Proceedings of the ASME 2014 33rd International Conference on Ocean, Offshore and Arctic Engineering
OMAE2014
June 8-13, 2014, San Francisco, California, USA

OMAE2014-23776

A SYSTEMATIC APPROACH TO RISK ASSESSMENT – FOCUSING ON AUTONOMOUS UNDERWATER VEHICLES AND OPERATIONS IN ARCTIC AREAS

Ingrid Bouwer Utne
Department of Marine Technology, NTNU
7491 Trondheim, Norway

Ingrid Schjølberg
Department of Marine Technology, NTNU
7491 Trondheim, Norway

ABSTRACT

Climatic degradation of equipment, in combination with stringent requirements for human safety and minimalistic environmental impact, need to be addressed through improved risk assessment in vulnerable areas, such as the Arctic. The performance of technologies and risk related to its utilization, for example in terms of autonomous operations, significantly impact future requirements for oil and gas exploration and production. An interdisciplinary and systemic approach integrating both risk to the environment and to humans is needed as the challenges related to operation in extreme environments directly impact risk, costs, and the general societal acceptance of the activities. Development of such an approach focusing on autonomous underwater vehicles (AUV) and operations is addressed in this paper.

INTRODUCTION

Rigs, ships, and subsea intervention systems operating in extreme environments needs to be safe, cost effective and with minimal environmental impact based on the societal expectations for responsible development. This is, for example, reflected in the polarized ongoing public debate about increased oil and gas exploration in northern Norway. Stakeholders either argue for the protection of the environment, or claim that exploration of these areas is inevitable due to global societal consumption of non-renewable resources and the need for increased business and industry development.

According to the Petroleum Safety Authority (PSA) in Norway (1), incidents at Snorre A (2004) and Gullfaks C (2010) on the Norwegian Continental Shelf (NCS) could have resulted in accidents similar to the Macondo blowout in the Gulf of Mexico in 2010. The PSA has argued that the risk reduction measures implemented by the oil and gas industry in Norway apparently are not sufficient. Further, the main focus of typical risk assessments in industry is on safety for human beings, whereas the public opinion is also more concerned about consequences to the environment. This indicates that there is a gap between the main societal concerns with respect to the environmental effect of oil and gas activities in the north and the main objectives of industry risk assessments of the production systems.

The special environmental conditions in the Arctic, such as ice, temperature, daylight, water depths, sea currents, permafrost, wind, and distance to shore, impact design criteria, choice of technology, and operational philosophy for an oil and gas facility. Ice influences all aspects of oil and gas Artic activities, including the design and construction of facilities to resist the ice conditions, operations, as well as transportation and rescue operations. The characteristics and potential impact on oil and gas field developments are addressed in specific studies on ice properties, ice drift and ice forces that actually are encountered in the prospective area. Icing on vessels is a concern in large areas of the Arctic, even during the ice-free seasons. Arctic icing and ice accretion caused by atmospheric icing and sea spray can cause problems on outdoor facilities, installations and structures in terms of increased weight on the installation and access to and workability of critical facilities. Dropping of ice loads should also be taken into consideration to prevent damage. Sensors and optical instruments are especially vulnerable to icing (2). This calls for a higher degree of autonomy to reduce operation time and dependency on weather conditions. Also, autonomy facilitates the execution of complex and/or repetitive missions, enabling faster, more reliable and safer operations without equipment damage and loss of human life.

Typical autonomous underwater operations in Artic areas are intervention, maintenance and repair, as well mapping and monitoring of installed equipment and the seafloor. Autonomous operations in Artic areas using underwater

vehicles equipped with tools and sensors are the main focus of the presented work.

Climatic degradation of equipment, in combination with stringent requirements for human safety and minimalistic environmental impact, calls for a systematic approach for risk management of such operations in vulnerable areas as the Arctic. The performance of technologies and risks related to utilization of autonomous systems significantly impact future requirements for oil and gas exploration and production. Design and operational challenges, as well as potential risks, have to be addressed when developing a safety philosophy and performing risk assessments for technological systems to be applied in the Artic areas.

Risk assessment of operations of autonomous underwater vehicles (AUV) has been addressed by (3, 4, 5 and 6), but their main focus is on determining the probability of loss of the AUV during a mission. (7, 8) develop an approach for determining the mission path with minimal risk for the AUV. Results of operational experience should be input to redesign or new developments of AUVs. (9) describes the main contributors to risk of AUV failure. For control systems these are in most cases related to input errors from the operator resulting in a major failure of the system. Further, the probability of an undesirable incident is highest during commissioning and decommissioning.

The objective of this paper is to develop a holistic approach to risk assessment of autonomous underwater operation, integrating both risks to the environment, humans and material assets. The work presents a taxonomy which can be used to identify and categorize hazards to be assessed and mitigated during the preparation of AUV's missions. The taxonomy can also be used as input to improve the design of the AUV, making it more robust and less vulnerable to technical faults and failures. Categories for frequencies and consequences of hazardous events are proposed, and use of IEC 61508 for development of safety systems is outlined.

The structure of the paper is as follows: the next Section gives an introduction to AUVs, then relevant standards are described, before the risk assessment framework is presented. Last, conclusions and further work are stated.

