Surry plant is a gravity-fed service water system with a canal that may drain during station blackout, thus failing containment heat removal. When power is restored, the canal must be refilled before containment heat removal can be restored.

The dominant accident sequence type at Zion is not a station blackout, but it has many similar characteristics. Component cooling water is needed for operation of the charging pumps and high-pressure safety injection pumps at Zion. Loss of component cooling water (or loss of service water, which will also render component cooling water inoperable) will result in loss of these high-pressure systems. This in turn leads to a loss of reactor coolant pump seal injection. Simultaneously, loss of component cooling water will also result in loss of cooling to the thermal barrier heat exchangers for the reactor coolant pump seals. Thus, the reactor coolant pump seals will lose both forms of cooling. As with station blackout, loss of component cooling water or service water can both cause a small LOCA (by seal failure) and disable the systems needed to mitigate it. The importance of this scenario is increased further by the fact that the component cooling water system at Zion, although it uses redundant pumps and valves, delivers its flow through a common header. The licensee for the Zion plant has made procedural changes and is also considering both the use of new seal materials and the installation of modifications to the cooling water systems. These measures, which are discussed in more detail in Chapter 7, reduce the importance of this contributor.

ATWS frequencies are generally low at all three of the PWRs. This is due to the assessed reliability of the shutdown systems and the likelihood that only slow-acting, low-power-level events will result.

While of low frequency, it is worth noting that interfacing-system LOCA (V) and steam generator tube rupture (SGTR) events do contribute significantly to risk for the PWRs. This is because they involve a direct path for fission products to bypass containment. There are large uncertainties in the analyses of these two accident types, but these events can be important to risk even at frequencies that may be one or two orders of magnitude lower than other sequence types.

During the past few years, most Westinghouse PWRs have developed procedures for using feed and bleed cooling and secondary system blowdown to cope with loss of all feedwater. These procedures have led to substantial reductions in the frequencies of transient sequences involving the loss of main and auxiliary feedwater. Appropriate credit for these actions was given in these analyses. However, there are plant-specific features that will affect the success rate of such actions. For example, the loss of certain power sources (possibly only one bus) or other support systems can fail power-operated relief valves (PORVs) or atmospheric dump valves or their block valves at some plants, precluding the use of feed and bleed or secondary system blowdown. Plants with PORVs that tend to leak may operate for significant periods of time with the block valves closed, thus making feed and bleed less reliable. On the other hand, if certain power failures are such that open block valves cannot be closed, then they cannot be used to mitigate stuck-open PORVs. Thus, both the system design and plant operating practices can be important to the reliability assessment of actions such as feed and bleed cooling.

8.4.4 External Events

The frequency of core damage initiated by external events has been analyzed for two of the plants in this study, Surry and Peach Bottom (Ref. 8.1 (Part 3) and Ref. 8.2 (Part 3)). The analysis examined a broad range of external events, e.g., lightning, aircraft impact, tornados, and volcanic activity (Ref. 8.8). Most of these events were assessed to be insignificant contributors by means of bounding analyses. However, seismic events and fires were found to be potentially major contributors and thus were analyzed in detail.

Figures 8.7 and 8.8 show the results of the core damage frequency analysis for seismic- and fire-initiated accidents, as well as internally initiated accidents, for Surry and Peach Bottom, respectively. Examination of these figures shows that the core damage frequency distributions of the external events are comparable to those of the internal events. It is evident that the external events are significant in the total safety profile of these plants.

Seismic Analysis Observations

The analysis of the seismically induced core damage frequency begins with the estimation of the seismic hazard, that is, the likelihood of exceeding different earthquake ground-motion levels at the plant site. This is a difficult, highly judgmental issue, with little data to provide verification of the various proposed geologic and seismologic models.

The sciences of geology and seismology have not yet produced a model or group of models upon which all experts agree. This study did not itself

produce seismic hazard curves, but instead made use of seismic hazard curves for Peach Bottom and Surry that were part of an NRC-funded Lawrence Livermore National Laboratory project that resulted in seismic hazard curves for all nuclear power plant sites east of the Rocky Mountains (Ref. 8.9).

