October 14, 2018

Hi all,

Here are my notes from reading the IAEA document from 2017 .

After section 4 I mainly skimmed for interesting points in the examples, due to time constraints. The IAEA document appears to have been transferred with an Optical Character Recognition (OCR) program; a few minor spelling corrections have been made.

Reviewed by:
Ace Hoffman
Carlsbad, California
October 11, 2018

List if Acronyms:

HCLPF: High Confidence of Low Probability of Failure
IAEA: International Atomic Energy Agency
ISFSI: Independent Spent Fuel Storage Installation
NPP: Nuclear Power Plant
PRAs: Probabilistic Risk Assessments
SSCs: Structures, Systems and Components

---
1. INTRODUCTION:

This report is about beyond design basis accidents: "**the focus is to identify what can go wrong in an existing installation when external events exceed the design basis.**" Technically, these should almost never occur, but occurred three times in Japan in 2011. The "**scenario had not been considered and no provisions had been made for it**" which is to say, planners did not travel into the mountains inland from Fukushima and see the ancient stone markers warning that tsunami waves -- even higher than actually occurred on 3/11/2011 -- had occurred in the past. There was, in short no reason to say this event was unexpected. It should have been planned for (by not building the reactors in the first place).

This Introduction makes clear that Probabilistic Risk Assessments (PRAs) are required for nuclear power plants to operate: Extreme accidents cannot be prevented, but it is hoped they will occur infrequently, or "**with a very low probability.**" At least the report admits that estimated hazard frequencies: "**could include a significant amount of uncertainty.**"

1.2 Objective:

"**[I]n the present context, every plant will have its 'vulnerabilities ' or 'weak links', and 'vulnerability' does not necessarily mean non-compliance with a regulatory requirement.**" But it does mean a potentially catastrophic extreme event.

1.3 Scope:

The scope of the document does NOT include "**willful human induced events (i.e. not accidental), such as military action or industrial sabotage.**" Therefore it's not relevant to many real-world conditions.

1.4 Overview of the Methodology:

"**Using a given set of screening criteria and conservative bounding analyses, the list is screened in order to eliminate from the assessment those hazards that do not need to be analyzed further. The screening criteria and bounding analyses are similar to those used in other contexts related with design or safety assessment [14-16].The only significant difference is that, except for extraordinarily rare events (e.g. large meteorite impact), the low frequency of occurrence cannot be used to screen-out a hazard at this stage.**"

It is extraordinary that meteorite impacts are excluded, considering that they could aerosolize the entire radioactive contents at the site. This is NOT how risk versus consequences should be balanced! The very next sentence indicates that events with "**very low probability**" need to be considered. Well? It's particularly odd since such events would be relatively easy to analyze: Nothing to mitigate, and

all the inventory aerosolized immediately. That would certainly be a good "bounding" scenario!

Clearly, the goal is to keep the plants operating: "**Throughout this process of risk identification and mitigation, the operating organization needs to maintain an approach of maintaining risks as low as reasonably practicable. This is particularly important in the assessment of extreme external events, where significant investments of resources are possible.**"

(Note: Meteorite impacts are briefly mentioned on page 145: "**the damage potential to objects on the earth being struck or even being near-missed by meteorites is enormous.**")

1.5 Structure:

Five specific hazards are assessed in this document: "**earthquake, high winds, flood, aircraft impact and explosion/hazardous releases.**" Interestingly, a tsunami can have much higher lateral forces than a mere flood, and of course, a terrorist can determine the strength of explosion he or she wishes to create in order to achieve the desired goal.

1.6 Uses of this publication:

The document is intended for plant operators.

---
2. SELECTION OF APPLICABLE HAZARDS:

2.1 Universe of External Hazards:

"**Willful human induced hazards"** are not included. So, what might be the most likely events and the only events actually designed to do damage are excluded from consideration.

2.2 Hazard Combinations:

Only non-random combinations are considered (for an obvious example, a tsunami following an earthquake).

