Comparison of safety system designs using risk assessment

Dr Mike Tainsh

BAE Systems Maritime, UK

ABSTRACT

Current work within the team of ergonomics, safety and operability specialists on user risk assessment for naval systems, has enabled the development of comparative techniques. They start from user system architectures, and the identification of user tasks in a form that supports assessment and mitigation of risks. In this paper the aim is to present assessment techniques for comparing safety aspects of design options. An example addresses the introduction of an automated information system.

KEYWORDS

User-centred risk assessment, complex systems, naval systems

Introduction

Risk assessment in ergonomics, when associated with user performance has tended to be identified with human reliability assessment (HSE, 2009) and quantified using measures or categories of likelihood. Safety assessments based on risk, are associated with both likelihood and impact of a hazard, and there is a need for comparing design options.

Performance and/or safety goals for complex (multiperson, computer based) systems are important and may be part of a more general HAZard and OPerability analysis (HAZOP). The hazards, to be controlled here, affect safety during work. The work is carried out by teams of users in combination with sets of equipment, in a range of operational conditions.

It is unclear how these risks might be quantified at a system level using conventional techniques. Hence, system designers and developers with responsibility for safety (for example Leveson and Thomas, 2018) need additional assessment techniques to compare system design options, and this work aims to provide a set.

The concept of risk is used frequently in ergonomics design work (for example MoD, 2019) often with little indication of how it might be used in the development of complex systems. This paper takes a concept of risk and indicates how it may be developed for addressing user performance in the context of complex systems assessment and comparison.

Aim of the study

The aim of this work is to develop a risk-based technique for use in the assessment of the safety characteristics of complex systems and in particular to understand the marginal differences between two sets of system designs. Previous work (Tainsh, 2019) has shown how the roles and tasks of teams of users can be represented for this purpose. This paper focuses on the assessment and comparison techniques.

The approach to assessment

There are four stages in this assessment process:

(a) Specifying the users, roles, tasks and equipment using the user system architecture (USA).
(b) Producing a task description of the team's working relationships, to help understand the task design requirements for the team.
(c) Quantifying the likelihood and impact of a hazard (the risk) as a result of individual user performance, their tasks and associated risk mitigation.
(d) Making a comparison of two or more sets of design characteristics with a view to making a judgment of preference.

A naval example – navigation

The design objective is to optimise the characteristics of a navigation system associated with its safety features and make a comparison between designs throughout the development process to ensure progress is being achieved, and goals being met. Optimisation is defined as risks at operationally acceptable levels (RAOAL) as defined in a previous paper (Tainsh, 2018).

The first stage is to specify the users, roles and equipment, along with the goals as defined by the hazard identification process or similar.

A control system as has four blocks of functions which become categories for describing user roles or sets of tasks:

- Sensing – includes gathering and collation of information and knowledge by members of the complex system team to feed through to the controlling function.
- Controlling – function carried out by senior personnel who have the responsibility for the performance and safety of the ship.
- Actuating – through the propulsion/steering system.
- Feedback – resulting from the motion of the ship, through the external environment and being detected by the sensors.

Suppose we have two design options as shown in Figure 1:

- Option A uses a sensor operator to provide reports on contacts around the platform
- Option B employs an automated information system (AIS) instead of a sensor operator.

