# Application of Design Review to Probabilistic Risk Assessment in a Large Investment Project

**Seppo Virtanen[a] (*), Jussi-Pekka Penttinen[b], Mikko Kiiski[c], and Juuso Jokinen[c]**
[a] Tampere University of Technology, Finland, [b] Ramentor Oy, Tampere, Finland
[c] Pöyry Finland Oy, Vantaa, Finland

**Abstract:** In this paper, we present a systematic and comprehensive Design Review (DR) process that is integrated in design and engineering stages of final disposal facilities of spent nuclear fuel. The review process consists of seventeen interconnected phases and in the paper the methodology of certain phases is described in more detail. The main tools in the design review process are probabilistic modeling, stochastic simulation schemes, and large computer-aided calculation. Based on experience of the design review process application at an early stage of the project design and development phase it becomes possible to identify the problem areas, which may reduce the system availability and safety, increase the system life-cycle costs, and delay the design or operation start-up time.

**Keywords:** Design Review, RAMS, PRA, ELMAS

## 1. INTRODUCTION

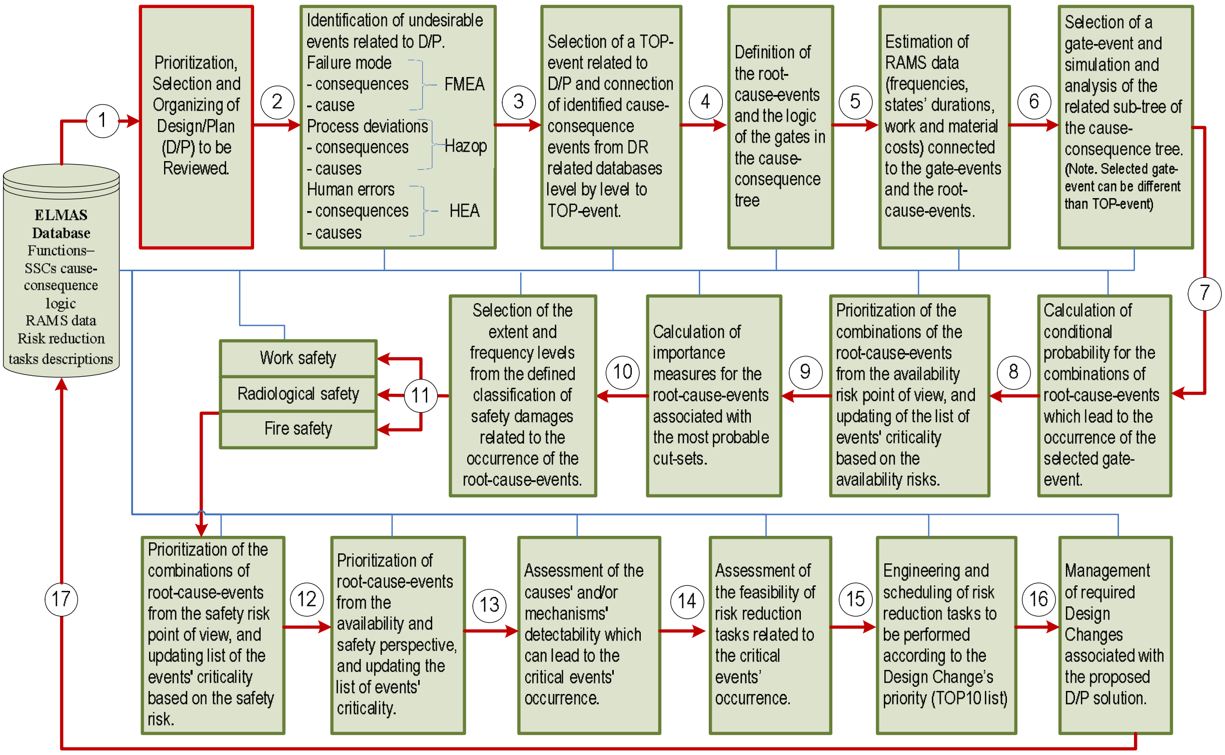
Final disposal facilities (FDF) of spent nuclear fuel must operate in a manner that meets their design intent over a period of many decades. Maintaining the safe operation expected of the FDF requires that the initial designs, as well as any changes made thereto during its lifetime are prepared, verified, validated, implemented, and controlled via a detailed, adequate, and structured process. As the owner of full responsibility for design, construction, maintenance, and operation of the FDF and as the maintainer of its reliable and efficient performance, the operating organization needs to establish and maintain a design review process that covers above aspects [1].

Since 1996 prof Virtanen's research team at Tampere University of Technology has produced design methods, simulation models and software to integrate the RAMS (Reliability, Availability, Maintainability, Safety) aspects into complex systems and service design and engineering processes. The research work has been carried out together with Finnish leading industrial companies, Finnish Defense Forces and the Finnish Funding Agency for Technology and Innovation (Tekes). The participants represent the manufacturers and users in metal, energy, nuclear power, electronics and process industries. Their systems have to meet high safety and availability demands. Ramentor Oy has successfully developed and refined these models and methods to a commercial software ELMAS. The focus of our research work during the last five years has been and still is to develop probabilistic methods for innovative system-service design and development, where ICT (information and communication technology) is integrated to the systems and IMS (intelligent maintenance system) is applied to the systems' probabilistic risk assessment and life cycle management.

The development of the design review process has been done since 2010 and applied in the design and engineering stages of the final disposal facilities of spent nuclear fuel, The facilities are to be owned and operated by Posiva Oy (www.posiva.fi/en) and the development of design review process has been managed by Pöyry Finland Oy (www.poyry.com) and done in collaboration with Tampere University of Technology (TUT) (www.tut.fi/en) and Ramentor Oy (www.ramentor.com). The review process consists of seventeen interconnected phases as shown in Figure 1. The main objective of the design review is to assure that at an early stage of the design is found and solved the problems, which delay the design or operation start-up time, reduce the plant's safety and availability, or increase the plant's life cycle costs.

The structure of the paper is as follows: In section 2 the method used for quantitative risk assessment is presented. In section 3 we discuss the system characterization for modeling of a power supply grid for the Encapsulation plant where the spent nuclear fuel is handled. Section 4 describes the principle of required design change management associated with proposed design solution. Section 5 deals with interpretation of the results.

