Special Workshop on Risk Acceptance and Risk Communication
March 26-27, 2007, Stanford University

Optimal Reliability of Components of Complex Systems Using Hierarchical System Models

Kazuyoshi Nishijima
Institute of Structural Engineering, ETH Zurich
ETH Hönggerberg, HIL E 22.3, Zürich, 8093, Switzerland

Marc Maes
Civil Engineering Department, Schulich School of Engineering, University of Calgary
2500 University Ave. N.W., Calgary, Canada T2N1N4

Jean Goyet
Bureau Veritas, Marine Division, Research Department,
Bereau Veritas, 17 bis Place des Reflets, La Defense 2, 92400 Courbevoie, France

and

Michael Havbro Faber
Institute of Structural Engineering, ETH Zurich
ETH Hönggerberg, HIL E 23.2, Zürich, 8093, Switzerland

Abstract

The present paper addresses the issue of optimization of reliability acceptance criteria for components of complex engineered systems with given criterion to acceptable system risk. To this end, the paper first describes how complex engineered systems may be modelled hierarchically by use of Bayesian probabilistic networks. The Bayesian probabilistic network serves as a function relating the reliability acceptance criteria of the individual components of the system to the risk acceptance criteria for the system. Thereafter, a constrained optimization problem is formulated for the optimization of the component reliabilities. In this optimization problem the system risk acceptance criterion defines the constraint and the expected utility from the system, is considered as the objective function. A ship hull structure is taken as an example of a complex engineered system to illustrate how the proposed framework may be implemented into a software tool using commonly available techniques and algorithms.

1. Introduction

Typically engineered systems are complex systems comprised of geographically distributed and/or functionally interrelated components, which through their connections with other components provide the desired functionality of the system expressed in terms of one or more attributes. This perspective may indeed be useful for interpreting and modeling a broad range of engineered systems ranging from construction processes over water and electricity distribution systems to structural systems. One of the characteristics of engineered systems is that, while the individual components may be standardized in

regard to quality and reliability the systems as such, they often cannot be standardized due to their uniqueness. The performance of systems will depend on the way their components are interconnected to provide the functions of the systems as well as on the choice of quality and reliability of their components. Thus, the design and maintenance of systems effectively concern about requirements to the quality and reliability of their components, which can be translated from given requirements to the attributes of the performance of systems in accordance with the way the components are connected.

Due to the complex nature of the problem, modelling and optimization of such systems generally requires that different levels of analyses provided by different experts are integrated interdisciplinary. Taking basis in engineered structures, at component level physical failure mechanisms may be analysed, such as yielding, fracture and corrosion. The component failure modes now constitute the building stones for the development of systems failure modes including the formation of failure modes for sequences of sub-systems, for which the corresponding consequences may be assessed. An optimization of the components of a given system i.e. a system with a given interrelation between its components must take basis in such analyses. Seen in this light, it is useful to establish hierarchical models for complex engineered systems which accommodate for the consistent integration of the different levels of analyses. Such a hierarchical approach may also prove to be beneficial as a means of communication between professionals representing the expertise required for the modeling of the performance of the different types of components and sub-systems.

The present paper addresses the problem outlined in the foregoing in the context of a hierarchical system modeling developed for risk assessment of engineered systems by the Joint Committee on Structural Safety (Faber et al. 2007). Taking basis in structural systems a framework is formalized in regard to how the hierarchical system model can be established and then applied to optimize the reliability and/or the risk acceptance criteria for components of structures based on specified requirements to the reliability and/or the risk acceptance criteria for the considered structural system.

The present paper first provides a short summary of available techniques on the modelling of complex systems as well as presently available and applied approaches for setting requirements to systems acceptable risks. Following this, a general framework for the optimization of reliability for components of systems for given criteria to the system risk is described. The proposed framework is composed of three steps; 1) adaptation of Bayesian probabilistic network representation for hierarchical system modeling, 2) translation of acceptance criteria from system level to component level, and 3) optimization of the reliability of individual components. Finally an illustrative example is provided considering the optimization of the reliability of welded details subject to fatigue in the hull structure of a Floating Production Storage and Offloading Unit (FPSO).

