

UNIVERSIDAD POLITÉCNICA DE CARTAGENA



Trabajo fin de master

Titulo

Análisis de riesgo de vehículos submarinos no tripulados

Title

Unmanned Underwater Vehicle Risk Analysis



Titulación: Ingeniería Naval y Oceánica

Alumno: Beata Myszkier

Directores: D. Gregorio Munuera Saura

Marzo de 2017

CONTENTS

Introduction	6
1. GENERAL DESCRIPTION OF UNMANNED UNDERWATER VEHICLES	10
1.1. Basic information about UUVs	11
1.2. Application and history of UUVs	14
1.3. UUV and risk assessment	16
2. RISK MODEL AND TECHNICAL DESCRIPTION OF THE VEHICLE	18
2.1. Technical description of UUV Seaglider	18
2.2. Safety features of UUV Seaglider	19
2.3. Principle of operation of Seaglider	20
2.3.1. Dive Cycle of Seaglider.....	22
2.3.2. System of launching and recovering.....	24
2.4. Communication and navigation systems of vehicle	24
2.5. System representation	25
3. RISK ANALYSIS METHODS	27
3.1. Definition of risk and risk analysis	27
3.2. Quantitative risk analysis methods	29
3.2.1. Fault Tree Analysis	31
3.2.2. Event Tree Analysis.....	32
3.3. Qualitative risk analysis methods.....	34
3.3.1. Brainstorming	34
3.3.2. Preliminary Hazard Analysis –PHA.....	35
3.3.3. What-if method	37
3.3.4. Safety Checklist.....	38
3.4. Software’s used for risk assessment	39
3.5. Basic definitions related to reliability.....	39
3.5.1. Survival estimation- the Kaplan-Meier estimator.....	41
3.5.2. Estimations in Statistics	42
3.6. Human Reliability- SPR-H method.....	43
4. RISK ANALYSIS	45
4.1. Failure database- Project GROOM	45
4.1.1. Probability density function of failure of Seaglider	48
4.1.2. Percentage of reasons of failures	49
4.2. Difficult area of operation	50
4.2.1. Coaster water analyzed using Preliminary Hazard Analysis	50
4.2.2. Comparison between areas of operation- based on Kaplan Maier estimator	52

4.2.3. Confidence level of failure on deep ocean	54
4.3. Analysis of navigational system	55
4.3.1. Preliminary Hazard Analysis for navigational aspect	55
4.3.2. Human Reliability Assessment and Event Tree Analysis	57
4.4. Analysis of risk for launching and recovering process	60
4.4.1. Preliminary Hazard Analysis for failure	60
4.4.2. Human Reliability Assessment and Fault Tree Analysis	61
4.4.3. Human Reliability Assessment and Event Tree Analysis	63
4.5. What-if Analysis for moving process	64
5. ANALYSIS OF RESULTS	65
5.1. Evaluation of Preliminary Hazard Analysis	65
5.2. Assessment of area of operation based on Kaplan Maier estimator	66
5.3. Analysis of confidence level of failure on deep ocean.	67
5.4. Evaluation of risk assessment for navigational aspect	69
5.4.1. Evaluation of Preliminary Hazard Analysis for navigational equipment	69
5.4.2. Analysis of Human Reliability Assessment for navigational system	70
5.4.3. Analysis of the result of the Event Tree analysis for navigational system	70
5.5. Analysis of launching and recovering process	71
5.5.1. Evaluation of Preliminary Hazard Analysis.....	71
5.5.2. Human Probability Assessment and Fault Tree for launching process	72
5.5.3. Human Probability Assessment and Event Tree for recovering process	73
6. EVALUATION OF THE ACCEPTABILITY OF THE RISK	74
6.1. Risk priority number	74
6.2. Method of acceptability of risk for owners	75
6.3. Farmer Curve's	78
6.4. Factors effecting on the acceptability of the risk	79
6.4.1. Revealed Preferences method –benefit effect	79
6.4.2. Evaluation of magnitude of risk consequence	80
6.4.3. Risk Reduction Cost Effectiveness Ratio	81
6.4.4. Risk Comparison.....	81
Conclusion.....	83
Bibliography	85
List of tables	87
List of figures.....	88
List of diagrams.....	88
Annexes	89

Abbreviations

ABE- Autonomous Benthic Explorer
ALARP- As low as reasonable practicable
AUV- Autonomous Underwater Vehicle
CIRIA- Construction Industry Research and Information Association
DNV GL- Det Norske Veritas and Germanischer Lloyd
ETA- Event Tree Analysis
FTA- Fault Tree Analysis
FMEA- Failure Mode and Effect Analysis
FMECA- Failure Modes Effects and Criticality Analysis
GPS- Global Positioning System
GROOM- Gliders for Research, Ocean Observation and Management
HAZID- Hazard Identification Studies
HAZOP- Hazard and Operability studies
HD- High Definition
HEP- Human Error Probability
IMESARF- Institute of Makers of Explosive Safety Analysis for Risk
ISE- International Submarine Engineering
LED- Light-emitting diode
NASA- The National Aeronautics and Space Administration
MTTF- Mean Time to Failure
MTTR- Mean time to Repair
NHEP- Nominal Human Error Probability
ONR- Office of Naval Research
PEST- Political, Societal and Technological
PLL- Potential loss of life
PRA- Probabilistic Risk Assessment
PHA- Preliminary Hazard Analysis
QRA- Quantitative Risk Assessment
ROV- Remotely Operated Vehicle
SPURV- Special Purpose Underwater Research Vehicle
SWOT- Strength, Weaknesses, Opportunities and Threats
UUV- Unmanned Underwater Vehicle
WHOI- Woods Hole Oceanographic Institution

Introduction

The world go ahead, and technology with him. A few years ago, nobody hear about device like Unmanned Underwater Vehicle, which is able to immerse and precede its task without help from people side. Engineers have conducted a lot of researches but only at universities and military units. The ordinary people were not interested about these devices at all. Times have changed. Nowadays, via the internet anyone can buy a water drone for their fun and use it in nearby lake or swimming pool. UUVs are very interesting devices; thanks of them scientists are able to perform many important and interesting surveys. They facilitate and accelerate the work of people, especially in difficult area of operation like deep seas.

The topic about the risk analysis of small semi-submersible object is very interesting because of two main aspects. The first reason is the rapid development of these devices. Forty years ago, nobody has heard about unmanned underwater vehicles and nowadays, they have started to substituting peoples in their works. These devices have become commonly used in bottom researching for oil and gas industry. They have been saving a lot of money and time for companies. They are very inquisitive because they are technologically advanced, but they have still a lot of things to improve. It is curious and requiring issue especially for marine engineers.

The second reason is interesting question of risk assessment. It can be found a lot of information about the risk in work, but really hardly anyone heard something about the risk assessment of object or device. The definitions like financial risk or credit risk are very good known, but few of us heard about the risk of the system. The risk analysis is quit new branch of science in the engineering, which is still developing. Often the engineers analyze a failure rate or a reliability of the system, forgetting that is only a narrow section of risk analysis.

This thesis consists of six main chapters. In the first chapter of this thesis, it will be presented the basis information about unmanned underwater vehicles. It will show the application of these devices and fields in which they are used. One of the most important aspects is short history of this system, which let to see and understand how fast these devices have been developing over the years. It is also essential to mention about the aspects, which need to be improve, which are not perfect yet. The chapter will be finished by short summarizing of the base of risk analysis of UUV's, why this task is performed and why it is so important especially for this equipment.

Subsequently chapter will discuss the model of risk, in this case UUV Seaglider from Kongsberg Company. To perform a good risk analysis, initially it is obligatory to have a defined object, which will be analyzed and is called risk model. Before analysis, it is essential to know parameters of object like length, beam, equipment in which is fitted or boundaries of device, like area of operation. The technical specification of this device will be present. Nowadays in industry it can be found a lot of different companies which are specialists in production

of gliders. The external appearance of the devices no is significantly different, but they can be fitted with different sensors, which cause theirs various applications.

The following part of the work, will present the main risk analysis methods which are used specially in engineering. The basics information about methods, ways of counting the probability, and fields in which these methods are commonly used will be discussed. Nowadays many different methods of risk analysis were involved, which are used in different branch to obtain intended results. No all methods are appropriate to obtain specific results, especially in engineering. The methods like Fault Tree Analysis, Preliminary Hazard Analysis or Brainstorming will be presented, which later will be used to perform the risk assessment. It will allow to knowing better and understanding these methods and seeing, which of them are suited to achieve a specified goal.

The most important in this thesis will be calculations and assessment of the risk. Different aspects and methods have been selected, which are the most essential in the view of risk analysis. The risk will be assessed in view of navigation system, difficult area of operation and moving system. These aspects are the most significant for devices like Seaglidgers. Navigation and communication is used to obtain UUVs position by different equipment's, which are installed on devices and to send the commands to the vehicle. The moving system is essential issue for device's move. UUV's are used specially in region where people cannot go, so very often they are used in difficult area of operation, where they can meet others objects (vessels, wracks, rocks) , weather condition are difficult (high wave, strong tidal or current) or the sea is very deep. For each of these aspects, other method of risk analysis has been selected.

The next chapter will be the continuation of the analysis and will discuss the results, which will be obtained. The correctness of results and selected methods will be accessed. Using the literature of this subject, based on the works performed by engineers from this branch, it is possible to check the results and the accuracy of the methods. The amendments and the errors of methods will be proposed. Worthy of mention is the issue connected with acceptability of the risk. Thank of this issue, the risk can be analyzed in the view of its permissibility. It is helpful to indicate the weak aspects of vehicle, which can be corrected latter or paid attention on them. It may happen that for some reasons, object cannot be used in industry because of the high risk associated with the system. The thesis will be finished by brief summarizing of the performed work. The methods which are the most suitable for risk assessment of Seaglider will be noted.

The risk analysis is very important issue and the contemporaries engineers cannot forget about that. The earlier development of hazards posed on the system, will help to protect against them and save a lot of many for companies, protect the human health and the environment. The prior analysis of the system will allow concentrating on the weakest points of the device and preparing a plan of action in the case of hazard. This is particularly important for vehicles like unmanned underwater vehicle, because they are relatively new

and still need to be improved. They move and work in dangerous and unstable environment and thereby they are exposed to big danger. These are expensive devices and the owner cannot afford to their lost.

1. GENERAL DESCRIPTION OF UNMANNED UNDERWATER VEHICLES

1.1. Basic information about UUVs

The UUV is an unmanned underwater vehicle similar to unmanned robot, which travels akin to the *Curiosity Rover* which is used by NASA on Mars, but it is travel underwater. They are known as underwater drones. They are able to perform the work without the human occupant. These devices can be divided into three main categories. First group are device called ROV- *Remotely Operated Vehicle*. They are supple in power and communication through tether and they are under control by remote operator. The second class is AUV- *Autonomous Underwater Vehicles*, which contain its own power and controlling itself [4]. The third groups are gliders, which are smaller and buoyancy-driven vehicles.

Many different technologies are needed for UUV's systems. For many years, these aspects have been improved, but some of them still have some problems to solve. To these issues belong: navigation, communication, energy and sensors [4]. First devices to control position had been using the dead reckoning. This method has a lot of errors, for example because is very difficult to take into account effect of winds, currents or tides. In the other side, acoustic transponder navigation systems have a greater accuracy but the cost of is significantly higher. Scientists try to improve accuracy and precision of navigation systems. In the past years, UUV have started to use the GPS on board. When the vehicles are on the surface, they are able to update internal system's information, but it is difficult to do it under the water. Nowadays it is still in interest of engineers to navigate relative to the environment in which the system exists [4].

The underwater acoustic communication is the most viable system of communication available for the system design [4]. In the past 10 years it could be noted the significant development of this type of communication. Nowadays some specialists try to involve laser communication which has relatively noise free communication. The ROVs to communication use normally a long tether cables, but nowadays the engineers from US WHOI developed a wireless underwater communication , to control the ROV in real-time. Thanks of this method, they eliminate the long tether cables and obtain better degree of freedom of underwater drone [43]. Other problem is to connect multiple vehicles which perform common task in the same time. A lot of effort is implementing to set an efficient network among underwater systems.

The durability of UUVs is varies from a few hours of work or days, but they can be found the systems which can perform mission of months or even the years. The durability varies because of different sensing capability and limited transit speed. The majority of systems have the lead acid batteries; next big group includes silver zinc batteries o lithium primary batteries. Nowadays in many UUVs started to use NiMH batteries [27]. Also it is important to mention about solar energy, which nowadays is used to power the UUVs. These systems required individual design of the system. It is unfailling system but its disadvantage is that,

it has to be emerged while is recharging the batteries. On the figure 1.1 is presented a basic design of this system.

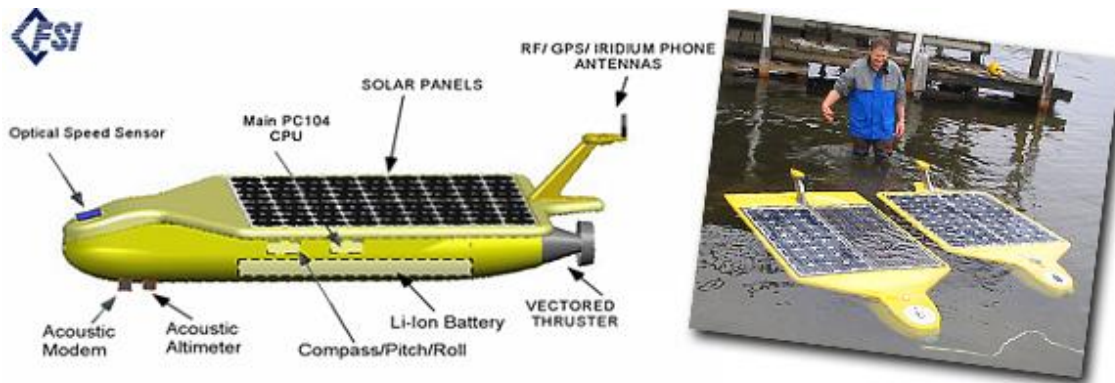


Fig.1.1. UUV with solar panels (Source: <http://ausi.org/research/sauv/>)

The UUVs are designed to perform specified issues and thereby they have a lot of different sensors in their platform to obtain data from the ocean environment. First devices have been created to perform basic operation. Together with the development of technology, more sensors were added to the system, to obtain more specified and accuracy data. A lot of effort have been put to integrate sensors and some unique constrains of the UUVs. Newly it has been ascertained that the development of the new sensors has to be based on the restrictions imposed by the vehicles. It has been caused the development of special sensors, especially for this group of vehicles: lower power, smaller, smarter and highly reliable. A lot of emphasis nowadays is putted on development optical and acoustic systems to obtain higher resolution images over longer ranges [4].

The huge numbers of vehicles have been designed in the range from approximately 50 kg to 900 kg of weight, but majority of them are these smallest one [3]. The operation speed is in the range from $0.5 \frac{m}{s}$ to $5 \frac{m}{s}$, but the most popular cruising speed is $1.5 \frac{m}{s}$ [3]. Due to the depth rating, the UUVs can be divided into three main groups: vehicles designed to depth of 50 meters (surface layer), vehicles for depth of 300 meters (interior layer) and to depth of 6000 meters (bottom layer). These first one, are mainly used on shallow water or coastal water, and the third one are mainly utilized in deep-surveyors in the oil and gas industry.

The main task which performs these devices is the bottom mapping and the observation of water columns [3]. They are able to do that, thanks to special equipment, for example: mechanically scanned sonar, laser-linescan imaging system, subbottom profilers' o side-scan sonar. They are able to measure parameters like: salinity, pH, optical backscatter, oxygen, temperature, chlorophyll fluorescence or inherent optical properties [3]. On the figure 1.2 is presented different applications and parameters of these vehicles.

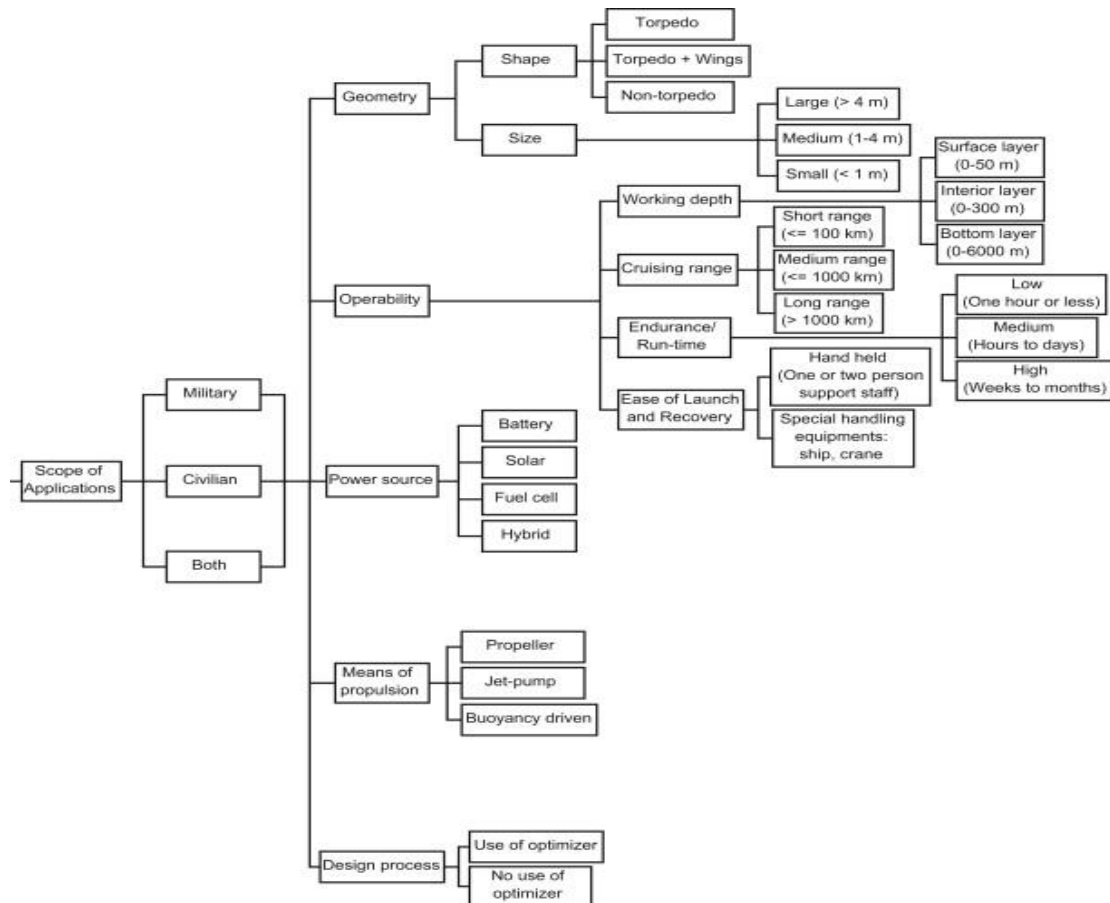


Fig.1.2. UUV's application and characteristics (Source: [49])

The deep-water survey is important application of UUVs, mainly because of economic reasons. For example in operation below 1000 meters, the tether dominates as a towed system; firmly reduce the speed and the maneuverability. In the opposed to this, UUV's survey at the depth 3000 meters has the speed two to four times greater. It should be also mentioned, that the process of turning of the system to pass across a survey area is eliminated, if we compare it to a vessel which has to turn with a towed system, which take several hours and much more kilometers and in this time, system is completely unproductive [3].

The companies, which employ the UUV's to bottom surveys, can also save a lot of money, because this equipment reduce numbers of ships required for a survey. In the normal cases, when the deep tow is performed, the company needs to employ two vessels, one for towing and second one to determining the position of the body which is towed. This second ship is obligatory, because they are cases when the towed body is several kilometers behind the tug (towing ship). To determine position, it is used acoustic tracking system and thereby, which cannot be effectively used by tug. This second ship is used to maintain station above towed-body. Additionally in one area of operation, many UUVs can be used to bottom survey, greatly accelerate the work [3].

1.2. Application and history of UUVs

Recently UUVs started to be accepted for task concerning: commercial, military missions or oceanographic issues. The market is divided into three main areas: science (especially research agencies and universities), commercial (oil and gas industry) and military use (battle space preparation). Nowadays, they can be met also other areas, where UUVs found their destiny, namely as a hobby and a use in illegal way.

These devices are very attractive for researches like: the bottom or the underwater parts of vessels research. The main attribute is that they can reach shallow water in contrast to boats, and some of them deeper water than divers. They have been using by scientists to create maps of the ocean bottom, to identify hazards, to ascertain the wracks, to study lakes, to record environmental information and to explore geologic formations. The UUVs are able to measure the concentration of various components or elements, the presence of microscopic life or absorption of reflection of the light. One of the interesting features is also that, this device can be configured as tow-vehicle and can deliver sensor packages to defined position.

In the industry, the UUVs are also used especially in oil and gas industry to make detailed maps of the sea bottom, before the start of building infrastructure like pipelines. After a survey, a base can be installed with minimum effect to environment and maximum cost effective manner.

These vehicles are also used by people as a kind of toy. Nowadays it can be seen a huge growth of technology for example: drones or very advanced telephones. Engineers start to create underwater unmanned vehicles for normal people as a kind of joy. As an example, it can be cited a *Ziphius* which is a first app-controlled aquatic drone. It is a small device, which can reach speed 5.4 of knots. It is fitted in skilled HD camera with the LED enhances and in extra sensor which allow to controlling it by smartphone or tablet. This technological advanced vehicle can be bought in internet¹.

On the other hand, the growth of the technology caused the increase of the use of technology in the illegal way. The sea drones are very interesting for drug dillers and smugglers. It is very easy way to transport a prohibited cargo to the other county. In the case if police find a drone with illegal load, it is very difficult to find a guilty, especially when everybody can buy a drone even on the internet. Where there is a crime, they have to be expected a police and army. Unmanned underwater vehicles are also used by army. These vehicles have a lot of different missions like: information operations, inspections, mine countermeasures or communication in battle field.

The UUVs have the applications in many different fields. Together with the development of technology, it can be observed a development of these devices, which a few years ago were only in the science fiction movies. The first vehicles were developed at the University

¹Ziphius <http://myziphius.com>

²Festo, <https://www.festo.com/group/en/cms/10227.htm>

of Washington at the Applied Physics Laboratory in 1975 by Stan Murphy, Bob Francois and Terry Ewart. The SPURV which mean a Special Purpose Underwater Research Vehicle, at the beginning was used to study diffusion, submarine wrecks and acoustic transmission [37]. One of the first underwater unmanned vehicles was founded by ONR. The United States Office of Naval Research (ONR) funded the researches and development of these vehicles, which became the US Navy's first unmanned underwater vehicles. Until 1979 the navy had been using a total of seven SPURVs [52]. One of the first, was able to dive up to 10 000 feet and operate 4 hours [37].

In 1985, the remotely operated vehicle *Argo* has found the wrack of the *Titanic* and four years later a World War II battleship *Bismarck* [37]. In the 1990's after two United States Navy ship badly damage by Iraq during Operation Desert Storm, the Navy initiated a program to create UUV to put the mines without notice from enemy side [37]. In 1994 the main objective of UUV program was to improve the systems to avoid the detection and dedicated minesweepers on sea surface. In 1996 was developed Near-Term Mine Reconnaissance System (NMRS) by Northrop Grumman, which was a two-vehicle platform to be launched from tube of submarine and was connected to the vessel by tether. Later the NMRS was replaced by LMRS- Long Term Mine Reconnaissance System [37].

The REMUS- Remote Environmental Monitoring Units are the most prolific family of UUV [37]. The commercially available vehicles include different designs as the REMUS 100AUV which is small and developed by Woods Hole Oceanographic Institution and produced by Hydroid Ins [52]. REMUS has been used to clear sea mines around the port of Umm Qasr. In this case, the UUV first time have been working in combat environment.

The hundreds of different UUVs have been designed, but only a few companies were managed to sell vehicles in significant amount. It was a time for experimentations, to define the potential of these vehicles. To big companies we can include Kongsberg Maritime, Bluefin Robotics, Teledyne Gavia and International Submarine Engineering Ltd [52]. Nowadays the market and designers want to follow commercial requirements. The future projects will include hover-capable UUVs, light-intervention and hybrid UUV design. It has to be remembered, that the market is driven by financial requirements and new designs will save a lot of money and expensive ship time.

In the 2008, new class of UUVs were developed, which design can be found in the nature. They are called biomimetic or bionic vehicles, which are able to achieve better degree of efficiency in maneuverability and propulsion, thanks to copy of successful designs from the nature. The example can be a Festo's AquaJelly and Evologics' Bionic Manta². The first vehicle is presented on the figure 1.3.

²Festo, <https://www.festo.com/group/en/cms/10227.htm>

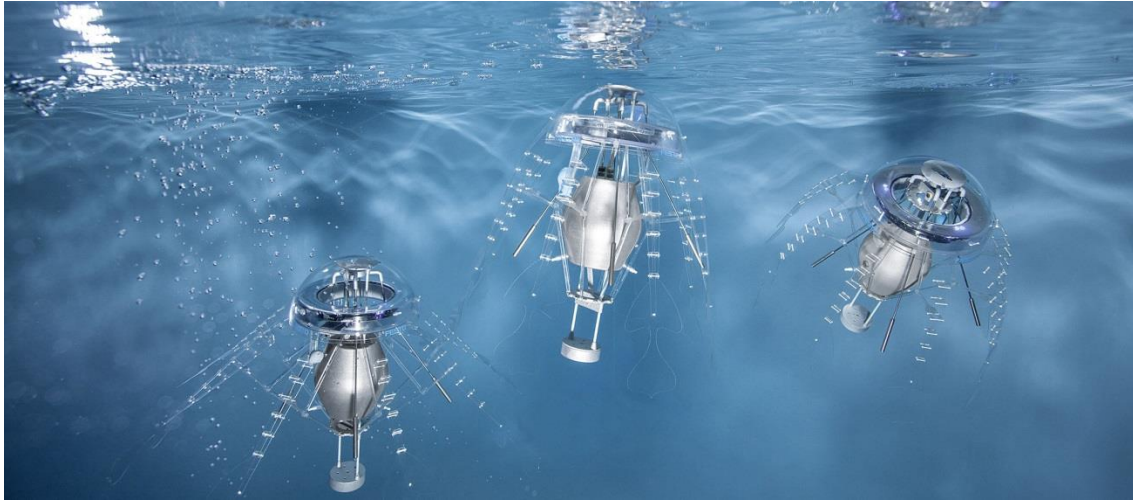


Fig.1.3. Festo's AquaJelly (Source: <https://www.festo.com/group/en/cms/10227.htm>)

1.3. UUV and risk assessment

All technologies, and ocean engineering is changing over the years. It has to be remembered, that in this branch of technology engineers are cooperating with the risk. Looking for a new technology like unmanned underwater vehicles engineers can expect that the risk assessment take on a slightly different dimension than this applied for conventional ships. To ensure reliability of UUV's engineers must to evaluate a new method or change a little older to perform a good risk analysis.

