NTNU – Trondheim
Norwegian University of
Science and Technology

Development of a Risk Management Process for NTNU's REMUS 100 AUV

Christoph Thieme

Marine Technology
Submission date: June 2014
Supervisor: Ingrid Bouwer Utne, IMT

Norwegian University of Science and Technology
Department of Marine Technology

Preface

This master thesis was written as requirement for graduation as M.Sc. in Marine Technologies at the Norwegian University for Technology and Science Trondheim, Department of Marine Technologies. The underlying project topic for the thesis is "Reliability of autonomous marine operations and systems". This was further specified in consultation with the project supervisor Ingrid Bouwer Utne to “Development of a risk management process for NTNU’s REMUS 100 AUV”. This thesis summarizes the work done during the course of the development. The thesis contains preparation work, which was done in the course of the project thesis. All sources used are indicated in the respective sections, no other sources have been used.

At this point I would like to make some acknowledgments. Firstly I thank Ingrid Bouwer Utne for the consultation and supervision, which gave valuable input to this thesis. Secondly I want to thank Martin Ludvigsen, who contributed strongly and gladly participated in the method’s application. Thirdly I would like to acknowledge the input, provision of information and help from the technicians Frode Volden and Robert Staven. Furthermore Petter Norgren is to be thanked for making the hardware available to accustom myself with the AUV operation software. I also want to acknowledge the assistance by Mauro Candeloro, who gave advice and input although not fully involved in operation. Last but not least I want to thank the crew of RV *Gunnerus*, who were kindly hosting the cruise from 08.04.- 10.04.2014 and thus allowing a deep inside in AUV operation.

Trondheim, 04. June 2014

Christoph A. Thieme

Abstract

Autonomous underwater vehicles (AUV) are highly complex electromechanical systems which act in a hazardous, unstructured environment. The AUR Lab of NTNU operates one REMUS 100 AUV and several other unmanned underwater vehicles in Norway's fjords. In order to minimize the risk, inherent to these operations, a risk management system should be developed.

This thesis summarizes the findings during development. The risk management process and the framework document are based on ISO 31000 (2009). In the course of the development, an exemplary risk assessment was carried out. The aim of the risk assessment was to assess the risk of loss of the AUV and unplanned mission abort. The assessment described is one of the first to use human risk analysis in connection with reliability analysis of AUV. Besides human reliability assessment, fault tree analysis, event tree analysis and expert estimation were the main methods used to assess the risk.

The results of the risk assessment were unsatisfying. The risk found seems to be overestimated, this can be accounted to some of the methods used, the low experience with these methods and the low experience in general with AUV operation. The methods applied seem to be suitable in most cases but some require modifications for future use. Despite the low confidence in the data obtained, the recommendations made, are assumed to be helpful to improve operation. The main recommendations are improved or newly written procedures for maintenance, planning of missions and fault recognition and solving.

The risk management framework still has to be reviewed by the heads of the AUR Lab. Thus it will be subject to changes and improvements. Nonetheless it is assumed that the risk management framework presented here is a good starting point to introduce a successful risk management system in the AUR Lab.

Contents

List of Figures

List of Tables

Abbreviations and symbols

ALARP	As Low As Reasonably Practicable
AMOS	Centre for Autonomous Marine Operations and Systems
AUR Lab	Applied Underwater Robotics Laboratory
AUV	Autonomous Underwater Vehicle
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
HEP	Human Error Probability
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HSE	Health Safety and Environment
LBL	Long Baseline
NFA	Norwegian Society of Automatic Control
NHEP	Nominal Human Error Probability
NTNU	Norwegian University of Science and Technology
PHA	Preliminary Hazard Analysis
PSF	Performance Shaping Factor

RCM	Risk Control Measure
RPN	Risk Priority Number
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
TBS	Trondheim Biological Station
UAV	Unmanned Aerial Vehicles
USBL	Ultra Short Baseline

Symbols

$F(T)$	Probability of failure
$P_{w/d}$	Task failure probability with formal dependency
$P_{w/od}$	Task failure probability without formal dependency
$Q_0(t)$	Top event probability
$\check{Q}_j(t)$	Probability of failure of a minimal cut set
$q_i(t)$	Basic event probability
$R(T)$	Survivor function

1. Introduction

1.1. Background

Autonomous underwater vehicles (AUV[1]) are complex underwater robots, getting increasingly interesting for use in commercial applications. Development of AUV started before the 1960s (Yuh et al., 2011), mainly driven by the technological challenge. Applications were mainly found in the military and scientific environment; conducting surveys and counteracting mines. With the beginning of the 2000s AUV were becoming available also for the offshore business by private manufacturers (Yuh et al., 2011). Today applications are seafloor mapping, capturing of Meso-scale geophysical data, monitoring and capturing of biological and chemical properties and inspection of structures, among others (Yuh et al., 2011). In order to be more cost efficient, operations are becoming more autonomous and more complex, enabling AUV to carry out also long time missions and intervention work (NFA, 2012, AMOS, 2013).

The oceans in which AUV operate are challenging with a corrosive environment, rapidly changing current and weather conditions. A fault or damage during operation, transport, deployment or retrieval, might lead to the loss of the vehicle. To reduce the probability of loss, it is beneficial to know the risk and propose measures to mitigate it.

For the Norwegian University for Technology and Science Trondheim (NTNU) the topic is also of high relevance because of the new established center of excellence for Autonomous Marine Operations and Systems (AMOS). AMOS conducts research to increase autonomy of AUV and improves their functional possibilities. For educational and scientific purposes, but also as contractor to the maritime industry NTNU employs AUV to demonstrate, test and advance technology. The AUV are managed by the Applied Underwater Robotics Laboratory (AUR Lab) at NTNU and are also subject to the challenges mentioned. The health safety and environment (HSE) regulations of NTNU for fieldwork, field-course, research cruise, on-site inspection and excursion (HMSR-07, 2006) requires that during preparation of an excursion, a risk assessment is carried out, to identify all hazards. Eventually measures shall be proposed to mitigate the risk. So far, no system is in place to fulfill this purpose.

[1]The term AUV will be used throughout the document for both singular and plural

1.2. Research question

Aim of the thesis is to develop a risk management system, adapted to the needs of the AUR Lab for the REMUS 100. The system shall provide tools, guidance and reference for future use. Exemplary and as basis for the management system, a risk assessment shall be conducted, covering the risk of loss of the AUV and mission abort.

1.3. Scope and limitations

The development of the management system shall be based on current procedures, standards and regulations. The risk assessment performed in this thesis shall be used as initial point to find suitable methods, which will be recommended for further use in the management system. The procedures should be generally applicable to other underwater vehicles of NTNU. For the analysis operations are considered, that are planned and will be carried out in the first half of 2014. Future missions with different operational conditions, such as under ice missions, cannot be covered. More specific limitations and assumptions are outlined along with the methods.

1.4. Thesis structure

In the following chapter the methods used will be explained. Chapter 3 will give a description of AUV and the system in concern and delve into the limitations outlined above. This will be followed by a short discussion of recent literature on the topic. The successive chapter will then present the results of the risk assessment and the resulting management process, followed by a discussion of these findings. Finally the last chapters will draw a conclusion and issue recommendations in respect to the management process, actual operation and general issues.

2. Methodology

This chapter contains three parts. Firstly the most important terms, which will reoccur throughout the thesis, will be presented. In the second part the methods used for the risk management process and subsequently for the risk assessment are described. Its structure follows the recommended pattern from ISO 31000 (2009). The last part describes how the risk management framework is developed.

2.1. Definitions

2.1.1. Risk

A very broad definition of risk is given by ISO 31000 (2009):

> "Effect of uncertainty on objectives"

Whereas effect is a deviation from the expectations. Another more distinct definition is given in NORSOK Z-013 (2010):

> "Combination of the probability of occurrence of harm and the severity of that harm"

Rausand (2011) defines risk in another way, which is thought to be more suitable here and more comprehensible.

> "[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? (3)"

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

2.1.2. 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).

2.1.3. Reliability

ISO 8402 (ISO 1994) defines the term reliability as:

> "The ability of an item to perform a required function under stated conditions for a stated period of time."

In addition it can be used as:

> "[...] A reliability characteristic denoting a probability of success or a success ratio."

Quantitative measures for reliability are reliability (survivor) functions expressed mathematically as R(T). Important functions in reliability engineering for modeling of failure behavior are among others; the exponential distribution, the Weibull distribution and the normal distribution (Rausand and Høyland, 2004).

The probability of failure F(T) is expressed as F(T) = 1 - R(T) These functions will not be further explained here but more information can be found in the literature, e.g. Rausand and Høyland (2004).

Failure and fault

A failure is defined as:

> "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.

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). Barriers are also known as risk mitigating measures or risk control measures (RCM).

2.1.4. Risk management

Risk management is the framework or architecture, procedures and processes, of how to manage risk. Whereas managing risk is the process of applying the framework to particular risks (ISO 31000, 2009). The risk management process comprises five steps which are interlinked. These steps are "establishing of context", "risk assessment", "risk treatment", "communication and consultation" and "monitoring and review". The latter two link the steps together and assure continuous improvement of risk (ISO 31000, 2009). The process described in ISO 31000 (2009) is depicted in fig. 2.1. Communication and consultation takes a major role, it shall ensure that experts from different fields are consulted to ensure identification of all risks and hazards.

Establishing the context is the process during which scope, purpose and goals are described. Risk assessment consists of three steps: Risk identification, risk analysis and risk evaluation. During risk identification hazards are reviewed and the possible harm is identified. Risk analysis identifies mechanisms, how the hazards might manifest and if the risk is relevant in the established context. Risk evaluation identifies the level of risk and gives input for decision making and risk treatment (ISO 31000, 2009).

During risk treatment measures are identified to reduce the risk of relevant risk contributors. The principle that risk should be reduced, as long as it can be proven that the associated effort is disproportional high, should always be applied (ISO 31000, 2009). Through the constant process of monitoring and review, the risk level should be constantly reduced. By reassessing the risk with the knowledge and experienced gained in the meantime, better and new ways of risk mitigation can be found.

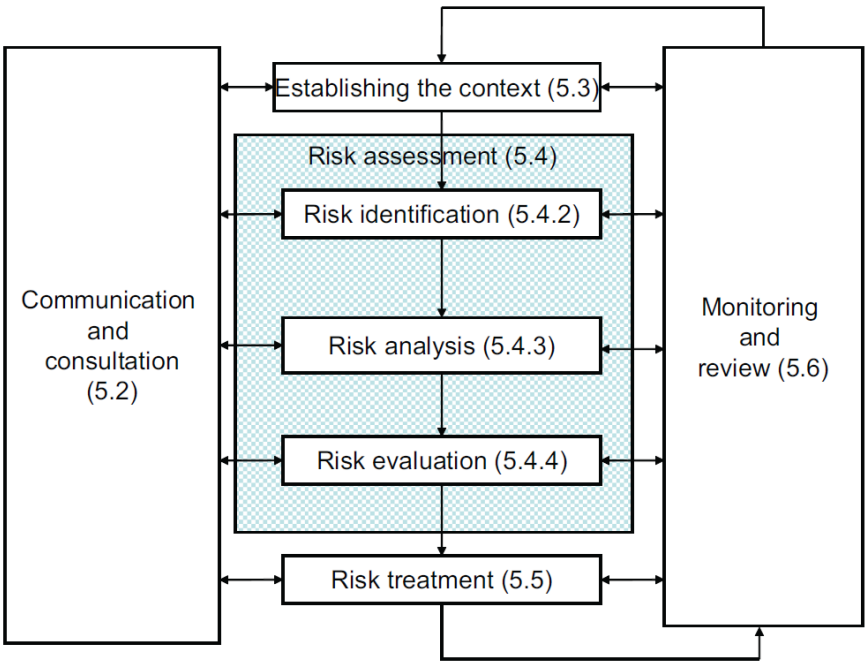


Figure 2.1.: Risk management process (ISO 31000, 2009)

2.2. Risk management process

2.2.1. Establish context

This part is a detailed exposition of the aims, scope, limitations and criteria. It is based on internal and external context (ISO 31000, 2009). Internal context can be found in the internal environment of the organization, in this case the AUR-Lab. It comprises inclusion of existing structures, procedures and the structure. The external context covers laws, regulations and other requirements from others, as well as the technical, natural, economic and financial environment (ISO 31000, 2009).

The context will be established through close communication with key personnel at AMOS and in the AUR Lab, to ensure a comprehensive foundation for this part. As reference guideline ISO 31000 (2009) will be used. The Context document can be found in the electronic appendix, it is not attached here, since all the information contained within the document can be found in this thesis.

2.2.2. Risk assessment

Risk in context with operation of AUV is connected with various hazardous outcomes. This includes loss of life and damage to health of operators, other personnel and third party people, or loss or damage to the AUV and other AUV, when operated as swarm. Furthermore

a consequence that could be considered is damage to the environmental resulting from contact between AUV and sub sea production facilities. These are very broad considerations, therefore risk in respect to loss of the vehicle, damage to the vehicle and a mission abort will be considered. Risk to the environment, arising from the loss of the vehicle is judged to be negligible, due to the low environmental impact of the vehicle itself. Additionally the AUV will not be operated near offshore or sub-sea facilities. The risk of loss of life and damage to health will be neglected since this is thought to be under control. Nonetheless these should be considered in a separate risk assessment.

Regionally the case study will focus on Norway, more specifically on Trondheimsfjord. This does not exclude other regions in Norway, such as Spitsbergen. The region itself is not this important, more the conditions that can be present such as ice coverage or excessive currents.

Operations are not only dependent on place but also on time. Several phases of operation have to be accounted for, with different conditions and varying focuses. The phases of interest are storage and transport, preparation and deployment, mission start and mission, retrieval and post-dive activities. A description of the different phases can be found in chapter 3.3.3.

The analysis is limited to a functional level of major components. In fig. 2.2 the subsystems of concern and the influences that are taken into account are summarized. Additionally it is assumed that 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 during operation. Another fact that should be kept in mind is that, so far, few REMUS 100 AUV have been lost. No loss or critical incidents have occurred at NTNU. Thus a too conservative estimation must be avoided.

Hardware damages is a wide time term therefore the interpretation in this thesis shall be briefly explained. It comprises internal and external damage. External damages are assumed to cover damages to the hull, propeller and fins. This includes these parts being broken off, chipped or cracked. Additionally it includes leakages to the inside, through broken seals, or similar. Internal damages are assumed to cover broken hardware inside the AUV, loose connections or internal corrosion. Summarized damages are meant, which are not recognized before deployment, might lead to loss of the vehicle.

2.2.3. Risk identification

For identification of risks and hazards a preliminary hazard analysis (PHA) for each phase will be carried out. The main function of a PHA is to identify the hazards and assess the relevant risks, in order to support the following risk assessment. This method is typically applied in the preliminary system design phase and basically reviews the energies or hazardous materials released in an uncontrolled manner (Rausand, 2011). Hazards are identified based

on relevant literature (e.g. Griffiths et al. (2003, 2009), Kirkwood (2009), Manley (2007), Podder et al. (2004), Christ and Wernli Sr (2007)), hazard checklists (e.g. Rausand (2011)), experience and judgment by the operators and personnel in the AUR Lab (M. Ludvigsen, F. Volden, R. Staven and M. Candeloro), the procedures for AUV handling and operation currently in place, and supplier information (e.g. Hydroid, 2013).

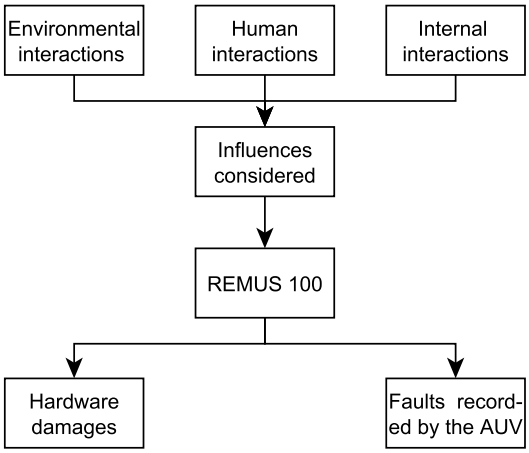


Figure 2.2.: Subsystems and interactions taken into account for the risk assessment

The findings are summarized in a PHA worksheet where the hazards, preceding causes, resulting consequences and possible mitigating measures are identified. A general layout for a PHA sheet, which will also be used in this thesis can be found in Rausand (2011, p. 229). 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 tab. 2.1 and 2.2 respectively. The categories are adaptions for this risk assessment from Rausand (2011) and are easily adaptable to other assessments. The preliminary risk is found by adding frequency and consequences together, the so called risk priority number (RPN). A high RPN corresponds to a high risk. The estimations of frequency and consequences are based on a subjective assessment and only reflect partly measured data. The use of categories is a rough estimation (Rausand, 2011) and the worst cases are assumed. A detailed analysis of frequencies and possible outcomes is carried out during the risk analysis. The results can be summarized in a risk matrix, exemplary shown in tab. 2.3.

Table 2.1.: Frequency/ likelihood categories used in the PHA (based on 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

Table 2.2.: Consequence categories used in the PHA

Category	Rating	Description
Loss of AUV	3	The AUV is not able to surface, can not be retrieved or is so severely damaged that further use is impossible
Severe damage of 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 2.3.: Risk matrix

Frequency / 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

2.2.4. Risk analysis

From the PHA (c.f. chapter 5.1) two main hazardous events have been identified; “Damage to the vehicle, which is undetected before the mission” and “Wrong planning or faulty set up of the vehicle”. These two hazardous events will be further analyzed with fault tree analysis (FTA) and event tree analysis (ETA). In a first step the events identified in the PHA are

connected in a logical way, according to the analysis type. Secondly the level of complexity is reduced and redundant events eliminated, by grouping of similar events to reasonable events. Not considered for the moment are collisions with other vehicles or vessels and the risk of ignition of the vehicle's battery. These events are considered very unlikely.

Not much statistical data is available for AUV reliability and safety. Thus the probabilities for all the basic events in FTA and ETA have to be found in a different way. The methods that will be used are evaluation of the fault logs, use of published data for similar systems, expert estimation and human reliability analysis (HRA). An overview of the different models and analysis techniques used for different aspects of the risk assessment are shown in fig. 2.3.

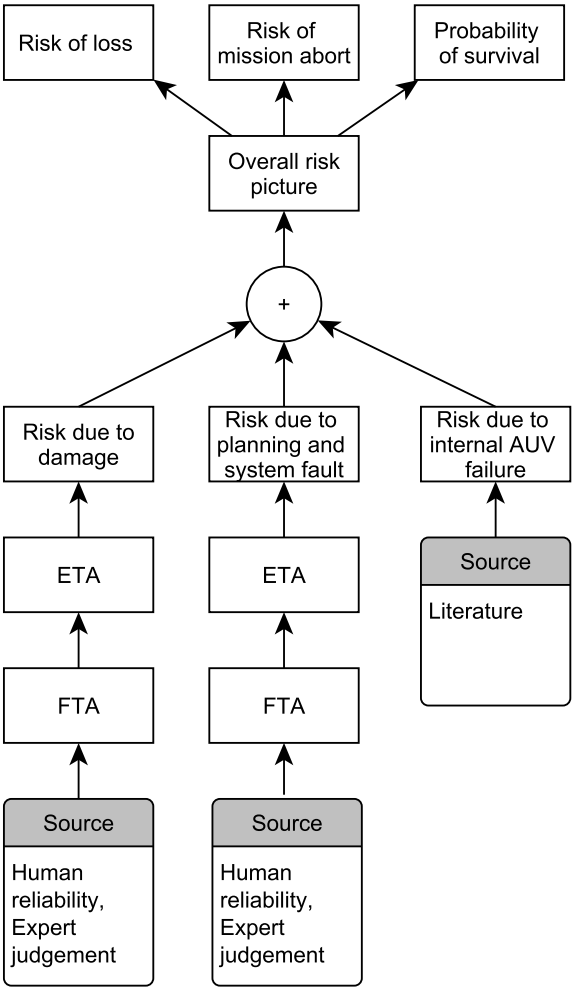


Figure 2.3.: Models used for the determination of basic event probabilities

Fault tree analysis

FTA is a tool to identify all combinations of basic events that may result in a critical event for the system (Rausand, 2011). In this case it will be used to analyze the interactions between the events identified in the PHA leading to the hazardous events, mentioned above.

