Ice management and design philosophy

S. Ruud & R. Skjetne
Sustainable Arctic Marine and Coastal Technology (SAMCoT)
Norwegian University of Science and Technology
NO-7491 Trondheim, Norway

ABSTRACT: Ice management (IM) is defined as all activities carried out with the objective of mitigating hazardous situations by reducing or avoiding actions from any kind of ice feature to a protected unit (e.g. a drilling vessel) and includes several types of barriers. IM barriers are ranging from ice observation, ice prediction, ice alerting, ice fighting with icebreakers, and disconnection procedures of the protected unit. The design decisions of the IM barrier systems can be based on qualitative or quantitative performance models. Qualitative descriptions of independent and dependent barriers are first defined and exemplified with qualitative decision criteria. Qualitative concepts for barrier performance of ice prediction are defined and illustrated in event trees. National barrier regulations (e.g. PSA) contain requirements to model quantitatively the barrier performances. Quantification of the IM performance, which are defined by probabilities of barrier functions, is a major challenge due to lack of data and existing uncertainties. Finally, the paper presents a brief plan for demonstration of the performance models in the design phase with experience data collection supporting the safe learning principle.

1 INTRODUCTION

Design decisions for safe and efficient ice management (IM) systems can be based on performance models and decision criteria for the overall or parts of the IM systems. The IM system performance models should be able to cover the following IM system parts (see Fig. 1):

- Ambient ice regime, ice hazards and ice risks to the protected unit operations.
- Operational ice observation, prediction and alerting functions.
- Operational physical IM or ice fighting with e.g. icebreakers.
- Operational disconnection and move-off procedures and systems for the protected unit. In this paper, a ship-shaped movable exploration offshore unit is chosen as the protected unit.

The Ice Management and Design Philosophy Work Package is a part of the SAMCoT research program. In the beginning of this project, complete methods for combining all the above types of information in qualitative and/or quantitative decision processes were not available. This paper is an attempt to put this together and contribute to the solution of the identified needs. The research and development work are ongoing.

IM design decisions are proposed to be based on a top-down approach of barrier performance descriptions, and the main description types are presented in sections 2-6 as indicated below:

2. The barrier definition and high level definitions of general barrier events are described.
3. Boolean representation of main barrier events. The success of a barrier system is dependent on fulfilment of the barrier internal and external requirements of several barriers.
4. Detailed barrier performance requirements. The detailed combined functional and ambient performance requirements for barrier success are defined.
5. Probabilistic barrier performance. Quantification of the barrier performance is based on the probabilities of successful performance of the Boolean expressions of the barriers.
6. Expected consequences and risk. Consequences associated to the resulting events can be used for estimating residual risk of the barrier system and as basis for design decision-making.

Section 7 describes a plan for a case study on testing and demonstration of the methods given in this paper.

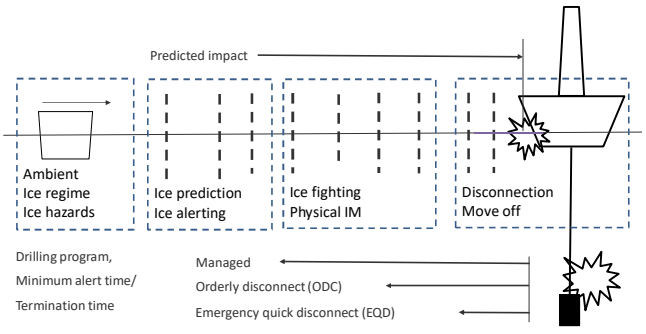

Figure 1. IM performance models cover ice regime models, ice observation and prediction, physical ice management (icebreakers), disconnection and move-off systems for the protected unit. The protected unit will need sufficient time durations for e.g. orderly disconnect or emergency quick disconnect procedures.

2 IM BARRIERS

The objective of IM is to mitigate hazardous situations by reducing or avoiding actions from any kind of ice (sea ice or glacial ice) at a specific location for planned operations by a protected unit.

The initial premise in this paper is that IM design shall be described in a top-down manner. The ice hazards and risk shall be sufficiently mitigated by the IM barriers. All elements shall be modelled in accordance with the given type of design decision acceptance criteria for the given decision scope. If more detailed information is needed the proposed IM design process shall advice how more detailed information may be incorporated to support an improved decision.

2.1 *Operational and environmental requirements*

The protected unit shall carry out operations within stated environmental limits for given durations.

Two typical operational situations are:

- Long term continuous operational durations (e.g. many years) with fixed environmental limits for e.g. a fixed production unit.
- For short term exploration projects (e.g. drilling 1-3 months) with specific activity durations and variable environmental limits.

Description of the planned activities and operational requirements shall be established in the beginning of an IM design project.

2.2 *Ambient ice regime*

In the beginning of an IM project, available information about the ice regime and the possible hazards for the planned operations shall be compiled.

We assume that the location of the protected unit is at a certain distance from the ice sheet and that possible arrivals of hazardous ice may occur seldom and with a low frequency (e.g., 1-5 times annually). This situation is sometimes denoted as *Workable Arctic Conditions*. The demand for operational IM responses by icebreakers is assumed to occur a few times annually.

The opposite situation is relevant for locations where the ice sheet may continuously surround the protected unit. The demand for IM response may in periods be continuous, and in other periods the ice conditions may be inoperable.

2.3 *Establishing the ice hazards and the ice risks*

Based on the information of the ice regime and the operational ice limitations, an ice hazard and risk analysis shall be prepared and quality assured.

The initial IM design decision shall therefore clarify if the actual risk identified will require additional risk reduction measures (or barriers) in order to comply with the stated acceptance decision criteria.

2.4 *IM performance acceptance criteria types*

The acceptance criteria for IM performance may be defined as requirements to the performance of the overall IM system scope, or at specific sub-scopes, e.g. ice observation and prediction (Fig. 2). The performance requirements may also be qualitative and quantitative. The main issue, however, is that the overall IM plan shall state the scope and the IM performance acceptance criteria to be complied with for the given scope.

