

2023年9月25~26日

規制基準の基盤となる安全論理

村上 健太 <murakami@n.t.u-tokyo.ac.jp>

東京大学大学院工学系研究科 レジリエンス工学研究センター

この講義は、北大・工・修士の集中講義「新型軽水炉安全工学」として実施しました

考えてみよう

- 東京電力福島第一原子力発電所事故を受けて、2012年に新しい規制基準が施行されました。
- それから10年以上が立つのに、多くの原発は未だに原子力規制委員会から原子炉設置変更許可を受けることができていません。
- 何が難しく、そんなに時間がかかっているのでしょうか？

規制とは (Regulation)

- 特定の目的の実現のために、許認可・介入・手続き・禁止などのルールを設け、物事を制限すること
- 設計段階であれば自由な発想が許される。実際に使用する前には規制をクリアする必要がある
- 原子力の場合、**深層防護**の各段階に応じて考慮すべき**誘因事象**を設定し、それに対する安全設計の有効性を**安全解析**して基準を満足することが義務付けられている。

誘因事象の選定 (Institutional Control)

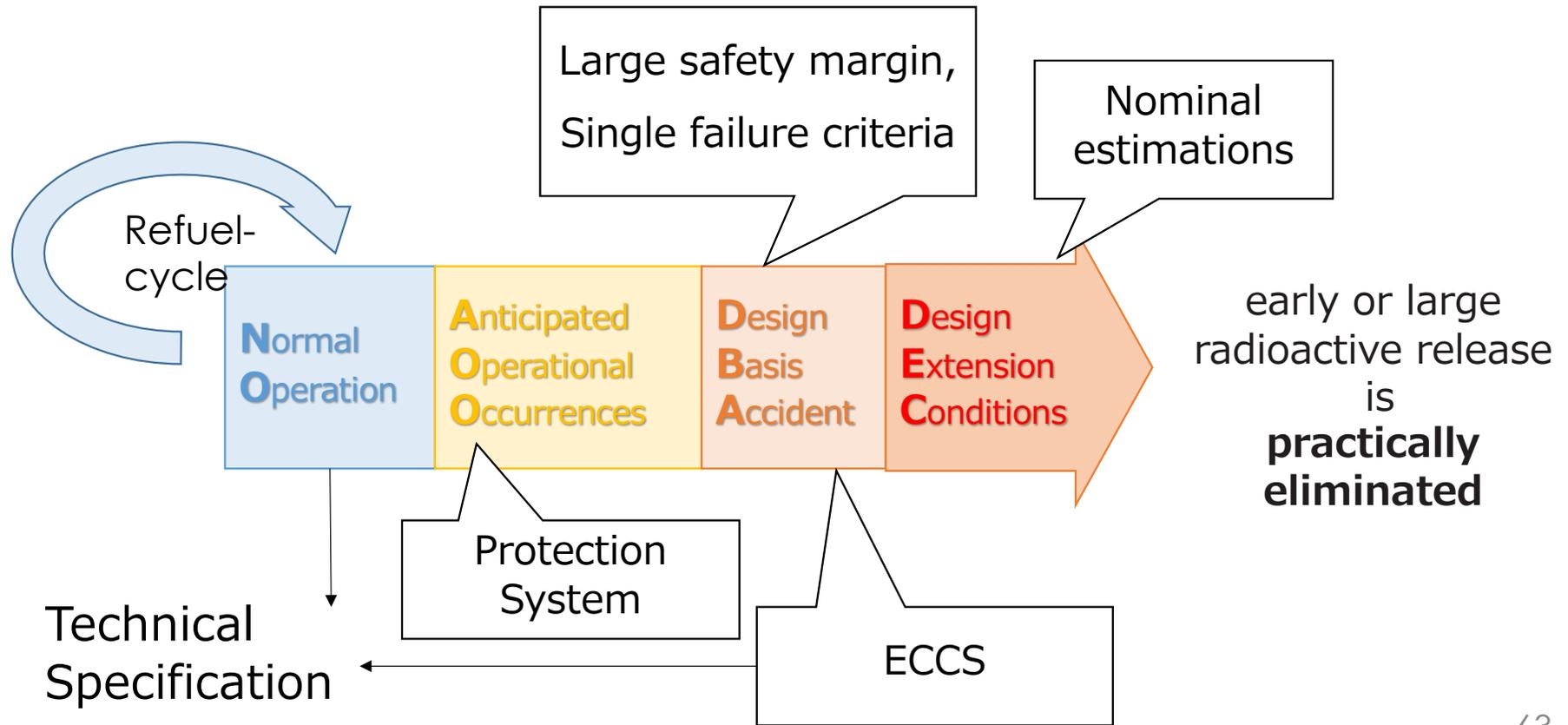
• 施設内の誘因事象

- 配管破断、ポンプ故障、制御棒誤操作、外部電源や最終ヒートシンクの喪失等、プラントの事故の誘因となるような機器等のトラブル
- 安全性を評価するために誘因事象の発生を仮定し、残った設備で安全性が維持できるかを検討する

• 施設外の誘因事象

- 地震、津波、火災など、プラントの事故の誘因となるような外的事象
- 安全性を評価するために誘因事象の発生を仮定し、機器の健全性を検証する。検証された機器のみで（かつ、いくつかの機器が故障するという仮定をルールに従って設定し）、安全性が維持できるかを検討する

原子炉発電システムにおける深層防護



防護レベル1 通常運転状態

- 通常運転状態からの逸脱と安全上重要な機器等の故障を防止する
- 品質管理、及び適切で実証された工学的手法に従って、発電所が健全でかつ保守的に立地、設計、建設、保守及び運転する
- 内部ハザードを管理する

2 運転時の異常な過渡変化

(AOO: Anticipated Operational Occurrences)

