European Clearinghouse: Events related to Low Power and Shutdown

Summary Report of a European Clearinghouse Topical Study

Miguel Peinador

2016
This publication is a Technical report by the Joint Research Centre, the European Commission’s in-house science service. It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC Science Hub
https://ec.europa.eu/jrc

JRC100426

EUR 27743 EN


ISSN 1831-9424 (online)
ISSN 1018-5593 (print)

doi:10.2790/93492 (online)
doi:10.2790/1897 (print)

© European Union, 2016

Reproduction is authorised provided the source is acknowledged.

Printed in The Netherlands

All images © European Union 2016, except:
Cover’s photo: United States Government (Idaho National Laboratory’s Advanced Test Reactor)

How to cite: M. Peinador; European Clearinghouse: Events related to Low Power and Shutdown; EUR 27743 EN; doi10.2790/93492
# Table of contents

Acknowledgements........................................................................................................... 3  
Abstract............................................................................................................................. 4  
1. Introduction .................................................................................................................... 5  
2. Scope and Methodology ................................................................................................. 6  
3. Summary of the event reports review ........................................................................... 7  
   3.1. Plant state .............................................................................................................. 7  
   3.2. Activity ................................................................................................................. 7  
4. Insights ......................................................................................................................... 10  
   4.1. On the conduct of shutdown operations ................................................................. 10  
   4.2. On coolant inventory and decay heat removal ....................................................... 13  
   4.3. On reactivity control ............................................................................................ 14  
   4.4. On maintenance ................................................................................................. 14  
   4.5. Other ................................................................................................................... 15  
5. Conclusions ................................................................................................................... 16  
References ......................................................................................................................... 17  
List of abbreviations and definitions ................................................................................. 18  
Annex – Selection of lessons learned ............................................................................. 19
Acknowledgements

This document summarizes a topical report [1] prepared by the European Clearinghouse on NPP Operating Experience Feedback at the Institute for Energy and Transport of the Joint Research Centre (JRC/IET) with the support of the Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France, and Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Germany.
Abstract

This summary report presents the main results of an extensive review of operating experience related to shutdown operation. The work covers all kinds of commercial power reactors currently or recently in operation and all off-power modes of operation. The sources of operating experience for the study were the IRS database, the Licensee Event Reports (LERs) of the US NRC, the French operational experience database of IRSN and the German operational experience database of GRS. Thousands of event reports were screened to select those which are relevant for the objectives of the study. This resulted in a list of 643 event reports.

It was found that the last phase of the refuelling outage, including the preparations for the return to power operation, the core physical tests and the start-up presents a significant rate of event reporting. Another quantitatively important family of events is the one formed by violations of the plant limit conditions for operation. Concerning the root cause, and not surprisingly, the human factor is behind the majority of events reported. The study raises many lessons learned and provides a total of 29 observations covering mainly outage schedule, team coordination, plant status monitoring, loss of coolant and decay heat removal, and maintenance.

The observations made are expected to help the licensees and the regulatory authorities (1) to improve the way in which operations are conducted during shutdown states, (2) to guarantee the main safety functions during shutdown, and (3) to keep shutdown maintenance activities under control.
1. Introduction

While reactor power in shutdown states is much lower than in normal operation, there are other factors contributing to risk which are specific to shutdown, namely:

- The technical specifications allow for more safety equipment to be unavailable because of repair, preventive maintenance or testing. Even if safety equipment is available, sometimes only manual start-up is possible, as automatic initiation may be disabled.
- In particular reactor system and containment may be open during some phases. Depending on the accident sequence, there is a risk increase relative to full power mode due to lack of the second and third safety barriers.
- The coolant inventory (in the primary and possibly in the secondary circuit) may be reduced.

Furthermore, instrument readings may be disabled, unreliable or misleading. Changes in the reactor coolant system configuration are frequent. Emergency procedures may not be configuration-specific and many annunciators in the control room are in alarmed status. All this leads to human actions demands which are both more frequent and more challenging for NPP staff.

The increase in the number of activities (operational, maintenance, testing, upgrades, etc.) during refuelling outages means that a much higher number of people are working on-site, including external contractors, not necessarily as familiar with the plant systems and procedures as the regular staff. Consequently, deficiencies in communication, supervision and planning, stress and organizational factors in general may have a stronger impact on safety than in power operation.

Thus, even if the accident sequence development due to the reduced reactor power and decay heat is in some cases slower than in normal operation, the contribution of low power and shutdown to overall risk has been a longstanding concern for the industry.

Several shutdown events observed in the late 80’s and early 90’s (for instance a loss of both trains of the Residual Heat Removal system during 1½ hours or the loss of offsite power with subsequent diesel generator failure to start) triggered regulatory action in the United States and a widespread interest on shutdown risk. At the same time, increasing efforts in Europe and the US were devoted to the development of shutdown probabilistic risk assessments during the nineties. In general, these studies confirmed the conclusion obtained from a review of operating experience, i.e.: that risk from low power and shutdown operational modes cannot be neglected and must be addressed by appropriate safety programs.


2. Scope and Methodology

The work covers all kinds of commercial power reactors currently or recently in operation: pressurised light water reactors (PWR and VVER), boiling light water reactors (BWR), light water cooled graphite moderated reactors, pressurized heavy water reactors and gas cooled graphite moderated reactors.

All off-power modes of operation are concerned. This includes hot standby, hot shutdown, cold shutdown (with and without vessel head on), refuelling (with and without fuel inside the vessel) and mid-loop operations or similar modes with reduced coolant inventory. Events which occurred during reactor start-up are included in the scope if they happened during activities performed up to, and including, the reactor physical tests.