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). In a quantitative analysis 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 analyzed. 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 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. For calculation of the top event probability $Q_0(t)$, CARA uses the approximation formula given in eq. 2.1. Where $\check{Q}_j(t)$ is the probability of failure of a minimal cut set, calculated in eq. 2.2. It is assumed that the basic events ($q_i(t)$) are independent from each other. A cut set is a combination of basic events that will lead to the occurrence of the top event. It is considered minimal if non-consideration of one event would not lead to the top event (Rausand and Høyland, 2004).

$$Q_0(t) \approx 1 - \prod_{j=1}^{k} (1 - \check{Q}_j(t)) \tag{2.1}$$

$$\check{Q}_j(t) = \prod_{i \epsilon K_j} q_i(t) \tag{2.2}$$

Event tree analysis

Similarly to FTA the events that occur after the hazardous event can be analyzed and different outcomes be assessed. For this 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 barrier failures (Rausand, 2011) but can also be significant events that may arise during an event chain. The event is either true or false, associated with a certain probability each. 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. For the whole analysis it is considered that only one event path can occur at a time. So if the vehicle is damaged, a fault in the navigational system is not considered, although this is possible. This is done for simplification, considering all possible event combinations would lead to a highly complex analysis with low readability.

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.

Evaluation of fault logs

In order to find out what faults occur in the system during a mission, the mission logs of the missions conducted, 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. and 24. January 2014 in a fjord near Ny-Ålesund Spitsbergen, Norway
- One mission conducted on 10. March 2014 in Trondheimsfjord near Hommelvik, Norway
- Four missions conducted between 08. and 10. April 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. Recurring 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 importance and relevant faults are identified. 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 operation.

Human reliability

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." (Rausand, 2011, instead of PSF the term performance-influencing factor is used)

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. Both are given a nominal HEP (NHEP), NHEP = 0,01 and NHEP = 0,001 respectively. 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 task types can be modeled if one task involves both actions. To find the HEP two formulas are used, normally eq. 2.3 is used, if more than three PSF >1 are used eq. 2.4 is used. In tab. 2.4 and tab. 2.5 a list of all PSF is given, a detailed description can be found in NUREG/CR-6883 (2005). The information is taken from the at-power worksheets, which represent a normal working operation and thus are believed to have adequate factors, suitable for this thesis.

$$HEP = NHEP \cdot \prod(PSF) \tag{2.3}$$

$$HEP = \frac{NHEP \cdot \prod(PSF)}{NHEP \cdot \prod(PSF - 1) + 1} \tag{2.4}$$

The task failure probability can be modeled by combining the diagnosis task and action task HEPs. First the probability of task failure without formal dependency ($P_{w/od}$) is calculated by eq. 2.5. For determination of the probability of task failure with formal dependency ($P_{w/d}$), firstly the degree of dependency has to be determined, c.f. tab. B.1, in the appendix. With the degree known the probability can be found with the respective equation given in tab. 2.6.

Table 2.4.: PSF in the SPAR-H method (Part 1) (NUREG/CR-6883, 2005)

PSF	PSF Levels		Multiplier	
	Diagnosis	Action	Diagnosis	Action
Available time	Inadequate time		P(F) = 1	
	Barely adequate time (≈ 2/3x nominal)	Time available ≈ time required	10	
	Nominal time		1	
	Extra time (between 1 and 2x nominal or > 30 min)	Time available ≥ 5x time required	0,1	
	Expansive time (> 2 x nominal and > 30 min)	Time available ≥ 50x time required	0,01	
	Insufficient information		1	
Stress/ stressors	Extreme		5	
	High		2	
	Nominal		1	
	Insufficient information		1	
Complexity	Highly complex		5	
	Moderately complex		2	
	Nominal		1	
	Obvious diagnosis	-	0,1	-
	Insufficient information		1	
Experience/ Training	Low		10	3
	Nominal		1	
	High		0,5	
	Insufficient operation		1	

$$P_{w/od} = Diagnosis\,HEP + Action\,HEP \tag{2.5}$$

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 skill and wrong decisions can easily lead to an undesired outcome. Secondly

the method can model, through the use of PSF, different environments and complexity. A short summary on how choice of PSF can be biased is given in the next section.

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 they were shortly briefed in HRA assessment and the method. One sheet is filled out for each basic event which was identified to be suitable for this method. Since the author of this thesis also has low experience with this method, it cannot be ensured that all details were presented correctly, despite thorough preparation. The events considered are listed below in tab. 2.7. Events marked with ETA are used in ETA and were given an abbreviation for easier handling of the documents. Non-marked events are part of the FTA.

Table 2.5.: PSF in the SPAR-H method (Part 2) (NUREG/CR-6883, 2005)

PSF	PSF Levels		Multiplier	
	Diagnosis	Action	Diagnosis	Action
Procedures	Not available		50	
	Incomplete		20	
	Available, but poor		5	
	Nominal		1	
	Diagnostic/ symptom oriented	-	0,5	-
	Insufficient information		1	
Ergonomics/ HMI	Missing/ Misleading		50	
	Poor		10	
	Nominal		1	
	Good		0,5	
	Insufficient information		1	
Fitness for duty	Unfit		P(F) = 1	
	Degraded fitness		5	
	Nominal		1	
	Insufficient information		1	
Work processes	Poor		2	5
	Nominal		1	
	Good		0,8	0,5
	Insufficient information		1	

Table 2.6.: Determination of probability of task failure (NUREG/CR-6883, 2005)

Degree of dependency	Equation for $P_{w/d}$
Complete dependence	1
High dependence	$(1 + P_{w/od})/2$
Moderate dependence	$(1 + 6 \cdot P_{w/od})/7$
Low dependence	$(1 + 19 \cdot P_{w/od})/20$
Zero dependence	$P_{w/od}$

Table 2.7.: Events identified for HRA for ETA and FTA event probabilities

Event	Description	Type
AN (ETA)	AUV is not properly monitored during mission	Action
BD (ETA)	Unexpected behavior is not detected	Diagnosis
DD (ETA)	Damage is not detected during preparation for deployment	Diagnosis
DM	AUV is dropped during moving from/ to maintenance area	Action
DrD	AUV is dropped during deployment	Action
DrR	AUV is dropped during retrieval	Action
DR	Damages are not detected and repaired	Diagnosis and Action
DT	AUV is dropped during manual transport from/ to the vessel	Action
FM	AUV is not placed correctly on workbench and falls off during maintenance	Action
FS	Existing faults of the AUV are not solved completely before deployment	Diagnosis and Action
LC	Local excessive currents and waves are not considered	Diagnosis
MC	Maintenance is carried out wrongly	Action
NC	Battery is not charged sufficiently	Action
RF	Faults are not recognized during planning phase or before deployment	Diagnosis
SH	Wrong use of software leads to wrongly implemented parameters	Action
TS	Transponders are not set up as planned before	Action
WB	AUV is wrongly ballasted	Action
WP	Implementation of mission path or map is done wrongly	Diagnosis and Action

Expert estimation

In order to analyze the FTA and ETA quantitatively some expert judgment of probabilities is needed. Thus a simple process was designed including elements of current practice (Burgman et al., 2006) and incorporating proven methods (Witteman and Renooij, 2003). But the process is simplified, since both the author of the thesis as well as the experts are inexperienced in expert estimation. Previous to the estimation the experts will be introduced to the method and pitfalls, which might be connected to the elicitation. The experts assigned in this process, are Martin Ludvigsen and Frode Volden. The events that are analyzed are summarized in tab. 2.9.

The probabilities are categorized in descriptive categories, which are associated with a certain probability, c.f. fig. 2.4 (Witteman and 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 estimation first verbally and then as percentage, according to the verbal expression.

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. tab. 2.8. The experts are also asked to give a comment on why they assessed the probability in this way. If the two experts have a similar assessment, the probability will be used directly. Otherwise it will be tried to find consensus between the two estimations.

Table 2.8.: Level of certainty assessment

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

Expert judgment is easily influenced, in the following list some of the sources for bias will be presented and shortly explained (Burgman et al., 2006). These biases derive mainly from psychological issues. The experts were asked to keep them in mind when assessing probabilities, to avoid bias or overestimation of the probabilities.

- Perception and memory
  - Judgments can be influenced by the way a question is formulated. A positive formulated question might be lower estimated then the question formulated in a more negative way.

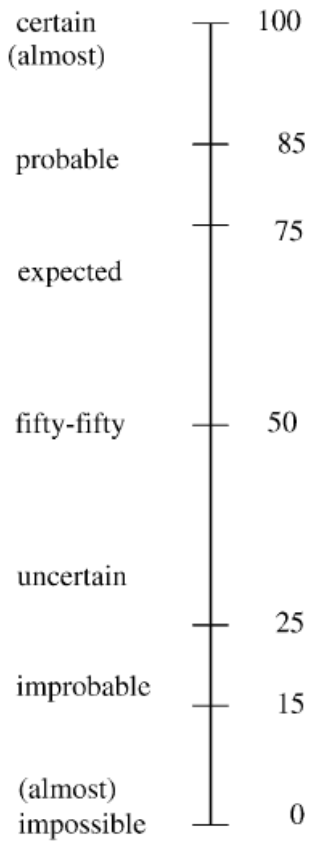


Figure 2.4.: Probability scale used in the expert estimation (Witteman and Renooij, 2003)

  - Events that already have occurred, are often higher estimated than events the expert never experienced.

- Framing

  - Choice can be influenced by the presentation of the question and choice alternatives, negative formulated choices are less likely to be chosen, even if they are the same as the "positive formulated".

- Heuristics and biases

  - Often the interpretation of a problem leads to an over-interpretation of the given data, thus leading to an overestimation/ false conclusion that cannot be drawn directly from the given data.

  - Events that recently occurred also tend to influence the choice, thus biasing judgment.

  - Anchoring happens if probabilities are associated to previously obtained data, from former assessments or suggestions of other experts.

- Overconfidence

  - Arises if the expert has more confidence in his estimate than the accuracy allows.

- Values and attitudes

  - Expert judgment is influenced by values and attitudes of the experts.

  - Values are expressions of preferences for goods/ activities and the moral or ethical beliefs that lead to these preferences.

- Motivated reasoning, decision bias and distortion

  - Predetermined choices can lead to a distortion of the elicitation to justify these choices.

  - A similar phenomena occurs when the experts has interest in the outcome from use of the data and thus tries to influence the outcome positively.

Table 2.9.: Events to be estimated by the experts

Abbreviation	Event description
Basic events for Fault tree analysis	
CV	AUV has contact with deployment vessel in water after deployment or during retrieval and receives damage
TD	AUV is damaged during transport in a vehicle (e.g. truck, airplane,...) from TBS to mission location (e.g. Svalbard)
Concerning wrongly implemented ways and planning so that contact with land or seafloor is very likely	
1	AUV does not abort mission automatically if the AUV is set up wrongly for the mission (e.g. wrong map datum, high deviations, wrong ballasting)
2	AUV is stuck in seabed and cannot be recovered with wrongly implemented parameters given that the AUV does not abort mission because of the faulty mission planning
Concerning damages that can lead to a loss of the AUV, e.g. cracks (leakage), loose connections (failure of subsystems), etc.	
3	Self-tests do not detect damage and abort mission given that a critical damage is present
4	Vehicle is not able to surface again due to a damage given that the damage is not detected before deployment

Data from literature

From the evaluation of the fault logs of the AUV, it can be seen that similar faults have occurred, as described in Griffiths et al. (2009). Thus it is assumed that their estimation for shallow coastal waters can be applied here for the risk from internal system faults. The risk of loss itself will be found from figure 7 in Griffiths et al. (2009) (fig. 4.1 (b) in this thesis). The graph for coastal waters is chosen, the average distance of a mission of the REMUS 100 of NTNU is used to find the optimist and pessimist estimation of probability of survival. These two values are then averaged with the arithmetic average. It is assumed that the probability of loss lies within these bounds. A mission is normally between 20 and 30 km long.

The risk might be evaluated redundant in this way, since internal faults are also parts of the FTA and ETA. This might lead to an overestimation of the risk of loss. Since few experience has been gained yet a small overestimation is assumed to be acceptable.

2.2.5. Risk evaluation

Following the risk analysis the risk is evaluated, determining which hazards are most significant for the operation. The combined risk found in the evaluation will be represented graphically and verbally.

2.2.6. Risk treatment

Risks that are unacceptable high have to be treated with high priority, risks that are in the limits will be treated as ALARP. This is the abbreviation for "as low as reasonably practicable" (Rausand, 2011). It means that hazards need control unless it can be shown that the effort connected with risk reduction is unacceptable high. Since the assessment presented here is quite coarse all events should be analyzed and methods identified to make the risk ALARP.

To identify possible RCM the basic events from the analysis are reassessed and high contributors are identified. A re-evaluation of the risk is then based on improved basic event probabilities. Thus the total impact of all measures can be evaluated. Re-estimation is based on the authors belief of the improvement. For demonstration purposes only the HRA events will be reassessed. It is assumed that the chosen measures reduce the corresponding PSF to a nominal level. The events of concern are changed for each expert in the respective event, the probabilities are averaged and give the new probability. These probabilities are then changed in the fault and event trees.

2.3. Risk management framework

In this part the development of the risk management process and how to keep it updated will be described. It will be based on the outline given in ISO 31000 (2009) and cover the recommended content. Suggestions for applicable methods in future assessment will be based on the experiences and steps taken during the risk assessment. Thus it will be possible to reproduce the assessment, keep the risk assessment updated and apply the risk assessment process to other hazards and vehicles. In addition ways of communication and reporting of incidents and risk will be described. Other hazardous sources that should be considered in the future are also mentioned.

3. Autonomous underwater vehicles

3.1. General

Some general information on AUV shall be presented first, followed by a short discussion on autonomy of AUV operation. The last section of the chapter covers a more detailed description of the REMUS 100 and the operations and usage in the AUR Lab.

The US Navy (2004) generally defines the term UUV, whereas this definition suits in a non-military context better AUV:

> "Self-propelled submersible whose operation is either fully autonomous (pre-programmed or real-time adaptive mission control) or under minimal supervisory control and is untethered except, possibly, for data links such as a fiber optic cable."

An AUV is not directly controlled by an operator and the main source of power is internal. Communication is done either for data transmission or for mission update of the AUV. AUV do not have a permanent connection, through a tether, sound or RF to the main operation base. AUV are normally cigar shaped to reduce drag and make them efficient in propulsion. They consist of four main parts: payload, energy system, power distribution and propulsion, and buoyancy and ballast. The payload includes control, data acquisition and storage, as well as communication and navigation system (Brighenti, 1990). Energy systems today mainly consist of battery packs (Antonelli et al., 2008), but experiments are made with fuel cells to increase the energy density in the system (e.g. Yamamoto et al., 2004, Raugel et al., 2010). Buoyancy foam and ballast are used to balance the system and keep it afloat. In general AUV are slightly positively buoyant, so they float on the surface or will float back to the surface in case of a critical fault. A very general setup of an AUV can be seen in fig. 3.1.

There are two types of AUV, self-propelled ones and gliders. Self-propelled AUV have a propeller or a jet-pump system to move through the water. Gliders are buoyancy driven versions of AUV which sink or rise and produce propulsion through fins, an example is given by Wolek et al. (2012). Focus of this thesis is on self-propelled AUV, since the REMUS 100 is such a vehicle. Until recently AUV were not used for manipulation intervention, Yuh et al. (1998) described such a vehicle, which was successfully tested in 2010 (Yuh et al., 2011).

Main challenge in autonomous manipulation work is the unstructured environment of the sea (Yuh et al., 1998).

-

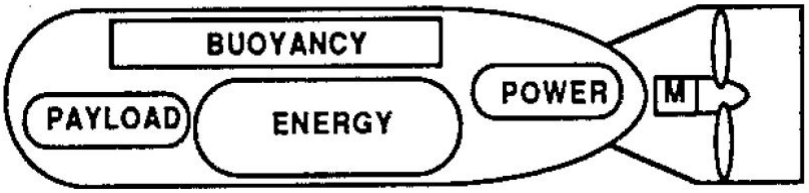


Figure 3.1.: General layout of an AUV (Brighenti, 1990)

3.2. Autonomy

Autonomy is a very broad term, often used with UUV. In this short section the concept of autonomy will be examined. The Norwegian society of automatic control (NFA) defines autonomy as "the ability of a system to achieve operational goals in complex domains, by making decisions and executing actions on behalf of or in cooperation with humans" (NFA, 2012). An important part inherent in this definition is the last part "on behalf of or in cooperation with humans". This shows that there are varying degrees of autonomy, with different levels of control of the human operator. There are various scales defining levels of autonomy, no standard definition of categories exists (Insaurralde and Lane, 2012). The US Navy defined six levels of autonomy, c.f. tab. 3.1. Currently AUV are found in levels three to five, where the human operator often has the control to abort a mission and has to give narrow mission definitions beforehand.

3.3. REMUS 100

3.3.1. System description

The REMUS 100, by Hydroid, is designed for coastal areas with depth up to 100 m. With a diameter of 19 cm, a length of 160 cm and a weight of 31 kg it is a rather small AUV. The internal energy source is a 1 kWh lithium-ion battery. It enables the AUV to conduct missions of maximal four to five hours (at 4 kn and 3 kn propulsion speed, respectively). Control of the motion is done with one directly driven propeller and four fins. The fins are mounted vertically and horizontally, for yaw and pitch control (Hydroid, 2013). The REMUS 100 is equipped with an ADCP, CTD sensors, internal position sensors and positioning sensors. Several other sensors can be added or exchanged. (Hydroid, 2013).

Table 3.1.: Levels of autonomy as defined by the US Navy (NFA, 2012)

Level	Name	Description
1	Human Operated	**All activity within the system is the direct result of human-initiated control inputs**. The system has no autonomous control of its environment, although it may have information-only responses to sensed data.
2	Human Assisted	**The system can perform activity in parallel with human input**, acting to augment the ability of the human to perform the desired activity, but has no ability to act without accompanying human input. An example is automobile automatic transmission and anti-skid brakes.
3	Human Delegated	**The system can perform limited control activity on a delegated basis**. This level encompasses automatic flight controls, engine controls, and other low-level automation that must be activated or deactivated by a human input and act in mutual exclusion with human operation.
4	Human Supervised	**The system can perform a wide variety of activities given top-level permissions or direction by a human**. The system provides sufficient insight into its internal operations and behaviors that it can be understood by its human supervisor and appropriately redirected. The system does not have the capability to self-initiate behaviors that are not within the scope of its current directed task.
5	Mixed Initiative	**Both the human and the system can initiate behaviors based on sensed data.** The system can coordinate its behavior with the human behaviors both explicitly and implicitly. The human can understand behaviors of the system in the same way that he understands his own behaviors. A variety of means are provided to regulate the authority of the system w.r.t. human operations.
6	Fully Autonomous	**The system requires no human intervention to perform any of its designated activities** across all planned ranges of environmental conditions.

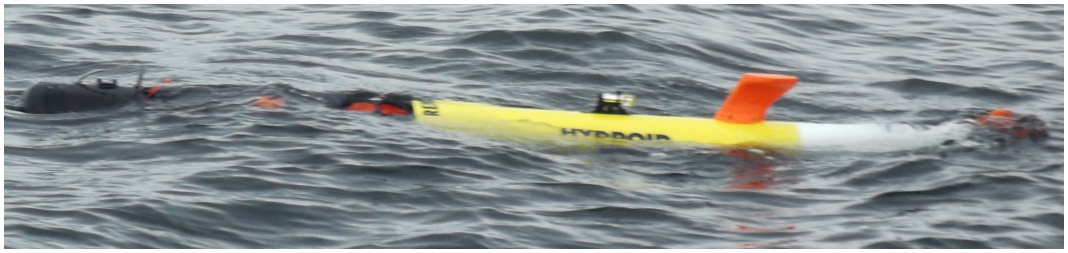
3.3.2. Applications in the AUR Lab

The REMUS 100 of NTNU was acquired at the end of 2013. Hence only few sea trials have been conducted yet and little experience has been obtained. The vehicle is primarily used for test and verification of control algorithms, newly developed equipment and scientific research cruises. Missions are taking place in several locations all across Norway. So far, the AUV was used on missions in Trondheimsfjord and in the fjords of Spitsbergen. Additionally the AUR Lab is working with UAV (Unmanned Aerial Vehicles), these are used in combination with AUV as a communication platform for observation missions.

