AUR LAB, NTNU TRONDHEIM

Risk assessment for the REMUS100 AUV

Context Document

Christoph Thieme – Initial 06.2014

10.06.2014

This document defines the objectives, external and internal parameters, scope and risk criteria for the Risk Management process employed on the AUV REMUS 100 belonging to the AUR Lab at NTNU Trondheim. The Risk Management process is established following the risk management standard ISO 31000.

Foreword

This document represents the basis for the risk assessment process of the REMUS 100 AUV of the AUR Lab of NTNU AMOS. It describes the scope, limitations and considerations which are relevant for the risk assessment process. It also comprises the risk criteria and acceptance criteria used in the following assessment. The document follows the guidelines of ISO 31000 (2009) standard.

Contents

Abbreviations

AMOS	Centre of excellency for autonomous Marine Operations and Systems
AUR Lab	Applied Underwater Robot Laboratory
AUV	Autonomous Underwater Vehicle
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
HEP	Human Error Probability
HRA	Human Reliability Analysis
NTNU	Norwegian University of Science and Technology
PSF	Performance Shaping Factor
RCM	Risk Reducing Measure
RPN	Risk Priority Number

Terms and definitions

1.1 Risk

The following risk definition shall apply in this document:

> "[Risk is] the combined answer to three questions: (1) What can go wrong? (2) What is the likelihood of that happening? What are the consequences?" (Rausand, 2011)

The Risk picture then represents the risk qualitatively and shows the dimensions and elements of risk (Rausand, 2011). This summarizes hazards, associated consequences and likelihood.

1.2 Hazard

A hazard is a "potential source of harm" (NORSOK Z-013, 2010). The harm may be "loss of life, damage to health, the environment, or assets, or a combination of these" (NORSOK Z-013, 2010). A hazardous event describes the event when a hazard is released (NORSOK Z-013, 2010).

1.3 Failure and fault

A failure is defined as:

> "[The] termination of the ability, of an item, to perform a required function." (NORSOK Z-016, 1998)

A failure is therefore an event. After a failure occurred the item has a fault, which is then the state of the item. A fault is often the result of a failure but may exist without one (NORSOK Z-016, 1998). A fault can be defined as:

> "State of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources." (NORSOK Z-016, 1998)

Faults and failure are important in connection with reliability and risk in AUV operation, since frequent failures imply a low reliability. A low reliability might increase the probability of loss, thus increasing the risk.

1.4 Barriers

Barriers are defined as physical or engineered systems or human actions (based on specific procedures or administrative controls) that are implemented to prevent, control, or impede

energy released from reaching the assets and causing harm (Rausand, 2011). Often the term risk mitigating measures or risk reducing measure (RCM) is used synonymously.

1.5 Risk management

Risk management is the framework, procedures and processes, so the architecture of how to manage risk. Whereas managing risk is the process of applying the framework to particular risks (ISO 31000, 2009).

2 Objectives

Aim of this risk management process is to assess the risk of current operations of the REMUS 100 autonomous underwater vehicle (AUV) of the AUR Lab at NTNU, Trondheim. The risk assessment shall give insight in weaknesses of the current operational procedures. With the identified risk, measures to reduce the risk shall be proposed. This process is the first iteration and shall ensure constant and continuous improvement of mission success rate and reduction in risk.

The assessment described here and the associated documents are the case study for developing a risk management suitable for the AUR Lab's needs, thus the methods used represent only some possible methods, which could be used.

3 Scope

The risk management process will cover the following operational phases:

- Storage and transportation
- Preparation and deployment
- Mission start and mission
- Retrieval and post-dive activities

A description of tasks in the respective phases can be found in the Operation and Maintenance Manual of the REMUS 100. The risk in respect to loss of the vehicle, damage to the vehicle and mission abort will be considered.

This study will focus regionally on Norway, missions where so far conducted in Trondheimsfjord and in the fjords around Spitsbergen. During the missions around Spitsbergen sea ice was present but will not be considered. Since the main focus of usage is in Trondheimsfjord.

The analysis is limited to a functional level and major components. Additionally it is assumed that the personnel are trained in the use of the AUV and that the procedures, given in the REMUS 100 user manual, are followed. This does not exclude that there might be errors or mishaps in handling.

3.1 Internal parameters

With internal parameters the considerations necessary which arise from the AUR Lab itself are meant. In the following parts these factors are discussed, grouped as suggested in ISO 31000 (2009).