A period covering the last 20 years of operational experience has been reviewed, except in the cases of the United States and France, where this period was limited to the last 10 years, due to the great number of events available.

The study is focused on those events which are relevant for low power and shutdown states, rather than simply on events that occurred during shutdown. Indeed, as extensive tests and maintenance operations are carried out during shutdown, many failures or deficiencies have been revealed at this occasion, but their causes are not specifically linked to shutdown operation modes. However, when the event itself was caused by the test or maintenance, then it is included in the analysis.

In addition, events which could have happened and which would have evolved in a similar way during power operation have also been excluded from the scope of the study.

Finally, an important additional exclusion is that of events related to fuel handling or to the spent fuel pool not affecting the nuclear power reactor. These events are covered by another topical study already published by the European Clearinghouse [2].

The sources of operating experience for this report are the IRS database, the Licensee Event Reports (LERs) of the US NRC, the operational experience database of IRSN and the operational experience database of GRS.

In order to retrieve the relevant events from these sources, a screening was necessary. As each database is structured in a different way, and features different searching capabilities, the screening criteria used were database-specific.

The result of the screening was a collection of 643 events (162 from IRS, 157 from NRC LERs, 153 from IRSN and 171 from GRS).

All these event reports were classified according to a number of criteria, namely the plant state, the activity more closely related to the event, the means of detection, the equipment or function affected, the direct cause, the root cause and the consequences.

However, this very wide operating experience base should not be used to draw overall quantitative conclusions, such as worldwide trends in number or severity of events, comparison among countries, etc., as the reporting criteria and internal structure of databases are not homogeneous.

A classification has been done in order to provide a phenomenological description of the events observed and to obtain lessons learned and insights into risks associated to shutdown modes of operation.
3. Summary of the event reports review

From the different criteria used to characterise the events, the plant operational mode and the type of activity are closely related to an event and proved to be the ones giving the most valuable insights.

3.1. Plant state

The figure below shows the distribution of events according to plant state or mode of operation. For the sake of clarity, in these charts the different cold shutdown modes were merged (except «refuelling» and «fuel unloaded»), and so were hot shutdown and hot standby. Note that «Other» includes events where the plant was known to be under shutdown but no more specific details are available.

The definition of operational modes in general varies with countries and reactor technology. This may create some confusion over on the data presented, and it may explain the differences among the four databases (for instance the large contribution from hot shutdown in the US case or from refuelling in the German case).

However, we can still observe that the contribution from start-up events is high (ranging from 17% in Germany to 28% in IRS), especially taking into account the relatively short residence time in this mode. A possible reason for this is that a significant number of problems are revealed only when plant systems are aligned for their power operation modes. Furthermore, at this stage of the outage, many activities are part of the critical path to return to power operation, placing an extra pressure on plant operators.

![Figure 1: Distribution of events per plant operational mode](image)

3.2. Activity

The human factor is directly related to events in a vast majority of cases. Thus, it was judged appropriate to classify the events according to the activity which was being carried out at the time of the event, or which was, for any reason, closely related to the event.

The activities found to be relevant are the following ones:
Transitions between plant operational modes: A typical case is the operation of the reactor outside the domain allowed by the limiting conditions of operation prescribed in the technical specifications of the plant. In nearly all cases, the excessive workload posed on control room operators is cited either as a root cause or as a contributing factor for the event. This is generally linked to deficiencies in the outage planning, in which the workload of control room operators is not properly addressed. Most of these events happened during start-up or preparation for start-up phases.

Other special shutdown operations: This group covers events linked to the execution of special operations specific to shutdown states, such as the opening of the primary system, the adjustment of primary coolant level or the handling of the reactor vessel head, among many others. The coolant inventory control is one of the critical functions which has to be assured during shutdown conditions. A particular configuration specific to PWR technology, the mid-loop operation, has been a special source of concern, given the short time available for recovery. Often, the following contributors are cited for these events:

- Inadequate or insufficient measurement of coolant level;
- Inexistence of an automatic water make-up system;
- Concurrence of mid-loop operations with maintenance or test activities rendering some of the equipment required for decay heat removal unavailable.

Major outage testing procedures: Certain complex test procedures require the reactor to be in operation modes different from power operation, so that the risks associated to their execution can be considered as shutdown specific risks.

The review of operating experience revealed a number of events related in particular to three major tests: Reactor Coolant System pressure tests, containment leak rate test and core physics tests. In many cases, deficiencies related to planning and coordination of teams performing different activities at the same time were the root causes or the contributing factors for the events.

Inspections and tests: Many of these activities need to be carried out during shutdown. Very often they reveal latent defects that could otherwise evolve into more serious events. However, in some cases it is the inspection or test itself that causes a problem. Only the latter type of events is included in this family.

Maintenance: The previous comment about inspection and tests applies to maintenance as well. Among the typical problems reported are confusions about the items which should be subject to maintenance due to labelling deficiencies, errors during RCPB safety valves servicing, wrong torque values applied to valves or other equipment, assembly of components in the wrong sense or inadequate use of temporary plugs.

