Poor Monitoring of the Navigation and Steering Equipment Increases the Reaction Time in Fault Situations

Sauli Ahvenjärvi

Principal Lecturer
Faculty of Technology and Maritime Management
Satakunta University of Applied Sciences
Suojantie 2, FI-26200 Rauma
Finland
Email: sauli.ahvenjarvi@samk.fi

Abstract Behaviour of the officer of the watch (OOW) in managing a failure in the automatic navigation and steering system has been studied by analysing five real accident cases. This paper describes the main results of the analysis. In all analysed cases the accident was partially caused by delayed operator action after a critical failure in the system. The situation is extremely difficult for the operator, when the system fails to give a direct alarm of the failure. The analysis revealed that the operator does not continuously monitor the performance of the equipment. The OOW concentrates on monitoring the overall situation and the movements of the ship rather than on finding out how the navigation and steering equipment is working. These two levels of monitoring are called 'the process level' and 'the equipment level'. Only if an abnormality is noticed on the process level the OOW pays attention to the equipment level. This can not be considered as a user error or an indication of fatigue, but a quite logical behaviour of the OOW. In all the five analysed accident cases the process level monitoring failed to give the OOW a reason to check the performance of the equipment until it was too late to avoid the grounding. This problem of delayed operator action is particularly dangerous in confined waters. It can not be solved by providing more visual information about the performance of the equipment, due to the behaviour of the operator. It can neither be solved by increasing the training of the users because the delayed operator action is not caused by lack of skills, knowledge or motivation. Some potential ways to solve the problem are discussed in the end of the paper.

Keywords bridge systems; navigation; automatic steering; safety; human factor

0 Introduction

The integrated navigation and control (INC) system of the ship is a technical entity able to

automatically measure the position, heading and speed of the ship and to automatically steer the ship after a heading setpoint, a course-over-ground setpoint or a track setpoint.

The basic components of the INC system contain a GPS receiver for defining the position of the ship, the gyro compass for measurement of the heading and the rate of turn, the autopilot for controlling the movements of the ship using the rudders or the azimuthing propulsion units of the ship. Often the system is equipped also with an acoustic log for measurement of the speed of the ship. The system contains also means for editing the track or the route plan and monitoring the system and the movements of the ship relative to the track.

Behaviour of the officer of the watch in managing a failure in the INC system has been studied by analysing five real accident cases. This paper describes the main results of the analysis. In all analysed cases the accident was caused by delayed operator action after a critical failure in the system. Also in all cases the self diagnostics and alarm functions of the system failed to make the operator fully aware about the dangerous failure. Obviously managing the situation becomes extremely difficult for the operator, if the system fails to give a direct alarm of the failure. The analysis also revealed that the operator does not continuously monitor the performance of the equipment. Actually this finding is not surprising. Naturally, it is much more important for the OOW to monitor the overall situation and the movements of the ship rather than to find out how the navigation and steering equipment is working. And most of the time there is nothing abnormal in the behaviour of the equipment anyway. It would be waste of resources to pay much attention to the technical system in stead of following the traffic situation.

These two levels of monitoring are called ‘the process level’ and ‘the equipment level’. The officer of the watch should concentrate on the process level monitoring. This is actually one of the main reasons for the increased use of automation, i.e. to provide the operator with better possibilities to transfer his/her attention from the equipment level to the process level. Consequently, the automatic systems must be designed and built assuming that the operator does not pay attention to the operation of the equipment. And, on the other hand, the operator must be able to assume that there will be a clear indication about any dangerous abnormality in the operation of the equipment. In other words, the system should be able to detect and give a clear alarm about all dangerous failures in the system.

