THE JOURNAL OF NAVIGATION (2013), **66**, 789–797. © The Royal Institute of Navigation 2013

Forum

doi:10.1017/S0373463313000180

Computer Safety For Modern Bridge Systems

Dr. Mark Nicholson

(*Department Of Computer Science, University of York, U.K.*)
(E-mail: mark.nicholson@york.ac.uk)

Computer Based Systems (CBS) and Integrated Bridge Systems (IBS) are being introduced. They provide enhanced navigation capabilities and promote ship safety. However, they are highly complex and are becoming the primary source of data/information used to navigate ships. CBS issues have arisen that challenge current safety assurance and certification practices. This paper explores the potential contribution of System Safety Engineering including technical, operational management and crew capability contributions to CBS/IBS safety. A six step roadmap for the production of best practice guidance for the safe development and operation of such systems is presented.

KEYWORDS

1. Integrated Bridge Systems. 2. System Safety. 3. Future Roadmap.

Submitted: 25 February 2013. Accepted: 29 March 2013. First published online: 29 May 2013.

1. INTRODUCTION. A significant number of new computer-based enhancements are incorporated into bridge systems. For example, Electronic Chart Display and Information Systems (ECDIS) are built on Electronic Navigation Charts (ENC) data (IMO, 2010) (Figure 1).

There is an ongoing push for integration of electronic equipment to alleviate workload and to maximise benefits to the operator. For example, Marine Electronic Systems Ltd (Marine Electronic System, 2013) markets itself as "systems integrator, supplier and installer of navigation systems (including integrated bridge systems), radio communications, Closed Circuit Television and video surveillance, internal communications and crew entertainment and mission systems."

According to the International Maritime Organisation (IMO) "The strategic vision for e-navigation, [is] to integrate existing and new navigational tools, in particular electronic tools, in an all-embracing system that will contribute to enhanced

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

Figure 1. ECDIS and Integrated Bridge Systems (Kongsberg 2013).

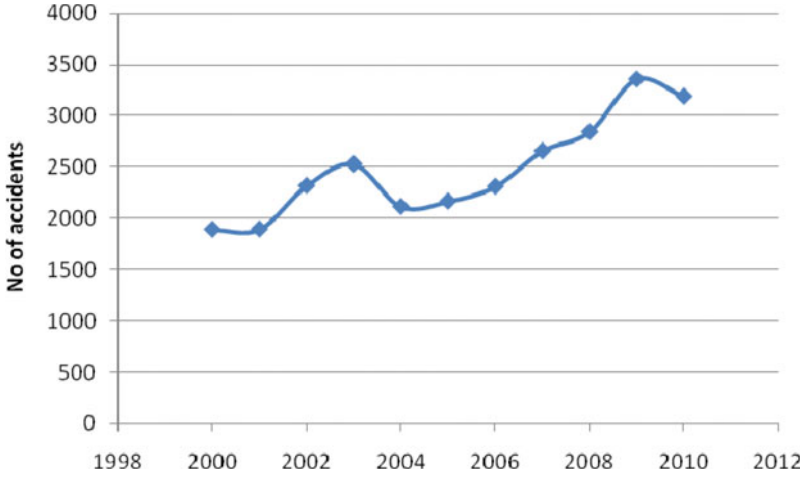

Figure 2. Navigational Safety (Uriasz, 2011).

navigational safety (with all the positive repercussions this will have on maritime safety overall and environmental protection) while simultaneously reducing the burden on the navigator." (IMO, 2013).

Despite the increase in technology and mandatory carriage of equipment such as ECDIS, the total number of navigational accidents of sea-going vessels has been increasing, see Figure 2.

