A Method for Guided Hazard Identification and Risk Mitigation for Offshore Operations*,**

Christoph Läsche, Eckard Böde, and Thomas Peikenkamp

OFFIS - Institute for Information Technology,
Escherweg 2, 26121 Oldenburg, Germany,
{christoph.laesche,eckard.boede,thomas.peikenkamp}@offis.de

Abstract. One of the effects of the radically changing energy market is that more and more offshore wind turbines are being constructed. To meet the increasing demand for renewable energy, many new companies with different levels of experience are entering the market. As the construction and maintenance of large offshore wind farms is a complex task, safety aspects of these operations are of crucial importance to avoid accidents. To this end, we introduce a method that assists in (1) identifying and precisely describing hazards of a scenario of an offshore operation, (2) quantifying their safety impact, and (3) developing risk mitigation means. Based on a guided hazard identification process, a formalization of hazardous scenarios will be proposed that unambiguously describes the risks of a given offshore operation. We will demonstrate the feasibility of our approach on a specific offshore scenario.

1 Introduction

The radical change in the energy market towards renewable energy production that has been initiated by politics causes a high demand for wind turbines to be built. Because of concerns regarding noise emissions and scenic impacts, there are ongoing plans to place more and more wind turbines into offshore wind parks. In Germany, 24 wind parks in the North Sea have been approved so far ([1], [2]). However, the construction of many of these wind parks is delayed.

As such a huge change in a short time can only be realized by a large amount of companies constructing multiple facilities concurrently, a lot new players rush into the offshore wind energy market. Not all of these companies have extended experience in the maritime or offshore sector and are familiar with the required safety assessment procedures. Implementing the necessary practices and processes is a highly complex task. Not supporting their adoption could be a delaying factor for the energy change. Recent events ([3], [4]) have shown that

* This work was partially supported by the European Regional Development Fund (ERDF) within the project *S*afe *O*ffshore *Op*erations (SOOP), http://soop.offis.de/.

** This work was partially supported by European Commission for funding the Large-scale integrating project (IP) proposal under the ICT Call 7 (FP7-ICT-2011-7) *D*esigning for *A*daptability and evolutio*N* in *S*ystem of systems *E*ngineering (DANSE) (No. 287716).

F. Ortmeier and P. Daniel (Eds.): SAFECOMP 2012, LNCS 7612, pp. 37–48, 2012.

nevertheless these assessments have to take place to protect personnel and environment In many aspects, offshore scenarios fulfil the criteria of a System of System (SoS). Maier[5], for instance, uses five characteristics that, depending on their strength, impose different challenges for offshore operations:

- *Operational independence of the elements:* To a small extend, the people and systems may act independently during an offshore operation. However, they are mostly directed by guidelines and supervisors.
- *Managerial independence of the elements:* The systems (e.g. construction ships) are to some extend not depending on other systems during an operation. Nevertheless, a complete independence is not given.
- *Evolutionary development:* While the first offshore operations had prototypical character, new technological possibilities as well as political/legal constraints lead to an evolution of the operations, its procedures, and the involved systems.
- *Emergent behavior:* As of today, there has (to our knowledge) not been a systematical investigation of the interaction of people and systems during offshore operations. To perform such an analysis, a model that consistently integrates the behavior of the involved systems is a preferable solution.
- *Geographic distribution:* There might be a large geographic distribution as the guidance authorities for an operation might reside onshore whereas the operation itself takes place offshore. Further, the geographic distributions of involved systems and people offshore has a strong impact on the efficiency.

Therefore, we consider the collection of all systems and persons involved in typical offshore operations as an SoS.

The SOOP project[1] aims at supporting planning and execution of safe offshore operations for construction and maintenance of offshore wind turbines. A special focus is set on the behavior of persons involved. To analyze an operation, a model based approach is used, including modeling the behavior of the involved persons, as described in [6]. Thus, a conceptual model is build and maintained that describes the interaction of systems and persons as well as the evolution of the system. The architecture of the system and thus the conceptual model will be changing over time as new needs might arise during the project implementation. Another aspect of the SOOP project is the identification and mitigation of possible risks during the planning process while also taking the situation into consideration. The results for this will also be used for an online assistant system that monitors the mission (e.g. the location of crew and cargo, cf. [7]) and warns if a hazardous event is emerging. This is intended as a further way to avoid risks during an offshore operation.