- 原子炉施設の運転寿命までの間に、少なくとも一度は発生することが予想される通常の運転状態から逸脱した操作手順が発生する事象を指す。（例えば、出力運転中の制御棒の異常な引き抜き、外部電源の喪失、通常運転時に使用しているポンプ類 1 台の不調など）
- 設置許可基準規則では「運転時の異常な過渡変化」と呼んでいる。
- 通常運転状態からの逸脱を検知して管理することを目的として、設計で特定の系統と仕組みを備え、有効性を安全解析により確認する
- AOOの起因事象を防止するか、その影響を最小に留め、発電所を安全な状態に戻す運転手順の確立する

3 設計基準事象 (Design Basis Events)

- AOOが拡大することや、想定起因事象が発生して設計基準事故に進展する場合を想定する。
 - 想定起因事象：発生頻度が十分低いが、発生すると深刻な影響を与える事象。一次冷却系配管の破断など 10^{-7} 炉年程度までスクリーニングして分類する
- 固有の安全性、工学的安全設備、手順のさまざまな組み合わせによって、事故を超える状態に拡大することを防止し、発電所を安全な状態に戻す
 - 工学的安全設備：緊急炉心冷却系、原子炉格納容器など、通常運転には使用せず、安全の目的だけのために要求される設備
- 保守的な仮定に基づく評価によって、検証する
- 炉心に著しい損傷が生じることを防ぐことを最大の目標として設計する

4 設計拡張状態 (Design Extension Conditions)

- 第3の防護レベルでの**対策が失敗した場合を想定**し（その理由は問わない）、事故の拡大を防止し、重大事故の影響を緩和することを要求する
- 時間的にも適用範囲においても限られた防護措置のみで対処可能とするとともに、敷地外の汚染を回避又は最小化する
- 早期の放射性物質(LER)の放出、又は大量の放射性物質の放出(LR)を引き起こす事故シーケンスの発生の可能性を十分に低くして、実質的に排除する (Practically Elimination)
- 最尤評価によって検証することが多い

5 緊急時の対策

- 重大事故に起因して発生しうる放射性物質の放出による影響を緩和することを目的とする
- 十分な装備を備えた緊急時対応施設の整備と、所内と所外の緊急事態の対応に関する緊急時計画と緊急時手順を整備する