What are the implications of these ongoing changes on the capability of bridge crews, the workloads they will face and the implications of Computer Based Systems (CBS) on ship safety? How can the expected improvements in navigational safety be assured? How these impacts can be understood and controlled is the focus of this paper. System Safety Engineering (SSE) and Safety-Critical Systems Engineering (SCSE) have evolved to address such issues. The elements of these disciplines will therefore be discussed first. The issues that can be addressed using these approaches

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

will be highlighted. Finally, a roadmap to adapt and incorporate these disciplines to ensure safety for the operation of ships incorporating such technologies will be presented.

2. SYSTEM SAFETY AND SAFETY-CRITICAL SYSTEMS ENGINEERING.

Safety is the "state in which the risk of harm to persons is reduced to, and maintained at or below, an acceptable level *through a continuing process of hazard identification and risk management*" (ICAO, 2009). An event that causes harm is an accident. A ship hitting an underwater obstacle has suffered an accident. SSE uses "systems theory and systems engineering approaches to prevent foreseeable accidents, and to minimise the result of unforeseen ones" (Leveson, 1995). A hazard is "a condition resulting from failures, external events, errors, or combinations thereof where safety is affected" (SAE, 2010). A ship that is unaware of underwater obstacles is in a hazardous state.

SSE emphasises building in safety features and explores the emergent safety characteristics of a system through analysis, as well as operational experience. SSE is fairly mature in the aerospace, military, railway and industrial process industries. It is less mature in domains like health services and Civil Maritime. Each domain tailors the details of the engineering process to its needs. However, SSE has six basic elements:

- *Understand the system of interest.* This includes not only how the system works but also how it may fail and the environmental/human/organisational context that the system operates in. The same system operating in a different environment will have different safety characteristics.
- *Identify and evaluate safety risks associated with the system*. Safety risk is measured as the product of the severity of the worst credible outcome and the probabilities of the set of safety outcomes occurring. So the risk associated with the hazard of "unaware of underwater obstacles" would be the loss of the ship times the probability of this happening. To determine the safety risks, usage pathways are identified and how failures affect these pathways. States that the system passes through and the outcomes of sequences of causal events are investigated.
- *Develop means of controlling risks*. In this step, the costs and benefits of a range of different hazard mitigation approaches are employed to eliminate the hazard, reduce its probability, give warnings that the hazardous state has been reached so that a fail-safe operation can be effected or a safety procedure enacted by the bridge crew. Multiple means of becoming aware of underwater obstacles and fail-safe scenarios may be provided.
- *Verify effectiveness of controls*. Analysis, testing, and operational feedback are employed to provide evidence of the effectiveness of the built-in control mechanisms.
- *Provide evidence of acceptable safety*. A safety case (Despotou et al., 2012) or conformance argument (Graydon et al., 2012) is produced to verify the overall level of safety risk the system exposes the ship to. This is used both for certification purposes and to ensure levels of safety acceptable to operators of the

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

ship and the public. The CBS/IBS is put into service on the basis of this argument and the evidence that backs it up.

- *Maintain safety throughout system life*: Inevitably the level of safety seen in operation will not be that envisaged at design time. It will also change through time as the equipment, usage profiles, and reliance on the equipment changes. As a result, a formal operational Safety Management System (SMS) (ICAO, 2009), including safety monitoring, is required.

Safety Critical Systems Engineering is the sub-discipline of SSE that focuses on the operational and technical impact of CBS on the safety characteristics of a system. It employs "*a systematic approach to identifying, analysing, tracking, mitigating and controlling software hazards and hazardous functions (data and commands) to ensure safe operation within a system*" (NASA, 2009). It addresses random failures of hardware components, systematic failures of the functional services being provided and human-machine interaction issues that can contribute to, or undermine, mechanisms intended to control safety risks.

3. SOFTWARE BASED SYSTEMS & BRIDGE OPERATIONS.

CBS are used in a number of ways in systems. First, to directly control the operation of equipment, for example engine management systems. Secondly, they are used to present data to an operator in such a way that they can extract information and take appropriate actions.

