website, retrieved 24 Mar 2008. http://www.hse.gov.uk/nuclear/silicon.pdf

6. Health and Safety Executive, Developing Process Safety Indicators, A step-by-step guide for chemical and major hazard industries, HSG 254, Sudbury: HSE Books, 2006. ISBN 0-7176-6180-6.
7. Tim Kelly and Rob Weaver, The Goal Structuring Notation – A Safety Argument Notation, In Proc. DSN Workshop on Assurance Cases: Best Practices, Possible Outcomes, and Future Opportunities, 2004. http://www-users.cs.york.ac.uk/~tpk/dsn2004.pdf

Biography

J. R. Inge, Head of the Ship Safety Management Office, Ministry of Defence, Directorate of Sea Systems, Abbey Wood, Bristol BS34 8JH, UK, telephone – +44 (0) 117 913 5143, facsimile – +44 (0) 117 913 5943, email – DESSESea-SSMO@mod.uk.

Mr Inge was lead editor for Issue 4 of Defence Standard 00-56 – Safety Management Requirements for Defence Systems. His experience is as a project manager and safety policy specialist in the UK Ministry of Defence. He is a Chartered Engineer, holds a MEng from Durham University, and is working towards a postgraduate diploma in Safety Critical Systems Engineering at the University of York. He contributes to the IET/BCS Independent Safety Assurance Working Group and the IET's Technical Advisory Panel on Functional Safety.