Degraded administrative lockout of systems alignment: After extensive maintenance carried out during a regular outage, various tests and verifications ensure the plant readiness before resuming power operation. These tests are governed by general work orders together with more specific functional procedures. It is a complex work that cannot be planned in the same way for every outage. Often, a system which had already been tested and declared ready has to be disabled again to verify the operability of other systems without undesired initiation of safety functions. Furthermore, additional unanticipated maintenance tasks due to revealed component failures or degradations usually call for re-scheduling of tests. As a result, the risk of returning to power operation after an outage with some systems or components inadvertently left in a wrong configuration despite of all the verification tasks, is significant, as revealed by operating experience analysis.

In some cases, the root causes were related to deficiencies in the procedures used to carry out the verification tests before declaring a system as operational. Sometimes the scope of the procedure was incomplete (for instance some valves were left out from the
check lists), sometimes the wording of the procedure was confusing or insufficiently detailed, and, in one case, no procedure existed for verification.

In other cases, the information about the status of system configuration was not adequately relayed to the following shift or to a different team for a variety of reasons, giving place to misunderstandings originating the event.

And yet other events reveal issues related to safety culture. A distinctive problem is the use of parallel, unofficial check lists to verify system status before returning to power. Another source of problems is that operators sometimes erroneously assume that the system configuration will be checked later, during the plant start-up, thus knowingly leaving a system in a wrong configuration. And finally, some events are caused by operators deviating from procedures, or signing off check lists while no verification was done.

Figure 2 summarises the number of events on each of the previously described cases, for each of the four data bases reviewed. The two activities with more events are transitions and maintenance, where mechanical equipment is the main contributor except in the US, where I&C appears more often.
4. Insights

In addition to specific lessons learned (a selection of which is collected in the Appendix) a number of more general insights can be derived from the review summarised in the preceding section. Focus has been placed on those issues that can be anticipated to have a wider significance or are supported by an important number of events or represent new problems or on those with new solutions not yet sufficiently discussed in literature.

While all insights may be traced back to some event (or, more frequently, to a group of events) identified in the OEF databases, this section is not intended to be an exhaustive compilation of good practices related to shutdown states.

Furthermore, even if most of the insights are general in nature, not all of them are applicable to all reactor technologies or even to all reactors of a given technology. Careful site-specific analysis is required to determine for each of them, whether it is applicable, and to what extent to a plant.

4.1. On the conduct of shutdown operations

Refuelling outages require carrying out a great number of complex activities in a relatively short period of time. This presents significant challenges from the point of view of outage planning, from the point of view of the coordination of many teams working on site (including subcontractors not necessarily familiar with the plant systems and practices) and from the point of view of plant monitoring.

**Insight #1 – The outage schedule should accurately take into account the overall workload on MCR operators during the start-up and during the preparatory activities leading to the start-up. Sufficient time should be allocated for the operators to carry out all activities and verifications.**

While all outage schedule phases are usually very tight and loaded, it is during the start-up and during the preparation for the start-up that event reports most often cite the excessive workload of the MCR operators or the planning pressure placed on the operators as root causes or contributors. Furthermore, two specific scenarios may aggravate the problem. One of them is when an unplanned outage occurs close to the end of the fuel cycle, with a subsequent restart. In that case, the moderator coefficient could be positive for certain temperature ranges, enhancing the nuclear heating of the coolant during the start-up and reducing the time available for the operator to follow the start-up procedures. The other scenario is present whenever the plant management takes advantage of the refuelling outage to carry out design modifications. The latter usually require additional requalification activities, making planning changes and delays more likely. In general, any schedule change seeking to reduce the total outage time should be carefully analysed.

**Insight #2 – As far as possible, the outage schedule should avoid to plan concurrently activities involving changes in valves alignments when those valves are part of the Reactor Coolant Pressure Boundary**

The chances of misunderstandings between the teams carrying out different tasks are significant, primarily when they belong to different departments (i.e. mechanical and electrical, for instance). Very often, the result of the misunderstanding is that someone believes that the valve he is working on is not part of the RCPB, when it actually is. As the valve is then operated, and the reactor coolant begins to be drained, there is a chance that the leak remains unnoticed for some time.

**Insight #3 – The outage schedule should take into account the needs of staff to be present in the MCR. Activities should be programmed in such a way that the number of staff required at the MCR is below a certain threshold, especially if testing or maintenance activities related to critical equipment or safety systems are in progress.**
One report cites a «noisy and crowded» control room as contributor for the event. An excessive number of people in the MCR may hinder verbal communications, cause distractions and increase stress on operators.

**Insight #4 – Work practices and routines should make a very clear distinction between a fully completed test procedure and a not fully completed procedure. Furthermore, once an activity is completed, it should not be reopened unless a new work order has been issued and a new procedure is available.**

Some events reveal that often the final alignment check of systems (electrical, I&C or mechanical) subject to maintenance or a test is postponed because it would interfere with the performance of other tests (for instance, an unnecessary actuation of a safety system). Thus, the system is consciously left inoperable for some time. But, as the main objective of the task has been achieved (the system functions have successfully been tested, or the repairs are complete), staff may refer to the task as «completed» and the potential for misunderstandings arises, especially when the information on the status of the system is not accurately relayed to the next shift.

**Insight #5 – The check lists used to verify the correct alignment of valves after conducting testing or maintenance should be reviewed for completeness and accuracy. In particular, it should be confirmed that valves which could have potentially been actuated during the preparation of the task are included in the check list. Furthermore, the check list should contain not only the tag of the valve to check, but also mark explicitly the correct position for the particular mode of operation.**

During shutdown, it is frequent that the alignment of systems which have already been serviced and checked for operability needs to be changed in order to carry out maintenance or testing activities in other systems. For instance, the containment filtered venting system may have been already serviced and declared operable. Later, in order to carry out the containment leakage test, some valves in the venting system are actuated for isolation, but the documentation of the leak test does not include explicitly the verification of these valve alignments and the venting system is left inadvertently unavailable. Similar problems may arise whenever a maintenance or testing operation has to be interrupted and is later resumed by the following shift.

