Failure mode and effect analysis of automation systems of ships

S. Ahvenjärvi
Department of Maritime Management, Satakunta Polytechnic, Finland

Abstract

A Failure Mode and Effect Analysis (FMEA) is a reliability evaluation technique that can be used in analysing risks involving the failure modes of the technical systems onboard a ship. The objective of this study is to examine the application of FMEA to automation systems of existing ships. Could FMEA be effective in improving the safety of an automation system, such as the integrated bridge system (IBS) of an existing ship?

Experiences gained from recent FMEA projects in Finland have been examined by interviewing key persons of the projects. According to the study, FMEA of a system on an existing ship should be organised so that the knowledge and experience of the users and maintenance personnel of the system can be utilised as much as possible. The active participation of the personnel of the ship is important also because of the learning process that takes place during FMEA. Identifying the possible failure modes and the consequences of them is very demanding, if the system consists of many computer-based units or subsystems connected to each other. An integrated bridge system is a typical example of this. A suitable “top-down” method, such as a failure tree analysis, can be used to complement FMEA in such cases. Attention should be paid also to updating the FMEA after system modifications and software updates. Based on the practical experiences some proposals for a successful FMEA project are summarized in the end of this paper.

1 Introduction

1.1 The FMEA method

The Failure Mode and Effect Analysis (FMEA) is a “bottom-up” type risk analysis technique that can be used to analyse different failure modes and their effects on a technical system. According to [1], the primary objective of FMEA
is to provide a comprehensive, systematic and documented investigation which establishes the important failure conditions of the craft and assures their significance with regard to the safety of the craft, its employees and the environment. FMEA technique was originally developed by US Military before World War II, and it has successfully been applied to car manufacturing, safety critical factory automation and industrial processes. An example of guidelines for carrying out an FMEA is at [2]. For many years FMEA technique has also been applied to dynamic positioning systems of offshore vessels.

The objective of FMEA is to identify the components of a system likely to cause serious failures, so that the potential failures then could be eliminated or risks involved could be reduced by modifying the system. A criticality analysis is often added to the FMEA. The method is then called Failure Mode, Effect and Criticality Analysis (FMECA).

FMEAs are usually categorised into two types, the design FMEA and the process FMEA. The former is used as a part of a product development project. Its objective is to identify design weaknesses and to help in eliminating failure causes before the product has been launched to the market. The objective of a process FMEA is to highlight weak points of a technical system or process and provide information to be used in improving the safety and reliability of the system. Some sources find three different FMEA types: the system FMEA, the construction FMEA and the process FMEA.

FMEAs can also be classified according to its depth. The more general level of FMEA is the functional level and the more detailed one is the component or equipment level. A proper FMEA of a larger system should include a functional level analysis and also the equipment FMEA for such parts and failure modes of the system, that contain higher risks. An example of applying a functional analysis and an equipment FMEA is at [1].

The steps of FMEA are typically:

1) defining the operational status and the environment of the system
2) identifying the system components and functions
3) identifying the failure modes
4) identifying possible causes of each failure mode
5) estimating the probability of the causes or the frequency of the failure
6) defining the effects of the failure modes
7) estimating the severity of the consequences of each failure mode under the defined operational conditions
8) identifying the way of detection of the failure
9) calculating the total risk of the failure mode
10) defining possible preventive actions and necessary system modifications

There are variations in FMEA procedure from case to case. Actually, the procedure described above is FMECA since it contains estimation of criticality i.e. the risk associated with each failure mode (step 8). A more detailed introduction of the FMEA methodology and performing FMEA is in [7].

Many software tools have been developed for an FMEA. Usually the results of the analysis are documented in a table. Summary of the findings, the
Onclusions and proposed corrective measures should be written in textual form. An example of a FMEA worksheet is shown below.

