Characterizing Previously Unknown Dependencies in Probabilistic Risk Assessment Models of Nuclear Power Plants

John David Hanna

Region III Office, US Nuclear Regulatory Commission, USA. E-mail: john.hanna@nrc.gov

The US Nuclear Regulatory Commission (NRC) maintains a set of Level-1 probabilistic risk assessment (PRA) models, called standardized plant analysis risk (SPAR) models, which are the analytical tools used by the agency to perform risk assessments. The SPAR models include elements of the initiating events (IE), mitigating systems (MS) and to a limited extent barrier integrity (BI) cornerstones.

Over the last 10 to 15 years, several events have occurred at nuclear power plants (NPPs) in the US which had substantial risk and where multiple cornerstones were simultaneously affected. The risk insights from these domestic events may indicate an existing completeness uncertainty, specifically that there are 'dependencies' between certain initiating events and availability/reliability of mitigating systems which are not currently captured in the PRA models.

These previously unrecognized dependencies can be included in the SPAR models and thus captured in subsequent risk assessments. This paper will review several examples from US commercial NPPs where these dependencies manifested themselves and demonstrate that the risk of lower intensity events (far less than a beyond design basis event) can be significant. Further, this paper will describe potential PRA modeling improvements and provide insights that may lead to modifications to existing procedures, plant structures, systems & components such that the previously unmeasured risk might be lowered, providing a benefit to public health and safety.

Keywords: nuclear power, dependency, external event, PRA, 'sunny day' event, Fukushima Dai-ichi.

1. Introduction

The US Nuclear Regulatory Commission (NRC) maintains a set of Level-1 probabilistic risk assessment (PRA) models, called Standardized Plant Analysis Risk (SPAR) models, which are the analytical tools used by the agency to perform risk assessments. The SPAR models, similar to the PRA models used by owners/operators of nuclear power plants (NPPs), include elements of the initiating events (IE), mitigating systems (MS) and to a limited extent barrier integrity (BI) cornerstones. These PRA models will occasionally represent complex scenarios that affect two or more of these cornerstones (e.g., a loss of component cooling water (CCW) simultaneously results in an initiating event and an impact on a mitigating system); however, the cornerstones are usually treated independently.

Over the last 10 to 15 years, several events have occurred at NPPs in the US which had substantial risk and where multiple cornerstones were simultaneously affected. (An extreme international example of this 'dependency' is the case of Fukushima Dai-ichi in Japan on 11 March, 2011 where the initiating external event affected mitigating systems, as well as barrier integrity and emergency preparedness (EP) via the impact to evacuation routes.) The risk insights from these domestic events may indicate an existing completeness uncertainty, specifically that there are 'dependencies' between certain initiating events and availability/reliability of mitigating systems which are not currently captured in the PRA models. These accident precursors remind us of the need to re-examine the fundamental assumptions used in risk analysis.

The SPAR models are maintained, frequently exercised by analysts within the agency, and are used to inform regulatory decisions. According to Regulatory Guide 1.200, PRA models need to have the appropriate scope, level of detail, and technical acceptability. (1) The NRC's 1995 PRA policy statement specified that PRA evaluations supporting regulatory decisions should be as realistic as practicable. (2) Consistent with this realism principle, these previously unrecognized dependencies can be included in the SPAR models and thus captured in subsequent risk assessments. This paper will review several examples of events and/or conditions from the US commercial NPPs where these dependencies manifested themselves and demonstrate that the risk of lower intensity events (far less than a beyond design basis event) can still be significant. Further, this paper will describe potential PRA modeling improvements and provide insights that may lead to modifications to existing procedures, plant structures, systems & components such that the previously unmeasured risk might be lowered, providing a benefit to public health and safety.

