

E U R O S A F E T R I B U N E

#002
OCTOBER 2002

SAFETY

OF REACTOR LOW-POWER AND SHUTDOWN STATES

- Probabilistic Safety Assessments
- International Feedback from Experience
- Radiological Protection Aspects
- Organisational and Human Problems
- Effects of Economic Constraints

INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE (IRSN)
B.P.7
F-92262 FONTENAY-AUX-ROSES
CEDEX

GESELLSCHAFT FÜR ANLAGEN-
UND REAKTORSICHERHEIT (GRS) mbH,
SCHWERTNERGASSE 1
D-50667 KÖLN

FOR FURTHER INFORMATION:
www.eurosafe-forum.org

E U R O S A F E

GRS

IRSN



Daniel Quéniart and Lothar Hahn

We are pleased to introduce the second issue of the Eurosafe Tribune, a periodical devoted to nuclear safety and directed at a readership composed of the different parties involved in the nuclear safety debate: scientists, researchers, engineers, operators, managers, regulatory bodies, NGOs, opinion leaders and policy makers. The present issue is focused on the safety of nuclear reactors during low-power and shutdown states. This topic has been a major issue in the field of nuclear safety over the last decade. The results of the research on the shutdown topic are now going to be introduced in rules and guidelines like in the PSA guideline, KTA Safety Standards or in the definition of criteria for declaring a site area emergency. This leads in the short term to particular consideration of safety aspects related to shutdown operations and has in some countries already led to an in-depth investigation of low-power and shutdown states as part of the periodic safety review for operating NPPs. Other countries will introduce these investigations into the periodic safety review in the near future. The treatment of low-power and shutdown states is also a good example of the growing convergence of nuclear safety approaches. From the beginning of the investigations, close co-operation between the experts involved has occurred either in IAEA and OECD working groups or in other international working groups like COOPRA (Co-Operative Probabilistic Risk Assessment). As a result there have been synergy effects during the investigations and a convergence of safety approaches. Convergence of technical safety practices has been selected as the topic of the next Eurosafe Forum, to be held in Berlin on the 4th and 5th November 2002. We would be pleased to welcome a large number of experts in the field of nuclear safety at this meeting which is increasingly becoming a platform for the presentation and discussion of recent developments in nuclear safety in Europe. We wish you a pleasant and profitable read, and we would like to remind you that the Eurosafe Tribune, printed in English, is also available in German and French on the GRS¹ (www.grs.de), IRSN² (www.irsn.org) and Eurosafe (www.eurosafe-forum.org) web sites. ●

1 - Gesellschaft für Anlagen- und Reaktorsicherheit.
2 - Institut de radioprotection et de sûreté nucléaire.

CONTENTS

Probabilistic Safety Assessments p. 4

► **The risk associated with a nuclear reactor may be higher in shutdown conditions than in power operation**
By Jeanne-Marie Lanore and Dieter Müller-Ecker p.4

► **The German experience in the safety assessment of LP&S states**
By Wolfgang Renneberg p.6

International Feedback from Experience p. 8

► **Safety in shutdown states: lessons learned from operating experience**
By Jacques Verlaeken and Jose Balmisa p.8

► **In search of good practices**
By Tsonka Grosdéva p.12

Radiological Protection Aspects p. 16

► **Radiological protection, the need for a comprehensive policy**
By Jukka Laaksonen p.16

► **Final shutdown: taking time to plan the best**
By Carl-Göran Lindvall p.18

Organisational and Human Problems p. 20

► **Safety aspects of operational management during low-power and shutdown operation: the GKN experience**
By Eberhard Grauf p.20

► **Organisational issues: a regulator's view**
By Lajos Vöröss p.25

Effects of Economic Constraints p. 29

► **Increasing availability means increasing safety**
By Julio González p.29

THE RISK ASSOCIATED WITH A NUCLEAR REACTOR MAY BE HIGHER IN SHUTDOWN CONDITIONS THAN IN POWER OPERATION

By Jeanne-Marie Lanore, Probabilistic Safety Assessment Manager, Institut de radioprotection et de sûreté nucléaire (IRSN), and Dieter Müller-Ecker, Project Manager, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS)

■ The first probabilistic safety assessments (PSAs) performed on nuclear power plants (NPPs) considered only accident sequences which could occur when the NPP is operating at full power, with the implicit assumption that during shutdown the risk is much lower. Due to several incidents observed in NPPs during shutdown in many countries, the first PSAs carried out in France investigated the risk of core melt when the reactor is in a shutdown condition. The results indicated a significant contribution, even higher than during full power for particular plant configurations. Later on, these results were confirmed by all the similar studies carried out in other countries, including Germany. Major safety improvements have been implemented as a consequence of these results.



Jeanne-Marie Lanore, IRSN



Dieter Müller-Ecker, GRS

The objective of a PSA is the evaluation of the safety level and safety balance of a technical installation such as a NPP. This assessment is performed with the help of *probabilistic methods* and is based on an identification as full as possible of all the combinations, called accident sequences, of material and/or human failures which could lead to serious consequences. The quantitative assessment is based on elementary data related to the components of the technical installation provided by operating experience. In the case of a NPP, the first serious consequence considered is generally a meltdown of the core. The frequency of a core meltdown is an indication of the safety level – or the risk – of a NPP, and the importance

of the failed parts an indication of the safety balance of the safety system. This type of assessment has been performed in many countries for over than thirty years.

In France, two PWR PSAs were completed in 1990 by Electricité de France (EDF) and the Institute for Nuclear Protection and Safety (IPSN). The first of these studies (PSA 900) concerned a standard reactor of the 900 MWe series, and was carried out by IPSN. The second study (PSA 1300) was carried out by EDF for a unit representative of the 1300 MWe series.

➤ **PSA results.** An interesting finding of these PSAs was the significant contribution of shutdown operating conditions to core melt frequency (CMF) per reactor-

year which was of the same order of magnitude as for power operation (approx. 1/3 of the total CMF for PSA 900 and 1/2 for PSA 1300). These results indicate that *the core melt frequency by time unit is higher during shutdown than during full power.*

After these findings, investigations were started in Germany to examine the importance of accident sequences during shutdown for German PWRs. This investigation was performed by the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) on behalf of the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) and led to some improvements in German PWRs too. A major PSA including shutdown states for a modern Konvoi-plant was finished in 2000. The findings concerning accident sequences during shutdown states were similar to the insights from the PSAs in France.

The core melt frequency was in all studies particularly high for a loss of residual heat removal system during mid-loop operation because only a short time is available for the operator to take any action, due to the low primary coolant inventory. Other particular sequences initiated by a spurious

Daya Bay Nuclear Power Plant.



primary coolant boron dilution were also identified. A rapid boron dilution could lead to a reactivity accident with serious consequences.

These findings could be explained by several reasons. In particular, during shutdown, many pieces of equipment are unavailable for maintenance and several automated systems are ineffective. So in many accidental situations, operator intervention is necessary, in cases where alarms, indicators and operating procedures are poor or inexistent.

➤ **Plant modifications.** The resulting activities are somewhat different in France and in Germany, in accordance with the particular findings and the type of plant series in the two countries.

In France, the safety authority required EDF to propose plant modifications to reduce the frequency of the dominant sequences. These sequences were similar for 900 MWe, 1300 MWe and 1450 MWe series and led to modifications for all series. Immediately EDF proposed preliminary measures: level measurement, technical specifications leading to the most critical situations being avoided, training of operators. After a more complete safety re-assessment, definitive measures were proposed, especially alarms, automated systems and improved operating procedures to help the operators.

The safety authorities considered that the assessed core melt frequency was significantly reduced by these measures, which should be rapidly implemented in all the plants. Moreover, some new significant sequences were identified during the analysis, in particular those leading to cold overpressurization and consequently to a risk of reactor vessel rupture. In order to avoid this risk new design and operation modifications were decided upon. ➔

→ In Germany, the improvements were initially very plant specific. Essentially, a larger number of safety trains were made available during mid-loop operation (e.g. RHR-trains, accumulators) and, conversely, maintenance work was limited; the test-period of the level measurement was optimized and – most importantly – a symptom-oriented procedure to cope with accident sequences was developed and is part of the operator training. In the long term, the necessity of PSA for shutdown states is going to be introduced in the PSA-guidelines for the periodic safety review. Nevertheless, for some plants, a shutdown PSA is required by the *Länder* safety authorities.

