Computer Assisted Mechanics and Engineering Sciences, 9: 41–54, 2002.

Nuclear power plant safety assessment and accident management: Practice in Sweden and computerized decision support systems

Wiktor Frid

Department of Nuclear Reactor Engineering, Royal Institute of Technology
Brinellvägen 60, SE-100 44 Stockholm, Sweden

(Received August 6, 2001)

The methods of nuclear power plant safety assessment and accident management used in Sweden and selected computerized decision support systems are briefly described. The defense-in-depth strategy, which comprises three elements, namely prevention, protection and mitigation, is essential for keeping the fission product barriers intact. The safety assessment program, which focuses on prevention of incidents and accidents, has three main components: periodic safety reviews, probabilistic safety analysis and analysis of postulated disturbances and accident progression sequences. Even if prevention of accidents is the first priority, it is recognized that accidents involving severe core damage, including core melt, may nevertheless occur. Therefore, measures are required to achieve reasonable capability to manage such accidents. Emergency Operating Procedures and Severe Accident Management Guidelines are the vital components of the Accident Management System. Computerized decision support systems, to be used during normal, disturbed and accident states of a plant are expected to play increasingly important role in safety assessment and accident management, including support in rapid evaluation of possible radioactive releases in the event of a severe accident.

1. Introduction

The present Swedish nuclear power program includes 11 light water reactors, which were built during the period from 1972 to 1985. At the Forsmark and Oskarshamn sites there are three BWRs (Boiling Water Reactor), at the Barsebäck site one BWR and at the Ringhals site one BWR and three PWRs (Pressurized Water Reactor). One BWR unit at the Barsebäck site was shut down in 1999 as a result of political decision. The BWRs are of ASEA Atom (now Westinghouse Atom) design and the PWRs of Westinghouse design. The total electrical energy produced in Sweden is 150 TWh of which 47 % is produced in nuclear power plants, 47 % comes from hydropower and 6 % is produced in thermal plants, using various types of fuel, mostly in industrial or district heating co-generation facilities.

A license to build and operate a nuclear installation is based on a safety case, presented by the licensee in safety analysis reports and reviewed by the Swedish Nuclear Power Inspectorate (SKI). The safety case should demonstrate not only that a minimum acceptable safety level is achieved, but also that the safety is as high as reasonably achievable with respect to the fundamental safety objectives. When a license is granted, the safety case is regarded as the safety level the licensee has contracted to at least maintain as a condition for permission to operate the installation.

In Sweden, as in all countries with nuclear power programs, prevention of core damage has first priority as a safety objective. This objective is achieved through:

- a defense-in depth strategy which will prevent accidents with unacceptable releases of radioactive materials, protect the physical barriers that should contain possible radioactive releases, and mitigate as far as possible the consequences of any such accidents,

- a record showing absence of accidents as well as of incidents indicating serious deficiencies in the defense-in-depth system.

The defense-in-depth strategy, i.e. prevention, protection and mitigation, may include a large variety of measures including physical and functional system separation, redundancy and diversity of engineered systems and components as well as organizational and human factor measures to reach the desired degree of protection.

The physical barriers that prevent the radioactive substances from being released to the environment during normal operation and accidents include:

- the structure of the fuel material,
- the cladding of the fuel rod,
- the pressure boundary of the fuel system,
- the leak-tight shell of the reactor containment,
- the reactor building (of the boiling water reactor).

The integrity of these barriers must be continuously assessed and verified for normal and accident conditions. Operating experience, analysis of postulated disturbances and incidents as well as results of safety research play an important role in this assessment.

Core damage may occur if the core is insufficiently cooled, also after the fission reactions in the reactor core have been interrupted using control rods, due to energy released from the decay of the fission products. The core damage also can occur as a result of uncontrolled increase of nuclear power. The prolonged loss of core cooling, due to malfunctions of reactor safety systems or total loss of electrical power, would result in core overheating followed by partial or extensive melting of the core, which in turn would result in extensive release of radionuclides to the reactor containment and, at worst, to the environment. Accidents involving core degradation and core melt are called severe accidents and they are beyond postulated accidents for which the safety systems of existing reactors have been designed. The latter accidents are called Design Basis Accidents (DBA).

In the aftermath of the Three Mile Island core melt accident in 1979, the Swedish regulatory authorities required measures to achieve reasonable capability to manage severe accidents and to limit radioactive releases to the environment in such accidents, especially of nuclides causing long-term ground contamination. These requirements were based on governmental decisions. In the bill to the Swedish Parliament in 1980/81, the government proposed guidelines for the nuclear safety work within the frame of the Swedish nuclear power program. In 1986, the Swedish government required that the severe accident mitigation program be implemented at all nuclear power plants by the end of 1988 [7].

2. Safety assessment

The safety assessment work focuses on prevention of incidents and accidents. It has three main components: periodic safety reviews, probabilistic safety analysis, and analysis of postulated disturbances and accident sequences as well as disturbances and incidents that have occurred. Management and man-technology-organization issues, as well as inspections, play an important role in the safety assessment. In the next two sections we will very briefly describe the main features of periodic safety reviews and probabilistic safety analysis. In-depth analyses of postulated disturbances and accident sequences in all relevant areas, such as reactor physics, thermal-hydraulics, structural integrity, control systems and human factors, are performed in order to ensure that appropriate safety margins are met.