Engineers have to work with vehicles which are able to submerge and proceed their work without a help from direct people side. They have to deal with the dangers of submerged units, which are on the large depth and on the large distance from the operator. The operator is obligated to operate according to procedures, which ensure a safety of the vehicle but also a safety for people on the vessel or around of the equipment [51]. For designers, this device should be design in view of many varied perspective of risk, remembering about insurance companies, lawyers and regulators. Other requirements must be prepared for these devices than for ships.

At the beginning, unmanned underwater vehicles started operate but only as experimental vehicles, especially in area of military operations, but thanks to growth of technology, industrial companies are allowed to work with them. Thanks to latest miniaturizations and technical advances many of companies could afford to use UUVs. According to Manley J.E. [19], one of the reason of slow growth of using of these vehicles, is operational risks. Engineers have been trying to approach to the problem of risk assessment. The most critical phases of operations are launching and recovering of device. This assumption is true but especially for deep ocean vehicles, because they are operating in quite calm environment. Regarding to vehicles which are used in shallow water, near the shore, the most dangerous are uncharted obstacles or vessel traffic especially intensive in port area [24].

Coastal waters are the most dangerous for UUVs because of potential risks of man-made structures, human activity or environmental hazards [24]. It has to be remembered, that such episodes occur with relatively high frequency and can be presented at the same time. To achieve a high survival probability, it is necessary a risk mitigation strategy. The community over the years has addressed risk by practical implementation like design as simple as possible, the reference mission as unpretentious as possible and the supervision as accurate as possible [5].

In recent years, there have been several of vehicle losses, for example Autosub2 and the Autonomous Benthic Explorer- ABE [5]. The first case is the most high-profile loss, which had the place on 16 February 2005 under the Fimbulisen ice-shelf. In that case, a formal inquiry ascertained, that the loss of power or abort command could cause the vehicle loss. Second accident is more recently, the loss of ABE in March 2010, which had place during the exploring the Chile Triple Junction [41]. It was the first underwater vehicle of this kind. It was designed at the WHOI- Woods Hole Oceanographic Institution in 1990's [41]. There was no formal inquiry about loss of the ABE. The operation team and the designer ascertained, that the vehicle suffered an implosion of a glass sphere, which was used for providing buoyancy, which caused a quick destruction of on-board systems [5].

The risk analysis of UUVs has to be estimated during the design and the development [5]. It has to be remembered, that the likelihood of event depends on several different factors, such as vehicle's internal reliability, the operational environment, the experience and the competence of the design team, the quality of the maintenance program etc. It should be noted that different stakeholder has different interest in the risk. The scientist is interested in recover of data gotten by vehicles or in his availability at a given time. On the other hand, the owner of the underwater vehicles is more interested in the safe recovery it from the water [5]. The highest risk is the loss of vehicle, but the process of risk management can be applied for other risk like loss of data or failure of equipment. The UUV risk management process was developed specially to support decision making.

In recent years, a lot of approaches have been made to quantify the ongoing risk of vehicles which operate in different scenarios [24]. The surveyors provide probability of survival in most challenging setups (coastal waters) between 0.97 and 0.99 for mission ranges below 30 km [24]. Coastal water is the most demanding scenario for vehicles, because the potential risks are numerous, for example: environmental hazards, man-made structures, human activity etc. The frequency of such episodes is high and they can be occurred at the same time [12]. To achieve high survival probability, the risk mitigation and acceptability assessment have to be performed.

2. RISK MODEL AND TECHNICAL DESCRIPTION OF THE VEHICLE

2.1. Technical description of UUV Seaglider

To perform a good risk assessment, it is obligatory to define a system, which will be analyzed. Based on the objectives of the risk model, the system boundaries are formed. In the development of the system definition, it is assisted the establishment of the boundaries. The goal of the analysis defines the items included in external boundary region. This is important step in system modeling due to exacted analysis will depend on the system boundaries which were defined [11].

The Kongsberg is company from Norway which delivers systems for: marine automation, dynamic positioning, subsea survey and construction and satellite positioning [38]. Seaglider is one of the UUVs sold by company Kongsberg. In the table 2.1 is presented the technical description of Seaglider.

Table 2.1. Technical description of vehicle Seaglider

Weight and dimensions	
Vehicle main body length	1,8m-2m long
Vehicle maximum diameter	30cm
Weight (dry)	52 kg
Wing spam	1m
Antenna mast length	0.43-1m
Dive statistics	
Maximum travel range/ dive cycles	4600 km (approximately 650 dives to 1 km depth)
Operating depth range	50m- 1000m
Speed	0,4 to 0,6 kt
Variable Buoyancy Volume	850 cc
Glide angle	16-45° (1:3,5 to 1:1 slope)
Battery	
Battery type	Lithium Sulfuryl Chloride primary battery packs, 18 MJ
Battery life	Up to 10 months
Optional battery	
Battery type	Lithium ion rechargeable battery packs
Battery life	Up to 2 months
Electrical features	Mechanical features
Ultra-low power microprocessor	Isopycnal pressure hull
High capacity compact FLASH memory	No external moving parts
4 open serial channels for sensors	Low drag fiberglass composite fairing
Telemetry :Iridium Satellite link	
Guidance and control	
Dead reckoning between surface GPS fixes using a 3-axis digital compass	
Kalman filter prediction for mean and oscillatory currents	
Bathymetry map system and acoustic altimeter for near bottom dives	

(Source: [38])

The navigation is performed by combination of GPS when the vehicle is on the sea surface and of internal sensors which monitor the vehicle depth, attitude and heading during the dives. The biggest advantages of this equipment are low cost of it, versatile payload capability and long deployment capacity. Thanks to satellite communication, the Seaglider can obtain most of the data in near real-time [38]. Its model and robust design allow performing researches in any sea state and weather conditions. It is very good vehicle to obtain

oceanographic and marine information around the world. It uses a wings and small changes in buoyancy to achieve forward motion. This method is extremely efficient and causes the longest endurance of the system. Other devices from this company are using an electrically driven propeller [38]. Glider has to surface periodically to obtain its position, receive commands via satellite telemetry and transmit collected data.

The vehicle has an interior aluminium hull which resists pressure and a complex hull with flooded fiberglass fairing, ensures a streamlined laminar-flow shape [25]. Seaglider streamlined shape provides higher drag at low speeds as well lower for higher speed [25]. The pressure hull is milled into fluted pattern which provide appropriate compressibility to that of seawater, so buoyant diving force remains when the vehicle change depths [9]. Thanks of that, the vehicle saves a lot of energy especially at large operating depths [25]. The hull is consisted of series of supported (by ring stiffeners) deflecting arched panels. Compared with conventional hull, the compressible hull allow to saving pumping well over 100 cm^3 at the sea bottom of 1 km dive [9].

2.2. Safety features of UUV Seaglider

The UUVs are very expensive, so the designers put a lot of effort to guarantee security of these vehicles. The company Kongsberg provides the special safety features like:

- Emergency Localization
- Health Monitoring and
- Communication and Tracking

The vehicle can be equipped with emergency radio beacon, satellite communication and strobe light to assist with recovery operation and emergency localization. In the emergency situation, via the Iridium network, the position and status of the vehicle can be sent to base simplifying port and to the operators – the emergency localization. In the case if two-way satellite communication is enabling, from anywhere in the world, it is possible to transmit and obtain mission plan [38].

The vehicles are also equipped in special designed system to monitor the operation and the status of essential components. This system includes monitor of the sensors, communication, batteries and also conditions as depth and water ingress. In the case of some abnormality information, the alarm is raised. During supervised missions, this information will be transmitted to the operator, which is enabling to decide about continuation of the mission or about cessation of it. In the case if the vehicle is operating autonomously, the response is determined by reselected response which is programmed in the mission plan [38].

Via an acoustic or satellite link, the operators can monitor the glider's progress and the status. This communication allows to making amendments to the mission plan. Also many of vehicles are equipped with acoustic positioning systems which allow obtaining real-time position, as accurate as it is possible. When the gliders are on the water surface, they

can communicate via radio or Wi-Fi with the operator. The Seaglider is also equipped with the GPS receivers which are able to update the position and provide the most accurate information [38].

2.3. Principle of operation of Seaglider

The motion of vehicle is obtained by buoyancy control effect by deviation of vehicle-displaced volume. The pitch and the dive angle are controlled by shifting the internal mass (batteries) fore and aft [25]. Seaglider was designed to proceed with pitch angle between 16° from horizontal to 45° [38]. Seagliders have long cylindrical antenna (0.43-1m) mounted behind the principal vehicle body [25]. This antenna is raised above the sea surface by pitching the vehicle nose down in order to obtain communication and navigational fixes [25]. Seaglider uses lithium sulfuryl chloride batteries, which are better than alkaline batteries because of two reasons: they are better built (with a much longer shelf) and they have twice the energy per unit mass [25]. But they are more expensive and less safer (bigger possibility of explosive failure).

Seagliders use adjustable ballast instead of external control surfaces to obtain effect on vehicle attitude. Thanks to that, the vehicle is controlled with no external moving parts and making it more reliable [38]. Seagliders can dive and climb by adjusting their volume to be a little larger, smaller or equal to mass of seawater. The control of attitude is performed by moving mass inside the vehicle, which eliminates the need for active external parts [10]. It can operate in wider range of water density without constant adjustment of the static ballast thanks to vehicle's large variable buoyancy. Seaglider travels at slopes as 1:35 to 1:1 [38]. The steeper slope is used to maintain position which is called *virtual mooring* [31].

Gliders use the buoyancy in combination with wings to change the vertical motion into horizontal [31]. The wings provide hydrodynamic lift to drive forward as it sinks or rises. Thereby they propel themselves forward with low power consumption. Gliders are not so fast like AUV with electric motor-driven propellers, but thanks to buoyancy-based propulsion, they have high level in range and duration of operation. The buoyancy in this vehicle is obtained by moving oil in and out of an external bladder [31]. The main objective of the design is low energy use and cost, high reliability and easiness of operation to perform a mission comparable to ocean basin depths [10]. Because drag scales as the square of UUV speed, they have, of the speed, quadruples mission duration and also double vehicle range.

On the figure 2.1 is presented sketch of the Seaglider with marked the most important parts of the vehicle. These parts are: a- Flooded fiberglass fairing; b- Antenna mast; c- Wing; d- Rudder; e- Acoustic transponder; f- Electronics and 10 VDC lithium sulfuryl chloride primary batteries; g- Electronics and 24 VDC lithium sulfuryl chloride primary batteries; h- Isopycnal pressure hull; i- External bladder

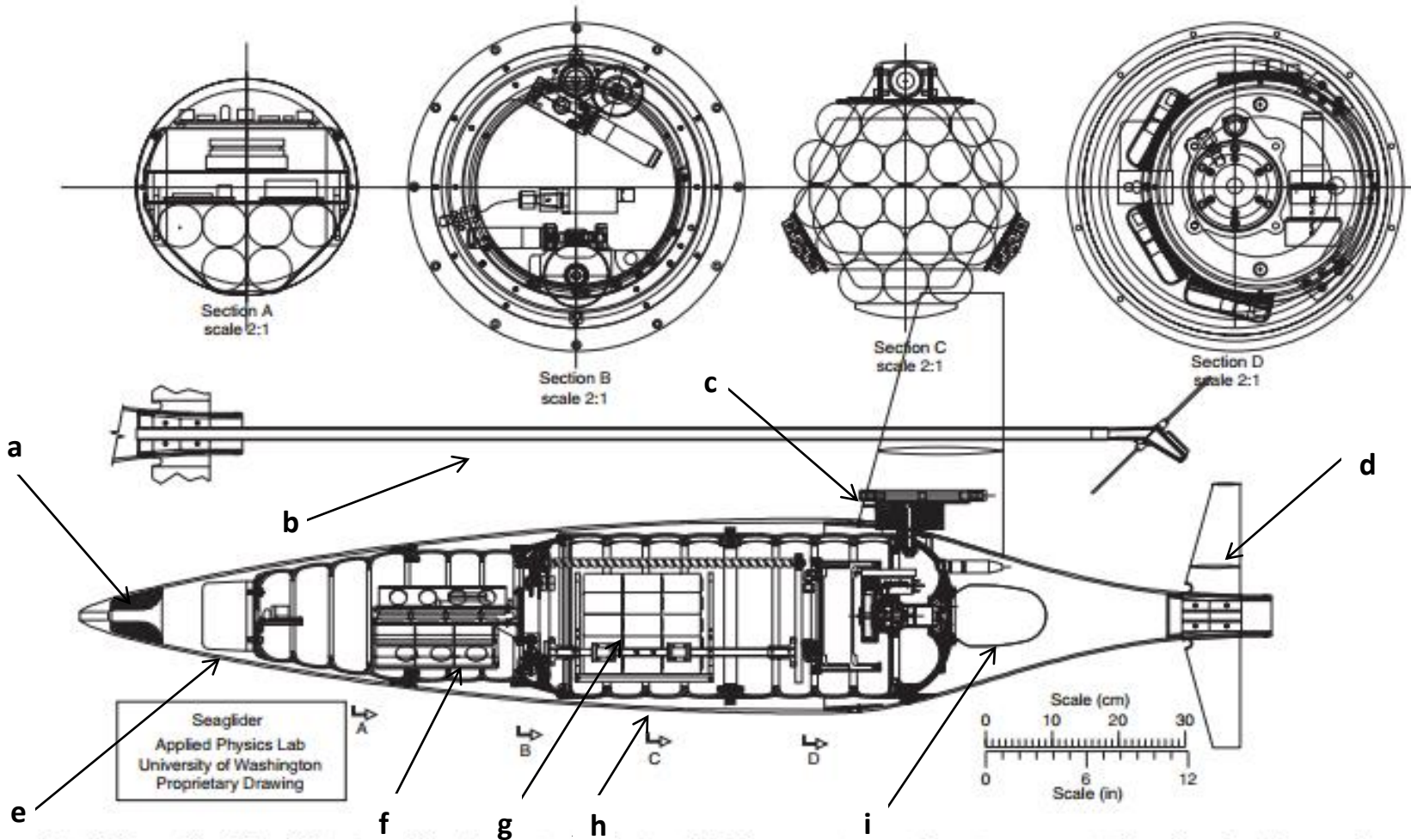


Fig.2.1. Sketch of the Seaglider and basics element including: hull cross section, the antenna mast, the wing plan section and side view (Source: [9])

2.3.1. Dive Cycle of Seaglider

Seaglider moves through the water in a special pattern which looks like saw-tooth, diving to the depths up to 1000 meters. To determine the position, send the collected data, and receive the commands via satellite telemetry, it has to surface periodically [38]. The dive cycle is composed of five main steps, which are presented on the figure 2.2. The vehicle uses the difference between actual displacement and its dead-reckoning to estimate depth-average current. By appropriate adjusted speed and direction to current averaged, it can set up vertically at a fixed geographic position which is called *the virtual mooring mode* [10].

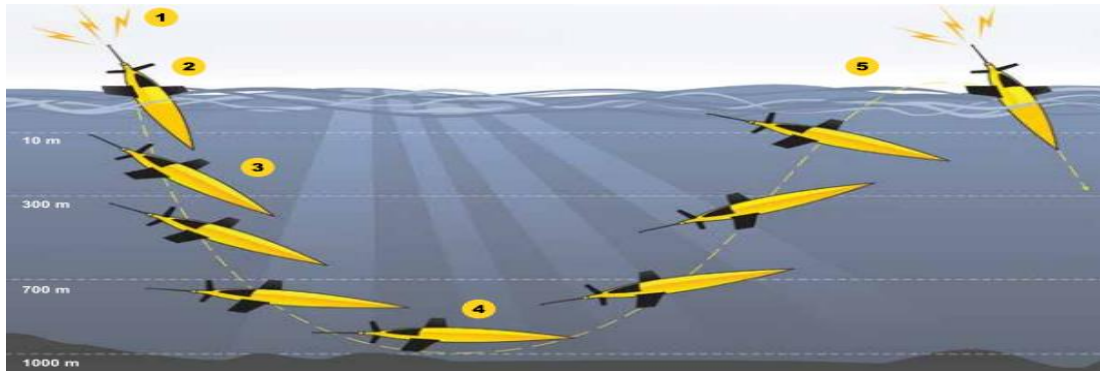


Fig.2.2. Seaglider dive cycle (Source: [38])

The diving cycle can be divided into 5 main steps:

1. Surface phase: First one is telemetry accomplished with iridium satellite communication [38]. At the water surface, the vehicle pitches downward to obtain approximately 45 degree to expose the antenna. This is obligatory to receive position from GPS and to transmit measurements data and receive new commands [38].
2. Diving phase: The vehicle converts its potential energy into kinetic one. To start this phase, it needs to empty its ballast and shift its inertial center to front part of body, by moving its battery [31]. On figure 2.3 is presented the scheme of moving the batteries packages, which allow changing the pitch of vehicle.

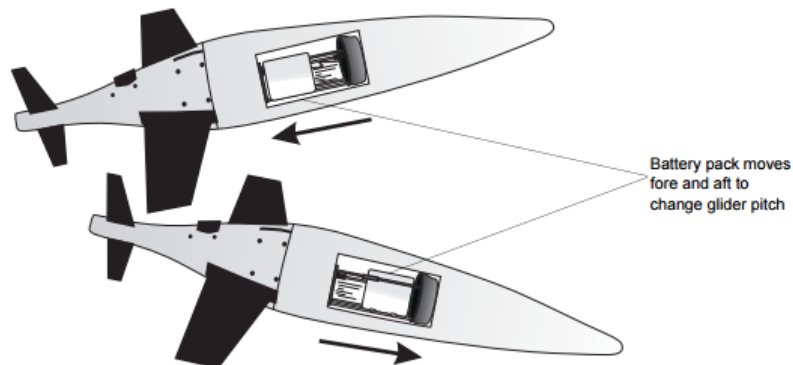


Fig.2.3. The mass shifter (batteries) causing pitch changes (Source: [47])

To change the vehicle buoyancy, it uses its external bladder.

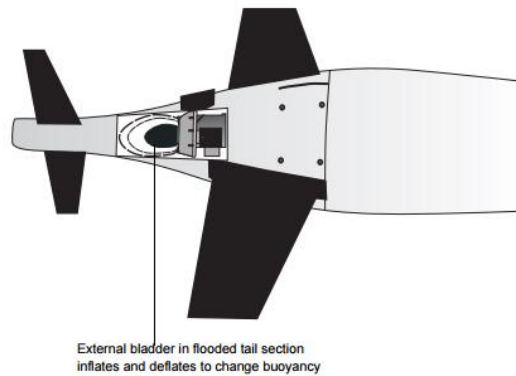


Fig.2.4. External bladder inflation and deflection (Source: [47])

3. Scanning phase: The vehicle uses its kinetic energy to dive. When the vehicle knows the distance to the target, the vehicle chooses the appropriate angle (slop) and bearing to approach it [38]. Under the water, the vehicle navigates using a 3-axis compass, altimeter and pressure sensor. Seaglider can dives maximum a depth of 1000 meters, and collect various oceanic data. To obtain the roll the vehicle moves the batteries from one side to other, which is presented on figure 2.5.

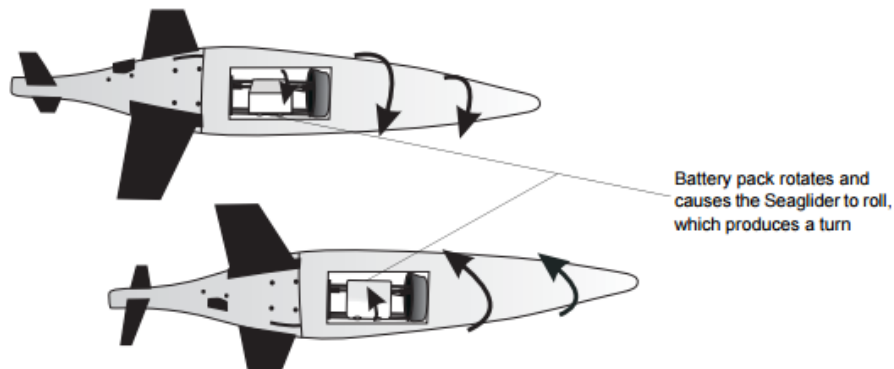


Fig.2.5. Mass shifter causing roll changes (Source: [47])

4. Ascension phase: When the velocity is too small to continue scenic, the glider is going up. In this phase, the vehicle moves its battery to his aft part and empties its ballast [31].

5. Reporting phase: After each surfacing the Seaglider dips its nose down in order to raise its antenna out of the water what allow to determining the position via GPS, uploads the oceanographic data, data telemetry satellite (via Iridium) and downloads the file with new instruction [31]. At the water surface, the vehicle pitches downward to obtain approximately 45 degree to expose the antenna. This is obligatory to receive position from GPS and to transmit measurements data and receive new commands [31].

2.3.2. System of launching and recovering

The launch and recovery is possible from small boats. The vehicle size was chosen to be suitable to contain necessary parts like buoyancy control system, centered on high-pressure pump, electronics and batteries to run the vehicle and to be able to be launching and recovery from smaller vessels.

The launch and recovery of UUV is one of the main challenges especially in open water and rough seas. The Seaglider weighs only 52 kilograms, so it can be easily carried by two people. Two main launching methods are presented on the following figures.



Fig.2.6. Launching methods for Seagliders (Source: [38])

2.4. Communication and navigation systems of vehicle

For UUVs, the issues like navigation and communication are very demanding aspects, because there are a little bit options for sent messages underwater [48]. First of all, the communication underwater uses acoustic waves which are less efficient comparing with electromagnetic waves. Above ground, it is possible to transmit data at speed approximately light speed, but in the water, the same signal has to pass through obstacle. In the Seaglider, this problem was solved by employment special diving cycle and the vehicle (antenna) can send the data when is above water surface.

The vehicle is equipped in standard components like: GPS, Iridium modem, Combined GPS with Iridium antenna, Acoustic transponder, 3-axis compass, base station software, external on-deck communication port, Kalman filter for mean and oscillatory currents and bathymetry map system with acoustic altimeter for near bottom dives [38].

The underwater altimeter at the beginning was using to measure the altitude of object above the sea bottom. Nowadays, altimeters from Kongsberg Mesotech's company are used in positioning, below surface monitoring and berthing. They have a robust design and are very easy to configurable by digital or analog outputs. They have wide range of operating depth (3000 m, 6000 m, and 11000 m) and are produced in wide range of models and frequencies.

The Kalman filter (linear quadratic estimator) is an algorithm which uses a series of measurements (over some time) containing: statistical noise and inaccuracies, and it is able to produce estimates of unknown variables. These unknown variables tend to be more precise, than these one based on a single measurement (based for example on Bayesian inference). This filter has a lot of applications in technology, especially in navigation, control of vehicles and guidance.

Bathymetric charts are maps which present the above water topographic bottom. They are created to present accurate and measurable description to visual the submerged terrain. The Global Positioning System also known as Navstar GPS is the most popular navigation satellite system, which provides geolocation and information about time to GPS receiver. This system has an intrinsic error source, which has to be taken into account. The main error is due to inaccurate time keeping by clock (receiver's). Other source of errors is atmospheric disturbances, reflection from building or another solid object, which distort the travelling signal before it reaches the receiver. The typical accuracy of GPS cannot be bigger than 3 meters. One of the causes is *Selective Availability*, which it is a purposeful disruption by US military.

Seaglider due to its properties found a lot of applications in Marine Biology (fisheries researches, aquaculture, seep sea ecology), in Physical Oceanography (climate changes, ocean observation), in environmental monitoring (emergency response, water quality, ecosystem assessment) or in offshore, oil and gas industry (baseline environmental assessment, geophysical survey) [38].

2.5. System representation

A main tasks of the representation of system is to enhance and facilitate the identification of different scenarios of events, which include all possible situations like large loads, chemical substances etc. The system can be present as a combination of different events acting on it [11]. Environment in which the system is working has to be taken into consideration. The vehicle is composed on different sub-system like: hull, sensors, navigational equipment, etc. To perform good risk analysis, all of the sub-systems and possibility scenarios have to be taken into account. On the figure 2.7 is presented the system representation. There is illustrated the area of operation, possible exposures, but also the sub-system like *Hull*, which has his own exposures. The sub-system *Hull* was illustrated as an example, but it cannot be forgotten that the system is composed of many different sub-systems.

The failure of the system which is caused by failure of the components is considered as a direct consequence [11]. The combination of constituent failures and the consequences cause appearance of indirect consequences. Indirect consequences can be caused for example by the loss of functionality of the system, caused by the one or more continued failures.

