HND
International Conference
Nuclear Option in Countries with Small and M
Opatija, Croatia, 1996

Risks Associated with Shutdown in PWRs

Igor Grlicarev

Slovenian Nuclear Safety Administration
Vojkova 59, 1113 Ljubljana, Slovenia

Abstract

The selected set of risks associated with reactor shutdown in PWRs are outlined and discussed (e. g. outage planning, residual heat removal capability, rapid boron dilution, containment integrity, fire protection). The contribution of different outage strategies to overall core damage risk during shutdown is assessed for a particular basic outage plan. The factors which increase or minimize the probability of rector coolant boiling or core damage are analyzed.

1.0 Introduction

The risks during reactor shutdown, refueling and startup are not negligible, therefore the premise that reactor shutdown inherently means "safe" is false. The events in the nuclear power plants, their investigation and evaluations regarding shutdown risk clearly show that the core-damage frequency for shutdown operation can be a substantial fraction of the total core-damage frequency.

The findings related to shutdown risks can be divided into following categories:

a) outage programs and planning,
b) conduct of outage,
c) residual heat removal capability,
d) rapid boron dilution,
e) containment integrity,
f) fire protection during shutdown,
g) electrical equipment.

The main focus is on the conduct of outage which comprises: a) the appropriate technical specifications and abnormal operating procedures applicable during the shutdown, b) the plant and hardware configurations such as fuel off-load, venting of the RCS, on-site and off-site electrical power supply and instrumentation.

The selected items such as defueling versus fuel shuffle, electrical diesel generator window timing, reduced inventory, RHR sump isolation and operator response were quantified in the Probabilistic Shutdown Safety Assessment. These results are presented and discussed.

The operator training is very important although in the above classification has not been pointed out as separate finding. It could be included in the conduct of the outage, but the preparedness of the operators to cope with the abnormal situation during the shutdown is invaluable. The proper training can not be limited solely to simulator training, because some situations require the appropriate actions which should be taken outside the control room.

2.0 Outage Programs and Planning

The longest time the reactor is in shutdown is during the outage, therefore special attention should be devoted to outage programs. Programs for conducting the outage should comprise:

- prudent, practical and well-documented safety principles and practices,
- organization dedicated to updating and improving the program,
- strong technical input to the program from onsite nuclear safety review group (e. g. meticulous review and safety evaluation of important modifications, review of new procedures),
- controlled program manual,
- training on the program and program manual.

In some cases safety is based upon individual approaches rather than being clearly defined in a management directive. Good safety principles include:

- minimized time of reduced inventory (e. g. midloop operation),
- introducing additional pathways of adding water to reactor coolant system,
- increase availability of different support systems with shortening the maintenance time or selective scheduling (maintenance performed on one support system at the same time).

Certain areas require more in depth consideration during the outage, such as instrument air, steam generator availability, d. c. power supply systems, gravity feed and use of firewater.

One interesting safety practice is "train outage" concept, which consists of removing one entire train out of service, all maintenance work is performed on that train (e. g. on valves, pumps, instrumentation, power supply, electrical motors, mechanical supports), but the other train remains operable (no work is allowed on it). Other safety practices can be summarized in the following:

- no single failure of an active system or component will result in loss of residual heat removal,
- add one injection system or train to that required by technical specifications,
- provide as many important systems as possible (e. g. power supplies, batteries, pumps),
- always have at least one emergency core cooling system available.

2.1 Conduct of Outage

Practices at conducting outages, which proved valuable in U.S. plants [1], are:

- place personnel with operations backgrounds into key positions and areas for planning and conducting outages - the organization during the outage should be changed that way to emphasize the operations experience for outage positions at all levels,
- conduct team meetings immediately after completing significant tasks,
- protect critical equipment (e.g. by roping off the areas of the operable train and/or identifying the operable train in each daily plan),
- rely on the people experienced in previous outages, which applies to the utility personnel, and to subcontractors as well,
- use of task forces to reinforce the work on critical path tasks or near-critical path tasks,
- introducing periodic reviews during outages (e.g. specialized meetings, outage schedules regularly updated, critical path scheduling).

2.2 Residual Heat Removal Capability

The statistics of loss of shutdown cooling in U.S. plants [1] showed that about 60 percent of the

events in PWR plants could be attributed to human error and about 16 percent are related to equipment problems. Loss of shutdown cooling could be due to the loss of RHR flow or due to the loss of intermediate or ultimate heat sink or both.