> **Insights and perspectives.** The investigations have demonstrated that the original idea of negligible risk during shutdown because of a large grace time is not valid for all states. In addition to the findings related to plants safety, the PSAs have underlined that in many cases the knowledge of the plant behaviour during an accident sequence was insufficient. For example, in order to assess the physical consequences of the injection or forming of unborated water in the primary circuit, it was and still is necessary to perform neutronics and thermalhydraulics calculations, and even experiments. The consequences of a cold overpressure also require physical and mechanical studies for some plants. PSA for shutdown situations has so far led to significant safety improvements of the plants and also to a knowledge improvement about the plant's behaviour during particular accident situations for which studies are still ongoing. In particular in Germany a PSA for shutdown states of a BWR of the 69-type has been started. ■



By Wolfgang Renneberg Director-General Nuclear Safety, German Federal Ministry for the Environment

THE GERMAN EXPERIENCE IN THE SAFETY ASSESSMENT OF LP&S STATES

■ In compliance with the requirements of the German atomic law concerning precautions against the risks associated with the operation of nuclear power plants, the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) entrusted GRS with an ongoing assessment of low power and shutdown (LP&S) states. The investigations have shown that LP&S makes a significant contribution to the damage states of a nuclear power plant. These findings have already led to a number of plant-specific improvements and provide a technical basis for the preparation of guidelines. The work also involved an exchange of experiences with other NPP-operating countries (i.e. France, Switzerland and the US) where similar studies were carried out. Wolfgang Renneberg summarises the work performed.

One of the fundamental aims of the Federal Regulator at the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) is to minimise the risks resulting from the operation of nuclear power plants. To this end, the safety of nuclear power plants must be analysed far in advance – before any hazard can occur – so that corresponding countermeasures can be taken in time.

▼ Within the framework of projects commissioned by the BMU and other international nuclear safety research projects, it was found that event sequences outside power operation – or for example, during an outage low-power operation – can also be highly safety-relevant and that their contribution to the overall probability of incidental situations cannot be neglected. The results have already led to a number of improvement measures, especially with regard to procedures.

▼ Owing to these results and due to the different system states during

low-power and shutdown (LP&S) states, and the difference in the way initiating events are controlled compared to power operation states, the investigation methods were developed further.

▼ The aim of the work carried out by GRS for the BMU has been and still is the continuing assessment of event sequences in pressurised water reactor (PWR) plants under the boundary conditions of LP&S states, so that their safety significance can be determined and a technical basis can be provided for the preparation of guidelines. The adaptation of the methodology developed in this process to boiling water reactors (BWR) will be the object of further studies.

▼ Part of the work consists of an exchange of experiences with the French Institut de radioprotection et de sûreté nucléaire (IRSN), the Swiss Hauptabteilung für die Sicherheit der Kernanlagen (HSK) and the US Nuclear Regulatory Commission (NRC). This way, the latest international developments

are considered, and the German activities are put forward for discussion on an international platform.

▼ On behalf of the BMU, the German Reactor Safety Commission discussed the results and came to the conclusion that further systematic investigations concerning damage states during LP&S operation need to be carried out as these states may represent a high contribution to the overall frequency of damage states. In principle, precautions against the risks of LP&S states are mandatory under German atomic law.

▼ The International Atomic Energy Agency (IAEA) and the Organisation for Economic Cooperation and Development (OECD) have also promoted the international exchange of experience with the aim to further harmonisation. These and other international activities have shown that, on an international level, the safety-related assessment of LP&S states belongs in many cases within the scope of mandatory safety-related investigations. ●

SAFETY IN SHUTDOWN STATES: LESSONS LEARNED FROM OPERATING EXPERIENCE

By Jacques Verlaeken, Experience Feedback Coordinator, Association Vinçotte Nuclear (AVN), and Jose Balmisa, Nuclear Power Plant Project Manager, Consejo de Seguridad Nuclear (CSN)

■ Contrary to the general belief that being at power is the most risky situation, numerous examples provided by international operating experience show that shutdown states could generate severely problematic situations. The lessons learned from this experience suggest improvement opportunities in various areas such as safety principles, fire protection, instrumentation, procedures, training and contingency plans, limiting operation conditions and reactor design. Rather than further increasing safety system complexity, such improvements may rely upon better planning and contingency plans, dependable instrumentation and a specific “shutdown state safety culture” shared by all players.

Why be concerned about shutdown states? The focus of formal safety assessment of NPPs is a selection of representative incidents and accidents, analyzed under conservative assumptions, in order to justify design features like automatic safety systems. One criterion is that operators must have at least a 10 minute (after the recognition of an incident/accident) “grace period” before any manual control. Within this period of time, all modifications of plant status – if needed – must be automatic. This philosophy explains why several plant states during shutdown are not formally assessed, based on the much lower dynamics: no nuclear power, only decay heat. Operational experience and the development of probabilistic safety assessment (PSA) have, however, highlighted that those shutdown states could be a significant con-



Jacques Verlaeken, AVN

tributor to the core damage frequency, and thus to the overall risk.

■ Shortly after shutdown, the high decay heat load significantly reduces the time available for shutdown cooling recovery before boiling or core uncover, especially when the water inventory is at its lowest (e.g. in PWR during the so-called mid-loop operation, which means that the reactor coolant level is reduced – in order to permit some maintenance – below the top of the primary piping).

■ During shutdown and refuelling outages, activities may increase fire hazards in safety-related systems.

■ Stress on personnel and programs has been identified as a significant contributor to errors made during shutdown activities.

■ Limiting conditions for operation (LCO)¹ for residual heat removal systems, emergency

core cooling systems and containment systems may not be detailed enough to address the number and risk significance of configurations used.

■ Wide variations exist in installed instrumentation.

The most significant events for PWRs are the loss of shutdown cooling², potential pressurization and boron dilution events. Loss of cooling shortly after plant shutdown may quickly lead to bulk boiling and eventual fuel uncover if cooling is not restored. In mid-loop situations, the increase of pressure in the void space may expel the water inventory if the temporary closure³ design pressure is exceeded, so that the cooling degradation is much faster. For BWRs, the more significant events are loss of coolant, loss of cooling and potential pressurization.

► **One example of a significant event: loss of shutdown cooling.** On 26 March 1986, after an 11-day outage period, the shutdown cooling system (SC) of the San Onofre 2 unit experienced a total loss of flow for a period of 49 minutes, resulting in local boiling. This occurred while the reactor coolant system (RCS) level was being reduced to repair a leaking cold leg steam generator nozzle dam which had been installed to allow work on steam generator channel heads. Using the normal indication level, which was later found to be in error⁴, the RCS was drained to a level when whirling of the primary coolant occurred (vortex) at the suction connection, eventually causing the SC pumps to become air-bound. The direct cause was erroneous level indication, resulting in the operators not recognising the RCS low-level condition and not understanding the pump problem prior to complete loss of SC flow.

“ The greatest challenge comes from the possibility of simultaneous unavailability of equipment causing the loss of a given safety function. ”

► **A second example of a significant event: loss of all AC power.** On 20 March 1990, Vogtle 1 unit experienced a loss of all safety (vital) AC power. The plant was in cold shutdown with reactor coolant level lowered to “mid-loop” for various maintenance tasks. Both the containment building personnel hatch and equipment hatch were open. One emergency diesel generator (EDG) and one auxiliary transformer were out of service for maintenance. A truck in the low-voltage switchyard backed into the support column for an offsite power feed to the auxiliary transformer which was supplying safety power. The insulator broke, a phase-to-ground fault occurred, and the feeder breakers for the safety buses opened. The only operable EDG started automatically because of the under-voltage condition on the safety bus, but tripped after about 1 minute. The EDG could only be restarted 36 minutes after the loss of power. During the 36 minutes following the loss of safety bus power, the reactor coolant system temperature rose from about 32°C to 58°C.

► **Shutdown states: a challenging period for operators.** The greatest challenge comes from the possibility of simultaneous unavailability of equipment causing the loss of a given safety function. During an outage, the role of the operations staff changes considerably when compared with full power operation. The operating circumstances are more demanding, the work more intensive, and shift turnovers more difficult. Reduced coolant inventory operations were identified as presenting the greatest challenge to the operator. Noted as difficult were maintaining awareness of plant status, keeping track of unavailable →

→ equipment and avoiding loss of information during shift turnovers.

