Journal of Energy

VOLUME 62 Number 1–4 | 2013 Special Issue

journal homepage: http://journalofenergy.com/

# Risk Impact of Maintenance and Other Activities with Regard to Plant Areas

**Ivan Vrbanić, Ivica Bašić**
APoSS d.o.o.
Repovec 23B, HR-49210 Zabok, Croatia
ivan.vrbanic@zg.t-com.hr, basic.ivica@kr.t-com.hr

## ABSTRACT

In all operating modes of a nuclear power plant a lot of activities take place, including maintenance, surveillance testing and plant modifications. Some of these activities can impose temporary increase in risk level, as they may change the status of equipment important to plant safety. Such risk increases are usually controlled by risk monitoring, which considers changes in risk due to changes in the status (e.g. availability) of plant systems and functions. Risk monitors are, in many cases, designed and operated to be system-oriented (or function-oriented), as they focus on "measuring" the risk associated with different system configurations (from where comes the often used term "configuration risk management").

On the other hand, components of plant systems are placed in various locations and at various floors (elevations) of plant buildings. Piping, as well as cabling, is routed through one or more buildings. Equipment performing different functions is, sometimes, located near each other due to architectural limitations. Where required, barriers are applied in order to ensure physical separation and independency. Due to these reasons, a particular plant area (compartment, room, part of a large room,…) can contain a variety of mechanical, electrical and / or other equipment with different safety implications. As well as system components, plant areas are also related to each other, with different degrees of relative importance. Since activities performed in different plant areas can imply changes, actual or potential, in the status of associated equipment, structures and / or barriers, there is also a need that risk monitoring considers the area-oriented aspects, beside considering those which are system-oriented or function-oriented.

Risk impact of an activity taking place in a particular plant area can be considered in terms of changes (potential or actual) to its three components: 1) likelihood of initiators which can be triggered by equipment in the area (but which are not mitigated by any of the equipment in the same area); 2) mitigating capability regarding the initiators which are not triggered in this area; 3) likelihood of initiators triggered in this area and mitigating capability regarding the same initiators. Activity in a particular plant area may be related to none or to any combination of the three risk impact components. Normally, risk impact under 3) is limited by the architectural engineering principles (because it may become very large risk contributor). However, it may be present in some residual form and it cannot be excluded (as demonstrated by area-related risk studies performed in the past, such as internal fire and internal flooding analyses).

With activity taking place in a particular area, the relevant importance of any other plant area (and, hence, potential risk impact of any activity that may be planned to go on at the same time) is then considered in terms of, respectively: 1) whether it contains the equipment relevant for mitigation of initiators that can be triggered in the considered area; 2) whether it includes the potential for triggering an initiator which is mitigated by the equipment located in the considered area; 3) whether it contains the relevant mitigation equipment or include the potential for relevant initiators.



I. Vrbanić, I. Bašić, Risk Impact of Maintenance and Other Activities with Regard to Plant Areas, Journal of Energy, vol. 62 Number 1–4 (2013) Special Issue,
p. 104–112
https://doi.org/10.37798/2013621-4222

The paper discusses these and other related issues and describes some basic concepts for the area-oriented risk management.

## 1 INTRODUCTION

In all operating modes of a nuclear power plant a lot of activities take place, including maintenance, surveillance testing, temporary and permanent design plant modifications performed when plant is in operation. Some of these activities can impose temporary increase in risk level even if they are not directly performed on the important to safety (ITS) systems, structures and / or components (SSCs), as they may change their status. Such risk increases are usually controlled by risk monitoring, which considers changes in risk due to changes in the status (e.g. availability) of plant systems and functions. Risk monitors (e.g. [1]) are, in many cases, designed and operated to be system-oriented (or function-oriented), as they focus on "measuring" the risk associated with different system configurations (from where comes the often used term "configuration risk management"). Many times, risk monitors do not recognize the non safety equipment or monitor activities related to them.

