Article

Situation Assessment—An Essential Functionality for Resilient Navigation Systems

Evelin Engler¹, Michael Baldauf², Paweł Banyś^{1,*}, Frank Heymann¹, Maciej Gucma^{3,*}
and Frank Sill Torres⁴

¹ DLR, Institute of Communications and Navigation, 17235 Neustrelitz, Germany; Evelin.Engler@dlr.de (E.E.); Frank.Heymann@dlr.de (F.H.)

² Institute of Innovative Ship-Simulation and Maritime Systems (ISSIMS), Dept. Of Maritime Studies Rostock-Warnemünde, Wismar University of Applied Sciences, 23966 Wismar, Germany; Michael.Baldauf@hs-wismar.de

³ Navigation Department, Maritime University Szczecin, Chair of Navigation, 70-500 Szczecin, Poland

⁴ DLR, Institute for the Protection of Maritime Infrastructures, 27572 Bremerhaven, Germany; Frank.SillTorres@dlr.de

* Correspondence: Pawel.Banys@dlr.de (P.B.); M.Gucma@am.szczecin.pl (M.G.); Tel.: +49-3981-480-216 (P.B.); +48-91-4809-400 (M.G.)

Received: 16 November 2019; Accepted: 24 December 2019; Published: 30 December 2019

Abstract: This paper discusses the application of resilience engineering principles by shipborne navigation systems. As a technological system, the ship navigation system comprises all the communication and navigation equipment required to operate a ship. If examined as a socio-technological system, one has to additionally consider the use of the ship navigation system by the bridge teams in order to perform the nautical profession in terms of safe and efficient ship navigation, taking into account environmental information received by communication. The first part of this work discusses the theoretical background of resilience engineering and situation awareness. Case studies are used to illustrate under which conditions the application of resilience principles may result in an improvement of the operational reliability. With the help of simulations, it is shown that a sub-optimal implementation and utilization of resilience principles may decrease the robustness of the technical ship navigation system, as well as the reliability and adaptability of the ship navigation system in use. The examples illustrate once again that monitoring is one of the four cornerstones of resilience: anticipating, monitoring, learning, and responding. This is due to the effectiveness of most resilience principles depending on the availability and trustworthiness of situational information in relation to system status and environmental conditions, irrespective of whether the generation and use of the situational information is machine-made or human-made. Therefore, the establishment of situation awareness is an essential accompanying functionality to be considered in design, operation, and use of resilient systems.

Keywords: situation awareness; resilience principles; ship navigation; threats; robustness; risk mitigation

1. Introduction

1.1. Resilience as Challenge

The term “resilience” has been used in many scientific and engineering disciplines with different meanings. For example, resilience is used to address the robustness of technological as well as socio-technical systems, on the basis of which disturbances, incidents, and accidents can be avoided [1–3]. Resilience reflects also the need for human skills “to anticipate developments, threats, and opportunities”

into the future and to make the right decision about an adequate response [4–6]. Further performance characteristics of resilient systems are the preservation of function in times of stresses and the adjustment to changed conditions [7–9].

A rather general definition provided by the United Nations Office for Disaster Risk Reduction (UNISDR) considers resilience as the “ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management” [10]. For engineered systems, resilience represents the ability to adapt the operation to changing conditions, to withstand interfering influences, and to rebound from disruptive and destructive effects [1,2,7,11]. The capability for “adaption” is based on the means to avoid unintended disturbances, to defend against intended threats, as well as to minimize damages resulting from unavoidable destructive events. “Withstanding” reflects the capability of the system to adjust or reduce the operational functionality and performance expecting or following an encounter with a threat. “Rebounding”, in an engineered system, covers the use of suitable means to restore or to recover the original or aimed level of functionality and performance.

At present, the technological part of the ship navigation system is a network of components, subsystems, assemblies, and human–machine interfaces. This equipment is used by the bridge team for nautical activities including monitoring, anticipating, and decision-making in the context of vessel handling, to ensure safe shipping during the complete voyage. The components and subsystems cover sensors, radio navigation and communication equipment, and data sources, as well as facilities for data processing, evaluation, and visualisation, whereby their functioning and performance also depend on human-made configuring and controlling.

Therefore, the currently applied ship navigation systems may be considered as technological systems (without human in the loop) or as socio-technical systems (with human in the loop). The specific view of a navigation system ultimately determines what criteria have to be applied in order to assess the existence of resilience. However, if the focus is on safe and efficient ship navigation, the technological system and the crew have to be considered “as unified entity in coordination with the dynamically changing environment” [12], taking into account the status of technique and crew.

An exclusively technological consideration assesses the technical resilience (robustness) based on how far the technical systems are capable of providing the necessary navigational information with the required performance. In case of a socio-technical consideration, the human influence has to be taken into account; it acts as configurator, communicator, controller, and decision-maker of a navigation system, as well as a management authority initiating and performing adjustment activities in the face of emerging or occurred threats. Here, resilience is considered as achieved if the ship is navigated during the voyage with negligible risks regarding the loss of safety.

1.2. Resilience Principles

The standard for good behaviour may be provided by certain principles [13]. Resilience principles as discussed in [1,2,14] specify potential sources of resilience of engineered systems abstractly. However, the effectiveness of a potential source of resilience depends on its specific implementation into the system, considering the methodology used and the effect on other measures implemented alternatively or complementarily to achieve or improve the resilience of the system.

