PROBABILISTIC ASSESSMENT OF POST-CASUALTY AVAILABILITY OF SHIP SYSTEMS

Jakub, Cichowicz, jakub.cichowicz@strath.ac.uk *
Dracos, Vassalos, d.vassalos@strath.ac.uk *
Jonathan, Logan, j.logan@safety-at-sea.co.uk **

*Ship Stability Research Centre (SSRC), Department of Naval Architecture and Marine Engineering, Universities of Glasgow and Strathclyde, 100 Montrose Street, Glasgow G4 0TL, Scotland
**Safety at Sea Ltd, 280 St Vincent Street, Glasgow G2 5RL, Scotland

ABSTRACT

This paper presents some considerations regarding post-casualty availability of ship systems as seen from the point of view of application of probabilistic tools towards SOLAS 2010 regulations. General deliberations on the assessment aspects and role of the tools supporting availability analysis are supplement by short description of the software developed at SSRC and further illustrated by some examples.

Keywords: *system, availability, probabilistic, SOLAS*

1. BACKGROUND

The new SOLAS introduces fundamental changes to the shipbuilding regulatory framework.

Firstly, the rules are becoming more open, i.e. tight and rigid frames are replaced by new policies allowing designers to comply with the idea of convention rather than with the exact wording of the regulations, as long as the vessel's safety can be assessed with use of commonly recognized and accepted tools and measures. This is meant to ease the designs to follow-up advancement in the knowledge and technology. This creates new opportunities for building better and safer ships.

The new regulations may also help to change the picture of the entire naval architecture, seen today as one of the most conservative branch of engineering. It should be noticed here that this derogatory opinion is only partially justified as the conservativeness has solid foundations built on a centuries-long experience of maritime people. Moreover, a naval architecture has always been craft rather than pure science, even though since the times of William Froude the science has been used as a key tool in the craftsmanship.

Contrasting to the revolutionary development of aeronautics, naval architecture evolves – it absorbs advancements in science and technology relatively slowly.

Second set of changes (known as SOLAS 2010 or Safe Return to Port- SRtP) concern large passenger vessels[1] built (keel laid) on or after 1st July 2010.

[1] Ships of length over 120 m or having more than three main vertical (fire) zones (MVZ). The SRtP

The concept of safe return to port makes use of the axiom that ship is its best lifeboat or putting in different words that ship, even damaged, is safest place to be at sea. Casting this truism into a truth is challenging undertaking and requires far more effort than simple rules compliancy.

The necessary condition is that ship must survive an accident (usually understood as a fire or flooding casualty) and stay afloat and upright indefinitely (i.e. for a period of time sufficient either to return to port, or more precisely, to sail under own power to the nearest port, or to await rescue). In order to fulfil the condition, certain onboard systems must remain operational after the casualty: to generate power, ensure safety and some level of comfort to passengers and to suppress spread of casualty. In a case the condition cannot be fulfilled the ship should be abandoned.

Again, to perform "safe and orderly abandonment" vessel should remain afloat (and as much upright us possible) for certain period of time (three hours), casualty spread should be constrained (controlled), etc.

To (help) distinguish between "fatal" or "surviving" scenarios the concept of casualty threshold has been introduced, namely it assumed that ship will be able to return to port (under own power or on tow) given after a fire within single A-class space or having single watertight compartment flooded. Should the casualty exceed the threshold the vessel must be abandoned. In any case dedicated systems and onboard functions are to remain available (operational).

Principles of the idea behind the rules are clear – an abandonment is hazardous prospect; although extensive numerical simulations, based on a state of the art algorithms, show it is possible to evacuate several thousands of people within reasonable time, it is certain that no-one would want to validate the results.

On the other hand although the intentions of the regulatory body (IMO) are good the rules lack common interpretations and are difficult to implement within design process.

Most of the SRtP concerns originate at or are closely related to ship survivability. It is ability of the vessel to survive a casualty that legitimate the SRtP concept and justify design effort.

From this perspective, the assumed threshold are modest; if for instance ship is able to survive multi-compartment flooding or can remain habitable having entire fire zone lost why must she be abandoned?

On the other hand, if one-compartment flooding leads to immediate (less than three hours) capsize what is the purpose of expensive systems' design?