.

AUTONOMOUS UNDERWATER VEHICLES (AUV) IN THE ARTIC

AUVs have several advantages related to the operational challenges of the Arctic. AUVs are less dependent on support of surface vessels and thereby less vulnerable to weather conditions reducing the exposure of personnel to cold climate conditions and reducing costs of operations. Areas that previously have been difficult to reach can be accessed (4). Less costly and more efficient data collection can be achieved with high data quality compared to surface vessel sampling (7, 8). AUVs can provide easier mapping and monitoring of ice (5). Further, AUV capabilities are emerging that enable subsea and deep water inspection, repair and light intervention (10).

Underwater vehicles can be categorized into manned submersibles and unmanned underwater vehicles (UUV), i.e., towed vehicles, remotely operated vehicles (ROV), and autonomous underwater vehicles (AUV). There are different levels of autonomy; i.e., manual operation, management by consent, management by exception, and fully autonomous. Currently, AUVs operate with management by consent, which means that the AUV recommends actions, but the system involves the operator at key points for information or decisions (11).

An AUV is not directly controlled by an operator, but is mainly preprogrammed for a mission. The main power source is integrated and communication with an operator is related to data transmission with limited bandwidth. Contrary to a ROV, an AUV has no permanent connection to an operation center.

Civil applications of AUVs are environmental monitoring and data collection, inspection of pipelines and subsea equipment. AUVs may also be equipped with manipulator arms enabling lightweight intervention.

In the following, the AUV system is defined to consist of seven main parts; (i) the guidance, navigation, and control, (ii) external linked system, (iii) the energy storage, (iv), thrusters, (v) sensors, (vi) emergency shutdown system, and (vii) the ballast and buoyancy system.

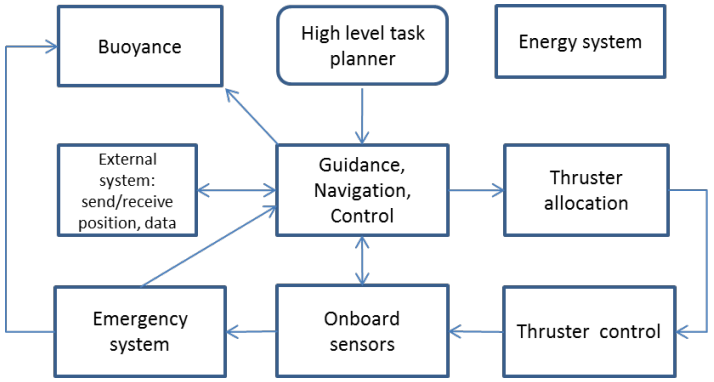

Figure 1. Main components of a typical AUV.

Important dimensions of an AUV´s quality are product safety, availability, functional safety, and maintainability. Hence, a producer of an AUV must therefore identify and ensure that such performance requirements to a system are fulfilled.

According to (12) we may divide the requirements into four categories, namely; (i) Functional safety and safety integrity requirements, (ii) Product or system safety requirements, (iii) Operational availability requirements, and (iv) Maintainability and maintenance support requirements. Further, it is necessary to look into performance in three different ways; (a) the desired performance, (b) the predicted performance, and (c) the actual performance. A successful system has a very narrow gap between (b) and (c). Obviously, the actual performance is impacted by operational conditions and maintenance, in addition to its design properties. The

predicted performance may be foreseen through analysis, simulation and testing.

A producer of an AUV has to establish a systematic way for ensuring that the performance requirements are addressed throughout the system life cycle. Hence, a system development process has to define the performance requirements, assess the risk involved and mitigate those that are unacceptable, plan and implement the design properties, ensure that the performance of the system is close to the desired performance, and follow up and monitor compliance during the system life cycle.

STANDARDS

An important basis for deriving safety performance requirements to an AUV system is found in standards, such as ISO 31000, IEC61508, IEC60300-3-9, NORSOK U-102, and NORSOK Z-013.

ISO 31000 AND ISO 31010

The risk management process in ISO 31000 (13) consists of establishing the context, risk identification, risk analysis, risk evaluation, risk treatment. In parallel, communication and consultations, as well as monitoring and review are essential activities (see Figure 2). The risk management process is feasible during all life cycle phases, as shown in Figure 2.

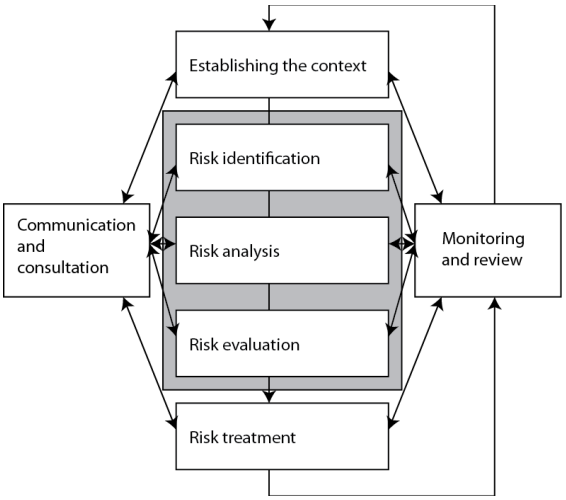

Figure 2. The risk management process in (13). The grey box highlights the main constituent parts of risk assessment.

