THE JOURNAL OF NAVIGATION (2019), **72**, 53–68. © The Royal Institute of Navigation 2018
doi:10.1017/S0373463318000553

Specification and Design of Safety Functions for the Prevention of Ship-to-Ship Collisions on the High Seas

Reyes Poo Argüelles[1], Jesús A. García Maza[2] and Felipe Mateos Martín[1]

[1](*Electrical, Electronic, Computers and Systems Engineering Dept., University of Oviedo, Spain*)
[2](*Marine Science and Technology Dept., University of Oviedo, Spain*)
(E-mail: repoo@uniovi.es)

Maritime accident statistics reveal that ship collisions are among the most frequent and severe accidents. The same statistics indicate that most of them are caused by human error, mainly due to breaches of the International Regulations for Preventing Collisions at Sea (COLREGs) and to the lack of communication between ships. There are also special situations where there is some ambiguity in the application of the COLREGs. In such occasions, and if there is no communication between the ships involved, compliance with the Rules may still end up in a collision. This article brings a new approach to Collision Avoidance Systems (CAS) and presents the earliest stages in the development of safety functions for the reduction of ship-to-ship collision risk on the high seas. These functions will help the concerned ships achieve coordinated compliance with the COLREGs. Functional safety standards are applied and, in their implementation, real, accessible electronic programmable systems (hardware and software) will be used.

KEYWORDS

1. COLREGs. 2. Command, Control and Communications. 3. Risk Minimisation. 4. Ship Collision. 5. AIS.

Submitted: 15 December 2017. Accepted: 30 June 2018. First published online: 2 August 2018.

1. INTRODUCTION. According to the Annual Overview of Marine Casualties and Incidents published by the European Maritime Safety Agency (EMSA, 2016), during the period 2011–2015 a total of 8,533 casualties involving a ship were recorded. Collisions represent 18% of these and are second on the list of accidents with the most serious consequences. The same source indicates that 62% of the accidental events analysed were attributed to human error.

Various reviews of statistical data and analyses of maritime accidents (Primorac and Parunov, 2016; Eliopoulou et al., 2016; Luo and Shin, 2016; Goerlandt and Montewka, 2015) have been published in recent years. Among them, several analyses of the origins of collisions, such as those using Fault Tree Analysis (FTA) (Uğurlu et al., 2013),

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

Human Factors Analysis and Classification System (Chauvin et al., 2013), or Bayesian Network model (Sotiralis et al., 2016) have been made. These analyses show that most collisions are due to wrong decision-making originated mainly by International Regulations for Preventing Collisions at Sea (COLREGs) (1972) violations and by the lack of inter-ship communication. It therefore seems appropriate to develop a collision avoidance system from the perspective of the Officer Of the Watch (OOW).

Functional safety standards provide requirements and approaches applicable to the implementation of systems (hardware and software) used to reduce the probability of accidents or failures. Functional safety is a term introduced in the series of standards by the International Electrotechnical Commission (IEC) as part of IEC 61508 (2010) "Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems". This refers to the part of the overall safety of a system where its components or subsystems, with safety implications, respond adequately to any external input including human errors, hardware and software failures and environmental changes. This standard is generic and applicable to any sector. Two more specific standards derive from IEC 61508: IEC 62061 (2005) "Safety of machinery", and IEC 61511 (2016) "Safety instrumented systems for the process industry sector". Activities in the process industries share many of the risks that can be found on board ships (Vairo et al., 2017; Aven, 2017; Kosmowski, 2006).

The use of these standards as the basis for the development of safety functions to reduce the risk of collision is compatible with the Formal Safety Assessment (FSA, 2014; Montewka et al., 2014), introduced by the International Maritime Organization (IMO) as a methodology aimed at improving maritime safety through the use of risk analysis and cost-benefit assessment. Functional safety techniques are applicable more specifically in step 3 of the FSA (risk control options).

The safety functions presented in this article are implemented by a safety-related Programmable Electronic (PE) system which will provide the OOW with information for the reduction of ship-to-ship collision risk on the high seas. This information includes detection, determination of the rules to be applied according to the COLREGs (1972), communication between both vessels through standardised messages and recognition of agreements or possible disagreements. Several collision analyses (such as those performed in Ever-Alexandra, 2015; Florida-Chou Shan, 2014; Hibiscus-Hyundai, 2013; Katre-Statengracht, 2014; Spring-Josephine 2013) show the relevance of these information parameters.

Safety functions are intended to reduce the risks of the Equipment Under Control (EUC) with respect to specific dangerous events. In our case, the EUC is the set of ships, and the main hazardous event occurs when the calculated Closest Point of Approach (CPA) between the own ship and another ship is less than a safety distance, and the Time to CPA (TCPA) is less than the predefined time. At any rate, the system to be developed should alter neither the normal operation of the EUC, nor other implemented safety measures.

Depending on the measured or received static data (ship type) and dynamic data (position, heading, navigation status, etc), the PE system of each ship shall:

- calculate the distance, bearing (clockwise angle between North and the target observed from the ship), CPA and TCPA relative to each nearby ship (target);
- determine the manoeuvres to be made based on the COLREGs to reduce the risk of collision;
- keep the OOW informed.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

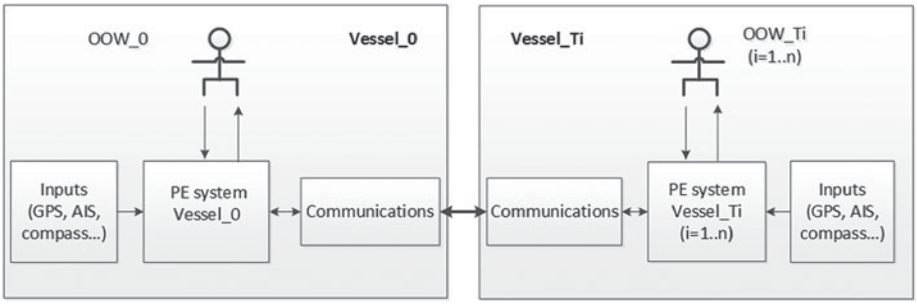

OOW_0
Vessel_0
Inputs (GPS, AIS, compass...)
PE system Vessel_0
Communications
Vessel_Ti
OOW_Ti (i=1..n)
Communications
PE system Vessel_Ti (i=1..n)
Inputs (GPS, AIS, compass...)

Figure 1. Diagram of implementation of safety functions for reducing the risk of collision.

PE systems of the ships involved shall also:

- communicate with each other safely, sending and receiving calculated manoeuvring data and OOW indications;
- compare their results and
- reach agreements or specify the disagreements.