Jackson remarked that in the last decades more than 40 resilience principles have been elaborated for engineered systems [1,2]. He proposed to structure the principles into 14 top-level principles (see Table 1) and into additional subprinciples such as margin, automated function, or regroup subprinciples. The application of a certain resilience principle serves the establishment and/or improvement of a specific system capability in relation to an aimed-for system attribute [1,14]. Jackson introduced and explained four attributes as resilience targets [1]: “to survive a threat” (capacity), “to adapt to a threat” (flexibility), “to degrade gracefully in the face of threat” (tolerance), and “to act as unified whole in the face of threat” (cohesion).

Table 1. Top-level resilience principles, system capabilities, and attributes corresponding to [1].

	Principle	Capability	Attribute
1	absorption	to absorb the magnitude of disruption	capacity
2	physical redundancy	to overbridge single failures by redundant layout	
3	functional redundancy	to provide different ways to perform critical tasks	
4	layered defence	to apply two or more independent principles	
5	human in the loop	to use humans' better dealing with unprecedented threats	
6	reduction of complexity	to limit the complexity to the necessary degree	flexibility
7	reorganization	to adjust structure and functioning to current situation	
8	reparability	to be prepared for recovery of origin functionality and performance	
9	loose coupling	to limit error propagation in complex, networked systems	
10	localized capacity	to perform the functionality using distributed resources	tolerance
11	drift correction	to mitigate risks by adjustment to changes	
12	neutral state	to ensure true situation awareness for right decisions	
13	Inter-node interaction	to ensure communication, cooperation, collaboration between nodes for a coordinated use of resources	cohesion
14	reduce hidden interactions	to avoid harmful interactions between nodes	

Woods structured a variety of resilience principles by definition of four resilience concepts that differ in their main targets [15]. The first concept (resilience as robustness) deals with the robust system operation under normal and slightly degraded conditions. The second concept focuses on an effective and efficient rebounding from traumatic as well as destructive events (resilient rebounding and recovery). The third concept considers resilience at times when the system operates near or beyond its capacity limits or is surprised by unanticipated as well as new emerging threats (resilience as opposite to brittleness). The remaining concept (sustained adaptability) refers to the management of functionality and performance in a changing and networked world, comprising assumptions and boundary conditions, user requirements, framework conditions (e.g., economic, ecological, and legal), as well as the diversity of relationships and interactions.

Sterbenz et al. elaborated a set of principles for the design of resilient information networks and communication systems [16,17]. In these publications the actual resilience principles are named as enablers and cover general approaches (e.g., redundancy, diversity) as well as application-specific approaches (e.g., context awareness and translucency).

Independent of the preferred structuring and use of resilience principles, two things are important: on the one hand the resilience of a system or system-of-systems is a design target to be qualitatively and quantitatively specified. This implies that the aimed level of robustness has to be defined by functional requirements and performance parameters based on assumptions covering operational conditions and threat scenarios. This also requires ensuring a foresighted provision of resources to be prepared for rebounding and recovery. On the other hand, the maintenance of resilience is an everyday task to be mastered in a coordinated manner by the system itself and associated control and management bodies. For this purpose, the establishment of situation awareness plays an essential part and should cover both the current situation (status, condition) as well as all resilience-relevant changes (e.g., emerging threats; ethical, legal, and social aspects).

1.3. Situation Awareness

Over 30 years ago, Endsley defined situation awareness as “knowing what’s going on” and “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future” [18]. Situation awareness reflects that

“humans need to be aware of certain aspects of the world—at specific moments in time, to make critical decisions” [19]. Meanwhile, situation awareness has been developed into a human concept, which may be represented by the levels of perception (including noticing), comprehension, and projection. A distinction between these levels enables highlighting the different requirements for the perceptual and cognitive abilities of humans, as well as to illustrate the different consequences in times of diminished abilities [20]. In recent decades, the attention paid to situation awareness has risen significantly. One reason may be the increased requirements for humans, due to operational controlling and managing of more complex systems and infrastructures. Other reasons may result from the environmental changes, the emergence of new and unexpected threats, as well as the remaining indeterminacy within increasingly interconnected systems and infrastructures. As a result, a wide variety of models, of means for improvement and of applications have been developed and discussed, e.g., in aviation [21], in maritime traffic [22], for smart manufacturing [23], for security risk management [24], but also as an essential prerequisite for resilient entities [25]. Normally, the establishment of situation awareness is organised in frames determining the boundaries, the objects of interests, and the current and future implications to be assessed. The frames change depending on tasks to be performed (new or additional tasks), perceived situations (detected anomalies, existing uncertainties), as well as new or more crucial questions. Therefore, the establishment and maintenance of situation awareness is a dynamic process, which is triggered by the current situation awareness (new findings) as well as by applications using these new findings [19].