In addition, the Electric Power Research Institute (EPRI) developed a separate set of models (Ref. 8.10). For purposes of completeness and comparison, the seismically induced core damage frequencies were also calculated based upon the EPRI methods. Both sets of results, which are presented in Figures 8.5 through 8.8, were used in this study. More detailed discussion of methods used in the seismic analysis is provided in Appendix A; Section C.11 of Appendix C provides more detailed perspectives on the seismic issue as well.

As can be seen in Figures 8.5 and 8.6, the shapes of the seismically induced core damage probability distributions are considerably different from those of the internally initiated and fire-initiated events. In particular, the 5th to 95th percentile range is much larger for the seismic events. In addition, as can be seen in Figures 8.7 and 8.8, the wide disparity between the mean and the median and the location of the mean relatively high in the distribution indicate a wide distribution with a tail at the high end but peaked much lower down. (This is a result of the uncertainty in the seismic hazard curve.)

It can be clearly seen that the difference between the mean and median is an important distinction. The mean is the parameter quoted most often, but the bulk of the distribution is well below the mean. Thus, although the mean is the "center of gravity" of the distribution (when viewed on a linear rather than logarithmic scale), it is not very representative of the distribution as a whole. Instead, it is the lower values that are more probable. The higher values are estimated to have low probability, but, because of their great distance from the bulk of the distribution, the mean is "pulled up" to a relatively high value. In a case such as this, it is particularly evident that the entire distribution, not just a single parameter such as the mean or the median, must be considered when discussing the results of the analysis.

1. Surry Seismic Analysis

The core damage frequency probability distributions, as calculated using the Livermore and EPRI methods, have a large degree of overlap, and the differences between the means and medians of the two resulting distributions are not very meaningful because of the large widths of the two distributions.

The breakdown of the Surry seismic analysis into principal contributors is reasonably similar to the results of other seismic PRAs for other PWRs. The total core damage frequency is dominated by loss of offsite power transients resulting from seismically induced failures of the ceramic insulators in the switchyard. This dominant contribution of ceramic insulator failures has been found in virtually all seismic PRAs to date.

A site-specific but significant contributor to the core damage frequency at Surry is failure of the anchorage welds of the 4 kV buses. These buses play a vital role in providing emergency ac electrical power since offsite power as well as emergency onsite power passes through these buses. Although these welded anchorages have more than adequate capacity at the safe shutdown earthquake (SSE) level, they do not have sufficient margin to withstand (with high reliability) earthquakes in the range of four times the SSE, which are contributing to the overall seismic core damage frequency results.

Similarly, a substantial contribution is associated with failures of the diesel generators and associated load center anchorage failures. These anchorages also may not have sufficient capacity to withstand earthquakes at levels of four times the SSE.

Another area of generic interest is the contribution due to vertical flat-bottomed storage tanks, e.g., refueling water storage tanks and condensate storage tanks. Because of the nature of their configuration and field erection practices, such tanks have often been calculated to have relatively smaller margin over the SSE than most components in commercial nuclear power plants. Given that all PWRs in the United States use the refueling water storage tank as the primary source of emergency injection water (and usually the sole source until the recirculation phase of ECCS begins), failure of the refueling water storage tank can be expected to be a substantial contributor to the seismically induced core damage frequency.

2. Peach Bottom Seismic Analysis

As can be seen in Figure 8.9, the dominant contributor in the seismic core damage frequency analysis is a transient sequence brought about by loss of offsite power. The loss of offsite power is due to seismically induced failures of onsite ac power. Peach Bottom has four emergency diesel

generators, all shared between the two units, and four station batteries per unit. Thus, there is a high degree of redundancy. However, all diesels require cooling provided by the emergency service water system, and failure to provide this cooling will result in failure of all four diesels.