Figure 1 is a schematic representation of the system for reducing the risk of collision between two ships, Vessel_O, the own ship and Vessel_Ti, one of the targets.

Some of the topics outlined in this introductory section will be further developed. The rest of the paper is organised as follows. Section 2 summarises general aspects of functional safety regulations and justifies their use in this proposal. Section 3 describes the structure of the specific E/E/PE system and communications between PE components. Section 4 presents the specifications of the safety functions and the safety requirements to be fulfilled by the PE system. Section 5 presents some details about their implementation and Section 6 summarises the main conclusions.

2. FUNCTIONAL SAFETY REGULATIONS.

2.1. *IEC 61508.* This standard establishes an approach for all activities related to the safety life cycle of systems that include E/E/PE elements used to perform safety functions.

To narrow down the meaning of some of the safety-related terms used throughout this article, some definitions are provided below:

- *Safety function*: A function performed by a safety-related E/E/PE system, or by another risk reduction measure, which is intended to achieve or maintain a safe state of the EUC with respect to a specific hazardous event.
- *Safety Integrity (SI)*: Probability that a safety-related E/E/PE system satisfactorily performs the required safety functions in all specified conditions over a specified period of time.
- *Safety Integrity Level (SIL)*: Discrete level (values 1, 2, 3 or 4) corresponding to the range of safety integrity values. It is related to the risk reduction factor that a safety function can provide. SIL 4 represents a Risk Reduction Factor (RRF) in the range $10^4 < \text{RRF} < 10^5$. SIL 1, a RRF in the range $10^1 < \text{RRF} < 10^2$.
- *Safety-related system*: A system that implements the safety functions required to achieve or maintain a safe state of the EUC and that is also expected to achieve,

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

> either by itself or with other E/E/PE systems, and other risk reduction measures, the safety integrity required for the safety functions. It may be designed to avoid a dangerous event (lowering the probability of occurrence to admissible levels), or to mitigate its effects. A safety-related system comprises everything (hardware, software and human elements) necessary to carry out one or more safety functions. It can be part of the control system or can implement safety functions with separate, independent systems.

The IEC 61508 (IEC, 2010) standard is generic and applicable to any sector. It sets the requirements to ensure that E/E/PE systems are designed, implemented, operated and maintained to provide the required SIL. In this paper, IEC 61508 is used as a guide of good practices applicable in the implementation of the system (hardware and software) that is proposed to reduce the risk of collisions.

The requirements for achieving safety integrity of E/E/PE systems include the use of validated hardware subsystems and software elements, with restricted and specified functionality and documented evidence of use. In the hardware architecture planned for implementing the safety functions of this proposal, two devices, well proven in systems and environments with high reliability requirements, are used together with a communication channel between them. These devices are the Automatic Identification System (AIS), and a Programmable Logic Controller (PLC).

2.2. *IEC 61511.* Standard IEC 61511 (IEC, 2016) has been implemented as an application of IEC 61508 to the process industry sector. According to this standard, in its first stage the safety life cycle assesses hazards and risks. The result of this assessment consists of a description of the safety functions required and the risk reduction associated to each function. In the second stage of the life cycle, these safety functions are assigned to "protection layers". Each layer consists of equipment and/or administrative controls that work in concert with the other layers of protection to control and/or mitigate process risk.

Figure 2, based on standard IEC 61511, shows a diagram of the various layers of protection in risk reduction. The innermost layer corresponds to the reduction of risks considered in the conception and design of process control. Critical alarms are the next level of active protection and require operator intervention.

Then, if a further reduction in the likelihood of the hazardous events is required, the layers called Safety Instrumented Systems (SIS) are added. These SIS layers, independent from the Basic Process Control System (BPCS), implement the safety instrumented functions. The rest of the layers correspond to systems and measures devised to mitigate damage when the accident has already occurred.

The E/E/PE system proposed would be placed between the two prevention layers, "Critical alarms and operator intervention" and SIS (Figure 2).

A Layer Of Protection Analysis (LOPA) (Summers, 2003; Stauffer and Clarke, 2016) could be performed to set the safety functions as an additional layer for reducing the risk of collision. It is necessary to consider what causes collisions, their probability of occurrence, how much risk reduction the existing layers represent, and what the required integrity level for the safety functions would be so that the level of risk is below a predefined threshold. If the tolerable risk is above the probability of the event, no additional reduction is required; but even in that case, it would be advisable to apply the safety functions to achieve a further reduction in probability of occurrence whenever they do not entail excessive costs (Melchers, 2001; FSA, 2014).

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

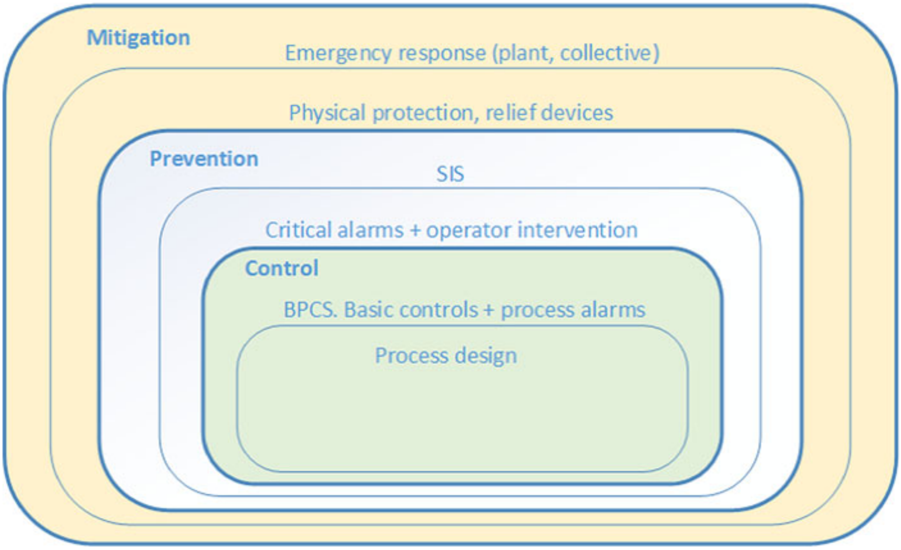

Mitigation
Emergency response (plant, collective)
Physical protection, relief devices
Prevention
SIS
Critical alarms + operator intervention
Control
BPCS. Basic controls + process alarms
Process design

Figure 2. Protection layers as methods of risk reduction.

3. E/E/PE SYSTEM. An E/E/PE system for safety functions comprises hardware components for input, logic and output. The proposed system includes as subsystems: an AIS station for Input/Output (I/O) operations (data acquisition and communication) and a PLC for logic (data processing). In an initial version, the AIS Class A station available on the ship can be used. In order to increase the availability and reliability of data and communications received, it will be necessary to analyse and evaluate the inclusion of redundant equipment in the system (Gamer et al., 2014).