**Insight #6 – Plant staff should strictly adhere to procedures and official check lists to verify system alignment after a maintenance or testing task is completed.**

Certain event reports mention some staff who tend to believe that checking the correct configuration of a system after its testing or maintenance has been completed during shutdown is not critical, as an overall final system alignment check is usually performed immediately prior to start-up. However, this mindset based on the idea that «someone else will check this later» can easily lead to misunderstandings and unsafe configurations. Furthermore, the use of unofficial check lists (not subject to the usual review and approval processes) has been observed in several cases.

**Insight #7 – Briefings for subcontracted maintenance staff before they carry out the work should be monitored, and the functions to be assured by plant staff supervising the subcontractor should be made clear in all applicable documentation.**

Subcontracted teams may believe that their scope of work and applicable requirements are different from what is expected by plant staff. For instance, they may not be aware of a foreign materials exclusion program requirements applying to their task, as reported in one event.

**Insight #8 – Work orders should not be released by the control room until all requisites to proceed with the work are met. The anticipated release of the work order associated to a fixed time window and requiring the outage
contractors to call the MCR to confirm permission to proceed should be discouraged.

The practice of anticipating the release of work orders by the Control Room to the outage contractors associated to a fixed time window requires the contractors to call the operators in the Control Room to request permission immediately before they start the work. This is of course needed because the outage planning may have changed between the work order was issued and the time the work actually starts. However, given the intensity of concurrent activities during many outage phases, this practice places the control room staff in a «reactive» position, as they receive constant requests from different outage contractors to proceed. Releasing the work order only at the actual time when conditions to proceed with the work are met would place the Control Room operators in a better position, avoiding unnecessary phone calls and distractions.

**Insight #9 – Modifications or add-ons to procedures needed to cope with specific situations should be written down, formally approved and clearly communicated to the staff in charge of its execution.**

Due to the great number and variability of possible configurations and operational transients in shutdown states, it is often required to modify a standard procedure to conduct a given task. Due to schedule constraints, there may be a trend not to adequately record the results of discussions or meetings about the modification, thus leading to wrong interpretations of the actions decided.

**Insight #10 – Responsibilities and scope of work for every organization or contractor participating in any complex activity should be accurately defined and communicated.**

During outage periods the complexity of operations or tests frequently calls for the participation of numerous contractors, manufacturers and technical organizations external to the plant staff. The risk of misunderstandings stemming from an incomplete or unclear definition of responsibilities assigned to every organisation involved is thus higher than in other plant conditions.

**Insight #11 – Alarms in Control Room not relevant for shutdown states should be filtered, so that the operator can easily tell the difference between shutdown-related alarms and those alarms intended only for power operation.**

The existence of many irrelevant alarms makes it more difficult for the operator to be aware of those which are relevant, thus strongly increasing the probability of an important alarm remaining unnoticed for relatively long times. Different filtering systems could be considered. For instance, plates of plexiglas have been used in France to blur irrelevant alarms.

**Insight #12 – The management of alarms from the remote shutdown emergency control room should not interfere with the alarm display in the main control room.**

Design deficiencies have been reported which may cause an alarm in the main Control Room to disappear as it is acknowledged in the emergency ("bunkerized") control room. This happened for instance in the case of a safety injection low pressure inhibition signal alarm, which remained unnoticed for three days and made the automatic protection unavailable when a failure to close a pressurizer relief valve occurred for other reasons.

**Insight #13 – Procedures used to monitor plant parameters during shutdown should be prepared specifically for shutdown states.**

Some plants may use procedures valid for all operating modes, but which contents is mainly intended for power operation modes. Many of the parameters listed in these procedures are irrelevant or not applicable in shutdown. The need to systematically follow all steps and checks in such procedures may load the operator with unnecessary
tasks, causing distraction and preventing them to focus on the safety-related and relevant parameters.

**Insight #14 – The information related to the current status of the safety systems should be readily accessible for the operator at all times during the outage.**

One of the main risks in shutdown states originates from the difficulty in assessing the availability of every safety system at a given time. This is due to constant changes in the status of safety frontal and support systems caused by testing, maintenance or design change activities. This situation may potentially lead to an unsafe configuration. Work practices and routines should allow for easy access to all information, for instance gathering it in one single place.

**Insight #15 – Vibration monitoring of equipment (e.g. pumps, piping…) should be implemented as much as possible.**

Vibration monitoring is particularly useful for shutdown states, as it allows the detection of foreign materials left inside a system after maintenance or of fatigue symptoms associated to specific shutdown configurations.

### 4.2. On coolant inventory and decay heat removal

**Insight #16 – Plants using mid-loop operations should consider outfitting the Reactor Coolant System with hardware improvements.**

Some of the upgrades which have proved to be helpful in preventing the risk of an excessive decrease in reactor coolant level are diverse reactor level measurements (e.g. ultrasonic level measurement), automatic water make-up on low level signal or RHR pump vibration and discharge pressure monitoring.

**Insight #17 – Procedures should provide specific guidance to the operator for the case when diverse reactor coolant level measurements during mid-loop operations give contradictory readings.**

Some plants have implemented hardware modifications to improve redundancy and/or diversity of reactor coolant level instrumentation during shutdown states, in particular PWRs for the case of operations at mid-loop level. In the absence of adequate guidance for the operator, however, the effectiveness of these measures may be limited in case of contradictory readings.