2. PRA Modeling and Limitations

The SPAR models have event trees that are created to delineate possible sequences of successes or failures of systems/functions that lead to specific endstates, (e.g., a safe/stable condition, or core meltdown and/or the release of radionuclides). Fault trees are used to estimate the failure probabilities of those systems/functions using information such as data on the reliability of components, common-cause failure likelihood or human error probabilities (HEPs). Using these techniques, thousands of possible core damage accident sequences are assessed for their likelihood.

Some IEs modeled in PRA models are clearly linked to mitigating systems (e.g., a loss of offsite power (LOOP) by definition removes the normal source of electrical power to the nuclear plant). However, for many initiating events, the potential failures of mitigating systems and barrier integrity are treated independently in the PRA models.

A limitation of the current PRA models is how they address ‘dependency.’ Customarily in PRA, the term ‘dependency’ is usually used to describe the commonality between two or more human actions. In other words, ‘dependency’ normally describes the relationship between action ‘A’ and the subsequently performed action ‘B.’ And factors (e.g., whether the actions were taken by the same operating crew, whether they happened “close in time” or whether there are cues to help the operator diagnose or take the appropriate action) are variables that affect the degree of ‘dependency.’ Sometimes the term ‘dependency’ is meant to convey the relationships between front-line systems and their associated support systems (e.g., emergency diesel generator dependency (EDG) on service water cooling.) However, for the purposes of this paper, a non-trivial probability relating IEs and either MS or BI will be referred to as a ‘dependency.’ This type of ‘dependency’ is distinguished from a ‘combined event’ because it is not simply two or more initiating events occurring simultaneously (e.g., strong winds and high sea water levels), but a single event that cuts through and creates additional events and losses of mitigating systems, barrier integrity, emergency preparedness, etc. Wherever possible in this paper, the effects on cornerstones will be noted (e.g., MS).

The PRA models used for US commercial NPPs possess both internal events and to some degree external events (e.g., fires, seismic, tornado/high winds, and flooding). (3,4) And while extreme external events have the capacity to create large consequences, the frequencies of those events lower the overall risk results. However, less severe events, referred to as “sunny-day events” in this paper can happen with higher frequencies and may provide less time for warning and mitigative actions to be taken. Examples, aside from those listed in Section 3 below, would include riverine flooding, not caused by dam failure or a large seismic event, that can inundate the plant and affect offsite power via the switchyard, but remains less than a beyond design basis external event (BDBEE).

3. Recent Examples

3.1. Duane Arnold derecho event

On 10 August 2020, a derecho swept through the states of Iowa and Illinois causing widespread destruction including extensive damage to the electrical grid. (A derecho is a widespread, long-lived wind storm with damage typically occurring in one direction along a relatively straight path extending for more than ~ 400 kilometers (250 miles), including wind gusts of at least 93km/h (58 mph) along most of its length, and also includes several, well-separated 121 km/h (75 mph) or greater gusts.) (5) Duane Arnold Energy Center (DAEC), a General Electric boiling water reactor-4 with a Mark 1 containment located near Cedar Rapids, Iowa experienced a reactor trip and an extended LOOP. However, though this was a severe storm, there was only 30 minutes advanced warning to the DAEC site due to the rapid nature of derecho formation. Simultaneously, the derecho with estimated wind speeds of 129-161 km/h (80-100 mph) for more than 30 minutes and gusts up to 209 km/h (130 mph), deposited significant amounts of debris and vegetation in the Cedar River. The river serves as the ultimate heat sink for the unit and is the suction source for the service water system, which provides cooling to pumps, heat exchangers and the EDGs. This debris loaded both the service water strainers to the point that one reached 103 kPa (15 pounds per square inch (psi)) differential pressure requiring it to be bypassed and the other reached 76 kPa (11 psi) differential pressure and then stabilized. This challenge to the strainers had the potential to stop cooling to both the EDGs and the other systems which maintain inventory and remove decay heat from the core in a post-accident scenario. Additional challenges to the plant were posed by the derecho in that the secondary containment was impacted and the potential, though not actual, effect on the evacuation routes. Hence this one, relatively common IE significantly impacted MS, had a minor actual impact on BI (secondary containment) and no actual, but some potential impact on EP (evacuation routes).