3.1. *PLC.* It has been decided to use a PLC as a PE system as PLCs have input and output interfaces for all process signals, and for communications with other devices. They are robust machines of proven use in industrial environments and there are PLCs specifically designed for safety applications up to SIL 3, approved to comply with IEC 61508 standards (IEC 61131-6, 2012).

The PLC will be responsible for the following operations:

- Receive from AIS, via a digital interface, the messages with static and dynamic information of the own-ship and the targets and the binary messages sent by them.
- Collect information from the OOW (alternatively called the Operator in this paper).
- Perform the appropriate calculations.
- Communicate the calculated data to own-ship OOW.
- Send messages to the OOWs of the targets, using AIS as the communication channel.
- Execute the implemented algorithms for dialogue and agreements between ships.

Figure 3 reflects the structure of the planned architecture, derived from the general image of Figure 1.

3.2. *AIS messages.* Communication will be carried out by means of predefined messages exchanged between ships equipped with AIS stations. AIS is a Time-Division Multiple Access (TDMA) protocol-based communication system that uses Very High Frequency (VHF) channels to exchange navigation data. International Telecommunication

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

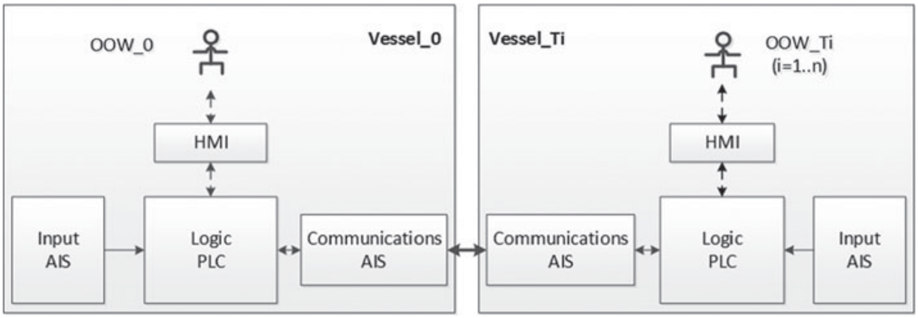


Figure 3. Current implementation diagram for safety functions.

Union Recommendation (ITU-R M.1371-5, 2014) describes two types of AIS: Class A used on large Safety Of Life At Sea (SOLAS) vessels and Class B, for smaller SOLAS vessels. AIS Class A stations are required for the development of this proposal. Studies on the reliability of data provided by AIS (Felski et al., 2015) show a high availability and integrity of dynamic information. Although the availability falls slightly for data on Rate Of Turn (ROT) and Heading (HDG) (Last et al., 2014), it could be improved by adding appropriate sensors to the AIS system.

There are 27 approved standard messages, shown in ITU-R.M 1371-5 (2014. Annex 8), of which the following are used in the implementation of the safety functions proposed here:

- Messages 1, 2, 3 include dynamic position information.
- Message 5, static ship data.
- Message 6, binary data for addressed (non-broadcasted) communication.
- Message 7, acknowledgment (ACK) of received message 6.

In addition to the exchange of information via VHF channels, AIS stations use maritime digital interfaces and data communication standards for the exchange of data with other devices, systems or networks. This facilitates the visualisation and on board use of AIS information (Pietrzykowski et al., 2017).

Through these digital interfaces, the AIS of a ship communicates its own static and dynamic navigation data and receives the same from other ships through VHF channels. This digital communication is performed by sentences or Parameter Group Numbers (PGN) coded according to National Marine Electronics Association (NMEA) standards (NMEA 0183, 2002; NMEA 2000, 2015). For this proposal, the communications shown in Figure 4 are required.

4. SAFETY FUNCTIONS.

A number of collision alert systems and methods have been proposed, as well as e-Navigation methods for manoeuvring support (Goerlandt et al., 2015; Baldauf et al, 2011). With the same aim of collision prevention, but focusing on direct and immediate assistance to the OOWs in the compliance with COLREGs, the safety functions presented in this paper have two main objectives:

- To assist in the early detection of ships located near to own-ship, thus, improving the reaction time available for performing manoeuvres. The safety function called FS_DETECT is in charge of this goal.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

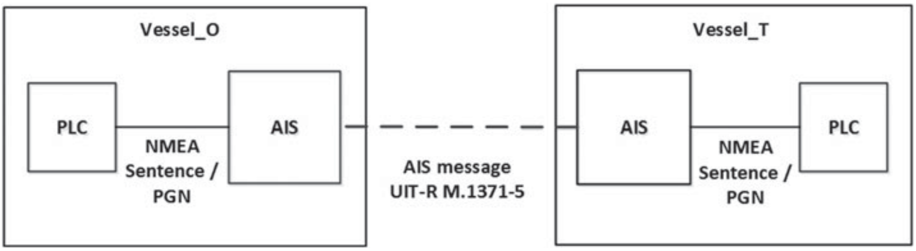


Figure 4. PE Communications.

- To increase the probability of adequate manoeuvring for both the own-ship and each target. This second safety function is called FS_MANOEV.

FS_MANOEV requires the establishment of communication between the PE systems (PLCs) of own-ship and the target involved in each manoeuvre. This communication will be used in two levels of agreements:

- *To check if the information handled by both PLCs fully agrees*. A ship's PLC must communicate to the other PLC the information it has available. This second PLC will compare the received data with its own data and will answer whether it is in agreement with it or not. If there are differences between the data they handle, each PLC will notify the discrepancy to its operator.
- *To reach agreements between the two operators*. The ship's PLC will inform its operator of the possible manoeuvres, deduced from the available information. Then, it will wait for the operator's decision. Next, it will transmit this decision to the other ship's PLC and will wait until the latter communicates its operator's response and sends his/her answer.

4.1. *Safety Function FS_DETECT.* From the static and dynamic information of own-ship and targets, FS_DETECT will calculate the bearing, distance, CPA, TCPA and true speed relating own-ship to each target. It will show the operator the "visible universe": information of those targets that are in an area centred on own-ship with an established radius, and with CPA and TCPA lower than specified and adjustable safe values.

The safety function shall use as input devices the AIS systems installed on board, which shall provide static and dynamic information on own-ship and targets. This information is received through the standard messages 1, 2, 3 or 5, already mentioned.

4.1.1. *Requirements.* For this safety function, communication between the ship's AIS system and the PLC will be done through a digital interface and NMEA communication standards. In order to calculate bearing, distance, CPA and TCPA for each target, it is necessary for the safety function to receive the dynamic data from the own-ship and from the target with a very small time interval between them. Maximum waiting times should be established for communications, as well as the actions to be taken in case of exceeding those times.