In the table of External Hazards (p 10) a landslide onto a body of water is included, but what is probably the most likely extreme event at San Onofre -- a completely underwater "land" slide among the nearby underwater canyons -- is not included. Because San Onofre does not consider such events, the 14-foot high sea wall is assumed to be adequate, because large offshore earthquakes are not considered possible close enough to produce larger tsunami waves than a few feet high.

2.3 Site Specific Screening of Hazards:

2.3.1 Purpose of Screening:

Sites are expected to eliminate consideration of hazards they consider impossible or unlikely at their specific site. The document notes, however, that:

"**It is emphasized that screening of hazards needs to be based on updated site and regional data. Updated data can be very different from the data used during the design of the NPP, especially for human induced hazards or meteorological hazards for which only a limited number of site specific records were available in the design phase.**"

2.2.3 Preliminary Screening Criteria:

The document states that hazards can be screened out if other, included, hazards would have equal or worse consequences, but should not be screened out based on "**comparison with the probability of occurrence associated to other hazards.**" However, a footnote to this section indicates that an annual (estimated) probability of less than 10^-7 (1 in ten million) is a common threshold for consideration of any particular extreme hazard event. However, undoubtedly the actual probability of

such low likelihood events is a wild guess.

It appears the goal is, ideally, to screen out all but one hazard, and study the consequences of that hazard. The ideal is probably seldom reached because different hazards would affect different aspects of plant safety.

2.3.3 Plant and Site Review:

A walk around the plant is recommended to be sure nothing that is site-specific has been screened that should have been included. (At San Onofre, for example, the consequences for the Independent Spent Fuel Storage Installation (ISFSI) of the low sea wall might be considered. (For example, at high tide on a day like today, when waves are at least seven feet, due to a storm hundreds of miles away.)

2.3.4 Bounding Analyses:

Bounding analyses as used here does not consider probability of events, but is to screen out only events that, at their worst, cannot actually damage the plant.

Also, meteorite strikes are specifically discussed here as an example of "**very rare events, for which there is wide consensus worldwide that consideration is not needed within nuclear safety analyses.**" (Satellite falls are also excluded.) A frequency of less than 10^-9 (one in a billion) per year is considered the threshold for bounding analyses elimination. It should be noted that with over 500 nuclear reactors operating worldwide (including military and research reactors) the actual risk for the ecosystem of the planet of a meteorite strike is over 500 times greater than for an individual reactor. So maybe someone at IAEA should consider what would happen?

2.3.5 Results:

"**[T]he site specific screening of hazards and especially the basis for screening out hazards and hazard combinations need to be published with sufficient detail and quality to allow independent assessment.**"

Well, that's certainly true.

---
3. SELECTION OF COMPONENTS:

3.1 General:

For each selected hazard, a list of Structures, Systems and Components (SSCs) that would be affected should be compiled.

"**The fundamental safety functions are defined in Ref [41]:**
(1) Control of reactivity;
(2) Removal of heat from the reactor and from the fuel store;
(3) Confinement of radioactive material, shielding against radiation and control of planned
radioactive releases, as well as limitation of accidental radioactive releases."

The location of an airplane strike would determine which SSCs are affected. Did it strike the switchyard? The spent fuel pool building? The control room? The intake structures? More than one of these? If there is a loss of offsite power, what if the on-site power is also unavailable (station black-out)?

Two approaches to studying the hazards are offered: A "**success path**" approach and an "**event tree/fault tree**" approach.

3.2 A Success Path Approach:

This approach looks at what could be done to put the plant into a safe condition. If operator actions are required, prior training needs to have been put in place, the environment at the time of the incident needs to be considered (is the control room on fire?), and egress routes need to be available for operator actions. It appears that suicidal missions which might save hundreds of thousands of lives are not to be considered. I guess this isn't Hollywood and heroes don't work in nuclear power plants.

