Polski Rejestr Statków

INFORMATIVE PUBLICATION NO. 19/I

FORMAL SAFETY ASSESSMENT METHODOLOGY
(FSA)

2002

Publications I (Informative) are issued by Polski Rejestr Statków S.A.
as guidance or explanatory notes to PRS Rules

GDAŃSK

Informative Publication No. 19/1 – Formal Safety Assessment Methodology (*FSA*), 2002, was approved by the Director for Ship Classification of the Polish Register of Shipping P.L.C. on 7 November 2002.

PRS/AW,12/2002

CONTENTS

1 INTRODUCTION

In many fields of industry and transport, mainly in the so called high risk areas, probability risk assessment methods are applied. In shipping industry they are called Formal Safety Assessment (FSA). In this *Publication*, the formal safety assessment method based on the guidelines developed by IMO is presented.

1.1 FSA Aim

FS aim is to facilitate the processes of safety management and standardisation and establishing the policy of safety-oriented activities. The method is universal and may be utilised as an aid tool in decision making not only during legislation but also during such processes as the ship design, classification, construction and service. In respect of ship technical requirements, the method is suitable both an individual ship and ship types, e.g. bulk carriers, high speed craft etc.

1.2 Definitions

Accident (A) – unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage.

Accident category (AC) – designation of accidents reported in statistical tables according to their nature, e.g. fire, collision, grounding, etc.

Consequence (C) – accident outcome.

Frequency (F) – number of occurrences per unit time (e.g. per year).

Hazard (H) – potential to threaten human life, health, property or the environment.

Initiating event (IE) – the first of a sequence of events leading to a hazardous situation or accident.

Risk (R) – the combination of the frequency and the severity of the consequence.

Risk control measure (RCM) – a means of controlling a single element of risk.

Equivalent fatality (EF) – 100 minor injuries or 10 severe injuries are equivalent to one fatality. Severe injury is considered when the person injured requires hospital treatment.

The above terms constitute the set of ideas used for determining the nature of safety and its management.

2 METHODS USED FOR IDENTIFICATIONS OF HAZARDS AND RISK ANALYSIS

2.1 Hazard and Operability Studies (HAZOP)

The studies use key words to prompt the team of experienced specialists to identify potential hazards related to a single component of equipment or the whole system. Key words describe potential deviation from the required condition, using such terms as: high, low, yeas, no, etc. to describe the process parameters, e.g. flow, pressure, temperature, etc. By brainstorming, specialists determine potential consequences of a deviation and, if found reasonable, they enter such consequences in the hazard list. This type of analysis is generally used to analyse technical systems and it generates main qualitative results. Exemplary applications of HAZOP technique are shown in Table 2.1.1.

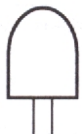
Table 2.1.1 Analysis of steam generating system operation hazards

Item	deviation	occurrence	fault	means of protection	recommendations
1. Fuel oil supply					
1.1	No flow	Burner incorrect operation	Fuel supply pump damaged	Redundant pump	Redundant pump to be supplied by a separate circuit
1.2	Low pressure		Clogged fuel filter	Periodical replacement of filter	Pressure check behind filter
2. Water supply system					
2.1	…	…	…	…	…

2.2 Fault Tree Analysis (FTA)

Fault Tree is a logic diagram showing the causal relationship between events to indicate logic relations between equipment failures, human errors and external causes which may contribute to the failure types under consideration. Fault Tree Analysis may be used for various applications, and is most effective in the analysis of failures caused by a combination of occurrences.

Symbol representing alternative – „or”



Symbol representing conjugation – „and”