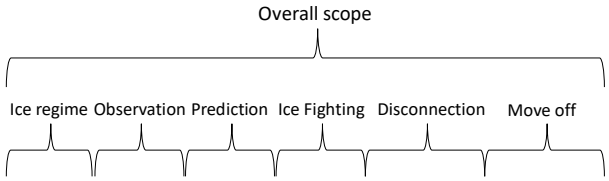

Figure 2. The IM performance acceptance criteria are formulated at the overall barrier system level or at subsystem levels.

2.5 *The barrier concept*

Operations on the Norwegian Continental Shelf shall be in compliance with the regulations from the Petroleum Safety Authority (PSA 2017). In this paper *§5 Barriers* is used as a reference for defining the barrier concept.

'…the responsible party shall select technical, operational and organisational solutions that reduce the likelihood that harm, errors and hazard and accident situations occur. … Barriers shall be established that at all times can a) identify conditions that can lead to failures, hazard and accident situations, b) reduce the possibility of failures, hazard and accident situations occurring and developing, c) limit possible harm and inconveniences… Where more than one barrier is necessary, there shall be sufficient independence between barriers.'

Figure 3 is an illustration of the main barrier events.

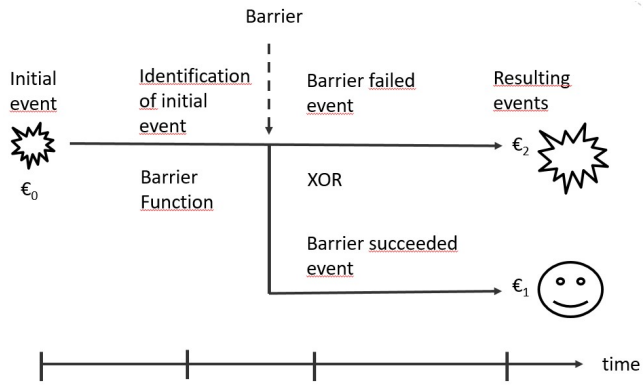

Figure 3. Barrier events in an event tree with one barrier. The barrier shall be able to a) identify conditions or initial events ($€_0$) that can lead to further consequences, b) reduce the possibility of development ($€_1$) of further consequences, c) limit possible harm, and inconveniences ($€_2$). In the figure the exclusive or (XOR) indicates that the barrier will either succeed or fail for one single initial event.

3 BOOLEAN REPRESENTATION OF MAIN BARRIER EVENTS

3.1 *Hazardous ice conditions*

IM is relating to ambient conditions where the conditions in the ambient area may be hazardous to the operation of the protected unit. The ambient conditions may also affect the performance of barriers.

Environmental or ambient parameters concerns:

- wind and current (including depth profiles),
- wave height and spectrum,
- temperature,
- sea ice and iceberg, size, thickness, strength,
- rain, snow, fog,
- visibility, and
- air pressure, polar lows.

Combinations of the environmental parameters must be considered, especially the fact that the ice conditions may take multi-domain characteristics with large spatial and temporal variations.

Examples of ice related events and conditions are:

- drift of ice islands and fragments,
- drift of ice that was land-fast and large areas of pack ice,
- large changing and reversals in ice drift,
- drift of old ice and glacial ice (icebergs) towards the operations sites,
- fast changes of wind speed and direction causing pressure,
- fast changes of currents (outflow from river or ice dam failure), and
- effects of polar lows.

In the context of this paper, occurrence of a hazardous condition at time t is denoted as an initial event $€_0(t)$ and represented as a Boolean variable normally being false, but taking the value true (.T.) when the event occurs (Fig. 3).

$€_0(t) = .T.$

During the design phase, the IM designers must apply given acceptance criteria and processes for reduction of the complete set of hazards to be handled in the following IM design process.

3.2 *Barrier function performance*

Traditionally, a safety function or a barrier function is referring to all elements needed for performing risk reduction. A pressure protection system (barrier) may have a sensor (e.g. pressure transmitter), a logic controller, and an actuating device (e.g. valve) which will reduce the pressure (physical risk) when the sensor is measuring an operating pressure above a given limit.

As an IM related example, consider the design of a barrier system with two barriers (A and B) for observing and alerting the protected unit about possible approaching sea ice.

The IM plan typically define 3 zones (Fig. 4) around the protected unit:

1. Zone 1 is secure zone with radius a.
2. Zone 2 is management zone.
3. Zone 3 is monitored zone.

Barrier A is based on a satellite with ice surveillance functionality. In the case that ice is entering Zone 2 from Zone 3, an orderly disconnect (ODC) alert shall be submitted to the protected unit. The protected unit should then initiate procedures for terminating critical activities and start disconnection of systems connected to the sea bed. The performance of barrier A is initially not proved sufficiently high. Hence, according to the safe learning principle, there is a need for extra high contingency (EHC) measures and a barrier B must be included.

Barrier B is based on a supply ship patrolling in Zone 2. The ship has ice detection radars specialized for identification of sea ice, and the crew are also watching for possible ice. In the case that ice floes are observed from the scouting vessel, the protected unit shall immediately be alerted (Fig. 5).

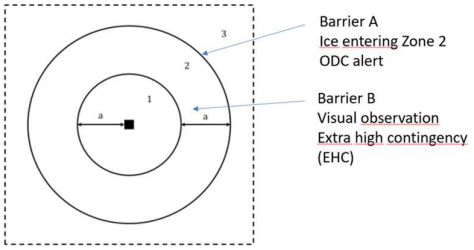

Figure 4. Ice zones for a MODU. 1: secure Zone, 2 : management Zone, 3 : monitoring Zone (ISO/FDIS 35104). Observation of ice entering Zone 2 shall trigger an ODC alert and this is considered as barrier A. Ice detection system and alerting in Zone 2 is considered as barrier B.