2. Problem setting

2.1. Modelling of complex systems

The requirements to the probabilistic modeling of complex engineered systems in the context of risk based decision making concerns the consistent representation of the physical characteristics of the considered system and the appropriate detailing to facilitate the assessment of the benefit associated with different decision alternatives. In addition, of course the modeling should also facilitate an efficient analysis of the probabilities and consequences required for the ranking of decision alternatives. Fault-tree analyses comprise classical techniques for the representation and analysis of systems failure modes , see (Vesely et al. 1981). Assuming that components in a system have only two states (failure and success) and that the component failures are statistically independent, the probability that a predefined state of the system (top-event) occurs may be quantitatively assessed, see e.g. (Bobbio et al. 2003). Fault-tree analyses have been applied to e.g. risk assessments of nuclear power plants ((USNRC 1975) and (USNRC 1990)) as well as for the reliability analysis of control systems for gas turbine plants, see

e.g. (Bobbio et al. 2003). Fault tree analysis is from a technical perspective relatively simple, and for that reason also in many ways attractive, however, for the same reason subject to important limitations. Among these limitations the difficulty in representing dependencies between basic events as well as the problems associated with updating based on new information should be mentioned. Techniques for probabilistic representations of systems such as Bayesian Probabilistic Networks (BPN's), seem to provide an interesting and promising alternative to the classical techniques for system analysis. A BPN is a probabilistic model representation in terms of a directed acyclic graph (nodes representing uncertain state variables logically interrelated by arrows) and conditional probability assignments, see e.g. (Jensen 2001). Any fault-trees can be mapped into Bayesian probabilistic networks as is shown in (Bobbio et al. 2001).

When modeling the performance of systems it is important to consider temporal aspects. Petri Nets provide a powerful platform based on which temporal dependencies associated with e.g. repair or replacement actions which may provoke cyclic references to states of the components in the model can be accounted for (Volovoi 2004). However, the evaluation of the reliability of a given system through a Petri Net takes basis in Monte Carlo simulation which in general requires a considerable amount of computational effort. BPN's are not immediately appropriate for the representation of cyclic effects, however, by introducing time slices in a BPN (so-called dynamic BPN), BPN's may also be applied for such analysis. Several efficient time slice BPN algorithms have been developed for calculating probabilistic characteristics of state variables of BPN's, e.g. expected values and conditional probabilities, see e.g. (Kjaerulff 1995). It should be noted that a dynamic BPN representation is equivalent to a Markov chain representation, see (Smyth 1997). The BPN approach for systems modeling has been utilized for the hierarchical analysis of structural systems in (Baker et al. 2007) where also an indicator of the system attribute robustness is proposed.

Another approach for the probabilistic modelling and analysis of complex systems is proposed by (Der Kiureghian and Song 2007). In this approach, the probability of an event of interest (related to the system performance) is formulated as a sum of the probabilities of the mutually exclusive combinations of the component states that govern this event. Upper and lower probability bounds on the system performance are calculated based on an out-crossing formulation and using linear programming techniques. Moreover, it is shown in (Der Kiureghian and Song 2007) that by aggregating several components as "super-components" and applying the linear programming method in a hierarchical way, the approach provides reasonable probability bounds on the system performance with a manageable computational effort. However, the applied scheme for component aggregation affects the efficiency of the computation and the width of the obtained probability bounds. An optimization of the aggregation scheme in principle requires trial and error, although general guidelines are provided in (Der Kiureghian and Song 2007).