The AUV is normally deployed from a small craft, which allows easy deployment and retrieval. But this limits the space which is available for corrections and operation. R/V Gunnerus is also used, which is larger and more space is available. Deployment and retrieval are not as easy from there, thus a second smaller craft is needed. The AUV itself is stored and maintained in Trondheim's biological station (TBS). An office was assigned for these purposes.

Currently three systems are used for position keeping and control. These are the long baseline (LBL) system, delivered with the AUV, GPS fixes on the surface and the inertia navigation system. In order to substitute the LBL sometimes, an ultra-short baseline system (USBL) - transponder was ordered. A LBL system uses at least two transmitters whose position is known to the AUV in global coordinates and the position is derived geometrically in the AUV. The USBL system is normally mounted below a vessel and the position of the AUV can be determined in relation to this vessel. The global position is then determined from the coordinates of the vessel. The advantage of the USBL system is that it is not limited in range, as long as the vessel is close enough to the AUV.

(a) REMUS 100 AUV in its transport box



(b) REMUS 100 AUV at mission start in the sea

Figure 3.2.: The REMUS 100 AUV of NTNU

3.3.3. Phases of operation

A short description of the activities conducted and conditions encountered in the different phases of operation will be given in the following paragraphs.

Storage and transportation

This phase comprises all activities connected with storing the vehicle on land, the transport from the storage to the vessel of operation and maintenance that is carried out while the AUV is not on a cruise. Vessel maintenance and storage are conducted in TBS. No strong variations in temperature or other conditions are to be expected. Normally all equipment needed can be found at TBS.

Transportation of the AUV occurs in a special hard plastic case. For AUV transport rails are attached to it, which allow an easy handling and prevent movement in the case. Other equipment, such as mission laptop, transponders, weights for transponders and small spare parts can be found in a second box which is specially designed for this purpose. Temperature changes during transport are expected to be within the allowable range.

Preparation and deployment

The preparation and deployment phase involves programming of mission parameters, preparation of the vehicle for the mission, pre-dive check and the deployment of the vehicle. For these actions procedures are described in the guidelines in the operation manual for the REMUS 100. This phase takes place on land as well as on board of the vessel. For programming the vehicle a sheltered area is preferable.

Especially during deployment rough conditions can be present, such as waves, strong wind, low temperatures and snow and rain. For deployment and retrieval a frame was designed that fits the AUV. With this frame the crew does not have to lean as far over the boat side.

Mission start and mission

Mission start describes the phase when the AUV is in the water and waiting to get the start signal and an initial GPS position fix. The mission is the phase during which data are collected and the purpose of the cruise is fulfilled. Especially at the beginning of the mission, surface conditions, as mentioned above, have an influence on the vehicle and operation. During the mission currents have major influence on the AUV, excessive currents can lead to drift, which cannot be corrected. During the whole phase the density of the water is an important factor, since the vehicle should be positively buoyant, so that it floats free if stuck on the ground or floats up if a system break down should occur.

The AUV is monitored during the dive by acoustic messages that it sends. The messages are received by a tow-fish acoustic transmitter. The Hydroid REMUS VIP - software translates

the information for the crew on a laptop. Monitoring is done from the work boat, where the AUV was deployed. A message is send every two minutes with position information and every four minutes a more detailed report is sent with current vehicle status. If the vehicle should be monitored from land, it sends regularly messages via the IRIDIUM satellite system. This is done in cold and harsh regions such as Spitsbergen.

Retrieval and post-dive activities

Actions that are included in these phases are locating the AUV after mission completion or abort of the mission, picking it up, cleaning it as prescribed, storing it in the transport case and retrieving the collected data. During this phase also rough conditions can be encountered: temperatures below 0°C, strong winds and waves. Activities such as cleaning or data download are executed on board of a bigger vessel (e.g. Gunnerus) or on land.

4. Literature review

4.1. Risk in AUV operations

Concerning risk and reliability of AUV operations only some publications on AUV, mostly scientifically used and often unique, are available (e.g. Griffiths and Trembanis, 2007, Manley, 2007). The most relevant literature from recent years is presented here. Generally modifications and upgrades of vehicles often lead to a reduction of reliability in the operations following right afterward (Griffiths and Trembanis, 2007).

Chance (2003) analyzed the reliability of the Huggins AUV. Since the first use in the beginning of 2001 to the end of 2002 the average percentage of successful operations increased from an average of about 20 % to 95 %. A continuous trend of improvement in correlation with experience was seen. Some major cuts in mission success can be seen when problems with the battery system or the electronics arose.

Manley (2007) differentiates two kinds of risk connected with AUV - technical risk and operational risk. Technical risk derives from the system itself. AUV are complex electromechanical artificial systems, which are in addition becoming more autonomous. The mechanical components can fail due to the harsh environment, inferior quality or alike. The software and mission program can contain faulty code and therefore cause a system failure. All failures can lead to a loss of the AUV or an abortion of the mission, thus creating a risk.

Manley (2007) highlights the energy supply as major source of risk, since energy is stored with a high density. Lithium batteries can cause substantial damage if failed. Other energy sources, mainly in developing states, like hydrogen cells are high risk contributors. Operational risk derives from the dynamical nature of the ocean and varying weather conditions during operation (Manley, 2007). Launch and recovery are proven to be the most critical phases. The AUV can fall during lifting operation, endangering the AUV itself as well as the operators and crew on board. Even if the AUV is in water there is the risk that it might get caught in the propeller of the vessel. During recovery similarly there is the danger of contact between vessel and AUV (Manley, 2007). As conclusion Manley (2007) states that a thorough evaluation of needs is important to identify the requirements and best strategy to handle operational risk. For the handling of operational risk an experienced and well trained operation team is of most importance.

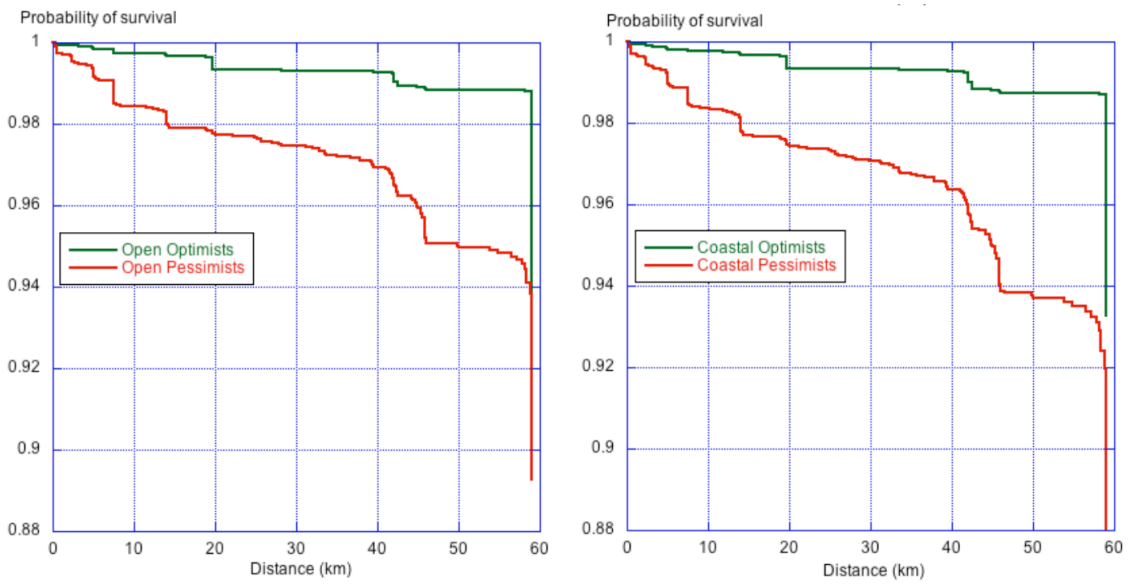
A simulation based analysis for AUV was carried out by Bian et al. (2009b), this was based on the fuzzy FTA used already in Bian et al. (2009a). They considered the subsystems navigation, computer, thruster, energy, communications, obstacle avoidance, security detection and environmental detection. The top event was characterized as "AUV works defectly", so not as intended. Since the top event is defined very broadly only or-gates were used, resulting that every basic event is also a minimal cut set. Analysis was carried out with a Monte Carlo simulation technique Bian et al. (2009b). The results showed a rather low probability of survival after some hundred hours of total operation time.

Griffiths and Brito (2008) modeled risk prediction for under ice missions with a scientific AUV with a Bayesian belief network. This model is based on expert judgment and observations made previously, as well as of observable features and their probability of encounter. With this model a probability distribution for the probability of loss of the AUV during an under sea-ice mission was determined (Griffiths and Brito, 2008). The authors claim that this approach will become a standard in the AUV offshore industry for under ice operation.

Kirkwood (2009) presents some incidents that happened to MBARI's autonomous platforms, including moorings and UUV with respect to interactions with other people. A problem that reoccurred from time to time was that people got close to the vessel while a ROV was under water. Due to low maneuverability this might lead to unwanted situations. From the incidents that happened to the institute's AUV it can be said that if an AUV is found, because it drifted ashore, it represents a risk to the people finding it, since it contains batteries. But it also imposes a risk to the AUV, since it might be opened. Kirkwood (2009) concludes that the risk of encountering third parties in a mission is increasing, which at least might affect AUV operations, since there is an increasing probability of losing the AUV by contact with other marine users.

Griffiths et al. (2009) investigated the fault history of two REMUS-100 AUV which were used at the Center for Coastal Marine Sciences at California Polytechnic State University. The AUV were in use at that time from 2001 to 2009 and from 2003 to 2009, in a total of 186 missions, of which 173 were considered satisfactory successful. In these missions 507 problems were logged, with 37 unique faults or incidents. Seven out of these 37 were responsible for 92 % of all problems recorded. The expert judgment executed and described in the article showed that the most reoccurring faults only played a very minor role in the risk of loss of one of the AUV during a mission. Griffiths et al. (2009) carried out an expert estimation of survival probabilities, using a modified SHELF approach. The experts were asked to estimate five measures characterizing the probability of loss, thus the risk. This assessment was combined with Kaplan Meier plots to find the probability of survival based on mission length. The found probability plots reflect the experience gained so far, with the vehicles. The process itself might be biased because faults were categorized and optimistic and pessimistic judgments not merged, therefore interpretation might also be biased and the

results viewed optimistic or pessimistic (Griffiths et al., 2009). The survival probability plots for open water and coastal water are shown in fig. 4.1. The pessimistic estimation was found to be too negative, since the average expected number of missions until loss was significantly lower than the total number of missions conducted until now, where no AUV was lost.



(a) Estimation for open waters

(b) Estimation for coastal waters

Figure 4.1.: Probability of survival plots based on expert elicitation and encountered faults of two REMUS 100 AUV (Griffiths et al., 2009)

In Brito et al. (2012) an improved risk assessment was introduced. The assessment for probability of loss, given a certain fault that was experienced during earlier missions, was improved. It was based on consensus for the distribution. Similarly a consensus based assessment of possible mitigation of these faults, was executed. The consensus is based on the experts discussing and elevating on the faults, the understanding of fault mechanisms and the effects on the AUV. The process described also includes a review process of risk after the mission, only taking into account the faults which occurred during the mission (Brito et al., 2012).

Brito and Griffiths (2011) used their experience with risk assessment and tried to model the whole deployment process in a Markov chain transition model. The model draws on experience and expert judgment to develop the transition probabilities from state to state. For deployment, transport, retrieval, etc., static transition probabilities are used, while the mission itself is modeled dynamically, depending on mission distance. With the model presented the risk for a total mission can be assessed, but still the model is full of uncertainties, due to

lack of data. It is therefore required to reassess and revise failure probabilities and validate the data after each mission (Brito and Griffiths, 2011).

Another FTA of an AUV was conducted by Xu et al. (2013). They analyzed the reliability of the 4500M AUV, a Chinese mineral exploration AUV. For this purpose the AUV system was divided into four levels and 39 basic failure events. The basic events were component failures, assumed to be distributed by an exponential distribution. For analysis of the tree Monte Carlo simulation was chosen. In their results, Xu et al. (2013) showed that the probability of the AUV working for 40 hours is 80,07 %, which is assumed to be satisfactory by the authors.

4.2. Risk management of AUV operations

A proactive and systematic risk management process for AUV was developed by Griffiths and Trembanis (2007). The process is designed as a framework tool to give AUV owners the possibility to assess the risk of loss of an AUV. It depends mainly on objective information, but also requires subjective expert evaluation. The process involves elements and uncertainties that come along with the handling of autonomous systems (Griffiths and Trembanis, 2007). The process is split in five steps (Griffiths and Trembanis, 2007):

1. Design of a risk acceptance process, including assignment of risk owner and technical assessment team
2. Campaign and mission requirements, also used as input for the risk owner
3. How can faults be assessed and the survival probability calculated, including actual calculation
4. Risk evaluation of calculated risk against risk acceptance criteria
5. Propose risk mitigation strategies, e.g. procedural measures, technical measure, quality assurance, use of tools is recommended (FMECA, FTA)

If the risk connected with AUV operation is assumed to be too high, although measures have been taken to reduce it, insurance might be an alternative. Griffiths et al. (2007) presents four cases in which AUV operations have been insured, they point out the difficulties connected with establishing a contract and the influencing factors of insurance premium. Two different kinds of insurance should be considered, insurance against the loss of vehicle or insurance of the vehicle and cost resulting from the loss, i.e. the unsuccessful mission. In one case the work with an insurance broker even led to a significant input for improvement of design and operation of the vehicle. Griffiths et al. (2007) conclude that insurance, especially for experienced users is a good option to cover the risk of loss, for new users and operators it might be difficult to obtain insurance.

5. Results

The main findings of the risk assessment process and the results of the risk treatment process will be presented below. Additionally a short summary of the risk management framework will be given. The documentation and therefore the unabridged results are gathered in the appendices A (PHA), B (risk analysis), C (risk treatment) and D (risk management framework).

5.1. Risk identification

The risks that were identified in the PHA are summarized in tab. 5.1. The numbers correspond to the description in the PHA sheet in the appendix. The most concerning risks, with a ranking of seven and higher are:

- (1-2) AUV falls during moving to/ from maintenance
- (1-6) AUV bumps into objects during transport with crane
- (1-7) AUV is dropped during manual transport on vessel
- (2-1) Wrong mission parameters are implemented during preparation
- (2-2) AUV is not correctly ballasted for operation
- (2-4) AUV is damaged during preparation
- (2-7) AUV has contact with vessel after deployment
- (3-3) Unexpected and unwanted behavior during mission

Table 5.1.: Risk matrix for all identified hazards

Frequency / Consequence	Improbable	Remote	Possible	Occasional	Fairly normal
Loss of AUV	1-3, 2-9, 3-6, 3-11, 4-5	2-8, 2-12, 3-1, 3-2, 3-4, 3-10	2-3, 2-11, 3-7, 4-3, 4-6	1-6, 1-7, 2-2, 2-4, 2-7, 3-3	2-1
Severe damage, Mission abort		1-8, 1-9, 3-5, 3-8, 3-12, 4-2	1-1, 2-5, 4-4, 4-8	1-4, 1-5, 2-6, 4-1	1-2
Small damage		3-9		2-10, 4-7	

5.2. Risk analysis

5.2.1. Fault log evaluation

During the evaluation a total of 1650 fault messages distributed over 29 faults were recorded by the AUV in the 12 missions conducted, so far. A graphical summary of the occurrence of faults is given in fig. 5.1, a description of the events can be found in appendix B.2. The most reoccurring events are:

1. #8 - 537 faults - Self test failure altitude (tilt), [80000010] pausing mission
2. #10 - 537 faults - Warning compass bias table entry is excessive
3. #12 - 166 faults - Vehicle at low altitude. Executing emergency climb
4. #1 - 147 faults - The ADCP is not sending water current data
5. #7 - 52 faults - Vehicle stuck on surface; attempting to drive it down
6. #5 - 48 faults - Fix needed: Get fix objective
7. #9 - 47 faults - No response from Iridium to command ATH0
8. #19 - 47 faults - Self test failure thruster, [A1020080] pausing mission

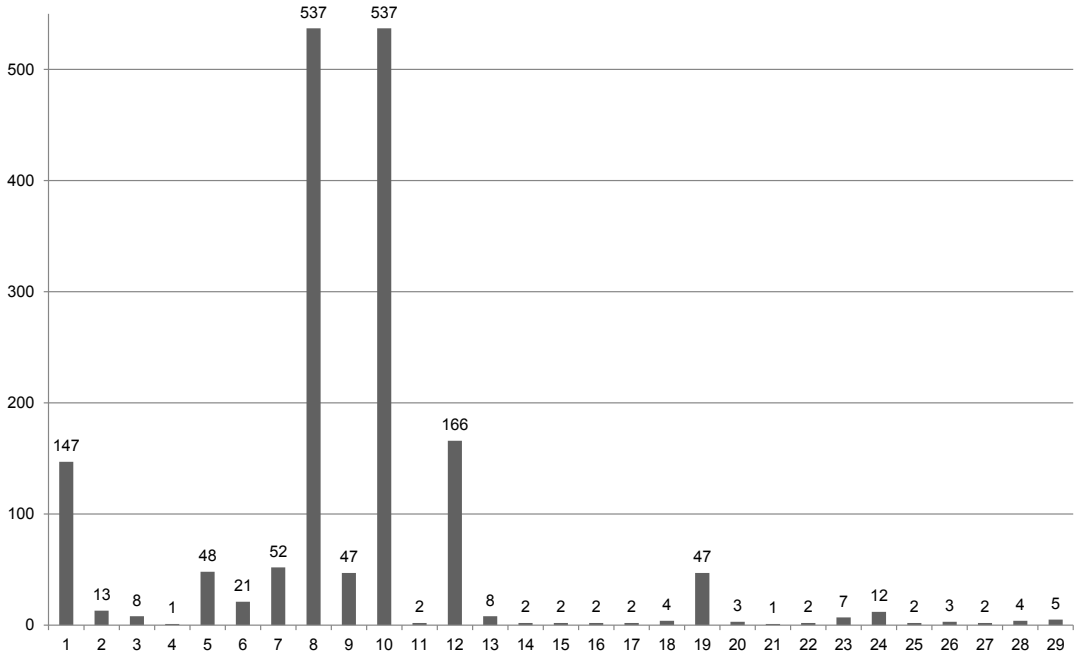


Figure 5.1.: Number of faults per fault type recorded

5.2.2. HRA

The HRA was completely conducted by one of the experts, the second expert could only assess half of the events. The results are summarized in tab. 5.2. A detailed listing of the HRA assessment with all PSF can be found in appendix B.3.

5.2.3. Expert estimation

The expert estimation could only be conducted by one expert. For the six events all probabilities and confidence in each estimate was assessed. This is summarized in tab. 5.3.

Table 5.2.: Summary of the HRA

Abb.	Estimation		Combined
	Expert 1	Expert 2	
AN	0,1305	0,0010	0,0658
BD	0,1600	0,0005	0,0803
DD	0,0800	0,0005	0,0403
DM	0,0200	0,0500	0,0350
DrD	0,0020	0,3336	0,1678
DrR	0,0477	0,3336	0,1906
DR	1,0000	1,0000	1,0000
DT	0,0010	0,0050	0,0030
FM	0,0006	0,0010	0,0008
FS	0,6059	1,0000	0,8030
LC	0,0748	n.a.	0,0748
MC	0,0060	n.a.	0,0060
NC	0,0119	n.a.	0,0119
RF	0,2878	n.a.	0,2878
SH	0,1072	n.a.	0,1072
TS	0,0005	n.a.	0,0005
WB	0,0060	n.a.	0,0060
WP	1,0000	n.a.	1,0000

Table 5.3.: Summary of expert judgment on probabilities

Event	Probability	Confidence
CV	10 %	Low
TD	15 %	Low
1	5 %	Medium
2	1 %	Medium
3	3 %	Medium
4	2 %	Medium

5.2.4. Data from literature

For 25 km missions, the probability of survival was found to be 0,995 from the optimist estimation and 0,973 for the pessimist estimation. This averages to 0,984 as probability of survival, the probability of loss for internal faults is thus 1,6 %.

5.2.5. FTA

Figures 5.2 and 5.3 show the fault trees drawn for the analysis. The basic event probabilities found previously were added to the events in CARA Fault Tree. The program then was used to calculate the top event probabilities. The probability for a "Damaged vehicle before it is deployed" was found to be 50,76 %. The event probability for a "Wrongly set up vehicle" was found to be 28,78 %.