2.1. Periodic safety reviews

Recurrent safety reviews of each reactor form a special part of the program on prevention. According to a Swedish parliamentary decision in 1981, each reactor must undergo such recurrent safety review about every tenth year. Each of the recurrent safety reviews must be as extensive as the safety review conducted before the commissioning of the reactor. The report describing the recurrent safety review has been given the acronym ASAR (As-operated Safety Analysis Report). The utility ASAR is reviewed by SKI, which then reports the results of its review to the government. Major components of the recurrent safety reviews include:

- a comprehensive analysis of how safety work at the plant is organized and implemented, including management and quality issues, human factors issues and the training of personnel,
- a comprehensive report on operational experience, the more important technical improvements, and other measures taken to improve safety both in the plant and in the organization since commissioning,
- a detailed, plant-specific probabilistic safety analysis,
- a comprehensive report on current safety improvement programs, as well as a proposed future program based on the findings and conclusions from the recurrent safety review.

Considerable improvements and strengthening of efforts have taken place during the last decade in the treatment of human factors. SKI reviews of training and retraining programs have been extended from control room personnel to key maintenance and operation management personnel. Capacity for simulator training has been and is being expanded both at the nuclear power plants (compact simulators) and at the utility owned facility of full-scale simulators. SKI regulatory attention has expanded from traditional man-machine interface and training issues to the full interaction between man, technology and organization (MTO). The analysis of a number of safety significant events at Swedish plants clearly demonstrated the usefulness of a systematic MTO analysis in order to identify and correct significant weaknesses in safety awareness, training, work organization and management — all important components of a high-level safety culture.

2.2. Probabilistic safety analysis

The probabilistic safety analysis (PSA) is used extensively for systematic evaluation and verification of the safety and to ensure that the overall reliability of the safety functions is sufficiently high and well balanced. A complete PSA comprises three components, depending on the scope of analysis, namely PSA Level 1, PSA Level 2, and PSA Level 3 [12].

The objective of PSA Level 1 is to estimate the core damage frequency, i. e. the probability of core damage per year of reactor operation. This includes the following steps:

- identification of accident sequences leading to core damage,
- analysis of the performance and reliability of the safety systems,
- quantification of probabilities of accident sequences.

PSA Level 1 is based on the systematic reliability analysis of systems and components of importance to event sequences that can lead to core damage. The event tree — fault tree methodology is generally used.

The PSA Level 2 comprises the evaluation of core damage frequency, i.e. PSA Level 1, as well as the analysis of physical processes in the reactor plant (accident progression) in order to provide an estimate of the frequency of radioactive release to the environment and of the so called source term, i.e. information about the magnitude, timing and composition of radionuclides released.

If PSA is extended to also include the analysis of the dispersion of radioactive substances in the environment and resulting consequences then it is called PSA Level 3.

Within the program on recurrent safety reviews all Swedish reactors have now been subjected to a plant specific, in depth PSA Level 1 from internal events. The PSAs are to a large extent based on plant-specific component and system reliability data, collected since the beginning of the Swedish nuclear program in a special data base [18]. Experience so far has shown that during the process of carrying out the ASAR program the Swedish utilities will implement changes in plant hardware and procedures to ensure that the calculated core damage frequencies fall below 10^{-5} per reactor operating year, which is about a factor of ten better then the figures cited in the pioneer WASH-1400 reactor safety study from 1975 [13]. However, the predictive value of such estimated core damages frequencies should be treated with caution. For example, the analysis includes some but not all types of human errors. The estimated frequencies can however be used as a figure of merit for the reliability of the technical safety systems.

An industry standard has been established in Sweden in regard of procedures and modeling of probabilistic safety assessments. The present standard is based on a thorough review of all PSA studies performed for the Swedish reactors which aimed at establishing well considered and uniform treatment in regard of initiating events, modeling of systems and sequences, common cause failures (CCF), human dependencies, and the use of reliability data.

Recent progress in PSA includes enhanced analysis of common cause initiators (CCI), greater detail in the analysis of small and medium break LOCA (Loss of Coolant Accident) and electrical systems, as well as extensions of the analyses to cover operational states other than power operation, e.g. refueling and maintenance outages, and risks for radioactive releases, i.e. PSA Level 2. The PSA methodology is in addition actively promoted for extended practical use in the daily planning of operations, maintenance, plant modifications and operational risk follow-up, so called living PSA.

The Swedish utilities have adopted a probabilistic target of 10^{-7} or less per reactor year of exceeding the release limit of 0,1% of the total core inventory in a reactor of 1800 MW thermal power of radioactive materials of significance in regard of land contamination (see below).

3. Accident management

Even if prevention of accidents is the first priority, it is recognized that accidents involving severe core damage, including core melt, may nevertheless occur. Therefore, measures are required to achieve reasonable capability to manage such accidents and to limit releases to the environment in such accidents. In order to comply with the guidelines given by the Swedish government it was required that fatalities due to acute radiation diseases shall not occur and that any radioactive release must be limited to noble gases and at most 0.1% of the inventory of the cesium isotopes 134 and 137 contained in a reactor core of 1800 MW thermal power, assuming that other nuclides of significance in regard of land contamination are released to lesser or, at most, equal extent. Guidelines were also provided with respect to the means of achieving the prescribed safety. By the end of 1988 the severe accident mitigation systems and emergency operating procedures were implemented at all Swedish reactors.