Leveson (Leveson, 2002) identifies information hazards as new types of hazards: "*Our increasing dependence on information systems are,* [...] *creating the potential for loss of information or incorrect information that can lead to unacceptable physical, scientific, or financial losses.*" Leveson (Leveson, 2002) also argues that: "*The 'head in the sand' approach of simply denying that software is safety-critical when it only provides information and does not directly release energy is becoming less and less acceptable as software plays an increasingly important role in accidents*." Ensor (Ensor, 2012) provides an illustration of the relationship between a typical navigational information system and potential hazards and accidents, Figure 3.

CBS are composed of hardware elements (sensors, computers, actuators), logic elements (software, VHSIC Hardware Description Language (VHDL), etc) and data elements (ENC, configuration tables, operator inputs, sensor values). Each of these elements is subject to failure and therefore can potentially have an impact on safety. Hardware failures are typically due to physical degradation mechanisms and are therefore random in nature. These failures are dealt with by setting maximum allowable failure rates and then providing evidence that the rate that will be seen in operation will be less than this target. Logic failures are systematic in nature, that is if the same input conditions hold, they will provide the same incorrect results. These logic failures could be due to a failure to specify the correct requirements on the system, an error introduced at design time, a change in the correct behaviour the system should exhibit in service due to a usage or environment change and a change in the system logic due to a change to the CBS. All of these elements need to be addressed to ensure that CBS do not introduce unacceptable behaviour in IBS.

Interactions between CBS and between CBS and Bridge crew are a significant source of failures that could lead to safety events. For example the ECDIS, and GPS

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

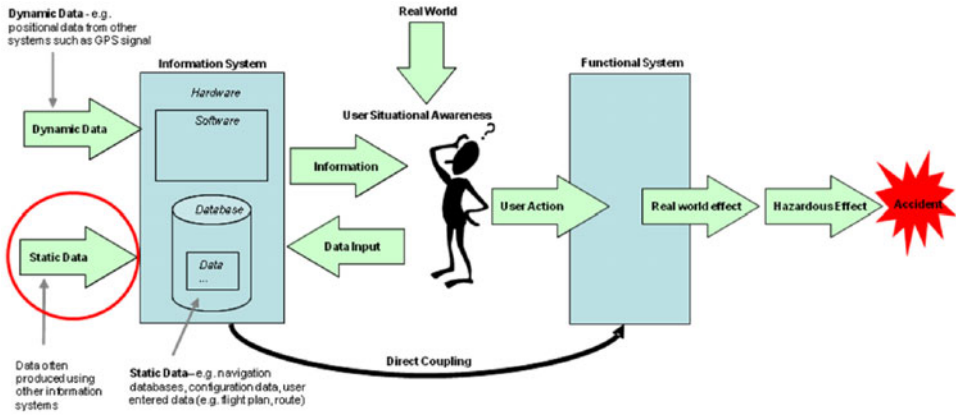

Figure 3. Data & Information Systems (Ensor, 2012).

systems can be incorporated into the autopilot to allow the ship to automatically manoeuvre around obstacles below the waterline. These larger integrated systems are known as Systems of Systems (SoS) (Rae and Alexander, 2012). Bridge crew have to monitor and instruct the CBS. As they become used to their operation, reliance on them grows and the actions of the crews adjusts to the perceived capabilities of the equipment. Unfortunately, Olivares (Olivares, 2002) has shown that a mismatch between the systems model of the appropriate action and the operators' mental model of operations can cause a breakdown that can lead to safety incidents. Crew need to be Suitably Qualified and Experienced Persons (SQEP) (HSE, 2007) to operate these systems when they are working but also when failures are extant.

A safety case provides "a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment" (MOD, 2007). Software safety cases consider the contribution of the CBS to this safety case. Best practice, risk-based, safety arguments decompose the safety claim into arguments that justify the acceptability of the risk posed by each identified system hazard. Software Safety Requirements (SSRs) should be valid, traceable and satisfied. If as a result of design actions new hazardous behaviour is identified this should also be mitigated. Figure 4 illustrates the four basic principles of software safety assurance (Habli, 2010).