**Insight #18 – Emergency procedures should cover the case of partial and total loss of Residual Heat Removal trains during shutdown states, including the instructions to align any other alternative cooling path available.**

Often, nuclear plants have several alternative paths to remove decay heat during shutdown states in case of loss of the RHR system. However, the alignments of these alternative paths require a number of actions from the plant staff. As these operations are not frequently carried out, it is likely that, in the absence of detailed procedures, a relatively long time is required to take the appropriate decisions. Experience shows that, when emergency procedures for this situation are available, they have significantly reduced the reaction time of the operators thus increasing the safety margin before the reactor coolant temperature approaches the boiling point. Even in the case of loss of only one RHR train a procedure in place may significantly help in taking provisions for the plant to be better prepared in case of an additional failure.

**Insight #19 – RCPB management responsibilities during shutdown should be clearly established and centralised, so that all changes in the status of valves being part of the boundary are immediately known to all applicable staff.**

When the outage planning cannot avoid carrying out concurrent activities on the RCPB, a strict and centralised management of the status of valves forming the RCPB together
with effective communication channels may prevent loss of coolant accidents due to misunderstandings between different maintenance teams.

**Insight #20 – In BWR plants, it should be assured that reactor vessel level measurements are reliable during cool down phases for all possible cooling rates.**

If the cooling rate is too high, there is a potential for the pressure in the vessel to fall below the saturation pressure corresponding to the actual temperature of the coolant in the measurement chamber rendering the level instrument unreliable. Measures to correct the problem may include to limit the cooling rate or to monitor more closely this parameter.

**Insight #21 – In plants featuring automatic water makeup systems to cope with an unexpected coolant level decrease during mid-loop operations, the availability of this system should be checked immediately before entering this condition.**

Some PWR plants have modified their design to include an automatic water makeup system, improving protection against losses of coolant intervening during mid-loop operations when the response time required from the operator is much shorter than in other shutdown states. As these systems are not usually in operation, it is important to check their availability right before entering the mid-loop condition or otherwise the effectiveness of this hardware addition could be limited.

### 4.3. On reactivity control

**Insight #22 – Adequate venting of the piping in the hydraulic control units of BWRs should be assured before restoring the HCUs to operable status after tests and inspections during outages.**

There is a potential for air or nitrogen to enter the circuit during tests or inspections of the hydraulic control units. Some unexpected insertions of control rods have been reported as a consequence of this.

**Insight #23 – Laboratory analysis to measure coolant boron concentration in PWRs during shutdown should be carried out with sufficient frequency.**

Even if boron concentration is continuously monitored, it is relatively likely that low boron alarms in control room remain unnoticed for a long time in shutdown states. Thus, results of laboratory analyses are still very useful as a backup of automatic monitoring.

### 4.4. On maintenance

**Insight #24 – Multi-unit plants should standardize, as much as possible, the spare parts, tools and maintenance procedures used in different units. When differences do exist, they should be highlighted in the documentation and in the training.**

Staff members are often shared by different units within a plant. Even if a maintenance procedure is clearly identified as applicable only to a given unit and if procedures for several units are very similar, it is likely that the operator overlooks the difference.

**Insight #25 – Correct labelling of equipment should be periodically reviewed, particularly for redundant equipment.**

Wrong or unclear labelling may lead the maintenance staff to mistake the equipment in train A for the one in train B. This is more likely to happen when the physical layout of equipment is spread out in different rooms or areas, so that the correct labelling of the equipment is the only way to determine which equipment belongs to which redundancy.

**Insight #26 – The use of temporary inflatable plugs should strictly adhere to vendor prescriptions and recommendations.**
Inflatable or ice plugs are frequently used during shutdown to isolate equipment subject to maintenance. Some event reports show that when vendor specifications for their use are overlooked the plugs may fail and become a hazard.

**Insight #27 – The application of tightening torques on mechanical components, particularly valves, should be subject to verification and should be recorded.**

Events caused by mechanical failures of valves due to inadequate tightening torques are frequent and may easily lead to consequences affecting the safety of the plant. A register of the used torque values is very useful in investigation of these events.

4.5. Other

**Insight #28 – Rare operational transients should be given more attention in the simulator training sessions. Furthermore, they should be covered by detailed procedures as much as possible.**

Certain transients after stopping the main RCPs in a PWR or formation of bubbles with natural circulation in VVER plants are examples of such situations. Specific shutdown operating ranges should be better explored during training on simulators, as the underlying physical phenomena may be not well understood by the operator.

**Insight #29 – During the preparation of any special operation which is performed for the first time or for the first time after a change in operating manuals or practices, a thorough risk analysis should be performed.**

Every refuelling outage is different from the preceding one. Even if the operation itself is carried out in every outage, sometimes a change in the operating practice of a system may lead to unexpected results. Some examples of special operations where a risk analysis would have helped to prevent an event are the handling of a 2.5 Tm load over the central hall of the reactor building, the oxygenation of the primary coolant with hydrogen peroxide or venting of the scram accumulators after a change in the operating manual.
5. Conclusions

A topical study has been conducted to review the recent worldwide operating experience in shutdown modes and to derive lessons learned and insights which may help to improve the safety of nuclear plants during outages.

The work covers all kinds of commercial power reactors currently or recently in operation and all off-power modes of operation.