The key elements in risk assessment are risk identification, analysis and evaluation, which are highlighted by the grey box in Figure 2.

ISO 31010 (14) supports ISO31000 and includes information to help selection and application of risk assessment techniques.

IEC 60300 PART 1-16

Dependability is a collective term addressing availability performance, i.e., reliability, maintenance, and maintenance support for simple products to complex systems. The different parts of the IEC 60300 standard (15) provides guidance on general principles for establishing dependability management systems, as well as more specific methods and tools for attaining the desired availability performance.

IEC 61508 PART 1-5

For all systems with an initial risk to human, equipment and/or environment, acceptable risk should be defined. According to (16) risk is the combined answer to three questions: (i) What can go wrong? (ii) What is the likelihood of that happening? (iii) What are the consequences? To achieve acceptable risk, safety systems based on different technologies can be implemented.

IEC 61508 (17) is an international safety standard that provides requirements to minimize dangerous failures when developing a safety-related system that use E/E/PE technologies. An E/E/PE safety-related system includes the complete system necessary to carry out the safety function; from sensors, through control logics and communication, to actuators. The standard is generic and may be used stand-alone, as well as a basis for sector and product standards. The standard provides an overall safety life cycle, divided into 16 phases, which are recommended to follow in order to claim conformance to the standard. The life cycle covers the safety system from concept to decommissioning or disposal. In addition to the life cycle phases, the standard has requirements to proper documentation, management of functional safety and verification during the project. To arrive at a judgment on the functional safety, a functional safety assessment, FSA, is required.

NORSOK U-102

The NORSOK-standards are developed by the Norwegian oil and gas industry to ensure safe and cost effective developments and operations. NORSOK U-102 (18) applies to all UUV, including ROV and AUV. NORSOK U-102 defines an ROV as “equipment used in water with an ability to observe the surroundings and positioning itself remote controlled from the surface through a cable”. Further, an AUV is “equipment used in water with an ability to positioning itself without interference from surface control”. An ROV system is a system, which comprises the ROV, the handling system, the surface control system and all associated equipment.

NORSOK U-102 classifies ROVs into three different classes; (i) Pure observation, (ii) Observation with payload option, and (iii) Work class vehicles, shown in Figure 3. Classes II A and B, and III A and B refer to potential intervention work and energy consumption.

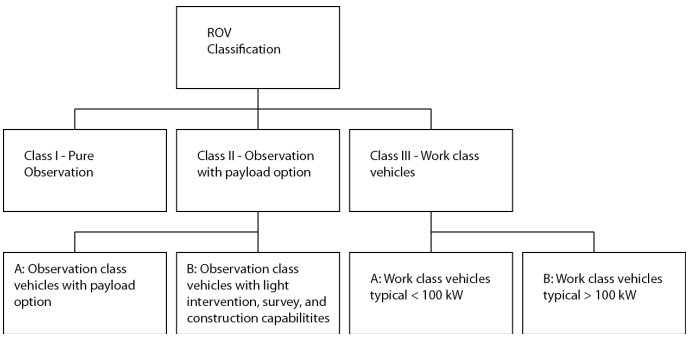

Figure 3. Classification of ROVs in NORSOK U-102 (18).

NORSOK U-102 is aimed at companies involved in oil and gas production, and the renewable energy sectors, but the standard may have relevance to other industries. The standard recommends a preventive maintenance scheme for UUV addressing the critical components for the system. The maintenance shall be based on manufacturer's recommendations and experience gathered, including collecting historical data to ensure continuous improvement. This means that faults, failures and maintenance actions need to be logged to obtain sufficient experience. The quantity of spare parts onboard during operation has to be defined. Spare part requirements are to be based on a failure mode and effect analysis (FMEA) and/or operational experience. A certain level of manning is required depending on the size of the UUV and the planned tasks and duties.

Risk assessments are to be actively used in preparations for operation. It is important to ensure that sufficient information with relevance to safe and efficient operational performance is exchanged during shift changes.

NORSOK Z-013

The purpose of NORSOK Z-013 (19) is to help ensuring that risk assessments are carried out as basis for decision-making in the Norwegian petroleum industry. The standard uses the same structure and model as ISO 31000, but modifies it to cover risk and emergency preparedness assessment only.

SYSTEMS ENGINEERING AND SAFETY PHILOSOPHY

The complexity involved in Arctic operations, due to the harsh environmental conditions, the many stakeholders involved, and the potential catastrophic consequences of system failure to the environment, human lives, and material assets means that there is a need for a new type of hazard analyses and risk assessments. According to (20) risk assessments should go beyond component failures and deal with the complex role software and humans have in high-tech systems. The basis for such new methods should be constituted by systems theory, which focuses on systems as a whole; more than the sum of its constituent parts (20, 21). In a systems perspective, accidents occur due to interactions among system components and are not due to single technical failures. In system models the focus is on operation and organization when investigating accidents.

(20) states that safety is controlled or enforced in terms of constraints on the system behavior. This means that safety can be considered a control problem and accidents happen when safety is not controlled sufficiently. Undesired events reflect inadequate control, for example, in the design process or during operation. As such, the control structure has to be understood in order to gain understanding of what went wrong.