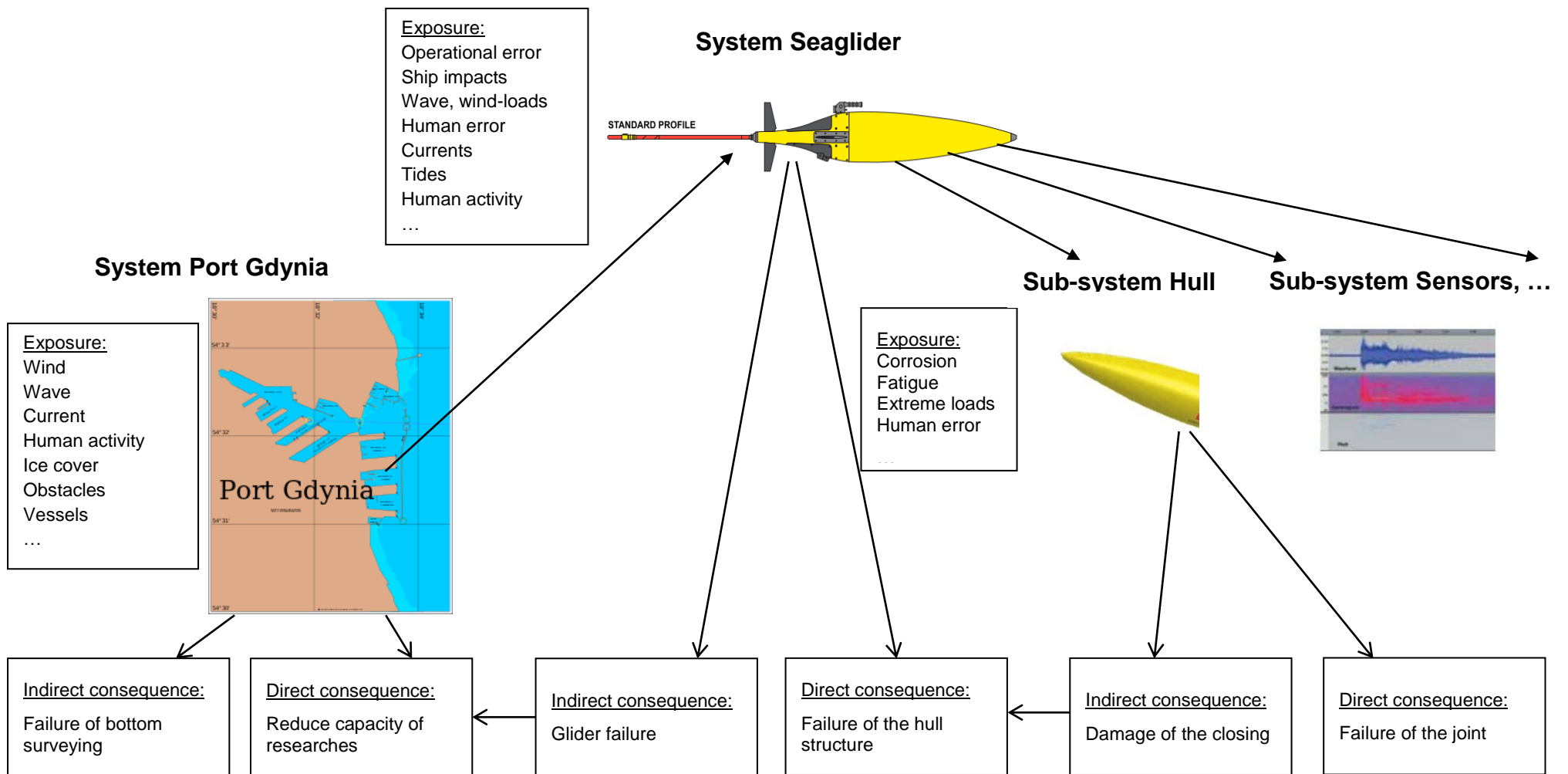


Fig.2.7. System Representation (Own development based on [11])

3. RISK ANALYSIS METHODS

3.1. Definition of risk and risk analysis

At the beginning, will be defined the word “risk”. In the literature are many different definitions, especially in different branch and sections of engineering. According to BusinessDictionary a risk is:

*“A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and small that be avoided through preemptive action.”*³ In short a risk is: *“the Possibility that something bad or unpleasant will happen”*⁴

According to Ayyub B.M. (Risk Analysis and Management for Marine Systems, p.3):

“Risk is defined as the potential for loss as a result of a system failure, and can be measured as a pair of factors, one being the potential outcome or consequence associated with the event’s occurrence. This pairing can be represented by the equation” 3.1:

$$\mathbf{Risk} \equiv [(\mathbf{p}_1, \mathbf{c}_1), (\mathbf{p}_2, \mathbf{c}_2), \dots, (\mathbf{p}_x, \mathbf{c}_x)] \quad (3.1)$$

Where:

\mathbf{p}_x - is the probability that the event x will occur

\mathbf{c}_x -is the consequence or outcome of the event’s occurrence

For each risk, two main assessments have to be done: likelihood and the consequences. Risk is also defined as the product of the likelihood (probability) of an event’s occurrence and the impact of the event, which illustrated equation 3.2 [2]:

$$\mathbf{Risk} \left(\frac{\mathbf{Consequence}}{\mathbf{Time}} \right) = \mathbf{Likelihood} \left(\frac{\mathbf{Event}}{\mathbf{Time}} \right) \times \mathbf{Impact} \left(\frac{\mathbf{Consequence}}{\mathbf{Event}} \right) \quad (3.2)$$

Risk analysis is connected with survey of the risk, their probability and evaluation. The formula implies that some form of qualitative or quantitative analysis has to be performed. Risk analysis is a process in which, first of all, hazard has to be identified and then analyzed and evaluated the risk connected with the hazard. The word hazard is often confused with the definition of the risk. According to dictionary a hazard is: *“an unavoidable danger or risk, even though often foreseeable”*⁵.

Risk analysis can be defined in many different ways, depend on how the risk is connected with other concepts. Risk management is broader definition and can be performed in seven steps [16]:

1. Establishing the goal and context
2. Risk identification

³Business Dictionary <http://www.businessdictionary.com/definition/risk.html>

⁴Merriam Webster <http://www.merriam-webster.com/dictionary/risk>

⁵Dictionary <http://www.dictionary.com/browse/hazard>

3. Analysis the risk
4. Evaluating the risk
5. Managing or treating the risk
6. Monitoring the risk
7. Communication (consulting with stakeholders and reporting)

To facilitate, the risk analysis can be divided into two main components: risk assessment which is associated with identification, evaluation and measure the probability and intensity of risk, and second component: risk management, where have to be decided what to do about the risks [15].

The first step is to understand the environment of the system. It means to get to know external and internal environment of the device. This part of analysis has to contain identification of constrains and opportunities. Methods to perform such a task are for example: SWOT and PEST which means in sequence Strength, Weaknesses, Opportunities and Threats and Political, Societal and Technological [21].

Second point, which is risk identification, is critical stage in good risk assessment process. Method of identification will depend on area of application: the nature of process, available resources, client's requirements etc. Risk identification of system may yield a large number of potential risks, what can make that each one will not be detailed analyze. In this step, fundamental methods are: HAZOP-Hazard and Operability studies, brainstorming, FTA- Fault Tree Analysis, logic diagrams o FMEA-Failure Mode and Effect Analysis [2].

To analyze the risk they have to be taken into consideration the source of the risk, the likelihood, and the consequences. In this point all techniques: quantitative, qualitative and semi-quantitative are acceptable, depend on the availability of the data. The risk matrix which is presented in figure 3.4 will be very useful in this step [16].

The forth step is to evaluate the risk, that means to compare it with the previously approved and documented tolerable risk criteria. If there is a situation in which the predictable risk is higher than tolerable, then the feature needs improvements in the effectiveness or additional control measures. The decision about acceptance of the risk has to be taken by appropriate designer or manager. The risk should be monitored and reviewed to ensure it remain acceptable [16].

If there is a situation that the risk cannot be acceptable, then it requires special treatment. They are available four treatment options: avoiding the risk, reducing the risk, transferring the risk or retaining the risk, which are illustrated on figure 3.1. In this step, the main process is to expand cost effective choice for treating the risk. These options are not mutually exclusive or appropriate, because this depends on the situations and outcomes. To choose appropriate kind of risk treatment, different factors should be considered like: if the possibility of the risk can be reduced or the consequences can be reduced [13]?

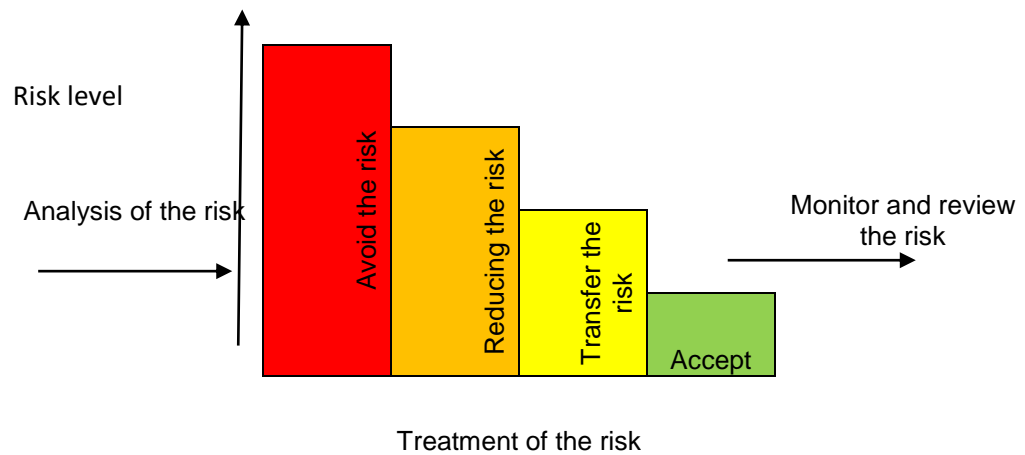


Fig.3.1. Treatment of the risk (Source: [13])

The sixth step is to monitor the risk. The risk has to be monitored continuously because the risk is dynamic and can change periodically. Also new risk can occur in the time of operation. In this step it is very important to describe how the outcomes will be measured. The period of reviews is determined by the environment, if the system is operating in variable and difficult environment, then the system has to be review more often.

The last step is communication, which is an essential stage of risk management process. To successful operation of system or organization is very important to reporting the risky situations. The reporting can be performed by annotation in documentation for example in management handbook [16]. The documentation is essential because can help in the future and provide history information about the causes, evolution and possible risks.

Risk analysis methods can be divided into two groups: quantitative or qualitative. The appropriate method depends on the availability of data and the level of knowledge of personnel. Risk assessment is a scientific and technical process in which the risk of event is modeled and quantified [2].

3.2. Quantitative risk analysis methods

Quantitative risk analysis is a technique concerned mainly on numerical calculations of probability over the possible consequences. This type of risk analysis tries to obtain numerically probability for the potential consequences. Often is called probabilistic risk analysis or probabilistic risk assessment– PRA [46]. This analysis often describes and present results in numerical units like dollars, live lost or time. Probabilistic risk analysis tries to find answers for following questions:

- What may happen? What can go wrong?
- How it is possible? What is the probability that it will happen?
- If it does happen, what consequences to expect?

The most widely known and adopted risk definition is this one proposed by Kaplan and Garrick [28]. In this quantitative definition of risk, the answer to the first question is denoted by S_i and defines a failure scenario. The second answer gives the information about probability,

which is denoted by p_i . The answer to the last question is the outcome or result Y_i , which is generated by the process-sequence of events. Thereby a risk is defined as a set of triples, and is formulated by equation 3.3:

$$\{S_i, p_i, Y_i\} \quad (3.3)$$

Where $i=1, 2, \dots, N$ and N is the total number of events which may happen, and should be big enough to form a “complete” set.

Each scenario is a totality of events illustrated formula 3.4:

$$S_i = \{F_{i1}, F_{i2}, \dots, F_{iK_i}\} \quad (3.4)$$

This information is produced for example by Fault Tree Analyses or similar methods which are associated with engineering safety studies [4]. Each of scenarios presents a thorough concentration of events. For example is F_{i1} is the initiating event which occurs with probability $p_i(1)$, then all succeeding event in this chain will occur with probabilities $p_i(k|k-1)$, and the likelihood of the scenario which is composed by K event presented by equation 3.5:

$$p_i = p_i(1) \cdot p_i(2|1) \dots p_i(K_i|K_i - 1) \quad (3.5)$$

The last two elements of risk definition proposed by Kaplan and Garrick specify a probability distribution over the result. The likelihood of the outcomes is identical to the likelihood of scenario. This is the Probabilistic Risk assessment heart.

To perform a risk assessment, people created several methods, which some of them are presented below in table 3.1. Each method is suitable in different stage of circle life or to obtain another result.

Table 3.1. Quantitative Risk Analysis Methods

Quantitative methods	Scope
Failure Modes and Effects Analysis (FMEA)	Inductive modeling approach. Identifies the components failure modes and the impacts on surrounding components of the system
Failure Modes Effects and Criticality Analysis (FMECA)	Inductive modeling approach. The same like FMEA
Fault tree Analysis (FTA)	Deductive modeling approach. Identify combination of equipment failure and human errors that can result in an accident
Event tree Analysis (ETA)	Inductive modeling approach. Identify various sequences of events, both failures and successes that can lead to an accident
Probabilistic Risk Analysis (PRA)	Methodology for quantitative risk assessment developed by the nuclear engineering community for risk assessment. This comprehensive process may use a combination of risk assessment methods.

(Source: [9])

In science this probabilities measure has been known a hundred years, but specific modes were developed specially to analyze engineering risk associated with space shuttle and nuclear power plants. Nowadays probabilistic risk assessment is applying in areas like climate changes, food safety, business or climate changes.





3.2.1. Fault Tree Analysis

Fault Tree Analysis (FTA) is deductive failure form of analysis. In this method undesired state of system is analysed using a Boolean logic to combine a series of lower-level events. This method is often used in fields like: safety engineering, reliability engineering, in fields like aerospace, nuclear power, pharmaceutical o high-hazard industries. This analysis allows understanding how and why the system can fail, shows the best way to reduce the risk, investigates potential faults and quantifies their contribution to system unreliability. In this method the graphical symbols are used, which are easy to understand and are based on Boolean logic.

First of all, analysis is performed from top and proceeds to down. Very important elements are: gates which are representing outcomes and events, which are representing inputs to the gates. At the top of tree is undesired outcome (root) for example failure of navigational system. Working backward from this event, they have to be determined the reasons that could cause this failure during for example normal operation or during maintenance operation. It should be remember that it is possible that are several different causes of failures. These causes introduce relations between events. When a specific event has a define failure probabilities, it can be calculated failure probabilities from tree analysis.

This analysis is based on Boolean algebra and every gate has their significance. Below in the table 3.2 are presented basic gates and theirs meanings.

Table 3.2. Basic gates used in Fault Tree Analysis

Gate	Illustration	Significant
OR		The output occurs if ANY input occurs
AND		The output occurs only if ALL inputs occur
Exclusive OR gate		The output occurs if EXACTLY one input occurs
Priority AND gate		The output occurs if the inputs occur in specific sequence

(Source: [33])

The Boolean algebra is the branch of algebra in which the values of the variables are denoted as 1 for truth values and 0 for false values. The main operations are the conjunction denoted as \wedge , the disjunction denoted as \vee and negation denoted as \neg . Symbols are used to describing logical relations in very similar way like original algebra describes numerical relations. These relations are presented in the table 3.3.

Table 3.3. Boolean algebra basic and composed operations

X	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$x \oplus y$	$x \equiv y$
0	0	0	0	1	0	1
1	0	0	1	0	1	0
0	1	0	1	1	1	0
1	1	1	1	1	0	1

(Source: [33])

From the basic operations can be obtained composed operations, including the following examples:

- $x \rightarrow y$ or Cxy is called material implication. If first value x is true, then the value of operation has a value of y . In other way, if x is false, the value of y can be ignored, because operation returns truth value.
- $x \oplus y$ or Jxy is called exclusive or XOR. Can be understand as $x \neq y$, being true only if x and y are different
- $x \equiv y$ or Exy is called equivalence or Boolean equality. It is true when x and y have the same value [33].

Based on Boolean algebra can be prepared a fault event tree. Starting from top event, have to be analyzed what can cause that event, and depending between the scenarios.

3.2.2. Event Tree Analysis

Event Tree Analysis is very similar especially in problem-solving, according to Fault Tree analysis but has some difference and they are used in different situations. Event tree analysis uses logical induction to proceed from general point of view to the specific, but Fault Tree Analysis is used to deductive reasoning or backward, in the other words, to move from general point of view to more specific. This type of analysis is also intended as a data-driven method.

The structure of an event tree involves following steps [20]:

- The identification of a first (initiating event) for accident sequence and its possibility of occurrence
- State the different components of the system, which can be affected by the initiating event
- Define the sequences of accidents though the different system workings assuming the two binary states : success state, failure state
- Designate possibilities or probabilities for the failure and success states
- Assign the Boolean expression for accidents assuming logical gate –AND
- Calculating the possibilities and probabilities of accidents sequence

When the main steps have been performed, then estimation of probability of each of sequences is needed [20]. In the system with binary nature the sum of probabilities of failure and success is equal to unity and can be formulated by equation 3.6:

$$P(S) + P(F) = 1 \quad (3.6)$$

After transformation the formula 3.6, the following equation 3.7 is obtained:

$$P(S) = 1 - P(F) \quad (3.7)$$

Assuming the independence of events and logical Boolean expression- AND in each accident sequence, the probability of the accident can be written as formula 3.8:

$$P(I, F_i, S_i) = P(I \text{ AND } F_i \text{ AND } S_i) = P(I)P(F_i)P(S_i) \quad (3.8)$$

And substituting from equation 3.7 into equation 3.8, following equation 3.9 is obtained:

$$P(I, F_i, S_i) = P(I)P(F_i)P(1 - F_i) \quad (3.9)$$

The possibilities or probabilities are generated from Fault Tree Analysis, which describes the top event estimating the probability of failure of each component in the system of interest. It is also possible to combine this two methods and carrying out joint analysis, which is presented on figure 3.2.

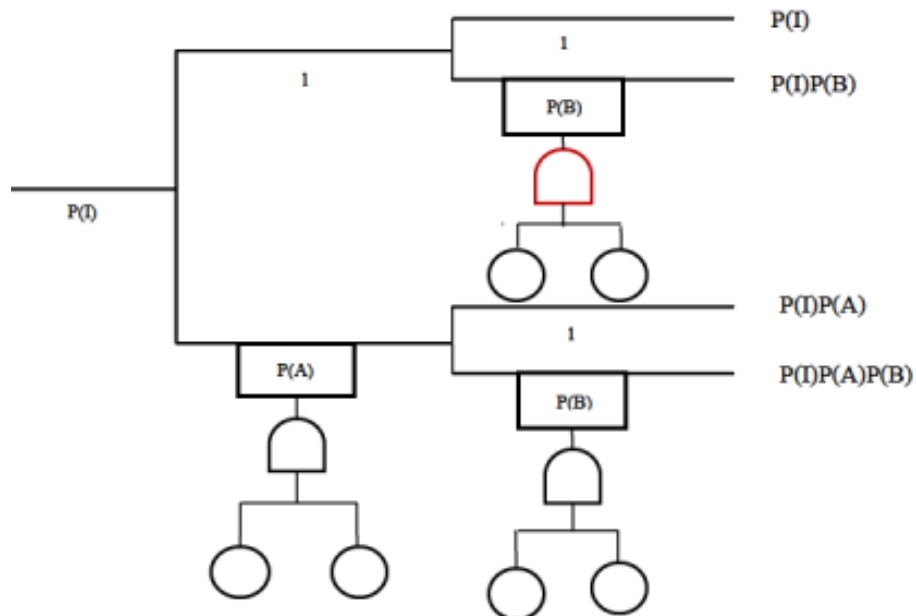


Fig.3.2. Coupling of Fault Tree Analysis and Event Tree Analysis (Source: [7])

3.3. Qualitative risk analysis methods

Qualitative methods can be used to screening the risk sources, but higher risks are subject to more complicated and expensive quantitative methods [16]. The risk can be estimated by qualitative methods using tools like: risk graphs, hazard matrices, risk matrices or monographs, but the most popular method is risk matrix [34]. In the table 3.4 have been collected different qualitative risk analysis methods.

Table 3.4. Qualitative Risk Analysis Methods

Qualitative methods	Scope
Safety/Review Audit	To identify equipment conditions or operating procedures that could lead to a casualty or result in property damage or environmental impacts
What-if	Identify hazardous situations, hazard or accident events that could result in undesirable and unwanted consequences.
Checklist	To ensure that organizations are complying with standard practice.
Preliminary Hazard Analysis (PHA)	Inductive modeling approach. Identify and their causes that can lead to undesirable consequences and determine recommended actions to reduce the frequency and/or consequences of the deviations.
Hazard and Operability Study (HAZOP)	Identify system deviations and their causes that can lead to undesirable consequences and determine recommended actions to reduce the frequency and/or consequences of the deviations.

(Source: [2])

3.3.1. Brainstorming

Brainstorming is mainly used to identify risks, hazards, stakeholders, risk management options or decision criteria. This is approach to obtain ideas from a group of people (participants), especially to generate a large number of creative ideas in short period of time, but does not involve the analysis. For successful brainstorming following inputs are required [36]: the problem which is well-defined, a team of people who has knowledge about the problem, a facilitator/mediator, good brainstorming technique and recording and disseminating the result of the process.

The output of a brainstorming could be a list of ideas, which can be later used for example in Fault Tree Analysis. The strengths of this action is that identifies new risks and new solutions, it is relatively easy to perform, it is quick and also involve key stakeholders and aids for communication overall. The weaknesses of these methods are:

- Social phenomena called “groupthink”
- Strong personalities or bosses which dominate the group
- Difficult to get the right mix of knowledge and skills in the group
- It is difficult to verify the effort (if it is comprehensive or not) [36]

3.3.2. Preliminary Hazard Analysis –PHA

In the industry different variants of PHA are known, sometimes under different names like: Hazard Identification (HAZID) o Rapid Risk Ranking [22]. This method is a semi-quantitative, which is performed to obtain 3 main objectives:

- to identify all accidental events and potential hazard which are possibly to cause an accident
- to rank accidental events according to their intensity
- and to recognize hazard controls and following activities

This type of analysis is used to study risk in early stage of a project. Thank of that, it can be identified accidental event, which may occur and can be estimated the severity of each action. It allows focusing on important issues and putting them in more detailed analyses. This analysis is very important for future detailed risk analysis of an existing system o system concept. If a simple system is analysed, this method can provide good and complete analysis. The Preliminary Hazard Analysis should consider objectives like [22]:

- dangerous components
- safety relations between different system elements (including also the software)
- environment, the constrains of environment
- fails of the system, subsystems and software's
- support equipment, property installed equipment and facilities
- safety procedures, safety equipment, maintenance, emergency procedures or possible alternate approaches

PHA consists of four main steps. First one is **prerequisites** like: establish appropriate PHA team, collect information about the risk from similar system or from precious operations. The good source of information can be accident data bases. They should be analysed: the system, system's description (block diagrams, drawings, etc.), environmental conditions, systems for detection hazards, emergency systems, etc. A good PHA team should consist of facilitator, secretary to report the results and team members who have an appropriate knowledge and experience [22]. Sometimes to identify all hazards and events, system must be split into parts. The result of this analysis can be reported using special worksheet and typical one is shown below on figure 3.3.

Example PrHA Worksheet				
Area: _____		Meeting Date: _____		
Drawing Number: _____		Team Members: _____		
Hazard: Potential Accident	Cause	Major Effects	Accident Severity Category	Corrective/Preventive Measures Suggested

Fig.3.3. PHA worksheet (Source: [42])

Second main step is **hazard identification**. It is important to consider all hazards and accidents which may happen. They have to be taken into consideration all parts of system, safety systems, maintenance operations and operational modes. All hazards shall be recorded. Sources of hazards should be analysed, some of them are common like: fire, explosion, moving parts, system incompatibilities, collision, toxic liquids, software error, human error, biological hazards etc. To identify hazards could be used following methods: brainstorming, examine existing system, review previous analyses of systems, consider hazardous materials, consider human errors or think about worst case using what-if analysis. The additional source of the data can be reports from authorities, dangerous occurrence reports, accident database or expert judgement.

Third step is to **estimate the frequency and the intensity** of each events. As was defined before, the risk is an event in function of the possibility and the severity of its consequences. The event may refer to wide ranges of consequences, from negligible to catastrophic. The intensity can be classified into broad classes. In the table 3.5 are presented example of classification of severity and frequency. Scenarios of different risk can be created by brainstorming or Fault Tree Analysis, Failure Mode and Effect Analysis (FMEA) or Event Tree Analysis (ETA). The probability can be presented either deterministically or probabilistically [22].

Table 3.5. Classification of hazard severity and frequency

Rank	Severity class	Description	Frequency class	Description
5	Catastrophic	Major injury or death of personnel	Frequent	Once per month or more often
4	Critical	Personnel exposure to harm chemicals, radiation, fire or release of chemical to the environment	Probable	Once per year
3	Moderate	Low level of exposure to personnel, or activates facility alarm system	Occasional	Once per 10 years
2	Minor	Minor system damage, not injury to personnel	Remote	Once per 100 years
1	Negligible	Without causes for system or personnel	Very unlikely	Once per 1000 years or more seldom

(Source: [42])

The risk is recognized as a combination of a given event's consequence and severity. This enable to ranking the events in a risk matrix, which is presented on figure 3.4. This is fourth step in the procedure- **risk ranking**.

Frequency/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic					
Critical					
Major					
Minor					

	Acceptable - only ALARP actions considered
	Acceptable - use ALARP principle and consider further investigations
	Not acceptable - risk reducing measures required

Fig.3.4. Risk Matrix (Source: [22])

This method has the advantages like: it ensures that the system is safe, it decreases design time thanks of reducing the number of surprises events and because the modification are cheaper and easier in earlier stages of work. The method has following disadvantages: interactions between hazards and are not easily known.

3.3.3. What-if method

What-if analysis is a method which uses a brainstorming to determine what can go wrong and judge the consequences and likelihood of these unwanted actions. The answers to these questions are useful to make judgment concerning the acceptability of the risk and they can help to determine a recommended action for these risks [39].