The focus was placed on those events which are relevant for low power and shutdown states rather than simply on events that occurred during shutdown. In general, events which could have happened and which would have evolved in a similar way during power operation were not studied. An important additional exclusion area is events related to fuel handling or to the spent fuel pool not affecting the nuclear power reactor.

It was found that the last phase of the refuelling outage, including preparations for the return to power operation, the core physical tests and the start-up represents a significant rate of reported events. This is probably linked to the performance of the last system alignment verifications before returning to power (giving the chance to detect anomalies caused by activities conducted during the prior phases of the outage) and to the constraints and pressure imposed by the outage schedule on the plant staff at this point (many activities become part of the critical path as the plant approaches the end of the outage).

Another quantitatively important family of events is formed by violations of the plant limit conditions for operation. Typically, in these events the plant conditions to be met before changing the reactor mode are not respected, inadvertently or not. Again, many of these events are related to the stress generated by the tight schedule on the operators.

Concerning the root cause it is not a surprise that the human factor is behind the majority of events reported.

The main part of the review presented here was the qualitative assessment of the events with an extensive discussion of lessons learned and insights that could be derived.

The results obtained are expected to help the licensees and the regulatory authorities (1) to improve the way in which operations are conducted during shutdown states, (2) to guarantee the safety functions during shutdown such as coolant inventory control and reactivity control and (3) to help to conduct shutdown maintenance activities as requested by regulations.
References

[1] Events Related to Low Power and Shutdown, Topical study, NRSA/CLEAR/15 06 001 Rev.00, 2015 – RESTRICTED DISTRIBUTION

## List of abbreviations and definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>BWR</td>
<td>Boiling Water Reactor</td>
</tr>
<tr>
<td>GRS</td>
<td>Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH</td>
</tr>
<tr>
<td>HCU</td>
<td>Hydraulic Control Unit</td>
</tr>
<tr>
<td>I&amp;C</td>
<td>Instrumentation &amp; Control</td>
</tr>
<tr>
<td>IRS</td>
<td>International Reporting System</td>
</tr>
<tr>
<td>IRSN</td>
<td>Institut de Radioprotection et de Sûreté Nucléaire</td>
</tr>
<tr>
<td>JRC/IET</td>
<td>Joint Research Centre / Institute for Energy and Transport</td>
</tr>
<tr>
<td>LER</td>
<td>Licensee Event Report</td>
</tr>
<tr>
<td>MCR</td>
<td>Main Control Room</td>
</tr>
<tr>
<td>OEF</td>
<td>Operating Experience Feedback</td>
</tr>
<tr>
<td>PWR</td>
<td>Pressurized Water Reactor</td>
</tr>
<tr>
<td>RCP</td>
<td>Reactor Coolant Pump</td>
</tr>
<tr>
<td>RCPB</td>
<td>Reactor Coolant Pressure Boundary</td>
</tr>
<tr>
<td>RCS</td>
<td>Reactor Coolant System</td>
</tr>
<tr>
<td>RHR(S)</td>
<td>Residual Heat Removal (System)</td>
</tr>
<tr>
<td>RPV</td>
<td>Reactor Pressure Vessel</td>
</tr>
<tr>
<td>RPS</td>
<td>Reactor Protection System</td>
</tr>
<tr>
<td>US NRC</td>
<td>United States Nuclear Regulatory Commission</td>
</tr>
</tbody>
</table>
a) Transitions between operational modes

Before restarting the reactor after a refuelling outage, the new core parameters should be studied to determine if start up procedures are well suited for start-up under all phases of the fuel cycle. In particular, it is important to analyse the case where an unscheduled shutdown takes place close to the end of cycle, with a subsequent restart. If moderator coefficient is positive for low temperatures, it should be checked if plant staff has the time required to carry out all start up activities in spite of the higher heat up rate.

Start-up of the plant after a refuelling outage is a phase with many concurrent activities, especially if the outage has included design modifications. Sufficient time and human resources should be available in the main control room to supervise all the activities. Operators should also be careful with alarms apparently not related to the current transient, as these might point to unavailability of a required safety system.

Regardless of any external pressure to bring the power plant back to operation after a refuelling outage, the operators at the control room remain responsible for the operational decisions and safety.

During refuelling outages, some plants may issue work orders to contractors based on time windows compatible with the outage schedule. As these time windows are only valid at the time the work order is issued, the contractors are requested to seek authorization from control room immediately before starting the activity. Events show that this practice puts the control room staff in a reactive position and adds the distraction of uncontrolled phone calls. It should be considered to assign the control room staff with an active role of issuing a work order only when all prerequisites and conditions are met.

Changes in outage planning seeking outage duration reduction should carefully assess the intensity of the resulting workload for control room operators.

Formal, official check lists should be used to make sure the configuration of the plant is as required by the technical specifications to enter a different mode or plant condition.

In one plant, the following check list was prepared (in addition to two existing check lists for entering refuelling and for bringing the reactor to the minimum controlled power level):

1. Conditions of starting the unit cooling down
2. Conditions of cooling down below the reactor vessel embrittlement temp.
3. Conditions of stopping the last main coolant pump
4. Conditions of starting the unit heating up
5. Conditions of heating up over 150 deg C

RPV level indications in BWRs based on float switches may be unreliable during the cool down phase, especially for high cool down rates. A possible solution could be to limit the cool down rate or to monitor more closely this parameter (i.e. monitoring the °C/min rate instead of the °C/hr rate).

b) Coolant inventory control

Risks associated to shutdown cooling pump vortex formation are limited by the presence of several diverse level measurement indications. However, the existence of diverse signals might not be very useful in practice if the operators are not provided with procedures instructing them what to do in case of discrepancies among signals.
Risks associated to shutdown cooling pump vortex formation should be carefully studied to determine safe limits for combinations of primary water level and pump flow conditions. These studies should account for actual conditions at the plant in order to be sufficiently representative.