The thresholds set the goals for the design but it is clear that designing ship "at" the thresholds only may result in very costly construction that will not be able complete the basic function – to avert necessity of evacuation. Therefore, although rules are clear (putting aside lack of common interpretations) and set apparent criteria, the design process of the ship being actually able to return to port or to safely await rescue should expand beyond simple obedience.

Furthermore, the safer, more robust ship does not have to be more expensive than the vessel built just to meet basic requirements.

The new regulations implicitly introduce concept of the absolute survivability, i.e. floatability combined with the sustainability of the functions. Therefore, it is thought that the probabilistic approach used in the damage

requirements refer also to special-purpose vessels, e.g. cable lying vessels, drilling vessels, etc.

stability to evaluate safety of the ship (probabilistic index[2]) can be successfully used for systems' availability assessment. The probabilistic, index-based, approach not only allows meet the criteria but it additionally ensures consistency between survivability of vessel and onboard systems[3].

2. PRINCIPLES OF THE AVAILABILITY ASSESSMENT

As it has been explained in the previous sections, the rules are meant to provide guidance [4] and therefore the decision taken during the design process (with regard to scope of the "absolute" survivability) and those to be taken during ship operation (whether to stay onboard or to abandon the vessel) are left to owner. The approval procedure involves authorities and class representative, working closely with designers, yard and consultants from the onset of the design to identify potential problems and to ensure that the criteria will be met at final stage and approval granted[5].

The relative autonomy of the decision making gives not only a chance to make the best use of knowledge end experience of the parties involved but it also implies that it might not be wise to follow minimal requirements when more robust and safer design does not have to more expensive (at the time of construction and may turn out to be much safer in the time of accident as potential consequences could be mitigated by built-in safety measures).

Starting point of a discussion about how to validate the ship design against new rules is a notion of "all possible casualty scenarios" (not exceeding casualty scenarios"). This, depending on perspective can have dual interpretations; one would be to analyze systems' availability using deterministic [6] approach, i.e. involving "all casualty [7] scenarios" and another approach would be to employ probabilistic methods to generate the scenarios. Both methods allow validate the design against requirements and certainly, in spite of particular choice the qualitative outcomes should be comparable. There are however two fundamental distinctions that should not be underestimated and that make significant difference to the scope of application.

Firstly, the deterministic cases are screened prior to analysis and therefore contain only subset of all possible scenarios, whereas the scenarios generated with use of probabilistic methods contain all the scenarios with screening performed in the time of analysis and with the vetting driven by the probabilities of scenarios occurrence.

The difference may seem to be slight but it may have major impact on the quality of the results as the latter case do not require any form of judgment and consequently the outcome is not biased by scenario selection (the results correspond to the statistical data available, and therefore they mirror state of the knowledge on fire and flooding casualties).
Furthermore, the probabilistic assessment provides not only information about rule compliancy but it also gives valuable

[2] The index A is an average probability of survival, with p-factors (damage probabilities) being weighting factors.

[3] This feature has impact not only on safety-related design attributes but also ascertains that cost-effective features of the fire and flooding subdivision can be projected on the onboard functions.

[4] See: 0

[5] Such the design team, consisting of authority (DMA), class (GL), system designer/supplier (SAM) and consultants (GL/SSRC) was established within SAFEDOR 6.12 subproject illustrating Preliminary Approval process. Some details of the work performed are given in the later paragraphs.

[6] As a matter of fact the word *deterministic* may be slightly misleading as the approach discussed is a rule-of-the-thumb. The notion deterministic will however used hereafter for convenience.

[7] But "all scenarios" do not include some negligible cases (e.g. fire originated from water tanks etc.).

information about vulnerability of the vessel (understood here as a unity) to the considered fire or flooding casualties. Such information can be used at very early design stage to introduce changes that may become crucial for ship safety in operation.

Secondly, creating link to probabilistic framework of ship damage stability seems to be the most natural way of enhancing ships absolute survivability.

Final advantage of involving probabilistic tools in the assessment process is that they may create background for superior design and as well as open new opportunities for constructing vessels that will not only meet the SRtP criteria but may also offer safety for passengers and crew after casualties exceeding predefined thresholds. This can not be done with use of deterministic approach as they lack any means of quantification and therefore any amendments to systems' topology cannot be (practically) verified[8].

