SECOND SPECIALIST MEETING ON OPERATOR AIDS FOR SEVERE ACCIDENT MANAGEMENT

PROCEEDINGS

Organised in collaboration with EDF/SEPTEN

Lyon, France
8-10 September 1997

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY

Le Seine Saint Germain - 12, Boulevard des Iles
F-92130 Issy-les-Moulineaux (France)
Tel. (33-1) 45 24 82 00 Fax (33-1) 45 24 11 10
ORGANIZATION FOR ECONOMIC
COOPERATION AND DEVELOPMENT

NUCLEAR ENERGY AGENCY

STEERING COMMITTEE
FOR NUCLEAR ENERGY

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

SECOND OECD SPECIALIST MEETING ON
OPERATOR AIDS FOR SEVERE ACCIDENT MANAGEMENT
(SAMOA-2)

Lyon, FRANCE
September 8-10, 1997

Organized in Collaboration with
Electricité de France
(Service Études et Projets
Thermiques et Nucléaires)

This meeting is organized by
CSNI’s Principal Working Group on the
Confinement of Accidental Radioactive Releases (PWG4)
Task Group on Containment Aspects of
Severe Accident Management (CAM)
OECD

The Convention establishing the Organization for Economic Cooperation and Development (OECD) was signed on 14th December 1960.

Pursuant to Article 1 of the Convention, the OECD shall promote policies designed:

. To achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;

. to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and

. to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The current Signatories of the Convention are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, The United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), and the Republic of Korea (12th December 1996). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention)

NEA

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958, under the name of the OEEC Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of all European member countries of OECD as well as Australia, Canada, Japan, Republic of Korea, Mexico, and the United States. The Commission of the European Communities takes part in the work of the Agency.

The primary objective of NEA is to promote co-operation among the governments of its participating countries in furthering the development of nuclear power as a safe, environmentally acceptable and economic energy source.

This is achieved by:

- encouraging harmonization of national regulatory policies and practices, with particular reference to the safety of nuclear installations, protection of man against ionizing radiation and preservation of the environment, radioactive waste management, and nuclear third party liability and insurance;

- assessing the contribution of nuclear power to the overall energy supply by keeping under review the technical and economic aspects of nuclear power growth and forecasting demand and supply for the different phases of the nuclear fuel cycle;
-developing exchanges of scientific and technical information particularly through participation in common services;

- setting up international research and development programmes and joint undertakings.

In these and related tasks, NEA works in close cooperation with the International Atomic Energy Agency in Vienna, with which it has concluded a Co-operation Agreement as well as with other international organizations in the nuclear field.

**CSNI**

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers. It was set up in 1973 to develop and coordinate the activities of the OECD Nuclear Energy Agency concerning the technical aspects of the design, construction, and operation of nuclear installations insofar as they affect the safety of such installations. The Committee’s purpose is to foster international cooperation in nuclear safety amongst the OECD Member countries.
SECOND OECD SPECIALIST MEETING ON
OPERATOR AIDS FOR SEVERE ACCIDENT MANAGEMENT
(SAMOA-2)

(Lyon, France; 8-10 September 1997)

Chairman : M. Vidard (EDF/SEPTEN)

PROGRAMME

MONDAY, 8 SEPTEMBER 1997

08.30 - 09.00  REGISTRATION

09.00 - 09.20  WELCOME :

M. Vidard, Workshop Chairman
J. Royen [OECD (NEA)]

09.20 - 15.00  SESSION I - OPERATOR AIDS FOR CONTROL ROOMS

Chairman : B. De Boeck (AVN, Belgium)

09.20 - 09.50  Some Problems on Operator Aids for Low Probable Severe Accident
Management in Connection with RBMK Channel Reactors
by A. Kramerov, È. Burlakov and D. Mihailov (RRC KI, Russia)
A. Bukrinsky (GAN RF, Russia)
09.50 - 10.35  System of Dynamic Barriers (SDB) Preventing the Development of Emergency Transients at Nuclear Power Plants as a Tool for Operators’ Aid
by I.D. Rakitin and S.D. Malkin (RRC KI, Russia)
A.S. Stebenev and M.M. Khoudiakov (Leningrad NPP, Russia)

followed by

Base Principles and Approach at Design of Generalized Operator Support System (GOSS)
by I.D. Rakitin and S.D. Malkin (RRC KI, Russia)
A.S. Stebenev and M.M. Khoudiakov (Leningrad NPP, Russia)

10.35 - 11.00  BREAK

11.00 - 11.30  Operator Support System for Multistage Accident Management
by Jaejoo Ha, Kwangsub Jeong and Jongtae Jeong (KAERI, ROK)

11.30 - 12.00  A Neuro-Fuzzy Model Applied to Full Range Signal Validation of PWR Nuclear Power Plant Data
by P.F. Fantoni (IFE, Norway-OECD HRP)
S. Figedy (VUJE, Slovakia)
B. Papin (CE Cadarache, France)

12.00 - 12.30  CAMS : A Computerised Accident Management System for Operator Support During Normal and Abnormal Conditions in Nuclear Power Plants
by P.F. Fantoni, A. Sørensen and G. Mayer (IFE, Norway-OECD HRP)

12.30 - 14.00  LUNCH

14.00 - 14.30  EC-Sponsored Research Activities on Accident Management Measures
by J. Martin Bermejo (CEC/DGXII-F-5)
M.L. Ang (NNC Ltd, UK)

14.30 - 15.00  General Discussion on Session I

15.00 -  Computer Demonstrations
TUESDAY, 9 SEPTEMBER 1997

08.30 - 10.30  Technical Visits (SIPA)

10.30 - 11.00  BREAK

11.00 - 17.30  SESSION II - OPERATOR AIDS FOR TECHNICAL SUPPORT CENTRES

Chairman: T. Bjørlo (IFE, Norway-OECD HRP)

11.00 - 11.30  Development of Emergency Response Support System for Accident Management
   by T. Taminami (TEPCO, Japan)
   R. Kubota and T. Fujiwara (Hitachi, Japan)
   N. Yamane and Y. Takizawa (Toshiba, Japan)

11.30 - 12.00  Computer Based Aids at the Spanish Nuclear Safety Council (CSN)
   Emergency Room (SALEM)
   by J.R. Alonso Escós, S. Aleza Enciso and A. Munuera Bassols (CSN, Spain)

12.00 - 12.30  Cofrentes Nuclear Power Plant Risk Management Tools
   by J. Suárez and L. Borondo (Iberdrola, Spain)

12.30 - 14.00  LUNCH

14.00 - 14.30  Reactor Safety Assessment System (RSAS) Development and Lessons Learned
   by J.B. O'Brien and D. Marksberry (NRC, USA)
   M. Modarres (U. Maryland, USA)

14.30 - 15.00  Guidance for Reactor Operators and TSC Personnel with the Severe Accident Management Guidelines
   by M.F. Van Haesendonck and R.P. Prior (W.E.S.E., Belgium)

15.00 - 15.30  Information Validation Tool for Technical Support Centres
   by Ph. Alexandre (CEA/SSAE, France)
   H. Cappon (Framatome, France)
   A. Serrot (EDF/SEPTEN, France)

15.30 - 16.00  BREAK

16.00 - 16.30  Methodology and Software Tools Used by IPSN Crisis Centre Experts During an Emergency in a French PWR
   by D. Winter and J.M. Agator (IPSN/DPEA/SEAC, France)
16.30 - 17.00  PWR Simulation Models Used by EDF/SEPTEN Crisis Team
by A. Sekri, B. de Magondeaux, F. Piza and A.C. Auge (EDF/SEPTEN,
France)

17.00 - 17.30  General Discussion on Session II
WEDNESDAY, 10 SEPTEMBER 1997

09.00 - 12.30  SESSION III - SIMULATION TOOLS FOR OPERATOR TRAINING

Chairman : M. Vidard (EDF/SEPTEN, France)

09.00 - 09.30  Severe Accidents and Operator Training : Discussion of Potential Issues
by M. Vidard (EDF/SEPTEN, France)

09.30 - 10.00  Full-Scope Simulator with an Extended Scope of Modeling as a Tool for
Development and Proof of Operator Aids for Severe Accident Management
by S.D. Malkin, V.V. Shalia, I.D. Rakitin and A.A. Tutnov (RRC KI, Russia)

10.00 - 10.30  Development of an Integrated Simulator and Real Time Plant Information
System for Training in Severe Accidents
by P. Corcuera, M. Garcés and J. Melara (University of Cantabria, Spain)
J. González and J.V. López (Nuclenor, Spain)

10.30 -11.00  BREAK

11.00 - 11.30  Phenomenology and Course of Severe Accidents in PWR Plants - Training by
Teaching and Demonstration
by M. Sonnenkalb and J. Rohde (GRS, Germany)

11.30 - 12.00  Integration of Operator Actions in Accident Sequence Simulation Tools -
Application to a BWR Plant
by J. Hortal and E. Melendez (CSN, Spain)
A. García-Zamorano (UPM/DSE, Spain)

12.00 - 12.30  General Discussion on Session III

12.30 - 14.00  LUNCH

14.00 - 15.30  GENERAL DISCUSSION

Chairman : M. Vidard (EDF/SEPTEN, France)

14.00 - 14.30  Session Chairmen Summaries

14.30 - 15.30  Questions from the Audience - General Discussion

15.30  Close of the Workshop
LIST OF PARTICIPANTS

BELGIUM

Mr. Benoît De Boeck
Director, Nuclear Safety Analyses Department
AIB - Vinçotte Nuclear (AVN)
Avenue du Roi, 157
B-1190 Bruxelles
Phone : +32 2 536 83 35
Fax : +32 2 536 85 85
E-mail : dbb@avn.be

Mr. Louis Vandermeeren
Head, Safety and Training Department
Electrabel
Zone de Production Nucléaire de Tihange
Avenue de l'Industrie, 1
B-4500 Tihange
Phone : +32 85 24 30 11 ext. 3900
Fax : +32 85 24 39 79
E-mail : louis.vandermeeren@electrabel.be

Mr. Michel Van Haesendonck
Training Coordinator
Safety & Systems Engineering
Westinghouse Energy Systems Europe S.A.
Boulevard Paepsem, 20
B-1070 Bruxelles
Phone : +32 2 556 87 98
Fax : +32 2 556 86 71

Mr. Patrick Wilmart
Head, Safety & Licensing Group
Tractebel Energy Engineering
Avenue Ariane, 7
B-1200 Bruxelles
Phone : +32 2 773 75 41
Fax : +32 2 773 89 00
E-mail : patrick.wilmart@tractebel.be
FRANCE

Mr. Philippe Alexandre
Engineer
SSAE/LAER
Département d’Etudes des Réacteurs (DER)
Bâtiment 238
Commissariat à l’Energie Atomique
Centre d’Etudes de Cadarache
F-13108 Saint Paul lez Durance CEDEX
Phone : +33 4 42 25 26 96
Fax : +33 4 42 25 24 08
E-mail : palexandre@cea.fr

Mr. François Arnould
Severe Accident/PSA Group Manager
Technicatome
445 Rue André Ampère
B.P. n° 34000
F-13791 Aix-en-Provence CEDEX 3
Phone : +33 4 42 25 10 37
Fax : +33 4 42 25 91 40
E-mail : -----

Mr. Hendrik Cappon
Technical Support Manager Emergency Organisation
EPE
FRAMATOME
Organisation de Crise
Tour Framatome
1 Place de la Coupole
F-92084 Paris La Défense CEDEX
Phone : +33 1 47 96 36 09
Fax : +33 1 47 96 16 80

Mr. Jérôme Delerue
Engineer
UNIPE/BEM
Electricité de France
Centre Affaires Michelet
F-92060 Paris La Défense CEDEX
Phone : +33 1 49 02 89 49
Fax : +33 1 49 02 89 88
E-mail : jerome.delerue@dept.edfgdf.fr
Mr. Jacques Duco (part-time)
Adjoint au Chef du Département de Prévention
et d'Etude des Accidents (DPEA)
Institut de Protection et de Sécurité Nucléaire (IPSN)
Centre d'Etudes Nucléaires de Fontenay-aux-Roses
Boîte Postale 6
F-92265 Fontenay-aux-Roses CEDEX
Phone : +33 1 4654 7068
Fax : +33 1 4654 4437
E-mail : jacques.duco@ipsn.fr

Mr. Bruno de Magondeaux
Head of "Systems" Group, Process and Operating Section
Engineering and Construction Division
Basic Design Department
Electricité de France
Service Etudes et Projets Thermiques et Nucléaires (SEPTEN)
12-14 Avenue Dutriévoz
F-69628 Villeurbanne CEDEX
Phone : +33 4 72 82 72 31
Fax : +33 4 72 82 77 05
E-mail : bruno.magondeaux@edfgdf.fr

Mr. Alain Serot
Engineering and Construction Division
Basic Design Department
Electricité de France
Service Etudes et Projets Thermiques et Nucléaires (SEPTEN)
12-14 Avenue Dutriévoz
F-69628 Villeurbanne CEDEX
Phone : +33 4 72 82 73 88
Fax : +33 4 72 82 77 05
E-mail : alain.serot@edf.gdf.fr

Mr. Michel Vidard
Project Leader, REP 2000 Programme
Electricité de France
Service Etudes et Projets Thermiques et Nucléaires (SEPTEN)
12-14 Avenue Dutriévoz
F-69628 Villeurbanne CEDEX
Phone : +33 4 72 82 75 65 (secretary : 77 53)
Fax : +33 4 72 82 77 01
E-mail : michel.vidard@de.edfgdf.fr
Mr. Denis Winter  
Deputy Head, Accident Studies Division  
Service d’Etudes sur les Accidents (SEAC)  
Département de Prévention et d’Etude des Accidents (DPEA)  
Institut de Protection et de Sûreté Nucléaire (IPSN)  
B.P. 6  
F-92265 Fontenay-aux-Roses CEDEX  
Phone : +32 1 46 54 91 11  
Fax : +32 1 46 54 32 64  
denis.winter@ipsn.fr

GERMANY  
Dr. Martin Sonnenkalb  
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH  
Schwertnergasse 1  
Postfach 10 16 50  
D-50667 Köln 1  
Phone : +49 221 2068 686  
Fax : +49 221 2068 888  
E-mail : som@grs.de

HUNGARY  
Dr. Iván Lux  
Division Head  
Hungarian Atomic Energy Commission  
Nuclear Safety Inspectorate  
P.O. Box 676  
1539 Budapest 114  
Phone : +36 1 156 27 72  
Fax : +36 1 155 15 91  
E-mail : h1738lux@ella.hu or lui@sunserv.kfki.hu

JAPAN  
Mr. Tadashi Fujiwara  
Senior Engineer  
First Power Plant Control System Engineering Department  
Electrical Machinery & Digital Control Systems Group  
Hitachi Engineering Co., Ltd.  
3-1-1, Saiwai-cho  
Hitachi-shi  
Ibaraki-ken, 317  
Phone : +81 294 23 5387  
Fax : +81 294 23 6617 or 6618  
E-mail : kozaki@cm.hitachi.hitachi.co.jp
Mr. Isao Sakaki
Chief Engineer
Systems Safety Department
Nuclear Power Engineering Corporation (NUPEC)
5F Fujita Kanko Toranomon Building
3-17-1, Toranomon
Minato-ku
Tokyo 105
Phone : +81 3 5470 5461
Fax : +81 3 5470 5466
E-mail : sakaki@nupec.or.jp

KOREA
Dr. Jaejoo Ha
Integrated Safety Assessment Team
Korea Atomic Energy Research Institute (KAERI)
P.O. Box 105
Yusung
Taejeon
Phone : +82 42 868 2755
Fax : +82 42 868 8374
E-mail : jjha@nanum.kaeri.re.kr

NETHERLANDS
Mr. Peter J.T. Bakker
Consultant
KEMA Nederland B.V.
Utrechtseweg 310
Postbus 9035
6800 ET Arnhem
Phone : +31 26 3 56 35 75
Fax : +31 26 4 45 90 35
E-mail : p.j.t.bakker@mta9.kema.nl

Mr. George L.C.M. Vayssier
Nuclear Safety Consultancy (NSC)
Akenwerf 35
2317 DK Leiden
Phone : +31 71 521 5144 or 70 333 5543
Fax : +31 71 521 5144
E-mail : vayssier@pi.net
RUSSIAN FEDERATION

Prof. Alexandre Kramerov
Head of Laboratory
Department of Channel Reactors
Nuclear Reactors Institute
Russian Research Center “Kurchatov Institute”
Kurchatov Square 1
123182 Moscow
Phone : +7 095 196 97 10
Fax : +7 095 196 96 68
E-mail : kramerov@kloss-gw.dcnr.kiae.su

Prof. Semion D. Malkine
Head, Department of Dynamics, Control and Mathematical Modeling
Russian Research Center “Kurchatov Institute”
Kurchatov Square 1
123182 Moscow
Phone : +7 095 196 93 78
Fax : +7 095 190 51 71 or +7 095 943 00 74
E-mail : sdm@odumm.imp.kiae.ru

Dr. Igor D. Rakitine
Head, Laboratory of Control and Automation
Russian Research Center “Kurchatov Institute”
Kurchatov Square 1
123182 Moscow
Phone : +7 095 196 93 78
Fax : +7 095 190 51 71 or +7 095 943 00 74
E-mail : igor_rakitin@odumm.imp.kiae.ru

SPAIN

Mr. José Ramón Alonso Escós
Consejo de Seguridad Nuclear (CSN)
c/ Justo Dorado, 11
28040 Madrid
Phone : +34 1 346 02 07
Fax : +34 1 346 05 88
E-mail : jrae@csn.es

Mrs. Lourdes Borondo
Nuclear Engineer
Nuclear Generation Department
Iberdrola Ingeniería y Consultoría
Avenida de Burgos, 8B
28036 Madrid
Phone : +34 1 383 31 80
Fax : +34 1 383 33 11
E-mail : lourdes.borondo@iberdrola.es
Mr. Mario Garcés  
Department of Applied Mathematics and Computer Science  
University of Cantabria  
Avenida de los Castros s/n  
39005 Santander  
Phone : +34 42 20 18 43  
Fax : +34 42 20 18 29  
E-mail : mario.garces@nuclenor.es

Mr. Javier Hortal  
Modelling and Simulation Expert  
Consejo de Seguridad Nuclear (CSN)  
c/ Justo Dorado, 11  
28040 Madrid  
Phone : +34 1 346 02 83  
Fax : +34 1 346 05 88  
E-mail : fjhr@csn.es

SWITZERLAND  
Dr. Olivier Zuchuat  
Hauptabteilung für die Sicherheit  
der Kernanlagen (HSK)  
CH-5232 Villigen-HSK  
Phone : +41 56 310 3866  
Fax : +41 56 310 3854  
E-mail : zuchuat@hsk.psi.ch

UNITED STATES  
Mr. James B. O'Brien  
EP Specialist  
Emergency Preparedness and Radiation Protection Branch  
Division of Reactor Program Management  
Office of Nuclear Reactor Regulation  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555-0001  
Phone : +1 301 415 2919  
Fax :  
E-mail : jbo@nrc.gov
OECD HALDEN REACTOR PROJECT

Mr. Thorbjørn J. Bjørlo
Division Head, Control Room Systems
OECD Halden Reactor Project
Institutt for Energiteknikk
P.O. Box 173
N-1751 Halden
Norway
Phone : +47 69 21 22 00 ext. 22 70
Fax : +47 69 21 24 60
E-mail : thorbjorn.bjorlo@hrp.no

Dr. Paolo F. Fantoni
Principal Adviser
OECD Halden Reactor Project
Institutt for Energiteknikk
P.O. Box 173
N-1751 Halden
Norway
Phone : +47 69 21 22 93
Fax : +47 69 21 24 60
E-mail : paolof@hrp.no

COMMISSION OF THE EUROPEAN COMMUNITIES

Mr. Joaquin Martin Bermejo
Directorate-General for Science, Research and Development (DG XII/F-5)
Commission of the European Communities (CEC)
Rue de la Loi, 200
B-1049 Brussels
Belgium
Phone : +32 2 295 8332
Fax : +32 2 295 4991
E-mail : joaquin.martin-bermejo@dg12.cec.be

OECD NUCLEAR ENERGY AGENCY

Dr. Jacques Royen
Deputy Head, Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine - Saint Germain
12 Boulevard des Iles
F-92130 Issy-les-Moulineaux
France
Phone : +33 1 45 24 10 52 (secretary : 10 53)
Fax : +33 1 45 24 11 10
E-mail : jacques.royen@oecd.org or royen@nea.fr
Local Organiser

Mrs. Neige Martin
Electricité de France
Service Etudes et Projets Thermiques et Nucléaires (SEPTEN)
Electricité de France
12-14 Avenue Dutriévoz
F-69628 Villeurbanne CEDEX
France

Phone : +33 4 72 82 74 11
Fax : +33 4 72 82 76 94
E-mail : neige.martin@de.edfgdf.fr
SUMMARY AND CONCLUSIONS

I) - INTRODUCTION

The second OECD Specialist Meeting on Operator Aids for Severe Accident Management (SAMOA-2) was organized in Lyon, France from 8th to 10th September 1997 in collaboration with the Thermal and Nuclear Studies and Project Department (SEPTEN) of Electricité de France.

It was attended by thirty-three specialists representing ten OECD Member countries, the OECD Halden Reactor Project, the Commission of the European Communities, and the Russian Federation.

A number of operator aids (OA) had been presented during the first OECD Specialist Meeting on Operator Aids for Severe Accident Management and Training (SAMOA-1) held at the OECD Halden Reactor Project in June 1993. Some of them were already in operation, others were under development with a view to implementation within the next few years. SAMOA-1 had shown that the field was very active because of real needs and the possibilities offered by computer technology. It had therefore been concluded that another meeting should be organized in the not too distant future.

As for SAMOA-1, the scope of SAMOA-2 was limited to operator aids for accident management which were in operation or could be soon. The meeting concentrated on the management of accidents beyond the design basis, including tools which might be extended from the design basis range into the severe accident area. Relevant simulation tools for operator training were also part of the scope of the meeting.

Twenty papers were presented during the meeting. There were two demonstrations of computerized systems: the ATLAS analysis simulator developed by GRS, and EDF's "Simulateurs Post Accidentels" (SIPA). There was also a video demonstration of the Full Scope Simulator developed by a joint Russian-U.S. team for the Leningrad nuclear power
II) - CONCLUSIONS

2.1 - General

*It is clear that the development and implementation of operator aids for accident management is in progress in several countries.

*Both at the level of nuclear power plants and in national emergency centers (those of the utilities and those of the regulatory organisations), the current computer-based calculational tools are essentially the same as those already presented at the SAMOA-1 meeting. However, they have been enhanced to a considerable degree with respect to both calculational scope and performance (predictions are now frequently much faster than real-time). Moreover, they have been extensively validated against best-estimate codes. Computer-based calculational tools are successfully used during safety drills to assess the state of the plant and to predict the possible progression of the accident. However, there is still need for further work to improve some of these tools, in particular with respect to additional accident sequences and the development of more plant-specific models.

*Implementation of the more advanced computerized tools for accident management support like advanced predictive simulators in the Technical Support Center (TSC) has proceeded much slower than was expected at the SAMOA-1 meeting.

*Although opinions differ on the extent of operator training needs for severe accident scenarios, as discussed below, training for severe accident management (SAM) is generally considered beneficial. However, it is lagging behind SAM implementation programmes. The main purpose of training on OA systems is to enhance operator readiness for emergency situations, increase his mental flexibility and test his reactions. This is the reason why a number of specialists think that full scope simulators should include severe accident models: operators should be faced with and understand the consequences of improper action. OA systems used for operator training should also have application in normal situations, in order to familiarize operators with their use.

*There is also debate on the need for advanced computerized tools in SAM. Some specialists feel that the use of such tools is too complex, that the operators would have too little time to wait for the results of simulations, and that it is not possible to guarantee computer availability. Other experts are of the opinion that computational aids may be useful during the mitigation phase of a severe accident as, in certain sequences, they can provide the operator with information which cannot be obtained from paper-based computational tools such as the computational aids of the Westinghouse Owners’ Group (WOG) Severe Accident Management Guidelines (SAMGs). More research and discussions are needed in this area.

2.2 - Operator training

Three objectives were developed and discussed to various extents:

*knowledge-oriented training, aiming at teaching the operators on severe accident phenomena and progression
*skill-oriented training, allowing to test operator behavior in case of severe accident-like situations

*efficiency-oriented training aiming at analyzing how all involved organizations would behave in case of emergency.

The first two objectives were more debated from the following standpoints:

*should training be knowledge-oriented or skill-oriented, and which conclusions could be drawn for simulators?
   There was no definite answers as some participants thought emphasizing knowledge was sufficient, while others stressed that testing operator behavior in highly perturbed situations would provide valuable information on human factors and would be beneficial for safety. At the simulator level, only the second objective was considered relevant for real-time simulations.

*should operator aids be used for training?
   Here also, there was no clear-cut answer as the need for such aids for SAM was still debated. However, for those considering operator aids, there seemed to be a consensus for recommending tool testing during training sessions.

*should training sessions be used for operator requalification for Severe Accident Management?
   There was a consensus amongst participating regulatory bodies to consider that, though SAM training was considered to be very beneficial, and might even be required in some countries, there was no plan to consider SAM skills to be part of the formal operator licensing.

Efficiency of the organization put in place in case of emergency was not extensively debated, but specific problems were mentioned such as diagnostic discrepancies in the course of the accident and their impact when interfacing with the media.

Though agreement was not complete amongst participants, a majority thought that developing aids for non technically-oriented managers should be considered as future deregulation of the electricity market could lead to dramatic changes at the plant management level.

At last, as training for severe accidents could still be considered in infancy, there was general agreement that there was room for exchanges of information and (or) cooperation for defining objectives more precisely, together with associated requirements for an effective implementation.

2.3 - Operator aids

With respect to the use of operator aids in severe accident management, it is clear that such tools must be integrated with the Severe Accident Management Guidelines (SAMGs) in order to be of practical use.

At the meeting, no actual use of advanced computerized operational tools in the control room or TSC at the plant was reported. At the moment, there seems to be no consensus with respect to the usefulness of such tools for SAM at the plant. One viewpoint is that the use of SAMGs including simple, graphical, and paper-based computational aids (CAs) is the most effective, and that use of more advanced, computer-based tools is too complicated and
unpractical. Another viewpoint is that such tools would be useful in certain accident sequences, especially for the TSC at the plant, as it would provide additional useful information which the paper-based tools cannot provide. This is an unresolved question, and further research is needed, possibly through human factors experiments comparing operator performance when using different tools.

Another conclusion from the meeting was that if computerized tools are to be used for SAM at the plant, the tools or at least tools with the same man-machine interface must be used also during normal operation to make the operators familiar with the tools so that they will use them in accident situations.

2.4 - Areas for improvement

Signal validation and more generally information validation is recognized as being an important aspect of severe accident management. Indeed plant operators and emergency team experts need to rely on information given by the plant instrumentation. However, this information might come from failed sensors or from instrumentation working outside its validity range. Several methods and tools able to screen and validate the information presented to the operators were presented and discussed at the meeting. It can be concluded that this area of expertise is not yet mature. The use of advanced techniques such as fuzzy logic and artificial neural networks is being tested. Such techniques look very promising, but important problems remain to be solved like their qualification and the formal proof of their reliability.

Another important aspect related to the use of operator aids is the need for good communication and understanding between the different teams involved. It has been noted that in some countries, different tools are being developed for the control room operators, the on-site Technical Support Center and national emergency teams. There is a possibility to arrive at conflicting conclusions at different places. The way to resolve such conflicts has to be taken into account beforehand in the emergency organization. On the other hand, if the consistency of the tools used at different places has been verified, their use could facilitate communication, because people would essentially use the same language.

Finally, the use of Internet was proposed as a convenient way to share information between interested countries. There was no time at the meeting to discuss what concrete form this collaboration could take, but the Programme Committee is of the opinion that the Internet offers a complementary way to let information circulate and recommends that an appropriate forum be found to discuss the use of the Internet in the area of operator aids for severe accident management.

2.5 - International Collaboration

It was agreed unanimously that international collaboration and information exchange should be increased with respect to the development of computer-based operator aids and their applicability to operator training for severe accident management. In particular, there is a strong need to exchange views and experience related to the sort of training to be given to operators to cope with severe accident management situations and the most appropriate simulators.
SESSION SUMMARIES

SESSION I: OPERATOR AIDS FOR CONTROL ROOMS

Session Chairman: Benoît De Boeck (AVN, Belgium)

Session I dealt with calculational aids the mission of which is to assist the operator in the control room to prevent and mitigate severe accidents. Rather than to report on experience with implemented systems, all papers presented during the sessions described either systems under development, or related research activities. The R&D activities reported at the meeting covered theoretical studies (in Russia), signal validation (at the OECD Halden Project), and the activities sponsored by the European Commission. Actual systems developed in Russia, in Korea and at the Halden Project were also described. In all, seven papers were presented during the session. They are briefly summarized below.

A. Kramerov (RRC KI, Russia) presented “Some Problems on Operator Aids for Low Probable Severe Accident Management in Connection with RBMK Channel Reactors”. Most of the problems that were faced during the development of operator aids for RBMK are however of a general nature. The first one concerns the need to build enough flexibility in the tools so that the operators are not lost if they encounter situations unforeseen in the symptom-oriented instructions. Connected with this is the problem of the identification and the classification of the severe accidents that are to be covered. To make sure that all essential cases are considered, the selection process was based on a combination of fission product barrier failure and the involved core part. It was then necessary to classify the great number of identified scenarios in a small number of groups that were felt to be most convenient for the operators. The severity of the event and the type of management strategy played an important role in this classification scheme. Finally, the need to evaluate and present to the operators parameters for which there exist no measurement was also felt by the author to be important for the diagnostic and the management of severe accidents.

I.D. Rakitin (RRC KI, Russia) presented “System of Dynamic Barriers Preventing the Development of Emergency Transients at Nuclear Power Plants as a Tool for Operators’ Aid”. The barriers here are the borders between the different plant conditions or states as defined in the INES scale. They have nothing to do with physical barriers like the ones that prevent radioactive releases. Because crossing such a barrier means increasing the severity level of the event, it is important that all features that can prevent this crossing are correctly identified. Such features include not only systems and components, but also procedures and communication means that can increase the reliability of the human intervention. Because these features can be different for the barriers between the different states, it is important to correctly identify the exact state of the plant and then to identify the means available to prevent the situation from worsening. A prototype of such an operator aid was described in the subsequent paper.

I.D. Rakitin (RRC KI, Russia) presented “Base Principles and Approach at Design of Generalized Operator Support System (GOSS)”. This paper presents a computerized operator aid based on the approach presented in the previous paper. The goal of the system is to help
operators manage incident and accident situations. The GOSS is being developed and tested on the Leningrad full scope simulator and is intended to be installed in the future in the main control room of the Leningrad power station. To increase the trust of the operators in the system and its applicability, the GOSS is designed to cover the full range of plant conditions from normal operation to incidents, design basis accidents and, at a later stage, severe accidents. The GOSS can identify and display the plant status, the critical safety functions and possible actions to control the situation. The feedback from the tests on the simulator has been very positive.

J. Ha (KAERI, ROK) presented “Operator Support System for Multistage Accident Management”. This paper describes the development at KAERI of an integrated computer aided accident management system called KAMP that is intended to be installed in the Korean NPPs. KAMP will cover three stages: (1) before the severe accident takes place, (2) after the initiation of the severe accident, and (3) the radioactive release phase. Stage 1 corresponds to the use of the Emergency Operating Procedures (EOPs), stage 2 is linked with the use of the Severe Accident Management Guidelines, and stage 3 with the emergency plan. The tool for stage 1 is called KOSSN and provides the operator not only with a list of actions based on the EOPs but also additional information like the success paths of the safety systems and the event tree from the plant specific Probabilistic Safety Analysis (PSA). This allows to select the strategy with the highest success probability. The development of a tool for stage 2 has not started yet but the present plan is to base it on MELCOR. The tool for stage 3 is called KACAP and its purpose is to calculate the radiological and economic impact of severe accidents in the environment. This module can have a variety of applications from level 3 PSA to real time operator advice to reduce offsite consequences.

P.F. Fantoni (IFR, Norway-OECD HRP) presented “A Neuro-Fuzzy Model Applied to Full Range Signal Validation of PWR Nuclear Power Plant Data”. To be able to manage an accident, operators need to know what is happening in the plant, and for this they have to rely on the information given by the plant instrumentation. But the question arises of the validity of this information: sensors or connections might fail, especially under severe accident conditions, or data processing might be operating outside its validity domain. It is therefore important for the operator to have some means to assess the reliability of available information. The Halden Reactor Project is studying the use of artificial neural networks and of fuzzy logic to this aim. Such models can be combined to exploit the learning and generalization capability of the first technique with the approximate (“possibilistic”) reasoning embedded in the second approach. The system under development at Halden has been tested in a simulated environment on a French PWR, to monitor safety-related reactor variables over the entire power-flow operating map. Sensor failures were successfully detected. In the presence of unknown scenarios, the model correctly alerted the user about the impossibility to provide a reasonable diagnosis. The capability of the model to operate under accident conditions will be tested in the near future.

P.F. Fantoni (IFR, Norway-OECD HRP) presented “CAMS: A Computerized Accident Management System for Operator Support during Normal and Abnormal Conditions in Nuclear Power Plants”. CAMS is a system that is intended to provide assistance to the staff in a nuclear power plant control room, in the Technical Support Center and in the national emergency center. Support is offered in identification of the current plant state, in assessment of the future development of the accident and in planning prevention and mitigation strategies. CAMS consists of a data acquisition module, a signal validation module, a tracking simulator, a predictive simulator, a state identification module, a probabilistic safety assessment module and a man-machine interface module. In addition, the possibility exists to include a strategy generator and a critical function monitor. The signal validation module is
based on the system described in the previous paper. The PSA module contains plant specific PSA data like event trees and failure probabilities. It calculates the core damage frequency based on the plant states and the component failures. It can also feed the strategy generator with information about the critical systems. The CAMS is designed to operate in all plant conditions, from normal operation to severe accidents (the development of the severe accident part has just started), giving continuity in its interaction with the user.

J. Martin Bermejo (CEC/DGXII-F-5) presented "EC-Sponsored Research Activities on Accident Management Measures". This paper discusses the objectives and achievements of a completed project of the 1992-1995 R&D Framework Programme known as "Accident Management Support" (AMS), and also presents the current status of an on-going project of the 1994-1998 programme called "Algorithm support for accident identification and critical safety functions signal validation" (ASIA). The objectives of AMS were (1) to define, investigate and develop means and methods to provide reliable information and diagnostics, as well as support tools for accident management, and (2) to investigate the different signal validation methodologies with emphasis on the existing instrumentation rather than on new instrumentation needs. The research activities of ASIA will extend and build on the work of AMS. In particular, it will further develop operator aids based on physical models in order to validate critical safety functions measurements and understanding accident progression by using search algorithms.

From these presentations, the first observation is that often the same tool is designed to be used by the main control room operators and the Technical Support Center team. The impression from the SAMOA-1 meeting that the needs of control room operators were very different from those of the emergency team does not seem to have materialized.

A second observation is that some of the tools presented include (or will include) a PSA module. The main goal of incorporating probabilistic capabilities into operator aids is to make a ranking of the proposed strategies according to their success probability. The merit of such an approach, and in particular the question of the added value compared to the added complexity, and the question of the validation, were not discussed in detail at the meeting. This is certainly an area in need of further research.

During the discussion period, participants agreed that signal validation was an important aspect of operator aids, but that signal validation tools are difficult to develop and qualify, especially if one wants to go further than simple cross-checks between redundant sensors. In particular, as artificial neural networks have the capability to recognize patterns, they are very attractive for this kind of activity. However, because they act as a black box, their reliability is hard to prove. More work is needed in the area of signal validation.

Finally, the merit of having the same tool or at least tools with the same man-machine interface giving advice to the operators in all plant conditions, from normal operations to severe accident conditions, compared to dedicated tools for each case was debated. To increase the probability that the operators will use and trust their tool, some advocate that the interface should be the same for all uses. Others are of the opinion that dedicated tools can be more easily optimized. No conclusion as to the best approach was reached at the meeting.
SESSION II : Operator Aids for Technical Support Centres

Session Chairman: Thorbjørn Bjørlo (IFE, Norway - OECD HRP)

The eight papers presented in this session covered a broad range of methodologies, computational tools and guidelines for use in the TSCs and by emergency teams in different countries. The presentations and discussions covered approaches and practices in the following countries: France, Belgium, US, Spain and Japan; utilities, designers (reactor vendors) and safety authorities points of view were presented.

From the presentations it became clear that development and implementation of Severe Accident Management Guidelines are in progress in several OECD Member countries. As an example, all plants in the US are committed to implementation of SAMGs, and it is expected that by the end of 1998 plant specific SAMGs will be implemented at all US plants.

One paper presented by M.F. Van Haesendonck, described the Westinghouse Owners’ Group SAMGs, in particular the graphical computational aids (CA)s incorporated in these guidelines. These are simple, paper-based tools which are used to fulfill the need for information that is not directly available from plant instrumentation.

Several papers addressed tools and simplified computational models to be used by national emergency evaluation teams, both those of the safety organizations and those of the utility. Three papers presented by H. Cappon (Framatome), D. Winter (IPSN) and B. de Magondeaux (EDF-SEPTEN), described the French efforts in this field as well as the latest development of tools used to support the 3D/3P (triple diagnosis / triple prognosis) methodology used to assess the state of the installation and to forecast the possible development of the accident.

In essence these tools are the same as those already presented at the SAMOA-1 meeting in Halden. However, they have been enhanced to a considerable degree with respect to both calculational scope and performance (predictions much faster than real time). Further, they have been extensively validated against best estimate codes like e.g. CATHARE. These tools are successfully used in emergency drills in France.

Also, CSN Spain (J.R. Alonso Escós) reported ongoing development to extend the use of computer-based aids at their Emergency Room. In particular, work is in progress to utilise MARS (MAAP Accident Response System) as a diagnosis and predictive tool based on the set of safety parameters transmitted from the plant in real time. Currently validation of the system towards thermal hydraulic and severe accident codes is taking place. The use of this tool in yearly drills and internal training exercises will improve the capabilities of the Operational Analysis Group of the Emergency Room.

Information Validation is an important issue in Severe Accident Management. In France, a signal validation tool for TSCs is under development (by IPSN/EDF-SEPTEN/Framatome) which aims at assessing the confidence in information based on an analysis of both sensor quality and other factors like redundancy, coherence with other measurements, and state of plant. This is ongoing development; testing and validation of this tool have to be performed before it becomes an important element among the tools used in French TSCs.

The Spanish utility Iberdrola reported a comprehensive programme for implementation of tools and guidelines in their TSC for coping with severe accidents (paper presented by L. Borondo). This includes implementation of SAMGs at the Cofrentes NPP through implementation of extensive Technical Support Guidelines (TSGs) for the TSC. At Cofrentes
they are also developing a severe accident management tool based on the MAAP code and the CAMS system of the Halden Project but this system is in its early development phase.

Two papers presented tools of the expert system type to be used for supporting the assessment of plant safety state by the TSC. The US NRC has developed the Reactor Safety Assessment System (RSAS) which will be used in their operations center (paper presented by J.B. O’Brien). Plant specific models have been made for all the PWRs; work on the BWR version is under way. The RSAS has potential for being very useful for assisting NRC in monitoring emergency response.

The Japanese BWR group (paper presented by T. Fujiwara, Hitachi) has developed a prototype of an Emergency Response Support System (ERSS). The prototype has undergone verification testing which shows that it can be useful and effective in accident management training, especially in improving communication between the control room, the TSC and the head office in emergency cases if all these locations have access to the ERSS.

One observation from the session was that the implementation of the more advanced computerized tools for accident management support like advanced predictive simulators in the TSC has proceeded much slower than expected at the SAMOA-1 meeting held in Halden in 1993. This is especially true for the TSC at the local level, i.e. the TSCs of the specific NPPs. In the discussion, the views from several participants were that at this level, at the plant, advanced computerized tools are not needed in SAM, that is in the mitigation phase, after core damage has occurred. Actually, the use of such tools is too complicated, operators cannot wait for the results of the simulations and one cannot rely on the computers being available, according to the view of these participants.

Other specialists were of the opinion that computerized aids may be useful also in the mitigation phase as they can provide for certain sequences information the operator needs and which he cannot get by paper-based computational tools like the CAs of the WOG SAMGs.

This is an unresolved issue, and more research is needed. Some participants suggested that human factors experiments should be carried out comparing the performance of TSC staff using different tools in simulations of accident scenarios.

With respect to use of tools at the national emergency centers, there has been progress since SAMOA-1, but few new tools were reported. The progress has more been enhancement of tools presented at SAMOA-1 and implementation of such tools in modern PC environments.

An issue brought up in the discussion was the use of different computational tools by the different national emergency centers and by the different emergency evaluation teams, e.g. those of the safety organizations and those of the utility. Could the use of different tools cause communication problems and potential conflicts? Even though the different emergency organizations have different, clearly defined responsibilities, some specialists felt that the use of different tools could be confusing and that some consistency might be called for. Some participants were even of the opinion that computerized tools for Accident Diagnosis and Management were not needed at National Authority Emergency Centers because the responsibility to manage the accident should remain with the utility.
SESSION III: Simulation Tools for Operator Training

Session Chairman: Michel Vidard (EDF-SEPTEN)

Five papers were presented in Session III devoted to Simulation Tools for Operator Training.

The paper presented by M. Vidard of EDF discussed some issues related to operator training for Severe Accident situations.

After recalling the main conclusions of the report issued by the SESAM group (Senior Group of Experts on Severe Accident Management), he noticed that training for Severe Accident Scenarios was considered beneficial but lagging behind implementation of SAM programs.

To explain this, he commented on some differences between accident management and severe accident management and concluded the first part of his presentation saying that, as the problem was complex and cost issues could not be neglected, training could be contemplated only after clear definition of utility objectives.

Three objectives were discussed, one stressing improvement of knowledge, the second operator behavior in case of severe accidents, the third one organization efficiency in case of emergencies.

His conclusion was that there was a potential for cooperation between OECD Member countries in this domain, at least to define what was needed.

The second paper, presented by S.D. Malkin, from the RRC Kurchatov Institute (Russia) described the main features of a full-scope simulator devoted to operator training on RBMK type reactors. After outlining the most significant characteristics of this type of reactors, he stressed that operator error was a non-negligible factor of risk and that the full-scope simulator had been designed to address this kind of problem.

After detailing options and possibilities offered to the user, he stressed the most significant capabilities of the simulator, in particular the adoption of 3-D neutron kinetics (STEPAN-SIM) and advanced thermal hydraulics (KOBRA-SIM) softwares. As mechanical behavior of the fuel plays a role in plant response, the need for implementing the STALACTITE software was also justified.

Finally, the full-scale simulator was tested on the Chernobyl accident scenario, and simulation showed that:

* the simulator had the capability to correctly simulate the accident.
* design upgrades (Safety Systems and fuel loading patterns) had the potential for preventing degradation into a severe accident.
* a skilled operator could prevent massive reactivity injection a few seconds before the neutron power burst.

The ODES on-line diagnosis code was also described, together with the GOSS (operator support system); the author's conclusion was that this type of simulation could be used to improve NPP safety.
The third paper, presented by M. Garcés from the University of Cantabria in Santander - Spain, described an Integrated Simulator and Real Time Information System. Based on the MAAP3 computer code, the simulator allows several operators to interact simultaneously on the process. It includes an anomaly-generating capability both before and during the accident, and operators can interact with the model at any time into the accident. Special attention was paid to visualization; the SCADA graphics software allows to display plant data in real time.

Applications and benefits of the system, already used at the Maria de Garoña Nuclear Plant was also detailed:

*periodic retraining of plant operators, emphasizing human reliability aspects,
*advantages resulting from the SPDS graphics system,
*the capability to feed the plant Technical Support Center, and the Emergency Response Center situated at Utility Headquarters, with simulator data,
*the possible use for training on severe accident scenarios.

At last, possible future developments, i.e. implementation of the MAAP4 code, and the connection of an Expert System allowing tracking of Emergency Operating Procedures, were also described.

The fourth paper, presented by M. Sonnenkalb from GRS Germany complemented the demonstration performed in session I. Responding to the interest of German Utilities, GRS had developed a special training course on the Phenomenology and Progression of Severe Accidents in PWRs.

After analysis of what was required to take full advantage of such a course, it had been decided to develop a numerical tool using off the shelf state-of-the-art Severe Accident modules (MELCOR, ATHLET, RALOC and WECHSEL).

As knowledge-based training was the objective, real-time was not the main concern in developing the numerical tool.

From a sequence (or scenario) standpoint, rather than offering the capability for simulating different types of accidents, emphasis was put on a very specific scenario, considered less improbable than the others in the German context, i.e. total loss of secondary feedwater and total loss of heat sink.

Emphasis is put on the most significant phenomena encountered during accident progression, and on problems specific to Severe Accident scenarios, e.g. instrumentation response or availability, or the consequences of Severe Accident Management Actions. For the latter case, guidance is provided and further justified.

Amongst the conclusion, it can be noted that this tool has the potential for adaptation to BWR scenarios. At the time being, GRS doesn’t consider that there is an urgent need to go beyond what is currently done (no need to evaluate other scenarios or test operator behavior).

The last paper, presented by J. Hortal from the Nuclear Safety Council (CSN) of Spain, Madrid, dealt with the Integration of Operator Actions in Accident Sequence Simulation Tools for a BWR Plant.

Starting from an analysis of some differences between normal operation and accident situations at the system level on one side, on the complexity of physical phenomena on the other side, he stressed that plant behavior during accident was dominated by phenomenology and manual or automatic protective actions. Also, operator actions play a very important role as nobody would expect an operator doing nothing in a perturbed situation.

It was therefore decided to develop a multi-purpose simulator combining simulation capabilities under normal and accident conditions and integrating operator actions. Potential
uses could be for PSAs and Individual Plant Examinations (IPEs), design and verification of procedures, including severe accident guidelines, and simulation of scenarios to derive criteria for operator training or evaluation activities.

The accident simulation package includes three softwares, TIZONA, COPMA II and MAAP. TIZONA simulates plant evolution and communicates with COPMA II, the latter feeding TIZONA with operator actions resulting from Emergency Operating Procedures. Once TIZONA detects that plant parameters are near the range of validity of the model, most simulation work is transferred to the MAAP code. System architecture is such that COPMA II does not make any difference between TIZONA and MAAP, thus simplifying software interface.

After a description of the detailed capabilities of the code, e.g. taking care of operator burden or synchronizing plant and procedure simulation, it was stressed, as a conclusion, that:

*the simulator has already been tested on a Station Blackout Scenario in a BWR, using real plant operating procedures,
*the TIZONA - MAAP software was being completed with manual control inputs needed for the implementation of some procedures,
*a complete set of EOPs for a BWR/6 plant had been edited.

Presentations were followed by a discussion on operator training allowing to stress the following:

*There was a consensus to say that operator training was beneficial.

*Opinions largely differed on what was needed. Some participants, considering that if there were a severe accident, it would anyway never look like scenarios chosen for training sessions, thought that only knowledge-based training was needed to make operators more familiar with physical phenomena and accident progression. Other participants, though agreeing that, if there were a real core melt situation, plant evolution would likely deviate from that seen in scenarios used for training, stressed the interest of analyzing operator behavior under perturbed situations, with the help of real-time simulators.

*Even for those agreeing on the latter, there was no agreement on the kind of simulator which would provide a reasonable approach to operator training.

*The need to provide operator aids and test them during training sessions was also debated, and the specific problem of providing plant managers with adequate tools for making decisions was evoked, in the perspective of more finance-oriented managers in a deregulated electricity market.
Annex

PROGRAMME COMMITTEE

Michel Vidard (EDF-SEPTEN, France) - Chairman

Benoit De Boeck (AVN, Belgium)

Thorbjørn Bjørlo (IFE Norway, OECD HRP)

Jacques Royen (OECD-NEA) - Secretary
SECOND OECD SPECIALIST MEETING ON OPERATOR AIDS FOR SEVERE ACCIDENT MANAGEMENT (SAMOA-2)

OPENING REMARKS

by

Jacques Royen
OECO Nuclear energy Agency

It is a great pleasure for me to welcome you to this Second OECD Specialist Meeting on Operator Aids for Severe Accident Management (SAMOA-2) on behalf of the Organisation for Economic Co-operation and Development (OECD), the OECD Nuclear Energy Agency (NEA), and its Committee on the Safety of Nuclear Installations (CSNI).

The meeting is organised in collaboration with the Department for Thermal and Nuclear Studies and Projects (SEPTEN) of Electricité de France, which we thank very much for their hospitality and for the excellent arrangements made. Our thanks are due to Mr. Michel Vidard, Project Leader of the REP 2000 Programme, who spent much time and effort not only on some of the practical arrangements necessary to make this meeting successful but also contributed ideas and initiatives to the work of the Programme Committee responsible for evaluating the abstracts of papers you submitted and for drawing up the programme of the Workshop. Our gratitude is also due to Mr. Vidard’s collaborators, Mrs. Neige Martin and Mrs. Ghyslaine Mey, who took care very efficiently of the local organisation of the meeting and gracefully welcomed you this morning.

Our thanks are of course also due to the other members of the Programme Committee, who, together with Mr. Vidard, will act as Session Chairmen: Mr. Benoît De Boeck and Mr. Thorbjørn Bjørlo. One of their tasks will be to write during the meeting brief summaries of the highlights and major points of interest of their session; these will be used at starting points for the general discussion closing the meeting. Another task of the Programme Committee members will be to prepare, in a session held immediately after the meeting, a report summarising the main points of the meeting, drawing conclusions and making recommendations.

Finally, I want to thank all the authors who contributed papers to the meeting. The Programme Committee found these generally of high quality. The Proceedings will be published by SEPTEN as soon as possible.

A number of operator aids were presented during the First OECD Specialist Meeting on Operator Aids for Severe Accident Management and Training held at the OECD Halden Reactor Project in June 1993. Some of them were already in operation, others were under development with a view to implementation within the next three years. The meeting showed that the field was very active because of real needs and the possibilities offered by computer technology.
Have these promises been kept? We shall find out during this meeting. Let me stress that the CSNI hopes that the meeting will generate information and conclusions useful for reactor safety applications. Let me emphasise the essential importance of the discussion periods closing each of the sessions. This is where progress is made. In your presentations, please make sure that you leave enough time - at least ten minutes - for discussions. The general discussion at the end of the meeting will be most important. We hope that you will participate actively. During the meeting, the Programme Committee members will try to collect questions, opinions and ideas which could deserve general attention during the debate. Your suggestions will be most welcome.

I wish you a profitable and enjoyable meeting, and a very pleasant stay in the beautiful and historic city of Lyon.
Some problems of operator aids for a low-probable severe accident management in connection with RBMK channel reactors.

A.Kramerov, E.Burlakov, D.Mikhailov, RRC Kurchatov Institute, RF A.Bukrinsky, Scienc-Eng.Centre on Nucl.Radiation Safety, GAN RF

ABBREVIATIONS: ALS- accident localization system (containment); ATWS- anticipated transient without scram; BLW- boiling light water; BDBA- beyond design basis accident; BDB- beyond design basis; DBA- design basis accident; BRUK- quick- action reduction set of condenser; DGH- distribution group header; ADGH- accident DGH; CPS- control protection system; CV- check valve; CL- cooling loop; ACL- accident CL; ECCS- emergency core cooling system; IE- initial event; FA- fuel assembly; FP- fission product; LOCA- loss of coolant accident; LPA- low-probable accident; LR- level regulator; MOC- main coolant circuit; MCP- main circulation pump; MPRT- multichannel pressure tube rupture; ORM- operational reactivity margin; PR- pressure regulator; PT- pressure tube; PH- pressure header; RC- reactor cavity; RIA- reactivity initiation accident; SA- severe accident; SD- steam drum (separator); SF- single failure; SH- suction header; SAR- safety analysis report; SOL- symptom-oriented instruction; SV- safety valve; SC- scenario.

INTRODUCTION

The specific features of BLW cooled graphite moderated channel RBMK-type reactors determine essentially specific severe accident problems - thermohydraulic, mechanic, engineering, technology, phenomenology and management. The last is practically most important and should be developed, although a lot of science engineering data are still absent in this area for such reactors, produced ~60% russian nuclear energy already ~300 r-years.

During the last years in Russia some practically important problems in this field are investigated; the first (preliminary) version of BDBA management guide was elaborated and implemented; now the second essentially changed version is being elaborated.

In this paper we describe and discuss briefly some main connected problems.

1. STATE OF PROBLEM

The designers and especially operators are oriented first of all towards relatively probable accidents resulted from the single failures of equipment, valves and other devices, but not towards very low probable accidents as LOCA, ATWS, RIA, loss of heat sink or DBAs with failures of safety systems, additional to SF.

Low-probable accidents (LPA) include severe accidents and BDBA with frequency <<0.01 1/reactor-year. Our LPA experience is very small; by this reason understanding and feeling of such LPA by operators are much worse than those of relatively probable accidents (frequency >0.1 1/r-year), such as MCP trip, feed water or other pumps trip, turbine condenser cooling water leakage etc.

For example, during the accident it is difficult for an operator to assess the cooling loop water inventory or to make
quickly decision on manual ECCS initiating or pressure quick dropping etc. It is more difficult to stop MCPs, to decrease ECC water flow rate, to cancel some project blockade or make other unusual BDB actions that are reasonable in some beyond design basis accident (BDBA) conditions.

As a rule the accident instructions (emergency operating procedure-EOP) do not give deep understanding and feeling of LPA. It is difficult to be sure that operators' actions will be more or less optimal under the typical LPA conditions: 1) unusual necessary extraordinary actions (such as quick pressure decrease, ECC water flow decrease or MCP trip and isolation and so one); 2) insufficient diagnostic data; 3) essential difference between actual accident progression and scenarios described in operating guides, when it is necessary to "correct" the guides recommendations on line. Moreover sometimes such actions do not agree with operators' usual habits and trends.

Symptom-oriented instructions (SOI) do not content broad explanations and do not make such situations essentially easier for operators.

Safety analysis report is oriented towards conservative justification of safety at the most severe DBAs under unreal extreme conditions. So SAR does not orient the operators towards actions in real conditions.

It seems reasonable to prepare the special operator-oriented description of phenomenology of LPA/BDBA in order to make the broad understanding/feeling of LPA/BDBA processes easier. This is to be done for operators and for the technical team of the SA management specialists who must help choose the optimum management strategy and decision during LPA. The implementation experience of the first version of BDBA-management guide for the first unit of the Leningrad NPP revealed (as a result of questioning) the positive attitude of the operators towards such phenomenology.

The next problem, which is not solved finally, is classification of BDB events most convenient for operators. The comparison of different types of classification (on the basis of initial symptoms; initial events; key processes; severity levels) shows that the most suitable BDBA subdivision would be connected with some intermediate plant states, defining the severity levels and sometimes - the strategy of operator actions.

To be sure that all essential LPA/BDBA will be considered, the classification, based on the combination of fission product barrier failure and the involved core part, is used, namely: the fuel rods or assemblies in one (sign 1) or many channels of one or several distribution group headers (sign 2) of one (sign 3) or both (sign 4) cooling loops; one or several channels without a reactor vessel-RC damage (sign 1) or a lot of channels with a vessel damage (sign 2); the different LOCAs without a confinement damage (sign 1) and with a confinement damage (sign 2) etc.

So, we can sign each accident level by a four-symbol code: FUEL:ASSEMBLY-CHANNEL-COOLING LOOP-CONFINEMENT, where 0 means "not damaged". Formally we can obtain 72 different combinations - "accident levels". Excluding unreal combinations,
29 different levels with several ways (scenarios), leading to each of them, remain. They are present in table:

<table>
<thead>
<tr>
<th>1000</th>
<th>2000</th>
<th>3000</th>
<th>4000</th>
<th>1100</th>
<th>2100</th>
<th>3100</th>
<th>4100</th>
<th>1101</th>
<th>2101</th>
<th>3101</th>
<th>4101</th>
</tr>
</thead>
<tbody>
<tr>
<td>1010</td>
<td>2010</td>
<td>3010</td>
<td>1110</td>
<td>2011</td>
<td>3011</td>
<td>4011</td>
<td></td>
<td>1111</td>
<td>2020</td>
<td>3021</td>
<td>4021</td>
</tr>
<tr>
<td>2110</td>
<td>3110</td>
<td>4221</td>
<td></td>
<td>2111</td>
<td>3121</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2121</td>
</tr>
</tbody>
</table>

This way gives too large an array of scenarios (about 100) for perception; so an additional analysis was made and a reduced set of main scenarios elaborated that is useful in general for compromise solution of the following two tasks:

1. The creation a "textbook" for BDBA studying by operators on the basis of groops of scenarios, each of which unifies the essentially similar BDBAs and lead to the same or different but linked consequences. Each group gives timing, limit points of sequence branching and requirements to effective information for BDBA identification and possible management actions assessment.

2. The set of scenarios that is visible enough for on-line operational consideration - on the basis of the first main expected symptoms of possible accident transition from the DBA to the BDBA field, with universal and specific measures for prevention, mitigation, identification and guide gaps filling, if it is necessary in accordance with additional real information.

For such reducing it is unified scenarios that may be considered as consequent stages of one scenario (moreover the last stages may be absent under some conditions):

For example, the scenario "The loss of flowrate in one fuel channel" has two stages: 1. Fuel assembly overheating/damage, FP release and pressure tube heating/deformation without or before PT-rupture; 2. PT-rupture, coolant discharge, reactor cavity pressure rise, reactor scram with some delay, FP release, reactor cooling.

The different BDBA with channel dewatering and steam superheating (as blackout; some ATWS, RIA, partial DGH break or PH break with ECCS initiation delay) consist of one, two or three stages:

1. FA overheating and failure;
2. PT overheating and failure;
3. RC disintegration.

The last stage may approximately be considered as independent from the way it appeared.