Systems engineering focuses on life cycle design, because any system develops and operates in the course of time. During the initial phases of system design and development requirements, for example, to reliability and maintainability are determined. Then risk management means focusing on design risk, i.e., the system´s performance requirements balancing system reliability with requirements to maintenance during operation. During operation, risk management has to focus on risks related to operation of the system, for example, during the mission of the AUV. These risk are formed due to system properties as a result of system design and operational conditions. Risk management is the process of controlling both risk due to design and operation. This is shown in 4.

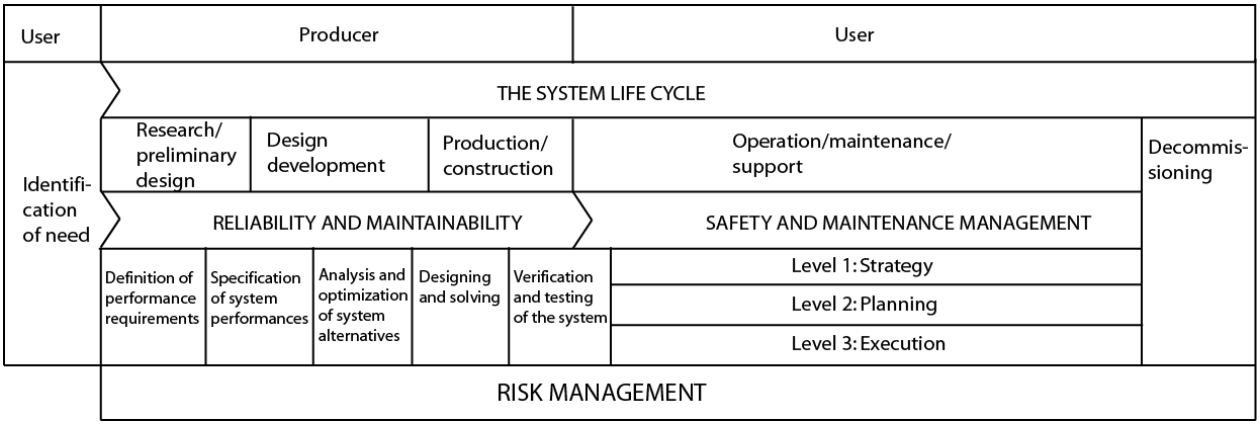

Figure 4. Risk management during the life cycle and its relation to reliability, maintainability, maintenance and safety performance. Extracted from (22, 23 and 24).

In the remainder of this paper we focus on those aspects of the systems engineering process that relates to risk assessment. Further description of the systems engineering process may be found in, e.g., (22).

RISK ASSESSMENT OF AUV

In general, safe operation of AUVs are related to (i) planning of the mission, and (ii) the functional performance of the AUV during the mission.

PLANNING OF THE MISSION

Mission planning is crucial for safe operation of AUVs and is related to operating procedures. The procedures should be developed based on risk assessments, manuals and system documentation, and should also contain contingency plans in case of unplanned mission termination.

An important part of the planning is to consider the environmental conditions, i.e., the sea state, the structure of the sea floor, the current weather and the weather forecast at the launch and recovery location, as well as the possible effects of currents and tides on the water column in the area where the AUV will operate. Obviously, the AUV should not surface in excessive sea states and there are limits to wave heights for launch and recovery. The sea floor and nearby installations, such as pipelines and subsea templates have to be identified. The water temperature and density may affect the buoyancy and the trim of the AUV, as well as acoustic communication.

In Arctic areas presence of ice has to be considered, both for the AUV and for the launch and recovery systems. Moving ice may impact the AUV during its operation, may make it difficult to reach, and worst case, the AUV may get stuck under ice. Surfacing in ice may damage the AUV´s communication systems and prevent recovery. Icing on equipment and machinery on deck may cause problems during launch and recovery. Hence, additional systems for recovery of the AUV may be needed

In addition to the environmental conditions, other activities in the surroundings, such as marine operations, vessel traffic, and diving, and possible interference with the AUV have to be assessed. A permit – to – work may have to be issued before the operation can commence.

AUVs are designed to terminate their mission if specific error conditions occur. This means that an unplanned recovery of the AUV may be required.

Last, but not least, the competence of the operating personnel is crucial. Excellent procedures are worthless if the crew does not follow them.

THE FUNCTIONAL PERFORMANCE OF THE AUV DURING THE MISSION

Part of the operating procedures should be the testing and verification of functionality of the main components of the AUV prior to the mission, such as data transfer to the AUV, sensor status, and power source status and endurance.

The availability of the AUV is related to its reliability (determined through design), maintainability and maintenance support. A preventive maintenance scheme should be executed on the AUV (18), based on vendor´s recommendations, condition assessments, and operating experience. The Reliability Centered Maintenance (RCM) approach could be used as basis for developing the maintenance program (see, e.g., IEC60300 – Part 3-11). The maintenance system has to contain records of executed work and system condition.