Unfortunately this is not the case in the real life. The self diagnostics of the navigation and steering system did notice or was not able to inform the user about the dangerous situation. The user of the automatic system is seen as the last back-up of the automatic system in failure situations. The designer of the system assumes that the operator can manage the situation if the automation fails. This is a clear conflict of targets: By introducing more automation, the operator’s attention is transferred from the equipment level to the higher process level. But, on the other hand, in order to be able to act as the back-up in failure situations, the operator should quickly notice any abnormalities in the operation of the equipment.

The analysed cases clearly show that the operator of an automatic system is not good in detecting equipment failures. The reaction time can be too long for successful handling of the situation, especially in confined waters. This is a consequence of the transfer of the operator’s attention to the process level. Only after an abnormality is noticed on the process level the OOW pays attention to the equipment level. This must not be considered as a user error or an indication of

fatigue, but an essential feature of the behaviour of the operator of an automatic system. In all the five analysed accident cases the process level monitoring failed to give the OOW a reason to check the performance of the equipment until it was too late to avoid the grounding. This problem of delayed operator action is particularly dangerous in confined waters. It can not be solved by providing more visual information about the performance of the equipment, since the operator does not pay attention to such information. It can neither be solved by increasing the training of the users since the delayed operator action is not caused by lack of skills, knowledge or motivation.

1 Analysis of the five accident cases

Navigating a ship is a safety critical function and the automatic technical system taking care of this task should be extremely safe and reliable. The INC system of a ship is backed-up by several manual control modes and extra navigation and steering equipment. But still accidents take place due to failures in the technical system. The back-up mechanisms do not always work properly. Is there a common reason why a single failure in the integrated navigation and control system leads to an accident? Is there a weak point in the system? An answer to these questions was searched by analysing the following five real accident cases:

- The grounding of m/s Royal Majesty close to the east coast of the USA in June 1995[1]
- The grounding of the passenger ferry m/s Silja Europa in the Swedish archipelago close to Stockholm in January 1995[2]
- The grounding of the tanker ship m/t Natura in front of Sköldvik, Finland in October 1998[3]
- The grounding of the ro-ro passenger ferry m/t Finnfellow in Åland, Finland in April 2000[4]
- The grounding of the passenger ferry m/s Isabella in Åland, Finland in December 2001[5]

The chain of events of each of these cases contains a failure, a disturbance, a malfunction or wrong use of the INC system, or a combination of these. The cases were analysed by looking at the failed protections and by investigating the timeline of the chain of events. The aim was to find out if the five cases have common factors explaining why the fault situation developed into an accident. Localising such factors could help in development of the safety of INC systems.

The protection methods were studied by asking the following two questions: “Which methods were used to prevent the development of the fault situation into an accident?” and “Why these protection methods failed?” The first question identifies the protection methods and the second one identifies the causes of breaking of the protections.

The analysis was simplified by dividing the protection methods into four categories:

- automatic recovery mechanisms
- operator action based on alarms from the equipment level self diagnostics
- operator action based on alarms from the system level self diagnostics
- operator action based on his/her own observations about the performance of the equipment

The timeline analysis of the chain of events focused in studying the failure tolerance time, the detection delay and the reaction delay. The timeline of a fault situation is shown in Fig. 1. The picture is based on the 'Fault timeline' by Powel-Douglass[6].

The most interesting moments in the timeline analysis are the time of the failure, the time of detection of the abnormality, the time of starting the corrective action, the last possible moment to take the corrective action to avoid the accident (i.e. the point-of-no-return) and the time of the accident. The time of the dangerous failure is T_0. After this moment the ship is in the dangerous state. An accident takes place if no effective corrective action is taken before the point-of-no-return. The time when the user detects the abnormality is T_h. After this moment the user has to decide what to do in the situation and to take the corrective measure. The time of starting the corrective action is T_k. There is a maximum time for starting the corrective action after the failure. This time margin varies case-by-case. This is called the *failure tolerance time* and it ends at the moment T_1, which is the *point-of-no-return* of the particular fault situation. After this moment the user does not have enough time for any corrective action to prevent the accident.