Fig. 2.2.1 Symbols used in fault tree analysis

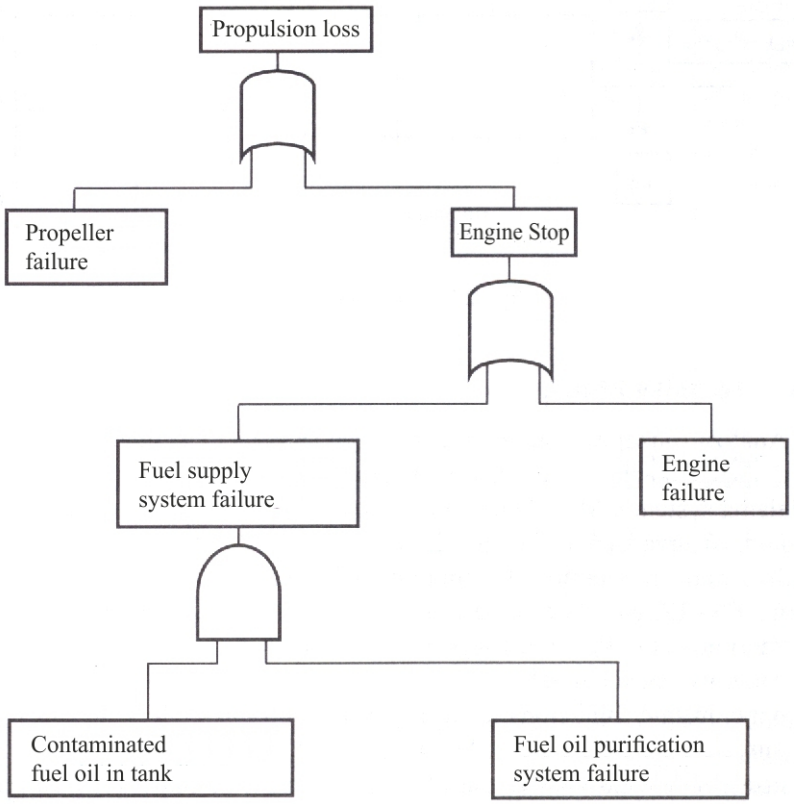


Fig. 2.2.2 Exemplary analysis with fault tree

2.3 Event Tree Analysis (ETA)

Event Tree is a logic diagram of the decision making tree used to analyse the effects of an accident. This type analysis may represent a qualitative description of potential problems (combination of a variety of problem resulting from the accident occurrence), and also a quantitative analysis of an occurrence frequency or probability. Event Tree may be applied to nearly all the possible

sequences of events, it is, however, the most effective to indicate all the possible accident effects. In Fig. 2.3, exemplary analysis showing the effects of steering gear failure in ship provided with an auxiliary steering gear.

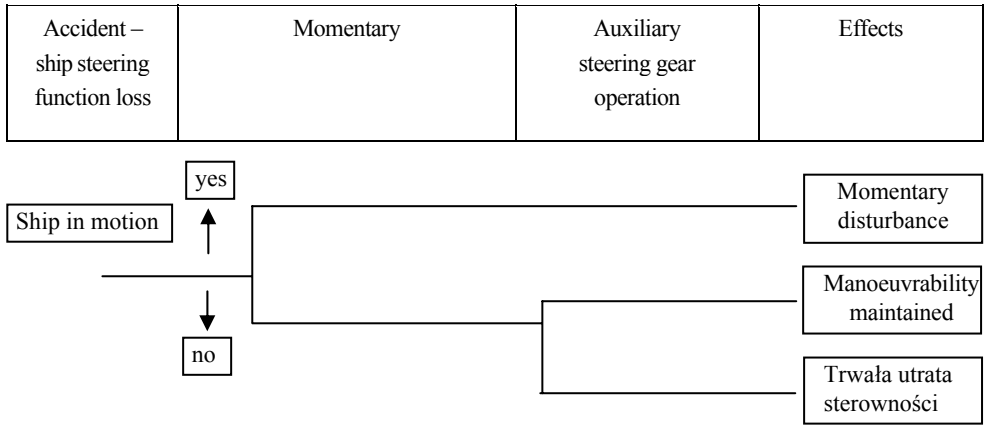


Fig. 2.3 ETA application

2.4 Failure Mode and Effect Analysis (FMEA)

FMEA is a technique used to identify failures of significant effect on the system operation effectiveness. It may be used to analyse the scale of failures of equipment made in different technologies. This enables an analysis of computer systems and human actions. FMEA is described in standard PN-IEC 812. Basic steps in FMEA are the following:

- defining the system and its basic functions, as well as minimum operational requirements;
- development of functional and reliability flow charts, other diagrams and/or models and mathematical descriptions;
- determining basic rules and respective documentation for the analysis;
- identification of failure types, causes and effects in respect of their significance and occurrence sequence;
- identification of methods and conditions for failure detection and isolation;
- identification of protective means, in the design and in operation, against particularly undesirable events;
- search for special combinations of group failures to be taken into account;
- recommendations.

