A New Approach for Human Factor Integration into Ship Design Process

Costantino BONGERMINO [a,1], Paola GUALENI [a], Fabrizio BRACCO [b], Michele MASINI [c] and Tommaso PICCINNO [c]
[a] *UNIGE DITEN, Italy*
[b] *UNIGE DISFOR, Italy*
[c] V.I.E. srl, Italy

Abstract. Ship safety and operations are driving issues of ship design and it is well recognized that such performances are strongly related to Human Factor (HF). In the paper a methodology to integrate HF into the ship design process since an early stage is envisaged, with the aim to improve the overall ship resilience when dealing with uncertainty of performance implied by HF element. The System-Theoretic Accident Model Process (STAMP, Leveson 2003) is investigated as a suitable methodology able to provide a significant asset in such perspective. The approach is widely applied in many industrial and transportation fields but in order to better understand its application into the marine context, a specific application will be briefly commented. In the attempt to define a comprehensive procedure, as a preliminary overview, some selected models suitable to classify the human behavior will be considered with specific focus on the reasons for performance degrade and/or uncertainty.

Keywords. Human Factor, Ship Design, STAMP, Safety Model

1. Introduction

The ship design process has changed radically in the latest decade especially for complex vessel (e.g. large passenger ships, navy vessels,…) characterized by intensive technology and outstanding intrinsic value. On the other side, the relevance of Human Factor in safety and operative ship performance is everyday evidence and recognized by fundamental rulemaking organizations like International Maritime Organization, IMO [1,2].

It is evident the need to intensify the research activity, looking for innovative approaches enabling the human integration into ship performance assessment during ship design process. This should be properly tuned with the consolidated 21st century trend at IMO i.e. the shift from prescriptive rule toward performance based approach. In fact the introduction of Formal Safety Assessment (FSA) [3] and Goal Based Standard (GBS) [4] in the very first years of the 2000s has created the premise for an inexorable process toward the proactive attitude in ship safety and the performance

[1] Paola Gualeni, Associate Professor, University of Genoa, DITEN - Department of Naval Architecture, Electrical, Electronic and Telecommunication Engineering, Via Montallegro 1, 16145 Genoa, Italy; E-mail: paola.gualeni@unige.it.

based approach during the ship design. In this evolutionary context, the so called Alternative Design [5,6] to SOLAS prescriptions has come out as well and a new approach for Human Factor integration into the ship design process is expected to promising in relation to such framework.

A successful final outcome in terms of ship safety is the result of the appropriate merge among ship platform, active safety devices and crew members performance (Figure 1). To assess the comprehensive integration outcome among all these safety players is very difficult, barely imaginable in a traditional prescriptive approach. The very different nature of all the involved issues suggests the development of an ad hoc assessment method/design tool able to investigate the influence of human factor on the ship resilience. For the purpose of this paper ship resilience is specifically defined as the capability of the ship to absorb, i.e. to withstand and handle a human error. The core of ship resilience performance is deemed to be the ensemble of active and passive systems (embedded in ship platform) devoted to ship safety.

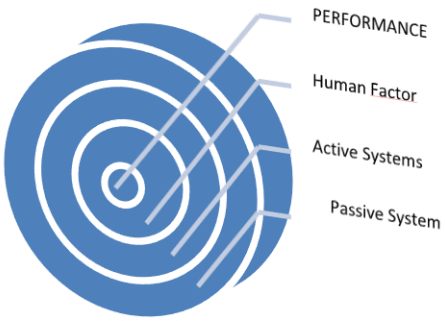

Figure 1. The ship safety comprehensive arena.

The increasing automation level of ships, in principle inserted in order to support and complement the human beings in systems management and decision making, is also likely to create the effect of expropriating the control of the situation. This is the reason why this component should be considered into the model of ship resilience proposed in Figure 1, as a ring between HF and Active+Passive Systems . The aim of the innovative assessment method/tool is the comparison, during the design stage, among different solutions in order to spot the ship configuration less vulnerable to the human error effects.