The external events (earthquake, airplane crush) and some internal events (such as hydrogen explosion, large LOCA - for the first generation units) are considered as common cause for additional failures that lead to the transition of DBA into BDBA.

Also the BDBAs with confinement failures are considered as more severe version of similar BDBA without confinement failure.

As a result of such a reduction the brief scenarios set contains 14 BDBAs including

9 BDBAs under reactor power condition:
- ATWS in a critical on line reactor with quick accident development after the total or partial loss of main heat removal functions (loss of coolant flowrate in one channel, in one DGH or in one coolant loop; loss of feed water; loss of steam
- 4 -
removal;  loss of electrical power supply);
-3 RIA under local or total overcritical conditions with the reactivity less or more than beta;

5 BDBAs after reactor scram:
- "blackout";
- loss of circulation as a result of water flash or steam carry under;
-3 LOCAs: 1) near critical DGH partial breaks (with steam stagnation); 2) large PH break with immediate DGH CVs closing and ECCS delay (water blowdown); 3) cooling loop and channel slow dewatering with weak steam back flow.

It is reasonable to consider as a separate scenario the third stage of some BDBAs mentioned above with potential possibility of RC damage and quick graphite oxidation opportunity.

The BDBAs during on line fuel reloading and BDBAs in spent fuel storage differ essentially from the reactor BDBAs and are not examined here.

We do not consider the modern computer possibilities for information of operators and technical teams, for analyses and for giving advice regarding management actions. These possibilities are object of the special papers [1,2,3].

11. SOME PROBLEMS EXISTING NOWADAYS.

1. There are some essential points to be concentrated on later in the area discussed:

1.1 The combination of strictly regulated SOI steps with sufficiently broad and deep understanding/feeling of BDBA phenomena in order to provide on line on principle permitted "corrections" of recommendations given by guides under new circumstances (so called filling of inevitable gaps of guides).

Probably this contradiction may be mitigated by means of separate training of operators and of special technical team for BDBA analysis;

BDBA-oriented SOI and a special "textbook" for the study of BDBAs and similar cases by operators and members of technical teams, so that they had more reasons to make concrete decisions, developed the decisions given in the guides if the real conditions differ from guide/ SOI conditions.

1.2. The subdivision of great number of BDBAs in a small visible number of suitable BDBA groups with different main symptoms, severity scale and types of management strategy; The elaboration of "universal" general (or small number basic) strategy with necessary branching: number of specific action modes for different diagnostic data sets or on line appearance of essential new information.

Now it is still early to make certain conclusion in regard to the most useful method of BDBA classification and study: it is reasonable to continue the work in this direction.

1.3 The early choice of management strategy under conditions of insufficient diagnostic data (e.g at LOCA events) or other uncertainties, adhering to the principle "do not harm" taking into account the narrow range of wittingly permissible actions;
1.4 Elaboration/implementation of the most important and
effective additional diagnostic/protection measures available.

Evidently the two previous tasks are interconnected; maybe
they are the main problems of the RBMK BDBA management.

Channel reactors, especially of the RBMK-type, have rather
many slowly developing BDBAs (as a result of high heat capacity)
and a lot of possibilities (as parallel lines, reserve systems,
control valves, check valves etc) for restricting identified
DBAs/BDBAs. For the LOCA management it is important to know the
accident circuit, break place/topology (inside/outside the
confinement, before/after CV, lower/higher core) and leakage
scale (more/less than ECCS capacity).

If BDBA is not identified correctly the choice of management
strategy may be not optimal. So, it is always reasonable to stop
fuel fission, to transfer reactor to subcritical condition and
to keep water in the cooling loop, in steam drum.

But sometimes the following points are not quite clear:
- the kind and place of leakage (see above);
- the accident cooling loop (left or right);
- the accident DGH and CV; the danger of stagnation and the
effective measures that break the stagnation;
- the degree of loop steaming and circulation loss after an
accidental pressure drop or steam carry under; the control of
circulation restoration;
- should operators decrease the steam pressure to provide the
integrity of accident heating "dry" channels and use the
independent source of low head water in spite of the saturated
water flashing, decreasing water inventory and mitigation of
cooling by back flowrate;
- how can the restoration of cooling water delivery in the
overheated core part be controlled to avoid the "waterhammer"
and "thermoshock".

2. There are some specific for operating RBMK problems connceted
with RBMK deficiencies; They should be taken into account
while considering operator aids. These deficiencies include:
- positive void reactivity effect (to exclude some severe ATWS
it is necessary to provide a very reliable reactor scram; this
is quite possible in channel type reactors that have much
convenient space for CPS channels with low pressure and
temperature conditions);
- channels' damage possibility as a result of their improbable
overheating at blockage conditions or some LOCAs and ECCS or
special check-valves additional failures;
- necessity to protect reactor cavity from pressure > 0.2 MPa;
- main safety valves capacity is less than reactor nominal
steam generation rate;
- a confinement system has relatively large leakage area under
condition of high "hydroseal" of steam condensation pool; the
confinement is absent at the top part of MCC; the first RBMK
generation have not a tight confinement;
- the management strategy at LOCA's depends on leakage scale
and location, but information for diagnostic is very limited.
All these deficiencies are not the inherent features of chan-
nel graphite reactors and will be eliminated in the new reactors of this type. Even for operated RBMK the most of them are partly eliminating rather easy; As a result of this upgrading the BDBA-management will be simplified.

111. CONCLUSIONS.

It seems reasonable to elaborate/implement the following:
1. Adequate and suitable BDBA classification and phenomenology description specially oriented towards operator aid for choice and branching of management strategy, taking into account the possibility of guide "gaps filling" based on broad understanding and feeling of BDBA processes; It is also useful (for more deep study) to elaborate the "textbook" of the phenomenology of the key DBA/BDBA processes and BDBA symptoms development;
2. A small number of basic management strategy with number of specific action modes for different diagnostic data sets;
3. Simple evaluations and suitable presentation of non measured parameters important for BDBA diagnostic: and management (as leakage location, scale and assessment of possibility to compensate the coolant inventory, based on the available balance of steam/water flowrates and level change, etc);
4. Additional most effective diagnostic/mitigation means available for upgrading; In particular for RBMK:
   a) some additional scram and ECCS initiating signals and LOCAs diagnostic data that can be based on reservation/variety of pressure measures in SD, RC, containment and turbine apartments; measuring pressure differences between SH and SD, DGH and SD; imbalance between the reactor and the turbines capacities;
   b) assessment of MCC water inventory, using the measure of SH-DS pressure drop;
   c) ECCS water flowrate distribution between the reactor cooling loops; The subcooling/superheating indication of outlet coolant- for ECCS flow optimization, to avoid steam condensation or superheating in SD;
   d) extraordinary SD-pressure decreasing or restricting up to cancelling of BRUK blockage and restoration of safety valves capacity;
   e) small completely independent low-power water source ("movable-type") for the compensation of MCC-water evaporation by residual heat.

REFERENCES
1. SD.Malink, V.V.Shalia, I.D.Rakitin, A.A.Tutnov. "Full Scope Simulator as a Tool for Development and Proof of Operator Aids for SA Management". SAMOA-2 meeting, Lyon, 8-10 sept., 1997
Appendix I

THE MAIN BDBA SCENARIOS

Taking into account the considered possibilities of reducing of the set of BDBA scenarios, we can briefly characterize the main BDBA groups of scenarios inside reactor:

1. BDBA under power conditions:
   Develope quickly (minutes or less from IE to essential consequences)
   The main tasks: assurance a scram, restriction of pressure rise, restoration of the water inventory, prevention FP spreading.

1.1 ATWS after loss of one of the main heat-extraction system; subscenarios:
   1.1.1 Loss of steam condensation (or 6kV AC supply) leads to quick pressure rise (till SV's steam discharge becomes equal to reactor steam generation),
   -to loss of feed water supply (when the pressure is above the max. feed pump head, 9MPa),
   -to MCP-trip and fuel overheating in 5-10 minutes; (Note: after 6kV AC loss, the MCPs and main FWPs stop immediately and fuel temperature rises at once).

   During these processes the "weak" part of MCC or some channels and RC can be ruptured, if the pressure does not drop enough.

   1.1.2 Loss of feed water leads to the similar scenarios way, as above, but without pressure rise and MCC rupture; The channels and RC can be ruptured, but later - after the strong reduction of MCC water inventory.

   1.1.3 Loss of MCPs; One cooling loop has as a rule 3 MCPs on line; One MCP trip does not lead to severe results; The loss of all 3 MCPs without loss of 6kV AC is very improbable accident and leads to somewhat less severe results than more probable loss of AC 6kV; So it is more important to consider the loss of two MCPs.

   The loss of two MCPs leads to rather strong coolant quality rise and to the possibility of strong channel flowrate oscillations, heat dryout crisis, fuel overheating and some cans' untightness; the channel ruptures are improbable.

   Symptom of ATWS - the scram is absent in spite of scram accident limits are achieved; Besides:

   In the case 1.1.1 - loss of condenser vacuum and closing of turbines' stop-valves; loss of AC 6kV; SD pressure rise in spite of SVs' opening; decreasing and loss of feed water and SD level; FPs' release in both loops; RC pressure rise above 0.2MPa;

   Later more severe consequences can take place.

   In the case 1.1.2 - the same as above but without SD pressure rise.

   In the case 1.1.3 - MCPs trip, FP release in SD of one loop.
1.2 "Quasi ATWS" - ATWS after DBAs with one or without failed automatic scram:

1.2.1 Loss of coolant flowrate in one channel without scram;

1st stage: fuel pins heating and rupture, FP release, PT overheating and creep; If PT is heated higher than 650 C, the 2d stage begins;

2d stage: PT rupture, RC pressure rise above scram limit (7.5 KPa), reactor is stopped; RC hydroseal is cleared (18 KPa) and steam-gas mixture with FP is removed in the condensation pool.

Initiation Event (IE): a) channel control valve (CCV) failure;

b) critical partial break (CPB) of channel's inlet feeder (IF);

Symptoms: Indicated flowrate drops (false channel flowmeter indications are possible), r/activity increase (channel activity meter requires a long time for indication);

On the 2d stage: pressure, temperature, wetness and activity rise in RC vessel and later - along the line for removing of steam-gas mixture from RC.

Accident Management (AM) actions: 1. To provide the scram during the 1st stage, before PT overheating;

2. To provide the readiness of ALS and the early SD pressure decreasing after reactor scram;

Note: 1. In the cases without scram after RC pressure rise or with large delay of PT rupture, the fuel rupture and FP release will be much more and fuel melting in one channel is possible.

2. In the case b (IE-CPB of IF) the part of FP release can enter through the IF break into the bottom room before the channel rupture.

1.2.2 The loss of flowrate from PH to one DGH without scram;

The coolant continue to come in this DGH only from ECCS header connected with PH; The coolant flowrate in the channels of this DGH decreases and outlet quality "x" increases many times, up to x=1 in average; Dryout crisis, fuel heating and failures appear; The steam superheating is possible and PT ruptures are not excluded in some channels. RC rupture is improbable.

IE: The DGH entry blockage by outside subjects; the passive bypass from PH to ECCS header and to DGH remains.

Symptoms: The flowrate decrease/loss in the channels of this DGH; r/activity increase in some channels (in outlet feeders) and in the SD.

AM: Enough early reactor scram or power decreasing to less than 50% (within minutes) stops development of BDBA.

1.2.3 The steam consumption decreasing by turbines without reactor scram because the pressure downstream RVs not achieves the trip point and because of failure of scram as a result of pressure rise upstream RVs; The QARS (BRUK) of condenser also fails.

The SD pressure rises till steam discharge through the opened SVs is equal to the steam generation in reactor; The feed water flow decreases to zero when the pressure is higher than the pump head. The MCC water inventory decreases, the circulation fails
and the opportunity of the PT ruptures appears; Some "weak" channel PTs can fail earlier;
IE: The grid frequency rises or pressure controller failes;
Symptoms: The SD pressure rise, in spite of SVs' oppening;
Partially closing of pressure control-regulation turbine valves (CRTV). Quick action pressure reduction set (BRUK) failes.
AM: The sufficiently early reactor scram or CRTV opening.

1.3 RIA:
1.3.1 Local overcritical conditions with LAR/LAZ failure, strong neutron field deformation.
The channels flowrates decrease, coolant quality rises, heat transfer crisis and fuel overheating can take place in the region of power "splash"; The channel overheating and rupture are possible if the channel power is large enough (3 times or more than normal); a RC rupture is improbable.
IE: a) CPS absorber selflifting with LAR/LAZ failure; (b) the attempt to restart of a reactor under conditions of a small operative reactivity margin (ORM).
Symptoms: Strong field deformation (>2 times), LAR/LAZ failure, channels flowrate decreasing near field maximum; RC pressure rise; absorber selflifting (IE a); neutron field instability (IE b).
AM: Reactor scram; AM for the case of channel rupture (see 1.2.1).

1.3.2 Reactor power rise for accident reactivity compensation
Reactivity of absorbers and voiding is compensated for by Dop- ler effect; heat transfer crisis, a fuel cans' heating and some failures occure if power rises rather strongly, at least two times; a steam pressure rises, the pressure control valves open (turbine/BRUK valves, SVs); MPTR is possible if power rise is essentially more than wo times. In long term - the influence of xenon and graphite temperature effects of reactivity.
IE: Self-lifting of CPS absorber group (reactivity < beta) with the "neutron scrams" failures.
Symptoms: Self-lifting of absorber group, rise of power and SD pressure without scram; SVs oppening.
AM: Reactor power reduction or scram.

1.3.3 The reactor self-acceleration at reactivity more than beta, as result of very quick dewatering of CPS channels without scram.
The scale of consequences is very large, although lesser than after Chernoble desease; The probability is very low because a scenario with sufficient quick insertion of reactivity by dewatering of CPS channels is not found, and additional failures of at least three redundancy scram signals transfered such accident in a very improbable region (can be neglected).

2. BDBAs after reactor scram:
2.1 The circulation disruption because of MCC steaming and ECCS initiation delay.
Strong oscillations of coolant flowrate, quality and sometimes
temperature rise appears; The fuel cans' failures are probable. The water blowdown is possible, the steam superheating and PT overheating are principally possible (but improbable) under strong pressure drop conditions.

IE: a) additional steam leakage (steam line rupture or SVs unclosing) or pressure controller (PC) failure leading to pressure drop and water flash in MCC;

b) feed water system failure (line rupture or level controller (LC) failure) leading to SD water level fall and steam carry under from SD into downcomer;

Symptoms: Case (a)-The strong SD pressure drop and level rise; symptoms of steam leakage and/or PC failure; Power increasing or adsorbers insertion;

Case (b)-The SD water level falls; The symptoms of feed water loss or LR failure.

In both cases-the MCP water subcooling falls to zero; the MCPs trip. The r/activity rise in both loops (a) or in one loop (b).

AM: The ECCS initiation for both loops (a) or for one loop (b); The SD pressure and water level restoration.

2.2 The long term loss of 6kV AC supply and DG failure ("blackout").

IE: External event (earthquake or airplane crash and so on) leading to loss of 6kV AC and DGs.

Symptoms: Loss of 6kV, DGs failure, the main pumps switch off (MCPs, FWPs, condenser cooling water pumps), the emergency pumps do not switch on, loss of SD water level.

Development: MCC water evaporates by residual heat; natural circulation and bubble cooling disrupt, as the water inventory gradually falls; the dry part of the core is overheated and damaged from top to bottom in 1-2 hours; In 5-10 hours occur the Zr oxidation by steam occurs, the H2 releases, the fuel liguation and replacement to bottom part take place etc. The main part of IRG and VFPs releases. The channels and RC can break if the SD pressure does not decreases essentially.

MA: The sufficient early restoration of small water supply from any source to compensate for water evaporation. The SD pressure decreasing to prevent the channels and RC rupture.

2.3 LOCAs with ECCS and/or DGH CV failure or delay.

The main symptoms: A pressure in MCC rooms increase above the scram limit; SD water level decrease.

The main AM actions: Check and providing of the automatic actions; Assessment of leakage characteristics: area, MCC part, upstream or downstream DGH CVs and MCPs; Assessment of the danger of stagnation; Rupture isolation; PTs integrity defense.

2.3.1 Uncompensated MCC leakage below core leading to loss of water in some DGH as a result of ECCS or DGH CV failures or DGH leakage under conditions of unclosing valves of one MCP.

IE and development: Leakage flow below the core level is more than the water flow from ECC pumps under conditions of strong untightness of valves of one MCP; Leakage can be
downstream DGH CV or upstream DGH CVs (latter - if CV is not closed). The channels of accident DGH (DGH with leakage or unclosed CV) are cooled by weak steam back flow and in cross direction - to graphite and other cooled channels, including independant CPS channels. Fuel cans overheating leads to their deformation (ballooning) and ruptures, and to PT rupture at the case of sufficient high SD pressure and improbably - to danger for RC integrity.

Under conditions of tight closed MCPs valves, the steam backflow is essentially more effective. However, at low SD pressure, it is also small, and is reasonable to check the cooling during this stage of such an accident. The channels superheating above the decreasing water level is important also during slow dewatering accident DGH channels. These cases are subsenarios of scenario 2.3.1.

Symptoms: Pressure rise in MCC-rooms; water level drop in SD of accident loop; flowrate decreasing in channels only of ADGH (till MPC trip).

2.3.2 Large LOCA on the MCC head part upstream DGH CVs (that leads at once to dropping the PH pressure below SD pressure and to closing the DGH CVs) and delay of ECCS water supply.

IE and development: The inlet water flow stops immediately in the channels of an accident cooling loop(CL); during a few seconds the channel water is carried out by steam into outlet lines and SDs, heat flux from fuel pins drops practically to zero and in few seconds the fuel cans achieve the level of initial average fuel pins temperature. This leads to the possibility of cans collapse and small leaks near the places where fuel pellets are absent.

The channel PTs are heated quickly up to surrounding graphite temperature and than they are heated slowly because of big graphite heat capacity. Zr oxidation accelerates these processes; ECCS water blockades them.

The PTs rupture and hazard for RC integrity are not excluded if delay of ECCS water supply is sufficient long. Fortunately the SD pressure drops also quick: such the minimum LOCA (~20% of full CL cross section) leads to pressure drop below 2 MPa within shorter than ten minutes; so the PT ruptures (and all the more so - RC break) are improbable.

SYMPTOMS: The dropping below zero of pressure difference between PH and SD; The fall of the flowrate indications in channels of accident CL; a MCPs trip, a ECCS delay.

2.3.3 Almost critical DGH partial break with DGH pressure dropped to the level near the SD pressure at the moment:

a) before removing heat accumulated in fuel, or
b) after removing accumulated heat; or
c) after MCPs trip/run off.

IE and DFVFLOPMENT: The quick coolant flowrate brake, water blowdown and stagnation of coolant; fuel cans heating during the period when DGH-SD pressure difference is very small; The back pressure drop and back coolant flow appear during farther
decreasing of DGH pressure; so, the fuel and channels temperatures decrease. The earlier stagnation begins— the quicker heating and earlier back flow appear. Fuel and sometimes channels failures are possible, RC failure is improbable.

**SIMPTOMS:** MCC rooms pressure rise, channels flowrates decrease (only in accident DGH before MCPs stop); activity rise in accident DGH channels and in SD.

**AM:** Destroy the stagnation by changing of "boundary condition": ECCS initiation and flowrate variation; feed water supply decreasing etc. The stagnation control will be possible by indication of pressure drop between DGH and SD.

**2.4 The last improbable stage of some BDBAs with MPTR leading to RC-vessel disintegrity.**

It is difficult for quantity assessment. We can anticipate in majority cases only rather slow and small lifting of upper reactor shielding plate untill RC-vessel is ruptured and RC pressure decreases.

The behavior of fuel channels and CPS absorbers and the rate of graphite oxidation are important questions.

The likelihood of MPRT leading to RC desintegrity should and can be made negligible small.
Appendix 2

ON GENERAL MANAGEMENT STRATEGY AND DIAGNOSTIC OF LOCAS

In spite of great diversity of LOCAs conditions, in majority cases the definite general AM strategy exists, directed to:

1. The check up and providing of automatic actions (scram, ECCS, pressure and level controllers, accident localization system (ALS) isolation etc);
2. Rupture and leakage identification (rough and then more exact); the assessment of the important leakage characteristics (region, scale, coolant stagnation/superheating dangerous etc);
3. The realization of according measures:
   - urgent (stagnation breake, ALS isolation, SD pressure restricton);
   - medium/long term (additional accident cooling loop (ACL) feeding, the isolation of ruptured ACL part, the defense of electrical equipment against steaming, the restoration of water store, providing of long term cooling and subcritical conditions etc).
4. More detail assessment of the medium/long term dangerous for the integrity of the fuel cans, circuits, and especially -of channels and RC, and realization of the necessary actions.

It is always reasonable:
- to shut down the reactor;
- to transfer reactor to deep subcritical conditions;
- to keep a normal water level in main circulation circuit (MCC)
- to isolate the confinement.

However some leakage features influence the choice of specific AM actions, especially the following that are not quite clear sometimes because of diagnostic data limit:
- a type of a circuit:
  - CPS, cooling loop (CL), steam lines, feed water lines or MCC;
  - an area (region):
    - left or right CL;
    - inside rooms with sensors (pressure, r/activity, acoustic);
    - in the head part of circuit upstream or downstream CVs or flowmeters; or upstream of MCPs, etc;
  - can the leakage be isolated or not; can the "usefull" part of discharge (through the core) be increased:
    - a leakage scale:
      - the leakage compensated by auto-controllers (power, pressure, level);
      - the leakage is so small that the room pressure sensors do not achieve the scram limits;
      - the leakage compensated by ECCS pumps;
      - the leakage not compensated;
      - the leakage upstream DGH CVs is more than MCPs capacity, (i.e. it leads to immediate closing CVs) or not;

Identification of such features is important for the AM choice.

For example: Because of coolant stagnation possibility in the case of so called Distributing Groop Header's (DGH) Critical Partial Break (CPB), it is very important to distinguish between MCC breaks upstream and downstream DGH CVs. This is possible till MCPs do not stop because the channel flowmeters can not indicate the under natural circulation (NC) or ECCS conditions.
"Critical" unclosing of one CV can also lead to coolant stagnation in the case of MCC break upstream CV.

The indication of small pressure drop (+/-0.01MPa) between DGH and SD provides: i) the most direct symptom of danger coolant stagnation, ii) the instrument for solution of both these problems (DGH’s CPB or CV’s unclosing) and iii) the control of management effectiveness for stagnation destroy by the periodic change of ECC water flowrate or by other measures.

The main initial symptom of sufficient large MCC LOCA is the MCC rooms pressure rise and reactor scram. The ECCS initiation is an additional symptom of ruptured CL. As mentioned above, it is important to record the fall of flowrate only in one DGH till MCP does not stop.

So, it can be distinguished between the sufficient large leakages in the SD room, in confinement appartments, in MCC upstream or downstream DGH CVs.

If the pressure in DGH or SD room is rising, but ECCS is not initiated, we can determine an accident CL (ACL) due to SD level dropping (at large power level) and/or due to large difference between the feed water delivery in ACL and an intact loop. The essential change in MCPs flowrate and current load of motors can also be used as symptoms of the place and scale of a leakage. But these means give a large uncertainties, require a lot of operator’s time and must be supported by simple and reliable on-line calculations.

As a rule we can believe that operators have time to analyze a situation if scram and ECCS initiation signals are absent.

However, sometimes the delay of management actions makes the situation worse. So a leakage not leading to scram limit or a leakage compensated (masked) by controllers can not be a little:

The coolant leakage up to 300-500kg/s from MCC to SD room can not rise the room pressure above the scram limit (200 KPa) because of steam-air release into reactor hall and hot (250 C) air cooling by "cold" saturated steam (100 C at 1 atm).

An other example - the steam leakage compensated by pressure controller leads to decreasing of turbine power and water inventories in feed water tanks. So, a scram will occur only after strongly decreasing of the feedwater store and flowrate.

Analyses and identification of such masked situations (on the basis of indirect symptoms) and the choice of proper AM-actions are the tasks of the next stages of a general strategy.

In particular it may be available (by measuring or on line simple calculations) the following additional indications with corresponding signals:

- difference between each DGH flow and average one (till MCPs are on line) - for early scram and ECCS initiation;
- pressure drop between each DGH and SD - for stagnation control;
- pressure drop between SH and SD - for MCC voiding control;
- pressure drop between PH and SD - for CVs state and back flow assessment;
- difference between feed water flow in left and right CLs;
- difference between steam generation and consumption - for revealing of "small" steam leakage - below regulator capacity;
- subcooling/superheating of outlet coolant - for ECCS flow optimization (to avoid steam condensation or superheating in SD)
SYSTEM OF DYNAMIC BARRIERS (SDB) PREVENTING THE DEVELOPMENT OF EMERGENCY TRANSIENTS AT NUCLEAR POWER PLANTS AS A TOOL FOR OPERATORS' AID

I.D. Rakitin, Chief of Lab., S.D. Malkin, Head of Dpt.

RRC Kurchatov Institute
1, Kurchatov Sq. Moscow, 123182, RUSSIA
<Igor_Rakitin@odomrn.imp.kiae.ru>

A.S. Stebenev, Chief Instructor, M.M. Khoudiakov, Head of Training Center,

Leningrad NPP,
Sosnovy Bor , 188537,
Leningrad Region, RUSSIA

ABSTRACT

Work justification: a need in an unambiguous and illustrative methodology of Nuclear Power Plant (NPP) safety control for practicable use by professionals.

Work aims and objectives: development of a unified professional language for all the NPPs to identify power unit status, the NPP operation violations and corrective actions, as well as NPP emergency status control algorithms' optimization (or symptom oriented emergency actions - SORA).

Results to be reached: optimization of all the areas of the NPP safety-related activities from normal up to severe accident states.

In accordance with the proposed System of Dynamic Barriers (SDB) all the activities aimed at the safe and reliable operations are integrated into a single structure. It is supposed that the required level of the equipment, personnel and procedure quality has been reached, and the appropriate surveillance for revealing and eliminating latent weaknesses is executed. All initial events (failures) are initiated by the loss of "NORMAL" function by any quality component. This moment is considered to be the beginning of the transient progress, and the transient itself is looked upon as a consequence of the seven main types of the power unit's conditions ("states"): from "normal" to "severe accident". The unit's "states" are prescribed and determined in accordance with the IAEA recommendations on the INES (International Nuclear Event Scale).

The SDB key terms are: "POWER UNIT CONDITIONS or STATES" and "BARRIERS" - borders between the given conditions, impeding the transition from a less "serious" condition to the "severe" one. The condition transitions are caused by the barrier violations.

In a case of any barrier failure it is necessary not only to analyze the causes of each of three quality component failures ("equipment", "personnel", "auxiliary communication means or implements"), but also to reveal the component non-used resources for each barrier strengthening. Thus, beginning with the design phase and up to an operation stage, it is possible to provide an optimal dynamic barrier structure and personnel working conditions in order to increase the safety level and human factor reliability.

1. INTRODUCTION
The main reason to work out and implement the SDB methodology is the necessity to obtain a complex approach to the safety control and regulation of NPP which could become commonly used as for all the Plants' types as well as for the experts and specialists in R&D, Project design, and operation.

That's why, the proposed methodology is based on generally accepted terms, principles and approaches that guarantee reliability and safety of NPP 1,2 in accordance with the IAEA recommendations and the International Nuclear Event Scale (INES). Also unambiguous and simple gradation of types of power generating units (PU) state (conditions) is done. Methodology is rather universal and unified, since all types of the possible PU states, all kinds of safety activity and all components guaranteeing the safety related quality are considered within.

The goals of the methodology elaboration are:

- to create a specialists' common language and a base set of definitions for all types of NPP, which should provide identification of PU states and disturbances in NPP work, operation and troubleshooting activity, and

- to optimize an approach for a system of dynamic barriers as a base for Operators' Aids development and operation.

In accordance with the proposed System of Dynamic Barriers (SDB) methodology all the activities aimed at the NPP safe and reliable operation are integrated into a single structure. It is supposed that at the given NPP, in accordance with the Quality Assurance Program, the required level of the equipment, personnel and procedure quality has been reached, and the appropriate surveillance for revealing and eliminating latent weaknesses is permanently executed. To perfect the normative, other NPPs' good practice and their own operation experience are used.

SDB is presented as a scheme in Figure 1. The concepts and their internal correlation are united in a natural way in the scheme. Progress of an accident is shown as the unit's sequential transition from one state to another.

The key terms of the methodology are "types of states" (or "states") and "dynamic barriers" (or "barriers").

Remark. The proposed "dynamic barriers" shouldn't be mixed up with the common used "physical barriers" - as the protective radiation activity limits (e.g., within the fuel, within the vessel, within the containment, etc.).

As a base of the states' classification the determined under project design transient of a unit, from a small deviation (anomaly) and down to severe accident, was
chosen. The states were chosen from the point of view of a safe control of NPP.

It can be said, that a dynamic model of the accident's progress and its propagation, schemed at Fig. 1, presents a transitional regime of a PU as a consecutive change of the unit's states. It is worth remembering too that "small and negligible" problems and/or troubles during the NPP exploitation are potential accidents.

Taking into account a probability of the accident's further progress, some small problems can reach the area of foreseen or not foreseen by the design project accidents and even severe ones as a result of a failure of the three quality guaranteeing components:

1) - equipment,
2) - staff (personnel), and
3) - man-machine auxiliary interface devices and implements.

Indeed, according to the research 2, "the probability of an operator's error during the first few minutes of an incident is close to 1, but after 40 minutes it is equal to $10^{-4}$. Since the first "small" problems and troubles during an undesirable propagation of a transient and/or incident are to be of utmost controlled and persistently supervised by operators from the very beginning and up to the severe consequences ones. In this connection let us recall that a common practice of so-called Symptom Oriented Emergency Actions (SOEA) or operating procedures is being engaged just only after the 5th barrier is crossed.3

It is hardly to make anybody be free of an apprehension that moment of the 5th barrier's violation could be too late for the success.

Thus, it is necessary to have "on operators' hands" a permanent and unified system of the unit's states and barriers' definition that should block a transient progress of an incident or accident from the very beginning and with the main goal to increase reliability of the human factor's barrier.

Naturally, there is a direct connection between the number of such accidents at NPP and the reliability of equipment, the qualification of staff and the adequacy of man-machine interface implements.

In other words, the number of such accidents at the NPP is a measure of its reliability and safety level. The final goal of any significant safety related activity is to execute any concrete contribution to make stronger the appropriate dynamic barrier that was week and violated.

Therefore, SDB presents a high-level structure with an unambiguously defined niche ("place, time and space point") for every kind of reliability and safety
related control and regulation. The main consideration in the methodology is focused on:
- functional activity of the operators when and under the progress of the incident/accident transient,
- support of the operators in order to organise a safe control of NPP,
- analysis and identification of disturbances at the NPP work and troubleshooting activity.

II. SDB DESCRIPTION AND EXAMPLES OF ITS APPLICATION

All kinds of the activity oriented for safe and reliable operation of NPP are united in a common permanent structure as shown in Fig. 1. It is supposed that a needed level of all the three quality assurance components (equipment, staff and auxiliary technique of a man-machine interface) is guaranteed. 

A discussionable note: The proposed here term "Man-machine auxiliary communication interface means and implements", in our opinion, is more comprehensive than the recommended by IAEA term "Procedures", as it includes all the means necessary and sufficient for the operator's reliable and safe operation of the power units (from the information display system, support system, diagrams, instructions, procedures, communications, hardware algorithms and up to the language of communication). This term or about the same term "auxiliary technique of human-machine interface" better describes the gist of the problem as a technique that allows for an operator to carry out safe and reliable control of PU. It is advisable to use shorter and more adequate term - "implement" while analysing the operators' activity.

As internal and external expert examination of NPP's activity as well as a supervision of an operation should be carried out in order to reveal "latent" shortcomings of components that guarantee its quality, namely, (a) equipment, (b) personnel, and (c) implements. As a result of the expert examination of NPP's activity certain corrections should be made and quality standards, instructions and procedures for equipment, staff and implements should be improved. To improve standards the "good practice" of other NPP can also be used.

The start of the safety violating transitional process in terms of SDB is initialised by a failure of any quality component (when the 1-st barrier is crossed). The moment of its initialisation is regarded to be the beginning of an undesirable transitional process and the transient itself is considered to be the sequence of the state (condition) changes.

The basis of the unit's states' classification is a sequence of states during the progress of the negative
safety violating transient from some initial failure of a quality component and down to severe accident. The numbers of the states are:
- #1 - no failure;
- #2 - failure (incident) which doesn't lead to power decrease;
- #3 - failure (incident) leading to power decrease;
- #4 - failure (incident) leading to engaging the safety protection systems;
- #5 - failure with breaching of critical safety criterion (accident state);
- #6 - accident with partly damaged core;
- #7 - severe accident with serious damage of core and environment impact.

So called "Intermediate safe" states that correspond to the states listed above are supplied with index "S" (refer to Fig. 1). Accordingly the initial incident events that are not foreseen by the design project, are transferred right away to the "Accident state", type "S", because of defence safety systems were not counted by design to prevent them (as by definition).
The Figure 1 is divided into three vertical parts that include the following information about:
- "negative" PU states (# 2-7);
- "intermediate safe" types of the states (or the goal states, which PU should be transferred to after the corresponding negative ones are appeared);
- achieving goals, # 2.S-7.S;
- ways to achieve goals (technical and organisational matters).

As it was mentioned above, the key terms of SDB are the types of PU states and the dynamic barriers.
The term "state" operationally means a minimum quantity of information that concerns and describes a deviation of limits and conditions of the normal ("safe") operation to guarantee a definite identification of the current PU state as one of the given seven state's types.
The term "barriers" means correspondingly the conditional borders between the PU states that prevent a negative transitional process from its undesirable development by means of a purposeful conversion of the negative PU states into the corresponding "safe" ones. To be more precise, the term "barrier" represents the complex of technical and organisational actions with the optimum contribution in the barrier reliability by each of the three quality components, namely: "equipment" (E), "personnel" (P), and "auxiliary technique of man-machine interface implements" (I).
Every barrier has the number (1-7) corresponding to the given PU state that should be transferred to a safe one. If any negative process begins, automatic and/or manual actions that are provided by the corresponding barrier should be undertaken.
The crossing of any barrier represents an incident or significant accident at the NPP that requires the correcting steps as well as elucidation of the direct and root causes of the accident.

If any barrier is crossed (corresponding with a failure of a quality component) the analysis of its causes should be undertaken together with a careful investigation of not used (missed) possibilities of the quality components for the purpose of making the crossed barriers stronger.

To guarantee the safe control of the NPP, operator must timely identify the PU state and undertake adequate steps in order to transfer the state of the PU to the more safe one, (so called "control by the state").

A particular (but very important) case of the "control by the state" is the use of the SOEA procedures or of a system to identify one of the cases "4.S" or "5" after the sanctioned engaging of protective safety systems (so called "scram"). 2,5

So, the operator’s support system should be firstly focused as to help him to identify definitely all the PU states mostly for the safety violating transients. Other words, the scheme shown at Figure 1 appears to be a high-level generalised videograph of any operator’s support system. This videograph allows to watch, supervise and control the progress of the negative transients in a dynamics’ form of the safety important states, and could be successfully used by the administrative staff, operators and specialists of Crisis Centers.

SDB methodology is the theory base for a development and adjusting of the Generalised Operator Support System (GOSS) which is under implementation at the Leningrad NPP 6. The GOSS prototype is installed as an additional workstation at the Full Scope Simulator of the LNPP. 7 It is operating now with a networking and "real time" Data feedback from the Simulator' computers. The first results of this R&D work are very positive and could allow to implement the System onto the real Unit's Control Room after the whole set of test and adjustment procedures.

The formal notation and classification of correcting actions and failures of the three quality components maintain with two indexes:
- one is the barrier’s number to be strengthened (or the one which was crossed),
- and the other is the component’s number that makes the crossed barrier stronger (or the one which failure led to crossing the barrier).

Example 1. The correcting action "5.P" means that the purpose (goal) of the action is the strengthening of the 5th barrier by means of training the personnel how to act when the 5th state happens (the "accident state").
Example 2: The installation at the Leningrad NPP Units (RBMK-1000 type) of the Emergency Reactor Subcooling System (ERSS) is identified with two symbols <4.E>, since the 4th barrier was made stronger for the "equipment" component.

Example 3: The crossed barrier coding "3.P" means the crossing of the 3rd barrier because of a failure of the "personnel" quality component.

Formal identification coding of incidents and/or accidents at the NPP consists of a sequence of the crossed barriers including failure components and the final state's type.

Example 4. The failure of the level's regulator in the drum separator at the RBMK-type reactor caused a deviation of the level above the appropriate "level set-point" and led to engaging the preventive automatics control for power decrease from normal 100% down to 60%.

Analysis and identification:

The coding of a regulator failure (under the SDB sense) is "1.I" because the 1st barrier was crossed at the "I" component ("auxiliary technique of interface implements"). It is very important to note the SDB selection of the "Implements" component but not the "Equipment" component as it were be under the common used IAEA identification. Indeed, according to the proposed SDB methodology all transient processes are classified from the "safe operational control of NPP" point of view. Under the given point of view it is clear the failure of "implements for operator in a technological process control" had happened in reality.

Unsatisfactory attempts of the operators to compensate the incident disturbance in the drum-separator's level led to crossing of the 2nd barrier that means the failure "2.P". The 3rd barrier fulfilled its safety function duty and transferred the PU from the state # 3 to the "intermediate safe" state "3.S" by decreasing the power level down to 60%. So, the incident code description is represented as follows:

100% - 1.I - 2.P - 60% - 3.S, where:

100% - the initial power level before the incident,
"3.S" - PU state after the incident,
60% - the final power level.

Complex databases of the NPP (RBMK-type) incidents and barriers' crosses are compiled now under the described above basis at the Leningrad NPP in order to undertake a comparative analysis of the dynamic barriers and correcting actions. It should be done for each type of NPPs.
The top priority steps of any action, modernisation, upgrade, etc. at the given NPP are those that exclude (or lessen the probability of) such the failures that lead to crossing (violation) of several barriers at the same time when there is no possibility to strengthen the crossed barriers with the help of other quality components.

The SDB as a complex systematic approach should guarantee the reliable and safe control of PU, so the ultimate goal would be that SDB and PU to be designed at the same Project time. Under that Project Design jointly with the PU itself the SDB approach should provide with the reasonable barriers and with an optimum contribution of each quality component in each barrier. Databases of incidents at different NPPs are to be used for those purposes. Thus, the optimum structure of dynamic barriers and high-reliability of a staff activity can be guaranteed during the project design process.

SDB for an operating Power Unit is supposed to be further continuously and permanently developed because of each kind of activity represents the root for more detailed steps in a personnel activity.

III. CONCLUSION

The SDB as proposed and proved at the Leningrad NPP methodology for organisation and regulation of important safety related activity can be used:
- for improvement of algorithms to realise the preventive control and emergency regulation of the main technological process;
- as a common algorithmic language which can help specialists to elaborate certain kinds of activity to improve safety and reliability of NPP;
- for analysis and formal estimation of incidents at NPP and for compilation of databases consisting of crossed barriers’ cases and quality components’ failures;
- for development and organisation of universal operator support systems;
- for comparative analysis of certain SDB for reactors of different kinds;
- for working out the simulator training scenarios with various combinations of incidents and failures of different quality components;
- to acquaint the personnel of NPP with the concept of "control by the state" as well as to teach to understand the problem of safe and reliable operation of NPP.

REFERENCES


ACKNOWLEDGMENT

Both the development and implementation of the methodology were greatly contributed by the RRC "Kurchatov Institute" administration and scientists, and were financially supported by the LNPP.

The significant personal contribution to the given R&D work and SDB methodology implementation at the Leningrad NPP are made by:
- the Leningrad NPP work's initiator and former General Manager A.Yeperin, LNPP General Manager V.Lebedev, LNPP specialists and experts V.Moskovsky, A.Zinchenko, and many others.

Authors would kindly acknowledge the sponsorship of the OECD/NEA Administration for the Paper presentation at this SAMOA-2 Specialists Meeting.
Fig. 1  System of dynamic barriers (SDB) preventing propagation of emergency transients on NPPs
BASE PRINCIPLES AND APPROACH AT DESIGN OF GENERALIZED OPERATOR SUPPORT SYSTEM (GOSS)

I.D. Rakitin, Chief of Lab., S.D. Malkin, Head of Dpt.

RRC "Kurchatov Institute"
1, Kurchatov Sq.
Moscow, 123182, RUSSIA
<Igor_Rakitin@odumm.imp.kiae.ru>

A.S. Stebenev, Chief Instructor, M.M. Khoudiakov, Head of Training Center,

Leningrad NPP
Sosnovy Bor, 188537 Leningrad Region RUSSIA

ABSTRACT

The Paper describes an approach, development, implementation and testing of the System's prototype at the Leningrad NPP Full Scope Simulator before the System's installation at the reference unit's Control Room. The Simulator ensures the modeling of a wide range of accidents and transients and provides with special software and ETHERNET data process communication to the Operators' Support system's prototype.

The System has been developed jointly by RRC KI and LNPP team. The first priority goal of GOSS is to decrease of mistakes' probability and, especially, of "wrong decisions" of personnel under NPP operation.

Founding for GOSS development is mostly a lack of an "Information Display System" (IDS) at the working places of so-called Supervising Operators of the RBMK unit.

The GOSS priorities are based upon a concept "System of Dynamics Barriers (SDB) to prevent a propagation of Accident Transients at the NPP" by the same authors. GOSS is oriented, at the first, toward a support of operators under "stress conditions" and is based on the hierarchical tree structure of display pictures with the root display picture "Safety Observation Screen" (SOS) where all the information needed for control of the main technology process and enough for a safety monitoring is to be displayed.

Features of the RBMK-type unit were put into consideration in a development of GOSS for the 3rd unit of the Leningrad NPP.

I. INTRODUCTION

In this R&D and project design work we are dealing with an improvement of Nuclear Power Plant (NPP) operators' tools, as the main way of "human factor" features increasing, mostly for the operating NPPs.

It is well known now that an improper operators' activity is the cause of about 50% of emergency situations, and that is why the MMI improvement has become even more important than the machinery technical improvements. 1.
According to the IAEA "ASSET" methodology \(^2\) and the NPP operation quality ensuring regulations \(^3\) the initial events of failure in NPP functioning are failures of (a) "Equipment", (b) "Staff" (or "Personnel") and (c) "Procedures", which are called as the "quality provision components".

**Important Note.** The term "MMT auxiliary means or implements" from our point of view explains the gist matter clearer, than "Procedures", since it includes and covers all the interaction means, used in the technological process control and supervising: starting with the information presentation system (including the operator's support systems), instructions, procedures, diagrams, communications, interactive language and ending with the automatics' algorithms and devices. However, it is not convenient to use it in all cases. And that is why we propose to use brief and more adequate notation for the operator's tools as "Implements".

As practice showed, the personnel erroneous decisions, which lead to the gravest consequences (TMI, Chernobyl NPP), are connected with imperfections of the Information Display Systems (IDS), namely:

(a) mostly of the unit conditions (or states) improper and wrong evaluation, and

(b) of the lack of the concise conception in the operation control organization (lack of so called "control by the state").

It should be emphasized that the both imperfection causes are connected with drawbacks of the same quality component - "Implements".

According to investigations, about 50\% errors of personnel, which were connected with incidents or accidents in NPP operation, were provoked by drawbacks of "Tools" (basically, of IDS). Unfortunately, for a number of reasons, the "Implements" for operators practically are not improved, in spite of their great role in the operators' reliable work providing. The reasons of personnel errors, connected with "Implements" imperfection are not revealed and all discussion is limited by a "personnel error" common notation.

The RBMK-type unit is operated by the team located at the Main Control Room (MCR) and consisted of the senior supervising operators as Plant Shift Supervisor (PSS) and/or Deputy Plant Shift Supervisor (DPSS) and of three executive operators as the Reactor Operator (RO to monitor and control core neutronics and thermal hydraulics, neutron flux and power distribution, reactivity, state of the Reactor Safety and Protection systems, reactor's heat and steam production, etc.), Unit Operator (UO to control balance-of-plant), and Turbine Operator (TO to control turbines, electrical
generators, electrical distribution and electrical devices, etc.)

In addition, there are Local Post Operators positioned at Local Control Rooms and Local Control Posts in different areas of the plant to control and supervise, e.g., Fuel Reloading Machine, Water Chemistry, Plant Electricity Dispatch Center, Reactor Main Circulation Circuit and Pumps, Turbine and Generators Central Hall, Radiation Monitoring and Environment Protection, etc.). These Local Post Operators are communicated with the MCR Operators.

So, the operation of the RBMK-type units is rather complicated and would require a set of measures, mostly to improve MMI and enhance safety features under normal, abnormal and accident modes in a view of the new RF and International Regulations and Recommendations.

Unfortunately, the PPC "SKALA" which is the main instrument to help for operators is rather obsolete as for hardware as well as for its software and Man Machine Interface (MMI) design of early 70-ies, and is under permanent up-grade and modernisation during last years. New tools, devises and systems for operators' support are under development, testing, and implementation.

E.g., a lack of the information display system at the MCR working places of the senior supervisor operators (PSS, and DPSS) is a serious obstacle to control the main technological process and provide timely measures for actions' insurance and support of executive operators under emergencies and accidents, especially severe ones.

More of that, significant efforts to up-grade RBMK Safety Design and implement a set of additional Safety Systems are provided by the Russian Project and Design Institutes and International Organisations and Communities. These measures and new designs should be tested, validated and verified with using any different possible vehicles - experiments, theory calculations, modelling and simulation.

The reasons for the GOSS development and working out especially for the Leningrad NPP are:
- the demand of Item 4.4.4 of the RF General Safety Rules 3 about the necessity of including in a structure of the IDS and safety protection and control of NPP unit "...a system of generalized information efficient presentation to Personnel about the current condition / state of the unit (reactor equipment, devices, facilities) and on NPP safety as a whole";

- the generally accepted conception about the necessity of operator "Implements" improvement as a first priority measure in "human factor" reliability increasing;

- the lack of the information display system at the RBMK Main Control Room for the working places of the senior supervisor operators (Plant Shift Supervisor - PSS, and Deputy Plant Shift Supervisor - DPSS). Such the system should be very important to provide an integrated control of the main technological process and timely measures for actions' insurance and support of executive operators;

- availability of the RBMK-type Full Scope Simulator at the Leningrad NPP with features and possibilities to provide any R&D work generally oriented at the MMT and operator "Implements" improvement and adjustment as a priority measure in "human factor" reliability increasing.

This R&D work's purposes are:

- creating of more perfect operator's Implements for increasing of the supervising control's quality and power unit's operation on the basic of new approaches to the matter, means and forms of the information presentation;

- working out an IDS content for working places of the shift supervisor operators (DPSS, PSS) for organization of an additional extra barrier for efficient control.

II MAIN PROPOSITIONS AND PRECONDITIONS FOR GOSS WORKING OUT AND DESIGN

Character of an operator's activity is enough wide and of a great variety: starting with routine checking and maintenance of machinery and ending with control of processes under conditions of stress and critical situations.

It is obvious, that user features of operator support systems (OSS) depend on which way and how these OSS are to take into account the character and the specificity of operator's activity to be supported with.

Accepted for the GOSS priorities of operator's support are determined from the conception "System of Dynamic Barriers (SDB)," (see Appendix II and the Paper of the same authors "System of Dynamic Barriers (SDB)"").
The SDB methodology allowed to solve such principal questions as:

- classification of types of power unit's conditions ("states");

- determination of the operator's and of the supporting system's main function as the proper power unit's "state" identification during the transient, incident, or accident;

- choosing with the optimal package of videogrammes (displays) for control of all types of power unit's conditions (states);

- choosing with the content and the optimal ways for the information presentation displaying, to be based on the condition's type, time of transient and character of tasks for the plant shift supervisor operator;

- determination of spheres for emergency procedures of different types (I, A, H1-4, U1-5 and others), worked out by International Communities.

The authors well understand the following statements could be seen as rather discussionable and arguable but it is necessary once more to point out and remember, that probability of an accident with a real violation of limits and conditions of the safe exploitation (of the critical parameters) represent not more than $10^{-4}$, so the operating personnel practically has no the urgent necessity to use separate specialized systems of safety parameters display (SPDS-type of any different kind).

It was noted not ones at many meetings and workshops on the operator's support systems (and authors may witness it to be based with their experience and interview with operators and administrators), that "psychologically the NPP personnel keeps on to consider the possibility of hypothetical emergency situations and severe accidents arising as incredible events and that is why they (operators) regard serving and monitoring of the special devices, which can only detect and alarm such "severe" situations, as rather useless work".

That is why for an operator's securing of the "interaction habit" with any additional display system it is necessary, that operator would use that given system constantly and permanently, both in the steady state ("normal") of power unit's work (during check-ups, maintenance of equipment, carrying out of the routine procedures), and in transition states and incidents, and in critical and emergency situations. It is well known, that a gun which is not used becomes "rusty".

Acquired habits of interaction with the support system would help operator to appraise the condition of a unit properly.
and take the right decision both in conditions of stress and during critical situations.

In other words, the operator support system should be universal and should be based with the same package of support display videogrammes for supporting all the types of an operator activity and under different conditions of power unit states.

This demand was taken into account on the development of GOSS for the Leningrad NPP provided a correspondence of supporting videogrammes (display pictures) as a hierarchical tree to different conditions of the reference 3rd unit. The GOSS methodology is elaborating now as a separate workstation mock-up facility network connected with the Full Scope Simulator of the 3rd unit and is adjusting under the operators demands and comments. After a validation and development it should be transferred to the real Control Room provided a connection with the Plant Process Computer System "SKALA".

A "Safety Observation Screen" (SOS), which is displayed permanently on the main monitor of a supervisor operator (DPSS), represents state conditions from the 1st (normal) to the 5th (emergency) one. That is, all deviations in the unit's work, important from the point of view of safety or reliability of the main technological process, are accompanied by generalized or individual signal image on SOS.

In a case of emergency conditions' arising, project - designed or severe accident ones (states or conditions' types ## 5,6,7), video screens are used to control and monitor conditions of critical safety functions. In a case of threat or clear violation of critical safety functions, the special program code of search any work- available protection channel for every safety protection system is foreseen and activated.

To make the skilled operators be interested with and to provide their direct participation in working out and adjusting of the support system is another important condition, determining the need and comfort of the system to be successfully created and implemented. Indeed, according to SDB principles, the main and the most difficult safety providing function of the responsible operator is the permanent supervising control of the power unit for the purpose of timely identification of unit's dangerous conditions, especially those demanding with reducing of the reactor's power, or the emergency shut down (scram), or the safety protective systems work activation.

Being determined in such a manner, the operator's main function is a "control on the unit's condition states" as the part of "symptom oriented emergency actions" (SOEA).
With these general principles in mind, it is reasonable, that a priority task for any supporting system should be an identification of unit's condition and displaying to an operator of information about quantity, quality and numbers of working in operation channels of safety protective system under all the condition states, with total failures as a result of common reason (fire, explosion, natural calamity and so on) to be included.

Multiple important and urgent demands are imposed on videogrammes' package - starting with an information content and structure and ending with comfort of perception and videogrammes' aesthetic design. To accomplish the goal a new approach have been used in the visual information technology with editing, filtration, generalization and suppression of information, which is irrelevant (inappropriate) in current moment.

Visualization information technology, including computer processing for its generalization, is presented in 4. The common demand for such videogrammes' schemes is they should represent the possibility of a "global view" on the controlled object, determination of its dangerous conditions and the most important control functions. Video display screens, meant for operative (prompt) operator's support response during rapid transients, under stress condition, are made on the basic of generalized schemes.

On the basic of SDB conception and worked out specifications the GOSS Prototype for the Leningrad NPP has been made (see Appendix I). Working out of this system the following features of power unit with RBMK-type reactor, were taken into account:

- availability of great number of indicators, displays, alarms, lights for different parameters (about 10,000), randomly settled on traditional stand-desks and control panels of the Mail Control Room (and, according to these circumstances, a great flow of non-organized information in transients, incidents and accidents);

- the necessity of the operative coordination of the three ordinary executive operators' actions by the supervising operators (DPSS, PSS);

- the lack of the project designed OSS on the plant shift supervisor operator's (DPSS, PSS) working places;

- the need of supervisory control and the check-up of the ordinary operators' action by the plant shift supervisor operator (DPSS, PSS).

III. STRUCTURE, CONTENTS AND WAYS OF THE INFORMATION PRESENTATION
The main phases of any information support display system design and creating are:

- putting together the common technology operation scheme and a harmonization of different parts of a power unit (equipment, automatic and manual control, safety protection systems, electricity, etc., united by one technological process);

- procedures and language working out for effective and comfort user friendly dialogue in the MMI;

- optimal set of display formats creating.

SOS format as a part of the GOSS is a video screen of upper level that represents a conception, image graphic model of power unit as a whole, starting with Nuclear Steam Supply System (NSSS) and ending with the electricity distribution to the region dispatch system. The main unit's facilities, systems and devices, as well as generalized functional nodes and generalized parameters and elements, important for the safety supervising control are harmonically united in SOS.

There is a special information presented there, necessary for through technological process control (electricity producing) and sufficient for control of safety.

For the first time for RBMK operators an opportunity occurs when without "moving glance", on the basic of one screen cadre, to monitor rapid transients with timely revealing of emergency protection automatics failure, violation of limits and normal operation conditions and environment conditions.

The main user features of the system are:

- generalized information presenting on power unit operation;

- simple and uniform mechanism of an information receiving and ordering;

- comfort of information perceiving;

- operator actions' initiation to parry deviations.

Uniform interface gives the possibility, through automatics or manually, to obtain the necessary information in no time. "One step and touch" graphic exit to any safety or technological system is provided from the SOS.

All the parameters, (as a rule generalized ones), are presented on display screens in the form of histograms. Multi-functional using of nodes', devices' and machinery's symbols is foreseen.

For timely revealing of emergency automatics malfunction, the special alarm indicator windows in the SOS are grouped
according to special rules, mnemonic ally to work algorithm of automatics and ordered to operator actions.

The "emergency information hot line" string is foreseen in SOS at the top of the screen to duplicate (through text) a mnemonic information about emergency protection automatics' failure.

The given channel of information carries out the function of an emergency call of MCR (Main Control Room) for establishing connection with remote (local) operator and technician posts at the unit to send them an urgent message.

For a condition state diagnostics the using of so called "sphere diagnostics principle" is proposed. A small depth of diagnostics is combined here with a wide spectrum of direct and indirect indications and signs, determining the state as a whole. These indications can be of the most different physical nature: starting with limits and conditions of safe operation and ending with TV monitoring of NPP halls, compartments and systems panoramic sight and possible outside influence (fire, explosion, natural calamity and so on).

The SOS information control system foresees two work mode options:

1. Mode with an information filtration. A minimum necessary information is displayed here; this condition is turned on by hand or automatically, when the power unit comes into condition # 3 and above. An indication "blinking" is only used in case of limits and conditions' safe operation violation or in case of failure of safety protection automatics; all the parameters are represent as a rule in a form of histograms.

2. Mode without an information filtration. It is distinguished from the previous one by additional more detailed information, which is necessary for the unit condition supervising control during the shift's acceptance - leaving operation and under the unit steady state operation. Any indication (sign) of changing of condition or position blinks. In case of "quick" conditions (e.g., scram) a mode with an information filtration is turned on automatically. It makes possible to use the same support system both in steady state and emergency transients.

The main elements of generalized schemes are "generalized functional nodes", consisted of several uniform executing units (pumps, valves, reinforcements, heat exchangers and so on), fulfilling (accomplishing) the same function. The functional unit (node) is outlined on generalized schemes as symbol of appropriate executive unit. Information about node's condition is processed according to special algorithms and displayed as a whole and significant for safety control:
a) node condition according reinforcement disposition
- all elements are closed, all elements are opened, even only one element has disposition, distinguished from the others (intermediate disposition);

b) failure (malfunction) for even only one executive element of a node to execute a command of automatic devices (or an "un-sanctioned work" of the element);

c) value for the given one element parameter from a number of uniform parameters of elements is shown on the generalized scheme, namely the one which has the least margin for regulation (the margin before a triggering of shut down or blocking of any system).

A new conception is used in the system design: an organized pre-determined flow of leakage (or emergency feed) of coolant, the symbol of that flow is a red (or blue) arrow. Taking into consideration that automatics command can be interpreted as an information organized flow, the arrows, disposed near executive devices' symbols, mean that these devices (pumps, reinforcement) can change its position (disposition) by automatics commands.

In case of automatics elements' failure or malfunctioning of an executive device to fulfill an automatics command, a "failure for executing of an automatics command" signal is created, accomplishing with blinking of this indicator on the screen.

For an operative control of equipment' and devices' condition the special operative control generalized schemes with using of normalized histograms for all the control points and settings independently from parameter types, have been worked out.

If any protection channel triggers, only one signal "the first reason" blinks on the SOS, but emergency effect signals appear in the hot line (string) of priority information without blinking, but in a consequence of their appearance. It is foreseen the information presentation on one screen:

- about reactor and turbines safety protection system conditions (in case of triggering, failure or output from operation the corresponded indicator is lighted);

- about the value of margin till triggering for each protection channel.

IV. FIRST RESULTS OF THE PROTOTYPE USE

GOSS prototype is being developed and implemented to provide communication and parameters exchange with LNPP Full Scope
Simulator (FSS). However, GOSS could be regarded as stand-alone off-line system and should provide the possibility of its operation both with the simulator and with the real PPC of the operating power unit too. For this reason a modular approach was standardised as well as the communication protocols, list of parameters, and so on.

