9th IFAC Conference on Control Applications in Marine Systems
The International Federation of Automatic Control
September 17-20, 2013. Osaka, Japan

Risk Assessment of Human Machine Interaction for Control and eNavigation Systems of Marine Vessels

Axel Hahn*, Andreas Lüdtke**
**University of Oldenburg, 26121 Oldenburg, Germany, (Tel: +49 441 798 4480; e-mail: hahn@wi-ol.de).*
***OFFIS, 26102 Oldenburg, Germany, (e-mail: andreas.luedtke@offis.de)*

Abstract: The design of human machine interaction for modern ship electronic systems has a significant impact on the safety of seafaring. There is a direct impact on the capability of the nautical personnel to efficiently recognize the situation and to decide correctly. Consideration of efficiency and safety in early design phases of eNavigation systems or other bridge equipment will improve the engineering processes in order to reduce design errors. Model driven design is one option for efficient development of technical systems that proves as a powerful tool getting popular due to the reusability of the models in verification, code generation etc. and leads to efficient processes. Based on former research on system engineering and on human machine interaction risks assessments using cognitive simulation this paper presents an integrated model based approach for analysis safety of human machine interactions. It combines technical, process and cognitive models for simulation based efficiency and risk assessment in bridge design.

Keywords: Navigation, Safety Analysis, Risk Assessment, Marine systems, Simulators, Human Machine Interface.

1. INTRODUCTION

Seafaring is and was always a joint undertaking between humans and their technology. Beside the impact of nature, such as wind, waves, etc. the reliability of the technical equipment and its correct usage ensure safe voyaging. This is still true with the introduction of eNavigation technology.

The eNavigation implementation process is accompanied by IMO's NAV and COMSAR sub-committees, as well as the International Hydrographic Organization (IHO) and the International Association of Lighthouse Authorities (IALA). These institutions did a comprehensive gap analyses as a part of their development of a joint implementation plan for eNavigation. In a ten year survey [GP07] investigated the causes of collisions and groundings, in which human error was the primary cause with 60%. Therefore the gap analysis of the IMO addresses numerous aspects of human machine interaction [IMO12], e.g. absence of structured communication link to notify incorrect operation of both shipboard and/or shore-based systems together with a lack of intuitive human-machine interface for communication and navigation means. Furthermore, the analysis revealed that existing performance standards/guidelines are not applied or are missing such as guidelines for usability evaluation [IMO12]. Analysing these gaps the IMO working groups identified user interface related requirements. They request:

- Ergonomically improved and harmonized bridge and workstation layout
- Single-entry of reportable information in single-window solution
- Integration and presentation of available information in graphical displays
- Provide an administrative human machine interface task concept for identifying updates and setting of presentation rules
- Implement harmonized presentation concept of information exchanged including standard symbols and text support taking into account human factors and ergonomics design principles to ensure useful presentation and prevent overload
- Develop a holistic presentation library as required to support accurate presentation across displays
- Harmonization of conventions and regulations for equipment
- Improved display of status of available data and indication of available updates
- Task-based information management

These requirements indicate why equipment providers should do a comprehensive usability and risk assessment of their products. IMO MSC Circular 878 states: 'A single person error must not lead to an accident. The situation must be such that errors can be corrected or their effect minimised. Corrections can be carried out by equipment, individuals or others. This involves ensuring that the proposed solution does not rely solely on the performance of a single individual.' Adaptive interfaces may provide the right information at the right time without inducing information overload. With a research background in system engineering / model driven design we propose the usage of models for usability and risk assessment in model driven engineering processes. During early design states adequate models of the product under development can be used to simulate the usage of the system to ensure safety and usability requirements. We bring together system engineering with simulation of cognitive models to make a risk assessments system including humans in control or execution function. The paper introduces a simulation environment to evaluate the product design based on several simulators to simulate traffic, vessel and systems response and human behaviour. Then we make a short digression about model based design because we want to demonstrate how to use models of first technical system design for usability analysis by using a co-simulation system. We propose a simulation environment and present the idea of using cognitive models to simulate seafarers (erratic) behaviour. So engineers can make first usability assessment in early engineering phases and avoid expensive redesign in latter design phases.