The severe accident mitigation was not considered as a formal design basis for the plants in the same sense as the traditional design basis accidents, but it is considered as an important element that extends the defense-in-depth concept protecting the containment integrity [17].

After the severe accident mitigation measures have been implemented, the major focus from the authority side is on the inspection that the measures are maintained to work as intended, that the emergency organization is in place, and that the procedures are regularly reviewed and trained. An important aspect is that the installed measures and accident management procedures are reviewed for the specific reactors in light of the development in the severe accident research.

In this section the basic features and structure of Emergency Operating Procedures and Severe Accident Management Guidelines used at the Swedish nuclear power plants are presented.

3.1. Emergency Operating Procedures

Emergency Operating Procedures (EOPs) and/or Severe Accident Management Guidelines (SAMGs), are the vital components of the Accident Management (AM) system. The scope and structure of EOPs and SAMGs are plant-specific but the main features are similar for reactors of the same type. Quite often, generic EOPs and SAMGs are first developed for a particular reactor design and later adapted to the specific plant.

The scope of EOPs can vary. In some cases the EOPs cover operational transients, design basis accidents and situations with serious degradation of ordinary safety systems. In other cases, the EOPs may cover the whole spectrum of accidents, including core melt and associated response of the reactor containment. However, for severe accidents, where uncertainties with regard to accident scenarios, accident phenomena and accident progression are significant, the procedures are replaced by knowledge-based guidelines, SAMGs. EOPs can be event and/or symptom oriented in order to provide the optimal guidance during accident conditions, as schematically shown in Fig. 1.

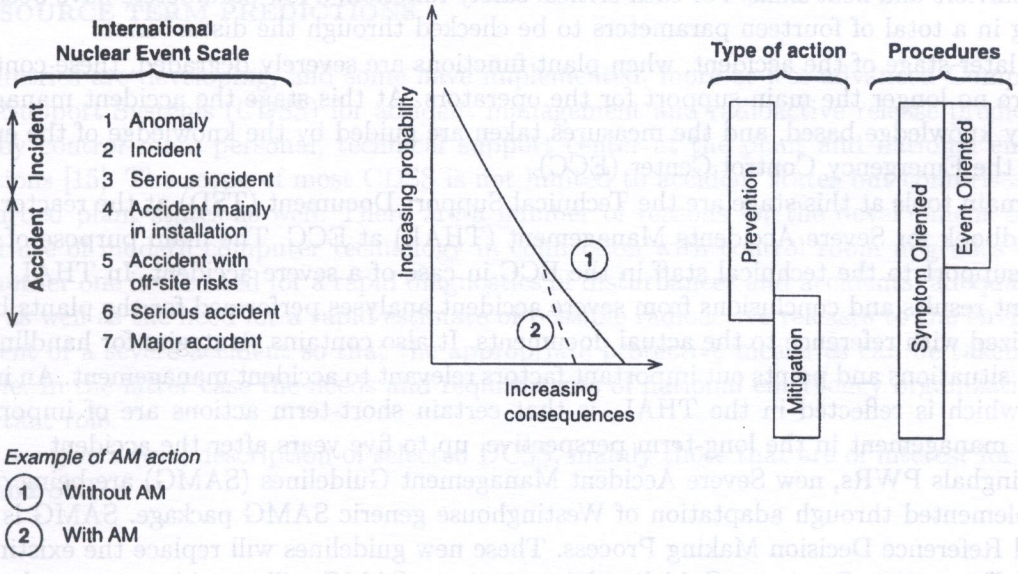

Fig. 1. Elements of accident management (Ref. [16])

The Swedish approach to EOPs and AM will be illustrated by the practice at Forsmark BWRs and Ringhals PWRs.

At the Forsmark power plant there are five levels of procedures to cover sequences from normal operation to severe accidents, as illustrated in Fig. 2 [2, 9, 10]. The normal operation conditions are covered by the System Operating Procedures, used to operate single systems, and Plant Operating Procedures, used to operate combination of systems.

There are two EOPs, one for the reactor operator and one for the shift supervisor. The EOP for the reactor operator is a symptom based step-by-step procedure following a checklist to verify that the automatic functions have worked as intended. In order to help the operator to overview the situation, the flowchart procedures are also included to be used before a more detailed check with the step-by-step procedure.

The EOP for the shift supervisor is a function based flow-chart procedure. This provides for a diversified way of working which reduces the probability for both the reactor operator and shift supervisor to make the same mistake.

Use of the EOPs is initiated by reactor scram (i.e. when the fission reactions in the reactor core have been interrupted using control rods) or an event that should have cased a scram. The shift supervisor will check the status of four critical safety functions: reactivity, core cooling, radioactivity

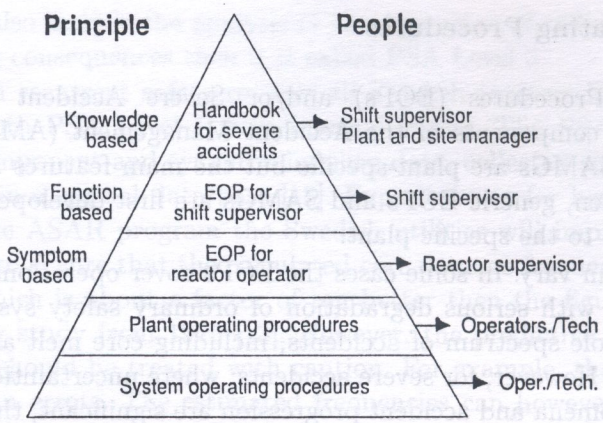

Fig. 2. Accident management documents at Forsmark BWR (Ref. [9])

release barriers and heat sinks. For each critical safety function, a few parameters have been defined, resulting in a total of fourteen parameters to be checked through the disturbance.