The Human-Machine Interface (HMI) will display information about ships that, within the given radius, have CPA and TCPA values lower than the established safety values (CPA_{Safe}, $TCPA_{Safe}$) which depend on the type and dimension of each ship. These data will be updated within a set period of time. No further information about other detected ships

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

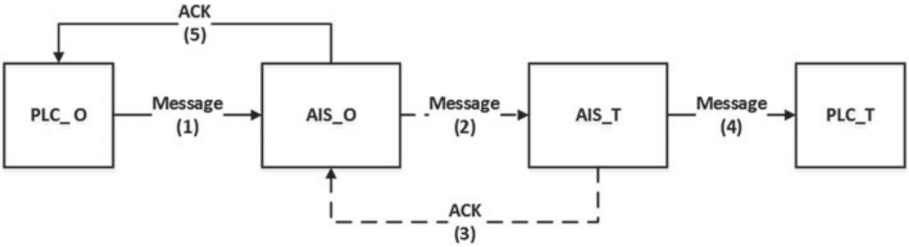


Figure 5. Sequence of PE-PE communication.

Table 1. Application identifiers in message 6.

bit	Description
15-6	Designated Area Code (DAC). This code is based on the Maritime Identification Digits (MID). Exceptions are 0 (test) and 1 (international).
5-0	Function Identifier (FI). The meaning should be determined by the authority which is responsible for the area given in the designated area code

will appear on the display, so as not to overload the operator with information non-relevant for safety (EU-OSHA, 2009). From this HMI, the operator will be able to modify the values set for the radius, refresh period and safe values for CPA and TCPA. It will also include an acknowledgment field (ACK) to ensure that the operator is aware of the information being displayed. The PLC will store all received and calculated information in an external database.

4.2. *Communication between PE systems.* Communication between the PLC of the own-ship and each of the targets will be carried out through the AIS stations, using standard messages 6 and 7. In a simplified way, communication will proceed according to the following steps (see Figure 5):

- Own-ship PLC will write the information to be communicated to the target in an addressed binary message (message 6).
- Own-ship AIS (connected to the PLC) will transmit the message to the target's AIS.
- When the target's AIS receives the message, it will send an ACK (message 7) to the source AIS, indicating that the message has been transmitted.
- Then, the PLC connected to the target AIS will read the received message, and the source PLC will read the ACK. If the message does not reach its destination, the source PLC will not receive the ACK. The waiting time between a PLC sending a message and receiving the ACK will depend on the number of retries and transmission intervals. A maximum waiting time must be set as a standard value.

Binary messages include a 16-bit application identifier, structured as shown in Table 1.

The test application identifier (DAC = 0) should be used for testing purposes. The international application identifier (DAC = 1) should be used for international applications of global relevance. For this application, DAC = 0 can be used and the FI (6 bits) will be employed for codifying the messages that a PLC is going to send to another PLC. Up to 64 messages can be codified.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

The binary messages that the PLC of the source ship will transmit to the PLC of the destination ship shall have as their purpose:

- To start the communication or accept the communication request.
- To check if the information handled by both PLCs fully agrees. This information includes the received values of the course and speed over ground, true heading and the calculated bearing, distance, CPA and TCPA. One PLC will send the information and the other will compare it with its own and will answer if it is equivalent or not.
- To agree on the possible manoeuvres, calculated by the PLCs from the available information.
- To transmit the established messages between the operators.

4.3. *Safety Function FS_MANOEV.* Depending on the distance, the CPA and the TCPA between own-ship and a target, three situations are defined: Safe, Prealert or Alert.

$$Safe : CPA > CPA_{Safe} \tag{1}$$

$$Prealert : (CPA \leq CPA_{Safe})\ and\ ((Distance \leq CPA_{Safe} * P1)\ or\ (TCPA \leq TCPA_{Safe})) \tag{2}$$

$$Alert : Prealert\ and\ (Distance \leq CPA_{Safe} * P2) \tag{3}$$

$P1 > P2 > 1.0$, parameters that depend on the relative speed, the visibility and on the type and dimension of the vessels. Their values will be calculated by each PLC from the received dynamic and static data.

With the dynamic data (latitude, longitude and true heading) received from own-ship and from each target and with the calculated data for bearing, distance, CPA and TCPA, and according to the COLREGs (Part B - Steering and Sailing Rules), the PE system of each ship should be able to determine a close-quarters situation between the two ships, which is the stand-on vessel and what is the correct action to be taken to avoid a possible collision. In case of Prealert, and after agreement between the ship's PE system and its operator, a dialogue must be established between both PE systems.

A close-quarters situation and the actions to be taken will depend, firstly, on the visibility conditions. Section II of COLREGs (1972) - Part B is dedicated to the conduct of vessels in sight of one another. Section III refers to the conduct of vessels in restricted visibility. As the decision on manoeuvring depends on the OOWs, it is necessary that they reach an agreement on whether the situation is one of reduced visibility or not, so as to apply the rules of Section III or Section II. It is therefore necessary to add to the HMI a field in which the OOW will establish whether there is good visibility or reduced visibility. Moreover, a further field to indicate whether there is radar detection or not is also called for.

In order to decide on the manoeuvre and which vessel must carry it out, account should be taken of rule 18, "Responsibilities between vessels", as well as of rule 17, "Action by stand-on vessel", in the case that the give-way vessel does not act as prescribed.

4.3.1. *Requirements.*

- All possible close-quarters situations between two ships, contained in COLREGs rules 11 to 19, must be considered.
- The manoeuvring messages to be communicated between the two ships involved (Own and Target) must be defined for each situation.
- The messages indicating the manoeuvre, in addition to the messages for initiating/confirming communication between the PLCs of the two ships, and the messages

for checking the matching of the information they handle, will be transmitted using AIS standard message 6. An appropriate encoding will be included in the lowest six bits of the field Application ID.

- Maximum waiting times should be established for communications, as well as the actions to be taken in case of exceeding those times.
- It is necessary to define what the system should do in the following cases:
  - The information available on both ships is inconsistent.
  - There is no agreement between the operator and the manoeuvre suggested by the PLC of the own ship.
  - There is no agreement between operators regarding the manoeuvre to be performed.
  - Alert situation starts.
- The most appropriate format for displaying messages on the HMI must be defined and standardised.

Figure 6 reflects the sequence of steps defined for the communication between the PE systems of own-ship and a target when entering a pre-alert situation, in order to reach agreements and reduce the risk of collision between both ships. It is developed following GRAFCET (GRAphe Fonctionnel de Commande des Étapes et Transitions) methodology (David, 1995; IEC 60848, 2013). The sequence will be replicated for each target detected in the visible universe of own-ship. It must include all possible states, the actions to be performed in each state and the transition conditions between them.