With increased automatization of shipping, the establishment of situation awareness is more and more supported by electronic means, acquiring, combining, and analysing data for the provision of assessed situation pictures and recommendations for actions. Upon this, it is remarked that autonomous shipping implies that human-made situation awareness has to be completely transformed into machine-made situation assessment. Here too, the machine-made situation assessment is premised on frames, objects, and implications, which are considered in a certain event horizon to ensure a safe and efficient operation of the autonomous system. The capability of the implemented machine-made situation assessment ultimately determines the boundaries for autonomous operation. Situation awareness as well as situation assessment are needed to anticipate situations and capacities to make sense of unexpected situations [19]. For a more general consideration of situation awareness and assessment, hereafter the paper uses the abbreviation SA irrespective of whether or not the SA is achieved by a human-made, machine-made, or a mixed approach. This allows the discussing of the role, importance, and influence of SA on the effectiveness of resilience principles [1,2] in relation to the cornerstones of resilience [25], and their use in one of the resilience concepts [15].

2. Ships' Navigation System

2.1. Carriage Requirements

Merchant vessels nowadays are equipped with increasingly sophisticated and complex navigational systems that have to comply with performance standards and being type approved after standard testing. Their task is to allow for an uninterrupted voyage in a dense traffic environment worldwide, and a safe and timely delivery of cargo to its destination. In order to standardise the requirements, merchant vessels engaged in international voyages have to meet the minimum safety standards in the construction and equipment defined by the International Convention for the Safety of Life at Sea (SOLAS). The SOLAS convention lays down the minimum carriage requirements, which ensure that the navigational capabilities of a given vessel class remain at the same technical level.

The carriage requirements for shipborne navigational systems and equipment are provided by Regulation 19 of the SOLAS convention Chapter V. Different rules apply to different vessel classes, which are categorised in terms of either their gross tonnage or their shipyard construction date. Another criterion is vessels primary operational characteristics (e.g., type of carried cargo on-board). When the matter of resilience is under consideration, the aspect of having redundancy of the on-board navigational

systems becomes significant. According to the aforementioned Regulation 19, the following elements of the navigation equipment have a clearly recommended back-up solution:

- ECDIS (Electronic Chart Display and Information System): it can either be supported by up-to-date paper charts or a secondary independent ECDIS device, which then renders the use of paper charts on board unnecessary.
- An auxiliary magnetic compass: interchangeable with the primary magnetic compass, independent of any power supply, it determines the magnetic course and to display its reading at the main steering position.
- a second radar, usually an s-Band radar.
- a second automatic tracking aid: a duplicate application to automatically plot the range and bearing of other targets to determine collision risks, which is functionally independent of the primary automatic radar plotting aid (ARPA).

It has to be emphasised that any implementation of additional redundancy into the navigational equipment is not forbidden by the regulations. The shipbuilders, manufacturers, and system providers are free to provide more duplicates of the safety-relevant system components to the navigators in order to improve the resilience. While Regulation 19 of SOLAS chapter V mentions the requirements for specific elements of the navigation equipment to be installed on board, IMO Resolutions and Performance Standards provide the technical specifications of the equipment. In this respect, legally binding standards for Integrated Navigation Systems (INS) are specified based on functional requirements for the navigational tasks and also require redundancy, back-up, and fail-safe arrangements. Consequently, INS as a whole is designed to partly or fully satisfy the requirements for minimum navigation equipment.

2.2. Technical Systems for Detection and Indication of Threats

Safe navigation needs to address all kind of risks and safety threats that can occur during a voyage from the port of departure to the port of destination. Such threats range from risks of potential damages caused, e.g., by environmental conditions (heavy weather, storms, waves) or traffic as well as societal threats like piracy or cyberattacks disturbing the functioning of technical systems. In this paper, we concentrate on threats caused by navigational errors, which means risk of collision, grounding, and stranding.

From a purely technical perspective, the detection of collision risks is mainly based on the determination of relative positions or distances using Radar-ARPA and the Automatic Identification System (AIS). Radar detects every object reflecting electromagnetic waves. AIS is a cooperative system and only works well in cooperation with participating vessels and equipped objects (e.g., oil rigs, off-shore wind mills, or Aids to Navigation etc.). AIS transponders use Global Navigation Satellite System (GNSS) signals primarily to synchronise the TDMA communication channels used for data exchange. Secondly, AIS transponders act as a back-up for electronic position fixing equipment. Therefore, among others, AIS will fail if GNSS fails. Analyses of dynamic ship data exchanged for collision avoidance have shown that erroneous position, course, or speed data may indicate safe situations while a collision is very probable [26]. The comparative consideration of radar and AIS data is a reasonable approach to detect inaccuracies of navigational data.

According to the International Rules for Preventing Collisions at Sea, encounter situations can be categorised into head-on, crossing, and collisions on parallel courses [27]. For each of these encounter situations, different GNSS-based parameters are taken into consideration for risk identification and threat detection. For example, while, in head-on situations the course errors are much more important than speed errors, in crossing situations both parameters are equally important, and in parallel course situations the speed is more important. This requires different threat detection strategies performed by algorithms to be implemented into the above mentioned mandatory tracking devices. However, at present, the navigation equipment does not support enhanced risk detection or threat identification algorithms, but is purely based on simplified and robust encounter warnings using

CPA (distance at the closest point of approach) and TCPA (time to CPA) thresholds. Consequently, in terms of resilience, the technical systems are insufficiently designed for effectively triggering collision warnings [28,29]. The detection of grounding and stranding threats is based on the knowledge of absolute positions and the existence of appropriate nautical charts. Here, two challenges have to be solved: the integrity assessment of GNSS-based navigational data and the integrity assurance of nautical charts. The latter follows from the fact that a perfect position is still not enough if the chart does not include, e.g., the correct water depth information.