The regulatory requirements can in general be divided into two categories: design requirements and operational requirements. The regulatory design requirements are contained in general design requirements, the primary source of operational requirements are technical specifications for individual plant, therefore the technical specifications for shutdown modes are presented in Table 1.

Table 1 : The technical specifications of the PWR in the low power and shutdown modes are mode dependent (for the four-loop plant)

	reactor coolant loops required	RHR loops required	steam generators
hot standby	2	*	*
hot shutdown	any combination of two loops		*
cold shutdown	*	2	if two S/G are filled to at least 17% of the normal level, then two S/G and one RHR loop is acceptable comination

For the Krško NPP (two loop Westinghouse PWR) the technical specifications for residual heat removal can be summarized:

(a) in mode 3 (hot standby):
* if the reactor trip breakers closed: both reactor coolant loops shall be operable,
* if the reactor trip breakers open: at least one reactor coolant loop shall be in operation (i.e. reactor coolant loop with its associated reactor coolant pump and steam generator)

(b) in mode 4 (hot shutdown):
- at least one of these combinations shall be operable and one of the loops shall be in operation:
  * two reactor coolant loops
  * two RHR loops
  * anyone reactor coolant loop and anyone RHR loop.

(c) in mode 5 (cold shutdown) with reactor coolant loops filled:
* at least one RHR loop shall be operable and in operation and one additional RHR loop shall be operable,
* at least one RHR loop shall be operable and in operation and the secondary side water level of at least one steam generator shall be greater than 35% narrow range.

(d) in mode 5 (cold shutdown) with reactor coolant loops not filled:
* two RHR loops shall be operable and at least one RHR loop shall be in operation.

(e) in mode 6 (refueling):
* water level above the top of the reactor vessel flange is greater or equal to 7 m: at least one RHR loop shall be operable and in operation,
* water level above the top of the reactor vessel flange less than 7 m: two RHR loops shall be operable and at least one RHR loop shall be in operation.

Some of the references (e. g. [1]) support the premise that current standard technical specifications for PWR reactors are not detailed enough to address the risk significance of reactor coolant system configurations used during cold shutdown and refueling operations.

Safety margin during the shutdown is related to time it takes to uncover reactor core. The proposal to improve the technical specification would include the sensitive conditions, such as midloop or reduced inventory.

Decay heat in PWR during startup and shutdown is removed through steam generators by dumping steam to condenser or to atmosphere. The boiled off water is replaced with the auxiliary feedwater (AFW) system. Due to the high reliability of the AFW system the losses of decay heat removal capability during the startup and shutdown transition modes are not frequent. But, there are many more events with the loss of decay heat removal during shutdown and refueling.

Maintaining high reliability of the decay heat removal the following should be addressed:

- if the procedures specify the use of steam generators or ECCS as the alternate methods for removing decay heat. The steam generator availability shall be maintained and a clear flow path through the containment sump shall be planned for,
- core temperature can not be obtained from readings of the RHR instruments if RHR pumps are not running,
- alternate residual heat removal methods:
  * in most PWRs the drain path between the refueling storage tank and the RCS can be established - the elevation difference between the RCS and the RWST determines the actual amount of water, which can be provided to RCS,
  * gravity drain from the accumulators can provide gained time in terms of hours if the event happens few days after shutdown. Due to limited amount of water this flowpath is negligible in terms of long term cooling.
  * reflux cooling requires that the steam produced by core boiling reaches condensing surfaces of the steam generator U-tubes.

Studies (NUREG/CR-5820, referenced in [1]) have been performed to determine the core uncovery due to the failure of the hot-leg nozzle dam with the manway on steam generator removed. The assumed pressure to cause nozzle dam failure was 25 psi. The results showed:

* RCS peak pressure is insensitive to decay heat level or to the time of loss of RHR system following shutdown,
* at the use of steam generators for RHR the RCS peak pressures approach 80 psig with initial RCS water level above the top elevation of the hot leg. At these levels the liquid (i.e. reactor coolant) fills the U-tubes high enough to prevent residual heat removal until pressure difference reaches 80 psig or sufficient primary to secondary temperature difference is established.
* the loss of the RHR system with the initial RCS water level above the top of the hot leg and using steam generators as the alternative means of decay heat removal may cause high enough pressure to jeopardize the integrity of temporary boundaries in the RCS
* the failure of RCS temporary boundaries and loss of the RHR capability in the first 7 days after shutdown may leave very little time to prevent core uncovery (i.e. about 30 to 90 minutes)

Generic Letter 88-17 [2] recommendations, besides training, procedures improvement and administrative controls, require:

- two independent, continious temperature indications that are representative of the core exit conditions whenever the reactor is in midloop operation and reactor head is located on top of the vessel,
- at least two independent, continious reactor coolant system water level indications whenever the RCS is in a reduced inventory condition,
- at least two available or operable means of adding inventory to the RCS in addition to the pumps that are a part of the normal decay heat removal systems.