3.1.1 Organization, roles and accountabilities

Head of the AUR Lab and therefore responsible for the AUV is Martin Ludvigsen, thus he is also the risk owner. All decisions which are made in respect to risk reduction measures are based on decisions by Martin Ludvigsen and the technicians; Robert Staven and Frode Volden.

3.1.2 Risk policy

NTNU emphasises a proactive approach towards risk and safety management. Therefore this shall be reflected in this risk assessment. Potential risks shall be identified, if possible quantified or estimated. Measures shall be taken to reduce the risk as much as possible without disproportional effort.

The risk assessment shall be kept updated, to ensure that risks didn't change or new risks arose due to new operational practices and environments.

3.1.3 Capabilities and resources

The resources for the risk assessment are limited. It is mainly carried out by Christoph Thieme, M.Sc. student at NTNU. The assessment is supported by Martin Ludvigsen, in respect to organization and operations, Frode Volden and Robert Staven in respect to operation and maintenance and Petter Norgren in respect to operation and software handling.

3.1.4 Technological environment

The Remus 100 vehicle is a highly complex underwater robot. There are two aspects to be covered; mechanical and software related. The Remus 100 is in (small scale) serial production and several AUV are in operation for years, thus the mechanical side of the AUV is assumed to be highly reliable. Manufacturing faults are assumed to be negligible, only erroneous maintenance, wrong preparation and damages are considered.

Regarding the software side of the AUV, these assumptions are not applicable. The AUV is subject to constant changes in the software code, thus the software is quite likely to contain errors and must be considered in several aspects

3.2 External parameters

These are the considerations that have to be taken into account, deriving from outside the AUR Lab.

3.2.1 Natural environment

The environment the AUV is operated in is quite harsh. The AUV is used subsea as well as on the surface. Especially near the surface high energy impacts from wind, currents and waves have to be expected. Subsea interactions with obstacles and the sea bottom have to be considered. Additionally the interactions between the deployment vessel and the AUV have to be considered.

4 Risk criteria

This part summarizes the methods used in the risk assessment process and the criteria that were given as risk acceptance criteria beforehand.

4.1 Risk assessment methods

4.1.1 Risk identification

For identification of risks, hazard checklists are used (e.g. Rausand (2011)) and the literature on risk in AUV operation and handbooks for underwater robots are consulted to identify possible risks.

The findings are summarized in a PHA worksheet, where the hazards, preceding causes, resulting consequences and possible mitigating measures are identified. The worksheet also contains an estimation of the risk. Frequency or likelihood (abbreviated with Freq.) and consequences (Cons.) are sorted in categories. These are described in Table 1 and Table 2, respectively. The risk is then calculated by adding frequency and consequences together, the so called risk priority number (RPN). A high RPN corresponds to a high risk.

Table 1 Frequency and likelihood categories, adopted from (Rausand, 2011)

Category	Rating	Frequency	Description
Fairly normal	5	10 - 1	Event that is expected to occur frequently
Occasional	4	1 - 0,1	Event that happens now and then and will normal be experienced
Possible	3	10^{-1} - 10^{-3}	Rare event, but will possibly experienced
Remote	2	10^{-3} - 10^{-5}	Very rare event that will not necessarily be experienced
Improbable	1	10^{-5} - 0	Extremely rare event

The estimations of frequency and consequences are based on a subjective assessment and do not reflect just measured data. The worst cases are assumed thus the most severe outcome or possible frequency is chosen when there are several categories involved. A detailed analysis of frequencies and possible outcomes is carried out during the risk analysis. The results can be summarized in a so called risk matrix, c.f. Table 3.

Table 2 Consequence categories used in the PHA

Category	Rating	Description
Loss of AUV	3	The AUV is not able to surface, cannot be retrieved or is so severely damaged that further use is impossible
Severe damage to AUV and/ or mission cruise abort	2	The AUV is damaged so severely that a mission/ cruise has to be aborted or is not started or all data collected is lost
Small damage to AUV/ loss of some mission data	1	The AUV is only damaged slightly and can be repaired during the cruise, within a short time, or data is lost only partially

Table 3 Risk Matrix

Probability / Consequence	Improbable	Remote	Possible	Occasional	Fairly normal
Loss of AUV	4	5	6	7	8
Severe damage/ mission abort	3	4	5	6	7
Small damage	2	3	4	5	6

4.1.2 Risk analysis

4.1.2.1 Event modelling

In order to analyse the interaction between the events identified during the PHA leading to the hazardous event, fault tree analysis (FTA) will be used. This is a tool to identify all combinations of basic events that may result in a critical event for the system (Rausand, 2011).This can be done qualitatively and quantitatively.