The overall IM system may consist of barriers denoted e.g. A, B, C… which initially are considered independent. This means that there are no common causes leading to simultaneous failures of A and B. Hence, it is assumed that:

- A failure cause leading to failure of barrier A will not cause barrier B to fail in the same manner.
- Failure of B shall not be a consequence of the failure effect of barrier A.

This means that the overall barrier system will alert correctly if either barrier A or barrier B will work correctly (Fig. 5).

The resulting events (€) from the barrier system design in Figure 5 can therefore be expressed by the Boolean equations:

$$€_1 = €_0 \cap F_A$$
$$€_2 = €_0 \cap \neg F_A \cap F_B$$
$$€_3 = €_0 \cap \neg F_A \cap \neg F_B$$

where

F_A= true; barrier A function on demand
F_A= false; barrier A is failing on demand
F_B= true; barrier B function on demand
F_B= false; barrier B is failing on demand
$\cap$: Boolean **AND** operator
$\neg$: Boolean **NOT** operator

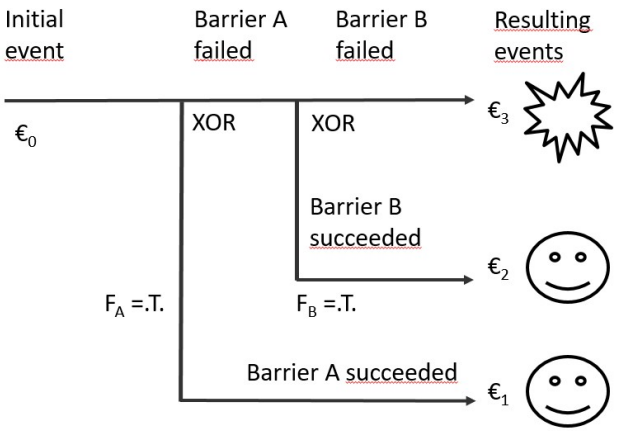

Figure 5. Barrier system event tree representing independent barrier A with function F_A and barrier B with function F_B. The overall barrier system will work as required if either barrier A or barrier B function. The barrier system will fail if both barrier function F_A and barrier function F_B fails.

The single failure criterion is the traditional type of qualitative functional acceptance criterion used by, e.g. classification societies in prescriptive technical rules for dynamic positioning (DP) system equipment classes 2-3 or for drilling systems (DNVGL-OS-E101, 2018). As the drilling and DP systems are parts of the IM scope, it is natural to start to cross-reference the requirement specifications of these systems to the traditional type of requirements.

In the previous example with barriers A and B, the overall barrier system will comply with the single failure criterion. The reason for compliance is that the two barriers A and B have to fail.

3.3 *Ambient and external conditions*

A technical barrier consist of several subsystems like detection, logic units, and actuating devices. All supporting and utility systems required for the barriers to work are also considered a part of the barrier. The barrier environment and connections to the other systems may also influence the vulnerability of a barrier. In order to organize and visualize these relations, the system boundaries (ISO 14224:2006) should be established. In this context 3 boundaries are described:

1. Barrier boundary, functional parts.
2. External connections and conditions.
3. Environmental and ambient conditions for barriers.

Assume that a Boolean F_A represents the function of barrier A where:

F_A= .T. (true); barrier A function on demand
F_A= .F. (false); barrier A is failing on demand

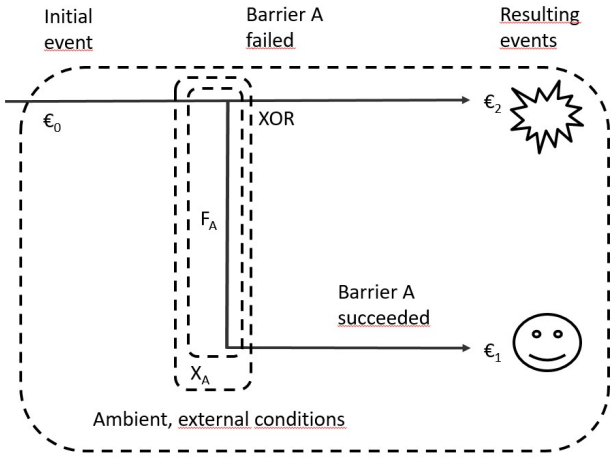

Figure 6. Barrier A will work if the functional part (F_A) is working when demanded and if the external conditions required are complied with (X_A).

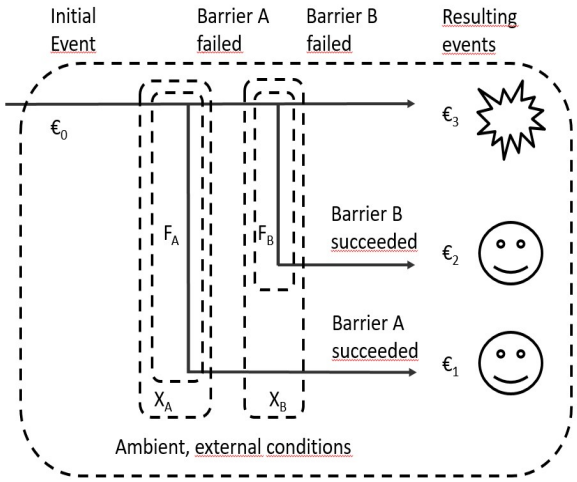

Figure 7. Barrier A will work if the functional part (F_A) is working when demanded and if the external (X_A) conditions required are complied with and similarly for barrier B. The overall barrier system will fail if both barrier A and B fails. Also, if the ambient conditions for both A and B are non-operable, the overall barrier system will fail.

Also assume that the function of barrier A is dependent on the state of external utilities or ambient conditions, denoted by a Boolean variable X_A where:

X_A= .T.; external/ambient state is workable
X_A= .F.; external/ambient state is not workable

The robustness of a barrier is the ability to function under relevant external conditions at the demand situation (Fig. 6).