**Figure 1: The concept of developed design review process**



ELMAS Database
Functions–SSCs cause-consequence logic
RAMS data
Risk reduction tasks descriptions
1
Prioritization, Selection and Organizing of Design/Plan (D/P) to be Reviewed.
2
Identification of undesirable events related to D/P.
Failure mode
- consequences
- cause
FMEA
Process deviations
- consequences
- causes
Hazop
Human errors
- consequences
- causes
HEA
3
Selection of a TOP-event related to D/P and connection of identified cause-consequence events from DR related databases level by level to TOP-event.
4
Definition of the root-cause-events and the logic of the gates in the cause-consequence tree
5
Estimation of RAMS data (frequencies, states' durations, work and material costs) connected to the gate-events and the root-cause-events.
6
Selection of a gate-event and simulation and analysis of the related sub-tree of the cause-consequence tree. (Note. Selected gate-event can be different than TOP-event)
7
Calculation of conditional probability for the combinations of root-cause-events which lead to the occurrence of the selected gate-event.
8
Prioritization of the combinations of the root-cause-events from the availability risk point of view, and updating of the list of events' criticality based on the availability risks.
9
Calculation of importance measures for the root-cause-events associated with the most probable cut-sets.
10
Selection of the extent and frequency levels from the defined classification of safety damages related to the occurrence of the root-cause-events.
11
Work safety
Radiological safety
Fire safety
Prioritization of the combinations of root-cause-events from the safety risk point of view, and updating list of the events' criticality based on the safety risk.
12
Prioritization of root-cause-events from the availability and safety perspective, and updating the list of events' criticality.
13
Assessment of the causes' and/or mechanisms' detectability which can lead to the critical events' occurrence.
14
Assessment of the feasibility of risk reduction tasks related to the critical events' occurrence.
15
Engineering and scheduling of risk reduction tasks to be performed according to the Design Change's priority (TOP10 list)
16
Management of required Design Changes associated with the proposed D/P solution.
17

## 2. METHOD USED FOR QUANTITATIVE RISK ASSESSMENT

A comprehensive system model that collects explicitly the facts affecting availability and safety risks is the basis of the design review process. The model is a result of risk identification made during the first 5) phases of the process. These phases detect, recognize and describe the root events with their likelihoods, the risk sources with the causal relations that lead to them, and the potential consequences of those risk sources. During the phases 6) to 12) the model is analyzed by means of stochastic discrete event simulation that produces quantitative risk results. In the last phase these results are used in risk evaluation and risk treatment that contains feasibility analysis and management of risk reduction tasks.

### 2.1. Simulation of Root Events

Those events that do not have their causes included in the model are called root events. A root event can be, for example, a failure or restoration of an item. The time until a root event occurs is defined by a cumulative probability distribution *F(t)*. The simulation of a random time *T* starts with computer generation of a random number *p* from the uniform distribution on the unit interval; this number is then transformed by the inverse of *F*, the so-called quantile function $F^{-1}$. For example, exponentially distributed random time with mean $\mu$ is given by

$$T = F^{-1}(p) = -\mu \ln(1-p) \qquad (1)$$

### 2.2. Causal Relations Model of Events that Lead to Risk Sources

Fault tree methods are traditionally applied to modelling of chains of events that lead to an undesired event [2,3]. A similar systematic approach is used in our causal relations model to model the chains of events that lead to risk sources. It should be noted that there can be more than one separate risk source.

The structure of a causal relations model is more versatile than traditional fault tree models and thus satisfies the needs of complex modeling situations more adequately. As a fault tree consists of events a causal relations model consists of nodes. A node models an item of the studied entity and it can have several states and be faced with several events. A state is a particular set of circumstances related to the item, for example normal operation, fault, maintenance or wait. An event is a state transition, for example failure, restoration, maintenance action or shutdown.

In the following examples, the nodes only have two states, that are 0 and 1, so that they can be directly used in calculations. At the end of this chapter, the changes required for the use of more than two states are explained. Besides the maintenance, for example operation strategies can require extra states. Failed waiting state must be included if component repair cannot be started while the system is operating and non-failed wait state if the component is shut down when the system is not operating. An example of operation strategies modelling is presented in chapter 2.5 [4].

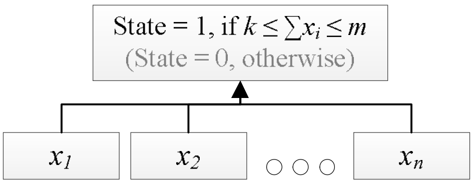
In addition, the relations between nodes are defined more freely with respect to traditional fault tree. The relation is a function from a list of states of input items to a list of states of output items. This relation function covers basic fault/cause tree relations that have several input items and a single output item and event/consequence tree relations that have a single input item and several output items.

As an example of fault/cause tree relation the basic logic relations can be defined by a function

$$L_{k,m}(x_1,x_2,\dots,x_n)=\begin{cases}1 & \text{if } k\le\sum_{i=1}^{n}x_i\le m\\ 0 & \text{otherwise}\end{cases} \tag{2}$$

in which the parameter where $x_i$ is the state of the input node *i*, and the return value of the function is the state of the single output node of the relation. The variable *k* is the number of inputs needed at least and the variable *m* is the number of inputs allowed at most, illustrated in Figure 2. As an example this function models the traditional fault tree OR-relation with parameters *k=1*, *m=n*, AND-relation with *k*=*m*=*n*, generalized XOR (exactly *a* inputs) with *k*=*m*=*a* and NOT-relation with *k*=*m*=0 [5].