Safety assurance of software is ultimately demonstrated by evidence. Types of evidence include testing, analysis, review and field experience. The only way to determine the sufficiency of the evidence is to consider its capability to address specific explicit safety assurance claims in a software safety argument. One lightweight approach to selecting and assessing software safety evidence (Hawkins and Kelly, 2010) is based on answering three questions:

- Is the *type* of evidence capable of supporting the safety claim?
- Is the particular *instance* of that type of evidence capable of supporting the safety claim?
- Can the instance of that type of evidence be *trusted* to deliver the expected capability?

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

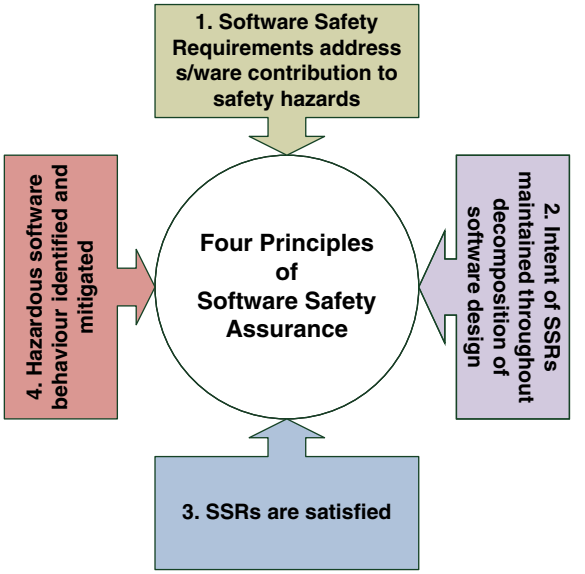

Figure 4. Principles of Software Safety Assurance (Habli et al., 2010).

The capability of a piece of evidence to support a claim is determined by the relevance, context and assumptions used, coverage and depth of design detail explored by the given piece of evidence. The trustworthiness of a piece of evidence is the confidence that the item delivers its expected capability. These elements together indicate the integrity of the evidence.

Data is the third element of a CBS and is at the centre of both direct control and information system CBS. Systems have a hierarchy of components; within this hierarchy the CBS have multi-layered architectures. Data is shared amongst the system's hierarchy and each level in the system's hierarchy may use the same data for different purposes. Data is created outside the CBS, is employed by the CBS and the results of the actions of the CBS are used to determine and undertake appropriate actions. Faulkner's (Faulkner, 2012) characterisation of a generic system that uses data is presented in Figure 5. Bridge operations could be considered to be one such system. A multi-layered architecture needs to be developed that incorporates the elements of this system and incorporates appropriate safeguards.

The final consideration for CBS safety is that of change management. A one-time only development of a safety case and/or certification compliance case is not appropriate. The safety cases must be maintained (Kelly and McDermid, 2001) in the face of increased understanding of the real characteristics of the system in its operating environment, changing operations, changing staffing levels and capabilities, changing system functionality, incorporation and integration of more systems throughout the lifetime of the CBS. This implies identifying the change, undertaking an impact analysis to determine the effect on the CBS and system safety case, updating the system and operations surrounding the system as required as a result, rebuilding the evidence via regression testing and reworking the set of ongoing monitoring actions. This is the role of the operational Safety management System (ICAO, 2009). As new