In this paper, we will focus on the risk assessment aspects of the project. We will discuss our current approach in performing those steps and present our methods we developed for an improved risk identification process. After introducing some terms and definitions, we will first give an overview about current hazard identification and risk assessment approaches. Later, we show

[1] `http://soop.offis.de/`

how the conceptual model can be used to guide the hazard identification and formalization process and how it can be used for modeling the relevant scenarios and risk mitigation possibilities.

2 Terms and Definitions

To ensure a common understanding of hazard related terms in this paper, we will give an overview over our definitions for which we follow ISO 26262[8] and IEC 61508[9]. In sec. 4, we will further describe why we use parts of the automotive standard in addition to the maritime approaches.

We define a *hazard* as an event that might lead to harm of humans or of the environment. The event that might lead to a hazard is called *failure*, it is the inability of persons or systems to perform the normative functions. A failure might be induced by an *error* which is an abnormal condition; its cause is called *fault*. An *operational situation* describes a process or setting during an operation, and the combination with a hazard is called *hazardous event*. This term is most commonly used in the automotive context, less often in other domains. We introduce it to be able to further differentiate hazards as the impact of a hazard depends on the situation. An example for this is an injury happening to a person working on a ship. It is less problematic happening while the ship is in the harbor, as transportation to the nearest hospital will take less time than transporting the person from an offshore location.

According to Vinnem[10], the risk in the offshore sector can be quantified by the expected harm that is caused by a hazard and its probability. In our approach that takes some aspects of the ISO 26262 into consideration, we extend this with the *controllability* of a hazard. A quantification respecting these parameters would describe the risk of an operation as $\mathsf{Risk(Hazardous\ Event)} = \sum_i (\mathsf{Probability\ of\ independent\ cause}_i) \times \mathsf{Consequence} \times \mathsf{Controllability}$. The controllability reflects the ability to avoid harm or damage by timely reacting to a hazardous event. This could be realized by alerting persons of emerging risks, hence they are aware of it and have the possibility to deploy preventive measures. More details on our extended risk definition can be found in sec. 4.

3 State of Practice in Risk Assessment

Oil and gas companies have collected a lot of experience in the offshore sector. Safety assessments have been performed in this area for a long time and a large knowledge base exists. Nevertheless, these experiences cannot directly be applied to offshore wind turbine operations as, although some similarities exist, most of the risks differ substantially. For example, there may be a lot of risks regarding fire and explosion when considering oil and gas rigs, as both of them handle ignitable compounds. Those are not primary risks when talking about offshore wind turbines. Neither are there risks such as blowouts or leakage. Besides these differences, some operations are common between both types of offshore operations. Therefore, Vinnem[10] has been taken into consideration as a reference to planning of oil rig related operations. It describes the state of the art in risk analysis in the domain. In detail, it addresses the steps of *Quantitative Risk Analysis* (QRA), which is a type of risk assessment that is frequently applied to oil and gas related offshore operations. Its approach is based in the standards IEC 61508[9] (which is also the base for ISO 26262) and IEC 61511[11]. The steps involved in the QRA approach are depicted in fig. 1, which we have extended with the shaded box (along with annotations of our developed methods). They include identifying possible hazards, assessing their risks and developing risk mitigation measures if the identified risk is not tolerable. We further describe these steps when introducing our modified approach in sec. 4.

In order to identify all possible hazards, Vinnem further introduces HAZID (*HAZard IDentification*) as an analysis technique, which basically suggests which steps need to be performed and which sources should be taken into consideration when identifying hazards. The sources include check lists, previous studies, and accident and failure statistics. Performing the approach requires a lot of manual work which demands experienced personnel. In newly planned operations, this is a time consuming and expensive process. In addition to this, the HAZID process is not well defined, not structured, and has no source that completely lists the relevant potential hazards or risks. To improve this, we introduce a guided way of identifying hazards, which is described in sec. 4.