The barrier robustness may also be denoted as survivability or vulnerability (Hauge, S. & Øien K. 2016). Robustness and survivability can be related to X(t)= .T., and vulnerability can be related to X(t)=.F..

3.4 *Functional and external performance*

The Barrier A Succeed on Demand (BSD_A) if both the function of the barrier and the external conditions are operable. Let $X_A(t)$ and $X_B(t)$ be Boolean variables for external conditions for barriers A and B.

Then

$BSD_A = (F_A \cap X_A)$; barrier A will work
$BSD_B = (F_B \cap X_B)$; barrier B will work

This means that the barrier system of A and B will work (refer to lower branch in Fig. 7) on demand on the initial event (€0) according to:

$$€_1 = €_0 \cap F_A \cap X_A$$

or if (refer to middle branch in Fig. 7):

$$€_2 = €_0 \cap \neg(F_A \cap X_A) \cap (F_B \cap X_B)$$

The barrier system will fail to protect the unit (represented by upper branch in Figure 7 if the following event occurs:

$$€_3 = €_0 \cap \neg(F_A \cap X_A) \cap \neg(F_B \cap X_B)$$

The €3 event represents a hazardous event and the corresponding consequence of the IM barrier system for the protected unit. The analysis of the conditions for event €3 has to start with a screening of the Boolean functions for €0, F_A, X_A, F_B and X_B.

3.5 *Acceptance criteria for loss of protection*

The analysis process of the €3 event shall be based on a stated requirement or acceptance criterion for loss of protection by the given function and ambient conditions of the barrier system.

Acceptance criterion scope: {F_A, X_A, F_B, X_B}.
Acceptance criterion: No single failure in the acceptance scope shall lead to loss of protection of PU.

The loss of protection condition is given by:

$$€_3(t) = .T.$$

meaning that loss of protection will occur if:

$$€_0 \cap \neg(F_A \cap X_A) \cap \neg(F_B \cap X_B) = .T.$$

Therefore, the task is to find possible solutions of this equation.

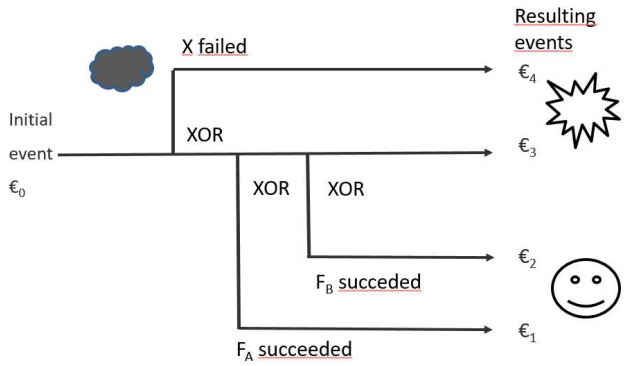

Figure 8. External effect $X=X_A=X_B$ may cause simultaneous failures of barrier A and B. This means that $X_A=X_B$ is a single condition that will not comply with the single failure acceptance criterion, although the functional (F_A, F_B) parts of barrier A and barrier B and X are independent.

Ideally the Boolean variables $€_0$, F_A, X_A, F_B and X_B should be independent, and the barrier variables should be true (.T.). In such cases it can be shown that there are no single failure (e.g. X_A=.F.) giving loss of protection such that $€_3(t) =$ .T..

In reality, the independence claim of the above variable set has to be analyzed and justified. In practice, such analysis could be a kind of FMEA or hazard identification in order to identify possible dependencies or common causes that may give $€_3(t) =$ .T..

In the case that the external requirements (e.g. visibility) for barriers A and B are equal:

$X = X_A = X_B$ = .F.

then both barriers A and B will be affected simultaneously by the common condition cause X.

By elaborating the Boolean expressions by means of standard Boolean algebra laws for the branches in Figure 7, it may be shown that the event tree may be reorganized as shown in Figure 8. The resulting events (note new numbering of events 3 and 4) will occur given the following conditions:

$€_1 = €_0 \cap F_A \cap X$

$€_2 = €_0 \cap \neg F_A \cap F_B \cap X$

$€_3 = €_0 \cap X \cap \neg F_A \cap \neg F_B$

$€_4 = €_0 \cap \neg X$

By inspection of the equations above, event $€_4$ will be the result of $€_0$ and a single non-compliance of the external factor X (e.g. no visibility).

This means that the barrier system design is not complying with the given acceptance criterion which

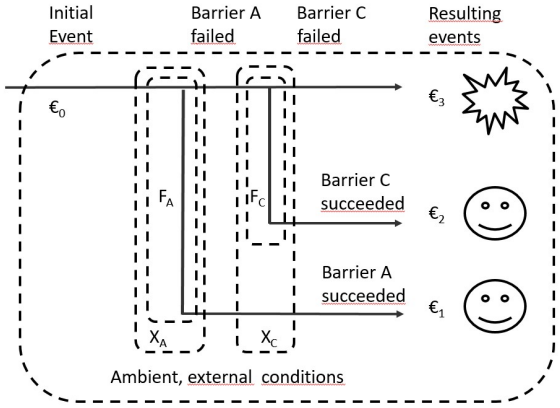

Figure 9. External effects $X_A \neq X_C$ are independent and will not cause simultaneous failures of barriers A and C. The single failure criterion for the barrier system A and C is now complied with.

states that the barrier system shall not fail due to a single failure or non-compliance.

Generally, the single failure criterion will require two independent barrier functions in the system. It must be verified that the claimed independent barriers do not contain functional relations which may reduce the number of independent barriers, as was shown in the previous example.

Continuing our example, since barriers A and B are dependent, the barrier B is exchanged with a new barrier C for which the ambient conditions X_C are different than for the A barrier. The cost for the C barrier is significantly higher than the B barrier, but at the decision point it is decided to start operations with this configuration (Fig. 9).