There is also one fundamental aspect of probabilistic assessment that may play significant role in the safety of the vessel. This is related to the damage penetration (both transverse and vertical). The regulations set "safety" limits as B/10 and B/20 for transverse (measured from the shell) and vertical (measured from the bottom) penetrations respectively. All system's components located within these boundaries are considered not to be mechanically damaged. Again, it is thought that these limits, based on statistical distributions[9], are set to enable deterministic assessment. Authors experience suggests however, that the penetration limits could be easily increased, e.g. to B/2 for collisions without any major impact onto assessment outcome, regardless the approach. Firstly, the penetration limits will concern mainly connectors, i.e. pipes and electrical cables[10] and structural tanks. The number of critical connectors and tanks could be brought further down, as most of them would be redundant anyway, as SRtP ship would have redundant propulsion, steering etc[11]. Therefore, even at the stage of preliminary design number of systems' components vulnerable to, say B/2 penetration would be rather small compare to total number of components. Therefore should huge investment is made to provide ship with redundant systems it would not be particularly wise to ignore risk (understood in a common sense of the word) of such components being unavailable if actual penetration were B/9 instead of assumed B/10. Again, once critical scenarios (and their probabilities) are known the cables (for instance) could be re-routed through the spaces having marginal probabilities[12] of being damaged.

[8] It is thought that the thresholds have been proposed in the current form to allow the design to be validated in a way of simple reasoning. From practical point of view even for those limits such approach may fail. Furthermore it should be emphasised again that if the goal is to design ship able to survive the damage and offer safety to those on board the limits are very modest. On the other hand, heavy damages should not be taken into account as separated from the survivability of the vessel, therefore probabilistic availability assessment is the most natural way of the design validation and improvement.

[9] Probability distribution functions (pdf's) obtained from the statistical data show clearly that most of the damage penetrations for collisions and grounding have been within B/10 and B/20.

[10] In general, the pipes and cables not serving damaged spaces as most of the equipment within damaged spaces would be directly affected by casualty (by unprotected terminals, connections, valves etc.)

[11] Furthermore, many of cables and pipes would be routed to avoid simultaneous damage due to fire casualty, which in many of cases would affect spaces enclosed by shell, main fire bulkheads and decks.

[12] It should be noted here, that for ships having no longitudinal subdivision, which is very often a case for large passenger vessels, the penetration is not explicitly taken into account whilst calculating probability of given damage case. Should ship have longitudinal bulkheads the penetration would be accounted for by means of weighting factor (r). The weighting factor would be incorporated into evaluation of probabilities (p-factors) by means of likelihood of breaching longitudinal bulkhead in the considered scenario.

All the above considerations are based on authors experience in the availability assessment of onboard systems and functions. The tool, SAVANT (System AVailability ANalysis Tool), presented in the following paragraph (developed at the SSRC and further refined within SAFEDOR project) to accommodate tools necessary to perform probabilistic assessment of systems and functions in a comprehensive way, with flexibility necessary to support complex process of designing ships *able* to return to port.

3. THE TOOL – SAVANT

The SAVANT is a software platform designed to combine ship arrangement with systems' topology and probabilistic models of fire and flooding casualties.

The tool is built of two modules – first supporting modelling, which supports GUI and scripting interfaces for placing components within model of vessels environment, editing and creating dependency structures and second, computational, module for solving logical expressions.

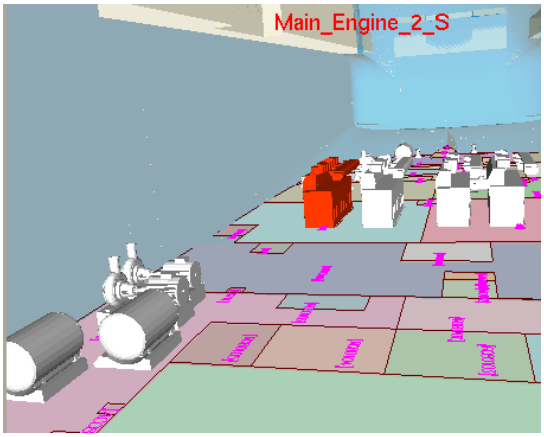

Figure 1. System components placed within ship model.

The first module supports the most common editing operations (place component, name-rename, create dependency, assign graphics, etc.) and is meant to create realistic spatial representation of the vessels interior and to debug the models during modelling.

Vessel's spatial arrangements is reproduced from deck layouts and converted into 3D geometrical database.