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

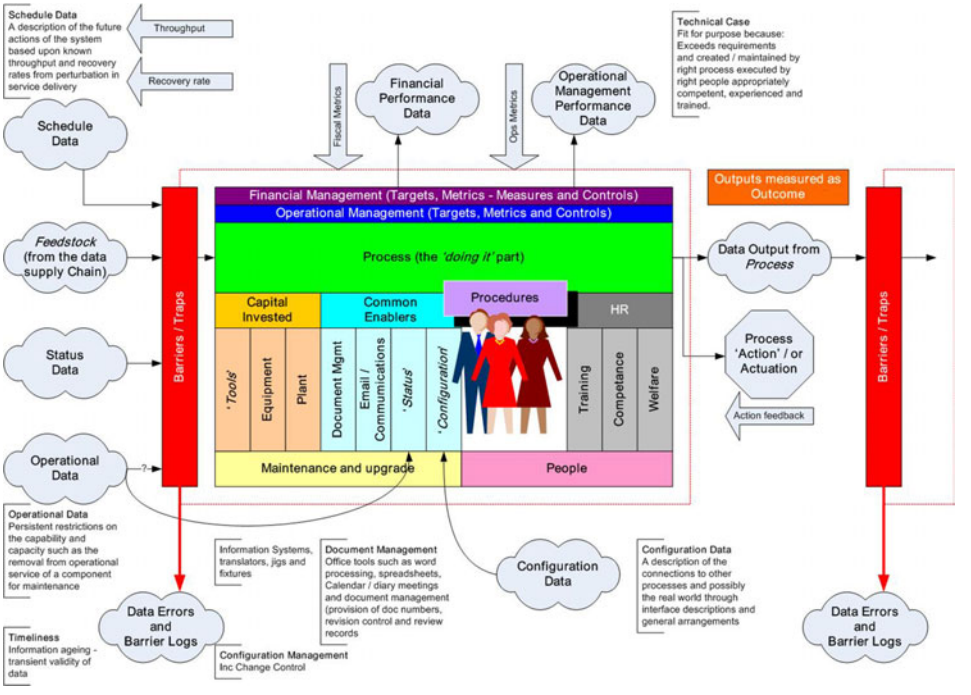

Figure 5. Generic System Incorporating Data (Faulkner, 2012).

technologies are introduced, rapid changes ensue in operations, working practices and what makes a crew SQEP.

4. CONCLUSIONS & FUTURE ROADMAP. Bridge systems incorporate a significant amount of complex computer-based functionality. The level of integration is expanding as the potential benefits of e-navigation become more obvious. Bridge crew working practices and staffing levels will change as this development progresses. The way that data is generated, packaged and incorporated is also changing. Numerous organisations are developing and selling compliant Computer Based Systems (CBS) packages via essentially an open network. All of these developments pose significant safety issues as they increase complexity, the set of interfaces to manage, and pose safety management issues. Ensor has already identified a number of instances where the Electronic Chart Display and Information Systems (ECDIS) and Electronic Navigation Charts (ENC) combination has led to safety incidents (Ensor, 2012).

It has been argued that a System Safety Engineering/Safety-Critical Systems Engineering (SSE/SCSE) approach is appropriate. The SSE approach emphasises the development of safety requirements that are flowed down to the CBS. Argument and evidence is provided of the contribution of CBS to safety and how any hazardous behaviour is controlled via appropriate built-in socio-technical safety features. Furthermore, an ongoing safety management regime backed by a maintained safety case is appropriate.

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

So what is the way forward?

i. Identify example existing systems and "systems of systems" (SoS) that are used in a bridge context. Use a systems engineering approach to model and understand the functionality, interfaces, associated operational procedures and environmental context.

ii. For the example systems and SoS, reverse engineer the existing system, system architecture, safety management system, safety risk control mechanisms and safety case.

iii. Critique this safety case against established SSE practices. Identify improvements and where tailoring standard SSE methods are required. For example, the way that different authorities require different solutions to the same risks, the significant variation in the ways that bridge operations are undertaken and the open network nature of the software provision will most likely need to be addressed in a unique manner. As a further example, domains such as the civil aerospace (RCTA, 2012) and automotive (ISO, 2012) make a clear distinction between standards for developing high quality software and those for developing safety-critical software. The appropriateness of such a distinction is not currently clear to developers and regulators of bridge equipment.

iv. Develop a Statement of Best Practice for CBS that incorporates a multi-layered architecture, an accompanying safety case and safety management system. This should take note of variation for direct control and information systems. It should also take into account data and data chain issues.

v. Run the best practice guidance by shadowing a research programme. For example there are a number of e-navigation research projects (ACCSEAS, 2013) developing prototype solutions.

vi. Run the best practice guidance in a development programme.