Review team consist of an experienced people, who can productively and effectively recognize issues concerning the system or process. Each member of the team, based on their knowledge and past experience of similar situation, is deciding what can go wrong. The team usually include people like: designer, operating engineers, maintenance personnel or safety representative, which has specific skills in fields like structural engineer, chemistry or radiation [39].

On each step of the process, what-if questions are asked and the answers are generated. The analysis is performed until all of the potential hazards are identified, because it provides minimization of the chance that some problem is not overlooked. The team makes assessment concerning the severity and likelihood. When some risk is unacceptable, the recommendations are made by the team for the next actions [39].

This type of analysis consists of three main steps. First one is developing the 'what-if questions' using previous documents and knowledge of the team. The questions can be formulated based on process upsets, equipment failures and human errors. All situations have to been analysed, during normal operation, construction, maintenance activities and debugging situations [39]. Different causes have to be taken into account like: equipment failure,

not trained operators, incorrect procedures, latest updates not used, utility failures such a gas or steam, external influences as weather etc. Personnel have appropriate knowledge of past failures and experience, which should be used to prepare what-if questions.

Second step is to determine the answers to questions: What can occur? What would be the result? If this step is performed correctly, the designers can solve not only safety problems but also minimize quality of operating problems. The last step is to assess the risk and making recommendations. The team members need to make assessment concerning the risk level and its acceptability.

3.3.4. Safety Checklist

The check list analysis is an evaluation against previously agreed criteria [42]. A checklist is used to reduce probability of failure by paying attention of human memory and attention [35]. It is systematic approach which is built on the knowledge and uses detailed analysis on high level. It is based on documentations reviews, interviews and field inspections. It is applicable for any system or activity, including human factors and equipment issues. Mostly it is performed by individual person, who is trained to understand checklist questions.

The performing of the checklist can be divided into seven steps, which are as follows [42]:

1. Definition of the activity or the system. Specification and definition of the boundaries
2. Definition of the problems for the analysis. Specification of the problems (environmental problems, safety issues or economic impacts)
3. Subdivision of the system or activity for analysis. Section of the subject into its major elements. At this level, the analysis will start.
4. Creation of relevant checklist. Identification and collection of important issues or questions related to the type of problems within the analysis
5. Answer to the checklist questions. The team of expert should respond to questions. Development of recommendations for improvement in case if the potential risk seems to be uncomfortable or unnecessary.
6. Subdivision of the elements of the system or activity. It may be necessary to perform more detailed analysis.
7. Using the results in decision making. Evaluation of recommendations and implementation, which will bring benefits over the life cycle.

This type of analysis is often using to guide team of inspectors about critical issues of the system. It is also used as a supplement to another method, especially to What-if analysis.

3.4. Software's used for risk assessment

Nowadays in engineering can be found different software's which are very helpful in the risk analysis. They are used in such branches like: financial sector, chemical or explosive industry. In the first branch, the QRA is used to calculate single loss expectancy. In chemical industry is used to define the potential loss of life (PLL) and in explosive industry to site risk analysis.

The risk analysis is very important issue in the engineering. To facilitate the work of specialists, many different software's were created, which are very helpful in the risk assessment. Below are presented programs used to perform this task:

- IMESARF- Institute of Makers of Explosive Safety Analysis for Risk
- RBM II- Risk Based Management II from Dutch Government
- iQRAS – ITEMSOFT Quantitative Risk Assessment System from ItemSoft
- Phast and Safeti- Integrated Consequence and Risk modeling from DNV GL

Existed also software's to assessment the risk used in naval industry or shipping sector like:

- Safeti Offshore- for Offshore structures with 3D real-time Modeling from DNV GL
- SOQRATES- Integrated Excel based system of Offshore QRA from DNV GL
- Shepherd- Frequency assessment software from Shell Global Solutions

For program Microsoft Excel exist special add-in packages which are available to perform risk analysis, for example Ersatz, ModelRisk industrial, Risk Solver pro or Risk analyzer [32]. Risk Analyzer is special add which allow performing tasks like: Monte Carlo Risk Analysis or automatically summary of results [32].

3.5. Basic definitions related to reliability

Reliability is: *"The ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time"*⁶. As a term *item* should be understood any component, system or subsystem. Mentioned required function can be a single function but also can be a combination of functions (if it is necessary to provide indicated service). Designed items are created to perform specified (one or more) functions, but, some of functions are activate and other are passive. In shortly reliability is the probability that the system will operate failure free in time $[0,t]$, what can be presented by formula 3.10:

$$R(t) = P(T > t); \text{ for } t > 0 \quad (3.10)$$

Where: T is time to failure

When the statistical distribution of the time to failure is known the probability density function of the time to failure $f(t)$ and the cumulative distribution function of the time to failure $F(t)$ can be used.

⁶ ISO 8402

Failure rate is the rate at which the failures can occur in the time interval and can be presented by formula 3.11:

$$h(t) = \frac{R(t_1) - R(t_2)}{(t_2 - t_1) \cdot R(t_1)} = \frac{R(t) - R(t + \Delta t)}{\Delta t \cdot R(t)} \left[\frac{\text{failures}}{\text{hour}} \right] \quad (3.11)$$

Mean Time to Failure (MTTF) denotes the mean functioning time and is formulated by formula 3.12:

$$MTTF = \int_0^{\infty} t \cdot f(t) dt = \int_0^{\infty} R(t) dt \quad (3.12)$$

The availability is:

*"The ability of an item (under combined aspects of its reliability, maintainability and maintenance support) to perform its required function at a stated instant of time or over a stated period of time"*⁷.

The availability at time t can be defines by formula 3.13 [23]:

$$A(t) = \text{Pr}(\text{item_is_functioning_at_time_t}) \quad (3.13)$$

Where functioning mean that the item is either able to operate or is in active operation. The average availability A_{av} is defined as mean proportion of time in which the item is functioning, and can be presented by formula 3.14:

$$A_{av} = \frac{MTTF}{MTTF + MTTR} \quad (3.14)$$

Where:

$MTTF$ –mean time to failure

$MTTR$ – mean time to repair

The reliability of system can be measured in different ways in different situation, for example using definition of MTTF, failure rate (number of failures per time), survival probability (the probability that the item does not fail in a time interval $(o, t]$) or availability at time t (the probability that the item is able to function at time t)

Important measures for the reliability have to been introduced like:

$R(t)$ –The reliability (survivor) function

$h(t)$ – The failure rate function

$MTTF$ –The mean time to failure

MRL –The mean residual life

Different probability distribution should to be used to model the lifetime of item like:

⁷ BS4778

- The exponential distribution (with parameter λ –failure (hazard) rate)
- The Weibull distribution (with β -shape parameter and α -scale parameter)
- The gamma distribution (in use three different parameterizations)
- The lognormal distribution (with parameters μ and σ as the mean and standard deviation $\ln(t)$)
- The normal distribution (with parameters μ as the population mean value and σ as the population standard deviation)

Time to failure:” is the time elapsing from when the item is put into operation until it fails for the first time.”⁸ The starting point is $t=0$. It is natural to understand that the time to failure as a T is a random variable. The relationship between the time to failure T and the state variable $X(t)$ is illustrated on the figure 3.5.

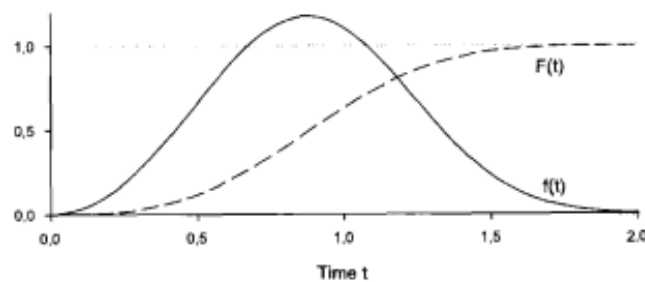


Fig.3.5. The relationship between the time do failure and the state variable $X(t)$ (source: [23])

3.5.1. Survival estimation- the Kaplan-Meier estimator

The most popular estimator of probability of survival is Kaplan-Meier estimator which is based on the failure history. The survival database consists of two different types of data: censored data and failure data [8]. A censored data is an observation in which failure was not observed and failure data present the recorded time at which failure has place. The Kaplan-Meier estimator is method to estimate the probability of survival, based on the historical data. The Kaplan-Meier estimator has formula 3.15:

$$S(k) = \prod_{i=0}^{i=k} \left(\frac{n_i - d_i}{n_i} \right) \quad (3.15)$$

Where:

n_i – Number of entries that haven't failed to interval i

d_i – Number of entries which have failed during interval i

$S(k)= 1$ for censored data

⁸ M.Rausand, A.Hoyland, *System reliability Theory. Models, Statistical Methods and Applications*, p.16

The estimator uses product rule to calculate probability of system surviving $S(k)$ in sequence of k intervals. The variance for this estimator is computed using Greenwood exponential formula⁹, defined as formula 3.16:

$$\hat{V}(k) = S(k)^2 \sum_{i=1}^{i=k} \frac{d_i}{n_i(n_i - d_i)} \quad (3.16)$$

3.5.2. Estimations in Statistics

Estimation in statistics is the process which makes inferences about all population based on information concerning a sample. An estimation of a parameter refers to population may be expressed in two ways [53]:

- point estimation of population parameter is a single value of a statistic
- interval estimate in which is defined interval by two numbers, between which a population parameter is said to lie

In the statistic the confidence interval is used to express the uncertainty and precision associated with a sampling method. Three parts make up the confidence interval: confidence level, statistic and a margin of error. The confidence level illustrates the uncertainty of a sampling method. The margin of error and the statistic describe the precision of the method. The range of values below and above the sample statistic is called the margin of error. To determine the confidence interval exist three different models:

- Model 1: The time to failure has a normal distribution. The mean time to failure is not known but the standard deviation of the time to failure is known
- Model 2: The time to failure has a normal distribution. The mean time to failure and standard deviation is not known (using Student's t-distribution)
- Model 3: The time to failure has an unknown distribution, the mean time to failure and standard deviation of the time to failure is not known. Sample size is large $n \geq 30$

In the Model 3 is applying the Central Limit theorem which says:

*"(...) the distribution of the sum (or average) of a large number of independent, identically distributed variables will be approximately normal, regardless of the underlying distribution."*¹⁰

Using this assumption (for $n \geq 30$), the confidence interval can be calculated like in Model 1, which is described by following formula 3.17:

$$\text{confidence interval} \in \left\langle \bar{x} - u_{\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}}, \bar{x} + u_{\frac{\alpha}{2}} \frac{\sigma}{\sqrt{n}} \right\rangle \quad (3.17)$$

The quantile of the normal distribution are presented in table 3.6.

⁹G. Rodriguez, *Non-Parametric Estimation in Survival Models*

¹⁰Central Limit Theorem, <http://www.math.uah.edu/stat/sample/CLT.html>.

Table 3.6. Quantiles of the normal distribution

α	0.9	0.95	0.975	0.99	0.995
$u_{\frac{\alpha}{2}}$	1.28	1.64	1.96	2.33	2.58

(Source: [17])

The standard deviation is approximate as σ , where the variance is expressed by formula 3.18:

$$\sigma^2 = \frac{1}{n-1} \sum_{i=1}^n (x_i - \bar{x})^2 \quad (3.18)$$

3.6. Human Reliability- SPR-H method

The proper functioning of system depends on different aspects like reliability of its technical elements, environmental conditions but also on human actions. These three things cannot be consider separately but consider as a holistically problem, treating the person as a component of system Man-Technology-Environment. In the engineering exists many different Human Reliability Assessments (HRA) methods like: Absolute Probability Judgement, Technique for Human Error Rate Prediction (THERP) or Accident Sequence Evaluation Program (ASEP).

Human Error Probability (HEP) is “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 even)”¹¹.

Performance shaping factor is (PSF)—“A factor that influences human performance and human error probabilities is considered in the HRA portion of the PRA. In SPAR-H, this includes: time available, stress/stressors, complexity, experience/training, procedures, ergonomics/human-machine interface, fitness for duty, and work processes”¹².

This method allows evaluating and identifying errors, which may happen, when person is acting on system. This method can be very useful, especially when it is difficult to find probabilities of failure (few failure databases). It can be assumed that in the large number of accident the crucial role plays human error.

The basis of this method is based on the special table, which contains different Performance Shaping Factor (PSF) like: available time, stressors, complexity, experience, procedures, ergonomics, fitness for duty and work processes. Two different tasks are taking into account: diagnostic and action. For each one, is given a Nominal Human Error Probability (NHEP), for diagnosis NHEP = 0,01 and for action NHEP = 0,001. This difference is because diagnosis is based on experience and knowledge to understand the situation and determine the action. In case of action, it is based mainly on diagnosis and involves work according

¹¹ NUREG/CR-6883, 2005

¹² NUREG/CR-6883, 2005

guidelines and procedures. The dependency of these two issues can be modelled in case if one of the tasks involves two actions. The special table, which allows to assessing if the tasks are involved by two actions, can be found in U.S. Nuclear Regulatory Commission, *The SPAR-H Human Reliability Method* (NUREG/CR-6883(2005)).

To find the human error probability, two formulas are used. First one, formula 3.19 is used when more than three PSF are bigger than 1. In the other cases formula 3.20 is used.

$$HEP = NHEP \cdot \prod PFS \quad (3.19)$$

$$HEP = \frac{NHEP \cdot \prod PFS}{NHEP \cdot \prod (PSF - 1) + 1} \quad (3.20)$$

In the case if two actions are taken into account (action and diagnosis) them the probability can be calculated from equation 3.21:

$$P_{d/a} = \text{Diagnosis HEP} + \text{Action HEP} \quad (3.21)$$

At the beginning, this method has been used in the nuclear industry. The method can be applied in this thesis because Unmanned Underwater Vehicle is complex system which requires a high level of skill of personnel and wrong decision can lead to an undesired outcome. In the other hand this method is complex and different environments can be modelled. In the table 3.7 are listed all PSF and descriptions of levels.

Table 3.7. PSF in the SPAR-H method

PSFs	PSF Levels	Multiplier for Diagnosis	Please note specific reasons for PSF level selection in this column.
Available Time	Inadequate time	P(failure) = 1.0 <input type="checkbox"/>	
	Barely adequate time ($\approx 2/3 \times$ nominal)	10 <input type="checkbox"/>	
	Nominal time	1 <input type="checkbox"/>	
	Extra time (between 1 and $2 \times$ nominal and > 30 min)	0.1 <input type="checkbox"/>	
	Expansive time $> 2 \times$ nominal & > 30 min	0.1 to 0.01 <input type="checkbox"/>	
Stress/Stressors	Insufficient Information	1 <input type="checkbox"/>	
	Extreme	5 <input type="checkbox"/>	
	High	2 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
	Insufficient Information	1 <input type="checkbox"/>	
Complexity	Insufficient Information	1 <input type="checkbox"/>	
	Highly complex	5 <input type="checkbox"/>	
	Moderately complex	2 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
	Obvious diagnosis	0.1 <input type="checkbox"/>	
Experience/Training	Insufficient Information	1 <input type="checkbox"/>	
	Low	10 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
	High	0.5 <input type="checkbox"/>	
	Insufficient Information	1 <input type="checkbox"/>	
Procedures	Insufficient Information	1 <input type="checkbox"/>	
	Not available	50 <input type="checkbox"/>	
	Incomplete	20 <input type="checkbox"/>	
	Available, but poor	5 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
Ergonomics/HMI	Insufficient Information	1 <input type="checkbox"/>	
	Diagnostic/symptom oriented	0.5 <input type="checkbox"/>	
	Good	0.5 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
	Poor	10 <input type="checkbox"/>	
Fitness for Duty	Insufficient Information	1 <input type="checkbox"/>	
	Unfit	P(failure) = 1.0 <input type="checkbox"/>	
	Degraded Fitness	5 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
	Insufficient Information	1 <input type="checkbox"/>	
Work Processes	Insufficient Information	1 <input type="checkbox"/>	
	Good	0.8 <input type="checkbox"/>	
	Nominal	1 <input type="checkbox"/>	
	Poor	2 <input type="checkbox"/>	

(Source: NUREG/CR-6883, 2005)

4. RISK ANALYSIS

Because of modern design methods for bridges, buildings or vessel they can survive extreme storms are exemplified of development of design methods which are great success in controlling of the risk. UUVs have a lot of different sources of risk like: human error, equipment failure, external event etc. First source, can be met when the crew is lack of skill, they are exhausted, fatigued or commit sabotage. Equipment failure is the most frequently hazard of marine systems, such a loss of steering or loss of electrical power. To external events can be included a collision with other object, grounding, sea state, or demanding weather conditions [6].

4.1. Failure database- Project GROOM

To perform a proper risk assessment, it is obligatory to has the information about the same (or very similar) object, which had a possibility to work in its proper environment, or to perform a lot of different tests to check if the object is safety and suitable to work. The Project GROOM – Gliders for Research, Ocean Observation and Management, accumulated 18 European partners to work together to “*design a new European Research Infrastructure that uses underwater for collecting oceanographic data*”¹³. The participants provided operational data from period of 2 years. The participants by online survey entered data like: vehicle identifier, start of mission, mission type, vehicle type, maximum depth, did the mission end with success or with failure or was the vehicle recovered at the end of mission [8]. If the mission has not finished with the success, the user had to select from 15 options, the primary cause of the failure. The options were as follows:

- Collision with the vessel
- Collision with seabed
- Collision with net or other obstacle
- Leak
- Iridium communications failure
- Power/battery failure
- Buoyancy pump failure
- Onboard software failure
- Control/command software failure
- Navigation sensor failure
- Data logging failure
- Altitude control
- Sensor failure
- Attitude sensor failure (roll, pitch, heading)
- Other failure

¹³ Brito M.P. Underwater slider reliability and implication for survey design, 2014

To the project, 205 missions have been reported, which were carried by 56 underwater gliders. The number of gliders and number of missions for different institutes are presented below in the table 4.1.

Table 4.1. Number of gliders and the number of missions in project GROOM

Center Name	Number of missions	Number of vehicles	Medium endurance (days)	Area of operation		
				Shelf % (number)	Shelf edge % (number)	Deep ocean % (number)
Centre National de la Recherche Scientifique	56	14	32	12 (7)	84(47)	4(2)
Consejo Superior de Investigaciones Cientificas	14	5	19	-	-	100 (14)
Isituto Nazionale di Oceanografia e di Geofisica Sperimentale	4	2	13	75 (3)	-	25 (1)
Alfred-Wegener-Institut fur Polar- und Meeresforschung	8	4	69	-	-	100 (8)
Consortio para el Diseno, Construccion, Equipamiento y Explotacion de la Plataforma Oceanica de Canarias	14	4	13	7 (1)	22 (3)	71 (10)
University of East Anglia	12	8	49	42 (5)	50 (6)	8 (1)
Oceanography Centre, University of Cyprus	7	2	80	71 (5)	29 (2)	-
Institut fur Meereswissenschaften	3	1	14	-	-	100 (3)
Helmoltz-Zentrum Geesthacht-Zentrum fur Material- und Küstenforschung	12	2	23	100 (12)	-	-
North Atlantic Treaty Organization	63	8	4	33 (21)	30 (19)	37 (23)
Scottish Association for Marine Science	3	2	123	-	33 (1)	67 (2)
Natural Environment Research Council	9	4	39	-	33 (3)	67 (6)

(Source: [8])

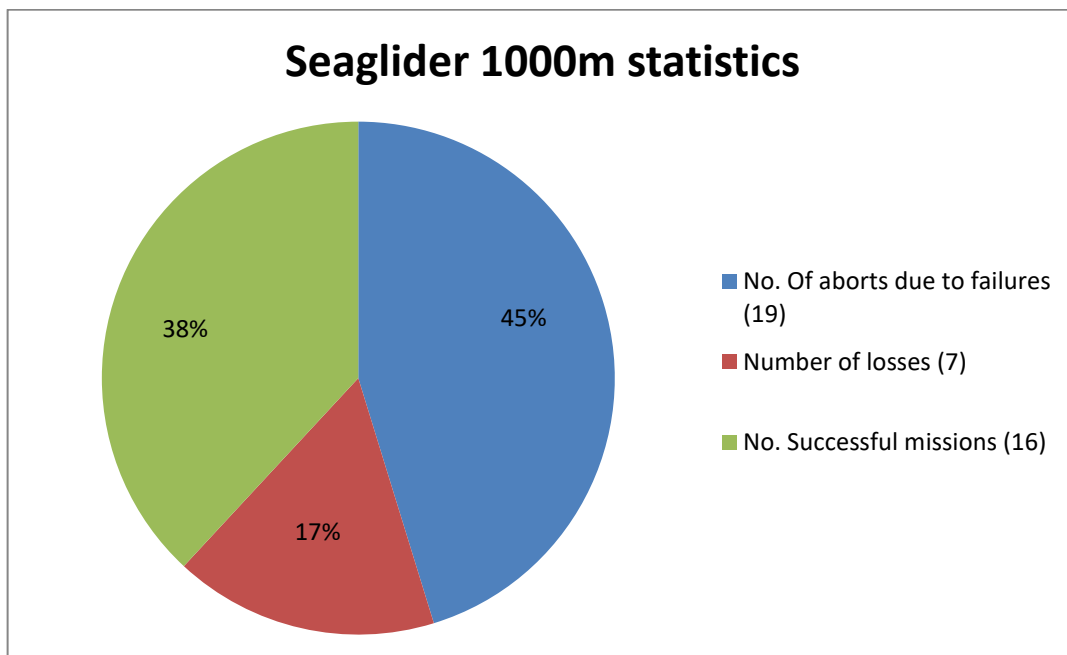
It is very important to remember that success of missions not depend only on the reliability of the particular type of UUV but also on the factors like the environment, the service history or on the procedures and on the practices of the operators [14]. Also the available options for recovery of UUV could lead on loss of the device [8]. In the table 4.2 is presented summary of glider's operation statistics depend on the type of vehicle based on the data from project GROOM [45].

Table 4.2. Operation statistics of different types of gliders

	Seaglider 1000m	Slocum G1 shallow	Slocum G1 deep	Slocum G2 shallow	Slocum G2 deep
Number of missions	42	68	72	9	14
Total endurance (days)	2514,5	772,05	1728	188	550,1
Median endurance (days)	64	7,65	19,5	18	12
Upper quartile (days)	80	15	37	25	25,8
Max endurance (days)	169	56	105	48	184
No. of aborts due to failures	19	13	23	3	5
Abort rate (per day)	0,00756	0,0168	0,0133	0,0159	0,00909
Number of losses	7	2	1	0	0

(Source: GROOM Project database)

After analyzing the data about failures of Seaglider in project GROOM, it is possible to prepare a graph which illustrate the percentage of mission, which are finished with successfully, missions, which have to be canceled due to failure and number of vehicle lost. The diagram 4.1 illustrated that from 42 missions (for Seaglider), only 16 of them have finished with success. On the other hand, 7 missions have finished due to the loss of vehicle.



