Living PSA

M.G. K. Evans

Workshop on "PSA Applications"
Sofia, Bulgaria
7-11October 1996

PRESENTATION OVERVIEW

The aim of this presentation is to gain an understanding of the requirements for a PSA to be considered a Living PSA. The presentation is divided into the following topics

- Definition
- Planning/Documentation
- Task Performance
- Maintenance
- Management

DEFINITION

- A Living PSA is a risk model of the plant which reflects the known design and operational parameters, and is documented in such a way that each aspect of the model can be directly related to existing plant documentation or the analysts assumptions, in the absence of such information. Inherent in this definition is that the psa will have the full acceptance of plant personnel.
- Desirable attributes are
  - → realistic success criteria
  - → plant specific data, when available
  - → reasonable solution time

PSA PLANNING AND INITIATION

- **Definition of the scope of the PSA**
  - → Based on the intended applications
  - → Information and experience of the PSA team
- **Minimal set of documentation**
  - → Project Plan
  - → QA Plan
  - → Task Procedures
  - → Analysis Files/Calculation Noted
  - → Document data Base
  - → Maintenance and Applications Manual

PROJECT AND QA PLANS

- **The Project Plan provides the guidance for the initial performance of the PSA and ensures that resources are used effictively**
- **The QA Plan provides the necessary quality controls for the performance of the initial analysis and the ongoing maintenance of the PSA**
  - → QA documentation
  - → List of documents subject to quality control
    - Analysis files
    - Procedures
    - Review documents
  - → Review
    - Internal
    - Plant
    - External

TASK PROCEDURES

- Methodology/Techniques to be used in the performance of each task
- Reference documents
- Modelling assumptions
- Interface with other tasks

ANALYSIS FILES

- Reference to all documents used in the development of the model
- Description of the system, events, etc
- Details of the development of each section of the model, including assumptions where there is insufficient information in the reference documents
- Hard copy of the model elements
  - → Event Sequence Diagram (ESD)
  - → Event Tree (ET)
  - → Fault Tree (FT)
  - → Data
  - → Etc

DOCUMENT DATA BASE

- List of all projects with cross reference to the sections of the analysis in which they are used. This includes the analysis files themselves, as there are many interactions between tasks. The minimum information in the data base is
  - → Document number/revision number
  - → Date of issue
  - → Analysis file section
  - → Source of document
  - → Section of document used

TASK PERFORMANCE

- There are a number of giudes for the performance of a PSA issued by the IAEA, so the aim in the following slides is to identify specific modelling issues which are directly related to the completion, and maintenance of a living PSA. The majority of these issues are associated with the intended applications of the model and ensure that the completed study can meet these applications

INITIATING EVENTS

- **Generic Events for rare events such as Loss of Coolant Accidents and steam/feedwater line break**
- **Plant specific events which have occured**
  - → Root cause of events. this is needed for applications relating to precursor analysis and use of the PSA in the safety monitor. The three categories are
    - Tests
    - Random
    - Maintenance activities
- **Combination of generic data and plant data**

ACCIDENT SEQUENCES

- **The development of Event Sequence Daigrams (ESD) is of great benefit in communicating the process of event tree construction to the plant staff not familiar with PSA. The essential elements are**
  - → Flow diagram of the performance of each of the systems required to maintain decay heat removal, following the initiating event
  - → Signal/ control actuations
  - → Operator interactions
  - → Beyond design basis events leading to core damage
  - → Low frequency events treated not developed further, so treated as leading to core damage

EVENT SEQUENCES DIAGRAM

- see fig.3

ACCIDENT SEQUENCES (contd)

- Event Trees
  - → Based on information in the ESD
  - → All safety function success criteria are clearly documented with reference to the source documents or T/H analysis
  - → Realistic T/H analysis performed where possible in order to establish the minimum system requirements and timing of required operator actions forthe human reliability task
  - → Inclusion of the containment systems, when a level 2 analysis is within the scope of the study. Even if a level 2 analysis is not part of the immediate project some thought should be given to the the relvence of the event tree structure to offsite release