1.1. Goal Based Standard, Formal Safety Assessment and Alternative Design – an overview

The notion of "Goal-Based ship Standards" (GBS) was introduced at IMO in 2002 putting forward the concept that ship design and construction standards should be formulated allowing innovation in design process. At present, there is an increasing tendency to adopt a Goal-Based approach for regulations and there are good technical and commercial reasons for believing this approach to be preferable to more prescriptive regulation.

“Goal-Based regulation”, in fact, by definition, does not specify the means of achieving compliance but it sets goals, allowing therefore alternative ways of achieving

compliance. It is well known the example made in [7] i.e. “People shall be prevented from falling over the edge of a cliff” is Goal-Based. In prescriptive regulation the specific means of achieving compliance is specifically identified, e.g. “You shall install a 1 meter high rail at the edge of the cliff”. For this reason Goal-Based standards are considered a proper tool for the future evolution of international regulatory standards, since in principle they allow for a larger range of design solution, to be supported nevertheless by a robust safety evaluation.

More or less at the same time, also Formal Safety Assessment (FSA) has been introduced at IMO and defined as a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment and property, by using risk analysis and cost benefit assessment.

FSA is considered an approach that in the longer term, can facilitate the development of rules and regulations targeting safety rather than technical details .

An interesting relation between GBS and FSA is presented in Figure 2 [8].

Goal-based standards		Formal Safety Assessment
Tier I	**Goals** (overall safety level criteria)	
Tier II	**Functional requirements**	- Identification of hazards, leading to functional requirements - risk analysis, leading to balanced risk acceptance criteria
Tier III	Verification for approval	
Tier IV	**International regulations, rules and standards** (IMO, Class, ISO, ...)	- risk control options - cost benefit assessment - recommendations for decision-making
Tier V	**Local standards and procedures**	

Figure 2. Conceptual and practical relation between GBS and FSA [8]

For the long term, GBS are also associated with the concept of the so called “safety level”, discussed at MSC 91 together with the "safety-level approach” defined as the structured application of risk-based methodologies for the IMO rule-making process. The risk based approach has been recognized as a possible methodology in order to verify/give evidence of goals achievements but the community recognized as well how it is challenging to develop a robust assessment in terms of risk analysis.

On the top of that, more or less again at the beginning of the 2000s IMO has introduced the possibility of Alternative Design and arrangements to specific SOLAS chapters II-1 (parts C, D and E) and III, implying that safe engineering alternative design solutions can be considered equivalent to SOLAS by technical justification.

Safety objectives and functional requirements are identified and these can be achieved either by compliance with the already existing prescriptive requirements or by alternative design and arrangements based on engineering analysis, evaluated and approved by the Administration.

To this aim the MSC 92 delivered specific Guidelines [5] with a view to providing a consistent process for the coordination, review and approval of alternatives and equivalents with regard to ship and system design as allowed by the 1974 SOLAS Convention. Within such Guidelines it is recognized that since a majority of incidents are strongly influenced by human error and operational faults, the design team should find solutions that minimize potential human error, if at all viable and efficient. The

Risk-based design is to be developed relying on a structured and systematic methodology aimed at ensuring safety performance and cost-effectiveness by using risk analysis and cost-benefit assessment: several analytical techniques, e.g. reliability, availability and maintainability engineering, statistics, decision theory, systems engineering, human behavior, etc. are to be applied in order to successfully integrate diverse aspects of design and operation while assessing risk.

In this paper the System-Theoretic Accident Model Process (STAMP) methodology [9] is proposed as a methodology for a further step forward, extending the meaning of risk assessment into a system engineering approach. The new paradigm relies of control system theory and safety constraints enforcement; it might represent a new solution for new current and future problems related to safety of complex systems.