The analysis is a graphical method based on Boolean logic and event gates. The most important gates are *and - gates,* the event happens if all sub events occur, and *or - gates*, the event happens if one of the sub events occurs. With the graphic representation of the interaction of the basic events it is easily possible to identify short comings in the system (Rausand, 2011). If a quantitative approach is chosen it is possible to calculate the top event probability. Basic events are the lowest events considered in the FTA and represent a certain resolution of analysis (Rausand, 2011).

The top event is described by a combined answer to: What happens in the event? Where does it take place? At which time? (Rausand, 2011). In a FTA only one top event at a time can be analysed. Additionally multiple failures at a time can only be included, if a basic event is created for this purpose. This will not be done in this case since the interactions are quite complex and focus will be on the single events occurring.

For the FTA analysis the tool CARA Fault Tree v.4.02b is used. With the program, fault trees can easily be drawn with standard symbols and their logic already stored in the library. After the fault tree is drawn and all reliability, fault or frequency data is entered, the top event probability can be calculated.

Similarly to FTA the events after the hazardous event has occurred can be analysed and different outcomes assessed. For this analysis event tree analysis (ETA) is used. ETA is a graphical approach which is set up left to right, whereas it starts from the hazardous events and splits at stages, the stages are often described as a barrier failure (Rausand, 2011). It can also be significant events that may arise during an event chain. The event is either true or false and each is associated with a certain probability. In a graphical way a true barrier failure propagates horizontal, where the false event branches downwards. On the right side of the event tree the consequences and the cumulative probability are listed, representing the risk arising from the specific hazardous event. The Event trees are drawn in Microsoft Excel, including the calculations for end event probabilities. The end event probabilities in an ETA are found by multiplying the probabilities along the event path with each other. The sum of all end event probabilities equals the probability of the hazardous event.

In a first step for both analysis types the events identified in the PHA are connected. Secondly the level of complexity is reduced and redundant events eliminated, by grouping of similar events.

For the whole analysis it is considered that only one event path can occur at a time. For example if the vehicle has is damaged, a fault in the navigational system is not considered, although this would possible. This is done for simplification, considering all possible event combinations would lead to a highly complex analysis with low readability. Not considered for the moment is the probability of collision with other vehicles or vessels and the risk of ignition of the vehicle’s battery. These events are considered very unlikely.

4.1.2.2 Models for basic event probability estimation

Evaluation of mission logs

In order to find out what faults occur in the system during a mission, the mission logs of the missions done so far are evaluated. For this purpose the fault logs were exported from the mission logs with the control tool of the REMUS 100; Hydroid REMUS VIP. The missions that will be evaluated are:

- Seven missions conducted between 17.01.2014 and 24.01.2014 in a fjord near Ny-Ålesund Spitsbergen, Norway
- One mission conducted on 10.03.2014 in Trondheimsfjord near Hommelvik, Norway
- Four missions conducted between 08.04.2014 and the 10.08.2014 in Trondheimsfjord near Skogn, Norway

In the evaluation only the faults will be considered, that occurred during the mission, so after deployment and before retrieval. Reoccurring similar faults are grouped to limit the number of different faults to a reasonable level. After evaluation of all fault logs, the faults are assessed for their criticality and relevant faults are identified. This process shall give a hint on probabilities, but since only few missions have been conducted yet, the data is not statistically satisfying, so no probabilistic conclusions should be drawn directly. On the other hand some insight on mission preparation can be found and thus give hints for improved procedures.

Human reliability analysis

HRA is a technique to systematically identify and evaluate errors that are likely to happen when personnel act in a system (Rausand, 2011). Human error is defined as:

"An out-of-tolerance action or deviation from the norm, where the limits of acceptable performance are defined by the system. These situations can arise from problems in sequencing, timing, knowledge, interfaces, procedures, and other sources." (NUREG/CR-6883, 2005)

Correspondingly human error probability (HEP) is defined as:

"A measure of the likelihood that plant personnel will fail to initiate the correct, required, or specified action or response in a given situation or by commission will perform the wrong action. The HEP is the probability of the human failure event." (NUREG/CR-6883, 2005)

In connection with HEP, performance shaping factors (PSF) are often mentioned. A PSF is:

“A factor that influences human performance and HEPs. Performance-influencing factors may be external to humans or may be part of their internal characteristics.”

