Integrated Navigation System Safety Assessment Methodology

A. Raffetti

(*Imperial College, London*)

F. Marangon and F. Zuccarelli

(*D'Appolonia S.p.A.*)

This paper was first presented at the NAV99/ILA28 Conference on 'Loran-C, Satellite and Integrated Systems for the 21st Century' held at Church House, Westminster, London from 1–3 November 1999.

The introduction of modern navigation systems highlights the need for efficient tools to assess the possible impact of these systems on the safety levels currently associated with the operation of a ship. In recent years this has led to investigation of the advanced safety/risk assessment techniques already applied in other industrial sectors, with encouraging results. The scope of this paper is to show a quantified safety assessment methodology that can be applied while designing or retrofitting navigation systems. The methodology adopted is the result of the review of the IMO Formal Safety Assessment (FSA) technique and comprises the development of a functional analysis, a hazard identification analysis and a risk assessment. The paper provides details on a specific application of this model to an integrated navigation system. This application is included in the work performed under the ATOMOS II research project, partly funded by the DGVII Directorate of the European Commission within the 4th Framework Programme in the field of Maritime Transport.

KEY WORDS

1. Marine. 2. Safety.

1. INTRODUCTION. The introduction of highly integrated and automated technology into modern navigation systems, aimed mainly at reducing the number of personnel onboard ship, highlights the need for efficient tools to assess possible impacts of this new trend on the safety levels currently associated with the operation of the ship. In recent years, this has led to the investigation of the advanced safety/risk assessment techniques already applied in other industrial sectors with encouraging results. The scope of this paper is to show a quantified safety assessment methodology that can be applied while designing or retrofitting navigation systems. The methodology adopted is the result of the review of the IMO Formal Safety Assessment (FSA: IMO, 1996) technique and comprises the development of a functional analysis, a hazard identification analysis and a risk assessment.

The methodology permits a 'marginal' risk assessment between a conventional ship (equipped with traditional navigation devices) and a new highly automated ship with an integrated navigation system. In the comparative analysis, different factors have been considered in domains such as: the development process, functional

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

performance, system architecture, new technologies, human/machine interface, operations and maintenance.

The application of the methodology comprises the following steps:

(a) definition of risk acceptance criteria for passengers and/or crew with respect to possible accidents associated with failures of sub-systems and equipment (including human failings). This activity has been carried out by deriving the actual level of risk suffered by the EU merchant marine fleet;

(b) functional analysis of the navigation systems by means of formal techniques (for example, Functional Block Diagrams, Functional Failure Analysis), highlighting the functional/architectural areas/systems where a modern integrated navigation system differs from a conventional configuration;

(c) hazard identification and analysis, developed in detail for the navigation equipment, considering both hazards resulting from failures of the equipment and hazards generated by human errors or external events;

(d) formal risk assessment for a specific collision hazard (two ships on a collision course) by means of quantified methods (fault tree analysis, event tree analysis, risk profile assessment);

(e) evaluation of the results with respect to possible safety requirements to be fulfilled by the integrated navigation system, with some consideration of the application of the new concept of Safety Integrity Level (SIL) requirements allocated to the Programmable Electronic Systems (PES) involved.

2. DEFINITION OF RISK ACCEPTANCE.

The definition of risk acceptance criteria has been carried out by determining the actual level of risk suffered by the EU merchant marine fleet in recent years. The historical trends of marine casualties were analysed to obtain an assessment of the frequency of occurrence of typical accidents. The casualty database adopted for this purpose is described in detail in the next paragraph.

2.1. *The Casualty Database*. A comprehensive database of casualties was acquired from Lloyd's Maritime Information Services Limited (LMIS). The LMIS database contains details of all reported serious casualties, including total losses, to all propelled sea-going merchant ships in the world of 100 g.r.t. and above from 1 January 1978, and all reported incidents (serious and non-serious) to tankers, including combination carriers and gas carriers/tankers, since 1 January 1975. To provide an appropriate quality and quantity of data, it was decided to perform the statistical analyses on a selected set of casualty data extracted from the complete LMIS database using the following criteria, which resulted in a database summarised in Table 1:

Table 1. Summary Statistics on Casualty Database.