At a later stage of the accident, when plant functions are severely degraded, these control room EOPs are no longer the main support for the operators. At this stage the accident management is primarily knowledge based, and the measures taken are guided by the knowledge of the emergency team in the Emergency Control Center (ECC).

The main tools at this stage are the Technical Support Document (TSD) at the reactor unit and the Handbook for Severe Accidents Management (THAL) at ECC. The main purpose of THAL is to be a support to the technical staff in the ECC in case of a severe accident. In THAL, the most important results and conclusions from severe accident analyses performed for the plants have been summarized with reference to the actual documents. It also contains strategies for handling various accident situations and points out important factors relevant to accident management. An important aspect, which is reflected in the THAL, is that certain short-term actions are of importance for accident management in the long-term perspective, up to five years after the accident.

At Ringhals PWRs, new Severe Accident Management Guidelines (SAMG) are being developed and implemented through adaptation of Westinghouse generic SAMG package. SAMG is bases on so called Reference Decision Making Process. These new guidelines will replace the existing BERG (Beyond Emergency Response Guidelines) instructions. SAMG will provide structured guidelines for:

- diagnostic of plant status,
- prioritization of accident management measures,
- evaluation of alternative measures,
- verification of conducted measures.

There are many differences between SAMG and BERG. One is that SAMG is symptom based while BERG was mainly event based. BERG is used in parallel with Emergency Response Guidelines (ERG), which correspond to EOPs for BWRs, until melt-through of the reactor vessel has been diagnosed. In contrast, there is a clear transition from ERG to SAMG. The objective of ERG is to prevent core damage while the objective of SAMG is to mitigate releases and protect the barriers. The flexible structure of SAMG makes it possible to consider plant specific features and results of PSA Level 2. Another important features of SAMG are that the availability of instruments is considered, that there is no need for diagnoses of reactor vessel melt-through and that uncertainties in the physical processes are considered. The SAMG will also provide support to the control room during the time period before Technical Support Center is operative.

3.2. Validation of EOPs

Validation of EOPs comprises both technical verification and control of usability. Technical verification is carried out by detailed accident progression analyses, including PSA Level 2, where the impact of EOPs on accident progression and consequences is evaluated. Usability is validated in nuclear power plant simulators.

The Nuclear Training and Safety Center (KSU), jointly owned by the nuclear power utilities, is responsible for providing measures to create and maintain the competence of the power plant operators. Among others, KSU trains nuclear power plant operators using simulators, which are replicas of plant control rooms. The training includes both normal operation and all types of plant disturbance. A validation program using full-scale simulators was carried out, where the usability of the EOPs was checked by exercises with several operator crews and different scenarios. Evaluation was made both by human factor experts as observers and by questionnaires to the involved crews.

4. Computerized Decision Support Systems for Accident Management and Source Term Predictions

Many countries are developing, and some have implemented, more or less advanced Computerized Decision Support Systems (CDSS) for accident management and radioactive release predictions to be used by control room personal, technical support center at the plant and national emergency organizations [15]. The scope of most CDSS is not limited to accident states but comprises normal and disturbed plant states as well. There are a number of reasons for the development of CDSS. Increased use of modern computer technology in connection with control room upgrades is one of these. Another one is the need for a rapid diagnostics of disturbances and accidents, adequate alarm handling as well as the need for a rapid estimate of possible radioactive releases to the environment in the event of a severe accident so that the appropriate protective measures can be taken as soon as possible. In the latter case the needs and requirements of national emergency organizations play an important role.

Below we give a brief description of selected DCSS, mainly those that are of interest for Swedish utilities and SKI.

4.1. Disturbance Analysis Expert System SAS-II

The main objective of the SAS II project was to develop and install in the control room of the Forsmark 2 nuclear power plant a computer-based operator support system which supports the shift supervisor in monitoring the plant and its defined critical safety functions (CSF) during plant disturbances and accidents [11]. SAS II was developed by the OECD Halden Reactor Project in cooperation with Forsmark nuclear power plant, SKI, the Swedish utility Vattenfall and the Swedish vendor ABB Atom (now Westinghouse Atom).

The monitoring of the CSFs is performed according to two principles:

1. SAS II shall on a continuous basis monitor and present the plant status with respect to whether or not any CSF is threatened. This is called the symptom supervision. Symptoms are mainly one or more process values per CSF, which indicate the status of the related CSF. A typical example is the water level in the reactor tank.

2. After a scram, SAS II shall automatically evaluate and present whether or not the automatically initiated safety sequences have achieved the expected result. This is called system supervision.

Overview of the SAS II design is shown in Fig. 3. The SAS II logic is a description of the "dynamic behavior" in Boolean logic form of the process systems with respect to symptom and system supervision.

