Proceedings of the ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering
OMAE2017
June 25-30, 2017, Trondheim, Norway

OMAE2017-61645

RISK MANAGEMENT OF AUTONOMOUS MARINE SYSTEMS AND OPERATIONS

Ingrid Bouwer Utne
Centre for Autonomous Marine Operations and Systems (NTNU AMOS)
Department of Marine Technology
Norwegian University of Science and Technology (NTNU)
7491 Trondheim, Norway

Asgeir J. Sørensen
Centre for Autonomous Marine Operations and Systems (NTNU AMOS)
Department of Marine Technology
Norwegian University of Science and Technology (NTNU)
7491 Trondheim, Norway

Ingrid Schjølberg
Centre for Autonomous Marine Operations and Systems (NTNU AMOS)
Department of Marine Technology
Norwegian University of Science and Technology (NTNU)
7491 Trondheim, Norway

ABSTRACT

Autonomous systems may lead to smarter and more efficient operations, but emerging risks are involved, because of lack of knowledge and operational experience with such systems, and challenges related to verification of safe performance. The objective of this paper is to clarify, categorize, and classify risk related to autonomous marine systems, and establish a foundation for risk management of such systems. Autonomous systems are usually associated with unmanned systems, but several manned systems, e.g., offshore oil and gas rigs and ships with complex automation and dynamic positioning (DP) systems, have certain control functionality that may be characterized as autonomous. Therefore, this paper addresses both manned and unmanned systems with different levels of autonomy. This means that the concept of autonomy in this paper includes a range of systems and operations with increasing complexity and major hazard potential, even though autonomous ships are used to exemplify. Hence, the paper addresses a broader approach in contrast to the traditional focus on robotics.

INTRODUCTION

The technological advances in automation and autonomous systems enable new and challenging marine and maritime processes, missions and exploration of areas [1]. An increased level of automation and autonomy in tedious operations may improve safety, efficiency, and performance, supporting the human operator in decision-making and supervision, and reducing human workload [2]. A motivation for autonomous ships is reduced building and operational costs as the ships can be completely redesigned. Research projects, such as MUNIN [3] and Advanced Autonomous Waterborne Applications (AAWA) [4], work with development of technological specifications and designs for autonomous ships.

Advanced control systems with autonomy functions may cause complexity and interlocks that are hard to identify and analyze. New types of failure modes may be introduced, due to unforeseen interdependencies in the system design, operation complexity, and environmental challenges. For systems, such as an advanced ship, a subsea production facility [5-7] or an offshore fish farm [8], shutting down and remobilizing the operation due to hazards caused by automatic or autonomous systems, including false alarms are not feasible. Therefore, to achieve a high system integrity, the autonomous systems must be able to identify and isolate failures and reconfigure to handle any deviations from normal operation, which is a challenge in the ocean space. The reconfiguration capability is dependent on the type of operation, system and/or control function redundancy, risk influencing factors (RIFs), and the risk level of the phase of operation.

The use of autonomous systems must rely on proper industry standards, certification and classification regimes. Hence, it is essential to develop a foundation for characterising autonomy levels, risk acceptance criteria, and testing and

verification methods subject to associated risk. For the society, it is of uttermost importance to ensure that the autonomous systems and operations are safe. Risk management should become a driver in the design and operation of these highly automated intelligent systems. The autonomous system must be able to determine if it can continue with possible degraded performance by detecting, isolating and handling failures and faults [9]. The systems must assess the level of tolerable risk by improving situational awareness capabilities, and in short; carry out decisions based on perception, comprehension and projection of the future situation that we today leave to a human operator.

The objective of this paper is to clarify, categorize, and classify risk related to autonomous marine systems, and establish a foundation for risk management and risk control that specifically entails these system's risk features. Currently, such a foundation does not exist that addresses the characteristics of systems with various autonomy functions. The paper creates a basis for developing safety requirements to autonomous systems and operations, and for implementation of dynamic risk monitoring and risk control through built-in intelligent functionality.

[10-14] address the need for safer autonomous systems and operations, such as unmanned aerial vehicles (UAVs). [15] discuss challenges with unmanned ships. [16-18] present risk and reliability issues related to autonomous underwater vehicles (AUVs). [19] address path planning and the risk of collision for AUVs. [20] focus on collision risk indicators for autonomous subsea intervention. [21] develop a method for safety performance monitoring of autonomous marine systems. In this paper, we focus on risk management and risk control related to a wide range of autonomous marine systems, including manned systems, exemplified for autonomous ships.

IMPORTANT CONCEPTS

Several manned systems, e.g., offshore oil and gas rigs and ships with complex automation and dynamic positioning (DP) systems, have certain control functionality that may be characterized as autonomous. Normally, autonomous systems and operations are associated with unmanned systems, and thus it is important to distinguish between unmanned systems and autonomy.

The National Institute of Standards and [22], defines unmanned systems as a powered physical system, with no human operator aboard the principal components. It acts in the physical world for achieving assigned tasks. It may be mobile or stationary and can include any and all associated supporting components. Examples are UAV, unmanned ground vehicles (UGV), unmanned underwater vehicles (UUV), unmanned water surface borne vehicles (USV), and unattended sensors (US).