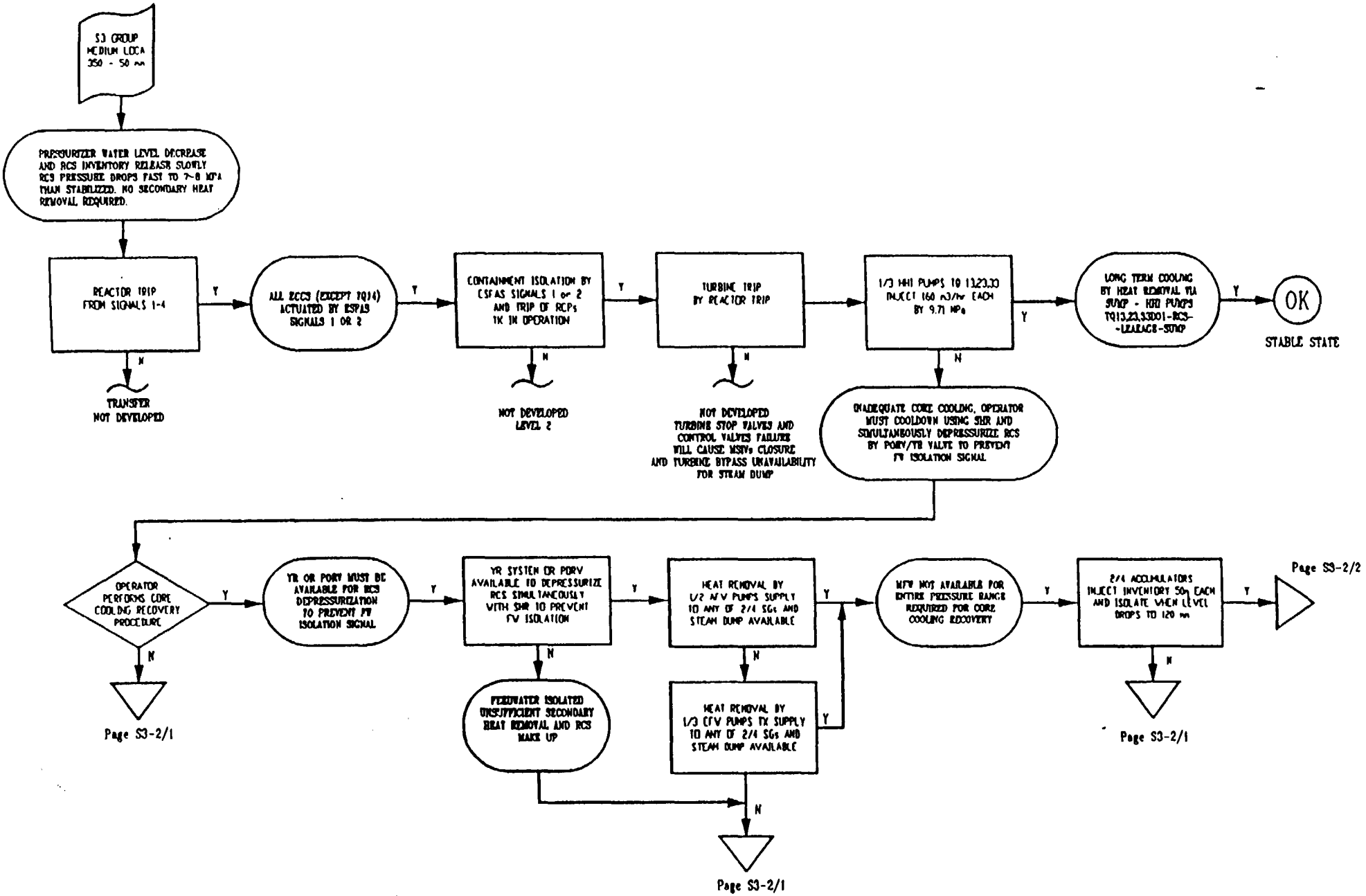

Fig.3 Event sequence diagram

ACCIDENT SEQUENCES (contd)

- **Safety Function development should be well documented and include the following information**
  - → All systems which can contribute to the function
  - → Dependence of the function on the success or failure of previous functions
  - → All relevent procedures and the resulting necessity to include operator actions, which are not in the fault trees, in the function, or as a unique function
  - → Boundary conditions which will uniquely identify the function and there dependency on the following
    - Initiating event
    - Success or failure of one or more early functions in the event tree
  - → Lists of house /switch events or "attributes" should be developed for each function

SYSTEM ANALYSIS

- **The following information relevent to each system should be clearly documented**
  - → The as installed design
  - → Operating experience
    - Failures of room cooling or cooling to the component
    - Instrumentation and control related events
    - Electric power dependency (cooling to room where breakers are located)
  - → System boundary and interface with other systems. This is important both to avoid gaps in the modelling of systems and overlap between models leading to double modelling of events
  - → Component boundaries
  - → Testing/maintenance/calibration matrix to assist in the identification of potential common cause operator actions or other contributors to common cause failures

DATA ANALYSIS

- **The following key areas need to be clearly documented**
  - → Component boundaries (exactly the same as in the systems analysis task)
  - → Iniating event groups (information supplied by the accident sequence subtask)
  - → Plant Specific data records
    - Initiating events
    - Component failures
    - Maintenance activities
    - Test activities (duration and impact on system availability)
    - Impact of test/maintenence activities on initiating event frequencies
    - Basic event naming scheme
      - Applications oriented
    - Common Cause failure analysis