It is also decided to record compliance and non-compliance with respect to ambient conditions related to requirements X_A, X_B and X_C, in the initial operation phase, in order to find the real operational performance of the barriers in the given environment.

3.6 *Reducible dependent barrier systems*

A barrier system design may consist of e.g. 3 independent functions or conditions (U, V, W) and 6 resulting events (refer to Fig.10). The barriers may be working with independent functions or external conditions (represented by Boolean variables e.g. U, V, W and functions). These functions and conditions may be combined and influence the outcome of several branches of the designed barrier system, leading to possible dependencies or impossible outcomes.

The general rule for confirming the independence of one barrier branch is that the expressions for the resulting event is such that no barrier functions or external conditions (U,V,W) are used more than once.

Example for resulting event €$_1$ in Figure 10 is based on:

$$€_1 = W \cap V \cap U$$

Here, €$_1$ is consisting of single use of independent functions, and therefore the expression for the resulting event is independent.

Resulting event €$_2$:

$$€_2 = W \cap V \cap \neg U \cap W$$

is the result of 4 barrier branches, and it is referring to W two times making the expression dependent. By the Boolean algebra identity law stating

$$W \cap W = W$$

the dependent expression is reduced to an independent expression for the resulting event €$_2$:

$$€_2 = W \cap V \cap \neg U$$

The assumed resulting events:

$$€_3 = W \cap V \cap \neg U \cap \neg W = 0$$
$$€_4 = W \cap \neg V \cap U \cap V = 0$$

can never occur due to the Boolean algebra law for complementation, stating:

$$W \cap \neg W = 0 \text{ and } \neg V \cap V = 0$$

The resulting event €$_5$:

$$€_5 = W \cap \neg V \cap U \cap \neg V$$

can be reduced to (note that €$_4$ is impossible)

$$€_5 = W \cap \neg V \cap U$$

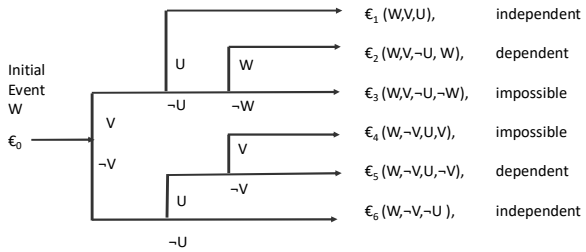

Figure 10. The initial event is dependent on external factor W and the barrier system tree has 5 barriers and 6 resulting events. The barrier functions U, V, W are independent. The resulting events €$_1$ and €$_6$ are based on the states of independent factors and functions. The resulting events €$_3$ and €$_4$ are based on negated dependent factors and might never occur. Resulting events €$_2$ and €$_5$ are based on repeated use of the same barrier function or external condition.

€$_6$ contains 3 Boolean independent conditions:

$$€_6 = W \cap \neg V \cap \neg U$$

The effects of the dependencies may either improve the overall performance of the barrier system, which could be achieved by e.g. applying operational predictions or forecasts to influence the barrier system to come out with the most favorable resulting events and associated consequences.

On the other hand, common causes may affect the initiating event and several barriers simultaneously, which may degrade the overall performance significantly by influencing the barrier system outcome adversely with less favorable resulting events and consequences.

Possible dependencies between the events in the barrier system may give the IM designer options to avoid events which are reducing the performance of the barrier system, or, on the other hand, to apply possible dependencies (e.g., prediction of the future) to improve the overall performances.

This indicates that special identification and analyses of common causes and dependencies for multiple barriers should be subject to further development of qualitative methods for barrier systems. Reference is made to similar practice where the industry use FMEA as a method for barrier analysis of redundant systems, e.g., for DP systems and redundant propulsion (DNV-RP-D102, 2012).

4 DETAILED BARRIER PERFORMANCE REQUIREMENTS

4.1 *On-demand and continuous performance models*

The on-demand modelling approach is assuming that there will be:

- few ice occurrences per season in the monitored area, and
- sufficient warning time from an ice alert is issued until the ice arrives the protected unit.

An ice occurrence in the monitored area will generate a specific demand on the ice management system, and consequently initiate a sequence of events. An event tree analysis modelling approach is considered in this paper. This on-demand method may be used in the flight mode ice management philosophy. Traditionally, the on-demand mode is generally applied in offshore risk analyses and barrier modelling (IEC 61508, 2010).

In the case where ice presence must be assumed to be continuous, the physical ice management (ice fighting) must be required to operate continuously in periods. This case of ice regime with a possible continuous ice fighting mode is not within the scope of this paper. The continuous ice fighting operation has similarities with requirements to and verification of e.g. maritime propulsion systems, dynamic positioning systems, and heave compensation for drilling systems.

4.2 *Barrier functional types*

IM systems and activities are covering a wide range of types of barriers and events. The outcome of resulting events could be:

1) Ice observations (observed/not observed)
2) Ice predictions (predicted/not predicted)
3) Ice alerting (alerted/not alerted)
4) Ice breakability (breakable/not breakable)
5) Physical ice management (ice broken/not broken)
6) Ice alerting after physical ice management (confirmed ice broken/failed to break ice)
7) Ice arrived in Zone 1.
8) Disconnection (disconnected/connected)
9) Move off (moved off/still at site)

The above events may be modelled as resulting events in barrier event trees, where the actual outcome will be governed by the state of the barrier function when the barriers are demanded.

From the list above, one observes that the nature of the barriers may be classified in at least the following types:

a. Ambient physical events
b. System and functional/failure events
c. Operational ice observations events
d. Operational ice predictions events
e. Operational decisions/commands events

A barrier succeeds on demand (BSD(t)) when the barrier functional requirements are fulfilled at the time t of the demand:

$$BSD_A(t) = (F_A(t) \cap X_A(t))$$

which is fulfilled (.T.) when

$F_A(t)$ = .T. and $X_A(t)$ = .T.