Autonomy can be defined as a system's or sub-system's own ability of integrated sensing, perceiving, analyzing, communicating, planning, decision-making, and acting, to achieve its goals as assigned by its human operator(s) through designed human-machine interface (HMI). This definition is based on [22], but adjusted for autonomous systems and operations, both manned and unmanned. This means that unmanned systems is a "sub category" of autonomous systems.

Autonomy levels (Table 1) can be defined as a set of metrics that describe detailed aspects of an autonomous system

Table 1. Levels of autonomous systems and operations.

Autonomy level	Type of operation	System description	Overall risk aspects
1	Automatic operation (Remote control)	The system operates automatically. The human operator directs and controls all high-level mission planning functions, often preprogrammed. System states, environmental conditions and sensor data are presented to the operator through a human-machine-interface (HMI) (human-in-the-loop/human operated).	Operator experience, procedures and training are essential.
2	Management by consent	The system automatically makes recommendations for mission or process actions related to specific functions, and the system prompts the human operator at important points in time for information or decisions. At this level the system may have limited communication bandwidth, including time delay, due to, e.g., distance. The system can perform many functions independently of human control when delegated to do so (human-delegated).	The human machine interface (HMI) is increasingly important. Software and the control system software, including anti-collision sensors, constitute an increasing risk with higher autonomy levels.
3	Semi-autonomous operation or management by exception	The system automatically executes mission-related functions when response times are too short for human intervention. The human may override or change parameters and cancel or redirect actions within defined time lines. The operator´s attention is only brought to exceptions for certain decisions (human-supervisory control).	Risk is highly dependent on the situation awareness capabilities of the system and operator. The risk related to an erroneous operator action may be lower, but a challenge is related to boredom for the human operator and unforeseen incidents the system is not designed for.
4	Highly autonomous operation	The system automatically executes mission or process related functions in an unstructured environment with ability to plan and re-plan the mission or process. The human may be informed about the progress. The system is independent and "intelligent" (human-out-of-the loop).	Risk reduction is completely dependent on a robust and resilient design of the system, but also on an online risk management system. Efficient and high integrity machine learning and adaptive functionality are very important.

and operation, including operator dependency, communication structure, human-machine interface (HMI), a dynamic or online risk management system, intelligence, planning functionalities and mission complexity. For most complex systems, for example, ships, the advancement is not from fully manned and manual operation to fully unmanned and highly autonomous operation; rather there is a gradual transition towards higher levels of autonomy. A future ferry may, for instance, not necessarily remove manning due to passenger safety, but operations, including docking and set sail, may become more autonomous. This could improve health, safety and environment (HSE). On the other hand, in an operational environment with a combination of manned and unmanned autonomous systems, the risk may increase since the human behavior represents an uncertainty that the unmanned system should cope with and vice versa. Hence, systems may have different levels of autonomy, depending on their functionality, risk acceptance criteria, and the different autonomy levels' impact on risk.

Table 1 contains four levels of autonomy (LoA), including overall risk aspects that are important for risk management. According to [23], there is no "correct" taxonomy; rather it should be selected and adapted to the specific problem at hand. [24] presents four and ten levels of autonomy, whereas, for example, [25] has proposed six levels of autonomy. In this paper, the term *autonomous system* is used for systems that may have functionality in one or several of the categories in Table 1. The four levels in the Table are rather coarse, but sufficient to illustrate the main challenges related to risk of autonomous systems. For more detailed analysis in the future, further sub-division will be necessary.

DEFINING RISK FOR AUTONOMOUS MARINE SYSTEMS AND OPERATIONS

The most common definition of risk focuses on a specific hazardous or undesired event e_i, its various causes and possible consequences c_i, which are associated with probabilities p_i. i is used as an index to capture all relevant events. Thus, the risk related to an activity can be represented by the triplet [26]:

$$\{e_i, p_i, c_i,\} \quad (1)$$

According to [27], the probabilities for two different events could be the same, but the strength of knowledge used to establish the probabilities could be completely different. This means that for new technologies, the strength of knowledge may be low and the uncertainties high. [28] presents a risk perspective consisting of (i) probability – based thinking, (ii) the knowledge dimension, and (iii) surprises ("black swans"). Based on this perspective, risk can be defined by:

$$\{a_i, c_i, q\}|k \quad (2)$$

where a is a hazardous event, c is the consequence(s) of a, q is a measure of uncertainty, and k is the background knowledge used for determining a, c and q [29]. Hence, uncertainty is the main constituent part of risk rather than the probability only. This means that risk becomes a subjective measure to be quantified in terms of, for example, Bayesian models instead of an objective risk metric.

Risk analysis in this perspective is performed by identifying a set of events a' and consequences c'. Probabilities p can be used as a tool for expressing uncertainties, but it cannot always describe all uncertainties in assumptions and background knowledge, accurately. Probability is seen as one of several tools for describing uncertainty, and risk should not be limited to this tool, only [27]. Hence, q is applied rather than p, to open for various quantitative and qualitative ways of expressing uncertainties [30]. For autonomous systems operating in an unstructured environment, with little or no a-priori information q may be assumed to be high and k low.