Diag.4.1. The percentage of the missions finished with failure (mission abort), losses of vehicle and missions successful (Own development, based on data from project GROOM [45])

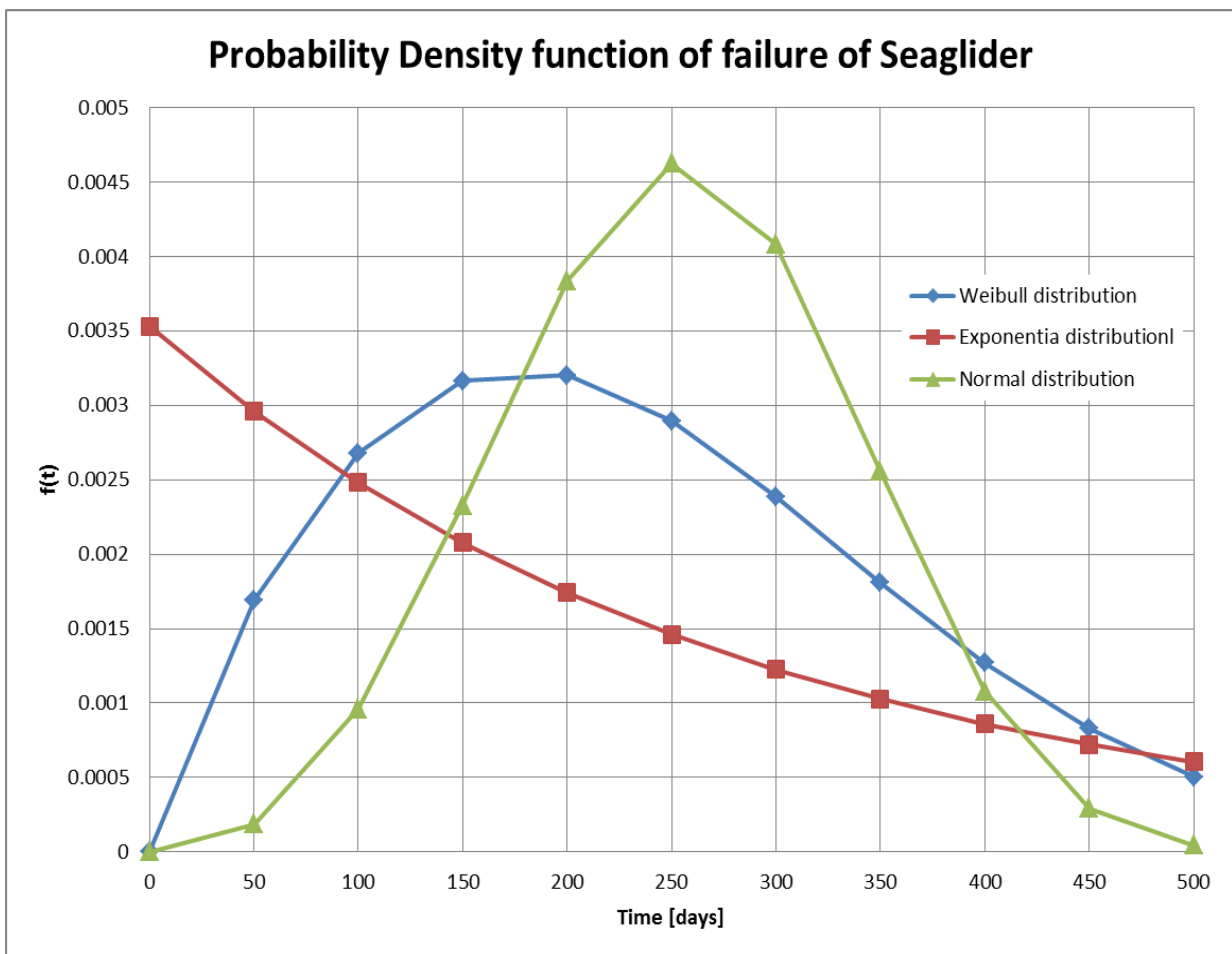
4.1.1. Probability density function of failure of Seaglider

The gliders sold by Kongsberg Company are Seagliders type 1000 meters. In the table 4.2 in the second column is information about number of missions, times of endurance and number of losses of this type of equipment. Using definition of Weibull distribution, it is possible to calculate and present probability density function which is described by equation 4.1 [32]:

$$f(x, \lambda, \beta) = \begin{cases} \frac{\beta}{\lambda} \left(\frac{x}{\lambda}\right)^{\beta-1} e^{-\left(\frac{x}{\lambda}\right)^\beta}, & x > 0 \\ 0, & x < 0 \end{cases} \quad (4.1)$$

The scale parameter λ is defined as time (range) after which 63,2% of devices will be failure. The shape parameter β is used to model situations where probability of failure changes over time and can obtained following values:

- $\beta < 1$, indicate that failure rate decreases over time
- $\beta = 1$, failure rate is constant (Exponential distribution)
- $\beta > 1$, failure rate is increasing with time



Diag.4.2. Probability Density functions of failure of Seaglider (Own development)

If parameter β is equal to 3.4, the probability density function will have normal distribution [17]. On the diagram 4.2 is presented three different probability density functions:

normal distribution (green), exponential (red) and Weibull distribution (blue). To calculate possibility of loss of Seaglider, it has to be calculated integral of these functions in defined boundaries, which is formulated by equation 4.2 [44]:

$$P(B) = \int_B^A f(x)dx \quad (4.2)$$

4.1.2. Percentage of reasons of failures

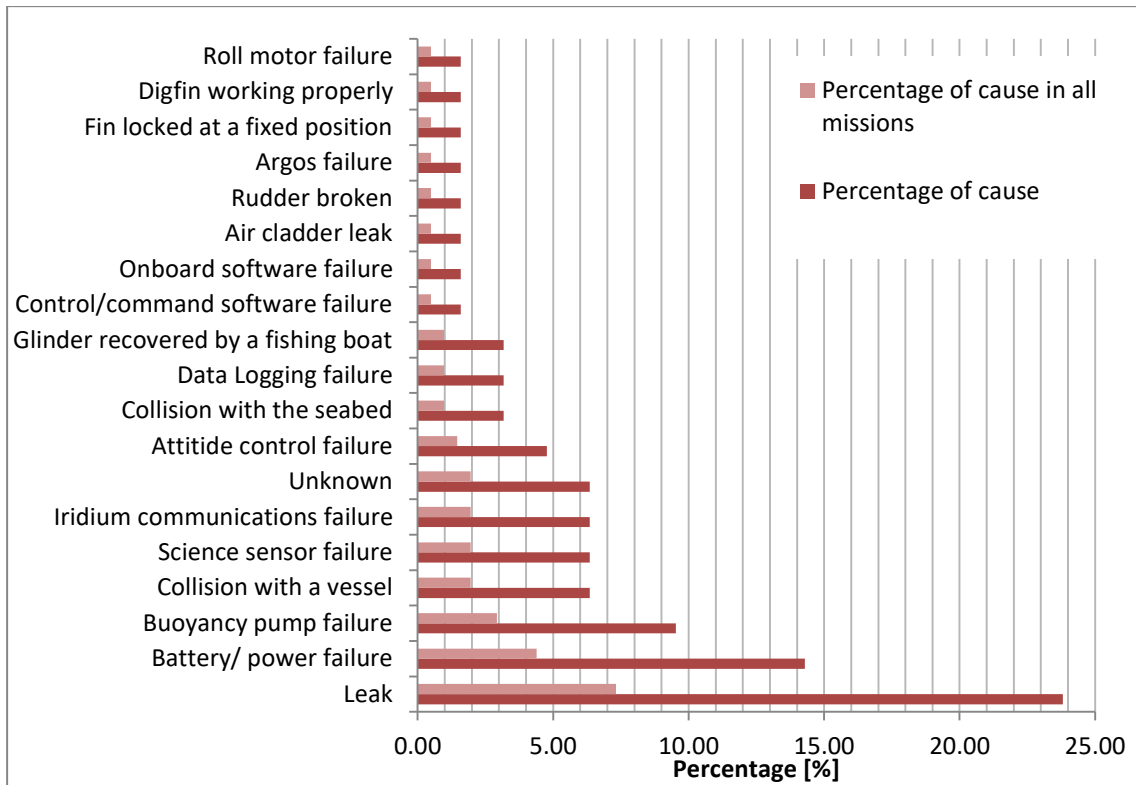
To the project GROOM was reported 205 missions and 63 of them were abort. The project specified seventeen different failure modes, which are presented below in the table 4.3 and on the diagram 4.3.

Table 4.3. Number of failures and aborts in function of different causes

Cause:	No. of failures	Percentage of cause [%]	Percentage of cause in all missions [%]
Leak	15	23,81	7,32
Battery/ power failure	9	14,29	4,39
Buoyancy pump failure	6	9,52	2,93
Collision with a vessel	4	6,35	1,95
Science sensor failure	4	6,35	1,95
Iridium communications failure	4	6,35	1,95
Unknown	4	6,36	1,95
Attitude control failure	3	4,76	1,46
Collision with the seabed	2	3,17	0,98
Data Logging failure	2	3,17	0,98
Glider recovered by a fishing boat	2	3,17	0,98
Control/command software failure	1	1,59	0,49
Onboard software failure	1	1,59	0,49
Air bladder leak	1	1,59	0,49
Rudder broken	1	1,59	0,49
Argos failure	1	1,59	0,49
Fin locked at a fixed position	1	1,59	0,49
Digifin not working properly	1	1,59	0,49
Roll motor failure	1	1,59	0,49
Number of aborts	63	100	30,73
Number of missions	205	30,73	

(Source: [8])

The main cause of the failures was: leak (23,81% of total failures), battery/power failure (14,29%), buoyancy pump failure (9,52%), collision with a vessel, science sensor failure, iridium communicate failure and unknown cause (each of 6,35%)



Diag.4.3. The percentage of the specific cause in the general number of failures and missions (Source: Own development based on [8])

4.2. Difficult area of operation

4.2.1. Coaster water analyzed using Preliminary Hazard Analysis

It was assumed that the researches are performed in Polish Port- Gdynia. It is the port on the Baltic Sea. The position of the port is: $\phi: 54^{\circ}32'10\text{ N}$, $\lambda=018^{\circ} 33'61\text{ E}$. The harbour is one of the most modern and largest ports within the Baltic area, which can handle with all kinds of cargo. The density of water is 1.06 g/cm^3 . The approach channel in 2009 had a depth 14.1m.

There are abnormal water levels: during long period of W winds the water level increase up to 0.6 m, E winds can decrease the water level by 0.5 m. In 2009 to Gdynia port arrived 3700 vessels with 32.5 millions of tons of cargo. The port is generally free of ice. Ice formation can occur especially from February to March. Winds from N, E and S can cause shifting ice fields in the roadstead which may create problems for small and medium-sized vessels. There is generally a weak N current set off the entrance to Gdynia Harbour. During winds from N to NE the set may turn to the S. Depending on the strength of the wind, the current may attain a rate of 2 kn.

A lot of failures have place in the coastal waters. To analysis it has been chose port in Poland- Gdynia. It was chosen fourteen different hazards which can meet the Seaglider in operation on the coastal waters which are presented in the table 4.4

Table 4.4. Preliminary Hazard Analysis for conditions of coaster water

Ref.	Hazard	Probable causes	Probability	Severity
1	Collision with vessel	Poor commands, errors in navigation, not trained operator, human errors, unexpected/unreported movement of ship in the area, prohibited movement of the vessels	Remote	Catastrophic
2	Collision with other UUV	Poor commands, errors in navigation, not trained operator, human errors, unreported movement of other UUV	Very unlikely	Critical
3	Getting stuck in net	Unmarked nets, nets in prohibited area, errors in navigation	Remote	Moderate
4	Getting stuck in ice	Unexpected glaciations, errors in navigation	Remote	Moderate
5	Pushed by strong current	Bad measurements, not taken into account information about currents in area, unexpected current	Very unlikely	Minor
6	Pushed by high tide	Bad measurements, not taken into account information about tides in area, unexpected high tide	Very unlikely	Negligible
7	Collision with wrack	Uncharted wrack, poor commands, human error, not trained operator, previously untested area, errors in navigation	Remote	Catastrophic
8	Grounding	Poor commands, human error, not trained operator, errors in navigation, bad data about bottom	Occasional	Moderate
9	Collision with marine infrastructure	Poor commands, errors in navigation, uncharted marine infrastructure	Occasional	Critical
10	The human activity	Unexpected human activity, human activity in prohibited area, unreported human activity	Probable	Negligible
11	Collision with the anchor chain	Vessel anchoring in inadequate position, poor commands, uncharted area of anchoring, previously untested area	Very unlikely	Moderate
12	Hit during recovering	Unexpected current or wave, bad measurements, poor commands, not trained operator	Remote	Catastrophic
13	Loss of vehicle	Human error, unexpected obstacles, error of equipment or software	Very unlikely	Catastrophic
14	Problems with launching	Poor commands, errors in setting up the vehicle, human error, unexpected weather conditions	Remote	Moderate

(Source: Own development)

Using the Risk Matrix, from table 4.5, it is possible to determine which hazards in view of likelihood and severity are the most demanding. The most demand scenario for Seaglider operating in coastal water are: collision with vessel, with wreck or with marine infrastructure.

Table 4.5. Scales to assess the probability and severity of hazards and Risk Matrix

a) Scale of severity and probability

Severity classes		Probability classes	
5	Catastrophic	5	Very unlikely
4	Critical/ significant	4	Remote
3	Moderate	3	Occasional
2	Minor	2	Probable
1	Negligible	1	Frequent

b) Risk Matrix

Likelihood (Probability)	Impact (severity)				
	1	2	3	4	5
1	Low medium	Medium	Medium High	High	High
2	Low	Low Medium	Medium	Medium High	High
3	Low	Low Medium	Medium	Medium High	Medium High
4	Low	Low Medium	Low Medium	Medium	Medium High
5	Low	Low	Low Medium	Medium	Medium High

(Source: Own development based on: [22])

4.2.2. Comparison between areas of operation- based on Kaplan Maier estimator

To analyze the quality of operation of glider in the different areas, the information about numbers of aborts in shelf and shelf-edge has to be taken into consideration. The information about the number of missions, vehicles and aborts is presented in table 4.1, which shows information about missions in coastal water and on deep sea from the Project GROOM. The totally number of shallow water missions is 135; 54 missions on shelf and 81 missions on shelf edge. The totally number of deep ocean missions is 70. The survival estimation can be based on Kaplan-Maier Estimator, which is presented by equation 4.3:

$$S(k) = \prod_{i=0}^{i=k} \left(\frac{n_i - d_i}{n_i} \right) \quad (4.3)$$

Where:

n_i – Number of entries that haven't failed to interval i

d_i – Number of entries which have failed during interval i

Three different regions of operations have been analyzed. The missions were performed on shelf, shelf edge and on deep ocean. For different scenario, they were calculated medium endurance times and probabilities of survive based on Kaplan-Maier Estimator. In the table 4.6 are presented obtained results.

Table 4.6. Probability of survive for different areas of operation based on Kaplan-Maier Estimator

a) Operation on shelf

SHELF	54	missions				
Medium endurance 23.7		days				
	Interval (days)	Number of entries n_i	Number of failure d_i	Failures/ Entries	Survival	Probability of survive
S(K)_0	32	7	1	0.143	0.857	0.86
S(K)_1	45	6	1	0.167	0.833	0.71
S(K)_2	58	5	1	0.2	0.8	0.57
S(K)_3	107	4	1	0.25	0.75	0.43
S(K)_4	130	3	1	0.333	0.667	0.29
S(K)_5	134	2	1	0.5	0.5	0.14

b) Operation on shelf edge

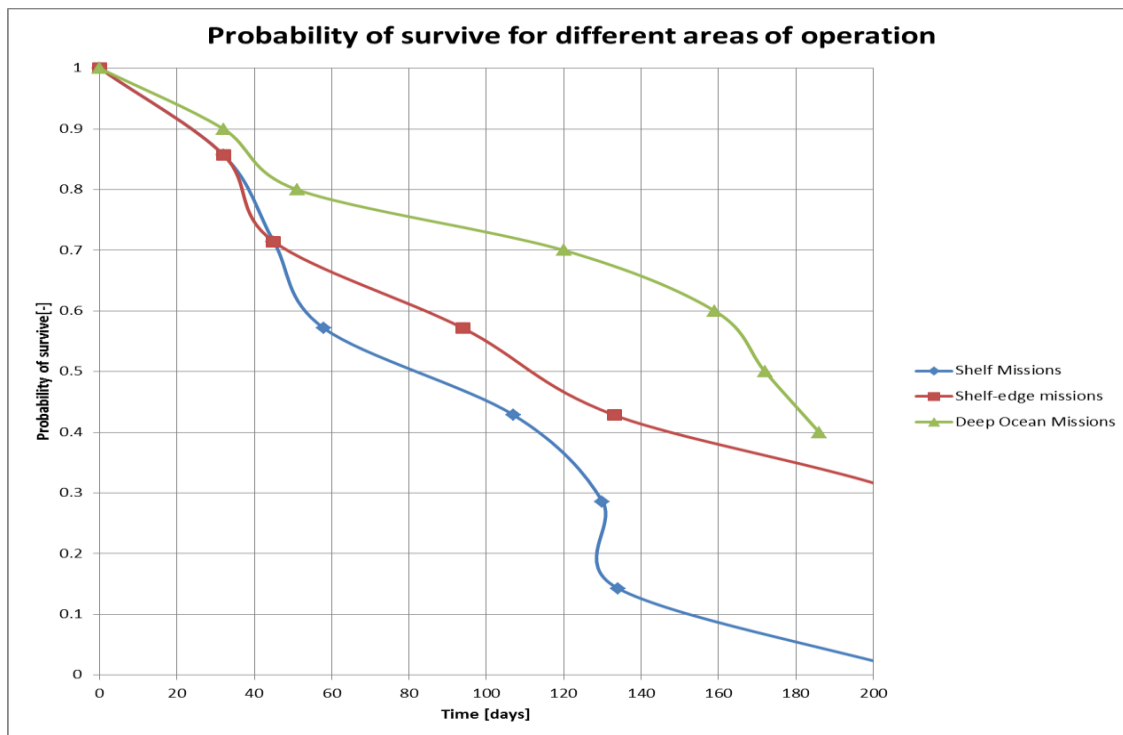
SHELF EDGE	81	missions				
medium endurance 28.6		days				
	Interval (days)	Number of entries	Number of failure	Failures/ Entries	Survival	Probability of survive
S(K)'_0	32	7	1	0.143	0.857	0.86
S(K)'_1	45	6	1	0.1667	0.833	0.71
S(K)'_2	94	5	1	0.2	0.8	0.57
S(K)'_3	133	4	1	0.25	0.75	0.43
S(K)'_4	213	3	1	0.333	0.667	0.29
S(K)'_5	217	2	1	0.5	0.5	0.14

c) Operation on deep ocean

c) Deep ocean	70	missions				
medium endurance 24.1		days				
	Interval (days)	Number of entries	Number of failure	Failures/ Entries	Survival	Probability of survive
S(K)"_0	32	10	1	0.1	0.9	0.9
S(K)"_1	51	9	1	0.111	0.888	0.8
S(K)"_2	120	8	1	0.125	0.875	0.7
S(K)"_3	159	7	1	0.143	0.857	0.6
S(K)"_4	172	6	1	0.167	0.833	0.5
S(K)"_5	186	5	1	0.2	0.8	0.4
S(K)"_6	235	4	1	0.25	0.75	0.3
S(K)"_7	248	3	1	0.333	0.666	0.2
S(K)"_8	252	2	1	0.5	0.5	0.1
S(K)"_9	375	1	1	1	0	0

(Source: Own calculations based on Kaplan-Maier estimator)

On diagram 4.4 is presented probability of survive for three different areas. The probability is the greatest for operation on deep ocean, but from the other side, the smallest possibility is for shallow water as a shelf. It can be seen that the most difficult and dangerous situation are met on coastal water and it can be caused because of big presence of human, the marine infrastructure, pipelines, other vessel etc.



Diag.4.4. Probability of survive for different areas of operation (Source: Own calculations based on Kaplan-Maier estimator)

4.2.3. Confidence level of failure on deep ocean

Based on definition, the confidence level of failure on deep ocean has been calculated. From table 4.1 the statistics have been taken which concerned the number of missions and medium endurance in days for deep ocean operations. To calculate confidence level it has to be known average, standard deviation and variance. The central limit theorem has been used. The calculated values and presented in table 4.7.

Table 4.7. Averages, the standard deviation and the variance of mean time to failure on deep ocean.

No.	Institute	Number of missions(N)	Medium endurance in days (t)	$N \cdot t$	Deviation $(x - \bar{x})^2$
1	CNRS	2	32	64	62,2
2	CSIC	14	19	266	26,2
3	INOGS	1	13	13	123,5
4	AWIPM	8	69	552	2014,7
5	CDCEEPCO	10	13	130	123,5
6	UEA	1	49	49	619,3
7	IM	3	14	42	102,3
8	NATO	23	4	92	404,6
9	SAMS	2	123	246	9778,4
10	NERC	6	39	234	221,6
		$\Sigma 70$	$\bar{x}=37,5$	$\bar{x}_{weighted}=24,1$	$\sigma^2 =1497,4; \sigma=38,7$

(Source: Own development)

They have been counted standard deviation and variance for two different averages: normal and weighted. The values of standard deviations are very similar but the mean time to failure (endurance) is significantly different $\bar{x} = 37.5$ days for normal average and $\bar{x} = 24.1$ for weighted. There have been selected three confidence levels: 99%, 95% and 90% for which significance level are 0.01, 0.05 and 0.10 in order. In the table 4.8 they are presented confidence intervals for different confidence levels.

Table 4.8. Confidence intervals for different confidence levels

	Confidence level	99	95	90
	Significance level %	1	5	10
	Significance level	0,01	0,05	0,1
	The quantile	2,33	1,64	1,28
Normal average	Lower limit (days)	9,0	17,4	21,8
	Upper limit (days)	66,0	57,6	53,2

(Source: Own calculations)

4.3. Analysis of navigational system

4.3.1. Preliminary Hazard Analysis for navigational aspect

This analysis is used to identify accidental events, which may occur and allow estimating severity of each action. Thanks to this method, the accidental events can be identified. It allows to focusing on important issues and then putting the aspects in more detailed analysis. Before main analysis by Human Reliability Method and by Event Tree Analysis, the PHA will be performed to assess the possibility events.

In the table 4.9 are presented the results of performed Preliminary Hazard Analysis for navigational aspect concerning Seaglider.

Table 4.9. Preliminary Hazard Analysis for navigational equipment

No.	Hazard	Cause	Consequence	Risk			Risk Reducing measures
				Freq	Cons	RPN	
1	Vehicle is not correctly monitored during mission	Fatigue of crew, lack of knowledge	Loss of glider, mission abort	2	4	8	Better control, training of crew
2	Damage of navigational equipment not detected during preparation for mission	Poor procedures, fatigue of crew, undetectable faults	Unexpected glider behavior, loss of glider, mission abort	1	4	4	Validate programming, training of crew, preparation conducted by specified procedures
3	Wrong implementation of mission plan (wrong programming)	Short time, fatigue of crew, unclear procedures	No collection of data, mission abort , Loss of glider	4	3	12	Validate programming, specified procedures, training of crew
4	Low battery, insufficiently charged	Lack of time, fatigue of crew	Mission abort, no collation of data	2	3	6	Specified procedures, training of crew, charge recommendation
5	Faults of equipment not solved before mission	Few experience, undetectable faults, fatigue of crew, negligence of crew	Unexpected glider behavior, loss of glider, mission abort	2	4	8	Better control of equipment, training of crew, regular inspection, elimination of faults
6	Unexpected behavior is not identified	Few experience, fatigue of crew, bad knowledge, lack of time	Loss of glider, mission abort, grounding,	2	4	8	Training of crew, specified procedures, careful control
7	Wrongly implemented parameters	Short time, fatigue of crew, misunderstanding between crew	No collection of data, mission abort, loss of glider	3	4	12	Monitoring after and during mission, validate programming, training of crew
8	Wrong use of software's	Lack of procedures, misunderstand of programming	Unexpected behavior of glider, mission abort	3	2	6	Check software's, training of crew
9	Damage of navigational equipment not detected (action)	Fatigue of crew, undetectable faults	Unexpected behavior, loss of glider, no collection of data	2	4	8	Better control, training of crew, better monitoring of equipment
10	Excessive currents, tides and waves not considered	Lack of experience, negligence of crew	Grounding, unexpected behavior, mission abort	1	3	3	Validate programming, training of crew

Freq-Frequency; Cons- Consequences; RPN-Risk Priority Number

(Source: Own development)

4.3.2. Human Reliability Assessment and Event Tree Analysis

To perform a Human Reliability Assessment, the events which may happen related to navigation system of Seaglider have to be identified. This step was performed using Preliminary Hazard Analysis. The next step is to assess the Human Reliability using SPAR-H method. The results are presented in table 4.10.

Table 4.10. Results of Human Reliability Assessment for navigational aspect

No.	EVENT	Description	HRA
1	CM (action)	Glider is not correctly monitored by crew during mission	0.02
2	DN (diagnosis)	Damage of navigational equipment not detected during preparation for mission	0.005
3	WI (diagnosis)	Wrong implementation of mission plan (wrong programming)	0.016
4	LB (diagnosis)	Low battery, insufficiently charged	0.001
5	FE (diagnosis)	Faults of equipment were not solves before mission	0.1
6	UB (diagnosis and action)	Unexpected behavior is not identified	0.256
7	WP (diagnosis)	Wrongly implemented parameters	0.01
8	WS (diagnosis)	Wrong use of software's	0.01
9	DE (diagnosis and action)	Damage of navigational equipment not detected	0.242
10	CW (diagnosis and action)	Excessive currents, tides and waves not considered	0.181

(Source: Own development)

Using theory about Human Reliability Assessment, it is possible to calculate possibility of preceding events. In the table 4.11 is presented the manner of calculation on the example of damage of navigational equipment not detected. The calculations of Human Reliability for all events in aspects of navigation are in table 4.13.

Table 4.11. PSFs for mission damage of navigational equipment not detected (diagnosis)

No.	PSFs	PSF Level	Multiplier	Reason
1	Available time	Nominal time	1	The crew has sufficient time to study the device
2	Stress/Stressors	Nominal	1	Normal function, the lack of stressful factors, normal procedures
3	Complexity	Moderate complex	2	Damage may not be noticed during routine check, imperceptible damage
4	Experience, training	High	0.5	The personnel is good prepared
5	Procedures	Insufficient Information	1	Lack of information. But normally personnel is good instructed
6	Ergonomics	Poor	10	The control performed at the sea
7	Fitness for duty	Nominal	1	Operating crew with adequate knowledge
8	Work process	Good	0,5	Specific crew

(Source: Own Development)

If all PFS are nominal then the human error probability (in case of diagnostic) is equal 0.01. In this case the PSFs have different values. The diagnosis failure probability in this case is equal:

$$HEP_d = 0.01 \cdot 1 \cdot 1 \cdot 2 \cdot 0.5 \cdot 1 \cdot 1 \cdot 1 \cdot 0.5 = 0.005$$

The evaluation of PSFs for the action of the task will be different. The active Failure Probability will be equal:

$$HEP_a = 0.001 \cdot 10 \cdot 2 \cdot 2 \cdot 0.5 \cdot 1 \cdot 1 \cdot 1 \cdot 0.5 = 0.01$$

The probability without formal dependency is calculated as:

$$P_{d/a} = HEP_d + HEP_a = 0.005 + 0.01 = 0.015$$

In the case of dependency, special table has to be taken into account, which is formulated and presented in table 4.12.

Table 4.12. Dependency Condition Table

Dependency Condition Table						Number of Human Action Failures Rule <input type="checkbox"/> - Not Applicable. Why? _____	
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		
1	s	c	s	na	complete	When considering recovery in a series e.g., 2 nd , 3 rd , or 4 th 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				na	low		
16			d	a	low		
17			zero				

Using P_{wod} = Probability of Task Failure Without Formal Dependence (calculated in Part III):

- For Complete Dependence the probability of failure is 1.
- For High Dependence the probability of failure is $(1 + P_{wod})/2$
- For Moderate Dependence the probability of failure is $(1 + 6 \times P_{wod})/7$
- For Low Dependence the probability of failure is $(1 + 19 \times P_{wod})/20$
- For Zero Dependence the probability of failure is P_{wod}

Calculate P_{wd} using the appropriate values:

$$P_{wd} = (1 + (\text{_____} * \text{_____})) / \text{_____} = \boxed{\text{_____}}$$

(Source: [30])

Using this table the dependency condition can be assessing. In the case of damage of navigational equipment not detected, the dependency between diagnosis and action is moderate. The assumption is that the personnel is the same (situation is on vessel board), the time is not close in time, and location is different (Seaglider work under the water) and the cause is no additional. Under the table is presented how to calculate Task Failure Probability for different dependency. In this case it will be:

$$P_{w/d} = \frac{1 + 6 \cdot 0.015}{7} = 0.156$$

After Human Reliability Assessment, the Event Tree Analysis can be performed. As an initial event the damage of navigational equipment was selected. In tab 4.13 the detailed analysis of Human Error Probability is presented. On the figure 4.1 performed Event Tree Analysis for initiation event damage of navigational equipment not detected is presented.