2.2. Acceptance criteria

Acceptance criteria are generally defined based on the attributes of the performance of systems considering the consequences due to possible failures. Recent design codes e.g (ASCE7-98 2000) provide acceptance criteria in terms of minimum requirements to structural performance. (JCSS 2001) recommends different target reliabilities for engineered structures in accordance with the consequences of failure as well as the relative cost of safety measures. (Pemex 2003) provides risk acceptance criteria for offshore structures for five different types of consequences: injuries and fatalities, effects to the general population, environmental impact, production loss, and damages to installations.

Recently, a general principle for evaluating the acceptability of a life saving measure has been proposed using the concept of Life Quality Index (LQI), e.g. (Nathwani et al. 1997) and (Rackwitz 2002). It provides a sound basis to judge if any given life saving measure is acceptable in a society taking basis in the demographical characteristics; GDP per capita, life expectancy at birth and the fraction of life spend for work. Based on the LQI concept it is possible to optimize and specify

requirements to the performance of engineered systems depending on their functions and the costs of improving their safety.

2.3. Objective

The acceptance criteria mentioned in the foregoing may be seen to constitute the boundary conditions which any engineered system must satisfy during its service life. The present paper takes the standpoint that the acceptance criteria for systems are a-priori given. This situation is often the situation which is encountered in practice; but it is in general not optimal. The generalization of the approach outlined in the following may, however, relatively easily be generalized to include also an optimization of the requirements with respect to the system performance. The goal of the present paper is, thus, to establish a framework for the optimization of the reliability for components of systems for given system performance requirements – in terms of acceptable risks, by minimizing life cycle costs for the design and operation of the system or more generally by maximizing the service life expected utility. To this end special attention is paid to the utilization of commonly available techniques and readily accessible algorithms.

3. Proposed framework

3.1. Hierarchical system modeling with Bayesian probabilistic network

A hierarchical system modeling for complex systems facilitates the representation of complex systems at an early stage of risk analysis, e.g. at the concept evaluation, but may also serve to optimize the final design as well as for the management of the risk during operation. In Figure 1 it is illustrated how the system functions are represented in terms of a hierarchical aggregation of components and their interrelations. At the same time the requirements to the system performance may be disaggregated into reliability performance requirements for the components. BPN models appear suitable as a platform for modeling complex systems, since they provide a causal and mind mapping representation of the system characteristics and functionalities. Furthermore, the general characteristic that engineered systems are comprised and built up by components which are standardized by codes and standards in regard to quality and reliability adds value to the use of object-oriented BPN representations. This special type of BPN models allows for creating classes of BPN's which are representative for sub-systems that have identical characteristics, see e.g. (Bangso et al. 2003) and (Bangso and Olesen 2003).

Having established the hierarchical system model with the corresponding BPN, any given performance characteristic of interest for the considered system, such as the service life utility u may be deduced from the BPN as:

$$u = f(x_1, x_2, ..., x_N) \tag{1}$$

where x_i i = 1, 2, …, N are the target reliabilities for the N individual components of the system, and f represents a function on the BPN.

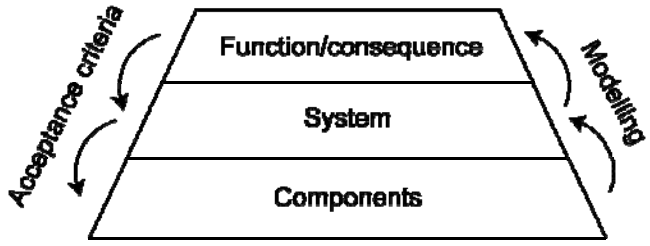

Figure 1: Hierarchical modelling and translation of acceptance criteria.

3.2. Acceptance criteria

Acceptance criteria are typically defined in regard to the functionality or performance of the considered system measured in terms of risks and/or reliability. Since the design and maintenance of a system usually specifically address the components of the system, it is of interest how the acceptance criteria for the components may be derived from the acceptance criteria specified for the system performance. Thus, the optimization of acceptance criteria for components in a system constitutes an inverse problem, see Figure 1.