Table 2.4 shows an exemplary application of FMEA for the compressed air system.

Table 2.4 FMEA application

System:		compressed air system				
System component:		compressor No. 1				
Analysed component:		compressor control system – start/stop related to air pressure – start: 2.0 MPa, stop: 2,6 MPa				
Failure type	Failure effects		Causes	Failure detection	Protection	Notes
	local	final				
does not start	low air pressure in the system	no air in the system	no power supply to compressor, damaged compressor power supply loop, damaged compressor starting control loop, damaged pressure sensor	power supply indication, air pressure management	control system failure indication system	consider application of redundant compressor with separate control system
does not stop	high air pressure in the system					

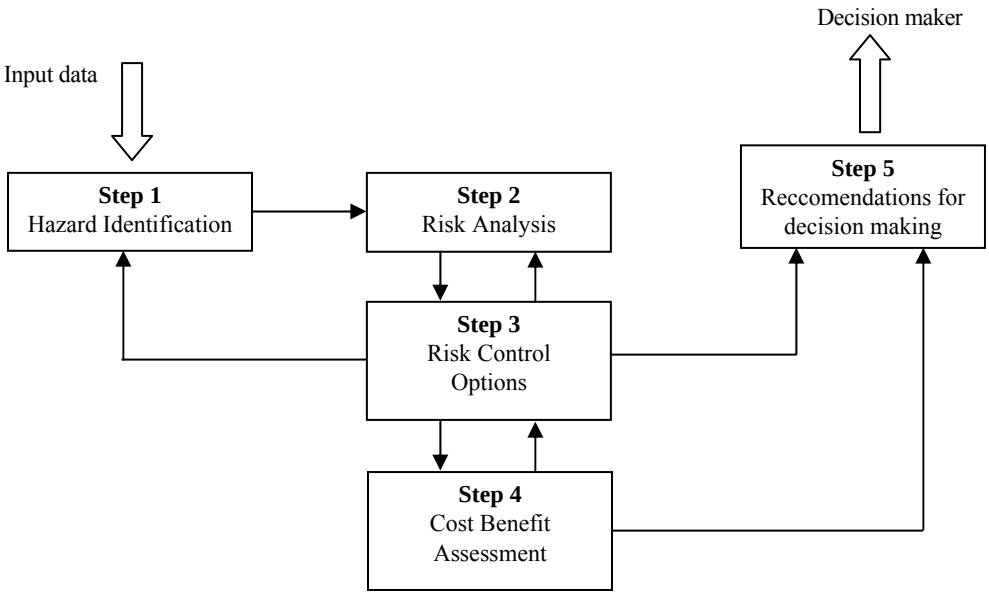
2.5 Human Reliability Analysis

The human element is one of the most important contributory aspects of technical system safe operation. Potential human errors of the operator and organisational negligence determine the risk level involved in an industrial facility operations. In the risk analysis such a facility should be considered as an social-and-engineering facility and human reliability should be taken into account. Human reliability analysis should be performed at the design stage of technical system and then verified during the system operation. An analysis of interaction between a human-operator and technical system in the foreseeable emergencies is particularly important. The Technique for Human Error Rate Prediction (THERP) is commonly used for that purpose.

3 FSA METHODOLOGY FLOW CHART

According to the *Draft guidelines for FSA application in the IMO rule-making process* (IMO MSC67/13, 1996), in the flow chart the following five steps are specified:

1. Hazard identification
2. Risk analysis.
3. Risk control options determination
4. Cost benefit assessment
5. Recommendations do decision making



4 HAZARD IDENTIFICATION

As hazards may lead to accidents and losses, risk analysis should begin with the identification and understanding of the associated hazards. Although hazard identification rarely contains data necessary for the decision making, it is a critical step in the risk analysis. It consists in listing crucial hazards as well as determining scenarios of elimination such hazards and the associated effects. Human factor and the environment impact should also be taken into account. Standard methods of hazard identification are presented in Chapter 2.

