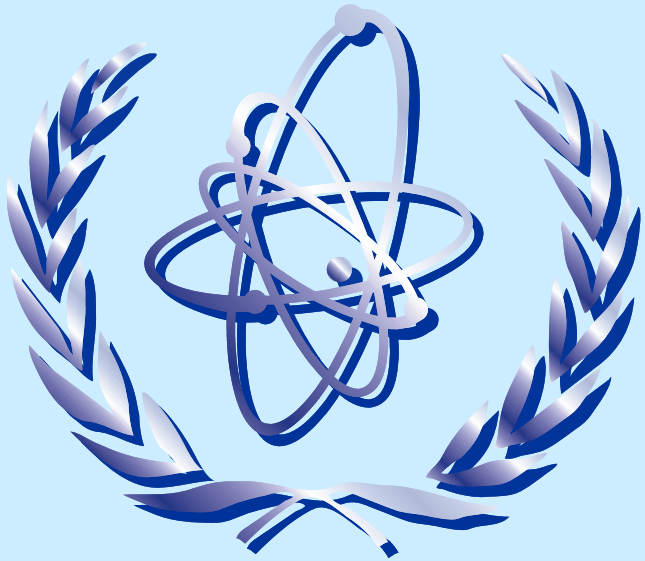
PSA applications



Risk/Safety monitors

Content

The aim of this presentation is to show the relationship between the PSA models and there use in the development of a model which is used on line in real time, usually known as a Safety/Risk Monitor.

Topics covered are:

- Definition
- Safety Monitor model development
- PSA - Safety Monitor differences
- Safety Monitor Usage
- Conclusions

DEFINITION

- A plant specific real-time probabilistic analysis tool which can be used by all plant personnel to determine the instantaneous risk based on the actual configuration of plant systems and components. The quantified core damage frequency is based on the configuration and the tests in progress. It is continually operating and, ideally covers all plant states. The generic terms “safety monitor” or “risk monitor” are used to describe such tools. Target solution times are 2-3 minutes

SOME MONITORS IN USE

• ESSM - Heysham 2	1990
• Safety Monitor - San Onofre	1993
• SAS - Dukovany	1995
• ORAM	1995
• SENTINEL	1995
• EOOS	1996
• LINKITT 2	1997

DIFFERENCES BETWEEN PSA AND SAFETY MONITORS

- The PSA is a comprehensive model which provides a considerable amount of information on the risk contribution from many aspects of the plant design and operation. In its complete form, and for its solution, assumptions are made about the expected annual frequency of the various initiating events and the occurrence of maintenance and test activities over the year. Its primary use is to predict the Core Damage Frequency (CDF/yr) or other risk measure over the life of the plant. It can then be used to assess the design strengths and weaknesses and if necessary any plant upgrades to reduce risk.

DIFFERENCES BETWEEN PSA AND SAFETY MONITORS (Cont.)

- The safety monitor is designed to indicate the current risk level for the plant configuration based on the actual configuration. Its primary use therefore is to enable maintenance and test activities to be planned and performed on a risk informed basis. As is shown later, this is done by continuously monitoring (and displaying) the current predicted core damage frequency (CDF), and having a target core damage probability (CDP) contribution for any configuration in which the predicted CDF is above a given threshold.

SAFETY MONITOR PSA MODEL

- There are a number of different ways of representing the plant risk model in the safety monitor in order to get the fast solution time:
  - Integrated core damage, core boiling, large early release fault tree model of the full PSA model for all plant operating modes (Fault tree linking or support state methodology from RISKMAN)
  - Integrated core damage fault tree model for power operation
  - Fault trees for specific initiators
  - Dependency matrices (system/train status)
  - Presolved cutset solutions for a range of configurations

RISK MODEL DEVELOPMENT

- Each of the approaches on the previous slide will give a different solution, and in many cases the difference will be small. The type of model used is determined by balancing four factors:
  - Size of PSA
  - Hardware on which model is to be installed
  - Speed of Fault tree algorithm
  - Required solution time
- The most accurate solution will be achieved from a fault tree model which is the Boolean minimisation of the PSA fault and event tree model. Such a model will contain all the information in the Living PSA

RISK MODEL DEVELOPMENT (Cont.)

- As the model is now to be used in real time additional in formation is required in order to accurately reflect the operation status of the plant rather than the average values used for various events in the Living PSA. These are:
  - Test/Environment modifying factors. Analysis of initiating events shows that the probability of an initiating event is higher when certain activities are taking place than at other times. This has to be reflected in the model
  - Plant component to basic event mapping. As the safety monitor is to be used by plant staff all interfaces must use normal plant terminology not he PSA shorthand for components

RISK MODEL DEVELOPMENT (Cont.)