2. MODEL DRIVEN ENGINEERING AND VERIFIATION OF ENAVIGATION EQUIPMENT

Engineering new systems requires a broad understanding of technologies to be selected and applied to the design and methodologies to handle complexity of the undertaking. Therefore engineering applies methodologies (to define tasks and their order), methods and tools (to support the tasks / how they are done) in addition to their technological knowledge [PWL07]. Engineering itself is an iterative process of synthesis and analysis tasks. During synthesis concepts and technologies are selected, applied and the design is elaborated: The system is under design. Then engineers validate (fulfils the system the right requirements) and verify (are the requirements implemented correctly) their design. As early and iteratively as possible engineers can thus validate and verify their design developments to reduce cost and safe time. In electrical engineering Bell Laboratories introduced the concept of system engineering in the 1940s [Sch56]. To understand the product as a system with dedicated sub elements, a system border and defined relationships can help to manage complexity. With the advent of technologies to describe elements and relationship in a reusable way by using computer models made this approach also popular in other engineering domains.

Reusable computer models of the system under design (the system model) allow continuous flow of information between the different tasks and simple implementation of the mentioned synthesis/analysis loop. Paying attention to the early phases of system design (identify and validate/verify the concepts of the product) reduce the risk of later design changes which are mostly cost intensive. Using reusable models during the early phases that are later usable for design, validation and verification is named frontloading and aims at improving design efficiency. The usage of models and automatically generated implementation specifications from them is called model driven design.

The IMO Formal Safety Assessment Methodology (s. Fig 1) requires hazard identification and a following risk assessment [IMO02]. It will improve the engineering process to apply this assessment already as soon as possible and iteratively during the design process to identify problems and follow the next steps of the FSA methodology as a concurrent process. This has to address all kinds of hazards. All systems including humans and machinery are sensitive to errors induced by human machine interaction problems (e.g. derived from usability problems). Starting point has to be an understanding of the HMI induced hazards and to check the risks during system design. Systematically the risks and vulnerability of the system have to be checked on every design stage of the system. Risks overseen during first design concepts may never be detected or be detected too late inducing high costs due to required design changes.

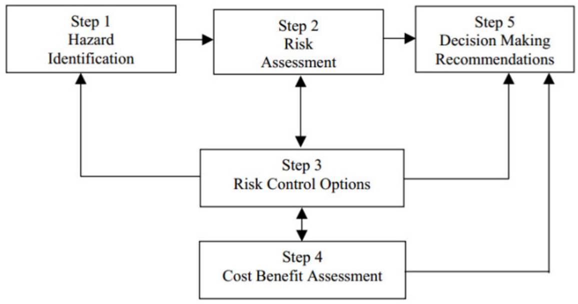

Fig. 1. IMO Formal Safety Assessment Methodology

Based on this requirement the authors propose a test bed for the required risk assessment to be implemented in a model driven design process by simulation systems to evaluate the designs. The system models are used by the simulator to systematically check hazards. A requirement with regard to the models is that they executable in a simulation environment.

3. SIMULATION SYSTEM

For the risk assessment we propose the approach depicted in Figure 2. The figure shows that the system model designed during the engineering process will be analysed by a co-simulation implemented in a joint simulation environment. Embedded in the engineering process the objective is to analyze the actual system model under design. For this the potential hazards are identified as requested according to the FSA methodology (upper left of Figure 2). The new system will be tested in a simulation of the environment of the system: the vessel in its actual traffic / manoeuvre situation (right simulator in the simulation environment which uses vessel and traffic models). The system may be used cooperatively by several users. They are implemented as agents in the simulation (left element in the environment in Figure 2). Cognitive models define the behaviour of the agents with respect of the normative processes which are defined by regulations. The embedding of the system model in the simulation depends on the phase of the engineering process. During the early design phases first functional models of the system can be analysed with the simulator. User agents directly apply a functional model of the system that is fed by a simulation of the environment of the vessel. In later design phases the system is elaborated and the user interface may be fully designed. Now its usage has to be analysed in context of a specific interface layout. The user interface specification has to be used to generate a virtual representation in a virtual bridge environment to be used by moving and interacting agents. The functional implementation of the new control or eNavigation system can run as a software sub system which is embedded in the