There is a variety of seismically induced equipment failures that can fail the emergency service water system and result in a station blackout. These include failure of the emergency cooling tower, failures of the 4 kV buses (in the same manner as was found at Surry), and failures of the emergency service water pumps or the emergency diesel generators themselves. The various combinations of these failures result in a large number of potential failure modes and give rise to a relatively high frequency of core damage based on station blackout. None of these equipment failure probabilities is substantially greater than would be implied by the generic fragility data available. However, the high probability of exceedance of larger earthquakes (as prescribed by the hazard curves for this site) results in significant contributions of these components to the seismic risk.

Fire Analysis Observations

The core damage likelihood due to a fire in any particular area of the plant depends upon the frequency of ignition of a fire in the area, the amount and nature of combustible material in that area, the nature and efficacy of the fire-suppression systems in that area, and the importance of the equipment located in that area, as expressed in the potential of the loss of that equipment to cause a core damage accident sequence. The methods used in the fire analysis are described in Appendix A and in Reference 8.7; Section C.12 of Appendix C provides additional perspectives on the fire analysis.

1. Surry Fire Analysis

Figure 8.10 shows the dominant contributors to core damage frequency resulting from the Surry fire analysis. The dominant contributor is a transient resulting in a reactor coolant pump seal LOCA, which can lead to core damage. The scenario consists of a fire in the emergency switchgear room that damages power or control cables for the high-pressure injection and component cooling water pumps. No additional random failures are required for this scenario to lead to core damage. It should be noted that credit was given for existing fire-suppression systems and for recovery by crossconnecting high-pressure injection from the other unit. The importance of this scenario is evident in Figure 8.11, which breaks down the fire-induced core damage frequency by location in the plant. The most significant physical location is the emergency switchgear room. In this room, cable trays for the two redundant power trains were run one on top of the other with approximately 8 inches of vertical separation in a number of plant areas, which gives rise to the common vulnerability of these two systems due to fire. In addition, the Halon fire-suppression system in this room is manually actuated.

The other principal contributor is a spuriously actuated pressurizer PORV. In this scenario, fire-related component damage in the control room includes control power for a number of safety systems. Full credit was given for independence of the remote shutdown panel from the control room except in the case of PORV block valves; discussions with utility personnel indicated that control power for these valves was not independently routed.

2. Peach Bottom Fire Analysis

Figure 8.10 shows the mechanisms by which fire leads to core damage in the Peach Bottom analysis. Station blackout accidents are the dominant contributor, with substantial contributions also coming from fire-induced transients and losses of offsite power. The relative importance of the various physical locations is shown in Figure 8.12.

It is evident from Figure 8.12 that control room fires are of considerable significance in the fire analysis of this plant. Fires in the control room were divided into two scenarios, one for fires initiating in the reactor core isolation cooling (RCIC) system cabinet and one for all others. Credit was given for automatic cycling of the RCIC system unless the fire initiated within its control panel. Because of the cabinet configuration within the control room, the fire was assumed not to spread and damage any components outside the cabinet where the fire initiated. The analysis gave credit for the possibility of quick extinguishing of the fire within the applicable cabinet since the control room is continuously occupied. However, should these efforts fail, even with high ventilation rates, these scenarios postulate forced abandonment of the control room due to smoke from the fire and subsequent plant control from the remote shutdown panel.

The cable spreading room below the control room is significant but not dominant in the fire analysis. The scenario of interest is a fire-induced transient coupled with fire-related failures of the control power for the high-pressure coolant injection

system, the reactor core isolation cooling system, the automatic depressurization system, and the control rod drive hydraulic system. The analysis gave credit to the automatic CO_2 fire-suppression system in this area.

The remaining physical areas of significance are the emergency switchgear rooms. The fire-induced core damage frequency is dominated by fire damage to the emergency service water system in conjunction with random failures coupled with fire-induced loss of offsite power. In all eight emergency switchgear rooms (four shared between the two units), both trains of offsite power are routed. It was noted that in each of these areas there are breaker cubicles for the 4 kV switchgear with a penetration at the top that has many small cables routed through it. These penetrations were inadequately sealed, which would allow a fire to spread to cabling that was directly above the switchgear room. This cabling was a sufficient fuel source for the fire to cause a rapid formation of a hot gas layer that would then lead to a loss of offsite power. Since both offsite power and the emergency service water systems are lost, a station blackout would occur.