2.3. Threat Management by Socio-Technical Ship Navigation System

Regardless of the degree of ship automation, nowadays the crew is still responsible for safe navigation of the ship. In this context, safety means the successful avoidance of collisions and groundings during all navigation phases of a voyage. This requires that the crew and the shipside equipment have to function as a whole under permanently changing conditions. The existing need for human cognition is provided by the crew and, consequently, the resilience principle “human in the loop” is satisfied. The crew on board the ship is responsible for the navigation of ship, the technical operation, the cargo and passenger handling or the provision of further services. Typical tasks of ship navigation include route planning, route monitoring, track control, and alert management, besides the avoidance of collisions and grounding. Most of these tasks require information provided by other traffic participants as well as information and infrastructure service providers. Moreover, the referred SOLAS chapter V lays down requirements for other means and measures to ensure safety of navigation from ashore, namely especially Vessel Traffic Services (VTS). It is described in Regulation 12 and detailed guidelines are provided through the related IMO resolution A.857(20). In terms of safety and resilience, VTS contribute to the safety of navigation as an additional barrier doubling parts of the on-board navigation process by monitoring the vessel traffic from the shore-side perspective and providing information, partly redundant, additional and complementary to the information available on-board through the installed equipment. Any VTS information broadcasted to all ships or transmitted as warning or advice is to support on-board decision making by improving on-board situation awareness. Similarly to VTS, so-called company owned Fleet Operations Centres (FOC) have been recently introduced to shipping and can be seen as another shore-based safety barrier. Contrary to VTS, FOC are monitoring the progress of the ships of the own fleet on a world-wide scale making use of enhanced data transmission from ship to shore and repeating the on-board equipment information in the shore-based FOC in nearly real-time. Operators in the FOC ashore can, in principle, communicate directly to the officer of the watch (OOW) on-board and make him aware of alerts that might have been overseen for any reason [30,31].

3. Case Studies

3.1. Resilience by Additional Capacities

In general, a system is designed to meet the requirements on functionality and performance at the most likely disturbance and disruption levels. Hardenings of the system components in order to decrease the vulnerability and an adequate consideration of margins in order to handle the uncertainties are some design aspects which may increase the ability of the system to absorb the “magnitude of the disruption that it encounters” [1]. This ability can be reliably obtained, if a retrospective situation assessment has been performed in order to achieve a realistic representation of the vulnerability in relation to the most likely disturbances and disruptions.

A further approach is the implementation of physical or functional redundancy in order to strengthen the system robustness against single failures as one facet of the resilience [1,15]. The implementation of replicas at systemic level (see Figure 1a, physical redundancy) may prevent a partial breakdown of one system branch (1 or 1') directly resulting in the loss of system's functioning [17]. If critical tasks are performed in independent ways (Figure 1b, functional redundancy) a decorrelation

of errors, hazard influences, and dependencies can be expected. The overcoming of technical failures via human interference also represents a kind of functional redundancy. For example, the loss of GNSS-based position determination can be overbridged by nautical staff using a sextant and mechanical clock. Therefore, the following studies apply regardless of whether the system is considered as a technical or socio-technical system.

Figure 1. Redundant layouts of a system (consisting of two system functions SF a and SF b) with physical redundancy (a), as well as functional redundancy (b), and remaining performance violation (c), as a function of the correlation factor between the redundant system branches and correctness of MED function.

It is well-known that the reliability P_s of the redundant system $P_s = 1 - (1 - P_1) \times (1 - P_2)$ may increase up to 99.75% if the reliabilities P_1 and P_2 of both system branches are assumed to be $P_1 = P_2 = 95\%$. It is fact that the implementation of redundancy extends over the system origin and may decrease the reliability if not properly implemented. As illustrated in Figure 1a,b the system extension results from the implementation of the additional branch (system 1' or 2) as well as from MED-functions to monitor (M), evaluate (E), and decide (D) about the use of the redundant branches.

Based on a basic simulation setup, the remaining performance violation of a system with two redundant branches is investigated. It is assumed that each of the branches has a reliability of 95% over the complete simulation time. During the simulations, the MED function (monitoring, evaluation, decision making) and the switch (control instance) are considered as one control function, MED (c), selecting which of the system branches should be currently operated. During each simulation run, the reliability of MED (c) is fixed either as 95%, 99%, or 100%. Random variables are re-determined for each simulation epoch as a decision criterion, if a system branch or MED (c) works in compliance with its specification or not. The specification is fulfilled if the random variable is inside the 95%, 99%, or 100% value range of normal distribution. The random variables of the system branches are generated by a 2-dimensional normal distribution function, whereby the selected covariance matrix specifies the correlation factor between both branches. If the correlation factor is 1, physical redundancy is given (Figure 1a). If the system branches are uncorrelated (correlation factor is 0), the layout is redundant and dispersive (Figure 1b, functional redundancy).

