Developing a Low Power/Shutdown PRA for a Small Modular Reactor

Nathan Wahlgren
NuScale Power, LLC, Corvallis, OR, USA

Abstract: A growing area of interest in the field of nuclear risk analysis is the application of PRA techniques to low power and shutdown configurations when the availability of systems and components may differ significantly from normal operation. Many operating plants have performed (or are in the process of performing) a PRA for low power operations, and new reactor designs are required to complete one as part of the design certification process.

NuScale Power is developing a natural-circulation small modular reactor, and certain features of the design require refueling and maintenance procedures different from any in the industry. This uniqueness eliminates some sources of risk traditionally addressed in a shutdown PRA, but also introduces entirely new areas of risk. One major challenge is that all modules in the plant share a common refueling area, so each module must be lifted and moved from its operating location with fuel in the core. The module is completely disconnected and most systems credited in the full power PRA are unavailable when the module is in transit.

This paper will give an overview of NuScale's design and refueling process and discuss some of the challenges involved with developing a shutdown PRA for a reactor that is designed to be moved with fuel assemblies in place. Special attention is paid to determining a failure probability for a single-failure-proof crane with little directly applicable publicly available data.

Keywords: PRA, Low Power/Shutdown, Nuclear, Small Modular Reactor, NuScale

1. INTRODUCTION

NuScale Power, LLC is developing a small modular reactor that seeks to incorporate proven light water reactor technology with revolutionary design concepts to provide a modular approach to nuclear power that is both innovative and exceedingly safe. The design draws upon proven technology and materials while incorporating new design features to enhance operability and safety.

2. NUSCALE DESIGN OVERVIEW

A NuScale module is a self-contained assembly composed of a reactor core, a pressurizer, and two steam generators integrated within the reactor pressure vessel and housed in a high-pressure compact steel containment vessel. Each module uses traditional light water reactor fuel assemblies to produce 160 MWth, and a dedicated steam turbine to produce 45 MWe (net). Coolant flows through the RPV by natural circulation, with no reactor coolant pumps required for either normal operation or shutdown cooling.

A NuScale plant combines 12 reactor modules into a common reactor building to produce a total of 540 MWe (net). Each module operates independently, but all modules are managed from a single control room. The modules are submerged in a below-grade reactor pool that includes the spent fuel pool and a common refueling area. The pool functions as the ultimate heat sink for the backup cooling systems and also provides radiation shielding.

2.1. Safety Systems

Safety cooling systems are passively operated and can be passively actuated, with no power required for either function. The containment vessel on a NuScale module is a high-pressure steel vessel that functions as an integral part of the safety systems, conducting heat to the surrounding reactor pool using the simple physical processes of convection and conduction.

The decay heat removal system is analogous to the auxiliary feedwater system in a traditional plant, providing cooling through the steam generators when normal feedwater is not available. Valves on the main steam and feedwater lines redirect the flow of secondary coolant from the steam generators through a pair of closed loop two-phase heat exchangers mounted on the outside of the containment vessel, with the reactor pool acting as heat sink. Each heat exchanger is independent and capable of removing 100% of reactor decay heat.

NuScale's emergency core cooling system is unique to the industry, providing passive cooling in the event that normal feedwater and both trains of the decay heat removal system are unavailable. Steam exits the RPV through vent valves in the head of the RPV, condensing on the inside of containment and collecting in the bottom of the containment vessel. Recirculation valves mounted on the side of the RPV allow water to flow back into the RPV and are positioned at a height that maintains the water level in the core above the top of active fuel. The coolant in containment is cooled by the containment conducting heat directly to the reactor pool.

The volume of the reactor pool is sufficient to provide cooling for thirty days, by which time the decay heat has been reduced to a low enough level to allow the module to be air-cooled indefinitely. The emphasis on passive cooling, combined with a large volume of water in the ultimate heat sink, allows a NuScale plant to safely shut down and indefinitely maintain cooling with no operator action, no AC or DC power, and no additional water.

The emphasis on passive safety systems has enabled NuScale to achieve a Level 1 core damage frequency (CDF) for internal events less than 1E-7 per module critical year. Analyses of Level 2 and Level 3 internal and external events are currently ongoing.