5 RISK ANALYSIS

Risk analysis is collecting data, by a detailed investigation of the events, and their synthesis to determine the level of risk associated with the system accidents. For that purpose, the following questions should be answered:

a) What may fail ?

b) What is the probability of such a failure ?
c) What is effect expected?

A qualitative answer to one or more questions often suffice to take the right decision. Where, however, more information is required for the analysis of cost benefit assessment regarding the decision taken, quantitative risk assessment (QRA) methods should be applied. In Fig. 5 risk assessment elements are shown.

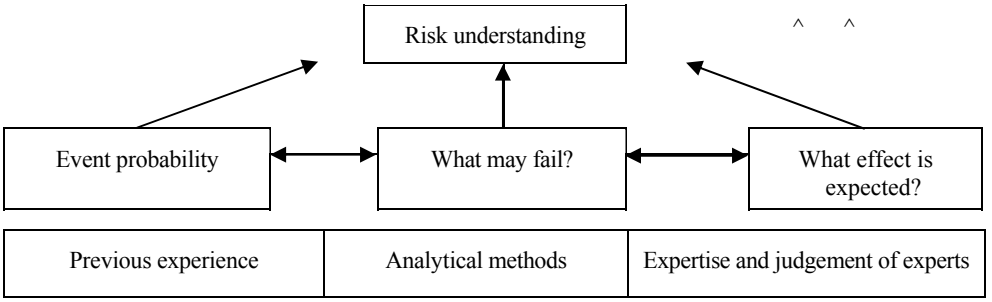


Fig. 5 Risk assessment elements

The most common risk analysis methods are given in Chapter 2. Irrespective of the technique chosen, it is recommended that in the hazard identification and risk analysis process both human and organisational errors be considered as significant contributors to many accidents, thus they should be taken into account in the hazard identification process. Risk analysis consists in qualitative and quantitative determination of accident risk and then their risk matrix. Quantitative risk analysis requires evaluation of the accident frequency and/or probability value(s) as well as the associated effects. The analysis and evaluation methods are also given in standard PN-IEC 60300 of June 1999.

5.1 Safety Criteria

Loss risk is a measure used for the object safety assessment. For the risk assessment, particular safety criteria should be adopted. These may be both qualitative and quantitative.

5.2 Qualitative Criteria

Qualitative criteria are presented in the risk matrix form where severity estimates are assigned to the pairs composed of accident frequency or probability and their effects. The procedure for the risk matrix construction is shown in the subsequent sub-chapters 5.2.1, 5.2.2 and 5.2.3.

5.2.1 Frequency Analysis

Frequency analysis is used to determine the accident frequency. The following three methods are commonly used:

a) The use of data on the previous occurrence frequency to be used as the base for their future occurrence estimate.

b) Occurrence frequency forecasting using such techniques as fault tree analysis or event tree analysis. Where previous experience are unavailable or inadequate, the occurrence frequency may be determined based on the system analysis and associated types of events. Then, in order to estimate the frequency the numerical data regarding all the respective events (including the equipment damage, human errors and external factors) should be linked. The analysis should take account of the possibility for the occurrence of damage resulting from the same cause, including simultaneous damage of a number of the system components.

c) Utilising experts' judgments.

Table 5.2.1 Effect severity criteria

Severity	Definition
Minor	Local equipment damage; single or minor injuries
Significant	Non-severe ship damage; multiple or severe injuries
Severe	Severe damage; single fatality or multiple injuries
Catastrophic	Total loss; multiple fatalities

5.2.2 Effect Analysis

Effect analysis covers the estimate of accident effects on Persons, property or the environment. The number of persons in various environments and at different distances from the event scene who are exposed to potential injury or fatality should be estimated. For the purpose of effect analysis, consequence models should be developed taking account of the accident type, as well as the release way of energy , toxic materials, fire etc. The analysis should be performed based on the methods specified in Chapter 2 or using simulation methods, e.g. Monte-Carlo simulation or other computation methods.