Quantity	Total entries in the database (years from 1/1990 to 4/1996)
Events	4478
GRT Tons involved in casualties	82600000
Fatal Events	128
Fatalities	1980
Spills	105
Tons Spilled	273000

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

(a) data relevant to ships owned by companies registered in the 15 EU countries;
(b) data related to casualties reported in the period from January 1990 to July 1996;
(c) data related to the EU-owned Merchant Fleet for each year of interest.

2.2. *Current Risk Levels.* The current risk levels suffered by the EU fleet have been derived from the database by analysing the fatal events that occurred in the reference period. For the purpose of the present work, only data relevant to non-passengers ships have been considered. In Figure 1, the calculated frequencies (in terms of events per ship per year) relative to the cumulative number of fatalities suffered have been plotted in a logarithmic chart. This calculation is performed for different classes of accident, for example: *contact/collision*, *fire/explosion*, *hull/machinery damage*, *wrecked/stranded*, *foundered* (ATOMOS, 1995). However, for higher classes of severity, the sample of casualties analysed is less significant; for instance, there were no reported accidents with more than 100 fatalities and few entries with more than 10 fatalities.

For this reason, the typical 1/N-slope curves for each accident type are also plotted in Figure 1. These curves were obtained using the calculated frequency for the lowest severity (at least one fatality) and then considering a decrease of one order of magnitude for each higher severity class. This quantitative safety criteria will be utilised as the reference for the final risk assessment described in the following paragraphs.

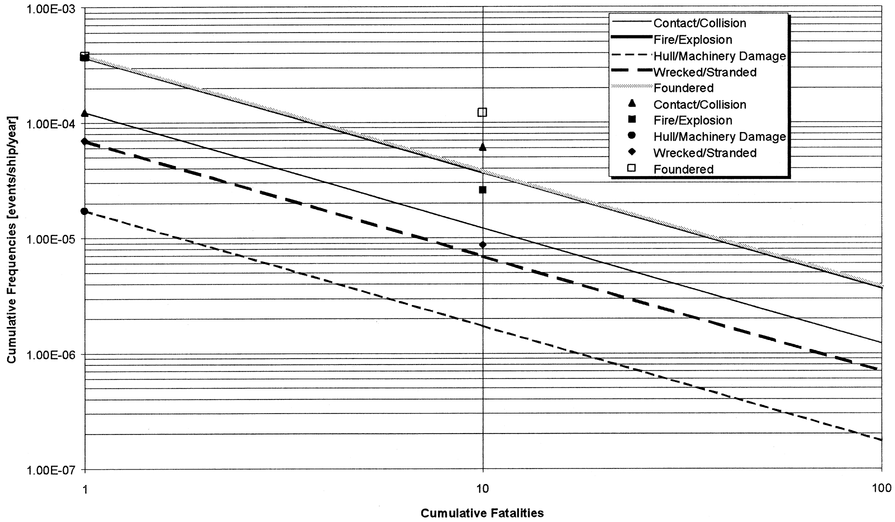

Figure 1. Quantitative safety criteria.

3. FUNCTIONAL ANALYSIS. The functional model for a generic ship is assumed to be the one as presented by IMO (IMO, 1996). The following functions have been identified: communications, navigation, anchoring, carriage, ship management (including emergency response and control, habitable environment, bunkering and storing), manoeuvrability, mooring and steering, power and

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

propulsion (including bunkering and storing relative to fuels, lubricants, etc.), and structure. These functions have been analysed separately in detail, highlighting the differences between a conventional ship and an ATOMOS II ship. The functional analysis has been performed by means of standard techniques, using Functional Block Diagrams (FBD). This analysis is the basis for the subsequent development of the other phases of the safety assessment process.

The functional analysis is based on the following criteria; a block can represent one of these elements:

(a) function;
(b) system;
(c) function or system ATOMOS II sensitive;
(d) function or system ATOMOS II specific.