2. The STAMP methodology

In the traditional risk assessment causality models, accidents are considered to be caused by chains of failure events, each failure directly causing the next one in the chain. However, these usual models are no longer adequate for the more complex sociotechnical systems that are being built nowadays. In particular this is a more and more evident issue when human factor integration is a determinant for the risk assessment.

The first step is to extend the definition of accident causation beyond failure events in order to include component interaction and indirect or systemic causal mechanism. In achieving this objective, an accident can be defined as an unplanned and undesired loss event that could result in fact from component failures, disturbances external to the system, interactions among system components and behavior of individual system component leading to hazardous system states.

2.1. General description

In the latest years a new approach has been developed in order to investigate incidents and find suitable countermeasure to avoid future possible recurrence [9] . It is named Systems-Theoretic Accident Model and Processes (STAMP) and it is based on a system engineering approach integrated with control theory and applied in system safety engineering.

In STAMP, systems are dynamic processes that are continually adapting and accidents can be analyzed in terms of an adaptive feedback function that fails to maintain safety performance since system behavior changes overtime to meet a complex sets of goals and values. In system engineering *safety* is considered as an emergent property i.e. it arises from the interactions among the system components and it is controlled by imposing *constraints* on the behavior of and interactions among components. In this way, safety becomes a *control* problem where the goal of the control is to enforce the safety constraints.

The most basic concept in STAMP is not an event, but a constraint and the importance of constraints is pointed out together with the concept that incidents are the results of an inadequate control and /or poor enforcement of constraints on safety related behavior.

In system theory, systems are viewed as hierarchical structures, where each level imposes constraints on the activity of the level beneath. Control processes operate

between levels to control the processes at lower levels in the hierarchy and these control processes enforce the safety constraints for which the control process is responsible (Figure 3).

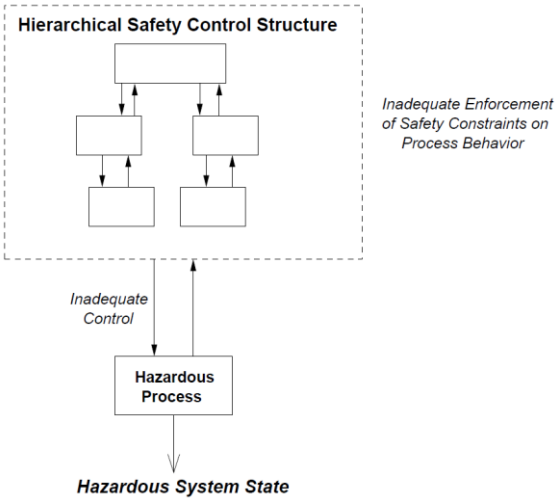

Figure 3. Safety as a Hierarchical Control structure [9]

Then, accidents occur when these processes provide inadequate control, that may result from missing constraints, inadequate safety control commands, commands that were not executed correctly at a lower level or inadequately communicated. For example, unsafe work instructions or procedures might be given to the operators, or instructions are appropriate and enforce the safety constraints but the operators may ignore them. In any case it is vital that feedback channels are provided to determine whether unsafe instructions were given or that safety-related instructions were not followed.

In this new safety-related approach it is necessary to identify the safety constraints to be enforced and then to effectively design control process/system to enforce them. To accomplish this goal, the first step is to state the system and component hazards in order to specify the system-level safety requirements and then design constraints necessary to prevent the hazard occurrence. These constraints will be used to guide the system design and tradeoff analyses in an iterative way in order to refine and expand the safety requirements and constraints that must be incorporated into the physical system design and into the safety control structure.

Several applications have been carried out in different industrial and transportation fields. Most of the literature is reported as proceedings of several workshops organized by Massachusetts Institute of Technology MIT. In the following, an application of STAMP for US Navy Positioning System [10] is briefly presented.