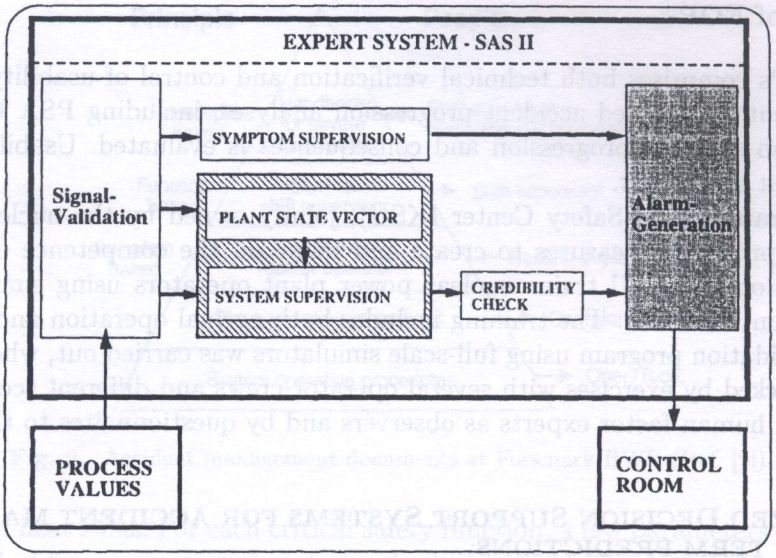

Fig. 3. Overview of the SAS II design (Ref. [11])

The process signals are validated before being used in the SAS II logic. Different methods are used, such as:

- Comparing signals from redundant instrumentation channels. Typical examples are all signals belonging to the Reactor Protection System, which is provided with four instrumentation channels.
- Crosschecking of signals based on different measuring methods. A typical example is the checking between the pressure of saturated steam and the temperature by means of steam table.
- Checking of the proper working environment for components in instrumentation channels. A typical example is checking of the temperature of the water inside instrumentation lines.

The result of this type of validation can be:

- Faults exist in the instrumentation but the process value can still be established by using the average value of redundant channels.
- Redundancy is lost and the information is unreliable.

The SAS II system was validated on the Forsmark compact simulator but the system has not yet been installed in the Forsmark 2 control room.

4.2. The Plant Safety Monitoring and Assessment System (PLASMA)

The PLASMA (Plant Safety Monitoring and Assessment) system can be seen as a further development of the SAS II system. PLASMA was developed by Institutt for energiteknikk (IFE) in Halden, Norway, and KFKI Atomic Energy Research Institute in Budapest in co-operation with Paks Nuclear Power Plant in Hungary [1]. The system is now installed at Paks on three plant computer configurations (full-scope simulator, Unit 1 and Unit 2).

The main task of PLASMA is to perform continuous plant safety status monitoring and to provide operator support in the control room during the execution of the symptom-based emergency operating procedures. This functionality is ensured by the following basic system services:

- on-line evaluation and presentation of critical safety function (CSF) status trees,
- continuous evaluation and presentation of the actual safety status of the plant,
- displaying and browsing the symptom-oriented EOPs,
- automatic displaying of those process signals which are quoted in the EOPs.

A block diagram of the main modules is presented in Fig. 4.

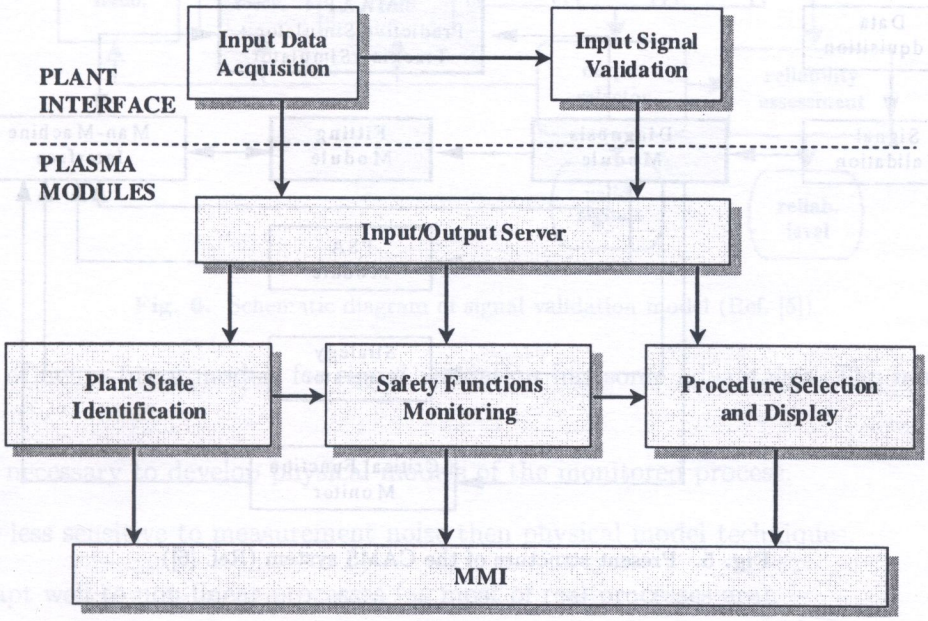

Fig. 4. Main modules of the PLASMA system (Ref. [1])

4.3. Computerized Accident Management Support (CAMS)

CAMS is a system developed to provide support in accident states and normal plant states [4]. This support is offered in identification of the plant state, in assessment of the future development of the accident, and in planning accident mitigation strategies. The CAMS system is being developed as a research activity at OECD Halden Reactor Project in Norway. The first CAMS prototype was completed in 1995.