During the simulations (100.000 epochs), a performance violation of the redundant system occurs if none of the redundant system branches operates reliable or if MED (c) is unable to select the reliable operating system branch. As can be seen in Figure 1c, the highest reliability of 99.75% is only achieved if both system branches are completely decorrelated (correlation factor 0) and the MED (c) function operates error-free (100% correctness). With increasing correlation factor, the performance violation of the redundant system increases from 0.25% to the performance violation of a non-redundant system

(5%). It cannot be expected that in reality the correctness of MED (c), or its reliability, achieves 100%. As can be seen, if the reliability of MED (c) is 95% or below, the reliability of the redundant system falls below the reliability of using only a single system branch. This illustrates the need for, as far as possible, high-performance monitoring and decision making.

As outlined in Section 2.1, a ship has to be equipped with 2 or more radio navigation receivers to ensure a reliable positioning. Using 2 GPS receivers for this purpose will result into a very high correlation factor (same GNSS signals, propagation errors, positioning methods, etc.). Assuming a correlation factor of 0.9 between the redundant branches and a MED (c) reliability of 99% ensures a reliability gain of 1% for the redundant system. If the MED (c) reliability decreases below 95%, the reliability of the redundant system is inferior to the reliability of a redundant system switching randomly between both branches. This explains the high demand on qualification and training for humans who perform MED (c) functions every day.

3.2. Resilience by Tolerance

A further approach improving the system resilience is to become open-minded towards the occurrence of isolated breakdowns, partial distortions, and major disturbances and to enable that a graceful degradation of functionality can be ensured in the face of any threats. This can be achieved if the functionality is distributed or dispersed to different modules and nodes (localized or dispersed capacity) [1]. Due to the modularisation, it can be ensured that in face of threats only a stepwise degradation can occur. This gives the time to limit negative effects and to minimize direct and indirect damages resulting from that threat.

Going back to the example illustrated in Figure 1a,b, where the redundant system is sensitive to a decrease of the reliability of MED(c), now the MED(c) function is implemented by the functions ME1 and ME2. Both functions perform nearly independently from each other the monitoring and evaluation of the usability of system branches. Furthermore, a perfectly functioning switch is triggered by the ME1 and ME2 evaluation results (Figure 2a).

Figure 2. Redundant layouts of a system (consisting of two system functions SF a and SF b) with functional redundancy and dispersive monitoring and evaluation functions (a) and remaining performance violation (b) as a function of correlation factor between the branches and correctness of ME1 and ME2 functions (assuming a perfectly functioning of decision logic and switch).

If ME1 and ME2 operate with 100% reliability, the performance violation of the redundant system (Figure 2b) behaves as the performance violation given in Figure 1c for a MED (c) reliability of 100%. However, it can be observed that the dispersion of monitoring and evaluation attenuates the reliability losses of the redundant system by non-perfect monitoring and evaluation. This confirms the notion

that the use of two resilience principles (here redundancy and localised capacity) may improve the resilience of the overall system. Figure 2 also indicates that, if the correctness of ME1 and ME2 falls below 80%, a possible reliability gain by redundancy is lost, too.

Drift correction means in general the use of corrective actions in order to avoid the drifting of a system towards the resilience boundary resulting in incidents, accidents, or other destructive events. In the case discussed here, drift correction enables detection of whether a system branch or both branches drift towards the resilience boundary. For this purpose, another kind of MED (c) is required that enables the monitoring and evaluation of changes of the system and conditions in order to forecast the criticality of the system behaviour. This allows the system to adjust to the detected drift for risk mitigation in real time and/or in relation to latent degradations. An example of a short-term drift correction is the detection of multipath effects on radio navigation signals and the exclusion of affected signals from positioning. Another example for a long-term drift correction is the aging process of GNSS equipment for predictive maintenance. In these cases, as already outlined, misinterpretation of situation-relevant information as well as insufficient availability of information may result in poor decision making.

3.3. Resilience by Flexibility

According to Jackson & Ferries [1] flexibility principles describe the ability of a system to adapt to threats and comprises the principles 'Reorganization', 'Reduce Complexity', and the 'Human-in-the-loop' principle. The principle 'Human-in-the-loop' contains the subprinciples 'human in control', 'human error', and 'automated function'. The principle requires that a human should always be in the system when there is a need for human cognition. Ship navigation requires multiple tasks to be performed in compliance with current IMO instruments by the nautical staff as 'Human-in-the-loop', using all means available and suitable for the specific tasks. However, numerous studies and statistics of maritime accidents identified the human in the loop as one of the major causes of collisions and groundings, quantifying it to 80% or even 90%. The authors are of the opinion that the high proportion may be a result of simplifying the complex processes and events that finally lead to collision or grounding. Consequently, it makes sense to discuss the effectiveness of flexibility as resilience principle in relation to intervention points of an occurred accident.

The chosen sample case is a collision between a RoRo-passenger 'Ferry' and a bulk carrier 'Bulker', which occurred in the Western part of the Baltic Sea. The collision happened near the easterly end of the southern traffic lane of the established Traffic Separation Scheme (TSS), located approximately halfway between Danish and German coast. The traffic lane's direction changes at the easterly end to a northerly direction. According to the official accident investigation report [32] there was calm weather and good visibility. The bridges of the involved ships were properly manned and equipped in compliance with SOLAS requirements. The AIS tracks of the ships that were involved in the collision scenario are presented in Figure 3. The gaps in these tracks and the obviously faulty heading of ships indicates a lack of AIS data exchange, which has been especially investigated and discussed in [33]. The official accident investigation report did not refer to such issues.