Table 5.2.2 Probability (frequency) criteria

Probability	Definition
Extremely remote	Accident scenario is highly unlikely.
Remote	Accident scenario is unlikely. Its occurrence would come much to one's surprise.
Reasonably probable	Accident scenario is likely. Its occurrence would not come to one's surprise.
Frequent	Accident scenario has occurred and/or is expected in the future.

5.2.3 Risk Matrix

In the risk matrix, columns represent the accident consequence severity, whereas lines – event probability/frequency. Inside the matrix, qualitative measures of risk severity (A, U, N) are indicated. The measures correspond to the decisions on risk acceptability. An exemplary risk matrix is shown in Table 5.2.3.

Table 5.2.3 Risk matrix

Frequency	Consequence			
	Minor	Significant	Severe	Catastrophic
Frequent	A	U	N	N
Reasonably probable	A	U	N	N
Remote	A	A	U	N
Extremely remote	A	A	A	U

Risk level:

A – acceptable risk
U – moderate risk
N – intolerable

5.3 Quantitative Criteria

Where a numerical value probability (frequency) is to be determined for the assessment of the requirements' compliance, the approximate values contained in Table 5.3.1 may be taken as useful guidelines for the common benchmark.

Table 5.3.1 Frequency index

Frequency	F
Frequent	$> 10^{-3}$ per year
Reasonably probable	$10^{-3} \div 10^{-5}$ per year
Remote	$10^{-5} \div 10^{-7}$ per year
Extremely remote	$10^{-7} \div 10^{-9}$ per year

Note: Various events may have different acceptable probabilities corresponding to the severity of their consequences.

5.4 Quantitative Risk Assessment (QRA) Methods

5.4.1 Risk Contribution Tree (RCT)

RCT models enable an analysis of risk distribution over the specific accident categories. For that purpose, each category is assigned a Failure Tree (FT) and an Event Tress (ET). FTs corresponding to accident causes are subject to being developed into the accident sub-categories to address the initiating events.

The following causes are distinguished:
- human error,
- technical unreliability,
- external events.

ETs correspond to the accident consequences and depend on the accident course. ET shows risk figures for each branch of the tree. Quantification of RCTs is based on historical data and/or expert judgments.

5.4.2 F-N Curves

In respect of fatality, its total risk can be expressed as F-N curves where F represents frequency related to 1000 ship-years, and N represents an equivalent number of persons affected. F-N curves are determined for the specific accident categories and then they are combined for all the categories.

The total risk indicated in all the branches of ET for all accident categories (AC) constitutes *potential loss of life* (PLL).

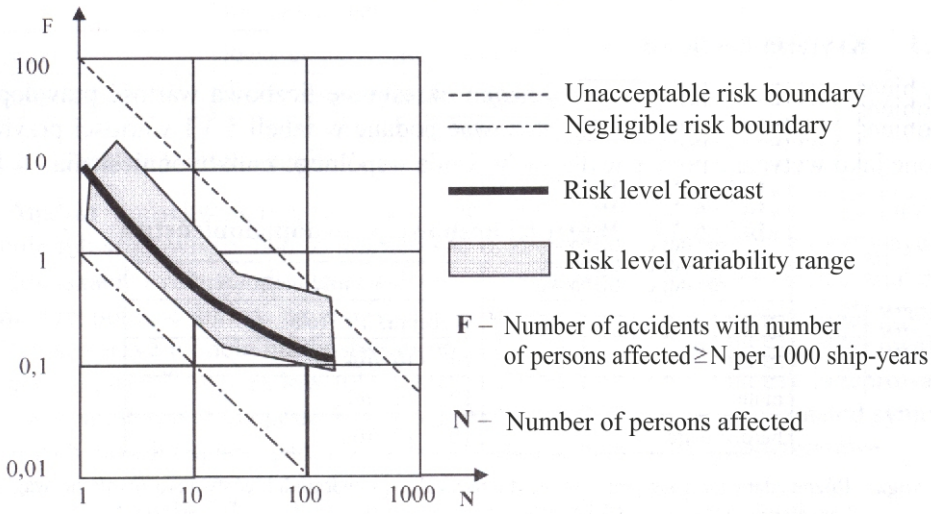


Fig. 5.4.2 F-N curves

5.4.3 Regulatory Impact Diagram (RID)

The purpose of RID approach is to determine and estimate the regulatory and organisational and other influences of the risk level. The RID idea is shown in Fig. 5.4.3.