Recently, the severe accident code MAAP4 has been integrated into the CAMS system [6]. As a result, two new modules have been developed, for both the BWR and PWR, for integration in the CAMS system. In addition, a parameter processing structure has been developed to implement the new theoretical models. The parameter processing structure makes use of fuzzy logic mechanisms.

The general structure of CAMS comprises three main modules: tracking simulator, predictive simulator, and state identification module. The tracking simulator module gives an estimation of the values that are not directly measured, calculates the initial values that are needed for the predictive simulator, and gives support in the validation of the signals by calculating values of certain parameters. The predictive simulator module predicts the evolution of the state of the plant, being faster than the real process. Finally, the plant state identification module gives information about the state of the plant, the state of the systems (their availability), and the state of the critical functions (heat sinks, core cooling, reactivity control, and containment integrity).

To be able to use the MAAP4 code in the CAMS system it has been necessary to modify the original structure of the system in order to include two new modules, the Diagnosis Module and the Fitting Module, instead of the original Tracking Simulator and State Identification modules of CAMS. The new structure is shown in Fig. 5.

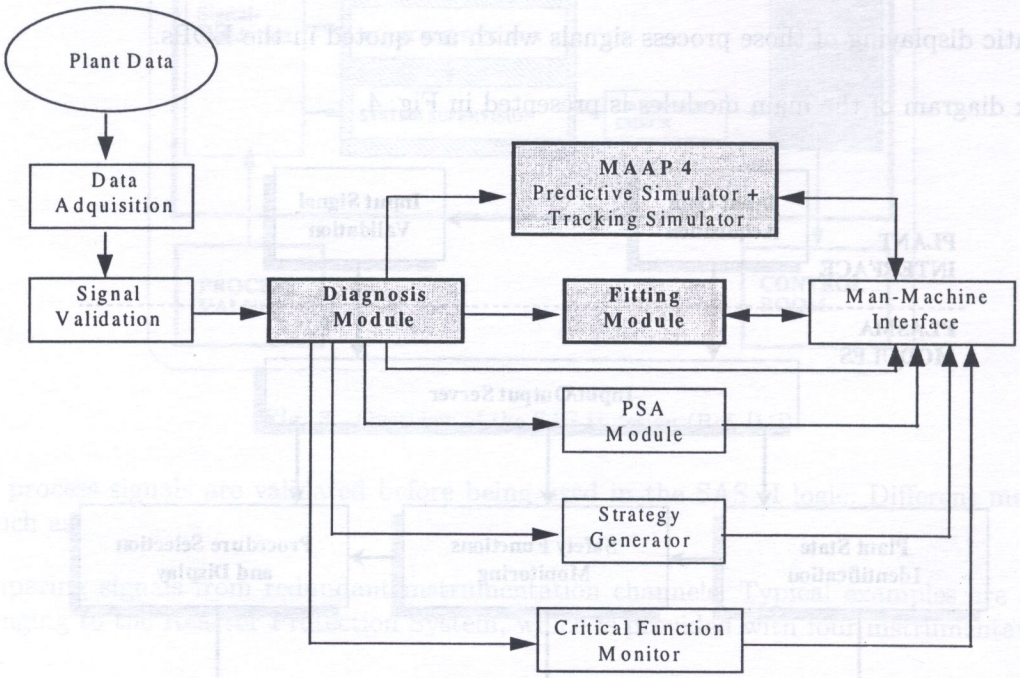

Fig. 5. Present structure of the CAMS system (Ref. [6])

The Fitting Module compares the plant state obtained from MAAP4 calculation to the new plant state processed through the Diagnosis Module and a set of additional rules, allowing the adjustment of the simulated scenario to the observed plant state from diagnosis module in a semiautomatic way.

In addition, there are the data acquisition module, the signal validation module, the probabilistic safety assessment module (PSA), the strategy generator, the critical function monitor and the man-machine interface module. The strategy generator and the critical function monitor have not been integrated into the present version of the CAMS prototype. The data acquisition module operates as an interface between CAMS and the monitored process. The purpose of the PSA module is to provide on-line accident prevention and mitigation strategies for a nuclear power plant. The module contains plant specific PSA data, comprising event trees, failure probabilities etc. The core damage frequency is re-calculated based on the current state of the plant and the pre-calculated PSA Level 1. The System Manager, not shown in Fig. 5, is the common functional interface to all the CAMS modules.

The signal validation is based on a fuzzy classifier and a set of Artificial Neural Networks (ANNs) [5]. Figure 6 shows a functional block diagram of the system. Basically, it is composed of a fuzzy classification stage that drives a bank of ANN modules, each trained in only a small region of the operation map. The classifier is based on fuzzy and possibilistic clustering techniques and it is trained to identify the incoming signal pattern (a snapshot of process signals) as a member of one of the possible categories (clusters) in which the operating space has been divided. Each cluster is associated with one ANN previously trained only with data belonging to this cluster. During the operation, the classifier provides an automatic switching mechanism to allow the best-tuned ANN to be used. The maximum membership grade of the sample in the particular cluster and the maximum signal mismatch in the neural network module are fed into a fuzzy model to estimate the reliability level of the validation.

