Rakenteiden Mekaniikka (Journal of Structural Mechanics)
Vol. 41, No 2, 2008, pp. 90-98

Risk-informed classification of systems, structures and components

Jan-Erik Holmberg and Ilkka Männistö

Summary. Risk-informed classification is based on utilising information from a risk analysis in a consistent way to select most cost-effective methods to control risk associated with systems, structures and components. An item's risk significance can be broken in two parts: probability of the failure and the consequence of the failure. Higher value in either will possibly mean a higher risk category, depending on the limit values for each category. Risk is controlled by assigning safety enhancing measures to each risk category. Risk-informed classification can be more efficient in reducing risks than the deterministic safety classification used in nuclear power plants. Nowadays also risk-informed classification is in use. Probabilistic safety assessments have shown that the risk significances of components and systems do not follow the simple assumption that components closer to the reactor have greater safety significance, and that many of the components and systems that in the traditional analysis are assigned to a higher safety class have low risk importance.

Keywords: probability, risk, risk analysis, probabilistic safety assessment, nuclear safety,risk-informed decision making, safety classification

Introduction

Classification tasks have been used to understand, manage and enhance a wide variety of real world processes and systems. These applications can range from assessing ships seaworthiness to organizing libraries. These are widely varying systems, except for one thing: they all can be very large and complex systems, given the large number of different kinds of ships and books in existence. Both of these systems have been simplified by classifying the ships or books into broader groups. Books are placed in different sections in library, and ships have classes for insurance purposes, for example. Finding anything in library would be more difficult without sections, as would be pricing insurance for a vessel if those were handled individually.

Classification can also be used for a greater understanding of a complex system. Qualities and relations inherent to the system being analyzed are many times more apparent when a broader class is examined, rather than individual items. Understanding a system is of course essential in the process of making it more efficient. Classification is not a purpose in itself — just a tool in improving or making viable another process.

The focus of this paper is to consider cases where classification is used as a method to allocate resources in safety management of hazardous processes or installations, such as a nuclear power plant. In this area of application, risk analysis can be used as a tool to

classify the items of the system under consideration. The findings presented is in this paper are based on a Master's Thesis (Männistö 2005).

Types of classification tasks

The basic classification task is to assign N items in terms of K classes based on the attributes of the item in question. Classification tasks may have different purposes such as:

- Pattern recognition. The purpose is to find a right solution using rules that generalises the essential features of the objects.
- Organisation of information. The purpose is to minimize the search effort by grouping items into classes that make the information more readily accessible, e.g., libraries organize books by their subject.
- Ranking systems. Ranking systems differ from the previous tasks in the sense that classes have an order. Ranking can be used to combine the relevant features of the item into a single measure, e.g., grading of exams into a few possible grades.
- Resource allocation. In cases where a cost or a use of limited resources is attached to each class, the goal of the classification task is an optimal distribution of the items to different classes.

This paper focuses on resource allocation type of classification problems in risk and reliability management context. The main idea in the classification is that the class of an item defines the resources used for the item, i.e., items within the same class are treated similarly. Another essential idea is that classes have an importance order. The items belonging to the most "important" class receive more resources while items belonging to less "important" class receive fewer resources. Examples of this kind of classifications are prisoner security classification, document security classification, maintenance strategy classification (e.g. of a nuclear power plant systems, aeroplane components, roads, buildings), risk classification of dams, safety integrity levels of automation systems (IEC 2005), patient or medical treatment classifications and insurance classifications.

In risk and reliability management application, two decision criteria are used in the selection of the class: cost and risk. Cost includes the certain part of the lifetime cost of an item, e.g. caused by scheduled maintenance. Risk expresses the uncertain part of the lifetime cost caused by randomly occurring events, e.g., failure of a technical system. In safety-critical systems, cost associated with failure events can be order of magnitude higher than scheduled costs. The small probability-high consequence feature of the system makes the classification task particular challenging for decision making. There are a few basic ways to construct a classification system. In an extreme case, there is only one class, and all items in the system are treated similarly. Another extreme case is that all items are treated exactly in proportion to their importance as if the set of classes was a continuous space. However, in relevant applications, a classification system has a finite number of classes. In a two-class system, the items are simply divided into important ones and non-important ones, e.g., safety-related components and non-safety-related components. A three-class system can be considered representative to all n>2 class sys-

tems, since in all these classification schemes the items are basically divided into three categories:

- items of highest importance receiving all reasonably available attention
- items of insignificant importance receiving minimal attention
- items of some importance receiving some attention.

Safety classification of structures, systems and components in nuclear power plants

In nuclear power plants, the systems, structures and components important to the safety are classified according to their safety significance. This safety classification determines requirements in design, qualification and regulatory review. It also implies the strictness of quality assurance (QA) controls that shall be followed in design, manufacturing, installation and operation of the items. QA requirements shall be consistent with the importance to nuclear safety of the item (IAEA 1996).

