TRANSNAV International Journal on Marine Navigation and Safety of Sea Transportation
Volume 3 Number 3 September 2009

The Problem of "Infant Mortality" Failures of Integrated Navigation Systems

S. Ahvenjarvi
Satakunta University of Applied Sciences, Rauma, Finland

ABSTRACT: This paper deals with the problem of high failure rate often experienced on ships that are equipped with a new integrated navigation system. These "infant mortality" failures of the navigation system can form a significant risk to the safety of the ship, as the history has shown. Some accidents caused by this type of failures are briefly discussed. The paper highlights some factors that promote this problem. One of the most important factors is the low degree of standardisation of the bridge systems. Another factor is the incompleteness of the self diagnostics of a new system. The role of the self diagnostics is crucial in coping with failures, because the redundancy of the navigation systems is typically based on manual activation of the back-up device or function. The necessary corrective action by the user can be delayed too much if the self diagnostics of the system is not able to detect the failure. Proper testing of the new system during the harbour trials and the sea trials as well as utilisation of efficient failure analyses techniques is important for reducing the safety risk caused by the infant mortality failures. In the end of the paper, some practical experiences of using FMECA and HAZOP analysis in the development of the integrated navigation system of a large cruise vessel are presented.

1 INTRODUCTION

The bathtub curve is a widely used figure to describe the failure rate of a product during its lifetime. The curve consists of three phases: the "infant mortality" period, the "normal operating" period and the "wear out" period, see Figure 1. This kind of failure curve is typical for complicated technical systems, such as cars, consumer electronics and computer hardware, for instance. The high failure rate in the beginning of the lifetime of a complicated automation system is mainly explained by the existence of latent software errors. The frequency of software-based failures is high in the beginning, but it decreases throughout the lifetime of the software product, as illustrated by the yellow line Figure 1. The explanation is that a piece of software does not wear out or fail, but all failures or malfunctions are caused by latent software errors, or bugs. There are more bugs in a new software product, but as the product gets older, the latent errors are gradually being found and corrected. Provided that the software updates are made correctly, i.e. new errors are not created when software bugs are being eliminated, the failure rate steadily decreases.

It can be assumed that the failure rate curve of an Integrated Navigation System (INS) of a ship has also the shape of a bathtub during its lifetime. There is some evidence about higher failure rates of new INSs, although extensive statistical data seems not be available about this matter. After 1994 on Finnish waters, there have been several groundings caused by a failure or a malfunction of the navigation and steering system of the ship [1]. Almost all the systems involved were new and the failures fell in the category of infant mortality failures.

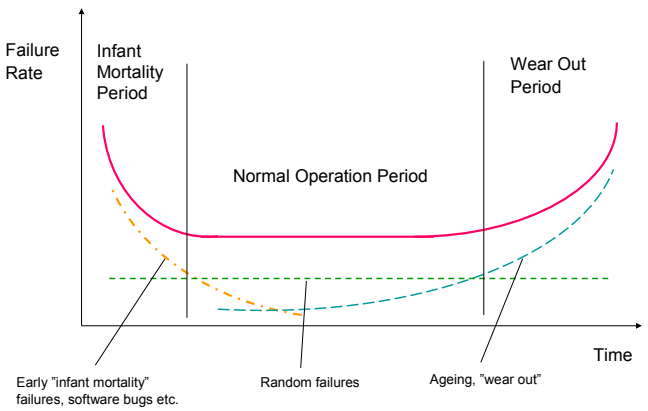

Figure 1. The bathtub curve

There are factors that seem to promote the infant mortality problem of INSs of ships. The first one is

the lack of standardisation. The INSs of ships are typically tailor-made. The risk for unknown failure modes and unknown software errors in such systems is higher than in standardised, mature systems. Gradually, as the unknown failure modes are found and eliminated, the failure rate decreases. When the ship and its navigation equipment have passed the infant mortality period, the probability of an accident due to unknown dangerous faults decreases.