Adequate supply of spares is crucial for successful operations. It is necessary to identify those spares that are critical for efficient and safe operation. In Arctic areas, the availability of spares and personnel may be limited and this has to be taken into consideration for spare parts management. In cold climate the power source may demand more maintenance and charging and/or fuel supply has to be sufficiently planned.

RISK IDENTIFICATION

Currently, there is little information about typical hazards related to operation of AUVs, even though (25) has made a brief attempt. Hazards related to operation have to be taken into account during the system design and development process, in order to achieve an acceptable risk level. Further, hazards have to be identified and risks assessed when developing operating procedures and planning a mission.

DESIGN

A general overview of potential hazards which should be specifically addressed during the design of AUVs is presented in Figure 5.

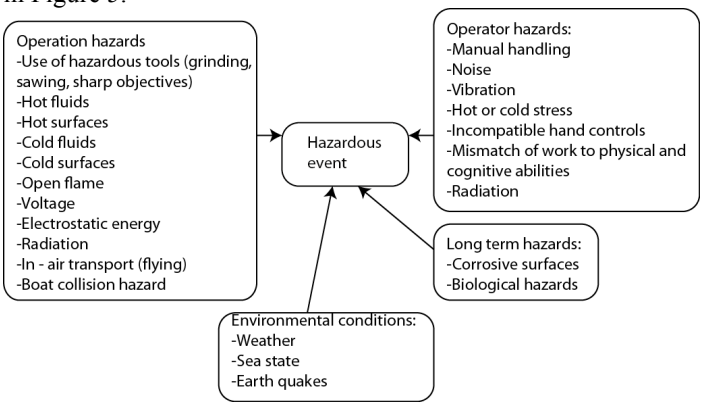

Figure 5. Potential hazards to be considered during the design of AUVs. Adapted from ISO 17776 (26).

OPERATIONS

Losing an AUV is costly and loss of control of the AUV may cause damage, e.g., to a pipeline or subsea template. Serious situations of hazard and accident are, for example, “drift off” and “drive off”. Drift off means that the AUV for not follow the path correctly due to for example propulsion or energy loss. Drive off means that there is something wrong with the input to the navigation or control system or that it does not respond correctly. This may be due to loss of

Table 1. Taxonomy for potential hazardous events related to AUVs. Extracted from (25, 27, 28 and 29).

Type	Level 1	Level 2	Level 3
Natural events	Meteorological; weather conditions	Strong wind	Navigation error in external positioning system
		Strong currents and tides	Navigation error in local positioning system
		Sea state and waves	External communication failure
		Visibility	Mission failure
		Temperatures	Hardware failure
		Salinity	Change in operation conditions
		Sea spray	Change in operation conditions
	Oceanography	Icebergs	Collision may occure; Recovery challenge
		Multi-year ics	Collision may occure; Recovery challenge
		Ice based changes of seabed	Collision may occure due to unknown terrain
	Geological	Earthquake	Loss of equipment
		Tsunamis	Loss of equipment
		Unknow hilly seafloor	Collision may occure to due unknown terrain
Technical event	Pollution	Release of dangerous substances	Battery leakage; loss of power
	Design	Power supply failure	Battery failure
		Structural failure	Pressure vessel leaks
		Buoyancy system failure	Pressure vessel leaks
		Propulsion system failure	Thruster failure
			Jet system failure (if applicable)
		Software failure	Control failures
			Electronics hardware failure
			Tether failure (if applicable)
			Sensor system failure
		Navigation system failure	Bad GPS
		Navigation system failure	Loss of contact with external system
		Sensor system failure	Sonar failure
			Failure in transponders/beacons
			Failure in beam
			Camera failure
			Lights failure
	Operational	Collision	Collision with seabed
			Collision with vessel
			Collision with subsea structure
			Collision with diver(s)
		Communication failure	Acoustic interference
			Tether failure (if applicable)
			Tether entanglement (if applicable)
	Site specific	Water depth	Tether failure due to associated drag (if applicable)
		Sea bed characteristics	Rocky (entanglement) or soft (stirred particles)
		Presence of hydrocarbons	Non-compliance with safety zone of oil and gas installation
Human behavior event	Individual	Negligent	Operation outside the design envelope
		Inexperience	Limited situational awareness and training
	Collective	Deficient safety climate	Inadequate focus on risk management
		Organizational weaknesses	Inadequate communication
			Unclear responsibilities
Malicious event	Sabotage		

communication where the AUV is not able to regularly confirm its position, nor send or receive data. A drive off scenario may be more severe than drift off, depending on the state of operation.

Table 1 proposes a taxonomy for potential hazardous events related to operation of AUVs. The different levels reflect the level of detail with respect to possible causes. The taxonomy may be used to determine the most critical issues required for more detailed risk assessment. This means that when developing an operational procedure or when assessing risks before a mission, the taxonomy may aid the risk identification of relevant hazardous events.

RISK ANALYSIS

There is lack of statistics, but the frequency of failure that is published is in general high. (28) presents an average failure

rate of 0.27 (64 failures of 240 missions), and the Weibull distribution fits best with the data set. (30) uses a Markov state space model to capture the sequence of events occurring during operation of the AUV and expert judgments to determine the transition probabilities between different states. The failure distribution may indicate when there is need for increased attention with respect to potential failure conditions, for example, during a mission. (31) calculates the reliability after 40 hours for an AUV to $R(40) = 0.8007$ using the exponential distribution.