Historically, the assessment of the safety significance has been based on general design criteria for nuclear power plants and on deterministic safety analyses. This assessment has been followed in the safety classification of systems, structures and components.

In the Finnish regulatory framework, the systems, structures and components of the nuclear power plant are grouped into Safety Classes 1 (highest safety significance), 2, 3, 4 and Class EYT (classified non-nuclear) (STUK 2000):

- Safety class 1 (SC1) comprises of reactor fuel and major piping components and related structures in the reactor primary circuit boundary. There are e.g. no electrical or I&C systems or components in this class.

- Safety class 2 (SC2) comprises of the critical safety systems that perform the necessary safety functions for maintaining reactor safety in disturbances and design based accidents. The safety functions are reactor shutdown, core cooling, residual heat removal and containment isolation.

- Safety class 3 (SC3) includes systems having an essential effect on the reliability of the safety functions. Systems by which the accomplishment of the safety functions is monitored shall also be classified in SC3. In addition, SC3 shall include systems whose function is to reliably prevent the progression of initiating events into situations during which a system maintaining or actuating a safety function is needed.

- Safety class 4 (SC4) is a new class introduced to systems that do not belong to a higher safety class and whose failure could, however, cause an initiating event that could significantly endanger nuclear or radiation safety. SC4 shall include systems that during internal or external initiating events protect systems carrying out safety functions, for example the fire and flooding protection systems.

Risk-informed safety classification

In many countries, regulatory decision making processes are being revised in response to the developments occurring in the nuclear energy field, where a restructuring is in progress due to market deregulation and plans of extending operating licenses and plant lifetimes. Following the developments by the United States Nuclear Regulatory Commission (US.NRC 1998), many countries are embarking on the implementation of *risk-informed* regulation. By this, regulatory bodies expect to increase the effectiveness of regulation. The objective of the risk-informed regulation is to define requirements that are consistent with the risk importance of the equipment, events and procedures to which the requirements will be applied.

Analysis of balance in safety classification is part of risk-informed regulation and is nowadays even required in the Finnish regulatory framework (STUK 2003). The risk-informed analysis of safety classification means use of the plant-specific probabilistic safety assessment (PSA) to identify deviations between risk importance ranking and safety classes. For example, low risk-significance could indicate candidates for reductions in QA requirements and high risk-significance items may need stricter QA requirements.

The components of a nuclear power plant function as parts of a complex system that interact with each other, which makes it impossible to evaluate each components risk or importance without looking at the importance and function of all the other components at the same time. PSA methodology was developed to evaluate the risks and importances of components, and the overall risk, in nuclear power plants.

Probabilistic safety assessment (psa) and risk importance measures

A PSA is a comprehensive reliability model of a nuclear power plant that is based on the principle of dividing the reliability assessment to smaller, more manageable analysis tasks which are combined with Boolean logic to correspond to the actual nuclear power plant. PSA model consists of large number of initiating events, event sequence models and system reliability models in order to assess the risk of a core damage accident (level 1 PSA), risk of external radioactive release (level 2 PSA) and risk to the environment (level 3 PSA). Level 3 PSAs is not required in Finland.

PSA-model can be used to assess the relative importance of items of the model with respect to the consequence events modelled. In simple terms, we can express the PSA-model as a probability function

$$P(TOP; X_1,..., X_n), \tag{1}$$

where TOP is the unwanted event (TOP event), e.g. a reactor core damage accident and X_i is a basic event i associated e.g. with a component failure.

The function $P(\cdot)$ is a reliability structure function with binary random variables as arguments, i.e., the basic events can have two values TRUE ($X_i = 1$, component failure) or FALSE ($X_i = 0$, component available).

In the risk-informed classification, we can use two simple probability measures to classify the components, namely

- Unavailability or failure probability of a component

$$P(X_i = 1). \tag{2}$$

- Conditional TOP-event probability given an unavailable component

$$P(TOP = 1 \mid X_i = 1). \tag{3}$$

These two risk measures decompose the risk into two parts as follows

$$P(TOP = 1) = P(TOP = 1 \mid X_i = 1) P(X_i = 1). \tag{4}$$

Equation (4) corresponds to the common engineering definition that risk is the product of the consequence of failure and the failure probability.

Using these risk measures an item included in the PSA-model can be categorised into one of four categories as shown in Table 1. $P(X_i = 1)$ expresses the reliability of the component, while $P(TOP = 1 \mid X_i = 1)$ expresses the importance of the component in the defence-of-depth of the nuclear power plant. The defence-of-depth is a fundamental safety principle of nuclear power plant safety requiring several, independent successive barriers (passive structures, active safety systems, administrative measures, etc.) to prevent the propagation of a minor incident into a large accident (IAEA 1996).