**Figure 2: Logic relation with parameters k (at least) and m (at most)**

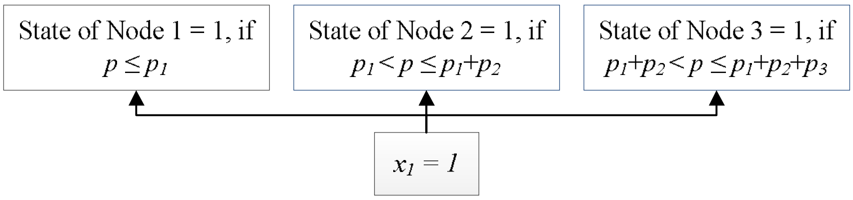


As an example event/consequence tree relation a stochastic relation between a single input node and three exclusive output nodes can be defined by a function

$$S_{p_1,p_2,p_3}(x_1,p)=\begin{cases}[0,0,0] & \text{if } x_1=0 \text{ or } p_1+p_2+p_3<p\\ [1,0,0] & \text{if } x_1=1 \text{ and } p\le p_1\\ [0,1,0] & \text{if } x_1=1 \text{ and } p_1<p\le p_1+p_2\\ [0,0,1] & \text{if } x_1=1 \text{ and } p_1+p_2<p\le p_1+p_2+p_3\end{cases} \tag{3}$$

in which parameter $x_1$ is the state of the input node number 1, *p* is a random uniform, $p_i$ is the probability that output *i* occurs, and the return value of a function is a list of the states of the three output nodes. The relation is illustrated in Figure 3.

**Figure 3: Stochastic relation of three exclusive outputs** (Nodes 1, 2 and 3)

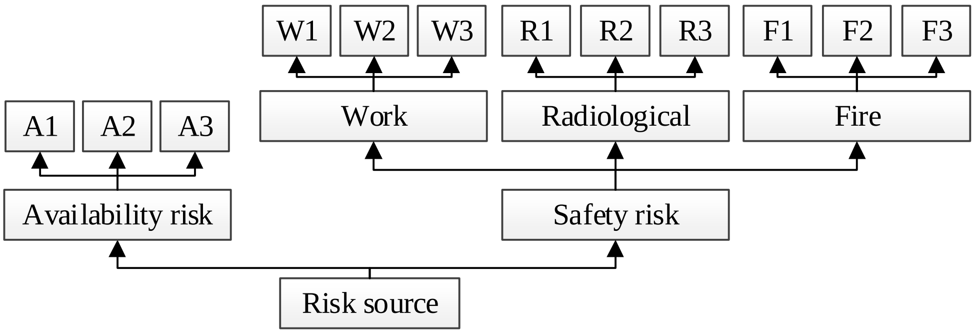

State of Node 1 = 1, if $p \leq p_1$
State of Node 2 = 1, if $p_1 < p \leq p_1+p_2$
State of Node 3 = 1, if $p_1+p_2 < p \leq p_1+p_2+p_3$
$x_1 = 1$

With models that have more than two possible states in each node the relation functions are extended correspondingly. The default solution is to use the simple two state function successively for each extra state. For example with three states, normal state, fault state and waiting state, the relation function is used twice. With the previously defined logic relation function, the number of fault states of the input nodes is calculated first. If there are at least *k* and at most *m* fault states, the output state is fault state. Otherwise, the number of waiting states of input nodes is added to the number of fault states. If the sum is between *k* and *m* then the output state is wait and otherwise the output state is normal. Of course, if the default solution is not satisfactory enough, it is possible to create a complex relation function that satisfies the needs directly.

## 2.3. Classification Model of Potential Consequences of Risk Sources

The causal relations model defined in the previous chapter is used to define the chains of events that lead to risk sources. The potential consequences of the found risk sources can be modelled by using the relation functions similarly. In the design review process, the consequences of each risk source are modelled by using classification. Before the risk classes are defined the risks are grouped to availability risk and safety risk which is related to work, radiological or fire safety, see Figure 4.

**Figure 4: Classification of potential consequences of a risk source**

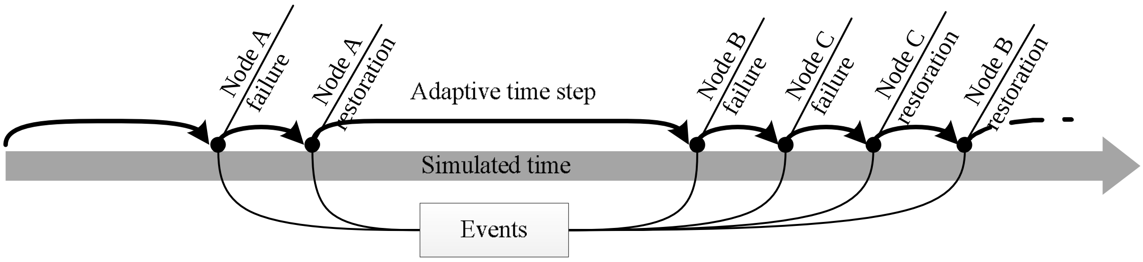


There can be as many risk classes related to each risk group as needed. For each class a probability is defined to model the relation between the risk source and the consequence. The probability is estimated based on the results of qualitative and quantitative analyses, the knowledge of experts or other available information.

## 2.4. Risk Analysis Based on Stochastic Discrete Event Simulation

Simulation is made by handling events in chronological order. The time step between events is adaptively based on stochastic occurrence times, see Figure 5. It is also possible that more than one event occurs exactly at the same time.

**Figure 5: Stochastic discrete event simulation with adaptive time step**



The root event times are simulated by using the likelihood quantile functions. After each root event the node states are updated based on the relation functions. After each step, the node states are stored for the calculation of versatile analysis results. The basic nodes related results are for example the times spent in each state or the number of occurrences of events. More complex results related to conditional probabilities, combinations or importance measures are also obtained [6].

### 2.5. Dynamic Modelling and Simulation

Special programming code can be included to nodes of the model for the handling of special situations. The code is divided into step code and event code based on the place of the simulation algorithm the code is attached to. The step code is executed between the events when the simulation time changes and the event code when an event occurs. In ELMAS software a library of predefined dynamic modules is made available so the user can only define needed parameters without programming skills required.

An example of a module related to the step code is the update of a buffer variable. The variable can be for example the charge level of a backup battery. The user gives only charging and power consumption speeds and the full charge limit as parameters and the code included in the dynamic module handles automatically the changes of charge level based on the node states. These added variables can also be used parameters in likelihood or relation functions. This way the dynamic relations can be defined and, for example, a failure time of an item can be different in different situations.

The programming code can be used to create events which are handled similarly to the root events. The rules when the events are created can be related to other events or, for example, if the battery is empty or full some special event can be created. It should also be noted that this way relations in opposite causal order defined by basic logic relations can be created. Otherwise, the loops in causal relations are not allowed.