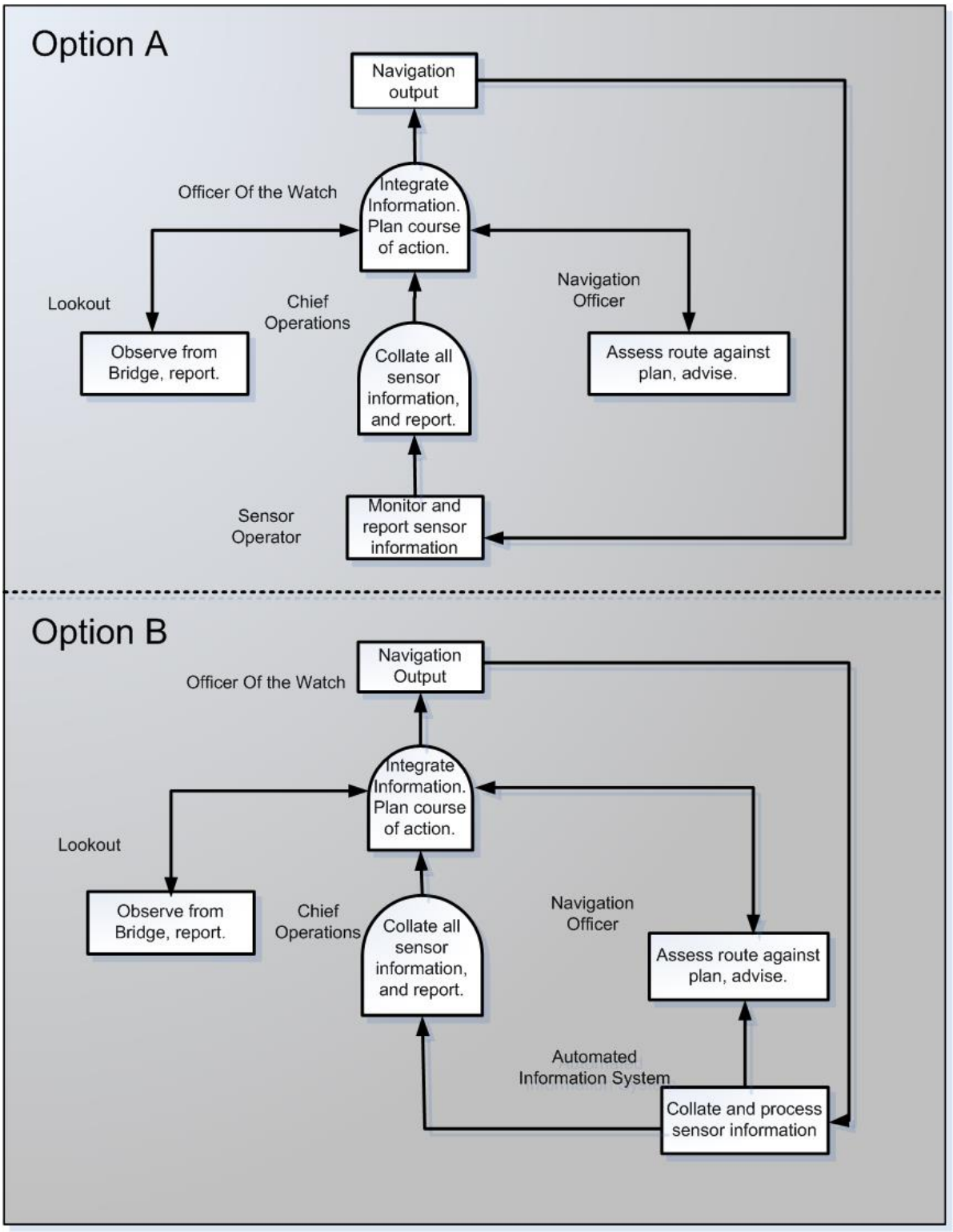

Figure 1: Design options for navigation control system.

Each of these options needs to be considered in turn and a comparison made of their characteristics.

The USA for this set of tasks is given in Table 1 for option A. Layers one, two, three and four are common to both options A and B, but in layer five option A has a sensor operator within the platform's operations room, whereas option B has an AIS.

Table 1: USAs (options A and B) for navigation.