There are few studies to calculate the risk associated with shutdown and refuelling conditions in BWRs. These preliminary studies show the importance of human error in many sequences and significant initiating events such as the loss of instrument air. The more severe events occur in plant operation stages from cold shutdown to refuelling with water raised to the steam lines. Most of the problems in BWRs come from complex system configurations⁵.

> Influencing factors in a sample of major events.

One difficulty in attempting any statistical or trend analysis is the need to be selective among the thousands of insignificant events. One approach is to limit the analysis to a very small number of major events, considering that they are the best candidates for any search for improvements. Besides engineering judgement by safety experts, analytical tools are available to provide some quantitative perspective (PSA based Event Analysis): an event where *conditional core damage probability* is of the order of $10E(-4)$ or more is certainly safety significant. For example, the *conditional core damage probability* for Vogtle was of the order of $10E(-3)$.

Such a study of 13 major events in the period 1981-90 found that nine were caused by personnel mistakes (operators or vendor/contractor). A mistake is an error type where the intention is erroneous:

- after a faulty diagnosis (3 cases);
- using an inadequate procedure (6 cases, see discussion below);
- after a miscommunication (1 case);
- due to inadequate planning (1 case)⁶.

The events were often described as errors by control room operators during perfor-

mance of some task associated with reactor coolant level and inventory control, the resulting safety challenge being:

- a loss of reactor coolant inventory (3);
 - a loss of electrical power (2);
 - a loss of shutdown cooling (for 10 cases).
- When there are no automatic controls, the quality of procedures is certainly important. When further analysing the 6 cases just mentioned, one finds that:
- the procedure was not used, because it was too difficult to use (1);
 - the procedure was followed incorrectly, because of inadequate details (2);
 - the situation was not covered by a procedure (2) or by one inconvenient to use (1).

> **Conclusion.** Shutdown states cover a variety of conditions where, contrary to the usual belief that being at power is the most risky situation, some critical situations can present a high risk. The mastering of those risks can be achieved by better planning and contingency plans and by dependable instrumentation rather than by further increasing safety system complexity. There must also be a specific “shutdown state safety culture” shared by all players. ■

1- Called Technical Specifications in the US, Belgium, etc.

2- Also called residual heat removal.

3- Often installed to permit inspection inside the steam generators.

4- The operators did not trust the newly installed remote indications (which were wrong because of a loop seal), and relied on a simple visible tube level, which was indicating too much because of an air bubble.

5- In some BWR with multi-mode RHR systems that perform the shutdown cooling function as well as a variety of ECCS and containment cooling functions.

6- The total is 11 because two events involved two distinct mistakes.

Fuel assembly transfer from storage pool towards reactor pool.



Possible improvements

It is beyond the scope of this article to identify what actions have been taken where. We therefore offer an overall view of the trends.

Safety principles highlighted in the outage programmes

Good safety principles are, for example, to:

- minimize time at reduced inventory;
- maximize pathways for adding water to the reactor coolant system;
- maximize availability of important support systems;
- minimize activities requiring mid-loop operation;
- maximize time with no fuel in the reactor vessel.

Fire protection

Increased presence of combustibles (e.g., lubricating oils, cleaning solvents, paints, wood, plastics) and ignition sources (e.g., welding, cutting and grinding operations, and electrical hazards associated with temporary power) present additional fire risks to those plant systems maintaining shutdown cooling. Administrative controls may need to be strengthened to improve fire prevention and protection.

Instrumentation

Too often, instrumentation quality is governed by accident design basis needs. It should be recognized that low-power and shutdown (LP&S) conditions also require high quality (dependable) instrumentation for core temperature, water coolant inventory (including refuelling cavity), coolant pressure and shutdown cooling monitoring. The indicators and alarms should be kept meaningful, for example by the intelligent suppression of non significant alarms.

Procedures, training and contingency plans

We have seen that there is a pattern of procedures providing inadequate guidance or not covering actual situations. But, procedures and training were also effective in ensuring adequate recovery¹. The paradox is that some procedures score negative (could create the event) but other procedures score positive (they allow recovery). Additional support (from technical support centres for example) should remain available at all time to cover situations where existing procedures are obviously not applicable: here we enter the realm of severe accident management. The applicability of existing severe accident management guidance to shutdown states is still to be verified.

Limiting conditions for operation (LCOs)

Many of the existing LCOs were written with a focus on power operation. The need to maintain redundant decay heat paths for such sensitive conditions as mid-loop and reduced inventory, and containment integrity has been recognized. Recirculation² capability must not be forgotten.

Design improvements

Some initiatives have been taken to increase the coverage of automatic systems, for example a system to avoid a critical accident due to the sudden introduction of a slug of pure water. The automatic actuation of engineered safety features must, however, be balanced against traditional risk to local personnel.

1- There was no core damage, even when coolant boiling started.

2- Process where the safety injection water is recirculated into the core from within the containment after a LOCA.

IN SEARCH OF GOOD PRACTICES

■ With a view to producing a complete set of good safety practices during planned outages at nuclear power plants in Europe, the European Commission decided, on the advice of an expert group - the Nuclear Regulator's Working Group (NRWG), to inventory the current safety practices applied in the different reactor technologies – PWR, BWR, VVER – operated throughout the continent. Thus it intended to contribute to aligning safety practices to a certain level and to promote experience sharing among operators from current member states and applicant countries.

In 1999 the European Commission¹ issued a call for tenders pertaining to a Study on European Nuclear Safety during Planned Outages at Nuclear Power Plants and provided both the budget and the procedures applicable to the tender. A consortium composed of four companies – Belgatom (Belgium), EDF (France), Fortum (Finland) and Paks NPP (Hungary) – under EDF's leadership, was selected by the EC to perform the study. The work was organised in three phases: first, collecting data on current practices; second, analysing questionnaire answers and drawing up good safety practices, references and recommendations; and third, collecting relevant ideas related to future reactors at design stage, such as the European Pressurised Water Reactor (EPR).

Drafting the questionnaire and enhancing comprehension

▼ It is worth noting that the study, recommended by experts from safety authorities, was performed by utilities and engineering firms. One of the key points of this survey was the elaboration of a specific questionnaire as an appropriate methodological tool for the participation of different nuclear operators in Europe. The selection and wording of questions was one

NPPS WHO ANSWERED THE QUESTIONNAIRE

Blayais – France (4 PWRs)
Bohunice – Slovakia (4 VVERs)
Borssele – Netherlands (1 PWR)
Bugey – France (4 PWRs)
Cofrentes – Spain (1 BWR)
Doel – Belgium (4 PWRs)

Krsko – Slovenia (1 PWR)
Loviisa – Finland (2 VVERs)
Olkiluoto – Finland (2 BWRs)
Paks – Hungary (4 VVERs)
Ringhals – Sweden (3 PWRs)
Tihange – Belgium (3 PWRs)



of the most important tasks that we performed with the goal of maximising the chances of collecting detailed answers and gathering relevant data. The methodology we used during this phase was the following:

- Brainstorming with experts involved in nuclear safety and plant operation, in particular plant shutdown project leaders, was organised: participants were asked to define the list of subjects deemed to be the most relevant to safety during outage;
- based on this, we elaborated a questionnaire structure and submitted it to the members of the consortium working team for validation;
- then, a total of 221 questions, including background explanations; covering the different subjects, were drafted; proofreading of the questionnaire by Paks NPP operators enabled us to verify that the questions were appropriate for VVER-type reactors and to introduce some additional questions.
- ▼ Specific care was also taken by the consortium working team to

enhance understanding of the questions: we drew up a glossary, focussed on plant shutdown, with the definition of key words; we checked its consistency with the “nuclear safety glossary” published by the IAEA. All the key words included in our glossary were highlighted in the questionnaire. In order to provide reliable data, we suggested that each plant set up a working team in charge of filling in the questionnaire and nominate a “local” project leader; also an e-mail “hot-line” was established to answer any further questions in case of need. We even formatted an answering form to facilitate the recipients’ work. Each plant was required to highlight the practices they considered as belonging to the “good practices” and to make sure that those practices, far from being declarations of intent, were actually implemented in-situ. (A good practice is a locally certified and approved procedure, in the technical or organisational areas, to face up to the difficulties met in normal working practices, and which experience shows to really solve the problem, and improve overall working quality.)