For "**extreme events**" there may not be redundant systems available for the success path. That's fine with the IAEA.

3.3 Event Tree/Fault Tree Approach:

An event tree model generally identifies what components can mitigate an event, while a fault tree identifies what components can cause an event. An "**accident sequence analysis"** identifies which components would fall into which model. The goal, of course, it to identify what systems can be used to bring the event to a safe conclusion.

3.4: Results:

Using either the Success Path approach or the Event Tree/Fault Tree approach, the identification of key components to mitigate or prevent a hazardous event from causing a catastrophic accident are (hopefully) identified so that procedures can be put into place to ensure the proper sequence is followed.

This author notes that some events will not have a successful ending, no matter what the operators do or are trained for.

---
4. GENERAL METHODOLOGY FOR PLANT CAPACITY ASSESSMENT:

4.1 General:

Plant capacity refers to the strength of hazard that could begin to compromise plant safety. It can be studied with either a deterministic procedure or a semi-probabilistic procedure. A walk-through to determine the actual condition of plant components should be made.

4.2 Deterministic Procedure:

4.2.1 Define Reference Strength for the Hazard:

For example, speed and size of an airplane, maximum ground acceleration of an earthquake, etc.. Once this has been determined, plant SSC's ability to handle that event can be estimated, and if they can handle it, they can be ignored for purposes of further calculations. However, picking the correct "**confidence capacity**" can make or break the accuracy of the calculations.

4.2.2. Plant response to the reference event:

This is a computed value for each SSC based on plant specifics and the reference strength of the hazard.

2.3. Capacity of the selected components:

This step rates the ability of an SSC to handle the reference hazard -- is there a 95% chance? 98%? This is known as the "**failure margin**" and should be determined conservatively and, if possible, by testing.

4.2.4. Plant-level capacity:

With the success path approach, "**the plant level capacity is assumed to be given by the high confidence capacity of the weakest component needed to accomplish the fundamental safety functions.**"

If using the event tree/fault tree approach, plant SSCs are rated on a "pass/fail" basis to determine the probability of the plant's response to a hazard event.

4.2.5. Discussion:

The purposes of the above procedures is to identify weak links in the plant's ability to handle hazard events, and determine the severity of events that would impact plant safety. The document notes that: "**A well-designed and maintained plant will normally have a plant-level capacity well above the design basis hazard strength.**" Let's hope so.

Because the deterministic approach requires using conservative assumptions, it is difficult to determine available margins of safety using this approach.

4.3. Semi-probabilistic procedure:

4.3.1. Define reference strength for the hazard:

This is similar to the first step of the deterministic approach. In both approaches, it is important to choose assumptions which are close to the plant's ability to survive the hazard, so that more precise determinations of the weakest links can be made. Repeated iterations may be necessary.

4.3.2. Plant response to the reference event:

This is also similar to the corresponding step of the deterministic approach.

4.3.3. Screening of robust structures, systems and components:

Here, "**Capacity is defined as the conditional probability of failure of a SSC for a given value of the hazard parameter.**" In seismic assessments, this is known as the "**fragility curve.**" A median value is determined and deviations from that value are estimated for both the chance the value is flat-out incorrect and the chance that it could be correctly calculated but the SSC might not behave as expected anyway. A "**high confidence capacity**" corresponds to a 1% failure probability in the mean fragility curve of the component. This author notes that perhaps that is not nearly good enough for nuclear plant meltdown estimates.

A plant walk down is considered useful to ensure that confidence estimates are likely to be accurate.

4.3.4. Fragility calculations:

The computed capacity of an SSC is assumed to correspond to a 1% failure rate, "**[t]hen, variability is conservatively estimated.**" Or so we hope.

4.3.5. Plant-level capacity:

Hazard event response can be influenced by component failures that are expected, but also by random failures and operator error. A 1% failure probability for any specific hazard is considered the plant-level capacity for that hazard.