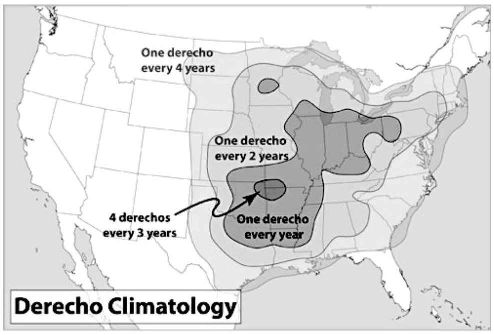

Fig. 1. Diagram of derecho frequency in the United States of America; The frequency of the derecho for the state of Iowa is in the range of once/two years – once/year.

However, it is important to note at this point that there was another layer of defense-in-depth (DID) in existence. Following the events at Fukushima Dai-ichi on 11 March 2011, the NRC issued Order EA-12-049, “Order Modifying Licenses with Regard to Requirements for Mitigating Strategies for Beyond-Design Basis External Events.” This order required all US commercial NPPs to develop diverse strategies for extended losses of alternating current (AC) power coincident with a loss of the ultimate heat sink. All licensees, including the owner/operator of DAEC came into compliance with the order. These diverse and flexible strategies (commonly known as FLEX, referring collectively to the procedures, equipment, etc.) added another layer of DID that is not reliant on existing AC power sources or the normal ultimate heat sink. The FLEX equipment at DAEC could have been deployed if the event had caused the loss of both EDGs.

The responsible NRC Regional Office performed a risk assessment in an effort to direct the inspectors who were responding to the site, and in anticipation that a review under Management Directive 8.3, “NRC Incident

Investigation Program" would be performed. (6) The incremental conditional core damage probability (ICCDP) was calculated to be approximately $2x10^{-4}$ to $2x10^{-3}$, which is one of the most risk significant events in the US since the reactor vessel head degradation issue that occurred at Davis-Besse Nuclear Power Station in 2002. (7) The Accident Sequence Precursor (ASP) analysis estimated the ICCDP to be $8x10^{-4}$. (8) The NRC evaluated the risk significance of this event for other US commercial NPPs using procedure LIC-504, "Integrated Risk-Informed Decision Making Process for Emergent Issues" and is evaluating generic correspondence to the industry on risk and operational insights. (9) It is also important to note that neither the licensee's model nor the NRC's SPAR model included high winds.

3.2. St. Lucie external/internal flooding event

On 9 January 2014 an extreme localized intense precipitation (LIP) event occurred at the St. Lucie NPP, a two unit site with Combustion Engineering pressurized water reactors (PWRs) with large dry containments. The thunderstorm was not part of a hurricane and the LIP occurred with little or no warning. The rainfall amounts are listed in Table 1 below.

Time	Cumulative Rainfall Amount
2 hours	13 cm (5 inches)
4 hours	17 cm (6.5 inches)
24 hours	19 cm (7.3 inches)

Table 1. Actual rainfall totals for Port St. Lucie on 9 January 2014.

Blocked pipes in the storm drain system within the owner-controlled area caused rainwater to backup into the Unit 1 CCW pit area. The water subsequently entered non-safety-related electrical conduits in the emergency core cooling system (ECCS) pipe tunnel. Missing flood seals in conduits then allowed water estimated to be approximately 189,000 liters (50,000 gallons) to enter the reactor auxiliary building (RAB). (10) Both units remained at 100 percent power and no safety-related equipment was submerged during the event.