In this article we discuss a simplified approach which can be used for the initial stages of scheduling of the activities, which considers also plant areas where they would take place. It can be based on the principles such as those established in the US NRC's Significance Determination Process (SDP), [2] and [3] which is used to obtain a risk characterization in terms of an order of magnitude (OOM).

Generally, risk impact associated with implementation of activities relates to two major aspects: Increase in the likelihood of relevant initiators ($I$) and reduction in the plant mitigation capability in the case that an initiator occurs ($M$).

## 2 RISK MODEL

Risk model consists of five elements. The first three of them are, basically, the three elements of the SDP model ([2] and [3]) for functionally oriented risk significance, in terms of an OOM. The elements 4 and 5 represent a characterization of plant areas and activities, respectively.

Element 1: Initiators and their frequencies. The element represents a list of all relevant initiator categories (internal and external) with corresponding frequencies characterized in terms of an OOM.

Element 2: Systems and initiators dependency matrix. The matrix relates supporting systems to supported systems. Furthermore, it relates all relevant systems to initiators (i.e. for a particular system, the initiator categories are identified which require the considered system for mitigation).

Element 3: Event sequences logic. For each initiator category, a list of accident sequences is provided in the form $I_x M_{xi} = I_x M_{xi1} M_{xi2} \cdots$, where "$i$" denotes $i^{th}$ core damage sequence for initiator category "$x$". Terms $M_{xi1}$, $M_{xi2}$,… represent the nominal mitigation capabilities of functions which need to fail in order that considered sequence ends with core damage (or radioactivity release). In the simplified approach, these nominal mitigation capabilities are characterized in terms of an OOM (i.e. corresponding failure probabilities are expressed as, e.g. 0.1, 0.01, 0.001,…). Term $I_x$ is initiator category from Element 1. The event sequences can be derived on the basis of simplified event trees from the plant specific PRA.

Element 4: Characterization of plant areas. Plant areas can be defined on the basis of (or, at least, an initial point can be) the PRA for the area events such as internal fires or internal floods. For each area, an inventory of equipment is established which is then related to the initiator categories $I_x$ and mitigation functions $M_{xi}$ . It is pointed that considerations shall also include forced shutdown and categories which may have been screened out during the fire PRA, flood PRA, etc., if presence of the activities changes the underlying screening reasoning. Characterization shall also include connections to the adjacent areas (e.g. fire doors).


I. Vrbanić, I. Bašić, Risk Impact of Maintenance and Other Activities with Regard to Plant Areas, Journal of Energy, vol. 62 Number 1–4 (2013) Special Issue,
p. 104–112

Element 5: Definition and characterization of categories / types of activities. In this element, for the classes of activities such as maintenance, surveillance test, etc., generic activity categories are defined such as "visual inspection", "pump lubricant sampling / exchange", "complete overhaul",… Each generic activity is characterized regarding its potential impact on initiator categories $I_x$ and mitigation function capabilities $M_{xi}$ . The impact is considered in terms of "by a factor" and "by an OOM". Here, both these terms should be interpreted in the sense of the mentioned SDP principles, e.g.:

- Impact "by a factor" would mean that change is of the same order as nominal value. The absolute conditional value remains within the same OOM.
- Impact "by an OOM" would mean that absolute conditional value is changed by an OOM.

Several (e.g. two or three) successive impacts "by a factor" in the same sequence would imply an impact "by an OOM". (For example, if considered set of activities has "by a factor" impact on the initiator likelihood and, also, "by a factor" impact on one of the required mitigation functions in the sequence, the overall impact may be considered to be "by an OOM". Similarly, if considered activities have "by a factor" impact on two or three required mitigation functions in the particular sequence, the overall impact may be considered to be "by an OOM". More specific rules can be defined for particular application.) Examples of activity impact characterization may include:

- Activity such as "welding" can increase a nominal likelihood of fire in the area by a factor or OOM.
- Manipulations with heavy pieces in the vicinity of an electric cabinet can cause damage or a loss of power to/from the cabinet. If the cabinet is related to certain initiator category (e.g. loss of support system or reactor trip), the activity can imply an increase in the initiator frequency by a factor or by an order of magnitude. (Example: temporary use of small cranes and associated chains or / and testing trolley.)
- Activity using a temporary sealing material on a valve which can impact the movement of a valve or even obstruct flow through a valve body.
- Activity at the "high energy" lines and valves which can impact environment conditions in certain areas and ITS equipment located there (harsh environment with pressure, temperature and humidity above design values.)
- Activity using the nitrogen to temporary freeze the water in the pipe due to the necessary corrective measures. The pipe can remain plugged if the time window for deicing has not passed or ice move downstream and potentially jeopardize active components in the line (e.g. pumps, valves,..)
- Activity requires that system train is isolated and put out of service. Therefore, the train is unavailable. (For a system with multiple redundant trains this would imply a decrease in mitigation capability by an OOM.)
- Activity requires temporary bypassing of the control and instrumentation signal. Effect is the same as above.
- Activity requires temporary opening of the fire doors or temporary removal of fire barrier. In such a case, for certain initiator categories (e.g. fire, an impact may need to be extended to other areas.

The activities also need to be characterized in terms of their duration which can, again, be done in terms of OOM (e.g. 1 hr, 10 hrs, 100 hrs… or similar scheme).

## 3 RISK ASSESSMENT

The risk assessment process is depicted in Figure 1. It would consist of the following general steps:

- Based on the macro-plan, select a desired set of activities and put them into desired time frames. Characterize time frames in terms of OOM (1 hr, 10 hr, 100 hr,…). Each time frame would correspond to a specific area / system configuration (parallel activities).
- Estimate risk impact of initial activities plan. For each time frame:
  - Relate the activities to equipment / systems and areas: use Element 2 to propagate supporting systems to all others; use Element 4 to to map the equipment to areas.
  - Identify implicated initiator categories: use Element 2 to identify the initiators with reduced mitigation capability; use Element 4 to identify initiators with increased frequency. (Note that both aspects may apply).
  - Identify affected event sequences from Element 3. For each, estimate the risk significance $\Delta R_x$ by applying generic characterization from Element 5 to the activities involved:

$$\Delta R_x = I_x M_x T \tag{1}$$

Term $T$ represents the time frame duration, while $I_x$ and $M_x$ are initiator frequency and mitigation capabilities involved in the sequence $x$:

$$I_x = I_{nx} F_{Ix} \tag{2}$$

$$M_{xi} = \prod_{xi} \left( \frac{M_{nxi}}{F_{xi}} \right) = \left( \frac{M_{nxi1}}{F_{xi1}} \right) \left( \frac{M_{nxi2}}{F_{xi2}} \right) \ldots \tag{3}$$

Here, index "$n$" refers to the nominal initiator frequency (Element 1) or the nominal mitigation function capability (Element 3). The terms (factors) $F_{Ix}$ and $F_{xi}$ generally represent an impact of undergoing activities on the initiator likelihood and mitigation capabilities, respectively. They are used to increase the initiator likelihood or to decrease the mitigation capability (or both). The above term $\Delta R_x$ is meant to represent an increase of the risk from the considered sequence, relatively to its nominal value. Therefore, the terms $F_{Ix}$ and $F_{xi}$ can, generally, be OOM(s) or 1.0 (if activity has no impact or an impact is only "by a factor"; in the latter case, the impact, by definition, remains within the same OOM), depending on the characterization of the set of activities.

  - Estimate total risk impact for the time frame as

$$\Delta R = \sum_x \Delta R_x \tag{4}$$

Here, the $\sum_x$ shall not be interpreted as an algebraic sum but, rather, as combining the contributions from sequences with differrent OOM risk significances (e.g. a "counting rule" in the mentioned US NRC's SDP process).