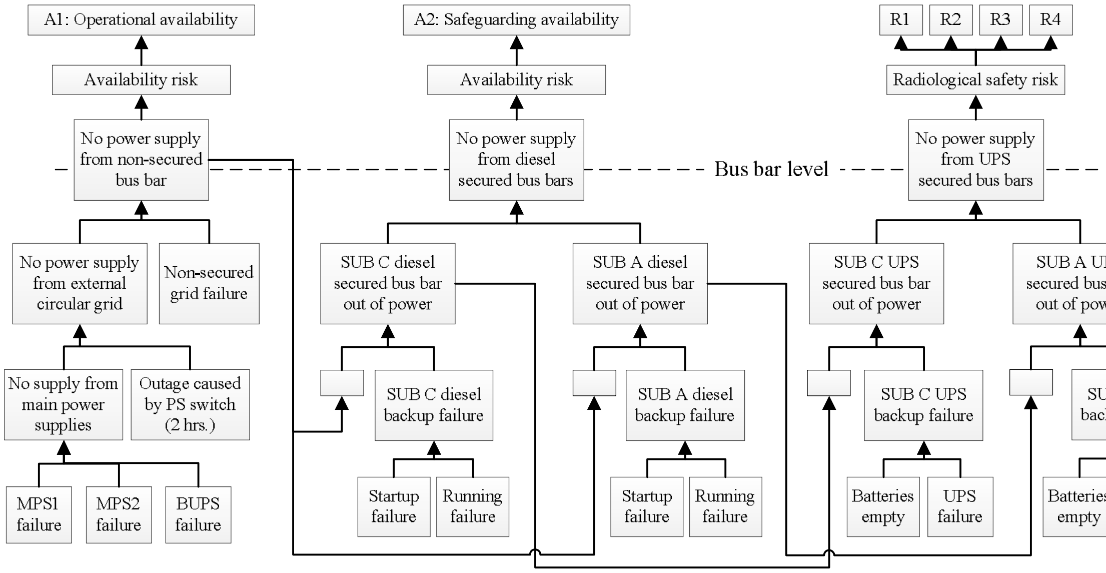
A module related to event code can be for example the choice of an operation strategy. The user can select from a check box whether the component can be repaired while the system is operating or not [4]. In case the repair cannot be started normally, the module includes a programming code to a simulation that sets the node to wait state after a failure occurs.

The event code can be used to model relations that contain delays. For example, a failure of a component can create an event that starts the backup component after a while. Another example is a rescue of a gate where the normal logic relation can be ignored after a certain special repair time. With the rescue of a gate module included, the user can just select the rescue mode on and define the repair time related to the rescue. The module adds the rescue event after the repair time and updates the relation function so that the basic logic relation is ignored [7].

## 3. POWER SUPPLY GRID EXAMPLE

The risk assessment method described in the previous chapter is applied to a power supply grid for the Encapsulation plant where the spent nuclear fuel is handled. The grid has three different priority bus bar levels, as shown in Figure 6. Lack of power supply in each of them is a separate risk source and requires separate classification for the potential consequences. A simplified structure of the power supply grid is shown as an example. Only the major sub-systems of the grid and the main connections between the bus bar levels are included in the causal relations model. The classification model of this example is simplified to contain only one class of availability risks for two of the risk sources and four level classification of the radiological safety related risk for the third risk source. A deeper modeling of root events and the more detailed classification is made similarly in the actual case.

**Figure 6: Simplified structure of the power supply grid**


A1: Operational availability
A2: Safeguarding availability
R1
R2
R3
R4
Availability risk
Availability risk
Radiological safety risk
No power supply from non-secured bus bar
No power supply from diesel secured bus bars
Bus bar level
No power supply from UPS secured bus bars
No power supply from external circular grid
Non-secured grid failure
SUB C diesel secured bus bar out of power
SUB A diesel secured bus bar out of power
SUB C UPS secured bus bar out of power
SUB A UPS secured bus bar out of power
No supply from main power supplies
Outage caused by PS switch (2 hrs.)
SUB C diesel backup failure
SUB A diesel backup failure
SUB C UPS backup failure
SUB A UPS backup failure
MPS1 failure
MPS2 failure
BUPS failure
Startup failure
Running failure
Startup failure
Running failure
Batteries empty
UPS failure
Batteries empty
UPS failure

### 3.1. System Description

The basis of the power supply grid is a non-secured bus bar, see Figure 6. It has two separate main power supplies (MPS1 and MPS2) and a third backup power supply (BUPS) with reduced supply capacity. A switch between power supply sources takes two (2) hours and coincidentally causes two (2) hours of downtime for non-secured normal bus bar. Because of the reduced supply capacity by the BUPS the main power supplies are preferred whenever available. In addition to the lack of power supply also grid failures of the non-secured bus bar are possible. The other causes for the failure are not included in this example.

The non-secured bus bar is used to supply power for non-critical loads. It also provides a normal power supply to two identical diesel secured bus bars (SUB C and SUB A), as illustrated in Figure 6. Both SUBs have their own diesel generators, which are used if the non-secured bus bar is down. The generators are all the time on warm standby and therefore the start-up delay is minimized but there is 0.29% probability of a startup failure. Either one of the diesel secured bus bars is alone capable to provide sufficient electricity for the critical loads.