Black swans [31] are outliers or hazardous events with extreme consequences that could not be expected due to our experience. The notion of black swans has been much debated in the risk community, but it has relevance for automated and complex systems, for which it is very challenging to analyze all possible accident scenarios. Uncertainty needs to be acknowledged and reduced by improving our knowledge basis. This implies a risk perspective for autonomous systems and operations in line with (2), rather than (1).

The complexity of autonomous systems and operations is highly related to uncertainty. The more complex a system and operation is, the more difficult it is to gain "perfect" knowledge of it. Complexity is related to the mission or the operation, the operating environment, and the system itself. The complexity of the system itself may be characterized by the number of input-output (I/O) channels, sensors, actuators, diversity of components, and functionality, such as embedded software, communication networks, couplings, system dynamics and operation in unstructured environments, and distributed decisions. [32] defines complexity of a system as: "characterized by our ability to predict the change Δy of the output caused by a specified change Δx of the input. If we, without any uncertainty, can predict the change Δy, the system is said to be linear. In the opposite case, the system is said to be complex. The degree of complexity increases with the uncertainty about the value of Δy".

To measure complexity of systems is not a simple task. The risk of a certain technological system may be known, but the interactions between these risks and other types of risks or activities could cause unexpected nonlinear and stochastic effects. Systems with embedded software and large degree of functional integration are complex, because physical separation and segregation of components, such as redundancy in ship machinery systems, may be overruled by software and control systems that operate across physical boundaries and separated systems.

The complexity of autonomous systems and operations needs to be assessed related to the specific operating context and autonomy level. In general, autonomous systems are exposed to mission or operation complexity, environmental complexity, and system complexity [33], as shown in Table 2. The three categories are interrelated with characteristics relevant for risk

Table 2. Categorization and description of types of complexity characteristics for autonomous systems and operations. Adapted from [33].

Category	Description	Complexity characteristics
Mission/ operation complexity	Mission or process complexity is related to the utilization of the system and how the system interacts with its surroundings. For example, oil and gas production has higher process complexity, than survey operations with an AUV or maritime transport with a container ship.	- Subtasks (e.g., path planning, navigation, manipulation) - Organization, collaboration, communication - Sensing and perception (situation awareness) - Duration of mission
Environmental complexity	For more complex missions or processes, the environmental complexity increases, as the number and types of interactions the system has with the surroundings can be expected to increase. Environmental complexity means that the operating surroundings are characterized by challenging communication constraints, weather issues or terrain/seabed characteristics. Subsea oil and gas production has lower environmental complexity than production on an offshore platform.	- Variability - Terrain variation - Object frequency, density, intent - Weather - Sea states - Mobility constraints - Communication dependencies, coverage areas
System complexity	This category can be considered a combination of the structural and dynamic complexity categories of [34]. The requirements to functionality of the system determines system complexity and characteristics, such as internal interactions, topology, number of components and IO/channels, and system states.	- Hardware and software (degradation, interfaces, security, energy) - Physical and functional integration - Redundancy - Frequency, robot initiated interactions - Operator workload, skill levels - Operator to unmanned system ratio

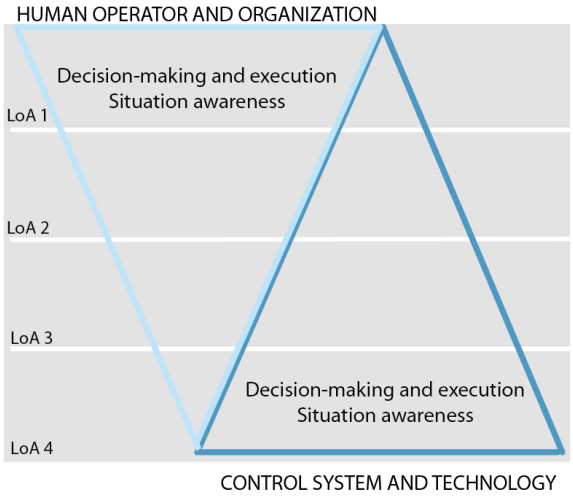
management. Hence, Table 2 may provide input to identification of hazards and RIFs, e.g., for risk assessment and modeling. Higher mission complexity may be due to higher environmental complexity, which again leads to more demanding system requirements and specifications (system complexity). This again may lead to a need for implementing a higher level of autonomy. This means that system complexity may increase to be able to handle the mission and environmental complexities.

RISK MANAGEMENT AND RISK CONTROL

Risk management is fundamental in decision-making processes, and is key to safe and cost-efficient design and operation of complex systems [35] Risk management is constituted by risk assessment, monitoring, control, and follow-up of risk [32, 36]. Risk control can be defined as a measure modifying risk [36].

Obviously, small, fully autonomous UAVs will not be associated with the same uncertainties, complexities, and risks as autonomous ships. Risk management of autonomous systems is not a simple task, because it needs to capture the dynamic and complex aspects of such a variety of systems, as well as uncertainties related to lack of knowledge from operational experience. Risk control related to autonomous systems can occur in two different, but complementary ways, depending on a system's autonomy level: (i) Risk control of the autonomous system performed by the human operator(s), which is mostly relevant for low levels of autonomy; (ii) Risk control performed by the autonomous system itself, which is increasingly important in the higher levels of autonomy. This is illustrated in Fig. 1, where the decision-making capabilities gradually is transferred from the human operator to the system itself with higher levels of autonomy. Risk management for autonomous marine systems has to take this aspect into account, as well as the two main life cycle phases of system. This is presented in Fig. 2 and further discussed and exemplified for an autonomous ship in the subsequent sections.