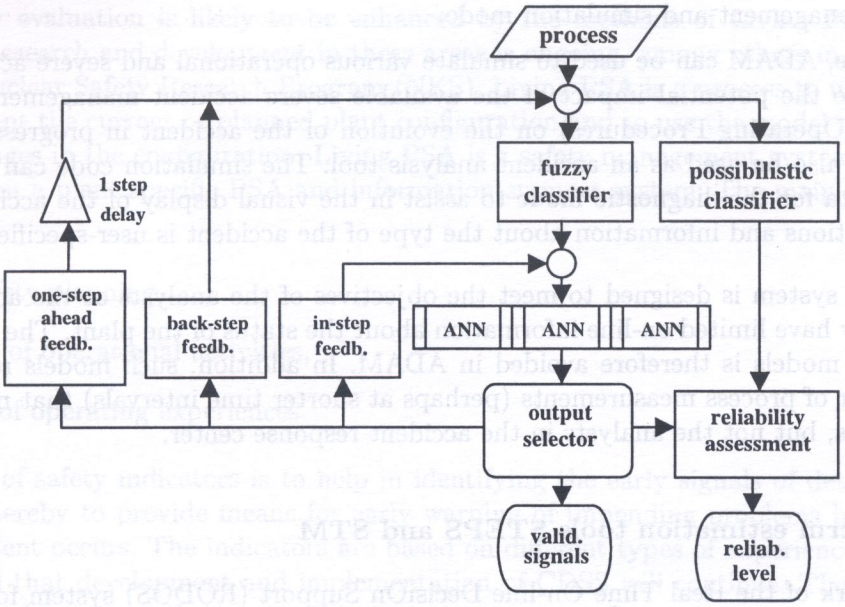

Fig. 6. Schematic diagram of signal validation model (Ref. [5])

The use of neuro-fuzzy models for signal validation has some advantages. The most important are:

- it is not necessary to develop physical models of the monitored process.
- they are less sensitive to measurement noise then physical model techniques.
- they adapt well to non-linear processes (as most of real processes are).
- they provide a confidence estimation of the validation process.
- they can be successfully used in multi-failure scenarios.

This signal validation model has been tested on a simulated data from the PWR type of a nuclear power plant, to monitor safety-related reactor variables over the operating region.

4.4. Accident Diagnostic and Management (ADAM)

The WINDOWS-based ADAM system has been developed at Energy Research, Inc. (ERI) in USA for analysis of selected plant data, following accidents, to arrive at symptom-based diagnostics of potential nuclear power plant accidents [3]. ADAM capabilities include evaluation of operator actions, emergency operating procedures, and severe accident mitigation strategies. ADAM is designed to execute several orders of magnitude faster than real time. It operates in two modes:

1. On-line accident diagnostics/monitoring mode.

   In this mode, selected plant parameters (as measured by plant sensors), arriving into ADAM at a pre-specified frequency, are used to assess the margins to core damage, containment failure, vent actuation, and hydrogen combustion (through appropriate alarms). In addition, the state of reactor, containment, and auxiliary building (if applicable), are assessed using a symptom-based diagnostics logic that is developed on a plant-specific basis, using results of extensive calculations, to arrive at the most likely scenario. There are provisions for a number of "alarms" within the ADAM logic to inform the analyst of certain conditions in the plant.

2. Accident management and simulation mode.

   In this mode, ADAM can be used to simulate various operational and severe accident scenarios to determine the potential impact of the available severe accident management strategies (or Emergency Operating Procedures) on the evolution of the accident in progress. Alternatively, ADAM can also be used as an accident analysis tool. The simulation code can also be used to generate data for the diagnostic mode to assist in the visual display of the accident. The plant initial conditions and information about the type of the accident is user-specified.

The ADAM system is designed to meet the objectives of the analysts at the accident response center who only have limited on-line information about the status of the plant. The implementation of complicated models is therefore avoided in ADAM. In addition, such models require access to a larger number of process measurements (perhaps at shorter time intervals) that may be available to the operators, but not the analysts in the accident response center.

4.5. Source term estimation tools STEPS and STM

In the framework of the Real Time On-line DecisiOn Support (RODOS) system for nuclear emergencies in Europe, two different and independent software modules have been developed for source term estimation; IPSN in France coordinated development of the deterministic STEPS system while NNC in the UK developed probabilistic STM module.

STEPS (Source Term Estimation Based on Plant Status) is a code suite, based on SESAME code system developed in France, (all plants in France are monitored and hard-wired into SESAME which is located at IPSN) designed to monitor the progression of an accident and to forecast the future behavior of the plant, including fission product behavior and the release to the environment. It is a modular system with models for the fuel, the primary circuit and the reactor building. Source terms are predicted based on the current plant status and are updated continuously. About 100 measurements are required from the plant. STEPS is lap-top based and requires running by an expert.

The STM (Source Term Module) software employs Bayesian analysis techniques, in particular belief network analysis to calculate the conditional probabilities and the potential magnitude of a release of activity into the environment [14]. STM had been designed to provide a rapid indication of the most likely source terms, prior to a release occurring, using plant data which will be available to the plant operator whilst following emergency procedures to control the critical safety functions. The module is stand-alone and PC based and does not require expert knowledge of severe accidents or fission product behavior. It has been developed using PSA Level 1 and Level 2 results for PWR Sizewell B plant in the UK. Source term categories are defined for the 3 release points (primary circuit/containment, secondary circuit and the auxiliary circuits) with information provided on the quantity and timing of the release.