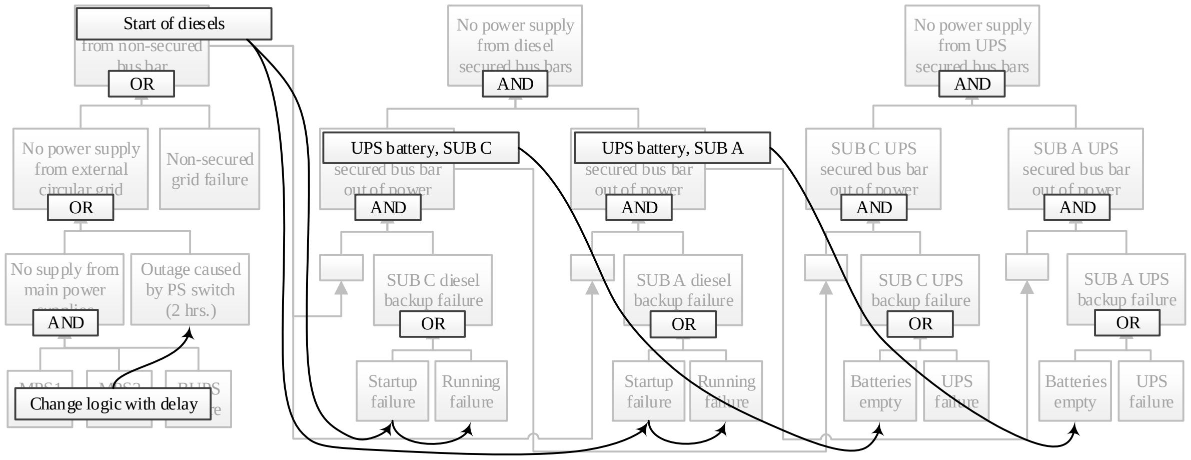
Both of the diesel secured bus bars provide power supply to their own UPS secured bus bars. The UPS secured bus bars are equipped with on-line UPS units that have three (3) hours of battery capacity each. Similarly with the diesel secured bus bar either one of the UPS secured bus bar is capable to provide sufficient electricity for the high priority critical loads.

The power supply grid is always in use and can also fail at any time. However, the handling of spent nuclear fuel to the Encapsulation plant is not made continuously. There is about 10% probability that a power supply failure occurs at the time when the handling operation is ongoing. The non-secured bus bar provides power supply needed in operations, and the diesel secured bus bars provide power supply for the safeguarding systems needed during the operation. The lack of power in UPS secured bus bar can cause radiological safety risk at any time, for example due to the loss of radiation monitoring. The extent of radiological safety risk is classified to four different levels that have their own probabilities R1 (100%), R2 (15%), R3 (1%) and R4 (0.1%), see Table 2. The three risk sources have also other potential consequences but the analysis of those is not included in this example. The probability values of Table 2 were derived based on the planned process cycle at the facility and for the diesel generator startup failure sourced from IAEA-TECDOC-478 [8].

### 3.2. Causal Relations Model of the Example System

The relations between the nodes of the model are mainly basic logic relations (OR, AND). Special rules are needed in three different situations. The first of them is a logic related to changing between MPS1, MPS2 and BUPS with the delay included in each change. The second is the startup of backup diesel generators after a lack of power supply in non-secured bus bar. The third is the use of UPS after a lack of power supply in a diesel secured bus bar. Causal relations added to the simplified structure of the power supply grid (Figure 6) are illustrated in Figure 7.

**Figure 7: Causal relations model of the example system**



Start of diesels
No power supply from non-secured bus bar
OR
No power supply from diesel secured bus bars
AND
No power supply from UPS secured bus bars
AND
No power supply from external circular grid
OR
Non-secured grid failure
UPS battery, SUB C
secured bus bar out of power
AND
UPS battery, SUB A
secured bus bar out of power
AND
SUB C UPS secured bus bar out of power
AND
SUB A UPS secured bus bar out of power
AND
No supply from main power supplies
AND
Outage caused by PS switch (2 hrs.)
SUB C diesel backup failure
OR
SUB A diesel backup failure
OR
SUB C UPS backup failure
OR
SUB A UPS backup failure
OR
MPS1
MPS2
BUPS
Change logic with delay
Startup failure
Running failure
Startup failure
Running failure
Batteries empty
UPS failure
Batteries empty
UPS failure

The change logic between MPS1, MPS2 and BUPS is a selection of a switch each time after a failure. If either MPS1 or MPS2 is available it is selected in use, otherwise BUPS is selected. If BUPS is selected a change is made back to MPS1 or MPS2 immediately when possible. All failure and repair times for root nodes are listed in Table 1. When the change is made an outage node is set failed for two (2) hours. A variable to tell the currently selected power supply is added to the simulation.

Both backup diesels are started after a lack of power supply of non-secured bus bar. There is no delay but there is 0.29% probability of a startup failure. All probabilities of the relations are listed in Table 2. For a dynamic simulation code, it is also possible to add tests including random number generation. In the case of a startup failure, the startup failure node is set failed with mean restoration time of 330 minutes. Running failure node is at wait state normally but after a successful startup, it is changed to operating state. In case operation failures occur, the node can change to failed state. When the non-secured bus bar provides power supply again, the node is set to wait state again.

Use of UPS battery is started after a lack of power supply in the corresponding diesel secured bus bar. Both bus bars SUB C and SUB A have similar operating logic regarding the UPS battery. A failure event for the ‘UPS battery empty’ node is created when the battery goes out of charge after 180 minutes of usage. After the revival of diesel secured bus bar, the node fault state ends. Modelling of the recharge time is not included in the example. The model is created in the phase 4) of the design review process.

### 3.3. Input Values for the Root Events and Probabilities of the Relations

It is possible to select the most suitable probability distributions for each root event. In ELMAS software a palette of probability distributions with various parameter inputs is made available for the user [4]. However, in this example all failure and restoration times are exponentially distributed and for power source switch outage and battery capacity an exact value is always used. This simplification does not affect the phases of the design review process.

Even though our simplified structure of the power supply grid does not contain component level nodes, the failure and repair data of root events were derived from the original component level power supply grid model. The component level model based on the application specific data, expert judgments data and use of data sourced from IAEA-TECDOC-478 [8], T-book [9], SINTEF PSA handbook [10] and this data is transferred to this simplified model. The input values for the simplified structure, compiled in Table 1, were calculated by simulating corresponding sections of the component level model. The difference between MPS1 and MPS2 input data is the result of differences in the power supply routing and components related to these power supplies outside our model boundaries.