Fig. 1. The higher level of autonomy (LoA), the more of the decision-making and situation awareness functionality is transferred from the human operator to the autonomous system.



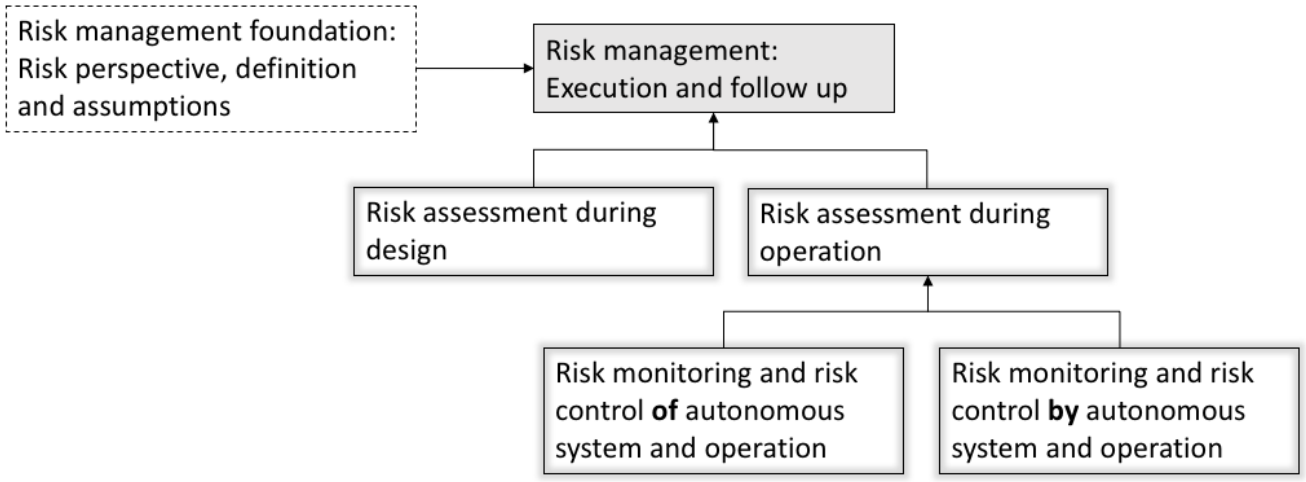


Fig. 2. Risk management of autonomous marine systems.

Risk assessment during design

Risk assessments should be carried out both during the design and operation of a system. For autonomous systems with embedded software solutions, upgrades may easily take place for bug fixes and improved functionalities. This should also trigger adequate testing and verification before the system is put into operation again to reveal any complex dependencies and malfunctions. During operation, risk can be assessed and controlled by the operator and/or by the autonomous system; the extent determined by the system´s level of autonomy.

Testing and verification of the systems are increasingly important for autonomous systems. Verification could lead to design improvements and risk reduction. A control system, such as a dynamic positioning system (DP)-system, may be more complex than any mechanical system onboard a ship. Without sufficient testing, such functionality may have dangerous hidden failures threatening the integrity of the system. In addition, the control system may interfere with several other systems which means that failure in one part of the system may cascade to other parts of the system.

A typical starting point in risk analysis is to identify what can go wrong, and describe a large number of such scenarios, even those that initially may be considered extremely unlikely. Brainstorming and checklists are often used, including human error, equipment malfunctions, extreme weather conditions, malicious acts, etc. The challenge is that it is impossible to foresee everything that may occur, and there are unknown unknowns or "black swans" [37-39]. For emerging risks, very little experience may exist.

The knowledge aspect k of the uncertainty dimension q can be represented by a semi-quantitative scale for assessing the strength of knowledge for the risk assessment, considering assumptions, data quality and information available [40]. For risk analysis of autonomous systems, such a knowledge scale is very much dependent on data quality, application area, level of autonomy (cf. Table 1), system complexity (cf. Table 2), and whether the technology is novel or widely used and proven (technological readiness).

*Risk monitoring and risk control **of** autonomous ships*

Risk related to an autonomous ship is constituted by hazardous events, such as degradation of power, collisions with obstacles in the ocean, and the presence of ice in case of Arctic operations, and RIFs, such as severe sea currents, weather conditions, and the quality of sensors and communication system. According to [32], RIFs are enduring conditions that impact barrier performance and the probability of hazardous events.

Current experience shows that there is a wide range of circumstances in which, e.g., communication links can be disturbed or broken. Autonomous ships may also be used as part of complex simultaneous operations. Collisions, including grounding, may threaten the integrity of the systems. An autonomous ship colliding with an offshore fish net cage may in worst-case lead to fish escape, which can be characterized as a major accident [8].

A challenge related to autonomous ship operation is the lack of precise information of the ocean environment and unpredicted situations may occur and require operator control. There are also constraints related to navigation, communication and positioning in the oceans. The simple interaction and supervision with a remotely situated human operator may take place over radio and satellite communication link with varying bandwidth capacity. The current limitations in communication between an operator and the autonomous ship create some challenges with respect to online risk monitoring during operation, but future technological development is expected to reduce this problem.