2.2. Significant Application Case

The research activity taken in exam demonstrates the efficacy of STAMP and the advantages that result from using this new safety analysis method compared to traditional techniques. Actually in the study one very useful tool for STAMP application is explored i.e. the so called STPA (System-Theoretic Process Analysis)

[11], that is a relatively new hazard analysis technique based on an extended model of accident causation. The study involves Naval Offshore Supply Vessels (OSV) equipped with software-intensive dynamic positioning system and operative in the escort activity of target vessel. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, not necessarily by a system component failure.

The analysis begins by analyzing the OSVs in the context of the Navy's organizational structure and then explores the functional relationship between OSV system components that can lead to unsafe control and the violation of existing safety constraints. The results of this analysis show that with STPA it is possible to find all of the component failures identified by traditional safety analyses of the OSV system. Moreover, the analysis shows that STPA finds many additional safety issues not identified or dealt with through the use of Fault Tree Analysis and Failure Modes and Effects Analysis on this system.

As put in evidence by the results of the STPA analysis on the OSV DP system, STPA provides a framework to identify unsafe control actions and causal scenarios that can lead to hazardous system states that fall outside of the failure-centric problem space captured by FTA and FMEA. Figure 4 illustrates this fundamental difference between FTA and FMEA's focus compared to STPA's focus.

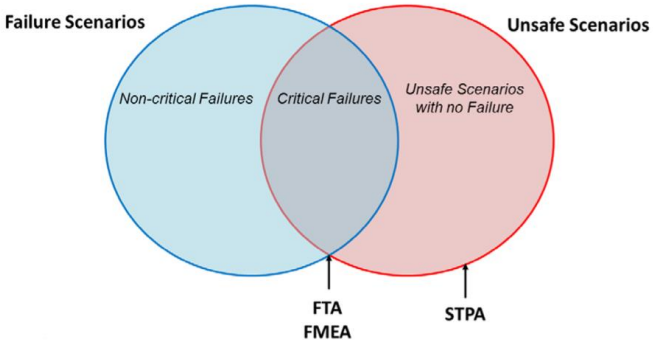

Figure 4. STPA's problem space compared to traditional Risk-based model [11]

Since FTA and FMEA focus solely on failure scenarios, these methods cannot identify unsafe scenarios with no failure. Failure scenarios are in strict relation with reliability problems and not necessarily linked to safety problems (although failure scenarios may also be unsafe, as shown into the picture, Figure 4). The major point is that reliability does not guarantee safety. Because FTA and FMEA focus solely on failure scenarios, there is a whole category of unsafe scenarios that will not be captured when using these methods to conduct a safety analysis.

While failure scenarios are identified as well, STPA permits the identification of hazardous situations that arise from unintended component interactions, inadequate design requirements, human errors and unsafe scenarios where no failures occur. STPA and FTA/FMEA techniques are difficult to compare but it has been shown that traditional methods like FTA and FMEA have limitations in comparison with the very interesting advantages of STPA.

The assessment has focused in particular on the collision problem and results of the case study have been judged as very useful to improve the dynamic positioning system safety.

3. Overview of methodologies for a Human Factor modeling

Within the great challenge of integrating the Human Factor effect into the design process the need of a cross cutting paradigm for Human Factor description is perceived and, in the following, a selection of methodologies deserving attention for the purpose is given. The selection is derived from [12] and the very same book has inspired the idea to investigate the application of STAMP methodology for ship design in a safety performance perspective. It is worthwhile to stress the concept that STAMP is the real kernel of the study proposed in this paper. It is the comprehensive system based approach able to move the focus from the isolated specific human error to the general view where to spot the possible violation of safety constraints.

Nevertheless in the next lines we briefly describe basically different and complementary approaches that can characterize the Human Factor modeling, for example the kind and the mode of "different from expected" performance or the level of "uncertainty in the behavior" , useful framework to define the safety boundaries.