- The above process should be repeated for all defined time frames.


I. Vrbanić, I. Bašić, Risk Impact of Maintenance and Other Activities with Regard to Plant Areas, Journal of Energy, vol. 62 Number 1–4 (2013) Special Issue,
p. 104–112

- Estimate risk reduction potential (RRP)for the involved activities / areas: e.g. reset all initiator frequencies and mitigation capabilities implicated by particular activity / area to their nominal values and re-estimate risk impact.
- Estimate risk increase potential (RIP) for other areas: e.g. increase $I_x$ and/or decrease $M_x$ values associated with an area by an OOM and re-estimate risk impact.
- Depending on the initial risk impact, two different types of further actions may be taken:
    - Reduce the risk impact. This may be done by removing from the schedule the activities or areas with largest RRP.
    - Expand the scope of the activities. This may be done by introducing additional activities to the other areas with lowest RIP.

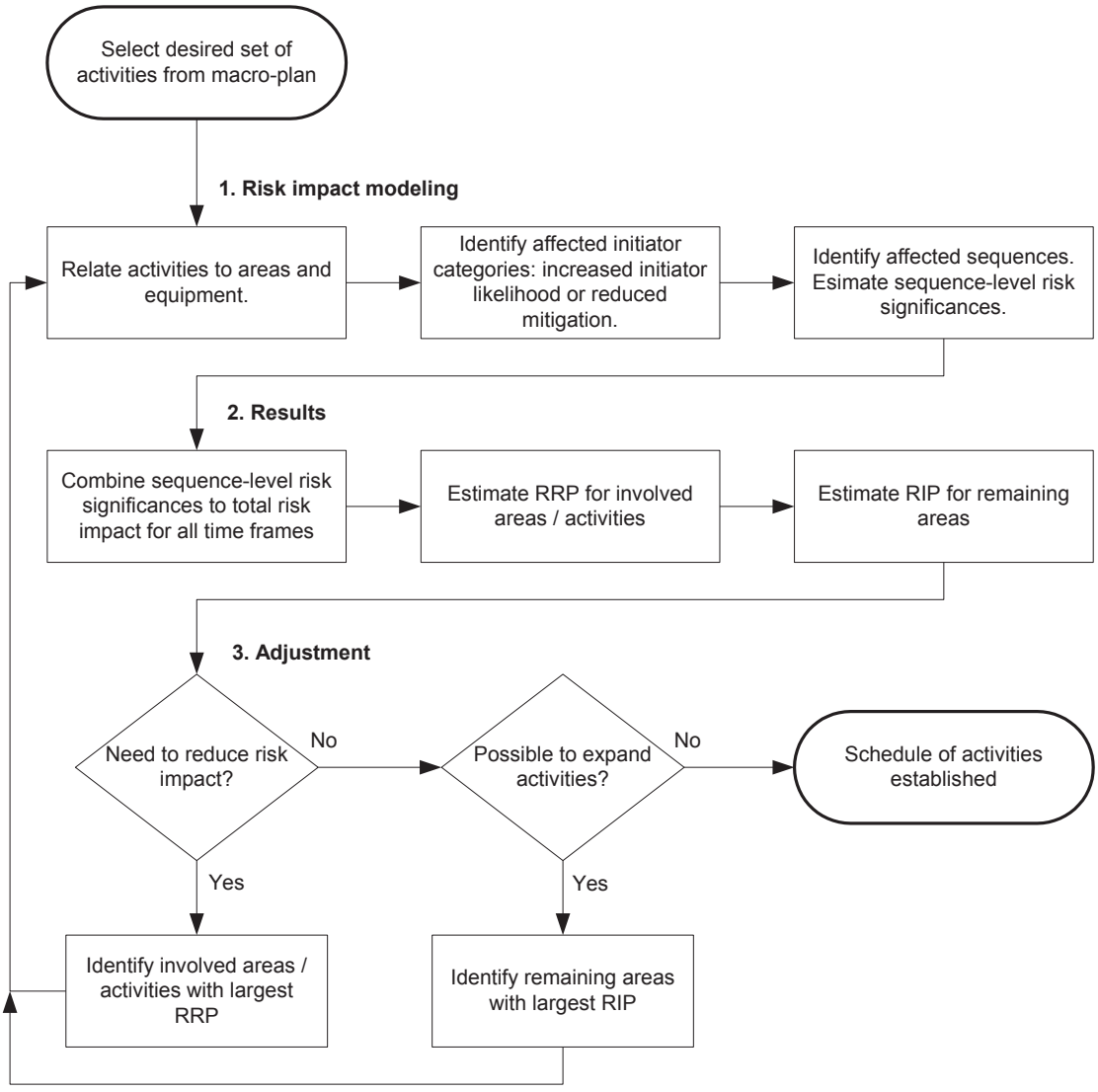


Figure 1: Simplified Risk Assessment Flow Chart


I. Vrbanić, I. Bašić, Risk Impact of Maintenance and Other Activities with Regard to Plant Areas, Journal of Energy, vol. 62 Number 1–4 (2013) Special Issue,
p. 104–112

## 4 SOME EXAMPLES

### 4.1 Risk from Transient Followed by a Loss of Secondary Heat Sink

In many cases, the risk from the ongoing online activities is related to the risk from induced reactor trip. The most important safety function following a reactor trip in a PWR plant is the secondary side heat sink.

Table 1 provides an OOM characterization of the baseline core damage risk from the accident sequence with reactor trip followed by a total loss of secondary heat sink, for a PWR plant with two loops (two steam generators (SG)). In such a sequence, assuming the total loss of Emergency Feedwater (EFW), the operators would be instructed by Emergency Operating Procedures to establish the secondary heat sink (keep the SG level) by means of Main Feedwater (MFW). If this function also fails, the operators are instructed by the procedures to initiate primary feed and bleed. Quantitative terms from Table 1 are based on the considerations from US NRC SDP documents [2] and [3]. They come from the considerations which include:

- Train-level credit for a motor operated system train, in OOM terms, is $10^{-02}$;
- Train-level credit for a turbine driven system train, in OOM terms, is $10^{-01}$;
- Multi train credit, in OOM terms, is $M_{TR}$ x $CCF$, where $M_{TR}$ is a single train-level level credit and $CCF$ a common cause failure probability. In terms of OOM, the $CCF$ is characterized as $0.1$ ("generic" beta factor). Therefore, in the case of multi train motor driven system, the mitigation credit is $10^{-03}$.

Table 1: Baseline OOM Risk Summary for the Sequence with Reactor Trip Followed by a Loss of Secondary Heat Sink

| Initiator | Baseline Mitigation Credit | | | |
|---|---|---|---|---|
| | Emergency Feedwater | Main Feedwater | Primary Feed and Bleed | Time Frame |
| Buildings / plant locations where related activities take place include (Note1): | | | | |
| TB, IB, CB … | IB,… | TB, IB,… | CB, AB, IB… | |
| In terms of OOM, reactor trip frequency can be characterized as:<br><br>$I = 1\ yr^{-1}$ | Assuming the configuration of two motor driven pumps, each per one SG, and one turbine driven pump for both SGs, the mitigation capability can be summarized as:<br><br>$M_{MDP} = 10^{-03}$<br>$M_{TDP} = 10^{-01}$<br><br>$M_{EFW} =$<br>$= M_{MDP}$ x $M_{TDP} =$<br>$= 10^{-04}$ | MFW is a multi train system. $M_{MFW}$ is considered to be at $10^{-03}$. The mitigation capability is driven by human action (to establish the heat sink from MFW), which is considered to be in the range of $10^{-02}$ to $10^{-01}$. Assume, for this example:<br><br>$M_{MFW} = M_{HA} = 10^{-01}$ | Both, feed and bleed functions are considered to have multi train mitigation credit and the credit for the overall function is driven by operator action, which is considered to be at OOM of $10^{-01}$:<br><br>$M_{FB} = M_{HA} = 10^{-01}$ | Baseline risk can be considered in the long time frame, such as time between two outages, i.e. of the order of $1$ year:<br><br>$T = 1\ yr$ |
| Baseline risk from the considered accident sequence is then characterized as: | | | | |