DATA ANALYSIS (contd)

- **Example Basic Event Naming Scheme**

abbcdddxxxxeefff

a - unit number

b - system identifier

c - train identifier

d - component type

x - component number

e - failure mode

f - location

HUMAN RELIABILITY

- Use plant procedures to identify and characterise the events identified in the event and fault tree analysis
- Use any plant experience
- Event Naming scheme should be aimed at enabling the analysis to be updated when procedures are modified, as shown in the example below

HEP-abbbbccc

a - prior to trip 1
post trip 3
recovery r
b - procedure number
c - procedure step

QUANTIFICATION

- All boundary conditions and attributes should be documented for each of the functions with cross reference to the event tree and sequence in which they occur
- Extensive sensitivity analysis an all epistemic uncertainty issues should be performed
- Importance analysis should cover system, trains, and functions as well as basic events
- Uncertainty analysis should be performed

SHUTDOWN MODES

- **Plant specific information relating to the following should be collected and documented**
  - → Plant operating states (POS)
    - Time in each state
    - Inoitiating events which can occur in each state
    - Equipment availability in each state. The boundary conditions leading to the isolation or removal from service of systems (such as high pressure injection when RCS pressure drops to a certain value) should documented
    - Plant procedures used in each state. Some of these procedures may have the potential to lead to initiating events as well as mitigate the consequences. For example draining the vessel prioe to head removal

EXTERNAL EVENTS

- **The following external events would normally be included in a living PSA**
  - → Internal fires
  - → Internal and external flooding
  - → Strong winds
  - → Seismic events
  - → Aircraft Impact
  - → Industrial facility/transportation accidents
- **Many events, within the above analyses, are screened out on frequency or other grounds. The basis for this, and events screened out, should be documented so that they can be reviewed following a design change**

FIRE ANALYSIS

- In the living PSA the development of the fire initiating events and barrier analysis should be strongly influenced by the plant walkdown and historical data on the following
  - → Position of fire doors
  - → Inspection of fire barriers
  - → Transient combustibles
- It is important to develop fire impact vectors for each fire area not screened out, relating components and cabling in the area to basic events in the fault tree models. This will be used to modify the fault trees developed for the internal events, for use in the fire event trees for each location. This information is critical for updating the study following design changes

FLOODING ANALYSIS

- The same comments on the plant specific information and the development of the impact vectors for the fire analysis are applicable to the flooding analysis.
- Additional analysis relating to floods from lakes, rivers, dams or the sea (tsunami) should be included

SEISMIC ANALYSIS

- The plant walkdown is an important part of this analysis. It should be repeated after each refuellig outage, or design change to ensure that the installation of new equipment or mounting of existing equipment meets the assumptions of the equipment fragility analysis
- Seismic impact vectors should be developed as forthe other tasks
- The hazard analysis information should be available to the analysts and periodically reviewed

OTHER EXTERNAL EVENTS

- A record should be kept of all industrial processes involving hazardous materials so that changes in the vicinty of the plant can be tracked and compared with the original risk assessment of such facilities
- Construction of new roads, railways, or changes in flight paths should be treated in the same way

MAINTENANCE OF THE LIVING PSA

- Two issues which arise are the frequency of updating and the process to be adopted
- Frequency of updating
  - → Following each refuelling outage
  - → After a design change/major reconstruction has been implemented
  - → Following a change in the understanding of plant performance (success criteria)
- Updating Process
  - → Identification of the necessaruy changes
  - → Implementation of the changes
- A scheme for the updating is shown in the following diagram