**Table 1: Root event input values for the analysis**

| Item(s) | MTTF | MTTR | Notes |
|---|---|---|---|
| Main power supply 1 (MPS1) | 3989 d | 1010 min | Primary source, most reliable supply |
| Main power supply 2 (MPS2) | 2397 d | 1059 min | Alternative, more complex source |
| Backup power supply (BUPS) | 824 d | 557 min | Limited capacity, least reliable supply |
| Power source switch outage | - | 120 min | Time when supply changed |
| Non-secured grid failure | 6444 d | 946 min | Grid failures, excluding supply |
| Backup diesel startup failure | - | 330 min | Repair time after startup failure |
| Backup diesel running failure | 114 d | 303 min | After startup successful |
| UPS failure | 3511 d | 603 min | Independent, can occur even without use |
| UPS battery empty | 180 min | - | Time of battery capacity |

**Table 2: Probabilities of the relations for the analysis**

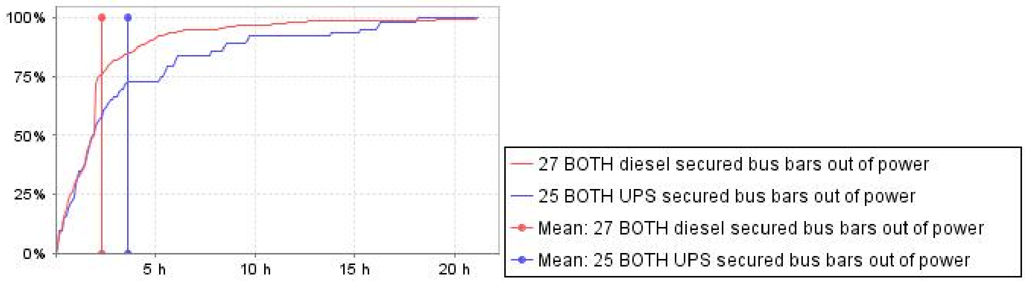
| Item(s) | Probability | Notes |
|---|---|---|
| Backup diesel startup failure (both) | 0.29 % | Started after non-secured bus bar failure |
| A1: Operational availability risk | 10 % | After non-secured bus bar failure |
| A2: Safeguarding availability risk | 10 % | After concurrent diesel secured bus bar failures |
| R1: Possibility of radiological safety risk | 100 % | After concurrent UPS secured bus bar failures |
| R2: Minor radiological safety risk | 15 % | After concurrent UPS secured bus bar failures |
| R3: Severe radiological safety risk | 1 % | After concurrent UPS secured bus bar failures |
| R4: Critical radiological safety risk | 0.1 % | After concurrent UPS secured bus bar failures |

An estimation of the input values is made in phase 5) of the design review process.

### 3.4. Analysis Results

The analysis is conducted by simulating a 120 year long period 500 000 times. The simulation is based on the estimated life cycle of the Encapsulation plant. According to the simulation results the mean frequency of no power supply from both UPS secured bus bars is 0.0001/120 a. The same result for both diesel secured bus bars is 0.0005/120 a. The mean duration of no power supply is three (3) hours with UPS secured bus bars and two (2) hours with diesel secured bus bars. The cumulative distribution of the out of power supply durations is shown in Figure 8.

**Figure 8: The durations of out of power supply situations**



The mean frequency of ‘No power supply from non-secured bus bar’ is 20/120 a. There will be at least 13 failures (5 % quantile) and at most 28 failures (95 % quantile). The mean time spent on restoration is 6.5 hours and the availability is 99.987%.

Conditional probabilities of combinations that cause non-secured bus bar failures are calculated and shown in Table 3. From the results, it can be found out that the ‘No power supply from non-secured bus bar’ is mainly caused by grid failure if we consider the fault time. However, the failures are most often triggered by the outage caused by power source switch. The similar results can also be seen from the importance measures.

**Table 3: Conditional probabilities of combinations that cause non-secured bus bar failures**

| Minimal cut set | Time of no power supply | Triggers no power supply situation |
|---|---|---|
| Non-secured grid failure | 80 % | 33 % |
| Outage caused by PS switch | 20 % | 66 % |
| All MPS1, MPS2 and BUPS failed | < 1E-4 % | < 1E-4 % |

Because of the possibility to add delays and other special rules in relations, the conditional probabilities and importance measures must be studied carefully. For example, based on the basic causality logic the ‘Outage caused by PS switch’ will lead to lack of power supply itself, but because of the special change logic relation of power supplies it never occurs by itself. To make the interpretation of the results more straightforward it is possible to consider the delays and special rules in the calculation of conditional probabilities and importance measures but the details of these procedures are not included in this paper. For very rare events, it is sometimes useful to combine the simulation results with analytical calculations. For example, with the selected classification model of potential consequences, the results for the consequences can be calculated analytically based on the simulated results of the risk sources. The results are shown in Table 4. The combination of simulation and analytical results is demanding if the consequence model is more complex.

**Table 4: Results for the potential consequences of the risk sources**

| Consequences of risk sources | Frequency during 120 a period |
|---|---|
| A1: Operational availability risk | 2.0 |
| A2: Safeguarding availability risk | 5E-5 |
| R1: Possibility of radiological safety risk | 1E-4 |
| R2: Type I radiological safety risk | 1.5E-5 |
| R3: Type II radiological safety risk | 1E-6 |
| R4: Type III radiological safety risk | 1E-7 |

The analysis is made during the phases 6) to 12) of the design review process.

### 3.5. Assessment of Design Change Priority related to Risk Reduction Tasks

The quantitative risk assessment made for the system in previous chapters points out the most significant failures and combinations of failures from availability and safety risk point of view. In order to be able to prioritize design changes to be performed, in phases 13) and 14) qualitative analysis methods are used to identify the failure mechanisms and to find out the risk reduction tasks related to these critical failures. The effect on the input values is estimated for each defined risk reduction task. The scenario analysis is made with the changed input values of root events and the results are compared to the results of the initial analysis.

Assessment of detectability of the causes' and/or mechanisms' (=weak spots) that can lead to these critical failures is studied in phase 13). Detection is an assessment of the ability of the design review process to identify potential weak spots with in design and development phases before the plant commissioning and startup. The detectability is estimated from 1 (almost certain) to 10 (almost impossible) as shown in Table 5 [11]. Assessment of the feasibility of risk reduction tasks related to occurrence of critical failures is studied in phase 14). Feasibility estimation of tasks is a challenging problem. The evaluation is performed by posing the questions: "How feasible is it to implement a given corrective action (which will reduce either frequency or extent of consequences) under the existing constraints of available technology, human resources, cost and time". The feasibility is estimated with the same scale as detectability, from 1 (almost perfect) to 10 (almost impossible), Table 5. [12].