High *P*(*TOP* =1 | *X* = 1) **Low *P*(*X* = 1)** • **Component is reliable** • **Component has an important role in the defence-in-depth of the plant**	**High *P*(*TOP* =1 | *X* = 1)** **High *P*(*X* = 1)** • **Component is unreliable** • **Component has an important role in the defence-in-depth of the plant**
Low *P*(*TOP* =1 | *X* = 1) **Low *P*(*X* = 1)** • **Component is reliable** • **Component has an insignificant role in the defence-in-depth of the plant**	**Low *P*(*TOP* =1 | *X* = 1)** **High *P*(*X* = 1)** • **Component is unreliable** • **Component has an insignificant role in the defence-in-depth of the plant**

Table 1. Interpretation of the risk importance measures.

The risk importance measures can be used in the selection of improvements in the following manner. High $P(X_i = 1)$ indicates that the reliability of the component should be improved e.g. by changing the component to a more reliability one or by increasing the reliability of the component by better quality control methods. High $P(TOP = 1 \mid X_i = 1)$ indicates that the degree of redundancy or diversity in the safety function should be increased.

The classification of the components using risk importance measures follows thus the principle that the risk importance measures determine the class and the class suggests the measures for controlling risk.

An X-Y plot can be used to visualize the components importance, by having the two measures on X- and Y-axes (Figure 1). The area is divided into three regions: the area of insignificant risk, the area of unacceptable risk and the risk trade-off area between them.

This division is consistent with the ALARA principle (As Low As Reasonably Achievable) followed in the radiation protection and also in nuclear safety management context (Bedford & Cooke 2001). The ALARA principle means that items in the unac-

ceptable risk area are not tolerated at all, items in the insignificant risk area are of no concern, and items in the middle are under further consideration for safety improvements if it can be economically justified.

The risk trade-off area or the ALARA area is further divided into three classes in this example as if we would have a three-class classification system (+ classes “unacceptable” and “insignificant”). The classes can have the following interpretation in nuclear power plant context:

Class 1

- Are part of important safety functions without back-up for mitigating rare initiating events
- Are part of important safety functions with back-up for mitigating common initiating event
- Can cause a very serious initiating event

Class 2

- Are part of back-up for important safety functions
- Can cause an initiating event of mediocre severity

Class 3

- Are part of back-up for less important safety functions
- Can cause a frequent initiating event.

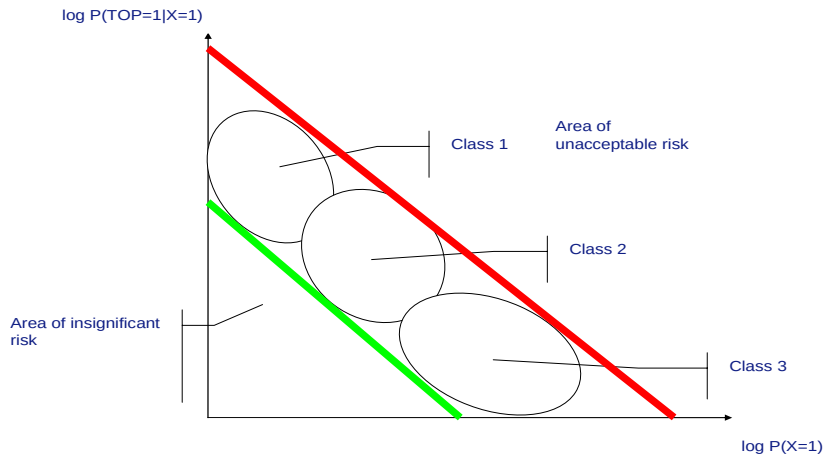

Figure 1. Principal XY risk plot dividing the area into three regions: area of insignificant risk, area of unacceptable risk and the risk trade-off area between them. The risk trade-off area is further divided into three classes 1–3.

The risk-informed classification approach presented here has been tested in a real case study where results from the level 1 PSA for Loviisa nuclear power plant were analysed using risk importance measures. Figure 2 shows a XY-plot of basic events included in the PSA model. In conclusion the Loviisa 1 safety functions are roughly bal-

anced. The initiating events with higher conditional core damage probabilities (CCDP) values also have small frequencies.