A further approach is *Formal Safety Analysis* which is also used for offshore safety assessment[12]. It is based on assigning risks (that are also identified using HAZID) to three levels: intolerable, as low as is reasonably practicable (ALARP), and negligible. Risk assigned to the ALARP level are only accepted if it is shown that serious hazards have been identified, associated risks are below a tolerance limit and are reduced "as low as is reasonably practicable". Because this concept does not rely on quantification and rather uses an argumentative method for assessing risks, the analysis might not be complete and requires a lot of manual expert effort. Because of this there are no concepts that are interesting for usage with our model-based approach.

Of particular interest is the current automotive standard as in contrast to the processes in the offshore sector, those in the automotive sector are more time and cost efficient. This is due to the strong competition between different manufacturers in this industry, the large amount of sold units, the short innovation cycles and a high volume market with many different car configurations. To achieve a cost efficient process of risk assessment, a specialized approach, defined in ISO 26262[8], is used by the automotive companies. In contrast to the offshore sector, the automotive industry also considers controllability as a factor for the risk assessment, which we have described in sec. 2.

4 Introducing a Modified Approach for Offshore Risk Assessment

We will introduce an improved approach of it in the current section as well as additional methods to support the risk assessment process. Our approach is model-based because this kind of analysis has proven to us to be effective in other domains. It enables us to model the expected behavior as well as possible dysfunctional behavior. It also makes it possible to reuse methods and techniques for model-based safety assessment, for instance those developed in the ESACS and ISAAC projects (cf. [13,14]) in the aerospace domain.

The most important difference between the risk assessment approach of the automotive sector and the one used in the offshore sector is that the automotive approach includes a third risk assessment factor, the controllability of hazardous situations. We borrow this concept as a further assessment factor of our approach, which will support the risk mitigation by introducing measures raising the awareness of a risk, thus allowing its prevention or reduction of its impact. Considering this parameter enables us to include human factors, that is the ability of humans to react to a hazardous event in a way that lowers its impact or even prevents it, in our analysis. Further, the mission assistant developed in the SOOP project (cf. sec. 1) that might alert the personnel about potential hazards and thus allows avoiding them or mitigating their impact can also be incorporated. The modified approach with added controllability (marked by shades) can be seen in fig. 1. Also, we added information about how our methods are integrated with the QRA approach in the boxes on the right side.

A further concept originating in the automotive sector and used in our approach are *Hazardous Events*. Their usage enables for us to further differentiate

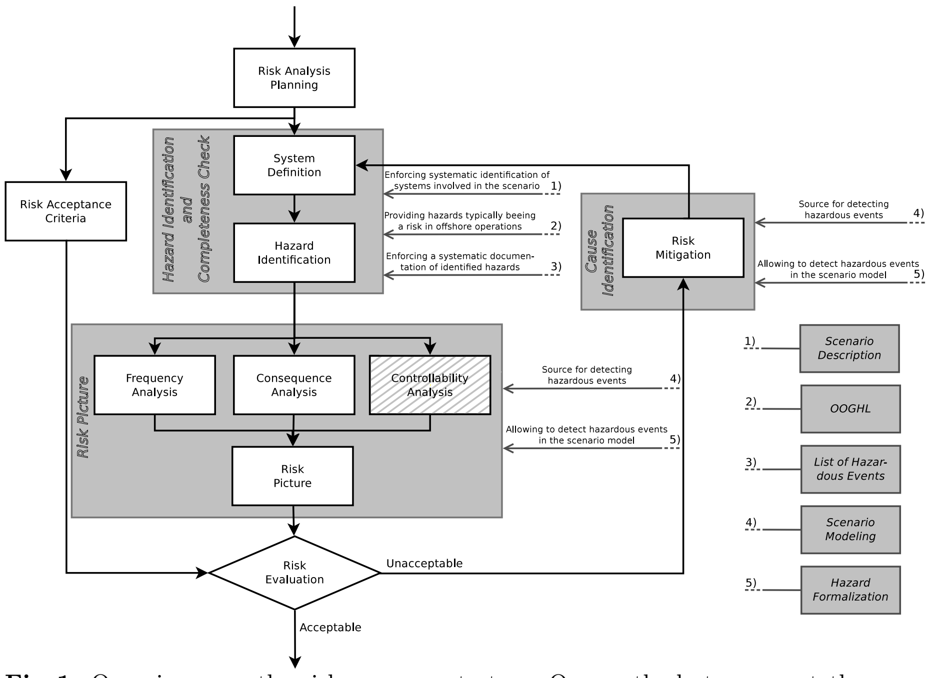


Fig. 1. Overview over the risk assessment steps. Our methods to support them are annotated by boxes. Enhanced version the QRA approach from [10]. Enhancements are marked by shades.

the hazards by specifying the situations in which they occur. This allows us to assess the impact of a hazard in a specific situation, as the impact might be dependent on the operational situation. A hazard might have a more severe consequence in some situations than in others. In a few situations, a hazard may even have no relevant impact at all.