GOSS prototype is running now under the standard UNIX at the INDY workstation or at the host FSS computer CHALLENGE (Silicon Graphics Int.) with X-Windows terminal displaying and under FSS environment with ETHERNET networking. A successful use of the base GOSS approach for the generalised description of the main technology process and of the unit’s systems and sub-systems had allowed already to use GOSS hierarchy of the display formats as the upper three-level process presentation for the Instructor Station and for the Analytical Simulator operators' interface development.

Since GOSS should be installed later at the real operating power units to be communicated and adjusted with the unit's PPC, and since some PPC's computers are running under UNIX, and others - under Windows NT, so the GOSS communication system has appropriate protocol features for on-line data exchange under different Operating Systems.

In addition, a new option of GOSS software to be run under Windows NT is under development now. This option shall be based with the new base platform, namely the new AIS-95™ ("Automated Interactive System") approach. The ELUD (Easy to Learn, Use & Develop) ideology has formed the basis for AIS-95™ and for new GOSS development. A joint platform's use would provide a compatibility of both systems with their possible merge and more wide options for their use at the PPSs.

GOSS' simulator-mode operation have allowed already to provide research and scientific study on elaborating the picture imagined hierarchy model of the RBMK unit and algorithms of the unit's modes (states) recognition as well as on use of the system as a mean for "on-line" operators' support and MMI improvement.
The experiments at the FSS with the given GOSS prototype have demonstrated its profound and stable communication and operation "on-line" work with the successful recognition of the unit's states and operators' support up to the 5th level ("design" accidents). The work with the severe accidents' operation modes recognition and operators' support would demand its further development and continuation as for the GOSS algorithms as well as (last but not least) for the FSS itself detailed severe accidents' modelling, adjusting, verification and validation.

By now the systems and sub-systems of the RBMK-1000 (LNPP unit # 3) are fully covered with the GOSS three-level picture images. The work for a permanent operators' support for each unit's state (mode) is under development as the most important part of GOSS for its further testing with the FSS. It is assumed, that after successful testing and validation of GOSS as a part of the simulator and after all the necessary modifications the system should be installed at the real power unit # 3 of LNPP to be communicated with its PPC.

Introduction of similar simulators' use as testing devices for the operators' support systems will make it possible to significantly improve NPP safety, as well as the qualities of its specialists training and operators' support, and to diminish the possibility of accidents' rise.

V. CONCLUSION

On the basic of new approaches in principle to the content (matter), kinds and forms of the information presentation the rules and technology of display schemes constructing with editing, generalization and filtration of information have been worked out.

This gave the possibility to create a simple graphics visual model of power unit as a whole (starting with the steam generation and ending with the electricity supply to the dispatch system), comfortable for control and supervising. The model presents an hierarchical tree with the root as Safety Observation Screen (SOS).
For the first time the RBMK supervisors and operators got an 
opportunity without "moving glance" from the one screen to 
control quick transients with prompt revealing of an 
emergency automatics failure or malfunction, violation of 
limits and normal operation conditions to take right 
decisions.

It should be stressed that these rules can be used for all 
complicated complex automated technological processes, 
starting with fossil power plant and ending with petrol-
chemical complexes.

GOSS can be used:

- as a display device for Plant Shift Supervisor and 
  Senior operators, for Safety Supervisors and NRC Inspectors, 
  for Plant men-on-duty;

- as a standard (for RBMK-type or WWER-type) IDS for 
  Crisis Center specialists;

- for accidents' analyses through the accident 
  progress slow-motion demonstration;

- for NPP Personnel training and teaching.

REFERENCES

1. Basic Safety Principles for Nuclear Power Plants - A 

2. Safety Culture- A Report by the International Nuclear 

3. Accident Management Programmes in Nuclear Power Plants - 

4. A.S.Stebenev et al. Ways of transforming and presenting 
   of information for generalized display schemes. Preprint. 

APPENDIX I

As an example we refer to the SOS for the GOSS of the 3rd 
unit of Leningrad NPP which is under evaluation and 
adjusting at the Full Scope Simulator. The following 
functional nodes are presented: pump sets, reinforcement 
units, main regulators, safety system executing devices. 
This SOS contents:

1. Condition of limits and sets of safe operation.

2. Readiness to work and safety systems work ("in", 
   "on", "off").
3. Monitoring of "margin" for triggering by analogue parameters of protection for reactor and turbines.

4. Parameters' condition of main technological process.

5. Condition's control of main automatic regulators of power unit.


7. Control of organized leakage and feed of coolant.

8. Control of aqua-chemical state of power unit.

9. Control of the integrity of physical barriers of radioactivity.

10. Control of feed supply for unit own steam and electricity self-needs.

11. Blocking and automatics failure / malfunction control.

12. Detailed information of the second level. It is used during shift's accepting-leaving. It is switched automatically off in case of the emergency states arising.

13. Extinguishing of fire protection system condition.

14. Information about an outside influence (flaring up, flooding, explosion, natural calamity).

15. Text information (hot line string of a priority information), namely:
   - Duplication (by text) of emergency automatics failure;
   - Providing of urgent communication with remote posts in case of failure of the main channel.

APPENDIX II. MAIN CONCEPTIONS AND TERMS

POWER UNIT CONDITION STATE - the minimum information about deviations of limits and conditions necessary for safe operation, giving the possibility to establish definitely the concrete condition according to one of the following possible state types:

1- conditions without deviations;

2- incident conditions with deviations, not demanding reactor power decreasing;
3- incident conditions, demanding reactor power decreasing;

4- accident conditions, demanding reactor shut down ("scram");

5- accident conditions, connected with malfunction of safety protection system; (power unit emergency conditions);

6- accident conditions, with partly damage of core;

7- severe beyond the project design accidents.

DYNAMIC BARRIERS - conventional limits between power unit's conditions, blocking negative progress of the incident or accident transient by means of transfer into more safe conditions. More precisely, that is a complex of specially developed organizational and technical measures, preventing transition of unit into more negative condition.

CONTROL BY THE STATE - identification of changing power unit's conditions for taking timely measures for back transition into more safe one.

PLANT SHIFT SUPERVISOR (PSS) and DEPUTY PLANT SHIFT SUPERVISOR (DPSS) - chief operators, who make identification of power unit conditions, control and coordination of actions of operator-executors (ordinary operators). PSS and/or DPSS makes a prognosis and provides with planning of actions for power unit control in case of emergencies.

OPERATOR-EXECUTOR - an operator fulfilling controlling actions on executive devices according with set procedures and instructions from the supervisor operators.

MARGIN FOR REGULATION of parameter - a value, which is equal to difference between parameter limit value and preventing alarm set point for parameter's deviation (i.e. between setting of alarm and setting of triggering of protection system). Support of an optimal margin for regulation is one of the condition of comfort operator activity during unit's control.

COMPONENTS OF ACTIVITIES' QUALITY (or components of quality): Equipment, Personnel, MMI auxiliary means (or "Implements" of operator).

OPERATOR IMPLEMENTS - operator' resources (interface), to be used during power unit operation control and supervising (starting with information display systems, support systems, procedures, schemes, automatics' algorithms and ending with operators' communication language.)

ACKNOWLEDGMENT
Both the development and implementation of the GOSS prototype at the Full Scope Simulator of the LNPP were greatly contributed by the RRC "Kurchatov Institute" administration and scientists, and were financially supported by the LNPP.

The significant personal contribution to the given R&D work and GOSS implementation at the Leningrad NPP are made by:  
- the Leningrad NPP work’s initiator and former General Manager A.Yeperin, LNPP General Manager V.Lebedev, LNPP specialists and experts V.Moskovsky, A.Zinchenko, and many others.

Authors would kindly acknowledge the sponsorship of the OECD/NEA Administration for the Paper presentation at this SAMOA-2 Specialists Meeting.
Operator Support System for Multistage Accident Management

Jaejoo Ha, Kwangsub Jeong, Jongtae Jeong
Integrated Safety Assessment Team
Korea Atomic Energy Research Institute
P.O.Box 105, Yusung, Taegus
Tel: +81 42 868 2755 Fax: +81 42 868 8374
Email: jjha@nanum.kaeri.re.kr

ABSTRACT

An accident, in general, starts from an abnormal plant event, and may develop to a severe accident, and to the release of radioactive materials. Since each stage has different characteristics, it is necessary to consider the corresponding multiple stage accident management system: (1) before a severe accident, (2) after the initiation of a severe accident, and (3) the release of radioactive materials. This paper describes the current status and plan of KAERI (Korea Atomic Energy Research Institute) to develop an integrated computer aided accident management system for nuclear power plants, covering the above three stages (KAMP : KAERI Accident Management Program). KAERI has developed KOSNN (KAERI Operation Supporting System for NPP) to assist emergency operation (Stage 1) and KACAP (KAERI Accident Consequence Analysis Program) to analyze consequences (Stage 3). The plan includes the modification of those systems, the development of SPDS (Safety Parameter Display System) and a fast running prediction module to assist sever accident management (Stage 2), and the integration of the subsystems.

1. Introduction

Since an accident, in general, starts from an abnormal plant event, and may develop to a severe accident, and to the release of radioactive materials, we considered an integrated operator aids framework of accident management corresponding to the following three stages:

- **Stage 1**: Emergency operation before a severe accident,
- **Stage 2**: Severe accident management after the initiation of a severe accident, and
- **Stage 3**: Offsite risk management after the release of radioactive materials.

In real plants, Stage 1 is managed by EOP (Emergency Operation Procedure), Stage 2 by SAMP (Severe Accident Management Procedure), and Stage 3 by E-Plan (Emergency Plan). The development of SAMP is undergoing in Korea to be developed in near future, and E-Plan has been prepared, but not considering-consequences in detail. KAERI (Korea Atomic Energy Research Institute) is planning to develop an integrated operator aids covering three stages of accident management (KAMP : KAERI Accident Management Program), that smoothly transits from Stage 1 to Stage 3. KAERI has already developed KOSNN (KAERI Operation Supporting System for NPP) to assist emergency operation for Stage 1. KOSNN was originally developed on a UNIX workstation and currently converted to the Windows NT platform. Three main functions of KOSNN are: (1) providing the operator action items for the emergency operation, (2) generating the success paths of the safety systems ranked based on the operability for restoring the challenged safety functions of a NPP, and (3) suggesting the appropriate event tree to the operator based on the present plant status in order to show the possible future courses of accident progression.

For Stage 2, we have not conducted any research nor implementation yet. It is our current plan to develop an operator aid for severe accident management for Stage 2 including severe accident SPDS and a fast running prediction module for the next five years.

For Stage 3, KACAP (KAERI Accident Consequence Analysis Program) is being developed. The objective is to simulate the impact of severe accidents at nuclear power plants to the surrounding environment. The principal phenomena considered in KACAP are atmospheric transport, dose accumulation by a number of exposure pathways, mitigative actions based on dose projection, early and latent health effects, and economic impacts. Some of the major features of KACAP are: (1) modularization, (2) window based program, (3) graphical display of the results. This code can be used for a variety of applications: level-3 probabilistic safety assessment (PSA) of nuclear power plants and other nuclear facilities, sensitivity studies to gain a better understanding of the parameters
important to PSA, and cost-benefit analysis. Since the original objective of KACAP was not to assist an operator but to analyze consequences, we consider necessary modifications and additions to KACAP for an useful operator assistance tool.

An overall configuration of multistage accident management framework is shown in Figure 1. According to stages, the corresponding procedures are followed. Operator aids ultimately assist the procedures using relevant information and interfaces. The following sections describe our work that has been done, including KOSSN and KACAP, and a framework of the integrated operator aids system.

II. Stage 1 for Emergency Operation

The emergency operation of nuclear power plants is performed based on the emergency operating procedures (EOPs). After the TMI-2 accident, the function-based approach is introduced into the EOPs and this has increased both the breadth and depth of the EOPs. The operator must be aware of the plant status on several levels concurrently to recover from a transient effectively. A human being, however, can consider the changes of plant status only in a serial fashion, and therefore may be unable to properly understand the overview of the plant condition [1,2]. Hence, a number of computerized operation supporting system (COSS) based on the EOPs have been developed. The COSS technique enables the operator to find the appropriate response actions without time stress due to information overload under emergency situations [3].

KOSSN provides the operator with not only a list of action items based on the EOPs but also additional information which is useful to take the actions more easily and to understand the overall status of a NPP. These additional information includes the success paths of the safety systems and the event tree from the plant specific probabilistic safety assessment (PSA).

A number of systems which have the similar objectives with KOSSN have been developed in the last few years. The characteristics of those systems are compared with that of KOSSN in Table 1 [4-11]. As shown in Table 1, there are two major differences between KOSSN and other systems. One is that KOSSN provides more detailed information and guidance such as the success path. The other is the use of PSA techniques such as the operability and the event tree. The success path means the steps that are required to operate a system successfully including the selection of a safety system and the operation of that system. The success path is generated by using the structure description and present status of the safety systems. The success paths are ranked according to the operability which is defined as the reliability of each path. The event tree are also used to enhance the capability of KOSSN. The success path with its operability value makes the operator to select the most reliable recovery action under the present status of a NPP. The event tree is a logical model used in the PSA to show the courses of accident progression due to an initiating event. The suggestion of the event tree corresponding to the present status of a NPP makes the operator to be aware of the possible courses of accident progression. Such a systematic and detailed guidance provided by KOSSN enables the operator to take corrective actions with more clear understanding about the status of a NPP.

KOSSN is developed in order to support the decision making of the senior reactor operator (SRO) level during an emergency situation. The system can be installed in the Technical Supporting Center (TSC) so that the information from KOSSN can be transferred to the SRO as an alternative.

1. KOSSN Configuration

The overall structure of KOSSN is shown in Figure 2. KOSSN consists of three parts: (1) the operator's action guide, (2) the success path generation, and (3) the corresponding event tree suggestion parts. Each part has its own knowledge base and inference engine. Main part of Figure 2 controls the information exchanges among the above three parts and provides the man-machine interface to the user. It is assumed that KOSSN can get all information that are required during the inference process by on-line and such information is validated.

Operator's Action Guide Part

In KOSSN, the operator action items are derived based on the EOPs. Two parts of the EOPs, i.e., the Optimal Response Procedures (ORPs) and the Functional Restoration Procedures (FRPs) are stored as the knowledge base in the form of "IF-THEN-ELSE" rules. According to the present plant status, the appropriate response actions are derived from these rules. In KOSSN, the EOPs of Kori Units 3 & 4 are used. Kori Units 3 & 4 are Westinghouse designed 3-loop pressurized water reactors (PWRs).

To build KOSSN, the operator actions of the EOPs are reorganized. During this process, the operator actions included in the EOPs are standardized and classified. We have paid attention to the point that the exactly same guidance is to be provided by the EOPs and KOSSN since we assumed that the contents of the EOPs should not be
changed. The operator action items have a hierarchy of three levels. The level 1 action is associated with the decision about the overall response strategy, and it can be regarded as the ultimate purpose of the operator's action. The level 2 action is regarding to the operation mode of a specific system or component. In other words, the level 2 action specifies what system should be turned on or off to achieve the present level 1 action. Finally, the level 3 is associated with the real operation in the component level. For instance, "if subcriticality is red state then borate the reactor coolant system (RCS)" is a level 1 rule for a critical safety function (CSF) item, "subcriticality." An example of the level 2 rule is that "if present level 1 action item is to borate RCS then operate chemical and volume control system (CVCS) for RCS boration." A level 3 rule is that "if present level 2 action item is to operate CVCS for RCS boration then start the charging pump."

For the inferred level 2 action item, the success paths are generated. The suggested system in the level 2 action is transferred to the "Success Path Generation Part" in order to generate the success path of that system. The level 3 actions are derived during this step.

**Success Path Generation Part**

In KOSSN, the success paths are generated by applying the path generation algorithm to the structural description of a particular system instead of using the predetermined success paths. In KOSSN, the structural descriptions of systems are stored as the database. The structural descriptions are based on the piping and instrumentation diagrams (P&IDs) of the safety systems. Most P&IDs consist of two parts: one is components which perform their intended function and the other the connection elements, e.g., piping. An example of knowledge representation form for the structural description is shown below:

```
component_db(Name, Type, Capacity, Next_Node, State).
```

In the above example, "Name" represents the specific name of a component such as the component tag number. "Type" is the type of that component, e.g., the check valve, motor-driven pump, etc. "Capacity" represents the capacity of the component with which KOSSN can consider a partial failure of that component during the generation of the success path. "Next_Node" represents the connection element related to the component, and "State" is the present state of the component.

It is assumed that all components have two states: the initial and demand states. The initial state represents the present state of the component, e.g., opened/closed/failed for the valves, running/standby/failed for the pumps, etc. The demand state is the state of a component in which the particular component can perform its intended function, namely, "open valve", "run pump", etc. Whenever the initial and demand states are different, the level 3 operator action item is provided to the operator. For instance, if a valve is in closed state at present and the demand state of that valve is a valve-open, then the level 3 operator action item such as "open the valve-XXXX" is suggested.

To generate the success paths, the initial and demand states of a given starting component are compared. If these two states are equal, the same logic is applied to the next components which are connected to the previous one. In the case that two states of a component are different, the level 3 action item is derived as mentioned above. This scheme is successively applied from the starting component to the final one, thereby, one success path is obtained.

The required capacity of the success path is determined previously from the technical specifications and/or other mechanistic calculations. The capacity of the generated success path is compared with the required capacity. When the capacity of a component is not enough to satisfy the required capacity of the success path due to the partial failure of that component, KOSSN searches the additional path(s) that can compensate the insufficiency of the capacity. The combination of these paths are regarded as one success path for the present system.

The generated success paths are ranked according to either its respective reliability or the number of the operator's actions required to complete that path. The operator can choose the most reliable success path or the success path that requires the least number of human actions. The results of previous PSA show that the human error probabilities are usually higher than the failure probabilities of equipment. In such cases, the success path with the least number of human actions coincides with the most reliable one. The reliability of components in each success path is obtained from the reliability database. The date used to calculate the operability are obtained from the general PSA database [14,15].

The selected success path is displayed on a screen with the different color and the required operator action items are also listed. The operability can be regarded as the heuristic measure for the effectiveness of the generated success paths, i.e., the system availability depends on the selected success path.
Event Tree Suggestion Part

In the PSA, the event tree is used to identify the accident sequences which lead to core melt/core damage. Each system event tree represents a distinct set of the accident sequences, each of which consists of an initiating event and a combination of various systems' successes and failures that lead to an identifiable plant state. In other words, the event tree shows a logical prediction of an accident sequence.

The event tree used in KOSSN is the small event tree type, and only the front line systems which can mitigate an accident or transient are addressed in this type of the event tree. The event trees are constructed according to the status of CSFs and related safety systems, hence, the high level operational guidance provided by KOSSN can be regarded as one of the event tree's heading.

In KOSSN, the event tree can be used in two different circumstances. If a transient is already identified, i.e., the operation guidance provided by KOSSN are based on the knowledge derived from the ORPs, the corresponding event tree is used to show the possible future courses of the accident progression to the operator. When the transient is not identified yet, that is, the operation guidance provided by KOSSN are based on the knowledge derived from the FRPs, a group of event trees which show similar characteristics with the transient are suggested as the candidates. These group of event trees are suggested by comparing the headings of the event trees with the operational guidance provided by KOSSN. As the transient progresses, the event trees belong to the candidate group are re-examined and the event trees which show discrepancy with the present status of a NPP are removed from the candidates. So the suggested event trees will be gradually reduced to a few event trees. This feature may help the operator to identify the transient.

2. Test and Evaluation

Implementation Test

KOSSN is applied to a SGTR transient for the implementation test. When the transient begins, the response guidelines derived by the rules corresponding to the E-0 of the ORPs are provided to the operator. The operator action item with the success path of a system is displayed as shown in Figure 2. In this case, the level 1 action guide is to "verify automatic action as initiated by protection and safeguard systems," the level 2 action item is to "check if safety injection (SI) is actuated." The success path of SI, hence, are generated. Among the generated success paths, the most operable success path is displayed on the simplified P&ID as shown in Figure 3. The derived level 3 action items to accomplish above level 2 action item are "open LV115D" and "open BH-HV20." The intended function of an initially selected level 2 action item may not be achieved due to various reasons such as the failure of some components. When a selected item cannot perform its function, then an alternative level 2 action item will be automatically suggested. For instance, if the operator confirms that SI does not perform its function, then "Establish secondary heat removal" will be suggested as an alternative level 2 action item and a new set of success paths to complete this action item will be generated for the corresponding safety systems.

While the operator performs the suggested action items, another CSF may be challenged. Usually, the newly challenged CSF has a higher priority. If this happens, the present CSF status and the CSF status tree of the challenged CSF item are displayed on the screen as shown in Figure 4. In such case, a new set of action items are derived from the FRPs. In Figure 4, the level 1 action item is to "attempt restoration of feed flow to SGs," and the level 2 action item is to "check if the secondary heat sink is required." The required conditions to achieve above level 2 action item is that RCS pressure should be higher than any intact SG pressure.

In this example, it is assumed that the transient is identified as a SGTR by the E-0 diagnosis procedures, therefore, the SGTR event tree is selected and displayed to the operator. An example of event tree display is shown in Figure 5. The display shows the present status of the plant:

- the SGTR is occurred,
- the reactor is tripped successfully,
- the high pressure injection system fails,
- the secondary heat removal succeeds, hence,
- the feed and bleed operation is not necessary.

Currently, the operator is trying to isolate the failed steam generator according to the operational guidance provided by KOSSN. According to the success or failure of the isolation procedures, the plant state should follows one of those sequences between sequence 11 and sequence 16 of Figure 5. From this event tree display, operator can recognize that the required future actions are the cool down and depressurization of RCS, the actuation of the low pressure safety injection (LPSI) or the residual heat removal system (RHRS). The operator, hence, can concentrate his/her effort to the operation of these systems.
When the transient cannot be identified at the initial stage of transient, the challenged CSFs and the corresponding safety systems to restore that CSFs are recorded and compared with the headings of the event trees. A group of the event trees which show the similar characteristics are suggested to the operator, that is, even though the accident progress is not matched exactly with the headings of the event trees and/or the order of headings, the event trees which show the most similar characteristics are suggested to the operator. For instance, when the first four safety systems used to restore the transient are "the reactor protection system," "HPSI," "the secondary heat removal" and "feed and bleed operation," the event trees of the small LOCA (Loss of Coolant Accident) and SGTR can be suggested as the candidates for this transient. If the next step of the operator's action is "the isolation of failed SG," then the event tree of SGTR is suggested as the final one.

Evaluation

To implement a COSS in the real world, the evaluation of the system is required. The COSS can be regarded as a kind of expert systems. The evaluation techniques of the expert systems, therefore, can be applied to the evaluation of the COSS. The evaluation of expert systems can be divided into three categories: verification, validation and evaluation [16,18]. The verification means to build the system right, and the validation means to build the right system. The verification focuses on the aspect whether or not the system is built as the designer of the system intended. On the other hand, the validation focuses on the aspect whether the inferred results are suitable in real world or not. The evaluation is a broader area to access an expert system's overall value - acceptable performance levels, usability, efficiency and cost effectiveness.

The method for verification, validation and evaluation can be divided into two groups: the empirical and logical methods. The empirical method is divided further into two groups: the qualitative and quantitative methods. In the logical method, the knowledge base is regarded as the collection of logical expressions, and the logical consistency is checked for the knowledge base. This method is good for checking the consistency and completeness of the knowledge base. In the empirical method, the inferred results of the expert system is reviewed by the human expert, and based on the review results, the performance of the expert system is estimated.

The expert systems of nuclear industry can be classified into six types [19,20]:

1. simple type, use only predefined and described knowledge,
2. same as type 1, but include uncertainty,
3. simple type, use the inferred knowledge,
4. same as type 2, but include uncertainty,
5. complex
6. complex, but include uncertainty.

The knowledge base of KOSSN is based on the EOPs, so KOSSN can be classified into type 1. It is, therefore, relatively easy to evaluate KOSSN. The logical method is used for the verification and validation. For KOSSN, the validation can be regarded as a part of verification since the knowledge base for the level 1 and 2 action items is simply the computerized text of the EOPs. If the logic of the EOPs are translated exactly into the knowledge base of KOSSN, the inferred results should be the same as the EOPs, and such results can be regarded as the correct one. We follow every steps provided by KOSSN and check whether or not the result is consistent with the EOPs. The result shows that the knowledge base of KOSSN has the same logic with that of the EOPs.

KAERI held a meeting to present KOSSN to the various fields of people such as the managers and operators of utility, KEPCO (Korea Electric Power Corporation), experts for expert systems. We demonstrated the example run of KOSSN which is described in the previous section, and surveyed their opinion about KOSSN. The followings are the major opinions from the survey:

- The display of P&ID is very helpful.
- The organization of EOPs to three level actions helps operators to understand overall structures and objectives of their recovery actions.
- The use of success paths with P&ID is helpful to understand possible success paths and the most available path.
- The use of event trees is an effective mean to provide operators possible future consequences and help decision makings.
- The operator should be included in the development stage of this kind of expert system, and the use of such system should be included in the operator training course, because they would not use it if they are not familiar with it.
- The system itself can be a another source of information overload, and Korean language should be used in the user interface.
III. Stage 2 for Severe Accident Management

Because of uncertainties involved in severe accident phenomena and the lack of precise procedures yet, the approach to develop an operator aid for severe accident management can be different comparing KOSSN where the EOPs are implemented. However, we consider the basic components of operator aid for severe accident management should include SAMP (Sever Accident Management Procedure) like the EOPs, SPDS which supports SAMP, and additional decision making information. This additional information may include a prediction of severe accident by the use of simulation code, involving expected operator actions as well as accident progression. MELCOR is a candidate of this core calculation module. In our analysis using MELCOR, a computing time to calculate a major accident such as core melt and vessel failure takes close to actual time in DEC2 machine. This is a remarkable improvement in computing speed that is almost 10-20 times faster than SUN4 machine. Considering this rapid improvement of computer speed, we expect computing time will be reasonably faster than actual time in near future. Surrounding MELCOR calculation module, an interface module to interact with operator will be developed in the following years with necessary modification. However, due to large uncertainties of this kind of analysis code, expert opinion should not be ignored. As we gather more information about severe accident phenomena, we plan to develop expert system working together with the prediction module.

IV. Stage 3 for Offsite Risk Reduction

1. KACAP for Consequence Analysis

KACAP is being developed in KAERI. The purpose of this code is to simulate the impact of severe accidents at nuclear power plants to the surrounding environment. The principal phenomena considered in KACAP are atmospheric transport, dose accumulation by a number of exposure pathways, mitigative actions based on dose projection, early and latent health effects, and economic impacts. Some of the major features of KACAP are: (1) modularization, (2) window based program, (3) graphical display of the results. This code can be used for a variety of applications: level-3 probabilistic safety assessment of nuclear power plants and other nuclear facilities, sensitivity studies to gain a better understanding of the parameters important to PSA, cost-benefit analysis, and a core module of operator aids to reduce offsite risk. The essential models included in the KACAP code is illustrated in Figure 6 and sequential flow diagram is shown in Figure 7.

Consideration of Source Term

The source term data which specify both the magnitude and the manner of release defined by a number of release parameters such as the time of the release after accident initiation, the release height, etc., are given by the input wizard in the form of isotopic release rate for the sixty radionuclides which are important for the accident consequence analysis or release fractions along with the release parameters. Either constant or variable weather conditions as input data can be used. Variable data is specified as a sequence of hourly values of wind speed, atmospheric stability class, and amount of precipitation, that begins at a time specified by the user or selected by the weather categorization and sampling algorithm embedded in the code such as weather bin-sampling and stratified random sampling method.

Dispersion and Deposition

Dispersion and deposition of radioactive materials released from the reactor containment to the atmosphere were modeled with a Gaussian plume model. Plume rise, plume depletion by dry deposition, wet deposition, and radioactive decay, and building wake effect were taken into account in the calculation module, and then air and ground concentration of radionuclides are calculated on the computational grid specified by a user as input.

Consideration of Exposure Doses

The exposure doses are calculated through three interacting processes: projection of individual exposures to radioactive contamination for each of the pathways, mitigation of these exposures by emergency response actions, and calculation of the actual exposures incurred after mitigation by emergency response actions. KACAP models six exposure pathways: exposure to the passing plume, exposure to materials deposited on the ground, exposure to materials deposited on skin, inhalation of materials directly from the passing plume, inhalation of materials resuspended from the ground, ingestion of contaminated foodstuffs.

The accumulation of doses to individuals affected by a reactor accident must take into account the location of these individuals during and following the accident, as well as the time period during which the doses were received. Actions to mitigate the effects of a release of radioactivity during a reactor accident can have a significant
impact on accident consequences. These mitigative actions are protective measures designed to reduce radiation exposures, public health effects, and thereby result in economic costs from an accident. Therefore, evacuation, sheltering, temporary relocation, disposal of contaminated crop, decontamination, temporary interdiction, condemnation, and restricting crop production are modeled as a protective measure.

Health Effects

Health effects are calculated from doses to specific organs by using dose conversion factors. Early injuries and fatalities which occur within one year of the accident are estimated using nonlinear dose-response models and hazard functions. As a late health effect, mortality and injury resulting from radiation induced cancers are calculated by using a linear-quadratic, zero threshold, dose response model.

Economic Impacts

Economic impacts resulting from an accident are estimated by summing the following costs: replacement power costs, plant onsite decontamination costs, worker health effect costs, reactor plant capital investment loss, costs due to early decommissioning, evacuation costs, temporary relocation costs, population health effect costs, costs due to the disposal of agricultural costs, offsite decontamination costs. The first five items among the cost items mentioned above are referred to the onsite cost items, and the rest are referred to the offsite cost items.

2. Offsite Risk Reduction Framework

The important area of the accident management is to mitigate offsite risks resulting from a reactor accident through appropriate countermeasures such as evacuation, sheltering, relocation, and so on. The useful way of offsite risk assessment and establishment of risk reduction strategy is integration as shown in Figure 8. As a basic concept, the integration recognizes that in any given software system for real world applications, more than one problem representation form or model, several sources of information or data bases, and finally a multi-faceted and problem-oriented user interface ought to be combined in a common framework to provide a useful and realistic information base [22]. At the level of data and background information, numerous sources of information have to be brought together. At the level of tools, there are several levels of integration, ranging from simple file transfer between different methods and programs to fully integrated systems. Typical examples of different methods that lend themselves to integration include geometrical information systems (GIS) and models as well as decision making support systems. The assessment of offsite risks resulting from an accident at nuclear power plants and the decision making about which countermeasure to apply in order to reduce offsite risks will be implemented on this concept of integration.

Geometrical information systems are tools to capture, manipulate, process, and display spatial or geo-referenced data. They contain both geometry data and attribute data, i.e., information describing the properties of geometrical spatial objects such points, lines, and areas. In the integration framework shown in Figure 3, the GIS is used as a tool to display spatial data of a reference plant site and the distribution of radionuclide concentration or risks related with health effects such as early injury, early fatality, and cancer fatality. In the analytical system of the integration, KACAP code will be used to calculate the distribution of radionuclide concentration or offsite risks. And through a decision making support system, one can find the most appropriate strategy for applying countermeasures to reduce offsite risks. The emergency response actions such as evacuation, sheltering, and temporary relocation will be considered as countermeasures to reduce offsite risks because these actions which last up to seven days after the initiation of reactor accident are meaningful in viewpoint of accident management.

In the following years, we plan to establish a database consisting of weather, site, population, and source term information, and calculate various exposure doses and risks based on the combination of the above data. Then using GIS, the risks are mapped to find the worst case and the optimal risk reduction strategy.

V. Discussion & Future Works

An integrated operator aid covering three stages has been planned in KAERI. For the first stage, emergency operation, KOSSN has been developed to support the operator's response to any abnormal state in a NPP. It is expected that the combination of the EOPs with the concept of success path and the PSA techniques such as the operability and the event tree allows a more effective and systematic response to the emergency situation of a NPP. The second stage, severe accident management, will be covered in the next five years. The basic components include SAMP assistant, severe accident SPDS, and fast running prediction module using MELCOR. It is now a concept building stage, and its feasibility will be studied. Offsite risk reduction framework is proposed using mainly GIS and KACAP. KACAP is a consequence analysis program which will serve an analytical tool to the
decision making process. In the following years, necessary improvement and development will be made to construct an integrated operator aid for multistage accident management.

REFERENCES

Table 1. Characteristics of KOSSN Compared with Other Operation Supporting Systems

<table>
<thead>
<tr>
<th>Name</th>
<th>Eveloper</th>
<th>Basis</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPA</td>
<td>OECD</td>
<td>EOPs, Normal Operating Procedures</td>
<td>on-line procedure</td>
</tr>
<tr>
<td>EOPTS</td>
<td>EPRI</td>
<td>EOPs</td>
<td>on-line tracking and explanation</td>
</tr>
<tr>
<td>SPMS</td>
<td>EPRI</td>
<td>CSF, Success Path</td>
<td>monitor the status of CSF &amp; deploy the appropriate success path</td>
</tr>
<tr>
<td>OPA</td>
<td>EPRI</td>
<td>EOPs</td>
<td>task schedule</td>
</tr>
<tr>
<td>REDIktor</td>
<td>Tech.Appl.</td>
<td>PSA</td>
<td>estimate the likelihood of core-melt</td>
</tr>
<tr>
<td>FORESTER</td>
<td>EG&amp;G</td>
<td>PSA</td>
<td>identify particular failure mode</td>
</tr>
<tr>
<td>KOSSN</td>
<td>KAERI</td>
<td>EOPs, PSA, Success Path</td>
<td>on-line procedure, success path and future status</td>
</tr>
</tbody>
</table>

A: Organization for Economic Corporation and Development,
B: Electric Power Research Institute,
C: Technology Application Inc.

Figure 1 Overall Configuration of Multistage Accident Management Framework
Figure 2. Overall Structure of KOSSN

Figure 3. Example Display of Operational Guidelines with Success Path
Figure 4. Example Display of CSF Status Tree

Figure 5. Example Display of Event Tree
Figure 6. The essential models included in the KACAP code

Figure 7. Sequential flow diagram for KACAP
Figure 8. An integrated framework for establishing risk reduction strategy
A Neuro-Fuzzy Model Applied to Full Range Signal Validation of PWR Nuclear Power Plant Data

Paolo F. Fantoni, OECD Halden Reactor Project, Halden, Norway (paolof@hrp.no)
Stefan Figedy, Vyskumny Ustav Jadrovych Elektrarni, Trnava, Slovak Republic
Bertrand Papin, Centre D’Etudes De Cadarache, France

ABSTRACT

Artificial Neural Networks and Fuzzy Logic models can be combined to exploit learning and generalization capability of the first technique with the approximate reasoning embedded in the second approach. Real-time process signal validation is an application field where the use of this technique can improve the diagnosis of faulty sensors and the identification of outliers in a robust and reliable way.

This study implements a fuzzy and possibilistic clustering algorithm to classify the operating region where the validation process has to be performed. The possibilistic approach (rather than probabilistic) allows a “don’t know” classification that results in a fast detection of unforeseen plant conditions or outliers.

Specialized Artificial Neural Networks are used for the validation process, one for each fuzzy cluster in which the operating map has been divided. They work concurrently on each signal pattern presented to the system and the overall contribution is weighted according to the membership function of the pattern in each cluster.

There are two main advantages in using this technique: the accuracy and generalization capability is increased compared to the case of a single network working in the entire operating region, and the ability to identify abnormal conditions, where the system is not capable to operate with a satisfactory accuracy, is improved.

This model has been tested in a simulated environment on a french PWR, to monitor safety-related reactor variables over the entire power-flow operating map.

1. INTRODUCTION

Previous work at the Halden Reactor Project\(^1\)\(^2\) showed how specialized supervised Artificial Neural Networks (ANN), driven by a pattern recognition algorithm, could improve the validation performance in highly non-linear processes like Nuclear Power Plants (NPP). There the classifier, based on the classic ISODATA\(^3\) algorithm, identified the incoming signal pattern (a set of reactor process signals) as a member of one of nine clusters covering the entire universe of discourse represented by the possible combinations of steady-state and transient values of the input set in the \( n \)-dimensional input world. Each cluster was associated with one ANN that was previously trained only with data belonging to that cluster, for the input set validation process.

During the operation, while the input point moved in an \( n \)-dimensional world (because of power manoeuvres or transients), the classifier provided an automatic switching mechanism to allow the best tuned ANN to do the job. The results were satisfactory, but the following two drawbacks were identified:

- the boundary problem. That model did not consider properly the transition area between clusters, where the input pattern could be considered a member of two or even three clusters at the same time. As a consequence of that, the switching mechanism changes the working ANN abruptly, when the input pattern moves in ambiguous areas, resulting in unexpected changes in performance.
- a crisp classifier always tries to find a reasonable membership cluster, even when the input pattern is far away from all the identified clusters. In turn, the activated ANN always gives a response, so that there is no way to have a reliability measure for the output. This is a very well known problem of every black-box approach (and there is nothing more than ANN modeling that can be called black-box), that could justify the very few industrial ANN applications currently existing in the world, at least in the nuclear field.

This work addresses the two problems above, introducing a possibilistic fuzzy clustering technique\(^6\) coupled to a set of concurrent specialized ANN and finally a fuzzy model (Mamdani type) for reliability estimation. This model has been developed and tested on simulated scenarios using data provided by CEA for a french PWR.

![Figure 1. Signal Validation Model schematic diagram](image)

2. **THE CLASSIFIER**

Let \( \bar{x} = [x_1, x_2, ..., x_N]^T \) a vector in \( \mathbb{R}^N \) representing an input dataset. The \( N \) components are correlated process signals that constitute a snapshot of the monitored process at a given time. Given \( X = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_P) \) the \( N \times P \) matrix of \( P \) patterns covering the \( \mathbb{R}^N \) operating region, the basic idea is to split this region in \( Q \) fuzzy clusters and derive a mapping function which assign each pattern \( \bar{x}_i \) \( k = 1...P \) to each cluster \( C_i | k = 1...Q \) at some degree. This transformation is expressed by the following equation:
\[ \bar{x}_i \Rightarrow \{u_{1k}, u_{2k}, \ldots, u_{Qk}\} \]  

(1)

and

\[ u_{ik} \in [0,1], i = 1, \ldots, Q, k = 1, \ldots, P \]  

(2)

where \( u_{ik} \) is the membership grade of the pattern \( \bar{x}_i \) in cluster \( C_i \). In pattern recognition, the \( Q \) clusters are identified by prototype patterns, which in the case of spherical or ellipsoidal clusters are also called centroids, so that the representation of a fuzzy classifier for a given \( X \) (\( N \times P \)) matrix dataset with \( Q \) clusters is completely defined by:

\[ B = (\hat{\beta}_1, \hat{\beta}_2, \ldots, \hat{\beta}_Q) \]  

(3)

\[ U = (\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_Q)^T \]  

(4)

\[ \hat{\beta}_m = [x_{1m}, x_{2m}, \ldots, x_{Nm}]^T \]  

(5)

\[ \bar{u}_m = [u_{m1}, u_{m2}, \ldots, u_{mP}]^T \]  

(6)

where \( B \) is the \( N \times Q \) matrix of the cluster prototypes and \( U \) is the \( Q \times P \) matrix of the membership grades of \( X \), also called the fuzzy \( C \)-partition.

The fuzzy partition problem, as expressed in (3), (4), (5) and (6) can be solved with the minimization of an objective function\(^1\), which can be written as:

\[ J(B, U, X) = \sum_{i=1}^{Q} \sum_{j=1}^{P} (u_{ij})^m \Delta^2(\bar{x}_j, \hat{\beta}_i) \]  

(7)

where \( m \in [1, \infty) \) is called the fuzzifier parameter and \( \Delta \) is a function representing the distance between two vectors. When \( m = 1 \) the classifier is crisp and when \( m \gg 1 \) fuzziness is maximized. \( m = 2 \) is the recommended value, for most applications.

The choice of the \( \Delta \) function depends by the expected shape of the clusters. If the Euclidean distance is used, which is the right choice for spherical clusters, the resulting algorithm is the popular Fuzzy \( C \)-means algorithm\(^5\). In this application clusters with different shapes and sizes are expected, so that Euclidean distances would not work well. To take care of the not uniform distribution of the patterns in the dataset, the GK algorithm, from Gustafson and Keller\(^6\), has been used. Here the distance function is expressed as:

\[ \Delta_{ij}^2 = (\det C_i)^{-\frac{1}{2}} (x_j - \hat{\beta}_i)^T C_i^{-1} (x_j - \hat{\beta}_i) \]  

(8)

where \( C_i \) is the fuzzy-covariance matrix for cluster \( i \), defined as:

\[ \frac{1}{\sum_{j=1}^{P} (u_{ij})^m} \sum_{j=1}^{P} (u_{ij})^m (x_j - \hat{\beta}_i)(x_j - \hat{\beta}_i)^T \]  

(9)
In fuzzy clustering, $U$ must satisfy the following three conditions:

$$
\sum_{i=1}^{Q} \mu_{ik} = 1, k = 1...P \quad (10)
$$

$$
\mu_{ik} \in [0,1], \ i = 1...Q, \ k = 1...P \quad (11)
$$

$$
0 < \sum_{j=1}^{P} \mu_{ij} < P, \ i = 1...Q \quad (12)
$$

Condition (10) reflects the probabilistic requirement that the total probability for an input dataset pattern to belong to any cluster is 1. In other words, patterns not reflecting any of the identified cluster prototypes are classified and assigned to the relatively most probable cluster, only because of the implicit certainty that all the patterns belong to the established partition. There can be uncertainty (or fuzziness) on where the incoming pattern could be assigned, but no uncertainty on if it can be assigned somewhere. When this methodology is applied to signal validation applications, a number of problems may arise:

- Lack of robustness against noisy data. There is no compensation for the noise in the calculation of $B$ and $U$.
- It is not able to say "I do not know", also when this would be the best answer. An incoming pattern might be given a high grade of membership in a cluster, even if it is far away from all the centroids, only because it is relatively closer to one specific cluster.

Relaxation of requirement (10) leads to a possibilistic approach, that results in a possible solution of the two above mentioned limitations.

A possibilistic classifier initially learns a dataset $X$ of pattern samples (in other words it calculates $B$ and $U$). During this process, the model increases its robustness to noisy data and many patterns in $X$ could be discarded as not representative of any developing cluster. When new patterns are examined, the possibilistic model evaluates in which cluster or clusters the incoming pattern could be possibly assigned, if any.

Following Krishnapuram and Keller’s work, minimization of the objective function (7), without the constraint in (10), results in the following equations for $U$ and $B$:

$$
\mu_{ij} = \frac{1}{1 + \left( \frac{\Delta^2(x_j, \hat{\theta}_i)}{\eta_i} \right)^{m-1}} \quad (13)
$$

where $m > 1$ and

$$
\hat{\beta}_i = \frac{1}{\sum_{j=1}^{P} (\mu_{ij})^m \bar{x}_j} \quad (14)
$$

where $\eta_i$ is computed by:

$$
\eta_i = (\det \ C_i)^{\frac{1}{N}} \quad (15)
$$
The step-by-step procedure used to develop the fuzzy and possibilistic classifiers can be summarized as follows:

- Given a set of samples \( X \), compute an initial set of cluster centroids using the ISODATA algorithm, that has been chosen because it automatically optimizes the number of required clusters.

- Initialize the elements of the partition matrix \( U \) with crisp values (0 or 1), using ISODATA. Then run the GK algorithm, which produces the fuzzy classifier.

- Use the updated matrix \( U \) and \( B \), from the previous step, to start the iterative process as shown in eqs. (13) and (14) to arrive to a possibilistic partition.

3. THE SUPERVISED NETWORKS MODULE

Sample data in dataset \( X \) are collected in \( Q \) training datasets, to be used for training \( Q \) supervised neural networks. Each pattern in \( X \) is assigned to one or more training set according to the fuzzy partition, as long as its possibilistic index in \( U \) is above a threshold value \( h \) in one or more identified clusters, with \( h = (0.5,1) \). The role of the threshold parameter \( h \) is twofold:

- sample patterns not adequately represented in any cluster are discarded, so that they have no influence on the network weights calculation.

- sample patterns possibly represented in many clusters (responsible of the above mentioned boundary problem) are used in the training set of many corresponding networks.

The network architecture used in this work is a five layers (three hidden layers), feedforward structure trained with the backpropagation algorithm. For better performance, a momentum term and an adjustable learning coefficient have been used\(^2\). The hidden layers use hyperbolic tangent transfer functions, while the output layer is linear. This architecture has been proved\(^2\) to be more robust to process noise and sensor faults.

The input to the ANN's is not limited to the current pattern. To capture the process dynamics, a number of past values of the time series are used, together with the current ones, so that the total number of input nodes in each ANN is \( N \times R \), where \( N \) is the number of signals and \( R \) the number of past values used. In this work, samples at \( t-0, t-2, t-5, t-13, t-34 \) and \( t-89 \) have been used for each signal. This allows to consider both short and long time constant effects in the process dynamics.

The three feedback loops in Fig. 1 are used during the recall (on-line validation).

The in-step feedback, in case of mismatch in one or more signals, re-evaluates the corrected pattern to get better estimates in the not affected channels. This feedback is triggered only if the signal mismatch is estimated to be above two standard deviations, to avoid instabilities.

The back-step feedback corrects mismatching signals for the future evaluations, when those values will be used as past values, as mentioned before. This also triggered by the same threshold value.

Finally, the one-step-ahead feedback monitors the next coming pattern for possible large deviations. Large deviations have a negative effect on the overall performance, because they lead to false classifications with the results that not optimal ANN's are triggered for recall, only as a consequence of a large deviation in one or more channels. Large deviations from the expected values are corrected before the classification, resulting in a much more accurate and stable validation. In Fig. 1, the expected, one-step-ahead values are calculated by a predictive ANN, but tests have shown that the current values (at time \( t \)) can be used as a rough estimation of the values at time \( t+1 \).
The recall strategy does not make use of the above threshold parameter to trigger one or more of the specialized networks. The algorithm used here, applicable only to signal validation processes, applies the concept of presumption of no sensor fault, if possible. This concept is based upon the well tested hypothesis$^{12,9}$ that when a neural network confirms the sensor input (no faults condition) and the relative cluster membership grade is high, the network output is reliable.

This leads to the following recall strategy:

- for each process sample: get the most representative cluster, which is the one with the highest membership grade $u1$ in $U$
- recall the output using the neural network associated to this cluster
- calculate the maximum absolute deviation, as follows:

$$err1 = \max|s_j - o_j| \times \text{sgn}(s_j - o_j) \quad j = 1, ..., N$$

(16)

where $s_j$ and $o_j$ are the $j$-th network input and output values for a process pattern
- if $err1$ is very low, accept the result, otherwise recall the pattern using also the network with the second highest grade of membership, $u2$
- calculate the following weighted error:

$$werr = \frac{err1 \times u1 + err2 \times u2}{u1 + u2}$$

(17)

where $err2$ is the maximum error with the second network. Now if:

$$\text{abs}(werr) > \text{abs}(err1)$$

(18)

accept the output from the first network, otherwise calculate a weighted output from:

$$wout = \frac{out1 \times u1 + out2 \times u2}{u1 + u2}$$

(19)

where $out1$ and $out2$ are the vector outputs from the two networks.

4. THE RELIABILITY ASSESSMENT MODULE

In a previous work$^*$ we tried to solve the reliability problem connected to the use of neural networks, using a Radial Basis Function network associated to a crisp pattern classifier. This work extends the idea, exploiting the unique features of a possibilistic classifier.

The possibilistic cluster membership has an important role in the final decision whether the network output can be considered reliable or not. A high membership grade in one or two clusters increases our confidence that the data sample is contained in the training volume of one or two neural networks, so that
they will be able to recall the output with low estimation error. On the other side, a low membership value in all the clusters is a clear warning that no network has been trained to recall such a pattern. Note that using fuzzy clustering techniques, it would not be possible to have neither low values in all the clusters, nor high values in more than one.

In this work, the reliability function is realized through a fuzzy model (fig. 2), where the input is the maximum membership grade of the sample and the maximum signal mismatch in the neural network module, while the output is the reliability membership grade in three fuzzy sets assessing at what extent the reliability factor can be considered high, medium or low. Figure 3 shows the shape of these three fuzzy sets, the way they have been used in this work.

This fuzzy model applies Mamdani-type implication rules, with the following fuzzy rules:

IF $\text{max-grade}$ is low AND $\text{max-mismatch}$ is not low
THEN $\text{rel-grade}$ is low

IF $\text{max-grade}$ is high
THEN $\text{rel-grade}$ is high

IF $\text{max-grade}$ is medium
AND $\text{max-mismatch}$ is medium
THEN $\text{rel-grade}$ is medium

For each data sample presented to the system, the three fuzzy rules are fired at different degree, resulting in three different membership values for $\text{rel-grade}$ in the three fuzzy sets high, medium and low. These values can give a clear idea about the accuracy of the network output. See ref. 9 for a deep explanation of Mamdani fuzzy models.

![Figure 2. The reliability fuzzy model](image-url)
5. RESULTS

The training dataset used to test the model was composed of 12000 samples and 14 signals. The model has been trained in normal operation conditions, varying from 105% power to 30%.

Noise and sensor faults have been added to the sample patterns, for training purposes. The training algorithms, the fuzzy and possibilistic classifiers, the neural network recall algorithm and the fuzzy model have been developed using the software package MATLAB 5.0

Table 1 shows the 14 input signals selected for the test, and Fig 2 the position of the sensors in the plant.

The training of the classifier resulted in the definition of 15 clusters and 15 corresponding ANN. The number of hidden nodes in the three layers have been calculated for each ANN, considering the number of patterns in each cluster.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Core neutronic power</td>
</tr>
<tr>
<td>2</td>
<td>Reactivity compensation control rods</td>
</tr>
<tr>
<td>3</td>
<td>Temperature compensation control rods</td>
</tr>
<tr>
<td>4</td>
<td>Primary loop average temperature</td>
</tr>
<tr>
<td>5</td>
<td>Pressurizer pressure</td>
</tr>
<tr>
<td>6</td>
<td>Pressurizer level</td>
</tr>
<tr>
<td>7</td>
<td>Steam generator level</td>
</tr>
<tr>
<td>8</td>
<td>Feedwater flow</td>
</tr>
<tr>
<td>9</td>
<td>Steam flow</td>
</tr>
<tr>
<td>10</td>
<td>Power setpoint</td>
</tr>
<tr>
<td>11</td>
<td>Steam generator pressure</td>
</tr>
<tr>
<td>12</td>
<td>Pressurizer heaters power</td>
</tr>
<tr>
<td>13</td>
<td>CVCS input/output flow balance</td>
</tr>
<tr>
<td>14</td>
<td>Reactor boron concentration</td>
</tr>
</tbody>
</table>

Table 1. The signals used in the validation test
Three tests have been built, in variable plant conditions and simulating one or more sensor failures. Another test was prepared simulating process failures not known to the model (because completely absent in the training dataset), to test the reliability assessment capability of the model. The nature and location of the failures (the training and test datasets have been prepared by CEA at Cadarache) were not known to the people involved in the tests at Halden, so that no model fitting has been possible. Model parameters tuning has been performed taking into consideration only the training set and the general process dynamics.

The four tests were as follows:

Test 1:
- **Plant condition:** constant power (100% of rated), plant in steady state for 4000 sec
- **Failure modes:**
  1) Coolant temperature noise (10 °C peak to peak) at about 3000 sec from start
  2) Pressurizer pressure drift down at -0.7°C/hr, starting at 1000 sec
  3) Steam generator level drop from 45% to 43% in one step, at 2000 sec

Test 2:
- **Plant condition:** Power decreasing from 100% to 50% in about 1 hour, then steady state
- **Failure modes:**
  1) Coolant temperature drifts up at +1.7°C/hr, starting at 5600 sec
  2) Neutron power drops 4% (constant error), at 7000 sec
  3) Steam generator level drifts up at 7.2 %/hr, starting at 10000 sec

Test 3:
- **Plant condition:** Small power changes, from 102% to 95%
- **Failure modes:**
  1) Pressurizer level drifts down at 3.6 %/hr, starting at 400 sec

Test 4:
- **Plant conditions:** The same as in Test 3
- **Failure modes:** Leakage in the pressurizer

The plots in the following pages show the results of these tests. The error bands in the mismatch plots are calculated by the models according to the expected system accuracy and should be interpreted as follows:

**First band:** It is set at 2 standard deviations of the expected error. Exceeding this band is considered a first warning, especially if the situation persists.

**Second band:** It is set at 4 standard deviations. Exceeding this band is considered a definitive alert signal.

From the analysis of the plots, it can be seen that the model was able to detect the abnormalities in the first 3 tests, providing also a good estimation of the right values for the failed sensors. In particular:

**Test 1:**
- Failure n.1 has been immediately detected, with the second band tolerance at +/-0.2°C
- Failure n. 2 has been detected after 1000 sec, when the drift was -0.2 bar (second band)
- Failure n.3 has been immediately detected
All the remaining signals were confirmed (well within the first error band), and the reliability flag was always set to high.

Test 2:
Failure n.1 has been detected after 400 sec, when the drift was +0.2 C
Failure n.2 has been immediately detected
Failure n.3 has been detected after few seconds, considering the high rate of drift
All the other signals were confirmed, at high reliability.

Test 3:
Failure n.1 has been detected after 600 sec, when the drift was -0.6%
All the other signals were confirmed, at high reliability.

As expected, the model was not able to recover from the failure mode in Test 4, but the reliability flag was correctly set to low at the beginning of the unknown failure.

6. CONCLUSIONS

The tests performed on the Neuro-Fuzzy model for signal validation, developed at the Halden Reactor Project, show that it can be successfully used to detect multiple sensor failures in PWR’s. In presence of unknown scenarios, the model correctly alerted the user about the impossibility to provide a reasonable diagnosis, avoiding to produce unreliable and dangerous answers.

The capability of the model to operate in accident conditions will be tested in the near future.

7. ACKNOWLEDGEMENTS

This work has been performed under the Joint Programme framework of the Halden Reactor Project. The tests using simulated data from a french PWR have been sponsored by Electricite’ de France (EDF SEPTEN) and prepared by the Centre D’Etudes De Cadarache.
The authors want also to thank Hilary Selmer-Olsen from the Halden Reactor Project, for her continous efforts in the graphic editing of this paper.
Test 2

Core neutronic power (%)

Time (s)

Mismatch (EU units)

Time (s)
Test 2

Coolant avg. temp (°C)

Mismatch (EU units)

Steam gen. level (%)

Mismatch (EU units)
REFERENCES

1. P.F. Fantoni, A. Mazzola, "Multiple-Failure Signal Validation in Nuclear Power Plants Using Artificial Neural Networks", *Nucl. Technol.* (March 1996)


CAMS: A Computerized Accident Management System
for Operator Support during Normal and Abnormal Conditions in
Nuclear Power Plants

by

Paolo F. Fantoni
Aimar Sørenssøn
Geir Mayer

OECD Halden Reactor Project
Halden, Norway

Abstract

CAMS (Computerised Accident Management Support) is a system that provides assistance to the staff in a nuclear power plant control room, in the technical support centre and in the national safety centre. Support is offered in identification of the current plant state, in assessment of the future development of the accident and in planning mitigation strategies.

CAMS is a modular system, where several modules perform different tasks under the control and supervision of a central knowledge based system, which is responsible for the synchronisation and the flow of information through the activated modules.

A CAMS prototype has been tested by the Swedish Nuclear Inspectorate during a safety exercise in Sweden in 1995, with satisfactory results.

Future developments include automatic control of the Predictive Simulator by the State Identification, for the generation of possible mitigation strategies, and the development of an improved user interface which considers the integration of the system in an advanced control room.

CAMS is a system developed as a joint research activity at the Halden Reactor Project in close cooperation with member organizations. The project, started in 1993, has now arrived to the second prototype version, which has been presented and demonstrated at several seminars and workshops around the world.

1. INTRODUCTION

CAMS (Computerized Accident Management Support) is a system that will provide support in normal states as well as in accident states. Support is offered in identification of the plant state, in assessment of the future development of the accident, and in planning of accident mitigation strategies. (It does not give support in execution of the chosen mitigation strategy.)

We imagine different types of users: operators and shift leaders in the control room, the staff in the technical support centre (TSC), and people in the national safety authorities. These different types of users need different types of support.

CAMS picks up information from the plant and transforms it into a more digestible form before presenting it to the users. This transformation process can be controlled by the user.
CAMS consists of a data acquisition module (DA), a signal-validation module (SV), a tracking simulator (TS), a predictive simulator (PS), a state-identification module (SI), a probabilistic safety assessment module (PSA), and a man-machine interface module (MMI). The work of these modules is coordinated by a module called the system manager (SM). In addition, there are the strategy generator (SG) and the critical function monitor (CFM), these two are not integrated into the present version of CAMS.

The purpose of the prototype is to study how advanced information techniques can be utilized efficiently in accident management. Various methods are tested. The possibilities and also the difficulties of the chosen design are evaluated.

The design of the first CAMS prototype has been described in an earlier report, HWR-390, Reference [1]. Since then several pieces of work have been done:

- CAMS has been tested at a safety exercise at the Swedish Nuclear Inspectorate in May 1995. This work has been reported in a joint paper between staff from the Swedish Nuclear Inspectorate and staff from the HRP, Reference [2]. The main conclusion was that CAMS was useful already in the incomplete form that it had at that time, and that it had room for improvement and extension.

- A lessons-learned report has been written, Reference [3], about on-line simulation and estimation, to review ideas that can be used in CAMS. Some of these ideas have been used in the TS.

Since the design reported in Reference [1], the prototype has been expanded in several ways:

- A special data acquisition module has been added, making it easier to couple CAMS to any data source, be it a plant or a simulator.

- The SV used an approach with a single neural network, and this module had not been integrated into the prototype. Now it has been expanded into an approach using combination of fuzzy logic and neural networks, and this expanded SV has been integrated into the prototype.

- The TS has been added to the system. The tracking is made by adjustment of parameters rather than of variables, using a least-squares criterion.

- In addition to the version describing the plant Forsmark-2, a version for another plant, the Barsebäck-1, has also been made. It is, however, the Forsmark-2 version which has been integrated into the present prototype.