The water accumulated on the lower level of the RAB, approximately 0.15 meter (0.5 feet) below mean sea level, on the level immediately above the various ECCS pumps approximately 3 meters (10 feet) below mean sea level. The upper floor is separated from the lower by means of walls, watertight doors, and isolation valves on the floor drains. These valves are designed to allow water to be admitted to the lower level such that sump pumps can then discharge them to waste hold-up tanks. During the event, the operators chose to open the drain valves in order to move the water from the upper level, to the lower so it could then be pumped to the hold-up tanks. The accumulated water on the upper level had accumulated to a depth of several inches and any increases threatened the lower portions of electrical cabinets in the area. In this scenario, both inaction and action carried some potential risk in either causing electrical shorts or flooding the ECCS pump room if isolation valve(s) failed.

A detailed risk evaluation (DRE) was performed to assess the increase in risk due to the performance deficiency (i.e., unsealed penetrations in the RAB enclosure). During the risk assessment process, the licensee performed a mass-flow balance evaluation of the RAB in order to assess the amount of rainfall necessary to overwhelm the sump drain system and/or submerge critical components. In the most limiting case, a rainfall amount of approximately 30 cm (12 inches) versus the amount experienced of 15 cm (6 inches) would have led to a submergence of all ECCS pumps. The external LIP event became an internal flooding event (IE) and threatened all the ECCS pumps (MS), the sources of inventory addition and decay heat removal.

Rainfall Amount	Exceedance Probability of Rainfall of Concern	Equipment Affected
24.5 cm (9.66 inches)	3.30E-02	One train of high pressure safety injection (HPSI) and low pressure safety injection (LPSI)
27.8 cm (10.95 inches)	1.92E-02	Both trains of HPSI and LPSI
31.0 cm (12.24 inches)	1.19E-02	Both trains of HPSI and LPSI and charging injection

Table 2. Hypothetical rainfall amounts with exceedance probabilities & equipment affected; case shown with floor drain valves open during a LOOP. The amounts & recurrence intervals are based on National Oceanic Atmospheric Administration (NOAA) data. (11)

South Florida routinely has large rainfall events (e.g., the probable maximum precipitation event = 119 cm (47 inches)) and this is reflected in the relatively large exceedance probabilities shown in Table 2. The DRE also considered the following factors: 1) various rainfall events, whether due to a LIP or a hurricane, 2) whether a reactor trip or a LOOP might occur due to the event, 3) the potential critical components and their various elevations in the RAB, 4) the HEPs for operator actions to mitigate the flood, and 5) the failure probabilities for the drain valves, especially the failure-to-close on demand. The increase in core damage frequency for the exposure time period was initially $2x10^{-5}$/year but later was estimated at $3x10^{-6}$/year, due in part to the crediting of the FLEX mitigating strategies. (12) Neither the licensee's model nor the NRC's SPAR model addressed external flooding, especially the ability of an external flood to become an internal one.

3.3. H.B. Robinson fire event

On 28 March 2010, H.B. Robinson Steam Electric Plant, Unit 2, a Westinghouse 3-loop PWR with a large dry containment, experienced a high energy arc fault (HEAF) and subsequent fire on an electrical bus. (As is usually the case with larger, more violent fires, it occurred with no warning.) An automatic reactor trip occurred due to a reactor coolant pump trip which resulted from an undervoltage condition on a non-safety related 4kV bus. The licensee responded and the first fire was extinguished at 7:05 p.m. Several other concurrent electrical failures, including a unit auxiliary transformer malfunction caused a 'unit lockout' to occur. The event had significant complexities and dependencies and because of that the event is decomposed into discrete themes below:

- The initial fire (an IE) and subsequent electrical failures caused reactor coolant pump (RCP) 'B' to lose power and this created a power-to-flow reactor trip (another IE). Following the reactor trip, an inadvertent safety injection (another IE) occurred due to low pressurizer pressure caused by an excessive cooldown due to valves on the secondary side being left open. The excessive cooldown could have challenged the integrity of the reactor coolant system (BI) through brittle fracture. This portion of the event was terminated when instrument bus '#3' was accidentally deenergized which then caused the main steam isolation valves to close.
- The event also impacted CCW and the centrifugal charging pumps (CCPs) both MS. Specifically, the fire and electrical failures caused a loss of instrument bus '#4' which caused the combined return isolation valve from the RCPs to shut, and thereby terminated seal cooling. Due to an unrelated design issue, the CCPs failed to automatically swap from the normal suction source to the alternate. As a result, the supply tank was depleted, seal injection had decreased to less than the minimum required and was at risk of being lost completely. This condition existed for approximately 17 minutes until RCP seal cooling/injection was restored. But if that had not occurred, or had happened later, an RCP seal loss of coolant accident (a joint IE and BI impact) might have occurred.
- During the transient, power was lost to the safety related 'E-2' bus requiring its associated EDG to power the bus. In an effort to restore a normal electrical alignment and transfer the bus 'E-2' off its emergency power supply and onto a normal source the reactor operators reset the generator lockout and inadvertently reenergized the fault. This created another HEAF, a fire on 4kV bus '#4,' and electrical grounds on both trains of the 125 Volt DC system (another IE). An EP Alert declaration was made for a fire lasting greater than 15 minutes. The licensee's fire brigade responded to the second fire and extinguished it.

	Mean Frequency	5% Value	95% Value
HEAF for medium-voltage electrical cabinets	2.13×10^{-3}	6.36×10^{-5}	5.93×10^{-3}

Table 3. Fire initiation frequencies for HEAFs. Note that the mean frequency is comparable to other relatively frequent events, e.g., loss of DC power (1×10^{-3} per year) or steam generator tube rupture (1×10^{-3} per year). (13)

The responsible NRC Regional Office performed a risk assessment in accordance with Management Directive 8.3, "NRC Incident Investigation Program." The ICCDP was initially calculated to be approximately 7.2×10^{-6} but was subsequently revised to 4.2×10^{-5} when the proximity to RCP seal failure became understood. (14) An NRC Augmented Inspection Team followed up on the event and assessed the operator performance and compliance aspects to the event. The ASP analysis later concluded the conditional core damage probability was 4×10^{-4}. (15) Neither the licensee's model nor the NRC SPAR model included fire at that time, but recently many models have been updated as plants have transitioned to requirements under National Fire Protection Association (NFPA)-805 code "Performance Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants."

4. Significant Attributes of these Events

Some of the risk insights that may be gleaned from these and similar examples at US commercial NPPs include the following:

- These events demonstrate that there may be unrecognized 'dependencies' where one initiating event can 'slice through' what are believed to be robust layers of defense-in-depth. The affected DID may include redundant trains within a single system, like the service water impact in Section 3.1 above, or multiple systems designed with similar purposes, as in Section 3.2 above. PRA modeling changes that add 'coupling factors' or transfers between existing event trees, e.g., LOOP and loss of service water, could address these unrecognized 'dependencies.'
- The external events of concern are occurring at infrequent but not rare intervals. The risk of these more frequent, but less intensive events may exceed the risk from BDBEE. Guidance from the US Bureau of Reclamation (who is responsible for management of many dams, powerplants and canals in the US) indicates that 'sunny day failures' may be higher contributors to risk than severe storms and seismic events. (16)
- The three examples that are the focus of this paper are considered 'sunny day' events in that little or no warning was provided, including the cases of the LIP rainfall event and the derecho.