3.1. ETTO

An intensive research activity has been carried out in order to identify and classify human error in order to eliminate, prevent and recover for it. The ETTO Principle [13] looks at the common behavior of people at work to adjust actions and performance to match the conditions - to what has happened, to what happens, and to what may happen. The concept is that efficiency-thoroughness trade-off (ETTO) is everyday life and usually thoroughness is sacrificed for efficiency. From the point of view of HF characterization this binary concept (i.e. thoroughness and efficiency) can be very helpful to identify hazards and unsafe control actions.

3.2. SHELL

The SHELL model [14], is very powerful in expressing interactions and interfaces among the major players when human beings deals with complex technology and problems. Each person (i.e. center "L" see Figure 5) interacts with the other four components (i.e. S, H,E , L see below for description) and from this theory it can be assumed that that interface issues between the center L and any other four components leads to a source of human error. The capital letters represented in figure 6 are respectively:

H –Hardware, such as equipment, tools, workspace, machinery; S- Software, that comprehends all non-physical resources, like organizational policies/rules, procedures, manuals, automation; E- Environment, which includes climate, temperature, vibration and noise, but also socio-political and economic factors.

Finally a double L with different meaning is necessary: L- Liveware i.e. factors like teamwork, communication, leadership, hierarchy and L- Central Liveware, which is in the centre of the SHELL Model, and can be defined as human elements such as knowledge, attitudes, cultures and stress. The SHELL model could be effective in order to describe the control structure at the base of the STPA analysis.

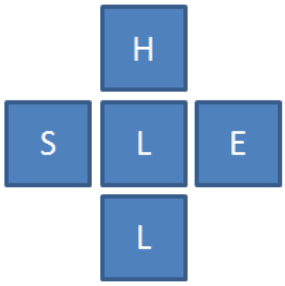

Figure 5. SHELL model

3.3. SRK

A very useful framework is given by Rasmussen [15] for identifying the types of error likely to occur in different operational situations, or within different aspects of the same task where different types of information processing demands on the individual may occur.

The model Skill-Rule-Knowledge (SRK) permits to classify the human behavior in three levels, from the performance relying on a lower cognitive workload to the one that demands higher cognitive workload:

- Skill-Based Behavior (SBB) – refers to the basic execution of actions for which the person in charge is extensively trained and there is virtually no conscious monitoring;
- Rule-Based Behavior (RBB) – this level is defined when some rules are previously defined and they are supposed to be applied. These rules may have been learned through formal training, or by working with experienced process workers. The level of conscious control is intermediate between that of the knowledge and skill based modes;
- Knowledge-Based Behavior (KBB) – The higher level is the knowledge based mode, the human carries out a task in an almost completely conscious manner. This would occur in a situation where a beginner was performing the task (e.g. a trainee process worker) or where an experienced individual was faced with a completely novel situation.

There is a further evolution named GEMS (Generic Error Modeling System) [16] as an extension of the SRK Approach and is intended to describe how switching occurs between the different types of information processing (skill, rule, knowledge) in tasks and it is illustrated in Figure 6.

SRK and GEMS are a very comprehensive model in order to define possible source and modality of human error and they can be very useful improve the description of HF interaction with complex technology and automation.