3. REFUELING PROCEDURE

The unique design of a NuScale plant requires a refueling procedure different from any in the industry. The most obvious difference is that modules are not refueled in place, requiring that modules be transported while fueled. In addition, water is never removed from the RPV, eliminating drain-down events, and the reactor pool ensures that the module never occupies a condition that could be consider mid-loop. Cooling throughout the refueling procedure is maintained by the reactor pool, first by conduction through the containment vessel, and then by direct submersion when the RPV is opened. The planned refueling cycle for one module is 24 months, with outages staggered to allow other modules in the plant to continue operating.

After shutdown, the module is cooled using normal secondary cooling, then the containment is flooded and the reactor vent and recirculation valves opened to establish passive cooling by convection and conduction to the reactor pool. The module is lifted from its operating bay using a single-failure-proof (SFP) crane and transported to the refueling area, where it is disassembled. The lower portion of the containment vessel and RPV, including the core, remain in their stands in the refueling area while the upper vessels are transported to a dry dock area for maintenance and inspection.

3.1. Single-Failure-Proof Reactor Building Crane

The Nuclear Regulatory Commission (NRC) requires an SFP crane be used when lifting critical loads; a critical load is defined as a load that can be a direct or indirect cause of a release of radioactivity [1]. This is not limited to loads that contain radioactive material, but also loads that are lifted over or transported above safe shutdown equipment, where dropping a heavy load may damage systems or components relied upon to prevent core damage. A NuScale plant is laid out in such a way that modules do not pass over safe shutdown equipment at any time, eliminating that source of risk and leaving only the possibility of damage incurred by dropping the module.

General requirements for SFP cranes are given in NUREG-0554, Single-Failure-Proof Cranes for Nuclear Power Plants [1]. The criteria are that the system be designed so that a single failure will not result in the loss of the capability of the system to safely retain the load. Also required is that the crane must retain control of the load upon loss of electrical power and allow it to be lowered in a controlled manner. This is accomplished with a combination of redundant components, large safety margins, and rigorous procedures for both operation and maintenance.

4. DEVELOPING A LOW POWER/SHUTDOWN PRA

The low power/shutdown (LP/SD) PRA is a required part of the application for design certification, and an important tool in understanding risk present during refueling procedures, especially for a plant with no operating experience. The process involves identification of plant operating states, a screening process for existing initiating events, identification of new initiating events, modification of existing event trees and addition of new ones to construct a model that accurately depicts the module configuration during refueling operations.

4.1. Plant Operating States

It is standard practice for an LP/SD PRA to define a plant operating state (POS) for each configuration that occurs during an outage. Each POS has distinct initiating events, each with its own event tree. NuScale's LP/SD includes a POS for initial cooling, cooling with flooded containment, module disconnection and reconnection, transport to and from the refueling area, module disassembly and reassembly, and restart; the event trees are populated with systems that are available during that POS.

4.2. Initiating Events and Initiating Event Frequency

Initiating events for the LP/SD PRA are identified as those events that will cause a disruption to the critical safety functions of decay heat removal, coolant inventory, or reactivity control and require a response, either automated or by operators, to restore the stable condition of the plant.

When normal secondary cooling is taken offline, initiating events such as loss of feedwater, loss of condenser heat sink, and steam generator tube rupture can be screened out. Loss of coolant inside containment events can be screened out once containment is flooded, and loss of coolant outside containment events can be screened when active systems are removed from service and the containment is isolated. At this point the module is in cold shutdown, effectively immune to effectively all internal initiating events, including internal fires, internal floods, and loss of power. The module can occupy this state indefinitely without electrical power or further action from operators.

4.2.1. Initiating Event Frequency

For initiating events from the Full-Power PRA that are applicable to one or more POSs, a simple unit conversion is used to adjust the frequency. The adjusted frequency is used to account for the amount of time the frequency and duration of the POS, and also converts from units of per reactor critical year to per calendar year. The uncertainty distributions and parameters are not changed. The following equation is used to perform the adjustment:

$$f_{\mathrm{LP}} = \frac{f_{\mathrm{FP}}}{\mathrm{CF}} \times f_{\mathrm{POS}} \frac{d}{8760}$$

Where

f_{LP}	low power frequency, per calendar year
f_{FP}	full power frequency, per reactor critical year
CF	module capacity factor, dimensionless
f_{POS}	frequency with which module enters POS, per calendar year
d	duration of POS, hours

For conservatism, the initial value of the module capacity factor is taken to be 0.844, the industry average for 2012* as calculated from the NRC's plant status data [3]. The f_{POS} term is estimated as the sum of the frequency of controlled shutdowns plus the refueling outage frequency, accounting for the fact that certain POSs will be applicable during each shutdown while others only apply to a refueling outage.