The acceptance criteria for the system can be related to the target reliabilities for the components as:

$$g_j(x_1, x_2, ..., x_N) \le c_j, \ (j = 1, 2, ..., M) \tag{2}$$

where g_j (i = 1, 2, …, M) represent the functions on the BPN calculating the quantities for which the acceptance criteria for the system are defined, and c_j (i = 1, 2, …, M) are acceptance levels for the corresponding quantities, and M is the number of considered acceptance criteria for the system performance.

3.3. Optimization of acceptance criteria for components of complex system

Since several combinations of target reliabilities for different components in a system may satisfy the prescribed acceptance criteria for the system, the optimal combination of target reliabilities for components may be identified as the combination which maximizes the expected utility u using Equation (1) and (2) formulated in accordance with the previous sections as:

$$\begin{aligned} &\text{Maximize } u = f(x_1, x_2, ..., x_N) \ \ s.t. \\ &g_i(x_1, x_2, ..., x_N) \le c_i, \ (i = 1, 2, ..., M) \end{aligned} \tag{3}$$

Since the functions f and g_i (i = 1, 2, …, M) are readily available, the problem is reduced to a standard non-linear constrained optimization problem.

4. Example

4.1. Risk acceptance criteria for components in a ship hull structure

The main functionality of ship hull structures for Floating Production Storage and Offloading Units (FPSO's) is to ensure the continued operation in accordance with design requirements. Typically considered events of system failure for FPSO's are:

- Loss of or damage to ship due to loss of buoyancy or explosions/fires
- Loss of production due to reduced functionality
- Loss of lives due to foundering or explosion/fires
- Leaks and other damages to the quality of the environment

Considering the hull as an assembly of components, the hull may be considered to comprise an assembly of tanks tied together with deck plates, tank partitions, and bottom and side plates. The individual components are furthermore stiffened by girders and web frames to ensure a sufficient structural integrity of the hull, see Figure 2. The corresponding hierarchical model representation is shown in Figure 3.

The hull components as described above have basically two functions, namely, to ensure that the overall ship has a sufficient structural integrity and provide the means for containing cargo and ballast. Failure of the components of the hull at this level can be assumed as the events of:

- Loss of or reduced structural integrity
- Loss of containment/leaks of the individual tanks

Considering now the individual components as outlined in the above these may be viewed upon as assembly of plates connected by welded joints. Failure of these components may lead to:

- Crack or pit through plate thickness
- Reduced overall plate thickness
- Joint stiffness reduction or failure

Thus, the losses or damages at component level may lead to the hull failure or undesired economic and environmental losses as well as loss of lives given the way how the components are interconnected. The problem in the example is to optimize the target reliabilities for the fatigue reliability of the welded joints in plate and tank partition components given the requirements to the functionality/consequence of the ship hull, e.g. the probability of hull failure. For this purpose a software tool is developed using Hugin for BPN representation and Microsoft Excel for the optimization algorithm as well as the interface.