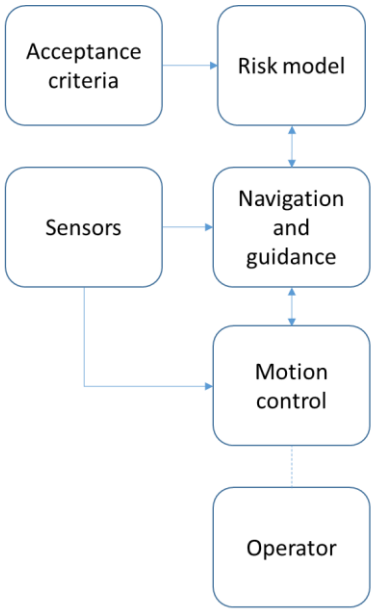


Fig. 3. The risk monitoring and control concept for an autonomous ship.

An important part of the risk monitoring and risk control of the autonomous system is related to the planning of the operation. [20] has developed collision risk indicators for autonomous remotely operated subsea vehicles. These indicators can be used to simulate a path and evaluate the associated risk. Hence, the operator may be informed in advance of specific locations along the path where he or she should be on alert in particular, or take over operation and maneuvering of the ship. An alternative outcome of such a simulation is to select another path.

Fig. 3 shows an online risk control concept for an autonomous ship. The on-line risk model utilizes data from different sources, such as historical data, measurements from sensors, and experience data, including information about the weather. The data models may vary from empirical models based on historical or online data to physics-based models.

An important part is visualization, human – machine interface (HMI) and organizational aspects. To visualize the risk to the human operator, indicators may be needed. Indicators can be monitored online or real-time during operation, or they may be sampled on a regular basis, independent of a specific mission. The former is most relevant for online risk assessment. In general, trending of indicators may contribute to more knowledge and information about a system and/or operation, reducing the uncertainty (k) in risk assessments, and providing useful input into the design and development of such systems.

[21] suggest a method for developing indicators for autonomous marine systems; and propose some indicators for AUVs. An example of a safety indicator for AUV operation can be *Percentage of anticipated status messages received from the AUV*, which is also relevant for risk monitoring of autonomous ships.

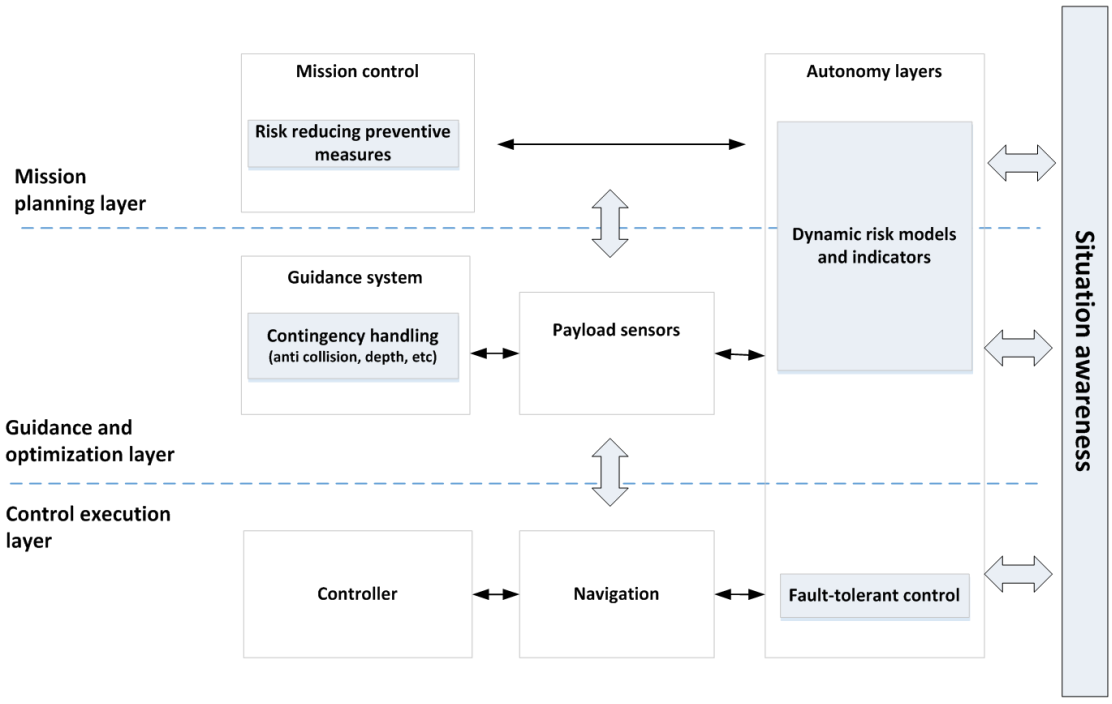


Fig. 4. System architecture for autonomous systems combining reactive and deliberative control, illustrating the steps from control execution level at the lowest level to mission planning at the highest level.

*Risk monitoring and risk control **by** the autonomous ship*

Autonomous ships will have functionality in autonomy level 2 - 3 (cf. Table 1). This means that the online risk control functionality should be implemented in the control system of the autonomous system to improve its decision-making abilities. This is shown in Fig. 4, which illustrates the general control system architecture of an autonomous system, further adapted from [41]. It is divided into three main layers; the control execution layer (the reactive control layer), the guidance and optimization layer, and the mission layer (the deliberate control layer).