A common way to express losses when there is lack of data is to use frequency/probability and consequence categories. Categories for frequencies are proposed in Table 2.

Table 2. Categories for frequencies.

Categories	Frequency (per year)
Frequent	1-10
Occasional	0.1-1
Possible	0.01-0.1
Rare	0.001-0.01
Improbable	0.0001-0.001

In general, the consequence categories in risk assessments are divided into impact on the environment, human life, material assets, and loss of reputation. Further, the consequences can be calculated, for example, with respect to potential loss of life (PLL) or in terms of costs. A consequence Table is proposed in Table 3.

Table 3. Consequence matrix for risk analysis of AUV operations.

Categories/ Dimensions	Impact on human lives	Impact on environment	Economic losses, including loss of reputation
No impact/ minor	No injury or illness	No impact or very short term limited impact	ALARP is not applicable
Moderate	Injury or illness that result in absence from work <3 days	Short term impact on habitat and/or species with restoration time < 1 year	USD 100 000 – USD 1 000 000
Serious	Serious injury or work related illness with absence from work > 3 days	Medium term impact on habitat and/or species and restoration time between 1-3 years	USD 1 000 000 – USD 10 000 000
Major/ catastrophic	>= 1 fatalities	Long term impact on habitat and/or species with restoration time > 3 years	> USD 10 000 000

RISK EVALUATION

Risk associated with the hazardous events can be assessed by integrating the categories for frequencies and consequences into a risk matrix and using risk priority numbers (For further information on risk matrices, see, e.g., (32)). This implies that an acceptable risk level has to be defined. There are different principles for determining acceptable risk of a system, for example, the As Low As Reasonable Practicable (ALARP) principle . For more details, see, e.g., (19).

Risk mitigation can be achieved through:

1. Removal of the risk.
2. Reduction of the risk, e.g., by implementing safety systems addressed by IEC 61508.
3. Provision of sufficient operator protection or operational procedures/warnings.

In the following, phases 1 to 5 in IEC 61508 are applied to define requirements for a safety system for an AUV.

THE IEC61508 LIFE CYCLE APPROACH TO SAFE AUV OPERATIONS

The five first phases of IEC 61508 are: concept, scope definition, hazard and risk analysis, safety requirement and allocation. Hazard and risk analysis was developed in previous section.

CONCEPT

The main objective is to develop an understanding of the EUC (Equipment Under Control), its environment and likely sources of hazards. This means that the design basis for AUV, including the control system, should be available as input. The basic components are presented in Figure 1. The most likely sources of hazards have been presented in Figure 5 and Table 1.

OVERALL SCOPE DEFINITION

The boundaries for the EUC and its control system is all physical equipment on-board the AUV, external data sender/receiver and external positioning system which may be located on-board a following vessel or mounted on a stationary system.

OVERALL SAFETY REQUIREMENTS

To identify the needed risk reductions, a risk and reliability study must be performed. The objective of this study is to produce a safety requirement specification (SRS). An SRS contains all the required safety functions that have to be performed by the safety system. A safety system is derived after a detailed walkthrough of the system and operation. For each safety function, a definition of safety integrity is developed, which defines the probability that a safety system will satisfactorily perform the required safety functions under all the stated conditions within a stated period of time. There are two methods to achieve this: (1) to prevent hazardous events before they occur, or (2) to modify the consequences of a failure caused by the hazardous events.

When the safety integrity for each safety function is defined, this is specified as safety integrity levels (SIL) in the

SRS. A safety system implements the required safety functions to achieve a safe state for the EUC and attains the necessary safety integrity for the required safety functions. The required safety integrity must be such that:

- The frequency of failure of the safety system is sufficiently low to prevent a hazardous event frequency that exceeds what is required to achieve acceptable risk (e.g., a pressure relief system);
- The safety system modifies the consequences of failure to the extent required to meet acceptable risk (e.g., an emergency shutdown system).

The SRS specifies the SILs for the safety system. The methods used to allocate the safety integrity requirements depend on whether the necessary risk reduction is qualitative or quantitative.

Based on the results from the risk identification safety functions and required risk reduction for each determined hazardous event should be defined. The safety functions will in this phase not be defined in technology-specific terms and will most likely be subject to modification in later phases. At this stage it can be assumed that the AUV will need a safety function that can shut down the whole process in case of an emergency and initiate the buoyancy system. It is necessary to have safety functions to handle loss of communication, collision, software failure and environmental impacts. These systems might be E/E/PE systems, mechanical systems or operational procedures and are realized in later phases of the lifecycle. Even though the realization of non-instrumented systems is not covered by IEC 61508, they will contribute to the overall risk reduction and will be part of the overall safety validation.

Table 4. Examples of safety system requirements.