<table>
<thead>
<tr>
<th>System</th>
<th>Unit function</th>
<th>Failure mode</th>
<th>Cause</th>
<th>Probability of failure</th>
<th>Failure effect</th>
<th>Severity</th>
<th>Failure detection</th>
<th>Total risk</th>
<th>Corrective actions</th>
</tr>
</thead>
</table>

![Figure 1: Example of FMEA worksheet](image)

.2 The objective of this study

There is no doubt about the need to improve the operational safety of existing integrated navigation and steering systems [3]. Too many accidents have occurred due to a failure in some part of the integrated bridge system. Perhaps the Royal Majesty case [4] is one of the most well known, but there have been also many others. Is there enough knowledge about the possible failure modes and their effects? Could FMEA be a suitable method for improving the safety of the integrated automation systems of ships? What would be the benefits of the application of FMEA on existing ships and how FMEA should be carried out in order to get the best possible results?

.3 The research method

Practical experiences from FMEA projects on ship systems, carried out in Finland during the 90's, have been studied by interviewing the key persons of the projects. The eight experts represent two shipyards, three shipping companies, one equipment manufacturer, one university and three consult companies. The interviewed persons have gained experience from nine different FMEA projects, three of which have been carried out on existing ships. The practical arrangements in carrying out the FMEA were discussed, as well as the usefulness of the results and the difficulties in carrying out the projects and applying its results. Based on this experience, some key elements of a successful FMEA project are drawn and the role of an FMEA in the safety of an automation system of a ship is discussed.

. Experiences from the FMEA projects

.1 Why to carry out FMEA?
The FMEA is a risk management tool and the basic motive of applying it is to improve the reliability and the safety of the system in concern. The International Maritime Organisation (IMO), the International Electrotechnical Commission (IEC) and some classification societies have been encouraging the application of FMEA. It is required by IMO's High Speed Craft code [1] and it is also included in the latest Integrated Bridge System (IBS) rules of the leading classification societies.

FMEA is obviously a useful tool in the design phase of a new ship, seen from the shipyard's point of view. The analysis can reveal shortcomings or mistakes in the system architecture already before the construction of the ship has been completed. From the shipowner's point of view, a design FMEA can give useful information about alternative technical solutions and their impacts on the reliability of the systems and the total safety of the ship. As mentioned earlier, a design FMEA might be needed also because it is required by IMO, or a classification society for a certain class notation.

The natural reason for providing an existing ship with FMEA is the need to increase reliability of the safety critical systems and to know more about the possible failure modes and the risks involved with them.

2.2 Comparison of FMEA on a newbuilding and on an existing ship

When a system of an existing ship is being analysed the practical arrangement of FMEA differs slightly from FMEA of a newbuilding. FMEA of a newbuilding could be bought from an outside FMEA consultant, who carries out the analysis practically alone with some help from the designers. The main source of information is the design documentation of the system and its components. Information about potential failure modes and their causes can be based on the experience of the consultant himself, or it has to be collected from appropriate reliability data bases.

In case of an existing system, the experience of the users and the maintenance staff is an important source of information. For this reason - and also because of the learning objective - it is crucial that the key users participate actively in the FMEA throughout the process. For example in one of the studied cases, the FMEA working group consisted of six persons: two persons from the ship, two persons from the technical department of the shipping company and two additional specialists outside the shipping company. The working group had meetings once in two weeks. An outside expert is obviously needed to keep the FMEA process alive, to help in preparing the documents and to keep it going into the right direction.

The amount of time and other resources needed to carry out a reasonable FMEA shall not be underestimated. The total costs depend much on the extent and depth of the analysis. The appropriate depth of the analysis is, indeed, an interesting and a difficult question. As suggested in [1], the analysis can be started on the functional level and brought to the equipment level on the most critical areas. In theory, there is no limit in the depth and the accuracy of FMEA. Perhaps FMEA should be considered an endless process and be made a part of the quality management system of the ship. This idea of a continuous FMEA process could be tested in the future.
3 On the results of FMEA

The immediate output of an FMEA procedure is a description of potential failure modes, the effects of the failures and the risks involved with the analysed failure modes. Proposals for corrective actions with an estimate of their effect on the calculated risk level can be included in the analysis. The main findings of the FMEA should be expressed in textual form, in order to make the results as usable as possible within the organisation.