Perspectives: General Observations on Fire Analysis

Figures 8.7 and 8.8 clearly indicate that fire-initiated core damage sequences are significant in the total probabilistic analysis of the two plants analyzed. Moreover, these analyses already include credit for the fire protection programs required by Appendix R to 10 CFR Part 50.

Although the two plants are of completely different design, with completely different fire-initiated core damage scenarios, the possibility of fires in the emergency switchgear areas is important in both plants. The importance of the emergency switchgear room at Surry is particularly high because of the seal LOCA scenario. Further, the importance of the control room at Surry is comparable to that of the control room at Peach Bottom.

This is not surprising in view of the potential for simultaneous failure of several systems by fires in these areas. Thus, in the past such areas have generally received particular attention in fire protection programs. It should also be noted that the significance of various areas also depends upon the scenario that leads to core damage. For example, the importance of the emergency switchgear room at Surry could be altered (if desired) not only by more fire protection programs but also by changes in the probability of the reactor coolant pump seal failure.

東電福島第一事故について

近藤駿介

原子炉安全の歴史

- 人里から出力に応じた適当な離隔距離Rをとれるところに立地すること $R^2 \sim P$　物理的安全
- 原子炉暴走時の発生エネルギーは負の反応度フィードバックを備えることにより制限できる→格納容器の導入で離隔距離を短くすることを容認：原子力発電の始まり
- 格納容器は炉心溶融時に機能するか？→緊急時炉心冷却システム（ECCS）の設置
- こうした工学的安全施設はどこまで信頼できるものであるべきか→How safe is safe enough? 信頼性論争の始まり；
  - 深層防護に基づく安全確保方針：高信頼設計の実施、設計基準事故・事象に備える工学的安全設備、防災計画の整備
  - リスク評価の実施：
    - 早期放出の防止、フィルター付き格納容器ベントの活用等のシビアアクシデントのマネジメントも効果的
    - 安全目標（世界に1000基の原子炉があるとして、これの大事故は、人がそれについて一生のうちに一度きくことがある程度まれなものにすべき）の達成には、
      - 設計基準事象には再帰期間が10000年の事象強度を選ぶこと
      - 設計に当たっては事象強度の不確実性が大きいことを念頭に、強度の不確実性に対して感度が低いようにすること

Reflections on Fukushima

19th International Conference On Nuclear Engineering (ICONE19) , October 24-25, 2011 Osaka, Japan
Dr. Nils J. Diaz
Managing Director, The ND2 Group, LLC Chairman, ASME Task Force- Japan Events

Nuclear Power Before Fukushima

- 25 years without a nuclear reactor accident provided assurance of safety worldwide. The two prior accidents:
  - TMI: Light Water Reactor (LWR), caused by internal event (open valve) and human factors, resulting in core degradation but no public health & safety/environmental effects.
  - Chernobyl: Graphite Reactor, caused by internal event, major errors in operation (human factors), resulting in core melting/burning, uncontrolled radioactive releases with major public health & safety and environmental consequences.
- No LWR accident until Fukushima had resulted in significant external radioactive contamination.
- No external event before Fukushima resulted in core degradation and uncontrolled radioactivity release (including Armenia).
- Regardless of initiating events, all accidents resulted in loss of core cooling after deficient accident management and human errors.

Reflections on Fukushima

19th International Conference On Nuclear Engineering (ICONE19) , October 24-25, 2011 Osaka, Japan

Dr. Nils J. Diaz

Managing Director, The ND2 Group, LLC Chairman, ASME Task Force- Japan Events

The Fukushima Daiichi Nuclear Plant Accidents

What should have happened?