2.3 Rapid Boron Dilution

The concern related to rapid boron dilution is fuel damage due to the power excursion caused by the slug of diluted water passing through the core. In general this process can be split into two stages:
(a) unborated or diluted water enters the primary system, which is normally borated. This diluted water is then assumed to accumulate without significant mixing.
(b) the startup of a reactor coolant pump pushes the slug of diluted water through the core.

The review and analysis of rapid boron dilution events indicates that core damage may occur for assumed extreme sets of parameters (e. g. reducing boron concentration in a slug from 1500 ppm to 750 ppm - [1, p.6-20]) and may occur with a frequency of the order 10E-5 per reactor year. The boron dilution accidents can be avoided by using of appropriate procedures anticipating the possibility of dilution in various situations and to prevent the inappropriate starting of the pumps until mixing is carried out.

2.4 Containment Integrity

The containment integrity has to be addressed during the shutdown due to the following:
- for Westinghouse four-loop PWR the loss of RHR during midloop can lead to boiling in 8 minutes, and the reactor vessel level can reach the top of the active fuel in 50 minutes since the boiling began,
- the retention factor of the containment is substantial [1]: the estimated dose from a core melt two days after shutdown with an open containment is approximately 800 Sv to the thyroid and 2 Sv whole-body at a one mile distance from the plant. A closed containment assuming 24-hours holdup and design leakage can reduce the dose to 2 mSv to the thyroid and to 10 microSv whole-body.

It is important that the working conditions in the containment can become extremely degraded after the loss RHR:
- the air temperature in the containment can rise from 20°C to 75°C in approximately one hour (the air at about 80 °C is hot enough to burn the lungs,
- boiling of reactor coolant would release dissolved fission products into the containment atmosphere and high radiation alarms would be actuated. It is very likely that people could have been evacuated before performing any operation required to close the containment, if the reactor coolant is not cleaned as required.

Therefore, the licensee has to address the containment work environment if it is planned to close the containment while steam is being released into containment.

2.5 Fire Protection during Shutdown

The potential fire could damage one or both trains of decay heat removal systems during shutdown. This situation could further deteriorate the plant's ability to remove decay heat. An increase of fire hazards during the shutdown should be noted and properly addressed. These fire hazards can include temporary wiring, transient combustibles (e.g. plastic sheeting, wood scaffolding, lubricants, cleaning goods, paper and rubber products) and increased welding activities. The most of the documents related to fire protection does not reflect the specific requirements during shutdown (e.g. Standard Review Plan, 10 CFR 50 - Appendix R). The fire protection personnel in the plants are usually overloaded with paper work related to maintenance or modifications during outage, therefore the fire prevention activities are minimized.

2.6 Electrical Equipment

During the outage the unusual electrical lineups exist and the equipment unavailability due to maintenance is high, therefore it is likely that single failure can disable two trains at the same time. The ac power is vital to the most of systems to be in operable status and the practices to provide the ac power in shutdown can be [1]:

- provide one emergency diesel generator (EDG) and one source of off-site power,
- always have three sources of power, one of which is EDG,
- have both EDGs operable when in midloop operation,
- allow both EDGs to be out of service when the fuel is off-loaded,
- for midloop operation: two EDGs and two off-site sources or at least one EDG and two off-site sources,
- have at least three separate ac power sources available to vital buses any time two RHR pumps are required operable.

3.0 Probabilistic Safety Shutdown Analysis - Selected Cases

Some cases of a Probabilistic Safety Shutdown Analysis for a particular power plant [3] are addressed in this section to outline the importance of assessing the shutdown risk to achieve outage plan with minimal risk to the population.

Base case represents the typical outage and all other cases are just variations of this base case. The ratio between the RCS boiling risk and the core damage frequency is 0.0138, therefore the boiling in the RCS is approximately 70 times more likely than core damage. The leading contributor to RCS boiling risk is loss of running RHR pump, which becomes of lesser importance at core damage, because the core damage takes more time, thus allowing for the repair of the RHR pump. The leading contributors to core damage frequency are simple RHR isolation event (loss of suction), loss of offsite power/SBO event and loss of ac bus to running RHR pump.