The detailed conditions for the successful function (F_A) will most often consist of a combination of many parameters.

In the top-down IM design/decision process, the IM designer should initially try to avoid detailed functional modelling of the barriers if a decision process on a high level information is sufficient to reach the acceptance criteria.

But if it is deemed necessary to go into details of a barrier, the detailed functional and ambient variables can be modelled as a kind of 'Safety Requirement Specification' found in IEC 61508 (IEC 61508), which is recommended by PSA for safety systems (PSA 2017). The functional requirements to F_A in the above example is similar to the Safety Requirements Specification (SRS) applied in IEC 61508.

4.3 *Functional and ambient variable requirements*

Detailed functional requirements for a traditional pressure safety function could be expressed by a Boolean safety requirements specification (SRS), according to:

F_A = (Tank pressure above 20 bar) ∩
(Detected overpressure within 2 s) ∩
(Safety valve closed within 3 s)

In this simplified example for F_A, the target reliability (SIL: Safety Integrity Level from IEC 61508) is not included.

The tank external conditions are required to fulfil the following requirements:

X_A = (-30ºC < Air temperature < 50ºC) ∩
(Incoming fluid viscosity less than Z) ∩
(Incoming fluid not contaminated by sand)

An IM example could be vessel-based ice surveillance functional and external variable requirements:

F_A = (Ice floe size > 10 m) ∩
(Distance to ice floe > 2 km) ∩
(Vessel with detector movements < Z) ∩
(Stable power supplies and communication)

X_A = (Visibility > 2.5 km) ∩
(Wave height < 1.5 m)

4.4 *Boolean operational prediction functionality*

Ice prediction barriers are relating to the functionality to predict correctly if an ice hazard may occur before the ice arrival actually occurs.

The initiating event $€_0$ may be a request for a prediction at t_0 for the future period t_1-t_2. This type of prediction can enable the operational decision maker to start correctly orderly disconnection (ODC) procedures at t_1 in order to be completed at t_2.

The Boolean prediction function F is specified by

$$F = F(X_D(t_1), X_R(t_2))$$

where $X_D(t_1)$ is Boolean variable for the observed environment at t_1, and $X_R(t_2)$ is a Boolean variable for the requested external condition at t_2 (see Fig. 11).

Requirements to observations (deterministic) of the ambient conditions during the lag time period (t_0-t_1):

$$\begin{aligned} X_D(t_1) = \; & (\text{Ice floe size} < 10\ \text{m}) \cap \\ & (\text{Optical visibility} > 2.5\ \text{km}) \cap \\ & (\text{Wave height} < 1.5\ \text{m}) \cap \\ & (\text{Sea current} < 0.5\ \text{m/s}) \end{aligned}$$

Note that the optical visibility in the example above is a requirement to the ambient conditions necessary for doing the prediction function F.

Required ambient condition at t_2 to the forecaster at t_1

$$\begin{aligned} X_R(t_2) = \; & (\text{Ice floe size} < 10\text{m}) \cap \\ & (\text{Wave height} < 1.5\ \text{m}) \cap \\ & (\text{Sea current} < 0.5\ \text{m/s}) \end{aligned}$$

Observed (deterministic, D) ambient condition at t_2 by protected unit

$$\begin{aligned} X_D(t_2) = \; & (\text{Ice floe size} < 10\ \text{m}) \cap \\ & (\text{Wave height} < 1.5\ \text{m}) \cap \\ & (\text{Sea current} < 0.5\ \text{m/s}) \end{aligned}$$

The prediction functionality is according to requirements if the operable ice condition in [t_1 –t_2] was predicted at time (t_1). There are four resulting events ($€_1$, $€_2$, $€_3$, $€_4$) where this is of special interest (DNMI 1979).

Optimism justified, the prediction at t_1 stated acceptable condition at t_2 (F=true, optimistic) which actually was fulfilled at t_2.

$$€_1 = €_0 \cap F(X_D(t_1), X_R(t_2)) \cap X_D(t_2)$$

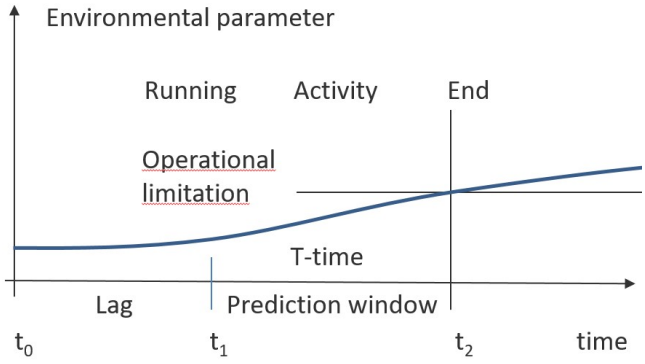

Figure 11. The correct prediction at t_1 in the figure is $€_4$ Pessimism Justified. At time t_1 the forecaster is requested to give a prediction for a prediction window starting at t_1 and ending at t_2 in order to start disconnection at t_1 if critical environmental parameters will exceed the stated limitation. The T-time is the required time for termination of the critical operation with environmental limitation.

Pessimism justified, the prediction at t_1 stated non-acceptable conditions t_2 (F=false, pessimistic) and this pessimistic situation actually occurred at t_2, or

$$€_4 = €_0 \cap \neg F(X_D(t_1), X_R(t_2)) \cap \neg X_D(t_2)$$

In the example in Figure 11 the Pessimism Justified is the correct prediction type and it was correct to start the orderly disconnect (ODC) procedure at t_1.

In the case that the predictions were not correct, we denote this as failure modes (ISO 14224:2006) of the prediction function.