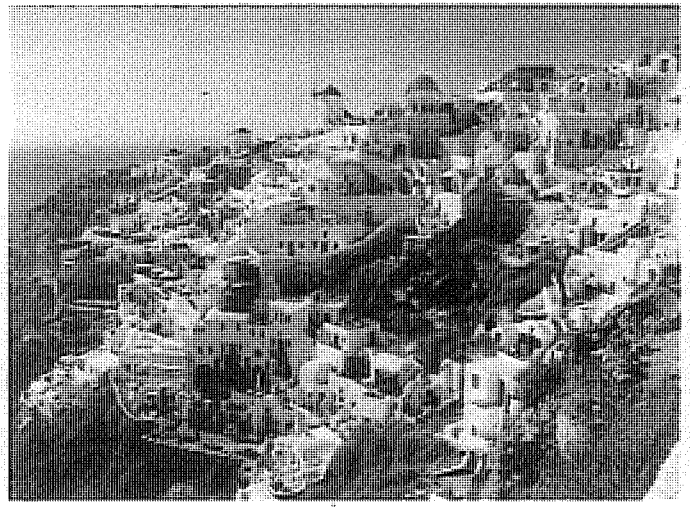
- Provide adequate heat removal for the reactor core and safety- related heat sources even during accident conditions.
  - The above dominant reactor safety criteria is met by: maintaining core cooling; maintaining cooling of spent fuel pools; maintaining containment integrity; maintaining command and control; effective accident management complemented by emergency preparedness to prevent or minimize radiological releases to the public and the environment.

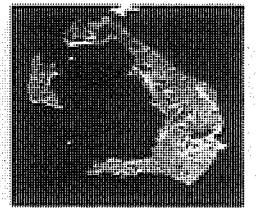
What happened?

- *Loss of power resulted in lack of heat removal and core degradation.*
- Multi-unit reactor accidents, most complex nuclear power scenarios
- ever.
- A major environmental radiological contamination, apparently without serious radiological public health and safety consequences.

事故は何故防げなかったのか

-東大原子力GCOEによる「ご意見を聞く会」から-



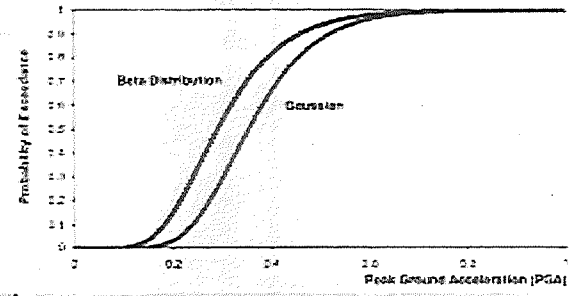


東大原子力GCOE　特任教授　尾本　彰
特任助教　寿楽　浩太
東大原子力国際専攻　教授　田中　知

尾本、寿楽、田中

自然災害への備えの不足

- 原子力安全をリードした専門家の間で、地震については危機感を持って検討がされたが、津波への警戒心が不足していた
- 地震に対して持つ工学的余裕特性と津波のそれとの相違に注意が必要だった（Fragility curve）



- 米国設計を墨守しすぎて日本固有の気候風土（地震津波火山）、社会（沿岸部の稠密利用、土地汚染の重要性）への配慮不足
- 内因事象検討に力点が置かれ、外因事象とテロ対策に遅れ、かつ、外因事象に関する情報源（認識科学）との間に隙間
- 理学における不確かさへの認識不足。工学的余裕を含め理学/工学の議論不足
- 自然災害（外因事象）への安全目標の適用が理解されていなかった
- 今回の津波は「合理的な予防行動」（十分な説得性をもって専門家間で予防行動を取るべきとの合意を得ての行動）には至らないであったろうが、残余のリスクにどう対処するかの視点が不足していた
- 5年前には気づいたとしても，その前の40年間にもリスクはあった。偶然今年起った。そう考えると、そもそも防げなかったのではないか？