The dependencies imposed on the systems' components can be presented graphically in the form of (expandable) graphs, which can be used during debugging and for presenting the results. There are no formal limitations of the form of logical structures and systems handles deeply nested and cyclic dependencies. This allows modelling process to be intuitive. Each system and/or function is represented by individual logical structure (systems may or may not be included into single envelope-function). In principle, systems are composed of physical (pump, switchboard, etc.) and abstract functions or sub-systems (e.g. power supply, propulsion, steering etc.). The first are directly linked to the corresponding spaces and therefore state of the space (intact or damaged) is automatically passed on to the components within[13].

The latter group, abstract components, can not be directly damaged – their state is logical consequence of system dependencies on the physical components.

The computational module is based on Binary Decision Diagrams (BDD) - an advanced and efficient[14] technique for solving Boolean expressions. In principle, the system logic (i.e. set of Boolean expressions describing physical couplings and functional relations between components and functions constituting a system) is defined by user in the form of success structure (i.e. dependencies are expressed as required in normal operation). The level of detailing in modelling of logic depends strongly on availability of data at particular

[13] Vulnerability of given component

[14] See: 0 and 0

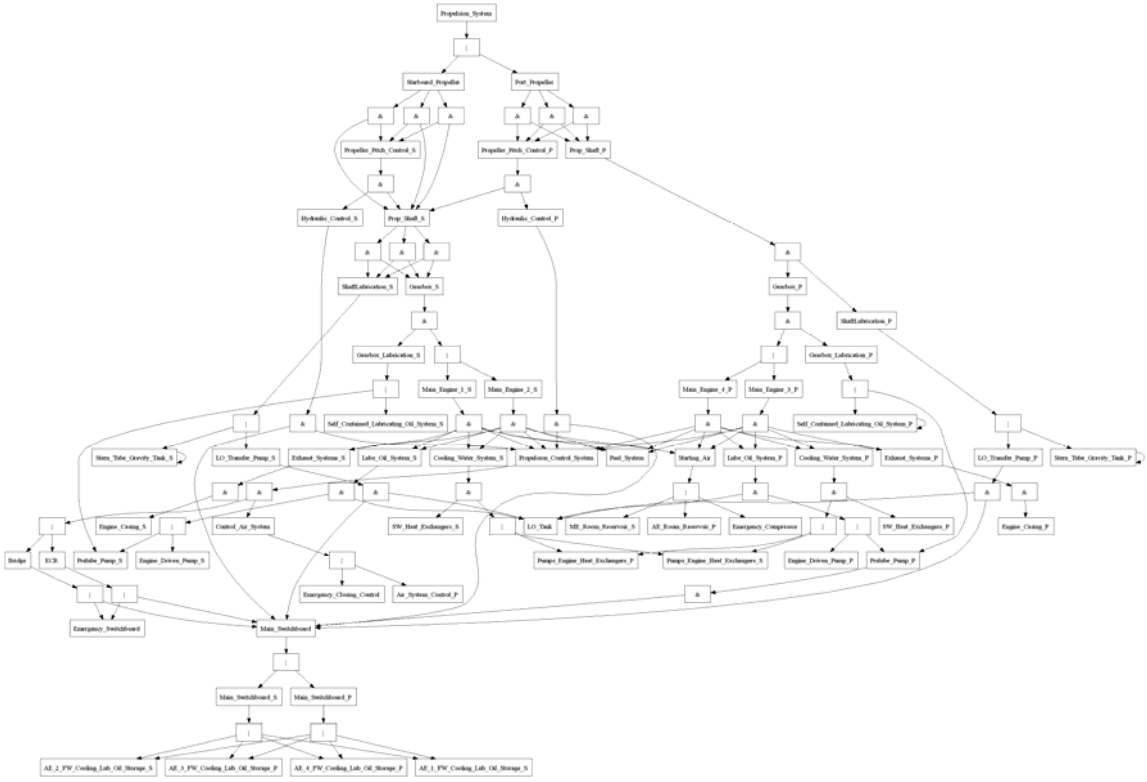

Figure 2. Example of dependency diagram created for simple model of Ro-Ro vessel propulsion system (partially expanded).

stages of analysis. Nonetheless the dependency model must:

- preserve physical and functional relations of the system and across the systems
- preserve spatial distribution of the system (this has twofold meaning: firstly, the components must be placed within appropriate rooms [15] or spaces, and secondly, a *redundancy* is modelled only if it is justified by model resolution (in room-wise environment two components sharing same room are not considered to be redundant unless they are separated by centre-plane, which in turn follows assumptions of maximum allowed penetration.