This type of representation allows simultaneous description of the functional relations for a conventional and for an ATOMOS II ship and underlines the differences between the two ships' concepts. An example of the FBD analyses for the navigation function is presented in Figure 2.

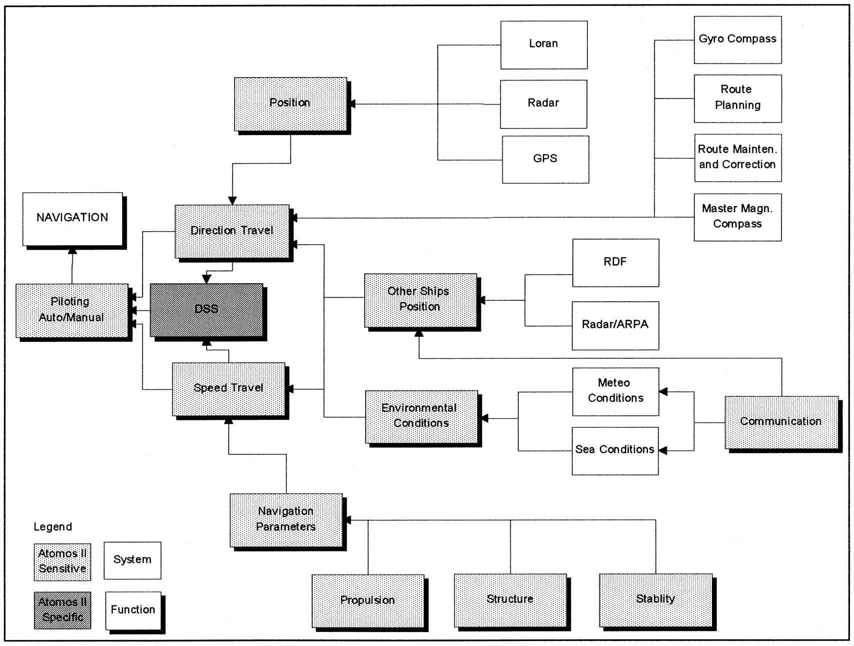

Figure 2. Navigation FBD.

The Functional Failure Analysis (FFA) identified the failures, or combination of failures, that can cause the loss of the functions and the expected consequences of these failures with respect to system availability and safety of the crew and third parties. It is noted that the failure analysis performed does not account for service disruptions due to software errors. The identification of the functions necessary for the correct ship operation requires an analysis of the major phases into which the normal operation of the system can be subdivided. These are: *mooring*, *anchoring*, *navigation in restricted areas*, *navigation in open sea*, *carriage*.

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

Each of these phases can be further detailed to identify the functions, sub-functions and systems that are involved in the successful completion of each operational phase. The analysis is completed with the effects on the system (i.e. the ship), caused by the function's loss, in terms of safety. This was classified in the following categories: *none* (*no direct safety consequences follow this failure*); *wrecked/stranded*, *collision*; *contact*, *foundered*; *fire/explosion*, *hull/machinery*.

4. THE HAZARD ANALYSIS.

The methodology adopted to develop the hazard analysis is shown in Figure 3. The FFA allowed, for each system, the identification of the consequences of all potential hazards on the ship status and their safety relevance. This is the basis of the Hazard and Identification Analysis.