5. Future safety work

Future reactor safety work in Sweden obviously will have its main focus on maintaining the safety of existing and aging reactors. Maintaining, and, where necessary and reasonably achievable, improving the safety of existing reactors will include three challenges: control of any degradations of materials and components, systematic reassessment of the safety cases and maintaining the necessary competence in nuclear technology as a part of the national infrastructure.

For many accidents and incidents that have occurred there have also been precursors. One very important safety issue is to identify such precursors before they are allowed to develop into a full-blown accident. Perhaps the best benefit for safety is to use advanced computer codes to try to analyze and understand the small trivial incidents that have the potential, combined with some human errors or inherent error, to develop into a severe accident.

Future safety evaluation is likely to be enhanced by the methods of Living PSA and Safety Indicators [8]. Research and development in these areas is ongoing, among others in the framework of the Nordic Nuclear Safety Research Program (NKS). Living PSA is a process to update the PSA model to represent the current or planned plant configuration and to use the model to evaluate and suggest the changes in the configuration. Living PSA is a safety management system for daily uses and it is based on a plant specific PSA and information support system. The main applications of living PSA are:

- long-term safety planning,
- risk planning of operational activities,
- risk analysis of operating experiences.

The purpose of safety indicators is to help in identifying the early signals of deteriorating performance and thereby to provide means for early warning of impending problems before a serious incident or accident occurs. The indicators are based on different types of experience data.

It is expected that development and implementation of CDSS will continue. The advantages of DCSS have been demonstrated during validation processes and the nuclear power plant operators have basically a positive attitude towards using the systems. However, the validation processes have indicated that CDSS can comprise too much information thus making the system too complex. Successful applications of CDSS will therefore require careful evaluation and validation, in particular the human factors aspects of introducing new functions in the control room.

References

[1] F. Adorján, A. Horneas, Cs. Horváth, J.E. Hulsund, Gy. Kapocs, S. Lipcsei, Cs. Major, J. Végh. The EOP visualization module integrated into the PLASMA on-line nuclear power plant safety monitoring and assessment system. *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, Washington, DC, November, 2000.

[2] T. Engquist, T. Lehto, B. Jansson. Principles and development strategies for procedures with a focus on abnormal situations. *IAEA Specialist Meeting on Operating Procedures for Nuclear Power Plants and their Presentation*, Wien, March 31–April 2, 1992.

[3] H. Esmaili, S. Orandi, R. Vijaykumar, M. Khatib-Rahbar, O. Zuchuat, U. Schmocker. ADAM: An accident diagnostics, analysis and management system. In: G. Guedes Soares, ed., *Advances in Safety & Reliability*, p. 257, 1997.

[4] P. Fantoni, Y. Iguchi, G. Meyer, A. Sörenssen, C. Van Dycke. *CAMS Achievements in 1996.* NKS/RAK-2(97)TR-B3, OECD Halden Reactor Project, 1997.

[5] P. Fantoni, M. Hoffmann, B, H. Nystad, M. V. Oliviera. Integration of sensor validation in alarm structuring and suppression. *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, Washington, DC, November, 2000.

[6] W. Frid, ed. *Severe Accident Research and Management in Nordic Countries: A Status Report.* NKS/SOS-2.3 Project, SKI Rapport 00:46, 2000.

[7] L. Högberg. The Swedish program on severe accident management and release mitigation. *Int. Symp. on Severe Accidents in Nuclear Power Plants*, Sorrento, Italy, 1988.

[8] J. Holmberg, K. Laakso, E. Lehtinen, G. Johanson. *Safety Evaluation by Living Probabilistic Safety Assessment and Safety Indicators.* Final Report of the NKS Project SIK-1, Tema Nord 1994:614, 1994.

[9] G. Löwenhielm et al. Verification of accident management strategies at the Forsmark Plant. *OECD/CSNI Specialist Meeting on Severe Accident Management Development*, Rome, Sept. 1991.

[10] G. Löwenhielm, B. Jansson, V. Gustavsson. New ideas about procedures and handbooks for severe accident management at the Forsmark Nuclear Power Plants. *The Fifth International Topical Meeting on Nuclear Thermal Hydraulics, Operations and Safety (NUTHOS-5)*, China, 1997.

[11] F. Övre, C. Holmström, S. Nilsen, P. van Gemst. *Safety Assessment and Post Trip Guidance — The SAS II Project for the Forsmark NPP: A Final Report.* OECD Halden Reactor Project, HPR-342, February 1993.

[12] B. Pershagen. *Light Water Reactor Safety.* Pergamon Press, 1989.

[13] *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.* USAEC Report WASH-1400, U.S. Nuclear Regulatory Commission, October 1975.

[14] C. Rojas-Palma et al. On and off-site source term estimation during nuclear emergencies. *7th Topical Meeting on Emergency Preparedness and Response.* California, USA, September 1999.

[15] A. Santinelli et al. *Operator Assisting Systems for Accident Management, State of the Art Report.* European Commission, EUR 16925 EN, 1996.

[16] *Severe Accident Management: Prevention and Mitigation.* OECD, Nuclear Energy Agency, Paris 1992.

[17] E. Söderman, ed. *Severe Accident Analysis in Sweden — Methods and Results.* RAMA III Final report, RAMA III 89-02, Studsvik Library, Sweden, December 1989.

[18] *"The T-Bok", Reliability Data of Components in Nordic Reactor Power Plants*, Fourth Edition. Jointly published by the Nordic utilities and SKI, 1994.