2 SOME ACCIDENT CASES

A fault of a critical component of the navigation system of the ship was the initial cause of the following five real accident cases: Grounding of the passenger ferry M/S Silja Europa in the Swedish archipelago close to Stockholm in January 1995, grounding of the tanker ship M/T Natura in front of Sköldvik in October 1998, grounding of the ro-ro passenger ferry M/S Finnfellow in Åland in April 2000 and the grounding of the passenger ferry M/S Isabella in Åland in December 2001 and the grounding of M/S Royal Majesty close to the east coast of the USA in June 1995 (OTK, 1995; NTSB, 1997; OTK, 1998, 2000 and 2001).

A remarkable feature about these five cases is that the failed equipment was rather new. M/S Silja Europa was constructed less than two years before the accident. M/S Royal Majesty was constructed three years prior to the accident. M/T Natura was constructed five years prior to the accident. The compass system of M/S Finnfellow was upgraded only 13 months before the accident. The INS of M/S Isabella had been renewed around six years prior to the accident. So the average age of the failed equipment was around 3,5 years, which is not much when it is compared with the typical lifetime of a ship, 25 to 30 years. So the critical faults of the five accident cases were not caused by ageing or "wear out", but by the "infant mortality" of the equipment. This applies even to the Royal Majesty case: Although the original fault, i.e. separation of the signal cable from the GPS antenna, can be considered a random failure, the other factors fall into the "infant mortality" class.

3 FACTORS THAT PROMOTE THE PROBLEM OF "INFANT MORTALITY" FAILURES

A critical fault in the INS of a ship represents a high safety risk especially in restricted waters and in areas with high traffic density. The south-west coast of Finland, for instance, is surrounded by a wide archipelago area. Navigation on these waters is very demanding. In Figure 2, there is a sample from the sea chart of the archipelago area close to the city of Turku. The fairways are winding with the minimum fairway breadth only ca. 150 metres.

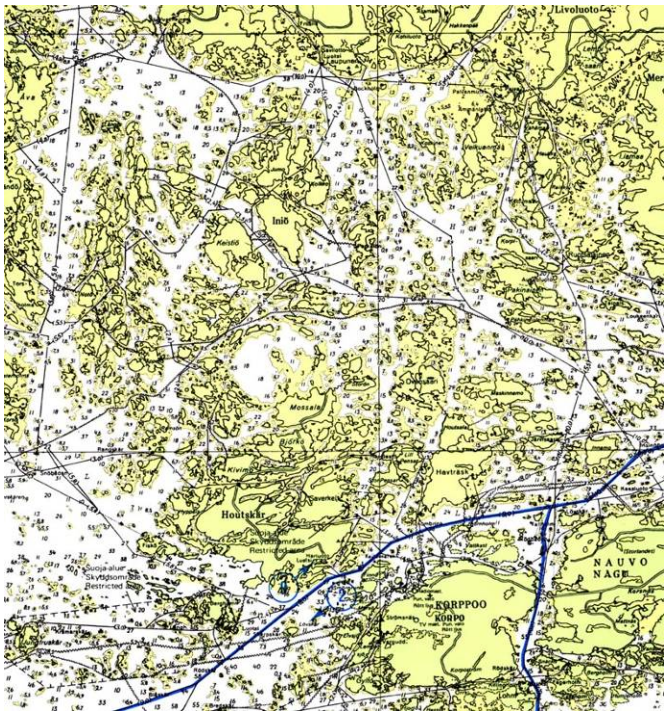

Figure 2. A sample of the archipelago of the south-west coast of Finland

In this area, the available time margin to avoid a grounding after a critical failure can be only a few seconds. For instance, the grounding of the ro-ro passenger ship M/S Finnfellow in April 2000 took place only 85 seconds after a fatal gyro compass failure. Even though the deck officers noticed the abnormal turning of the ship 30 seconds after the failure, it was too late to avoid the grounding (OTK, 2000). Figure 3 shows the position of the ship only 90 seconds after the failure!