However, the published report identified a variety of factors and causes, which were found ultimately led to the accident. Hereunder, we exemplarily discuss selected identified causes in relation to potential interventions that may have avoided the collision. The first item to discuss is that the Roro-passenger ferry was the vessel with highest speed in relation to the other vessels already sailing inside the TSS. 'Ferry' entered the separation scheme aft of these ships to avoid close-quarter situations. At this point, in anticipating the long-term development of the situation (including direction change of traffic lane, own route and speed as well as that of the other vessels, known by AIS or VHF-voice communication) the possibility was given for 'Ferry' originally planning and taking her route north of 'Alpha', and not between the northernmost 'Alpha' and the second to north 'Dana'. Due to the taken decision, 'Ferry' lost the chance to follow the regular track without interference from the other ships. It is assumed that this would have reduced the complexity of the situation.

Figure 3. Automatic Identification System (AIS) tracks of collision scenario (adapted from [33]).

The developing close-quarter situation of the four ships was obvious and potential course changes were to be expected from the traffic lane's direction change ahead of all ships. In the face of this situation, an appropriate adaptation of the speed of 'Ferry' would have created the room to be able to grasp the changes in the situation and carry out adequate manoeuvres (reorganize own ship operation to be able to act as human in control). Similarly, it would have been possible for the 'Bulker' to slow down to enable a conflict-free passing of the port side ships before changing the course to follow the traffic lane.

Although 'humans in the loop' were on board both the colliding ships, they were not able to perform assessment of the situation correctly and in due time. 'Ferry' primarily observed 'Alfa' and consequently did not notice the turn to port and new course of the 'Bulker'. On the other hand, 'Bulker' was unable to take notice of the 'Ferry', which may have been as a result of the violated rest hour requirements. However, the shortcomings in the assessment of the situation on both vessels resulted in the humans' inability to act and react flexibly (reorganize situation assessment to consider the current situation as whole). A further point of discussion is the lack and inadequacy of direct communication between the traffic participants. It is known that a limitation of the 'Human-in-the loop' principle is the lack of information needed to make correct decisions and to take action in ample time, quickly enough for the avoidance of incidents, accidents, and damages. A proactive communication would potentially have made it possible to take into account the planned routes before the ship manoeuvres were carried out (communication reorganized to be able to act as whole). Finally, let's have a look at the last action of 'Ferry'. Approximately 45 s before the collision, she started a hard to port manoeuvre, but it was obviously too late and could therefore not avoid the collision, which was claimed to be a combination of various human errors. The subprinciple 'reduce human errors' asks for standard strategies reducing human errors if employed. Therefore, violations of IMO's Convention on the International Regulations for Preventing Collisions at Sea (COLREGs) shall be avoided, in general. In addition to the shortcomings already mentioned, this also concerns the manner in which 'Alfa' and 'Dana' left the traffic lane and the compliance of 'Bulker', with rules for overtaking manoeuvres.

In respect to resilience by flexibility, shore-based support to accident avoidance needs to be taken into account. At the time of the accident, there was no VTS, although technical means such as shore-based radar and AIS were already available. From a technical point of view, monitoring and intervening of vessel traffic were feasible. Nevertheless, it was not from a legal point of view (VTS area did not cover the location of the accident). However, recognizing that a VTS is not able to avoid collisions directly, a VTS may act as independent monitoring instance and can therefore contribute to on-board decision making by informing involved vessels about the situation assessment from the shore-side perspective. This also enables, when there is a need for coordination and adjustment, stimulation of, or calling for, appropriate actions. VTS provides additional intervention possibilities and corresponds with other resilience principles serving the establishment of 'layered defence', distributing safety-critical tasks among different nodes ('localized capacity'), or establishing 'functional'

redundancy in relation to situation assessment. In relation to the considered accident, the availability of additional intervention options could have compensated the insufficient situation awareness and situation assessment.

4. Conclusions

The reliable provision of nautical data to the bridge team is a prerequisite for safe and efficient ship navigation during each voyage. Safety is reflected by the successful avoidance of collisions, groundings, and fire. Efficiency is measured in relation to the cost–benefit ratio of each sea voyage. This implies that the ability of the shipborne navigation system to adapt its operation to changing conditions, to withstand interfering influences, and to rebound from disruptive and destructive effects is a recurring challenge and task to be solved during design (to become resilient) as well as operation (to manage resilience). The empowerment to be resilient covers, amongst others, the maintenance of robustness, reliability, and adaptability and cannot be discussed without consideration of monitoring as one of the cornerstones of resilience [33]. The interdependency between applied resilience principles and MED-capabilities has been illustrated and discussed for selected examples. As seen, the implementation of redundancy into the shipborne navigation systems results in enhancement of reliability, only if the functions of redundant system branches operate as much as possible in a decorrelated manner and if an extremely high detection rate of the usable system branch is achieved. It was shown that the application of a second resilience principle (localized or dispersed capacity) on the MED (c) functionality helped to reduce the negative influence of wrong monitoring, evaluation, and/or decision making. However, in this case, there is a remaining risk that despite the application of two resilience principles the reliability of the redundant system may fall below the reliability of a single system branch, irrespective whether or not the incorrect decision making is caused by technical functions or human activities to perform the MED (c) functionality.