Truly exhaustive requalification/periodic tests guaranteeing the availability of systems required during certain phases of shutdown (and not challenged during normal operation) should be carried out. In particular, availability of the automatic water makeup to the RCS should be checked just before entering reduced inventory conditions.

Status lights in control room should allow the operator to clearly identify the difference between «light on» and «light off» state, especially if protective covers are used.

Refuelling planning should avoid to have too many concurrent activities involving changes in the valve alignment of systems connected to the RCS.

c) Natural circulation degradation in VVER reactors

Draining procedures should warn the operator that level measurements can be affected by the formation of gas bubbles inside the primary piping. Thus, approximate draining times and water volumes to be drained should be included in these procedures.

Specific training to operators covering the topic of natural circulation degradation in VVER reactors should be given including guidance on how to proceed in case of contradictory level measurements.

d) Other special shutdown operations

TV camera monitoring of the reactor vessel head lifting should be considered, so that it is possible to detect a jamming of the control rod drive shaft before the control rod leaves the fuel element.

e) Major outage testing procedures

When teams from different organisations are involved in maintenance or testing operations the communication among teams should be assured at all times. Furthermore, the responsibilities for issuing worksheets should be very clear to all staff involved.

When a test that has been interrupted is restarted all initial conditions should be checked again.

Deviation for operating instructions should be documented and formalised in a systematic manner. Transfer procedures from an instruction to another one should be revised to avoid that something is missed in the middle. For instance, a term such as "reinstate" in one instruction should not be replaced by "control" in another instruction.

The shift supervisor’s working routines, instruments and means to supervise ongoing activities should be improved. Much of the information about the status of the systems in the station is spread in many different places, e.g. in the operational logbook and the shift supervisor's file of notes to be transferred to the next shift. All important information about the status of the safety systems should be gathered in one place.

The procedure for the preparation for the RCS hydrostatic test should be sufficiently detailed regarding to how the pressurizer safety valves are prepared for the test.

Technical documentation of safety valves should include tolerance values for serviced parts.
Test procedures used for online check of RCPB safety valves set point («trevi test» method) should take into account the valve reseat pressure, such that specified system operating pressures allow sufficient margin for the "blowdown" to ensure the valve will reseat after the assist pressure is removed. If this is not practical, the trevi-test equipment can be used to force closing the valve but this needs to be clearly identified in the procedure.

When performing online check of RCPB safety valves set point («trevi test» method), a provision should be made to allow the test team to check that the valve reseats after opening. This can be done using existing instrumentation in the discharge line (if any), or using temporary instrumentation (ultrasonic leak detectors, pyrometers, stem valve position indicators). It is also important that the test procedure requires constant monitoring of pressure and level in the tank that receives the safety valve exhaust.

The wide pressure variations experienced by the RCS during the conduction of hydraulic tests may give rise to hydrogen release. Thus, careful attention should be paid to flammability conditions during venting operations of the RCS and prior to the hydraulic test.

Lock out of all safety relief valves prior to the RCS hydraulic test should be carefully checked as the test may reveal hidden design deficiencies in the relief piping.

Procedures and relevant documents related to physical tests should clearly describe the configuration to which the reactor has to be restored after the tests are completed and the unit is handed over to the shift supervisor.

f) Inspections and functional testing

An event revealed that a number of alarms designed to alert the operator about undesirable conditions while the unit was shut down were ineffective. The operator should be able to easily distinguish between those alarms that are due to a particular operational mode in which the plant is at that moment and those alarms revealing true anomalies.

For plants featuring bunkerized emergency control rooms for remote shutdown the design of alarms related to inhibition of signals should be such that the acknowledgement of an alarm from the bunkerized control room does not cause the alarm to disappear from the main control room.

g) Maintenance

Labelling of equipment in redundant trains of safety systems should be verified, especially when the system layout (i.e. with equipment located in different rooms or areas) does not allow to easily identify each train.

Reactor coolant boundary management responsibilities should be clearly established and centralised and procedures should give clear instructions on how to deal with changes in the boundary (for instance, due to problems found in valves during inspections). Specifically the procedures should make sure that all teams involved in maintenance are aware of these changes.

Maintenance strategy for outage refuelling periods should ensure that the third common pump in the reactor cooling chain is available when one of the two trains is unavailable. This is applicable for configurations of 2*100% trains in the cooling chain equipped with a third pump common to both trains.

Standardization of spare parts in twin units may reduce the risk of using wrong spare parts.
Inspection of pilot operated safety valves should include geometrical inspection of the valve internals and especially a check of the absence of spindle deflection against an accepted tolerance value.

Applying an excessive torque on bolts can cause a latent failure of safety systems, due to rupture of the excessively stressed bolts after heat-up of the system. Such defects can simultaneously lead to the occurrence of an initiating event, for which the failing systems have been designed as mitigating safety systems. When the cause is related to inadequate choice of the hydraulic spanners or to the use of wrong or inadequate procedures, the potential for a common cause failure of redundant safety systems is very high.