In the mission planner level, the mission objective is defined and planned (and possibly re-planned). In the guidance and optimization level, the waypoints and reference commands to the controller are handled. Optimized model-predictive control (MPC) may also be used accounting for varying references and forecasted variations in environmental and operational conditions. In the control execution level, the plant control and actuator control occur at the highest bandwidth.

The autonomy layers' box to the right in Fig. 4 contains functionality, depending on a system's level of autonomy, which transgresses the three architectural layers. The autonomy layers in this Figure reflects the layers and the functionality shown in Fig. 4. The blue boxes in Fig. 4 represent online risk control and shows how it should be embedded in the different layers. This means that the system architecture of future autonomous systems should include capabilities related to sensing and perception of risk (SA) to evaluation, control and follow up. Contingency handling covers basic safety functions, such as anti-collision and depth control. In addition, risk control in terms of monitoring is performed by the human operator.

Intelligent behaviors of autonomous systems are decision-making, mission planning and re-planning, and fault tolerance [42]. Fault-tolerant control is an important feature of many engineered systems. It enables a system to accommodate the effect of faults [43, 9]. In general, fault-tolerant control consists of two steps: (i) detection and diagnosis of the fault; and (ii) control re-designs [9]. This field is mainly focused on reducing the consequences of internal faults, and offers methods for diagnosing whether a behavior is normal or not at levels where information is metric, whereas the risk control concept is more proactive and systemic, working to prevent failures related to

Table 3. Examples of risk influencing factors (RIFs) and hazardous events impacting the collision risk of autonomous ships. Based on complexity characteristics in Table 2, existing risk models [45-46] and ongoing research work.

Risk influencing factors (RIFs) and hazardous events		**Data available (sensor/estimate)?**	**Proactive risk management**	**Contingency handling – anti collision**	**Fault tolerant control**
Mission/operation	Path length	X	X		
	Voyage planning		X		
	Human fatigue		X		
	Human absence from control room		X		
	Human operator intoxication		X		
	Vessel or obstacle not detected		X		
	Failure of ship initiated recovery		X	X	
Environment	Number of vessels traveling in route	X	X	X	X
	Shielding	X	X	X	X
	Wave height	X	X	X	X
	Sea current/vessel drift	X	X	X	
	Wind speed	X	X	X	X
	Weather forecast		X		
	Vessel speed	X	X	X	X
System	Vessel age		X		
	Flag state		X		
	Loss of steering	X	X	X	X
	Remaining power capacity	X	X	X	X
	Navigation equipment error or failure	X	X	X	X
	Communication equipment error or failure	X	X	X	X
	Power/propulsion error or failure	X	X	X	X
	Human operator training and experience		X		

both human and technical errors. Often, hindsight has shown that if signals or early warnings had been detected and managed in advance, the undesired event could have been prevented [44]. The difference between the online risk monitoring functionality and the contingency handling feature in Fig. 4 is that the risk monitoring is based on an online risk model, which considers all relevant risk aspects to proactively avoid the need for activating any contingency system.

Using collision risk as an example, we may have different collision scenarios for an autonomous ship, such as maneuvering collision and drifting collision. Different risk models can be developed for the scenarios. The risk modelling, e.g., using Bayesian networks, has to take features of the autonomous ship into consideration, including energy storage and capacity, path length, speed of vehicle, location, operational aspects, environmental conditions (wind, waves, current). RIFs are, for example, traffic density, path characteristics, visibility, sea temperature, vehicle characteristics, battery management, the technical condition of vehicle, its position, and detection capability. Hazardous events may be technical failures or human supervision errors. Table 3 shows that some of these RIFs and hazardous events can be measured by sensors mounted on the autonomous ship or estimated, whereas others are predetermined by the vessel itself and the operation. Table 3 includes a selected number of RIFs and hazardous events based on the complexity characteristics in Table 2, existing collision risk models [45-46] and ongoing research work. The Table shows that some of the information that is needed to calculate collision risk is readily available today from sensor measurements or can be estimated, whereas other types of information need to be established from historical data, expert judgments, considering uncertainty. The Table also shows that proactive risk management encompasses a lot more information than contingency handling and fault tolerant control. Still, contingency handling and fault tolerant control can be considered parts of risk management.

The factors' quantitative impact on risk can be calculated from conditional probability tables (CPT) and Bayes' theorem (for more on BN, see, e.g., [32]), and the risk model can be updated "continuously" as a dynamic BN.

DISCUSSION AND CONCLUSIONS

The presented foundation for risk management is exemplified for an autonomous ship, but it is relevant for different stakeholders of both manned and unmanned systems. Producers of autonomous marine systems need to develop an overall strategy for requirements to safety and reliability ensuring that the systems fulfill the requirements. Authorities have to be more proactive when it comes to regulating and follow up of this kind of technology. This does not apply to autonomous marine systems only, but also other types of systems, such as UAVs. The whole life cycle of the system needs to be focused on with respect to risk, and data and information have to be collected systematically and used for risk information and implementation of sufficient risk reducing measures. Too often, safe performance is seen as important too late in the design and development process, when too many system constraints are already determined.