- The SI, which existed only in a rather rudimentary form in the previous prototype, has been expanded and integrated into the prototype.

- A PSA module has been written and integrated into the prototype.

- New pictures have been added to exploit the new modules; SV, SI and PSA. The new and improved trend system of Picasso-3 version 2.0 has been taken into use and all the supporting programs use the new application program interface.

- As the prototype now contains a large number of modules, a SM has been added to coordinate the other modules.

- Emphasis has been placed on making a general design and structure facilitating easy maintenance and adaption to different reactor types. Although specific plant knowledge is implemented inside each module, it should not be necessary to rearrange the whole design when changing to another plant.

The present prototype has been made for a boiling-water reactor, but the possibility of making a version for pressurized-water reactors will be investigated.

This report will concentrate on the prototype as it is today, its various modules, and how they work together.
2. THE STRUCTURE OF CAMS

Figure 1 shows the main modules of CAMS and the data flow between them.

First we note that CAMS is an information system, data flows from the plant to the user. You can influence what goes on in the modules close to the Man-Machine Interface, but you cannot operate the plant through CAMS.

The plant data are picked up by the Data Acquisition module (DA). From there they flow to the Signal Validation module (SV). Validated data flow to the Tracking Simulator (TS) and to the State Identification module (SI). The TS augments the measurements with three sorts of extra data:

- data which the user should like to know, but which are not measured,
- data that are used for initialization of the predictive simulator, but which are not measured, and
- data that are measured, but which also can be calculated from independent measurements.

In the latter case the TS acts as the calculation assistant of the SV. The cooperation between the SV and the TS is indicated by the double arrow between them.

From the TS, validated and augmented data are available to any module that may request it. In addition to the SV already mentioned, the main customers for such data are the Man-Machine Interface (MMI) and Predictive Simulator (PS). When requested by the user, the PS will pick up the current state from the TS. The PS may be asked to predict what will happen if no intervention is carried out, or if a certain sequence of interventions is carried out.

The SI produce qualitative information about the plant state: there is or is not a leakage, a component is or is not available, etc. This information is communicated to the user by the MMI. It is also the starting point for the analyses done by the Probabilistic Safety Assessment module (PSA), the Strategy Generator module (SG), and the Critical Function Monitor (CFM).

As indicated, the SG and the CFM have not been integrated into the present version of the prototype.

Data from all these modules flow to the Man-Machine Interface (MMI) to be examined by the user. The user can control the data transformation going on in the PS, PSA, etc., this is indicated by the arrows going backwards from the MMI to these modules.
3. **THE SYSTEM MANAGER (SM)**

3.1 **Purpose**

The SM (which is not shown in Figure 1) is the common functional interface to all the CAMS modules. The main tasks performed here are:

- **Functional linking:** All the modules communicate with each other only through the SM.
- **Synchronization:** Activity in different modules must be synchronized to produce meaningful outputs. This is particularly true in this system where the modules operate concurrently.
- **Switching:** Every module can be switched on and off without limiting the operation of other modules.
- **Monitoring:** The SM controls the activity and the flow of information through all the modules. A dedicated SM display has been designed, to be used by the CAMS supervisor on site.
The SM has been developed using the real-time expert system shell G2, by Gensys Corp., Reference [5].

3.2 Description

Figure 3 shows the logical connections among the CAMS modules and the SM. External processes (external to G2) used by each module to perform a task, are represented in circles. In this diagram the modular nature of CAMS is emphasized: each functional module has the same structure and all of them work concurrently under the supervision and coordination of the SM. Basically, each module has the following building blocks:

- an external process, performing the main task (for example a Picasso-3 process for the MMI module)
- a G2 module, that drives the external application and receives the results,
- a communication block (dac, svc,...), which contains the data that must be shared with the SM.

Figure 4 shows one possible display from the SM console. Here the Data Acquisition main controls have been selected.
Figure 4. The System Manager console
4. THE DATA ACQUISITION MODULE (DA)

4.1 Purpose

This module operates as an interface between the CAMS and the monitored process. The main requirement in the development of the DA module was to avoid any dependency of other CAMS modules of the external data source, with only a few exceptions.

4.2 Description

Figure 5 shows how the DA module is connected to the rest of the system. A description of the blocks comprising the DA process follows:

![Diagram of DA logical diagram]

Figure 5. DA logical diagram

4.2.1 DA core

This is where the plant signals are acquired and stored to be processed on demand. At any time the last $N$ samples are available for each signal. The length $N$ of the memory can be adjusted.

Two additional functions are present in this block, to be used for test and training purposes:

- The noise simulator. It is used to add random Gaussian noise, at an adjustable level, to one or more incoming signals.
- The fault simulator. It is used to simulate drifts or failures in a limited set of signals.

This block has been implemented G2.

4.2.2 Configuration

This block contains information on the number, type and characteristics of the process (the plant). Noise detection flag. To be used for detecting stuck signals. The configuration block has been implemented in G2.

4.2.3 DA comm

This block handles the information to be exchanged with the System Manager. A block like this exists in all the CAMS modules, to identify the link between each module and the SM. No link exists between DA and any other module in CAMS, except SM (the Bridge block is an exception).
This block is implemented in G2.

4.2.4 DA bridge

This is a direct link from the plant to the Picasso-3 display. It is used to update the display with information not relevant for other CAMS modules. This block might be removed in the future, because it is not consistent with the module-isolation concept that is the basis of the current CAMS design.

4.2.5 DA-GSI Interface

This is the software interface between the plant and the G2 process where DA has been implemented. A block like this exists in all the modules where there is a need to interface external processes.

5. THE SIGNAL VALIDATION MODULE (SV)

5.1 Purpose

The Signal Validation module (SV) in CAMS is currently based on neuro-fuzzy techniques. The complete algorithm and procedure can be found in Reference [12]. Currently, a set of reactor safety related signals has been used in the SV module (see Table I) but the same design can be applied concurrently to other sets of process signals.

<table>
<thead>
<tr>
<th>Sensor name</th>
<th>Range</th>
<th>Validated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core power</td>
<td>0-100%</td>
<td>Yes</td>
</tr>
<tr>
<td>Control rods position</td>
<td>0-3.65 m</td>
<td>No</td>
</tr>
<tr>
<td>Core flow</td>
<td>0-10500 kg/s</td>
<td>Yes</td>
</tr>
<tr>
<td>Core pressure</td>
<td>0-7 MPa</td>
<td>Yes</td>
</tr>
<tr>
<td>Feedwater flow</td>
<td>0-1500 kg/s</td>
<td>Yes</td>
</tr>
<tr>
<td>Steam flow</td>
<td>0-1500 kg/s</td>
<td>Yes</td>
</tr>
<tr>
<td>Feedwater temperature</td>
<td>0-170 °C</td>
<td>Yes</td>
</tr>
<tr>
<td>Control valves position</td>
<td>0-100%</td>
<td>No</td>
</tr>
<tr>
<td>Bypass valves position</td>
<td>0-100%</td>
<td>No</td>
</tr>
</tbody>
</table>

Table I. Signals used in the validation model

5.2 Description

Figure 6 shows a simplified diagram of the neuro-fuzzy model. The possibilistic fuzzy classifier is used to identify one or more possible regions of the process operating point (as defined by the set of signals to be validated), to which the incoming sample could belong. The possibilistic nature of this classifier results in a prompt detection of patterns outside the module training volume (which can introduce unacceptable errors in the neural networks response).
The neural networks (ANN) have been trained, each in a different region, in the set of the possible regions identified by the classifier. They work concurrently during the validation process and their output is averaged using the fuzzy membership value of the incoming pattern in each cluster (region). In this implementation, seven clusters have been identified, which cover the entire power-flow map of the reactor.

6. THE TRACKING SIMULATOR (TS)

6.1 Purpose

The purpose of the TS (Tracking Simulator) is to calculate:

- Quantities that are not measured, but which the user should like to know.
  Used by: MMI.
- Quantities that are not measured, which are to be used as initial values when predicting what will happen.
  Used by: PS.
- Quantities that are measured, but which can also be calculated from other independent measurements.
  Used by: SV.

6.2 Requirements

For this prototype, the required estimates are:

- Cladding temperature,
- Relief valve flow,
- Steam leakage inside the containment,
- Water leakage inside the containment.
More requirements may be added to this list later, for instance:

- Water level in the reactor tank (for the SV).
- Steam leakage outside the containment,
- Water leakage outside the containment.

Further, some estimates may be available at no extra cost.

6.3 Description

There are several tools available for building simulators, but they all appear to be made for building predictive estimators, rather than tracking ones. The facilities they offer are essentially this:

They have a set of ready-made components like pipes, valves, pumps, turbines, reactors and so on. You can describe the components of your plant by giving parameters to these ready-mades. I have a pipe, you say, the tool gives you its pipe component and ask you to describe your pipe. Its length is this, you say, and its diameter is that.

You then describe the topology of your plant. The water running out of this tank runs into the pipe, the water running out of the pipe runs into that valve. The modelling tool will establish and solve the corresponding algebraic equations.

Finally you give the initial conditions of your plant and ask what the situation will be a certain time from now. The tool will establish and solve the corresponding differential equations.

No suitable tool for making tracking simulator seems to be available on the market. How can we turn a predictive simulator into a tracking simulator? What we want is an estimation tool. And estimation has a mathematical relationship to prediction.

We receive new measurement data at regular intervals \( t = k \Delta t \). But not all the interesting state variables are measured. We arrange all measured variables \( y_1, y_2, \ldots, y_L \) into a vector \( y \), an arbitrary one of these measured variables is denoted by \( y_l \). Similarly, we arrange all non-measured variables \( z_1, z_2, \ldots, z_M \) into a vector \( z \), an arbitrary one of these non-measured variables is denoted by \( z_m \). Finally, all parameters \( p_1, p_2, \ldots, p_N \) that shall be updated are arranged into a vector \( p \), an arbitrary parameter is denoted \( p_n \). The complete state vector \( x \) is then the collection of all these:

\[
    x = \begin{bmatrix} y \\ z \\ p \end{bmatrix}.
\]  

Here, \( 1 \leq l \leq L \), \( 1 \leq m \leq M \), and \( 1 \leq n \leq N \). The number of adjustable parameters \( N \) should preferably be much smaller than the number of measurements \( L \).

Non-measured and measured variables are for instance temperatures, pressures, positions, velocities, quantities for which we can establish equations describing the main part of their development with time, even though our knowledge is never precise.

Parameters are quantities that normally do not change, or at least change only slowly, like lengths and cross sections of pipes, the thicknesses of steel walls and electric resistances. The existence or non-existence of a leakage also is included in this category. These latter things, which we often call "constants", may also change, but we are not able to predict how, or we decide not to do so even if we could. We shall assume that a parameter does not jump wildly around, it displays some sort of continuity. Rather than making the parameter directly a Gaussian stochastic variable, we make its change between one measurement and the next a Gaussian stochastic variable. This does not mean that parameters cannot change, only that we cannot predict how it will change. The entire time development of these quantities is described by a noise term.
The classification into variables and parameters is not always obvious. If we for example enlarge our description of flow phenomena to also include the corrosion of a steel pipe, and establish equations for the change of the wall thickness with time, the wall thickness will be a variable rather than a parameter.

Given initial values for estimates of $y$, $z$ and $p$, a prediction tool can tell you the corresponding estimates one time interval later. The $p$'s are trivial, of course, as the prediction will be that they have not changed.

Then the measurements at $t = (k + 1)\Delta t$ arrive, and we have new values for the $y$'s. They will be similar to the estimated $y$'s, but not identical. The differences between measurements and estimates are called residuals or innovations and they are denoted by $r$. They represent what we have learnt by the measurements, the amount of surprise. We can use them to improve our estimates of the measured variables $y$, the unmeasured variables $z$, and the parameters $p$.

In each time interval the state vector is therefore changed twice, by the equations of motion which are handled by the prediction tool, and the updates based on the residuals. This is illustrated in Figure 7.

Figure 7. The state vector is modified alternatively by the equation of motion and the update equation. The update equation is fed from the residual equation.

7. THE STATE IDENTIFICATION MODULE (SI)

7.1 Purpose

The purpose of the State Identification (SI) module is to identify the state of the plant and to communicate information to the user and to other CAMS modules. In the current version, the outputs of the SI module are the following
• output to the user: textual information describing the plant state, status of critical safety functions and availability of safety systems (see the MMI chapter for more details),

• output to the TS: presence of a steam or water leakage inside or outside the containment and the occurrence of steam release through relief valves,

• output to the PSA: the occurrence of initiating events and the availability of front-line and support systems.

7.2 Description

The state identification module is a knowledge based system with the classical main components: a knowledge base and an inference engine. It is developed using a specific tool: GPS (Goal Planning System, Reference [8]) which provides the inference engine and the knowledge-acquisition tool.

7.2.1 The knowledge base

The current knowledge base contains 3 parts:

1. Safety objective trees

State Identification is based on Safety objective trees as defined by the NRC, Reference [13]. The safety objective trees identify the relationships between plant safety objectives, challenges to the safety objectives, mechanisms that cause the challenges and strategies that would mitigate or prevent the mechanisms using a hierarchical tree structure. We have chosen to represent safety objective trees, from the safety objective level to the mechanism level. The strategy level will be the purpose of the future SG module.
So far, we have implemented the trees related to the following safety objectives:

- prevent core damage,
- maintain containment integrity.

2. Leakage detection and steam release

The current knowledge base only detects leakage inside the containment by monitoring the evolution of the containment pressure and temperature and the water level in the reactor vessel.

Steam release through relief valves is monitored by checking the position of the relief valves but also the temperature in steam relief lines to prevent errors due to wrong information about the position of the relief valves.

3. Safety systems availability and initiating events

The safety systems monitored by the SI module are automatically started under given plant conditions. When the starting conditions of a safety system are fulfilled, the SI module checks if the system is really working and if not, it tries to identify the reason why the system does not work.

For example, when the starting conditions for the low pressure cooling system are met, the flows in the low pressure cooling lines are checked. If there is no flow, the system is declared unavaila-
ble. Then the speed of the pumps and the position of the related valves are verified and the user is informed of abnormal situations.

The considered initiating events are LOCA of different sizes (large, medium, small), manual or automatic shutdown of the reactor and loss of important functions like heat sink, feedwater or external power. The occurrence of these events is already detected in the previously described parts of the knowledge base. The information is transmitted to the user and to the PSA module.

8. THE PREDICTIVE SIMULATOR (PS)

8.1 Purpose

The purpose of the Predictive Simulator is to tell the CAMS user what the future state of the plant will be, by running a model of the plant faster than real time. In the case of an accident, the user will see if the safety systems of the plant are sufficient as the accident evolves, or if some interference is needed to reach a safe state. If a safe state cannot be reached, the simulator will give indication of when the plant reaches a critical state.

When the user wants to run a prediction, he will initialize the simulator with the current state of the plant (which is a major task of the Tracking Simulator). The user can then let the simulator run by itself to see what will happen if no mitigation strategy is tried, or by manipulating the controls of the simulator he can test different strategies to see which effect they have and choose the better one.

The simulator can also be used to check what might happen before it happens (if ever). Say, we have lost all auxiliary feedwater pumps but one. If the last one should also fail, how much time do we have before the core is uncovered? With this information the user can be prepared if so should happen (this sequence of events happened at the safety exercise at the Swedish Nuclear Inspectorate in May 1995, see Reference [2]).

8.2 Description

No modules use the output from the simulator. The output goes directly to the relevant predictor pictures and the trend system within Picasso-3. But the control of the simulator goes through the System Manager. In this way the System Manager knows the commands to the simulator, without being loaded with all the display data.

Operating the simulator is done using three pictures, “Predictor Control”, “Predictor Panel” and “Predictor Setup”.

“Predictor Control” is similar to the process picture, which gives an overview of the process, regarding layout and placement of components. This has been done so that the user will recognize and be familiar with the picture during an accident. There is one important difference; in “Predictor Control” one can control the Predictive simulator. This is done using a mimic style interface where one can point and click on components. A small window will pop up and the state of that component can be modified (a pump can be started, a valve opened etc.).

“Predictor Panel” has a more traditional layout with buttons and sliders to mimic what operators are used to from the control room. This layout gives a more detailed control of the systems in the plant, like manual scram and suppression pool cooling.

“Predictor Setup” is used to start, stop and initialize the predictor. Start and stop are self-explanatory, and initialize is used to make the predictor reflect the state of the plant. Normally initializing will be activated when the plant has changed its state, or when the user wants to try a new mitigation strategy. It is not necessary to stop the predictor to control and modify components, it can be done while running.
9. THE PROBABILISTIC SAFETY ASSESSMENT MODULE (PSA)

9.1 Purpose

The purpose of this PSA module is to provide on-line accident prevention and mitigation strategies for a nuclear power plant (NPP) as one module of the CAMS (Computerized Accident Management Support).

9.2 Description

This module contains plant specific PSA data, comprising event trees, failure probabilities etc. It has several event trees categorized according to the initiating events (IEs). Each event tree has an initiating event frequency and a branching probability. The various support systems for branches are considered and their dependencies are calculated logically.

The risk or Core Damage Frequency (CDF) is re-calculated based on the current state of the plant and the pre-calculated level 1 PSA. The CDF is relatively low when the plant is operating normally. However, if a component or a system becomes unavailable for one reason or another, say failure or maintenance, the failure probability is changed and the current risk is re-calculated and displayed. This function can be activated by data from the state identification (SI) module of CAMS.

If an initiating event occurs, the event tree is re-calculated and the PSA module shows which systems of the plant that should operate normally. If the plant responds to the event in the normal way, the plant will be shut down and come to a safe state. However, if some functions do not work, the PSA module generates another path and gives the information about the critical systems to the Strategy Generator (SG) module. The new path is checked by the SG and if the state of the plant is changed, either by the operators or automatically by the control system, the PSA module follows the new route.

9.3 Functions of the PSA module

The PSA module calculates the core damage frequency using the latest status of the plant periodically (the period is 10 seconds now). The status of each safety functions is obtained from the SI module. The module has a calculation part implemented in the C++ language and a display part made with Picasso-3. The user can interact with the module, i.e. the system status can be modified temporarily. However, the data from the SI override the user input.

10. CONCLUSION

This report shows the actual status of the CAMS project. The first phase of the project (1992 - 94), which is described in Reference[1], [2], and [3], focused mainly on the following tasks:

- information needs during normal and accident conditions in a NPP,
- methods that can be successfully applied to a CAMS system,
- MMI and human factors requirements.

In the second phase of the project the development of those ideas into a working prototype has begun. Its main purpose is to test those methods in a simulated environment, to verify that the many developed functions, using different techniques, can work together producing the desired result in an efficient way. In other words, this prototype can be considered a test platform to do the following:

- Develop and integrate modules like Tracking Simulator, Signal Validation, State Identification, PSA, and Predictive Simulator. Evaluate how each task is performed, and identify advantages and drawbacks in the methods used.
• Design a functional structure able to coordinate and synchronize the activities that take place in all those modules. The overall output of the CAMS system should then be able to satisfy the information needs requirement mentioned above.

• Design and test an appropriate user interface for different kinds of users, with different needs and knowledge.

During the CAMS design, a considerable effort has been made to maintain the generality of the CAMS concept; although the referenced process has so far been a BWR plant, the use of this structure and design can be applied to other processes, including non-nuclear processes. An important feature of the system, in this respect, is that all the functions or modules (TS, SI, SV, etc.) are completely independent of each other and that modules can be deleted, added or changed without affecting the rest of the system. Moreover, the external tools here used (APROS, GPS, Picasso-3, etc.) are just plugged into CAMS, so that other tools can be easily used, depending on the application. This solution is also in line with the “testing platform” concept cited above, where the need to test different solutions for a single module within the general CAMS framework (with other functions turned off) can be anticipated.

11. ACKNOWLEDGEMENT

APROS was received from VTT and IVO (Finland). They have also provided excellent support. A large amount of PSA data for the Forsmark-2 plant was received from Forsmarks Kraftgrupp and Vattenfall (Sweden). EdF (France) has participated in technical discussions. SKI (The Nuclear Inspectorate, Sweden) has provided data for the Barsebäck plant, and they provided staff to evaluate the predictive part of the system. Tractebel (Belgium) has permitted us to use their tool GPS.

We are also grateful to VTT, IVO, PNC (Japan), and Tractebel, who have sent delegates working on the project.

We have also received good help from an advisory group during the early parts of the CAMS project.

12. REFERENCES


[6] APROS has been developed by IVO and VTT in Finland.

A knowledge-based system to support nuclear power plant operators.  

[9] K. A. Barmsnes, A. Hornæs, Ø. Jakobsen, R. Storkås:  
Picasso-3 system design.  

[10] Tord Akerbæk, Michael Louka:  
The software bus, an object-oriented data exchange system.  
HWR-446. Halden, April 1996.

[11] ORBIX is a trademark of IONA Technologies Ltd.


Accident Management Information Needs.  

[14] Yukihiro Iguchi, Masutake Sotsu, Kazutoshi Isomura:  
PSA related activities and an application to the maintenance in Fugen.  
ICONE-3, April 1995, Kyoto, Japan.
EC-SPONSORED RESEARCH ACTIVITIES ON ACCIDENT MANAGEMENT MEASURES

J. Martin Bermejo, European Commission, DGXII/F/5
M. L. Ang, NNC Limited

ABSTRACT

The European Commission (EC) is currently funding, via the 1994-1998 R&D Framework Programme, a number of activities in the field of Nuclear Fission Safety (NFS), and particularly in several areas related to "Reactor Safety/Severe Accidents". This programme continues the research activities of the previous Community Reactor Safety Programme which was carried out as a Reinforced Concerted Action (RCA) during the period 1992-1995.

The group of multipartners projects selected for financial support from the EC under Area B.5.1 of the current NFS Programme, "Supporting Activities / Accident Management Measures" (known as the "AMM" cluster) are basically aiming at implementing the results of severe accident research into practical Accident Management (AM) strategies. The generic objective is to exchange information and to develop a common European approach regarding aspects such as phenomena related uncertainties, possible adverse effects of operator actions on the progression of the accident, interpretation of measurements, equipment performance, instrument survival and human error under stress.

This paper briefly discusses the objectives and achievements of a completed project of the 1992-1995 RCA, known as "Accident Management Support" ("AMS"), and also presents the current status of an ongoing project of the 1994-1998 NFS Programme, "Algorithm support for accident identification and Critical Safety Functions signal validation" ("ASIA").

The objectives of the "AMS" project were (i) to define, investigate and develop means and methods to provide reliable information and diagnostics, as well as support tools for accident management, and (ii) investigate the different signal validation methodologies with emphasis on the existing instrumentation rather than on new instrumentation needs. The work started with the writing of two state-of-the-art reports (SOARs) in these two areas. In parallel to the compilation of the SOARs, and later in a second phase, specific research activities were also conducted for this project.

The activities of the "ASIA" project will extend and build on the work of the "AMS" project mentioned above. In particular, it will further develop operator aids based on physical models in order to validate Critical Safety Functions (CSF) measurements and understanding accident progression by using search algorithms. The instrument survival in severe accident environments expected for PWRs will also be further assessed, in particular for the neutron flux sensors.

These EC-sponsored research projects are proving to be very valuable for the improved understanding of some of the key AM issues mentioned above, and are also contributing to stimulate cooperation among organisations from different EU member states, to avoid duplication of R&D efforts and to use the available resources in an efficient way. The area of AM support can be considered one of the most promising R&D fields in which effective solutions can be reached with reasonable efforts and in a realistic timeframe.

1. INTRODUCTION

Nowadays in many countries of the European Union (EU) the ultimate goal of nuclear reactor safety experts is to render "practically" unnecessary extensive evacuation precautions for populations in the site vicinity. This means essentially developing safety systems and procedures to respond to the challenge of the hypothetical severe accidents, which are beyond-design-basis events, assuming that the accident prevention measures have failed.
The subject of severe accidents in light water reactors (LWRs) is usually so complex to understand and the investigations are so expensive, that international research efforts are needed to come to firm conclusions. At the European Commission (EC), two programmes were focused on the understanding of the physics of beyond-design-basis accidents and on the development of accident management measures for LWRs of both the present and the future generation, namely: the Reinforced Concerted Action (RCA) 1990-1994 and the current EURATOM Framework Programme 1994-1998 on Nuclear Fission Safety.

Throughout the two aforementioned EC research programmes, many aspects of severe accident analysis were addressed, starting from early accident progression in the primary coolant system and extending to severe challenges to the containment integrity, assuming that the safety systems are unavailable or not working satisfactorily. Special emphasis was put on the application of the findings to the development of measures for the mitigation of the consequences of severe accidents.

The goal of Severe Accident Management research is to incorporate the insights and results of severe accident research programmes into practical accident management, by identifying and assessing candidate management strategies. Current research on accident management strategies shows that methods and tools need to be developed for dealing with uncertainties regarding phenomena, possible adverse effects of operator actions, improved instrument survival and reduced error, equipment performance and human error under stress.

Successful accident management includes many tasks related to the use of information technologies, such as reliable identification of the actual plant and components state, information for assessing the accident progression and the plant response to operator action, and information for planning the mitigation strategy with potential uncertainties due to failed or misleading instrumentation. As a result of the fast progress in numerical techniques and the availability of very powerful computer systems with acceptable economic conditions, the area of accident management support is considered nowadays one of the most promising Research and Technological Development (R&TD) fields in which very effective solutions can be reached with reasonable effort and in a realistic time frame.

2. (1990-94) EU RESEARCH PROGRAMME ON REACTOR SAFETY

Under the 3rd Framework Programme for Community Research (1990-1994), the Council of Ministers approved on 28 November 1991 (Decision 91-626/Euratom) a research and education programme on Nuclear Fission Safety with a budget of 36 MECU and a duration up to 31 December 1994. Following a subsequent Council Decision the budget was increased by 21 MECU and the programme was extended till 30 June 1995. The programme had two activity fields, one on Radiation Protection and one on Reactor Safety, with a funding of 42 MECU and 15 MECU, respectively.

The research on Reactor Safety was focused on the understanding of scenarios and phenomena of beyond design-basis-accidents (beyond DBA) and on the development of accident management measures for LWRs of both the present and the future generation. It was executed as a "Reinforced Concerted Action" (RCA), in which the EC contribution to the different projects was around 20% of their total value.

Special emphasis was put on the application of this research programme to the development of measures for the mitigation of the consequences of severe accidents in LWRs, mostly of the evolutionary type in Western Europe, in the hypothetical case that the accident prevention measures fail. The attention was focused on conducting separate effects tests as well as large integral experiments of common interest to provide a database against which numerical codes could be validated in view of the extrapolation towards the real reactor situation.

This research programme was conducted through a 2.5 years joint effort from the end of 1992 till early 1995 and involved 20 contracting organisations coming from 9 EU member states, in co-operation with some Central- and East-European research organisations. A wide spectrum of severe accident scenarios and phenomena have been investigated both from an experimental and an analytical point of view. The work programme addressed 3 main areas, namely accident progression, containment integrity and accident management support, and was subdivided into 8 projects. The final report of this programme covering the outcome of all 8 projects has been published as a EUR report [1]. The project No 8 of this programme, known as "Accident Management Support" ("AMS") addressed mainly, signal validation under extreme accidental conditions and development of improved man-machine interfaces in advanced nuclear power plant control rooms with a view on new strategies for accident management support. A brief description of this project as well as the most relevant results and conclusions is presented in section 4 of this paper.

3. THE 1994-1998 EU RESEARCH PROGRAMME ON NUCLEAR FISSION SAFETY

The European Union (EU), via a Council Decision of April 26th 1994, adopted a EURATOM Multiannual Programme for Community activities in the field of Nuclear Fission Safety (NFS) R&TD for the period 1994 to 1998. This programme consists of five main activity areas:

Area A. Exploring Innovative Approaches
Area B. Reactor Safety
Area C. Radioactive Waste Management, Disposal and Decommissioning
Area D. Radiological Impact on Man and the Environment
Area E. Mastering Events of the Past

This Programme is being implemented either via direct actions under the responsibility of the Joint Research Centre (JRC) of the EC, or via indirect actions co-ordinated by units F-5 and F-6 of Directorate General XII of the European Commission (EC). The latter are structured around a limited number of significant projects which were selected by the EC and a group of independent experts with the aim to stimulate co-operation among public and private organisations of different Member States, to avoid unnecessary duplication efforts and to use the available resources in an efficient way.

Most of these projects are essentially carried out through "shared cost" actions, for which the EC contribution is up to 50% of the total project costs. A small part of the programme, though, is carried out through "concerted" actions whose objectives are the exchange of information, on some critical R&T&D issues, or the development of a consensus on specific problems of common interest. For the concerted actions the EC reimburses only co-ordination costs, such as travel and living expenses, meetings, etc.

The research activities of Area B ("Reactor Safety") of this programme continued those of the 1992-95 RCA mentioned in the above section. They are structured into 6 clusters, each containing several projects. As shown in Table 1:

<table>
<thead>
<tr>
<th>Cluster Acronym</th>
<th>Field of Research</th>
<th>Number of Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>INV</td>
<td>In-vessel core Degradation and coolability</td>
<td>8</td>
</tr>
<tr>
<td>EXV</td>
<td>Ex-vessel Corium behaviour and coolability</td>
<td>4</td>
</tr>
<tr>
<td>ST</td>
<td>Source Term</td>
<td>10</td>
</tr>
<tr>
<td>CONT</td>
<td>Containment Performance and Energetic Containment Threats</td>
<td>8</td>
</tr>
<tr>
<td>AMM</td>
<td>Accident Management Measures</td>
<td>5</td>
</tr>
<tr>
<td>AGE</td>
<td>Ageing</td>
<td>7</td>
</tr>
</tbody>
</table>

At present, the "AMM" cluster is composed of five different projects. Only two of these projects are dealing strictly with Accident Management related measures. Their acronyms are "SAMEM" and "ASIA".

The SAMEM project has, as its main objectives, to develop integrated Accident Management (AM) models for the assessment of the feasibility and effectiveness on potential severe accident management measures.

The survival potential of instruments needed for Critical Safety Functions monitoring and the use of algorithms for processing plant measurements in order to allow accident identification and signal validation on PWRs will be addressed in the ASIA project. Details of this project are presented in section 5 of this paper.

4. THE "AMS" PROJECT

The acronym "AMS" stands for "Accident Management Support". This project was the result of the combination of two originally envisaged projects of the 1990-1994 Research Programme, namely "Instrumentation and Signal Validation" and "Operator Assistance". The project started in June 1993, and was carried out as a "Reinforced Concerted Action" (RCA) during a period of 25 months. The co-ordinator of the multi-partner team was GRS/ISTec (Germany). The other organisations involved were: Ansaldo (Italy), NNC (GB), CEA (France), FRAMATOME (France), SIEMENS (Germany), ECN (Netherlands) and TRACTEBEL (Belgium).

4.1. Objectives and Scope

The general objectives of this project were (i) to define, investigate and develop means and methods providing reliable information and diagnostics as well as support tools for accident management, and (ii) investigate the different signal validation methodologies with emphasis on the existing instrumentation rather than new instrumentation needs. The basic scope of this project was:

1. To carry out investigations about real-time monitoring and decision-making techniques, using neural networks, advanced modelling and noise analysis techniques. Expert system based strategies were further developed for design and maintenance of emergency guideline in connection with an "automatic operator model". Adaptative algorithms and extrapolations from recorded plant data have been developed with the aim of predicting critical milestones and optimising command/control under emergency conditions such as to enable the operator to take the optimal recovery actions in response to an accident.

2. To conduct investigations in signal validation methodology and sensor modelling/signal processing. There are two basic approaches to match the requirements of reliability and validity of a plant
signal: model-based methods realizing functional redundancy and noise diagnostic methods, using the signatures of inherent signal noise as "finger prints" of specific sensors and plant conditions. Sensor modelling activities were performed for a fission chamber model in an extended range of faulty operating conditions. Noise diagnostic methods were developed using advanced signal identification techniques.

4.2. Technical Work Content

Following the procedure in the other RCA projects the work was started with writing state-of-the-art reports (SOARs) in the two main areas: Instrumentation/Signal Validation and Operator Support Systems. In parallel to the compilation of the SOARs and later in a second phase of the project, new work has been performed with respect to developments of advanced signal validation methods, new tools and systems for operator support, and investigation of human-machine aspects with emphasis on the operators' role in a highly computerised environment. All these tasks were structured as described in the following sections.

The work performed and the results of the different contributions of the partners to the AMS project are documented in detail in two state of the art reports [2] [3] and in three full papers [4] - [6] presented during the FISA-95 Symposium on "EU research on Severe Accidents" held in Luxembourg from 22-24 November 1995. This symposium was organised in order to publish the results of the 1990-1994 Fission Reactor Safety Programme of the EC. The FISA papers of the AMS session provide a good insight into the technical results of method and tool developments in both the area of instrumentation/signal validation in accident situations and in the area of operator supporting tools in accident management.

4.2.1. State of the Art Reports (SOARs)

The SOAR on "Instrumentation and Signal Validation in Accident Situations" [2] contains a review of the following topics: Scenarios in Accident Situations, Instrumentation in Accident Management and Signal Validation.

In the section on "Scenarios in Accident Situations", relevant scenarios leading to severe accidents are described in order to illustrate the different types of accident progression that may occur, the potential size of the release to the environment, and the potential accident management measures that may significantly reduce the release. An overview of the existing concepts and practices related to procedures for post-accident operation in several EU member states is also presented.

The section on "Instrumentation in Accident Management" outlines different approaches to determine the required information for accident management, and particularly the methodology developed in the Idaho National Engineering Laboratory, are presented in detail [7]. The Sizewell B plant is used as an example to assess its existing instrumentation and their capabilities, as well as their potential availability and survivability following a severe accident. Finally several alternatives for gaining the required information are briefly discussed, e.g. use of additional sensors, new measuring methods, software aids, etc.

The section on "Signal Validation" presents the evolution and improvement of the methods used in the process industry for signal validation. In particular, the issues related to sensor validation (e.g. measurement systems, electrical range, comparison methods, response time and process noise analysis, etc) are discussed in detail. The application of analytical redundancy methods (or model-based methods) for instrument fault detection and isolation (IFDI), like generation and evaluation of "residuals", are also briefly discussed. Finally a survey of surveillance methods for instruments based on noise analysis techniques, as well as their advantages and disadvantages, is illustrated in detail.

The SOAR on "Operator Assisting Systems for Accident Management" [3] deals with the problem of giving the operators the support needed for accident management (AM), with reference to design basis conditions, beyond design basis conditions and severe accidents. After an introductory chapter, the material of the report is organised as described below, with the main body devoted to a general overview of the present practice and recent developments of operator assisting systems, while the Appendices give more details on specific realisations.

Chapter 2 begins with a general introduction which gives some basic definitions. It also contains a discussion on the operator role during AM and a review of the topics related to severe AM strategies, and a classification of the procedures generally used, with emphasis on possible ways of integrating Severe Accident Management into the "classic" plant procedures. A section illustrates the impact on AM practice of the two last decade's most significant nuclear events (TMI-2 and Chernobyl accidents) on information presentation and procedural guidance. A description of the general basis of integrating accident management and of the interface with emergency planning is also provided.

Chapter 3 presents a review of the different national development of AM procedures and related assisting systems. It includes the present AM situation in France, Germany, United Kingdom, Netherlands, Belgium, Sweden, U.S.A., Japan and Finland. Finally, a comparison of different situations and trends is performed. More complete details of French and German practice are given in appendices A and B of this SOAR.

Chapter 4 is mainly devoted to computerisation of procedures, accident analysis and modelling aids and their
use in AM. Typical requirements and problems arising from computerisation of operating procedures are illustrated. The general state-of-the-art operator aids based on accident analysis codes and models, to be used for diagnosis or prediction both at site and off-site, is presented. Their relevant features and the different modelling methods are discussed. The use of some simple analysis and decision aids in USA, France and Japan is reviewed.

Chapter 5 is devoted to overview, discussion and description of recent developments in computer-based systems in the fields of:

- safety functions monitoring in several Western countries;
- knowledge-based operator support systems (which can include procedures);
- predictive and diagnostic systems based on models

The report finally draws some conclusions, summarising the consolidated design bases for current operator assistance systems, and the basic characteristics and requirements for each to them. A critical review is then performed, concluding with requirements for possible improvements and suggested lines of research.

4.2.2. Description of the research activities

In the second part of the "AMS" Project, specific research activities performed by the partners, was devoted to the investigation of specific tasks, related to two basic topics:

- analysis of the operator role and human-machine interface in an advanced control room environment;
- analysis and development of new tools and computerised systems for operator support in accident situations.

A synthesis of these activities is presented below. For further details, reference is made to the final report of the RCA Programme [1] as well as to the papers [4] - [6] presented at the FISA-95 Symposium.

4.2.2.1. Optimisation of advanced plant operating (ESCRIME)

The aim of the ESCRIME project performed by CEA Cadarache, was to define, for better safety, the optimal share of tasks between operators and computerised operating systems in control rooms, under normal and incident/accident nuclear plant situations. Three main steps were planned in the development of the project, the first of them being the subject of the "AMS" work. The starting point of the research was a thorough analysis of the French PWRs operating procedures which enabled the definition of a unified scheme for both normal and abnormal operation.

A demonstration application was developed on a UNIX workstation. The demonstration included a PWR simulator for normal and accident situations (like breach in primary circuit or SGTR), an interface to permit the operator sending and receiving information and a surveillance module for detection of events which can have consequences on functional objectives. The human-machine interface consists in a sequence of interactive screen images, the chaining of which allows the operator to focus on the current goal by successive orientation steps. All the images are designed on the basis of common principles giving each of them a unified presentation.

4.2.2.2. Ergonomic principles for design of AMS systems

The influence of AMS systems on the operator in highly automated control rooms was investigated by ISTEC/GRS. Compared with classical ergonomic design, ergonomics in AM situations additionally have to consider the dynamics of the situation as well as the requirements of the complex diagnosing and decision making tasks of the operator. These requirements are difficult to be covered, because the tasks in AM situations are complex closed-loop tasks and cannot be handled in classical approaches which cover open-tasks.

A framework was developed that is able to classify the closed-loop tasks of an AM situation by system ergonomic aspects and by the operators' cognitive perception of the AM situation. For the case of severe accidents, the results of the investigation are indicating that it is not enough to provide the operator with several (probably each of them ergonomically well designed) AMS systems. The operator needs an integrated homogeneous Human-Machine Interface which includes the functionality and the models behind the AMS systems but is supporting him in finding the appropriate path through the entire space of possible severe system states.

4.2.2.3. Environment Tool for Development of Accident Management Procedures (DIAM)

Current on-going activities on computerised procedures regard especially knowledge representation formal aspects, Human-Machine interface and procedure life cycle management. This aspects have been investigated in depth by Ansaldo, and partially incorporated in the DIAM prototype.

DIAM has been designed to give the necessary support to procedure designers and users. It can supply support for procedure editing, consultation and maintenance, and regarding merely the topological aspect of procedure design, it assures top quality in terms of clarity in flow diagrams readability, in rules for objects placements and lines routing, and in navigation aids like page structuring, indexing, zooming, and documentation consistency and completeness. As an on line procedure facility, DIAM can allow the procedure text interpretation, assuming that the
procedure text as been written with the DIAM context guided editor and proper signals are supplied.

The development of new procedures (as Accident Management Procedures would be), requires many different checks, and consequent revisions, that could be much more easily handled by a computerised environment like DIAM. A first prototypical version of DIAM has been completed and tested. It incorporates a portion of existing emergency procedures. The testing has been performed with the aid of a simplified plant simulator.

4.2.2.4. Design and Maintenance of emergency guidelines (SAMARIA)

The aim of this FRAMATOME project is to improve the efficiency and the reliability of the design and maintenance of the emergency guidelines with the support of computerised systems. The application was implemented with procedures based on the French approach for their PWR plants.

The software relies on an object oriented approach, OMT (Object Modelling Technique). OMT covers analysis, design and development stages in a traditional software life cycle and draws up the operating strategy. One strategy is composed of tests and modules which are themselves composed of tests and actions. Each strategy is represented by a flow chart.

The software architecture is based on a client-server mode composed of a Graphical Editor Module which allow the user to define the objects and of an Information Management Module for data handling and manipulation. The system has been developed on a UNIX environment. Three different operational modes are at the user disposal: "design", "maintenance" and "edition".

4.2.2.5. Transient Analyser for Accident State Assessment (TRANSAL)

The TRANSAL system was developed by FRAMATOME within the "AMS" project framework. It continued the previous developments of computerised thermal hydraulic tools designed to support the experts during emergency drills.

TRANSAL is based on automation of human expert reasoning. The analysis of accident processes by a human expert, does not refer to a "high level" or perception or understanding but rather of the elementary rules which associate a cause to an effect. The cause of the perturbation can be identified from the amplitude of the perturbation and the status of the system. An expert uses his experience of accident to carry out an implicit reduction in the cause identification. With thermal hydraulic tool support, the expert can confirm or invalidate his assumptions and provide quantitative information. The rules used by experts constitute the knowledge base which is implemented in TRANSAL.

A user-friendly interface in Windows has been specially developed in object oriented Visual C++ (Microsoft). TRANSAL is designed as a host structure which allows both the description, through the interface, of the characteristics of the plant and the processing of the transient assessment. All data describing the different types of plant, the sensors (name, units, supply, accuracy, linked physical parameter, etc), the thermal hydraulic modelling (capacities, junctions, external "object", link with physical parameters, etc.), the expert rules used by the different modules, the shape and the content of the displayed information are captured through the interface.

4.2.2.6. Recommendations for VDU design and their use in accidents (INTERACT)

NNC investigated Visual Display Unit (VDU) designs and made recommendations on the content, layout and navigation methods. Recommendations for design of displays for touch screen and soft screen display and plant control.

A demonstration method of VDU presentation of Station Operating Instructions (SOIS), called "INTERACT", has also been developed by NNC. It covers the feasibility studies, display investigation and development to simulate soft screen display use for actions to mitigate threats to critical functions during an accident. The intention is to demonstrate rolling displays under control of the operator using simulated touch screen control. The displays take the operator progressively and under direct control through the diagnosis of the severity of the threat to the CSFs, and follow on with presentation of the SOIs for a selected CSF threat and accident.

4.2.2.7. Fast model-based computational tools for assistance in Accident Management (PASS)

Using a set of analytical models, diagnostic and prognostic tools have been developed by GRS to assist the operator in recognising specific abnormal situations and to evaluate the time available for recovery before the plant reaches an undesirable state.

First-level, single-task modules for fast calculation of water and steam properties, computation of decay heat power and integrated power following a reactor shutdown, and computation of the break flow rate have been developed and integrated in an expert system environment. On a higher level, these tools, plant measurement data, and first principle energy and mass balance equations have been combined into physical models to solve the problems of detecting a rupture or leak in the primary circuit (including steam generator tube rupture), evaluation of the break area in the primary circuit and assessment of the dry-out time of steam generators secondary side for various scenarios.
according to the availability of feedwater and/or emergency systems.

The set of problems to be solved and the corresponding simulation modules have been developed, verified against the models used in the plant analyser and integrated into the knowledge base of an expert system shell. The expert system performs analyses of emergency procedures as well as the support of operators during procedures. The integration of the developed modules in procedures provides valuable operator decision support.

4.2.2.8. A decision support system for Containment and release management (CRM)

The acquired knowledge in the research programs on severe accident phenomena cannot readily be applied for decision support in the course of a severe accident. In order to structuring existing information on severe accidents in a suitable format for the staff of the technical support centre in a nuclear power plant or for national emergency centres, ECN developed a Computational Aid (CA) for Containment and Release Management (CRM).

This CA provides beneficial and adverse effects of operator actions and performs predictions of the key events based on simplified engineering methods, and can be easily updated by including new information, should it become available.

The CA developed by ECN took as reference a two-loop PWR (i.e. Borssele) and addressed two different types of information: plant and accidental management. The first one contains mainly the design data as well as precalculated MAAP results. The second type provides aid to maintaining the containment safety functions (i.e., integrity and long term cooling) and to mitigating, the release of radioactive material in the event of containment failure.

4.2.2.9. Situation Related Operator Guidance (SIROG)

The objective of the SIROG concept is to provide an integrated, process-coupled, computerized information source for complex situations with the following features: guidance for normal, upset and accident conditions, detail ranging from overall strategy to step-by-step program; for operating crew in the control room and for the crisis management team; presentation of preplanned procedures and ad-hoc-planning of new strategies; access to reasoning, background information, plant documentation. Special emphasis is placed on the symptom-based accident management approach which will be applied in accident situations when the automated measures after reactor trip do not work in the expected manner and important safety functions of the plant are challenged.

The SIROG concept has been developed under the viewpoint of the existing SIEMENS post-accident management concept. To demonstrate the way in which this would be realized by the means of SIROG, examples of both an event-oriented (Steam Generator Tube Rupture) and a safety function oriented (Criticality Control), emergency operating procedure were implemented in a "rapid" prototype. While the first version of this prototype was implemented on a Macintosh system in order to limit programming efforts, the second version was completely restructured and reimplemented on a UNIX platform in order to bring its performance nearer to what would be required in a real application. Coupling to a plant analyzer allowed to simulate the interaction between the operator and the process.

4.2.2.10. Operator Advisor System for use in Severe Accident (OPA)

The OPA system is a knowledge-based system developed at TRACTEBEL, aimed at supporting the operator crew in disturbed operating conditions. The knowledge base was built upon several emergency procedures of the Doel 1 nuclear power plant and complemented by knowledge resulting from operational experience. An OPA prototype was validated at the Doel 1 training simulator by both operators and instructors, and the possibility to use the OPA system in severe accident conditions has been assessed.

5. THE "ASIA" PROJECT

The acronym "ASIA" stands for "Algorithm Support for Accident Identification and Critical Safety Functions Signal Validation". This project is a "shared-cost" action which started in January 1997, and is being carried out by a multipartner team involving 4 organisations (NNC Ltd, FRAMATOME, CEA, and ECN) under the co-ordination of NNC Ltd. The expected duration of this project is 26 months.

As this project has recently started, this section will briefly describe its objectives as well as the main activities foreseen, the expected output for each of the work packages and the progress made so far.

5.1. Objectives

In the unlikely event of a severe accident, the instruments needed for critical safety function (CSF) monitoring may only survive for a limited period and their performance may also be degraded during this period. As discussed in section 4, this issue was addressed in the earlier CEC Framework Programme [2]. The study focused mainly on two aspects:

- a review of proven and developing methods of signal validation, and
- a review of existing instrumentation and their capabilities

- a review of proven and developing methods of signal validation, and
- a review of existing instrumentation and their capabilities

- a review of proven and developing methods of signal validation, and
- a review of existing instrumentation and their capabilities
In this project, the study is further extended with an objective of developing a methodology to systematically assess the survival potential of selected flux instruments under accident conditions. This uses signal processing techniques first to assess the state of the sensor, second to extract if possible useful information from a possibly failed sensor. The study will also investigate potential improvements in process instrument survival, based on consideration of the environments for representative accident sequences [2].

Another related issue addressed in the earlier CEC Framework Programme concerns the application of computer-based tools used for supporting the operating staff, before and during accidents [3]. The potential of using simple algorithms based on thermal-hydraulic modelling for diagnosis and prognosis in accident situations is illustrated in the development of the TRANSAI system in France (see section 4.2.2.5). This process can also provide signal validation by direct and by analytical redundancy. This use of simple algorithms has also been extended in the deployment of 'computational aids' in Severe Accident Management (SAM) [9]. The application of algorithms for signal validation and accident identification also forms part of this project. An objective for this study is to develop a methodology to systematically identify the key parameters for safety function monitoring and to develop algorithms for selected parameters. The emphasis is on simple algorithms based on engineering principles rather than on sophisticated theoretical models.

The overall aim of this project is to produce strategic recommendations on the method of use and environment of the operator support tools needed. The algorithms and use of the surviving instruments will be integrated into a strategic guide for operations support. The potential safety role of the support given will be identified, for the system developer.

The project is comprised of three work packages and the scope is described in this paper. The paper also provides a discussion on the progress made so far.

5.2. Technical Work Content

The activities of this project have been broken down into three work packages. The following outlines the scope of the three work packages.

5.2.1. Work package 1 - Algorithm development.

Work package 1 concerns further development of operator aids based on physical models. Two specific aspects of application for severe accident conditions are addressed, viz:

(a) validation of Critical Safety Function (CSF) measurements
(b) understanding the accident progression

The work is partly based on an extension of the concept developed by Framatome in the SOAR1 study of severe accident conditions [2]. The Framatome method is based on the Technical Support Centre (TSC) experts reasoning while assessing the validity of information transmitted in the remote TSC. The scientific basis of the CSF signal validation approach of Framatome is, in general terms, that the expert compares values and trends of a set of measurements in order to validate or invalidate the checked value. The process formalises the different types of rules which are explicitly or implicitly used by the experts. The aim of the validations is to transform a set of raw measurements into a global consistent set of physical values; and for faulty or non-measured values, to provide substituted values. The solution of the system of relationships linking measurements is carried out with search algorithms and constraint solving methods. In a second stage, the set of validated values is transmitted to the thermal-hydraulics module which provides analytical redundancy and computes non-measurable information.

The scientific basis of the algorithms for accident understanding can however vary considerably. This is illustrated by the different diagnostic and prognostic tools developed for severe accident management [3], [8], [9]. Depending on the intended application, the tools can vary from simple calculations to more complex computer code calculations. This study provides the framework to allow an appreciation and a demonstration of the different features in the methodologies adopted by the partners to derive mutual benefits.

The approach adopted for this study is as follows:

The study is based on three phases of an accident:

- Phase 1 - initiation of accident until fuel melting (DBA - design limits)
- Phase 2 - fuel melting until failure of Reactor Pressure Vessel (RPV) lower head
- Phase 3 - failure of RPV lower head to severe containment challenge

The study for each phase generally comprises the following tasks:

- define list of important functions
- select relevant parameters for function monitoring
- identify measurements required
- determine measurement quality
- develop algorithms for selected safety functions

The study for each phase is undertaken by a partner and the demonstration of the methodologies is based on a reference severe accident sequence.

The work done so far has centred mainly on three activities:

d:\data\word\bermejo\mission.rep\samoab3.doc
- reference scenario selection
- safety function selection
- review of computational aids

5.2.1.1. Reference Scenario Selection

The demonstration of the methodology is to be based mainly on a reference severe accident sequence. An initial list of scenarios was proposed and it included Steam Generator Tube Ruptures, Interfacing System LOCAs, Small Break LOCAs, Mid-Loop Operation and Station Black-Out. This list was considered and elimination of scenarios that are either too plant dependent (e.g. Station Black-Out), or are known to be difficult to simulate (e.g. Mid-Loop situations), or are not relevant for the containment safety function (e.g. SGTR causes containment by-pass) or take too much time before core recovery (e.g. ISLOCA), led to the choice of a small break loss of coolant accident (SBLOCA). The sequence is characterised by a break size of 25cm² with a release path from the containment provided by venting at a pressure of 4.8 bar. The severe accident progression is described by existing analysis provided by the MAAP code. The prediction will also provide the environmental conditions for Work Package 2.

5.2.1.2. Safety Function Selection

As it is expected that the parameters required for each of the three phases mentioned above, different approaches have been adopted to select them.

For phase 1, the French "State Approach" for post accident operations will be used. With this approach, three Critical Safety Function (CSF) are important in this phase: Reactivity, Heat Removal and Containment. However for the reference scenario (i.e. SBLOCA), only Heat Removal and Containment are relevant. Further assumptions, such as no loss of electrical power supplies and reactor initially at full power, can be made. Then the status of each Safety Function is determined by the monitoring of particular "State" functions (e.g. Containment Integrity), which in turn are defined by parameters reflecting the actual plant measurements (e.g. Containment pressure, Reactor vessel water level, etc...). This parameters list provides the starting point for the development of validation algorithms.

The study will further include the development of a methodology to derive a "confidence factor" for each CSF. This confidence factor can be calculated as combination of the individual "quality factors" associated with each parameter. This is further discussed in section 5.2.2.

The approach followed in phase 3 consists basically in developing a diagnostic scheme for reactor pressure vessel (RPV) failure, which provides the interface between the in-vessel and ex-vessel severe accident events. Three main factors are considered in this scheme:

(i) parameters to be monitored
(ii) key accident characteristics associated with these parameters
(iii) further actions for incorrect or uncertain diagnosis

The status of individual instruments in each phase of a severe accident has been reviewed in [10]. From this review, it is concluded that, for the parameters to be adopted for the mentioned diagnostic scheme, to place greater reliance on the containment instrumentation than the RCS instrumentation, is appropriate. On this basis, the diagnostic scheme development involves two groups of parameters:

(i) primary parameters, which provide the confirmatory symptoms and are based on containment instrumentation
(ii) secondary parameters, which provide the indicative symptoms on core melt progression, and are based partly on the RCS instrumentation and partly on containment instrumentation

Work is currently in progress on a review of the general characteristics of severe accident behaviour that are pertinent to the parameters which provide the basis for the development of the diagnostic scheme. This is based on existing MAAP code analysis for a number of representative accident sequences.

5.2.1.3. Review of Computational Aids

Computational Aids (CAs) examined in this review are tools for control room operators and Technical Support Centre (TSC) staff which provide information to assist them in the decision making process for SAM. They can range in complexity from simple charts and graphs to sophisticated software tools running in faster than real-time to predict future plant behaviour. The scientific basis of the algorithm development for each CA can also differ considerably. The review covered three categories of CAs:

- Simple CAs

The simplest CAs consist of graphical tools that provide information in an easily usable form based on symptom-based behaviour of the plant [9]. They provide the users with only the information 'needed' within the decision making process and thus avoid overloading the users with unnecessary information during a stressful operation. They are developed for a specific plant and are available to the users without the need for any on-going calculations during the accident.

- Intermediate CAs

These CAs are PC-based and computationally simple, consisting of simple engineering models, correlations of rate processes and relevant experimental data. It is intended that the CAs are collections of simple nomographs, and/or
step-by-step instructions which can be executed on hand-held calculators or lap-top PCs and thus are independent of external electrical supplies. Some examples are provided in [11] and they include CAs for decay heat, water addition rates for core recovery, containment pressurisation and vent sizing, RCS pressurisation during core recovery and concrete ablation during core-concrete interactions in wet and dry cavities.

- **Complex Codes**

The most complex type of CAs consists of the use of one or more computer codes which are run during a severe accident and which perform several of the following functions: (i) validate the instrumentation, (ii) diagnose the fault sequence, (iii) calculate the expected course of the accident based on specified procedures, (iv) investigate the course of the accident with postulated operator actions, (v) calculate expected release rates.

An example of such a code is MARS (MAAP Accident Response System [12]).

5.2.2. Work package 2 - Instrument validation and survival

As discussed, the SOAR1 study [2] showed that the instruments needed to monitor reactor conditions during a severe accident are unlikely to survive for more than a limited period. This conclusion was based largely on judgement using environmental time profiles forecasted for a set of severe accidents identified in the report. There is therefore a need to establish the developing environments more accurately and to take due account of this and of the difference in instrument location and other factors on the study conclusions. There is also a need to consider ways in which the instrument survivability could be improved, to establish levels of confidence for the survivability of different types of instrument based upon the environment experienced and to know with greater certainty when an instrument has failed.

From the above, the aims of work package 2 of this project can be considered sixfold:

(i) to confirm the parameters and hence the types of measurement required to monitor reactor conditions during a severe accident

(ii) to gain a better understanding of the change in environment with time at the relevant instrument locations during a severe accident

(iii) to consolidate the existing judgements on the expected duration of instrument survival under severe accident conditions

(iv) to investigate ways in which the survivability of instruments could be improved

(v) to investigate the relationship between the probability of instrument survival and the environment experienced

(vi) to investigate ways in which the status of instruments could be more accurately determined.

The specific tasks to be undertaken as part of this work package in order to meet the above aims are:

(i) to identify the list of CSFs needed for the reference severe accident and to identify the main CSF parameters useful for monitoring each phase of the accident. From this information, to list the relevant measurement instruments and their locations for a reference PWR. (Feedback from work package 1 required)

(ii) to establish the pressures and temperatures (and possibly radiation levels) for the specific instrument locations identified. (Feedback from work package 1 required)

(iii) to review the survivability of the identified instrument types for the specific locations and environment, and to reconsider the SOAR1 conclusions.

(iv) to consider the potential for development, relocation or protection of instruments to increase the probability of their survival into the accident regime. From this, to make recommendations on how to improve the survival probability of those instruments required for monitoring the CSFs under such conditions.

(v) to assess the quality factor of the measurements from consideration of the environmental conditions (temperature, pressure, and if available, dose rates). In the case of measurement failure, to suggest a correction rule (if possible).

(vi) to study the effect of changing environmental conditions on the characteristics of neutronic signals and to search for a qualitative criterion for signal change detection due to the reference accident scenario. To examine the potential for inserting the resulting methodology into a real neutron flux measurement line.

An important aspect of the work in tasks (iii) and (iv) is to gain a physical understanding of the methods of degradation of instruments due to extremes of temperature, pressure and radiation. From the point of view of accident monitoring, instruments can be divided into the following three groups:
Group 1: - Instruments available during normal operation

This group comprises all available instruments. These may indicate process perturbations as precursors to a malfunction or degraded function which could lead to a design basis or potentially beyond design basis or accident condition.

At this stage, the emphasis for the operator will be to prevent the process perturbation (or its cause) from developing into a more serious situation.

Group 2: - Instruments available for accident monitoring

This group is a subset of the first group and includes instruments which are specifically designed to withstand the environmental conditions that could occur in a design basis event. These are generally restricted to those instruments required to meet the requirements of US regulatory guide RG 1.97 [13] or equivalent national standards. Instruments provided for CSF monitoring form a significant proportion of this group, and these provide the input to the information displays and operator support tools used for decision making in the control room, technical support centre and emergency operation centre.