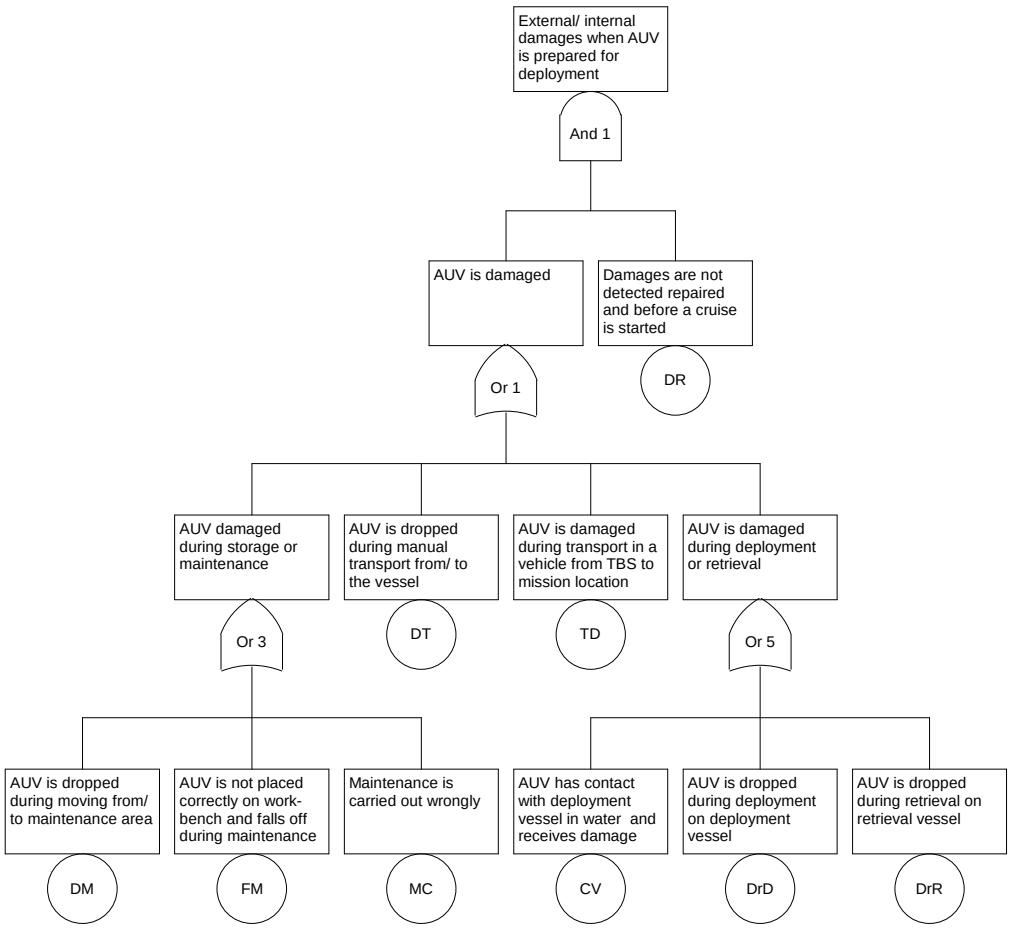


Figure 5.2.: Fault tree with top event: "External/ internal damages when AUV is prepared for deployment"

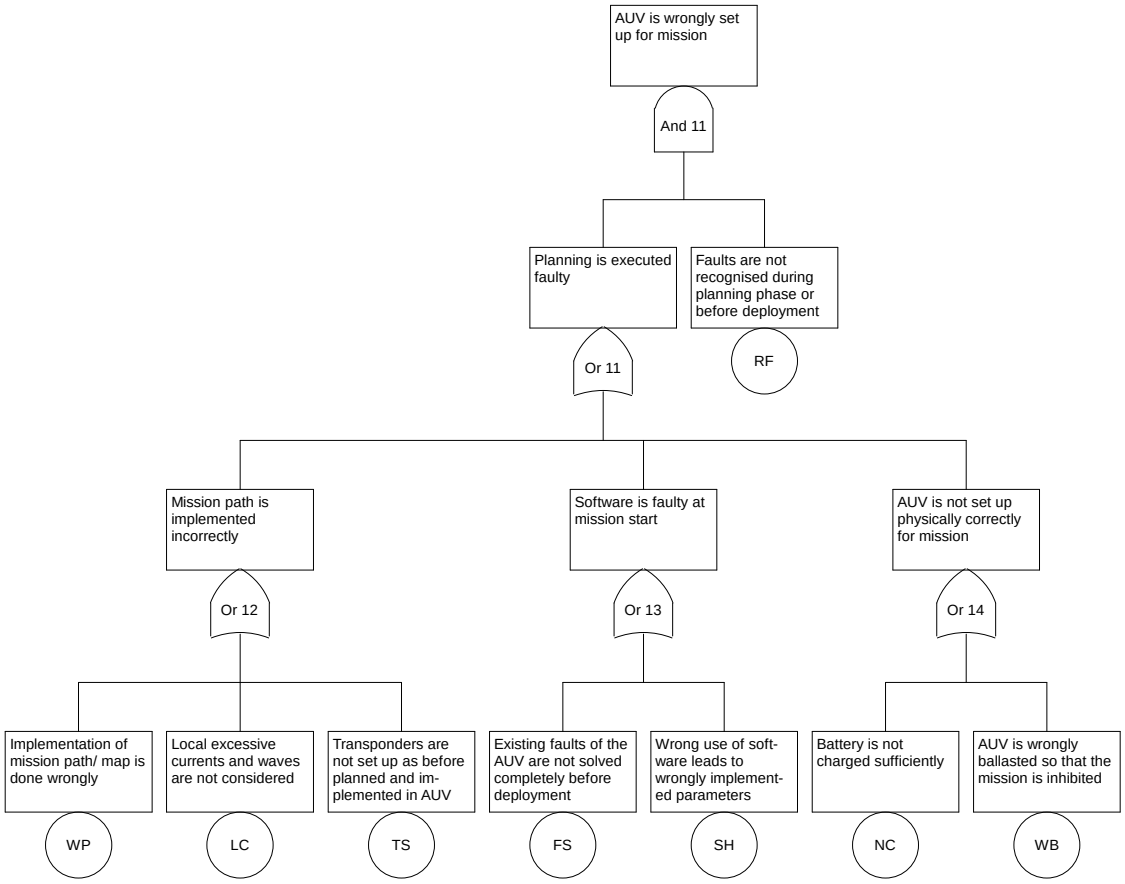


Figure 5.3.: Fault tree with top event: “AUV is wrongly set up for mission”

5.2.6. ETA

Three types of end events were identified in the ETA: Loss of AUV, Mission completed with faulted/ damaged AUV and mission abort. The event trees are shown in fig. 5.4 and 5.5. All outcomes and their respective probabilities can be found in the last two columns of the trees. It is notable that the risk of loss of the vehicle is relatively low in both trees. A more detailed representation of the total risk is found in the next section.

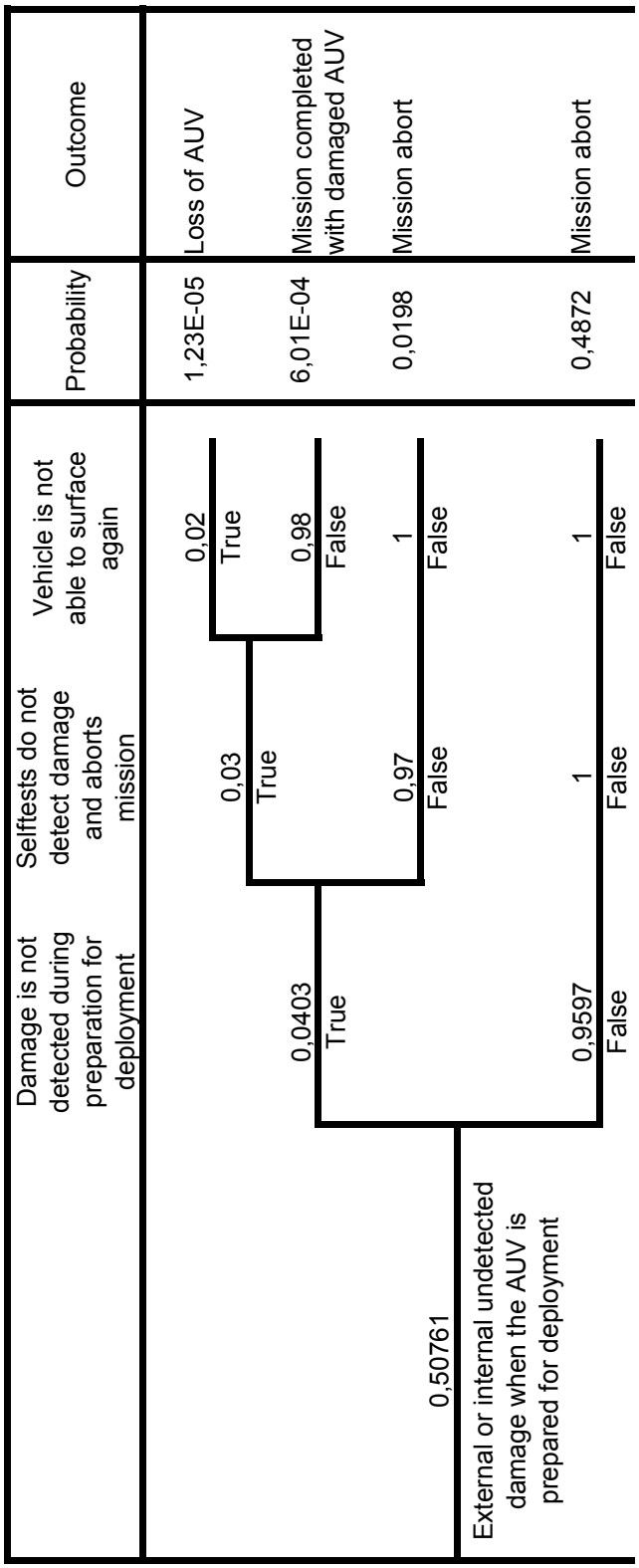


Figure 5.4.: Event tree for the start event "External or internal undetected damage, when the AUV is prepared for deployment"

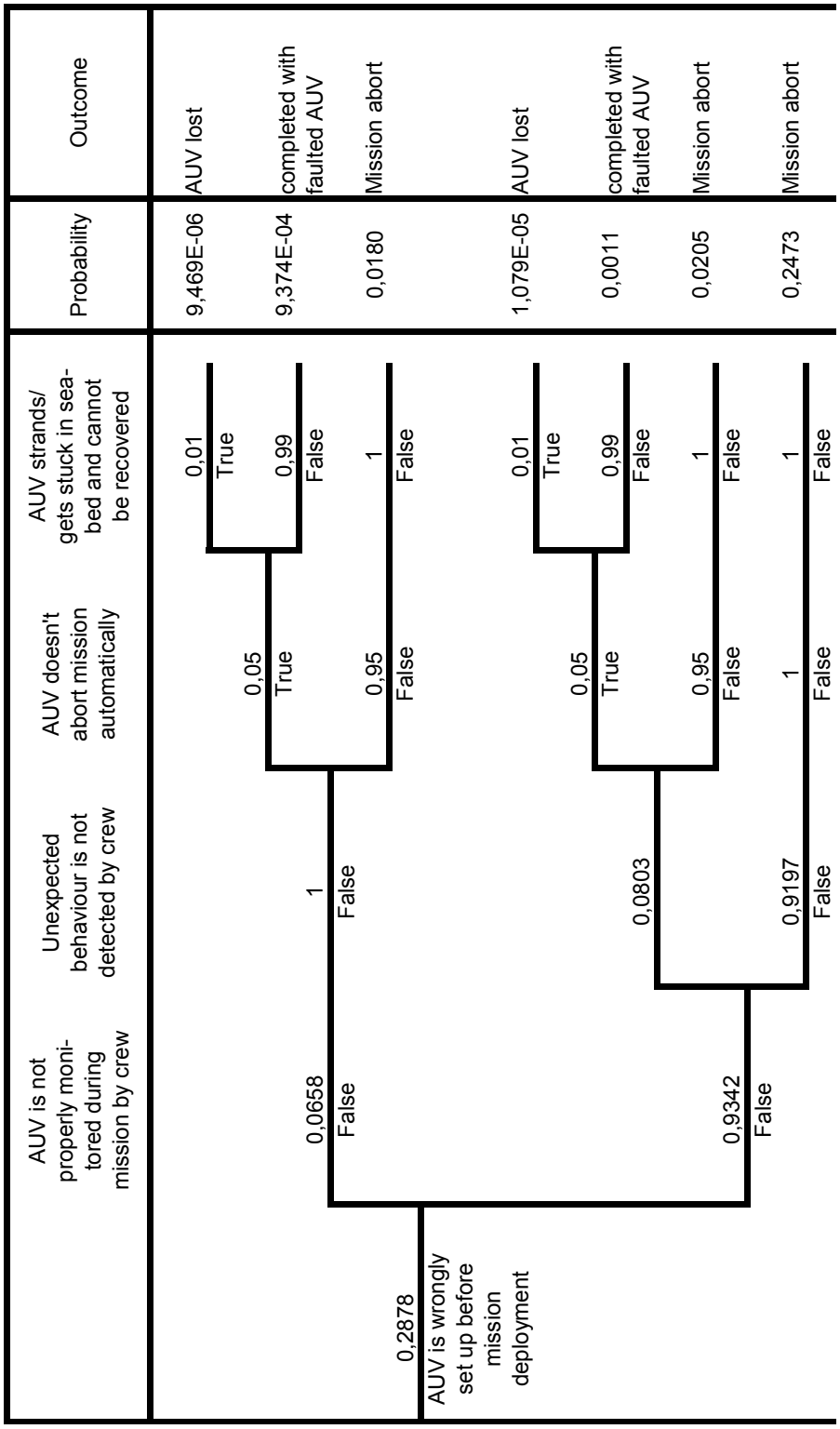


Figure 5.5.: Event tree for the start event “AUV is wrongly set up before mission deployment”

5.2.7. Risk evaluation

Tab. 5.4 summarizes the risk found from the two event trees and the literature data, it also shows the possibility to have a successful mission. This is better visualized in fig. 5.6. Accordingly in almost four out of five cases the mission should be aborted and in 1,6 % of missions the AUV might be lost. Finished mission with fault, in this context means that the mission was finished without mission abort. The results from such a mission can be expected to be not totally satisfying.

Table 5.4.: Summary of mission outcomes and associated probabilities

Event	Damage	Planning	Literature	Sum
Loss of AUV	$1{,}227{\cdot}10^{-5}$	$2{,}026{\cdot}10^{-5}$	0,016	$1{,}603{\cdot}10^{-2}$
Mission abort	0,5070	0,2858		0,7928
Finished mission with fault	$6{,}014{\cdot}10^{-4}$	$2{,}006{\cdot}10^{-3}$		$2{,}608{\cdot}10^{-3}$
Successful mission				0,1886

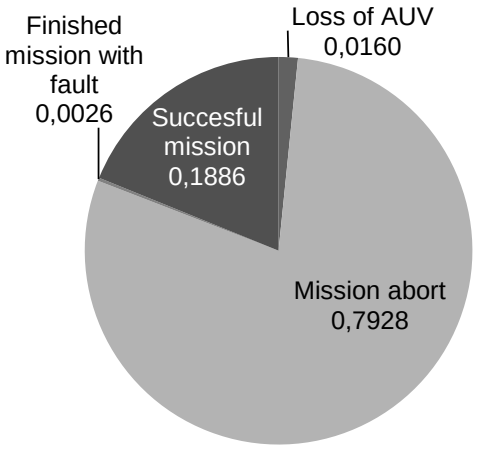


Figure 5.6.: Probabilities of mission outcomes

5.3. Risk treatment

5.3.1. Proposed measures

From the HRA assessment it became obvious that the operators have a need for better procedures. Looking at the experience/ training and the procedure PSF reveals the tasks

where the most problems are seen. The tasks that were identified have a rating in one of the PSF of low (training/ experience) or poor (procedures). This evaluation showed that there is need for more guidance in:

- Maintenance of the AUV, especially how to detect damages and repair these
- Planning of the mission in respect to
  - Consideration of local environmental loads on the vehicle, such as currents, etc.
  - Implementation of way points and mission path in Hydroid REMUS VIP - software
- Fault of the AUV recognition and solving them, during preparation and operation

Thus it is recommended to develop procedures and manuals which are adapted to the needs of the AUR Lab. For the last point, which includes solving of all faults previous to the mission and interpretation of fault messages during the mission, it is recommended to build on the experience of the whole team. A database or document should be created that includes the fault messages, their meaning and especially how to solve and handle the problem. This would increase the efficiency during preparation for deployment and facilitate this process. If all current operators are involved a wide knowledge base can be built and future operators can profit from this.

5.3.2. Reduced risk

HRA

For the mentioned events in tab. 5.5 the human error probabilities were re-assessed. For these events the corresponding PSF for procedures was reduced to 1. The table also shows the new human error probabilities and the reduction of probability. Some events were notably influenced with a reduction in probability by more than 10 %, whereas others were not influenced at all.

FTA

The newly found probabilities were used to update the existing fault trees. For the top event “Damaged AUV before deployment” the probability was reduced to 0,3303. This is a reduction of about 0,17. Thus it can be assumed a significant improvement. For the top event “AUV is set up wrongly” the probability was not reduced, this is discussed later.

Table 5.5.: Reassessed basic event probabilities of the HRA

Abb.	First assessment	Re-assessment	Reduction
AN	0,0658	0,0151	0,0507
DM	0,0350	0,0255	0,0095
DrD	0,1678	0,0465	0,1213
DrR	0,1906	0,0505	0,1402
DR	1,0000	1,0000	0,0000
DT	0,0030	0,0010	0,0020
FS	0,8030	0,8030	0,0000
LC	0,0748	0,0040	0,0708

ETA

By re-evaluation of the event trees the new probabilities for the aforementioned events were found. They are summarized in tab. 5.6. The complete revised trees can be found in appendix C.1.

Table 5.6.: Summary of the re-assessed fault trees

Event	Damage	Planning
Loss of AUV	$7{,}987{\cdot}10^{-6}$	$1{,}988{\cdot}10^{-5}$
Mission abort	0,3299	0,3282
Finished mission with fault	$3{,}913{\cdot}10^{-4}$	$1{,}969{\cdot}10^{-3}$

5.3.3. Risk evaluation

With the reassessed data the risk during a mission is now different. Fig. 5.7 shows the composition of probabilities for a mission. The probability of a successful mission is improved by a factor of about 1,5, while the other event probabilities were reduced significantly.

5.4. Risk framework

The risk framework for the AUR Lab was written in accordance with ISO 31000 (2009). It is designed as a living document. Fig. 5.8 summarizes the interconnections between the different actors and their roles in the system. The framework itself is the central point of the management. It is aid to clarify responsibilities, gives assistance in choice of methods and

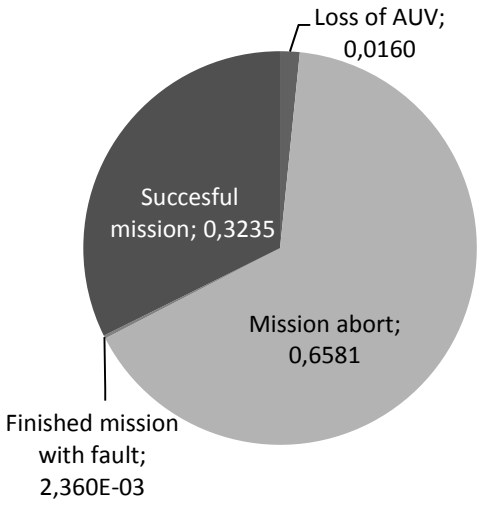


Figure 5.7.: Probabilities of mission outcome with implemented RCM

helps to record gained experience. A high emphasis was put on cooperation and communication within the AUR Lab. Such that decisions are made that have the support of all who are affected by it.

The main components of the risk management framework are listed below. The last two points should be regularly updated, so that gained experience is saved and accessible for others working with risk management. The framework document itself is at a point ready for review by the AUR Lab, due to time limitations that was not possible before completion of the thesis.