**Table 5: Ranging of detectability and feasibility**

| Detectability | | | Feasibility | | |
|---|---|---|---|---|---|
| Almost certain | 1 | Review/inspection will almost certainly detect a potential cause/mechanism and subsequent failure mode. | Almost perfect | 1 | Fully available resources, remote cost and time consumption, 100% chance of success and zero probability of undesirable |
| Very high | 2 | Very high chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Very high | 2 | Very highly available resources, very low cost and time consumption, near 100% chance of success and near zero probability of undesirable impact |
| High | 3 | High chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | High | 3 | Highly available resources, low cost and time consumption, high chance of success and low probability of undesirable impact |
| Moderately high | 4 | Moderately high chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Moderately high | 4 | Rather highly available resources, rather low cost and time consumption, rather high chance of success and rather low probability of undesirable impact |
| Moderate | 5 | Moderate chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Moderate | 5 | Moderate availability of necessary resources, moderate cost, mderate time consumption, moderate chance of success and moderate probability of undesirable impact |
| Moderately low | 6 | Moderately low chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Moderately low | 6 | Rather low availability of necessary resources / Rather high cost or time consumption / Rather low chance of success / Rather high probability of undesirable impact |
| Low | 7 | Low chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Low | 7 | Low availability of necessary resources / High cost or consumption / Low chance of success / High probability of undesirable impact |
| Very low | 8 | Very low chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Very low | 8 | Very low availability of necessary resources / Very high cost or time consumption / Very low chance of success / Very high probability of undesirable impact |
| Remote | 9 | Remote chance the review/inspection will detect a potential cause/mechanism and subsequent failure mode. | Remote | 9 | Remote availability of necessary resources / Unacceptable cost or time consumption / Remote chance of success / Almost 100% probability of undesirable impact |
| Almost impossible | 10 | Review/inspection will not / cannot detect a potential cause/mechanism and subsequent failure mode or there is no review/inspection. | Almost impossible | 10 | Safety problem / Noncompliance to government regulation / Unavailable necessary resources / Impossible cost or time consumption / Zero chance of success / 100% probability of undesirable impact |

In our example system, two root events related to operational availability risk caused by ‘No power supply from non-secured bus bar’ node are defined. The risk reduction tasks and their impact on the operational availability risk are shown in Table 6. In the design review (DR) debriefing meeting in phase 15), the design change’s priority is assessed based on the combination of tasks' impact on availability risk, and detectability and feasibility according to Table 5. The risk reduction tasks’ availability improvements are simulated with new task-updated root event input values. By comparing these results with the initial simulation results the task related availability improvement can be measured.

**Table 6: Scenario analysis of the risk reduction tasks**

| Root event | Risk reduction task | Availability improvement (ΔA) | Detect-ability | Feasibility | Design change’s priority |
|---|---|---|---|---|---|
| Non-secured grid failure | Grid improvement: MTTF doubled (12888 d) | 99.992 % (0.005 pp) | 2 | 3 | 1 |
| Outage caused by PS switch | Streamlining of PS switch process: switch time halved (60 min) | 99.988 % (0.001 pp) | 2 | 7 | 2 |

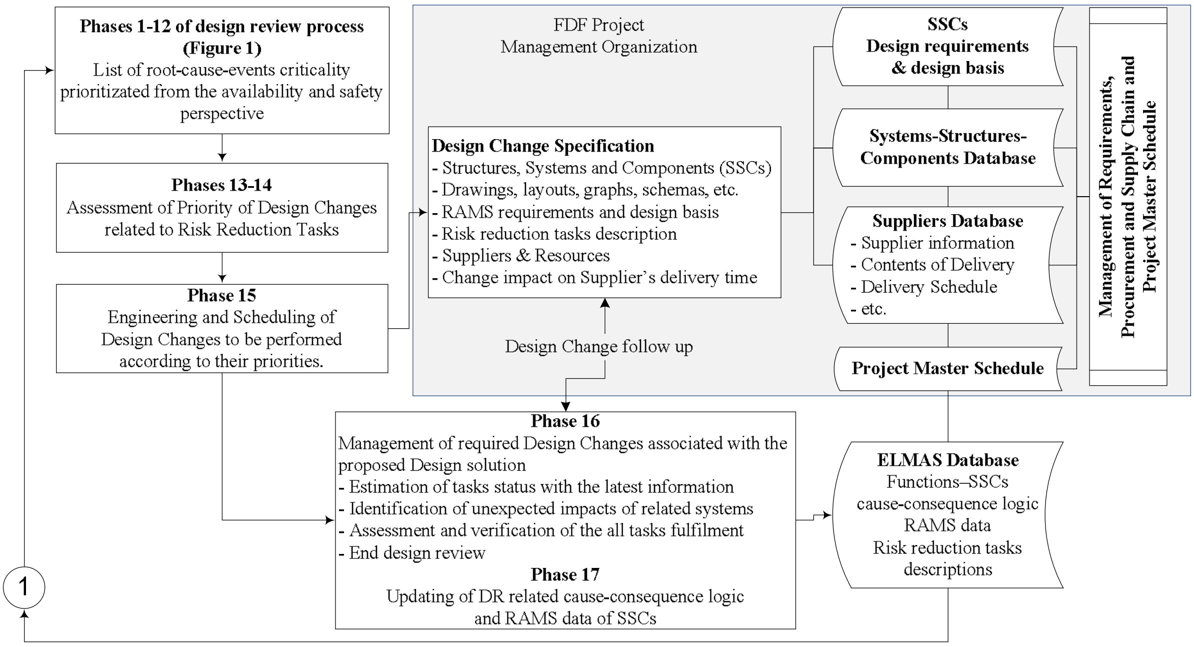
The participants in DF debriefing meetings should be from different design disciplines in order to have the tasks cross-disciplinary effects taken into account. Decisions made in design review debriefing meetings defines the measures for the selected prioritized improvement tasks including for example task description, responsibilities, suppliers/resources, status, expiry date and history.