I. Vrbanić, I. Bašić, Risk Impact of Maintenance and Other Activities with Regard to Plant Areas, Journal of Energy, vol. 62 Number 1–4 (2013) Special Issue,
p. 104–112

$$R = I \times \left(M_{EFW} \times M_{MFW} \times M_{FB}\right) \times T = 1(yr^{-1}) \times 10^{-04} \times 10^{-01} \times 10^{-01} \times 1(yr) = 10^{-06}$$

Notes:

1. Note that related activities could take place in other buildings and locations, when considering associated supporting systems and, for example, cable routing. (The acronyms used in the above example stand for: TB = Turbine Building; IB = Intermediate Building; AB = Auxiliary Building, CB = Control Building.)

The characterization given in Table 1 results with OOM estimate of baseline risk from the considered accident sequence of $10^{-06}$. This is, indeed, the range of expected CDF contribution from this type of sequence, as can be confirmed by the plant-specific PRA models for the nuclear power plants of this type. For the purpose of plant area-oriented risk impact considerations, this very simple example already provides certain insights.

The activities which require formal declaration of safety system train being out-of-service (OOS) are not so much of interest here since they normally raise awareness of both plant maintenance crew and operators due to entering the Limiting Conditions for Operation (LCO). Those activities can also, very effectively, be addressed by the "conventional" system-oriented risk monitors. Of more interest are the activities which, although not requiring the declaration of formal OOS condition, can still imply the reduced availability or reliability of considered systems. From the above simple risk model for the considered accident sequences the following can be readily seen:

- Presence of "non-OOS activity" which implies an impact "by a factor" (as discussed earlier) on the initiator likelihood (i.e. an activity with some residual potential to induce a reactor trip) during a time frame of several days (i.e. 0.01 yr in the OOM scheme) does not imply relevant risk impact: $\Delta R = 0.01 \times R = 10^{-08}$.
- Even a presence of such activity during several weeks or a month, cumulatively, over a year (i.e. duration of 0.1 yr in the OOM scheme) would not imply significant risk impact: $\Delta R = 0.1 \times R = 10^{-07}$.
- However, presence of "non-OOS activity" with stronger potential to induce an initiator, considered to have an impact "by an OOM" (as discussed above) rather then "by a factor", through several weeks or a month (0.1 yr) over a year could have a moderate risk significance: $\Delta R = 0.1 \times 10 \times R = 10^{-06}$
- Single AOT event for EFW pump, being of duration up to 0.01 yr (e.g. three days) is not an event with relevant risk impact ($\Delta R = 10^{-08}$ as shown above), as long as operability of remaining pumps is out of question. However, combined with multiple activities with potential for inducing a reactor trip it can become risk significant (depending, also, on the confirmed status of remaining pumps.)
- Special category represents the activities with potential for inducing a trip of MFW or Condensate System and, consequentially a Turbine and Reactor trip. The nominal OOM initiator likelihood, from PRAs and SDP ([2], [3]), for the initiator category "reactor trip with MFW unavailable" is 0.1 /yr. From Table 1, the remaining nominal mitigation credit is $M_{EFW} \times M_{FB} = 10^{-05}$. Therefore, if there is an activity with an "impact by an OOM" (i.e. $\times 10$) on this initiator, concurrent with AOT of single EFW pump, then the combined risk impact is: $\left(10 \times 0.1/yr\right) \times \frac{10^{-5}}{10} \times 0.01yr = 10^{-06}$, which is considered to be in the range of a moderate risk significance.