- Short overview over risk management vocabulary
- Implementation of the system
  - Clarification of roles
  - Communication and cooperation
  - Monitoring of risk and review of risk assessments
  - Review of the risk management system
- Risk assessment methodology
- Hazards and risks that should be considered

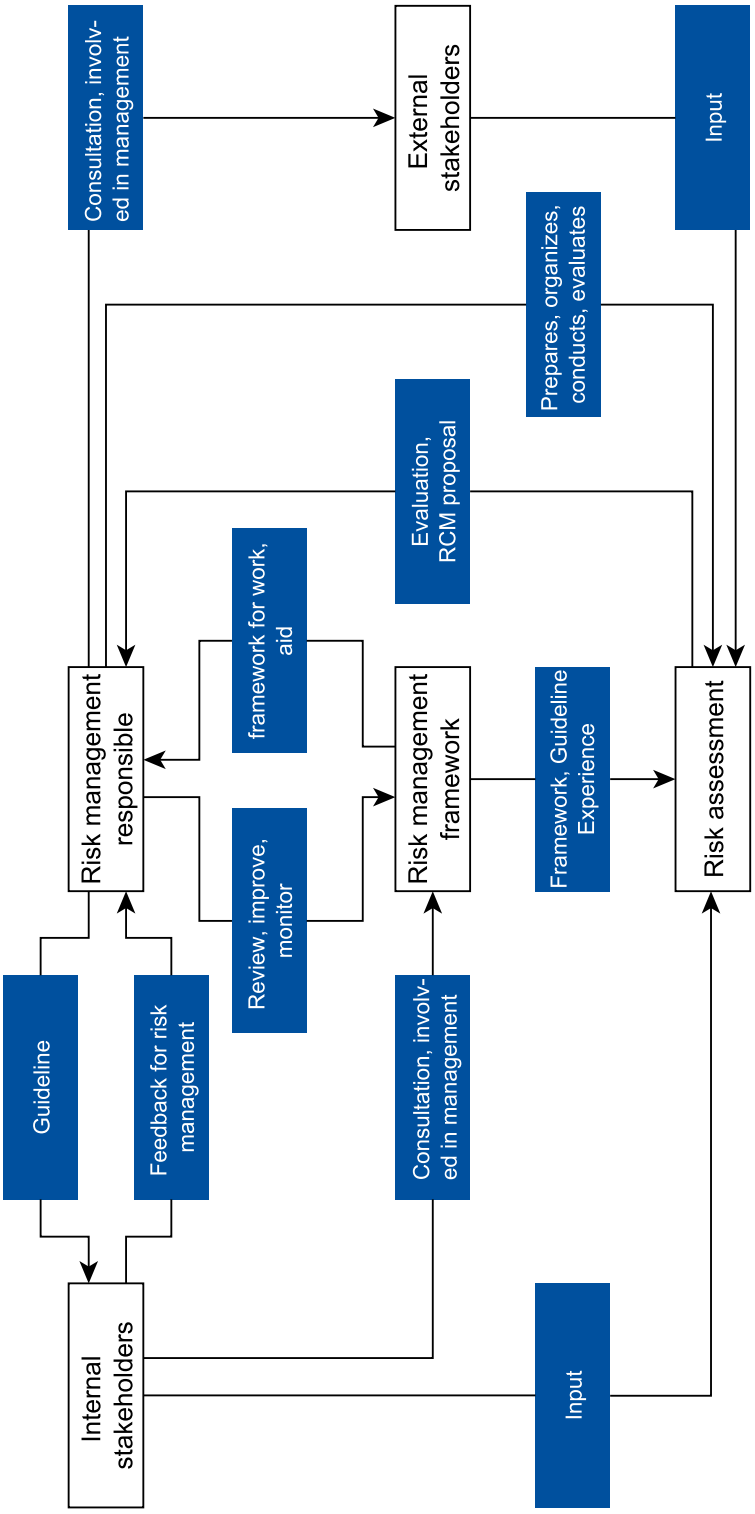


Figure 5.8.: Roles and links in the risk management system

6. Discussion and evaluation

In this chapter the results of the risk assessment will be discussed and evaluated.

6.1. Risk identification

The PHA revealed several possible hazardous events, but it can't be excluded that some events have not been identified. Through collaboration with personnel involved in operation, use of reported incidents and checklists the attempt was made to identify comprehensively all hazardous events. Thus it is believed that the identified events are, at least, the most relevant ones. The tables in the appendix contain events that are not further discussed here, such as loss of data. These events were identified when the scope was wider, which was eventually reduced to the scope presented here.

6.1.1. Risk analysis

Fault log evaluation

In general all logged messages have been evaluated. It cannot be excluded that faults which are not in the AUV's database were not recorded, since they were not recognized as such. Of the fault messages recorded some are mere status messages, which actually are not a fault, such as "Executing cmd from Digital Tx Bd: Run". It was found that only 13 of the recorded fault types were of significance for the safety of the vehicle. Fig 6.1 shows the observed number of these relevant faults.

It is notable that the faults no. 1, 2, 3 and 4 only occurred during the first mission, which was a test run, accustoming the operators with the vehicle. Thus the significance of these faults should not be overestimated, although they occurred quite frequently during the mission. Faults 18 and 19 only occurred during mission 7, faults 26 and 28 only occurred during missions 9 and 10 respectively.

The vehicle was stuck a total of 12 times in three missions, while the warning of low altitude was issued 166 times during almost all missions. This seems most alarming, since in almost 14 % of the cases the vehicle was stuck but, so far, always managed to resurface.

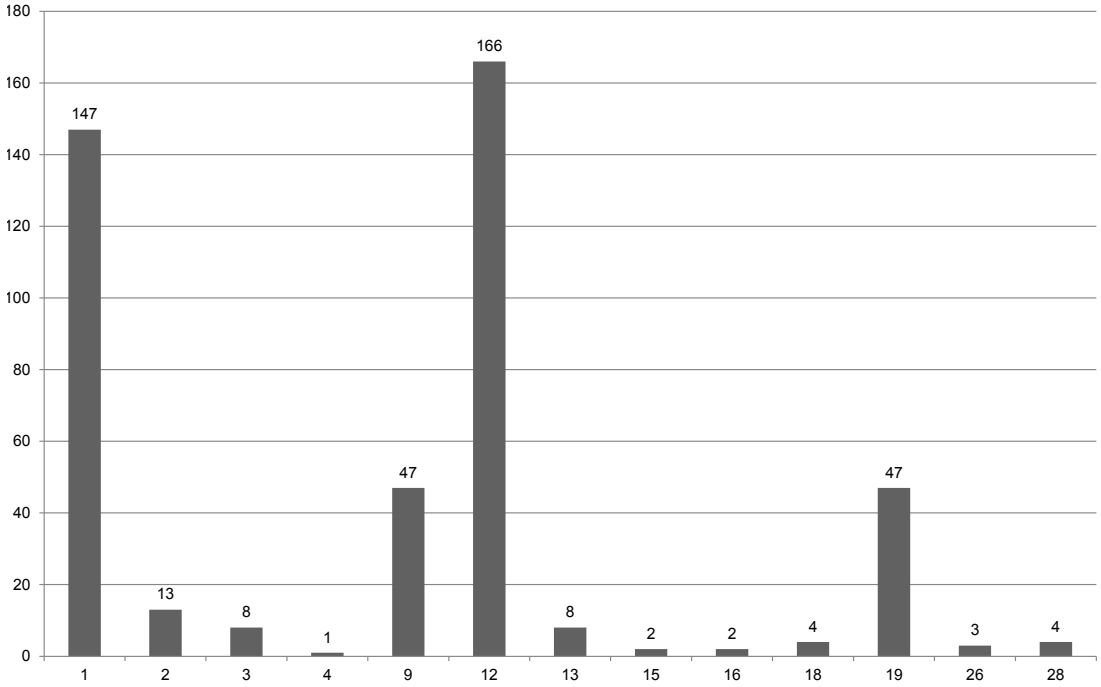


Figure 6.1.: Relevant recorded faults sorted by fault ID

Fault number 9 should also be kept in mind, the fault is relevant when the mission is depending on communication via iridium. This was the case during the seven missions in Spitsbergen, where the weather conditions did not allow a permanent monitoring with the tow fish. Faults 15 and 16 occurred as part of the mission plan, since the mission was continued until a certain battery level was reached, then it moved to the end position, here it is important, that the battery level is set high enough that there is enough time for recovery.

HRA

The judgments from the experts differ quite drastically in some events. This might have several reasons. As mentioned earlier there are some pitfalls connected with expert judgment, which might lead to an over- or underestimation of influences. As NUREG/CR-6883 (2005) states, it is possible to interpret the PSF differently. This might have occurred, indications were observed when clarifying some of the events. This is allowed, but distorts the HRA since not all PSF have the same weighting factors for the same weighting evaluation.

It is assumed that the averaging of the probabilities from the two experts reduces the uncertainty and the "true value" lies within these two values. Unfortunately only the first expert could finish the assessment, while the second could only assess half of the events. Thus the second half of the events might be more biased than the other events.

Another factor that influences the HRA assessment was the combination of action and diagnosis probabilities. The events FS and WP were assessed to have a failure probability of 1, which means that they will be carried out wrongly in every case. The method for combining diagnosis and action tasks in general is thought to be good. The description and combination of the single matrix cells should be changed, since they are not adequate in this case. In connection with the AUV this assessment will always lead to a total or high dependency. This might lead to a probability, which is overestimated by several magnitudes. The error introduced by the mentioned issues, cannot be quantified. It is assumed that it is significant, which might lead to a wrong focus during assessment of RCM, thus the focus for RCM was on the PSF, since those reflect where the users see most problems.

Expert estimation

The first evaluation by the experts individually should have been followed by a second group estimation. Due to time limitations and availability of the experts this was not possible. Only one expert submitted the worksheet back. A group discussion and assessment would have removed uncertainty and reduced bias, since the experts would have to find consensus. The expert, who submitted the probabilities had low or only middle confidence in his evaluation.

FTA

It is assumed that all important basic events were considered, while redundancy was avoided. Events that were not identified in the PHA, were not included. If hazards were missed, this mistake could not be corrected.

Concerning the result from the FTA some remarks should be made. Firstly it is notable that in the fault tree for "Wrongly set up vehicle" the top event probability is solely determined by the basic event RF. This results from the structure of the tree. Only one "and-gate" is included, which makes RF a part of every minimal cut set. The other events sum up to a higher failure probability than 1. Already the basic events FS and WP have $F(t) = 1$ and will always occur. Thus only RF is important for the top event probability. This circumstance can be accounted for by the high event probabilities derived from the HRA, as discussed earlier.

Similarly, the top event probability for the fault tree "Damaged AUV before deployment" is governed by the sum of all basic events which are not DR. The basic event DR has a failure probability of 1, which results from the HRA assessment. Almost all basic events in the Fault trees were modeled by HRA. Accordingly the HRA assessment has a significant influence on the top event probabilities. The uncertainty connected with the HRA results therefore in an accumulation of uncertainty in the FTA.

ETA

For the ETA it is assumed that the interconnections were modeled sufficiently. A compromise was taken between many events and a high number of branches, and few events, which might not reflect real operation sufficiently. In the ETA both HRA and expert estimation have been used to assess the probabilities. Here the uncertainties of both have a huge influence since they multiply with each step. The results have therefore to be seen skeptical. It is assumed that the proportion between loss of the vehicle and mission abort is realistic, whereas the end result is assumed to be too high. This is discussed next.

Risk evaluation

The risk quantification presented here, has to be beheld with care. As mentioned, the basic event probabilities are not of high confidence. The confidence interval is hard to determine in this case. All the methods applied were new to most of the participants and not much experience had been obtained, in relation to operation and handling of the AUV. In the offshore industry this would be unsatisfying, but since this thesis represents a demonstration of methods and overall principle, it is assumed to be acceptable. Interpretations that are made from the results should be considered carefully.

Regarding the whole risk picture, the probability of loss is within the bounds given by the pessimist and optimist estimation of Griffiths et al. (2009). The contribution from ETA and FTA to the risk of loss is comparably low to the risk indicated by the authors. Griffiths et al. (2009) also stated that the pessimist estimation is probably too low. Because the probabilities were just averaged from optimist and pessimist estimation, it can be assumed that the risk of loss is overestimated.

The probability of mission abort is found to be too high, to reflect real operation. The estimation suggests that about 79 % of the missions will be aborted. So far, during 12 missions conducted, only one was aborted (the AUV was too far away from the planned path). This is not a statistically satisfying number of missions conducted, but the literature on AUV supports this as realistic. These high probabilities can be accounted for by too high probabilities which resulted from the FTA and were the basis for the ETA.

6.2. Risk treatment

For the risk treatment suggestions measures have been selected where the operators saw most difficulties. Thus it is assumed that the reassessment of probabilities by the experts

themselves would have led to a similar result. What was not included was the expected experience gain in the next months and years of operation. This will supposedly lead to an additional reduction of basic event probabilities, since PSF would be evaluated differently and with lower uncertainty. This is especially valid for the HRA, but also an expert estimation will gain a higher confidence and resulting in a higher quality of the assessment.

In general it is assumed that improved guidance will reduce the risk in the areas mentioned. The quantification of this gain is difficult due to the lack of reliable data, as was mentioned earlier. But resulting from the re-assessment a high reduction in risk can be expected. With the probabilities assessed here mission success would increase by about 15 %. This is supposedly still too low but it shows that a risk reduction is likely.

6.3. Risk framework

The risk framework as described, as result of the executed risk assessment, is to be seen as a guideline. The framework still needs to be reviewed by the decision makers of the AUR Lab. So far, all people involved have little experience in risk management and risk assessments, thus an experience base has to be built. This is reflected in the contents of the framework documents, which summarizes experiences made and makes suggestions for the future. It is assumed that the framework is a good starting point to introduce a risk management system in the AUR Lab.

7. Conclusion

This thesis aims at presenting a risk management process for the REMUS 100 of the AUR Lab at NTNU. It is based on a previously carried out risk assessment, also described in this thesis. It is believed that a well implemented risk management helps to facilitate operation, makes it safer, reduces the probability of loss and improves the overall efficiency of operation.

The risk assessment carried out is one of the first to link HRA with AUV operation in order to find the risk of these operations. Only two aspects of risk in AUV operation are analyzed, assessments with different aims might help to identify further risk contributors and eliminate them consequently. From the results of the risk assessment it can be concluded that in the current operations there is need for new or improved procedures. The procedures should aim towards maintenance, fault detection and solving and mission planning. More precisely formulated measures and improvements are presented in the recommendations.

Although the total risk presented here seems to be too high, it is assumed that the methods are used correctly. Most are well proven while some are only simplified adaptations, due to a lack of time and experience. Due to the absence of statistical satisfying data the assessment is based on estimation methods. The standard methods PHA, ETA and FTA seem suitable for this case. Expert estimation is also a tool, which is very suitable for these kinds of assessments. It is reckoned that the SPAR-H HRA might not be as suitable as was assumed initially. Despite the shortcomings mentioned it is assumed that the methods used herein are a good starting point for application in further assessments. Accordingly a gain in experience will also help to improve use of the methods and simplify the whole assessment process.

From the fault log evaluation one can conclude that the faults that occurred so far, except when the vehicle was stuck, are often not critical. But it should be the aim, to find root causes for all of these faults and eliminate them as far as possible.

8. Recommendations and further work

8.1. Further work on the risk management for the AUR Lab

For the risk management presented here to be successful all affected parties have to be involved in and convinced of the advantages of the risk management system. Key personnel in the AUR Lab has to be committed and willing to invest time to make it an efficient tool. For this purpose it is recommended to appoint a risk management responsible. This person should prepare, conduct, review and involve all relevant people in risk management. He should also ensure that all relevant risks are covered and new hazards and risks are identified.

Only two elements of risk have been analyzed here. Thus it is recommended that future risk assessments cover the following outcomes: loss of life, damage to health, damage to the environment, damage to assets belonging to the AUR Lab and damage to assets of third party people. A more detailed list of possible outcomes of concern and hazards is presented in the risk framework document.

In general, it is assumed that the methods proposed here, such as ETA, FTA, PHA, HRA, etc., can be used, but some comments in respect to their use will be made. For the HRA it is recommended to find a better method to model dependency between action and diagnosis. Additionally the PSF should be described adapted to the vocabulary and circumstances of AUV operation. These two aims can be achieved by using a different, more generic method or by adapting the method which was used here.

From the HRA it can be seen that the operators of the AUV need more guidance in:

- Maintenance of the AUV, especially how to detect damages and repair these
- Planning of the mission in respect to
  - Consideration of local environmental loads on the vehicle, such as currents, etc.
  - Implementation of way points and mission path in Hydroid REMUS VIP - software
- Fault of the AUV recognition and solving them, during preparation and operation

Thus it is recommended to develop procedures and manuals which are adapted to the needs of the AUR Lab. These should be written both in English and Norwegian, in this misunderstandings can be partly avoided. For the last point, which includes solving of all faults previous to the mission and interpretation of fault messages during the mission, it is recommended to build on the experience of the whole team. A database or document should be created that includes the fault messages, their meaning, how to solve the fault and behavioral advice. This would increase the efficiency during preparation for deployment and facilitate this process. If all current operators are involved, a wide knowledge base can be built and future operators can profit enormously.

The fault logs revealed that a lot of failure messages are generated during one mission. Thus the AUR Lab should monitor the fault logs, find the basic reasons for faults and try to eliminate them as far as possible. This will not only reduce the number of fault messages but also help in the process of setting up the vehicle for a mission. This also complies with record keeping of experience, mentioned above.

Two more things that were seen from the fault log evaluation shall be highlighted. Firstly if steep terrain is expected, a higher altitude over ground should be selected, in order to avoid contact with the seabed. Secondly it should be assured that the mission abort voltage is chosen high enough, so that enough time is available to recover the AUV. This time strongly dependents on the conditions at the site and environmental influences and thus should be decided individually for each mission at the site.

8.2. Data availability

As became obvious from the beginning and throughout the risk assessment only few statistical data for AUV reliability is available. Judgment from experts can also be difficult, especially when little experience with judgment processes and the operation to be judged is available. One idea that was already expressed earlier by others is a common database for AUV faults and incidents. In this respect an anonymous web based system for the REMUS 100 AUV could be imagined . There is a large group of users of this AUV, thus all could benefit from the common experience. Incidents, such as loss or major damages, could be reported and together with some measure of total or relative operation time lead to statistical significant data for quantitative risk assessment. The system could be similar to the OREDA offshore reliability database or the sea-web accident database. Setting up this database would require a lot of effort from all parties, but likewise all could profit from it.

Bibliography

AMOS. Homepage amos, 2013. URL `http://www.ntnu.edu/amos/about-amos`. accessed 20.02.2014.

Gianluca Antonelli, Thor I. Fossen, and Dana R. Yoerger. Underwater robotics. In Bruno Siciliano and Oussama Khatib, editors, *Springer Handbook of Robotics*, pages 987–1008. Springer Berlin Heidelberg, 2008. ISBN 978-3-540-23957-4. doi: 10.1007/978-3-540-30301-5_44.

X. Bian, C. Mou, Z. Yan, and J. Xu. Reliability analysis of auv based on fuzzy fault tree. In *2009 IEEE International Conference on Mechatronics and Automation*, pages 438–442, Changchun, 2009a. ISBN 9781424426935. doi: 10.1109/ICMA.2009.5246655.

X. Bian, C. Mou, Z. Yan, and J. Xu. Simulation model and fault tree analysis for auv. In *Mechatronics and Automation, 2009. ICMA 2009. International Conference on*, pages 4452–4457, 2009b. doi: 10.1109/ICMA.2009.5246716.

A. Brighenti. Parametric analysis of the configuration of autonomous underwater vehicles. *Oceanic Engineering, IEEE Journal of*, 15(3):179–188, 1990. ISSN 0364-9059. doi: 10.1109/48.107146.

M. Brito, G. Griffiths, J. Ferguson, D. Hopkin, R. Mills, R. Pederson, and E. MacNeil. A behavioral probabilistic risk assessment framework for managing autonomous underwater vehicle deployments. *Journal of Atmospheric and Oceanic Technology*, 29(11):1689–1703, 11 2012. URL `http://search.proquest.com/docview/1270170849?accountid=12870`.

M.P. Brito and G. Griffiths. A markov chain state transition approach to establishing critical phases for auv reliability. *Oceanic Engineering, IEEE Journal of*, 36(1):139–149, 2011. ISSN 0364-9059. doi: 10.1109/JOE.2010.2083070.

Mark Burgman, Fiona Fidler, Marissa McBride, Terry Walshe, and Bonnie Wintle. Eliciting expert judgments: Literature review. Literature Review, Project Report 1, ACERA, University of Melbourne, 2006.