The modelling itself can be performed in a way most convenient for user, as the user input is pre-processed (expression expansion, detection of cyclic references, substitutions etc.) by the module.

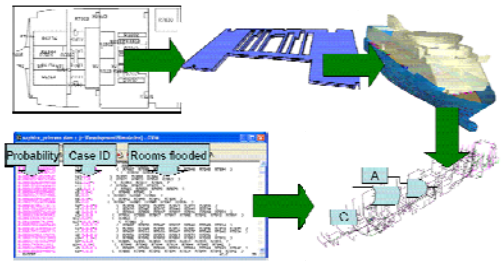

Figure 3. SAVANT – flow of information.

At the final stage the model is fed by set of damage scenarios defined as a combination of probability of occurrence p_i and a list of spaces (rooms) affected. In case of deterministic approach, the probabilities are dropped ($p_i=1$ for all the cases). At the next step space states

[15] Here, spatial arrangement of the vessel corresponds to NAPA standards and therefore a room constitutes smallest, undividable volume enclosed within the ship. A collection of rooms may form WT compartment etc. A default resolution of SAVANT modelling is also "room-wise". Exact position of the components is assumed to be irrelevant (although can be assigned within the software) which has been discussed in the previous paragraphs.

are passed in to the corresponding components and the satisfiability problem solved (i.e. it is checked if given combination of causes (initiating events) is sufficient to cause systems' unavailability)[16].

The following equation illustrates the numerical scheme used for evaluation of unavailability rates for all the physical components, functions and systems modelled (components F_j of the column vector $\boldsymbol{F}$).

$$\boldsymbol{F} = \begin{bmatrix} F_1 \\ \vdots \\ F_N \end{bmatrix} = \frac{1}{\sum_{i=1}^{n} p_i} \begin{bmatrix} S_{11} & \cdots & S_{1n} \\ \vdots & \ddots & \vdots \\ S_{N1} & \cdots & S_{Nn} \end{bmatrix} \begin{bmatrix} p_1 \\ \vdots \\ p_n \end{bmatrix} \qquad (4.1)$$

The elements of the matrix $\boldsymbol{S}$, S_{ji}, stand for state ([0;1] – for availability or unavailability respectively[17]) of the *j-th* component in the *i-th* damage scenario. Finally, column vector $\boldsymbol{p}$ contains probabilities of all the damage scenarios ($i = 1 \ldots n$) in consideration.

[16] It is worth noticing that the modelling process and applying damage scenario is not trivial task. It is usually determined by imposed criteria and it often requires advanced strategies. The penetration issue can be, for instance, resolved by creating redundant (OR) dependencies on two components (one in the portside and one in the starboard part of the given room) and use only selection of scenarios (e.g. portside damages). Should the vulnerability of components to the damage cause were set to 1 and 0 for portside and starboard components respectively only the first would be damaged and therefore system would survive. Similarly, in some cases selectivity of scenarios may be applied if the criterion says that, for instance, system in consideration should remain operational outside the casualty area (fire main is an example of such system). In the cases like this selectivity of scenarios is an attractive alternative to difficult and error-prone permutation-based modelling.

[17] Apart from binary mode, the component vulnerability to the damage cause can be adjusted by use of weighting factor α=0...1. This could be used to investigate sensitivity of the design on the given component (e.g. sensitivity studies on the impact of penetration on the overall functioning of system. Should a is used for given physical component, say j-th, the component S_{ji} would be replaced with the following: $S_{ji}^{*} = \alpha \cdot S_{ji}$.

4. INTEGRATION OF THE TOOL INTO A DESIGN PROCESS

The design process of vessels fulfilling SRtP requirements is by definition cross-disciplinary undertaking. Until now ships could be designed by number of teams and in general, each team would work independently on another. The boundaries of competence and responsibility would be set clearly by the rules and overlapping activities would be reduced to necessary minimum with all the pieces joined at the very last stage. Nowadays with flexible rules and new requirements, the process of design has to be managed jointly from the very beginning, as every change in arrangement may and possibly will have impact on systems' availability which should be re-assessed immediately after significant amendments have been introduced. In addition to that the process should (ideally) be continuously monitored by classification body and flag state.

