Complex Systems' Safety: an example from Naval navigation

Mike Tainsh, Ph D (Wales), CErg, FIEHF

BAE Systems Maritime, Frimley, UK

ABSTRACT

This work addresses the development and application of an ergonomics contribution to the process of safety assessment for complex systems. The approach is general, but in a Naval context.

KEYWORDS

Safety, assessment, complex systems

Introduction

The term "complex systems" is used here to refer to systems which have information and knowledge processing and handling as major functions e.g. for controlling remote devices during operations. Typically they are "closed loop" with high levels of automation. In this example, the objective is to reduce the risk to safety associated with a vessel, its complement and equipment, during operations. The aim of the investigations is to reduce safety risks to a level that is "tolerable" as defined within UK MoD, Defence Standards. The techniques emphasise both likelihood and impact/consequence of carrying out an operation safely through a consideration of the fault tree associated with controlling processes. Ergonomics tends to handle human errors as independent events; in this case they are within the control loop and it is necessary to understand the contribution of sequences of events defined by roles, equipment and task design to overall system safety.

Naval Example: Navigation of Safe Passage

Figure 1 represents part of a closed loop system for controlling navigation using a Layered Description. Layer 1 is the overall safety goal, Layer 2 is the description of the operational scenario, Layer 3 is the layer that describes the highest level of operations, and it is supported by Layers 4 and 5 which are technical layers. The control loop is guided by a decision maker (Officer of the Watch) in Layer 3 and the Navigation Officer working with route information coming from Layers 4 and 5 to meet the safety goal.

The quantitative assessment of safety related characteristics is presented as a process starting from fault trees based on the roles, tasks and information/knowledge flow (Figure 1). The next steps are:

- Develop observable likelihood data from trainers and SQEP Users to understand the likelihood of Users' task outcomes;
- Assess the impacts associated with User failures (whether user bias, drift, catastrophic failure or other) in conjunction in terms of risk to the safety of the vessel and its systems, operations loss, manpower efforts, cost etc.;
- Combine the likelihood and outcome estimates across a set of tasks e.g. from Operator to Chief Operations, to Officer of the Watch to generate a risk based assessment;

- Aggregate the sets of task information to characterise the safety risks for the complete system;
- Generate a "Safety Assessment" for the safety goal as shown in Figure 2.

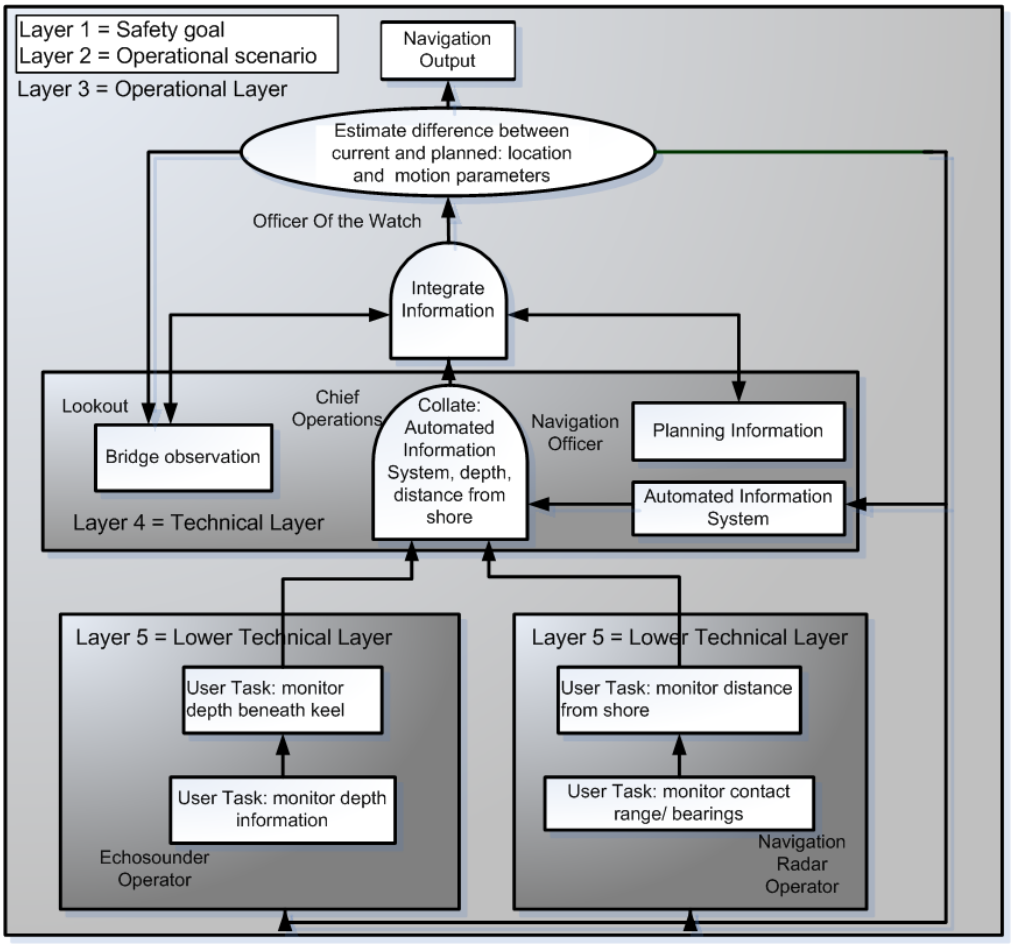

Figure 1: Layered description of roles and tasks showing information and knowledge flow

Assessment of the design of a complex system

The safety of the vessel must meet the criterion As Low As Reasonably Practicable (ALARP) i.e. at least "tolerable risk" as defined in Defence Standards. ALARP is estimated in terms of likelihood and impact as shown in Figure 2.

		Impact		
		Recoverable failure	Major failure	Complete failure
Likelihood of failing Goal	Highly unlikely	Trivial	Tolerable	Moderate
	Unlikely	Tolerable	Moderate	Substantial
	Likely	Moderate	Substantial	Intolerable

Figure 2: Risk matrix for specifying the Safety Assessment of a Complex System

Conclusion

The approach here is general and could equally be applied to a range of systems both military and civil. The strategy being developed here is being discussed across a number of BAE Systems applications with the intention of addressing the Navy Safety Centre's need to improve the safety maturity of Naval operations.