Requirements		**Allocation**		
Overall safety function	Risk reduction require-ment	Safety system	Concept	SIL
Prevent navigation failure	10^{-2}	Redundancy in sensors Activate buoyancy	E/E/PES	3
Prevent propulsion system failure	10^{-2}	Activate buoyancy Early collision warning system Activate emergency GPS when surfaced	E/E/PES	2
Prevent communica tion loss	10^{-3}	Activate buoyancy Activate emergency GPS when surfaced	E/E/PES system	2

For each hazard identified, required risk reduction shall be defined. For example, in the current literature the frequency of mission failure of an AUV is much higher than the general risk acceptance criteria used in the oil and gas industry of $10^{-4.}$ The safety functions must therefore contribute to a substantial risk reduction in the order of magnitude of 10^{4}. However, loss of an AUV does not necessarily cause other serious consequences than economic loss, which means that the risk acceptance criteria may be set lower.

The IEC 61508 standard outlines that the EUC control system may place a demand on the safety systems. This implies that all dangerous failure modes of the control system must be specified and considered when developing the safety requirements. In addition, the control system must be completely independent from the safety systems to ensure that whatever happens to the control system, the safety systems will be able to perform their functions.

OVERALL SAFETY ALLOCATIONS

The main objective of safety requirement allocation is to describe the safety system required to handle the overall safety functions and to suggest system design concepts. In Table 4 some examples are given. Risk reduction levels have been proposed for illustration only since acceptable risk levels has not yet been defined for the autonomous operations in Artic. Depending on the required risk reduction for each safety function, a SIL requirement will be allocated for each system. SILs are separated into four levels depending on the average probability of failure on demand (PFD) to perform its intended function. For safety functions that are normally not activated as part of normal operation (as opposed to, for example, signaling systems in railway applications where each signal change is a safety function), low demand mode of operation can be claimed. In this case, a SIL 1 represents $10^{-1}< \text{PFD} \leq 10^{-2}$, SIL 2 represents $10^{-2}< \text{PFD} \leq 10^{-3}$, etc.

Each safety system shall be independent of other safety systems, to avoid common cause failures. Redundancy can be achieved by physical separation, use of different sensors and technology, etc. Similar requirements are relevant for devices required to perform the same safety function.

The result of the first five phases of the lifecycle shall be summarized into a Safety Requirement Specification (SRS) for each safety system.

DISCUSSION

The main risk to humans in AUV operations in Artic areas are during launch and recovery of the equipment and, in general, detainment in such areas where there is a risk of the vessel getting stuck in ice and/or losing power on-board. Environmental risk is due to drive or drift off which may lead to collision causing damage to subsea equipment and leakage. Material asset cost is related to loss of AUV and inability to recover.

In general, the oil and gas industry has set the risk acceptance criteria to 10^{-4}. This could be a natural approach especially in AUV operations related to inspection,

maintenance and repair of subsea manifolds and equipment. In Arctic areas, additional risks apply which may make it even more challenging to fulfil typical risk acceptance criteria. The Arctic conditions may imply redesign of systems and operations, e.g., related to collision avoidance and ice. Presence of ice may require deep water operations instead of shallow water demanding more complex collision avoidance systems.

Arctic operations with AUV will make risk assessments even more important, but operational procedures should encounter these risks to such an extent so that detailed and cumbersome risk assessments are not necessary for each mission. As more operational experience becomes available, the operating procedures can be updated and risk assessments before a mission becomes more focused.

CONCLUSIONS AND FURTHER WORK

As oil and gas operations move deeper into the ocean and more remote and vulnerable areas, such as the Arctic, and utilize a growing number of subsea installations, autonomous operations will become increasingly important. Currently, AUVs have preprogrammed missions, include an anti-collision system and depend on external communication. The technological development is foreseen to enable fully autonomous vehicles and operations with advanced decision – making systems.

Current AUVs experience low availability and the frequency of mission failure is reported to be high. Operations with ROV and AUVs today are very costly and may cause damage to people and the environment, which means that low risk is required. Better risk assessments are therefore needed during the entire lifecycle of the AUV; to develop more robust AUVs, for example, focusing on endurance and navigation/control systems, and to improve operations, for example, for future interventions.

This paper presents a structured and holistic framework for risk assessments to be used for AUVs focusing on hazardous events related to technical failures, natural events, operator errors and organizational defects. Improved risk assessment will be even more important in the future as the requirements and regulations concerning oil and gas activities in the Arctic are more stringent and the public more concerned about environmental impact. The paper presents typical hazards to be considered for design of AUVs and a taxonomy to be used as a starting point for risk identification in operations. Important to remember is that experience from operation should be fed into redesign and modifications, as well as new developments. Standards that provide guidance and useful information for developing safe and reliable AUVs and operations are described.

With the current lack of quantitative data this paper suggests categories for frequencies and consequences for risk analysis. Further, development of safety systems by use of IEC 61508 is outlined.

Despite the many advantages of AUV operations, it is necessary to further investigate the interaction between operators and the AUVs and possible impact on safety. Also, more data on failures should be systematically collected to enable more detailed information about risk.

ACKNOWLEDGMENTS

This work was supported by the Research Council of Norway through the Centre of Excellence funding scheme, project number 223254 AMOS.

REFERENCES

(1) Anda, I. 2012. Letter demanding improvements in Norwegian). In "Sikkerhet, status og signaler» 2011-2012. Petroleum Safety Authority Norway, http://www.ptil.no/getfile.php/PDF/SSS%202012/Sikkerhet%20%20status%20og%20signaler2012_No._pdf.pdf (Accessed: Jan. 2014).