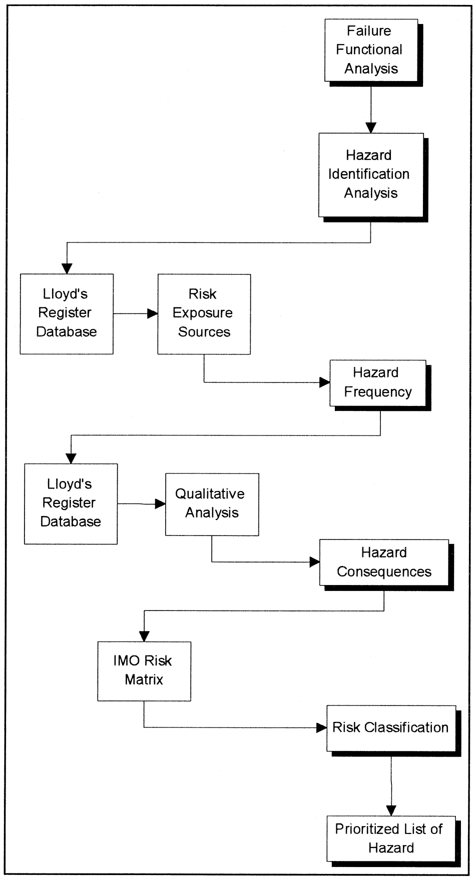
Failure Functional Analysis
Hazard Identification Analysis
Lloyd's Register Database
Risk Exposure Sources
Hazard Frequency
Lloyd's Register Database
Qualitative Analysis
Hazard Consequences
IMO Risk Matrix
Risk Classification
Prioritized List of Hazard

Figure 3. Hazard analysis methodology.

The hazards' frequency classification was developed in two steps:

(a) determination of the relative frequency of each of the main categories of consequence;

(b) determination of the rate of occurrence for each specific hazard, when this leads to the aforementioned category of consequence.

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

Table 2. Frequency class definition.

Frequency class	Fatal events per ship per year	
	From	To
F0	—	$1{\cdot}1 \times 10^{-8}$
F1	$1{\cdot}1 \times 10^{-8}$	$1{\cdot}1 \times 10^{-7}$
F2	$1{\cdot}1 \times 10^{-7}$	$1{\cdot}1 \times 10^{-6}$
F3	$1{\cdot}1 \times 10^{-6}$	$1{\cdot}1 \times 10^{-5}$
F4	$1{\cdot}1 \times 10^{-5}$	$1{\cdot}1 \times 10^{-4}$
F5	$1{\cdot}1 \times 10^{-4}$	$1{\cdot}1 \times 10^{-3}$
F6	$1{\cdot}1 \times 10^{-3}$	—

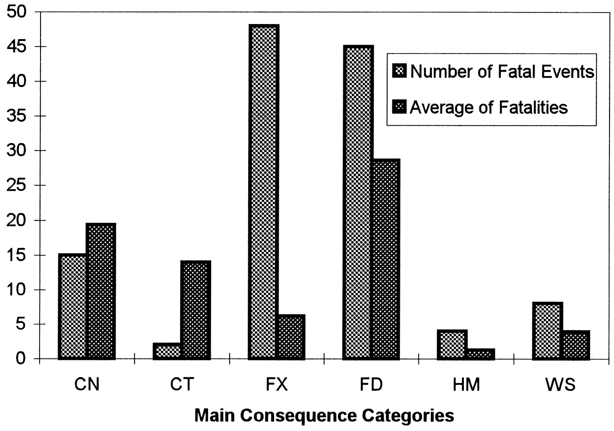

Figure 4. LMIS database; main consequence categories, average number of fatalities. (CN – collision, CT – contact, FX – fire and explosion, FD – foundered, HM – hull/machinery, WS – wrecked/grounded/stranded).

The frequency classification was performed utilising the frequency classes (in accordance with IMO, 1996) presented in Table 2.

The consequence classification is based on the IMO criteria that suggests definition of four classes. In the present analysis, we have adopted the following consequence classes:

(a) S1 (minor): no fatalities;
(b) S2 (significant): from 1 to 10 fatalities;
(c) S3 (severe): from 10 to 100 fatalities;
(d) S4 (catastrophic): more than 100 fatalities.

The above classification was applied using two criteria:

average consequence: is the result of a qualitative analysis for the average number of fatalities for each main consequence class (Figure 4) and the location of each fatality (Figure 5), on the basis of the Lloyd's data;

worst case consequence (independent of the location): based only on the maximum number of fatalities for each main consequence class.