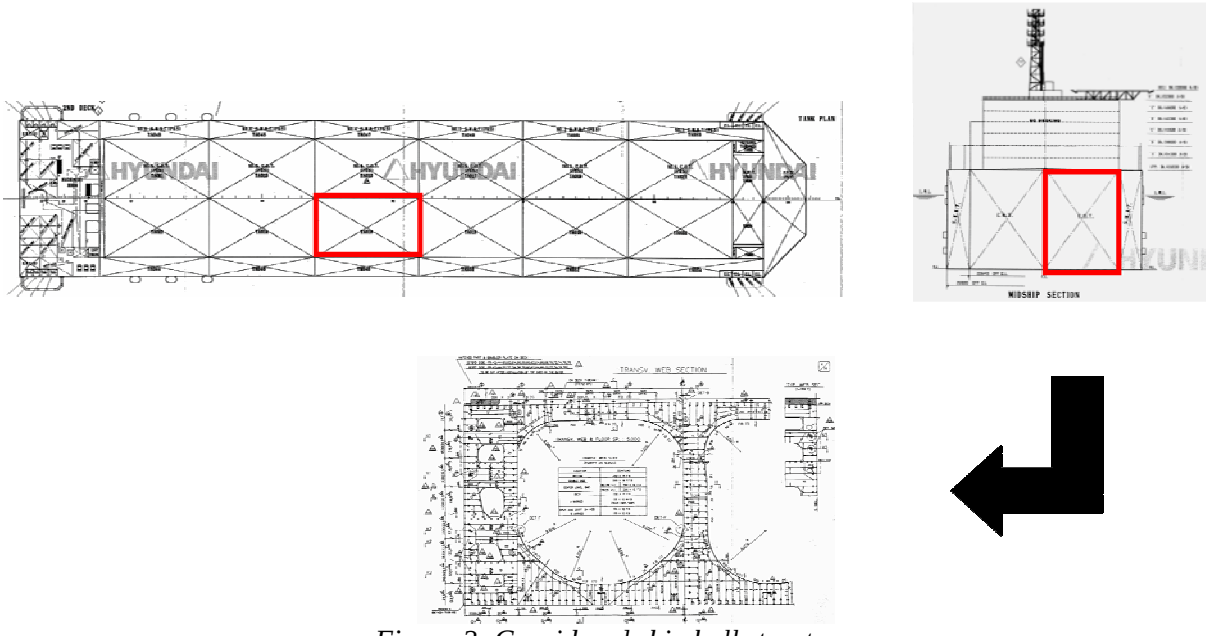

Figure 2: Considered ship hull structure.

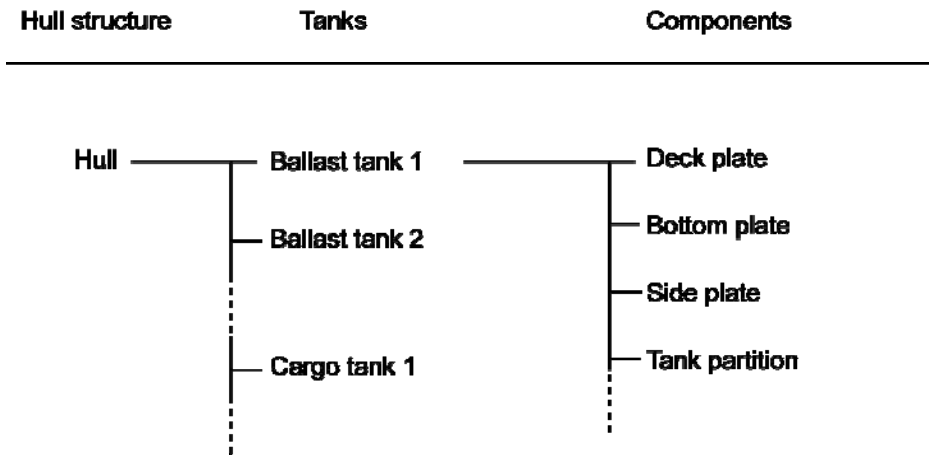

Figure 3: Hierarchical modeling of hull structure.

4.2. Optimization of target reliability for welded joints in components

The developed software tool provides an easy interface to obtain the optimal target reliabilities for welded joints. Microsoft Excel (hereafter Excel) is used as a platform for integrating the various computational modules and storing information required for calculations. The Excel platform is linked dynamically to Hugin ActiveX server (hereafter Hugin). In order to use the software tool the user has to define, through Hugin files, the BPN corresponding to the hierarchical model of the hull structure as described above. The outputs, i.e. optimized target reliabilities for all welded joints, are written into the Excel file.

