

自主的リスク低減の為の PSA/PRA の活用についてコメント

11Sept2013 尾本

1. PSA/PRA は意思決定のための情報を齎すツールの一つ。リスクと不確かさをできるだけ定量化し、どこに弱点と強みがあるのかを明確にし、決定論による安全/リスク評価を補完するものと考えている。なお、 $\text{risk} = \text{確率} \times \text{結果}$ だから PRA は確率を2度使っているゆえ PSA が正しいという人もいれば PSA は安全であるとの証明に使うとの意図が見えてよくないという意見もある。WG ではどちらを何故使うか明確化必要。

2. この場合は、自主的な安全確保を議論する場なのだから、事業者がリスク低減の為に「PSA/PRA 情報をどのように作り出しどんな風に使うことが望まれるか」が論点と思う。福島事故の反省も踏まえ、その観点から6つの見方を提出

- 1) 設置者が実施し、適切さについてレビューを受ける事が必要ではないか
 - 継続的な安全の改善のために、保有する財産について弱点と強い点を把握し、決定論を補完する意思決定のツールとして活用できる。問題意識をもって（つまり、リスクは社会的な広がりをもつことを意識し）供給者に依存せずに（コンサルタント活用あるいは自ら実施）、できるだけ自ら計算すべきではないか
 - 専門家によるレビューも客観性確保とバイアス除去のために重要
- 2) 外因事象 PSA/PRA の不確かさをよく考えることが必要ではないか
 - 起回事象/確率/イベントツリーいずれにも認識論的な不確かさとデータの不足による不確かさがあり、ことに外因事象では甚だしい
 - 「そんな中で、不測事態への備えをどうするか」という観点からは、PSA/PRA データを参考にしつつも決定論的にどこに cliff edge があってどう対策すれば良いかを検討すべき→ストレステストの重要性
- 3) DinD とのリンクを意識して見る事が必要ではないか
 - PSA の結果を「それぞれのシナリオで深層防御のどこが弱い」という観点で眺めることができる→福島事故は深層防御の第三層と第四層が電気品室の冠水で共に駄目になった。各層の独立性が確保されていなかった
 - 福島事故は、PSA/PRA 以前に外因事象に対する深層防御はどうあるべきかの議論が不十分だったことを示している
- 4) 特に外因事象について継続的なデータ拡充が必要ではないか
 - 我が国では地震が多数あり産業施設の被害データがあるのに地震 PSA/PRA のフラジリティデータは海外に依存していると推定
 - 4月に東京で開かれた PSAM2013 他で EQE 創始者の P. Yanev が J-SQUG (Seismic qualification group)をつくり機器のフラジリティデータ収集を提言。産業界の自主的安全確保の為の努力の一部とすべきではないか

5) **PSA/PRA の限界認識と改善が必要ではないか**

- 意思決定に係る組織要因や安全を確保するための **socio-technical control structure** や環境条件の変化による機器の信頼性の変化というリスク管理上の重要問題を従来の **PSA/PRA** では適切に扱えないのではとの疑問
- 例えば、受動安全系の信頼性と性能は、環境条件で大きく変化：非凝縮性ガスの存在下での **IC** のモデルのように微妙な物理条件の変化により駆動力の弱い受動安全系は性能が変化するが、これを静的な論理モデルによる **PSA/PRA** ではどう扱うか
- このような観点から **STAMP**(Systems Theoretic Accident Modeling and Processes)や **Dynamic PSA** あるいは **IDPSA**(Integrated Deterministic Probabilistic Safety Analysis)が提案されている
- 組織要因について言えば、**CAIB report chapter 7** について **causal relationship** を明らかにしながらの分析が存在しない→**JANSI** 活動の出発点の一つではないだろうか

6) **意思決定にあたっては、PSA/PRA のようなツール活用だけでなく、安全確保の考え方そのものに再考が必要ではないか**

- 「何故 **B5b** が日本では生まれなかったか」(何故日本の規制当局が米国から知らされたのに国内で適用しなかったのかだけでなく) を考える必要
- 様々な要因があろう中、機器信頼を高める事が安全に繋がる(防波堤で防ぐ、格納容器の堅牢生で防ぐ) という機器尊重に走り過ぎで、機器信頼性には想定上の限界があり、限界を超える事態の有った時にどう安全機能を確保するかというシステムのレジリアンス確保の発想が欠如との面もあったのではないか

[註]

- ✓ **STMP**: **Systems Theoretic Accident Modeling and Processes** : event-chain model に依拠せず、安全上の拘束(**safety constraints**)が適切にコントロールできていない結果として事故が生ずるとの見方で、社会と組織の中でこの拘束を確保する管理システム(**socio-technical control structure to enforce the safety constraints**)と管理プロセスの分析を通して問題点を把握し改善に繋げることができる
- ✓ **IDPSA** : **Integrated Deterministic-Probabilistic Safety Analysis**) to address aleatory/epistemic uncertainties and handling time-dependent interactions (**Dynamic PSA** to identify unknown vulnerable scenarios belongs to the family of **IPSA** methods)