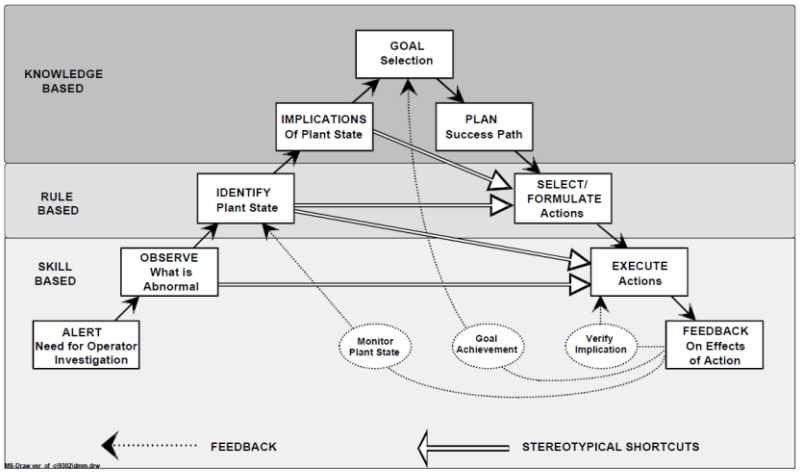

Figure 6. Link among *skills, rules* and *knowledge* [16]

4. A proposal for a new approach

In the frame of a performance based assessment for safety rules compliance it is necessary to effectively integrate *Human Factor* in the design process in an improved safety perspective.

The traditional decision-making approach is inclined to see decisions as discrete processes that can be separated from the context in which the decisions are generated and to set up them as isolated phenomena. Nowadays, this view in some occasions is not appropriate, especially when dealing with operations of complex systems like large passenger ships or navy ships: instead of thinking about operations on board as predefined sequences of actions, human interaction with a system is increasingly being considered to be a continuous control task in which separate decisions or errors are difficult to be identified.

A new approach could be to assume that HF in the system can be treated in the same way as autonomous components; however, the causal analysis and scenario generation for humans controllers and operators is much more complex than that of software devices, where the algorithm is known and can be modelled and assessed. The main difference between humans and automatic controllers is the intrinsic possibility that, for different reasons, the operator could feel the necessity to change the procedure, even if they are given a procedure to follow. In other terms, humans control algorithm is dynamic and, in order to be realistic, has to be able to evolve as a result of feedback and changes in goals.

Human decision making has to be viewed as a control model and its study has to be integrated with the study of the social context, the value system in which it takes place and the dynamic work process that is intended to be controlled and managed (Figure 7). The new view of Human Factor in the decision making process needs a new approach to represent and understand human behavior, focused not specifically on human error and violation of rules but on the mechanism generating behavior in the actual, dynamic context.

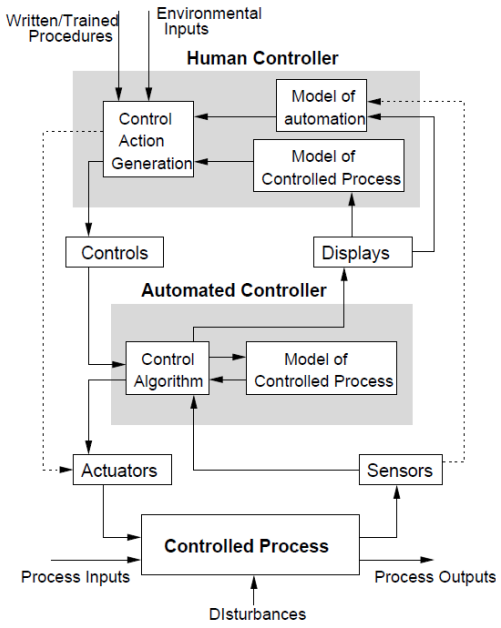

Figure 7. A human controller /automated controller/ physical process model

In this view of innovative integration of Human Factor in the ship design for improved safety and operations efficiency, STAMP is a promising tool since it is characterized by a systemic approach and dynamic analysis, that take into account the work system *constraints*, the boundaries of acceptable performance, the need for experimentation the subjective criteria guiding adaption to change. In this approach, it shall be very beneficial to refer to the interface human-machine not only in terms of traditional ergonomics, but considering the *cognitive work/task analysis*, in which behavior is modeled in terms of the objectives of the decision maker, the boundaries of acceptable performance and the adaptive mechanisms of the human actors.