Too optimistic, the prediction at t_1 stated acceptable conditions (F=true, optimistic) and this required situation actually did not occur at t_2

$$€_2 = €_0 \cap F(X_D(t_1), X_R(t_2)) \cap \neg X_D(t_2)$$

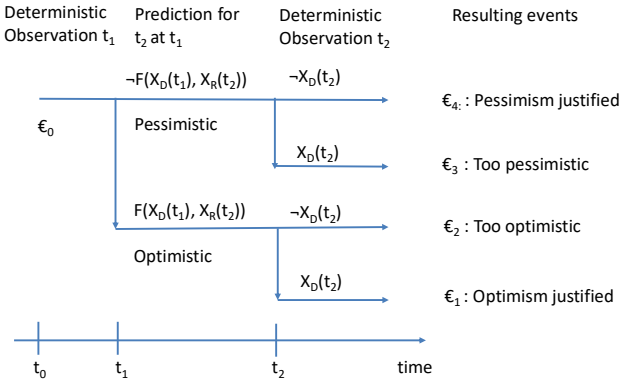

Figure 12. Event tree for representation of 4 resulting events for the prediction function F.

Too pessimistic, the prediction at t_1 stated non-acceptable conditions (F=false, pessimistic), but the required situation actually occurred at t_2

$$€_3 = €_0 \cap \neg F(X_D(t_1), X_R(t_2)) \cap X_D(t_2)$$

The prediction function F is not testable or verifiable at the time of prediction or alerting (t_1), but it is observable and testable after the prediction window (t_2) has elapsed. Hence, it is important to log the input and output data for such prediction function in order to get statistics on its performance over time. This can then be used to improve its performance, replace it, or include an additional prediction barrier in a new design decision.

5 PROBABILISTIC BARRIER PERFORMANCE

5.1 *Probabilistic integrity of barrier function*

The integrity of a barrier function may be defined as the ability to function when needed. The integrity of the barrier function F_A may be expressed by the probability of success on demand at $t=t_d$:

$$PSD\ (t_d) = P(F_A(t_d))$$

and probability of failure on demand:

$$PFD\ (t_d) = P(\neg F_A(t_d))$$

Referring back to the example given in Figure 5 with independent barriers A and B, the probabilities of the resulting branch events can be estimated by:

$$€_1 = €_0 \cap F_A$$
$$€_2 = €_0 \cap \neg F_A \cap F_B$$
$$€_3 = €_0 \cap \neg F_A \cap \neg F_B$$

$$P(€_1) = P(€_0) \cdot P(F_A)$$
$$P(€_2) = P(€_0) \cdot P(\neg F_A) \cdot P(F_B)$$
$$P(€_3) = P(€_0) \cdot P(\neg F_A) \cdot P(\neg F_B)$$

5.2 *Probabilistic robustness or survivability*

The robustness (survivability or vulnerability) of the barrier is the ability to function under relevant external conditions at the demand situation.

The probabilistic robustness of the barrier external conditions X may be expressed by the probability that external conditions are complying with the requirements to the environment at $t=t_d$:

$$PSD\ (T_d) = P\ (X(t_d))$$

and probability of failure of robustness on demand:

$$PFD\ (T_d) = P\ (\neg X(t_d))$$

The combined requirements of both functional F_A and external requirements X at demand may be expressed as:

$$BSD_A = (F_A \cap X)$$

and assuming that F_A and X are independent, the probability of success on demand of the barrier A can be expressed as:

$$PSD_A = P(F_A \cap X) = P(F_A) \cdot P(X)$$

Please refer back to example Figure 6. For event trees with common causes (X_A, X_B), we get:

$$€_1 = €_0 \cap (F_A \cap X_A)$$
$$€_2 = €_0 \cap \neg(F_A \cap X_A) \cap (F_B \cap X_B)$$
$$€_3 = €_0 \cap \neg(F_A \cap X_A) \cap \neg(F_B \cap X_B)$$

and assuming $X = X_A = X_B$ the probabilities for the resulting events can be expressed by:

$$P(€_1) = P(€_0 \cap (F_A \cap X))$$
$$P(€_2) = P(€_0 \cap \neg(F_A \cap X) \cap (F_B \cap X))$$
$$P(€_3) = P(€_0 \cap \neg(F_A \cap X) \cap \neg(F_B \cap X))$$

In the case that automatic tools should calculate above estimates, it should be noted that the two lower branches are statistically dependent due to the two occurrences of X in the two branches. Hence, the probabilities for the Boolean expressions for $€_2$ and $€_3$ can not be calculated in the same manner as shown in Section 5.1. The Boolean expressions have to be reduced by application of standard Boolean algebra laws for distributivity, identity and complementation in the same way as shown in Section 3.5, leading to:

$$P(€_1) = P(€_0) \cdot P(F_A) \cdot P(X)$$

$$P(€_2) = P(€_0) \cdot P(\neg F_A) \cdot P(F_B) \cdot P(X)$$

$$P(€_3) = P(€_0) \cdot P(X) \cdot P(\neg F_A A) \cdot P(\neg F_B)$$

$$P(€_4) = P(€_0) \cdot P(\neg X)$$

where we note that the expressions for the 4 resulting events are based on single use of each independent variable F_A, F_B, and X.

Calculation of the expected performance probabilities have to take into consideration the differences between Boolean and ordinary algebras.

5.3 *Probabilistic operational predictions*

The probability of the Boolean expressions for the resulting events for the 4 types of prediction resulting events are:

Probability of optimism justified:
$P(€_1) = P(€_0 \cap F(X_D(t_1), X_R(t_2)) \cap X_D(t_2))$

Probability of pessimism justified:
$P(€_4)=P(€_0 \cap \neg F(X_D(t_1), X_R(t_2)) \cap \neg X_D(t_2))$

Probability of too pessimistic:
$P(€_3)= P(€_0 \cap \neg F(X_D(t_1), X_R(t_2)) \cap X_D(t_2))$

Probability of too optimistic:
$P(€_2)=P(€_0 \cap F(X_D(t_1), X_R(t_2)) \cap \neg X_D(t_2))$

It should be noted that the Boolean expressions may contain dependent elements, and that the effects of the dependencies must be handled in the probability estimates.