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

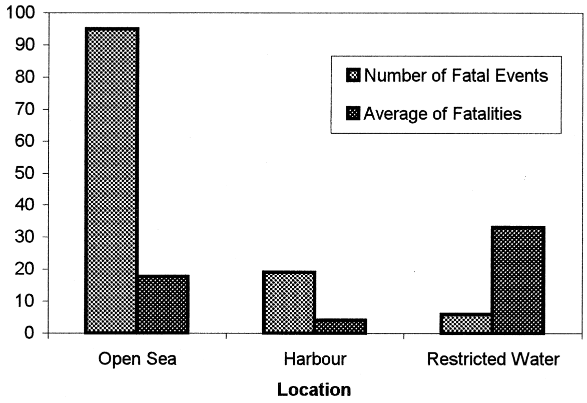

Figure 5. Location, average number of fatalities.

Table 3. Consequence classification.
(For legends, see Figure 4; NA = not applicable)

Location	Main Consequence Categories					
	HM	WS	FX	CN	CT	FD
Open Sea	S2	S2	S2	S3	S3	S3
Harbour	S2	S2	S2	S2	S2	S2
Restricted Water	S2	S2	S2	S3	S3	S3
Everywhere	S2	S2	S2	NA	NA	NA
Worst Case	S2	S3	S4	S4	S4	S4

Table 4. Risk matrix.

Safety consequences		Frequency						
		Low	→	→	→	→	→	High
		F0	F1	F2	F3	F4	F5	F6
Minor	S1	1	2	3	4	5	6	7
Significant	S2	2	3	4	5	6	7	8
Severe	S3	3	4	5	6	7	8	9
Catastrophic	S4	4	5	6	7	8	9	10

The results of the consequence classification for each of the main consequence categories and for each location are presented in Table 3.

The combination of the classifications, in terms of frequency of occurrence and possible severity of the outcomes, results in the risk classification performed in accordance with the IMO Risk Matrix (IMO, 1996) presented in Table 4. The risk classification has therefore been used as the criteria to compile the prioritised list of hazards to be further analysed in the risk assessment phase.

5. THE RISK ASSESSMENT.

As an example, a quantified risk assessment analysis has been completed with respect to a collision hazard. The risk event

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

considered for this analysis was a 'ship on collision course with another ship'. Using the safety criteria previously adopted, the results for the ATOMOS II ship have been compared with the results for a conventional ship. In the comparative analysis, the influencing factors have been considered at the following levels:

(a) at the *process* level, because ATOMOS introduces a new approach to the design and development of a ship to better perform and control the various phases of the ship's lifecycle;
(b) at the *functional* level, because ATOMOS introduces new functions (or new integration of functions) to the conventional set of ship's functions in order to better or more safely perform the ship's mission;
(c) at the *systems/technological* level, because ATOMOS introduces new systems and/or technologies to support both new and conventional functions;
(d) at the *Human Machine Interface* (*HMI*) level, because ATOMOS introduces new concepts for a usable interface to the human operator in order to provide easier and safer control of the ship's systems.
(e) at the *Operation and Maintenance* (*O&M*) level, as ATOMOS introduces new operational and/or maintenance procedures based both on reduced crews and on enhanced support to the operator/maintainer by means of the integrated SCC.

Each of the identified influencing factors can affect the safety of a ship both in 'positive' and in 'negative' ways, where 'positive' means an increase in safety and 'negative' an increase of risks.

The Risk Assessment has been performed for only the two most critical hazards identified during the previous hazard analysis phase. Nevertheless, the results obtained are sufficient for a first validation of the ATOMOS II concept, as the hazards analysed cover two of the main causes of marine casualties experienced by the EU fleet. The results of the analyses show an increased level of the safety for an ATOMOS ship. In comparison with the conventional ship, the following are the most important differences as highlighted by the analyses:

(a) The introduction of an advanced decision support function and the availability of the associated Decision Support System (DSS), because this decreases the frequency of human error.
(b) The advanced Diagnostic & Alarm Handling System, as it contributes to a general improvement of the operator's awareness during critical situations associated with multiple alarm conditions.
(c) The presence of an advanced network has been considered as a possible critical 'bottleneck' for the management of future vital information/commands .
(d) Improved operator awareness and capability to identify alarms and malfunctions.
(e) The availability of a reduced crew was considered to be a possible critical factor during emergency manual operations.