The risk perspective suggested for autonomous marine systems emphasizes uncertainties and knowledge/lack of knowledge characterizations, rather than a purely probability based (objective) risk definition. It is expected that by focusing on the knowledge and uncertainty aspect, risk can be integrated more easily along with the other disciplines from the initial start of development. The autonomy levels and risk aspects in Table 1 along with the complexity characteristics in Table 2 provide basis for design constraints for the system. Higher autonomy levels imply that decision-making and situation awareness capabilities are transferred from the human operator to the system itself, which impacts the risk spectrum.

Testing and verification of autonomous systems with increased intelligence and the ability to learn will be even more challenging, because it is harder to predict and simulate everything that may occur and how they will behave in every situation.

Risk models that can provide online decision support subject to environmental and operational conditions and limitations, failure scenarios, consequence classes, both proactively and reactively, for safer operation are needed. Proactively means early warnings on possible violations of the operating envelope. Reactively means that human operators are given more time for efficient responses and enhanced crisis intervention by providing predictions of possible outcomes. Autonomous marine systems may provide input data to online risk models for larger operations. However, online risk modeling should also be developed as an integral part of more intelligent autonomous systems. Such risk models have not yet been developed.

ACKNOWLEDGMENTS

This work has been carried out at the Centre for Autonomous Marine Operations and Systems (AMOS). The Norwegian Research Council is acknowledged as the main sponsor of NTNU AMOS through the Centres of Excellence funding scheme, Project number 223254. We appreciate the comments by two anonymous reviewers to an earlier version of this paper.

REFERENCES

[1] Norwegian Research Council (NRC), 2016, "Maritime 21. A holistic maritime strategy for research, development and innovation" (Report in Norwegian).

[2] Department of Defense (DoD), 2011, "Unmanned systems integrated roadmap FY2011-2036", Reference number: 11-S-3613.

[3] Rødseth, Ø.J., Tjora, Å., 2014. "A risk based approach to the design of unmanned ship control systems". In: Maritime-Port Technology and Development – Ehlers et al. (Eds), Taylor & Francis Group, London.

[4] Advanced Autonomous Waterborne Applications (AAWA), 2016, "Remote and autonomous ships. The next steps", Position paper. http://www.rolls-royce.com/~/media/Files/R/Rolls-

Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf (Accessed: 2017-02-14).
[5] Sørensen, A. J., Ådnanes, A.K., 2005, "Reconfigurable Marine Control Systems and Electrical Propulsion Systems for Ships". ASNE Reconfiguration and Survivability Symposium, February 16-18 (RS 2005), Florida, USA.
[6] Schjølberg, I., Utne, I.B., 2015. Towards Autonomy in ROV operations., in: International Federation of Automatic Control, Navigation, Guidance and Control of Underwater Vehicles (Girona, Spain), 28 (2), pp. 183-188.
[7] Schjølberg, I., Gjersvik, T. B., Transeth, A. A., Utne, I. B., 2016, "Next Generation Subsea Inspection, Maintenance and Repair Operations", in: International Federation of Automatic Control, 49 (23), pp. 434-439.
[8] Utne, I. B., Schjølberg, I., Holmen, I. M., 2015, "Reducing risk in aquaculture by implementing autonomous systems and integrated operations". Proc. (Safety and Reliability of Complex Engineered Systems) of the 25th European Safety and Reliability Conference, ESREL, Zurich, Switzerland.
[9] Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M., 2015, Diagnosis and fault tolerant control. Springer, 3rd edition.
[10] Clothier, R. A., Greer, D. A., Greer, D. G., Mehta, A. M., 2015, "Risk perception and the public acceptance of drones", Risk analysis, 35(6), pp. 1167-1183.
[11] Clarke, R., 2014a, "Understanding the drone epidemic", Computer Law and security review, 30, pp. 230-246.
[12] Clarke, R., 2014b, "What drones inherit from their ancestors", Computer Law and security review, 30, pp. 247-262.
[13] Clarke, R., 2014c, "The regulation of civilian drones' impacts on behavioural privacy", Computer Law and security review, 30, pp. 286-305.
[14] Clarke, R., Moses, L. B., 2014, "The regulation of civilian drones' impacts on public safety". Computer Law and security review, 30, pp. 263-285.
[15] Remenyte-Prescott, R., Andrews, J. D., Chung, P. W .H., 2010, "An efficient phased mission reliability analysis for autonomous systems", Reliability Engineering and System Safety, 95, pp. 226-235.
[16] Brito, M. P., Griffiths, G., Challenor, P., 2010. "Risk analysis for autonomous underwater vehicle operations in extreme environments", Risk analysis, 30 (12), pp. 1771-88.
[17] Brito M., Griffiths, G., Ferguson, J., Hopkin, D., Mills, R., Pederson, R., MacNeil, E., 2012, "A Behavioral Probabilistic Risk Assessment Framework for Managing Autonomous Underwater Vehicle Deployments", Journal of Atmospheric and Oceanic Technology, 29, pp. 1689–1703.
[18] Brito M., Griffiths, G., 2016, "A Bayesian approach for predicting risk of autonomous underwater vehicle loss during their missions", Reliability Engineering and System Safety, 146, pp. 55-67.
[19] Lefebvre, N., Schjølberg, I., Utne, I. B., 2016, "Integration of Risk in Hierarchical Path Planning of Underwater Vehicles2, IFAC-PapersOnLine vol. 49(23), pp. 226-31.
[20] Hegde, J., Utne, I. B., Schjølberg, I., 2016, "Development of collision risk indicators for autonomous subsea inspection, maintenance and repair", Journal of Loss Prevention in the Process Industries, 44, pp. 440-452.
[21] Thieme, C., Utne, I. B., 2017, "Safety performance monitoring of autonomous marine systems", Reliability Engineering and System Safety, 159, pp. 264-275.
[22] National Institute of Standards and Technology (NIST), 2008, "Autonomy levels for unmanned systems (ALFUS) Framework", Volume I: Terminology, version 2.0, NIST Special Publication 1011-I-2.0.
[23] Vagia, M., Transeth, A. A., Fjerdingen, S. A., 2016, "A literature review on the levels of automation during the years. What are the different taxonomies that have been proposed?" Applied Ergonomics, 53, Part A, pp. 190–202.
[24] National Research Council (NRC), 2005, "Autonomous Vehicles in Support of Naval Operations, Committee on Autonomous Vehicles in Support of Naval Operations, US", ISBN: 0-309-55115-3.
[25] Lloyd's Register, 2016, "Cyber-Enabled Ships. ShipRight Procedure – Autonomous Ships", Report. First edition, July 2016
[26] Kaplan, S., Garrick, B. J., 1981, "On the quantitative definition of risk", Risk Analysis, 1(1), pp. 11-27.
[27] Aven, T., Krohn, B. S., 2014, "A new perspective on how to understand, assess and manage risk and the unforeseen", Reliability Engineering and System Safety, 121, pp. 1-10.
[28] Aven, T. 2013. Practical implications of the new risk perspectives. Reliability Engineering and System Safety, 115 (136-145).
[29] Khorsandi, J., Aven, T. 2014. A risk perspective supporting organizational efforts for achieving high reliability. Journal of Risk Research, 17(7), 871-884.
[30] Aven, T., Zio, E., 2011, "Some considerations on the treatment of uncertainties in risk assessment for practical decision making", Reliability Engineering and System Safety, 96, pp. 64-74.
[31] Taleb, N. N., 2007, The black swan. The impact of the highly improbable. Random House.
[32] Rausand, M., 2011, Risk assessment. Theory, methods, and applications. Wiley, Hobroken, USA.
[33] Huang, H-M., Messina, E., Jacoff, A., 2010, "Performance measures framework for unmanned systems (PerMFUS). Initial perspective", ACM 978-1-60558-747-9/09/09.
[34] Wall, K., 2009, "Complexity of chemical products, plants, processes and control systems", Chemical engineering research and design, 87, pp. 1430–1437.
[35] Aven, T., Vinnem, J. E., 2007, Risk management. With applications from the offshore petroleum industry. Springer Series in Reliability Engineering.
[36] ISO 31000, 2009, "Risk management – Principles and guidelines".
[37] Haugen, S., Vinnem, J. E., 2015, "Perspectives on risk and the unforeseen", Reliability Engineering and System Safety, 137, pp. 1-5.
[38] Aven, T. 2015a. "Implications of black swans to the foundations and practice of risk assessment and management". Reliability Engineering and System Safety 134, pp. 83–91.

[39] Aven, T., 2015b, “Comments to the short communication by Jan Erik Vinnem and Stein Haugen titled “Perspectives on risk and the unforeseen””. Reliability Engineering and System Safety, 137, pp. 69–75.
[40] Bjerga, T., Aven, T. 2015. “Adaptive risk management using new perspectives – an example from the oil and gas industry”, Reliability Engineering and System Safety, 134, pp. 75-82.
[41] Ludvigsen, M., Sørensen, A. J., 2016, ”Towards integrated autonomous underwater operations for ocean mapping and monitoring”, IFAC Journal of Annual Reviews in Control, Volume 42, September, pp. 1-13, Elsevier Ltd.
[42] Seto, M. L., Paull, L., Saeedi, S., 2013, “Introduction to autonomy for marine robots”. In: Seto, ML (ed). Marine robots, Springer, N.Y.
[43] Strigini, L., 2012, “Fault tolerance and resilience. Meanings, measures and assessment”. In: K. Wolter, A. Avritzer, M. Vieira & A. van Moorsel (Eds*.),* Resilience Assessment and Evaluation of Computing Systems, Springer, Germany.
[44] Øien, K., Utne, I. B., Herrera, I. A., 2011, “Building safety indicators: Part 1 - Theoretical foundation”, Safety Science, 49 (2), pp. 148-161.
[45] Hassel, M., Utne, I. B., Vinnem, J. E., 2014, “Analysis of the main challenges with the current risk models for collisions between ships and offshore installations on the Norwegian Continental Shelf”, In Proceedings of the Probabilistic Safety Assessment and Management (PSAM) Conference, Honolulu, Hawaii.
[46] Hassel, M., Utne, I. B., Vinnem, J. E., 2015, “Challenges with bringing collision risk models used in the North Sea and Norwegian Sea to the Barents Sea”, Proc. of the Port and Ocean Engineering under Arctic Conditions (POAC) Conference, Trondheim, Norway.