Representative frequency calculations are shown in Table 1 for three initiating events for POS1 (initial cooldown), POS2 (cooling with flooded containment), and POS7 (restart). For the purposes of this calculation, full-power frequencies are taken from generic values from the NRC Operating Experience Database [4] and expressed in units of per reactor critical year (rcry),. Two of these events are not applicable during POS2, as during that POS the module does not rely on secondary cooling or any system that requires electrical power.

Table 1: Sample Frequency Calculation for Initiating Events

Initiating Event	POS	Duration (hours)	f_{FP} (per rcry)	f_{POS} (per year)	f_{LP} (per year)
LOCA outside containment	1	10	3.67E-4	2.5	1.24E-6
Loss of secondary cooling	1	10	1.28E-1	2.5	4.33E-4
Loss of offsite power	1	10	6.14E-2	2.5	2.08E-4
LOCA outside containment	2	15	3.67E-4	1.5	1.12E-6
Loss of secondary cooling	2	15	1.28E-1	1.5	N/A
Loss of offsite power	2	15	6.14E-2	1.5	N/A
LOCA outside containment	7	20	3.67E-4	2.5	2.48E-6
Loss of secondary cooling	7	20	1.28E-1	2.5	8.65E-4
Loss of offsite power	7	20	6.14E-2	2.5	4.15E-4

4.3 Event Trees

Event trees in the LP/SD PRA are based on event trees in the Full Power PRA, especially for existing initiating events that are applicable to one or more POSs. The major change for all shutdown POSs is the removal of sequences that include a failure of the control rods to shut down the module. Several other changes are implemented to ensure that the top events reflect only those events that are applicable to the POS. For example, the definition of POS2 is that the containment is flooded with the vent and recirculation valves open; since opening these valves actuates the emergency core cooling system, any sequence that includes a failure of the emergency core cooling system to actuate are removed.

Quantifying the modified event trees for all POS not involving module transport gives a CDF that is approximately two orders of magnitude lower than that of the Level 1 PRA.

4.4. Reactor Building Crane in the LP/SD PRA

Due to the role that the crane plays in a NuScale plant, it is receiving special attention from both design and safety analysis engineers. Crane failure has been added to the LP/SD PRA as an initiating event, though the associated event trees are still in preliminary form as analyses of the potential effects of a crane failure are still in development.

* Although NuScale plants have no operating history, the design, including the power conversion system, is far simpler than existing design and therefore not subject to many of the upset events that can disrupt operations in the more complex plants that are currently operating. The industry average is therefore expected to be conservative.

4.4.1 Crane Failure Probability Estimation

The crane failure probability is estimated using operating experience data for cranes, which is compiled in NUREG-1774, A Survey Of Crane Operating Experience At U.S. Nuclear Power Plants From 1968 Through 2002 [2]. Cranes at nuclear power plants are used so frequently that it is difficult to find data of the total number of lifts performed, but the category of loads classified as "very heavy" (greater than 30 tons) was studied more closely by the authors of NUREG-1774; with a weight in excess of 500 tons, a NuScale module is certainly in this category. It was estimated that 54,000 very heavy load lifts were performed at nuclear power plants between 1980 and 2002, during which time nine failure events (six load slips and three load drops) were recorded. Note that most of these failures did not occur in SFP cranes.

Calculating a point estimate with these data gives a failure probability of 9/54,000 = 1.67E-4 per lift, however this is not a good indication of the failure rate of NuScale's crane. The narratives of the nine failure events suggest that none of the events are directly relevant to the NuScale design, due to the fact that the cranes involved in most of the failures were not SFP, or temporary rigging straps were not connected properly or failed, or the load was not dropped. A load drop caused by the mechanical failure of a single component in the temporary rigging system is not credible for NuScale crane due to the single-failure-proof crane and the dedicated coupling mechanism it uses to interface with the module, whereas a load dropped by a SFP crane caused by human error is more relevant.

A weighting system was developed to adjust each failure event for relevance. The narrative of each event was used to identify the consequence (slip or drop), the cause (human error, mechanical failure, or rigging), and the crane used (SFP or non-SFP). A weighting factor was assigned to each category, and the product of these weighting factors was used as the equivalent number of failures for that event. The sum of all nine equivalent failures is used to calculate the failure probability.