Figure 3. Position of M/S Finnfellow 90 seconds after the critical compass failure (OTK, 2000)

The risk of an accident caused by unknown failure modes is high when recovery of the failure is dependent on proper corrective action of the user. This is still the case in most of the new INS installations. The user has to activate the back-up device or

function if the active unit fails. In order to be able to do so, the user has to be aware of the operational status and condition of the system and its critical components. The self diagnostics of the system is crucial for the user to maintain the situation awareness and to be able to react quickly and correctly to failures. It can be seen quite easily from the past accidents, that the user of the INS can have serious difficulties in registering a failure in the system, if the system does not give any alarm about the situation. The failure detection delay can in some cases be extremely long, as was in the M/S Royal Majesty case.

The user's dependency on the self diagnostics makes unknown "infant mortality" failure modes especially dangerous, because they have not been anticipated by the software engineer who designed the self diagnostics of the system. In other words, an unknown "infant mortality" failure will probably not cause an immediate alarm. It is interesting that actually the designers of the system make a double error when they do not recognise a dangerous failure mode: no measures will be taken to eliminate the failure mode in concern AND it will not be ensured that the self diagnostics of the system is able to detect the failure.

Poor or incomplete self diagnostics is a typical problem of new technical systems. Development of proper self diagnostics is expensive and it may be 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 to the manufacturer years after the commissioning of the system. Nancy Leveson states that ”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” (Leveson 1995, p. 400). The development of this important area of system safety need new regulations about self diagnostics, for instance demonstration of the completeness of the self diagnostics as a part of the type approval procedures.

The disability of the system to detect failures and malfunctions, i.e. the deficient self diagnostics, is a serious weakness of new INSs. Increasing complexity of the systems and the relatively short lifetime of product generations seem to promote this weakness. Another factor is the lack of standardisation. In order to make the detection of abnormalities quick and reliable, there has to be much knowledge about the structure and operation of the individual parts and devices of the system, and a lot of practical knowledge about the use and the operation of the system. Fulfilment of these requirements is difficult without better standardisation of INS systems. It is a well known fact that the INSs are too often tailor-made entities. Even sister-ships are too often equipped with different INS setups. However, in order to reduce the safety risk caused by "infant mortality" failures, that kind of tailoring should be stopped. From this point of view, it would be ideal if there were only very few alternative system setups available on the market. Moreover, the INS manufacturers should make the lifetime of a product generation as long as possible. Unfortunately, due to the competition (obviously), the manufacturers tend to introduce new product generations more and more frequently. That is a wrong strategy for reducing the safety risk caused by "infant mortality" failures.

4 WHAT CAN WE DO ABOUT IT?

Alternative methods to reduce the safety risk caused by "infant mortality" failures of INSs would be

1 to increase the lifetime of INS product generations
2 to improve standardisation of INSs
3 to require better testing of new products from INS manufacturers, including the demonstration of completeness of the self diagnostics
4 to make the INSs more fault tolerant
5 to apply different failure analysis methods to new systems prior commissioning

The first method is difficult to accomplish. The competition on the market seems to force the manufacturers to introduce new innovative system generations every other year. As customers, are we happy about this situation? Would we prefer a fully tested, reliable INS in stead of a brand new system with all latest features - and with all those "infant mortality" problems? The customers must realise the importance of this matter and ask for reliability rather than for new architecture or new functions. Would it be a good idea to establish a www-based failure register for the INS products on the market. The database could be maintained by all users of the INSs. It could give the customers some idea about the reliability of different products on the market and hence make the reliability more important also for the manufacturers.

The second and the third method would require new regulations from the international shipping community. The new concept of e-navigation should be used for this purpose. Thorough failure mode testing and demonstration of the completeness of the self diagnostics should be included in the type approval test requirements. Introduction of new system generations would become more difficult, which would also support the increase of product lifetimes.

The fourth method would consist of automatic recovery functions in fault situations. This is the most powerful method to reduce the risk of accidents due to a single failure in the system - no matter if it was an "infant mortality" failure or something else. Au-

tomatic redundancy has been successfully applied in many areas of safety critical automation, such as dynamic positioning of offshore vessels and automatic flight management of modern passenger aircrafts.