▼ We also searched in bibliographical records for the possible existence of a past survey in collecting good practices concerning plant shutdown phases, but none was found. A specific questionnaire, aiming at understanding the present status of nuclear safety and design features related to outage ●●●

By Tsonka Grosdévá, Senior Project Manager, Nuclear Generation Division, EDF Industry Branch

●●● conditions was also established for answering by future nuclear designers.

Collecting and analysing answers

▼ Introduced by a cover letter from the European Commission, our questionnaire was sent to several operators throughout the continent, using the personal network of each member of the consortium. Answers came back from 12 operating utilities representing PWR, BWR and VVER technology in 9 European countries (see Table).

▼ The analysis of answers was divided by chapters among the members of the consortium working team. For each specific subject or question, what appeared to be a common practice on one hand or an original feature on the other was derived from the collected answers. Plenary sessions of the consortium working team were then organised to discuss all the subjects and to consolidate the results of the analysis phase.

▼ Conclusions were drawn under six headers: organisational survey and generalities; organisational effectiveness; quality of maintenance; quality of operation; engineering support and management of modification; specific aspects. The conclusions related to each analysed subject include four items:

- background questions with a summary and the aim of the questions;
- the current status, describing common practices and good specific

practices, as derived from answers to the questionnaire;

- the identified good practices;
- recommendations that are a subset of the common good practices worth promoting, according to the expert judgement provided by the consortium working team.

The final report was submitted to the European Commission for validation by the end of December 2001 and published as an EC document in March 2002.

Lessons learnt

▼ This survey showed a greater convergence of safety approaches and practices than expected. It also showed that a consensus on the prioritisation of the criteria could emerge easily among operators: for instance, project type management reveals the most widely used way of managing plant shutdowns; risks linked to fire and flooding are also approached in a very similar way; the Alara² concept and associated good practices are of common understanding; all operators use maintenance programmes based on predictive maintenance. In the chapter devoted to probabilistic safety assessment (PSA), we emphasised the importance of defining a specific policy for the implementation of PSA on each site. And, as a last example, the operating technical specifications are commonly regarded as a guarantee of safety evidence.

▼ The implementation of the good practices and recommendations

MILESTONES OF THE SURVEY

- April 2000:** Kick-off meeting
- September 2000:** Draft of the questionnaire completed
- October 2000:** End of the validation step
- November 2000:** Final version of the questionnaire
- December 2000:** Answering the questionnaire
- March 2001:** Summary document
- May 2001:** Draft on current status descriptions
- July 2001:** Report with current status and set of good practices
- December 2001:** Draft of final report
- March 2002:** Issue of the final report as EUR document

provided in the survey report should result from the decision to be made by each operator and not from a systematic standard approach: a “good practice” is not equivalent to a standard since it is meant to provide a specific problem with the appropriate solution rather than handling all problems in the same way.

Feedback for future reactor design

▼ The Study on European Nuclear Safety during Planned Outages at Nuclear Power Plants was also an opportunity to provide knowledge from future reactor design projects: how plant safety and the maintenance activities during planned outages are considered at the design stage of the projects. With this in mind, we asked the team in charge of designing the European Pressurised Water Reactor (EPR) to provide us with the chapter headers pertaining to the safety of planned outages of this future reactor. We compared the suggested breakdown with the ones performed by several designers of future reactors: European Utilities Requirements Project, European Passive Plant Project, Utility Requirements Project (US Electric Power Research Institute), Westinghouse (AP 600, AP 1000 and EP 1000 passive design projects). A specific chapter of the report provides this knowledge concerning the next generations of reactor. ●

1- The project was launched by the then Directorate General XI – Environment, Nuclear Safety and Civil Protection- now only DG Environment – and completed within DG for Energy and Transport.

2- Alara: As Low As Reasonably Achievable.

WORK TEAM MEMBERS FOR THE STUDY



The survey was monitored by José A. Gomez who represented the European Commission. Deeply involved in the project, he participated in all the technical sessions, received all intermediate versions of the study and provided useful remarks for integration into the draft. This close relationship between the owner of the study and the consortium enabled resulting quality through an iterative process.

Top, from left to right :
José Gomez, EC (Belgium),
Jozef Elter, packs NPP (Hungary)
Sylvain Deriot, EDF (France).

Middle, from left to right :
Luc Van Assche, Belgatom ((Belgium)
Tsonka Grosdéva, EDF (France).

Bottom, from left to right :
Jarmo Korhonen, Fortum (Finland),
Christian Breesch, Electrabel (Belgium),
and lower down :
Jean-Pierre Schweitz, EDF (France).

Not pictured :
Anne d'Eer, Belgatom (Belgium),
Kalle Jänkälä, Fortum (Finland),
Jean-Michel Laverdure, EDF (France),
Ilkka Paavola, Fortum (Finland),
Dominique Vasseur, EDF (France).

RADIOLOGICAL PROTECTION, THE NEED FOR A COMPREHENSIVE POLICY

By Jukka Laaksonen, Director General of
the Radiation and Nuclear Safety Authority
of Finland (STUK)

■ Historically, Finnish reactors are reputed for their availability and quality of management. Among other operations, outages are performed so as to enable outstanding work efficiency and safety, in particular in terms of radiological exposure. Placed under the supervision of the Radiation and Nuclear Safety Authority of Finland (STUK), utilities plan and execute work with a view to keeping the collective dose below a threshold estimated prior to planning the operations. In the radiological protection area too, Finland is used to performing remarkably well with a 1 to 2 manSv collective dose in most years throughout the operating life, and in some years even a 0.5 manSv dose for its two unit stations. It is noticeable though that the progress accomplished by European and American utilities over the years brought them roughly to the same level. The most significant measures aimed at minimising radiological exposure at Finnish utilities are reviewed below.



Jukka Laaksonen, STUK

Adopt exposure-driven planning and work coordination. With this purpose, all tasks related to refuelling and plant modification are planned in specific meetings held with radiological protection experts at early stages in order to identify radioactive hazards. The plants are then required to prepare a specific radiological protection plan and submit it for the approval of STUK. This plan provides procedural features in compliance with administrative requirements as well as special arrangements for work associated with specific hazards. The collective dose is estimated in advance and the work is planned accordingly.

➤ **Efficient exposure control equipment.** Careful planning at the early stages is balanced by the thorough control necessary to establish that nobody is exposed over the limit during shutdown opera-

tions. In this respect, the most important measurement device used by Finnish utilities is an individual electronic dosimeter which will alarm at a dose rate of 2 mSv/h and also if a 2 mSv dose is reached within one day. Prior to entering a controlled area, each individual worker is provided with such a dosimeter, which is collected upon clearance of the area, providing real-time follow-up of exposure. A complementary control device is the thermoluminescent dosimeter, which enables the total dose received by an operator over the entire outage to be recorded. Unlike most European countries, where each operator is supposed to record and keep track of its own workers' doses, Finland has established a national register of all workers involved in nuclear operations, where the official doses per person are stored for the entire country.

➤ **Measures to limit contamination in the facility.** From the radiological point of view, a major issue is the monitoring of the iodine content of the primary coolant after reactor shutdown. Operators are not permitted to open the reactor pressure vessel until the iodine concentration is reduced below a certain limit (105 kBq/m³ for I₁₃₁) by circulating water through filters. Another issue is the strict control of all kind of radioactive leaks inside the plant, to keep the plant as clean as is achievable. In this respect, the cleanliness of Finnish NPPs should be acknowledged.

➤ **Monitoring of the plant spaces.** This aspect is of utmost importance in planning work efficiently. A computer data file, available for each room of the facility, should enable the radiological protection experts to check and update the contamination level of the rooms involved in the operations at the beginning of each outage. Besides improving work planning, these data files provide on-going, real-time information on the radiological status of the rooms.

➤ **Monitoring of individual exposure to radionuclides.** In addition to checking the contamination level of the premises and clothing and skin contamination of persons at each exit, Finnish regulatory authorities require each individual to be monitored before starting and after finishing work, with the purpose of ensuring that nobody collects radioactive contaminants within the body. The plant's management is supposed to perform a fast 100% monitoring which is double-checked by the STUK in about 30 to 100 cases. This accurate,

20-minute/person whole-body counting confirmed work practices to be good enough to keep contamination within negligible levels.