In Figure 4, the illustration of the hierarchical BPN representation of the ship hull structure is given. In the entire BPN the conditional probability tables are assumed given by experts, see e.g. Figure 5 (which is the conditional probability table for node “Explosion_1”), whereas the nodes that represent the components serve as root nodes whose probabilities are represented in terms of unconditional probabilities, which are derived from the target reliabilities for welded joints in each components. Therefore, by changing the target reliabilities for the welded joints which are set in the Excel file, see Figure 6, the unconditional probabilities for the components are changed accordingly. In turn, the corresponding probabilistic characteristics, e.g. expected total cost or probability of hull failure are changed and stored in the Excel file, see Figure 6. This process is made automatically through ActiveX. The design and service life maintenance cost for the different welded joints is in general a function of the target reliability in regard to fatigue failure, and this is implemented in a VBA code. For the assessment of the relationship between fatigue reliability and service life costs the iPlan software described in (Straub and Faber 2006) may be utilized. Finally, the optimal target reliabilities for welded joints are obtained using the Solver add-in provided in Excel – target reliabilities correspond to “changing cells”, and acceptance criteria for the ship hull correspond to “constraints” in the Solver add-in. The result appears on the Excel interface, see Figure 6.

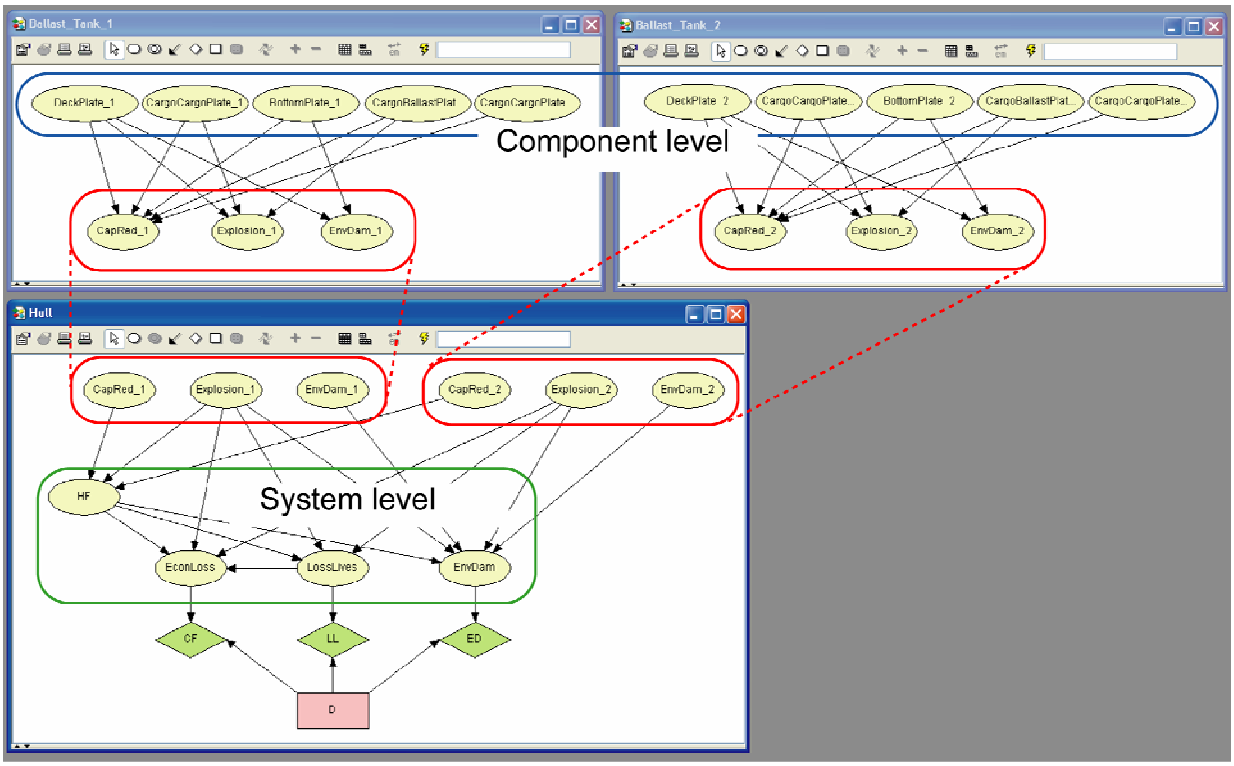

Figure 4: BPN's representative of tanks and hull structure.