The fifth method is already in use. The difficulty in making proper failure analysis for a new INS is that the manufacturer has got the best and the most important information about the system. It is well known that the all failure analysis methods, such as the Failure Mode, Effect and Criticality Analysis (FMECA), is very much dependent on the quality of the data about the technical structure and the software of the analysed system. In practise, the manufacturer is the only party that possesses this information and thus can make a good and comprehensive failure analysis for the product. The author of this paper has coordinated recently two failure analysis projects for large INS systems of passenger cruise ships (see Ahvenjärvi, 2005). These projects confirmed that the manufacturer of the system, indeed, plays the key role in analysis of a new product. It turned out that an FMECA made by the manufacturer(s) and commented by the shipyard / the owner of the ship, combined with a Hazard and Operability Analysis (HAZOP) can give useful results for reducing the risk of an accident due to unknown failure modes. The problem of these methods is that you can never know, if all failure modes - or even most of them - have been detected in the analysis. Actually it is unrealistic to assume that all possible failure modes have been found by using these techniques. Suokas et al. (1988) studied the validity of different methods of identifying accident contributors in process industry systems. The study showed relatively low validity figures for the FMEA, only 17 % of contributors of hazards could be identified by applying FMEA. Other methods were not better than FMEA. Thus it can be assumed that even the combined use of FMECA and HAZOP would cover less than half of all potential failure modes, i.e. the other half of the "infant mortality" failures would remain unpredicted.

5 CONCLUSIONS

A brand new INS with updated architecture and a new software with the latest innovations is not necessarily the best choice for a ship, especially if it will be sailing in areas with narrow fairways or dense traffic. A new system suffers from the "infant mortality" failure phenomenon discussed in this paper. The problem is a combination of three factors: increased failure rate (due to hardware failures and software errors) in the beginning of the operational time of the system, unknown failure modes and incompleteness of the self diagnostics of the system. As the result, the user may lose the control of the situation, if a failure hits the system and it is not capable of giving an alarm about it. The risk of an accident is high if the time margin to make a corrective action is short. Several accidents have taken place due to this kind of "infant mortality" failure.

Obviously the most powerful methods to reduce the risk of this kind of accidents is to make the lifetime of product generations longer and by placing more strict requirements for testing of new systems before they can be taken into use. Standardisation would also be a useful way to limit the number of different types of INSs and hence to reduce the risk of unknown failure modes. These methods, however, require international cooperation and new regulations. Perhaps a web-based failure database could also be useful to encourage the system manufacturers to put a higher priority on reliability and safety than on introduction of new features and new design as frequently as possible. Risk evaluation techniques, such as FMECA and HAZOP can also be used to analyse potential failures of a new INS, but it should be realised that even a good analysis will cover only a fraction of all possible unknown failure modes.

REFERENCES

Ahvenjärvi, S. (2005). Failure Analysis of The Navigation and Steering System of Freedom of the Seas, paper at the 125th Anniversary Conference of Maritime Training in Rauma, October 6-7, 2005

Leveson, N. (1995). Safeware, Addison-Wesley Pub Co. USA

National Transportation Safety Board, NTSB (1997). *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

Onnettomuustutkintakeskus, 'OTK' (1995): The Grounding of the M/S SILJA EUROPA at Furusund in the Stockholm Archipelago on 13 January 1995. Report N:o 1/1995. Onnettomuustutkintakeskus, Helsinki.

Onnettomuustutkintakeskus, 'OTK' (1998): M/T NATURAN karilleajo Emäsalon edustalla 13.10.1998. Report C 8/1998. Onnettomuustutkintakeskus, Helsinki. (in Finnish)

Onnettomuustutkintakeskus, 'OTK' (2000): M/S FINNFELLOW, Grounding near Överö in Aland, April 2, 2000. Report B 2/2000 M. Onnettomuustutkintakeskus, Helsinki

Onnettomuustutkintakeskus, 'OTK' (2001): Matkustajaautolautta ISABELLA, pohjakosketus Staholmin luona Ahvenanmaalla 20.12.2001. Report B 1/2001. Onnettomuustutkintakeskus, Helsinki. (in Finnish)

Palady, P. (1995). Failure Modes and Effects Analysis, PT Publications Inc, West Palm Beach, USA

Suokas, J. & Pyy, P. (1988). Evaluation of the validity of four hazard identification methods with event descriptions. Valtion Teknillinen Tutkimuskeskus (VTT). Espoo, Finland..