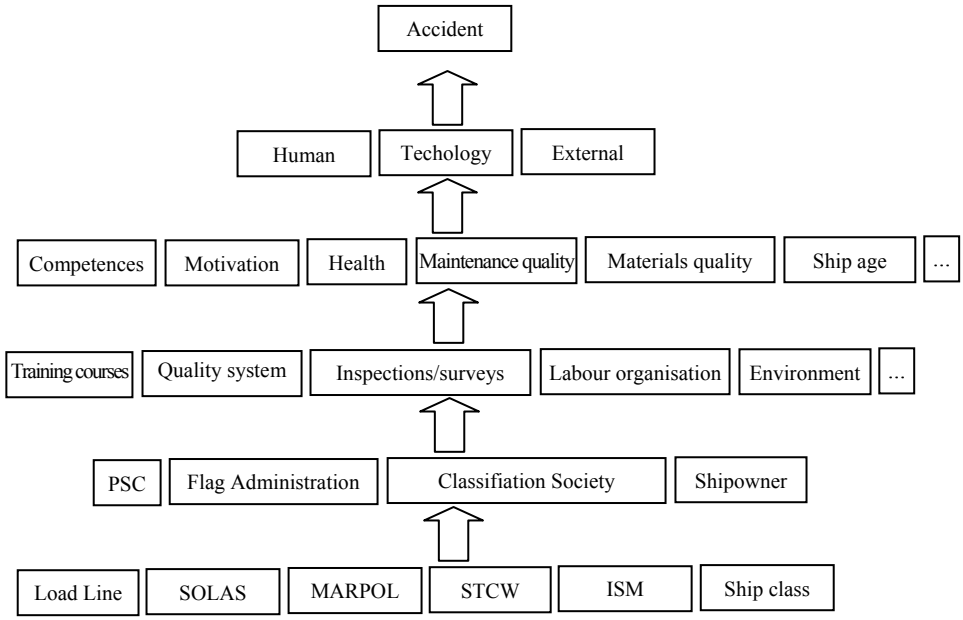


Fig. 5.4.3 Regulatory Impact Diagram

In the figure, levels are marked with numbers 1÷6 where particular characters correspond to the following levels:

1 – Political level
2 – Regulatory regime
3 – Organisational level
4 – Direct level
5 – Failure level
6 – Event level

Diagram modelling consists in determining structural links between particular influence factors (IF) shown as rectangulars at all the levels in the picture. Specific IFs are assigned rating values „r^{E}". Those are subjective marks given by experts out of three-grade scale: 0 – negative, 0.5 – neutral, 1 - positive. Particular relations are assigned, by experts, weighting values „w^{E}" out of the interval <0,l>. Factors w^{E} represent relative influence of lower level factors on higher level factors. The sum of weights of the relations between a particular influence factor must always be equal to 1.0. For all the IFs at level 2 calculated rating from below is determined in accordance with the following formula:

$$r2j^{C} = \sum_{i=1}^{n} w1i \times r1i \;,\; j = 1.2,...n, \qquad (5.4.3.1)$$

and then calculated rating *r2j* :

$$r2j = 0.5\ [r2j^{C} + r2j^{E}],\ j = 1.2,...n, \qquad (5.4.3.2)$$

to be used in calculations at level 3. Following this procedure, the event level is reached.

At that level, only formula 5.4.3.2 is used, and the ratings are named as: influence diagram index – I and their uncertainty is to be determined.

6 DETERMINING RISK CONTROL OPTIONS

Based on the risk estimate, areas requiring risk control are to be determined taking account of the following:

1. high level of risk;
2. high level of accident probability;
3. high level of accident severity level.

Risk control methods are to be determined by the assignment of respective attributes and identification of causal chains. The attributes indicate the risk control method and they can be categorised as follows:

A – attributes related to the risk reduction method and the risk itself,
B – attributes related to the required actions, e.g. procedural or technical,
C – attributes related to the confidence that a specific method is practicable.