The criticalities associated with the introduction of new technologies based on Programmable Electronic Systems, as well as with the increased involvement of software and networking have been take into account. For this reason, the Safety Integrity Level (SIL) approach applied in other industrial sectors is briefly discussed.

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

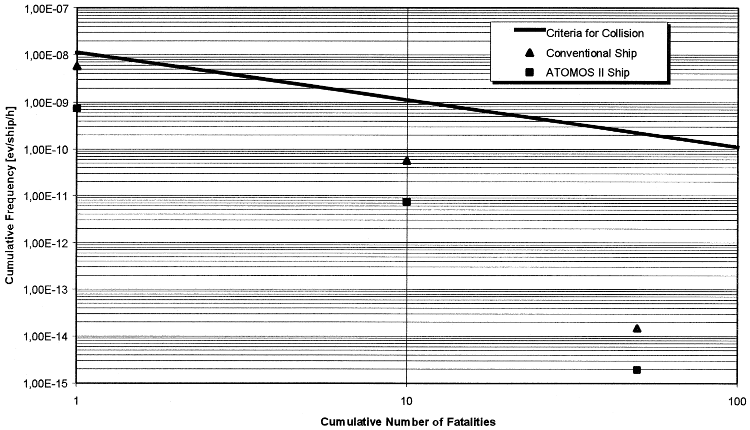

Figure 6. Risk profile for 'Collision'.

Table 5. Safety integrity levels: target failure measures.

SIL	Demand mode of operation (Probability of failure to perform its function on demand)	Continuous/high demand mode of operation (Probability of a dangerous failure per year)
4	$\geqslant 10^{-5}$ to $< 10^{-4}$	$\geqslant 10^{-5}$ to $< 10^{-4}$
3	$\geqslant 10^{-4}$ to $< 10^{-3}$	$\geqslant 10^{-4}$ to $< 10^{-3}$
2	$\geqslant 10^{-3}$ to $< 10^{-2}$	$\geqslant 10^{-3}$ to $< 10^{-2}$
1	$\geqslant 10^{-2}$ to $< 10^{-1}$	$\geqslant 10^{-2}$ to $< 10^{-1}$

6. SAFETY INTEGRITY LEVELS.

Existing *norms* (IEC 1508 in particular) require that Safety Integrity Levels (SIL) are allocated to Programmable Electronic Systems (PES) when they perform safety-related functions. These *norms* impose stringent verification and validation activities as well as hardware architectures for high safety integrity levels. As such, defining the SIL for a given function or system is a crucial factor when designing a PES-based system. With respect to numeric targets associated to Safety Integrity Levels, Table 5 shows the targets reported by IEC 1508.

The overall safety lifecycle outlined in IEC 1508 foresees the following steps up to the allocation phase:

Step 1 – overall concept description,
Step 2 – overall scope definition,
Step 3 – hazard and risk analysis,
Step 4 – overall safety requirements,
Step 5 – safety requirements allocation.

In other words, when the level of safety for the application has been set (Step 4), and the necessary risk reduction has been estimated on the basis of the results of the risk assessment process (Steps 3 and 4), the safety integrity requirements can be derived (Step 5). SILs are first allocated to safety functions, and then transferred down to designated safety-related systems. This process also needs to take into

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

account the existence of 'external risk reduction facilities', for example, physical measures taken external to the safety-related systems to reduce or mitigate the risk (such as a fire wall), as well as procedural means that again may reduce the risk.

A possible general methodology to apportion SILs comprises the following steps:

Step 1 – Functional analysis of the system to identify all safety related functions.

Step 2 – Identification of the required level of safety for the safety related functions. This step is based on hazard and risk analyses.

Step 3 – Assignment of each safety related function to safety systems.

Step 4 – Identification, where applicable, of external risk reduction facilities. Redundant or back-up risk reduction measures can be a combination of system design, procedures and external facilities. (In this case the safety function can be performed by devices having SILs lower than the one required for the safety function, provided that the required independence and functional diversity can be demonstrated).