Throughout the progression of the accident, the operator will be taking actions to mitigate its consequences and to try to prevent its escalation. In particular, the latter actions will be aimed at maintaining the integrity of both the fuel (phase 1) and the reactor pressure vessel (phase 2).

Group 3: - Instruments available for severe accident monitoring

This group is a subset of the second group above. Instruments in this group are generally located outside containment and obtain either indirect measurement of parameters inside containment through sensing lines or direct measurement of parameters outside containment, such as radiation or stress.

Due to the nature of severe accidents, these instruments should mainly be used for ensuring containment integrity and containment heat removal, and to assist with decisions such as whether to vent to atmosphere to prevent containment failure.

Regarding task (vi), the scientific base of the work on flux sensors (task vi), it includes the careful study of the AC information attached to the signal formation inside the sensor. This can be used for detection of anomalies and incipient failures by spectral comparison with reference values for the instrument. This self-validation methodology has two main advantages in accident situations. Firstly, it does not rely on any kind of classical or analytical redundancy, and is thus robust against multiple sensor failure. Secondly, it does not use any kind of process model, and this prevents it from giving erroneous results in the event of an abnormal change of the process itself.

5.2.3. Work package 3 - Implementation strategy

This work package will examine the operating staff requirement for appropriate algorithms, and make recommendations for their strategic implementation. The personnel concerned will include the plant operating staff, the staff in the TSC and possibly also those in other crisis management centres. The inputs to this work package will include the experience of the partners of the different operating roles of the main control room and TSC, the background of the SOAR2 [3] study, and the experience of the partners in regulatory acceptance of operator support algorithms.

Several factors will be considered and they include, for example,

- regulatory requirements for the implementation of algorithms for operator support
- the safety role of the support provided by the algorithms
- the technical quality of algorithms which will be needed for implementation for the intended safety role
- the need for clarity, due to increasing stress on the operating staff as an accident progresses

This work package is scheduled for later on in the project in order to fully exploit the results generated from Work Packages 1 and 2.

6. CONCLUSIONS

Comprehensive work related to different areas of accident management support for reinforcing the defence-in-depth concept utilising new scientific and technological methods and tools have been successfully performed within the AMS project of the EU 1990-1994 Research Programme on Reactor Safety. The variety of tasks investigated in the project reflect the wide-spread issues where further progress and improvement by applying modern information technologies seem to be achievable. Based on two state-of-the-art reports (SOAR) on "Instrumentation/Signal Validation" and on "Operator assisting systems for Accident Management", [2-3] it can be concluded that the situation in European nuclear power plants with respect to instrumentation, signal validation and operator support is in accordance with the operational safety needs, but ongoing activities in many countries are directed to further improvement of nuclear safety by developing measures for prevention of incidents and accidents even beyond the design basis.

The methods and tools investigated in the AMS project have shown that due to the availability of powerful information processing systems, advanced methods and systems are feasible for research activities related to signal
validation, process and system state assessment, human-machine interface optimisation, and operator advising and assisting systems for diagnosis, execution of accident management procedures, and safety-function or situation-related decision-making. However, the general opinion is that considerable progress in the different tasks can still be achieved.

The work of the "ASIA" project, which is being performed in the framework of the 1994-1998 EU Research Programme on Nuclear Fission Safety, will continue and further develop some of the methods and tools investigated in the "AMS" project. The expected results of this project will be (i) recommendations on algorithms for processing plant measurements and their use for accident identification and signal validation on PWRs; (ii) development of a method to assess the survival potential of selected flux instruments in accident conditions; and (iii) strategic recommendations on the method of use and environment of the operator support tools needed.

This various projects described have shown that the progress in numerical techniques as well as the availability of powerful and cost-effective information technology systems, has made of the area of Accident Management Support a promising R&TD field for the future. The enforced involvement of partners from different EU member states in these projects, has also proved to be very positive to stimulate co-operating among public and private organisations, to avoid duplication of efforts and to use the available resources in an efficient way.

REFERENCES


MAAP-GRAAPH

Use of MAAP-GRAAPH for training of Borssele NPP plant operators

Poster at SAMOA-2 meeting, Lyon 8-10 September 1997

P.J.T. Bakker, KEMA, The Netherlands
(p.j.t.bakker@mta9.kema.nl)

1) MAAP-GRAAPH

Default the MAAP code is extended with a visualisation possibility:

**MAAP-GRAAPH**

(Graphically Represented Accident And Phenomena).

Purpose of this MG application:
- enlarge understanding of analyst on global accident progression
- enlarge understanding of outsider on accident progression.

Default MG has 3 BWR and 3 PWR visualisations:

2) ZION NPP MG visualisation:

![ZION NPP MG visualisation](image)

3) MG

Main visualisation items are:
- water levels
- availability of pumps and tanks
- temperature and location of core
- containment failure.

Options are:
- stopping of ongoing calculation, change of parameter and restart
- show parameter as function of time
- replay option.

4) Borssele NPP

Utilisation of MG for Borssele NPP first focuses on:
- enlarging severe accident knowledge of plant owner (operator, technical support, management)
- serving as a practice tool for the to be implemented severe accident management measures.

The present status of the Borssele MG picture:

5) Borssele NPP MG visualisation

![Borssele NPP MG visualisation](image)

6) Ongoing work for Borssele:

- addition of systems visualisation
- study of PC windows version of MG
- simplifying of Borssele MAAP model to speed up analysis time
- inclusion of print options
- enhancement of input and output understanding.
SIPA: POST-ACCIDENT SIMULATORS

SIPA is one product of the CATHARE program, developed by Electricité de France (the French electricity utility) and CEA (the French atomic energy commission) with FRAMATOME collaboration. This program has aimed at understanding and modelling sharply, thanks to the advanced CATHARE code, the PWR thermohydraulic behaviour during an accident. Therefore SIPA is a Simulator whose the physical domain has been extended to the Post-Accident situations and which goes beyond the capacities of usual training simulators.

It is also a manufacturing workshop for idiosyncratic simulators: SWORD* (Software Workshop Oriented towards Research and Development).

A FLEXIBLE HARDWARE ARCHITECTURE...

SIPA hardware mainly comprises:

- A Remote Super Computer **

- An "Engineering network" to create software applications

- A "Training network" for real time running of these applications, under the control of a Scheduler Computer.

The ETHERNET networks of workstations and the Remote Super - Computer operate under UNIX and TCP - IP.

...ADAPTED TO ITS OBJECTIVES

SIPA architecture meets the following requirements:

- EDF operator training

- Safety analysis and study preparation and performance

- Crisis drill preparation and performance (linked to the National Crisis Center).

* In French : AGLAE.
** See note in page 4.
THE SWORD WORKSHOP

The SWORD workshop is part of SIPA project:

- It gives the user integration standards to build simulation modules.

- It enables the engineer to enter topology and data of a system, with an user-friendly CAD software (PHENIX) and then to automatically build the corresponding code modules for steady state and transient calculations. All necessary data can be processed (geometry, process control and protection system set points, ... and also possible failures).

- It makes it possible to gather custom-made modules and off-the-shelf modules (such as CATHARE code) so as to form an executable “batch” assembly.

- or standard conventional : e.g. diagrams currently available either to the Operators on the Data Acquisition and Safety Panels or to the crisis team in the NCC.

- Finally, it links the above-mentioned assemblies, the M-MIS images and the initial condition data sets in order to launch an application which will be executed with “real time” outputs on target computers (RSC** and workstations).

SWORD modularity, flexibility and portability make SIPA a configurable simulator, which can be used for other processes than PWR, in other domains (presently from accident up to core melting), even with other computers (either real or unreal time).

- It provides this assembly with a man-machine interface system displaying pictures:

  - computerized: interactive mimic diagrams on the Main Operating Desk and on the Instructor Station
  - sophisticated: images visualizing the inner part of the NSSS on the Pedagogic System

![Simplified SIPA architecture](image-url)
FIRST APPLICATIONS OF SIPA: THE FRENCH 900, 1 300 and 1 450 MW PWR UNITS

The NSSS of each of the French PWR series (3 and 4 loops) is described by a speeded-up release of CATHARE code. About 60 modules, representing the most important thermalhydraulic circuits and Instrumentation and Control systems (reactor containment atmosphere, engineered safeguard systems, electric power supply,...) complete the simulation scope.

Thus, this tool allows a realistic simulation with interactivity and real time respect, of any accident up to fuel melting, such as a 12 Inch Loss Of Coolant Accident, Using emergency procedures.

Looking forward 1995, EDF is preparing an application for the new 1 450 MW "N4" series.
SIPA has been designed by Electricité de France and carried out by THOMSON - CSF/Division Simulateurs. For its training and engineering needs, Electricité de France placed an order for SIPA 1, commissioned in December 1991. For safety analysis needs, CEA-IPSN participated in the project, to purchase its own SIPA 2 simulator, commissioned in February 1992.

The software (except CATHARE, PHENIX and other software products) suppliers are THOMSON - CSF/DSI and, for the DASP, SEMA - GROUP/Division Energie. Equipment are CRAY-C98**, SUN and, for the DASP, BULL products.

** Initially, SIPA was designed in order to run on a Remote Super-Computer (RSC), none other than the CRAY-XMP of EDF. Now, it can run on a Local Super-Computer, or even on a small hardware structure (one server and two workstations), much cheaper and almost as quick as the previous system: this is the new "mini-SIPA". **
DEVELOPMENT OF EMERGENCY RESPONSE SUPPORT SYSTEM
FOR ACCIDENT MANAGEMENT

Tatsuya TAMINAMI
Tokyo Electric Power Company
1-1-3 Uchisaiwai-cho, Chiyoda-ku,
Tokyo 100, JAPAN
+81-3-3501-8111

Ryuji KUBOTA & Tadashi
FUJWARA
Hitachi Works, Hitachi, Ltd.
3-1-1 Saiwai-cho, Hitachi-shi,
Ibaraki 317, JAPAN
+81-294-21-1111

Noriyuki YAMANE & Yoji
TAKIZAWA
TOSHIBA CORPORATION
4-1 Ukishima-cho, Kawasaki-ku,
Kawasaki-shi, Kanagawa 210,
JAPAN
+81-44-288-8171

ABSTRACT

Specific accident management (AM) strategies have already been worked out and are being applied to each plant. On the other hand, it is essential to grasp the plant status accurately to ensure effectiveness of AM. From such point of view, a kind of tool would be useful that can support AM activities by showing the important plant information. Based on such background, the Emergency Response Support System (ERSS), computer assisted AI system, was developed by a joint study of Japanese BWR group. This system can show not only real-time plant parameters but also information that support judgments and predictions under an emergency condition. After the development of proto-type system, the effectiveness of the system was confirmed by the verification test.

I. INTRODUCTION

Since the March 1979 accident that hit the #2 reactor at the Three Mile Island nuclear power plant, aggressive researches on severe accidents have been made in a number of countries. Debates on severe accidents and AM have also been active since the Chernobyl accident. Under these conditions, the electric power companies in Japan examined AM as the independent preservation countermeasure. The electric power companies reported on the AM of each nuclear power plant March 1994. These AM reports were abstracted from the AM countermeasure. Meanwhile we advanced the information processing technologies in order to support the AM. The electric power companies have also developed the ERSS under a joint study of Japanese BWR group.

II. OUTLINE ON DEVELOPMENT OF THE ERSS

A. An overview of the ERSS

The ERSS aims at providing staffs in the Technical Support Center (TSC) and the head office and operators in the control room with important information in a quick, accurate manner under the plant emergency condition. To accomplish this purpose, the ERSS takes in plant parameters on-line, and calculate these parameters by its diagnostic logic and prediction simulators. The results of calculations are converted into a visual form, and displayed on the CRT. The output of the ERSS are as follows.

1. The current status of the plant parameters
2. The current status of the plant systems and components
3. The relevant emergency action level
4. Guidelines suited for the current plant status
5. Radioactivity release and dose effect
6. Prediction of the future plant status

To accomplish the above objectives, the ERSS has two functions. One is to provide the TSC staff with the plant parameters that indicate the real status of the plant. The other is to provide with the prediction of the plant status and the judgment of the plant status. Fig. 1 shows a basic configuration of the functions of the ERSS. From the aspect of the sharing common information, it would be effective that the system is installed in the TSC, the head office and the control room and linked each other by on-line network.
B. Description of the system's functions

Given below is a description of the functions of the ERSS in terms of an overview of its functions, main methods of judgment and prediction, typical screens, along with other details.

1. Information display

This function displays plant information in an easy-to-read manner in order to allow the staff and operators to monitor the plant status accurately in an emergency in the plant. The four items of information listed below are considered to be necessary in such an emergency. The ERSS is therefore designed to display in one place all plant signals related to these four items of information. A summary screen (Plant Summary) has also been made available to provide a summary of these four items of information.

1. Has the plant shut-down normally? (Core reactivity status)
2. Is the core cooled enough? (Core cooling status)
3. Has the containment vessel cooled? (PCV status)
4. Make sure that no radioactive substance has left the power plant? (Radiation status)

2. Information transportation

This function is designed to allow positioning marks on the screen so that the staff in the TSC, the head office, the control room, and other sites can share information quickly and smoothly. These positioning marks allow the personnel to check which screens are being watched by other departments. These positioning marks also facilitate the transportation of information while the TSC staff shares information with the head office personnel by phone. Fig. 2 shows the plant summary screen with positioning marks attached to it.

3. Judgment and prediction summary

This function gives a summary of important information related to the function for judgment and prediction, including emergency level, plant status, operation guidelines, operation status of the water injection system into the reactor pressure vessel, operation status of the containment vessel cooling, evaluation results of radioactivity-related analysis, and prediction results of the plant status.
4. Judgment as to the plant status

This function provides judgment as to core damage, pressure vessel failure, containment vessel failure, and other plant status. More specifically, the judgment results of the plant status are displayed on the screen. The ERSS also judges the status of the water injection system into the pressure vessel and other systems that may affect the plant status, and displays those systems together with the process quantity. Here, the plant status is judged with consideration given to the priority of calculation use according to the AM guidelines. Operating conditions of the water injection system etc. that may affect the plant status are judged on the process signals.

Fig. 3 shows a typical screen representing the status of the judgment as to the plant status. Here, the plant status, water injection, and other operating conditions are displayed in the form of buttons on the screen. The plant status etc. are displayed with a logic-tree and a success-tree.

5. Supporting of the emergency procedure guide

This function displays which operating guideline is best suited for the current plant status. More specifically, the function displays the current progress status of an operation in the Emergency Procedure Guideline (EPG) and also displays whether a specific operation deviates from the EPG and needs to shift to the AM guideline.

6. Evaluation of radioactivity release

If large quantities of radioactive substances were released or were likely released, the nuclear power plant must be evaluated in terms of the amount of radioactivity released into an environment. This function therefore evaluates and displays the following:

① Evaluation of radioactivity release amount and release rate
② Prediction of future release amount
Here, radioactivity release amount and release rate are evaluated as shown in Fig. 4. Future predictions are made by making corrections with the containment vessel pressure and other factors based on PCV radiation monitor level and previous analysis results.

7. Evaluation of dose effect

If large quantities of radioactive substances were released or were likely released, the nuclear power plant must be evaluated in terms of exposure dose level of the area surrounding the plant, together with the evaluation of radioactivity release. This function evaluates and displays the following:

* Evaluation of exposure dose level and predictions level

Here, exposure dose level are evaluated with an Emergency Environment Impact Evaluation System on the basis of radioactivity release rate and meteorological data determined as shown in Fig. 5. This system displays these evaluation results. Fig. 6 shows a typical screen displaying the status of the evaluation function of dose effect.

8. Judgment as to the emergency action level

This function supports the judgment which the electric power utility should cope with the emergency action level on the basis of the plant status. Here, the emergency action level for judgment consists of four organization degrees listed below. The progress of the emergency action level, is also judged and related information is provided.

1. Accident and failure organization
2. Primary emergency organization
3. Secondary emergency organization
4. Tertiary emergency organization

9. Supporting of the AM guide

The BWR utilities are preparing the AM guideline in order to manage the severe accident. This function supports the TSC staff by the computer system when the AM guideline is used. This function provides the staff in the TSC and operator in the control room with the operation guide and verification guide. These guide are used the operations to prevent the pressure vessel failure and the containment vessel failure. Concretely this function judges the position in the AM guide flow-chart. These results are displayed and it is enable to refer the operation guide and the verification guide in the strategy on the display.

10. Recording of the accident history

This function displays the history of main plant
Fig. 4 Radioactivity release amount and rate evaluation method

Fig. 5 Radiation exposure dose level evaluation method

Fig. 6 The screen of evaluation of dose effect
parameters, judgment results, and other factors in order to monitor the history of accidents and the long-term behavior history of accidents. Items displayed in the form of history are main plant parameters, operation status of safety systems, judgment results of plant status, and judgment results of emergency action level. Displays are given on a time basis to make it readily intelligible for operators. A history list is provided as a low-level screen, which also displays the times when the above items are activated.

11. Prediction of accident scenario

This function judges the operation status of the mitigation system and qualitatively predicts the plant status. More specifically, an event-tree is first used to judge the operation status of the mitigation system from the time when an accident occurred up to the present time. The ERSS then judges whether the accident may lead to core damage based on the flow of the event-tree and displays the results. The ERSS also displays a success path that prevents core damage and displays a success-tree to recover the faulty mitigation systems. Fig. 7 shows a flow-chart of how the prediction function progresses of accident scenario. Fig. 8 shows a typical screen displaying the status of the prediction of accident scenario.

12. Prediction of plant status

This function predicts the onset times of core damage and other plant status on the basis of previous analysis results and simulations. Together with the above predictions, this function predicts temporal changes in plant parameters related to them. This function is started up on demand. Especially, the containment vessel failure, which is important in a sense of the radioactive barrier, is predicted in real time by the computer simulation in the system.
III. VERIFICATION OF THE FUNCTIONS OF THE ERSS

After the development of the ERSS, the verification test was conducted by using proto-type system to verify the functions and usefulness of the system.

A. Method of verification test

Verification test was executed in the nearly same conditions as the ones where this system will actually be used. For this verification test, we decided to use scenario data for severe accidents incorporated in this system, and we simulate emergency training. More specifically, this method progresses as follows: By using plant parameters displayed on the screen and judgment and prediction results calculated by this system, the examiners monitor the plant status and other factors and report the information to the head office and the control room. To verify the effect of information sharing, we installed ERSS, one at each of three locations: a simulated control room, a simulated TSC, and a simulated head office. Given below is a description of the location, examinees, and verification test scenarios.

(Location)
* Three rooms are provided: a simulated control room, a simulated TSC, and a simulated head office. Liaison work is conducted by phone.
* The examinees are selected from emergency readiness team (Information Liaison Team, Technology Team, Operation Team, etc.).
* Two scenarios are provided: a scenario that enables a maximum check of the function of the proto-type system and a realistic scenario for emergency exercise. The test will last about one hour. We also decided to accelerate this test when accidents progress gradually. (For verification test, we used a realistic scenario.)

For verification test, which is to be conducted in a near-actual form, we decided to have the control room take charge of the developers and have the control room give the information actively to the TSC. As for the TSC and the head office take charge of the examinees, we provided advisers and made sure that they use this system effectively. We also provided an observer to check how the examinees respond and how they operate this system, thus verifying the usefulness of the system with an objective method. Fig. 9 shows an overview of verification test.

![Diagram of verification test](image)

*Fig. 9 An overview of verification test*
B. Function verification results

To evaluate function verification results, we used a subjective and an objective method. The conceivable items of subjective evaluation are the usefulness of this system as viewed from the examinees, the sharing of information among the control room, the TSC, and the head office, and the human-machine interface of this system. To pick up the items of subjective evaluation, we conducted a questionnaire and interview survey of the examinees. As a result, we found that this system obtained good scores and would be useful in an emergency. Fig. 10 shows the findings in the questionnaire of the examinees.

![Graph: The usefulness of the ERSS](image)

For objective evaluation, on the other hand, we decided to have an evaluation made by the observer provided at the time of verification tests and to evaluate which screen was often used by the examinees. Many of the observers found that the examinees were making effective use of this system. And the most frequently used screen was the plant status screen before the action level, and the radioactivity screen after the action level.

This system is originally aimed to support the operation in an actual emergency. And this system was well evaluated to be effective in the AM education and training.

IV. SUMMARY

Having developed an ERSS and tried it in a verification testing and emergency training, we obtained the following:

1. The ERSS was confirmed very useful to support emergency staffs, and would also be effective from the aspect of sharing information among the control room, head office, and TSC.
2. The ERSS was found to be effective in AM education and training.

REFERENCES


José Ramón Alonso Escós
Santiago Aleza Enciso
Antonio Munuera Bassols
CONSEJO DE SEGURIDAD NUCLEAR (CSN)
Justo Dorado, 11 28040 Madrid (SPAIN)

COMPUTER BASED AIDS AT THE SPANISH NUCLEAR SAFETY COUNCIL EMERGENCY ROOM (SALEM)

1.-THE CSN AND THE NUCLEAR EMERGENCIES

The nuclear Spanish fleet is currently composed of 7 NPPs accounting for a total number of 9 units (two of GE design, one from KWU and the rest from Westinghouse), producing about 35% of the total electric energy. The CSN (“Consejo de Seguridad Nuclear”) is the regulatory body in Spain. In case of a nuclear emergency, the CSN has a well defined set of duties (mainly to be the major advisor of the civil authorities and to maintain the appropriate international liaisons). To fulfill them under such a nuclear emergency condition, the CSN has delineated a special hierarchical structure as shown in figure 1.

In this structure a key individual is the CSN “Emergency Director”, main responsible of the activities done in the Emergency Room (SALEM). Two specialized groups assist him on his job: the Operating Analysis Group (GAO) and the Radiological Group (GR). The first one dealing with the operational aspects of the accident. Figure 2 shows how the GAO interacts with the rest of the SALEM staff.
2.- CSN-GAO COMPUTER AIDS

SAFETY PARAMETERS RECEPTION & PROCESSING

In case of activation of the "Internal Emergency Plan" (PEI) in a Spanish nuclear unit, the SALEM computers start to receive, in a continuous time frame of 30 seconds, a selected set of plant critical parameters. This task is done by a dedicated transmission system called SCADA-CSN.

The received data are first processed by the IGPS system ("Safety Parameters Graphical Interface"). This tool has been internally developed having specific models for each plant. The IGPS first aim is to friendly display the safety parameter current values and trends, making use of different graphic capabilities. Also the system does some calculations in order to estimate parameters not directly available, like the core residual heat, current accumulator inventories, etc. Additionally, the system evaluates, and displays in the appropriate colour range, the status of some Critical Safety Function (CSF) previously defined: for the Westinghouse plants, these CSF have been developed following the general scheme of the corresponding EOPs, with the only restrain of the number of variables available at the system. In the other hand, it is well known that for GE and KWU plants, though, such kind of functions are not explicitly defined in the Procedures. So, a specific development is now in progress in order to allow similar capabilities for these plant models. It is worth to say IGPS has been conceived as a modular one, and in the future new capabilities would, as required, enhance it.

PLANT DATA BASES

Another interesting tool used by the GAO is the program so-called DIAGRAMS. This tool runs on a PC platform and has been internally developed as a
consequence of the "lessons learnt" along many drill exercises. According to that, it permits a fast and easy access to a certain number of data bases containing "static" plant-specific information: EOPs summaries, geometrical data, and above all fire zones, flood areas and equipment electrical supplies data bases that, rightly interconnected, allow the user to gain insights on the potential impact over the global plant safety of those type of incidents. Not a surprise, the quality of the different plant models relays strongly on the detail and reliability of each of the data bases used.

**MARS: AN EMERGENCY PREDICTIVE TOOL**

Other computer tool is installed at the SALEM facilities: **MARS** (MAAP Accident Response System). This one is a commercial application developed by an external consultant with the main aim of giving support to the emergency centre staff to evaluate the current and, more specially, potential future accident states (see reference 6.8). MARS works in two main operative modes: first one is "Tracker"; it receives (in Real-Time) both plant data and IGPS-calculated parameters and initialises, at any time along the accident sequence, the severe accident code MAAP. To fulfil this task MARS tries first to determine the current plant situation and the accident root-cause. Then, it follows the plant behaviour comparing the real plant evolution with the MAAP dynamically obtained results: if there is no good agreement MARS automatically re-initialises. On the contrary, if the two evolutions are consistent, the second mode ("Predictor") can be activated, performing a much faster than Real-Time accident simulation. Different "operator-action options" can be implemented in PREDICTOR: hands-off, EOPs, SAMG, etc. For this purpose, the corresponding set of actions must be explicitly defined into specific input files.
3.- CSN-MARS

DEVELOPMENT & SCOPE

The CSN MARS has been developed for 4 out of 7 Spanish NPPs. Only a limited set of sequences are by now covered by the code capabilities, mainly Station Blackout (SBO) and small/intermediate LOCAs.

In a initial effort, the consultant developed models for Vandellós (W-3L) and Garoña (BWR-3). Later, the CSN has implemented, with the external support, plant specific models for Almaraz and Asco NPPs. A new Project is now planned in order to increase the current scope (plants and sequences). Both CSN and the consultant would work together in this development phase.

CSN MARS models make use of the MAAP Parameter Files specifically developed and tested by the utilities under the umbrella of the Spanish PSA program.

VALIDATION

A concern the GAO staff has always been aware is the need to know as much as possible about the confidence level that such a predictive tool deserves in the different potential scenarios, with the implications of using it for nuclear emergency situations decision making process support. Logically, this concern leads to adopt a quite cautious approach in the use of MARS.

In this sense, an extensive validation process is considered critical to gain confidence about the code capabilities. Also it should be very helpful to gain insights over potential code use and limitations. It is also expected these activities, when finished, will increase the due staff training level.
According to this idea the GAO has established a plan to exercise MARS by using accident scenario data generated with other than MAAP thermohydraulic and severe accident codes. For this task, a two steps plan has been proposed: first the activities have focused in the use of non-severe accident and in-vessel scenarios, due to the fact of easier data accessibility. So, results from RETRAN and RELAP codes have been generated and then used. Second phase, now in progress, includes the generation and testing of MELCOR results. In both cases plant specific inputs are considered a basic condition. Table 1 shows the total set of cases included in the CSN MARS validation.

### TABLE 1: CSN MARS BENCH-MARKING

<table>
<thead>
<tr>
<th>#</th>
<th>PLANT NAME</th>
<th>REF. CODE</th>
<th>SCENARIO</th>
<th>TIME(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GAROÑA</td>
<td>RETRAN</td>
<td>SBO w/o ADS</td>
<td>5000</td>
</tr>
<tr>
<td>2</td>
<td>GAROÑA</td>
<td>RETRAN</td>
<td>SBO w ADS</td>
<td>4500</td>
</tr>
<tr>
<td>3</td>
<td>VANDELLOS 2</td>
<td>RETRAN</td>
<td>SBO</td>
<td>5000</td>
</tr>
<tr>
<td>4</td>
<td>VANDELLOS 2</td>
<td>RELAP</td>
<td>SMALL LOCA</td>
<td>12000</td>
</tr>
<tr>
<td>5</td>
<td>VANDELLOS 2</td>
<td>SCDAP-RELAP</td>
<td>SBO-TMLB'</td>
<td>21000</td>
</tr>
<tr>
<td>6</td>
<td>VANDELLOS 2</td>
<td>SCDAP-RELAP</td>
<td>SBO-S3TB'</td>
<td>18000</td>
</tr>
<tr>
<td>7</td>
<td>GAROÑA</td>
<td>MELCOR</td>
<td>SMALL LOCA</td>
<td>(*)</td>
</tr>
<tr>
<td>8</td>
<td>ASCO 1</td>
<td>MELCOR</td>
<td>PORV OPEN</td>
<td>(*)</td>
</tr>
<tr>
<td>9</td>
<td>ASCO 1</td>
<td>MELCOR</td>
<td>SBO-S3TB'</td>
<td>(*)</td>
</tr>
<tr>
<td>10</td>
<td>VANDELLOS 2</td>
<td>MELCOR</td>
<td>SBO</td>
<td>(*)</td>
</tr>
<tr>
<td>11</td>
<td>VANDELLOS 2</td>
<td>MELCOR</td>
<td>SBO</td>
<td>(*)</td>
</tr>
</tbody>
</table>

(*) MELCOR sequences will be run up to the time of Containment Building failure

Up to the moment, the results obtained in this project show lights and shadows in the code performance; Both
are being analysed in order to take the most appropriate actions. As an example the attachment 1 presents a brief summary of one of the bench-marking case analysys.

USER TRAINING

Another important issue that, logically, appeared along the MARS use implementation in the normal GAO/SALEM procedures was the one of what people, and with what level of training, should be able to use this tool. The approach taken assumes two type of users are going to run the tool: an executive level user, with no special familiarization with the code characteristics, which should only expect from MARS information about the current plant status: essentially Root Cause Identification and Fission Product Barrier Status. In the other side, an upper level user, with training and experience enough to make a right interpretation of all the information available that permits him to start-up the required predictions. Not to say, the people involved in all these activities must have, as a prerequisite, a relatively deep knowledge of the different plant main systems, accident sequences and recovery strategies for each of the plants so modelled.

4.- CSN-SEALEM: COMPUTER AIDS IN EMERGENCY DRILLS

Finally an important experience has undoubtedly been the use of all these tools along the year-round emergency drills. These exercises are performed once each year for any one of the Spanish plants. And they usually follow a pre-run scenario that is played on real time conditions both at the plant site and at the SALEM computers. Blind drills are an excellent mean to test the global interaction among different groups involved, and also to check the benefits the available computer aids are able to provide.
5.- CONCLUSIONS

The Operative Analysis Group (GAO) is one of the Spanish Nuclear Safety Council (CSN) teams directly involved into the Nuclear Emergency activities. To rightly fulfil their duties, this group has available at the Emergency Room (SALEM) facilities a set of computer aids specifically developed for such a task: mainly the program "Diagrams", which contains a big amount of specific plant information into the appropriate Data Bases; the program "IGPS", devoted to friendly display the Safety parameters transmitted from the plant on Real-Time; and MARS, a diagnosis and predictive tool which makes use of the above cited Plant Safety Parameters.

The continuous use the GAO staff is making of these tools, mainly on the yearly Drills and the internal training exercises, is clearly improving the group capabilities. Worth to notice is also that this process is taking to light some weaknesses present in both the internal and procedural organisation initially defined, and in the computer codes themselves.
6.- REFERENCES

6.1 "Informe de valoración del programa MARS para su uso en Emergencias". CSN report number: CSN/IEV/OPERA/GENER/0000/9501/231. Rev.0 (Feb/95). Author: S. Aleza (CSN) et Al.
6.2 "Medios de Apoyo para Situaciones de Emergencia (CSN)". Presented at the SNE meeting’95. Author: José R. Alonso (CSN) et Al.
6.3 "MARS Application and Bench-marking". Presented at the PSA meeting’95. Author: A. Munuera (CSN) et Al.
6.4 Using MARS to support a Simulated Emergency Drill at CSN". Presented at the ANS meeting’96. Author: J.C.Raines (FAI) et Al.
6.5 "Faster than Real-Time Accident Management Predictions at CSN using MARS". Presented at the PSA meeting’96. Author: A. Munuera (CSN) et Al.
6.6 "Informe de cierre Fase II Proyecto MARS-CSN". CSN report number: CSN/IEV/OPERA/GENER/0000/9703/348. Rev.0 (March/97). Author: Jose R. Alonso (CSN) et Al.
6.7 "Partial Comparison between MELCOR 1.8.2 and SCDAP/RELAP5 Calculations of two High Pressure sequence accidents (TMLB’ and S3TB’). Author: F. Martín-Fuertes (UPM), E. Menéndez (CSN) et Al.
6.8 "Cálculo de la Secuencia de un Accidente de Pequeña pérdida de Refrigerante en la línea de Recirculación de la Central Nuclear de Sta. María de Garoña". UPM-ETSII-CTN report number CTN-12/97. DRAFT (May/97). Author: M. Martín (UPM) et Al.
6.8 "Proceedings of the SPECIALIST MEETING ON OPERATOR AIDS FOR SEVERE ACCIDENTS MANAGEMENT AND TRAINING (SAMOA)". Halden, Norway 1993. NEA/CSNI.
ATTACHMENT 1

ANALYSIS OF MARS RESPONSE WHEN TESTED AGAINST DATA GENERATED WITH RELAP5.MOD2

This Attachment is just an example of the way the GAO staff is proceeding with the Benchmarking activity. Essentially what is done is: i) run, or make to be run by other organisation, the selected case; ii) analyse the plant data-like file and validate it; iii) run the adequate "Trackings"; iv) check the code behaviour, analysing the potential error correction and/or code improvements, and v) transmit the conclusions to the external contractor to discuss the ways to solve the concerns. If the problem were considered "not easy to solve", the case is then a "lesson learnt" to be taken into account as a limitation in the code use strategies.

A small break LOCA sequence, for Vandelllos-2 NPP, was run with the code RELAP5.mod2 in order to generate an appropriate file containing the set of plant parameters available at the SALEM computers.

The RELAP model that had been previously developed for other purposes (see Ref. 6.7) was enhanced to cover the specific needs associated to this case: main change was the addition of a simple Containment model. The sequence was run by assuming that neither Safety
Injection nor Containment Sprays were available along the accident.

Two different MARS initializations, at 120 and 4000 seconds on to the accident, were run in order to track the plant-like (RELAP) data.

Figures 3 to 6 show the evolution of some of the main parameters in RELAP and MARS-TRACKER.

O RELAP evolution:
The break flow produces a fast Primary system depressurization down to the saturation conditions. At that time the RV water level is at the nozzle height. Then, the pressure and level stabilizes due to the loop seal on the intermediate legs. After the seal clearing, those parameters rapidly evolve producing the Accumulator to inject in three consecutive discharges. Simultaneously the upper plenum thermo-couples are detecting core heat-up. The Accumulator discharges are able to refill, partially at least, the core and makes it to return to saturation temperature.

O TRACKER evolution:
* First initialization (120 seconds). The code identifies the break, but with a slightly bigger size. The quite simple thermohydraulic MAAP models (MARS base code) can not rightly identify the seal loop phenomenon, producing a fast transition to “all gas” break discharge making the system to depressurize faster. In the other hand, the system inventory depletes sooner as a consequence of the bigger break size, this leads to an early core heat-up: this process is in some way overpredicted by TRACKER due to the “conservative” approach MAAP does with the core cooling phenomenon. After a while the internal MARS control logic identifies the increasing mismatch between the “plant data” and the calculated results and automatically re-initializes the tracking process at a time
of 3420 seconds. From here the tracking is quite similar to the second case below described.

* Second initialisation (4000 seconds). Now TRACKER identifies quite well the sequence. Pressure and level are strongly correlated to the Accumulator behaviour, what is well tracked by the code. After 10250 seconds TRACKER died due to some math error.

CONCLUSIONS TAKEN:

. TRACKER shown a quite conservative behaviour, as it was expected. From the regulatory body point of view this is not a big problem, on the contrary, the potential actions to be taken outside of the plant site should always be done on this base.

. The first initialisation was not right because of: i) problems on the TRACKER identification of the size and location of the break and ii) simplifications included into the code physical models. The problem must be further investigated and, if possible, the code adjusted.

. The second initialisation performed adequately. Undoubtedly, this phase of the sequence had clearly permitted to start-up any PREDICTOR, if it were user required.
FIGURES

FIGURE 1: CSN ORGANISATION CHART ON EMERGENCIES

FIGURE 2: GAO INTERACTIONS SCHEME

FIGURE 3: RELAP SLOCA TRACKING: PRIM.SYSTEM PRESSURE

FIGURE 4: RELAP SLOCA TRACKING: REACTOR VESSEL LEVEL

FIGURE 5: RELAP SLOCA TRACKING: CORE EXIT TEMPERAT.

FIGURE 6: RELAP SLOCA TRACKING: CONTAINMENT PRESS.
FIGURE 2: OPERATIONAL ANALYSIS GROUP INTERACTIONS SCHEME

1. GAO ACTIVATION
2. PLANT DATA RECEPTION
3. PLANT DATA VALIDATION
4. REAL PLANT STATUS ASSESSMENT
5. FUTURE PLANT EVOLUTION ASSESSMENT
6. DEACTIVATION

INFORMATION TO E.D.I. AND OTHER SALEM GROUPS
MARS BENCH-MARKING: RELAP5 SLOCA
FIG. 4: REACTOR VESSEL COLLAPSED LEVEL (M)
MARS BENCH-MARKING: RELAP5 SLOCA
FIG. 6: CONTAINMENT PRESSURE (Pa)
COFRENTE'S NUCLEAR POWER PLANT RISK MANAGEMENT TOOLS

Joaquín Suárez
Lourdes Borondo

1. ABSTRACT

Cofrentes Nuclear Power Plant (CNPP) is aware of tendencies and improvements in helping operator burden caused by accidents. CNPP recognizes the importance of being prepared to face any kind of accident and to improve the operation alike. For that reason CNPP is trying to get the available tools on the market and to adapt them to the plant as well as to build their own ones.

These are reasons that drove CNPP to install the EPRI's Risk Monitor EOOS at the plant. The main features of this tool are: the use of plant specific PSA models, the requantification of the entire PSA in minutes, the quantitative and qualitative evaluations, the instantaneous and cumulative core damage frequency (CDF) and the evaluation of alternative maintenance configurations and strategies. The potential users of this tool are schedulers, operators and PSA analysts.

About severe accident management, CNPP, as part of the Spanish-BWROG, is currently analyzing the generic products of the US-BWROG Accident Management Guidelines (AMG) in order to generate their specific ones. Also, in this BWR group, the development of tools to simulate accident scenarios beyond core damage will be studied and a training process oriented to warrant the optimum use of new EOPs/SAGs in accident scenarios will be implemented.

As a starting point for a simulation tool development, CNPP has its specific model of some severe accident codes: to support IPE analysis a model for CNPP with MAAP3.0B was developed and qualified. The purpose of the model qualification was to check the correct operation of systems and equipment, together with the simulation reliability of the phenomena that occur in various scenarios. This was structured in four groups: operational transients; abnormal transients simulated previously with RETRAN; loss of coolant accidents and sequences for checking the appropriate behavior of the drywell, suppression pool and vent models and containment systems. Other severe accident codes as CONTAIN and MAAP4 were prepared in order to use them for some containment analysis in the CNPP-IPE.

With all the sequences run with MAAP3.0B a database was built to allow operation people training in sequences evolution. This is called DATAMAAP.
The specific MAAP4-CNPP model is being improved through the controls and kinetics in order to get a more reliable code and to use it as the core of a severe accident management tool. This tool is currently under development and it has a modular design. All the simplified diagrams of the important systems are being integrated in its structure and the user will be able to operate the simulator through these pictures. Other modules to be developed are those used to validate the signals and to estimate variables not directly measured. It will be connected to DATAMAAP in order to allow selecting cases and running them again changing the final time or whatever other parameter.

CNPP is also developing its specific Technical Support Guidelines (TSGs). The purpose of the TSGs is to specify engineering support activities which may be undertaken by the Emergency Response Organization staff to directly assist the control room operating crew in the execution of EOPs/SAGs. The TSGs will provide the following products to the operating crew: current and forecast values of the EOPs/SAGs control parameters, continuing assessment of the plant status or condition, evaluation of the continued availability or the time required to repair and restore plant systems and recommendations about priority for system restoration. CNPP is implementing these TSGs in a database structure designed to be easily handled for non-expert users. This tool will be located at the Technical Support Center (TSC).

CNPP is trying to get ready for any kind of accident that may occur at the plant. CNPP has learnt through PSA/IPE which accident sequences are the most significant and which are the most likely. This knowledge is also being useful for operation and maintenance people through the risk monitor. Also, a number of severe accident codes have been adjusted to the particularities of the plant to undertake these PSA/IPE studies and now they are essential for the accomplishment of simulation tools helpful in severe accident situations.

2. INTRODUCTION

The Cofrentes Nuclear Power Plant, owned by IBERDROLA, is located in Valencia (in Southeastern Spain). It has a BWR/6 boiling water reactor, and a Mark III containment, both General Electric design. Its nominal electric power is 990 MWe. It has three electrical divisions, with three emergency diesel generators. Its commercial operation began on May 1985.

In 1989, IBERDROLA began CNPP Level I PSA activities, with a large participation of own personnel. The acquired knowledge was useful for improving some punctual aspects of design and procedures concerning generation and plant maintenance. Likewise, the availability of probabilistic tools allowed their use on license and exploitation support.

Currently the CNPP IPE is being finished, and its results will be useful for the implementation of the Severe Accident Guidelines at the plant during next years.

In order to obtain and use the maximum information from the PSA/IPE study, CNPP is currently developing different computerized tools to support maintenance, engineering, and operational activities.
This tool is expected to be user-friendly and does not require the deep knowledge of the PSA/IPE itself or a specific experience with thermal-hydraulic codes.

3. **CNPP Risk Monitor**

CNPP as other nuclear power plants is trying to remain cost competitive with other energy producers reducing cost. One of the areas in which cost reduction is getting significant is in Operation and Maintenance (O&M). O&M costs are being reduced by increasing the intervals between refueling, reducing outage duration, and increasing the amount of maintenance performed at power. Plants performing on-line-maintenance must clearly justify these activities by demonstrating a net safety benefit. Plant evolution must be adequately monitored to prevent high-risk configurations and the plant must demonstrate the ability to evaluate and respond to emerging issues effectively.

CNPP is working in this way and is using the EPRI's Risk Monitor EOOS, which is a tool that contains the infrastructure to assist the PSA staff in expanding and expediting their analysis capabilities.

EOOS is a tool that has also other important uses at the plant:

- **Operation support in decision making.** EOOS can provide operator with valuable information about the possible risk increasing if some component is declared inoperable. This information helps the operator to choose the best moment to do some actions.
- **PSA and PSA applications support.** EOOS is able to quantify the entire PSA in minutes. This tool is able to assist in addressing issues like a justification of a technical specification change or an analysis of a modification.
- **Maintenance Rule support.** This tool is useful in tracking the performance criteria.

EOOS has been installed at the CNPP Maintenance Technical Office since last year and nowadays it is being installed at the Control Room for a testing period of six months, in order to have the tool ready there during next year.

3.1. **EOOS for Operators**

EOOS for operators provides a real-time equipment status and risk calculation for specific configurations.

EOOS can help operators develop strategies for responding to emerging work:

- **The EOOS Dynamic Model can quickly evaluate any unforeseen configurations**
- **The EOOS "Top 10" list can be used to determine the most important equipment to restore and protect**
- **Equipment status displays provide for user input to compensatory actions and contingency planning**
EOOS can be tailored to operator needs
EOOS can model other risk measures that may concern an operator, such as likelihood of plant trip or significant event
Tracking routines allow operators to determine causes of loss of defense-in-depth for safety functions
The EOOS validation features helps builds operator confidence

Some of the main features of EOOS are:

- Automatically loads from the electronic book and the plant database. This allows the user to communicate with the tool in the plant language and the translation into basic events is done automatically.
- Selection from drawings. The user is allowed to select components from plant system diagrams.
- Manual selection from “pick list” hierarchy (i.e., select by activity, system, train, component, etc.)
- Output Display:
  - A risk-based Plant Safety Index (PSI) number
  - A multicolored PSI “meter” to trigger safety management actions
  - A time limit for the current configuration, based on a preset goal for plant safety
  - A panel of system status-based defense-in-depth indicators
  - List of activities that cause loss of function

Color coded P&IDs help explain and communicate system status.
Component selection from drawings

3.2. **EOOS for Schedulers**

EOOS is useful in programming future activities of maintenance, testing and surveillance, that generate unavailabilities of systems and equipment in acceptable risk basis criteria. EOOS calculates the combined effect of simultaneous maintenance activities over the front line systems, safety functions and global risk.

The information generated by EOOS is:
- Status of systems and safety functions versus time
- Probabilistic Safety measure, in terms of PSI (Plant Safety Index)
- Identification of components with mayor impact on PSI

EOOS for Schedulers uses data from the planning schedule to provide:
- Automatic schedule loading that is consistent with schedule method (e.g., component, train)
- Output displays
  - Schedules, system status-based defense-in-depth, and plant risk; and
  - Multiple time scales (several different schedule results can be displayed simultaneously)
- Interpretation
- View of schedule, system status-based defense-in-depth and risk levels on same screen
- All operator screen functions are accessible by clicking on the schedule display, and
- Unavailability summary report for Maintenance Rule performance evaluation

EOOS helps schedulers plan more efficiently by:

- Using a dynamic model that can evaluate alternate configurations and alternate strategies
- Operating at multiple levels of detail. Schedulers do not have to determine system or train status
- Validating defined system windows at a component level of detail. This eliminates misassigning a component to an improper system window
- Linking to pre-defined maintenance activities

EOOS also helps schedulers control O&M costs by minimizing both actual and potential downtime. In addition, by addressing all modes of plant operation, it minimizes training time and eliminates the effort needed to translate from one modeling framework into another.
3.3. EOOS for PSA Analysts

PSA Analysts are in charge of providing support to Operators and Schedulers, through a deep interface with EOOS. PSA Analysts tasks are:

- EOOS database generation. This database should have seven tables which define the relationship among components, systems, trains, maintenance and basic events from the PSA.
- Operator screen definition.
- Connection of plant systems diagrams to EOOS to allow its use by Operators.
- Environment effect definition. E.g., increased trip likelihood by severe weather.

EOOS displays are driven by PSA-based logic models. The model maps both combinations of equipment needed to satisfy plant requirements and combinations of failures leading to core damage.

EOOS processes equipment and plant status information input manually or from plant information systems to update the PSA model. EOOS then solves the model to provide both qualitative (e.g., equipment status, functions or tech specs) and quantitative (e.g., safety index, core-damage frequency, train availability) results. EOOS presents plant operators with a single "snapshot" of plant status. When used for scheduling, EOOS solves the model for each "time step" (configuration change) in the schedule. The results
then appear as a risk profile versus time that appears on the same screen with the schedule.

EOOS dynamically manipulates pre-validated results, and solves the model to evaluate unaanalyzed configurations. This approach maximizes speed (seconds) and accuracy of the results, while preserving flexibility in evaluating all possible configurations. PSA analysts do not need to evaluate hundreds of pre-solved cut sets.

3.4. Possible additional uses of EOOS

Currently the Risk Monitor is designed and used to support plant normal operation and maintenance, but several ideas are foreseen to use its capabilities to support severe accident management in conjunction with other tools.

A new module can be developed to evaluate the progression of a level 1 sequence into the level 2, and quickly quantify its impact on the release frequency.

Any change in plant configuration could be introduced to EOOS and the core damage frequency of this new plant state could be rapidly evaluated. This can be connected to a new module which could associate this level 1 sequence to a Plant Damage State (PDS) and a specific Containment Event Tree (CET).
This module could connect EOOS with the severe accident management tool which is currently under development.

4. **CNPP SEVERE ACCIDENT MANAGEMENT TOOL**

4.1. **Current Development**

CNPP has carried out an study for the definition of the most interesting severe accident management tools for the plant. The purpose of this study was the definition of the optimum graphical interactive tool which allow the viewing of data received in real time from the MAAP (Modular Accident Analysis Program) code for severe accident analysis. This tools will be also useful for training in severe accidents as well as for emergency drills preparation.

After reviewing most of the tools related with this main purpose available in the market, it has been decided that a modular structure supported on PC is the best option with a structure like this:

![Diagram of CNPP Severe Accident Management Tool](image)

A hardware configuration of two computers will be needed: one with D.O.S. operating system in which the MAAP code will be installed, and the second one with MS Windows NT in which the SCADA Factory Link and the database will be installed.

This tool will consist in several modules:
• The MAAP code, in its advanced version MAAP4.0.3 for BWR. This code covers all
  the severe accident phenomenology, in a simplified way, allowing short execution
times. The scope of this tool development includes two improvements in the MAAP
code: Control and Kinetics.
The MAAP code is able to carry out predictive and tracking functions, since the code
is built with some degrees of freedom to adjust the phenomena to the diagnostic
conditions.
Using the MAAP code, the on-line actualization is not possible but a new case with
the new boundary conditions determined from the new diagnosis. This is due to the
complexity of the phenomena treated in an interrelated way which difficult the
adjustment. It is also due to the difficulty in obtaining some variables needed to
initialize the calculations even by indirect methods.

• A database recording the experience gained with the code through the years doing
  IPE/PSA and license analyses. This database will include the main information of the
  accident sequences analyzed with the MAAP code for different purposes. It is also
  foreseen to enhance this database with data of the sequences analyzed with other
codes like CONTAIN which can provide the user with useful information of the
  progression of the accident in the containment.
This database will have also the possibility of be used for training purposes, because it
will be easy to find which sequences have been analyzed, and the evolution of the
main parameters in them looking through:
  • systems out of service,
  • initiating events like LOCA, ATWS,
  • initial conditions of the plant
The information that the database will be able to provide with is:
  • Plots of significant variables evolution
  • Timing of significant events: core melting, vessel failure, containment failure, etc.
  • Status of systems
  • Main parameters values
This will be useful not only for training but for managing an accident, since a forecast
plant status and evolution forecast could be quickly done when a sequence from the
database is identified to be similar to the accident sequence.

• A graphical interface will be developed. The simplified diagrams of the main system of
  the plant will be included as screens, with the possibility to interact with the rest of
modules through hot points. A different set of screens will be developed too in order
to show the evolution of the main parameters of the plant.

This tool will have also three additional modules:

• The signal validation module which will identify faulty process signals and will generate
  best estimates for process variables. This module is not developed yet, but probably will be
made using fuzzy logic and neural networks.

• To prepare the entry data to the code, it will be necessary to build a new module
  which main purposes will be:
  • to pick up the necessary plant data from the signal validation module,
• to calculate the plant variables that are not directly measured and are needed to do a diagnosis,
• to determine the plant state: initiator event, status of systems and containment,
• to give recommendations about the sequence evolution for the first input to the code.

This module will be the diagnosis module which will process the data coming from the plant through the signal validation module and will process them allowing the user to identify the status and conditions of the plant in a single moment of the accident.

• The fitting module which will control the MAAP code execution. Through this module it will be possible to compare the results of a simulated scenario with the diagnosis done at equivalent time and measure their differences, in order to adjust the input to the code to reproduce the initial moments of the accident sequence closely. This module will also be able to look for an analyzed sequence in the database similar to the new diagnosis done. With this two inputs this module will provide to the user with recommendations to initialize a new simulation which will be closer to the diagnosis that the former one. This process will be repeated any time the diagnosis module produces a new result: the fitting module will compare the plant state obtained from MAAP4 calculation with the new plant state processed through the diagnosis module, allowing the adjustment in a semiautomatic way of the simulated scenario to the diagnostic done.

All the modules will communicate through a graphical interface created in Factory Link. This interface will have several screens which will allow an easy use of the tool and a quick way to interpret the obtained results.

4.2. Use of HALDEN Project tools

IBERDROLA, as part of Spanish membership of OECD HALDEN Reactor Project, has been interested in its work concerning the area of Man-Machine Interface and in particular the CAMS (Computerized Accident Management Support) which is a system that can provide assistance to the staff in the control room and in the Technical Support Center. This system offers support in identification of the plant state, in assessment of the future development of the accident, and in planning of accident mitigation strategies. In this way, the purpose of this system is quite similar to the purpose that CNPP is looking for with its own severe accident management tool, but inside design basis conditions.

Since currently the CAMS system is being developed to cope with non severe accidents, CNPP together with other Spanish participants in HALDEN identified the possibility to enhance the capabilities of this system making possible the integration of the MAAP code in it; in order to extend CAMS to the severe accidents field.

To be able to use the MAAP4 code in the CAMS system it is expected a modification in its structure in order to include in it two new modules, the diagnosis module and the fitting module to use them instead of the original Tracking Simulator and State Identification modules of CAMS in severe accident analysis. The possible new structure is shown in the following figure:
Therefore, the main purpose of this two modules is to introduce the possibility of using, in a controlled way, the MAAP4 code in the CAMS system for severe accident analyses.

On the other hand, CNPP will take advantage of the idea of the signal validation module of CAMS although it will probably need to be adapted to the severe accident field too.

5. TECHNICAL SUPPORT GUIDELINES

A nuclear power plant severe accident management program will be comprised at least of the following six elements:

- Severe accident management guidance
- Training in severe accident assessment and mitigation
- Computational aids for decision support
- Definition of instrumentation needs
- Delineation of decision-making responsibilities
- Continuous reevaluation of severe accident response capability.

To support these programs, the BWR Owners Group has issued a document which include the guidelines for the severe accident management in the Spanish plants.

This document was based on the following from the US BWROG:
1) Emergency Procedure Guidelines Update  
2) Severe Accident Guidelines  
3) Technical Support Guidelines

The EPGs update provides several changes to the existing Revision 4 of the EPGs. These changes are focused on identifying the entry point into the Severe Accident Guidelines (SAG). The SAGs include guidance on the Integrated Containment Flooding Strategy along with revisions to containment venting strategies. The bulk of the development effort is found in the Technical Support Guidelines and describes how engineering support activities may be undertaken by the Emergency Response Organization (ERO) staff to assist the Control Room in Severe Accident Management.

5.1. TSGs Implementation at CNPP

Implementation of the TSGs involves the development of data tables and plots to be used in responding to a potential severe accident, which will be implemented in a database, making easy its use by TSC people. These tables and plots are focused on:

1) Identification of current conditions  
2) Predicting the evolution of EOP control parameters  
3) Estimation of system availability and recovery times  
4) Updating EOP limit curves as accident conditions change  
5) Prioritizing system restoration

These major tasks are described in the following four sections.

5.1.1. Control Parameter Status Assessment Guideline (CPAG)

The purpose of the CPAG is to evaluate the operability and reliability of instrumentation needed to assess the plant status. A Parameter Assessment Table (PAT) is constructed for each parameter that is identified in the EPG and Severe Accident Guidelines (SAG). The input information for each instrument includes:

- Instrument ID  
- Location of Readout  
- Range of Instrument  
- Required Power Source  
- Environmental Limitations: Temperature, Pressure, Radiation, and Water Levels

Actual implementation of the CPAG involves adding the following current plant conditions to the table as the sequence develops:

- Power Source Availability  
- Is instrument in service?  
- Environmental Conditions: Temperature, Pressure, Radiation, and Water Levels  
- Current Instrument Readings
The output from each table is a "best" value for each control parameter.

Reference material being used to develop the tables includes:

- Cofrentes Level 1 IPE
- Plant Final Safety Analysis Report
- Plant Technical Specifications
- Plant Equipment Environmental Qualification Study

Approximately 11 control parameters exist in the Cofrentes EOPs and a table is required for each. This parameters are:

- Reactor pressure vessel water level
- Reactor pressure vessel pressure
- Reactor power
- Suppression pool temperature
- Drywell temperature
- Drywell pressure
- Hydrogen concentration in drywell
- Primary containment water level
- Primary containment temperature
- Primary containment pressure
- Hydrogen concentration in primary containment

5.1.2. Plant Status Assessment Guideline (PSAG)

The purpose of this guideline is to:

1) Forecast control parameters,
2) Determine current plant state, and
3) Update EPG limit curves.

Through the use of Parameter Trend Plots (PTP) and Parameter History Tables (PHT), the control parameters are tracked as a function of time. Critical limits on these parameters are also identified. Some simple calculations are also used to supplement the estimation of future values. Also included in this guideline are techniques to aid in the identification of events such as "RPV Breach by Core Debris." Finally, EPG limit curves can be re-calculated as conditions change to provide a more accurate limitation.

The activities required to implement this guideline include:

1) Create Parameter Trend Plots that include identification of all important limits. Actual data for each parameter will be added as accident sequence progresses.

2) Create relationship plots to support PTP (e.g. a graph of pool level vs. volume).
3) Create "Blank" Parameter History Tables for each control parameter.

4) Create a series of source term results from MAAP analyses. Plots of containment radionuclide concentrations will be generated for each accident class to assist in responding to a hypothetical accident. These results can be useful in confirming sampled radionuclide concentrations and can provide needed insight if gas sampling is unavailable.

5) Create plant-specific tables for recording appropriate plant environmental conditions.

6) Similar to item 4 above, create figures depicting accident signatures for each accident class. This signatures will be, for instance, the expected RPV pressure, Drywell Temperature, and Drywell pressure trends for a hypothetical Class III (LOCA) core damage sequence, previously analyzed with MAAP.

7) Prepare alternate EPG limit curves that reflect conditions that are different from the original basis for the curve. Approximately six limit curves would be constructed using new boundary conditions.

8) Create a flow chart which allows the identification of vessel breach occurrence.

5.1.3. System Status Assessment Guide (SSAG)

The purpose of this guideline is to evaluate the operability and reliability of plant systems through the creation of a set of tables which require that the following component level data be collected:

- Component ID
- Location
- Restoration Requirement (if out of service)
- Control Power Source and its availability in hours
- Motive Power Source and its availability in hours
- Pneumatic Source and its availability in hours
- Component Cooling and its availability in hours
- Environmental Limitations; temperature, radiation, and water level.

The following information is required on the overall system.

- Valve positions when system is aligned
- Time required to align components
- System limits other than alignability and component operability (i.e. system interlocks)

This set of tables is being created for each system required by the EPG to perform a function. The list of systems is on the order of 10-20 and is based on the systems modeled in the Cofrentes Level I PSA.
Also, a System Utilization Table (SUT) is created which lists each system, system functions, and all of the EPG control parameters that are controlled by the utilization of that system. This information is available from the existing Cofrentes Level 1 PSA.

5.1.4. EPG Action Assessment Guideline (EAAG)

The purpose of this guideline is to prioritize system restoration and to estimate times for specific actions to be taken. In order to accomplish these tasks, input from the control room on their current location within the EOPs is needed.