It is undisputed that the safety of navigation is to a much larger extent ensured through actions of human operators compensating failures or shortcomings of the technical systems (as, e.g., incorrect or lately triggered collision alarms). Rather conversely, technical systems presently in use are still far from sufficiently resilient, to compensate a poor performance of a human operator. The grounding of the ‘Costa Concordia’ was caused by a number of influencing factors [34], but none of the technical systems were resilient enough to compensate quickly enough for the insufficient situation awareness and inappropriate decision making of the human operators of the bridge team. Further research is needed in order to study the processes and interactions on a more comprehensive and holistic basis.

The idea of using resilience principles to ensure safety of navigation and enhance shipping is not new [5,6,35–37] and is applied to different aspects of safe shipping, e.g., improvement of vessel traffic service, investigation of ship accidents, development of safety II perspective [38] for the maritime world, or awareness of traffic situation for safe navigation. All of the papers (including this) make clear that the consideration of single factors is insufficient to achieve resilience. Furthermore, regardless of whether the focus is more on the technique or the human factor, it is mandatory to model ship navigation as a set of processes under consideration of dependencies and interactions. For example, the model of maritime perspective-taking presented in [12] provides a generalized process-model for navigational decision-making. The main challenge has been identified as the interaction between the knowledge and experience related to initial parameters, represented as ship profiling, and to the situation at hand, expressed as situation assessment, in order to make navigational decisions in an environment of partially uncertain situations and situation development.

Author Contributions: For this research article the specifying of the individual contributions of the authors is as follows: conceptualization, E.E., P.B. and F.H.; methodology, E.E. and M.B.; investigation, E.E., M.B., and P.B.; software and visualization, E.E. and M.B.; writing (original draft preparation) E.E. and P.B.; writing (review and editing) E.E., M.B., P.B., F.H., M.G. and F.S.T.; supervision, E.E. and F.S.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jackson, S.; Ferris, T.L.J. Resilience Principles for Engineered Systems. *Syst. Eng.* **2013**, *16*, 152–164. [[CrossRef](#)]
2. Jackson, S.; Ferris, T.L.J. Designing Resilient Systems. In Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructures Safeguarding, Azores, Portugal, 26–29 June 2016; pp. 121–144.
3. Sansavini, G. Engineering Resilience in Critical Infrastructures. In Proceedings of the NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructures Safeguarding, Azores, Portugal, 26–29 June 2016; pp. 189–203.
4. Clarke, D. Human redundancy in complex, hazardous systems: A theoretical framework. *Saf. Sci.* **2005**, *43*, 655–677. [[CrossRef](#)]
5. Praetorius, G.; Hollnagel, E. Control and Resilience Within the Maritime Traffic Management Domain. *J. Cogn. Eng. Decis. Mak.* **2014**, *8*, 303–317. [[CrossRef](#)]
6. Praetorius, G. Vessel Traffic Service (VTS): A Maritime Information Service or Traffic Control System? Understanding Everyday Performance and Resilience in a Socio-Technical System under Change. Ph.D. Thesis, Chalmers University of Technology, Gothenburg, Sweden, 2014.
7. Woods, D.; Branlat, M. Essential characteristics of resilience. In *Resilience Engineering in Practice: A Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Ashgate Pub Co.: Surrey, UK, 2011.
8. Hollnagel, E.; Leonhardt, J.; Licu, T.; Shorrock, S. From Safety-I to Safety-II. In *A White Paper*; European Organisation for the Safety of Air Navigation: Bruges, Belgium, 2013; Available online: <http://www.skybrary.aero/bookshelf/books/2437.pdf> (accessed on 27 December 2019).
9. Hollnagel, E. Prologue: The scope of Resilience. In *Resilience Engineering in Practice: A Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Ashgate Pub Co.: Surrey, UK, 2011.
10. United Nations. *UNISDR Terminology on Disaster Risk Reduction*; United Nations International Strategy for Disaster Reduction: Geneva, Switzerland, 2009; Available online: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf (accessed on 15 July 2019).
11. Fiksel, J. Designing resilient, sustainable systems. *Environ. Sci. Technol.* **2003**, *37*, 5330–5339. [[CrossRef](#)] [[PubMed](#)]
12. Wahlström, M.; Forster, D.; Karvonen, A.; Puustinen, R.; Saariluoma, P. Perspective-Taking in Anticipatory Maritime Navigation - Implications for Developing Autonomous Ships. In Proceedings of the 18th International Conference on Computer and IT Applications in the Maritime Industries, Tullamore, Ireland, 25–27 March 2019; pp. 191–200.
13. Cambridge Dictionary. Available online: <https://dictionary.cambridge.org/de/worterbuch/englisch/principle> (accessed on 2 September 2019).
14. Madni, A.M.; Jackson, S. Towards a Conceptual Framework for Resilience Engineering. *IEEE Syst. J.* **2009**, *3*, 181–191. [[CrossRef](#)]
15. Woods, D.D. Four concepts for resilience and the implication for the future resilience. *Reliab. Eng. Syst. Saf.* **2015**, *141*, 5–9. [[CrossRef](#)]
16. Sterbenz, J.P.G.; Hutchison, D.; Cetinkaya, E.K.; Jabbar, A.; Rohrer, J.; Schöller, M.; Smith, P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Comput. Netw.* **2010**, *54*, 1245–1265. [[CrossRef](#)]
17. Sterbenz, J.P.G.; Hutchison, D.; Cetinkaya, E.K.; Jabbar, A.; Rohrer, J.; Schöller, M.; Smith, P. Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance. *Telecommun. Syst.* **2014**, *56*, 17–31. [[CrossRef](#)]
18. Endsley, M.R. Toward a theory of situation awareness in dynamic systems. *Hum. Factors* **1995**, *37*, 32–64. [[CrossRef](#)]
19. Lundberg, J. Situation Awareness States, Systems, and Processes: A holistic framework. *Theor. Issues Ergon. Sci.* **2015**, *16*, 447–473. [[CrossRef](#)]
20. Wickens, C. Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement. *Hum. Factors* **2008**, *50*, 397–402. [[CrossRef](#)] [[PubMed](#)]