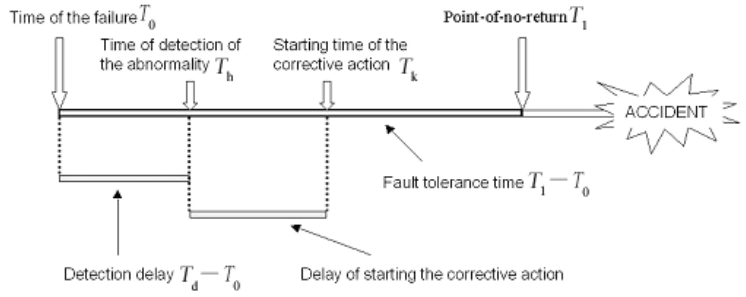

Fig. 1 The timeline of a fault situation

2 The main findings of the analysis

As the result of the analysis, some interesting factors common to the accident cases were found:

Firstly, the standard protection mathod against failures in the automatic system is based on manually activated back-up functions and devices. It is up to the user to activate the necessary back-up function or device after a dangerous failure. In other words, everything depends on the user after a dangerous failure.

Secondly, the self diagnostics of the automatic system seems to have serious shortcomings. Disability of the system to provide the user with appropriate information about the failure and its severe consequences was common to all analysed cases. Consequently the user lost the situation awareness and did not realise the necessity of a particular corrective action to avoid the accident until it was too late.

The third feature common to the analysed accident cases is the inactivity of the user to monitor the equipment. In all cases the user had several indications about the abnormal behaviour of the system on the bridge. However, the user of the INC system did not notice these indications because he/she did not actively check the operation of the equipment. Not even the most critical ones, such as the rudders and the main propellers.

Fourthly, as a result of the factors mentioned above, the activation of the manual back-up device or function failed. In all five cases the user had a possibility to take a corrective action and to avoid the accident. But this action was either delayed or did not happen at all.

These factors together form a dangerous combination. It seems that groundings and incidents due to a technical failure in the automatic navigation and control system are typically developed according to the chain of events shown in Fig. 2.

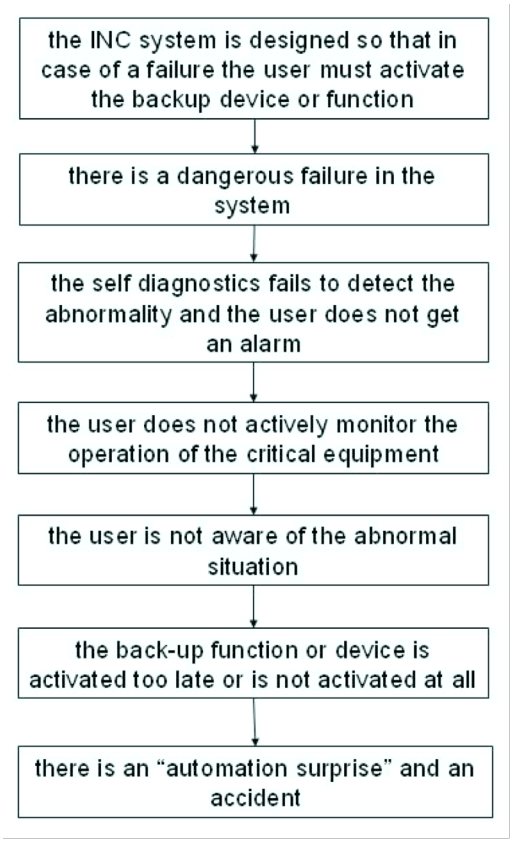

Fig. 2 The chain of events of a typical accident due to a fault of the INC system

3 The monitoring strategy of the OOW and its consequences

It might seem strange that the user of the INC system does not pay too much attention to the operation of the equipment. In the accident investigation reports this behaviour is often interpreted as an operator error. Is it a sign of fatigue or over-reliance on the technical system or is there something wrong with the design of displays or with the placing of critical indicators? Is there lack of information on the bridge about the performance and condition of the equipment or is this a result of insufficient training of the deck officers to use the INC system in the right way?