Table 4.13. Detailed Human Error Probability Analysis for navigational aspects

Abb.	PSFs									HEP	P_w	Dependency					P_w
	T	S	C	E	P	Er	FfD	WP	Cr			Ti	L	Ca	De		
CM	-	-	-	-	-	-	-	-	-	-	0.02	-	-	-	-	-	0.02
	10	2	1	1	1	1	1	1	1	0.02							
DN	1	1	1	0.5	1	1	1	1	1	0.005	0.005	-	-	-	-	-	0.005
	-	-	-	-	-	-	-	-	-	-							
WI	1	2	2	1	0.5	1	1	1	0.8	0.016	0.016	-	-	-	-	-	0.016
	-	-	-	-	-	-	-	-	-	-							
LB	0.1	1	1	1	1	1	1	1	1	0.001	0.001	-	-	-	-	-	0.001
	-	-	-	-	-	-	-	-	-	-							
FE	1	2	5	1	1	1	1	1	1	0.1	0.1	-	-	-	-	-	0.1
	-	-	-	-	-	-	-	-	-	-							
UB	1	1	2	1	5	1	1	1	1	0.1	0.132	s	nc	d	na	mod	0.256
	10	2	2	1	1	1	1	1	0.8	0.032							
WP	1	1	2	0.5	1	1	1	1	1	0.01	0.01	-	-	-	-	-	0.01
	-	-	-	-	-	-	-	-	-	-							
WS	1	1	2	0.5	1	1	1	1	1	0.01	0.01	-	-	-	-	-	0.01
	-	-	-	-	-	-	-	-	-	-							
DE	1	1	2	1	1	1	1	1	0.8	0.016	0.116	s	nc	d	na	mod	0.242
	10	2	5	1	1	1	1	1	1	0.1							
CW	1	1	1	1	1	0.5	1	0.8	0.004	0.044	s	nc	d	na	mod	0.181	
	10	2	2	1	1	1	1	1	0.04								

Abb- abbreviation; PSFs- Performance Shaping factors; HEP-Human Error Probability; T-time; S-Stress; C-complexity; E- experience; P procedures; E-ergonomic; FfD-fitness for duty; W.P- Work Process; Cr- crew; Ti-time; L- location; Ca-Cues; Dep-dependency;

(Source: Own development)

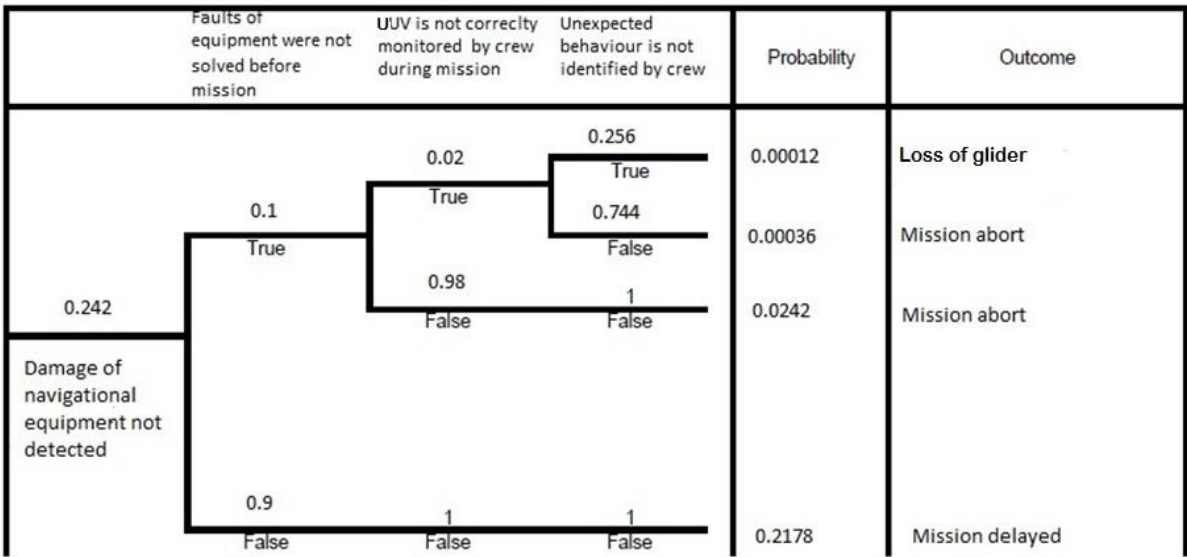


Fig.4.1. Event tree analysis for navigational aspect (Own development)

As an initiating event, the damage of navigational equipment not detected has been selected. If the crew does not detect the damage, it can cause that failures will not be solved before mission. The vehicle is not correctly monitored during mission what can cause unexpected behavior is not detected. The entire events are based on the Human Reliability Error Assessment.

4.4. Analysis of risk for launching and recovering process

4.4.1. Preliminary Hazard Analysis for failure

This analysis is used to identify accidental events, which may occur and allow estimating severity of each action. Before main analysis by Fault Tree Analysis and Event Tree Analysis, the PHA will be performed to assess the possibility events. For launching process, the detailed analysis is presented in Attachment A, *The results of Preliminary Hazard Analysis for launching process*, and for recovering process in Attachment C, *The results of Preliminary Hazard Analysis for recovering process*.

4.4.2. Human Reliability Assessment and Fault Tree Analysis

To perform a Human Reliability Assessment, the events related to launching which may happen, have to be identified. This step was performed using Preliminary Hazard Analysis, and results are in Attachment A, *The results of Preliminary Hazard for launching process*. The next step is to assess the Human Reliability using SPAR-H method. The results are presented in the table 4.14. The calculations for particular events are in Attachment B *Detailed HRA, summary for launching process*.

Table 4.14. Events and values of human probability calculated by SPAR-H method

No.	Event	Description	HRA
1	WD (diagnosis)	Wrong density used	0.00125
2	WC (diagnosis)	Wrong calculations	0.00250
3	PC (diagnosis)	Payload configuration error	0.00625
4	WS (diagnosis)	Wrong parameters implemented	0.001250
5	EE (diagnosis and action)	Error of equipment not detected	0.237
6	SU (diagnosis)	Glider is not set up physically correctly to launching	0.02
7	WB (diagnosis)	Glider is wrongly ballasted for launching	0.0025
8	PI (action)	Glider position is inappropriate	0.01
9	DT (diagnosis)	Glider is damage during transport to launching location	0.05
10	DL (action)	Glider is dropped during launching	0.025
11	SE(diagnosis and action)	Software error not detected	0.1536

(Source: Own development)

On the figure 4.2 is presented Fault Tree Analyse. The top event is failure during launching. As a reasons for failures have been selected for main causes: glider is damage, error of equipment not detected, Glider is not set up physically correctly for launching and wrong calculations.

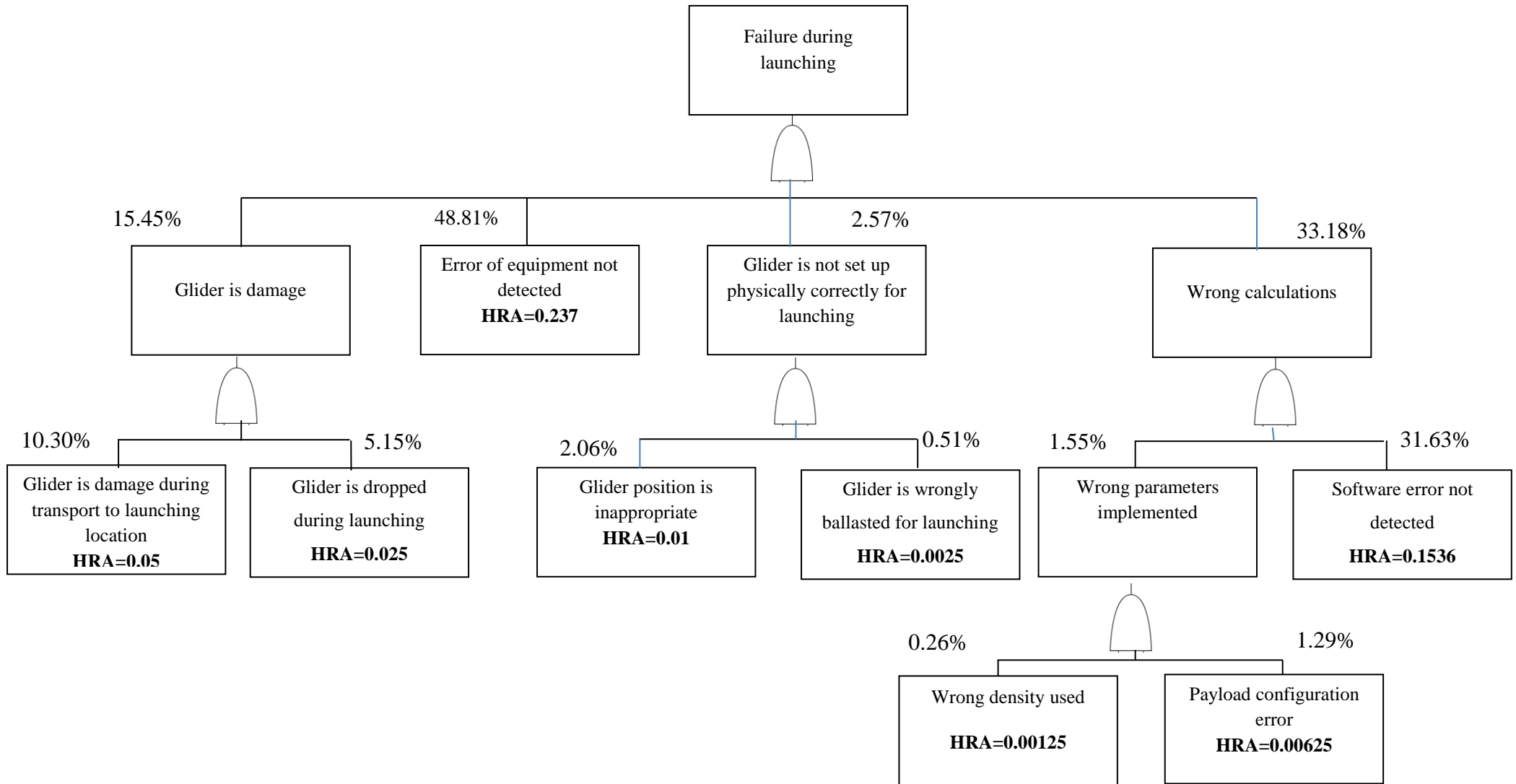


Fig.4.2. The Fault Tree Analysis for event Failure during launching (Own development)

4.4.3. Human Reliability Assessment and Event Tree Analysis

To perform a Human Reliability Assessment, the events related to recovering which may happen, have to be identified. This step was performed using Preliminary Hazard Analysis, which results are presented in Attachment C, *The results of Preliminary Hazard Analysis for recovering process*. The next step is to assess the Human Reliability using SPAR-H method. The results are presented in the table 4.15. The calculations for particular events are in Attachment D, *Detailed HRA, summary for launching process*.

Table 4.15. The Human Reliability Assessment for recovering process

No.	Event	Description	HRA
1	CC (diagnosis)	Current not considered	0.01
2	SB (action)	Hit the ship board	0.01
3	DW (diagnosis)	Difficult weather conditions not considered (high wave)	0.02
4	EE (action and diagnosis)	Error of equipment not detected	0.229
5	GB (diagnosis)	Glider is wrong ballasted	0.0005
6	UH (diagnosis)	Unexpected high tide	0.01
7	WA (diagnosis)	Wrong calculations	0.01
8	IP (action)	Inappropriate position of vessel	0.16
9	LD (action)	Lifting devices inappropriate prepared	0.02

(Source: Own development)

The figure 4.3 presents the performed Event Tree Analysis. As the initiation event have been selected wrong calculations. From this event, the future scenarios have been evaluated.

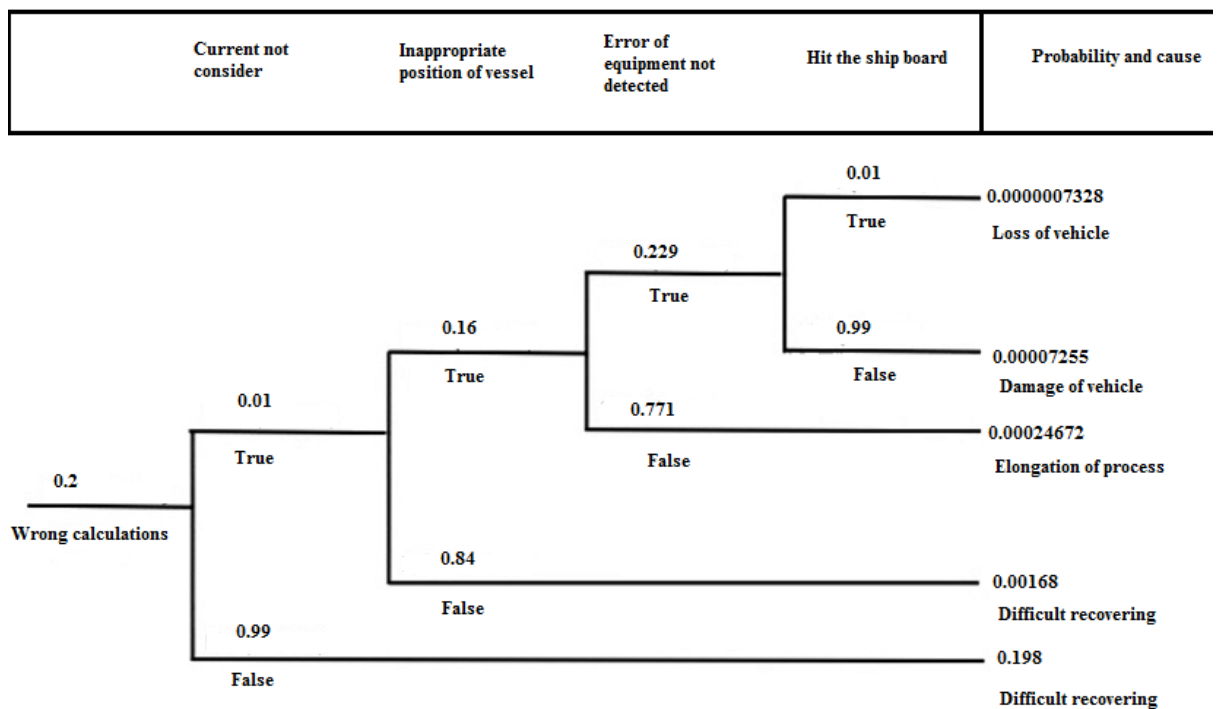


Fig.4.3. Event tree analysis for recovering process (Source: Own development)

4.5. What-if Analysis for moving process

The gliders have a cigar shaped body to reduce the drag and obtain better efficiencies. The UUVs type gliders are buoyancy driven version, which can sink and rise. It uses the small changes in its buoyancy together with wings to precede vertical motion to horizontal. Thanks of that the vehicle propel itself to forward with low power consumption. It is not so fast like other UUV but thanks of buoyancy-based propulsion, it has a significant bigger range and duration of operation. Seaglider follows saw-tooth pattern up –and-down through the water. The vertical pitch and roll are controlled by movable internal ballast (by battery packs).

The What-if analysis has been performed for UUV Seaglider in aspect of moving system. The results of the analysis are in the table 4.16.

Table 4.16. The results of What-if Analysis.

Revision: Moving system	Desc. of Operation: Preparation for mission			By: Review Team Date 01/17
What If?	Answer	Likelihood	Severity	Recommendations
1. The battery is not charged?	1. Problems during mission, mission will be abort	1. Quite	1. Minor	1. Check correctly before mission
2. The battery is broken?	2. Problems during missions, mission will be abort	2. Remote	2. Moderate	2. Check correctly before mission, constant control during mission
3. The buoyancy control system is not working correctly?	3. Problems with driving the glider, uncontrolled moves of vehicle	3. Very Unlikely	3. Critical	3. Train personnel, check before mission
4. The high-pressure pump is not working correctly?	4. Abort the mission or lost the vehicle	4. Very unlikely	4. Critical	4. Train personnel, constant monitoring
5. The electronics are not working correctly?	5. Other devices do not working correctly, broken controls, wrong readings	5. Very unlikely	5. Catastrophic	5. Advanced method of verification
6. Wrong powered the batteries?	6. Failure of other controls	6. Remote	6. Minor	6. Train personnel, check correctly
7. The buoyancy system is broken?	7. Problems during mission, mission will be abort or loss of the vehicle	7. Very unlikely	7. Catastrophic	7. Constantly checked during mission, train personnel prepared check list
8. The wings are broken?	8. Unexpected moving of vehicle, loss of glider	8. Very unlikely	8. Catastrophic	8. Check before mission, appropriate care of vehicle

(Source: Own development)

5. ANALYSIS OF RESULTS

5.1. Evaluation of Preliminary Hazard Analysis

Based on Preliminary Hazard Analysis, which was performed in chapter 4.2.1, the acceptability of the risks and analysis of results can be performed. Fourteen events have been selected, for which the probability and severity have been assumed. Based on Risk Priority Number, each of situation consist of two products, one is the probability (likelihood) and second is the severity (occurrence). The multiplication of this two products, assume the Risk Priority Number, which can access the acceptability of the risks.

Table 5.1. Assessment of Risk Priority Number for Events in Coastal Waters

Ref.	Hazard	Probability	Severity	RPN
1	Collision with vessel	2	5	10
2	Collision with other UUV	1	4	5
3	Getting stuck in net	2	3	6
4	Getting stuck in ice	2	3	6
5	Pushed by strong current	1	2	2
6	Pushed by high tide	1	1	1
7	Collision with wrack	2	5	10
8	Grounding	3	3	9
9	Collision with marine infrastructure	3	4	12
10	The human activity	4	1	4
11	Collision with the anchor chain	1	3	3
12	Hit during recovering	2	5	10
13	Loss of vehicle	1	5	5
14	Problems during launching	2	4	8

(Source: Own development)

The biggest Risk Priority numbers have following events: collision with marine infrastructure (RPN = 12), collision with vessel (RPN = 10), collision with wrack (RPN = 10), hit during recovering (RPN = 10) and grounding (RPN = 9). These situations are the most demanding because they can cause the loss of the Seaglider. In the port area are many activities like vessel traffic, human activity, fishing boat and nets. Based on the RPN, none of this situation is unacceptable, but for some of them, the ALARP is needed. The ALARP is needed for events like: collision with the vessel, collision with other UUV, getting stuck in net, getting stuck in ice, collision with wrack, grounding, collision with marine infrastructure, hit during recovering and problems during launching.

The ALARP means- as low as reasonable practicable, which means:

“To reduce a risk to a level which is ‘as low as reasonably practicable’ involves balancing reduction in risk against the time, trouble, difficulty and cost of achieving it. This level represents

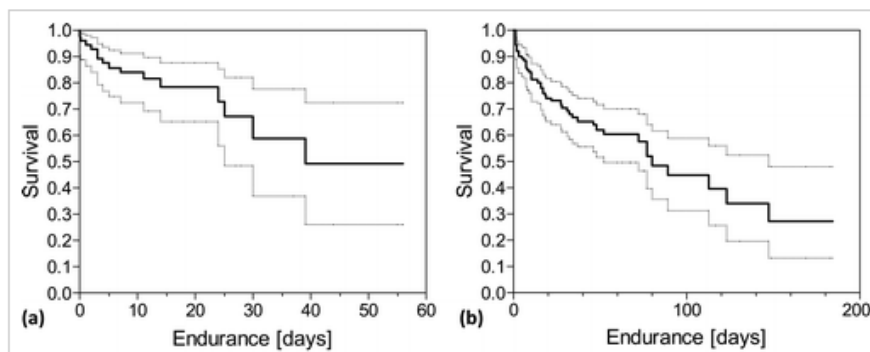
*the point, objectively assessed, at which the time, trouble, difficulty and cost of further reduction measures become unreasonably disproportionate to the additional risk reduction obtained*¹⁴.

Coastal areas like ports are the most demanding for vehicles like autonomous underwater vehicles. To the most dangerous can be counted: collision with vessel, with wrack, with marine infrastructure and hit during recovering. These hazard were considered as the most dangerous because can cause big loss, like the failure of equipment and even loss of vehicle. To less risky are: pushed by strong current or high tide and the human activity. In port of Gdynia, according to information in Admiralty Sailing Directions [29] there is a weak N current set off the entrance to Gdynia Harbor. The Baltic Sea is non-tidal area, so the risk of pushing by high tidal is very small.

The greatest possibility of occur have following hazards like: grounding, collision with marine infrastructure and human activity. The harbor area is shallow and the Port of Gdynia has only 14 meters of depth, what makes that is a very shallow area. The harbor due to the large movement of vessel has to be marked well and this cause a large number of different infrastructures like: breakwaters, buoys, light vessels etc. In addition, in the port are performed many different tasks concerning with infrastructure, cargo transferring, dredging the port which is connected with human activity.

5.2. Assessment of area of operation based on Kaplan Maier estimator

The data to perform analysis based on area of operation were taken from Project GROOM data base. In this project area of operation was divided into three main groups: shelf, shelf edge and deep ocean. The information about the number of missions, vehicles used and aborts have been presented in chapter 4.1 of this work.



Diag.5.1. Probability of survive for different areas of operation, (a-shelf and b-deep ocean) (Source: [29])

Three different regions of operations were analyzed. The missions were performed on shelf, shelf edge and on deep ocean. For different scenarios, were calculated medium endurance time and probability of survive based on Kaplan-Maier estimator. Based on the data from the from GROOM project, it can be noticed that reliability of the system is higher

¹⁴OGP Report No. 6.36/210, *Guidelines for the Development and Application of Health, Safety and Environmental Management Systems*, International Association of Oil & Gas Producers

for missions performed on deep seas than on self or shelf edge. The reliability of the system for approximately 100 days of work for deep ocean is 0.7 but for shelf edge is 0.57 and for shelf is 0.43.

On the diagram 5.1 are presented probability of survive for two areas: shelf and deep ocean performed by M. Brito, D.Smeed and G. Griffiths [8]. The probability is greater for operation on deep sea, and smallest for shallow water as a shelf. Comparing with the results from chapter 4.2.2 it can be noted that obtained results are very similar. It can be seen that the most difficult and dangerous situation are met on coastal water and it can be caused by big presence of human, the marine infrastructure, pipelines, other vessel etc.

In recent years, a lot of approaches have been made to quantify the ongoing risk of vehicles which operate on different scenarios [24]. Coastal surveys have been recognized and different scenarios have been studied. The surveyors provide probability of survival in most challenging setups (coastal waters) between 0.97 and 0.99 for mission ranges below 30 km [24]. Coastal water is the most demanding scenario for vehicles, because the potential risks are numerous, for example: environmental hazards, man-made structures, human activity etc. The frequency of such episodes is high and they can be occurred at the same time [12].

Engineers have been trying to approach to the problem of risk assessment. The most critical phases of operations are launching and recovering of device. This assumption is true but especially for deep ocean vehicles because they operate in quit calm environment. Regarding to vehicles which are used in shallow water, near the shore, the most dangerous are uncharted obstacles or vessel traffic especially intensive in port area [24].

5.3. Analysis of confidence level of failure on deep ocean.

Based on definition, the confidence level of failure on deep ocean was calculated. The medium endurance time in days was calculated in two ways, using to different averages: normal and weighted. For the weighted average, the numbers of deep ocean mission were taken as weights. The medium endurance days for deep ocean missions are:

$$\bar{x}_{normal} = 37.5 \text{ days}$$

$$\bar{x}_{weighted} = 24 \text{ days}$$

The standard deviation is $\sigma = 38.7 \text{ days}$ and the variance is $\sigma^2 = 1497.4 \text{ days}^2$

From the subsequent calculations, it can be noted that values of mean time of failure (endurance) does not have a normal distribution, but according to central limit theorem, it have to be assumed that the MTTF has normal (Gaussian) distribution. There have been selected three confidence levels: 99%, 95% and 90%, for which significance level are 0.01, 0.05 and 0.10 in order. In the table 5.2 are presented confidence intervals for different confidence levels.