➤ **Special training and work permits.** Besides operational planning and exposure control, radiological protection in nuclear facilities relies upon the preparedness of those entrusted with outage operations. With this aim, a four-hour training session on safety practices is organised by the NPP's owner for any person expected to work on the plant. The session's contents provide general knowledge about radiation protection. A worker who goes through the training and passes a subsequent written examination at one facility is given a certificate accepted at all Swedish and Finnish facilities. This fairly inexpensive training has to be repeated every three years. Additional job-specific training is provided to each team of workers who are going to do a job that involves the risk of a significant dose. Furthermore, a special license – called a radiological work permit – is required for any work to be conducted in controlled areas. Attachments to this work permit provide information and guidelines about such matters as special clothing, or whether a radiological protection expert is needed to escort the worker or not. This has proved an efficient way to make sure that people are correctly instructed for each particular assignment. ■



For more information about the scope of Stuk's activities, see: www.stuk.fi

FINAL SHUTDOWN: TAKING TIME TO PLAN THE BEST

■ Located on the Kattegat straight in the Swedish province of Scania, the Barsebäck NPP has two BWR-units with a capacity of 615 MW each. The reactors were commissioned in 1975 and 1977. Barsebäck 1 was closed in 1999 (on 30 November) due to a political decision made in 1998. Still in operation, Barsebäck 2 produces 3.5 to 4.5 TWh per year, which covers approximately 30 percent of the electricity consumption in the southernmost part of Sweden, which has around one million inhabitants. At Barsebäck 1, the fuel was removed but it has been decided not to perform any dismantling work for the moment. After the closure of the unit, Barsebäck Kraft AB and Ringhals AB were merged, the reactors' ownership being split among the two major Swedish utilities, i.e. Vattenfall AB (75%) and Sydkraft AB (25%). Barsebäck 2 could only be closed in 2003 if the equivalent amount of energy can be saved or if it can be replaced by energy sources which do not contribute to the greenhouse effect. This decision is likely to give the operator some time to plan the closure of this second unit.

Plan things long in advance

▼ The case of Barsebäck 1 is particular, for the reactor was closed for dismantling and not shut down temporarily for maintenance and refuelling. In this context, tasks are planned in a completely different way, since there is no time pressure for restart. The work can be entirely focussed on minimising the radiological exposure and costs linked to dismantling.

▼ As the operator, the key issues for us are to know things like what activity is present in the station, what the records tell, and to have interim storage for the spent fuel as well as for the medium- and low-level waste removed from the reactor.

If such a facility is planned from the beginning, when reactors are constructed, storage costs can be decreased substantially. If it is not available when phase-out is decided, it becomes a major hindrance to closing down the reactor. In the case of Barsebäck 1, the fuel elements removed from the reactor could be sent to the Clab, an interim storage facility located near Oskarshamn NPP. The decisions on final storage will be made in the next few years, since such a facility requires 15 years to be built. Another key issue is decontamination: like interim storage, it proves cost-effective to invest in a large decontamination facility.

The third key issue is having a legal framework to refer to for decommissioning. In many countries today, the regulatory authorities don't have the legal framework required by operators for plant decommissioning and site remediation in place.

Take advantage of experience and discussion

▼ Our experience shows that it makes sense not to rush away and have to do things twice, but plan the whole phase carefully before starting work. From 1999 onwards, we therefore decided to travel around the world to survey reactor decommissioning experiences and find out what proved successful and what went wrong. This benchmarking phase provided us with valuable experience feed-back and increased our awareness on several points such as documentation (how to keep it operational after 15 years, for example), the calculation of the activity level to be anticipated, the sourcing (is it better to perform decommissioning and dismantling work using in-house personnel, to subcontract the work, or to set up mixed teams?) We decided to take our time to consider the issues...

▼ With the local authority we also spent time discussing matters that concern the public around the Barsebäck plant. Fire is one of them. Even after the fuel is removed from a power station, an alert system for the public has to be maintained as long as waste – resins for ion exchange for example – are stored on-site and could be

released by a fire, even an ordinary fire with no nuclear accident affecting the public. We also discussed how to define the moment when the station becomes a normal industry for the public: does it start when the fuel is removed? Or is it when the site has reverted to greenfield?



CLAB interim storage facility at Oskarshamn, Sweden.

Take account of future uses when planning decontamination

▼ The closure of a nuclear power reactor does not mean that the plant cannot be used for other purposes, research and development for instance. These possibilities have to be considered carefully, since they impact the decontamination planning. If one considers using the power station for R&D purposes, the dismantling, decontamination and removal of equipment then have to be performed early. This makes the availability of accurate records on activity levels in the different rooms, on activation products, etc. even more stringent. Where no future use is contemplated, the right option might be to wait several years before removing the equipment, which will thus necessitate less decontamination. Moreover, the decontamination method can be selected regardless of the necessity to restart.

Focus on quality and knowledge management

▼ Final closure of a reactor is an irreplaceable opportunity to plan work much better than in temporary outage situations, to plan the best in terms of schedule, choice of materials, methods, etc. The absence of time pressure should therefore be systematically taken advantage of in trying to reach optimum quality. The impact on every aspect should be considered: for instance, different materials might be selected for temporary or permanent shielding.

Every aspect should be documented *from the beginning* so as to build a comprehensive quality system: the cutting of a pipe, for example, must be traceable many years later, when dismantling begins. At Barsebäck, we have a dedicated person for recording modifications and we developed high quality systems for keeping records.

▼ One should be aware that the management of knowledge is crucial for safe and cost-effective decommissioning and dismantling. In this respect, it is worth noting that the situation is different if a stand-alone reactor is closed or if one unit gets closed while the other is continues to be operated. In the former case, most of the personnel leave the site and knowledge decays early; in the latter, knowledge can be kept on-site over the long run. Two different knowledge and skills management strategies have to be developed accordingly. ●

SAFETY ASPECTS OF OPERATIONAL MANAGEMENT DURING LOW-POWER AND SHUTDOWN OPERATION: THE GKN EXPERIENCE

By Eberhard Grauf, plant manager GKN II

■ Since the beginning of the 90s, the nuclear industry has come to see that plant standstills do not per se pose a lesser risk than “normal” power operation. This insight established itself more and more with the growing number of research results that became available – especially from so-called “shutdown PSAs” – as well as on the basis of operating experience world-wide.



Eberhard Grauf, GKN II

The results of the shutdown PSAs that have been performed in various countries are largely identical as concerns their general conclusions and can be summarised in a few words as follows:

- Any increased risks during low-power and shutdown (LP&S) states mainly result from
- the reduced availability of systems;
 - the comparatively small amount of coolant during certain phases;
 - the lack of automatic measures to control abnormal events;
 - the considerably increased difficulty – compared with power operation – of monitoring and keeping track of plant states;
 - the fact that many maintenance and inspection activities take place at the same time.

Practically all shutdown PSAs have shown that if one looks at the analysis of the actual plant condition, the shutdown risk always lies within the same order of magnitude as that of power operation and often even clearly exceeds the latter. In most cases, technical and/or administrative improvements were required to

achieve a balance between the risks resulting from power operation and LP&S states.

➤ **Low-power and shutdown states: a special challenge to plant organisation.**

A plant shutdown state – which usually comes a round every year for the purpose of refuelling and carrying out maintenance measures in the nuclear power plant – in many ways represents a special challenge to the operator. Around 3,000 individual tasks have to be carried out in a relatively short time. These tasks have to be supervised to guarantee that they are properly executed; the interfaces with ongoing plant operation and other activities have to be co-ordinated, and it has to be ensured that the conditions that are necessary for the safe overall condition of the plant are maintained over the entire period. To make things even more difficult, important information sources to check the plant’s condition are much less effective than during undisturbed “straight” operation – for example, the incoming signals in the control room are much more difficult to

interpret due to the fact that there are many more of them than under normal operating conditions. Such circumstances are mirrored in typical refuelling and maintenance outage events such as:

- violation of safety specification requirements;
- overlooking of important signals with the consequence of system failures;
- system failures due to (mostly inspection-related) inadvertent triggering of protection signals;
- inadvertent isolation of systems or components, with the corresponding consequences, such as the release of media, component damage or personal injury.