The initial step (Safe state) of the own-ship PE system is deactivated for one of two reasons:

- It detects a Prealert situation with respect to the target and takes the initiative in the communication (right branch).
- A message is received from the target (MSG_Ini), which indicates that the target has detected the Prealert situation (left branch).

Following the right branch, and the communication described in Section 4.2, own-ship PLC first displays the calculated manoeuvre and waits for the operator acknowledgement. Then it sends a message (MSG_Dyn_Data) to the target-ship's PLC to check if there is agreement in the information handled by both PLCs, and waits for the target-ship PLC's answer. After that, it sends the message with the manoeuvre (MSG_Manoe) and waits for the answer of the target-ship operator. If there is agreement, it waits for the manoeuvre to be performed. The rest of the steps deal with the different alternatives: delays, disagreements and the alert situation.

5. IMPLEMENTATION OF THE SAFETY RELATED SYSTEM.

5.1. *Software design of safety functions.*

Principles and techniques for coding and verification of software identified in IEC 61508 (2010) apply to the implementation of a safety-related system as proposed here. Part 7 - Annex C includes recommendations on coding techniques, including code intelligibility, a modular approach and encapsulated information, use of proven/verified software elements and suitable programming languages. It also covers software verification techniques, including data analysis and recording, interface and limit values tests, assumption of errors, data flow analysis and process simulation.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

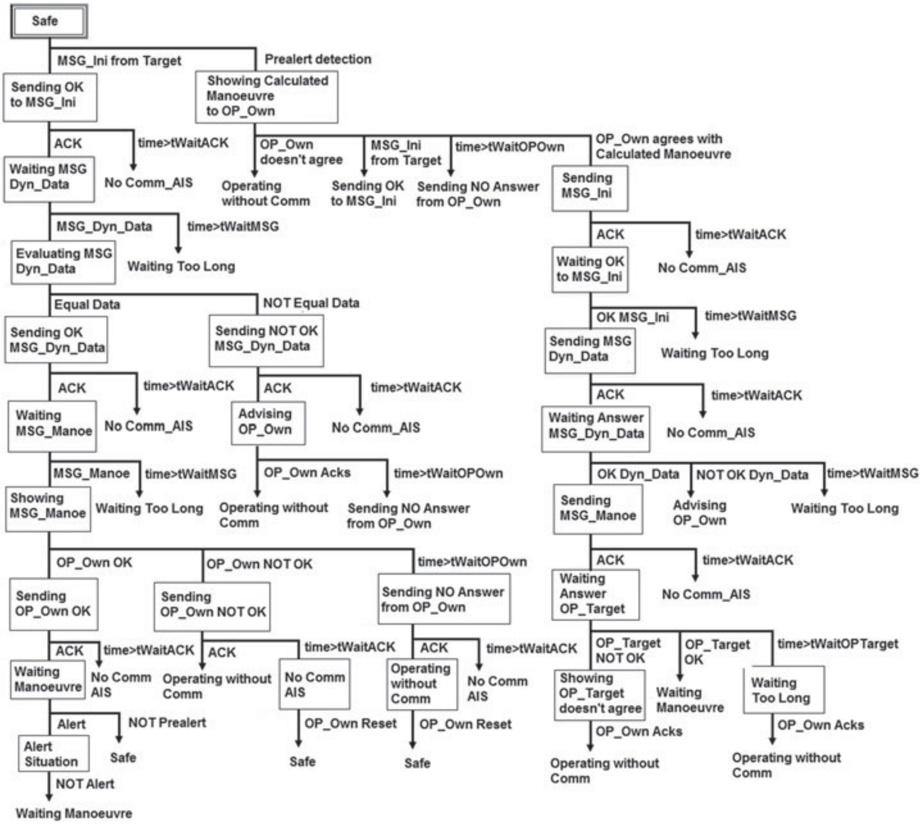


Figure 6. Sequence of steps of the dialogue between own-ship and a target PLCs.

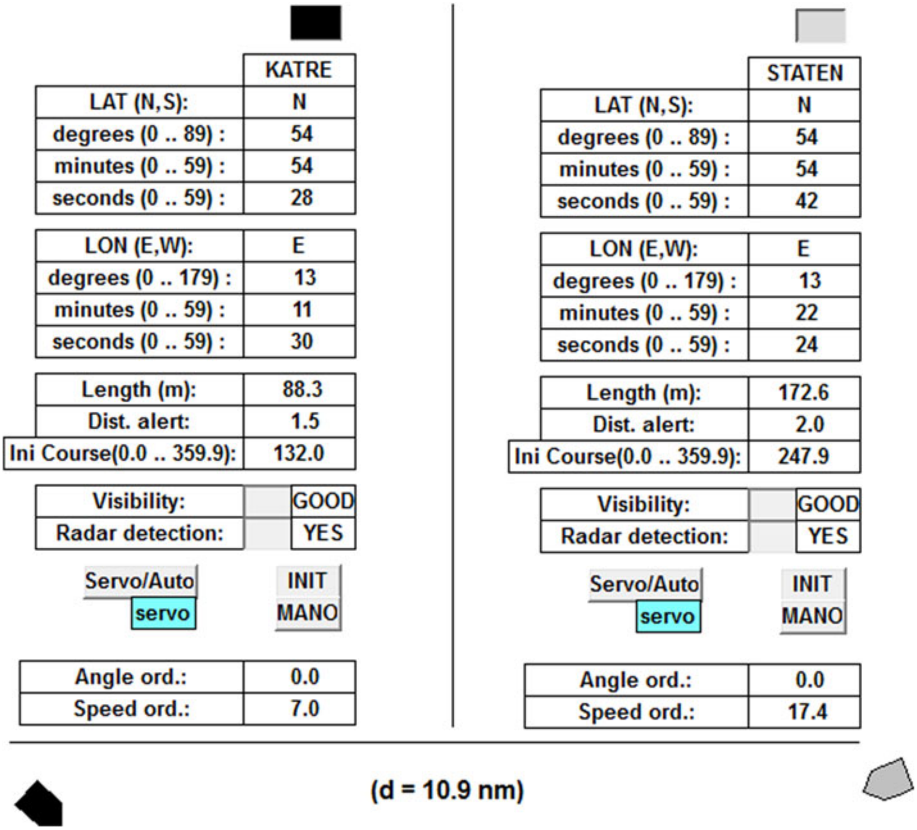
The safety functions are programmed using languages that comply with IEC 61131-3 (John and Tiegelkamp, 2010; Estévez et al., 2009). This standard defines the basic programming elements and rules for PLC programming languages. The Program Organisation Units (POUs) consist of small size encapsulated modules, each with a particular task that must be well defined and documented.