Explosion_1

CargoBallastI	Fail				Survive			
CargoCargoP	Fail		Survive		Fail		Survive	
DeckPlate_1	Fail	Survive	Fail	Survive	Fail	Survive	Fail	Survive
No	0.4	0.5	0.8	0.8	0.4	0.5	0.6	1
Minor	0.5	0.45	0.1	0.19	0.55	0.49	0.35	0
Maior	0.1	0.05	0.1	0.01	0.05	0.01	0.05	0

Figure 5: Illustration of conditional probability table.

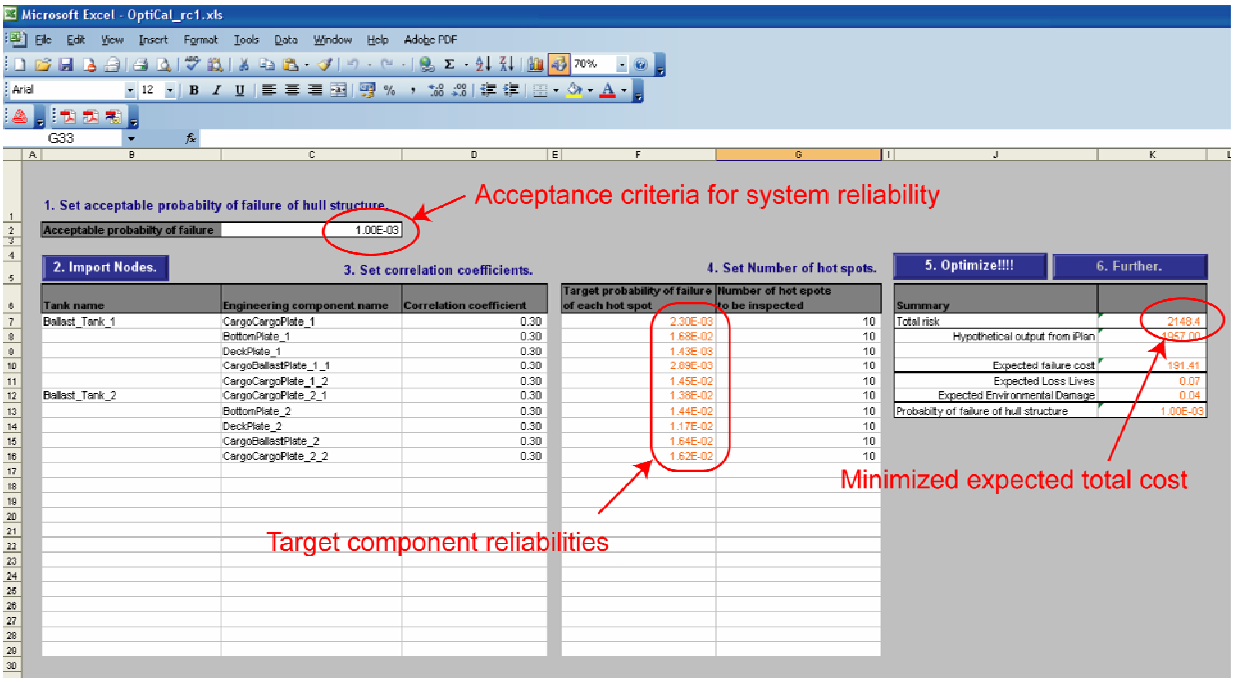

Figure 6: Screen dump of user interface of developed software tool.