In the following sections, we introduce every step of our approach as well as the supporting methods.

4.1 Hazard Identification and Completeness of Identified Hazards

The base for the assessment of risks are the hazardous events. To create this base, it is necessary to identify all possible hazards including the related faults, environmental conditions, and operational situations of which the hazardous events consist. We introduce three steps that result in a list of hazardous events and the corresponding causes.

The first step is obtaining a detailed *Scenario Description* out of which the possible hazards have to be identified in the next step. To support this process we introduce a concept of a *Generic Hazard List*. As a final step, the results of the identification process have to be documented.

Scenario Description: A precondition for identifying the hazards that could occur during a scenario is a detailed description. An interview with maritime experts is one way to reach this description. During the interview, guidance by the interviewer is necessary to ensure that all steps are captured completely, as the interviewed persons might omit intermediate actions and checks that seem obvious to them because of their many years of experience. Each step has to be collected and every single sub-step has to be gathered to get a detailed description. Additionally, potential hazards might be collected, too, to extend the amount of hazards detected using the *Generic Hazard List* introduced in the next section. As explained in the introduction, these scenario descriptions are used to update the conceptual model.

Offshore Operation Generic Hazard List (OOGHL): The HAZID approach described in sec. 3 takes several sources of information about potential hazards into consideration (e.g. previous studies, accident reports, etc.). These sources lack structure that allows their use as an efficient guide for hazard identification. Furthermore, similar hazards might be described in different sources which causes additional effort in harmonizing them. Another problem is that merging different sources might lead to oversight of a relevant hazard.

This is why we developed a special instrument, the *Offshore Operation Generic Hazard List* (OOGHL). It consists of an abstract description of possible actions during an offshore operation, as well as of descriptions of the hazards to which the actions might contribute to. Its structure is based on the approach of an *Automotive Generic Hazard List* (AGHL) as described by Reuss[15] and Beisel[16], but as their GHL is optimized for automotive assistance systems, it cannot be applied directly to the offshore sector. The nature and the complexity of interactions and hazards differ in an extensive manner. Thus, we have developed a GHL that is specifically adjusted to offshore related interactions and hazards. The data of our GHL is based on accident reports (e.g. *Lessons Learned for Seafahrers*[17]), guidance documents (e.g. IMCA publicatons[2]), and expert interviews. Our data is not complete by now and currently limited to assess two example scenarios as we focus on them in the research project. Further sources can be reviewed to extend the OOGHL which currently consists of about 450 entries.

In order to use the OOGHL, a detailed description of the scenario is required (see above). Using this description, a step by step walktrough of the scenario is possible and every step can be analyzed by looking up the potential in the OOGHL. To allow such a lookup systematically, the OOGHL comprises of all possible actions that might be part of an offshore operation. It also contains points of interaction between persons, resources, and the environment (e.g. other traffic, fixed installations, or other resources) and, as a third component, the potential hazards that might occur in the analyzed scenario. The structure of the OOGHL is depicted in fig. 2.

When using the OOGHL to look up hazards, all actions that are performed in the step of the scenario have to be considered. As an example, we show how to identify the hazards for the step *Stepping Over to the Offshore Turbine* of a scenario that comprises transferring persons to the turbine. We match our descriptions of the steps taken during the scenario to the actions listed in the OOGHL. The description of the example includes a step in