Moreover if a tool like SAVANT were to be used for the assessment the team would include naval consultants as well. It has been proved within SAFEDOR 6.12 sub-project that such team can work efficiently and deliver high quality product. Furthermore, it is thought that such multi-perspective cooperation may offer great opportunity of refining the design at very early stages ensuring time efficient development.

Obviously, any tool used for availability assessment should be used from the very beginning. As authors experience indicates it is the modelling process that allows identify many undesirable features of the project and make "run-time" changes and therefore the first assessment (at the preliminary stage) serves mainly to confirm that there are no conceptual errors in the design.

At the following stages detailed analysis of critical (or simply dispersed) systems can be performed to achieve design goals. It should be noticed here, that these later stages will bring real quality to the design as it is details that will

provide the ship with real ability to return to port or to provide the required safety and comfort levels to passengers and crew.

The modelling (constantly monitored by class and flag representatives) is certainly time-consuming process, however once the models are created at the preliminary stage any changes can be readily introduced.

5. EXAMPLES OF APPLICATION

The tool has been employed in number of research and commercial projects. One of the most significant was a SAFEDOR exercise[18] (WP 6.12) where the tool was used within the demonstration of preliminary approval process with Danish Maritime Authority, STX Europe (formerly Aker France), SAM Electronics and Germanisher Lloyd[19] among the partners. The subject matter was innovative power distribution system to be integrated within an existing Ro-Ro vessel. The goal was to establish whether the rule challenging (mainly from conceptual perspective stemming from the very nature of the system, e.g. absence of main switchboard etc.) design could be proved to be at least as safe as base design.

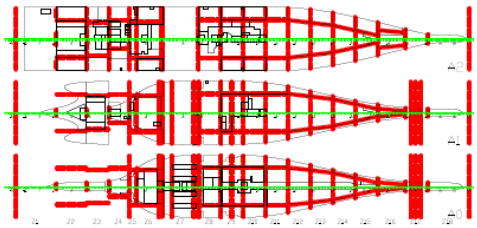

Figure 4. WT subdivision of the analysed vessel. Courtesy of STX Europe.

Although either design solution would comply with the SRtP requirements (the base vessel has been in service for relatively long time and was built according to older regulations) the verification process was very rewarding.

In the course of quantitative analysis it has been shown that although the original and novel systems are utterly different[20] they share same level of safety with regard to probability of internal failures (GL).

Similar conclusions have been withdrawn from fire casualty availability assessment performed by SSRC. In case of flooding however things were different.

The results showed that the unavailability rates of some onboard functions supplied the novel system were much higher compare to base-design (e.g. increase of propulsion unavailability due to power omission to some auxiliary services, like engine room ventilation,

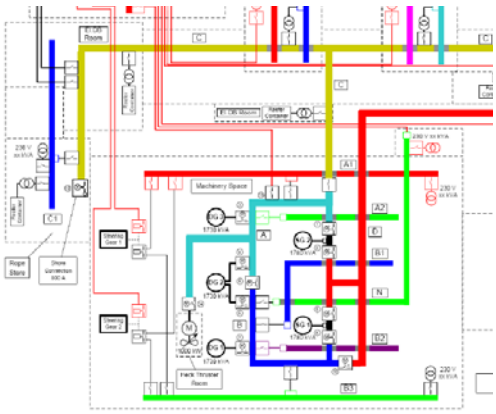

Figure 5. Single-line Diagram of the novel distribution system (fragment). Courtesy of SAM Electronics.

went from 0.05 to 0.48[21]).

[18] See: 0

[19] www.**dma**.dk
www.germanlloyd.org
www.**sam-electronics**.de
www.**stx**europe.com

[20] The models have been very advanced and included not only all the equipment but also cable routes, switchboards, distribution boxes etc.

[21] The numbers are to be understood as an average probability of the system being unavailable given one compartment collision and flooding casualty.

Further investigation that followed revealed that such unexpected rise in the unavailability rates was due to certain topological features of the bus-based (novel) system. As a first it was found that the extension of power bus A (see: Figure 4) towards the aft thrusters-room had not been isolated by circuit breaker[22] from the main bus in engine room. This increased rate of the bus unavailability from 0.005 (as for bus-bar B) to 0.1. Furthermore, the bus-bar C (distributing power to the fore thrusters room and upper deck consumers) was connected to the bar A instead of B. The bar C had unavailability rate ~0.5, caused by combination of connecting it to the A (0.1) and routing through the spaces potentially affected by the damage with probability 0.4[23]. Should the bar C were routed a deck above (unaffected by any considered damage scenario) and circuit breaker present on the extension to A, the unavailability rate of the engine room ventilation would drop roughly to ~0.005, a level of magnitude less than in base design.