(2) Gudmestad, O.T., Quale, C. 2011. Technology and operational challenges for the High North. Report IRIS – 2011/166.

(3) Griffits, G., Brito, M. 2008. Predicting risk in missions under sea ice with autonomous underwater vehicles. IEEE

(4) Brito, P.B., Griffiths, G., Challenor, P. 2010. Risk analysis for autonomous underwater vehicle operations in extreme environments. Risk Analysis, 30(12), 1771-1788.

(5) Griffiths, G., Brito, M.P. 2011. Risk management for autonomous underwater vehicles operating under ice. OTC 22162. Offshore Technology Conference, Houston, USA.

(6) Brito, M., Griffiths, G., Ferguson, J., Hopkin, D., Mills, R., Pederson, R. MacNeil, E. 2012. A behavioural probabilistic risk assessment framework for managing autonomous underwater vehicle deployments. American Meteorological Society, 1689-1703.

(7) Pereira, A.A., Binney, J., Jones, B.H., Ragan, M., Sukhatme, G.S. 2011. Toward risk aware mission planning for autonomous underwater vehicles. IEEE/RJS International Conference on Intelligent Robots and Systems, San Francisco, California, USA.

(8) Pereira, A.A., Binney, J., Hollinger, G.A., Sukhatme, G.S. 2013. Risk-aware path planning for autonomous underwater vehicles using predictive ocean models. Journal of Field Robotics, 30(5), 741-762.

(9) Manley, J.E. 2007. The role of risk in auv development and deployment. In OCEANS, IEEE.

(10) McLeod, D. 2010.Emerging Capabilities for Autonomous Inspection Repair and Maintenance OCEANS, IEEE.

(11) Rothgeb, M. 2007. Intelligent autonomy for reducing operator workload. Intelligent Control Systems Department, Autonomous Control and Intelligent Systems Division, http://engineering.tamu.edu/media/699818/intelligent_autonomy_2007.pdf (Accessed: 13.11.2013).

(12) Lundteigen, M., Rausand, M., Utne, I.B. 2009. Integrating RAMS engineering and management with the safety life cycle of IEC 61508. Reliability Engineering and System Safety, 94, 1894-1903.

(13) ISO 31000. 2009. Risk management.

(14) ISO 31010. 2009. Risk management – Risk assessment techniques.
(15) IEC 60300. 2013. Dependability management.
(16) Rausand, M., Utne, I.B. 2009. Risk analysis. Theory and methods (in Norwegian: Risikoanalyse. Teori og metoder). Tapir Akademisk Forlag, Trondheim, Norway.
(17) IEC 61508. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1-5.
(18) NORSOK U-102. 2012. Remotely operated vehicle (ROV) services.
(19) NORSOK z-013. 2010. Risk and emergency preparedness assessment.
(20) Leveson, N. 2011. Engineering a Safer World. Systems Thinking Applied to Safety, MIT Press, Ma, U.S.A.
(21) Utne, I.B. 2006. Systems engineering principles in fisheries management. Marine Policy, 30, 624-634.
(22) Blanchard, B., Fabrycky, W. 1998. System engineering and analysis, Pearson Prentice Hall.
(23) Kobbacy, K.A.H., Murthy, D.N.P. 2008, An overview, in Kobbacy, K.A.H. (Ed.), Complex System Maintenance Handbook, Springer Series in Reliability Engineering, Springer, Berlin.
(24) Utne, I.B. 2010. Maintenance strategies for deep sea offshore wind turbines. Journal of Quality in Maintenance Engineering, 16 (4), 367-381.
(25) The International Marine Contractors Association (IMCA). 2009. Code of Practice for The Safe and Efficient Operation of Remotely Operated Vehicles. (Accessed: http://www.imca-int.com/media/72417/imcar004.pdf Dec. 22nd 2013)
[26] ISO 17776. 2000. Petroleum- and natural gas industry. Production installations, hazard identification and risk assessment.
(27) Thieme, C. 2013. Project thesis, Department of Marine Technology, NTNU, Trondheim, Norway.
(28) Griffiths, G., Millard, N.W., McPhail, S.D., Stevenson, P. and Challenor, P.G. 2003. On the reliability of the Autosub autonomous underwater vehicle. Underwater Technology: International Journal of the Society for Underwater Technology, 25, (4), 175-184.
(29) Brito, M.P., Griffiths, G. 2009. Results of expert judgments on the faults and risks with Autosub3 and an analysis of its campaign to Pine Island Bay, Antarctica, 2009. In, Proceedings of the International Symposium on Unmanned Untethered Submersible Technology (UUST 2009), Durham, New Hampshire.
(30) Brito, M., Griffiths, G., A Markov chain state transition approach to establishing critical phases for auv reliability. IEEE Journal of Oceanic Engineering, 36 (1) 139-149.
(31) Xu, H., Li, G. Liu, J. 2013. Reliability analysis of an autonomous underwater vehicle using fault tree. Proceeding of the IEEE International conference on information and automation, China, 2013.
(32) Rausand, M. 2011. Risk assessment. Theory, methods, and applications. Wiley, Hobroken, U.S.A.