	Actions											Hazards											
	Approaching	*Communicating*	*Evaluating Situation/Checking*	*Safeguarding/Desafeguarding*	*Starting*	*Entering/Moving/Navigating*	*Using*	*Watching*	*Lifting/Letting down*	*Positioning/Tilting*	*Preparing/Finishing*	*Collision*	*Grounding*	*Damage at ship/at equipment*	*Damage at offshore object*	*Capsizing*	*Sinking*	*Fire*	*Loss of oil*	*Person falling over/slipping*	*Person falling into water*	*Person getting hit by (falling) object*	*Person injured*
Wind	X											1.1	---	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12
		X										2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12
			X									3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	3.10	3.11	3.12
				X								---	---	---	---	---	---	---	---	4.9	4.10	4.11	4.12
					X							---	---	---	---	---	---	---	---	---	---	---	---
						X						6.1	6.2	6.3	---	6.5	6.6	---	6.8	6.9	6.10	6.11	6.12
							X					---	---	---	---	---	---	---	---	---	---	---	---
								X				---	---	---	---	---	---	---	---	---	---	---	---
									X			---	---	9.3	---	---	---	---	9.8	---	9.10	9.11	9.12
										X		---	---	---	---	---	---	---	---	---	---	10.11	10.12
											X	11	---	11.3	---	---	---	---	11.8	---	11.10	11.11	11.12
Rain/Fog (wetness)	X											---	---	---	---	---	---	---	---	12.9	12.10	---	12.12
		X										---	---	---	---	---	---	---	---	13.9	13.10	---	13.12
			X									14.1	14.2	14.3	---	14.5	14.6	14.7	14.8	14.9	14.10	14.11	14.12
				X								---	---	---	---	---	---	---	---	15.9	15.10	15.11	15.12
					X							---	---	---	---	---	---	---	---	---	---	---	---
						X						---	---	---	---	---	---	---	---	17.9	17.10	17.11	17.12
							X					---	---	---	---	---	---	---	---	18.9	18.10	---	---
								X				---	---	---	---	---	---	---	---	---	---	---	---
									X			---	---	---	---	---	---	---	---	---	---	---	---
										X		---	---	---	---	---	---	---	---	---	---	---	---
											X	---	---	---	---	---	---	---	---	---	---	---	---
	X											23.1	---	23.3	23.4	23.5	23.6	23.7	23.8	23.9	23.10	23.11	23.12

Fig. 2. Excerpt from the OOGHL

which a ladder is used and the matching action from the OOGHL would be *Entering/Moving/Navigating*. After this, every row of the column of the action containing an `X` is considered. The label of this row reflects a possible point of interaction. For our example, a possible row would be *Rain/Fog (wetness)*. If this combination with the action seams feasible, the descriptions of the potential hazards referenced in the table will be taken into consideration. In addition, this descriptions include promotive and preventive factors for the hazard. In our

[2] `http://www.imca-int.com/documents/publications.html`

17.9
Slipping off while using a ladder during wet weather

Involved Actors:	Person, Safeguarding
Locations:	Ladder
Potential Source:	---
Description:	A person uses a ladder during wet weather. The person slips off and falls down.
Possible Reasons:	Sudden weather change, wrong evaluation of situation, faulty safeguarding
Promotive Factors:	Missing maintenance, missing training, missing safety equipment
Preventive Factors:	Not letting persons use ladder during wet weather, improve safeguarding
Related Entries:	17.10
Further Information:	---

17.10
Falling into water because of slipping off a ladder during wet weather

Involved Actors:	Person
Locations:	Ladder
Potential Source:	17.9
Description:	A person uses a ladder during wet weather. The person slips off and falls down. The person land in the water
Possible Reasons:	Sudden weather change, wrong evaluation of situation, faulty safeguarding
Promotive Factors:	Missing maintenance, missing training, missing safety equipment
Preventive Factors:	Not letting persons use ladder during wet weather, improve safeguarding
Related Entries:	---
Further Information:	---

Fig. 3. Example entries for detailed description of hazards

case, the descriptions for the entries 17.9 to 17.12 are taken into account, of which two are shown in fig. 3.

Using the OOGHL to identify possible hazards has the advantage that only one source has to be taken into consideration (in contrast to HAZID). This leads to less time expense in processing hazard descriptions in contrast to the HAZID approach.

Identifying Hazardous Events: To assess the risks associated with the identified hazards, the hazards have to be documented. As we use *Hazardous Events* which we introduced in sec. 2 and sec. 4, we extended the documentation with these events as well as with all their dependencies and the dependencies for the hazards. The documentation is realized by a list consisting of all events and conditions. They are distinguished by a type and linked by a dependency structure for each event through an column that lists the causes for each event. An excerpt of possible content of the table is depicted in fig. 4 showing the previously identified hazards with some of their causes and two resulting hazardous events. By parsing the *Causes* column, a fault tree can automatically be generated. Further to this, the dependency structure can be used to formalize the hazardous events listed in the table which is useful for analyzing the scenario, as we will demonstrate in the next section.