The monitoring strategy of the operator of an INC system is, however, very logical. There are two entities to be monitored: the process and the technical system controlling the process. The process in this case means the movements of the ship relative to the planned route and possible obstacles, the weather conditions, the traffic situation and also the communication with the outside world. The technical system consists of the navigation sensors, the communication links between the

units of the system, the power supplies, the processing units, the automatic pilot, the propulsion units and the steering equipment. It is quite natural and also correct that the monitoring of the process is on the highest priority. An experienced deck officer does not pay too much attention to the instruments, but focuses his/her attention to the traffic situation and to the movements of the ship. After using the automatic system for a longer time the operator has learned that the system operates properly as far as there are no alarms about failures in the system and no indications about abnormalities of the behaviour of the ship on the process level. The equipment level gains attention only if there is an indication about an abnormality on the process level or if there is an alarm. This kind of operator behaviour was quite clearly seen in all analysed cases.

What are the consequences of this kind of operator behaviour? Clearly it has implications on the safety of the INC system in fault situations. The strongest concerns are related with maintaining the situation awareness in abnormal events. If the operator des not actively follow the indications about the behaviour of the equipment, the self diagnostics and the ability of the system to detect and indicate faults and other abnormalities becomes extremely critical. This was confirmed by the analysed cases. If the system can not make the operator aware of the dangerous failure by giving a clear alarm, an accident can be close. A failure without an alarm leads always to delayed operator action. The operator does not initiate a corrective action before some abnormality has been registered on the process level. In the Royal Majesty case the officer of the watch did not notice anything abnormal on the process level and the corrective action was delayed for over 30 hours! In confined waters even some tens of seconds might be too long delay to avoid grounding.

Unfortunately many INC systems seem to contain such failure modes which are not covered by the self diagnostics. The manufacturers of INC systems and navigation equipment have a temptation to put too little effort in development of comprehensive self diagnostics to a new product. The reason is apparent: the customers normally do not pay much attention to such additional features as self diagnostics and alarms. Factors like performance, user friendliness, ergonomics, outlook, compatibility, brand, price etc. are much more important when a comparison between different alternatives and a purchase decision is being made. Good self diagnostics is one of the last things to be developed to a new product. The weaknesses of the self diagnostics may become apparent to the user-and sometimes also to the manufacturer-years after the purchase. Nancy Leveson states: “the carefulness in designing and testing is too often directed to the normal operation of the system, while the unexpected and erroneous states get much less attention”[8].

4 Some proposals

Firstly one has to remember, that it is not necessarily an operator error if the operator does not behave as the designer has planned or assumed. The mismatch of the design of the system and the behaviour of the user could also be seen as a design error. Design errors tend to appear as operator errors during the use of the system. James Reason has addressed this problem by saying: “*the active errors of stressed controllers are, in large part, the delayed effects of system design failures*”[9]. The poor monitoring of the operation of the equipment is not a result of missing knowledge or skills or correct attitudes. It can be seen as a natural and even intentional result of the use of automation. An essential goal of the introduction of navigation automation has been to allow the OOW to transfer his/her attention from the equipment to the traffic situation. So the

correct method to solve this problem is not training of the users. Training of the designers might perhaps offer better results.

It is quite obvious that the INC system should not be designed assuming that the user is aware of the operation of different pieces of the equipment. The performance of individual devices is checked only after an alarm or if an abnormal event on the process level gives the operator a reason to do so. This must be the basic assumption in the design of the safety of INC systems in fault situations.