安全機能

- 反応度の制御
- 原子炉及び燃料プールの除熱
- 放射性物質の閉じ込め、放射線の遮蔽、放射性物質の放出の管理、事故による放射性物質放出の制限

安全機能

- 反応度の制御
- 原子炉及び燃料プールの除熱
- 放射性物質の閉じ込め、放射線の遮蔽、放射性物質の放出の管理、事故による放射性物質放出の制限

安全システムの分離と、重要度の設定

- 安全システム、又はシステム内の冗長要素間の干渉を防止する（物理的・電氣的・機能的分離、通信などの独立性）
- 安全上重要なアイテムをすべて特定し、その機能と安全上の重要度に基づいて分類する
- 安全上重要なアイテムの信頼性は、その重要度に合わせて決定する。日本では次の通り。
 - ✓クラス1：合理的に達成し得る最高度の信頼性を確保し、かつ、維持すること
 - ✓クラス2：高度の信頼性を確保し、かつ、維持すること
 - ✓クラス3：一般の産業施設と同等以上の信頼性を確保し、かつ、維持すること

日本の規制における安全機能と重要度（少し古い！）

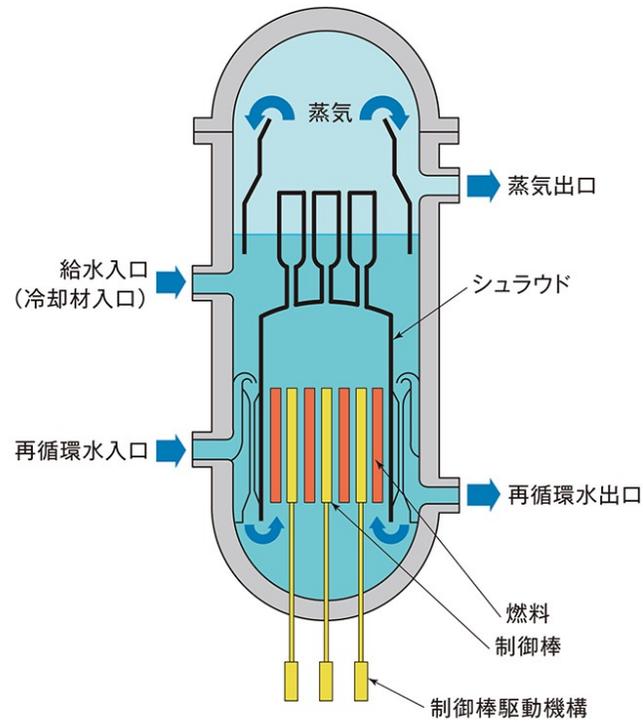
	バウンダリ機能	冷却機能	制御機能	その他(共通機能)
第1層	<ul style="list-style-type: none"> 原子炉冷却材圧力バウンダリ(PS-1) 原子炉冷却材を内蔵する(PS-2) 原子炉冷却材圧力バウンダリに直接接続されていないものであって、放射性物質を貯蔵する(PS-2) 放射性物質放出の防止(MS-2) 原子炉冷却材保持(PS-1/2以外)(PS-3) 放射性物質の貯蔵(PS-3) 核分裂生成物の原子炉冷却材中への拡散防止(PS-3) 	<ul style="list-style-type: none"> 炉心形状の維持(PS-1) 通常時炉心冷却(PS-3) 	<ul style="list-style-type: none"> 過剰反応度の印加防止(PS-1) 原子炉冷却材の循環(PS-3) 	<ul style="list-style-type: none"> 燃料を安全に取り扱う(PS-2) 電源供給(非常用を除く)(PS-3) プラント計測・制御(1)(2)(3)(安全保護系除く)(PS-3) プラント運転補助(1)(2)(PS-3) 原子炉冷却材の浄化(PS-3)
第2層	<ul style="list-style-type: none"> 原子炉冷却材圧力バウンダリの過圧防止(MS-1) 安全弁及び逃がし弁の吹き止まり(PS-2) 	<ul style="list-style-type: none"> 原子炉停止後の除熱(MS-1) 制御室外からの安全停止(MS-2) 原子炉圧力の上昇の緩和(MS-3) 原子炉冷却材の補給(MS-3) 	<ul style="list-style-type: none"> 原子炉の緊急停止(MS-1) 未臨界維持(制御棒による系)(MS-1) 未臨界維持(ほう酸水注入系)(MS-1) 出力上昇の抑制(MS-3) 	
第3層	<ul style="list-style-type: none"> 放射性物質の閉じ込め機能、放射線の遮へい及び放出低減(PCV)(MS-1) 放射性物質の閉じ込め機能、放射線の遮へい及び放出低減(R/B)(MS-1) 	<ul style="list-style-type: none"> 炉心冷却(MS-1) 燃料プール水の補給(MS-2) 		<ul style="list-style-type: none"> 事故時のプラント状態の把握(MS-2)
第4,5層 (*)	<ul style="list-style-type: none"> 過酷事故対応(PCVベント)(MS-3) 	<ul style="list-style-type: none"> 過酷事故対応(補給水系)(MS-3) 過酷事故対応(消火系)(MS-3) 	<ul style="list-style-type: none"> 過酷事故対応(ほう酸水注入系)(MS-3) 	<ul style="list-style-type: none"> 緊急時対策上重要なもの及び異常状態の把握(1)(2)(3)(MS-3)