It should be noted here that although the "missing" circuit breaker could be easily identified as a critical component, the routing of the bar C could not (original and alternative routes located at adjacent car decks). It was the probabilistic analysis that indicated the direction of design changes (which, introduced at early stage could be readily made).

The next example shows application of the availability assessment to a large propulsion vessel.

The results shown in the Figure 6 show clearly that applying certain design measures and taking advantage of the experience and capability of tools may lead to the situations that the systems supporting vessel's safety will be as reliable after casualty as the ship herself.

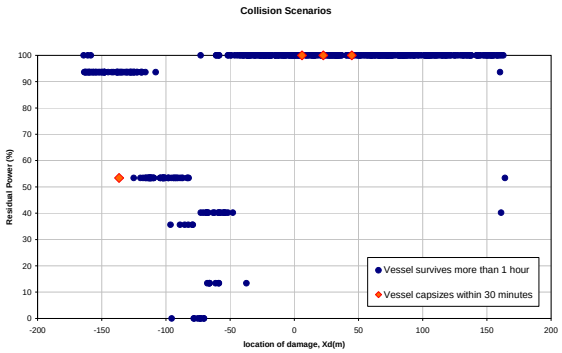

Figure 6. Propulsion availability after one-compartment flooding casualty. In total in 96% (335 out of 350 cases) more than 30% of the contract power was available. It is worth noticing that the vessel's survivability rate [afloat for more than 30 minutes] was 98%.

6. CONCLUDING REMARKS

Originally, this paper aimed at presenting details of the SAVANT development with stress put on the technical side of the matter. However, in the course of author's involvement within various design projects it has become clear that there is large amount of confusion around the rules itself as well as implementation of the SRtP idea to actual design process. It was not the authors' intention to explain the rules and therefore any references to them are vague and rough. The paper aims rather at the very application of the assessment tool to the design's validation.

All the considerations presented here originated whilst working on real designs, during discussions with number of various people, looking at the problem from distinct perspectives. The final conclusion could be that the rules do not guarantee successful design neither does money spent on equipment. It is combination of experience, knowledge and will that may turn the SRtP idea into great and safe vessel.

As one has put it: that animal, SOLAS 2010, can be domesticated.

[22] The circuit breaker was omitted unintentionally and this mistake propagated to the SAVANT models (created according to the documentation).

[23] Fact that the numbers add to 0.5 is a coincidence.

7. ACKNOWLEDGMENT

The software (SAVANT) presented in this paper has been refined under the SAFEDOR Project, IP-516278, with partial funding from the European Commission.

Contribution of WP3.4 and WP6.12 partners, as well as colleagues from SSRC and SaS is gratefully acknowledged.

8. REFERENCES

SOLAS II-1/8-1, II-2/21, II-2/22

R.M. Sinnamon, J.D. Andrews "Improved efficiency in qualitative fault tree analysis", Quality and Reliability Engineering International, vol. 13, 293-298 (1997)

Fault Tree Handbook For Aerospace Applications: Dr. Michael Stamatelatos, NASA HQ, OSMA, Dr. William Vesely, SAIC, Report prepared for NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546, August, 2002

Graph Based Algorithms for Boolean Function Manipulation, Randal Bryant, IEEE Transactions on Computers, C-35-8, pp. 677-691, August, 1986

Fault Tree Analysis and Binary Decision Diagrams, R. Sinnamon and J. Andreas, Proceedings of the Reliability and Maintainability Symposium, January 1996, pp 215-222.

New Algorithms for Fault Tree Analysis, A. Rauzy, Reliability Engineering and System Safety, Vol. 40, 1993, pp 203-211.

The Synthesis of Two-Terminal Switching Circuits, Claude Shannon, Bell System Technical Journal, vol.28, pp.59-98

Risk Analysis of Innovative System, R. Hamann, E. Rüde, J. Voelker, J. Cichowicz , SAFEDOR Deliverable 6.12.2, 2009

[…] Explanatory notes…, IMO, FP 53/WP.7, 19 February 2009