Thomas S. Chance. Auv surveys - extending our reach, 24000 km later. In *Proceedings UUST 2003*, New Hampshire, 2003. AUSI.

Robert D. Christ and Robert L. Wernli Sr. *The ROV Manual*. Butterworth-Heinemann, Oxford, 2007. ISBN 978-0-7506-8148-3. doi: http://dx.doi.org/10.1016/B978-075068148-3/50006-2.

G. Griffiths and M. Brito. Predicting risk in missions under sea ice with autonomous underwater vehicles. In *Autonomous Underwater Vehicles, 2008. AUV 2008. IEEE/OES*, pages 1–7, 2008. doi: 10.1109/AUV.2008.5290536.

G. Griffiths and A. Trembanis. Towards a risk management process for autonomous underwater vehicles. In G. Griffiths and Collins, editors, *Proceedings of a Masterclass on AUV Technology for Polar Science*, pages 103–118, London, 2007. Society for Underwater Technology.

G. Griffiths, N. W. Millard, S. D. McPhail, P. Stevenson, and P. G. Challenor. On the reliability of the autosub autonomous underwater vehicle. *Underwater Technology*, 25(4): 175–184, 12 2003. URL `http://search.proquest.com/docview/20643183?accountid=12870`.

G. Griffiths, N. Bose, J. Ferguson, and D. R. Blidberg. Insurance for autonomous underwater vehicles. *Underwater Technology*, 27(2):43–48, 06 2007. URL `http://search.proquest.com/docview/20646318?accountid=12870`.

G. Griffiths, M. Brito, I. Robbins, and M. Moline. Reliability of two remus-100 auvs based on fault log analysis and elicited expert judgment. In *Proceedings of the International Symposium on Unmanned Untethered Submersible Technology (UUST 2009), Durham, New Hampshire, 23-26 August 2009*, page [12p]. Autonomous Undersea Systems Institute (AUSI), Durham NH, USA, 2009. URL `http://nora.nerc.ac.uk/169184/`. Proceedings issued on CDROM.

HMSR-07. *HMSR-07: Fieldwork, field-course, research cruise, on-site inspection and excursion*. Norges teknisk-naturvitenskapelige universitet HSE, 2006. URL `http://www.ntnu.edu/hse/guidelines/d`.

LLC Hydroid. *REMUS 100 Autonomous Underwater Vehicle*. Kongsberg, 2013. URL `http://www.km.kongsberg.com/hydroid`.

C.C. Insaurralde and D.M. Lane. Autonomy-assessment criteria for underwater vehicles. In *Autonomous Underwater Vehicles (AUV), 2012 IEEE/OES*, pages 1–8, 2012. doi: 10.1109/AUV.2012.6380746.

ISO 31000. Iso 31000 risk management - principles and guidelines, 2009.

ISO 8402. Quality management and quality assurance – vocabulary, 1994. URL `http://www.nb.no/nbsok/nb/71378921220b3e7ac883d9b9cf7457ca.nbdigital;jsessionid=37283AB7F2628CDCAEA2401211CC679C.nbdigital1?lang=no#49`. Replaced by ISO 9000:2000.

W.J. Kirkwood. Auv incidents and outcomes. In *OCEANS 2009, MTS/IEEE Biloxi - Marine Technology for Our Future: Global and Local Challenges*, pages 1–5, 2009.

J.E. Manley. The role of risk in auv development and deployment. In *OCEANS 2007 - Europe*, pages 1–6, 2007. doi: 10.1109/OCEANSE.2007.4302219.

NFA. Autonomous systems: Opportunities and challenges for the oil & gas industry. Technical report, Norwegian Society of Automatic Control, 2012.

NORSOK Z-013. Risk and emergency preparedness assessment, 2010.

NORSOK Z-016. Regularity Management and Reliability Technology, 1998.

NUREG/CR-6883. The spar-h human-reliability analysis method, 2005. D. Gertman, H. Blackman, J. Marble, J. Byers, C. Smith.

T.K. Podder, M. Sibenac, H. Thomas, W.J. Kirkwood, and J.G. Bellingham. Reliability growth of autonomous underwater vehicle-dorado. In *OCEANS '04. MTTS/IEEE TECHNO-OCEAN '04*, volume 2, pages 856–862 Vol.2, 2004. doi: 10.1109/OCEANS.2004.1405576.

E. Raugel, V. Rigaud, and C. Lakeman. Sea experiment of a survey auv powered by a fuel cell system. In *Autonomous Underwater Vehicles (AUV), 2010 IEEE/OES*, pages 1–3, 2010. doi: 10.1109/AUV.2010.5779676.

M. Rausand. *Risk Assessment - Theory, Methods, and Applications*. Wiley, 1. edition, 2011. Hoboken.

Marvin Rausand and Arnljot Høyland. *System reliability theory - Models, statistical methods and applications*. Wiley series in probability and statistics. Wiley & Sons Inc., Hoboken, New Jersey, 2. edition, 2004.

US Navy. The navy unmanned undersea vehicle (uuv) master plan. Technical report, United States of America Department of the Navy, November 2004.

Cilia Witteman and Silja Renooij. Evaluation of a verbal-numerical probability scale. *International Journal of Approximate Reasoning*, 33(2):117 – 131, 2003. ISSN 0888-613X. doi: http://dx.doi.org/10.1016/S0888-613X(02)00151-2.

A. Wolek, J. Burns, C. Woolsey, J. Quenzer, L. Techy, and K. Morgansen. A maneuverable, pneumatic underwater glider. In *Oceans, 2012*, pages 1–7, 2012. doi: 10.1109/OCEANS.2012.6404989.

Hongli Xu, Guannan Li, and Jian Liu. Reliability analysis of an autonomous underwater vehicle using fault tree. In *Information and Automation (ICIA), 2013 IEEE International Conference on*, pages 1165–1170, Aug 2013. doi: 10.1109/ICInfA.2013.6720471.

I. Yamamoto, T. Aoki, S. Tsukioka, H. Yoshida, T. Hyakudome, T. Sawa, S. Ishibashi, T. Inada, K. Yokoyama, T. Maeda, S. lshiguro, H. Hirayama, K. Hirokawa, A. Hashimoto, N. Hisatome, and T. Tani. Fuel cell system of auv "urashima". In *OCEANS '04. MTTS/IEEE TECHNO-OCEAN '04*, volume 3, pages 1732–1737 Vol.3, 2004. doi: 10.1109/OCEANS.2004.1406386.

J. Yuh, S. K. Choi, C. Ikehara, G. H. Kim, G. McMurty, M. Ghasemi-Nejhad, N. Sarkar, and K. Sugihara. Design of a semi-autonomous underwater vehicle for intervention missions (sauvim). In *Underwater Technology, 1998. Proceedings of the 1998 International Symposium on*, pages 63–68, 1998. doi: 10.1109/UT.1998.670059.

J. Yuh, G. Marani, and D.R. Blidberg. Applications of marine robotic vehicles. *Intelligent Service Robotics*, 4(4):221–231, 2011. ISSN 1861-2776. doi: 10.1007/s11370-011-0096-5.

A. Risk identification - PHA

In the following pages the PHA sheets that were filled out during the assessment are presented.

Study Object: REMUS 100 **Phase:** Storage/ Transport **Date:** 2014-03

Name/s: Ch. Thieme

System element / activity	No.	Hazard/ threat	Hazardous event (what, where, when)	Cause (triggering event)	Consequence	Risk			Risk Reducing measure	Comment
						Freq	Cons	RPN		
Storage	1-1	Potential Energy	AUV falls from table during/ between maintenance	Insecure position	External and internal damage, damage to health	3	2	5	Stable position	
Storage/ maintenance	1-2	Potential Energy	AUV falls during moving to/ from maintenance	Stumbling, carelessness, slippery case	External and internal damage, damage to health	5	2	7	Clear way to walk in advance, wear clothes, ensure oil free case	
Storage	1-3	Thermic Hazard	AUV battery ignites during storage	Bad contacts, water in AUV, wrong charging, short circuit	External and internal damage, loss of AUV, damage to health, loss of other assets	1	3	4	Regular inspections, charge and discharge on recommendation	Constant hazard in all phases
Storage	1-4	Moved turn-off magnet	Battery drains during storage	Vibration, shock, bad/ forgot to position	AUV not operable when needed	4	2	6	Check magnet before storage, check AUV several days before usage	
Storage/ Maintenance	1-5	Less than adequate maintenance	AUV is in bad condition/ damaged when needed	Maintenance is inadequate or carried wrongly	External and internal damage	4	2	6	Verify maintenance by second technician, follow instructions, training, recording experience,	
Transport	1-6	Kinetic energy	AUV bumps into objects during transport with crane	Carelessness during crane operation, bad visual estimation, crane malfunction	External and internal damage, loss of AUV, damage to health	4	3	7	Approved crane operators, guides for assistance, AUV safely secured in case, no hurry in loading operation	Crane lifting on/ off board, rarely the case
Transport	1-7	Potential Energy	AUV dropped during manual transport on vessel	Stumbling, carelessness, slippery case, slippery gangway	External and internal damage, loss of AUV, damage to health	4	3	7	Clear way to walk in advance, wear clothes, ensure oil free case, precautions walking when slippery gangway	In case

Storage/ transport	1-8	Material degradation	Parts loosened during transport with car, vessel, etc.	Degradation, vibration, internal corrosion	Internal damages, bad electric conduction	2	2	4	Adequate maintenance	Transport to destination
Transport	1-9	Kinetic energy	AUV is subjected to shock during transport with car, vessel, etc.	Carelessness handling, insecure positions	Internal and external damages	2	2	4	Secure AUV good in case	In case

Study Object: REMUS 100 **Phase:** Preparation and Deployment **Date:** 2014-03

Name/s: Ch. Thieme

System element / activity	No.	Hazard/ threat	Hazardous event (what, where, when)	Cause (triggering event)	Consequence	Risk			Risk Reducing measure	Comment
						Freq	Cons	RPN		
Preparation	2-1	Interaction Hazard	Wrong mission parameters are implemented during preparation	Wrong programming, short time, misunderstand-ing between people involved, unclear procedures	Loss of AUV, stranding of AUV, premature mission abort, no collection of data	5	3	8	Validate programming and mission parameters, run test checks, training in programming, monitoring of vehicle at the beginning of mission	
Preparation	2-2	Stability	AUV is not correctly ballasted for operation	Wrong, insufficient ballasting	Loss of AUV, mission abort, insufficient diving depth	4	3	7	Control weight of AUV before deploying, check for density of water in target area	
Preparation	2-3	Interaction Hazard	Software containing errors is implemented	Insufficient AUV software	Loss of AUV, unexpected AUV behaviour	3	3	6	Check software, simulation, validation by other people	
Preparation	2-4	Bad weather	AUV is damaged during preparation	Vessel severely moves	Damages to AUV, loss of AUV, mission abort	4	3	7	Preparations conducted in controlled environment, cruise abort	
Deployment	2-5	Bad weather	Deployment is not possible	Storm, bad conditions	Mission not started	3	2	5	Verify weather beforehand, reschedule if necessary	
Deployment	2-6	Potential energy	AUV dropped during deployment	Slippery, mishap	Severe damages to AUV, cruise abort	4	2	6	Careful handling	
Deployment	2-7	Bad weather	AUV has contact with vessel after deployment	Heavy sea	Severe damages to AUV, loss of AUV, mission abort	4	3	7	Launch off thrusters, don't launch above recommended sea state	
Preparation	2-8	Interaction Hazard	Pre-test is passed with undetected fault	Undetectable faults	Loss of vehicle, unplanned behaviour, mission not successful	2	3	5	Visual inspection, following instructions, on land test runs, proper maintenance	

Preparation Deployment	2-9	Thermic Hazard	AUV battery ignites during preparation/ deployment	Bad contacts, water in AUV, wrong charging, short circuit	External and internal damage, loss of AUV, damage to health, loss of other assets	1	3	4	Regular inspections, charge and discharge on recommendation	Constant hazard in all phases
Preparation Deployment	2-10	Potential energy	Fins or propeller damaged during handling	Mishaps	Small damages	4	1	5	Handle with care, two to carry it, have easy spare parts ready	
Preparation	2-11	Interaction Hazard	Faults are not correctly eliminated during preparation	Complex interaction, few experience, unclear fault description	Unplanned behaviour, mission failure	3	3	6	Careful elimination of all faults, test runs	
Preparation	2-12	Human error	Mission is planned without considering capabilities of AUV	Bad knowledge, few experience, mishap, disregard	Unplanned behaviour, AUV grounds, loss of AUV, AUV travels further than expected	2	3	5	Consider limits of the vehicle, re-evaluate mission after planning	

Study Object: REMUS 100 **Phase:** Mission and mission start **Date:** 2014-03

Name/s: Ch. Thieme

System element / activity	No.	Hazard/ threat	Hazardous event (what, where, when)	Cause (triggering event)	Consequence	Risk			Risk Reducing measure	Comment
						Freq	Cons	RPN		
Mission	3-1	Kinetic energy	Collisions with other vessel	Vessel not aware of AUV, near surface mission	Severe damage to AUV, loss of AUV, mission abort	2	3	5	Make other vessels aware of AUV when in near surface mission	
Mission	3-2	Short circuit	Short circuit during mission	Bad connections internally	Loss of vehicle, mission is aborted	2	3	5	Checks and internal control algorithm, redundancy, self-check, monitoring for anomalies	
Mission	3-3	Interaction Hazard	Unexpected and unwanted behaviour during mission	Wrong programming variousreasons from before	Loss of vehicle, no data collection	4	3	7	Monitor the AUV at beginning, test beforehand	
Mission	3-4	Kinetic energy	AUV gets stuck in seabed	Wrong depth parameters	Loss of vehicle	2	3	5	Use depth over seafloor function	
Mission	3-5	Environ-mental hazard	AUV can not follow pre-programmed way	Strong currents	Mission not successful, difficult retrieval	2	2	4	Estimate currents in target area	
Mission	3-6	Thermic Hazard	AUV battery ignites during mission	Bad contacts, water in AUV, wrong charging, short circuit	External and internal damage, loss of AUV, damage to health, loss of other assets	1	3	4	Regular inspections, charge and discharge on recommendation	Constant hazard in all phases
Mission	3-7	Kinetic energy	AUV does not follow path	Wrongly programmed way points, strong currents, failure in navigational system, insufficient GPS fix, wrong map datum	Loss of vehicle, severe damages to vehicle, loss of data, mission unsuccessful	3	3	6	Checks and internal control algorithm, redundancy, self-check, monitoring for anomalies	

Mission	3-8	Interaction Hazard	Mission data not recorded	Fault in data memory	Loss of data, mission unsuccessful	2	2	4	Check memory beforehand, test, get positive confirmation of recording	
Mission	3-9	Interaction Hazard	Mission data not recorded	Fault in sensors	Loss of data, mission unsuccessful	2	1	3	Check sensors and recording on pre-dive check, get positive confirmation of recording	
Mission	3-10	Interaction Hazard	AUV gets stuck under ice	No ice sensor, sudden ice coverage, wrong paths	Loss of vehicle, time delay in retrieval	2	3	5	Check for ice coverage, implement ice detection	
Mission	3-11	Interaction Hazard	System failure during mission	Internal fault of control system, fault detection acts	Loss of AUV, mission abort	1	3	4	Mission test runs before mission, solve faults already diagnosed	
Mission start	3-12	Interaction Hazard	Mission is immediately aborted due to internal error	Internal fault, fault detection acts	Mission abort	2	2	4	Mission test run, eleminate faults before mission	

Study Object: REMUS 100 **Phase:** Retrieval and post-dive **Date:** 2014-03

Name/s: Ch. Thieme

System element / activity	No.	Hazard/ threat	Hazardous event (what, where, when)	Cause (triggering event)	Consequence	Risk			Risk Reducing measure	Comment
						Freq	Cons	RPN		
Post dive activity	4-1	Potential energy	AUV dropped after retrieval	Slippery AUV	Sever damage to AUV	4	2	6	Wear gloves	
Post dive activity	4-2	Interaction Hazard	Failure while downloading data	Wrong interaction with AUV	Loss of data	2	2	4	Follow procedures, act cautiously and not hectic, training in use of software	
Retrieval	4-3	Bad weather	AUV not able to be picked up	Strong currents/ heavy sea	Loss of AUV, damages, AUV strands	3	3	6	Check weather forecast, only deploy if conditions allow safe retrieval, abort mission if weather deteriorates	
Retrieval	4-4	Bad weather	AUV has contact with vessel during attempt to retrieve	Heavy sea	Severe damages to AUV, loss of AUV, mission abort	3	2	5	Launch off thrusters, don't launch above recommended sea state	
Retrieval and post dive activity	4-5	Thermic Hazard	AUV battery ignites during this phase	Bad contacts, water in AUV, wrong charging, short circuit	External and internal damage, loss of AUV, damage to health, loss of other assets	1	3	4	Regular inspections, charge and discharge on recommendation	Constant hazard in all phases
Retrieval	4-6	Interaction Hazard	AUV can not be seen in order to retrieve it	Wrongly programmed parameters, AUV is somewhere else, wrong ballasting	Loss of AUV delay of mission progress	3	3	6	Check mission parameters and validation by 2nd person	
Retrieval and post dive activity	4-7	Potential energy	Fins or propeller damaged during handling	Mishaps	Small damages	4	1	5	Handle with care, prepare for pick up	
Post dive activity	4-8	Interaction Hazard	Deleting data previous to download	Mishap, missing training	Loss of data	3	2	5	Follow procedures, training	

B. Risk analysis

B.1. HRA supplementary material

Table B.1.: Dependency condition table (NUREG/CR-6883, 2005)

Condition Number	Crew (same or different)	Time (close in time or not close in time)	Location (same or different)	Cues (additional or no additional)	Dependency	Number of Human Action Failures Rule ☐ - Not Applicable. Why?_____
1	s	c	s	na	complete	When considering recovery in a series e.g., 2nd, 3rd, or 4th checker If this error is the **3rd error in the sequence**, then the dependency is at least **moderate**. If this error is the **4th error in the sequence**, then the dependency is at least **high.**
2				a	complete	
3			d	na	high	
4				a	high	
5		nc	s	na	high	
6				a	moderate	
7			d	na	moderate	
8				a	low	
9	d	c	s	na	moderate	
10				a	moderate	
11			d	na	moderate	
12				a	moderate	
13		nc	s	na	low	
14				a	low	
15			d	na	low	
16				a	low	
17					zero	

B.2. Summary fault log analysis

In the following table all the faults are listed with a description. Some of the descriptions were taken directly from Griffiths et al. (2009), these passages are explicitly marked.