For each EPG action, a Timing Assessment Table (TAT) is created to assist in identifying the optimum time for performing that action. Input for the TAT includes:

- system availability from SSAG
- estimated times to reach system and EPG limits from PSAG

For each EPG action, all control parameters that are affected are listed. For each control parameter, a list of all specific effects are listed. For example, the EPG action to initiate wetwell venting can impact the RPV water level, Suppression Pool Temperature, and the Primary Containment Pressure. The specific impact on the RPV water level may be due to NPSH limits on pumps currently taking suction from the suppression pool. Timings for the EPG action are also identified based on the predicted evolution of control parameters and the impact of this on systems availability. Using a series of weighting factors, the importance of performing a specific EPG action at a specific time can be calculated. Adding the weighted importance for an action for all of the control parameters that are affected allows for the determination of the optimum time to perform an action.

A total of approximately 5-10 actions would be investigated. Close communication with the plant staff is essential to assist in determining the importance that each action has on individual control parameters.

5.2. Use of the TSGs by the Technical Support Center

The database containing the TSGs will be installed at the Technical Support Center. It will be a useful reference tool for gathering information about Severe Accident Guidelines steps, in conjunction with the rest of computerized tools that will be available at the Technical Support Center.

6. SUMMARY AND CONCLUSIONS

As a consequence of the PSA/IPE and with the purpose of the integrating all the knowledge acquired through this studies, it seems convenient the development of computerized tools that do not require a deep knowledge of the PSA/IPE methods. These tools should be user friendly and should be able to provide the user with information about core damage frequency. The purpose is also to get tools that will be useful under severe accident conditions, being able to forecast the core damage
frequency and the progression of the accident into the containment much faster than real
time for any plant configuration.

These tools will be useful as a support in decision making for people responsible of the
accident management.

Some of these tools has been installed at CNPP and some others are still under
development. It is foreseen its continuous development and improvement as a function
also of the response of plant people.

These tools are being developed in a modular way, in order to allow the
interconnectability among them, as well as with some other tools for the plant data
acquisition or with new tools that could be acquired in the future.

For all this work it has been taken advantage from the international experience, like this
from EPRI through the Risk Monitor, EOOS, or through the MAAP code for
thermohydraulics and severe accident phenomena, and also like the HALDEN
International Program through CAMS.
Reactor Safety Assessment System (RSAS) 
Development and Lessons Learned

James O'Brien and Donald Marksberry, 
U.S. Nuclear Regulatory Commission 
Mohammed Modarres, University of Maryland

ABSTRACT

An overview of the NRC's Reactor Safety Assessment System (RSAS) is provided, including a description of its features, the stages of its development, and lessons learned. RSAS is intended to be used at the NRC Operations Center if a serious event occurs at a nuclear power plant. RSAS utilizes two generic models (one for pressurized-water reactors and another for boiling-water reactors), which are automatically edited using data from plant-specific files to provide plant-specific instances of the models for each nuclear power plant in the United States. The RSAS model consists of two diverse hierarchical logic trees for determining the status of critical safety functions.

1 Introduction
The United States Nuclear Regulatory Commission (NRC) is developing a knowledge-based system for use at its Operations Center should a serious event occur at a commercial nuclear power plant in the U.S. This system is called the Reactor Safety Assessment System (RSAS).

Before discussing RSAS, the NRC's organization for responding to nuclear power plant events in the U.S. is briefly described in order to provide an understanding of how RSAS fits into this organization. Nuclear power plant operators have primary responsibility for operating the plant safely and for responding to an event at the plant. The NRC is responsible for monitoring plant operator response in order to ensure that appropriate onsite corrective actions are being taken and appropriate offsite protective actions are being recommended. The NRC responds by activating its Operations Center, located in the main offices of the NRC in the suburbs of Washington, D.C., to monitor the event remotely and by sending a site team to the plant to monitor the event locally. The NRC developed RSAS to help the NRC staff at the Operations Center monitor the status of the plant during an event.

This paper provides an overview of the features and operation of RSAS, and describes the developmental process and the lessons learned from the development of RSAS.

2 RSAS Features and Operation
The following features of RSAS are described in this section: (1) critical safety functions, (2) equipment and parameter trees, (3) support system matrix, and (4) parameter displays.
In addition, the operation of RSAS and the tools for generating a generic plant model and editing the generic models to develop plant-specific models are briefly described.

2.1 Critical Safety Functions
The primary feature of RSAS is its ability to monitor, evaluate, and display the status of critical safety functions. The following critical safety functions have been defined in RSAS for pressurized-water reactors (PWRs):

- Reactivity Control: Ability to reach and maintain shutdown conditions
- Inventory Control: Ability to maintain adequate water inventory for heat transport
- Reactor Coolant System (RCS) Pressure Control: Ability to maintain pressure which supports heat removal
- RCS Transport Control: Ability to transfer heat to the heat sink
- RCS Integrity Control: Ability to maintain the pressure boundary integrity
- Heat Sink Control: Ability to maintain an ultimate heat sink (i.e., a reservoir to which decay can be transported to)

These critical safety functions were identified from a review of emergency procedure guidelines (Refs. 1 to 3) prepared by PWR owners groups. Each of these critical safety functions supports the goal of core protection.

Two different methods are used to determine the status of each of these critical safety functions: (1) the critical safety functions are determined from current readings and trends of parameters (e.g., reactor pressure and core exit thermocouple readings) compared to normal bands for these parameters; (2) the critical safety functions are determined from the availability of plant equipment needed to support the critical safety functions. Both methods use logic trees to identify the equipment or parameters supporting the critical safety functions. These trees are described in the following sections.

2.2 Parameter Trees
The parameter trees are made up of "nodes" that are connected to a top "critical safety function" node via logic gates. See Figure 1 for an example of a parameter tree for determining the status of one of the critical safety functions. The status of each of the nodes can be either: (1) normal, (2) improving, (3) degrading, (4) degraded, (5) unknown, or (6) conditional. The status of each of the nodes is automatically determined by evaluating the parameter against setpoints which delineate normal conditions from degraded conditions. The parameter values are provided to RSAS via a link to the Operations Center Emergency Response Data System (ERDS) computer, which is also linked to each of the nuclear power plant ERDS computers to obtain real-time plant data (Ref. 4).
2.3 Equipment Trees

Similar to the parameter trees, the equipment trees are made up of "nodes" which are connected to the critical safety function nodes via logic gates. See Figure 2 for an example of an equipment tree for determining the status of one of the critical safety functions. However, in contrast to the parameter trees, the status of each or the nodes for the equipment trees can be either (1) confirmed available, (2) assumed available, (3) unavailable, (4) unknown, or (5) conditional. In further contrast to the parameter tree nodes, the statuses of the majority of the equipment tree nodes are not automatically determined; rather, the statuses of the lowest level nodes need to be set manually by the RSAS operator. Initially, upon RSAS startup, the status of all the equipment nodes is set to "assumed available." For this status, the nodes have a white background. If a node is set to "unavailable," the background color is changed to black and any of the parent nodes connected to this node will change status (and background color) depending on the logical relationship between the parent node and its "children" (and the status of the other children nodes).
2.4 System Matrix
In order to show, in a compact manner, the relationship between the front-line safety systems and their supporting systems (i.e., electrical and cooling water), a support system matrix is used in RSAS (see Figure 3). The nodes on this matrix have the same status options as the equipment trees, i.e., (1) confirmed available, (2) assumed available, (3) unavailable, (4) unknown, or (5) conditional. The status of the nodes on the left-hand side of the matrix is set by the operator, and the status of the nodes on the top of the matrix is determined by the logical connection with the support systems.
2.5 Parameter Displays
Another useful feature of RSAS is its ability to display the current value and trends of key plant parameters that may have an impact on the critical safety functions. Figures 4 and 5 show examples of the displays that are available. The RSAS operator has control over the parameters and the ranges of the parameters that are displayed in the trend plots.

Figure 4: Parameter Schematic Display

Figure 5: Parameter Plots Display
2.5 RSAS Operation

During an event RSAS will be operated in the "ERDS input" mode. Other available modes are the training, system manager, or auto test modes. The ERDS input and system manager modes are briefly described.

2.5.1 ERDS Input Mode of RSAS Operation

In the ERDS input mode of RSAS operation, the user selects the data input mode (automatic or user request). In the automatic mode, the user selects the input interval. RSAS was developed considering that a 2-minute input interval would typically be selected; although, RSAS can accept up to a 1-minute ERDS input interval.

RSAS then will obtain ERDS data at the interval specified by the user and will display the status of the critical safety function as determined by the status of supporting nodes, which are in turn determined by the ranges within which the ERDS parameters fall. The RSAS display is shown in Figure 6. The critical safety functions windows are always displayed at the top of the screen. The RSAS user can select what is to be displayed in the middle part of the screen, e.g., parameter or equipment trees, support system matrix, or parameter plots. When the status of the critical safety function changes, the critical safety function display flashes until the RSAS user acknowledges the change. The critical safety functions can also be determined by the status of equipment supporting the function which is manually input by the RSAS user. The status of the equipment is obtained via phone communication with the plant. In addition the user can perform "what if" runs to determine how the status of the critical safety functions would change if the status of certain equipment were to change.

2.5.2 System Manager Mode of RSAS Operation

This mode of RSAS operation is used to generate the generic model and plant-specific files. Software tools have been built into RSAS for creating nodes and specifying the logic between nodes. In addition, rules can be specified for determining the bands of parameter values which indicate whether the node status is "normal," "degraded," etc. A primary function of the system manager mode is to develop plant-specific models from the generic model. This is done by deleting inapplicable nodes, changing the names of generic nodes to reflect plant nomenclature, and providing plant-specific setpoints. When the plant-specific model is saved, the RSAS software saves the instructions that specify the changes that were made to the generic model. When a specific plant is chosen to be operated or edited in RSAS, the generic model loads up and then is automatically edited using the instructions in the plant-specific file. The RSAS operator then "sees" the same plant-specific model which was created in the system manager mode.

3 Steps in RSAS Development

The development of RSAS involved the following steps: (1) identification of the need that the system was to fulfill and performance of a feasibility study, (2) identification of the scope, requirements, and limitations of the project, (3) choice of a logic model and software to develop the system, (4) prototype development and testing, (5) generic model development, and (6) plant-specific file development.
3.1 Need for RSAS

RSAS development began with the identification of the information that would be beneficial to the NRC in its response to events. The status of critical safety functions was identified as beneficial information. The RSAS development team determined that it would be beneficial to determine the status of the critical safety functions from two different perspectives, i.e., by parameters that indicate degradation of the functions and by the status of equipment that is needed to support these functions.

A feasibility study was performed by developing and testing a paper model of the logic for determining the status of critical safety functions. The paper model showed that a system for determining the status of critical safety functions could be developed for the NRC Operations Center and that such a system would be useful; however, because of the large amount of information that would need to be updated as plant conditions changed, a computerized version of the model was developed.

3.2 Scope, Requirements, and Limitations of RSAS

The next stage in the development of RSAS was to identify the scope, requirements, and limitations of the project.
In regard to the scope of RSAS, the system was designed to monitor plant status during an event at any of the more than 100 commercial nuclear power reactors in the United States. About two-thirds of the reactors are of the PWR type and one-third are of the boiling-water reactor (BWR) type.

In regard to the requirements for RSAS, the system had to be easy to use in a stressful environment and to require minimal training for the RSAS operator. In addition, RSAS was required to have software tools that would allow for updating plant model knowledge without having to modify the underlying computer program.

Cost and information availability were the two primary limitations of RSAS. In order to minimize the cost of generating a logic model for each plant, a generic logic model was developed which could then be edited to account for plant-specific features. The data sources that were available for use with RSAS during an event were limited to those that were already available to the NRC Operations Center: plant parameter data via the ERDS computer and system status information via telephone lines connected to the plant's emergency response facilities. In addition, there were limitations to the sources of plant information available for developing the plant-specific RSAS models. The information used to develop RSAS was obtained from NRC Operations Center's plant information books that, in turn, were developed from plant-specific final safety analysis reports and technical specifications. Plant-specific emergency operating procedures and piping and instrumentation drawings were not used.

3.3 RSAS Model Selection
The next step in the RSAS development was the selection of the type of model to use. The NRC chose the goal-tree success-tree as the model for the system because its functional and hierarchical form provided a good structure for developing a generic model. There are many differences between the plants in the United States, but from a functional view, the plants' systems serve similar functions (e.g., reactivity control, heat removal). Other benefits are that the goal-tree success-tree model is easy to understand, build, update, and review. Because of the significant differences between PWRs and BWRs, two generic model was developed for each of these types of reactors. The PWR model was developed first.

3.4 Prototype and Generic Model Development
Following the choice of the model type, the NRC first developed and tested a prototype of RSAS for the Calvert Cliffs plant and then developed a generic PWR model. In addition, a set of software tools was created for modifying the generic model to reflect plant-specific features. Next, plant-specific models were developed for the Three Mile Island and Braidwood plants from the generic model in order to test the ability to create plant-specific files from the generic model.

3.5 Current Status of RSAS Development
Currently plant-specific files for all of the PWR plants\(^1\) have been developed. In addition, a

\(^1\) Except for one plant-specific model which is pending completion of the plant information book.
generic model for BWRs has recently been completed and a plant-specific prototype of the Nine Mile Point Unit 2 power plant is being developed. This model is scheduled to be tested during Nine Mile Point’s September 1997 emergency preparedness exercise. Plant-specific files for all of the BWR plants should be completed in October of this year.

4 Lessons Learned
Many technical lessons have been learned during the development of RSAS. However, before discussing some of the individual technical lessons learned, some important general factors that should be considered during the development of a knowledge-based system are discussed.

The first factor is that the system users (including people who will get data from the system) need to be kept involved in the development of the system. A knowledge-based system will not be useful if it is not well integrated with the organization in which it is to be used. Early in the development process, users were kept closely involved in RSAS’s development. A second factor is that human factors should be considered during a knowledge-based system’s development to ensure that the information that it displays will be easy to understand (i.e., the right type and amount of information, good spacing between different information types, and the right fonts and size of displays). Human factors were considered during the development of RSAS.

4.1 Benefits and Limitations of the Equipment Tree Model

Benefits
The use of a hierarchical tree for determining the status of critical safety functions has some benefits and some limitations. Among the benefits is the capability to provide multiple layers of detail for the way in which the critical safety functions are met. This is beneficial because the upper part of the tree will be the same for all PWR plants. The bottom part of the tree, which refers to actual systems and components, will need to be changed to reflect the specific plant being modeled. This allows for a very structured process that makes it possible to quickly modify the generic model to develop the plant-specific models. The use of a generic model has been very beneficial in minimizing the time needed to produce plant-specific files for each nuclear power plant in the United States.

Limitations
One limitation found in developing the equipment tree model is that it is difficult to account for the many alternate ways that systems may be operated. This caused problems in (1) determining whether to provide credit for certain cross-connects, (2) finding information on the availability of cross-connects or alternate configurations, and (3) increasing the size and complexity of the tree. This was mainly a problem in modeling cooling water systems (e.g., service water and component cooling water).

Another limitation is that the model does not simply account for time dependencies. An example of this is the situation in which two different systems are dependent on each other for operability, such as ac power and cooling water. The ac power is needed to run the cooling water pumps and cooling water is needed to run the emergency diesel generators. A method was devised to work around this limitation using an iterative
procedure.

4.2 Availability of Plant-Specific Data
During the editing of the PWR generic model to develop plant-specific models, a large amount of equipment and setpoint data which was called for in the generic model was found not to be provided in the some of the plant information books. In addition, some of the parameter data required in the model was not provided as ERDS data for a specific plant or the ERDS data did not contain needed supporting information. Examples of the type of information which was missing include:

**Missing Plant Equipment Data**
- pump shutoff heads (condensate, safety injections, etc.)
- support system normal lineups and cross-connects
- power supply data for safety-related components

**Missing ERDS Data For Plant Parameters**
- tank levels (Condensate, Boric Acid Water Tank)
- pump flows

**ERDS Data Lacking Supporting Information**
- steam generator level conversion data (from percentage to a referenced level in the steam generator)
- valid range of some ERDS data not provided

In some cases, the missing data will place added burden on the RSAS user to obtain and input data needed to determine the status of critical safety functions. For example, not having information on steam generator levels makes it impossible to automatically determine the status of the heat sink critical safety function from the parameter tree. In order to minimize this burden, a change to the RSAS software is being pursued to ease the process for setting node status. The availability of plant-specific data is being taken into at an early stage in the development of the BWR generic model in order to minimize the impact of information limitations.

5 Conclusion
RSAS is potentially a very useful system for assisting the NRC in monitoring emergency response. The editing of generic models to develop plant-specific models is a good method for minimizing the cost of the plant-specific model development. The PWR version of RSAS is in the final stages of development. Lessons learned from development of the PWR version will be useful in expediting the completion of the BWR version of RSAS.

**Acknowledgements**
Idaho National Engineering and Environmental Laboratory provided substantial support in the RSAS software, BWR generic model, and plant-specific file development. Principal contributors include Don Sebo, Tom Ballard, and Steven Conroy.
References


Guidance for Reactor Operators and TSC personnel with the Severe
Accident Management Guidelines

M. F. Van haesendonck
R. P. Prior
Westinghouse Energy Systems Europe S.A.

Final Paper

The Westinghouse Owners Group Severe Accident Management Guidelines (WOG
SAMG) were developed between 1991 and 1994. The primary goals for severe accident
management that form the basis of the WOG SAMG are to terminate any radioactive
releases to the environment; to prevent/failure of any containment fission product
boundary and to return the plant to a controlled stable condition.

The WOG SAMG is primarily a TSC tool for mitigation of low probability core damage
events. Their philosophy is that control room operators should remain focused on the
prevention of core damage, whereas the TSC personnel should concentrate on the
mitigation of the severe accident. The symptom based package is built up as a
structured process for choosing appropriate actions based on actual plant conditions.
No detailed knowledge of severe accident phenomena is required.

The WOG SAMG is made up of a number of components, among which the Graphical
Computational Aids (CA). These CA's were defined to fulfill the need for information
that is not available directly from plant instrumentation. The information they provide
has to meet certain requirements:

a. information on the CA must be directly needed within the decision-making
   process;

b. quantification of the information must be necessary;

c. the uncertainty of the computation should be low enough so as to provide
direction to the decision maker

The purpose of this paper is to provide some insights on how WOG SAMG, and also
more specifically CA's, can aid operators and especially TSC - personnel in the
mitigation of a severe accident.

A. Introduction

Accident Management refers to the overall range of capabilities of the plant to prevent and
mitigate accident situations which involve damage of the fuel.

Preventive Accident Management refers to the strategies that aim to prevent or delay the
onset of core damage during an accident. Preventive Accident Measures are the first
actions to be taken since they give priority to fuel integrity and restoration of core cooling.
In the Westinghouse approach to Accident Management, the preventive accident measures
are included in the Emergency Response Guidelines (ERGs), and based on those, the
plant's Emergency Operating Procedures (EOPs). Note that the EOPs deal with design basis accidents as well as beyond design basis events before the start of core damage.

In most cases, the ERGs as included in the EOPs and implemented by the operating crew result in recovery of the plant without any core damage. Should however the preventive accident measures be unsuccessful and core damage occur, then subsequent recovery actions, which place priority on containing fission products and minimizing releases, are necessary.

Events that progress past core damage are called severe accidents and the accident management measures taken to mitigate the consequences of core damage are referred to as severe accident management measures; in the Westinghouse approach they are called Severe Accident Management Guidelines (SAMGs).

The SAMGs thus contain all instructions for the implementation of mitigative severe accident management measures.

**B. Overview of the Westinghouse SAMG**

The Westinghouse SAMG package consists of symptom based guidelines that are designed to interface with the Westinghouse EOPs.

Should an accident occur that causes an actuation of the plant's automatic safeguards system then the plant operators are directed to the EOPs which provide them recovery guidance measures. However the entire purpose of the EOPs is to recover the plant before core damage occurs. Obviously, the EOPS place priority on preventing or delaying core damage. If these measures are unsuccessful core damage will occur. As soon as conditions indicating a severe accident is in progress have been detected, EOP usage is terminated and a transition to the SAMGs is established. Note that there can be no return to the EOPs. In the Westinghouse approach of SAMGs, although two control room guidelines are provided, the main part of guidance is for use in the Technical Support Center (TSC). The SAMGs are totally symptom-based. There is no requirement to diagnose the cause of the accident, the amount of core damage or the status of the reactor vessel. The SAMGs should allow the TSC to identify plant recovery actions, which will be communicated to the plant's operating crew, which is responsible for carrying out the actions. The SAMGs are a structured guidance in the form of flowcharts, status trees and guidelines. They are specifically designed for a high stress environment, therefore they are easy to use.

**B.1. Diagnostics**

The diagnostics part of the SAMGs, which is to be performed by the TSC, consists of two parts:

- a flow chart for diagnosis of the plant status in relation to a controlled stable condition,
• a status tree for diagnosis of ongoing fission product releases and challenges to fission product boundaries.

The diagnosis flow chart (DFC) specifies the key parameters to be monitored and controlled during a severe accident. It provides for continual periodic monitoring of each key parameter until all parameters are such that the plant can be declared to be in a controlled state state. The DFC considers all severe accident phenomena that may challenge the fission product boundaries. In case the value of a certain parameter is above the limit specified for a controlled stable state, the TSC must evaluate the need to implement strategies to bring the parameter to a controlled stable condition.

The Severe Challenge Status Tree (SCST) diagnostic contains four key plant parameters which must be monitored on a regular basis to determine if their value exceeds a setpoint which indicates that a more serious condition exists. The SCST is monitored in conjunction with the DFC and the evaluation of strategies identified by the flow chart diagnostics. If a setpoint value in the SCST is exceeded, all other actions are terminated and a severe accident management strategy must be implemented immediately to deal with the more serious condition. As in the case of the diagnostic flow chart, a priority amongst the severe challenges in the status tree has been established.

In summary, both the DFC and SCST identify specific Severe Accident Management Guidelines which are appropriate for a given key parameter. Each of these contains one or more strategies which might be used to respond to that parameter. The guidelines present a method for the systematic, logical evaluation of the possible strategies that can be used to respond to a given challenge.

Each of these guidelines helps the TSC staff in answering four important questions:

1. Is implementation of a strategy possible with the current plant configuration?
2. What is the balance between the potential positive and negative impacts associated with implementing a strategy?
3. How can you determine if the strategy has been successfully implemented?
4. What are the long term concerns associated with implementation of a strategy?

Computational Aids (CA) are also provided to aid the TSC staff in performing the diagnostics and in answering certain aspects of the questions raised in each of the guidelines. These CA’s are generally in the form of plots of two or three variables. They have been designed to be efficient and simple to use, requiring no computer capabilities.
C. Computational Aids

The SAMGs contain mitigative accident measures that should bring the plant to a controlled stable state and above all, mitigate any challenges to the fission product boundaries. Obviously efficient decision making is essential under these high stress conditions. In the SAMGs this decision making process is symptom-based. The plant personnel must use the available plant information to determine the best severe accident management measures. Not all of the necessary information can be determined directly from plant instrumentation, therefore computational aids were developed. Computational aids (CA) are graphical tools that will provide information that affects the decision making process. Since there is the potential for overloading the TSC personnel with too much information, CA’s were created only for needed information within the decision making process.

C.1. Development Process for Computational Aids

Since in a plant the instrumentation is limited and the extent of equipment failures may not be known, the CA’s must:

- provide results based on input parameters that can be measured at the plant,
- be useful for a wide range of accident measures.

Another issue that had to be dealt with when developing CA’s is the uncertainty regarding its calculation. Ideally all possible cases would be covered. However, taking the range of input parameters, it is clear that even for simple calculations the outcome can be different by an order of magnitude. The uncertainties and complications increase further when considering severe accident phenomenological issues. Indeed, phenomenological models can be “best fit” empirical correlations of experimental data that exhibits a significant degree of scatter. Certainly, this scatter can be further correlated to experimental conditions, but the difference in conditions cannot be measured with plant instrumentation. This leads to the prediction of an outcome based on a computational aid to be able to incorporate all the uncertainties and variabilities.

How much time is available during an accident for performing the calculation associated with a CA? To answer this question, one should keep in mind:

- during a severe accident there is an exceptional degree of stress,
- accurate answers are required,
- familiarity with the tool will most likely be limited to some training and drill exercises.
Therefore CA's should be kept simple user friendly. Computerized models were considered but not applied since:

- during a severe accident one cannot always guarantee the availability of a computer and its power source,
- complex models will not necessarily predict more accurately than simple models because of the uncertainty in severe accident analytical models,
- the cost of producing user-friendly error-free software is significant.

The format of computational aids was chosen as simple, paper-copy graphs.

The presented issues, available input data, uncertainties in the calculations and time availability led to the philosophy that CA's should not be developed unless they would directly impact the accident management decisions. Overall, this resulted in the following criteria for CA's:

- the information provided by the CA must be directly needed within the decision making process,
- quantification of the information must be necessary. This means that if a result can be trended over time, there is no need for a CA since trending provides real-time information with no uncertainty, outside of instrumentation accuracy,
- one must be able to perform the calculation with a reasonable degree of certainty. If results cannot provide direction to the decision makers during the accident, then obviously it is not worthwhile.

C.2. Usage and Examples of CA's

In this paragraph two examples of CA's are given to the reader that will illustrate their usage.

a. Volumetric Release from Vent Computational Aid

The first example presented is of the computational aid to estimate the maximum volumetric flowrate of gases that could be released due to venting of the containment (see figure 1). Obviously this information can be used to investigate if off-site dose considerations have to impact the method or timing of the venting operation. Inputs for establishing this CA are the containment pressure and the diameter of the vent line to be used. The computational aid will provide the volumetric flowrate of the containment gases based on standard atmospheric conditions (15 C and 1,013 bar). The output of this CA is intended to be used with dose projections.

Technical basis behind this CA: if a vent pathway is opened from a containment that is pressurized above atmospheric pressure then gases will flow out of the containment. The exact content of these ejected gases is rather uncertain considering the wide range of possible severe accident sequences. However the exact make-up is not that important
since it has little impact on the volumetric flowrate. The calculation of the flowrate assumes the containment atmosphere to be an ideal gas. For low pressures, i.e. below 1.87 bar, the flowrate is calculated using:

- Bernouilli’s equation,
- the density of the gas,
- the pressure difference between the containment and the atmosphere.

At 1.87 bar, the downstream pressure no longer affects the flowrate any longer because the flow becomes choked. Therefore only containment pressure and density determine the flow velocity through the orifice.

Since the output of this CA is to be used for dose calculations, the flowrate is converted to standard atmospheric conditions. Once a choked flow condition is reached, the flow velocity remains relatively constant, although the density difference from containment to atmosphere increases with containment pressure. This means that the CA results show an increase in standard flowrate with increasing containment pressure. (Note however, that if the results were based on the actual volumetric flowrate, one would see an almost constant flowrate after choked flow conditions are reached.)

The application of the First Law of Thermodynamics and fluid dynamic principles to an ideal gas are the technical basis for this CA. The possibility of aerosols plugging vent lines has not been taken into account since the purpose is to come up with the maximum volumetric release rate.

![Diagram](image_url)

**Figure 1:** Volumetric Release from Vent Computational Aid
b. Hydrogen Flammability in Containment Computational Aid

The purpose of our second example computational aid (see fig. 2) is:

- to define if the hydrogen in the containment atmosphere is flammable
- to estimate the hydrogen concentration in the containment atmosphere based on an estimated oxidation percentage.

The flammability of the containment atmosphere is not only dependent on the hydrogen concentration, but also on the presence of steam and other gases. Well-defined flammability limits were set up and formulated as a correlation with steam as the inerting medium. It was indicated that if sufficient steam is released to a combustible environment, hydrogen combustion can be precluded regardless of the hydrogen concentration in the containment. Should however a global burn occur then the resulting pressurization could cause a challenge to containment integrity. This CA thus not only provides guidance on whether a hydrogen burn can occur, but also on whether the resulting pressurization is expected to be severe enough to result in containment failure. The prediction of this maximum pressure increase is based on the simplified Isochoric Complete Combustion.

The CA is based also on the ideal gas law. In relating the volume fractions of atmospheric components to containment pressure, two main assumptions become critical: the temperature of the atmosphere and the noncondensable gases in the atmosphere. The temperature of the atmosphere is an assumption which is based on the containment atmosphere being at 100% humidity. The overall containment temperature is therefore fixed at the saturation temperature corresponding to the partial pressure of steam, which is valid for most of the postulated accident scenarios. Should the containment atmosphere become superheated, the increased temperature will cause an increase in the total containment pressure. Superheating the containment to a significant degree will occur only when the core is no longer in the reactor vessel and there is no water to cool the core debris. Superheating causes a substantial shift in the non-flammable vs. flammable regions and is taken into account in this CA. The temperature of the containment is assumed saturated for most of the CA; superheated conditions are assumed for CCI scenarios.

Usually, the atmosphere is assumed to be composed of steam, air and hydrogen. Pressurization of the containment is assumed to be the result of steaming. As the containment pressure increases, the amount of air is assumed to remain constant. The equation defining the flammable vs. non-flammable conditions is a function of the concentration of steam and hydrogen. If one uses this equation to define containment conditions as a function of pressure then it is clear that assumptions regarding the amount of air have a significant impact on the results. Obviously, the presence of any noncombustible, non-condensable gas can affect the CA figures, so “air” is used in this CA to represent all non-combustible, noncondensable gases. The higher the concentration of non-combustible, noncondensable gas, the more the containment must pressurize before a steam inert, i.e. non-flammable, state will be reached.
For two cases, the results of this CA can be significantly impacted by the amount of “air” in the containment:

- When the containment has been vented or did not isolate as designed, steam and noncondensable gases will be released. This results in a reduced hydrogen content will allows there to be a higher percentage of hydrogen before the containment is challenged by a hydrogen burn. The reason for this is that fewer moles of hydrogen produce less energy if burned. For the CA this means that the bottom line that defines the HYDROGEN SEVERE CHALLENGE region moves upwards.

Also, the reduction in noncondensable gases (“air”) causes the NOT FLAMMABLE region to be reached at a lower pressure. For the CA this means that the line that defines the right side of the HYDROGEN SEVERE CHALLENGE and HYDROGEN BURN regions move to the left.

So, if the containment has been vented or did not isolate as designed, avoiding a hydrogen burn or hydrogen severe challenge becomes easier because the regions have become smaller.

- In case of core/concrete interaction (CCI) more hydrogen and carbon monoxide are created. Both gases are combustible and increase the potential of a containment challenge. CCI also produces non-combustible, noncondensable gases which will cause the flammable vs. non-flammable regions to shift with respect to containment pressure. Containment pressure needs to increase to a higher value to become not flammable in this case; therefore it may be more difficult to avoid a hydrogen severe challenge when CCI occurs.

The computational aid contains three regions: NOT FLAMMABLE, HYDROGEN BURN and HYDROGEN SEVERE CHALLENGE. The last region indicates that a hydrogen burn can occur and the resulting pressure spike can be expected to challenge the integrity of the containment. Two additional lines can be noted on the CA, they represent the hydrogen fraction in the containment atmosphere that can be expected if 56% or 75% of the Zr-cladding is oxidized. The purpose of them is to replace or confirm instrumentation output on hydrogen concentration. This information provides bounding estimates that could be used in the absence of better data.
The two examples presented illustrate how simple and user friendly CA's are. Both input and output are in terms of variables that can be used as such by the plant personnel.

**Conclusion**

In the next few years, many LWR plants will be implementing SAMG. In the US, all plants are committed to developing SAMG, and many will use the WOG SAMG as a basis.

As part of the SAMGs, computational aids are tools required for the severe accident decision making process based on the lack of direct instrumentation indication of specific symptoms during a severe accident.

Generally, there is a tendency to provide too much information in relation to that required for severe accident decision making. This means that when best estimate predictions have not been achieved, the decision making process can make a wrong turn or even stop while discrepancies are investigated.

The generic computational aids were validated in 1994. Another validation, this time of a plant-specific SAMG-package, took place in 1995 at the Koeberg plant in South Africa.
References

3. Debra K. Ohkawa, Lutz R Jr., Taylor J., “Computational Aids for Severe Accident Management”
1) Introduction

The French National Emergency Organisation, set up and managed by Electricité de France (EDF exploitation du parc nucléaire), relies on the expert advice given by the different Technical Support Centres (EDF/SEPTEN, CEA/IPSN, FRAMATOME). For several years a great effort has been made to improve tools. The first generation was mainly concerned with computational aids such as real-time plant data acquisition and visualisation, break size calculations, containment release estimations, ... These tools were presented by CEA/IPSN and EDF/SEPTEN at the OECD NEA Specialist Meeting in 1993. Currently work is performed in the field of validation of information available to the Technical Support Centres. The three partners, EDF, CEA and FRAMATOME, have developed a prototype implementing the diagnosis and the quality of the information pertaining to the 3D/3P method.

2) Role of the Tool in the French Emergency Organisation

At the moment, the Technical Support Centres of EDF (FRAMATOME and SEPTEN) use a list of one hundred appropriate measurements that have been selected from the whole nuclear plant information. This system provides data for the 900 MWe and 1300 MWe series of the French power plants. Concerning 1400 MWe power plants, another system is under development by CEA which will use about one thousand logic and analogue measurements, allowing a wider range of validations.

The first task of the Technical Support Centres teams is to confirm the type of accident that occurred in the primary and/or secondary circuit. Then, the teams have to supply some specific calculation which will allow the triple diagnosis/prognosis on the barriers of the damaged unit.

The validated information will be used by the experts to calculate the size of the break, to try to localise it, to prognose the beginning of core uncovering and core melting or to estimate the accidental releases.

In order to get a sufficient level of confidence in the results of these calculations, it is necessary to use validated information. It was the purpose of the CEA software tool prototype. After validation, FRAMATOME and EDF/SEPTEN plan to use it early 1998.

3) Technical Presentation of the Tool

The philosophy of this tool is to present to the expert a set of essential information (e.g. state of the fuel barrier, primary water inventory, ...) for the diagnosis with a confidence level (between 0 and 1) associated to each information and the adequate explanations.

In fact the expert has not only to know the diagnosis but also how reliable the information is and why. Subsequently, the algorithms used to elaborate the diagnoses and the confidence factor have to be simple enough so that the user is able to consult the explanations in a fast and easy way.

The process to elaborate the diagnosis and the confidence factor is performed in three steps:
First step:

Each sensor is given a quality factor (FQ1) between 0 and 1. This quality factor depends on the one hand on the signal analysed for noise and saturation and on the other hand on the qualification of the sensor with respect to environmental conditions of the containment (for example, a non-qualified K1 sensor in the containment will have its FQ1 divided by two when the containment environment condition deteriorates).

Second step:

Each measurement is given a quality factor (FQ2)

Three cases are possible

a) Redundant measures, where the FQ2 factor varies between 0 and the order of redundancy. For example, with a redundancy of order 2, if each of the two sensors has a FQ1 factor equal to 1 and if the difference in the resulting measurement value is small (less than their precision) then the FQ2 factor of the measurement will be equal to 2.

b) Non-redundant measurement, but important for the elaboration of the information diagnosis. They are validated:
   - by comparing them to similar measurements. For instance the core outlet temperature is compared with the hot leg temperature.
   - by verifying physical coherence. For instance, we verify (when the reactor water level is between 78% and 100%) that the core outlet temperature measurement is equal to the saturation temperature calculated from the primary pressure measurement.

c) All other measurements. They have the FQ2 factor equal the FQ1 factor.

Third step:

By using the results of steps 1 and 2, the status of the diagnosis with the confidence factor is determined.

There are six different information pieces to be treated.

1. State of the fuel barrier

For the fuel barrier three different diagnosis are possible

- fuel barrier integrity good (state #1)
- fuel cladding rupture possible (state #2)
- fusion probable (state #3)

The diagnosis can elaborated by taking into account the following measurements:
Core outlet temperature (TRIC)
Containment dose rate (DDE)
Primary Activity (AP)

Using TRIC, four cases are possible

- TRIC has always been smaller than 700°C → range #1
- TRIC has always been smaller than 1100°C but has been larger than 700°C → range #2
- TRIC has been larger than 1100°C → range #3
- TRIC is never available → range #0

Using DDE, four cases are possible

- DDE is smaller than 10 rad/h → range #1
- DDE is smaller than 10,000 rad/h but larger than 10 rad/h → range #2
- DDE is larger than 10,000 rad/h → range #3
- DDE is not available → range #0

Using AP, three cases are possible

- AP has always been smaller than 0.2 rad/h → range #1
- AP has been larger than 0.2 rad/h → range #2
- AP is never available → range #0

The table here below synthesises the diagnosis according to the three measurements

<table>
<thead>
<tr>
<th>TRIC</th>
<th>700°C</th>
<th>1100°C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range_TRIC = 1</td>
<td>Range_TRIC = 2</td>
<td>Range_TRIC = 3</td>
</tr>
<tr>
<td>DDE</td>
<td>10 rad/h</td>
<td>10 rad/h</td>
</tr>
<tr>
<td>Range_DDE = 1</td>
<td>Range_DDE = 2</td>
<td>Range_DDE = 3</td>
</tr>
<tr>
<td>AP</td>
<td>0.2 rad/h</td>
<td></td>
</tr>
<tr>
<td>Range_AP = 1</td>
<td>Range_AP = 2</td>
<td></td>
</tr>
<tr>
<td>Fuel barrier State</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Diagnosis &quot;fuel barrier state&quot;</td>
<td>Integrity good</td>
<td>Fuel cladding rupture possible</td>
</tr>
</tbody>
</table>
The general principle for processing the diagnosis of this information and its confidence factor, is obtained by constructing a truth-table using the diagnoses as given by each measurement and the FQ2 factor associated to it. Core outlet temperature (TRIC) and containment dose rate (DDE) have been sorted into three categories:

- **good** (FQ2 > 1.5)
- **average** (0.8 < FQ2 < 1.5)
- **bad** (FQ2 < 0.8)

Primary activity (AP) has been sorted into two categories:

- **good** (FQ2 > 0.8)
- **bad** (FQ2 < 0.8)

The table here below illustrates part of the complete table:

**Range_TRIC not equal 0 and average TRIC FQ2 factor**

<table>
<thead>
<tr>
<th>Range_TRIC = Range_DDE</th>
<th>Range_TRIC = Range_A_P</th>
<th>Range_DDE</th>
<th>FC_DDE</th>
<th>Range_A_P</th>
<th>FC_A_P</th>
<th>Etal_1**_B</th>
<th>FC_1**_B</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUE</td>
<td>TRUE</td>
<td>GOOD or MEDIUM</td>
<td></td>
<td></td>
<td>Range_TRIC 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>TRUE</td>
<td>BAD</td>
<td>GOOD</td>
<td>&quot;</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>BAD</td>
<td>&quot;</td>
<td>0.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>FALSE</td>
<td>&quot;</td>
<td>0</td>
<td>&quot;</td>
<td>0.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>0</td>
<td>GOOD</td>
<td>0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>BAD</td>
<td>&quot;</td>
<td>0.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>GOOD</td>
<td>&quot;</td>
<td>0.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>BAD</td>
<td>&quot;</td>
<td>0.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>FALSE</td>
<td>&quot;</td>
<td>0</td>
<td>GOOD</td>
<td>0.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>TRUE</td>
<td>&quot;</td>
<td>Range_DDE</td>
<td></td>
<td>0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>MEDIUM</td>
<td>= 0</td>
<td>0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>TRUE</td>
<td>&quot;</td>
<td>0</td>
<td>GOOD</td>
<td>0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>BAD</td>
<td>Range_TRIC</td>
<td>0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>FALSE</td>
<td>&quot;</td>
<td>0</td>
<td>GOOD</td>
<td>0.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>&quot;</td>
<td>BAD</td>
<td>Range_TRIC</td>
<td>0.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;</td>
<td>FALSE</td>
<td>&quot;</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Range_TRIC not equal 0 and average TRIC FQ2 factor*
2. Primary water inventory

Four diagnoses are possible for this information:

1) inventory not deteriorated (↔ state 1)
2) deteriorated (↔ state 2)
3) uncovering risk (↔ state 3)
4) uncovering (↔ state 4)

The diagnosis of this information can be obtained by using the measurement for reactor water level (Ncuve) and subcooling margin (Dtsat). The table below presents the diagnosis according to these measurements.

<table>
<thead>
<tr>
<th>Ncuve</th>
<th>Range_Ncuve</th>
<th>N1</th>
<th>Range_Ncuve</th>
<th>N2</th>
<th>Range_Ncuve</th>
<th>N3</th>
<th>Range_Ncuve</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>= 1</td>
<td>20°C</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ΔTsat</td>
<td>Range_ΔTsat</td>
<td></td>
<td>ε</td>
<td>-ε</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prim. water invent. state</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnosis</td>
<td>Not deteriorated</td>
<td>Deteriorated</td>
<td>Uncovering risk</td>
<td>Uncovering</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

N1 = High level  N2 = Intermediate level  N3 = Low level

The following assumptions are taken for the measurements:
- Ncuve and Dtsat have three FQ2 quality factor categories:
  - .good (FQ2 > 1.5)
  - .average (0.8 < FQ2 < 1.5)
  - .bad (FQ2 < 0.8)

- Ncuve is a direct indication of the water inventory so it has to have a larger weight than Dtsat in the logics for elaborating the diagnosis and its confidence factor.

The table here below illustrates part of the algorithm (corresponding to Ncuve of average quality) used for the diagnosis and the confidence factor elaboration.
3. Water consumption inventory of the RWST (Refuelling Water Storage Tank)

The purpose is to check that the volume decrease in the RWST matches the total water consumption by the safety injection system, the containment spray system and the primary charging system. The inventory is performed between an initial time \( t_0 \) to be chosen and the present time \( t \).

The volume decrease is given by the difference of the RWST level measurement between the initial and final time. The total consumption is the integral in time of the 4 safety injection flow measurements, the 2 containment spray flow measurements and the charging flow measurement.
The RWST inventory information has 4 possible diagnoses:

1) Not available
   This is the case when either the RWST level measurement is not available at time \( t_0 \) or \( t \) or when one of the different flows becomes unavailable between \( t_0 \) and \( t \).

2) Normal consumption
   When the difference between the level decrease and the consumption is smaller than a certain threshold (depending on the precision of the measurements used).

3) Abnormal consumption
   When the difference between the level decrease and the consumption is greater than this threshold.

4) Recirculation on containment sumps
   When the RWST level at time \( t \) is smaller than a certain level (MIN 3) the systems stop taking water from the RWST and switch over to the containment sumps.

The confidence factor for each diagnosis relies on the different measurement qualities.

4. Operation analysis of the safety injection system

The purpose is to control the operation of the safety injection system by checking the coherence between the flow measurements (for the 2 high head pumps and the 2 low head pumps) and the theoretical flow (as a function of primary pressure and pump characteristics).
For this information, there are 5 diagnoses possible:

1) Not available
   When the primary pressure measurement or one of the 4 SI flow measurements is unavailable.

2) Security Injection (SI) stopped
   When the 4 SI pumps are stopped.

3) SI operation satisfactory
   When the 4 SI pumps are running and the measured flows are coherent with the computed theoretical flows.

4) SI operation abnormal
   When the 4 SI pumps are running and at least one pump has an abnormal flow with respect to the theoretical flow.

5) At least one SI pump stopped
   When at least one of the 4 SI pump is stopped. The information about the operation of each pump is given in the explanations associated with this diagnosis.

The confident factor of each diagnosis relies on the different flow measurement qualities.
5. Analysis of the RWST isolation in recirculation mode

The purpose is to verify that when the recirculation mode is operational, the water taken from the containment sumps (for cooling the reactor core) does not flow back into the RWST.

This is only checked when between the present and the beginning of the emergency situation time the RWST was below the minimum level MIN3 and the systems (SI and containment spray) switched over to recirculation mode.

Taking into account the fact that the RWST level measurement is not very precise and that the recirculation phase lasts for a long time (in general more than ten hours), it is convenient to calculate the change in the RWST level by comparing the average level in the \[ t - 30 \text{ minutes} ; t \] span with the average level in the \[ t - 60 \text{ minutes} ; t - 30 \text{ minutes} \] span.

Four diagnoses are possible for this information:

1) Not available
   When the RWST level measurement is not always available.

2) Not applicable
   When the MIN3 level has never been reached since the beginning of the emergency situation

3) No RWST isolation problem detected
   When the calculated level variation is smaller than a certain threshold (taking into account the uncertainty of the measurement averaged on 30 minutes).

4) Important RWST isolation default
   When the calculated level variation is larger than this threshold.

The confident factor of each diagnosis relies on the level measurement qualities.

6. Probability of reactor vessel failure

The last information concerns the diagnosis of a severe accident, characterised by the fact that available measurement will be of bad quality as the environmental conditions in the containment will be seriously deteriorated.

The elaboration of the diagnosis of this information is not yet finalised.

4) Future Work on the Tool

The prototype was developed as a tool for the French Technical Support Centres. As described here above, it has to be used as a tool allowing validation of the information needed by experts in formulating their technical advice. The French National Emergency Organisation relies extensively on the expertise of the engineers manning the TSCs. Tools are important to help the experts but in no way they can replace the man-in-the-loop. The expert has the ultimate control and all advice must be human-based.

The tool currently covers the 1300MWe series of the French power plants and for the time being, it concentrates on the diagnosis part. It takes into account the quality of the measurements and diagnoses the state of six pieces of information, with a confidence level attached to it, relevant to the expert for his advice.
Besides extending the tool to all French plant series, two future actions have to be undertaken(*).

First, to test and validate the mechanism determining the measurement quality.

Second, to investigate the behaviour of the safety functions.

The quality mechanism can be extensively tested by using transients recorded during the French emergency drills (about 10 per year) and by running specific accident scenarios on real-time simulators (SIPA of CEA/IPSN and EDF/Septen, and SAF/SAPHIR of FRAMATOME).

Typical examples of the problems encountered are as follows:
- What to do when a measurement is not available ?
- What to do when too many measurements for the same physical parameter are available?

The current approach is to use consistency checking applied to a limited set of important measurements, such as reactor sub-cooling margin, reactor vessel water level and core exit temperature. The cross-checking based on physical coherence rules mutually validate these measurements within a certain domain.

Missing measurements can then be replaced by linear combinations of available measurements.

Redundant measurements that are too far away from the cross-checked value can be eliminated.

The expert is also allowed to manually replace missing or badly behaving measurements.

In the final step of the process a limited set of important values is obtained. These values are consistent within the applicable domain and have a known confidence level. They can be used either by the expert or by thermal-hydraulic codes.

The critical part of the problem is to define what (physical) conditions are required for applying a validation and substitution rule.

The second step for future action is to investigate the behaviour of the safety functions along the evolution of the accident.

The current information available in the prototype has to be enlarged to compute also the status of important safety functions, such as sub-criticality, heat sink and containment. A safety function in general is based on the state of different physical parameters, e.g. for the heat sink status one requires reliable knowledge on sub-cooling margin, reactor water level, steam generator level, core exit temperature,...here after referred to as building blocks.

Typical problems encountered are as follows:
- What are the relative priorities of the building blocks used for assessing the status of a safety function ?
- What is the impact on a safety function when other safety functions change ?
- What is the confidence level of the status ?

Once the status of each safety function and its confidence level have been computed at a given time of the known transient (diagnosis), one can try to cope with the prediction for future evolution (prognosis).

This is a difficult problem. The anticipation has to be coupled to the predictive power of a thermohydraulics model and is a function of the working assumptions of the expert. The expert will probably try out a perturbation approach
- What happens if no input change is observed and the model evolves freely ?
- What happens if the most important parameter changes (improving/worsening) ?
- What is the impact if the second most important parameter changes ?
Up to now, no reasonable simple model is available for PC based software tools. The prognosis is based on the expertise of the man-in-the-loop with the help of easy calculation aids.

The expert identifies the accident and the relevant phase changes by watching the evolution of key parameters. When he is alarmed by the fact that a particular safety function has a degraded status trend, he will use empirical behaviour rules with graphical representations. Also, when the environmental conditions in the containment become seriously degraded, very few instrumentation will survive and few safety functions remain observable.

Typical problems encountered are as follows:
- What are the critical parameters indicating a phase change in the accident?
- How to switch over from one set of safety functions to another?
- What instrumentation will survive?
- How to give swift and simple advice to the operator?

Typical calculation aids include
- Core uncovery and fuel failure diagnosis
- RPV failure diagnosis
- Hydrogen behaviour model

It is obvious that in the short term the priority of future work will be in the areas of measurement validation and status evaluation of safety functions in the accident phase before fuel melting.

**In conclusion,** the prototype for information validation is an important element in the growing set of tools used by the French TSCs. Currently developed for the 1300MWe series, it has to be extended to the 900 and 1400 MWe series. Subsequently it has to be tested and validated by using results from standard design codes (e.g., Cathare), transients run on the accident simulators (SIPA of CEA/IPSN and EDF/Septen, and SAF/SAPHIR of Framatome) and the experience feedback from emergency exercises (about 10 per year with scenarios played on EDF full-scope simulators). The purpose of the tool is to deliver validated information with indication of a confidence level. The expert in the TSC can use this information for formulating his diagnosis and advice on the state of the three barriers in the damaged plant unit.

(*)Part of this work is sponsored by the European Commission (DG XII / ASIA Project with partners NNC (GB), Framatome (F), CEA (F) and ECN (NL)).
METHODOLOGY AND SOFTWARE TOOLS USED

BY IPSN CRISIS CENTRE EXPERTS DURING AN EMERGENCY IN A FRENCH PWR

D. WINTER, J. M. AGATOR

Institute for Nuclear Safety and Protection (IPSN)

60-68 avenue du Général Leclerc, BP 6

92265 Fontenay-Aux-Roses, CEDEX, France

Abstract

The French nuclear power plants presently in operation are standard pressurized water reactors. Due to the potential consequences of an accident in this type of installation, a national emergency organization was constituted which has the capacity to implement countermeasures for the control of the risks for the surrounding population. The Institute for Nuclear Safety and Protection (IPSN), the technical support of the French nuclear safety authority, has thus defined and constituted a support system which could, in case of an emergency occurring in a French PWR, help to reach this aim. First of all, IPSN has defined and utilizes in its emergency technical centre a methodology to evaluate the plant status and to estimate the evolution of the accident, in order to be able to calculate the consequences of releases in the mean terms. To apply this methodology, a support system, constituted by software tools, was developed and is used in such case. To help decision, two systems are currently used: SESAME for the evaluation of the installation status and potential releases and CONRAD for radiological consequences calculations. The diagnosis of the status of a PWR during an accident is based on the analysis of plant-specific data. The information transmitted from the plant is organized in such way that the expert team assesses rapidly the status of the different safety functions and barriers. The specific tools of the SESAME system are used to quantify parameters such as break size or potential fission product release within or outside the plant. The prognosis of the evolution of safety functions and barriers is based on the assessment of the current and future availability of the safety systems and on extrapolations to forecast the evolution of the accident (time to core uncovering and core degradation, fission product release prognosis etc.). The system CONRAD is mainly oriented to the prediction of the consequences in the early phase of the accident for the short term countermeasures. It is composed of a set of tools used to calculate of the concentrations in the air and on the ground, the doses and dose rates due to the release of radionuclides. At last, an organization of the IPSN emergency technical centre was set in place to give advice to government authorities. The IPSN emergency teams follow training programmes runned each year. The whole system is regularly tested during emergency exercises which involve parts or the overall of the national emergency organization. This system is continually improved (tools, methodology, organization) taking advantage of experience feedback of the emergency exercises and could also be enhanced by applications to other nuclear installations.
I. INTRODUCTION

The French nuclear power plants consist of standardized pressurized water reactors. In view of the potential consequences of an accident in this type of installation, a national emergency management system has been created providing the capacity to implement the necessary countermeasures to protect nearby populations. The Institute for Nuclear Safety and Protection (IPSN), the technical support body of the French safety authority, has therefore devised and set in place an aid system which could, in the event of an emergency occurring in a French PWR, enable the predetermined objectives to be attained.

The following description only relates to the first phase of an accident, i.e. the first few days after its occurrence; IPSN action in the post-accident phase is not presented in this paper. In view of the national context and the missions entrusted to the IPSN in the field of reactor emergency management, the different aspects of the IPSN action are reviewed, showing their interaction and their overall coherence. Thus, issues relating to training and to organization and participation in exercises are described as they provide the opportunity to check the validity of the IPSN action and make improvement possible by constant experience feedback.

II. THE NATIONAL EMERGENCY MANAGEMENT SYSTEM

The French national emergency management system for PWRs involves the different governmental bodies with special responsibilities for nuclear safety, radiological protection and civil defence. Here we shall restrict ourselves to those relating to the IPSN's emergency centre.

The nuclear operating organization - Electricité de France in the case of PWRs - remains, in an accident situation, responsible for the safety of its installation and its staff. Therefore two centres of decision-making exist at local level:
- the management of the damaged plant, which has the task of returning the installation to a safe state, to limit the release and to protect the staff;
- the prefecture of the administrative département in which the reactor is located, which has the task of protecting the population from the consequences of the accident. The prefect of the département involved constitutes the representative of the government and coordinates, as necessary, the action of other neighbouring prefectures affected.

The actions specified in the emergency plans are then initiated, whether they appear in the on-site emergency plan within the installation or in the off-site emergency plan for the neighbouring populations.

Aid in decision-making is supplied at a national echelon by, on the one hand, an EDF emergency team and, on the other hand, emergency teams from the safety authority (DSIN), the radiological protection authority (DGS/OPRI) and the civil defence authority (DSC), all of which are located in Paris. These six teams described before are constantly connected to each other during a nuclear emergency situation.

At both national and local echelons, technical emergency teams are formed to supply the necessary inputs to the decision-making bodies: that of the damaged installation to meet the needs of the manager of the plant, that of EDF at corporate level and that of the IPSN to advise the DSIN. These three technical teams are connected to each other to enable the necessary technical dialogue to take place.
The main role of the IPSN is thus, in the PWR case, to advise the government authorities for any countermeasures to be set in place to protect the population, following the assessment of the potential hazards represented by the damaged installation. The current design of the French PWRs has led the IPSN to estimate that, in most accident situations, the dynamics of an accident would be relatively slow and no major releases would occur before some twenty hours. Therefore, the IPSN’s objectives in the event of an emergency in a nuclear facility will be:

- to assess the state of the installation and to monitor its development,
- on the basis of this assessment, to forecast the possible development of the accident and to estimate the associated consequences,
- in parallel, to estimate the consequences of the releases of radioactivity into the environment, this estimation being based on both the preceding assessments and on the measurements which may have been taken in the environment,
- on the basis of the above, to inform the government authorities of the situation and the foreseeable potential consequences, notably by advising them about the countermeasures to take.

III. THE METHODOLOGY AND TOOLS OF THE IPSN

The methodology used by the IPSN is called the 3D/3P approach (triple diagnosis/triple prognosis). It was developed in collaboration with the operating organization. This method is intended to indicate the options available to the emergency teams and to be used as a common reflection support for the technical dialogue between the different players during an emergency. The approach is a deterministic one and is based on the concept of defence in depth. The state of the installation is evaluated throughout the accident with special reference to the three safety barriers, successively considering their physical state, the state of the safety functions guaranteeing their integrity and finally the state of the systems available to monitor these functions. The first stage is determination of the type of accident, which makes it possible to obtain an initial estimation of on-going and foreseeable releases into the environment. On the basis of this diagnosis, a prognosis of the development of the state of the safety functions is made, essentially by determining the current and foreseeable availability of the associated safety systems. Change in the state of the safety barriers then governs the evaluation of the eventual radioactive releases. Application of the technique ends with filling in a special synopsis sheet describing the current and eventual state of the barriers and safety functions and systems, as well as the associated releases. This will be used as a basis for discussions between the IPSN and EDF during the accident.

This methodology is applied by using two computer systems: the SESAME system designed to provide answers to questions concerning the state of the installation and another named CONRAD designed to calculate the radiological consequences in the environment.

III.1 Description of the SESAME system

The tools described below were developed with the objective to assist the expert appraisal. They are in no case intended to replace the expert, who remains responsible for his own assessment. It is therefore necessary for him to properly understand the scope of validity of the various tools he may be required to use and to maintain a critical attitude concerning the results provided.

To describe these tools in the context of their utilisation, two sets of accident sequences are considered hereafter, a loss of coolant accident (LOCA) and a steam generator tube rupture (SGTR). These two sets of accident sequences make it possible to demonstrate the
performance of these tools, even though they remain applicable to other situations. The description of the evaluation tools is preceded by a summary of the data acquisition system, which plays a major role as the quality of the work carried out by the technical emergency response centre greatly depends on it.

A. Reception and processing of data

Before any evaluation can take place the data must be acquired. This is done by a data processing system capable of transmitting one hundred analogue readings per minute, via the TRANSPAC network, between any PWR unit and the emergency response centres of the IPSN and EDF. The values transmitted are the readings recorded by the sensors at the accident-stricken site.

A program called ACQUISITION has been developed to utilize this data. It receives the readings transmitted and stores them in a database accessible to all members of the corresponding emergency response team. It applies the conventions adopted for representing unavailable readings and generates a statement of availability for all the sensors over time that the different specialists can read. During these operations, it is possible to evaluate the validity of the values transmitted by means of on-screen forms describing the sensor involved (its measurement range, its accuracy and its location).

In the event of unavailability of the data link, the ACQUISITION program enables pre-formatted messages to be entered for some fifty readings. These messages are faxed by the accident-stricken plant every fifteen minutes. If this mode of transmission of the data also fails, prevision is made by using simpler messages which can be exchanged by phone with the accident-stricken plant. These messages are then keyed-in using the ACQUISITION program. A degree of redundancy in the transit of data is thus provided.

B. Use of the SESAME system in the event of a loss of coolant accident (LOCA)

Basic diagnosis and monitoring of the situation require a comparison between the readings transmitted by the installation and correlations or typical values. This task is performed with the assistance of the 3D/3P program. The "initial diagnosis" function of this tool proposes a selection of reference data and readings making it possible to rapidly determine the type of accident.