A list with 28 different manoeuvres has been defined, deduced from possible close-quarter situations, priorities and visibility conditions. The source PLC transmits the calculated manoeuvre using the AIS addressed binary message 6. This message includes the identification of the source and destination ships, that is, their Maritime Mobile Service Identity (MMSI) and, as binary data, only the number of the manoeuvre's order in the list (1...28). The destination PLC receives the message with that number and presents the associated manoeuvre on its HMI.

Module checking and integration tests should be carried out, following, for example the V-model (Mathur and Malik, 2010; Deuter, 2013; Lloyd and Reeve, 2009) accepted by the functional safety standards.

5.2. *Testing and integration.* A first version of the software modules for the described safety functions has already been developed. At present, it is being checked with simulated ship movements and communications, and with a basic HMI. A potential test follows, with data extracted from Katre-Statengracht (2014).

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press



	KATRE
LAT (N,S):	N
degrees (0 .. 89) :	54
minutes (0 .. 59) :	54
seconds (0 .. 59) :	28
LON (E,W):	E
degrees (0 .. 179) :	13
minutes (0 .. 59) :	11
seconds (0 .. 59) :	30
Length (m):	88.3
Dist. alert:	1.5
Ini Course(0.0 .. 359.9):	132.0
Visibility:	GOOD
Radar detection:	YES
Angle ord.:	0.0
Speed ord.:	7.0

	STATEN
LAT (N,S):	N
degrees (0 .. 89) :	54
minutes (0 .. 59) :	54
seconds (0 .. 59) :	42
LON (E,W):	E
degrees (0 .. 179) :	13
minutes (0 .. 59) :	22
seconds (0 .. 59) :	24
Length (m):	172.6
Dist. alert:	2.0
Ini Course(0.0 .. 359.9):	247.9
Visibility:	GOOD
Radar detection:	YES
Angle ord.:	0.0
Speed ord.:	17.4

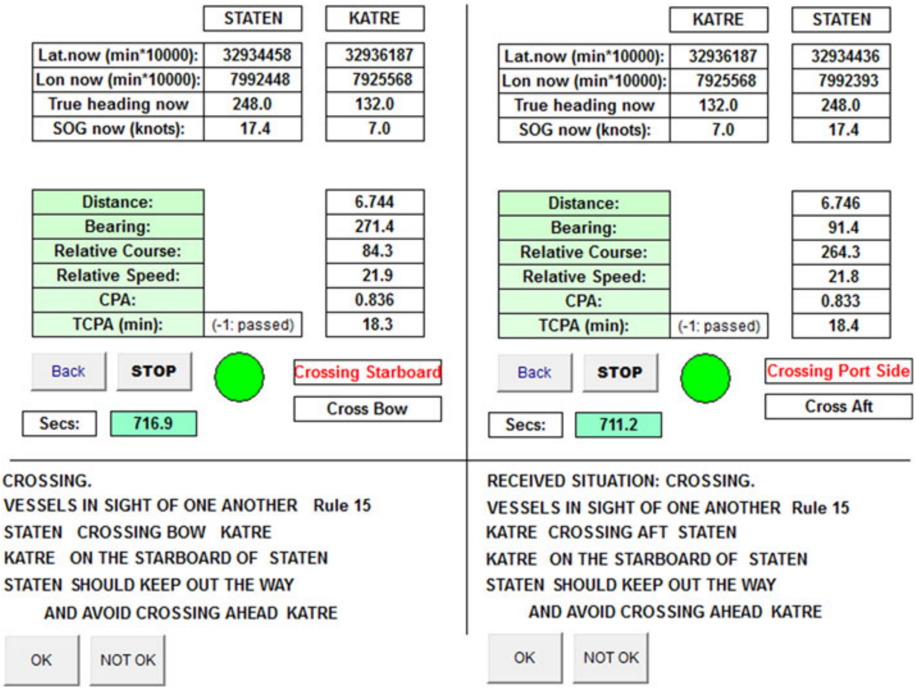
Figure 7. Initial data inputs (2 ships).

Figure 7 shows the initial data for two ships (KATRE and STATEN). The manoeuvres can be performed by varying the ordered courses (angles) or speeds. The models for the simulation of movements have been programmed following the standard ISO 11674-A (2006).

Figure 8 shows the values calculated by the corresponding POUs executed in the PLC of each ship from the AIS received dynamic positions. On the bottom left, the text with the calculated manoeuvre when STATEN PLC indicates a detected pre-alert. If the OOW taps OK, it is transmitted and KATRE PLC will display the message shown on the bottom right. The manoeuvring text includes ships names, visibility conditions, close-quarters situation and the COLREGs rule to apply. Messages are inspired by standardised phrases, which must be understood by all OOWs. With these written messages and data, errors of pronunciation or mistakes in understanding of their meaning would be avoided.

A special message will be displayed in both ships if the alert distance is reached by one of them, indicating that both vessels must manoeuvre.

Other messages (apart from manoeuvring) have been defined, associated to different steps in Figure 6: dynamic data handled by both PLCs are non-consistent, there is not agreement between OOWs, an OOW does not answer, etc.



	STATEN	KATRE
Lat.now (min*10000):	32934458	32936187
Lon now (min*10000):	7992448	7925568
True heading now	248.0	132.0
SOG now (knots):	17.4	7.0

Distance:		6.744
Bearing:		271.4
Relative Course:		84.3
Relative Speed:		21.9
CPA:		0.836
TCPA (min):	(-1: passed)	18.3

Secs: 716.9

Crossing Starboard

Cross Bow

CROSSING.
VESSELS IN SIGHT OF ONE ANOTHER Rule 15
STATEN CROSSING BOW KATRE
KATRE ON THE STARBOARD OF STATEN
STATEN SHOULD KEEP OUT THE WAY
AND AVOID CROSSING AHEAD KATRE

	KATRE	STATEN
Lat.now (min*10000):	32936187	32934436
Lon now (min*10000):	7925568	7992393
True heading now	132.0	248.0
SOG now (knots):	7.0	17.4

Distance:		6.746
Bearing:		91.4
Relative Course:		264.3
Relative Speed:		21.8
CPA:		0.833
TCPA (min):	(-1: passed)	18.4