Layer number	USA – task performance viewpoint		
1	Operational policy: effective and safe navigation.		
2	Operational requirement/scenario: move vessel through confined waters without grounding or collision, in other words safely avoiding hazards.		
3	Officer of the watch (OOW) within operations room. Task – Receives reports from navigation officer (NO) and chief operations (CHOPS), executes decision and command function on the basis of an understanding of the plan, platform control characteristics (actuators) and sensor information (from feedback).		
4	Lookout on bridge. Task – observes external objects and landmarks, reports to CHOPS and OOW.	CHOPS within operations room. Task – carries out collation of sensor information with reports from lookout. Reports to OOW.	NO in operations room. Task – receives reports from CHOPS and lookout, carries out comparison of actual versus planned location and motion characteristics. Reports to OOW.
5	Option A: sensor operator within operations room on above water surveillance. Task – obtains sensor evidence and reports to CHOPS.		Option B: AIS. Commercially available equipment is provided which provides a communications feed of contacts with their characteristics. Output available to CHOPS and NO.

This means that the risk analysis will be different from conventional human reliability analysis as described by HSE which depends on concepts of fault trees. This assessment is different because:

- It cannot assume independence of task- or performance-based events.
- It depends on concepts of control systems.
- It takes into account an assessment of the impact of hazards, including catastrophic failure.

The consideration of the task failures or errors must be compatible with the concept of a control system and its time-based processes. It is clear that the users may include checking for errors, and have the opportunity to recover any errors as part of their tasks.

Hence there must be three sets of elements, feeding through to the actuator:

- Sensors – in this case layers 4 and 5.
- Decision-making – in this case layer 3.
- The actuator is not considered part of the control system. Rather it provides a set of constraints about the nature of the control characteristics. In this case it is the propulsion and steering of the ship.
- Feedback to the decision-maker on system performance – in this case via the movement of the ship being detected and influencing the displays on the sensors.

In practice, there may be additional processes supporting the sensors and/or decision-maker.

Risk information and presentation

Table 2 shows how the risk information may be presented. It presents summary descriptions of the fault paths within each layer. These support an understanding of the organisational context of any possible error producing conditions:

- It enables an understanding of how risk characteristics change as information is processed through the work organisation and its equipment.
- It supports an understanding of how risks can change over the course of time or scenario.
- It enables an understanding of risk mitigation in relation to the hazard.

In particular, the upper and lower bounds of risk can be highlighted so the best and worst possible outcomes are known. The best paths are highlighted in Table 2. The human reliability estimates provided in Table 2 are for presentation purposes only. It is important for designers and potential users to understand the task performance associated with a hazard, to ensure that the likelihood of human error is compatible with the hazard risk category.

Assessment technique – comparison between design options, or requirements

Overall assessment

The overall comparison is made from the content of Table 2.

Table 2: Risk information for navigation control actions (greyed cells show the path with the highest probability of correct outcomes).

Layer No	Information sources or combinations				Task details	Human reliability information		
	Info source		Info source	Info source		Human reliability	Impact	Risk Cat
Layer 3	Operations team advice correct		OOW correct		Information or knowledge from sensor operators/CHOPS/AIS, navigation and lookout provides basis for making decisions and controlling vessel.	99.59	CRI	RAOAL
			OOW incorrect					
	Operations team advice incorrect		OOW correct					
			OOW incorrect					
Layer 4	Option A or option B correct	Lookout correct	Chief ops correct	NO correct	External information from sensors, including that from lookout is collated by CHOPS, and made available to OOW with route information supplied by NO.	99.69%	CRI	RAOAL
				NO incorrect				
			Chief Ops incorrect	NO correct				
				NO incorrect				
		Lookout incorrect	Chief Ops correct	NO correct				
				NO incorrect				
			Chief Ops incorrect	NO correct				
				NO incorrect				
	Option A or option B incorrect	Lookout correct	Chief Ops correct	NO correct				
				NO incorrect				
			Chief Ops incorrect	NO correct				
				NO incorrect				
		Lookout incorrect	Chief Ops correct	NO correct				
				NO incorrect				
			Chief Ops incorrect	NO correct				
				NO incorrect				
Layer 5	Option A with sensor operators, or option B with AIS			Sensor operator or AIS correct		99.99% for option A. Availability and security risks for option B	CRI	RAOAL
				Sensor operator or AIS incorrect				

Table 3: Comparison of system design characteristics.