Like the deterministic approach, this approach is also supposed to determine the plant's weak link as well as the threshold of hazard strength that the plant will probably be able to survive. In addition, this approach is better able to consider random failures and operator errors. The semi-probabilistic approach requires specialized software and properly trained engineers.

4.4. In-plant evaluation:

4.4.1. General:

An accurate assessment of plant safety margin requires knowing the current condition of the plant. One cannot assume that fire doors are always kept closed, sealing of penetrations are air-tight, etc..

4.4.2. Review of plant status:

A review of plant design and of "as-is" plant status is done in this step.

4.4.3. Plant walk down:

Plant walk downs should begin with a preparation step, a preliminary walk down or walk by, and a detailed walk down. A full database of all SSCs should be used.

4.4.4. Special topics of in-plant evaluation:

Interactions between two reactors, two spent fuel pools, etc.. need to be evaluated. Also structural integrity, pipe, vessels and all anchors, etc.. Look for what kinds of tornado missiles might be generated on site or nearby.

4.5. Results:

A list of "weak links" and high confidence SSCs can be generated from the plant walk down.

---
5. PLANT CAPACITY ASSESSMENT FOR SELECTED HAZARDS:

Selected hazards reviewed are: Earthquake, High winds and tornados, floods, aircraft impacts, jet fuel fires, explosions and hazardous releases.

For earthquakes, a "**High Confidence of Low Probability of Failure (HCLPF)**" is calculated for the plant and for individual components. This is supposed to represent "**conservative, but realistic capacity**." In talking to an NRC employee some years ago, he assured this author that San Onofre was undoubtedly built well beyond its required strength, a claim he was never willing to verify and undoubtedly never could, nor did he offer a confidence level for that assessment: Was he 95% sure of that? 99%? Did he mean 1 whole unit on the Richter scale (which would be a 10-fold increase in resistance capacity)? A half unit (a 5-fold overage)? Who did he think paid for the added strength he asserted the plant had? This discussion was brought about because expert geologists had recently determined that a

beyond design basis earthquake was possible in the area, so it definitely matters.

For jet fuel fires from a commercial jet impact, a fireball can blast through doors, windows and light walls. A "**ventilation controlled internal fire**" can burn for several hours. Smoke and fire can prevent plant personnel and emergency responders from getting close to the impact area. Underground conduits can be flooded with burning jet fuel. This author notes that San Onofre's dry casks could be, too, and the fire could burn for longer than the casks can withstand. Also, the area of "fire and smoke" could encompass both spent fuel pools at San Onofre, or the entire ISFSI island.

---
6. ASSESSMENT OF PERFORMANCE OF FUNDAMENTAL SAFETY FUNCTIONS:

This analyses takes into account likely conditions after an extreme hazard event, such as: "**partial site devastation, overstressed operators, or severe environmental conditions (smoke, fire, etc.).**" Also **station black-out** and **loss of ultimate heat sink**.

---
7. RISK ESTIMATES

A hazard assessment expresses the "**relationship between the strength of the hazard and the annual frequency of exceeding this strength.**"

On page 87 is a chart of "Historical probability vs. Risk assessment studies" for a particular set of dams. The dam estimates were undoubtedly supposed to be "conservative" in all cases, and for five of the seven categories, they turned out to be. (The categories were Overtopping, Foundation, Piping, Sliding, Structural, Spillway and Earthquake.) But in two of the seven categories (Overtopping and Sliding) the historical probabilities were larger, sometimes much larger, than the risk assessment study estimates. In this author's opinion, while dam failures can be a serious problem and lead to many deaths if the area downstream is heavily populated, such failure rates for risk assessments at nuclear power plants should be totally unacceptable, in part because the systems are much more complex, requiring far more than just seven categories, and also because the capacity for long-term catastrophic impacts is so high.

The above notes written October 10 - 11, 2018 by Ace Hoffman, Carlsbad, California

---