ID	Type	Description	Causes	Comments	Consequence	Probability	Controlability
7	Hazard	Falling into water	18; 39; 75, 62; 18, 75; 63, 75; 64, 75; 65, 75; 39, 75; 92; 93			0.01	
43	Environmental Condition	Fog				0.2	
44	Environmental Condition	Rain				0.2	
45	Environmental Condition	Slickness	43; 44			0.4	
76	Failure	Missing safeguarding	3; 4; 11; 33; 35			0.04	
86	Fault	Slipping off the ladder	45; 54; 55; 56; 57; 71; 84; 84, 85; 85			0.06	
91	Human Failure	Not at least one hook hooked in	3; 4; 33; 35; 78			0.02	
92	Failure	Falling down the ladder	76, 86; 86, 91			0.05	
103	Operational Situation	Temperate water				0.3	
104	Operational Situation	Cold water				0.7	
108	Hazardous Event	Falling into cold water	104, 7		0,8	0.71	0.2
109	Hazardous Event	Falling into temperate water	103, 7		0,3	0.31	0.4

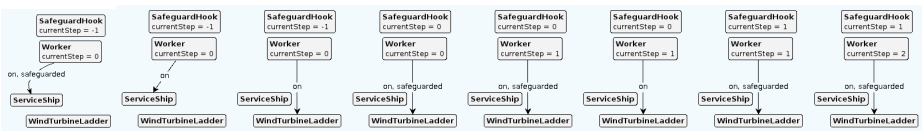
Fig. 4. Excerpt from the list of events. The Hazardous Events are marked.

4.2 Risk Picture

After all potential hazards of the scenario are defined, a risk picture can be created. This can be achieved by formalizing the scenario description as well as the hazardous events to analyze their occurrence and causes. While creating the risk picture, the risks associated with the hazardous events are assessed by evaluating the frequency, consequence, and controllability. This is realized by assessing the hazardous events regarding their consequences (i.e. harm caused to humans and to the environment, costs caused, etc.) and their controllability (i.e. if the event can be controlled if it occurs, thus mitigating its impact) and investigating the underlying causes for the hazardous event regarding their frequency of occurrence.

Modeling the Scenario: To perform a model-based risk assessment, we have to model the scenario we want to analyze. Because the behavior of the involved actors the model is highly dynamic, we decided to use a graph transformation model. This allows us to reflect this behavior in a way that is not possible when using, for instance, finite state machines. Graph transformations allow us to dynamically add or remove actors and allows changing the way of interaction and the relations between actors during execution.

As a demonstration, we modeled the previously mentioned example using GROOVE[3]. Within the project, we are planning to develop software to automatically generate models out of the conceptual model. Fig. 5 (a) shows the initial state of our modeled graph from the example. The worker is safeguarded using a safety rope which is hooked on the service ship and he is not yet on the ladder of the wind turbine to which he wants to step over. For this, the hook has to be removed and he has to step onto the ladder before he can hook in the safeguarding again. This is realized in the model by using transformation rules that describe how the graph may be modified and leads to the state *s3* after passing the states *s1* and *s2*. To step up the ladder, the hook has to be removed and hooked into the next step of the ladder. This can be seen in fig. 5 in the attributes *onStep* of the *Worker* and the *SafeguardHook*, which reflect the current step of the worker and the hook. The worker may not use the next step until the hook is attached on the current step of the ladder.



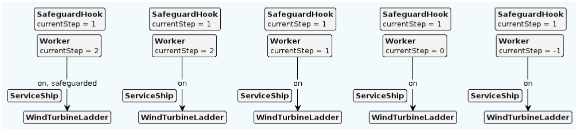
(a) *s0* **(b)** *s1* **(c)** *s2* **(d)** *s3* **(e)** *s4* **(f)** *s5* **(g)** *s6* **(h)** *s7*

Fig. 5. States (*s0–s7*) of an example of a scenario modeled using GROOVE

Fig. 5 only shows the correct process of stepping over and climbing up the ladder. In order to detect potential hazards in the scenario, a formalization of the hazardous events can be used.