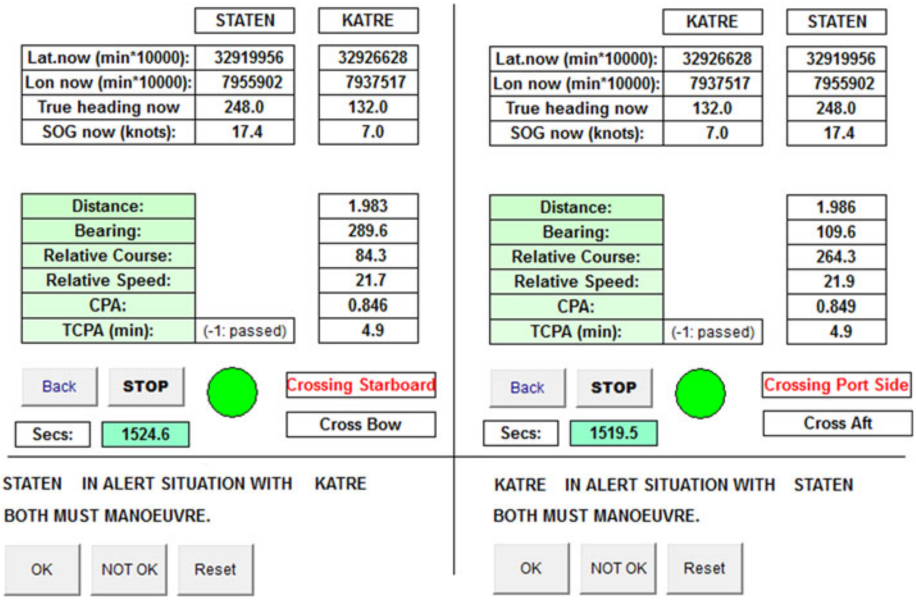
Secs: 711.2

Crossing Port Side

Cross Aft

RECEIVED SITUATION: CROSSING.
VESSELS IN SIGHT OF ONE ANOTHER Rule 15
KATRE CROSSING AFT STATEN
KATRE ON THE STARBOARD OF STATEN
STATEN SHOULD KEEP OUT THE WAY
AND AVOID CROSSING AHEAD KATRE

Figure 8. Dynamic data and manoeuvring messages at pre-alert (2 ships).



	STATEN	KATRE
Lat.now (min*10000):	32919956	32926628
Lon now (min*10000):	7955902	7937517
True heading now	248.0	132.0
SOG now (knots):	17.4	7.0

Distance:		1.983
Bearing:		289.6
Relative Course:		84.3
Relative Speed:		21.7
CPA:		0.846
TCPA (min):	(-1: passed)	4.9

Secs: 1524.6

Crossing Starboard

Cross Bow

STATEN IN ALERT SITUATION WITH KATRE
BOTH MUST MANOEUVRE.

	KATRE	STATEN
Lat.now (min*10000):	32926628	32919956
Lon now (min*10000):	7937517	7955902
True heading now	132.0	248.0
SOG now (knots):	7.0	17.4

Distance:		1.986
Bearing:		109.6
Relative Course:		264.3
Relative Speed:		21.9
CPA:		0.849
TCPA (min):	(-1: passed)	4.9

Secs: 1519.5

Crossing Port Side

Cross Aft

KATRE IN ALERT SITUATION WITH STATEN
BOTH MUST MANOEUVRE.

Figure 9. Dynamic data and manoeuvring messages at alert (2 ships).

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

More software testing and HMI enhancements are currently underway. The next step will be to perform integration with the hardware (PLC and AIS) and validation tests.

6. CONCLUSIONS.

Safety functions are being developed with the aim of reducing the risk of collisions between two ships (own-ship and each of N targets) due to errors in collision avoidance manoeuvres. For this purpose, the functions are designed to generate an alarm event and identify the type of dangerous encounter and suggest the manoeuvre to be performed, all of it always in compliance with COLREGs. The system needs to establish a reliable and unambiguous communication between the two ships involved, seeking to reach agreements at two levels:

- Agreements between PE systems, which ensure that both have the same dynamic information and the same calculated manoeuvre.
- Agreements between operators, which ensure that both accept (or not) the calculated manoeuvre.

The novelty of this proposal lies in that, for the first time, a system allows the user to know if both OOWs agree or not on the manoeuvres to be carried out. This makes it possible to act accordingly, since if a discrepancy arises, the safety margins can be increased, and the wrong decision properly identified.

It should be noted that the programming of the safety functions is carried out following basic principles of the functional safety regulations for software and that the final implementation will require only a PLC connected to AIS class A of each ship. The planned system does not interfere with the operation of the ship under normal conditions and it does not entail an excessive cost. To achieve a high degree of resilience, ensuring the quality of the data handled in the system, a strong emphasis must be placed on the improvement of the reliability and security of AIS transmissions, which may be directly affected by, among others, the use of insecure channels.

In a later stage, once the ship-to-ship encounters have been properly delimited, multi-vessel encounters will be studied. This scenario is significantly more difficult to resolve (Wen et al., 2015). The E/E/PE structure used here seems suitable, but the safety functions will need to be adapted to this new multiple vessel scenario, always counting on the experience gained from the ship-to-ship case development.

REFERENCES

Aven, T. (2017). Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliability Engineering and System Safety*, **167**, 42–48.

Baldauf, M., Benedict, K., Fischer, S., Gluch, M., Kirchhoff, M., Klaes, S., Schröder-Hinrichs, J.-U., Meißner, D., Fielitz, U. and Wilske, E. (2011). e-Navigation and situation-dependent maneuvering assistance to enhance maritime emergency response. *WMU Journal of Maritime Affairs*, **10**, 209–226.

Chauvin, C., Lardjane, S., Morel, G., Clostermann, J.P. and Langard, B. (2013). Human and organisational factors in maritime accidents: Analysis of collisions at sea using the HFACS. *Accident Analysis & Prevention*, **59**(C), 26–37.

COLREGs. (1972). Convention on the International Regulations for Preventing Collisions at Sea. *International Maritime Organization*, London.

David, R. (1995). GRAFCET: a powerful tool for specification of logic controllers. *IEEE Transactions on Control Systems Technology*, **3**(3), 253–268.

Deuter, A. (2013). Slicing the V-Model – Reduced Effort, Higher Flexibility, *IEEE 8th International Conference on Global Software Engineering (ICGSE)*, 1–10.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

Eliopoulou, E., Papanikolau, A. and Voulgarellis, M. (2016). Statistical analysis of ship accidents and review of safety level. *Safety Science*, **85**, 282–292.

EMSA. (2016). Annual overview of marine casualties and incidents 2016. *European Maritime Safety Agency.*

Estévez, E., Marcos, M. and Irisarri, E. (2009). Analysis of IEC 61131-3 Compliance through PLCopen XML interface. *7th IEEE International Conference on Industrial Informatics*, 757–762.

EU-OSHA. (2009). The human machine interface as an emerging risk. *European Agency for Safety and Health at Work*.