尾本、寿楽、田中

規制

- ➢事故は規制システムの欠陥によっておきた
  - ✓新しい科学的知見を法規制に反映する仕組みの不足と遅れ
  - ✓シビアアクシデントを含め規制の国際整合への立ち遅れ
    （2002年の東電問題で別の課題解決に奔走など）
  - ✓規制一貫化前の2段階規制の後遺症として、構造材料規制偏重
  - ✓IAEA基本安全原則に忠実でなく、安全目標も無い独自の規制
  - ✓安全委員会と保安院の責任範囲分解が不明瞭、不適切
    (例：基準策定箇所と基準を用いて審査する箇所の分離)
  - ✓実プラントの設計や運転の判る規制当局者が居ない
    （専門能力涵養に適さない役人の人事異動システム)
  - ✓ 規制の過剰な品質保証重視行政によって発電所員が書類作成に追われ現場にも行けず安全への問題意識が希薄に
- ➢貞観地震津波をきちんと受け止めず適切な措置を取らなかった
- ➢事業者/規制ともに、安全文化と責任感と敏感さが不足
- ➢研究者には意見を求めてもプラントを知る事業者に意見を求めず
- ➢事業者と大学等の専門家が個別許認可に関して間接話法
- ➢規制に世界の風を感じつつ世界に発信する能力が不足

尾本、寿楽、田中

安全問題への対処姿勢

（事業者の安全文化）

- 事業者/規制ともに、安全文化と責任感と敏感さが不足
- 安全文化の劣化
  - ✓発電所長に事務系職員を任命など地元重視の一方で、技術と安全を軽視
  - ✓運転員以外には運転の知識が不足
  - ✓SBOルールやB5bなど海外の動向への敏感さ/学ぶ姿勢不足
- 事前に考えることなく、何か起きないと対処しない姿勢（例：免震重要棟は柏崎刈羽の2007年地震の経験を踏まえたものだが、もしその経験が無かったらどうなっていたか）
- 2007年地震で安全機能が確保された経験から自然災害に対して「安全だ」との思い込み/過信/慢心
- 電力に「規制要求への対応＝安全確保」との誤解があったのでは
- 継続的な改善を行いにくい社会環境（「安全か否か」の二元論、「安全問題があるなら改造完了迄止めるべき」との地元の声）の中で安全問題への対処の遅れ

尾本、寿楽、田中

安全問題への対処姿勢(…続)

(日常に埋没)

- LPHCリスクに鈍感になって行った可能性。日々起こる些細な問題の処理にかまけて、時間を掛け深く考えるべき安全問題が後回しに
- 様々な疑問を封じ込めた日常管理
- 新しい設計に挑戦する機会が減り、ルーチンの運転保守主体の発電所運営で設計や潜在的安全問題への関心低下

(安全専門家)

- 近年、安全専門家が居なくなった
- 真の意味の深層防護(防護手段を尽くしてもなお、その手段を無効にする事象は起こりうるとする思想)が理解されていなかった
- 領域横断型(航空/鉄道/化学)の安全専門家の不在
- 欧米における安全論(技術と社会との係りの議論など)からの隔絶
- 確率を重視し、事故の結果(とりわけ土地汚染)への配慮不足
- 内因事象(TMI, Chernobyl)を重視し外因事象がなおざりに
- 外因事象に対し内因事象と同じ安全目標値を適用するとの合意が不十分

(安全研究)

国の安全研究から軽水炉分野を除外したのは科学技術政策の誤り

尾本、寿楽、田中

原子力界の在り方：社会とのインターフェイス、文化

（責任感）

- 組織を超えて原子力技術者個人が社会に対し有する責任が欠落
- 原子力を担う組織はそれぞれ巨大で、原子力技術者はその巨大組織の一部としてしか能力を発揮できない。その巨大組織は大きすぎて身動きが取れなくなってきているのでは

（自分の立場に囚われすぎて）

- 外部からの批判に無関心または反発（排他性）
- 推進と反対のどちらも自分の立場に囚われすぎて柔軟にリスク低減問題に対処できない
- リスク管理と低減のための活動が堂々と出来ない。当該問題の処理完了まで停止を求められる恐れ等を考え、問題を封印する傾向

（国策推進体制）

- 国策民営の中で、国の権威を利用し産官学が一致して原子力を進める中、疑問を提示しにくい環境、率直な議論がしにくい環境の形成
- 社会的合意形成不足なまま、国と自治体の役割分担不明な儘推進