- Note also that these events were not single IEs, but rather multiple, complex events where one event cascaded to another with a synergistic effect. While the PRA models typically approach IEs individually the actual events are demonstrating that the 'real world' does not follow these constraints. These complexities can have an impact on diagnosis which may: 1) further complicate event response, 2) stretch operator/licensee resources in ways that were not expected in emergency operating procedures, and 3) may require operators to take actions that may increase the risk in order to respond to the event, for example:
    - Admit unfiltered service water to EDGs during a LOOP event
    - Open drain valves to allow water to enter spaces with ECCS components that are important to protect
    - Re-energizing a bus for the purpose of restoring the electrical system to a normal line-up, yet ultimately causing another fire/explosion

5. Conclusion

The US commercial NPPs are managed by well-trained operators, designed with multiple layers of DID, engineered to have significant safety margins, and have feedback loops of corrective actions that seek not merely to fix short-term problems but prevent recurrence of more significant ones. However, these examples above show that there should not be overconfidence in the estimation of plant safety. They are accident precursors that remind us of the need to re-examine the fundamental assumptions used in risk analysis, and use the risk insights from PRA to monitor performance of our facilities, inform our activities (e.g., maintenance, inspection, etc.) and maintain DID.

These examples are not presented here to purport that they are representative of all recent external events or that they typify the risk increases due to owner/operator performance deficiencies at NPPs. These cases are meant to show initiating events with dependencies that simultaneously affect mitigating systems, barrier integrity, etc. can 'cut through' design basis assumptions, perceived DID, safety margins, etc. The Fukushima-Dai-ichi incident was an extreme event but should not be dismissed as an isolated episode that 'can't happen here.' These events have occurred at infrequent - but not rare intervals – and have revealed specific weakness in the DID of NPP facilities. As regulators and risk analysts we should pay attention to these lessons. Therefore, the reaction to these events should not be limited to isolated, plant specific changes alone, but the industry should consider responses that bolster those barriers to core damage for all NPPs for the long term.

References

1. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Revision 2, March 2009
2. US Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," Federal Register, Vol. 60, p. 42622 (60 FR 42622), 16 August 1995
3. ASME/ANS RA-S-2008, "Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," Revision 2019
4. US Nuclear Regulatory Commission, NUREG/CR-5042 "Evaluation of External Hazards to Nuclear Power Plants in the United States," Lawrence Livermore National Laboratory, Livermore, USA, 1998
5. Corfidi, Stephen, "About Derechos," 15 May 2018, https://www.spc.noaa.gov/misc/AbtDerechos/derechofacts.htm
6. US Nuclear Regulatory Commission, Management Directive 8.3 Analysis, "Duane Arnold Energy Center," 22 January 2021 – ML21022A415
7. NRC Inspection Report 05000346/2002-008, "Davis-Besse Control Rod Drive Mechanism Penetration Cracking and Reactor Pressure Vessel Head Degradation Preliminary Significance Assessment," 25 February 2003
8. Final Accident Sequence Precursor Analysis, "Loss of Offsite Power Caused by High Winds During Derecho," 4 March 2021, ML21056A382
9. "Duane Arnold Energy Center LIC-504 Team Recommendations," 30 March 2021, ML21084A010
10. Licensee Event Report 50-335/2014-001, Revision 1, "Internal RAB Flooding During Heavy Rain Due to Degraded Conduits Lacking Internal Flood Barriers," 12 May 2014
11. NOAA Atlas 14, Volume 9, Version 2, Precipitation Depth for Partial Duration at Hutchinson Island South, Florida, US
12. US Nuclear Regulatory Commission Inspection Report 05000335/389/2014-009, "Preliminary White Finding and Apparent Violations," 24 September 2014 – ML14267A337
13. US Nuclear Regulatory Commission, NUREG-2169, "Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database for the fire Initiating Event frequencies," US NRC, Office of Research, Washington, USA, January 2015
14. US Nuclear Regulatory Commission, Management Directive 8.3 Analysis, Revision 1, "HB Robinson," 14 April 2010
15. Robinson Final Accident Sequence Precursor Analysis – "Electrical Fault Causes Fire and Subsequent Reactor Trip with a Loss of Reactor Coolant Pump Seal Injection and Cooling," 23 September 2011 – ML112411359 (3)
16. US Department of Interior, Bureau of Reclamation, "Dam Safety Risk Analysis Best Practices Training Manual," USBR, Denver, USA, 2010