Ever-Alexandra. (2015). Report on the investigation of the collision between the container ship Ever Smart and the oil tanker Alexandra 1. https://assets.publishing.service.gov.uk/media/5665aff8e5274a0367000010/MAIBInvReport-28_2015.pdf. Accessed 4 March 2018.

Felski, A., Jaskólski, K. and Banyś, P. (2015). Comprehensive Assessment of Automatic Identification System (AIS) Data Application to Anti-collision Manoeuvring. *The Journal of Navigation*, **68**, 697–717.

Florida_Chou Shan. (2014). Report on the investigation of the collision between CMA CGM Florida and Chou Shan. https://assets.publishing.service.gov.uk/media/547c6f36e5274a4290000017/CMACGMFlorida_Report.pdf. Accessed 4 March 2018.

FSA. (2014). Revised guidelines for formal safety assessment (FSA) for use in the imo rule-making process. *International Maritime Organization*, London.

Gamer, T., Oriol, M. and Wahler, M. (2014). Increasing efficiency of M-out-of-N redundancy. *Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Barcelona*, 1–8.

Goerlandt, F. and Montewka, J. (2015). Maritime transportation risk analysis: Review and analysis in light of some foundational issues. *Reliability Engineering and System Safety*, **138**, 115–134.

Goerlandt, F., Montewka, J., Kuzmin, V. and Kujala, P. (2015). A risk-informed ship collision alert system: framework and application. *Safety Science,* **77**, 182–204.

Hibiscus-Hyundai. (2013). Report on the investigation of the collision between ACX Hibiscus and Hyundai Discovery. https://assets.publishing.service.gov.uk/media/547c6f6ce5274a4290000029/ACXHibiscus-HyundaiDiscovery_Report.pdf. Accessed 4 March 2018.

IEC 60848. (2013). GRAFCET specification language for sequential function charts. *International Electrotechnical Commission*. https://webstore.iec.ch/publication/3684

IEC 61131-6. (2012). Programmable controllers - Part 6: Functional safety.

IEC 61508. (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. http://www.iec.ch/functionalsafety/

IEC 61511. (2016). Functional safety/safety instrumented systems for the process industry sector. https://webstore.iec.ch/publication/24241

IEC 62061. (2005). Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems. *International Electrotechnical Commission*. https://webstore.iec.ch/publication/22797

ISO 11674-A. (2006). Ships and marine technology – Heading control systems. Annex A: Ship-motion simulator. *International Organization for Standardization.* https://www.iso.org/standard/44047.html

ITU-R M.1371-5. (2014). Recommendation ITU-R M.1371-5. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band. *Radiocommunication Assembly*, *International Telecomunication Union*. https://www.itu.int/rec/R-REC-M.1371/en

John, K.H. and Tiegelkamp, M. (2010). IEC 61131-3: Programming Industrial Automation Systems. *Springer Publishing Company, Inc*.

Katre-Statengracht. (2014). Safety investigation into the collision between the Maltese registered general cargo KATRE and the Dutch registered general cargo STATENGRACHT. http://mtip.gov.mt/en/document%20repository/msiu%20documents/investigations%202013/mv%20katre_final%20safety%20investigation%20report.pdf. Accessed 4 march 2018.

Kosmowski, K.T. (2006). Functional safety concept for hazardous systems and new challenges. *Journal of Loss Prevention in the Process Industries,* **19**, 298–305.

Last, P., Bahlke, C., Hering-Bertram, M. and Linsen, L. (2014). Comprehensive Analysis of Automatic Identification System (AIS) Data in Regard to Vessel Movement Prediction. *The Journal of Navigation*, **67**, 791–809.

Lloyd, M.H. and Reeve, P.J. (2009). IEC 61508 and IEC 61511 Assessments. Some Lessons Learned. *4th IET International Conference on Systems Safety*, 1–6.

Luo, M. and Shin, S. (2016). Half-century research developments in maritime accidents: Future directions. *Accident Analysis & Prevention*. Available online 19 April 2016.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press

Mathur, S. and Malik, S. (2010). Advancements in the V-Model. *International Journal of Computer Applications*, **1**(12), 30–35.

Melchers, R.E. (2001). On the ALARP approach to risk management. *Reliability Engineering and System Safety*, **71**(2), 201–208.

Montewka, J., Goerlandt, F. and Kujala, P. (2014). On a systematic perspective on risk for formal safety assessment (FSA). *Reliability Engineering and System Safety*, **127**, 77–85.

NMEA 0183. (2002). NMEA 0183 Standard for Interfacing Marine Electronic Devices. *National Marine Electronics Association*.

NMEA 2000. (2015). NMEA 2000 Standard for Serial-Data Networking of Marine Electronic Devices. *National Marine Electronics Association*.

Primorac, B.B. and Parunov, J. (2016). Review of statistical data on ship accidents. *Maritime Technology and Engineering*, **3**, 809–814.

Pietrzykowski, Z., Woejsza, P. and Borkowski, P. (2017). Decision Support in Collision Situations at Sea. *The Journal of Navigation*, **70**, 447–464.

Sotiralis, P., Ventikos, N.P., Hamann, R., Golyshev, P. and Teixeira, A.P. (2016). Incorporation of human factors into ship collision risk models focusing on human centred design aspects. *Reliability Engineering and System Safety*, **156**, 210–227.

Spring-Josephine. (2013). Spring Glory / Josephine Mærsk Collision. http://www.dmaib.com/SiteCollectionDocuments/Ulykkesrapporter/Handelskibe/kollisioner/SPRING_GLORY_JOSEPHINE_MAERSK_2012.pdf. Accessed 4 March 2018.

Stauffer, T. and Clarke, P. (2016). Using alarms as a layer of protection. *Process Safety Progress*, **35**(1), 76–83.

Summers, A.E. (2003). Introduction to layers of protection analysis. *Journal of Hazardous Materials*, **104**(1–3), 163–168.

Uğurlu, Ö., Köse, E., Yıldırım, U. and Yüksekyıldız, E. (2013). Marine accident analysis for collision and grounding in oil tanker using FTA method. *Maritime Policy & Management*, **42**, 163–185.

Vairo, T., Quagliati, M., Giudice, T., Barbucci, A. and Fabiano, B. (2017). From land- to water-use-planning: A consequence based case-study related to cruise ship risk. *Safety Science*, **97**, 120–133.

Wen, Y., Huang, Y., Zhou, C., Yang, J., Xiao, C., Wu, X. (2015). Modelling of marine traffic flow complexity. *Ocean Engineering*, **104**, 500–510.

https://doi.org/10.1017/S0373463318000553 Published online by Cambridge University Press