A significant factor in FMEA is the availability of the data on the failure modes and the failure rates. It can be difficult to get this information from the manufacturers, and examining failure rates by running extensive and expensive practical experiments is impossible for obvious reasons. Therefore the experience and the opinions of the persons who participate in the process is crucial. It should be understood, that even though FMEA produces an estimate of the risk involved with different failure modes, the intention is not to provide exact and absolutely correct figures about the risk levels. This is obvious, as there is simply not enough reliable data available about the failure modes. What is more important, FMEA can help to predict and to take precautions against dangerous failure modes and to locate weak points in the system. FMEA can also direct the development of the system to right areas. For example, FMEA could reveal lack of redundancy, i.e. a weak point of the system where a single failure mode could cause a loss of a critical function leading to catastrophic consequences.

In case of an existing ship, it may be very difficult to make a large modification to a system onboard. FMEA has not led to many major system modifications, although smaller adjustments have been done and clear mistakes been corrected in the studied cases. The result of FMEA has been more often an improvement in preventive service or a maintenance procedure, or a change in monitoring a critical part of the system.

It seems, anyhow, that the most valuable feature of FMEA is the learning that takes place during the process. A very good result of FMEA is an increase in the knowledge about the system and the interdependencies between its components. A positive result of FMEA is also learning of the language and the terminology of risk management. Also the process helps to correct wrong mental patterns about the system and its operation in exceptional situations. Conducting FMEA is a learning process, which can be even more valuable than the cold figures in the final FMEA report.

4 FMEA of an integrated system

Conducting an FMEA of a mechanical system is a rather straightforward process. That is not the case, when the system consists of many computer-based sub-systems. Identifying the failure modes and their consequences becomes difficult due to the vast amount of different operational states of the system. When the system consists of intelligent units, failure modes can be caused not only by hardware failures, but also by program errors. It is hardly possible to identify all potential software-based failure modes in that case. As mentioned earlier, IMO
suggests in [1] that FMEA of an integrated bridge system should be done in two phases. The first phase is a functional fault analysis, where the following failure modes should be considered:

1) complete loss of function
2) rapid change to maximum or minimum output
3) uncontrolled or varying output
4) premature operation
5) failure to operate at a prescribed time
6) failure to cease operation at a prescribed time

If some of these failure modes in any sub-system would lead to catastrophic consequences, a more detailed equipment level FMEA should be conducted for that sub-system.

Identification of different failure modes and consequences of the failure modes can be quite laborious even for a single sub-system, as can be seen from the following example (a similar case has been actually examined by the author using real equipment): Let us consider the loss of a valid output message from a DGPS receiver to a navigation system. The navigation system has three different operation modes and four alternative parameter settings that define the reaction of the navigation system to the loss of the DGPS message. That gives twelve alternative consequences for a single DGPS failure mode. Let us then assume that the loss of the DGPS output message was caused by an antenna fault, and the DGPS receiver had three alternative ways to react to that particular fault (depending on the value of a specified parameter). The number of cases to be analysed is thirty-six! The situation becomes even worse, when different software versions are considered. The DGPS receiver might react in a different way to the antenna fault after a software update.

One could ask, if application of FMEA would have been enough to eliminate such accidents as described in [4], [5] and [6]. Obviously the answer depends on the quality and depth of the presumed FMEA. In any case, a well organised FMEA would have given the deck officers in each case more knowledge about the bridge system of the ship and its behaviour in an abnormal situation.

5 Conclusions

Experience from FMEA was studied by interviewing key persons of some recent FMEA projects. The objective was to examine the application of FMEA to automation systems of existing ships and to find the answer to the question: could FMEA help in improvement of the safety of an automation system, such as the integrated bridge system (IBS) of an existing ship?

According to the study, the application of FMEA is a useful way to identify and localise weak points of safety critical systems of an existing ship. FMEA shall be arranged so, that the experience of the users and the maintenance personnel can be utilised as much as possible. This can be done by establishing a FMEA working group to carry out the analysis. The most valuable result of FMEA seems to be the increased knowledge about the analysed system in
general, about the safety risks involved with its different failure modes, about the interdependencies between the sub-systems and about the behaviour of the system in abnormal situations. If FMEA is applied to an integrated system consisting of several computer-based units, identification of potential failure modes and possible consequences of the failures can be hard. In that case FMEA could be divided to a functional level analysis and an equipment level FMEA. FMEA could also be considered as a continuous process and be made a part of the quality management system of the ship.

References