共通原因故障 (Common Cause Failure)

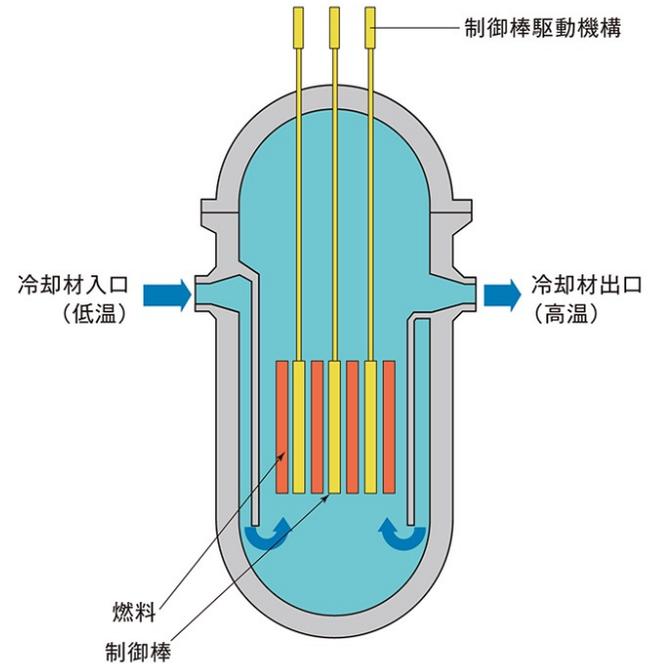
- 複数の機器又はシステムが、共通の原因によって損なわれてしまうような事態を指す。
- 例えば、地震等の外力、不純物や異物の混入、同時に発現する経年劣化、冗長性を有する機器のメンテナンスマニュアルの誤り、等が考えられる。
- 機器の設計は、安全上重要な項目の共通原因故障の可能性を十分に考慮し、必要な信頼性を達成するために、多様性、冗長性、物理的分離、機能的独立性の概念をどのように適用しなければならないかを決定しなければならない。

原子炉压力容器断面図

沸騰水型原子炉 (BWR)



加圧水型原子炉 (PWR)



原子力エネルギー図面集

<https://www.ene100.jp/zumen/5-1-6>

単一故障基準 (Single Failure Criterion)

- 単一故障：一つの原因によって、一つの機器又はシステムが設計上の安全機能を果たす能力を喪失するような故障のこと
- 単一故障基準：単一故障が発生した場合でも、安全上重要なシステムは、そのタスクを遂行する能力を有していなければならないという基準
- 安全解析では、単一故障基準を適用して、例えば緊急炉心冷却系を構成する機器の一つが偶発故障した場合でも、残りの機器を使って事故を安定に収束させられることを示す必要がある。

機器の性能検証 (Equipment Qualification)

- 安全上重要なアイテムは、設計寿命を通じて、必要なときに、必要とされる環境条件下（例えば、設計基準事故の環境）で意図された機能を果たさなければならない
- 評価では、アイテムの耐用年数にわたる環境要因（振動、照射、湿度、温度）による経年劣化の影響を考慮する。
- アイテムが地震などの外的誘因事象の影響を受け、そのような事象の発生時に安全機能を果たす必要がある場合、試験や分析によってその条件を再現する