Table 5.2. Confidence intervals for different confidence levels

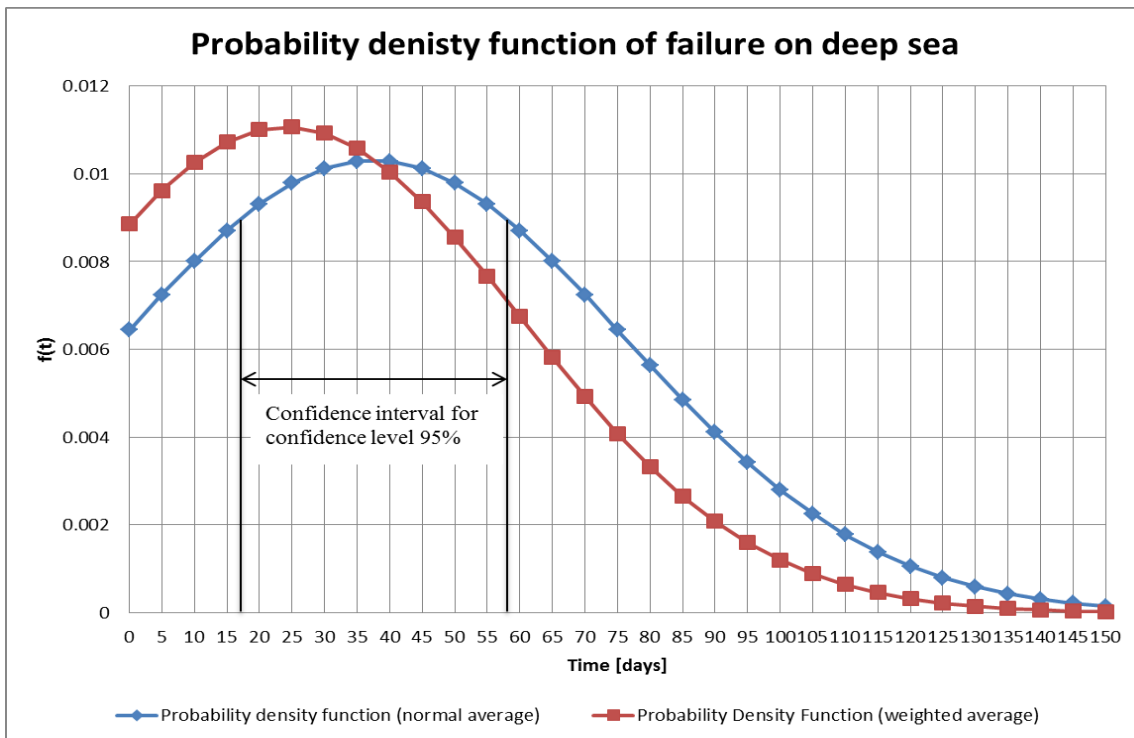
	Confidence level	99	95	90
	Significance level %	1	5	10
	Significance level	0,01	0,05	0,1
	The quantile	2,33	1,64	1,28
Normal average	Lower limit (days)	9,0	17,4	21,8
	Upper limit (days)	66,0	57,6	53,2

(Source: Own calculations)

For the weighted average, the lower limit of interval for level 99% is -2,4 days what is incorrect because failure cannot occur before the start of operation. The more accurate results are for normal average. For two different situations, were calculated probability density functions of failure on deep sea using following expression 5.1:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{-(x_i - \bar{x})^2}{2\sigma^2}\right) \quad (5.1)$$

On the diagram 5.2 are presented probability density functions calculated using above formula. As can be seen, the mean time to failure in this case does not have normal distribution, but according to central limit theorem it must be established.



Diag.5.2. Probability density functions of failure on deep ocean

“The probability density function is nonnegative everywhere, and its integral over the entire space is equal to one”¹⁵. The integral of the probability density function in this case

¹⁵Probability Density Function https://en.wikipedia.org/wiki/Probability_density_function

is not equal one, what can be noted from diagram. On the diagram 5.2 has been marked confidence interval for confidence level of 95%. The confidence interval is $< 17.4 \text{ days}; 57.6 \text{ days} >$. It can be stated that failure will occur with 95% certainly between 17.4 and 57.6 day of operation. It has to be taken into account that in industry are a lot of different types of gliders. The above statistics are huge averaging because of different areas of operations of this vehicle, quality of equipment, and age of vehicles which effect on accuracy of results. It has to be noted that the medium time of operation is 38,7 days, which is the long period if we compare it with operation of UUVs [38].

5.4. Evaluation of risk assessment for navigational aspect

5.4.1. Evaluation of Preliminary Hazard Analysis for navigational equipment

This analysis is used to identify accidental events, which may occur and allow estimating severity of each action. Before main analysis by Event Tree method, the PHA will be performed to assess the possibility events. In chapter 4.3.1 are presented detailed analysis which is shorted in table 5.3. The multiplication of two products: the frequency and the consequences assume the Risk Priority Number, which can access the acceptability of the risk.

Table 5.3. Assessment of frequency and consequence for different events

EVENT	Risk		RPN
	Frequency	Consequence	
CM	2	8	8
DN	1	4	4
WI	4	3	12
LB	2	3	6
FE	2	4	8
UB	2	4	8
WP	3	4	12
WS	3	2	6
DE	2	4	8
CW	1	3	3

(Source: Own development)

The biggest Risk Priority Numbers have following events:

- WI: Wrong implementation of mission plan, wrong programming (RPN = 12)
- WP: Wrongly implemented parameters (RPN = 12)

These situations are most demanding because can occur very frequently. The wrong implementation parameters and mission plan is caused by human negligence and provoke the abort of the mission, loss of data or loss of the vehicle. Based on the RPN, none of this situation is unacceptable, but for some the ALARP is needed. The acceptability of the risk is based on the pre-established values of RPN.

The risk is acceptable for following events: damage of navigational equipment not detected during preparation for mission (RPN = 4) and excessive currents, tides and waves not considered (RPN = 3). These situations are the least demanding because the frequency of these events is very low. It was assumed that the personnel are good prepared for the job, and the routine actions are performed well.

5.4.2. Analysis of Human Reliability Assessment for navigational system

The Human Reliability Assessment was performed using method called SPAR-H. The results were presented in table 4.10 in chapter 4.3.2 and the more specified calculation of Human Error Probability are in table 4.13. From this analysis, the following conclusions may be drawn:

- „Unexpected behavior is not identified” has the human reliability equal to 0.256. This event has the biggest value of this indicator. The reason is that this event is connected with action and diagnosis, what cause that the reliability has higher value compared with events which take place only in diagnosis.
- “Damage of navigational equipment not detected” also has human reliability high and equal to 0.242. The reason is like in the previous assessment.
- “Damages and unexpected behaviors” are very stressful for crew members, and also the available time is shorted to detected this failures and repair it.
- The lowest value has “Low battery, insufficient charged”. The crew has a long available time, and this event is not so stressful, and procedures are good prepared.
- The assumption was that the crew is good prepared for the work (PSF- experience, training, and fitness for duty), the main factors which effects on Human Error Probability have been the availability time, stressors and complexity of the task.

5.4.3. Analysis of the result of the Event Tree analysis for navigational system

Based on Human Reliability Assessment, The Event Tree was created. The initiating event was “damage of navigational equipment not detected”. The outcomes and subsequent event were analyzed. The subsequent events were:

- Faults of equipment were not solved before mission, $P(\text{FE}) = 0.1$
- Glider is not correctly monitored by crew during mission, $P(\text{CM}) = 0.02$
- Unexpected behavior is not identified by crew, $P(\text{UB}) = 0.256$

Three outcomes were found: Mission delayed with probability 0.2178, Mission abort with probability 0.02456, Loss of vehicle with probability 0.00012.

As can be noted, the probabilities are very small. If the damage of navigational equipment will not be detected, the most likely is mission delayed with probability 0.2178. In the case if the damage of navigational equipment will not be solved before mission

and Seaglider will not be corrected monitored and behavior will not be identified, them this can cause loss of the vehicle.

5.5. Analysis of launching and recovering process

5.5.1. Evaluation of Preliminary Hazard Analysis

The Preliminary Hazard Analysis was performed to identify events, which may occur and allow estimating severity and consequences of each action. In table 5.4 are presented the results of Preliminary Hazard Analysis for launching and recovery.

Table 5.4. Preliminary Hazard Analysis and Risk Priority Number

a) Launching process

No.	Abb.	Hazard	Risk		
			Freq	Cons	RPN
1	WD	Wrong density used	2	2	4
2	WC	Wrong calculations	1	3	3
3	PC	Payload configuration error	1	4	4
4	WS	Wrong parameters implemented	3	2	6
5	EE	Error of equipment not detected	2	4	8
6	SU	Glider is not set up physically correctly to launching	2	4	8
7	WB	Glider is wrongly ballasted for launching	2	3	6
8	PI	Glider position is inappropriate	3	4	12
9	DT	Glider is damage during transport to launching location	2	4	8
10	DL	Glider is dropped during launching	1	5	5
11	SE	Software error not detected	1	3	3

b) Recovering process

No.	Abb.	Hazard	Risk		
			Freq	Cons	PRN
1	CC	Current not considered	2	2	4
2	SB	Hit the ship board	3	5	15
3	DW	Difficult weather conditions not considered (high wave)	2	4	8
4	EE	Error of equipment not detected	2	5	10
5	GB	Glider is wrong ballasted	1	5	5
6	UH	Unexpected high tide	2	1	2
7	WA	Wrong calculations	2	4	8
8	IP	Inappropriate position of vessel	2	5	10
9	LD	Lifting devices inappropriate prepared	2	4	8

(Source: Own development)

For launching process, the events with the higher Risk Priority Number are: glider position is inappropriate (RPN = 12), error equipment not detected (PRN = 8), glider is not set up physically correctly to launching (PRN = 8) and glider is damage during transport to launching location (PRN = 8). These events are the most demanding because they have the biggest consequences, and can cause failure of the equipment or even the loss of it. Inappropriate position of glider and inappropriate physically set up, can cause its damage and even loss. When the error of equipment is not detected early it can cause the impossible process of launching and unexpected behaviour of glider, which can cause the elongation of the launching process. The risk is acceptable for following events (where RPN < 5): wrong density used (RPN = 4), wrong calculations (RPN = 3), payload configuration error (RPN = 4) and software error not detected (RPN = 3). None of the events are unacceptable but for some of these the ALARP is needed.

For recovering process, the events with the higher Risk Priority Number are: hit the ship (RPN = 15), error of equipment not detected (RPN = 10) and inappropriate position of the vessel (RPN = 10). First event is the most dangerous because can cause the loss of vehicle. When the glider hit the ship board it can damage itself seriously and be impossible to recovering. Additionally it can cause the damage of ship sides. When the error of equipment is not detected early it can cause the impossible process of recovering or elongation of it. The consequences of these situations are high, but the assumption is that the crew is good prepared for work, and the frequency of this situation is low.

The risk is acceptable for following events: current not considered (RPN = 4), and unexpected high tide (RPN = 2). The unexpected high tide it does not cause the threats during recovering. The tides have only impact in shallow water, because can cause the grounding of the equipment (the depth is lower/higher than expected). The current is taking into account by glider system so it is able to set up according to current.

5.5.2. Human Probability Assessment and Fault Tree for launching process

The Human Reliability Assessment was performed used SPAR-H method. The calculations for particular events are presented in Attachment B, Detailed HRA, summary for launching process. The events with the highest probability of occur are: error of equipment not detected (HEP = 0.237), software error not detected (HEP = 0.1536) and glider is damage during transport to launching location (HEP = 0.05). The high value for two first events is due to the fact that these events are possible during diagnosis and action. The lover probability has the following events: wrong parameters implemented (HEP = 0.00125), wrong density used (HEP = 0.00125), wrong calculations (HEP = 0.0025) and glider is wrongly ballasted for launching (HEP = 0.0025).

The Fault Tree Analysis was performed. The top event was “failure during launching”. There were selected four mean reasons of it: glider is damage (15.45%), Error of equipment not detected (48.81%), glider is not set up physically correctly for launching (2.57%), wrong

calculations (33.18%). The analysis was performed based on assumption that the top event has to have probability equal to one (main foundation of Fault Tree Analysis). The bottom events in this case have to have sum of probability equal to one.

5.5.3. Human Probability Assessment and Event Tree for recovering process

To perform a Human Reliability Assessment, the events related to recovering which may happen, have to be identified. This step was performed using Preliminary Hazard Analysis. The next step is to assess the Human Reliability using SPAR-H method. The calculations for particular events are in Attachment D, *Detailed HRA, summary for recovering process*.

The event with the higher Human Error Probability is error of equipment not detected. The first reason is that this event can cause during the diagnosis and action. The dependency cause that the probability is higher than for other events. The next event is inappropriate position of vessel ($P(IP) = 0.16$). This situation is very stressful for crew, because can cause impossibility of recovering of vehicle. In case of bad weather condition, the setting of the ship can last long, causing fatigue and stress of crew.

The lowest probability equal to 0.005 has the scenario: glider is wrong ballasted. The vehicle is suited with many controls and advanced systems which provide high reliability of vehicle. The situations like current not considered, hit the ship side, unexpected high tide and wrong calculations have low probability of occurrence, but it has to be remember that they can cause a very risky situation. A good example is presented in performed Event Tree Analysis. As the initiation event are wrong calculations, which can cause that current will not be consider. The current not considered seems to be not so dangerous for equipment and crew, but can cause that crew set up inappropriate position of vessel. If this error is not detected, the vehicle can hit the ship board and can cause loss of vehicle. The possible situations were presented on Event Tree Analysis for recovering process.

6. EVALUATION OF THE ACCEPTABILITY OF THE RISK

The risk acceptance must be defined as “*safety for defined scenario, but is a complex and controversial task*”¹⁶. In the industry is a several methods, which have been developed to help in determining the acceptability of the risk, which will be discuss in this chapter. The acceptance criteria are the standards, which help to perform decision making during the evaluation phase of analysis. The evaluated risk have to be compared with risk criteria (with the specified level of acceptance and tolerance) to determine the ability of accept. The methods are briefly summarized in the table 6.1.

Table 6.1. Methods used to determine Risk Acceptance

Risk Acceptance Method	Summary
Risk Priority Number	Method design for risk analysis method Failure Modes and Effect Analysis. It multiple assigned probability and severity.
Farmer Curve	It is an estimated curve which demonstrates graphically the region of risk acceptance or no acceptance.
Revealed Preference	Comparison of risks and benefits for different events, categorized in voluntary and involuntary expose to risk
Evaluate Magnitude of Consequences	Compares the likelihood and consequence magnitude of the risk. It is used to determine acceptable level risk based on consequences
Cost Effectiveness of Risk Reduction	Ratio for comparing cost to the magnitude of risk reduction
Risk Comparison	Best suited to comparing risks of the same type. Compare various industries, activities.

(Source: [2])

6.1. Risk priority number

Risk priority number or RPN: “*is a numeric assessment or risk assigned to a process, or steps in a process, as part of Failure Modes and Effects Analysis, in which a team assigns each failure mode numeric values that quantify likelihood of occurrence, likelihood of detection and severity of impact*”¹⁷.

This method is especially design for risk analysis method *Failure Modes and Effects Analysis*. It can be however used after other analysis. It is very common approach in which team members multiply the assigned probability of occurrence (O) and severity (S). The Product of these two values is the risk Priority Number is presented by formula 6.1 [40].

$$RPN = O \cdot S \quad (6.1)$$

In FMEA method, the likelihood of detection is taken into consideration. When the detection is included in analysis, the Risk Priority Number is the product of occurrence, severity and detection, formula 6.2.

¹⁶ B.M. Ayyub and others, *Risk Analysis and Management for Marine Systems*,

¹⁷ Institute of Healthcare Improvement,

<http://www.ihl.org/resources/Pages/Measures/RiskPriorityNumberfromFailureModesandEffectsAnalysis.aspx>

$$RPN = O \cdot S \cdot D \quad (6.2)$$

The acceptability of the risk is based on the pre-established values of RPN. In the case if occurrence and severity was taken into consideration (two products), the values can be as follows:

- $RPN \leq 4$, the risk is acceptable
- $RPN > 4$, but $4 < RPN < 15$, the investigation should be perform to reduce the risk and implement risk controls (for example ALARP)
- $RPN \geq 15$, the risk is unacceptable, the changes in design are required to mitigate the risk

The result of this analysis is the risk evaluation matrix, which show, which of events are unacceptable or acceptable and noted the situations when the ALARP has to be performed.

Likelihood (Probability)	Impact (severity)				
	1	2	3	4	5
5	Yellow	Yellow	Red	Red	Red
4	Yellow	Yellow	Yellow	Red	Red
3	Green	Yellow	Yellow	Yellow	Red
2	Green	Green	Yellow	Yellow	Yellow
1	Green	Green	Green	Yellow	Yellow

Fig.6.1. Risk Matrix to calculate Risk Priority Number (Source: [40])

The pattern is symmetrically because Occurrence and Severity in this case have the same weight. The manufacturers have not been not agree with this assumption that occurrence have the same weight as severity, because the risk with high severity are more important than the risks with high occurrence. As the result, they used asymmetrical matrices, to better expose their tolerance for risk [40].

6.2. Method of acceptability of risk for owners

G.Griffiths and A. Trembanis proposed how the owners of AUVs (but can be also used to other types of UUV) can decide about the acceptable level of risk based on the costs [13]. This approach can be illustrated by following figure 6.2. This process consists of eight main steps which are:

1. Establish the capital cost of the vehicle C . It can be cost of build but also cost of purchase or cost of replace.
2. Identify the typical daily cost of operation D . The cost can be varied depend on the type of campaign, the technical support requirements, the part of charter rate, the cost of science team and etc.
3. State the fraction of the daily rate D they are agree to accept as a loss substitution fee for each day of vehicle operation (through its service life) $x\%$.

4. Calculate the required service life (in days) by formula 6.3:

$$S = 100 \cdot \frac{C}{x} \cdot D \text{ [days]} \quad (6.3)$$

5. Assign the relative risks R and subsets S . They have to be recognized varying risks through vehicle service life (which is split into n user subsets). Each one of subset i , has S_i days and relative assessment risk R_i .

6. Declaration of the minimum acceptable probability K .

7. From previous assumption, the hazard rate can be calculated by formula 6.4:

$$\lambda = -\frac{\ln(K)}{\sum_{i=1}^n R_i S_i} \quad (6.4)$$

8. Calculation of acceptability of loss for a campaign of m subsets (y days) of activities S_j , each one with risk factor R_j , from equation 6.5.

$$y = \sum_{j=1}^m S_j \quad (6.5)$$

And the probability of loss is calculated from equation 6.6.

$$P(\text{loss}) = 1 - \exp\left(-\lambda \cdot \sum_{j=1}^m R_j \cdot S_j\right) \quad (6.6)$$

On the table 6.2 is presented spreadsheet which can be used by the owners to take decision about acceptability of the risk. The spread sheet was created based on the above formulas.

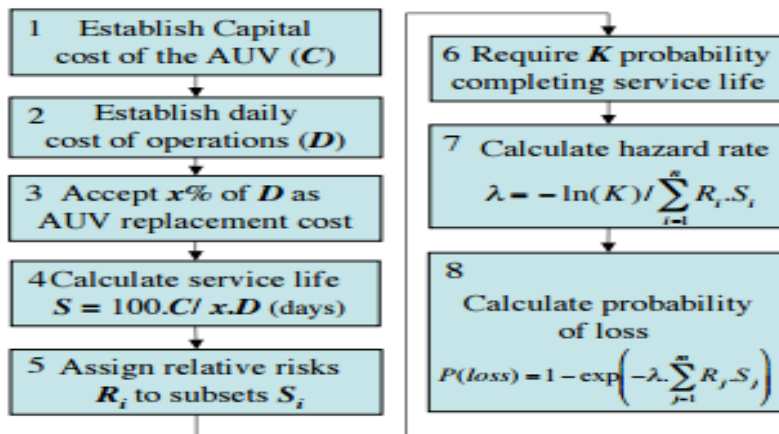


Fig.6.2. A process for the owner to decide about acceptability of the risk (Source: [13])

Table 6.2. Spreadsheet for owners to calculate acceptability of the risk

Owner initial Inputs			
UUV Capital Cost (C)	180000	Euros	
Replacement cost charge (x%)	20	% of daily operations cost	
Required probability of reaching end of life (K)	15	%	
Cost of Daily operations			
Direct UUV charge	400	Euros per day	
Fraction science team	1000	Euros per day	
Fraction of ship	2000	Euros per day	
Daily cost of operation (D)	3400	Euros per day	
Risk subsets	% Service life	Relative risk	Days
Open water	50	1	132
Shelf water	40	3	106
Under shelf ice	10	10	26
Other subset
Calculated parameters			
Required service life (S)	265	operational days	
Replacement cost charge	680	euro per day	
Hazard rate (λ)	0.002654407	per day	
Campaign details			
Number of service days	15	days	
Risk subsets	% campaign	Relative risk	Days
Open water	10	1	1.5
Shelf water	30	3	4.5
Under shelf ice	60	10	9
Other subset
Acceptable probability of loss for the campaign	24	%	

(Source: Own development based on [13])

In the grey boxes are parameters which can be changed by the owner to obtain acceptable probability of loss for the campaign which is presented in yellow box.

6.3. Farmer Curve's

The curve was introduced by Frank Reginald Farmer. He had worked in the nuclear branch and he had postulated that whole spectrum of events which have to be considered, not only the maximum credible accident. Accidents which have fewer consequences which are more probable also have to be taken into consideration. This curve presents cumulative probability versus consequences [2]. This graph introduces a probabilistic approach in case of determination of acceptability safety limit. Probabilities values have to be calculated for each level of risk, thanks of that generate a unique curve for hazard of concern [2].

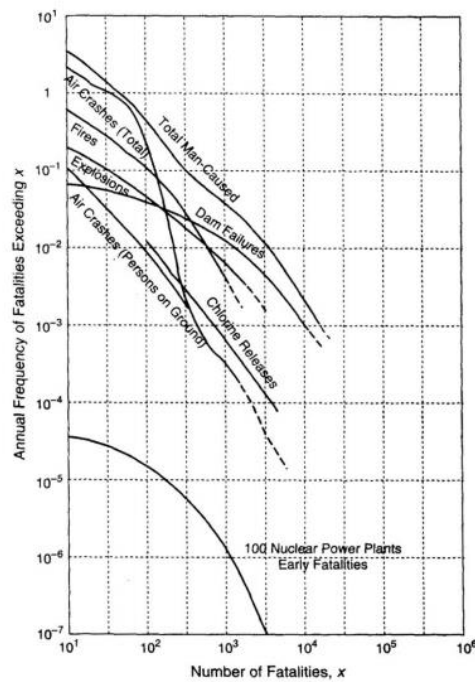


Fig.6.3. Farmer curve, Annual frequency of facilities from man-made structures, compared with risk profile of 100 operational nuclear plants (Source: [21])

The horizontal axis can display the: “number of facilities” or “accident severity”, on the other hand the vertical axis show complementary cumulative risk which is “frequency of facilities exceeding x” [21]. The area on the right side, or “outside” of the curve is consider as unacceptable for this hazard, because the risk and frequency are higher than estimated values by this curve. On the left side or “inside” is consider as acceptable because the risk and frequency are less than average value of the curve [2]. When lines are intersecting that means that different situations have equal risk and consequence.

6.4. Factors effecting on the acceptability of the risk

6.4.1. Revealed Preferences method –benefit effect

The method of Revealed Preference associate the risk to benefit and them categorize different types of risk. The main motivation for set this type of relation is obvious that the risk is not taken unless benefits not come and are high. The benefit can be determined by monetary value or by some other measurements of worth, for example pleasure or satisfaction [26]. On the figure 6.4 is plotted the risk relative to the benefit.

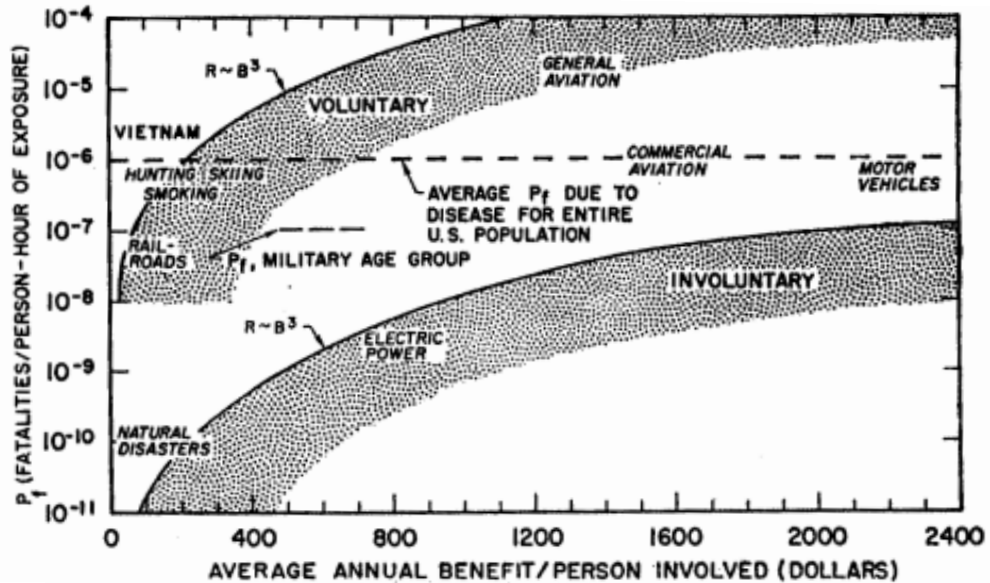


Fig.6.4. Risk plotted relative to benefit, for various kinds of voluntary and involuntary exposure (Source: [26])

This method assumed that the risk which can be accepted by society when is in equilibrium with benefits. As can be noted from the graph, there are two estimated lines which are divided into voluntary and involuntary risk categories. According to Starr (1969) [26]: “The acceptance of individual risk is an exponential function of the wage, and can be roughly approximated by a third-power relationship in this range”. This relationship between benefits and the risk can be formulates by formula 6.7 as:

$$\text{Risk} \sim \text{Benefit}^3 (R \sim B^3) \quad (6.7)$$

6.4.2. Evaluation of magnitude of risk consequence

Another factor which effects on the acceptability of the risk is the magnitude of the consequences of the incident what can cause some failure. Briefly summarizing, if the consequence is larger them the likelihood of the event has to be lower [47]. This method has been used in industry to illustrate the position of the industry within a society's risk acceptance levels based on the magnitude of the consequence, which can be shown by figure 6.5.

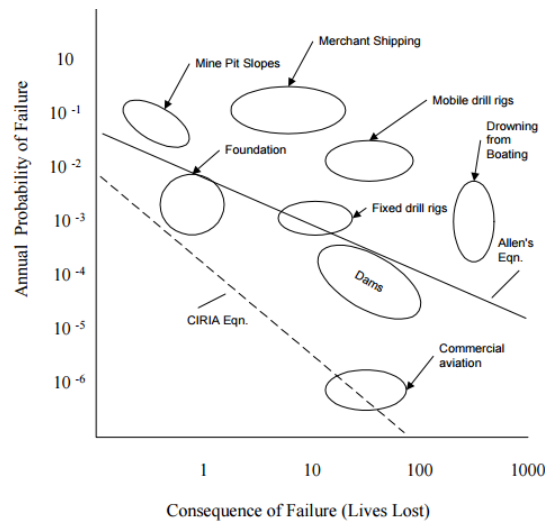


Fig.6.5. Target Risk Based on Consequence of Failure for Industries/Activities (Source: Whitman 1984)

Further evaluation has resulted in numerous estimates for relationship between magnitude of consequence for failure and the accepted probability of the failure. Two equations can be mentioned here, first one (equation 6.8) is the CIRIA (Construction Industry Research and Information Association):

$$P_f = 10^{-4} \frac{KT}{n} \quad (6.8)$$

Where:

T - The life of the structure

K - Factor regarding the redundancy of the structure

n - Number of people exposed to risk

Other estimation is known as Allen's estimation (1981) and is as follows, equation 6.9:

$$P_f = 10^{-7} \frac{TA}{W\sqrt{n}} \quad (6.9)$$

Where:

A and W – The factors regarding the type and redundancy of the structure.