Fault log evaluation summary

Fault #	Text	Description of fault	no. of faults	Source for description
1	The ADCP is not sending water current data. Either WP=0, or faulty ADCP firmware.	ADCP not sending data	147	
2	Battery #0:Internal voltage ref out of range,	-	13	
3	Warning! Depth offset is -12.3 meters, expecting about -10.5	-	8	
4	Warning! REMUS is drawing 104.0 watts, more than expected 95.0 watts	More then expected maximum power consumption is observed.	1	
5	Fix needed: Get fix objective	AUV didn't receive a position fixing signal, thus going to surface, getting a GPS fix	48	
6	PP CMD: ID = 156 Len = 2, data[0]= 0xC1, data[1]= 0x80, total len = 416	-	21	
7	Vehicle stuck on surface; attempting to drive it down	Delay in vehicle dive due to buoyancy (10-20s), no affect on mission. Sea conditions/buoyancy may prevent vehicle diving first time. If so, vehicle tries again using a 'porpoise' mode.	52	Griffith et al 2009
8	Self test failure attitude (tilt), [80000010] pausing mission	Vehicle rolled to side after trying to avoid bottom, everything okay. Vehicle uses combined ADCP beams as altimeter. When sensed as too close to bottom vehicle pitches up and propeller stops, the tilt is therefore outside normal limits. When vehicle assumes proper attitude, propeller starts and mission continues.	537	Griffith et al 2009
9	No response from Iridium to command ATH0	AUV is trying to send messages via iridium, no response, most of the failures occured when the Iridium transmitter was not used on the cruise	47	
10	Warning compass bias table entry is excessive (-12.2 deg). Suggest deleting (line 8)	When AUV losses track of the bottom, the reference speed is missing and IMU is producing faults	537	
11	Ignoring commanded fix (Get fix objective), vehicle depth (62.9) is greater than max fix depth (60.0)	Depth is exceeding the maximum depth to get a fix, thus no fix is obtained	2	
12	Vehicle at low altitude. Executing emergency climb	Executing emergency climb, too close to bottom, hit bottom and bounced. Controlled climb only good to 10° pitch, to get more than that propeller is stopped.	166	Griffith et al 2009

13	Vehicle stuck on bottom, attempting to float free	Vehicle drove it into seafloor or got entangled into near floor objects and can't move satisfactically anymore.	8	
14	Warning: Verify transponder range test disabled in mission file, line 163	Transponder range test was disabled, AUV asks for verification of this circumstance	2	
15	Batteries below abort to end cut-off (18.9 percent left). Redirecting to endpoint	Batteries are drained below threshold, mission is aborted and recovery intiated.	2	
16	Executing cmd from Batteries: Abort to end position	Command is result of fault 15, mission is ended if battery is drained to a certain level	2	
17	Calibration Score, keeping old offsets! var = 2.2, X = -9, Y = -199, Z = -217	Calibration variables of Sidescan 0	2	
18	Thruster motor controller fault	A fault in the thruster controller is found. Expected behaviour is not equal to observed bahaviour.	4	
19	Self test failure thruster, [A1020080] pausing mission	Thruster is not behaving as intended, selftest to check for problems	47	
20	Ignoring stbd vel of 0.42 at altitude of 0.73 (1)	Starboard sidescan sonar gives an implausible hieght, which is ignored.	3	
21	Objective Navigate timed out, aborting mission	AUV is too far away from next target, when getting a fix, AUV aborts mission and waits for retrieval	1	
22	Executing cmd from Digital Tx Bd: Abort to end position!	Mission is ended, number of legs intended is fulfilled, AUV moves to the indicated end position	2	
23	Executing cmd from Digital Tx Bd: Abort mission now!	AUV is at the end position and mission is aborted directly	7	
24	Executing mission from VIP Run button	Mission is started from the Laptop via a wireless connection	12	
25	Rx'd command 128 from digital transponder while modem transmitting, ignoring	AUV received a command from digital transpinder which is ignored, since it is sending.	2	
26	TNT compass checksum error! <rcvr=,N,56.9,4166*34	Internal compass calculates a wrong check sum, happened when the AUV was in its box turned on for too long	3	
27	Warning, sidescan range set to 50 M, altitude 10.0 M; recommend altitude of 5.0 M.	Recommendation to lower hight over seafloor, to adapt to the sidescan SONAR range	2	
28	Vehicle at bollard (stuck!). Expecting 139.1 watts, drawing 181.9 watts. Attempting to float free	Vehicle is stuck, excessive Energy usage was the indicator	4	
29	Executing cmd from Digital Tx Bd: Run	AUV starts on mission after all pretests in water are done and a GPS fix was obtained	5	

B.3. Detailed HRA summary

In the following the detailed summary of the HRA from the experts is presented. It includes all assessed probabilities, dependency assessments and calculations.

Abb.	PSFs								HEP	P_w/od	Dependency					P_w/d
	Time	Stress	Comp-lexity	Experience/ Training	Proced-ures	Ergo./ HMI	FfD	Work Process			Crew	Time	Loc.	Cues	LoD	
AN	-	-	-	-	-	-	-	-	-	1,305E-01	-	-	-	-	-	1,305E-01
	10	1	2	3	5	1	1	0,5	1,305E-01							
BD	1	1	2	10	1	1	1	0,8	1,600E-01	1,600E-01	-	-	-	-	-	1,600E-01
	-	-	-	-	-	-	-	-	-							
DD	1	1	1	10	1	1	1	0,8	8,000E-02	8,000E-02	-	-	-	-	-	8,000E-02
	-	-	-	-	-	-	-	-	-							
DM	-	-	-	-	-	-	-	-	-	2,000E-02	-	-	-	-	-	2,000E-02
	0,1	1	2	1	20	10	1	0,5	2,000E-02							
DrD	-	-	-	-	-	-	-	-	-	1,998E-03	-	-	-	-	-	1,998E-03
	0,1	2	2	1	1	10	1	0,5	1,998E-03							
DrR	-	-	-	-	-	-	-	-	-	4,766E-02	-	-	-	-	-	4,766E-02
	0,1	2	5	1	5	10	1	1	4,766E-02							
DR	10	1	5	10	1	1	1	1	8,347E-01	1,066E+00	s	c	d	a	high	1,000E+00
	10	2	5	3	1	1	1	1	2,309E-01							
DT	-	-	-	-	-	-	-	-	-	1,000E-03	-	-	-	-	-	1,000E-03
	0,1	1	2	1	1	10	1	0,5	1,000E-03							
FM	-	-	-	-	-	-	-	-	-	6,002E-04	-	-	-	-	-	6,002E-04
	0,01	1	2	3	1	10	1	1	6,002E-04							
FS	1	1	2	10	1	1	1	1	2,000E-01	2,119E-01	s	c	d	a/na	high	6,059E-01
	1	2	2	3	1	1	1	1	1,187E-02							
LC	0,1	2	2	1	20	1	1	1	7,477E-02	7,477E-02	-	-	-	-	-	7,477E-02
	-	-	-	-	-	-	-	-	-							
MC	-	-	-	-	-	-	-	-	-	6,000E-03	-	-	-	-	-	6,000E-03
	1	1	2	3	1	1	1	1	6,000E-03							
NC	-	-	-	-	-	-	-	-	-	1,187E-02	-	-	-	-	-	1,187E-02
	1	2	2	3	1	1	1	1	1,187E-02							
RF	1	2	2	10	1	1	1	1	2,878E-01	2,878E-01	-	-	-	-	-	2,878E-01
	-	-	-	-	-	-	-	-	-							
SH	-	-	-	-	-	-	-	-	-	1,072E-01	-	-	-	-	-	1,072E-01
	10	2	2	3	1	1	1	1	1,072E-01							

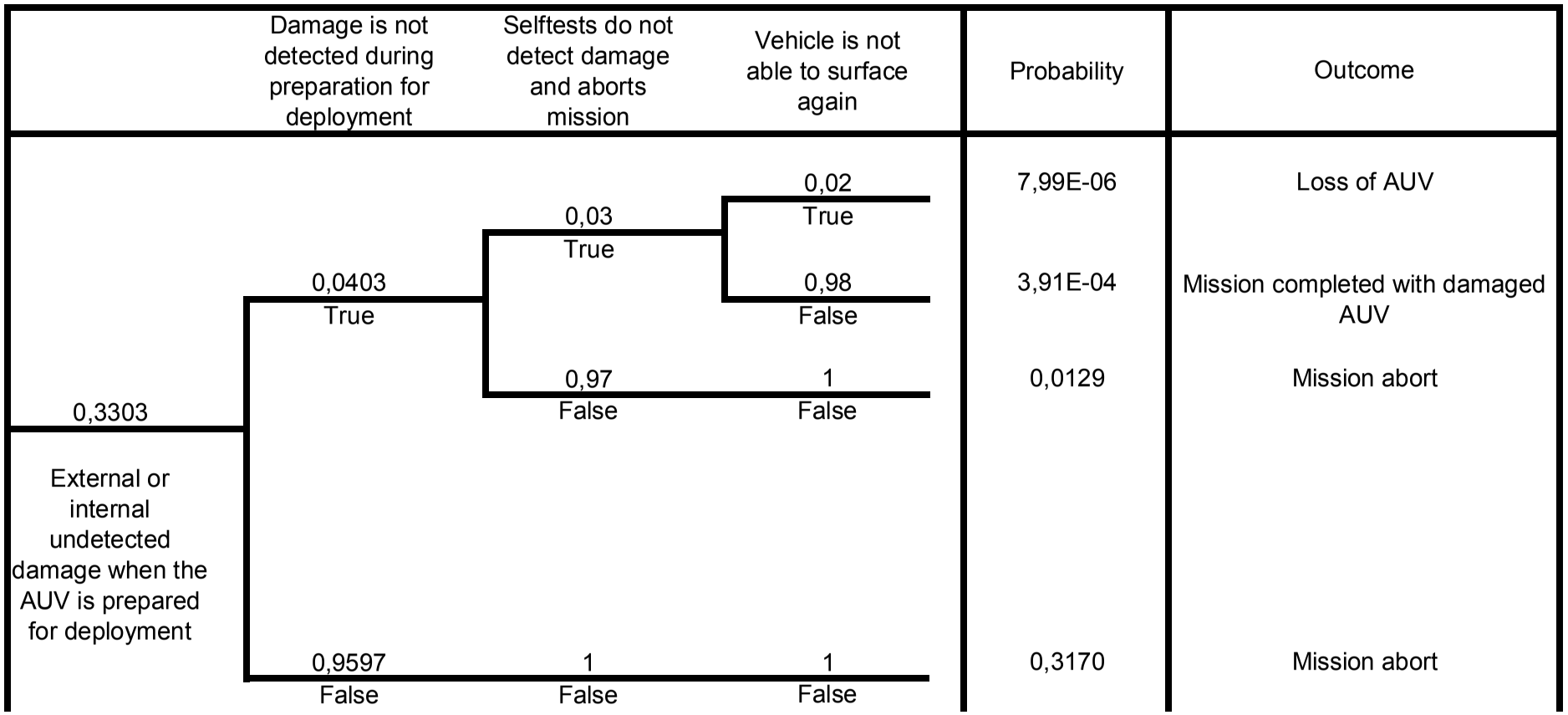
TS	-	-	-	-	-	-	-	-	-	5,000E-04	-	-	-	-	-	5,000E-04
	1	1	1	1	1	1	1	0,5	5,000E-04							
WB	-	-	-	-	-	-	-	-	-	6,000E-03	-	-	-	-	-	6,000E-03
	1	1	2	3	1	1	1	1	6,000E-03							
WP	1	2	2	10	1	10	1	1	8,016E-01	8,401E-01	s	c	s	a/na	com-plete	1,000E+00
	1	2	2	1	1	10	1	1	3,850E-02							

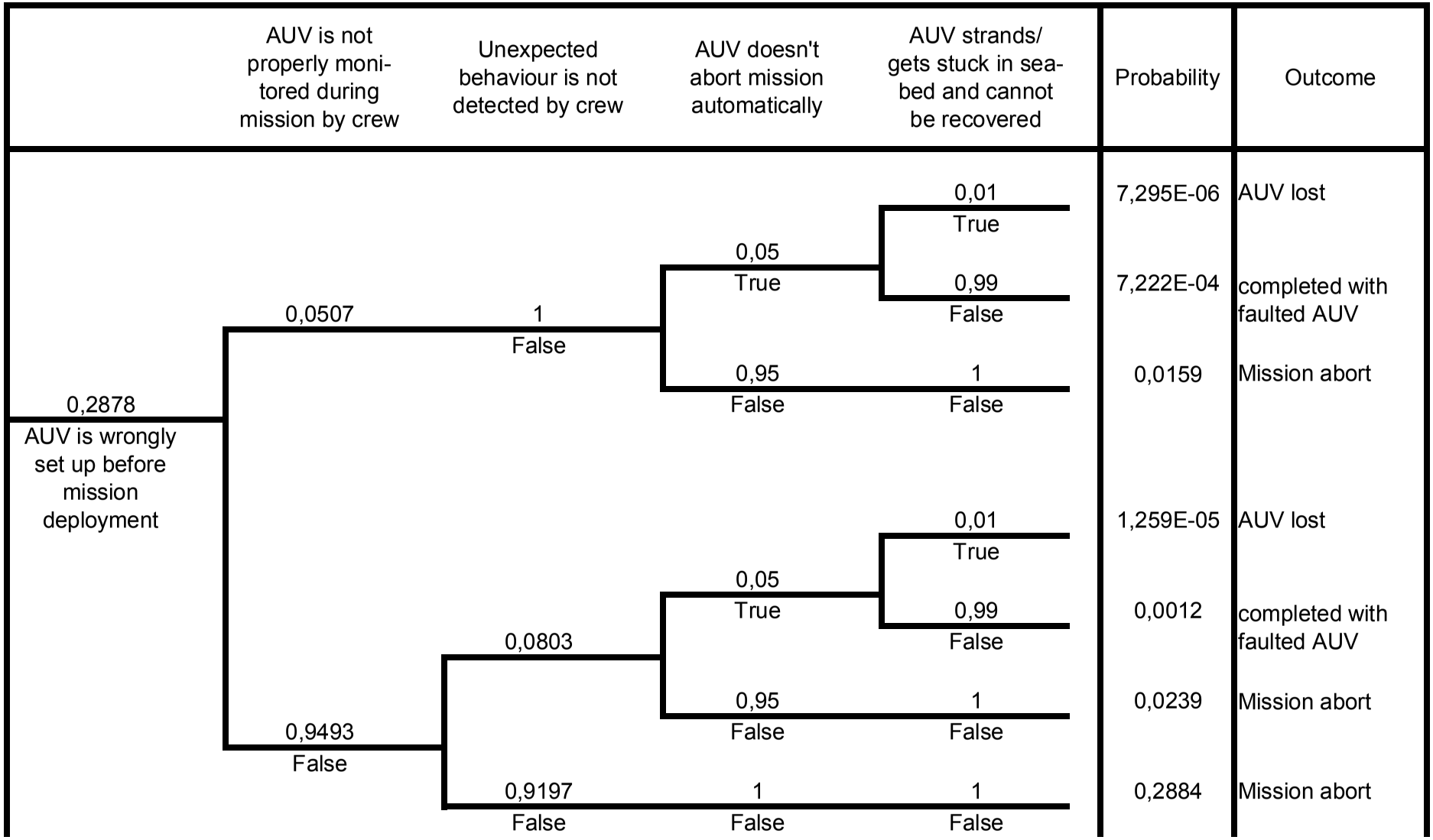
Abb.	PSFs								HEP	P_w/od	Dependency					P_w/d
	Time	Stress	Comp-lexity	Experience/ Training	Proced-ures	Ergo./ HMI	FfD	Work Process			Crew	Time	Loc.	Cues	LoD	
AN	-	-	-	-	-	-	-	-	-	1,00E-03	-	-	-	-	-	1,00E-03
	1	1	2	1	1	1	1	0,5	1,00E-03							
BD	0,1	2	1	0,5	1	0,5	1	1	5,00E-04	5,00E-04	-	-	-	-	-	5,00E-04
	-	-	-	-	-	-	-	-	-							
DD	1	1	0,1	0,5	1	1	1	1	5,00E-04	5,00E-04	-	-	-	-	-	5,00E-04
	-	-	-	-	-	-	-	-	-							
DM	-	-	-	-	-	-	-	-	-	5,00E-02	-	-	-	-	-	5,00E-02
	1	1	1	1	1	10	5	1	5,00E-02							
DrD	-	-	-	-	-	-	-	-	-	3,34E-01	-	-	-	-	-	3,34E-01
	1	2	1	1	5	10	5	1	3,34E-01							
DrR	-	-	-	-	-	-	-	-	-	3,34E-01	-	-	-	-	-	3,34E-01
	1	2	1	1	5	10	5	1	3,34E-01							
DR	1	1	2	1	5	1	1	1	1,00E-01	3,31E-01	s	c	s	na/a	com-plete	1,00E+00
	1	1	5	3	20	1	1	1	2,31E-01							
DT	-	-	-	-	-	-	-	-	-	5,00E-03	-	-	-	-	-	5,00E-03
	1	1	1	1	5	1	1	1	5,00E-03							
FM	-	-	-	-	-	-	-	-	-	1,00E-03	-	-	-	-	-	1,00E-03
	1	1	1	1	1	1	1	1	1,00E-03							
FS	1	1	2	1	1	1	1	1	2,00E-02	7,67E-02	s	c	s	a/na	com-plete	1,00E+00
	1	2	2	3	5	1	1	1	5,67E-02							
LC									0,00E+00	0,00E+00	-	-	-	-	-	n.a.
	-	-	-	-	-	-	-	-	-							
MC	-	-	-	-	-	-	-	-	-	0,00E+00	-	-	-	-	-	n.a.
									0,00E+00							
NC	-	-	-	-	-	-	-	-	-	0,00E+00	-	-	-	-	-	n.a.
									0,00E+00							
RF									0,00E+00	0,00E+00	-	-	-	-	-	n.a.
	-	-	-	-	-	-	-	-	-							
SH	-	-	-	-	-	-	-	-	-	0,00E+00	-	-	-	-	-	n.a.
									0,00E+00							

TS	-	-	-	-	-	-	-	-	-	0,00E+00	0,00E+00	-	-	-	-	-	n.a.
									0,00E+00								
WB	-	-	-	-	-	-	-	-	-	0,00E+00	0,00E+00	-	-	-	-	-	n.a.
									0,00E+00								
WP									0,00E+00	0,00E+00	0,00E+00	s	c	s	a/na	high	n.a.
									0,00E+00								

C. Risk treatment

C.1. Revised event trees


Damage is not detected during preparation for deployment
Selftests do not detect damage and aborts mission
Vehicle is not able to surface again
Probability
Outcome
External or internal undetected damage when the AUV is prepared for deployment
0,3303
0,0403
True
0,03
True
0,02
True
7,99E-06
Loss of AUV
0,98
False
3,91E-04
Mission completed with damaged AUV
0,97
False
1
False
0,0129
Mission abort
0,9597
False
1
False
1
False
0,3170
Mission abort


AUV is not properly monitored during mission by crew
Unexpected behaviour is not detected by crew
AUV doesn't abort mission automatically
AUV strands/ gets stuck in seabed and cannot be recovered
Probability
Outcome
0,2878
AUV is wrongly set up before mission deployment
0,0507
False
1
False
0,05
True
0,01
True
7,295E-06
AUV lost
0,99
False
7,222E-04
completed with faulted AUV
0,95
False
1
False
0,0159
Mission abort
0,9493
False
0,0803
0,05
True
0,01
True
1,259E-05
AUV lost
0,99
False
0,0012
completed with faulted AUV
0,95
False
1
False
0,0239
Mission abort
0,9197
False
1
1
False
False
False
0,2884
Mission abort

D. Risk management framework

Risk assessment for the REMUS 100 AUV

Risk management framework

Christoph Thieme – Initial 06.2014

10.06.2014

This document is the risk management framework for the risk management process of the AUV REMUS 100 belonging to the AUR Lab of NTNU Trondheim. It will give an outline on how to carry out risk assessments and how to use them. The Risk Management process is established following the risk management standard ISO 31000.

Document change history

Version	Change description	Revised by
1.0	Initial Version, ready for internal review	Christoph Thieme

Contents

Abbreviations

AMOS	Centre of excellency for autonomous Marine Operations and Systems
AUR Lab	Applied Underwater Robot Laboratory
AUV	Autonomous Underwater Vehicle
CREAM	Cognitive Reliability and Error Analysis Method
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HRA	Human Reliability Analysis
NTNU	Norwegian University of Science and Technology
PSF	Performance Shaping Factor
RCM	Risk Reducing Measure
ROV	Remotely Operated Vehicle
RPN	Risk Priority Number
THERP	Technique for Human Error Prediction
UUV	Unmanned Underwater Vehicle

1 Introduction

1.1 Background

The AUR Lab of NTNU operates the unmanned underwater vehicles (UUV) owned by NTNU. Operations include use of autonomous underwater vehicles (AUV) and remotely operated underwater vehicles (ROV) in the fjords of Norway. While the Trondheimsfjord is the main area of use also other regions are used, such as Spitsbergen. Operation takes place in a corrosive medium, strong currents and rapidly changing weather conditions, which form a hazardous environment.

During operation the operators and assets are vulnerable in this environment. NTNU emphasizes a proactive approach towards risk and safety. As part of NTNU, the AUR Lab should implement a proactive approach to manage the risks, so that the hazard will not manifest in an incident with unwanted outcome.

1.2 Scope

The scope of this framework is to give tools for risk assessment to the AUR Lab to assess and monitor the risk of the AUR Lab's UUV operation. The risk management is built on the ISO 31000 (2009) standard.

The risks, hazards, tools and methods are noted, only intended for record keeping of proven methods. Other methods should be used if more applicable in order to advance risk management and assessments. Chapters 3 and 4 are intended as way to record the methods that were used and experiences that where made with them. This shall facilitate selection of applicable methods in the future.

1.3 Terms and definitions

1.3.1 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.

1.3.2 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).

1.3.3 Failure and fault

A failure is defined as:

> “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.

1.3.4 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 measures (RCM) are used synonymously.