For the estimation of HEP in this thesis, the SPAR-H (Standardized Plant Analysis Risk Human Reliability Analysis) method, described in (NUREG/CR-6883, 2005), is used. The model is using PSF to account for situational influences on the person which carries out tasks. Two kinds of tasks are differentiated; diagnosis and action. A diagnosis task is based on knowledge and experience to fully understand the situation, plan and determine the course of actions. Action tasks are based mainly on the diagnosis task and involve carrying out work according to procedures or guidelines. A dependency of these two tasks types can be modelled if one task involves both actions. The full process and worksheets can be found in (NUREG/CR-6883, 2005), which is here referred to.

Being developed for event sequences in the nuclear industry it is assumed that the SPAR-H method still applies here for two reasons. An AUV is also a complex system which requires a certain level of skills and wrong decisions can easily lead to an undesired outcome. Secondly can the method model through the use of PSF different environments and complexity. A short summary of bias that can occur is given in the next part on expert estimation.

The evaluation itself for the basic events was conducted by Martin Ludvigsen and Frode Volden, both accustomed with the AUV. Before they filled out the worksheets, one for each basic event identified to be suitable for this method, they were shortly briefed in HRA assessment and the method. Since the author of this thesis also has low experience with this method, it can’t be ensured that all details were presented correctly, despite thorough preparation. The events considered are listed below in tab.2.8. Events marked with ETA are used in ETA and where given an abbreviation for easier handling of the documents.

Expert estimation

In order to analyse the FTA and ETA quantitatively some expert judgement in probabilities is needed. Probability is categorized in descriptive categories, which are associated with a certain probability, c.f. Figure 1 (Witteman & Renooij, 2003).

Except fifty-fifty which is the 50% probability mark, all categories are associated with a range of probabilities. The expert can, as aid for the assessment express his probability assessment in verbal words first and then in a percent value. It shall be noted that this scale is difficult for handling small probabilities, such as 0,1 % and 0,01 %. Thus there is a high

uncertainty connected with this assessment. For this reason the Experts are also asked to indicate their level of certainty, c.f. Table 4.

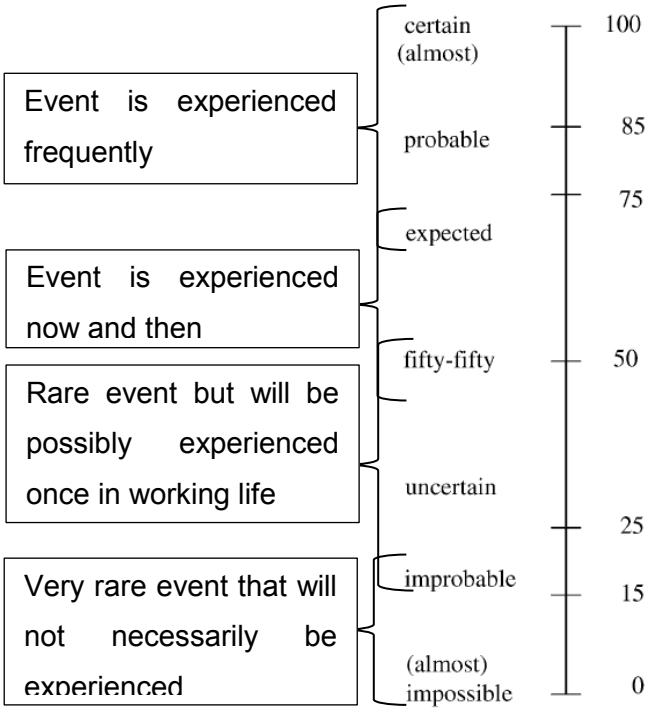

Figure 1 Probabilistic scale used for the assessment (Witteman & Renooij, 2003)

Table 4 Level of certainty for the assessment

Confidence level	Probability range
High	Event probability is within ±1 %
Medium	Event probability is within ±2 %
Low	Event probability is within ±5 %

For more information on bias and the assessment the reader is referred to the corresponding document “expert estimation of probabilities”, which was designed for the experts as working aid.

4.2 Risk acceptance

The risk as stated before should be as low as possible. Since no reference values are available and little experience is obtained yet an absolute value cannot be stated.

References

ISO 31000, 2009. *ISO 31000 Risk Management: Principles and Guidelines,* Geneva: International Organization for Standardization.

NORSOK Z-013, 2010. *Risk and emergency preparedness assesment.* Lysaker: Standards Norway.

NORSOK Z-016, 1998. *REGULARITY MANAGEMENT AND RELIABILITY TECHNOLOGY.* Lysaker: Standards Norway.

Rausand, M., 2011. *Risk Assesment- Theory, Methods and Applications.* Hoboken, New Jersey: John Wiley and Sons, Inc..