Design feature	Comparison technique	Criteria
Goal satisfaction.	Comparison of overall risk at the highest layer, layer 3 in this case.	The design must demonstrate user performance to reach the agreed system risk criteria for the hazard as defined for an operational scenario.
Acceptability of performance levels throughout the set of tasks.	The risk scores at layers 4 and 5, or more are used to determine if any unacceptable risk is found as part of the event analysis.	The risk scores must meet RAOAL criteria in all cases. It is not acceptable for any path to be associated with unacceptable risks.
Potential for increase in risk with time.	The risk is not only assessed in terms of a given moment in time, but also as they might develop – increasing or decreasing.	There should be no increase in risk over time – any increase should be expected to be recovered. RAOAL criteria apply.
Adequacy of mitigation techniques.	The mitigation provided must be appropriate to the assessed risk level.	The mitigation techniques must be declared and demonstrated as meeting all risk criteria.

Goal satisfaction

A set of tasks must be identified for the team such that the predicted performance characteristics can satisfy the safety requirement. Unless an identifiable path exists, with an estimated likelihood that meets RAOAL criteria, then the design is invalid as a solution. The path (indicated in grey in Table 2) showing human reliability of correct performance must show sufficient levels of performance characteristics to meet agreed risk requirements – the combination of user reliability and impact.

Options A and B in Table 2 show the fault paths that were investigated with indicative reliability estimates of acceptable performance. The clear paths show the sequences associated with known partial and overall failure. There will be many paths, on a large-scale design, which are unacceptable and these should be assessed against RAOAL criteria so that mitigation can be applied.

Comparison of performance levels and error rates

There is a need to ensure that all possible task performance combinations as shown in Table 2 are assessed sufficiently well to ensure that one means of the system working is not being designed with disregard for other possible paths.

There will be a need to understand the consequences of failures which are non-human and the performance associated with them. All risks must be open to appropriate mitigation. The identification of risks is likely to be well understood by qualified and experienced users and their advice will be a major input to the design process.

The possibility exists for any continuous risks which have the potential to build up as bias or drift, over time, to turn into a performance risk where mitigation needs to be demonstrated.

Option B which may be open to bias, availability and security risks without user input may be open to additional investigation as a result of this comparison.

Inclusion of mitigation on Table 2

The mitigation information associated with the risk assessment may be included on Table 2, to provide a comprehensive record of the outcome of the assessment. Mitigation procedures were proposed and assessed.

In the example shown in Table 2, the introduction of the AIS may be considered as a mitigation feature for an unacceptably high likelihood of hazardous failure in the event of a lack of sensor surveillance, even if it was considered an unacceptable replacement for a user.

Conclusion

This example makes clear how risk arising from user performance can be addressed in support of the development of safety cases for large scale systems. Comparisons between design options can be made which are useful to supporting a user input. The likelihoods associated with the user performance will be indicative, but by laying the assessment open to scrutiny it is believed that system engineering advantage can be gained when making safety assessments.

This technique is currently being widely used within BAE Systems Marine and carries with it a number of advantages:

- Development of task descriptions using systems architecture and organisational diagrams in common use. These aid traceability of operational and safety related inputs.
- It provides an understandable summary of the high-level task descriptions showing risk and safety information.

References

HSE/HSL. (2009). Review of Human Reliability Assessment Methods.
UK Ministry of Defence. (2015). Acquisition Operating Framework.
Leveson, N. G. and Thomas, J. P. STPA Handbook. Private Publication.
Tainsh, M. A. (2018). User System Architectures in Naval Ergonomics – a New Paradigm. CIEHF Ergonomics & Human Factors Conference 2018.
Tainsh, M. A. (2019). Do our complex systems meet requirements? An example from naval ergonomics. CIEHF Ergonomics & Human Factors Conference 2019.