(In the SDP scheme, [2], [3], the instances with impact between $10^{-06}$ and $10^{-05}$ are considered to have low to moderate risk significance; impact between $10^{-05}$ and $10^{-04}$ is considered to have

substantial risk significance; finally, impact larger than $10^{-04}$ is considered to have high risk significance.)

### 4.2 Risk from Station Blackout

Certain combinations of activities can have an impact on the risk from Station Blackout (SBO). Very simple risk model for SBO sequence can be established as follows (once again, the use is made of considerations from the SDP documents [2] and [3]):

- OOM initiator likelihood for Loss of Offsite Power: $I = 10^{-02}$ /yr
- Mitigation credit for Emergency Diesel Generators (multi train system): $M_{EDG} = 10^{-03}$
- Heat sink by EFW TDP and power recovery before depletion of batteries: $M_{REC} = 10^{-01}$
- From the above, the overall mitigation credit for SBO: $M_{SBO} = 10^{-04}$.

This simplistic SBO risk model yields the SBO contribution to CDF at the OOM of $10^{-06}$ per year, which can be confirmed by plant specific PRAs for this type of the plant.

As an example: any activity with "impact by an OOM" on the LOOP likelihood (e.g. switchyard related activities) concurrent with an AOT (the OOM of 0.01 yr) associated with a single EDG would produce the risk significance of: $\Delta R = \left(10 \times 10^{-2} \text{ /yr}\right) \times \frac{10^{-04}}{10} \times 0.01 \text{ yr} = 10^{-06}$. This is considered to be in the range of moderate risk.

### 4.3 Risk from Induced LOCA

Many times the perception is that online plant activities are not relevant for the risk from LOCA (i.e. their risk relevance is related to the risk from transients). This is not completely true. When an activity has a potential to induce a reactor trip this also means that it has a potential for producing a pressure transient caused by a plant trip, which can challenge the pressurizer relief or even safety valves and eventually, if any of challenged valves sticks open, induce a LOCA event (which may or may not be isolable).

Therefore, certain activities in plant areas such as TB or IB when combined with AOTs or certain activities in the AB related to the reliability / availability of ECCS can prove to be risk significant.

## 5 CONCLUDING REMARKS

The above process can be made more sophisticated and automated by the use of PRA or a risk monitor. The PRA elements such as initiators and basic events would be related to plant areas and then, instead of simplified OOM estimate, the conditional risk related to plant areas would be re-quantified in detailed manner. However, special attention would still need to be paid to the screened out sequences and areas in the PRA, as well as to the equipment not represented in the model. Also, the impact of activities would still, probably, be characterized in terms of "by a factor" or "by an OOM". The simplified OOM approach discussed above can be taken as a first step in a detailed process based on the risk monitor or, for example, to address the residual risk from the screened out areas / sequences or equipment, i.e. those not shown in the PRA used as a basis for the risk monitor.

However, it is emphasized here that the point of this paper is not on a quantitative risk estimate for ongoing activities and plant areas, in a mathematical sense. Rather, the point is that the principles outlined above can be, in a relatively simple and straightforward manner, used to produce a risk map of plant areas. That is, a cross-referential map can be developed which would for each plant area and associated set of activities point to those other areas / activities which have

significant risk implications, when combined with the considered area / activities. Such a map can be used in macro and micro scheduling of the proposed activities.

In this way, a concept of a "protected train", which is used in many plants, can be enhanced by a concept of "protected areas".

## REFERENCES


[1] Risk Monitors, The State of the Art in Their Development and Use at Nuclear Power Plants, Produced on behalf of IAEA and OECD NEA WG Risk, NEA/CSNI/R(2004)20, OECD, 2004

[2] US NRC Inspection Manual, Chapter 0308, Attachment 3 "Technical Basis for Significance Determination Process 10/16/06" with Appendices

[3] US NRC Inspection Manual, Chapter 0609, "Significance Determination Process 06/02/11" with Appendices