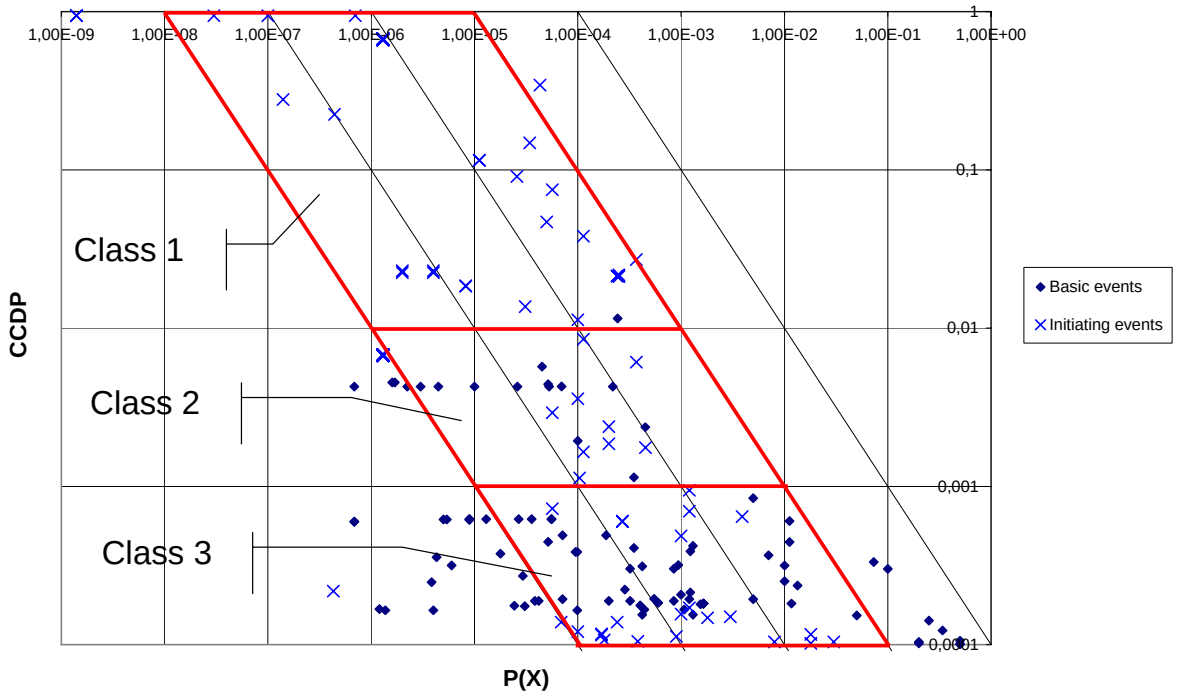

Figure 2. Three class classification of the components and initiating events in PSA for Loviisa 1. CCDP = conditional core damage probability, P(X) = basic event probability.

Conclusions

Risk-informed classification is used to control the overall risk in a systematic way. Each component that contributes to the risks in the system is classified based on its attributes, which are here the failure probability and consequences of the failure. Other risk measures could also be used depending on which actions are available to control the risk. Each class has measures that reduce the risks associated with the component. In the risk classification method presented here the risk control methods would have to either reduce the probability of failure or the consequences of the failure. Measures that reduce risks (redundant components, components with higher quality) consume resources, so it is very importance to identify the targets where the resources are most needed.

Risk-informed classification can be more efficient in reducing risks than the deterministic safety classification used in nuclear power plants, because risk studies have shown that the risk significances of components and systems do not follow the simple assumption that components closer to reactor have greater safety significance, and that many of the components and systems that in the traditional analysis are assigned to a higher safety class have low risk importance. However, it must be understood that the two principles are complementing each other, not competing with each other.

References

[1] T. Bedford and R. Cooke. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001.

[2] IAEA. Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installation: *Code and Safety Guides Q1-Q14, IAEA Safety Series No. 50-C/SG-Q*, International Atomic Energy Agency, Vienna, 1996.

[3] IAEA. *Defence in depth in nuclear safety, INSAG-10,* International Atomic Energy Agency, Vienna, 1996.

[4] IEC. *Functional safety of electrical / electronic / programmable electronic safety-related systems (E/E/PES), IEC 61508*, International electrotechnical commission, 2005.

[5] Männistö, I. *Risk-informed classification of components of nuclear power plants*, M.Sc. Thesis, Helsinki University of Technology, Department of engineering physics and mathematics, Espoo, 2005.

[6] STUK. *Nuclear power plant systems, structures and components and their safety classification*, Guide YVL 2.1, Radiation and Nuclear Safety Authority (STUK), Helsinki, June 2000.

[7] STUK. *Probabilistic safety analysis in safety management of nuclear power plants*, Guide YVL 2.8. Radiation and Nuclear Safety Authority (STUK), Helsinki, May 2003.

[8] U.S.NRC. *An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes to the licensing Basis*, Regulatory Guide 1.174, United States Nuclear Regulatory Commission, Washington, D.C., 1998.

Jan-Erik Holmberg and Ilkka Männistö
Technical Research Centre of Finland
Systems Research
P.O.Box 1000
FI-02044 VTT
Finland