1.3.5 Risk management

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

The risk management process comprises five steps which are interlinked. These steps are establishing of context, risk assessment, risk treatment, communication and consultation and monitoring and review. The latter two link the steps together and assure continuous improvement of risk (ISO 31000, 2009).

The process described in ISO31000 (2009) is depicted in Figure 1. Communication and consultation takes a major role, it shall ensure that experts from different fields are consulted to ensure identification of all risks and hazards.

Establishing the context is the process where scope, purpose and goals are described. Risk assessment consists of three steps: Risk identification, risk analysis and risk evaluation. During risk identification hazards are reviewed and the possible harm is identified. Risk analysis identifies mechanisms, how the hazards might manifest and if the risk is relevant in the established context. Risk evaluation identifies the level of risk and gives input for decision making and risk treatment (ISO 31000, 2009).

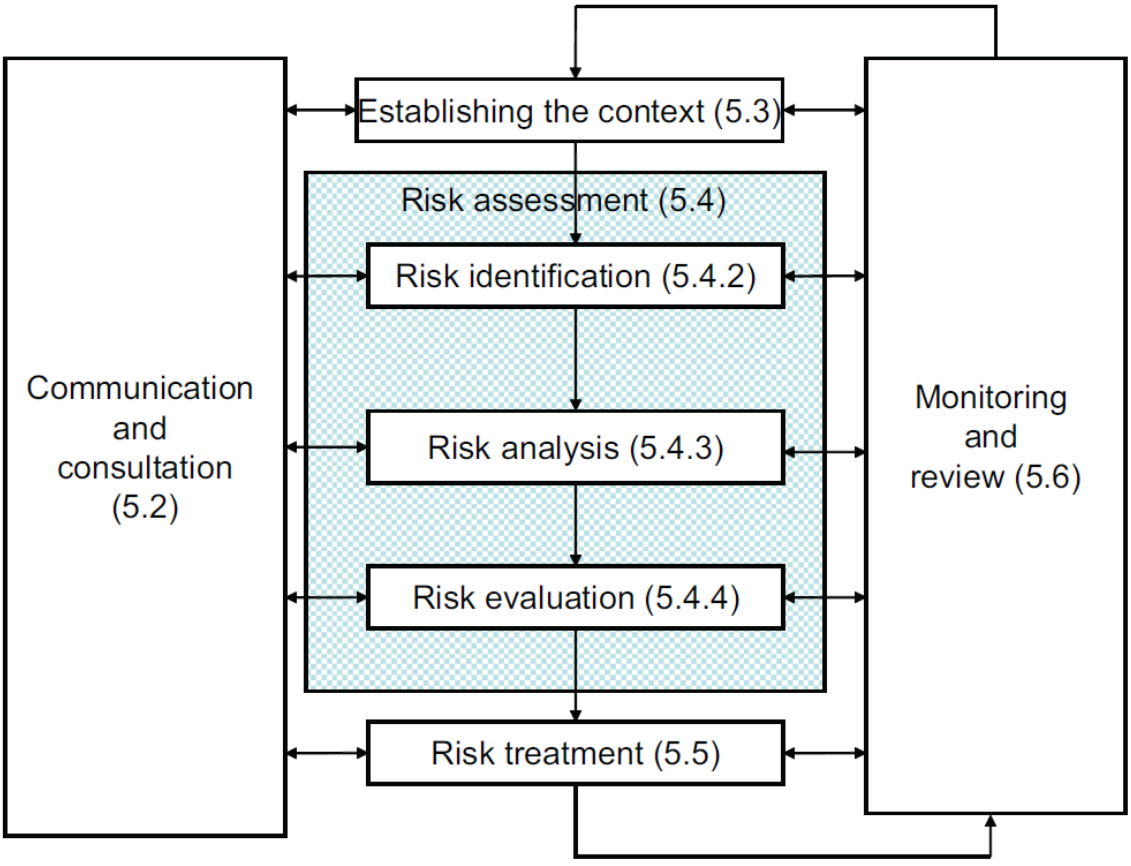


Figure 1 Risk management process described in ISO 31000 (ISO 31000, 2009)

During risk treatment measures are identified to reduce the risk of relevant risk contributors as much as possible. The principle that the risk should be reduced as long as it can be proven that the associated effort is disproportional high should always be applied (ISO 31000, 2009). Through the constant process of monitoring and review the risk level should be constantly reduced, by reassessing the risk with the knowledge gained in the meantime.

2 Implementation of risk management

The risk management system is summarized in Figure 2. It shall show links between different actors in the system and their roles. The risk management framework is the central point of the risk management system.

2.1 Responsibilities

Head of the AUR Lab is Professor Harald Ellingsen. Martin Ludvigsen, as head of operations of the AUR Lab, is responsible for planning and organisation of research cruises with UUV.

So far no risk management responsible has been assigned. This person is in charge of organisation of risk assessments, preparation and conduction, with the resources necessary. The person is also responsible for updating and monitoring the risk assessments and risk management, based on the findings, experience and input gathered since the last update.

Decisions, e.g. measures to reduce risk or other operation patterns, based on the risk assessments have to be made by the heads of AUR Lab and if necessary by the head of the research mission and other relevant parties involved in the operation, such as the crew of Gunnerus, external participants etc.

2.2 Communication and cooperation

For the risk assessments and risk management system the risk management responsible is the key figure in communication. It is his responsibility to communicate the importance of a risk management system and the advantages. Additionally he is responsible to identify experts needed for risk assessments and review of the system.

All parties involved in UUV operation should be involved in the risk assessment as needed, such as, among others, the head of operation, technicians, mission operators, support vessel operators and external stakeholders in the operation and mission.

The risk management responsible should ensure that meetings are scheduled in such a way that the aim can be reached efficiently and in the time planned. The head of daily operation should support the risk management responsible as far as possible in the organisation.

2.3 Monitoring and review of risk and risk management

The risk itself should be monitored. Incidents should be recorded and relevant risk assessments reassessed. The reassessment should reflect experiences made and also reflect changes in operation and hazards. The statistics should also show if the risk found is over- or underestimated. This can only be made to some extent, since few operations are carried out per year which might easily be mistaken for a high safety level though the data is not statistically precise.

Monitoring of the risk level can also be done by recording of faults of the UUV. From these faults shortcomings in planning, maintenance or software might be derived. A way to extract faults from the REMUS 100 is described later.

2.4 Review of the management system

The management system, along with this document should be kept updated and revised. This should be done on a regular basis to ensure that gained experience is saved and available for others and later use. For the review process all parties involved in recent or ongoing risk assessments and operation should be involved to gain a comprehensive impression where improvements can be made.

An adequate interval still has to be found.

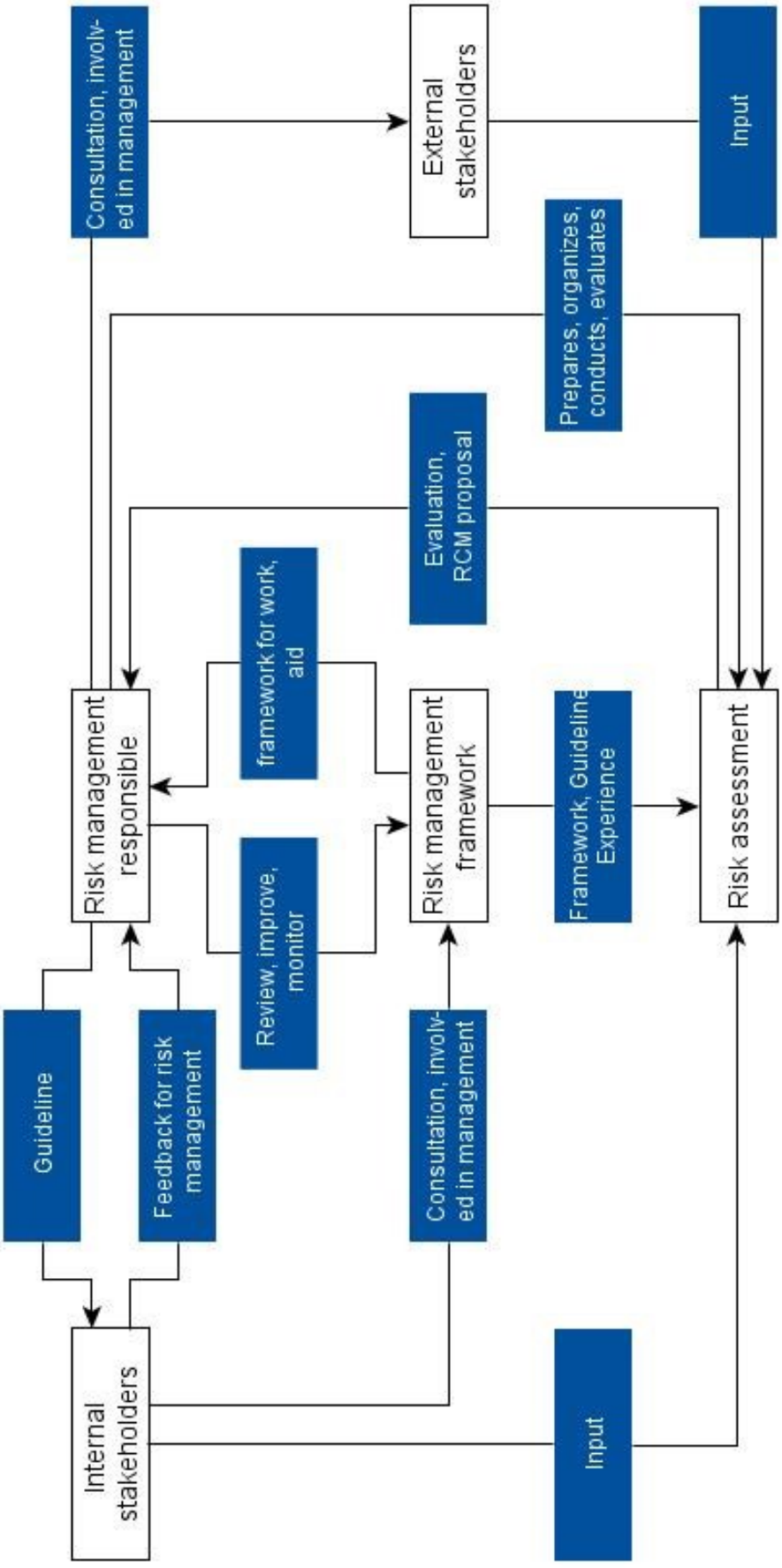


Figure 2 Risk management system interactions

3 Risk assessment methodology

In the following part methods shall be shortly described which can be part of the risk assessment. References are made to further literature which explains the methods in more detail. For a more detailed information ISO 31000 (2009) should be consulted.

3.1 Context

In this part the aim of the risk assessment is defined. This includes objectives, scope, risk criteria and external and internal parameters. External and internal parameters should be described in more detail and better evaluated than described in this framework. (ISO 31000, 2009)

3.1.1 External context

The external context can include, among other topics (ISO 31000, 2009):

- The environment in which operation is taking place, e.g. legal, regulatory, technological and natural
- The setting of operation and consideration; international, national, regional or local
- Trends and drivers that impact the objective the organization
- External Stakeholders; their values, aims, perceptions and the relationship to them

3.1.2 Internal context

This part describes the internal environment in which the objectives shall be achieved. The values and organizational procedures of NTNU should be reflected in this part. The internal context can include among others (ISO 31000, 2009):

- Organizational structure, roles and accountabilities
- Objectives and strategies to achieve them
- Capabilities, resources and knowledge available for the risk management; E.g. capital, time, people, processes, systems and technologies
- Internal stakeholders, relationships between them and their values
- Information systems and flow and the decision making process
- Standards, guidelines and methods in use

3.1.3 Defining risk criteria

Criteria for risk assessment should be defined before the actual risk assessment is conducted. They should reflect resources available, objectives and values. Some can be derived from laws and regulations. They should be regularly reviewed and be reflected in the risk management. Factors to be considered for risk criteria are listed below (ISO 31000, 2009).

- Types of causes and consequences, their nature and how they can be measured
- How likelihood is defined
- Timeframe of likelihood and consequences
- Determination of level of risk
- Views and values of stakeholders
- Possibility of combination of multiple risks and how they can be combined

3.2 Risk identification

For identification of risks and hazards, hazard checklists can be used (e.g. Rausand (2011)). Other sources include literature on risk in AUV operation and handbooks for underwater vehicles.

The findings can be 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. Possible categories 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.

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 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

Table 2 Possible Consequence categories

Category	Rating	Description
Loss of AUV/ Loss of life	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/ mission abort/ Severe injury	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/ minor damage to health	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

3.3 Risk analysis

3.3.1 Modelling of risk

3.3.1.1 Fault tree analysis (FTA)

FTA is a tool to identify all combinations of basic hazardous 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 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.

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).

For FTA analysis the tool CARA Fault Tree v.4.02b can be used. With the program, fault trees can easily be drawn, with standard symbols and their logic already stored in the library.

3.3.1.2 Event tree analysis (ETA)

ETA is a graphical approach which is set up left to right, whereas it starts from the hazardous events (e.g. the top event of a FTA) 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 can easily be drawn in Microsoft Excel, including the calculations for the end event probabilities. Other commercial solutions are also available. 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.

3.3.2 Modelling of event probabilities

In order to gather basic event probabilities for the above mentioned analyses several tools can be used. Some will be described below.

3.3.2.1 Statistical data

Data of incidents or faults that were recorded can be used to find probabilities. One premise is that data is sampled regularly and enough data is collected.

To extract failure data from the REMUS 100, the control software can be used. A mission file has to be selected and loaded in the program. In the task bar, in the menu “Export” the option “Export fault log” is available. The user is asked upon selection to define a destination and name, after saving the fault log for the mission is saved in .txt format.

The format is similar to a comma separated value (.csv) –file and thus can be analysed automatically by a script in mathematical processing software. Fault recording should also include a time/ distance notation for statistical evaluation.

With this data available, the criticality of the events should be assessed, often the messages are mere warnings, which are not relevant for the risk. For the critical events a distribution can be chosen to assess the frequency or probability of occurrence. For a large amount of reoccurring faults a Weibull distributions might be used. With the parameters different function characteristics can be modelled. For less reoccurring events the Kaplan Meier estimator might be more adequate. For more information it is referred to the literature.

3.3.3 Expert estimation of probabilities

Expert estimation of probabilities is recommended if no or few data is available. Through involvement of several experts it is believed that a probability close to the “real” probability can be assessed. So far one simple assessment method was used which applied a verbal-probabilistic-scale, described by (Witteman & Renooij, 2003).

Another method which is more advanced is the SHELF v2.0 method (Oakley J. E. and O'Hagan, 2010), which was already successfully used for estimation of probabilities in context with AUV operation (Griffiths, et al., 2009).

A variety of more methods is available, it is referred here to two review papers, one from the U.S. Army (Ayyub, 2000) and a thorough review for different sectors of application (Jenkinson, 2005).

3.3.3.1 Human reliability analysis

Several methods for human reliability analysis (HRA) exist. So far the Spar-H method was used. The method was developed by US nuclear energy authorities and is described in NUREG/CR-6883 (2005). But as was found out during the first risk assessment, it has also some shortcomings in relation to modelling of interconnection of events. It requires a lot of clarification work in the beginning to instruct the analysts, otherwise misunderstandings and misinterpretations might result.

In the following some more general methods will be presented, which might be worth consideration instead (Rausand, 2011):

- THERP (Technique for human error prediction)
    - Widely used and well documented method
    - Can be resource intensive and requires high level of detail

- HEART (Human error assessment and reduction technique)
    - Does not require high level of skill or knowledge in HRA
    - Quick and straight forward use
    - No modelling of dependencies
    - Subjective perspective of analyst is having an influence
- CREAM (Cognitive reliability and error analysis method)
    - Considering context
    - Well-structured and systematic
    - Resource intensive and overwhelming for new users
    - Requires knowledge in human factors and cognitive psychology

3.3.3.2 Data from other publications

Only few data from published literature is available. For the REMUS 100 one thorough analysis was conducted and published (Griffiths, et al., 2009). It is believed that the AUR Lab can profit from the experiences described and built on the knowledge presented there.

3.4 Risk treatment

The risk treatment should consist of three parts.

1. Identification of high risk contributors
2. Identification of risk reduction measures (RCM)
3. Re-evaluation of the risk and decision making

Identification of high risk contributors can be a straight forward task, depending on the model used. It should be kept in mind that all the events have a certain level of uncertainty. Events with a high probability and associated high uncertainty should be closer investigated first, reducing the uncertainty, by collecting further data.

Identification of risk reduction measures should be conducted in cooperation with the experts already involved in the assessment and if necessary further experts should be consulted. It is important to quantify the impact of the measures. Methods for reduction assessment could be, among others, HRA, expert estimation or data from publications.

The reduced probabilities then can be used to re-assess the risk. This should be done individually for each RCM proposed or in feasible groups to assess if the risk reduction effort results in an accordingly high risk reduction. Thus a risk reduction to effort factor should be defined beforehand. This limit is often expressed as the difference in risk over the cost of implementing the RCM.

4 Hazards and risks of concern

In the following chapter some remarks will be made, which hazards and risks might be relevant. The list is in no case complete and should be enhanced when new hazards are identified or arise.

4.1 Risk

Normally three types of risks are analysed:

- Risk to humans
  - Loss of life
  - Injuries
  - Permanent damages to health
  - Loss of life or damage to third party people
- Risk to assets
  - Loss of the AUV
  - Damage to the AUV
  - Loss or incomplete mission results
  - Loss of equipment
  - Damage to equipment
  - Damage to assets not belonging to the AUR
- Risk to the environment
  - Hazardous materials leaking to the environment
  - Release of hazards/ hazardous material due to interaction with other assets

4.2 Hazards

The following hazards might be considered in risk assessments, it is recommended to use additional checklists, a rather brief checklist of hazards can be found in (Rausand, 2011). It might also be worthwhile to look into operational handbooks and literature on AUV reliability and incidents.

- Mechanical hazards
  - Kinetic energy
  - Acceleration/ retardation
  - Potential energy
  - Sharp edges/ points
  - Vacuum
  - Moving/ rotating parts
  - Stability/ toppling problems

    - Material degradation; corrosion, wear, fatigue, etc.
- Dangerous materials
    - Flammable
    - Explosive
    - Corrosive
- Electrical hazards
    - Electromagnetic hazard
    - Electrostatic hazard
    - Short circuit
    - Overload
- Thermic hazard
    - Flame
    - Explosion
- Environmental hazards
    - Lightning
    - Storm
    - Fog
    - Sea state
- Hazards through neglected ergonomic principles
    - Unhealthy postures, excessive effort required
    - Mental overload or underload, stress
    - Human error, human behaviour
- Organizational Hazards
    - Safety culture
    - Maintenance (less than adequate)
    - Competence (less than adequate)
- Interaction Hazards
    - Electromagnetic interference or incompatibilities
    - Hardware and software control

5 Literature

Ayyub, B. M., 2000. *Methods for Expert-Opinion Elicitation of Probabilities and Consequences for Corps Facilities - IWR Report -00-R-10,* Alexandria, VA 22315: U.S. Army Corps of Engineers Institute for Water Resources.

Burgman, M. et al., 2006. *Eliciting Expert Judgments: Literature Review,* Melbourne: ACERA, University of Melbourne.

Griffiths, G., Brito, M., Robbins, I. & Moline, M., 2009. Reliability of two REMUS-100 AUVs based on fault log analysis and elicited expert judgment. In: *Proceedings of the International Symposium on Unmanned Untethered Submersible Technology (UUST 2009), Durham, New Hampshire, 23-26 August 2009.* Durham NH, USA: Autonomous Undersea Systems Institute (AUSI), p. 12.

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

Jenkinson, D., 2005. *The Elicitation of Probabilities - A Review of the Statistical Literature.* [Online]
Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.6173&rep=rep1&type=pdf
[Accessed 08. May 2014].

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

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

NUREG/CR-6883, 2005. *The SPAR-H Human-Reliability Analysis Method.* Washington D.C.: Office of Nuclear Regulatory Research - U.S. Nuclear Regulatory Commission.

Oakley J. E. and O'Hagan, A., 2010. *SHELF: the Sheffield Elicitation Framework (version 2.0),* (http://tonyohagan.co.uk/shelf): School of Mathematics and Statistics, University of Sheffield, UK.

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

Witteman, C. & Renooij, S., 2003. Evaluation of a verbal-numerical probability scale. *International Journal of Approximate Reasoning* , pp. 117 - 131.