The most obvious example is the clearly increased occurrence probability of off-site power losses during low-power and shutdown states.

➤ **Implementation of safety-relevant outage requirements.**

In the face of the outage-specific risks it has proved expedient to take them into account by implementing corresponding measures.

At GKN, these measures are as follows:

- highly detailed outage planning;
- strict allocation of individual maintenance measures to specific redundancies, also during the outage;
- bans on certain kinds of work and inspections in selected areas during mid-loop operation;
- modification of shift team organisation to monitor the plant;
- minimisation of the maintenance scope by the introduction of preventive maintenance during power operation;
- performance of enveloping functional tests prior to the re-start of the plant.

The safety-related aspects of these measures are explained in more detail below.

➤ **Outage planning.** Measures for the detailed planning of an outage were introduced at GKN as early as the mid-80s. Originally, the main motivation was to reduce the number of necessary system isolations by better co-ordination of the maintenance activities, especially by the synchronisation of electrical and mechanical work. Apart from the fact that unnecessary work for the shift personnel is eliminated, this also has a positive safety-related effect, since there is a linear reduction in the probability of inadvertent system isolations as a result of the reduction in the number of isolation processes. Over around 10 years, outage planning continued to be optimised. Today, each individual activity is planned in advance, taking interdependence and temporal sequences into account. During complex phases, e.g. start-up and shutdown, when in a particularly large number of inspection activities have to be tied into the operational processes, the timing of the different activities is even done in minutes. Consequently, detailed preplanning relieves the duty shift supervisor of the otherwise necessary assessment of each inspection activity for compatibility with the plant state and ongoing parallel work. The very fact that preplanning takes many days – even months – shows the enormous effort this important activity represents to avoid disturbances and comply with the operating conditions. It inevitably ensues from this approach that the planning defaults must also be adhered to consistently and that any adjustments that become necessary because of unforeseen events may only be carried out following consultation with the planners.

Besides the safety-related advantages, the above-mentioned measures have also ➔



→ resulted in a considerable shortening of outage times at GKN II. Unfortunately, many people only perceive this aspect of time-saving and – without taking a closer look – conclude that outage shortenings are primarily a cost reduction measure with an associated lowering of the safety level. It must be pointed out in this context that despite comparatively short outages there have been none of the typical “outage events” at GKN II during the last few years. After all, the duration of an outage is not an indication of the safety-related quality of outage management. For such an assessment an evaluation of other indicators and of the boundary conditions which have led to the respective results is necessary.

There is one major prerequisite in perfecting outage planning: detailed knowledge of the work to be done. Unfortunately, this requirement is difficult to realise in practice. For example, those involved (own technical departments, external experts and authorities) often show little understanding of why they should commit themselves to a specific work schedule several months in advance, arguing that there is “still enough time to think about it a week before the actual outage”. To overcome this mentality among all those involved is one of the key factors in a carefully planned, safe outage. Although there will always be unforeseen – and therefore unplanned – work to do, the number of modifications should not exceed 5%, so that sufficient planning reliability is ensured. At GKN II, this proportion is currently around 1% in the area of the safety systems: clearly far less owing to the low rate of events.

Planning an outage has turned into a full-time job at GKN II. Throughout the entire year, a full-time outage planner deals with

“ There is one major prerequisite in perfecting outage planning: detailed knowledge of the work to be done. ”

the long-term planning, the timely drafting and compilation of the quantity structure, and the general co-ordination of an outage. The aim is to have identified the activities with critical deadlines nine months in advance. The complete quantity structure should be available no later than four months prior to the start of the outage, and all planning activities including the planning of system and component isolations should be finalised one month prior to the start of the outage at the latest. Detailed planning, which further below will be described takes about three months and is done by the staff of the “outage shift”. This means that the planning as well as the co-ordination of the outage lies in the hands of the same staff members.

› **Safety-train-related maintenance.**

For better clarity, work at GKN is always strictly limited to specially chosen redundancies, during power operation as well as during an outage. Safety systems that need to be operational so that minimum availabilities are ensured are separated not only administratively but also physically (locking of rooms). This procedure makes it much easier for the shift on duty to control the plant and also minimises the risk that safety-relevant systems may be impaired by maintenance activities. The above-mentioned “major-safety-train concept” ensures that maintenance activities are largely concentrated on one safety train.

› **Ban on work during mid-loop operation.**

One of the major findings of the shutdown PSAs was the sensitive behaviour of pressurised water reactors during mid-loop operation. GKN therefore minimised the risk of inadvertent actuations or operator errors that could lead to the fail-

ure of residual-heat removal or to coolant losses by banning all activities and inspections carrying such a risk during the course of mid-loop operation.

› **Modification of shift personnel responsibilities.**

During normal operation, the shift personnel on duty are responsible for monitoring the plant’s condition, coordinating/approving the ongoing work and carrying out operational in-service inspections. It has proved to be of advantage to divide these functions during an outage. Here it is important that the resulting interfaces are clearly defined and that the responsibilities for safe plant operation continue to be ensured. This is achieved by the following division of labour and provisions:

- monitoring of the plant with regard to its compliance with safety-related requirements and the surveillance of all operating systems is the responsibility of the shift supervisor on duty;
- the handling and co-ordination of all systems isolated for maintenance is carried out by a special “outage shift team” working in parallel;
- the large number of function tests is managed and co-ordinated by a special function test team.

A system is passed over by the shift personnel on duty to the outage personnel by releasing it for removal from plant operation (“release for isolation”). Later, the operable system is returned for plant operation by the “release for operation”, which is also documented. As in the case of the release for isolation, each operating systems function test also has to be permitted by the shift supervisor on duty.

With this division of labour, the shift personnel – now largely relieved of the outage

activities – can focus on ensuring plant safety. Since many systems are out of operation during an outage, the number of shift personnel on duty can be reduced.

The outage shift team prepares all isolation and overall coordination plans over a period of several months. The advantage of this system is that the outage shift personnel have detailed knowledge of all planning aspects. It would not be possible to impart such a high level of background knowledge to a normal duty shift. The latter therefore strictly stick to the procedures specified in the outage plan.

If it becomes necessary for unforeseen reasons to deviate from the specifications of the outage plan, the planning documents are amended accordingly by the planners of the outage. Following quality assurance, the documents are then handed over to the shift personnel on duty as updated procedures.

This approach requires the continuous presence of the outage planners. During an outage at GKN, they are therefore available around the clock.

› **Preventive maintenance during power operation.**

Since 1998, part of the maintenance work on safety systems in GKN II has been carried out during power operation. As regards this strategy, the general opinion seems to be that this leads to a noticeable reduction in outage times. However, this is not the case. As on-power maintenance (OPM) on safety-related systems mainly comprises mechanical systems, it does not shorten the critical path of an outage since the work relating to I&C systems is still performed during the outage. However, one advantage of OPM is the reduced work load for the maintenance and supervision personnel →



→ during the outage, leaving more capacity to carry out and supervise the remaining tasks. The slightly reduced system availability, on the other hand, is negligible, as the degree of redundancy is $n + 2$.

> **In-service inspections prior to restart.** After the maintenance measures have been completed, an enveloping functional test is required to demonstrate functional ability. This inevitably results in a large number of functional tests after outages. A wide area of the functional tests is covered by routine tests of the reactor protection system. Moreover, it is common practice at GKN II to subject all vital components that were isolated during the outage to systematic function tests as well. For the coordination of these tests, the formation of an especially dedicated team has proved useful.

> **Supervision of outage activities.** It is quite understood that the success of an outage is not only based on good scheduling but above all on the technical quality of the work. The latter is performed by a multitude of contractors; their personnel have to be coordinated and supervised by the operating personnel on site. Many power plant personnel who carry out maintenance work during power operation primarily fulfil supervisory functions in outage times. Should one carry this concept further and contract out all activities to external firms for power operation as well, that would mean that there would not be sufficient numbers of qualified in-house personnel available to supervise contract work at peak times, e. g. during an outage. One would then have to rely to a large extent on the quality of the contract personnel and on the final functional tests. Such a strategy

would inevitably raise questions as to the operator's responsibility under atomic law.