In the case of a LOCA, the expert first checks the state of the first barrier by comparing the temperatures measured at the core outlet with temperature thresholds signifying degradation of fuel (cladding failure or core meltdown). The presence of activity within the containment, while enabling him to confirm his diagnosis concerning the first barrier, also enables him to have an opinion on the second barrier (primary break located in reactor building). He can verify this diagnosis by displaying the trends of other parameters such as the pressure and temperature within the reactor building. The various stack activity readings enable him to form an initial opinion on the state of the third barrier.

This material enables the expert to select, using the REJETS-TYPES program, a predetermined accident scenario using the following parameters: reactor type, operation of spraying in the containment and core and containment degradation states. This stage enables the emergency response team to rapidly provide a first evaluation of radioactive releases outside the installation.
Once the presence of a primary break is diagnosed, the size of the break is evaluated using the BRECHEMETRE program. Two modes of evaluation are available:

- the first, based on variation of the water level in the pressurizer, gives the leak rate by means of a primary system mass balance. Comparison of the leak rate with critical flow correlations then gives the cross-sectional area of the break diagnosed by the experts. This model has been qualified using the CATHARE thermohydraulic computer code and a version of it on the SIPA simulator to take into account the effect of the reactor protection systems;
- the second, which is less precise, is based on the comparison of the pressure peak measured in the containment when the break appears with the standard pressure peaks for a spectrum of known break sizes and given cooling conditions. The standard pressure peaks were obtained by calculation using the PAREO design code (developed by EDF) and verified with the JERICHO code of the ESCADRE system (a set of severe PWR accident computer codes developed by the IPSN).

The diagnosis of a primary break immediately leads the expert to ask oneself about the eventual state of the "water inventory" safety function which determines the state of the "fuel" barrier. To provide assistance in evaluating the risk of uncovering of the core and, when applicable, the time available before the onset of uncovering, the SCHEHERASADE program is available to the expert. This program uses mass and energy balances as a basis and applies hypotheses concerning the size and location of the break, as well as the cooling induced by the control actions executed by the operators. Assessment of the time available before degradation of the core (failure of cladding or meltdown of the core) is made using correlations derived from studies carried out with the VULCAIN reference code of the ESCADRE system.

In the event of a severe accident, it is necessary to evaluate the risk of combustion of the hydrogen present in the containment. On the basis of the temperature and pressure conditions in the containment, and hypotheses concerning the degradation rate of the fuel, the HYDROMEL program provides the composition of the containment atmosphere, indicates whether there is a risk of combustion and provides, when applicable, the maximum pressure and temperature liable to be reached during combustion. HYDROMEL was fitted with results of the JERICHO code of the ESCADRE system.

Finally, calculations are made of the ongoing and potential releases of fission products, which depend on the state of the third barrier. For 900 MW PWRs, the IPSN has developed an expert system called ALIBABA which, on the basis of containment isolation reports and activity readings in the different rooms and in the ventilation ducts, can be used to detect any leak paths. Experience feedback on this 900 MW PWR version from emergency drills is currently being the subject of analyses pending the development of a 1300 MW PWR version.

To complete this diagnosis of the state of the containment, it is necessary to describe the transfer of fission products within the installation and to compare the activity thus calculated with that measured in the accident-stricken installation. This calculation of the transfer of fission products is made using the PERSAN program. This covers four families of fission products: noble gases, iodines, caesiums and telluriums. For iodines, it takes into account the different physical and chemical forms (aerosols, molecular iodine and organic iodine). The fission product behaviour laws are derived from parametric studies conducted by the IPSN. The PERSAN program can also handle the prognosis part by entering hypotheses such as the eventual state of the fuel, of the containment and of systems such as ventilation and containment spraying. It has been qualified using accident sequences covered with the ESCADRE system codes.
C. Use of the SESAME system in the event of a steam generator tube rupture (SGTR)

The initial diagnosis made with the assistance of the 3D/3P and REJETS-TYPES programs is essentially based on observation of the results of activity readings in the blowdown lines of the steam generators and in the uncondensables extracted from the condenser.

The number of tubes ruptured is evaluated using the BRECHEMETRE software. In the opposition to the LOCA case, only evaluation based on variation of the water level in the pressurizer is available. Here, the mass balance principle is maintained, only the correlations used to obtain the size of the break from the flow rate at the break being different. Qualification was also carried out using the CATHARE code and the SIPA version of it.

In the event of a SGTR, the "thermohydraulic" and "fission product transfer" aspects are closely linked. Thus, the experts in charge of handling the "thermohydraulic" and "containment" parts evaluate, in close collaboration, the release of fission products into the environment using the "RTGV" program. On the basis of, on the one hand, the thermohydraulic conditions determined from the readings transmitted by the accident-stricken unit and, on the other hand, hypotheses such the number of tubes ruptured, the RTGV program draws up mass and activity balances. It thus calculates the primary activity peak due to the transient, the transfer of fission products from the primary system to the secondary system, and the transfer of fission products from the secondary system to the environment. The thermohydraulic part was qualified with the SIPA version of the CATHARE code while the "fission product transfer" part was qualified using the steam generator tube rupture studies made using the AXEL code.

III.2 Description of the CONRAD system

The CONRAD system is mainly oriented to the prediction of the consequences in the early phase of the accident for the short term countermeasures.

It is composed of a set of tools permitting the calculation of the concentrations in the air and on the ground, the doses and dose rates due to external exposure and inhalation, following the release in the air of radionuclides. It includes:

- a database containing the characteristics of approximately 300 radioisotopes,
- a set of atmospheric dispersion methods, covering different spatial scales,
- a module for the calculation of doses by plume irradiation, contamination by inhalation to different organs and irradiation due to deposition,
- a geographic information system allowing the presentation of the results (curves of isoconcentration, isodoses,..) on maps.

The system can process either isotopes (11 simultaneously) or families of isotopes (noble gases, iodines, telluriums,...) corresponding to the composition of a PWR core for different cooling times and burn-up.

The system runs on the computer network of the IPSN's technical emergency centre; a version of the system runs also on PC micro-computers.

Simple methods, adapted to the objectives and the needs of the early phase of a crisis situation, have been retained in the CONRAD system. They are all based on the Gaussian
puff model using the Doury's standard deviations. They take into account the dry and wet
deposition on the ground, the depletion of the pollutant and the radioactive decay.

Note: in the framework of the French-German commission (DFK), a collaborative work has
been done in order to develop a common set of standard deviations to be used in a
Gaussian puff model in both countries in case of emergency. This new set will replace those
presently used in France and Germany.

A. Local Scale

For the consequences at local scale (about 30 km around the site), two main methods have
been developed.

B. Operational Graphs

During the early phase of the accident, the main objective is to determine the zones where
short-term countermeasures have to be taken. Both a prediction of the source term and the
forecast of the local weather are required\(^1\). In the context of such a situation, characterized
by large uncertainties in the input data, a simple tool, consisting of precalculated graphs,
giving values of atmospheric and surface transfer coefficients, has been adopted. These
graphs permit the calculation of the doses and dose rates after the plume passage. They are
drawn up for 11 classes of meteorological conditions (combining the atmospheric stability,
the wind velocity, and rain) and are suitable for gases or aerosols. They appear as circles for
low wind situations and as angular sectors for the other meteorological situations.

They take into account the uncertainty on the forecast of the local wind direction. For simple
sites (without significant topographic effect), this uncertainty has been estimated to be
\(\pm 15^\circ\). In fact, later studies conducted by the French meteorological office have shown that it
may be higher on rather complex terrains. Therefore, specific adaptations of the graphs for
such sites (complex terrain) have been brought. They consist in an increase of the angle of
the sector which may be reached by the plume. This increase has been evaluated, site by
site, according to studies performed on the site itself or to the expert judgement.

Note: an automatic transmission of the results of SESAME (system of the technical crisis
centre devoted to the prediction of the source-term in case of accident on a PWR) to the
"operational graphs" computer tool has been established and permits a direct calculation.

C. Gaussian Puff Model SIROCCO

The second method consists in using a Gaussian puff model, called SIROCCO. All types of
release kinetics and meteorological conditions, eventually varying with time during the
release, can be taken into account. The doses and dose rates, at different instants during
and after the plume passage, are calculated on a grid of some hundred to thousand points
around the site, permitting the drawing of isocurves.

\(^1\) The weather forecast is given by the French Meteorological Office in the framework of an agreement with
IPSN.
D. Long Range Transportation

For regional and long distances, the version SIROCCO-LD of the Gaussian puff model has been developed. In this model, the puffs travel along trajectories considered as the locations of the mass centres of pollution. The trajectories are derived from the forecast or the analysed wind field calculated by the French Meteorological Office. The time interval between two trajectories is one hour. The concentrations and doses are computed, at different times, for each point of a grid of maximum 160 x 160 points. A version with a smaller mesh size for regional problem is also available.

IV. ORGANIZATION OF THE IPSN

The IPSN’s technical emergency centre comprises four units:

- a management unit (CD) with the task of co-ordinating the work of the two technical units, collating the results obtained and transmitting the necessary informations and recommendations to the safety authority. It must be pointed out that a video conference facility therefore links the management unit to the DSIN emergency team;
- a secretariat unit (CS) with the task of dispatching the information received and transmitting the previously-validated advice and data obtained;
- two technical units, designated "installation assessment unit (CEI)" and "radiological consequences unit (CCR)" with the task of processing the information received and, more specifically, analysing it.

For the PWRs, the CEI is composed of 9 experts: a co-ordinator, a technical secretary, the delegate for the plant involved, two audioconference workers, a data processing worker and three specialists (operation, thermohydraulics and containment) who have the various modules of the SESAME system at their disposal. This unit is linked to the other technical emergency teams by an audio-conference system making it possible to periodically assess the situation from a technical point of view.

The CCR is composed of 7 experts: a co-ordinator, a deputy, a technical secretary, two experts in charge of relations with outside of the unit and two experts in charge of the consequences calculations (manual or with the CONRAD system). Links are in place between the unit and the staff of the French meteorological authority, the OPRF and the EDF technical emergency teams.

V. TRAINING AND EXERCISES

The IPSN does not consider it necessary to train permanent teams of emergency specialists totally detached from other IPSN activities. Staff composing the teams is thus chosen from all the IPSN’s experts. The emergency specialists regularly undergo training in emergency situation management and participate in national exercises which represent the best hands-on training.

In accordance with the specialities of each of the units, special sessions derived from a common basis are organized:

- phenomenology of severe accidents;
- the context of an emergency situation;
- understanding of the missions, techniques and tools (paper and computer) available;
- hands-on experience.
Some one hundred IPSN experts have undergone such training and are ready to deal with an emergency situation on a PWR.

The entire system set in place by the IPSN to tackle an accident situation in a PWR, as well the national emergency management system (see § II), have been regularly tested during exercises. These exercises are organized by the government authorities and involve the PWR plants 6 to 8 times per year. The exercises involving the PWR plants are jointly prepared by IPSN and EDF specialists. The scenarios are established considering the objectives of the exercise, the resources and organizational structures involved, as well as the planned durations, on the basis of the results obtained with the computer codes - CATHARE or SIPA simulator as well as ESCADRE system - developed in France.

Two or three years after setting this structure in place within the IPSN, training sessions and exercises which have been organized have showed the coherence of the arrangements and their adequacy as regards the objectives of IPSN.

This structure should also be enhanced by applying it to other nuclear installations, with some necessary adaptations.
PWRs SIMULATION MODELS
USED BY EDF/SEPTEN CRISIS TEAM

A. SEKRI, B. de MAGONDEAUX, F. PIZA , Miss AC. AUGE
Electricité de France
SEPTEN
12-14, avenue Dutriévoz
69628 Villeurbanne Cedex - France
Phone: 33.4.72.82.75.35, Fax:33.4.72.82.75.55
E-mail: Ahcene.SEKRI@de.edfgdf.fr

KEY WORDS
Nuclear engineering /
Decision support systems / Model analysis

ABSTRACT

ELECTRICITE de FRANCE has developed a set of tools and simplified models named TOUTEC and CRISALIDE which are aimed to be used by the French Utility National Crisis Team in order to perform the task of diagnosis and prognosis during an emergency situation.

As a severe accident could have important radiological consequences, this method is based on the diagnosis of the state of the safety barriers and on the prognosis of their behaviour. These tools allow the crisis team to provide advices to mitigate the accident on the damaged unit and to deliver public authorities with information on the radiological risk.

At a first level, the software TOUTEC is intended to complement the handbook of crisis team members with simplified calculation models and predefined relationships. It can avoid tedious calculation during stress conditions. The main items are the calculation of the primary circuit break size and the evaluation of hydrogen burning.

The set of models named CRISALIDE is devoted to evaluate the following critical parameters: delay before core recovery, containment pressure behaviour and finally source term. With these models, EDF Crisis Team is able to take into account combinations of boundary conditions according to safety and auxiliary systems availability and operator's actions.

The set of models CRISALIDE and its man machine interface TOUPEC are running under WINDOWS environment on a Personal Computer.

Assessment tests have shown a very good accuracy with best estimate codes as CATHARE. The models have become operational since the beginning of 1992 and they have been already used successfully during crisis drills.

1 INTRODUCTION

This presentation will describe briefly the method performed by the EDF National Crisis Team in order to manage any crisis situation.

Then, we will focus on the EDF Nuclear Basic Design Department task and, especially on the relevant computational tools that would be used to carry on the plant state diagnosis and prognosis.

1.1 THE FRENCH NATIONAL CRISIS TEAM ORGANIZATION

The main task fulfilled by the EDF National Crisis Team follows on from the responsibility of EDF as a Nuclear Power Plant utility:

- responsible for operations on the power plant,
- responsible for the radiological consequences and pollution caused outside the nuclear power plant in the event of an accident.

This means that the EDF must be able to:

- ensure staff protection,
- supply the civilian authorities in charge of public protection plans with information on the situation and its likely evolution,
- ensure that the damaged unit returns to a safe and controlled state by means of operating advice when the operators' procedures are no longer appropriate.

The Technical National Crisis Team is located in Paris - La Defense and brings together various specialists in the fields of emergency procedures, systems, equipments and instrumentation. The Nuclear Basic Design Department members add their experience in safety analysis and accidental thermohydraulics. The EDF team also receives technical assistance from the Constructor of the nuclear steam supply-systems.
1.2 DIAGNOSIS - PROGNOSIS APPROACH

In order to fulfill this mission and as a result of a common development of EDF and the French Nuclear Safety Institute (CEA-IPSN), a method called Triple Diagnosis - Triple Prognosis (see fig. 1) aims to structure the task of the French Crisis Teams to evaluate the radiological release risk (Soldemann et al. 1991).

FIG. 1

"TRIPLE DIAGNOSIS-TRIPLE PROGNOSIS" METHOD

The goal of the approach is very consistent with the general agreement about the accident management whose priorities are:

- prevent core damage,
- maintain containment integrity as long as possible,
- minimize offsite releases.

There are two stages in the method: Diagnosis and Prognosis.

Diagnosis:

This step depends mainly on the measurements. First, the state of the fuel and the three barriers (damping - primary circuit - containment) are identified. Secondly, the state of Safety functions (Subcriticality, water inventory, residual heat removal, containment integrity) and systems ensuring their control are estimated in terms of margins. Thirdly, are estimated:

- the rate of fission products released away from the fuel,
- the activity in suspension in the containment atmosphere,
- the release pathway,
- and the amount of activity released to the environment.

Prognosis

In this second stage, we take into account:

- operator actions laid down in the EOP's or in the Severe Accident Intervention Guideline (in French named "GIAG"),
- the availability of systems ensuring the control of safety functions, safety systems or back up with auxiliary systems if they are available,
- restorations on release pathway.

This leads to the definition of new fuel and barrier states and therefore, of a new release pathway, together with the corresponding time scale. We use the data to produce an estimate of the amount of activity escaped from the fuel and which would be released to the atmosphere in the following 24 hours.

These evaluations will allow EDF, radiological specialists to assess the environmental consequences and to inform civilian authorities and their own support crisis team (CEA-IPSN).

2 EDF CRISIS TEAM EVALUATION TOOLS

2.1 PRINCIPLES FOR THE DEVELOPMENT OF TOOLS

This presentation is focused on the plant state evaluation tools which are developed within the framework of the Triple Diagnosis - Triple Prognosis prediction process (see fig. 2) (Gimadi et al. 1993)

FIG. 2

EXPLANATORY DIAGRAM OF TOOLS USE

These tools have been developed with respect to the following principles:

- simple tools and method fitted to limited data processing equipment in the event of crisis,
- very fast calculation,
- good accuracy on the main physical parameters,
- portability and operating on a micro-computer (PC).

These computational aids can be applied on any of the French 55 PWRs (900, 1300 eMW and N4 series).

2.2 FIRST LEVEL TOOLS

At the first level, the EDF/SEPTEN Crisis team uses a manual hand-book and a computational help named TOUTEC (French acronym meaning Tools for Crisis Team Members) for rough estimates.

TOUTEC completes the hand-book with predefined relationships and so avoids tedious calculations (decay-heat, critical break flow relationship, water and steam properties,...).

The main items have been related with the first priority which is core uncover risk evaluation associated with the second barrier state and safety systems:

- calculation of primary circuit break size:
  
  The calculation is based on the mass balance in the primary circuit and uses mainly the pressurizer level evolution.
- Simplified calculation of core uncover delay:
  
  This tool should be used in case of total loss of primary water injection following the previous break size evaluation.

For the containment integrity evaluation, an hydrogen calculation has been developed to find out the maximum containment pressure value in case of hydrogen burn, and allows different input data modes (fig. 3):
2.3 SIMULATION MODELS

Physical models become necessary to perform the general task of source term release prognosis as soon as time dependent phenomena or changes in boundary conditions are to be taken into account. For this reason, EDF/SEPTEN has developed a set of physical models named CRISALIDE which is detailed in this paper (§3). This set of models allows a very fast and relevant source term calculation for the next 24 hours.

Thanks to the high calculation speed-up, these tools may also be used to confirm some basic hypothesis like break size or containment leakage during the phase of diagnosis by comparing the calculated results with the plant parameter evolutions.

Because of this high speed-up, the simulation is running in a "batch mode" without any drawbacks.

An user-friendly interface, illustrated below (named TOUMEC, french acronym for Models Tools for Crisis Team members) has been developed and implemented under WINDOWS environment on a personal computer. Figure 4 below shows a typical form of visualization (a mimic diagram) which completes the more conventional form, time-series plots.

3 CRISALIDE: A QUICK AND SIMPLE SIMULATION TOOL DEDICATED TO THE CRISIS TEAM

3.1 PRINCIPLE AND OBJECTIVES

Crisis drills, frequently organised in France, have shown the limits of elementary calculation ("rule of the thumb") methods in diagnosing and predicting the consequences of an accident occurring on a French Pressurized Water Reactor:

- specialists experience and abacus are based on existing accident studies with standard initial states and scenarios,
- calculation methods such as TOUTEC ones, are punctual tools, unable to take into account interactions between phenomena and real history of the event, such as temporary unavailability of ECCS.

This led EDF to develop a set of fast simulation models able to cope with effective, complicated situations that may result after an accident.

Efficiency during crisis conditions needs a very user friendly interface and calculation speed up of more than 50 times faster than real time on personal computer.

3.2 MODELLING CHAIN STRUCTURE

Three models are used in the CRISALIDE calculation chain:

1. PROMETHEE is a thermohydraulic model which calculates, if necessary, the Nuclear Steam Supply System behaviour after the reactor trip, from the beginning of the accident to the core meltdown and the rupture of the vessel. According to the availability of the safety and cooling systems, it can give the delay before core uncoverage.

2. ENCEINTE is a thermodynamic model which calculates pressure and temperature containment evolution with the results provided by PROMETHEE relative to mass and energy released and hydrogen released from the RCS. The coupling of the two codes, PROMETHEE and ENCEINTE, has been carried out in order to be more realistic and to simplify the use of this chain of models.

3. The REJECTS model uses the information on core damage, fission product releases and containment pressure to calculate activity in suspension in the containment then releases into the environment according to the identified or supposed leakage pathways of containment.

3.3 RCS and Secondary SG Model: PROMETHEE

The Nuclear Steam Supply System is represented by the Reactor Coolant System and 3 (or 4) Steam Generators as showed in figure 5.
The RCS is divided into two modules:
- the pressurizer and surge line,
- vessel and loops (primary loops are not individually described).

Each module is made of three "volumes" or nodes, a cold liquid water part, a warm liquid water part and a steam part. Each node can be in a thermal equilibrium or non-equilibrium.

According to the phase we consider during the degraded core simulation, the "Vessel" module is differently nodalized as showed below:

The new nodalization (fig. 6b) implemented after the beginning of uncover, allows to keep the hot liquid water from being residual.

During the fuel relocation into the reactor vessel lower plenum, we assume that the core is completely relocated due to the simplified core model - we indeed use a single node for the uncovered fuel.

**SG MODEL (fig. 5)**

The 3 or 4 steam generators (secondary side) are individually simulated by a sub-cooled or saturated liquid volume and a steam volume at saturation. The steam lines are not modelled.

**OVERVIEW OF THE CONSERVATION EQUATIONS**

The main variables of the system are:
- enthalpy and mass of each node for each module,
- pressure, common to any part of a given module,
- uncovered fuel temperature,
- mass of cladding ZrO₂.

Consequently, RCS state is described by 16 variables and each Steam Generator, by five variables.

The calculation of thermal hydraulics is based on the conservative equations of mass and energy written for each node of each defined module, and the volume conservation of each module:

**MASS BALANCE** (module i, node j):

\[
\frac{dM_i^j}{dt} = \sum Q_i^j
\]

**ENERGY BALANCE** (module i, node j):

\[
\frac{d(Mh_i^j)}{dt} - V_i^j \frac{dP}{dt} = \sum F_i^j
\]

**VOLUME CONSERVATION** module i:

\[
V_{i} = \sum M_i^j \rho_i^j
\]

With:
- \( h \): specific enthalpy (kJ/kg)
- \( V \): geometrical volume (m³)
- \( \rho \): density of the fluid (kg/m³)
- \( Q \): mass flux (kg/s)
- \( F \): heat flux (W)
- \( P \): pressure (Pa)
- \( V_{tot} \): total volume

After the beginning of the core uncover (fig. 5b), we take into account the uncovered fuel energy balance and the cladding ZrO₂ mass balance.

**"Behaviour laws"**

As fluid velocities are not considered in this model, and due to some component simplifications, physical phenomena are simulated thanks to "behaviour laws" included in transfer terms such as:
- break flow rates,
- mass transfer between the vessel and the pressurizer (including flooding-example of TMI-2 accident),
- evaporation and condensation terms,
- spray and heaters in the pressurizer,
- heat exchange in the steam generators.
• heat exchange with structures.
• sink and source of RCS (for instance, safety injection flow rates, CVC System,...)
• reflux cooling flow rates....

The qualification of this model enables us to define a single set of correlations, separately tuned on basic qualification tests.

The set of conservative equations leads to a non-linear system which is solved with a numerical scheme based on a fully implicit NEWTON's iterative method, and therefore with a variable time-step. The coupling between the primary circuit and the secondary circuit is achieved through heat exchange terms in an explicit way.

Validation

Then, the validation of PROMETHEE has been performed in order to test the physical relevance of the modelling and the reliability of the computation.

The model obtained has been assessed by referring to more than 30 transients simulated either with the French best-estimate code CATHARE or with the MAAP code.

Figure 7 shows the PROMETHEE and MAAP simulations for a 2" cold leg break on a three-loop plant without HPIS and LPIS and reactor coolant pumps trip five minutes after SI actuation. The curve of the uncovered fuel temperature shows a good agreement between these two codes in predicting the core uncovering time and a difference in the relocation time which is explained by the non meshed core of PROMETHEE.

Energy and mass transfer taken into account are the following:
• condensation and evaporation at the liquid/gas interface,
• recirculation flow rate from the sump (liquid volume),
• spray system : water flow rate, condensation, reexchangers......
• condensation and heat exchange on walls and structures,
• at each time-step, mass and energy flow rates at the break are taken from PROMETHEE model results.

Hydrogen release from oxidation of fuel cladding is also given by the PROMETHEE core degradation model.

Since 1994, the interaction of corium with concrete and burning hydrogen are also taken into account in the ENCEINTE model.

The Numerical calculation of the system is also a mainly implementing Newton method. Calculation speed is very high (at least 100 times faster than real time).

The validation of this simplified containment model has been successfully achieved by comparison with PAREO code results for break transients: discrepancies are lower than 10%.

The containment pressure evolution relative to the previous transient is visualised in figure 9.

3.4 CONTAINMENT MODEL : ENCEINTE (fig.8)

The inner free volume of the containment is represented by two parts:
• a liquid volume (sumps),
• a gas volume composed of nitrogen, oxygen, steam and hydrogen, carbon oxide and dioxide.

Walls and inner structures are modelled by five (resp. seven) conducting systems on a three-loop (resp. four-loop) plant.

The description is quite similar to that of EDF containment design code PAREO.

Each of the two volumes is defined by its mass, enthalpy and common pressure for a total of five main variables.
3.5 SOURCE TERM CALCULATION MODEL: REJETS (fig.10)

The calculation of radioactive release towards the environment by the REJETS model can be done either separately (stand-alone running), or automatically linked with PROMETHEE and ENCEINTE calculations. That last solution is named the CRISALIDE chain. The first solution allows a rapid evaluation of the source term if the NSSS parameters cannot exactly be assumed out when the prognosis of the safety barriers state and containment systems availability can be forecasted.

REJETS takes into account the Fission Products inventories of the reactor coolant fluid, of the fuel gap and of the fuel pellets itself. Six species of Fission Products are considered:

- nobbies gases,
- organic iodine,
- molecular iodine,
- particular iodine,
- cesium,
- tellurium.

In a first stage, REJETS calculates the release of activity in the containment itself, according to the degradation state of RCS (primary fluid inventory), cladding (gap inventory) and fuel pellets (melting).

Then, depending on the FP species, it calculates the flowrate of activity through the different leakage paths that may occur:

- direct by-pass of containment,
- natural and extra leakage of containment,
- containment vent (*U5* sandfilter),
- ventilation of auxiliary nuclear buildings.

The retention mechanisms considered by REJETS are:

- spray system effect and natural deposition in the containment itself,
- filtration and deposition in peripheral buildings and annulus compartment (for French PWR 1300 eMW),
- filtration by sandfilter of the containment venting system.

Figure 10 below sums up this REJETS model processing.

Balance relationships are written for each FP species, with a semi-implicit method for numerical resolution. The speed of calculation is very high in stand-alone running mode.

Realistic or conservative hypotheses about leakage, deposition and filtration could be adopted. The qualification of the REJETS mode has been achieved by intervalidation with the CEA-IPSN (French safety Authority Technical support team) code named PERSAN. Recent developments have also added the rough calculation of radioactive dose rates inside the containment and in the environment depending on the meteorological conditions.

4. CONCLUSION

In the frame of EDF crisis organization, the CRISALIDE chain used by the SEPTEN Crisis Team has been very efficient and its Man-Machine Interface user-friendly. Being started after the beginning of an accident, this tool allows to check and to improve the accuracy of the diagnosis through fast simulation of the concerned transient, even if there are little information available. Then, it allows to forecast their consequences on plant and environment.

The CRISALIDE further developments will be mainly oriented towards extension of the domain of simulation (SGTR, break on secondary circuit...), while preserving the speed and accuracy of this simulation tool.

REFERENCES


SEVERE ACCIDENTS
AND
OPERATOR TRAINING

DISCUSSION OF POTENTIAL
ISSUES

Michel VIDARD
EDF-SEPTEN
12-14 Avenue DUTRIEVOZ
69628-VILLEURBANNE CEDEX
FRANCE

I)-INTRODUCTION

In the last ten years, a significant amount of resources has been devoted to Severe Accident related issues. R&D programs developed throughout the world allowed significant progress in the understanding of physical phenomena and Severe Accident Management (SAM) programs started in many OECD countries. Basically, the common denominator to all these SAM programs was to provide utility operators with procedures or guidelines allowing to deal with complex situations not formally considered in the Design Basis, including accidents where a significant portion of the core had melted. These SAM procedures or guidelines complement the traditional accident management procedures (event, symptom or physical-state oriented) and should allow operators to deal with a reasonably bounding set of situations.

Between 1989 and 1995, the Senior Group of Experts on Accident Management (SESAM) followed the development of these SAM initiatives and issued reports documenting the work done in OECD countries. The main conclusions of the report, confirmed by the presentations made during the Specialist Meeting organized by SESAM in Niantic, Connecticut, USA in June 1995 were:

- implementation of SAM programs had been done, or was in progress in all countries
- though there could be differences in the details of SAM procedures, there was general agreement on what had to be done to terminate the accident and limit risks outside the plant.
- Severe Accident knowledge could be improved, but some uncertainties would remain in any case, and further R&D results were not likely to modify current SAM strategies.

Dealing with operator or crisis team training, it was recognized that training would be beneficial but that training programs were lagging, i.e.
though training sessions were either organized or contemplated after implementation of SAM programs, they seemed to be somewhat different from more traditional training sessions on Accident Management.

This presentation will try to underline some potential difficulties for training operators and discuss problems to be addressed by organisms contemplating SAM training sessions consistent with similar activities for less complex events.

II) DESIGN BASIS ACCIDENTS AND SEVERE ACCIDENTS

Before dealing with training issues, some differences between Design Basis accidents (DBAs) and Beyond Design Basis Accidents (BDBAs), with or without coremelt, can be stressed.

2.1) To summarize the situation, it could be said that the main difference between DBAs and BDBAs is rather conventional. In the case of DBAs, one has to demonstrate that coremelt never happens, using a well defined set of assumptions (system availability or capability, acceptance criteria...). DBAs are so used to assess plant robustness from a system capability standpoint and a sound engineering practice standpoint.

From an accident management standpoint the conclusion is that, as long as one remains in a domain bounded by the design basis, everything needed to terminate the accident, i.e.:

- information on process parameters allowing to assess plant status
- safety-related system(s) (with adequate capability) needed to address challenges to safety functions or plant integrity

is still available.

From an operator standpoint, this doesn't mean that, if he were confronted to such situations, identifying the cause of the accident or bringing the plant back into a steady state where all safety functions could be fulfilled would be straightforward. He would more simply have enough information to assess whether the situation is degrading further, or evaluate the consequences of his accident management decisions, and perform adequate actions.

2.2) Considering BDBAs is simply recognizing that reality is more complex than depicted in the design basis. This complexity is not resulting from consideration of new challenges to plant integrity, but from the possibility of occurrence of scenarios where the minimum capability of essential systems cannot be contemplated any longer.

This, of course, does not imply that all transients beyond the Design Basis would result in core melt situations. Essential safety functions can be restored when functional redundancy exists, or process parameters
exhibit substantial margin compared to that considered in the Design Basis.

From an operator standpoint such situations are of course more difficult to handle.
-First, part of the instrumentation could operate in adverse environmental conditions: assessment of plant status is so more complex. In particular, after the core has started to melt, part of the instrumentation is lost or malfunctioning: it must then be made clear that answering to some questions related to plant status could be conditional (i.e. available information could lead to more than one credible conclusion), or impossible when no information at all is available.
-Second, at the system level as at least part of the functional capability is lost, the question is how to restore this capability. This could mean operating some components beyond their intended range of operating conditions, and result in temporary improvement followed by further degradation resulting from component failure.
-Third, as Severe Accident related phenomena are very complex, the evolution of some plant parameters could be misleading, at least temporarily.
-Fourth, though actions recommended in SAM procedures or guidelines are clearly aiming at limiting or stopping accident progression, success cannot be guaranteed, contrary to what happens before the core has started to melt. For example, if the water injection capability into the Reactor Coolant System (RCS) has been recovered, injecting water into the RCS is recommended but, once the core has started to melt, corium cooling (and thus accident stabilization) cannot be guaranteed, but water injection is clearly the best strategy as melt progression would continue if nothing were done.

To help operators handle such degraded situations, operator aids need to be developed and tested, and adequate training will have to be provided.

III) POSSIBLE OBJECTIVES FOR TRAINING

Many objectives can be contemplated for operator training. Without pretending to be exhaustive, the following can be mentioned, together with comments on related requirements:

-Improvement of knowledge: in this case, the main goal is to teach operators what happens in case of accidents degrading to coremelt scenarios.
It is so important to:

*explain how, from a system standpoint, the accident could degrade in a coremelt scenario
*provide the operator with a good description of all successive steps of core degradation and accident progression,
*explain the most significant phenomena and their consequences in terms of plant behavior
*justify recommended SAM actions, explain potential drawbacks, and develop consequences of partial or total failure on accident progression.

Though lectures on the above mentioned items could be deemed sufficient in some cases, maximum efficiency would require use of a computer model. Main characteristics of this model should be:

*consistency with models implemented in current training simulators for the phase in-between accident initiation and the onset of coremelt. Operators must not be distracted by parameter evolutions or accident progressions they are not used to seeing during their normal training sessions
*use of state of the art knowledge for representing severe accident phenomena
*computer graphics to support explanations and help operators understand accident progression (including parameter evolutions)
*simulation of system recovery
*simulation of partial success of accident management actions (e.g. possibility to interrupt a scenario at some point in time and show the influence of full or partial success of water injection)
*fast running model, allowing discussion of specific issues in parallel with accident progression in the model.

-severe accident management:

The main goal is to teach the operator how he would have to react if an accident were to degrade in a coremelt situation. One point which could be discussed is which kind of operator reaction should be tested.

Examples are:

*in managing "conventional" accidents, the operator heavily relies on a rather complete set of information. Of course, these informations don't give a very detailed picture of accident evolution, but they are nevertheless sufficient, in most cases, to understand accident evolution and so limit the risk of human errors. If the situation were to degrade beyond the onset of coremelt, information would become a key issue as many sensors would have to operate under environment conditions making equipment survivability questionable.
The operator would then have to decide which sensor is available, and which information is reliable (crosschecking of informations). 
Making the operator aware that monitoring sensor status is difficult could be one of the objectives.

*assuming this monitoring is done, the next question is the kind of information available sensors actually provide. For example, after the core has started to melt, and assuming ex-core chambers and activity detectors in the containment atmosphere are still available and provide reliable information, is it possible to make conclusions on the molten portion of the core?
Consistent use of operator aids, if any, or testing operator conclusions on plant status with or without guidelines could be contemplated depending on utility objectives.

*in case of accidents progressing beyond the domain bounded by the Design Basis, the operator has to make critical decisions (i.e. decisions he would not make otherwise), or experience plant evolutions he is unused to (e.g. fast pressure increase when injecting water into the RCS).
Analyzing operator response in such cases to properly understand human factor issues (if any) resulting from such situations could also be of interest.

As compared to the previous objective, additional versatility could well be needed. Beyond the above mentioned capabilities, the following could also be of interest:

*flexibility for break location in the case of LOCA  
*potential for keeping the pace with accident progression  
*potential for simulating failures or Accident Management actions at any time into the accident  
*simulation of sensor capabilities (e.g. span, on-line testing) and malfunctions  
*potential for connecting operator aids and feed them with adequate information

*storage of all informations allowing proper delayed analysis of accident progression, consequences of operator action, adequacy of operator aids  

-testing of severe accident management efficiency
Here, the main goal would be to test the behavior of the whole organization in non "ideal" accident scenarios. To be more specific, it can be noted that, for risk analysis or knowledge oriented training, accident scenarios emphasize short-term coremelt, either because they reasonably bound consequences for the environment, or because it is more efficient in terms of teaching on severe accidents. However, both the TMI2 accident and the Tchernobyl accident developed slowly, and if a coremelt scenario developed one day, it could well be after a series of failures resulting from progressive degradation of components or systems extending over a long period. Resulting coremelt would then progress slowly.

For such situations, many operators or crisis team specialists would have to be involved to perform the same job and it could be useful to understand whether such situations would create new conditions for SAM. Issues to be analyzed could be:

*how to keep track of accident progression, operator actions, and analyses supporting some interpretations and decisions for SAM consistency

*evolution of judgement on plant status when shifts change, and potential consequences for accident management

*communications between plant staff, the technical support center and the crisis team

*potential divergence on what to do (e.g. if diverse means and operator aids are used to evaluate plant status and potential strategies, how to handle the situation to minimize risks of choosing poor SAM strategies. Influence of computer software and hardware could be significant)

*how to keep track of the whole scenario for accident debriefing.

Basically, problems are not very different from that related to SAM, except that more data need to be stored, by different organisms, and that drill conclusions are likely to be more difficult to draw, in particular if contradictory interpretations emerge at some point into the accident.

IV)-CONCLUSIONS AND PERSPECTIVES

As was stressed in the final report issue by SESAM, SAM implementation has been progressing tremendously since 1992, and many utilities already have, or are on the verge of having implemented SAM programs.

These programs recognize that Beyond Design Basis events, in particular those leading to coremelt are intrinsically more difficult to handle
because physical phenomena are very complex and the operator is in adverse conditions.

They also recognize that the potential lack of information on plant status results in the need to recommend simple actions based on easily understandable information. Besides, comparison between SAM approaches in OECD countries shows that, though minor differences exist in the detailed implementation of SAM programs, recommended actions are very similar based on convergent analysis of their advantages and drawbacks.

The need for training people is also recognized, but implementation of training programs seem to be lagging behind SAM programs. This is not actually surprising considering the complexity of the problem and the potential financial implications of training program implementation. As is the case for "conventional" training, many objectives can be contemplated to take full advantage of training sessions, but besides the complexity of computer models, needed resources could vary widely, and utility objectives must be carefully weighed against costs incurred and potential benefit for Accident Management. Analysis of drills, including operator aids response, also requires highly skilled people, at least at the time being.

The real question behind is which kind of training is needed for plant operators, and is there room for cooperation between utilities vendors and regulatory bodies to define versatile tools adapted to a wide variety of situations.
FULL SCOPE SIMULATOR WITH AN EXTENDED SCOPE OF MODELING AS A TOOL FOR DEVELOPMENT AND PROOF OF OPERATOR AIDS FOR SEVERE ACCIDENT MANAGEMENT

S.D. Malkin, Head of Dpt., V.V. Shalia, Chief of Lab., I.D. Rakitin, Chief of Lab., A.A. Tutnov, Chief of Lab.
RRC "Kurchatov Institute", Kurchatov sq., 1, 123185, Moscow, Russia
<sdm@odum.m.imp.kiae.ru>

ABSTRACT

Factor of risk caused by the personnel's faults primarily in non-regular and emergency situations may be rather great. In the world practise the major way of it's diminishing is the application of simulators. It betokens the RRC "Kurchatov Institute" experience in creating the full-scope simulators, analysers and large modelling complexes for Nuclear Power Plants (NPPs) and other nuclear facilities.

Recent developments of RRC "Kurchatov Institute" are aimed at the soonest and minimum expenditure's creation of modern high-performance means for personnel's training and regular re-training and also at the development of means of modeling, safety analysis and operators' support with severe accidents to be included. In this view, the most elaborated one is the Training Support Center (TSC) created at the Leningrad NPP, Sosnovy Bor, Russia. To be applied in this center, GSE Systems of USA and RRC "Kurchatov Institute" have jointly developed the Total Training System that incorporates full-scope simulator, analytical full-scope simulator, expert system, interactive system, psycho-physiological system, and training support programs.

Mathematical models creating and special software developments were the responsibility of RRC "Kurchatov Institute", the hardware and general purpose software were the responsibility of GSE Systems.

Presented are the basic specifications of one of the world's largest simulators - the full-scope simulator for the Leningrad NPP that is the new-generation one. Owing to the extended modelling scope accomplished is the possibility of training personnel to act in terms of not only the design-basis but rather the severe beyond the design-basis accidents. As an example, the Chernobyl accident and disaster modelling are presented for the "old" and "new" up-graded RBMK Safety Systems design and core features.

I. INTRODUCTION. FEATURES OF THE RBMK-TYPE REACTOR AS THE CHALLENGE FOR ITS SIMULATION

The specialised design of commercial channel-type graphite moderated boiling reactors (to be based with the USSR late 40-ies - early 50-ies design of so called "production" reactors for military use) RBMK-1000 (1,000 MW(e)) had been firstly implemented at the Leningrad NPP from 1974 y. (1st unit), till 1981 y. (4th unit).

There are now thirteen (13) RBMK-1000 units under operation at Russia and Ukraine, and two (2) RBMK-1500 units at Lithuania.

The RBMK-type unit's main features are such that provide a lot of obstacles and difficulties for its modelling and full scope simulation, e.g.:
- coolant's boiling and saturated steam generation at each of the 1,600 pressure tubes (channels) of the huge core (7 m height and 12 m diameter);
- as neutron flux and power distribution, as well as reactivity control are provided with using a sophisticated system of in-core distributed detectors and by each of 220 control rods, to be autonomously (manually and automatically) driven and positioned onto the different heights in the core;
- permanent "on-line" refuelling at a full power (2-3 fuel channels per day);
- an absence of primary and secondary circuits as well as of a steam generator in the "common sense" traditional meaning. Namely, a saturated steam and water mixture from each core channel are to be combined and accumulated above the core at the four drum separators, and after that separation the saturated high pressure steam passes onto the two turbines with electrical generators 500 MW(e) each. But the remaining water from the drum separators as well as the turbine condensate are passed back to the group header collectors by means of feedwater pumps and main circulation pumps, and further to the core channels;
- the core neutron flux and power distribution instability and a need in a special distributed automatics control system to cope with it,
- a need in a complex and sophisticated Plant Process Computer (PPC) system (SKALA) to control the unit. Importance of SKALA is such that under its malfunctioning the unit should be immediately passed to decreased power levels and later passed to shut down,
- a need in very sophisticated neutronics and thermal hydraulics codes to support as the design and operation, as well as the simulation.

The a.m. RBMK features provide with complicated and detailed 3-D tools for the core modelling (neutrons and two phase thermal hydraulics), sophisticated tools and codes for the Balance-of-Plant, and, last but not least, solving the question for the modelling of the Plant Process Computer (PPC) "SKALA".

The RBMK-type unit is operated by the team located at the Main Control Room (MCR) and consisted of the senior supervising operators as Plant Shift Supervisor (PSS) and/or Deputy Plant Shift Supervisor (DPSS) and of three executive operators as the Reactor Operator ("RO" to monitor and control core neutronics and thermal hydraulics, neutron flux and power distribution, reactivity, state of the Reactor Safety and Protection systems, reactor's heat and steam production, etc.), Unit Operator ("UO" to control balance-of-plant), and Turbine Operator ("TO" to control turbines, electrical generators, electrical distribution and electrical devices, etc.)
In addition, there are Local Post Operators positioned at Local Control Rooms and Local Control Posts in different areas of the plant to control and supervise, e.g., Fuel Reloading Machine, Water Chemistry, Plant Electricity Dispatch Center, Reactor Main Circulation Circuit and Pumps, Turbine and Generators Central Hall, Radiation Monitoring and Environment Protection, etc. These Local Post Operators are communicated with the MCR Operators and their activity is of utmost important to provide the plant's safety and operation. Since that, the LNPP Customer's Full Scope Simulator Project specification required quite reasonably with the complex joint training of the whole Operation Team, as of the Main Control Room, as well as of the Local Posts. So, the operation of the RBMK-type units is rather complicated and would require a set of specialised measures to be simulated with.

In addition, the PPC "SKALA" as the main instrument to operators' support is rather obsolete as for hardware as well as for its software and Man Machine Interface (MMI) design of early 70-ies, and is under permanent up-grade and modernisation during last years. New tools, devises and systems for operators' support are under development, testing, and implementation. Since, it was demanded to provide with the "open" possibilities for SKALA algorithms simulation to be up-graded and changed. This goal was successfully achieved with development of a special tool for SKALA codes' emulation.

And, last but not least, there was a Specification requirement of modelling RBMK severe accidents under the Project Design for the Leningrad NPP Simulator. Putting in mind the Chernobyl Accident and a very sensitive attention to the RBMK up-grade and to its future fate as from the RF Regulatory Bodies, as well as from the International Communities, mass media, publics, etc., this "severe accidents" requirement is seemed as fully reasonable and timely one.

It is well known that factor of risk caused by the operators' faults primarily in non-regular and emergency situations may be rather great. In the world practise the major way of the human factors' risk diminishing is the application of simulators. The recent developments by RRC "Kurchatov Institute" are aimed at the soonest and minimum expenditure's creation of modern high-performance means for personnel's training and regular re-training and also of means for modelling, safety analysis and operators' aids development with severe accidents to be included. In this view, the most elaborated one is the Training Support Center (TSS) created at the Leningrad NPP, Soznoy Bor, Russia. To be applied in this Center, GSE Systems of USA and RRC "Kurchatov Institute" have jointly developed the Total Training System (TTS) that incorporates:
- full-scope simulator;
- analytical full-scope simulator;
- expert system;
- interactive system;
- psycho-physiological system;
- training support programs.

Mathematical models and special software creating were the responsibility of RRC "Kurchatov Institute", the hardware and general purpose software were the responsibility of GSE Systems.

Owing to the advanced technologies and recent accomplishments in mathmodeling by RRC "Kurchatov Institute" the LNPP full scope simulator enables maintaining and training with operational personnel the correct actions' skill in real time under the assigned emergency situations' conditions and with involving in this training the enlarged shift's staff. Possible is to apply not only the full-scope Main Control Room (MCR) operational prototype (MCR-O), but non-operational MCR (MCR-N) panels, as well as the local posts control panels' computer models and their "soft panel" presentation.

LNPP full-scope simulator utilises the high-capacity I/O system to ensure data exchange and display on the MCR panels and on the colour graphic displays in 27,000 parameters. There are 3 instructor stations at the MCR and 6 remote instructor work stations for the Local Posts included in the full-scope simulator for providing effective training process.

The simulator provides the new scope of options and possibilities for the user:

1. The possibility of holding the training process for the entire shift of 50 persons by employing the six 'remote work stations as the operations' reproduction from the local control posts.

2. The portion of work stations and instructor stations has a form of main and local CR "soft panels".

3. The here above Items 1 & 2 enable the reproduction of real mistakes by the whole shift' personnel that arise during training.

4. The component malfunctions allow to perform with practically infinite number of variables and emergency situations with severe accidents to be included.

5. The prototypes of the personnel support systems (Operator Aids) are included in development, testing, adjusting and evaluation which enable the monitoring of
the training process by the application of special formats.

6. The possibility of local posts' operation jointly with the simulator and in off-line mode.

It's the first time ever that the full scope and analytical simulators ensure the modelling of the severe beyond the design-basis accidents, making the appropriate technology processes' analysis and trying out provisions. Therefore, these new-generation simulators are apt for training the personnel to act in severe beyond the design-basis accidents, and also for the development and evaluation of the appropriate scenarios to provide emergency training as well as for development, up-grade and proof of the Operator Aids, e.g. SPDS-type systems.

Training Support Center (TSC) created at the Leningrad NPP, Solnovy Bor, Russia, provides a new scope of R&D work as for the vendor and/or developer as well as for the user. Severe accidents modelling as well as possibility of development, adjusting and testing of any new or up-graded Operators' Support System before its installation at the reference unit' Control Room are the most important ones.

II. FEATURES OF THE RBMK-TYPE SIMULATORS' MODELING

With a view to modelling, the RBMK-type reactors are among the world's most complicated ones. The "real time" on-line 3-D mathmodel of RBMK utilised in the LNPP full scope and analytical simulators has as its base the most detailed and verified "best estimated" off-line codes developed in RRC "Kurchatov Institute":

(a) the advanced STEPAN_SIM 3-D neutron kinetics "real-time" model and code to calculate fuel channels with various degrees of enrichment and burnup, all kinds of absorbers and control rods. The delayed neutrons incorporate 24 groups for U-235, U-238, Pu-239 and Pu-241. Neutron cross sections are the functions of fuel temperatures, coolant density, fuel burnup, etc. Neutron cross sections are the functions of the core nodes' properties with a partial and total melting too. This "real-time" code is based upon the STEPAN "best estimated" off-line model and code.

The "base principle" STEPAN model is verified by the wide set of static and dynamic reactor experiments. Thus, STEPAN full-scope neutron-physical module, integrated with KOBRA full-scope thermal-hydraulic module to incorporate the distributed mathematical description of all the RBMK 1661 fuel channels of multiple forced circulation circuit have been enabled first time ever to reproduce complete and non-contradictory pattern of the Chernobyl accident.
development initial phase as based on data actually registered at the Chernobyl NPP unit #4 during the Accident.

STEPLAN and STEPLAN_SIM codes are based on a realistic 3-D representation with no simplifications as synthesis, symmetry, etc.

(b) the advanced KOBRA_SIM thermal hydraulics "real-time" code and model, which is thermally unbalanced and mechanically non-homogeneous (steam and water). The code is based upon the KOBRA "off-line" model. This model utilises so called "first principle approach" with a full-scale map of modes, reliable constitutive correlation and properties of water and steam through the entire range of steady-state and emergency modes.

The "base principle" KOBRA thermal-hydraulic code may be applied for the calculation of non-stationary processes in the random system of interconnected steam generating channels with heat exchange. This code allows to make calculations for a wide range of the modes' parameters (including the superheated steam up to 100,0 MPa pressure) and is used for modelling various nuclear power units' dynamics.

Numeric methods utilised in KOBRA code are based on the direct solution of mass, pulse and energy conservation equations. KOBRA code allows to calculate non-stationary processes in an unbalanced approximation.

(c) the advanced STALACTITE thermal dynamics and mechanics "real time" code and model, which is used for calculations of the fuel rods and assemblies, pressure tubes (channels), their Stress and Strain State analysis, and the coolant's hydraulic processes in any local area of the core, where an accident takes place. The code is applied for core elements melting, distortion & destruction processes, etc.

Thanks to the KOBRA_SIM, STEPLAN_SIM, and STALACTITE modelling systems' integration, first in world simulators' practice it is capable to describe and demonstrate not only the interconnected neutronics and thermo-hydraulics processes, but also the integrated with them thermal-mechanics distortion & destruction and melting processes in the nuclear reactor core, and the impact & disturbances introduced by automatic control, protection devices, as well as by the operators of MCR and other control posts.

Simulation tool "STALACTITE" has been developed as a simplification of the "base principles" fundamental "off-line" calculation codes "RADAR" and "PULSAR", created in RRC "Kurchatov Institute" for a detailed modelling of thermal physics, deformation and strength analysis processes in fuel rods under normal (steady state and transients) and accidental reactor conditions. Calculation
code "STALACTITE" is intended too for a simulation of a coolant behaviour (thermal hydraulics) in any accidental area (zone) of the core. In spite of a computer's performance limitation of the "STALACTITE" code (a significant calculation time for the full scale reactor core description with all the RBMK 1661 fuel channels) this one code is able to be adjusted and activated for a chosen limited number set of nodes with fuel channels to be dependent with the heat fluxes of the given set. Since the code could accept an unlimited heat flux from the outside source (e.g., from the fuel elements) into the given set of nodes of a hydraulic computation numerical scheme. Under that, stability and approximation problems of the used numerical algorithm are not infringed. That one condition is needed and very important under a simulation of a fuel fragmentation during any RIA ("reactivity insertion accident").

The "base principle" code "RADAR" is intended for a simulation of fission products storage in a fuel, of fission products release through the leaking fuel rods into the coolant, and of its spreading and decay into the reactor coolant system. The "RADAR" code could estimate a radioactivity spreading onto the reactor premises too.

The enumerated above "off-line" calculation codes "RADAR" and "PULSAR" have been chosen as a base for creating of the simplified "STALACTITE" simulation tool owing to the following reasons:

- Codes "PULSAR" and "RADAR" are tested, verified and licensed by the Russian NRC ("GOSATOMNADZOR") for the given use.
- The codes are accepted and adopted as a part of the Russian Federal Program on fuel modelling and experimental support. Therefore, the codes' verification with new experimental data should be carried out all the time, and the algorithms are to be permanently upgraded with increasing the codes' possibilities. In particular, it is related to modelling and experimental data transfer from the fresh fuel and cladding properties with taking into account the fuel burn-up and cladding fluence. Hence, modernising of the "real-time" tool requires with minimal supplementary funding and manpower expenditures.

The following conditions and assumptions have been used to perform the severe accidents' calculation code's simplification for a "real-time" simulation:

- All the processes are taking place under the first "controlled" stage of the accident, i.e. when a connection and communication with the Main Control Room do make sense, to be simulated in detail.
- After the reactor control has been lost, destruction processes in the core are considered just only with a "binary tree" scenario, according to the criterion's principle "Yes-No".
The simulation tool "STALACTITE" has been successfully used for the Full Scope Simulator severe accidents' description. The Simulator's software and hardware development as well as the Training Programs implementation have demonstrated a successful possibility of integration between this tool and other simulation tools. So, the "STALACTITE" tool has been combined with the real-time thermal hydraulics simulation tool "KOBRA_SIM", with the real-time neutronics tool "STEPAN_SIM" and other tools and codes of this LNPP simulator.

"LOCA-type" accident at the RBMK-1000 reactor (when one of the core channels is corked at its bottom part) has been successfully realised for a training demonstration. The result of the accident is the fuel rods' and channel's cladding depressurization and possible fuel damage and radiation leakage.

III. CHERNOBYL SEVERE ACCIDENT MODELLING AND ITS SIMULATION OPTIONS AT THE LNPP FULL SCOPE SIMULATOR

Another one example of interest is the "RIA-type" accident's simulation of the Chernobyl NPP disaster (April 26, 1986) with using LNPP Simulator. The accident took place during the experiments for the turbines and Main Circulation Pumps (MCP) work under so called "MCP run out".

The analysis of this accident showed that the physical reasons for its catastrophic sequence were the positive void reactivity coefficient and the deficiency of the RBMK control rods past design (so called "positive scram" for some specific positions of the control rods under specific core conditions). These reasons were aggravated by improper operators' actions and their malfunctioning with a serious violation of the Procedures and Rules for the unit operation.

This conclusion was obtained by a number of independent researchers with using different "off-line" best estimate codes, with "off-line" STEPAN and KOBRA "first principles" codes to be included. But the engineering analysis was performed (by definition) without detailed descriptions of the Safety and Protection systems, its logic, presets, etc., and, of course, without the "real time" simulation of the systems' and operators' actions and/or malfunctioning under the accident's propagation.

These new challenging goals could be performed only with using the full scope simulator. The first in the world "real time" Chernobyl accident simulation was performed under some special assumptions and modifications of the
existing LNPP Full Scope Simulator models and Systems specifications.

Namely, as it was mentioned before, the LNPP Unit # 3 "design as it is by now" was chosen as the reference one for the Simulator. But, there were plenty of modernisation and up-grade works after the Chernobyl severe accident with the RBMK-type reactors' design, fuel enrichment, additional absorber features and its positioning, additional Safety systems implementation, Control and Protection systems and control rods' re-design. These works had been oriented to increase and enhance the operational safety, to eliminate or decrease drastically so called "positive void reactivity effect", obtain with additional Protection systems' scrams and blocking presets, etc.

In such a way, we have now the RBMK reactors' design and feature to be completely different of those which took place during the Chernobyl disaster, and the Simulator of the LNPP reflects this new design correspondingly.

In order to provide the Chernobyl-type accident modelling we have been obliged to perform a lot of the models' changes, to return back with the "old" design specifications to be adjusted with that time Chernobyl Unit # 4 1986 y. reactor's features in order to evaluate different causes and sequences of the accident propagation. This modernisation had been developed successfully for the Simulator. So, the given Simulator's models include by now optionally the "old" and up-graded safety and protection systems with its logic and presets, "old" and "new" core loading with corresponding properties (loading map, fuel channels burn out, macro constants) and all the rest needed for the proper simulation.

There were obtained the three main results of the modelling during these simulation experiments.

1. It was demonstrated in details that the "new" up-graded design of the Safety Systems and of the reactor's core fuel loading does prevent the disaster and severe accident propagation. The RBMK reactor is to be safely scammed even after the personnel malfunctioning and improper actions of the same type as during the past Chernobyl accident.

2. It was restored the same severe accident propagation with the "old" safety systems' design and the reactor's "old" loading and "old" control rods design corresponding with the Chernobyl Unit # 4 ones as on the tragedy date April 26, 1996. The simulation results correspond well as with the engineering codes' results as well as with the real data registared at the Unit # 4 during the accident by the SKALA system.
Namely, the run out of the four MCP (the experiment's goal) was started in 1 hour 23 min. 04 s. on April 26, 1996. The reactor was operated at the low power level (200 MW) with practically all the control rods out above the core. (This was a serious violation of the Procedures and Rules requiring to have sufficient operation reactivity margin).

The reactor coolant flow was decreased in by 10 % till the moment 1 hour 23 min. 40 s. and was not changed significantly during the next 5-6 s.

The push button AZ-5 ("manual total scram" initiation with all the control rods' immediate insertion into the core) was pressed (actuated) by the operator in 1 hour 23 min. 40 s. and registered by the SKAL with no power rising on this time. It should be noted that the given accident sequence of events was opposite to "usual" one where the power rise protection signal should appear before AZ-5 initiation. The operators were scared with something but the real reasons of this button pressing are not quite clear till now. And this action was the actual beginning of the disaster.

The sharp power rise triggered the reactor automatic protection signals that were detected 3-4 seconds later AZ-5 actuation.

The accident was initiated by positive scram effect, i.e., the positive reactivity was introduced by the control rods' insertion. The resulting power rise led to coolant boiling and thus additional positive reactivity due to large positive void reactivity coefficient. The integral energy release was sufficient for fuel fragmentation in the bottom part of the core after 5-6 s. The maximum fuel enthalpy in the core bottom was about 300 cal/g.

The result of this accident's simulation is a fuel fragmentation, total core destruction, and total radioactivity pollution.

3. Under the specifications of the 2nd simulation (see above) it was assumed that the past Chernobyl Plant operators were trained with the RIA-type Severe Accident event sequence at the would be Full Scope Simulator of our type and be prepared with the possible positive scram effect under specific core conditions and control rods' positions. Other words, the operators were trained with the special manual control rods' manipulations prior to the AZ-5 push button actuation provided the a.m. core specifics.

It was demonstrated that the skilled and trained reactor operator could successfully prevent the disaster within few seconds prior the neutron power burst and provide the designed reactor scram.