Causal chains locate the particular risk control methods and may be expressed as follows:

Causal factors → initiating events → accident → circumstances → consequences

Risk control methods may be oriented to:

1. reducing the frequency of initiating events through better design;
2. mitigating the effect of initiating event consequences;
3. alleviating the circumstances of initiating events;
4. mitigating the consequences of accidents.

The identified risk control methods are to be grouped in the limited number of risk control options (RCOs).

The output of this step results comprises:

1. a range of RCOs which are assessed for their effectiveness in reducing risk; and
2. a list of interested entities (stakeholders) affected by the identified RCOs.

7 COST BENEFIT ASSESSMENT

The purpose of this step is to identify and compare benefits and costs associated with the implementation of each identified RCO. The analysis outcome is presented as net present value (NPV):

$$NPV = \sum_{t=0}^{n} \left[(C_1 - B_1)(1+r)^{-t} \right] \tag{7-1}$$

where:

B_1 – annual sum of benefits /
C_1 – annual sum of costs t
r – net present factor
t – consecutive years in the system life cycle, t = 1,2, 3,..., n
n – assessment time horizon.

The costs should be related to object life time and comprise the production/purchase costs as well as operation, training, inspection, certification costs, etc. Benefits should include the reduction in the costs associated with fatalities, personal injuries, environmental damage and its rectification, liability insurance, ship repair etc., as well as the benefits from the increased average life-time of ship. For each RCO, cost per unit reduction in risk (CURR) is determined:

$$CURR_{(\,foreachRCO)} = \frac{NPV}{BRM_E} \tag{7-2}$$

where:

BRM_E – benefit from risk reduction for each RCO.

The output of this step results comprises:

1. Cost and benefit breakdown into each RCO,
2. Cost and benefit breakdown into each stakeholder,
3. RCO list prioritised by cost per unit reduction in risk (CURR).

8 DECISION MAKING RECOMMENDATIONS

FSA methodology is an aid in the decision making process taking account of the risk involved. Risk control option selected through steps 1 to 4 enable identification of higher risk areas, the assessment risk-related costs as well as costs and benefits due to the risk reduction.

Decision making recommendations will depend on the scope of work covered by FSA methodology. For the engineering project they will cover application of additional equipment and/or arrangements to reduce costs with the same level of safety. For large groups of objects, e.g. ship type, they will entail amendments to the classification rules or international conventions. The process of issuing recommendations to decision makers is shown in the flow chart in Fig. 8.

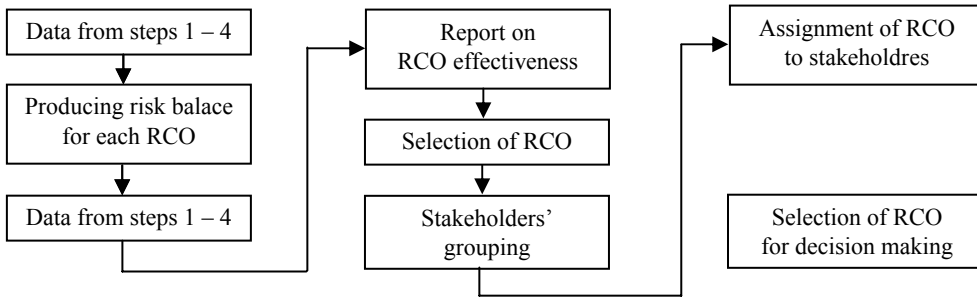


Fig. 8. Flow chart for the process of issuing recommendations to decision makers.

9 APPENDICES

9.1 Accident Categories

- Collision
- Contact
- Fire
- Explosion
- Loss of hull integrity
- Flooding
- Grounding and refloating after ship lighterage or at high tide
- Stranding
- Machinery related accidents
- Payload related accidents
- Hazardous substance accidents
- Accidents to personnel

9.2 Exemplary Hazards

.1 Shipboard hazards to personnel:
- asbestos inhalation,
- burns from caustic liquids and acids,
- electric shock and electrocution,
- falling overboard,
- pilot ladder/pilot hoist operation.