5. Conclusions

The present paper proposes a framework for the modeling of complex system and for optimizing target reliabilities for components of systems with given requirements to the system performance, e.g. in terms of maximum acceptable risk. Appreciating the perspective that engineered systems are built up by standardized components which through their connections with other components provide the desired functionality and that the system performance will depend on the way the components are interconnected, the proposed framework takes basis in a hierarchical system modelling facilitated by an object based Bayesian Probabilistic Networks. Acceptance criteria defined on the system performance can be translated into the target reliability for the components through the hierarchical system model. Optimization of the target reliabilities for welded joints in a ship hull structure is shown as an example to illustrate how the proposed framework can be implemented into a software tool and thus utilized in practical situations.

References

ASCE7-98. (2000). "Minimum design loads for buildings and other structures, Revision of ANSI/ASCE."

Baker, J. W., Schubert, M., and Faber, M. H. (2007). "On the assessment of robustness." Structural Safety, In Press, Corrected Proof.

Bangso, O., Flores, M. J., and Jensen, F. V. (2003). "Plug & Play OOBNs." Lecture Notes in Artificial Intelligence, Springer Verlag, 457-467.

Bangso, O., and Olesen, K. G. "Applying Object Oriented Bayesian Networks to Large (Medical) Decision Support Systems." Proceedings of 8th Scandinavian Conference on Artificial Intelligence, SCAI'03, Bergen, Norway.

Bobbio, A., Ciancamerla, E., Franceschinis, G., Gaeta, R., Minichino, M., and Portinale, L. (2003). "Sequential application of heterogeneous models for the safetyanalysis of a control system: a case study." Reliability Engineering & System Safety, 81(3), 269-280.

Bobbio, A., Portinale, L., Minichino, M., and Ciancamerla, E. (2001). "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks." Reliability Engineering and System Safety, 71(3), 249-260.

Der Kiureghian, A., and Song, J. (2007). "Multi-scale reliability analysis and updating of complex systems by use of linear programming." Reliability Engineering & System Safety, In Press, Accepted Manuscript.
Faber, M. H., Maes, M. A., Baker, J. W., Vrouwenvelder, T., and Takada, T. "Principles of Risk Assessment of Engineered Systems." 10th International Concerence on Applications of Statistical and Probability in Civil Engineering, Chiba, Japan, Accepted to presentation.
JCSS. (2001). "Probabilistic Model Code." The Joint Committee on Structural Safety.
Jensen, F. V. (2001). Bayesian Networks and Decision Graphs, Springer, New York.
Kjaerulff, U. (1995). "dHugin: A computational system for dynamic time-sliced Bayesian networks."
Nathwani, J. S., Lind, N. C., and Pandey, M. D. (1997). Affordable Safety by Choice: The Life Quality Method, University of Waterloo, Waterloo.
Pemex. (2003). "Lineamiento para la determinación del nivel de riesgo tolerable en las instalaciones de proceso de la región marina noreste, Clave: 250-22100-SI-212-0001. Gerencia de seguridad industrial y protección ambiental, Enero del 2003, versión primera."
Rackwitz, R. (2002). "Optimization and Risk Acceptability Based on the Life Quality Index." Structural Safety, 24, 297-332.
Smyth, P. (1997). "Belief networks, hidden Markov models, and Markov random fields: A unifying view." Pattern Recognition Letters, 18(11-13), 1261-1268.
Straub, D., and Faber, M. H. (2006). "Computational Aspects of Risk-Based Inspection Planning." Computer-Aided Civil and Infrastructure Engineering, 21(3), 179-192.
USNRC. (1975). "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014)." U.S. Nuclear Regulatory Commission.
USNRC. (1990). "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150)." U.S. Nuclear Regulatory Commission.
Vesely, W. E., Goldberg, F. F., Roberts, N. H., and Haasl, D. F. (1981). "Fault Tree Handbook (NUREG-0492)." U.S. Nuclear Regulatory Commission.
Volovoi, V. (2004). "Modeling of system reliability Petri nets with aging tokens." Reliability Engineering & System Safety, 84(2), 149-161.