> **Safety and commercial aspects of outages.** There is a general rule that safety does not come free. The time and personnel needed for outage planning has increased significantly in the course of the optimisation process; however, the inevitable associated close analysis of all processes also has contributed to the shortening of outages – despite increased selective restrictions, e. g. in mid-loop operation. In the context of the shutdown PSA, some improvements were carried out which did not contribute to the facilitation or acceleration of the outage. Another characteristic example of a gain in safety despite a (considerable) gain in time is the practice of “in-core shuffling”, the introduction of which clearly improved the planning and supervision of core loading with regard to ensuring subcriticality. Other outage shortenings could be achieved by investing in technically improved systems (e. g. refuelling platform). This also helped raise the safety level of these systems.

Finally, it can be stated that the in-depth analysis and optimisation of outage processes at GKN II have had positive safety-related and economic effects. However, one has to warn against outage shortenings based exclusively on competition-oriented attainment targets and which may entice operating personnel not to take safety-relevant boundary conditions too seriously despite lacking boundary conditions (such as sufficient planning and implementation capacities) or not to apply the necessary diligence to maintenance work. The price of “achievements” reached this way may yet prove a high one. ■

ORGANISATIONAL ISSUES: A REGULATOR'S VIEW

■ **Plant outage as well as refuelling completion requires regulatory approval granted only after selected items have been witnessed by safety authorities and the corresponding reports duly issued. A daily report is thus drafted and sent to the Authority over the entire outage period and complemented by a final report. Since every outage means economic loss for the plant, operators and safety authorities strive to make it as short a duration as possible. This imperative can lead to some conflicts of interest in the event of a fault being discovered during shutdown, the regulator's priority being to have full awareness of the solution envisaged whereas the operator's primary concern is to restart as early as possible.**

From 1996 onwards, numerous safety upgrade measures have been implemented on Paks NPP, mostly during plant outages. One special type of planned shutdown called extended outage is performed on one of the four units of the plant every four years. The reactor internals are then taken out and thorough inspections are completed, extending the shutdown's duration from 24 days for a regular outage to as 60 days. The outages offer also an opportunity to repair some failures that are potentially conducive to unexpected events.

Plant shutdown, a major source of risk

▼ In spite of a deeply rooted but false assumption, the global risk related to plant shutdowns for maintenance or refuelling is comparable or even higher than in the course of full power operation. There are several reasons for this.

Firstly, transitional phases – i.e.

shutting down and restarting – as well as maintenance and refuelling activities involve a lot of manual actions, which is not the case for “normal” operation. For comparable reasons, plane accidents mainly occur at take-off and landing, not at cruising speed and altitude. Secondly, a reactor shutdown for refuelling means that a large number of fuel assemblies remain inside the vessel, calling for the continuous evacuation of the residual heat. Thirdly, the configuration of the plant at shutdown is such that many safety systems are undergoing maintenance. There is thus less usable equipment than during normal operation. Finding the minimum necessary configuration then becomes crucial, as an unexpected failure can impair the ability to assure safety. Fourthly, logistics. The replacement of parts is often a problem. In many cases, the original spare part supplier was lost track of or

By Lajos Vöröss, Deputy Director General, Nuclear Safety Directorate, Hungarian Atomic Energy Authority



●●● modifications were performed which significantly altered the equipment from its original design. This poses a safety problem, for instance where earthquake – resistant equipment is concerned. Fifthly, procedures. Each task carried out in the context of operation at power is very precisely prescribed and the limits/thresholds are explicitly mentioned. This is not true in the same way for actions related to shutdown, neither in Hungary nor anywhere else.

Management of risk: a matter of organisation

▼ As numerous sources of risk might interact and result in an unexpected event, many different means are obviously operative in mitigating those risks. One is PSA. Regularly updated probabilistic safety assessments reflect the actual configuration of the plant at the time of outage. As every configuration has a risk factor, PSA helps make quick decisions in the case of an unexpected situation. We currently have plans to develop such a powerful tool for Paks NPP. This implies a considerable amount of work, as the tasks generating risk during a plant shutdown are plentiful and the inter-relations between them even more so. ▼ Another tool is experience. Since models and input data used for PSA are based mainly on practice, a clear picture of the different kinds of risk at every stage of the plant’s outage is necessary. The difficulty in determining the risk factors and quantifying their comparative weight is amplified by unanticipated factors, i.e. by

“ *As the Deputy Director General of the HAEA and Head of the Nuclear Safety Directorate, I am in charge of making regulatory decisions in the field of licensing, inspection and the enforcement of decisions made by the regulatory body. A very low percentage of my decisions are appealed by operators. Only in the case of such a disagreement, the final decision is made by the Director General of the HAEA himself.* ”

OUTSOURCING: A BENEFICIAL TREND FOR SAFETY

The tendency in Hungary is towards more outsourcing than in the past. Whereas the entire work associated with maintenance and modifications used to be executed in-house by a fairly large plant staff, subcontractors now take a growing share of the work. For the safety regulator, the problem was then one of confidence in the subcontractors’ qualification and identifying who would be liable for it. It was decided that the operator would be responsible for selecting the subcontractor and checking if the adequate quality system was put into practice by the selected company. This major change in the organisation of shutdowns and maintenance did not impact safety negatively since both the internal personnel of Paks NPP as well as subcontractors are trained in the same facility: the Paks maintenance training centre.

defects remaining in spite of the careful design and construction of the plant and which can be discovered only upon dismantling. In that case, one’s own experience is irreplaceable. ▼ A third means is the ALARA (As Low As Reasonably Achievable) principle. Compliance with this rule demands cautious manpower economy so as to minimise the dose received by every individual during the operations. In Hungary, the State Public Health & Medical Officers Service (ANTSZ), in charge of radiological protection, puts emphasis on ALARA and on the need to have a sufficient number of people available. ▼ A fourth method is having accurate information. In order to avoid misunderstandings, to keep track of what happens from the beginning of operations and to provide a basis for well-founded decisions, efficient communications both among people on the plant’s site and with the safety authority as well as quality document management are of utmost importance. ▼ A fifth tool is housekeeping. Outage is a period of time where quantities of people and equipment are temporarily stationed on the plant’s site, calling for strict procedures to be followed by everybody to avoid any equipment left in place after maintenance causing problems as foreign objects after restart. Last but not least, a good quality assurance and safety culture is required from the operator to produce adequate relations with the regulatory body and prevail over the temptation to hide information as a way of accelerating the approval process.

Progress and challenges in the Hungarian arena

▼ In Hungary, commendable progress is being made regarding safety as operators continuously improve their maintenance tools, technology and practice. Adding to the preparatory centre for maintenance which came into operation some 15 years ago, sophisticated software and information systems enable tasks to be performed in a much more systematic way than previously. Among other things, a maintenance training centre enables agents to carry out the work in conditions which reflect – in an inactive context – the real operating situation. ▼ Obviously, the Hungarian safety policy is on the right track. Nevertheless, additional effort still has to be devoted to increasing our awareness and preparedness further, particularly in the area of maintenance outages. We now recognise the importance of that kind of shutdown

and are determined to do more than before. For instance: ● the HAEA is developing new regulatory guidelines for maintenance outages after having studied the US NRC practices very carefully and recognised that such an approach would prove beneficial for us. We are currently striving to get the new guidelines ready by the turn of the year, with consideration also being given to the planned lifetime extension of the units at Paks NPP; ● we thoroughly reassessed the safety goals associated with shutdowns to decide what type of analytical tools are needed to improve our safety level; ● we reengineered our regulatory oversight strategy so as to take better account of maintenance-related tasks in plant outages. For instance, we reconsidered the acceptable safety thresholds for this type of operation;

● we provide our inspectors with the same level of preparation and training for inspections, evaluation and enforcement for maintenance/ refuelling outages as for full power operation. ▼ In this process, European and international cooperation in the field of nuclear power plant shutdown is of utmost importance to us, since highly developed safety practices are a valuable source of inspiration. ●



Reactor vessel at Paks Nuclear Power Plant, Hungary.



Paks Nuclear Power Plant, Hungary.