.2 Hazardous substances on board ship:
- combustible furnishings,
- cleaning materials in stores,
- oil/fat in galley equipment,
- cargo,
- paint, solvents, oil, grease in deck stores,
- cabling,
- fuel and diesel oil for engines, boilers and incinerators,
- fuel, lubricating and hydraulic oil in bilges and drip trays,
- refrigerants,
- thermal heating fluid systems.

.3 Potential sources of ignition:
- electric arc,
- friction,
- hot surface,
- incendiary spark
- naked flame,
- radio waves,
- electronic navigation equipment,
- laundry facilities – irons, washing machines, tumble driers, etc.,
- deck lighting,
- funnel exhaust emissions,
- hot work sparking,
- air compressor units,
- generator engine exhaust manifolds.

.4 Hazards external to ships:
- storms,
- lightning,
- unchartered submerged objects,
- other ships.

9.3 Safety of Bulk Carriers – MSC 74/5/X

For the sake of bulk carriers' safety IMO adopted document MSC74/5/x, developed by IACS, regarding fore-end watertight integrity of bulk carriers where emphasis was put on the bulk carrier hull integrity taking account of the risk control option assessment to prevent or mitigate the first cargo hold flooding consequences.

The scope of that study incorporated the specific steps of FSA methodology, in accordance with "FSA Interim Guidelines" and covered:

1. step 1
   Review of the previously performed risk identification (MSC72/INF.4) and other relevant information gathered during the work co-ordinated by UK MCA. Defining a generic ship – bulk carrier. Collection and analysis of relevant data from different sources at all levels.
2. step 2
   Analysis of the risk of watertight integrity of forepeak and the first cargo hold or ventilation ducts or cargo hatch covers' damage through the analysis of event frequency and consequences.
3. step 3
   Identification of risk control options through the review of previous studies presented by IMO, such as e.g. report on Derbyshire case, latest international regulations and standards suitable for the bulk cargo construction design.
4. step 4
   Cost analysis for selected risk control option.
5. step 5
   Preparation of the documentation to form the base for decision making.

Consideration was given to the following risk control options already incorporated into international conventions:

1. SOLAS, Ch. XII.
2. Enhanced survey programme – ESP.
3. Cargo hold hatch covers' strength – IACS UR S21.

as well as risk control options, such as:

1. Forecastle or bulwark.
2. Bulkhead strengthening.
3. Cargo hold hatch cover strengthening and application of friendly hatch cover closing system.
4. Carrying capacity reduction / freeboard increase.
5. Deck openings' flooding alarm.
6. Verification of deck opening design standards.
7. Construction of bulk carrier with double-side skin.
8. Application and maintenance of cargo hold internal lining for single-side skin construction.

10 BIBLIOGRAPHY:

1. Metodyka formalnej oceny bezpieczeństwa żeglugi (FSA) – A. Brandowski, 1998.
2. Procedura analizy rodzajów i skutków uszkodzeń – PN-IEC 812 of 1994.
3. Analiza ryzyka w systemach technicznych – PN-IEC 60300-3-9 of 1999.
4. Guidance notes on risk assessment applications for the marine and offshore oil and gas industries – American Bureau of Shipping – June 2000.
5. Problemy oceny bezpieczeństwa statku morskiego – A. Brandowski, May 2000.
6. Niezawodność człowieka – K. Kosmowski, January 2000.
7. Formal Safety Assessment – IMO MSC66/14.
8. The Interim Guidlines for the Application of FSA to the IMO Rule – Making Process – MSC/Circ.829/MEPC/Circ. 335.
9. Formal Safety Assessment – Trial Application to high speed passenger catamaran vessels. Finał Report – IMO DE 41/Inf.7 of 12.12.1997.
10. Formal Safety Assessment – IMO MSC 72/INF.4.
11. Bulk Carrier Safety, Formal Safety Assessment, Fore-End Watertight Integrity – IMO MSC 74/5/X.
12. FSA Report - Bulk Carrier Safety, Formal Safety Assessment, Fore-End Watertight Integrity – IACS, May, 2001.