Very important factor to core damage risk during the refueling period is RCS vent. If the large RCS vent is opened, the fill and spil mode of gravity feed from the RWST is enabled, thus reducing the core damage risk for 60%.

(a) Case #1: Defueled Reactor Vessel versus Fuel Shuffle

- same as the base case except:
  - * flooded up window is extended to only one long window,
  - * EDG work will be coincident and non coincident with the fuel movement.
- the dominating initiating event to core damage risk is loss of ac bus to runnung RHR pump, because it is assumed, that only one dc train was available before the loss of ac bus. The core damage frequency is approximately 60% larger in the fuel shuffle case than at the defueled reactor vessel.

(b) Case #2: EDG Work Window Timing

- the work on EDG is prolonged for 14 days (e.g. for 4 days on the EDG #1, and for 10 days on EDG #2). The EDG outage is performed consecutively, because the technical specifications do not allow coincident outage.
- the increase of the core damage frequency in this case is negligible - only 4%, what would have been different in case the typical outage had not comprised defueled reactor.

(c) Case #3: Reduced Inventory

- these case is split into two:
  #3a - entrance to midloop condition is delayed for 3 days,

#3b - duration of the first midloop condition is prolonged for 3 days.

- Case #3a decreases core damage frequency for 50%, which suggests that the entrance to midloop condition is very sensitive to the time after shutdown of reactor (i. e. to the decay heat produced in the reactor).
- Case #3b increases core damage frequency for 50%, what brings us to the conclusion that 6 days of extra midloop operation has equal risk for core damage as all the activities performed during typical outage.
- the leading contributors to core damage are the same in both cases (#3a and #3b): loss of ac bus for running RHR pump, loss of offsite power/SBO event and simple RHR isolation event.

(d) Case #4: Operator Responses

- ranking the operator actions in terms of their contribution to core damage risk had been performed and the results are in the following order: isolation of RHR (LOCA event in RHR), implement gravity feed from the RWST, initiate alternate decay heat removal, makeup to the RCS for LOCA events (using SI or charging - this was quantified separately, although could be included into alternate decay heat removal).
- the non response to the above actions actually contributes to core damage frequency and is in all cases at least one order of magnitude larger than in anyone of the previous cases. This results reflect the importance of the operator prompt and efficient response, thus appropriate training resources should be provided.

4.0 Operator Training

The shutdown risk issues should be reflected in the training program for a specific outage and for the operator licensing program.

The outage training program shall be completed before the outage and can comprise:

- new or revised procedures for the outage,
- refresher on the abnormal procedures which are related to the outage (e.g. alternate means of decay heat removal),
- use of specific equipment: fuel handling tools, principles of instrumentation operating only in shutdown modes, communication between the reactor building and control room.

The operator licensing program shall include standards for the initial examination of at least one job performance measure related to shutdown and low-power operations and for the requalification exam test the shutdown and low-power operation shall be comprised.

5.0 Conclusions

The shutdown risk can contribute a substantial fraction of the overall core damage risk, therefore it has to be properly addressed. The steps have been taken to determine initiating events and to quantify the risk contribution of each event, but it does not seem that this issue is concluded. The NPP personnel must pay attention round-the-clock to the fact that "shutdown does not automatically mean safe". The Nuclear Safety Committee in each power plant is in the forefront to boost the Safe Shutdown Program, which considers the outage planning, shutdown risk studies and administrative controls. Enough support has to be given to the teams reviewing events during the shutdown. Action plans to prevent consecutive similar events have to be determined and implemented as a separate program or in the framework of "operating experience feedback program". Indoctrination of the NPP personnel, and even more important for the subcontractors, has to be performed for the workers of all ranks. The workers have to be stimulated for their active and effective contribution to safety. The incidents during shutdown still happen [4], although many actions have been taken to prevent them, therefore during the

shutdown the personnel should be aware of specific risks and to be on watch for them all the time.

References

[1] NUREG-1449, Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States, Draft Report for Comment, February 1992

[2] Generic Letter 88-17, Loss of Decay Heat Removal, October 17, 1988

[3] NPP Krško Probabilistic Shutdown Safety Assessment, Final Report, ERIN Engineering and Research, Inc., May 1994

[4] NRC IN 96-37: Innacurate Reactor Water Level Indication and Inadvertent Draindown during Shutdown, June 18, 1996