21. Shook, R.W.C.; Bandiero, M.; Coello, J.P.; Garland, D.J.; Endsley, M.R. Situation awareness problems in general aviation. *Proc. Hum. Factors Ergon. Soc. Annu. Meet.* **2000**, *44*, 185–188. [\[CrossRef\]](#)
22. Van Westrenen, F.C.; Praetorius, G. Situation awareness and maritime traffic: Having awareness or being in control. *Theor. Issues Ergon. Sci.* **2009**, *15*, 161–180. [\[CrossRef\]](#)
23. Park, C.Y.; Blackmond, L.K.; Salim, S.; Lee, J. Predictive situation awareness model for smart manufacturing. In Proceedings of the 20th International Conference on Information Fusion, Xi'an, China, 10–13 July 2017.
24. Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G. A situation awareness model for information security risk management. *Comput. Secur.* **2014**, *44*, 1–15. [\[CrossRef\]](#)
25. Hollnagel, E. The four cornerstones of resilience engineering. *Resil. Eng. Perspect.* **2009**, *2*, 117–134.
26. Banyś, P.; Heymann, F.; Engler, E.; Noack, T. Comparison of AIS-based Prediction of the Distance at the CPA with Factual Separation Between Vessels. *Annu. Navig.* **2014**, *21*, 5–18. [\[CrossRef\]](#)
27. Hilgert, H.; Baldauf, M. A common risk model for the assessment of encounter situations on board ships. *Dtsch. Hydrografische Z.* **1997**, *49*, 531–542. [\[CrossRef\]](#)
28. Baldauf, M.; Benedict, K.; Fischer, S.; Motz, F.; Schroder-Hinrichs, J.-U. Collision avoidance systems in air and maritime traffic. *J. Risk Reliab.* **2011**, *225*, 333–343. [\[CrossRef\]](#)
29. Baldauf, M.; Mehdi, R.; Fischer, S.; Gluch, M. A perfect warning to avoid collisions at sea? *Sci. J. Marit. Univ. Szczec.* **2017**, *49*, 53–64. [\[CrossRef\]](#)
30. Van Westrenen, F.; Baldauf, M. Improving conflicts detection in maritime traffic: Case studies on the effect of traffic complexity on ship collisions. *J. Eng. Marit. Environ.* **2019**. [\[CrossRef\]](#)
31. Baldauf, M.; Fischer, S.; Kitada, M.; Mehdi, R.A.; Al-Quhali, M.A.; Fiorini, M. Merging Conventionally Navigating Ships and MASS—Merging VTS, FOC and SCC? *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 495–501. [\[CrossRef\]](#)
32. Department of the Environment, Transport and Regions; Marine Accident Investigation Branch. *Report on the Investigation of the Collision Between Swedish Roro Vessel FINNSAILOR and Maltese Bulk Carrier GENERAL GROT-ROWECKI*, Sjöfärhatsinspektionen, Sjöfartsverkets Rapportserie B 2006-7; R-Report; Department of the Environment, Transport and Regions: London, UK, 2007.
33. Baldauf, M.; Benedict, K.; Motz, F. Aspects of technical reliability of navigation systems and human element in case of collision avoidance. In Proceedings of the Navigation Conference & Exhibition, London, UK, 28–30 October 2008.
34. Wreathall, J. Monitoring—A critical ability in Resilience Engineering. In *Resilience Engineering in Practice: A Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Ashgate Pub Co.: Surrey, UK, 2011.
35. Schröder-Hinrichs, J.-U.; Praetorius, G.; Graziano, A.; Kataria, A.; Baldauf, M. Introducing the Concept of Resilience into Maritime Safety. In Proceedings of the 6th Resilience Engineering Association Symposium, Lisboa, Portugal, 22–25 June 2015.
36. Smith, D.; Veitch, B.; Khan, F.; Taylor, R. Using the FRAM to Understand Arctic Ship Navigation: Assessing Work Processes During the Exxon Valdez Grounding. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2013**, *12*, 447–457. [\[CrossRef\]](#)
37. Wahlström, M. Resilience on the seven seas: perspective -taking in anticipatory ship navigation. In Proceedings of the 8th REA Symposium Embracing Resilience: Scaling Up and Speeding Up, Kalmar, Sweden, 24–27 June 2019.
38. Hollnagel, E. RAG—The resilience analysis grid. In *Resilience Engineering in Practice: A Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Ashgate Pub Co.: Surrey, UK, 2011.