Formalizing Hazardous Events: Using a model of the scenario, it can be checked if it is possible to reach a hazardous event by utilizing a model checker. For this, an observer has to exist that is used to check if a state has been reached

[3] `http://groove.cs.utwente.nl/`



(a) *s7* **(b)** *s8* **(c)** *s9* **(d)** *s10* **(e)** *s11*

Fig. 6. States (*s7–s11*) of an example of a scenario modeled using GROOVE

that might constitute a hazardous event. One way to create such an observer is to formalize the hazardous events from the list of events as presented prior. As the formalization of hazardous event is currently under development in the SOOP project, developing a specialized formalization language, we use a Linear Temporal Logic with past operators (PLTL, cf. [18]) to demonstrate the formalization. Formalization allows assessing each state of the simulation regarding if a hazardous event has occurred, thus generating observers that permit to realize an automatic detection of all hazardous events happening in a modeled scenario.

An example of how a hazardous event might occur can be seen in fig. 6, continuing the scenario depicted in fig. 5. After removing the safeguarding hook in order to hook it into the next step of the ladder, the worker slips off the ladder. Because he is not safeguarded anymore, he falls from step to step until he lands into the water (i.e. *currentStep* becomes -1). This is caused by the environmental condition *Wet Weather* that causes the ladder to become slippery.

The dependency structure allows to use the list as a source for formalization. Resolving the dependencies, a LTL formula can be developed stepwise with which it can be assessed whether a state (π^i) satisfies ($\models$) the formula. The following gives an example for this process:

$$\pi^i \models \text{Falling into cold water}$$
$$\pi^i \models F(\text{Cold Water} \wedge O(\text{Falling into Water}))$$
$$\pi^i \models F(\text{Cold Water} \wedge O(\text{Falling down the ladder} \wedge \text{Missing Safeguarding} \vee \ldots)).$$

The formalization also models the faults and environmental conditions that are necessary for the hazardous event to occur. This list of faults can be used as a source for the causes that might lead to the hazardous event and thus should be injected into the model to provoke a hazardous event. The model is modified to be able to represent faults and those faults are systematically triggered. By this, it is possible to detect which faults are required to cause a hazardous event. A detailed methodology for fault injection and model checking has been developed in the ESACS and ISAAC projects (cf. [13,14]).

After having detected all possible causes of a hazardous event, the frequency of the independent causes (that e.g. origins from reference manuals or, in case of humans, analyses of behavior) has to be summed up and thus the frequency of the occurrence of the hazardous event is calculated. The consequence and controllability of the hazardous events have to be assessed, too. Finally, a quantification for each hazardous event exists. If the quantified risk value is higher than the risk acceptance value, a risk mitigation has to take place.

4.3 Risk Mitigation

In order to minimize the risk of an offshore scenario, a risk mitigation process for hazardous events that have a high risk quantification value has to take place. This can be realized by developing measures to prevent certain faults, thus lowering the frequency of occurrence of a hazardous event. Another way to minimize the risk is to raise the controllability of the hazardous event. To reach this, the awareness of potential hazards has to be raised so that proper reaction to the hazardous event can happen or other technical measures have to be considered. A third option is to minimize consequence of a hazardous event if it occurs. To minimize the risk in the example scenario, possible causes for risks can be avoided. The easiest way for this is not to allow the operation to be performed during wet weather as this removes one cause for the hazardous event, thus reducing the probability.

Another way is to add additional safety measures. As described in the example description, there is only one safety hook that is attached while using the ladder. The use of a second hook, attached in alternation with the first one, fixes this flaw as there now is at least one hook that might catch the worker when falling down the ladder. This way the risk is reduced because of the improved controllability. To minimize the consequence in the example, the worker falling down the ladder should be required to wear a life belt so that drowning would become less likely.