This one convincing simulation experiment has clearly demonstrated the usefulness of the Simulators with the Severe Accident modelling option.
IV. THE SIMULATORS' USE FOR OPERATORS' AIDS DEVELOPMENT

The LNPP full-scope and analytical simulators are also used to evaluate the safety and efficiency of engineering approaches to maintenance, modernization or equipment replacement, that is, upgrading process systems or control & protection systems, operators' support computer systems (expert "advisers"), and also maintenance and emergency provisions and any other MCR improvements prior to their accomplishment at real power units. The development and adjustment of two state-of-the-art Operators' Support Systems with using of LNPP Simulators are of interest. These systems have been developed jointly by RRC KI and LNPP team.

1) ODES (Operational Diagnostics Expert System)

ODES is provided for the operational "on-line" automated diagnostics of malfunctions at NPP's basic process equipment and for an intellectual support of operators. The ODES is a further development of the approach had been successfully implemented in two codes:

DIAG code which was firstly commissioned at the Smolensk NPP. It is used for the NPP basic process equipment malfunctions operational diagnostics and for the intellectual support of the operators and, if necessary, of the premises shift personnel.

and SPRINT code which is under pilot operation at the Ignalina NPP Unit #1. At present, within its scope are 27 streamline process systems of the power unit (with 60 subsystems in total). Over 10,000 malfunctions are subject to diagnostics, and upward 30,000 rules are installed in data/knowledge base.

The ODES system proved to be particularly effective at:
- avalanche data flows;
- diagnostics of control equipment and automatics;
- operators' errors;
- onset of violations.

Present ODES is aimed at on-line diagnostics of the NPP basic process equipment malfunctions. The ODES Prototype is under testing and adjusting now with the Full Scope Simulator. The foundation of ODES is formed by expert models of diagnostics, which comprise database of measuring process parameters, knowledge base of parameters behaviour, assorted texts of diagnostics messages and recommendations for the operator.

To make reference for the elements of the basic process equipment, ODES is provided with Network On-line Data Base (NODB) consisting of measured power unit parameters' current values.
ODES system creating is aimed at increase in safety reliability and power unit operation effectiveness by:
- automated (with pre-set time interval) early-stage detecting of malfunctions and breaks in all the basic process systems;
- output of diagnostics results for the operational personnel in concise and suitable form;
- output of recommendations (advice) for the operator on confining malfunctions and trouble-shooting (as per the current process regulations, technical manual and other specifications);
- diagnostics results and adjoining process data archiving on computer storage media.

Fulfilment of works is tied with algorithms and diagnostics codes creating, analytical and experimental study of static and dynamic characteristics of basic nuclear power unit equipment, optimization of diagnosis process and its confining advice messages results visualisation; optimisation of man-machine interaction (MMI).

It is assumed, that after testing of ODES as a part of the simulator and after all the necessary modifications the system should be installed at the real power unit # 3 of LNPP.

2) GOSS (Generalised Operator Support System)

The first priority goal of GOSS is to decrease of mistakes' probability and, especially, of "wrong decisions" of personnel under NPP operation from normal and up to accident states of the power unit, severe accidents to be included with. A detailed description of the System and a ground of its testing with the Simulator is presented at this SAMOA-2 Meeting. It is planned, that after a thorough testing and validation of GOSS for all the modes as a part of the simulator and after all the necessary modifications of models and codes the system should be installed at the real power unit # 3 of LNPP.

V. CONCLUSION

The LNPP simulator creating work meets the advanced criteria for full scope simulators' development, creation, integration and testing. American National Standard "Nuclear Power Plant Simulator for Use in Operator Training ANSI/ANS-3.5." is used as the basic standard.

The simulator' section pertinent to modelling the severe accidents employs the major provisions specified in IAEA documents and the RF NRC (Gosatomnadzor) recommendations.
Introduction of similar simulators' use as for severe accidents description as well as for testing, adjusting and up-grade of the Operators' Aids will make it possible to significantly improve NPP safety, to rise qualities of its specialists training and operators' support, and to diminish the possibility of accidents' rise and propagation.

REFERENCES


ACKNOWLEDGMENT

The significant contribution to the LNPP simulators creating is made by:
- the Leningrad NPP work's initiator A.Yeperin, LNPP General Manager V.LEBEDEV, LNPP experts and specialists M.Khoudiakov, V.Moskovsky, V.Romanov, A.Glebov, Test-operators and many others;
- the team of specialists by the US GSE Systems headed by E.Lin, the former heads of the US GPI T.Jenkins and A.Arora;
- the group of the "Electropult" plant employees headed by V.Kuznetsov and A.Fedorov;
- the group of the "NIKIET" headed by M.Mikhailov, V.Postnikov, and A.Aleksakov.

And, lastly, both the development and creation of the new-generation simulators and the creation of new modelling technology were greatly contributed by the "Kurchatov Institute" scientists E.Riazantzev, N.Kuharkin, E.Burlakov, A.Krayushkin, and others.

At the entire work stages we felt the complete understanding and deep support by the President of "Kurchatov Institute" Academician E. Velikhov and Vice President Academician N. Ponomarev-Stepnoi.

Authors would kindly acknowledge the sponsorship of the OECD/NEA Administration for the Paper presentation at this SAMOA-2 Specialists Meeting.
Development of an Integrated Simulator and Real Time Information System for Training in Severe Accidents

AUTHORS

Pedro Corcuera, Mario Garcés, José Melara
Department of Applied Mathematics and Computer Science
University of Cantabria
Av. de los Castros s/n
39005 - Santander - SPAIN

Tlf 34 42 20.18.43  Fax 34 42 20.18.29
email: pedro.corcuera@nuclenor.es
mario.garces@nuclenor.es
jose.melara@nuclenor.es

Julio González, Jose Vicente López
Nuclenor, S.A.
Hernán Cortés, 26
39003 - Santander - SPAIN

Tlf 34 42 24.51.00  Fax 34 42 24.51.23
email: josev.lopez@nuclenor.es
julio.gonzalez@nuclenor.es
Development of an Integrated Simulator and Real Time Information System for Training in Severe Accidents

Abstract. As part of a Research and Development project jointly undertaken by Nuclenor S.A. and the Department of Applied Mathematics and Computer Science of the University of Cantabria, at the beginning of 1995 a plant transient and accident simulator was released, based on the MAAP computer code, which is able to analyse emergency situations beyond the design basis. The use of this tool at Sta. María de Garoña NPP has significantly improved the operators and support personnel training on Emergency Procedures. This simulator has an interactive graphic interface to control the simulation itself and the safeguard systems. It also allows the link with the SPDS.

The simulator is designed in such a way that several users can interact simultaneously on the process. It currently consists of six monitors assigned both to control and to visualise systems. The instructor can provoke anomalies before and during the training exercises. The operators have several consoles (5) from which they can interact in real time to control operations and resolve the conflictive situations. It is important to note that the use of a common tool for training and safety analysis favors the collaboration of the plant and engineering personnel responsible for these two areas. An additional capacity already incorporated into the simulator is the possibility of visualising the real time plant data from the SCADA system. The same screens developed for the training simulator are used for this purpose and vice versa. This capacity can be achieved from any computer station at the network.

The paper describes the following applications and benefits of the system:

- The simulator is used for periodic retraining of Plant operators on abnormal and emergency operating procedures. Its use has facilitated the collaboration of the operator on the accident sequence analysis part of the PSA. Some human reliability aspects, especially those relating to operator response are better analyzed with the help of the simulator.
- The SPDS system developed represents a substantial modernization of the plant data display system. The maintenance of the system, required by plant modifications and other reasons, is readily transferable to the simulator. It is easy to switch between the display of real data or simulated data from any monitor connected to the LAN.
- The accident scenarios prepared for the emergency drills are currently run on the simulator. The simulated data can be displayed on the Plant Technical Support Center and on the Emergency Response Center at the Corporate Office. This capability has introduced more realism in the drill and contributed to the improvement of training on emergency response.
- The Severe Accident Management programme that is currently being developed for the Spanish nuclear power plants considers the training on severe accident scenarios. It is considered that our simulator offers a good way to comply with this new requirement with minor modifications. Moreover, it could be used to validate the new guidelines for severe accident management and in its training.

Additionally, we describe two possible applications in the area of operator support related with the simulator:

- The incorporation of a data analysis module to treat plant data and convert it into a MAAP input file. In this way, the simulator can be initialized at a point in time into a Plant transient and used as an operator aid, given that it can run much faster than in real time.
- An expert system for the tracking of the Emergency Operating Procedures in such a way that the transient evolution reflects the actions that the operator should perform at any time.

The main conclusion of this project is that we have gained a lot of experience adjusting the simulation code to our plant and the capacity of distribution of the results across the computer network in a graphical manner and real time.
1. Introduction

This paper describes the results of a series of research and development projects in the area of simulation and plant data management that have been carried out for Santa María de Garoña NPP over the last ten years. It is important to observe that Garoña plant, a General Electric Boiling Water Reactor with a nominal thermal power of 1381 Mwt, has been connected to the grid since 1971, being the second oldest Spanish nuclear power plant and, therefore, having accumulated a large experience in all these years of operation.

Most of these projects, as that of the Interactive Graphic Simulator, have been developed jointly by Nuclenor S.A., the owner of Garoña NPP, and the Department of Applied Mathematics and Computer Science at the University of Cantabria. As we will see later, the benefits derived from them have outdone by far the design objectives, revealing useful for many other applications. In this way, Garoña NPP currently holds the suitable tool for accomplish most of the training requirements that Severe Accident Management imposes.

The first section of the paper includes a brief explanation of the simulation background that led to the undertaking of these projects. Then, the Interactive Graphic Simulator is described in detail: simulating code, graphical interface, configuration and current uses. The next section refers to the Real Time Plant Information System; its relationship with the simulator and the advantages of having integrated both tools. Finally, a set of future projects and feasible applications, some of them already started, is shown.

2. Background

From 1984 up to these days, the Spanish nuclear power plants have been performing Probabilistic Safety Analysis (PSA) of a continuously increasing scope. The first of these studies was the Santa María de Garoña Level I PSA, as required for the Spanish Nuclear Safety Council (CSN). This study, finished in 1985, was performed with limited information on plant transient behavior and without any simulation tool.

Since 1987 we have been working on plant simulation models aiming to study, analyse and develop information science techniques for the control and simulation of the systems which make up a nuclear power plant. Our interest was focused in the fields of Neutronics and Thermalhydraulics with specific application to Garoña plant.

Taken into account that codes capable of simulating the running of a nuclear power plant such as Garoña were already available, the first stage was to develop a set of applications that, by incorporating graphic capacities, would enable a faster interpretation of the results of the simulations obtained by these codes, mainly LTAS.
TRAC and MAAP. These applications were designed in such a way that real plant events could also be analysed and even compared to the corresponding simulations.

With the experience acquired from these works, it was decided to develop a training simulator which, while maintaining and also improving the previously mentioned graphic features, would allow an interactive link with the adopted simulation code.

Lacking of a full scope simulator, Garoña's operators are trained at the Monticello NPP full scope simulator, so the main requirement to the new graphic simulator was to be able to cover at least the operator training in Emergency Procedures Guidelines (EPG's), saving an important amount of training hours at Monticello. To achieve this goal it was necessary to develop an interface through the SPDS (Safety Parameter Display System) displays with the interesting consequences that are described later.

3. The Interactive Graphic Simulator TSG

TSG (Training Simulator for Garoña Plant) is the Interactive Graphic Simulator that resulted from that project. It was released at the beginning of 1995 after a thorough validation against real plant events. The CSN acknowledged it as a valid tool for training and, since then, Garoña's operators spend a fixed amount of hours training on it every year. The tests related with EPG's to obtain the operator and supervisor licenses are also carried out on it.

The simulator is capable of simulating the plant behavior, in real time or much faster, during abnormal and emergency events, including those beyond the design basis and also severe accidents. In addition to some specific displays, the results of the simulation running are shown through the same SPDS displays that are used at the Control Room.

3.1 The simulator core: the thermalhydraulical code

In order to choose the most appropriate code to build this interactive simulator, the TRAC and MAAP codes were studied in depth: structure, modelisation capacities, accuracy, speed of calculation, suitability for interactive use and so on. Finally, MAAP 3.0B was selected as the inner code of the simulator. Being an integral code, capable of simulating much faster than in real time the thermalhydraulics of the primary system, containment and auxiliary building with all the associated systems, either under normal operation or during any kind of accident or malfunction, seemed to match perfectly with the simulator requirements. Its degree of accuracy was high enough for its main purpose of training as the complete test of transients compared to actual plant behavior proved later. Moreover, regarding its application to severe accident management, the code has
been specially designed to carry on the sequences after core melting and calculate the source term.

Some others reasons favored this decision. In 1995, the CSN required a revision of the Garoia Level I PSA that had been performed ten years before and MAAP 3.0B was selected to support the accident sequence analysis part of the study. The advantages of using the same code for training and PSA are described later.

The modular structure of MAAP constituted an additional help for the development of the simulator. Apart from the easy way provided to link the code with the user interface, also allows to improve some physical models or add new routines with little effort. Therefore, the original MAAP has been adapted to the training requirements. Some modifications were needed to permit an interactive use and a series of other changes have been performed until now, including:

- Feedwater and pressure control modules based on the TRAC model.
- A simplified kinetics model by means of correlations between the water temperature and the core flow. It is also possible to modify the total thermal power, while the sequence is running, in order to simulate a manual control rods insertion.
- Splitting of some systems that the original MAAP treats as a single loop, like the Core Spray, Control Rod Drive System, Stand-by Liquid Control and Shutdown Cooling System.
- Possibility of changing gradually a tube rupture area for a period of time during the simulation.
- Introduction of new user events to represent either operator actions or added malfunctions.

Provided that they are the main users of the application, many of these modifications have been developed taking into account the instructors' and operators suggestions after each training period. In this way, the simulator is evolving continuously. It is supposed that future training on Severe Accident Management will imply new changes but the acquired experience assures us that they will be easily implemented.

### 3.2 Simulator architecture: the interface

The simulator interface was designed according to the following criteria: it should result a friendly application, directly connected to the inner code, easy to improve and portable to different machines. The Dataviews® software, a real time graphic application, was chosen due to its orientation towards instrumentation engineering and process control. In addition, this software uses the graphics standard X-Window (X11) running under the UNIX operating system and can be executed even on PC platforms.
Therefore, the simulator consists of several graphical screens which constitute a user environment. The plant systems and components are represented by objects whose dynamic properties are associated to the events and variables which determine their performance. A program written in C language and linked with the needed DV-Tools’ routines from the Dataviews® package manages the human-machine dialogue, while the FORTRAN MAAP routines perform the thermalhydraulic calculations. At the beginning of each session, a routine creates the connections among the objects’ properties and the matching MAAP events and variables. The communication between both programs is maintained as long as the simulation runs using a shared memory area that includes the needed MAAP COMMON blocks.

Several users can interact simultaneously with the simulator. It is possible to create malfunctions or make the plant systems respond to such anomalies clicking with the mouse on the buttons or sliders of the corresponding screens. The remaining screens are designed as a help to the operator. They display information about the sequence evolution and the systems situation. The users have the possibility to navigate among these last screens which include the SPDS displays.

In order to facilitate the training of the operators, two auxiliary tools have been developed to manage the input and output data. Instead of writing a MAAP input file for each scenario, the instructor has a graphical application available for the automatic generation of the MAAP input code in such a way that he can set the initiating events and operation conditions at the beginning of the sequence by just using the mouse. In the same way, another application allows to plot any output variable to analyse the results of the exercise at the end of each simulation. Both tools have also been developed with Dataviews® software.

3.3 Current configuration

At the moment, the simulator layout at the plant training building consists of six monitors (X-11 terminals) as shown in figure 1.

One of them constitutes the instructor’s console from where he can define the scenario to run, cause new malfunctions in the course of the simulation and control the evolution of the sequence (real time or faster, backtrack or restart). The operator has his own console, with all the plant safety systems represented, to interact in real time with the simulation and try to manage the plant behavior. He can start or stop systems, adjust flows, open or close valves and so on.

The other four monitors are used to visualise the plant situation and help the operator in his task. One of them shows a group of alarms, resembling the actual alarm panels at the Control Room, although only the most significant ones are represented. A sound signal warns the operator each time a new emergency signal is detected. Other
monitor displays a set of messages describing in detail the actions taken by the operator and the response of the plant itself. In the remaining two monitors several displays can be selected to observe the plant evolution and the systems state.

![Figure 1. Current disposition of the simulator at Garoña NPP training building.](image)

Among the available displays for these last monitors there are the SPDS ones. The reason is obvious as stated above in this paper. The Interactive Graphic Simulator must serve to train operators on Emergency Procedures Guides and so, the same information should be used during training and during operation. However, the relationship between the simulator and the SPDS is stronger as will be described in the following section.

Currently, the simulator is running on a Hewlett Packard series 9000/712 workstation with 100 MHz processor. For training purposes the system runs in real time, but for other applications it may run even twenty times faster, depending on the sequence. The hardware that constitutes the simulator layout also includes one laser printer for the printing of graphics of the desired variables evolution, during or at the end of each session. An appealing feature of the simulator is that the machines in which it is installed do not need to be particularly powerful; low priced workstations and/or high level personal computers are enough.

Figure 2 represents the system hardware as well as some typical displays of each monitor.
3.4 Current uses and derived benefits

The main purpose for which the simulator was designed, training of operators on EPG's, has been fulfilled. Periodically, Garoña's operators receive courses on EPG's following the SPDS displays at the Interactive Graphic Simulator, reducing the amount of training hours at the Monticello full scope simulator that otherwise would have been required. So, the simulator has revealed itself as a very efficient and cost effective tool.

Furthermore, several different applications, some of them unexpected, have been found since it was released. For instance, it has become a very useful aid to the engineering staff responsible for the PSA simulations. Apart from the advantages of being able to analyse any PSA sequence, or some period of it, in real time while it is running on the Interactive Graphic Simulator, it has been used to verify all the new models or improvements added to the MAAP code for the PSA study. It is known that some of the lots of physical phenomena handled by MAAP are not modelled with the required detail. Thus, many times they raise some kind of problem that can only be solved by modifying the original code. Following this procedure it is sure that all these changes will be readily included in the training simulator model.

Besides, the use of a common tool for training and safety analysis favors the collaboration between the personnel responsible for these two areas. In this way, some human reliability aspects of the PSA, especially those relating to operator response, have been better analysed with the help of the simulator, discussing the evolution of the sequence and the operator actions with the operators themselves or their instructors.
The Severe Accident Management programme that is being currently developed for the Spanish nuclear power plants considers the training on severe accident scenarios. At the same time, Garoña Level II PSA study will be performed and so, the same profitable collaboration will be exploited.

Finally, there are supplementary benefits derived from the simulator output through the SPDS displays but they will be exposed in the next section because of their relationship to the Plant Information System.

4. Real Time Information System

The varied set of parameters which affect the plant operation (process data, control rod monitoring, water supply or meteorological data for example), are acquired by several systems with different purposes. These systems have been installed gradually during the operational years of the Garoña plant and now constitute an heterogeneous data access system, which uses diverse operating systems and with its output consoles located exclusively at the Control Room or at the Process Computer Room.

From 1988 Nuclenor has been working on the computerized management of plant data, mainly focused on plant operation personnel. In this way, the SPDS was developed to substitute the software included in the process computer for data display, initially as a closed proprietary system that only reached the Control Room. The Dataviews® package was also chosen due to its characteristics as process surveillance software.

After the development of the Interactive Graphic Simulator and with the gained experience, it was decided to implement a new application to distribute the SPDS displays through the company’s local network in real time, facilitating the access of all the personnel to plant data. It was released in the middle of 1995.

4.1 Description of the system and evolution

This new application, the SPDS-D (SPDS-Distributed), benefits from the open protocol that represents the standard X11. So, any computer connected to the Nuclenor network, with the unique requirement of being a X-Window station or a PC with X-emulation software for Windows, can access to the real plant data contained within the SPDS displays and navigate among them in real time. Furthermore, as the software runs in a number of different computer systems, it is not likely to be a limitation when considering alternatives in computer hardware. Other features include plotting of trends of selected parameters, printing graphics of their historical values or the access to the additional displays which were developed for the TSG, with their corresponding data from the actual plant situation.
The next step in the evolution of the system was logical. As long as the same displays were used as output of the simulations executed on the Interactive Graphic Simulator, it was easy to integrate both tools in such a way that now, from any computer connected to the network, it is possible to feed the SPDS either with real data or simulated data. It is also feasible to visualise previously recorded SPDS data.

The integrated system layout is shown in figure 3. As can be observed, the company holds a local area network (LAN) with Ethernet links, optical fiber and a microwave link between the plant and the corporate offices which are 140 km away. The plant is also linked to the Emergency Room (SALEM) at the CSN in Madrid.

![Integrated system layout](image)

**Figure 3. Integrated system layout.**

Nowadays, Nuclenor is in the process of configuring the Real Time Plant Information System in a more simplified manner. Plant data, captured by all the acquisition systems, will be send to a Data Concentrator-Distributor (CDD). This machine, an UNIX computer, will process the information as required and then act as a server, sending the processed data to the client applications. The simulated data from the TSG, which is being configured as a client/server application too, will also be sent to the CDD allowing that the SPDS clients may switch between real and simulated data when desired.

At the same time, the SPDS pages are going to be replaced with a more modern design, similar to the Monticello’s SPDS. As it was mentioned, Garoña’s operators must use those pages during its training at the full scope simulator and, besides, they incorporate a series of interface improvements resulting from the latest standards and
studies on human-machine interface. This new SPDS will constitute the first client application of the new information system.

4.2 Related TSG applications

With its present configuration, the integration of the Interactive Graphic Simulator with the SDPS-D application has produced substantial benefits. The simulator served to validate the first SPDS pages with the needed dynamic approach due to the slight variability in the visualised process during normal operation. Moreover, since their installation at the Control Room, the generation and maintenance of operator interface software has been common for the plant data system and the simulator.

However, the most attractive application of the distribution of simulated data through the Nuclenor network has been experienced in the last emergency drills. These exercises are carried out periodically at the plant, aiming the training of all the personnel on emergency response. Since 1995, the accident scenario prepared for the drill runs on the TSG. In this way, the simulated data is displayed simultaneously on the Plant Technical Support Center and on the Emergency Response Center at the Corporate Office. At the same time, the required data is sent to the CSN’s SALEM in real time directly from the simulator. This capability has obviously introduced more realism in the drill contributing to a better training of the personnel.

Regarding the substitution of the current SPDS, the Interactive Graphic Simulator has been recently applied to the dynamic validation of the new pages, as done with the first SPDS. A series of sequences have been executed on a new version of the TSG, configured to send data to the CDD, in order to verify the proper working of the system. To remark the simulator significance at Garoña NPP, it is interesting to note that this validation has been required as a compulsory previous step before the installation of the new SPDS at the Control Room. Meanwhile, the operators will get used to the new displays training on this version of the TSG that, eventually, will become the definitive one.

5. Work in progress

As shown in the previous sections, the simulator has been evolving continuously since it was released, taking into account its users’ suggestions and the company requirements. Nowadays, a set of potential future applications are being studied and some of them have already started its development. In this section we explain briefly the most relevant ones.
5.1 Severe Accident Management

As said above, in a short time the operators training on severe accident scenarios will be required to all the Spanish nuclear power plants. It will be easy to adapt our simulator to accomplish this task, introducing some minor changes on the interface and the MAAP code modifications resulting from the Garoña Level II PSA that is being performed these days. The simulator could serve to validate the Severe Accident Management Guidelines (SAMG’s) that will be developed.

We are also considering the possibility of upgrading the simulating code from MAAP 3.0B to MAAP 4, with its enhanced capabilities regarding severe accident. Nevertheless, having completed the Level I PSA with MAAP 3.0B, it seems more reasonable, at least while the Level II is performed, to maintain the present version that benefits from all the changes already implemented and the achieved experience of the engineering staff.

A more ambitious project deals with the potentiality of linking the MAAP code to a dose calculation code (e.g. ORIGEN). This tool could be used for the future Level III PSA and, if the simulator was adapted to use it as its inner code, it would become an integrated application and cover all the stages of any kind of conceivable accident.

5.2 Additional interactive displays

Nowadays, we are modifying the simulator control model in order to obtain several additional interactive displays for the operator, as a replica of the real panels present at the Control Room. Currently, the operator acts on the simulated systems by means of sliders and buttons using a simplified display. The new detailed displays will contain all the switches, buttons and controls of the real panels, adding more realism to the operator actions. The final purpose of this project is to replicate every panel present at the Control Room in such a manner that the training at the TSG will resemble the training at the full scope simulator.

5.3 Expert systems

The simulator could incorporate an expert system for tracking the EPG’s, assisting the operators with its indications to manage emergency situations. This system could be configured as a client application of the new plant information system. Further, the expert system does not need to be restricted to give advices; it could be implemented in such a way that the transient evolution run on the simulator would reflect the actions that the operator should apply according to the EPG’s, working as an ‘automatic operator’. This last approach could be used as a very valuable tool for developing and testing the future SAMG’s.
A plant data analysis module would allow the generation of a MAAP input file reproducing the actual plant situation. In this way, and given that it can run much faster than real time, the simulator could be initialized at any point in time into a plant transient serving as an operator aid. The module to track the EPG’s would reinforce this support.

6. Conclusions

The development of the projects described in this paper has supposed a very profitable experience, not only to the personnel involved in the developing process, but also to all their users during the time they have been working. We must remark the needed effort to adjust the simulating code to our plant and to distribute the results across the network in a graphical manner and real time and, consequently, the great experience acquired with this tasks.

As a result of all this work, now Nuclenor is capable of carrying out an important aspect of the training of Garoña’s operators at the plant itself and holds a modern plant information system with a constantly growing range of applications. Future requirements in any of these areas could be undertaken with sufficient assurance of success.

References


Phenomenology and Course of Severe Accidents in PWR-Plants
- Training by Teaching and Demonstration -

M. Sonnenkalb, J. Rohde
GRS mbH, Cologne

Paper presented at SAMOA-2
2nd OECD Specialist Meeting on Operator Aids for Severe Accident Management
EDF/SEPTEN Lyon, France, September 8-10, 1997

Abstract

A special one day training course on „Phenomenology and Course of Severe Accidents in PWR-Plants“ was developed at GRS initiated by the interest of German utilities. The work was done in the frame of projects sponsored by the German Ministries for Environment, Nature Conservation and Nuclear Safety (BMU) and for Education, Science, Research and Technology (BMBF).

In the paper the intention and the subject of this training course will be discussed and selected parts of the training course will be presented. Demonstrations are made within this training course with the GRS simulator system ATLAS to achieve a broader understanding of the phenomena discussed and the propagation of severe accidents on a plant specific basis. The GRS simulator system ATLAS is linked in this case to the integral code MELCOR and pre-calculated plant specific severe accident calculations are used for the demonstration together with special graphics showing plant specific details.

Several training courses have been held since the first one in November, 1996 especially to operators, shift personal and the management board of a German PWR. In the meantime the training course was updated and suggestions for improvements from the participants were included.

In the future this type of the training course will be made available for members of crisis teams, instructors of commercial training centres and researchers of different institutions too.

1 Introduction

Operators of German NPP’s are required to attend training courses on plant specific full scope simulators several times per year. These training courses covers normal plant conditions as well as training of accident situations together with existing preventive accident management measures and emergency operating procedures (EOP’s). The preventing of core melt sequences is trained intensively. For NPP operators up to now no training courses are required which covers e.g. the mitigation aspects of core melt sequences respectively the course of severe accidents.

Mainly due to the interest of German utilities GRS developed a special training course on „Phenomenology and Course of Severe Accidents in PWR-Plants“ in the frame of a
project sponsored by the German Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU). This is the first training course so far which has been held several times since the first one in November, 1996. Up to now the training course was primarily held to operators, shift personal and the management board of a German NPP with PWR. The feedback was very good and some impressions are discussed at the end of the paper.

It should be pointed out here, that there is no obligation by the NPP management board for the operators and shift personal to participate in the GRS training course. Nevertheless the number of participants is high and they are very interested on the subjects being presented.

2 Knowledge Basis

A wide spectrum of research work is ongoing at GRS sponsored by the German Ministries BMU and BMBF forming the basis of the development of this severe accident training course too. In summary main contributions to the development of the different lectures of the training course are from:

- the research work performed at GRS in different accident management (AM) projects resulting in the development of AM measures, e. g.
  - prevention of RPV-failure under high pressure by secondary and primary bleed and feed measures,
  - prevention of over pressure containment failure by filtered containment venting procedure,
  - prevention and/or mitigation of consequences of possible hydrogen combustion in the containment by a passive autocatalytic recombiner (PAR) concept which is under development,
- the knowledge gained from several severe accident calculations performed at GRS within AM projects with the detailed codes ATHLET, RALOC and WECHSL and the integral code MELCOR using detailed PWR plant specific input decks,
- an extended literature investigation to define the level of state of the art on special subjects, where only limited research work is done at GRS.

Finally the development of such a training course is not possible without a powerful tool for the visualisation of different phenomena typical e. g. for severe accidents especially in relation to the detailed NPP behaviour. The ATLAS analysis simulator was developed by GRS with the aim to create a multi-purpose tool for analyses in the filed of nuclear and industrial safety /BER 92/, /LUP92/. It is based on the GRS computer code ATHLET modelling the dynamic processes in different plants /BUR 89/. In the past an extension of the system was made to make the system useful for different other codes /POI 96/, /SON 95/ and in many different areas of safety analysis too. The analysis simulator offers a simulation environment in which the presentation and evaluation of the numerous resulting data is supported by an interactive visual display system and which makes it possible to intervene directly in the simulation as it proceeds.

The power of the system will be demonstrated on examples showing the visualisation of a broad variety of MELCOR results for the primary and secondary circuit behaviour, the core melt process, the process of core concrete interaction and the containment behaviour of a German PWR plant, used within the training course.
3 Intention of the Training Course

The main intentions of the training course are summarised in the following topics:

1. Development of a training course containing information on a state of the art basis and modern computer code based demonstrations about main phenomena of severe accidents related to German PWR.

2. Demonstration of a possible severe accident on an example (pre-calculated sequence with MELCOR) e. g. for the following main phenomena and phases:
   - initial plant conditions and early accident phase,
   - core heat-up and core melting,
   - core slumping into lower plenum and RPV failure,
   - molten core concrete interaction (MCCI),
   - fission product release (in- and ex-vessel), transport and behaviour in the containment,
   - hydrogen production (in- and ex-vessel) and release into containment,
   - measures of hydrogen recombination/ignition in the containment,
   - long-term thermohydraulic containment behaviour.

3. Demonstration of the usefulness of different plant specific accident management measures respectively EOP’s in different situations, e. g.:
   - the primary and secondary bleed and feed procedure,
   - different systems related to the hydrogen subject - the advantages and disadvantages of the use of autocatalytic recombiners or/and igniters,
   - the filtered containment venting system.

4. Sensibilisation of the audience for special severe accident problems, e. g.:
   - the instrumentation and information available during different stages of a severe accident to determine the plant status and to assess the accident progression,
   - the possible consequences of e. g. a very late injection of water into a hot or partly molten core as an additional accident management measure.

5. Development of a training course useful to held to a broad variety of people working in the nuclear field. Nevertheless the special interest is given to operators and engineers from German NPP’s with PWR at the moment.

For completion it should be mentioned, that it is currently not the intention of this training course to focus on the detailed timing of different severe accidents. It seems also not possible to provide an „on-line“ severe accident training course, running a severe accident code on a simulator tool and to allow interactions of the simulation by the people trained nor is it necessary at the moment for the people selected. Reasons which are preventing such an on-line training are e. g. the level of development and validation and the robustness of the severe accident codes used and the speed of such a calculation with a detailed plant specific input deck, too, which is several times less than real time.

Finally all these definitions above should clarify what we understand by training in the case of „Phenomenology and Course of Severe Accidents in PWR-Plants“. It is really a seminar to increase the knowledge about severe accidents and to make sensitive to special problems and aspects of them.
4 Overview of the Training Course

The training course is divided in three parts. These are an introduction into severe accidents and the used simulator system, phenomena related to in-vessel phase and phenomena related to ex-vessel phase. In each part of the training course short presentations of basic knowledge alternate with supporting demonstrations by the ATLAS simulator. Within the frame of this presentation it is not possible to discuss all the details of the one day training course. Therefore we would like to focus only on main subjects.

4.1 Introductory Chapter

In the introduction some information about the general safety concept are given first. Even if the basis of this concept is well known it seems to be necessary to replay some of the main topics and to generate a basis for further discussions. The following topics are presented:

- definition of design basis accidents (DBA), beyond DBA's and severe accidents,
- use of different accident management measures to prevent core damage or to mitigate the consequences,
- probability of different core damage states dependent e. g. from the system pressure.

In the second part of the introduction the used simulator system ATLAS and the used code system MELCOR is presented. Special attention is given to the discussion of the advantages and disadvantages of the used integral code MELCOR together with the presentation of the plant specific nodalization schemes (Fig. 1+2).

Figure 1 MELCOR Nodalisation Scheme of PWR-1300 Type KONVOI
4.2 Phenomena related to In-Vessel Phase

4.2.1 Initial Conditions and Early Accident Phase

The boundary conditions and assumptions of the scenario "Total loss of steam generator feed water supply and loss of heat sink" used as example for the training course are discussed first. The intention was to use a scenario with a relevant probability and a RPV failure at low pressure, where the most of the relevant phenomena of severe accidents can be demonstrated and where the use of existing accident management measures (secondary and primary bleed and feed, filtered containment venting) can be demonstrated as close as possible following the instructions of the existing EOP's. For all the discussed sequences the failure of high and low pressure injection systems was assumed from the beginning. The assumptions lead to the earliest time of core melting but causes also a lot of discussions from the audience.

The attention during the presentation of the early accident phase was given to actions e. g. of functions of the volume control system, the time dependent behaviour of main parameters and initial criteria for the used bleed and feed measures, well known by the NPP operators. So they can familiarise with the different kind of graphical presentation of plant specific parameters by the ATLAS simulator too.

The examination of the needed information and the available instrumentation to determine the plant status showed, that the normal plant instrumentation is challenged by the containment conditions (temperature and humidity) soon after the depressurization of the primary circuit. Those instruments are not qualified for the expected
containment conditions. Therefore only a limited number of information are available mainly from the safety-related and the wide-range instrumentation.

The main graphic used for the demonstration is the one named "PWR Reactor Circuit". Figure 3 shows one example at a time of normal plant operation.

![PWR Reactor Circuit](image)

**Figure 3** ATLAS graphic "PWR Reactor Circuit" - Situation of Reactor Circuit during Normal Plant Conditions

A large number of dynamic effects are included in all graphics. In this case the water temperature dependent on a pre-defined colour scale is shown in all parts of the reactor circuit with exception of the core. But this is only one example of the large number of physical parameters which can be selected immediately coming from the MELCOR simulation.

To allow the demonstration of the core melting process together with the reactor circuit behaviour the detailed fuel element \((\text{UO}_2)\) temperature is shown in each cell of the MELCOR core nodalization scheme dependent on a separate colour scale too.

**4.2.2 Phase of Core Heat-Up and Core Melting**

The discussion of phenomena of core melting is one of the main interesting parts of the training course. Because of the wide spectrum of existing information and experimental knowledge about the core melting process it becomes important to focus only
on topics supported by examples from the TMI accident and from one typical experiment of the CORA facility of FZK.

In relation to the course of the core heat up phase the early destruction of control rods by different phenomena including eutectic reactions is discussed first. Principles of the candling process of the molten material and the solidification and possible formation of local blockages in lower, colder elevations inside the core are presented than. After that the principles of the fuel element failure mechanisms are discussed and especially the oxidation process of the fuel element rods and the \( \text{H}_2 \) production is shown. At the end we discuss the formation of a debris pool in the lower core region supported by information from the TMI examination and from a CORA experiment.

It is well known, that the computer simulation of the core melting process by an integral code can be done only with some limitations. Therefore the audience is informed in each part of the training course about the simplifications of the code system used related to the special accident phase. Nevertheless based on the feedback from the first training courses we think that the developed and used graphics gives equivalent support to the complicated subject of the core melting and relocation process.

The main graphic used for the demonstration is the one named „PWR Reactor“. Figure 4 shows one example at a time just before the beginning of fuel element melting and relocation.

[Diagram of a reactor with labels and a description of the reactor's conditions.]

**Figure 4** ATLAS graphic „PWR Reactor“ - Begin of Core Melting Process
The core heat-up process as well as the heat up and candling of control rods just before fuel element melting can be demonstrated quite well. The relocation of the fuel element material and the formation of a debris pool can not be demonstrated in the same way mainly due to code (MELCOR) limitations.

Finally the available instrumentation to determine the plant status is discussed. It is very likely that during the core heat-up and core melting phase all instruments located in the reactor may be experienced by temperature conditions beyond their qualification limit. Therefore the determination of the exact plant situation seems to be impossible. Further investigations are necessary to assess the influence of those high temperatures to measurement techniques inside the primary circuit.

4.2.3 Phase of Core Slumping into Lower Plenum and RPV Failure

Based on knowledge gained e. g. from the TMI accident and from experimental investigations the events and phenomena during core slumping, molten pool formation inside the lower plenum and the RPV failure mechanisms are described.

As in the chapter before only some topics can be explained, e. g. the mechanisms of material relocation due to local or global failure of a molten pool above the core support plate, the quenching mechanisms of the molten material in the residual water inside the lower plenum, the potential of high energetic in-vessel steam explosions and the different RPV failure mechanisms depending e. g. on the design of the vessel and the system pressure. In addition an overview on expected loads to the reactor cavity and the supporting concrete structures dependent on the RPV failure mode respectively the system pressure is given. Finally the ongoing experimental and theoretical research work on the subject of cooling of a molten pool inside the RPV bottom head by external flooding of the reactor cavity is discussed.

During the first hours of such an accident a large number of instrumentation is expected to be failed. No special instrumentation is available to determine the RPV failure. Some information can be taken from the pressure measurement of the reactor circuit and the containment. It should exist a difference between both pressures until the RPV fails. Nevertheless it is not well known, if the pressure measurement of the reactor circuit will fail or not before.

Mainly due to code limitations (MELCOR) the possibilities to visualise the physical phenomena (material relocation, steam explosions, molten pool behaviour in the lower plenum) are rather limited. Therefore we focus on the pressure behaviour and on the oxidation behaviour and \( H_2 \) production during relocation and quenching. Thus the ATLAS graphic „PWR reactor circuit“ together with history diagrams of different parameters are used.

4.3 Phenomena related to Ex-Vessel Phase

4.3.1 Phase of Molten Core Concrete Interaction (MCCI)

The reactor cavity of German PWR containments consist of an inner cylindrical biological shielding surrounding the RPV and an outer thick cylindrical support structure, made both of reinforced concrete. It is typical for German PWR containments that the reactor cavity is dry. Thus a dry MCCI reaction is expected during the first hours after the RPV failure. Due to radial erosion of the concrete a sump water ingestion into the reactor cavity is expected to occur some hours after RPV failure followed by a long-term evaporation of the incoming water. Very special plant specific details of the cavity
design (inspection openings, air ventilation pipes) have not been included in the re-
search so far, leading to discussions with the audience during the training courses.

The presentation in this chapter focuses on chemical reactions between different re-
action partners, the type of the reaction as well as the long-term behaviour of MCCI
especially the non-condensable gas generation.

A simplified graphics (figure 5) is prepared showing a part of the reactor cavity where
the erosion front behaviour can be demonstrated.

![Diagram of Reactor Cavity](image)

**Figure 5** ATLAS graphic „PWR Cavity“ - Molten Core Concrete Interaction

The figure shows a situation some hours after RPV failure but in any case before
sump water ingestion. The temperature of the melt and the atmospheric temperature
inside the rooms as well as the sump water level is shown. The erosion front behav-
iour as well as the thickness of the melt can be expected from the axis included in the
graphic.

4.3.2 Fission Product (FP) Release and Transport in the Containment

Within the limited time frame of such a training course only a well selected overview
on important phenomena related to the FP behaviour can be given. The presentation
focuses first on the initial FP core inventory. The different phases of the FP release
and transport during core melting are discussed together with some influencing fac-
tors. The time dependent concentrations of aerosols and noble gases released can be
shown by different graphics of the ATLAS system. One example is given in figure 6,
showing the release of air born aerosols during core melting and the transport through
the primary circuit.
Simultaneously the time dependent behaviour of aerosols and noble gases in the containment can be shown by the ATLAS simulator. One example is given in figure 7, showing the transport of air born aerosols inside the containment released from the primary circuit during core melting.

Typical phenomena related to the general FP behaviour are discussed too, as e. g. sedimentation, absorption, condensation and deposition of FP. Also some information are given to the importance of Iodine and its behaviour in comparison to other aerosols. So the theoretical presentation of the aerosol behaviour in the containment is supported by this graphic. The same graphic is used to demonstrate the FP release from the reactor cavity during the early phase of MCCl in the reactor cavity.

At the end of this part of the course some results of plant specific calculations of FP release rates to the environment are presented. The importance and the influence of FP retention in the primary circuit, in the containment and in filters of the containment venting system on the release rates into the environment becomes obvious and furthermore the importance of a late initiation of filtered venting too. It can be demonstrated that the noble gases are the main contributor to the release rates into the environment. These elements can not be retained by the filters of the venting system. So about 75 % of the noble gas inventory is released into the environment.
Figure 7 ATLAS graphic „PWR Containment“ - Aerosol Transport through the Containment released from Primary Circuit during Core Melting

4.3.3 Hydrogen Production, Release and Behaviour

As for the selection of topics on FP behaviour it is very important to concentrate only on main phenomena of the large area of hydrogen behaviour. Several specialists meetings and workshops have been held world wide on this general topic and a large number of experimental research is ongoing. In Germany these general topic is very important because extended research work is ongoing on the development of a PAR concept for German dry PWR containment’s. Therefore the actual situation in Germany and the extended research work at GRS is characterised. First results of calculations with the detailed containment code RALOC for a German PWR containment are presented. The detailed containment behaviour during a selected severe accident is shown with and without an assumed distribution of a large number of PAR’s. It becomes obvious, that such an PAR system is very useful to remove large amounts of hydrogen within an acceptable time frame. The prevention of combustible conditions inside the most of the containment compartments can be shown. It is concluded that local combustions expected only during special situations will not influence the containment integrity.

In addition special attention is given during the presentation on the main phenomena of hydrogen generation during core melting and MCC1 and basic knowledge about deflagration, DDT and detonation phenomena and the related challenges to the containment integrity are presented.
The demonstrations by the ATLAS system supporting the information of this chapter are made with the graphics showing the „PWR containment“ (see example in figure 7) and using the hydrogen mole fraction as selected parameter. In addition a graphic is used showing the flammability limits in for selected rooms of the containment (figure 8). So it can be determined if a combustible situation exists in the selected rooms or not.

![Flammability Limits of H2–Air–Steam Mixtures](image)

**Figure 8** ATLAS graphic „Flammability Limits“ - Determination of the Situation in 4 different Containment Rooms and History of Total Hydrogen Generation

Due to limitations of the MELCOR code no demonstration is possible on the influences of a PAR system on the containment behaviour. Only if there is enough time remaining during the training course, a demonstration is made showing some influences of local hydrogen combustions on the containment loads. A pre-pared MELCOR calculation exist in this case for the same accident scenario including the calculation of hydrogen combustions initiated by assumed igniters.

### 4.3.4 Long-Term Containment Behaviour

The final part of the training course deals with the containment behaviour (temperature, pressure) and the use of the filtered containment venting measure. Special attention is given to the phenomena and events influencing the containment pressure during all phases of the accident. The example in figure 9 shows the pres-
sure history (trace back from actual time by 6 hr) in the primary and secondary circuit as well as in the containment and the annulus.

![Graph showing pressure behavior](image)

**Figure 9** ATLAS history „Pressure Behaviour“ at different Locations

In the history diagrams in this figure the influence of the secondary bleed and feed measure on the primary and secondary circuit pressure (measure initiated at -5 hr) becomes obvious. The influence of the primary bleed measure on e.g. the containment pressure can be seen too (measure initiated at -2 hr).

Information about the energy respectively steam release into the containment at different locations (pressurizer relief tank, cavity) during all phases of the accident are also included to demonstrate e.g. the temperature behaviour inside the containment. The example in figure 10 shows the steam release into the containment after the primary bleed of the primary circuit. It is interesting for the audience to notice that during some time intervals large differences in the concentration of physical parameters (e.g. steam, non-condensable gases, aerosols, noble gases) are expected inside the different rooms of the containment.

Last but not least this final chapter summarises the main contributions to the containment loads. The importance of the filtered containment venting system to prevent an over-pressure containment failure is underlined too. Finally the critical situation regarding the available instrumentation and the needed information during severe accidents is repeated ones more.
Figure 10  ATLAS graphic „PWR Containment“ - Steam Release from Primary Circuit into the Containment after Primary Depressurization

5  Feedback and Summary

In the previous chapters the intention and the main subjects of the training course on „Phenomenology and Course of Severe Accidents in PWR-Plants“ developed by GRS are discussed. It becomes obvious that we may interpret differently the word „training“ depending on the subject being presented in the training courses. For training courses on severe accidents it seems not necessary to provide them „on-line“, running a severe accident code on a simulator tool and allowing interactions of the running simulation by the participants. One main reason which prevents such an on-line training is the level of development and validation of the existing (integral) codes, their robustness and the time which would be required for such a training.

The lessons we learned from our training courses being held are described in the following without any hierarchical order.

1. The time frame of one day is very short to present all main topics of the wide range of severe accidents including an extensive demonstration by the ATLAS simulator. Therefore the subjects of the different chapters of the training course should be well balanced.
2. We would prefer to present the materials in the future on 1 ½ day or 2 day training course. We thus would split the course into the areas of in-vessel phenomena (first day) and ex-vessel phenomena (second day).

3. The participants from various departments of the NPP were interested in the general subject of "severe accidents" but their special interest varies depending on the scope of duties.

4. Nearly all of the participants underlined that the training course becomes so interesting due to the mixture of short compact presentations and informative demonstrations by the ATLAS simulator system used.

5. The training course described here is presented by two persons working in the area of severe accident research for several years. A detailed knowledge on most of the subjects presented and on plant specifics by the lecturers is necessary to get confidence from the audience and to answer the different questions. The confidence in the results presented rises also due to the discussion of disadvantages and limitations of e.g. the used simulation tools.

6. Examples of topics from the discussions during the courses are the following:
   - Why do you assume the failure of all safety injection systems?
     (done for the scenarios used as examples)
   - What are reasons for large differences between the probabilities of different events in different plants shown in the introduction of the training course?
   - Would you recommend to inject water into RPV at any time during core melting and before RPV-failure?
   - In which way does the plant specific cavity design may influence the course of MCC1 and the containment behaviour?
   - What do we notice in the control room from the different processes in the containment during severe accidents?

For the near future it is planned to present this training course to instructors from a commercial NPP training centre and to researchers working for PSA level 2. At the beginning of the next year additional training courses are under discussion at further German NPP's. An application of the training course to the behaviour of German BWR under severe accident conditions is planned too.

**Literature**


/POI 96/ W. Pointner, M. Sonnenkalb, D. Beraha, V. Maidanek,

/SON 95/ M. Sonnenkalb,
„Application of MECLOR for German LWR; Results of Accident Analysis and Visualisation of Data“, Paper presented at 3. MCAP Meeting, Bethesda, 26.-28. April, 1995
Integration of Operator Actions in Accident Sequence Simulation Tools. Application to a BWR Plant

Javier Hortal *
Amparo García-Zamorano †
Enrique Meléndez *

1 Introduction

Engineering simulators have been widely used for transient and accident analysis[1]. They are specially suited for those scenarios where the operators are not expected to play a significant role and the nature of the phenomena to be simulated does not change dramatically along the simulation time. However, in long-term accident sequences, actions cannot be ignored and the plant behavior ranges from control transients to core melting and fission product release.

For this kind of scenarios the use of engineering simulators is difficult and sometimes questionable. Operator actions have been typically included by forcing them at fixed times determined in the input data file or by interactively introducing them during the simulation.

Since operator actions are mostly proceduralized in nuclear power plants, they can be implemented by simulation tools able to follow operating procedures, at least for those analyses where the behavioral aspects are not the main concern. The current development status of a coupled plant-procedures simulation tool is presented in this paper.

2 Accident Sequence Simulation Approaches

Accidental sequences begin at normal operation, either at power or shutdown modes. At the first stages, specially when the sequence starts from power operation, the plant behavior is characterized by a high number of working systems and a global behavior dominated by the performance of the control systems. Physical processes are usually within their optimal design conditions and a number of assumptions and approximations can be done in the simulation models. The main simulation concern at these stages is to take into account all the interactions between involved systems and/or processes.

*CSN - Nuclear Safety Council
†DSE-UPM - Department of Energy Systems. Polytechnical University of Madrid.
When the accident is already in progress, the number of interacting systems and processes is significantly less, but the phenomenological complexity is usually much higher. New systems that were in standby or passive modes at normal operation come now into play and new interactions become important. The requirements for the simulations models are, in many aspects, very different from normal operation models. Some of the assumptions and approximations are no longer applicable but, in some cases, other simplifications could become feasible. The global plant behavior is mainly dominated by the phenomenology and the automatic and manual protective actions.

In order to cover all the stages of the accident sequence, the simulation models should meet one of the following requirements:

- They are detailed enough as to cover all the situations.
- Different models are used in each situation and smooth transfer mechanisms are guaranteed when switching from one model to the other.

The first solution requires very high computing power since the maximum model complexity is always used. The second one is much more convenient. It saves computing power and allows for the use of existing simplified models applicable to specific situations.

Operator actions play an important role in accident sequences. They are guided by emergency operating procedures (EOP) and severe accident guides (SAG), that can be considered as a part of the plant protection. The objectives of the EOP/SAGs and their design methodology are in many aspects parallel to those of the automatic protection systems. Operators are intensively trained in its use. This allows for the consideration of EOP/SAGs as the standard operator behavior during an accident. Operator errors would be deviations from this behavior.

The integration of operator actions in engineering simulators is not straightforward. They can be forced at given times through the input data file. They can also be executed interactively if the simulation code provides a suitable user interface. Finally, they can be automatically executed when the plant conditions ask for a given actuation.

The first method requires a high number of simulations since the actuation time depends on the dynamic process evolution. Provisional simulations must be run to determine the actuation time for each manual action. This is a tedious and time consuming task.

Interactive execution could be acceptable, depending on the objective of the analysis, although this mode of operation fits better in training (replica) simulators. The amount of simultaneously available information in engineering simulators is usually significatively less than in training simulators. On the other hand, manual actions in engineering simulators are usually much more easily issued although they might require several mouse operations. The main drawback of this method is the lack of repeatability.

Automatic execution provides the best performance for analysis oriented to plant behavior and procedure verification. This method requires a procedure-following system able to interact with the plant model. Standard execution times are assigned to each procedure instruction, assuming the procedure executed by an ideal operator.
An improved mode of interactive operation may consist of using a procedure-following system, as in the automatic execution, asking for operator confirmation before executing each instruction. If the system automatically selects the information related with the current instruction and issues the actuation orders upon operator acknowledgement, many non-essential window switching operations can be avoided.

3 Automatic Wide-range Simulation Applications

A simulation tool able to automatically compute accident sequences, combining simulation capabilities under normal and accident conditions and integration of operator actions can be applicable for a variety of purposes that include:

- Realistic simulation of level 1 PSA sequences.
- Supporting analysis for IPE and level 2 PSA studies.
- Design and verification of operating procedures, including Severe Accident Guides.
- Analysis of normal, abnormal and emergency scenarios in order to derive criteria for operator training or evaluation activities.

In addition, new analysis methodologies can be developed based on this kind of simulation instruments. A case of particular interest is the possibility of using a simulator driver able to generate tree-structured simulation sequences. This technique, when combined with suitable methods for fault tree quantification, allows for the application of risk-based methodologies for various purposes, including the evaluation of Emergency Procedures and Severe Accident Guides.

An example of such methodologies is the Integrated Safety Assessment, a systematic verification approach that can be considered as an extension of PSA and accident analysis techniques. It replaces the PSA static event tree with a generalized dynamic event tree concept based on the theory of probabilistic dynamics. The mathematical support of this methodology has been described in [6] and [7]. Both components of the risk, damage and probability are considered in this approach in a balanced and simultaneous way. The feasibility of the application of the ISA methodology to the validation and verification of the Emergency Operating Procedures of Nuclear Power Plants is described in [2].

4 Development of an Accident Sequence Simulation Package

A combined simulation system for accident sequences is being developed under a cooperative agreement between the CSN and the DSE-UPM. It consists of the combination of three elements:
• A plant transient simulation code (TIZONA[3]) developed by the DSE-UPM.

• A severe accident simulation code (MAAP[4]), widely used in the nuclear industry.

• A computerized procedure system (COPMA-II[5]) developed by the OECD-Halden Reactor Project and adapted for simulation at CSN.

4.1 The Plant Simulation

During pre-accident conditions, TIZONA takes the responsibility of the simulation. It has a complete representation of plant systems including electric equipment and detailed automatic control. Also, TIZONA sends to COPMA-II information about process variables, needed to follow applicable operating procedures. COPMA-II, in turn, sends to TIZONA the requests for operator actions derived from the procedures. Manual controls have been included in the plant model, able to receive the action requests from COPMA-II.

When the code detects that its models are near their applicability limits, most of the simulation work is transferred to MAAP. This will likely occur when the accident is already in progress. Some selected parts of the simulation, however, may still be performed in TIZONA, that will remain at work, exchanging information with MAAP. Also, TIZONA will continue sending process information (including that computed by MAAP) to COPMA-II and receiving from it operating instructions. Only TIZONA is connected to COPMA-II. Its simulation capability is complemented with the ability to act as intelligent interface, so that the joint system TIZONA-MAAP is seen as a single simulation package from COPMA-II.

TIZONA knows at every moment what parts of the simulations are being computed by each code. When a manual action request is received from COPMA-II, TIZONA addresses it to the right destination. The capability for manual operation is not limited in TIZONA. The user may build as many manual controls as desired. This is not the case for MAAP where the number and nature of available control signals cannot be modified by the user. Nevertheless, this set of control signals is rather complete and, if needed, TIZONA may help in improving the MAAP control capability.

4.2 The Procedure Simulation

COPMA-II is a procedure following system developed at the Halden Reactor Project. It has been designed as an operator support system guiding the execution of operating procedures. COPMA-II is connected to the plant process computer (or to a plant simulator) from which it receives the information needed for procedure execution. The system displays, among other things, the procedure instruction that should be executed next, along with the process information concerning this particular instruction. Under the control of the operator, it has the capability of sending to the process computer or to any other external process, orders for plant component manipulation.

Although not designed for procedure simulation, COPMA-II has two features that make it very close to a simulation system: the ability to receive process information
and to send manipulation orders to the outside. With no much effort, COPMA-II can be used as a true procedure simulation system. In its standard use, the interaction between the operator and COPMA-II is performed through a graphic interface. This interface is a computer process that runs independently of the COPMA-II kernel and that communicates with it. All the operator interventions are received by the kernel as function calls resulting in instruction execution, information generation, etc. If any other external process has the capability of automatically generate the same function calls that the operator would, COPMA-II could be used as an unattended simulator.

The user configuration of COPMA-II is done by editing two *lisp* source files known as *kernel-init* and *simdefs* respectively. The first one contains, among other things, the definition of the action instructions used in the procedures. The second one contains the specifications of an internal simulator where the information to be sent or received from the external simulator is declared and/or manipulated. These two files give to COPMA-II a high flexibility for user configuration.

Standard elementary actions were already present in the *kernel-init* file of the COPMA-II distribution, such as open/close, start/stop or auto-on/off. As part of the present development, other complex actions have been developed. For example, the instruction *control* activates a control mode that emulates the behavior of an operator trying to maintain the controlled variable between two values specified in the operating procedure. The user has the capability to modify the manual control strategy, implemented as a TIZONA function.

The internal COPMA-II simulator can be used as a pure interface containing only declarations of variables or as a complement of the external plant simulator. In our case, it is being configured in order to perform the following functions:

- To declare the variables that support the information exchange with the external simulator and the operations derived from action instructions.
- To define some logical flags representative of the state of the plant and/or selected systems. These flags are functions of the process variables received from TIZONA-MAAF and are checked by the operating procedures.
- To establish associative relationships between variables so that action instructions can identify the variables to be modified. For example, the manual control signal corresponding to the named plant component in the procedure can be determined in this way. These relationships are defined through the list of properties associated to each variable in *lisp* language.
- To define logical and computational relationships between variables so that incompatible variable values could be avoided. For example, if a system is in manual control mode because of a previous *control* instruction and the *auto-on* instruction (i.e., put the system in automatic control mode) is issued for that system, the manual mode is automatically deactivated.
COPMA-II is being used so far in interactive mode. This means that any action request to be sent to the plant simulator must be acknowledged by an operator sit in front of the terminal. However, completely automatic simulation is possible by developing an interface module. The tasks to be assigned to this module include:

- To assign to each operating instruction an execution time either deterministic or with some degree of randomness.
- To take care of the task load of the operation crew in order to avoid excessive number of simultaneous instructions.
- To scan all the open procedures issuing the execution order of a new instruction when execution times and task load allow for it.
- To synchronize the plant simulation and the procedure simulation so that the same time scale is used in both systems.

Future development will also include tree-structured sequence simulation.

5 Pilot Study

The new combined system is being applied to analyze station black-out sequences in a BWR plant, using the real plant operating procedures [8].

The plant model for TIZONA-MAAP has already been set up. It is being completed now with manual control inputs needed for procedure execution.

A complete collection of EOP corresponding to a BWR/6 plant has been edited in the COPMA-II format. The simdefs file linking the two models has been set up and the first simulation exercises have been performed.

The pilot study will be finished by the end of the year and new applications will be scheduled from then on.

References