Weighting factors were determined by engineering judgment. A slip is assigned a consequence factor of 0.5, implying that two load slips have the same impact as one drop. A drop is assigned a consequence factor of 1.0. Human error is assigned a cause factor of 1.0, and mechanical and rigging failures are each assigned a cause factor of 0.1. The crane is designed to prevent mechanical failures from causing a drop, and the module is lifted with a purpose-built and permanent rigging device that attaches to the same points on the module each time, eliminating the need for temporary moveable rigging that is reattached at each lift. A failure involving a non-SFP crane is assigned a crane factor of 0.1 and those involving an SFP are assigned a crane factor of 1.0. By this system, the most relevant events will be counted as one failure, with each factor reducing the worth to less than that of a full failure.

The weighting factors are shown in Table 2 and application to the operating experience data is shown in Table 3.

Table 2: Weighting Factors for Crane Failure Events

Consequence	Factor	Cause	Factor	Crane	Factor
Slip	0.5	Human	1.0	SFP	1.0
Drop	1.0	Mechanical	0.1	Non-SFP	0.1
		Rigging	0.1		

Table 3: Applying Weighting Factors to Operating Experience Data

Date	Plant	Consequence	Cause	Crane	Equiv. Failures
11/1985	St. Lucie 1	Slip	Mechanical	Non-SFP	0.005
4/1990	Fort Calhoun	Slip	Rigging	SFP	0.050
9/1993	Arkansas Nuclear One 1	Slip	Human	SFP	0.500
12/1997	Byron	Slip	Human	Non-SFP	0.050
10/1999	Comanche Peak	Slip	Mechanical	Non-SFP	0.005
11/1999	Crystal River 3	Slip	Rigging	SFP	0.050
12/1997	Byron	Drop	Human	Non-SFP	0.100
5/2001	San Onofre	Drop	Rigging	Non-SFP	0.010
6/2001	Turkey Point 4	Drop	Rigging	Non-SFP	0.010
				Total	0.780

The 0.780 equivalent failures are used to estimate a failure probability of 0.780/54,000 = 1.44E-5 per lift, reducing the original estimate by an order of magnitude to approximately one failure is 70,000 lifts.

The uncertainty for this event is assigned a lognormal distribution with a error factor of 10 to account for the uncertainty in engineering judgment. OpenBUGS was used to perform uncertainty sampling calculations, resulting in a 90% confidence interval of 5.37E-7 to 5.38E-5, as shown in Table 4; the script used to generate these numbers is given in the Appendix.

Table 4: Summary of Uncertainty Sampling

Mean	Standard Deviation	5% Value	Median	95% Value
1.437E-5	3.411E-5	5.368E-7	5.383E-6	5.350E-5

4. CONCLUSION

NuScale's innovative design has proven to be exceedingly safe in the realm of normal operations, and the preliminary LP/SD analysis indicates the refueling process can be executed safely as well, with the CDF due to internal events approximately two orders of magnitude below the full power CDF. Future work will involve a more detailed examination of the crane that incorporates the results of analyses currently underway, as well as an expansion of the LP/SD PRA to include internal fires, internal floods, and external events.

APPENDIX

OpenBUGS script used to perform uncertainty sampling. The script was written by Sara Misic of NuScale Power, LLC.

```
Component : Crane
Failure Mode: Crane failure
Model: Lognormal distribution fit to data with error factor = 10
Analyst: Sara Misic
Date: 02/03/2014

Model {
lambda ~ dlnorm(mu, tau)
mu <- log(1.44E-5) - pow(log(EF)/1.645,2)/2
tau <- pow(log(EF)/1.645,-2)
}

Data
list(EF= 10)

end
```

References

[1] U.S. Nuclear Regulatory Commission, "Single-Failure-Proof Cranes for Nuclear Power Plants," NUREG-0554, May 1979.
[2] U.S. Nuclear Regulatory Commission, "A Survey Of Crane Operating Experience At U.S. Nuclear Power Plants From 1968 Through 2002," NUREG-1774, July 2003.
[3] U.S. Nuclear Regulatory Commission, *Power Reactor Status Reports for 2012*, 1/30/2014, http://www.nrc.gov/reading-rm/doc-collections/event-status/reactor-status/2012.
[4] U.S. Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, February 2007 (2011 data update).
[5] NuScale Power, LLC, *NuScale Power Technology*, 2/3/2014, http://www.nuscalepower.com/ourtechnology.aspx.