5 Conclusion

In this paper, we have presented a new method to improve risk assessment for construction and maintenance operations for offshore wind energy parks. We have based our approach on existing techniques used for risk assessment of offshore and maritime operations. To extend the approach, we adopted methods from the automotive domain for improving and optimizing the risk assessment process by adding the factor *Controllability* (as defined in ISO 26262) to complement the existing factors *Frequency* and *Consequence* for forming the risk picture. Taking controllability into account enables better distinction between possible outcomes of a *hazardous event* (which is also a concept taken from the ISO 26262), thereby improving the correct assessment of the actual risk. Furthermore, it improves the ability to evaluate the effectiveness of mitigation measures. This is especially important with respect to the SOOP project in which we plan to develop an assistant system that is intended to raise awareness of developing critical situations and suggest mitigation measures in case a hazard has actually happened (cf. sec. 1).

One of the central improvements is our *Generic Hazard List* that we are specifically developing to systematically identify potential hazards and their causes in offshore operations. The idea of a generic list of hazards was adopted from a similar concept, originating from automotive projects. In our approach, we have taken this tool and further improved it to not only address the topic of hazard identification, but also to include the possible causes leading to a hazard. Once this data has been captured, we were able to formalize the dependency relation between faults, errors, failures, and hazards.

Our next step is to model the behavior of the system, the environment, and participating persons. This behavior model is the necessary precondition for further model-based safety analysis of the system. Techniques to be used include those developed during the ESACS and ISAAC projects which enable model-based FMEA (Failure Mode and Effect Analysis) and FTA (Fault Tree Analysis) (cf. [13,14]).

References

1. Bundesamt für Seeschifffahrt und Hydrographie: Genehmigung von Offshore Windenergieparks (2012), http://www.bsh.de/de/Meeresnutzung/Wirtschaft/Windparks/index.jsp
2. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Entwicklung der Offshore-Windenergienutzung in Deutschland/Offshore wind power deployment in Germany (2007)
3. Brandt, J.: Stundenlange Suche nach dem Vermissten auf See. Ostfriesen-Zeitung (January 26, 2012)
4. Vertikal.net: Fatal accident in Harwich (May 21, 2010), http://www.vertikal.net/en/news/story/10145/
5. Maier, M.W.: Architecting Principles for Systems-of-Systems. TiAC White Paper Repository (December 20, 2010), http://www.infoed.com/Open/PAPERS/systems.html
6. Lenk, J.C., Droste, R., Sobiech, C., Lüdtke, A., Hahn, A.: Towards Cooperative Cognitive Models in Multi-Agent Systems. In: International Conference on Advanced Cognitive Technologies and Applications (2012)
7. Wehs, T., Janssen, M., Koch, C., von Cölln, G.: System Architecture for Data Communication and Localization under Harsh Environmental Conditions in Maritime Automation. In: IEEE 10th International Conference on Industrial Informatics (2012)
8. International Organization for Standardization: ISO/DIS 26262 - Road vehicles Functional safety (2011)
9. International Electrotechnical Commission: IEC 61508 (2010)
10. Vinnem, J.E.: Offshore Risk Assessment, 2nd edn. Springer (2007)
11. International Electrotechnical Commission: IEC 61511 (2003)
12. Wang, J.: Offshore safety case approach and formal safety assessment of ships. Journal of Safety Research 33(1), 81–115 (2002)
13. Peikenkamp, T., Cavallo, A., Valacca, L., Böde, E., Pretzer, M., Hahn, E.M.: Towards a Unified Model-Based Safety Assessment. In: Górski, J. (ed.) SAFECOMP 2006. LNCS, vol. 4166, pp. 275–288. Springer, Heidelberg (2006)
14. Åkerlund, O., et al.: ISAAC, a framework for integrated safety analyses of functional, geometrical and human aspects. In: ERTS (2006)
15. Reuß, C.: Automotive Generic Hazard List. Technische Universität Braunschweig (2009)
16. Beisel, D., Reuß, C., Schnieder, E.: Approach of an Automotive Generic Hazard List. In: Proceedings of European Safety and Reliability, ESREL (2010)
17. IMO: Lessons Learned from Casualities for Presentation to Seafahrers, (2004/2006/2010), http://www.imo.org/blast/mainframe.asp?topic_id=800
18. Latvala, T., Biere, A., Heljanko, K., Junttila, T.A.: Simple Is Better: Efficient Bounded Model Checking for Past LTL. In: Cousot, R. (ed.) VMCAI 2005. LNCS, vol. 3385, pp. 380–395. Springer, Heidelberg (2005)