The risk of applying inadequate torque on check valves which are part of RCS pressure boundary should be minimized by measures like:
- Allocation of sufficient resources to preparation and execution of the tasks.
- Assurance of independent verification of the procedures and of task execution.
- Formal pre-job briefings.
- Training, testing and certification of staff able to use hydraulic spanners.
- Formal hold point in the procedure to independently verify the hydraulic pressure and corresponding torque value applied by the hydraulic spanners.
- Reduction of the number of different models of hydraulic spanners available in the workshop.

Tightening torques applied during assembly of valves after maintenance should be registered and checked.

The supervision of vibrations of the main coolant pumps represents an appropriate and necessary surveillance mechanism of the reactor coolant system.

In plants with twin units maintenance procedures should be as much standardized as possible and when differences do exist they should be highlighted in training and documentation.

As electrical system interactions are difficult to recognize, administrative controls should be in place to avoid maintenance work in electrical equipment when no alternative and independent offsite power source is available. These administrative controls should be applied to all modes of operation even with fuel unloaded from the vessel.

Outage and start-up planning should avoid as much as possible to conduct too many tasks concurrently in the control room when testing or maintenance operations on safety systems are being carried out.

**h) Degraded administrative lockout of systems alignment**

Due to outage planning constraints staff often needs to realign a system which had already been serviced during the outage and declared operable in order to proceed with an additional test such as the containment leak test. In this case, the procedure for this additional test should include checklists of valve alignment for all valves which have been actuated during the preparation for the test.

Work routines should clearly differentiate fully completed testing procedures from not fully completed procedures (for instance, when the test has been done, but the realignment after the test is still pending).

The existence of alarms in the control room to detect wrong configurations of relays belonging to the reactor protection system after refuelling is a very effective way to prevent reactor protection system failures.
Verification of valve line-up before start-up should be done using official check lists. Other unofficial lists used in parallel should not be allowed.

For all safety relevant level measurements, when the threshold cannot be tested during or immediately after their maintenance, the following measures for quality assurance are advised:
- Isolation and equalization valve positions need to be checked after maintenance activities;
- Creation of a procedure for the sealing of concerned valves and armatures in general, covering the following aspects: definition of the responsible staff, conditions under which the sealing may be executed, control of the measurement after sealing by approaching the threshold value or, if this is not possible, by the “four-eyes-principle”, documentation of sealing and control.

Staff working in test and maintenance during refuelling tends to assume that safety-related equipment configuration will be checked at the latest moment prior to resuming power operation thus relaxing the administrative procedures for system alignment control during the outage. Experience shows that in some cases this assumption is wrong.

It should be considered to use plug-in units instead of jumpers to carry out the interlocks of the RPS. These plug-in units should feature lamps in the I&C cabinet front doors to signal interlocks.

### 1) Foreign materials

Briefings for subcontracted maintenance staff before they carry out work on unsealed reactor equipment should be monitored. Clear requirements concerning foreign materials exclusion should be included in the documentation for the task.

Whenever activities potentially generating foreign objects near the reactor cavity area are executed, the foreign material exclusion program should include a vacuum cleaning not only of the reactor cavity floor, but also of any object or structure projecting out above the reactor cavity. Also, at the time of performing the activity, thorough shielding of the reactor cavity should be enforced.

### 2) Reactivity control degradation

Stainless steel gate valves used for hydraulic control unit venting are susceptible to internal leak due to seat surface damage when the angular adjustment between the valve disk and the valve seat surface is not accurate.

Air or nitrogen can enter the hydraulic control unit piping during tests and inspections performed in shutdown periods. It is therefore important to ensure venting of the circuit before restoring the hydraulic control units to operable state.

Reactor coolant boron concentration alarms are likely to remain unnoticed during start up preparation activities due to many other alarms present in the control room and the heavy workload during that phase. Thus, laboratory analyses are important as a backup to detect boron dilution and should be conducted frequently enough.

Chemistry and plant start up procedures should contain precautions in relation to reactivity excursions concerning ion exchanger demineralizer conditioning before its first use after a refuelling outage.

Shift chemists training should include theoretical contents related to the conditioning of ion exchangers in relation to reactivity.
When chemistry alterations are detected in primary or moderator circuits, immediate action should be taken to restore the design conditions. Experience shows that non-standard chemical parameters may trigger unknown processes with unexpected consequences. In particular, in the case of CANDU type reactors, leakage of CO\(_2\) from calandria tubes into the moderator should be repaired as soon as possible.

During the preparation of the boron dilution operation, attention should be paid not only to the initial and final concentrations of boron, but as well to the transient itself and to local concentrations during the dilution process.

A thorough review of all the shutdown check sheets that are completed by the control room staff should be done. Many of the required checks are only relevant when at power. The check lists should concentrate on the issues that are safety critical when the unit is shutdown. Routine recording of parameters should be automated (for instance by an automated shutdown data logger) instead of overloading operators.

Any troubleshooting of the neutron monitoring system should assess the entire chain of measurement and reporting system and not only an isolated component.

### k) Radiological events

Whenever changes in the operating manual are planned, the possible paths for radioactivity released should be very carefully analysed.

All interfaces between controlled areas and the external environment should be monitored for radiological releases.

Valves preventing the transfer of radioactivity between systems should be classified and tested accordingly.

When a hydraulic gradient between systems is used to prevent contamination of a system, it should be monitored and the operating manual should contain instructions for the case when the gradient is lost.

If a connection between a normally clean system and a normally contaminated system is only rarely used, it should be considered as a temporary connection.
How to obtain EU publications

Our publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.
JRC Mission

As the Commission’s in-house science service, the Joint Research Centre’s mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2790/93492