Such an approach leads to consider the operator behavior as a product of the environmental in which it occurs, so in order to reduce operator *error* the designer has to previously and effectively change the environment in which the operator works. In this way, the final aim has to be the comparison of different design solutions in terms of safety or operational performance, considering in the trade off exercise that the users are humans with all their peculiar and challenging characteristic.

5. Conclusions

In this paper the need of an innovative approach to integrate Human Factor performance into the ship design process has been evidenced. The recent IMO rulemaking evolution toward performance based assessment is assumed as a valid framework where to root a new methodology based on the STAMP approach, already extensively applied in several industrial and transportation fields. The most basic concept in STAMP is not an event, but a constraint and the importance of constraints is pointed out together with the concept that incidents are the results of an inadequate

control and /or poor enforcement of constraints on safety related behavior. To investigate the possible application into the marine field, an existing study involving OSV vessels engaged in navy activity has been analyzed. In such application the STPA tool has shown to be more effective than more traditional risk analysis hazard identification approaches to spot out critical situations.

The main outcome of this preliminary study is that human beings can be visualized as a part of a complex model where they are supposed to be a control element that nevertheless should be characterized and studied appropriately. The great challenge is that for different reasons, the operator could feel the necessity to change the procedure, even if they are given a procedure to follow. The need to find suitable paradigms for Human Factor characterization and description has been underlined as well into the paper and some interesting models derived from literature have been briefly described to this aim.

As a conclusion it seems therefore that there are good premises for the formulation of a comprehensive approach based on the methodologies and models proposed above and in the next future some selected application cases will be identified in order to gain a further insight into the innovative methodology and to gain the experience about the real capability to overcome and complement traditional risk analysis when developing performance base safety assessment.

References

[1] J-U Schröder-Hinrichs, E. Hollnagel, M, Baldauf, S. Hofmann, A. Kataria Maritime human factors and IMO policy, *Maritime Policy & Management*, 2013

[2] H.P. Berg, Human Factors and Safety Culture in Maritime Safety (revised) *The International Journal on Marine Navigation and Safety of Sea Transportation* Volume 7 Number 3 September 2013

[3] IMO, MSC-MEPC.2/Circ.12/Rev.1 Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process, 18 June 2015.

[4] IMO, MSC.1/Circ.1394 Generic Guidelines for Developing IMO Goal-Based Standards, 14 June 2011

[5] IMO MSC.1/Circ.1455 Guidelines for the Approval of Alternatives and Equivalents as Provided for in Various IMO Instruments 24 June 2013

[6] IMO MSC.1/Circ.1212 Guidelines on Alternative Design and Arrangements for SOLAS chapters II-1 and III 15 December 2006

[7] H. Hoppe, Goal-based standards : — A new approach to the international regulation of ship construction, *WMU Journal of Maritime Affairs* Volume: 4 Issue Number: 2, 2005

[8] M. Huss, Status at IMO: Where are we Heading with Goal-Based Standards? *SAFEDOR – The Mid Term Conference*, May 2007

[9] N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, *MIT Press*, 2011

[10] B.R. Abrecht, Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System, *Master of Science in Engineering Systems at the Massachusetts Institute Of Technology* June 2016

[11] N.G. Leveson, J.P. Thomas, STPA Handbook, 2018

[12] F. Bracco, Promuovere la sicurezza. La gestione dei rischi nelle organizzazioni complesse, Roma, Carocci Editore, 2013

[13] E. Hollnagel, The ETTO Principle: Efficiency-Thoroughness Trade-Off—Why Things That Go Right Sometimes Go Wrong, *Risk Analysis* Volume 30, Issue 1, January 2010

[14] F.H. Hawkins, "Human Factors in flight" Ashgate, London (second edition) 1993

[15] J. Rasmussen, Skills, Rules and Knowledge. Signals, Signs and Symbols and Other Distinctions in Human Performance Models *IEEE Transactions on Systems and Man and Cybernetics*, 13 pp. 257-66

[16] J. Reason, Human Error. Cambridge University Press, Cambridge 1990