- Large early release core damage cutset assignment when the monitor is to be used for looking at the impact of maintenance of containment systems on the frequency of large early release
- Decay heat algorithm for the various plant states during the shutdown process
- Plant specific data

TEST EFFECTS

- If a root cause analysis of initiating events is performed it is seen that some events are not random but are more likely to occur when testing is taking place. This is not of significance in the PSA when all events are viewed on an annual basis. In real time, this may be significant in terms of leading to an unacceptable risk spike because of other activities going on at the time the test is due. This is handled in the safety monitor by multiplying the initiating event frequency by a factor when the associated test is in progress. Similar effects may be seen due to external environmental conditions. This can be handled in the following way.

TEST EFFECTS (Cont.)

TEST	IE	FACTOR
MSIV Testing	Turbine trip	2
	Loss of MFW	1.5
Diesel Generator	Loss of 6kV bus	2
Turbine Stop Valve	Turbine trip	3
RPS	Reactor trip	2.5

The frequency of the basic event in the fault tree would be multiplied by this factor whenever the test is in progress

TYPICAL OPERATIONAL SPECIFICATIONS

- All modes of operation (modes 1 - 6)
- Batch mode solution for schedules (power and refuelling)
- Dynamic human error probabilities for modes 5/6 depending on decay heat/vessel status
- Maintenance rule tracking
- Automated data interface with scheduling and plant process computers
- Extended to Level 2 for large early release frequency
- Fuel in RCS or spent fuel pool
- Track and store risk history
- Rule based recovery actions
- Component outage data

SAFETY MONITOR CRITERIA

- System status- qualitative, defined by user; three levels normal, degraded, unavailable.
- Core damage frequency- quantitative, settings defined by user; three levels, normal, warning, high.
- Core boiling, large early release frequency- quantitative, settings as for core damage
- Allowed time in configuration- quantitative, based on criteria such as:
  - fixed increment i.e. $1x10^{-6}$
  - fixed percentage of annual risk i.e. 1%

MONITOR USAGE (INPUTS)

- Inputs from plant operations and maintenance personnel are:
  - Changes in system configuration (alternating systems such as service water or charging)
  - Changes in component status (maintenance)
  - Tests in progress
  - Changes in the environment external to the plant which may influence the expectation of an initiating event
  - Maintenance schedule for future quarter/month/ week or upcoming refuelling outage

MONITOR USAGE (OUTPUTS)

- Out put available to plant staff
  - Current core damage frequency and cumulative core damage probability for the year; system status
  - Past core damage core damage frequency history
  - Recommended time in a given configuration once a predefined core damage frequency is exceeded
  - Importance of currently available components
  - Restoration advice (components ranked by risk reduction potential)
  - Time to boiling (when shut down) and large early release frequency
  - Risk profile for outage schedule and integrated core damage probability for the whole schedule

CORE DAMAGE PROBABILITY ASSESSMENT

- The PSA is used to predict the core damage frequency (CDF) usually per year. If the frequency is multiplied by 1 yr the core damage probability for the year is defined.
- The safety monitor records the CDF and period of time for the given CDF for each configuration so can be used to determine the CDP for the year by summing over all plant states.

CORE DAMAGE PROBABILITY ASSESSMENT (Cont.)

- Care should be taken in comparing the two results as the basis under which they are calculated are not the same.
- The value of the information derived from the safety monitor is that it allows a year on year comparison to be made of the operating risk profile

FIGURES OF MERIT

- A safety monitor can be used to derive a range of figures of merit for use in risk informed regulation. Some examples are
  - Annual CDP
  - Peak CDF during the year
  - Length of time in defined CDF bands
  - Length of time above PSA CDF
  - Safety system (component) unavailability and associated CDF
  - Total maintenance time for safety related components
  - Activities which lead to peak CDF
  - Activities contributing to time above PSA CDF

CONCLUSIONS

- It can be seen from the foregoing that the requirements for the safety monitor are different from those in the PSA model. Because it is required to operate in real time, follow the plant operating profile, take into account testing and maintenance activities which are taking place, and, most importantly be used by plant staff with no knowledge of PSA techniques, it is not possible to use the existing PSA software.
- The safety monitor plays an important part in developing a wide understanding of the role that PSA can play in the safety culture of plant operations without having to understand the techniques required to perform a PSA. It is now widely used with more than 30 units having some form of safety monitor in 5 countries