This procedure can be implemented in various ways. Two possible techniques are identified: by means of a complete risk assessment methodology, or by means of a simplified approach, deriving the SIL requirements directly from the hazard analysis. This approach is justified if the SIL apportionment is performed early in the design stage.

6.1. *Using the Risk Assessment*. The SIL of an ATOMOS system can be directly derived from the failure probabilities used within the risk assessment model. For example, the SIL of the ATOMOS network shall be consistent with the failure probability used in the fault tree model. Such failure probability corresponds approximately to $8{\cdot}10^{-2}$ events/year. Entering this value in Table 5 results in the SIL required for the network within the fire protection function as 1.

6.2. *Using the Hazard Analysis*. In the absence of a complete risk assessment, the simplified methodology can be used. We applied this approach to a fire event in machinery spaces. From the report 'Safety Assessment – Part I: Hazard Analysis' (Zuccarelli *et al.*, 1998), hazard No. FX01 represents a fire event in the engine room; the hazard is monitored by a fire detection system. This hazard was preliminarily associated with an average severity S2 'significant: between 1 and 10 fatalities', and to a frequency F5 'between 10^{-4} and 10^{-3} events/year'. Applying the methodology, the following values can be used:

(i) P(A), the frequency associated with this event and which cannot be exceeded, is approximated by $5{\cdot}10^{-4}$, the average frequency of the range F5;

(ii) P(hazard), representing the number of demands for the protection system (i.e. the number of incipient fires that have to be detected), is approximated by $3{\cdot}10^{-1}$ events/year, which is the estimated value for incipient fires due to release of flammable material;

(iii) P(A|FD), the probability of having an accident when the protection is not working, is approximated by 0·1; in other words, it is assumed that only one tenth of the incipient fires develop into an accident if the protection system does not intervene.

The following results using the formulation already introduced:

$$P(FD) = 1{\cdot}8 \times 10^{-2}$$

Therefore, this approach leads to a SIL 1 apportionment for the of function monitoring and fire detection.

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press

7. CONCLUSIONS.

This paper summarises a quantified safety assessment methodology that can be applied while designing or retrofitting navigation systems. The research was subdivided into two main phases. The first comprised quantification of safety criteria obtained through an analysis of the LMIS database of casualties followed by the selection of relevant applications aimed at identifying a selected sample of ship types and hazard scenarios that are the most relevant with respect to safety. In the second part of the work, a safety assessment model was defined and applied to a selection of the identified hazards. The methodology adopted in this study is the result of a review of the IMO methodology and comprised the development of a functional model for all the functions involved in navigation, hazard identification and risk assessment.

Emphasis was placed on the marginal difference, in terms of safety, between a conventional ship and a new ATOMOS II integrated and low-manned one. This goal has been achieved by focusing the research on those aspects of the risk analysis process, in particular in the fault tree and event tree analyses, which are identified as 'ATOMOS II sensitive'. The risk assessment was used to consider the risk to a ship on collision course with another vessel and comparing the results obtained for both the ATOMOS II ship and a conventional ship. The results show an increase in safety levels for a ship where the new ATOMOS II concept is implemented. The criticalities associated with the introduction of new PES-based technologies, as well as with the massive involvement of software and networking, have been take into account.

REFERENCES

ATOMOS. (1995). *Optimisation of manpower in maritime transport*; *improvement of competitiveness in Community marine transport through implementing advanced technology*. DGVII Directorate of the European Commission, 3rd Framework Programme Transport – Waterborne.

ATOMOS II. (1998). *Advanced technology to optimise maritime operational safety – integration and interface*. DGVII Directorate of the European Commission, 4th Framework Programme Transport – Waterborne.

International Maritime Organisation (IMO). (1996). *Formal Safety Assessment* (*FSA*). Draft of guidelines for FSA application to the IMO Rule-Making Process, IMO MSC 67/13.

https://doi.org/10.1017/S0373463300008985 Published online by Cambridge University Press