UPDATING PROCESS

- see fig.4

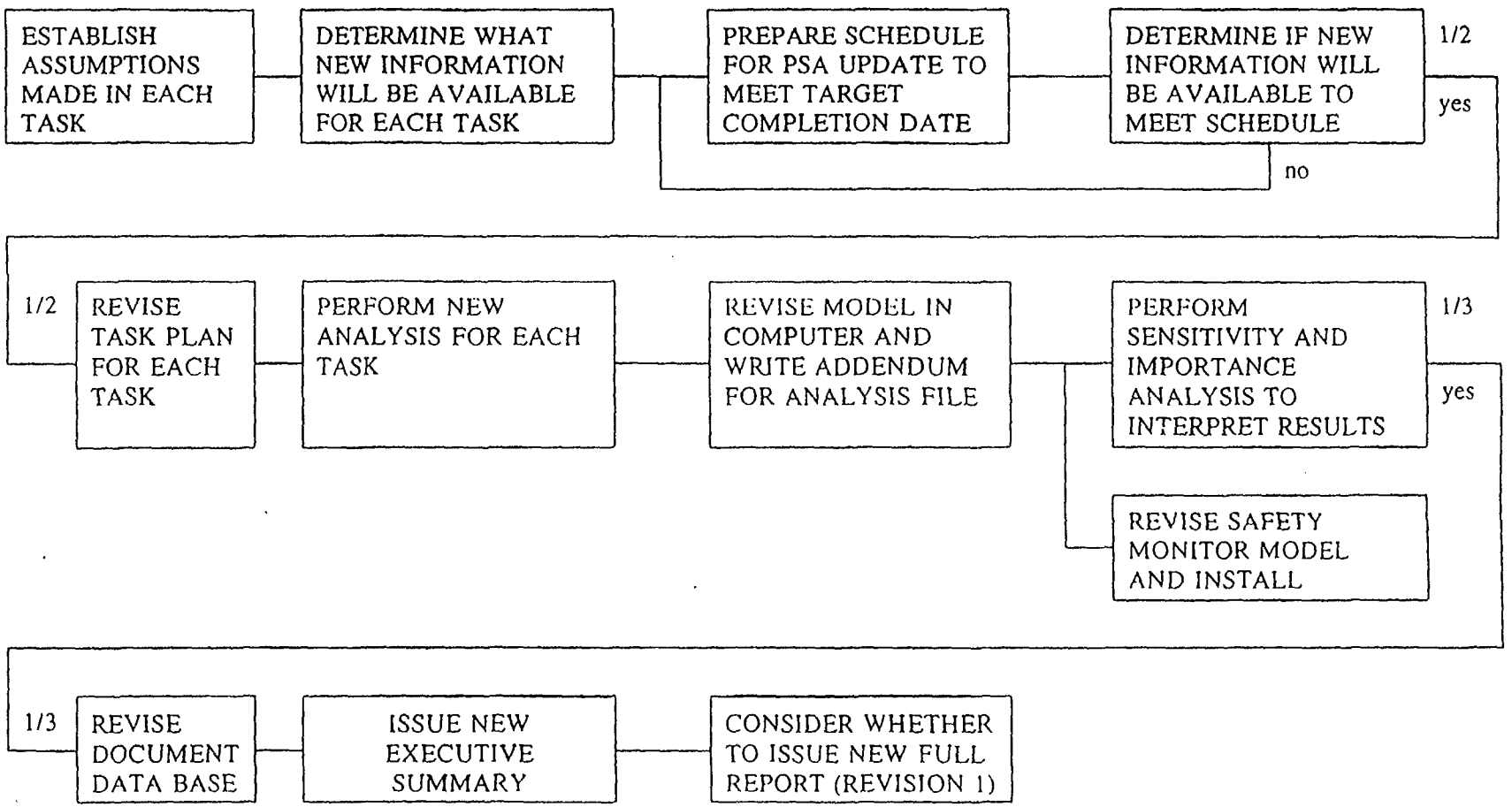

Fig. 4 Updating process

MANAGEMENT AND RESOURCES

- Approved by plant manager
- Budget item at the plant
- Specific department responsible for the maintenance and application of the PSA
  - → Independent Safety Group
  - → Nuclear analysis/fuel group
  - → Engineering (rarely)
- The resources depends on the number of units and the level and scope of the PSA. Examples of staff are
  - → Temelin (2 units) 4
  - → Virginia Power (4 units) 4
  - → Perry (1 unit) 1

MANAGEMENT AND RESOURCES

- The majority of plants with a living PSA use contractor staff for specialist areas of the analysis, or when there is a peak workload. Typical tasks supported in this way are
  - → Human reliability analysis
  - → Thermal hydraulic analysis
  - → Special aspects of data reduction and common cause failure analysis
  - → Level 2 and containment analysis
  - → Seismic hazard and fragility analysis

PROJECT STAFF QUALIFICATIONS

- The living PSA project team is usually made up from personnel from the various departments at the plant so that they have a good background in plant operations , maintenance, training, engineering and safety analysis
- They will all be capable of performing the basic fault and event tree analysis. If there are three or four members, then it is usually for each member to concentrate on specific areas. A typical split would be
  - → Team Leader - Accident sequence analysis, Interpretation of results
  - → Team member - Quantification, Data, Human Reliability
  - → Team member - Systems analysis

CONCLUSIONS

A number of plants have Living PSA. In all cases they were implemented as the result of a positive decision by the top management to establish a strong safety culture. The existence of such a culture results in all potential design and operational changes, and deviations from normal operation, being submitted to the PSA staff, for assessment of the risk implications of the change or event. Once such a PSA is developed, and the organisation for its use established, the team are contacted on a daily basis by any of the departments at the plant. It also forms an integral part of the routine inspection process performed by the regulator.