What should be done? Either the self diagnostics of the INC system has to be designed and tested to cover all possible failure modes of all individual devices as well of the whole system in order to make the user aware of all abnormalities in the operation of the equipment. Unfortunately this is hardly possible in the reality. The other alternative is to set the requirements for fault-tolerance of the INC systems higher, i.e. the redundancy has to be based on automatic activation of back-up functions or components after any single failure. These solutions are common in dynamic positioning systems of offshore vessels and in the automatic flight control systems of modern passenger aircrafts[10].

5 Conclusion

Behaviour of the officer of the watch in fault situations of the INC system has been studied by analysing five real accident cases. In the analysed cases the operator action after a critical failure in the system was too much delayed to avoid grounding. The situation seems to be extremely difficult for the operator, if the system fails to give a clear alarm of the failure. The user of the INC system does not continuously monitor the performance of the equipment. In stead of checking the indicators of individual devices the OOW concentrates on monitoring the overall traffic situation and the movements of the ship. These two levels of monitoring are called ‘the process level’ and ‘the equipment level’. Only if there is an alarm or if an abnormality is noticed on the process level the OOW pays attention to the equipment level. This should not be interpreted as a user error or an indication of fatigue, but a part of very logical behaviour of the OOW. In all analysed accident cases the process level monitoring did not give the OOW a reason to check the equipment until it was too late to avoid the grounding. This delayed operator action is extremely dangerous in confined waters due to short time margins, but the case of M/S Royal Majesty shows that sometimes the corrective action of the user may lead to a grounding tens of hours after the failure.

The problem can not be solved by providing more visual information about the performance of the equipment on the bridge. It can neither be solved by increasing the training of the users because the delayed operator action is not caused by lack of skills, knowledge or motivation. Some potential ways to solve the problem were mentioned in the end of the paper, perhaps the most promising one being the introduction of full automatic redundancy to INC systems.

Reference

[1] National Transportation Safety Board, NTSB. Grounding of the Panamanian Passenger Ship. Royal Majesty on Rose and Crown Shoal Near Nantucket, MA, June 10,1995 (Marine Accident Report NTSB/MAR-97/01).

Washington DC: NTSB, 1997.

[2] Onnettomuustutkintakeskus' OTK (1994): m/s SALLY ALBATROSS in pohjakosketus Porkkalan Edustalla 4.3.1994. Report No 1/1994. Onnettomuustutkintakeskus, Helsinki (in Finnish).

[3] Onnettomuustutkintakeskus' OTK (1995): The Grounding of the M/S SILJA EUROPA at Furusund in the Stockholm Archipelago on 13 January 1995. Report No 1/1995. Onnettomuustutkintakeskus, Helsinki.

[4] Onnettomuustutkintakeskus' OTK (1998): m/t NATURAN Karilleajo Emäsalon Edustalla 13.10.1998. Report C 8/1998. Onnettomuustutkintakeskus, Helsinki. (in Finnish).

[5] Onnettomuustutkintakeskus' OTK (2000): m/s FINNFELLOW, Karilleajo Överön Luona Ahvenanmaalla 02.04.2000. Report B 2/2000 M. Onnettomuustutkintakeskus, Helsinki (in Finnish).

[6] Onnettomuustutkintakeskus' OTK (2001): Matkustaja-autolautta ISABELLA, Pohjakosketus Staholmin Luona Ahvenanmaalla 20.12.2001. Report B 1/2001. Onnettomuustutkintakeskus, Helsinki (in Finnish).

[7] Bruce P D. Designing Safety-critical Embedded Systems. Embedded Systems Programming Europe. November 1999: 34-47.

[8] Leveson N. Safeware. Addison-Wesley Pub Co USA, 1995: 400.

[9] Reason J T. Human Error. Cambridge, UK: Cambridge University Press, 1990: 183.

[10] Ahvenjärvi S. Safety of an Integrated Bridge System in Fault Situations. Proc of the 2nd International Congress on Maritime Technological Innovations and Research, eds. F.Piniella A, Bocanegra J, Olivella R, Rodriquez Martos. Cadiz, Spain, 2000: 803-813.