First equation offers a lower boundary, and the second one offers a middle line.

6.4.3. Risk Reduction Cost Effectiveness Ratio

This factor assesses the risk acceptance in the determination of risk effectiveness which can be formulated by equation 6.10 as [2]:

$$\text{Risk Effectiveness} = \frac{\text{Cost}}{\Delta \text{Risk}} \quad (6.10)$$

Where the cost should be ascribed to risk reduction and the ΔRisk is the level of reduction of the risk, and can be formulated as equation 6.11:

$$\Delta \text{Risk} = (\text{Risk before mitigation action}) - (\text{Risk after mitigation action}) \quad (6.11)$$

Risk effectiveness can be used to evaluate numerous risk reduction efforts. The most benefit of the cost can be achieved with the smallest risk effectiveness. This measurement can be used to determine the acceptability level of the risk. The inverse of this formula can express the cost effectiveness. The relationship can be illustrated by the graph, where the equilibrium between risk and cost is showed on following fig.6.6. The main question is which level of risk is acceptable (or replaced) and how much people are willing to pay to avoid a risk [18]. The trade-off point is consider where the $\frac{\Delta R}{\Delta C}$ is equal -1. But to find this point and to draw this graph it is necessary to measure the cost and the risk in the same units for example dollars [18]. The decision based on cost- benefit consideration cannot be match with societal values about safety.

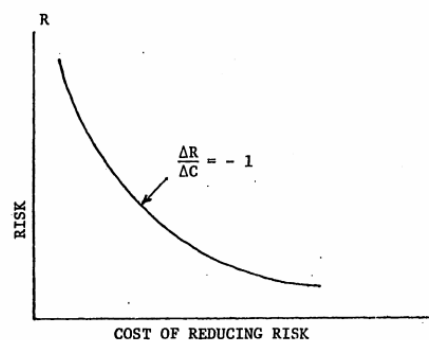


Fig.6.6. Cost effectiveness of risk reduction (After Rowe, 1977)

6.4.4. Risk Comparison

The Risk Comparison method is the most common practise to evaluating the risk. This method uses the frequency of the consequences to compare the risks in different areas of interest [2]. The frequency of mortality, morbidity, damage compared between various activities, between countries, regions, cities, are compared to encourage some desired action [37].

This method is affective when the risk is compared in the same human consequences and perception (categories). When the comparison is performed between different categories, should be done very cautiously. One of the assumptions in this method is that the risks which have been accepted in the past will be accepted also in the future [37].

Conclusion

The thesis was purposed to present and analysed different method of risk analysis used in engineering, and found the appropriate method to analyse the complex system like Unnamed Underwater Vehicle type Seaglider. In the thesis have been listed and described several methods which are used in naval engineering and are opportunely to examine this system like: fault tree analysis, preliminary hazard analysis or what-if method. The risk analysis is quiet new branch of the engineering, which is not yet known well. On the other hand, nowadays more researched are performed to expand this field of science.

In the engineering, they can be found qualitative and quantitative methods of risk analysis. The choice depends on the results, which may be obtained, but also on the data that are available to analysis. In the first type of methods, the reason is to describe the risk by words by the following methods like: brainstorming, what-if or Preliminary Hazard Analysis. On the other hand, using qualitative methods is possible to obtain the numbers with will describe the risk (for example the probability of occurrence). The knowledge about different methods allow to selecting the appropriate one, to obtain the intended target. The different methods are used to different objectives, and allow to obtaining dissimilar effects. One of the limitations in the choice of the method is the held data and second one is the desired result.

The risk analysis methods, allow to checking before the launch of product, the weakest aspects of the system. They help to create a list of probably failures, which can help to note the most demanding parts of the system. Thanks of that, the operational team can create checklist, which allow to checking the parts of the object exposed to failure. Good performed risk analysis allows focusing on defects of the system and allows repairing them.

The problem in some analysis can be the lack of the data and information about the system. To obtain some values like probability or frequency, the data is needed. The good source of data is historical data base, but not in all cases is available. An example can be the new and innovative device, which is not in the market. The analysis can be based on expert judgement, data base or on human reliability. In this thesis in some studies the Human Reliability Assessment was performed. This method is very useful if there is not enough data to perform other types of analysis. However, should be remembered that for good reliability assessment, person performing the analysis should has the experience and knowledge about the system and environment. Additionally, this technique was created for Nuclear Plants, what can cause some inaccuracies.

The risk analysis can be performed for every system in the nature. Additionally different aspects of system can be extracted on different pieces. For the UUV Seaglider were selected aspects like navigational equipment, area of operation or moving system. The UUV is the hard object to studies. Its environment is variable and not entirely explored. On the other hand, the object itself is not explored properly yet. A lot of companies try to improve these vehicles but there are a lot of factors to repair. For good risk analysis it is needed the knowledge about

the system and the environment in which this system is moving. For this reason, the characterization of the object and environment should be performed. It allow to better understanding the vehicle and knowing its characteristic.

The risk analysis of the gliders presents that these devices are very durable and can work approximately 30 days. It is very long period of time if it is compared with endurance time of other vehicles, for example with autonomous underwater vehicles. Additionally, the analysis shows the weak points of these devices. The worst scenarios for these vehicles are shallow water like port area, because of human activity, marine infrastructure or vessel traffic. They are better suited to work on deep sea. On the other hand, for oceans the launching and recovering procedures is more demanding.

The risk analysis is better method to check the reliability of the system than trial and error method. This technique can save a lot of many for companies, because these vehicles are very expensive and the price is approximately 100,000 \$.

Summarizing, the knowledge about risk analysis should be still expanded. It allows improving the existing devices but also to create and design more safety in the future. The UUVs have a lot of features, which can be improved and are the challenge for contemporaries' engineers.

Bibliography

1. Ayyub Bilal M.: *Risk Analysis in Engineering and Economics*, Chapman & HALL/CRC, 2000, p. 103-104
2. Ayyub Bilal M. and others: *Risk Analysis and Management for Marine Systems*, <http://citeseerx.ist.psu.edu> (access: 27.11.2016)
3. Bellingham J., John J.H., Thorpe S.A., Turekian K.K.: *Autonomous Underwater Vehicles*, Encyclopaedia of Ocean Sciences, Academic Press, 2001
4. Blidberg D.R.: *The Development OF Autonomous Underwater Vehicles (AUV); A Brief Summary*, January 2001
5. Brito M.P., Griffiths G.: *Autonomy: Risk Assessment*, Springer Handbook of Ocean Engineering, 12 November 2015
6. Brito M.P., Griffiths G., Challenor P.: *Risk Analysis for Autonomous Underwater Vehicle Operations in Extreme Environments*, Risk Analysis 30(12), December 2010
7. Brito M.P., Smeed D.A., Griffiths G.: *Analysis of causation of loss of communication with marine autonomous systems: A probability tree approach*, Methods in Oceanography, 2014
8. Brito M.P., Smeed D.A., Griffiths G.: *Underwater glider reliability and implications for survey design*, Journal of Atmospheric and Oceanic technology, No.31 (12), 2014
9. Davis E., Eriksen C., Jones P.: *Autonomous Buoyancy-driven underwater gliders*, <http://www.ifremer.fr/lpo/gliders> (access: 15.02.2017)
10. Eriksen C. and others, *Seaglider: A Long-Range Autonomous Underwater Vehicle for Oceanographic*, IEEE Journal of Oceanic Engineering, Vol.26", No.4, October 2001
11. Faber M.H.: *Risk Assessment in Engineering. Principles, System Representation & Risk Criteria*, June 2008, ISBN 978-3-909386-78-9, p.13-16
12. Fornes P.R., Vilanova N.P.: *AUV Risk Management in Coastal Water survey*, <http://digital.csic.es/bitstream/>, (access: 13.10.2016)
13. Griffiths G., Trembanis A.: *Towards a Risk Management Process for Autonomous Underwater Vehicles*, University of Southampton, March 207
14. Griffiths G. and others, *On the Reliability of the Autosub Autonomous Underwater Vehicle*, Submitted to Underwater Technology, July 2001.
15. Haimes Y.Y., *Risk Modelling, Assessment, and Management*, Wiley, 2004, p.32-35
16. Heinz-Peter B.: *Risk Management: Procedures, Methods and Experiences*, June 2010
17. Kryszicki W., Bartos J., Dyczka W., Królikowski K., Wasilewska M.: *Rachunek Prawdopodobieństwa i statystyka matematyczna w zadaniach, część I*, PWN, Warszawa 1995, p.55-56
18. Litai D.: *A risk comparison methodology- For the assessment of acceptable risk*, Doctoral thesis of Philosophy at Massachusetts Institute of Technology, January 1980
19. Manley J.E.: *The Role of Risk in AUV Development and Deployment*, Oceans, June 2007
20. Ragheb M.: *Event Tree Analysis*, 30.10.2013, <http://mragheb.com> (access: 04.01.2017)
21. Ragheb M.: *The Risk Assessment Methodology*, 27.10.2016, <http://mragheb.com> (access:04.02.2017)
22. Rausand M.: *Preliminary Hazard Analysis*, <http://frigg.ivt.ntnu.no/ross/slides/pha.pdf> (access: 20.12.2016)
23. Rausand M., Hoyland A.: *System reliability Theory. Models, Statistical Methods and Applications, second edition*, Wiley-Interscience, New Jersey 2004, p 5-32

24. Roque D., Rodriguez P., Labarta U.: *Deploying AUVs in restricted Areas*, Sea Technology, August 2012
25. Rudnick L., Davis E., Eriksen C., Fratantoni M., Perry J., *Underwater Gliders for Ocean Research*, http://pordlabs.ucsd.edu/rdavis/publications/MTS_Glider.pdf (access: 5.01.2017)
26. Ch. Starr, Social Benefit versus Technological Risk, American Association for the Advancement of Science, reprinted from 19 September 1969
27. Størkersen N., Hasvold Ø., *Power Sources for AUVs*, Paper submitted to the "Science and Defence Conf", Brest, France, 19 October 2004
28. Wall K.D., *The Kaplan and Garrick Definition of Risk and its Application to Managerial Decision Problems*, 2011
29. Sailing directions, Pub. 194, Baltic Sea (Southern Part), 17 edition, The British Admiralty, 2014
30. NUREG/CR-6883, 2005. The SPAR-H Human-Reliability Analysis Method, Washington D.C.: Office of Nuclear Regulatory Research - U.S. Nuclear Regulatory Commission
31. Veress A., Lecointre B. and others, Vehicle Control for Autonomous Underwater Vehicle, http://vbn.aau.dk/ws/files/58194559/Work_sheet.pdf (access:15.02.2017)

Websites

32. *Add-ins*, <https://www.add-ins.com/analyzer/>
33. *Boolean Algebra*, https://en.wikipedia.org/wiki/Boolean_algebra
34. *Causal Capital*, <http://causalcapital.blogspot.com.es>
35. *Checklist*, <https://en.wikipedia.org/wiki/Checklist>
36. *Corps Risk Analysis Gateway*, <http://www.corpsriskanalysisgateway.us>
37. *Drone centre*, <http://dronecenter.bard.edu/underwater-drones/>
38. *Kongsberg Company*, <https://www.km.kongsberg.com>
39. *Massachusetts Institute of Technology*, <http://web.mit.edu>
40. *Medical Device Compliance Consulting*, <http://www.medicept.com>
41. *National Oceanic and Atmospheric Administration*, <http://oceanexplorer.noaa.gov>
42. *Occupational Safety & Health Training*, <http://www.oshatrain.org/>
43. *Offshore engineer*, <http://www.oedigital.com/>
44. *Probability Density Function* https://en.wikipedia.org/wiki/Probability_density_function
45. *Project GROOM*, <http://www.groom-fp7.eu/doku.php>
46. *Risk Analysis*, https://en.wikipedia.org/wiki/Risk_analysis
47. *Seaglider manual*, http://doga.ogs.trieste.it/sire/gliders/manuali_seaglider/
48. *Schmidt Ocean Institute*, <https://schmidtocean.org/cruise-log-post>
49. *Science direct*, <http://www.sciencedirect.com/science>
50. *Single loss expectancy*, https://en.wikipedia.org/wiki/Single-loss_expectancy
51. *Society for risk analysis*, <http://www.sra.org/about-society-risk-analysis>
52. *SPURV*, <https://en.wikipedia.org/wiki/SPURV>
53. *Teach yourself statistics*, <http://stattrek.com>

Program:

Microsoft Excel, 2007

List of tables

2.1. Technical description of vehicle Seaglider.....	18
3.1. Quantitative Risk Analysis Methods.....	30
3.2. Basic gates used in Fault Tree Analysis.....	31
3.3. Basic Boolean algebra and Composed operation.....	32
3.4. Qualitative Risk Analysis Methods.....	34
3.5. Classification of Hazard severity and frequency.....	36
3.6. Quantiles of the normal distribution.....	43
3.7. PSF in the SPAR-H method.....	44
4.1. Number of gliders and the number of missions in project GROOM.....	46
4.2. Operation statistics of different types of gliders.....	47
4.3. Number of failures and aborts e in function of different causes.....	49
4.4. Preliminary Hazard Analysis for conditions of coaster water.....	51
4.5. Scales to assess the probability and severity of hazards and Risk Matrix.....	51
4.6. Probability of survive for different areas of operation based on Kaplan-Maier estimator....	52
4.7. Averages, the standard deviation and the variance of mean time to failure on deep ocean.....	54
4.8. Confidence intervals for different confidence levels.....	54
4.9. Preliminary Hazard Analysis for navigational equipment.....	55
4.10. Results of Human Reliability Assessment for navigational aspect.....	57
4.11. PSFs for mission damage of navigational equipment not detected-diagnosis and action.....	57
4.12. Dependency Condition Table.....	58
4.13 Detailed Human Error Probability Analysis for navigational aspects.....	59
4.14. Events and values of human probability calculated by SPAR-H method.....	61
4.15 The Human Reliability Assessment for recovering process.....	63
4.16. The results of What-if Analysis.....	64
5.1. Assessment of Risk Priority Number for Events in Coastal Waters.....	64
5.2. Confidence intervals for different confidence levels.....	68
5.3. Assessment of frequency and consequence for different events.....	69
5.4 Preliminary Hazard Analysis and Risk Priority Number.....	71
6.1. Methods used to determine Risk Acceptance.....	74
6.2. Spread sheet for owners to calculate acceptability of the risk.....	77

List of figures

1.1. UUV with solar panels.....	12
1.2. UUV's application and characteristics.....	13
1.3. Festo's AquaJelly.....	16
2.1. Sketch of the Seaglider and basics element including: hull cross section, the antenna mast, and the wing plan section and side view.....	21
2.2. Seaglider dive cycle.....	22
2.3. The mass shifter (batteries) causing pitch changes.....	22
2.4. External bladder inflation and deflection.....	23
2.5. Mass shifter causing roll changes.....	23
2.6. Launching methods for Seagliders.....	24
2.7. System Representation.....	26
3.1. Treatment of the risk.....	29
3.2. Coupling of Fault Tree Analysis and Event Tree Analysis.....	33
3.3. PHA worksheet.....	36
3.4. Risk Matrix.....	37
3.5. The relationship between the time do failure and the state variable $X(t)$	41
4.1. Event tree analysis for navigational aspect.....	60
4.2 The Fault Tree Analysis for event Failure during launching.....	62
4.3 Event tree analysis for recovering process.....	63
6.1. Risk Matrix to calculate Risk Priority Number.....	75
6.2. A process for the owner to decide about acceptability of the risk.....	76
6.3. Farmer curve, Annual frequency of facilities from man-made structures, compared with risk profile of 100 operational nuclear plants.....	78
6.4. Risk plotted relative to benefit, for various kinds of voluntary and involuntary exposure....	79
6.5. Target Risk Based on Consequence of Failure for Industries/Activities.....	80
6.6. Cost effectiveness of risk reduction.....	81

List of diagrams

4.1. The percentage of the missions finished with failure (mission abort), losses of vehicle and missions successful.....	47
4.2. Probability Density functions of failure of Seaglider.....	48
4.3. The percentage of the specific cause in the general number of failures and missions.....	50
4.4 Probability of survive for different areas of operation (Source: Own calculations based on Kaplan-Maier estimator).....	54
5.1 Probability of survive for different areas of operation (a-shelf and b-deep ocean) (Source: Own calculations based on Kaplan-Maier estimator).....	66
5.2 Probability density functions of failure on deep ocean.....	68

Annexes

<i>Annex A The results of Preliminary Hazard Analysis for launching process.....</i>	<i>90</i>
<i>Annex B Detailed HRA, summary for launching process.....</i>	<i>91</i>
<i>Annex C The results of Preliminary Hazard Analysis for recovering process.....</i>	<i>92</i>
<i>Annex D Detailed HRA, summary for recovering process.....</i>	<i>93</i>

Attachment A The results of Preliminary Hazard Analysis for launching process

No.	Hazard	Cause	Consequences	Risk			Risk Reducing measures
				Freq	Cons	RPN	
1	Wrong density used	Fatigue of crew, lack of experience	Difficult launching,	2	2	4	Training of crew
2	Wrong calculations	Wrong parameters used, lack of experience and knowledge	Unexpected Glider behaviour	1	3	3	Training of crew
3	Payload configuration error	Lack of experience, lack of control and procedures	Unexpected behaviour of glider	1	4	4	Preparation conducted by specified procedures
4	Wrong parameters implemented	Lack of time, experience and knowledge	Unexpected glider behaviour	3	2	6	Training of crew
5	Error of equipment not detected	Inappropriate control, lack of procedures, negligence of crew	Unexpected glider behaviour, mission abort, data not collected	2	4	8	Specified procedures, better control of equipment, careful control
6	Glider is not set up physically correctly to launching	Lack of time, negligence of crew, lack of experience	Difficult in launching, damage to Glider	2	4	8	Training of crew, better control of equipment, better procedures
7	Glider is wrongly ballasted for launching	Lack of time, fatigue of crew, lack of experience and knowledge	Difficult launching, unexpected behaviour	2	3	6	Training of crew, validate programming
8	Glider position is inappropriate	Lack of experience and knowledge	Difficult launching, damage to Glider	3	4	12	Better control, specified procedures, training of crew
9	Glider is damage	Inappropriate treatment of vehicle	Difficult launching, unexpected behaviour, loss of Glider	1	4	4	Better control
10	Glider is damage during transport to launching location	Improper packing, improper stowage, imprudence, bad preparation	Impossibility of launching, launching and mission abort	2	4	8	Specified procedures
11	Glider is dropped during launching	Fatigue of crew, Imprudence, bad preparation	Impossibility of launching, launching abort	1	4	4	Specified procedures, training of crew, better control of equipment
12	Software error not detected	Lack of procedures, misunderstanding of program	Unexpected behaviour, mission abort	1	3	3	Specified procedures, better control

Attachment B Detailed HRA, summary for launching process

Abb.	PSFs								HEP	P_w	Dependency					P_w
	Time	Stress	Comp.	Exp.	Proced.	Ergo.	FfD	W.Process			Crew	Time	Local	Cause	Dep	
WD	1	1	1	0.5	1	0.5	1	0.5	0.00125	0.00125	-	-	-	-	-	0.00125
	-	-	-	-	-	-	-	-	-		-					
WC	1	1	1	1	1	0.5	1	0.5	0.0025	0.0025	-	-	-	-	-	0.0025
	-	-	-	-	-	-	-	-	-		-					
PC	1	1	1	0.5	5	0.5	1	0.5	0.00625	0.00625	-	-	-	-	-	0.00625
	-	-	-	-	-	-	-	-	-		-					
WS	1	1	1	0.5	1	0.5	1	0.5	0.00125	0.00125	-	-	-	-	-	0.00125
	-	-	-	-	-	-	-	-	-		-					
EE	1	1	2	1	1	1	1	0.5	0.01	0.11	s	nc	d	na	moderate	0.237
	10	2	5	1	1	1	1	1	0.1							
SU	1	2	2	0.5	1	1	1	1	0.02	0.02	-	-	-	-	-	0.02
	-	-	-	-	-	-	-	-	-		-					
WB	1	1	2	0.5	1	0.5	1	0.5	0.0025	0.0025	-	-	-	-	-	0.0025
	-	-	-	-	-	-	-	-	-		-					
PI	-	-	-	-	-	-	-	-	0.01	0.01	-	-	-	-	-	0.01
	10	2	2	0.5	1	0.5	1	1	-							
DT	1	1	1	1	1	1	1	0.5	0.005	0.005	-	-	-	-	-	0.005
	-	-	-	-	-	-	-	-	-		-					
DL	-	-	-	-	-	-	-	-	-	0.025	-	-	-	-	-	0.025
	10	5	2	0.5	1	0.5	1	1	0.025							
SE	1	1	2	0.5	1	0.5	1	0.5	0.0025	0.0125	s	nc	d	na	moderate	0.1536
	10	2	2	0.5	1	0.5	1	1	0.01							

Abb- abbreviation; PSFs- Performance Shaping factors; HEP-Human Error Probability; Comp-complexity; Exp- experience; Proced- procedures; Ergo-ergonomic; FfD-fitness for duty; W.Process- Work Process; Local- location; Dep-dependency;

Attachment C *The results of Preliminary Hazard Analysis for recovering process*

No.	Hazard	Cause	Consequences	Risk			Risk reducing measures
				Freq	Cons	PRN	
1	Current not considered	Wrong parameters used, lack of experience	Difficult recovering, unexpected behaviour, elongation of the process	2	2	4	Better procedures and software's
2	Hit the ship board	Bad preparation process, lack of knowledge , inappropriate position of vessel	Loss of equipment and data, damage of ship side	3	5	15	Training of crew, better prepared devices and equipment
3	Difficult weather conditions not considered (high wave)	Lack of time and knowledge, negligence of crew	Difficult recovering, damage of vehicle, loss of vehicle	2	4	8	Training of crew, better preparation for mission
4	Error of equipment not detected	Inappropriate control, lack of procedures, negligence of crew	Unexpected glider behaviour, loss of data, loss of equipment	2	5	10	Specified procedures, better control of equipment, Carrefour control
5	Glider is wrong ballasted	Wrong parameters used, lack of knowledge and experience	Difficult recovering, unexpected behaviour, hit the ship board	1	4	4	Training for crew, specified procedures
6	Unexpected high tide	Wrong calculations, wrong parameters used, lack of experience	Difficult recovering	2	1	2	Training of crew
7	Wrong calculations	Wrong parameters used, lack of experience and knowledge	Unexpected behaviour, elongation of the process	2	4	8	Better procedures, better preparation
8	Inappropriate position of vessel	Wrong preparation for recovering, wrong calculations, inappropriate preparation	Damage of vehicle, loss of vehicle, loss of data	2	5	10	Better procedures and preparation, training of crew
9	Lifting devices inappropriate prepared	Wrong preparation for process, lack of knowledge, human error	Damage of vehicle, loss of vehicle	2	4	8	Training of crew, better procedures and control of equipment

Attachment D Detailed HRA, summary for recovering process

Abb.	PSFs								HEP	P_w	Dependency					P_w
	Time	Stress	Comp.	Exp.	Proced.	Ergo.	FfD	W.Process			Crew	Time	Local	Cause	Dep	
CC	1	1	1	1	1	1	1	1	0.01	0.01	-	-	-	-	-	0.01
	-	-	-	-	-	-	-	-	-		-	-	-	-	-	
SB	-	-	-	-	-	-	-	-	-	0.01	-	-	-	-	-	0.01
	1	5	2	1	1	1	1	1	0.01		-	-	-	-	-	
DW	1	1	2	1	1	1	1	1	0.02	0.02	-	-	-	-	-	0.02
	-	-	-	-	-	-	-	-	-		-	-	-	-	-	
EE	1	1	0.1	1	0.5	1	1	1	0.0005	0.1005	s	nc	d	na	moderate	0.229
	10	5	2	1	1	1	1	1	0.1		-	-	-	-	-	
GB	1	1	0.1	1	0.5	1	1	1	0.0005	0.0005	-	-	-	-	-	0.0005
	-	-	-	-	-	-	-	-	-		-	-	-	-	-	
UH	1	1	1	1	1	1	1	1	0.01	0.01	-	-	-	-	-	0.01
	-	-	-	-	-	-	-	-	-		-	-	-	-	-	
WA	1	2	2	1	5	1	1	1	0.2	0.01	-	-	-	-	-	0.2
	-	-	-	-	-	-	-	-	-		-	-	-	-	-	
IP	-	-	-	-	-	-	-	-	-	0.16	-	-	-	-	-	0.16
	10	2	2	1	5	1	1	0.8	0.16		-	-	-	-	-	
LD	-	-	-	-	-	-	-	-	-	0.02	-	-	-	-	-	0.02
	10	2	1	1	1	1	1	1	0.02		-	-	-	-	-	
WP	-	-	-	-	-	-	-	-	-	0.1	-	-	-	-	-	0.1
	10	2	5	1	1	1	1	1	0.1		-	-	-	-	-	

Abb- abbreviation; PSFs- Performance Shaping factors; HEP-Human Error Probability; Comp-complexity; Exp- experience; Proced- procedures; Ergo- ergonomic; FfD-fitness for duty; W.Process- Work Process; Local- location; Dep-dependency;