There are significant challenges ahead. The gain from the use of CBS is potentially high. However, reliance is transferred to such systems and as such they have the potential to be significant contributors to safety incidents. A way forward using the lessons from other domains exists.

REFERENCES

ACCSEAS. *Accessibility for Shipping, Efficiency Advantages and Sustainability Project*, www.accseas.eu/ accessed 8 January 2013.

Despotou, G. et al. (2012). Introducing Safety Cases to Health IT, *Proc. 4th Intl. Workshop on Software Engineering in Health Care*. Zurich.

Ensor, P. (2012). The Safety of Data & Information Systems. *BCS Workshop on Data Safety*

Faulkner, A. (2012). How to Stop Data Causing Harm – introduction. *BCS Workshop on Data Safety*

Graydon, P. et al. (2012). Arguing Conformance. *IEEE Software*, **V29**(3), 50–57.

Habli, I., Hawkins, R. and Kelly, T. P. (2010). Software Safety: Relating Software Assurance and Software Integrity. *International Journal of Critical Computer-based Systems*, **V1**(4), 364–383.

Hawkins, R. and Kelly, T. P. (2010). A Structured Approach to Selecting and Justifying Safety Evidence, *5th IET Conference on System Safety*, Birmingham, UK.

HSE (2007). *Managing Competence for Safety-related* Systems. Part 1: Key guidance", HSE. HSE.

ICAO (2009). *Safety Management System Manual doc 9859 ed2*. ICAO.

IMO (2010). *S-100 Universal Hydrographic Data Model. ed 1.0*. IMO.

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press

IMO. *E-Navigation* at www.imo.org/ourwork/safety/navigation/pages/enavigation.aspx, accessed 8 January 2013.

ISO (2012). *IEC-26262 Road vehicles – Functional safety*. ISO.

Kelly, T. P. and McDermid, J. A. (2001). *A Systematic Approach to Safety Case Maintenance*, *Reliability Engineering and System Safety*, **71,** 271–284.

Kongsberg Maritime. *ECDIS Chart Display System, K-Bridge*, www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/39DAD27FC6D37518C1256E150038656C?OpenDocument. Accessed 8 January 2013.

Leveson, N. (1995). *Safeware*. Addison-Wesley. ISBN: 0-201-11972-2.

Leveson, N. (2002). *System Safety Engineering: Back to the Future*, Accessed 2 January 2013: sunnyday.mit.edu/book2.pdf

Marine Electronic Systems Ltd, www.mesuk.com/, accessed 8 January 2013.

MoD. (2007). *Def-Stan 00-56 Safety Management Requirements for Defence Systems. Issue 4*. U.K. MoD

NASA. (2009). *Safety and Safety Assurance Definitions*. www.hq.nasa.gov/office/codeq/software/umbrella_defs.htm

Olivares, C. S. (2002). *Systems, Advisory Systems and Safety*. Department of Computer Science, University of Newcastle upon Tyne, UK.

Rae, A.J. and Alexander, R. (2012). Is the "Systems of Systems" a useful Concept for Hazard Analysis? *Proc 29th Intl. System Safety Conf. (ISSC)*. U.S.

RTCA. (2012). *DO-178C: Software Considerations in Airborne Systems and Equipment Certification*. RTCA.

SAE. (2010). *Aerospace Recommended Practice 4754a – Guidelines for Development of Civil Aircraft and Systems*, SAE.

Uriasz, J. (2011). Determination of ship's safe navigation lane in the navigational information system, *Annual of Navigation*, **17**.

https://doi.org/10.1017/S0373463313000180 Published online by Cambridge University Press