## 4. MANAGEMENT OF REQUIRED DESIGN CHANGES

The principle of required design change management associated with proposed design solution is illustrated in Figure 9. The key success factor for the design change management (phases 15, 16 and 17) is the causal connection to the management of design requirements, procurement and supply chain, and project master schedule (see Figure 9). When the FDF is being built the designing is an integrated process involving mainly the vendors, which range from systems and structures suppliers to the suppliers and designers of main and individual components, but it also includes many other entities involved in construction and commissioning. These entities should conform to the appropriate RAMS assurance requirements in order to ensure a safe and efficient design of the FDF.

The owner/operating organization bears the full responsibility for the correctness and adequacy of the design of the facility and is fully responsible for its independent verification, even if parts of it are entrusted to separate vendor organization [1]. Thus, it has to verify the vendors' work through a discerning design review. The operating organization should therefore have the capability of understanding and confirming the design and the design changes through a rigorous and structured design review and acceptance process throughout the plant lifetime.

**Figure 9. Principle of risk reduction tasks management**


Phases 1-12 of design review process (Figure 1)
List of root-cause-events criticality prioritizated from the availability and safety perspective
Phases 13-14
Assessment of Priority of Design Changes related to Risk Reduction Tasks
Phase 15
Engineering and Scheduling of Design Changes to be performed according to their priorities.
FDF Project Management Organization
Design Change Specification
- Structures, Systems and Components (SSCs)
- Drawings, layouts, graphs, schemas, etc.
- RAMS requirements and design basis
- Risk reduction tasks description
- Suppliers & Resources
- Change impact on Supplier's delivery time
Design Change follow up
SSCs
Design requirements & design basis
Systems-Structures-Components Database
Suppliers Database
- Supplier information
- Contents of Delivery
- Delivery Schedule
- etc.
Project Master Schedule
Management of Requirements, Procurement and Supply Chain and Project Master Schedule
Phase 16
Management of required Design Changes associated with the proposed Design solution
- Estimation of tasks status with the latest information
- Identification of unexpected impacts of related systems
- Assessment and verification of the all tasks fulfilment
- End design review
Phase 17
Updating of DR related cause-consequence logic and RAMS data of SSCs
ELMAS Database
Functions–SSCs
cause-consequence logic
RAMS data
Risk reduction tasks descriptions
1

After the phase 15) the FDF project management organization conducts the Design Change Specification. In phase 16) The FDF project management organization provides the latest information from the Design Change Specification status to the DR team managing the DR data and analysis for the DR follow-up meetings. The DR team uses the information to manage the improvement tasks cross-disciplinary. It is important to make an estimation of tasks status and identification of unexpected impacts of the design on all related systems. Also the assessment and verification of the change impact to risk reduction and/or prevention tasks with the latest information will be conducted. After the analysis with the latest information the DR team will send the updated proposal task listings to DR follow-up meeting participants.

DR follow up meetings are held for selected improvement tasks at predetermined dates depending on their status. The participants of the meeting will define the status and possible measures for the selected improvement task based on the latest analysis and information. Depending on the decision, the tasks will be revised to be redesigned or to be closed. In phase 17) the DR related database and the cause-consequence logic related to the DR object will be updated and the information will be taken into account for later decisions for example to carry out a new DR process for the system starting again from phase 1).

## 5. CONCLUSION

In this paper, we presented design review process that consists of seventeen interconnected phases and described its certain phases in more detail. The design review process is integrated in the design and engineering project stages of the final disposal facilities of spent nuclear fuel. The main tools in the design review process are probabilistic modelling, stochastic simulation schemes and large computer-aided calculation. Based on the experience of the design review process' application at an early stage of the project design and development phase, it becomes possible to identify the problem areas which may reduce the system availability and safety, increase the system life-cycle costs and delay the design or operation start-up time. Application of the design review process and its methodology is not limited to large scale investment projects, such as new nuclear power plant, but it can also be applied to other industrial investment projects with probabilistic risk assessment and management as an integral part of it.

### Acknowledgements

We would like to express our special gratitude and thanks to Posiva Oy for funding and supporting this research and development work as part of the final disposal facilities of spent nuclear fuel project. We extend our gratitude to the concerned members of Posiva for providing us the user cases, helpful for this research work.

### References

[1] IAEA, 621-15-TM-44714, "Technical meeting on "Design review process to support expansion and new NPP programme", IAEA Headquarters, Vienna, Austria..

[2] Fault Tree Handbook. U.S. Nuclear Regulatory Commission, Nureg-0492. (Co-author David Haasl) ISBN/ISSN 1051-H-02. 1981, p 209

[3] J. Norman, McCormick, Reliability and Risk Analysis, Methods and Nuclear Power Applications. Academic Press. Inc. 1981, p 446.

[4] Hagmark, P-E. and Virtanen, S. Simulation of Reliability, Availability and Maintenance Costs. Recent Advances in Stochastic Operation Research II, edited by Tadashi Dohi, Shunji Osaki & Katsushige Sawaki, Japan, 2009. ISBN 978-981-279-166-5K.

[5] Virtanen, S., Hagmark, P-E. and Penttinen, J-P. Modelling and Analysis of Causes and Consequences of Failures. IEEE, Proceeding: Annual Reliability and Maintainability Symposium (RAMS). January 23 – 26, 2006. Newport Beach, CA, USA. pp. 506 – 511.

[6] M.Cheok, G. Parry, R. Serry, "Use of Importance Measures in Risk-Informed Regulatory Applications". Reliability Engineering and System Safety, 1998.

[7] Virtanen, S. and Hagmark, P-E. Determining Reliability Performance and Maintenance Costs of Selected Design Solution and Maintenance Strategy. Springer-Verlag London Ltd: Proceedings of the 3rd WCEAM-IMS 2009. ISBN 978-1-84882-216-0. pp. 1568 – 1579.

[8] IAEA-TECDOC-478

[9] T-book, Reliability Data for Components in Nordic Nuclear Power Plants)

[10] SINTEF PSA handbook, Probabilistic Safety Assessment in the Chemical and Nuclear Industries

[11] Jhon B. Bowels, An assessment of RPN prioritization in a Failure Mode Effects and Criticality Analysis, IEEE Proceeding, Annual reliability and Maintainability Symposium 2003.

[12] Zigmund Bluvband, Pavel Grabov, Oren Nakar. Expanded FMEA (EFMEA). IEEE Proceeding, Annual Reliability and Maintainability Symposium 2004.