Estimates of the prediction probabilities may be produced by comparing time series of environmental data X_D required to be predicted and time series of actual predictions F according to required conditions X_R for a given location.

6 EXPECTED CONSEQUENCE AND RISK

Assume that the consequences £ associated to the resulting events € are $€_1$: $£_1$, $€_2$: $£_2$, $€_3$: $£_3$ (Fig. 13).

The expected consequences or risk of the barrier system may then be defined as:

$$R = P(€_0) \cdot \sum_{i=1}^{3} P(€_i) \cdot £_i$$

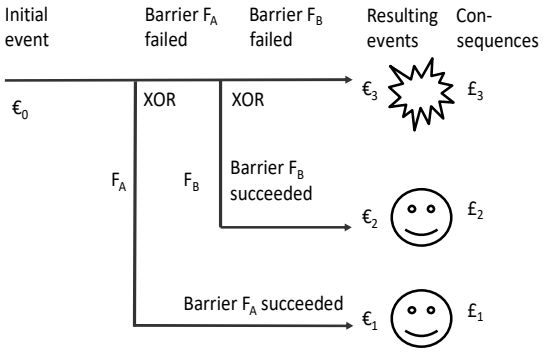

Figure 13. Resulting events $€_1$, $€_2$, and $€_3$ with associated consequences $£_1$, $£_2$, $£_3$.

Expected consequences and risk can be used for estimating residual risk of the barrier system and such estimates can be used as a basis for design decision-making at top-level or at sub-levels according to the stated acceptance criteria.

7 PLANS FOR IM DESIGN CASE STUDY

The descriptions given in previous sections are based on some of the ongoing research and development in the SAMCoT program. A plan for validating the applicability of the IM performance models for design decisions is developed (Fig. 14).

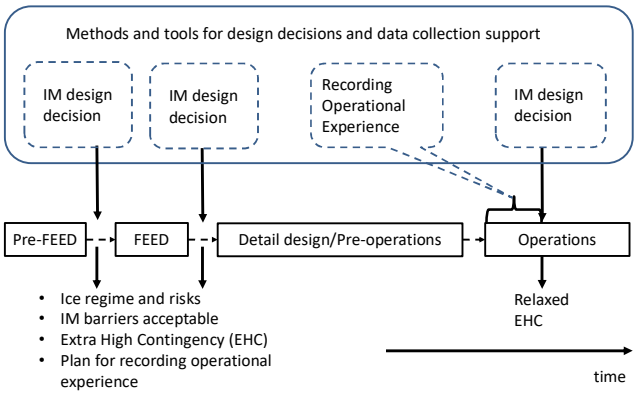

Figure 14. The first IM design decision establishes ice regime and risks, IM barriers system performance, Extra High Contingency compensating for initial uncertainties and a plan for recording operational experience according to stated acceptance criteria. The IM design decision during operations may relax the extra high initial contingencies based on recorded experience.

The following topics are considered to be included in the planned study case:

- The ice regime model, assuming an on-demand IM flight response.
- IM design acceptance criteria including acceptable uncertainties with qualitative and quantitative models.
- Establishment and analysis of initial IM barrier system, including extra high contingencies at first design decision in pre-Feed/Feed phase.
- Proposals for improved IM barrier system at design decision after initial operations.
- Identifying the detailed need for collection of operational experience data during the initial operations (Fig. 14).
- Collection of the operational data.
- Conclusion on relaxation of EHC at design decision.

The study case and demonstration is proposed to be presented in 2019.

8 SUMMARY AND CONCLUSIONS

A top down method for modelling ice hazard and barrier performance for IM is presented as ongoing research in SAMCoT. The model is covering the demand mode and the flight mode of ice management. The model is flexible and modular and may be used for qualitative (Boolean) and quantitative (probabilistic) acceptance criteria. The model is flexible with regard to the level of details in the barrier descriptions, and it starts with a Boolean model of barrier performance which may be detailed with analysis of common cause failures and/or probabilistic functional performance. The failure modes for on-demand ice prediction are proposed and defined with probabilities.

The IM model is a natural extension to existing regulations, theories and practices in the O&G industry and the maritime industry. The model is planned to be further developed, tested and validated in study case and demonstrators.

9 ACKNOWLEDGMENTS

The authors would like to thank the Research Council of Norway (RCN) for financial support through project no. 203471 CRI SAMCoT.

10 REFERENCES

DNV-RP-D102: 2012, *Recommended Practice: Failure mode and Effect Analysis (FMEA) of Redundant Systems, 2012*

DNVGL-OS-E101: 2018, *Drilling facilities, Offshore Standards, 2018*

DNMI 1979, Table with estimates of '*Confidence tag forecast ing Statfjord 1979'*

Eik, K. J. 2010, *Ice Management in Arctic Offshore Operations and Field Developments, Doctoral Thesis NTNU*

Hauge, S. & Øien K. 2016, *Guidance for barrier management in the petroleum industry, 2016-09-23, SINTEF A27623*

ISO 14224:2006 -- *Collection and exchange of reliability and maintenance data for equipment* Petroleum, petrochemical and natural gas industries

ISO/FDIS 35104 2017, *Petroleum and natural gas industries — Arctic operations — Ice management*

IEC 61508-2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems -*

070 – NORWEGIAN OIL AND GAS 2004, *APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY, Norwegian Oil and Gas Association*

PSA 2017 *The Management regulations, 2017, Petroleum Safety Authority of Norway (PSA)*

Haimelin R., Goerlandt F., Kujala P., Veitch B. *Implications of novel risk perspectives for ice management operations,* Cold Regions Science and Technology, Volume 133, January 2017, Pages 82-93

Ruud, S. & Skjetne, R. 2014. "*Verification and Examination Management of Complex Systems". Journal of Modeling, Identification and Control,* 2014, Vol 35, No 4, pp. 333-346.