THE HUNGARIAN ATOMIC ENERGY AUTHORITY (HAEA)

The HAEA is a central public administration organisation with a general scope of authority, with its own tasks and regulatory competence being directed by the government. The HAEA both regulates all nuclear safety activities (in particular licensing and inspection of nuclear facilities) and coordinates the regulation of other activities by ministries and administrative bodies. The director general of HAEA and his deputies are appointed and relieved by the Prime Minister according to the new atomic law issued in 1997. The Government exercises supervision over HAEA through the president of the Hungarian Atomic Energy Commission. The HAEA comprises two directorates, the General Nuclear Directorate (GND) and the Nuclear Safety Directorate (NSD). The GND is entrusted with the safeguarding and packaging of nuclear material as well as the licensing of transportation and packaging, while the NSD’s rights and responsibilities

cover licensing, inspection and enforcement of nuclear facilities. The NSD employs 40 professionals with university or college degrees. The HAEA-NSD supervises 4 facilities: ● the Paks NPP (4x460 MW VVER 440/213-type reactors) where the NSD has a site inspectorate; ● the 100 KW nuclear training reactor operated by the Institute for Nuclear Techniques of the Technical University of Budapest; ● the 10 MW Budapest Research Reactor operated by the KFKI Atomic Energy Research Institute; ● the Paks interim spent fuel storage facility operated by the Public Agency for Radioactive Waste Management (PURAM). The HAEA operates centres for emergency response, training and analyses (CERTA), covering practically all the roles needed for a regulatory body.

INCREASING AVAILABILITY MEANS INCREASING SAFETY

■ As a private utility in a deregulated electricity market, Nuclenor pays utmost attention to increasing the cost-effectiveness of its operations. The 50% Iberdrola and 50% Endesa subsidiary company owns and operates a 466 MWe BWR located at Santa María de Garoña near Burgos, and owns a 2% share in the 1066 MWe Trillo PWR located in the Guadalajara region. Headquartered in Santander, Nuclenor was founded in the 60's with the objective of designing and building the Santa María de Garoña plant, the third Spanish NPP to come to power. The company thus enjoys a valuable experience in reactor design, construction and operation. An important goal now set for employees is to improve the plant's availability through shorter shutdown periods. Responsible for systems engineering, plant simulation, probabilistic risk assessment (PRA), safety analyses, etc. in relation to safety and regulatory requirements, and responsible for the company's information systems and technologies, Julio González explains the competitiveness challenge Nuclenor is faced with and the ways to make plant shutdowns more cost-effective while maximising safety.

There is no discrepancy between availability and safety

▼ Plant shutdowns are critical periods for several reasons. First, they are a minor part of a reactor's lifetime compared to "normal" operation, but the most significant changes take place in this period. The associated processes and procedures are therefore rarely as detailed and repetitive as operating procedures. Second, shutdowns are periods of time where large members of "unusual" and delicate tasks such as opening and closing the vessel, moving the fuel, etc. are performed within a tight schedule. Coordinating and planning these many tasks – as well as the corresponding transitional

states – are therefore highly complex. Third, the intervention of subcontractor teams present on the site only temporarily, for maintenance or modifications, poses the problem of acquaintance with the facility and equipment. Fourth, outages are regarded as merely unproductive periods of time, and the pressure to restart as early as possible keeps growing. For these many reasons, guaranteeing the safety of shutdown states while increasing the plant's availability is a real challenge. Nevertheless, at Nuclenor we are convinced that safety is fully consistent with efficiency in the economic area and that plants with the best availability also have the best

safety records. There is no discrepancy between both objectives. In other words: no compromise with safety is possible in the context of cost-effective operation.

Take advantage from international cooperation

▼ At Santa María de Garoña, the average duration of outage for refuelling has been around 40 days over the last three occasions, whereas a significant number of US utilities are performing much better. Consequently, we decided to try to carry out the next shutdown scheduled for March 2003 within 21 days, i.e. cutting outage time roughly by half. The aim is ambitious, granted, but realistic.

▼ As our company is involved in many international cooperations, we are used to paying particular attention to the experience gained by our colleagues in various electricity companies. Our participation in the BWR *Owners Group*, organised by General Electric, is a major source of information for improvement, since it gives us the opportunity to hear about the experience capitalised worldwide. Moreover, we keep closely in touch with Exelon (merger formed by Philadelphia Power & Light and Unicom), which operates reactors very similar to our Santa María de Garoña plant. Exelon is a reference for us, since the company has achieved great progress in the management of plant outages. We intend to take advantage of their experience and of our cooperation with European BWR

“ We believe that efficiency in the economic area has to be consistent with safety. No compromise with safety is possible in the context of cost-effective operation. ”

operators, especially the Swiss Mühleberg BWR which is very similar to ours.

Pay shutdown states as much attention as normal operation and perform thorough PRA analysis to obtain guidance

▼ After careful analysis, we decided to make rigorous planning the key to halving the duration of the next shutdown while increasing safety at Santa María de Garoña. With this in mind, we relied upon a guide issued in 1991 by the Nuclear Utility Management and Resources Council, Numarc¹. This document, titled *Guidelines for Industry Actions to Assess Shutdown Management*, offers guidance on controlling that enough power sources, systems and redundancies are available during shutdown to ensure safety. The method makes it possible to rate how long and far one went out of the safety margins should that occur. We are thus able to know at all times if we are working under green, yellow or red conditions.

▼ We have recently performed a probabilistic risk assessment related to shutdowns. This analysis showed that the major risk for a BWR-type reactor is linked to losing the capability of removing the residual heat due failure to maintain water inventory.

As a result of the PRA analysis we decided to draw up procedures for shutdown and for contingencies with levels of detail and coherence comparable to those of operating procedures. ●●●

●●● ▼ My view is that the risk is not so much associated with shutdown as with shutting down, i.e. with changing conditions and transitional states. A mistake, a wrong manoeuvre for instance, might produce a leak. Then the risk is associated with draining the water from the reactor cavity and the fuel pool. Having said that, I do not claim that shutting down is more risky than normal operation, as long as tasks are planned carefully and in detail. In this respect, market deregulation and tougher competition are a formidable incentive to re-engineer plant outages to obtain higher availability through shorter shutdown periods.

Towards increasingly cost-effective working methods

▼ The following key factors were identified in achieving short, safe outages:

- make refuelling floor activities – i.e. the activities linked with refuelling such as opening and closing the reactor, moving the fuel, inspecting, etc. – the critical path of the outage;
- plan the shutdown operations as team work, develop a detailed programme of what will be performed by each team;
- establish a highly detailed schedule each operation, in particular those related to refuelling;

- consider the working conditions to make sure the personnel required to perform the tasks are available. Higher personnel availability during outage periods can be obtained through negotiation and incentives to achieve the objectives;
- shift certain tasks such as preventive maintenance from shutdown periods to normal operation.

▼ Since one of the crucial planning aspects are the “windows”, i.e. the periods of time when some systems are available or unavailable, performing preventive maintenance at power provides more relaxation during shutdown by decreasing the number of operations to be carried out and the number of systems and equipment impacted. It also enables more control and higher quality during normal operation, as the workload is split over a long period of time.

Since the collective dose per day tends to remain unchanged, better planning conducive to shortening the outage period results in a lower total dose.

▼ Now, where do we stand and what is the work to be carried out to achieve our goals? First, we have to come out with a new maintenance programme that shifts preventive maintenance to normal operation (on-line maintenance). If we prove successful, we shall complete shutdown in a much shorter period of time than at present. Then we

have to use our probabilistic risk assessment to evaluate the new situation, so as to control the impact of the changes on the shutdown-vs-operation safety balance. To provide good performance indicators over the mid- and long-term, will require us, the operator, use our PRA and to keep it updated. This is an area where an agreement is currently discussed with the regulatory authorities. Third, we still have to work out some regulatory aspects and to carry out some negotiations with our own personnel and subcontractors in order to complete the planning aimed at halving the duration of shutdowns. Last but not least, we have to prepare and plan well the substantial modifications to be performed during outages to keep the plant in a condition compatible with our long-range objectives. The basic design, as well as a major part of the detailed design, is executed in-house, the implementation being partly subcontracted. Undoubtedly, a new era opens at Santa María de Garoña. ●

1- Numarc is part of the Nuclear Energy Institute (NEI).

The next Eurosafe Forum will be held in Berlin on 4 and 5, November 2002, focusing on the convergence of nuclear safety practices in Europe.

The lectures and discussions from the Forum will be reported in the third issue of the Eurosafe Tribune, due January 2003.