原子力発電所緊急対応の知的支援のための多重防護リスク解析フレームの適用研究

Application Study of Defense-in-Depth (DiD) Risk Analysis Framework as Intelligent Support for NPP Emergency Response Management

京都大学	吉川　榮和	Hidekazu YOSHIKAWA	Member
華南理工大学	楊　軍	Jun YANG	
深圳大学	楊　明	Ming　YANG	
宇都宮大学	松岡　猛	Takeshi　MATSUOKA	

Abstract

How to design, develop, and maintain a comprehensive environment, means, and capabilities for the whole system which is composed by engineering system with human organization that operates nuclear power plants (NPP) to respond appropriately under tense situations that the superimposition of unexpected events may lead to severe accidents? Taking into account of the IAEA's Defense-in Depth (DiD) concept, DiD risk analysis framework is introduced, and to meet with the above-mentioned goal, several design support methods have been proposed that utilize advanced information technologies which include artificial intelligence. Some of the research progress and results are discussed with their future issues.

Keywords

Defense-in Depth, Risk monitor, Emergency response management, Intelligent support

１．はじめに

人工知能（AI）を活用して人間の知識、知能や作業上の能力の限界を補い、技術システムと人間とで構成されるシステム全体の安全性向上を図ることで社会の安全・安心の希求に応えることを目的としている。具体的には想定外事象の重畳でシビアアクシデント事態に至る可能性のある緊迫した状況下に、原発を運転する人間組織が適切に対応できるため、人間と機械システムで構成される総合システムの環境、手段、能力を整備することを知的に支援する総合的設計論を、多重防護を考慮したリスク解析フレームをもとに構成する。本論文では筆者らが進めている日中共同研究の経過と成果の一端をまとめ、今後の課題を展望する。

連絡先 :吉川榮和、〒611-0011 宇治市五ケ庄 京大エネルギー理工学研究所内 シンビオ社会研究会
E-mail: yosikawa@kib.biglobe.ne.jp

２．多重防護リスク解析フレーム

吉川および楊明は、原子力発電所の安全運転に資するための統合型多重防護（Defense-in-depth：DiD）リスク解析システムを提起している[1]。DiD とは IAEA による 5 層の多重防護概念[2]だが、著者らは進んだリスク解析に期待される役割として次の 5 つを上げた。

① 運転員チームのための意思決定支援システムを現代のヒューマンインタフェース技術を応用して設計開発するためにオフラインのリスク分析が実行できる.

② 安全性とセキュリテイの両面を統合してリスクを分析し評価できる.

③ 事故シナリオの定義、分類、判断基準に基づくリスクの測度とその推定法を確立する.

④ 計測制御系の役割を物理的な防壁と人間工学的検討により機能的な階層構造として決定できる.

⑤ デイジタル技術による自動化，運転員行動の認知的側面，先進的な計算機支援手順の開発の文脈の中で人間信頼性解析を実施できる

統合型 DiD リスク解析システムは、以下に述べる 3 つのコアシステムとそれに付随する種々の支援ツールキットで構成される。

2.1　3 つのコアシステムの定義とその構成

統合型の DiD リスク解析システムを実際のリスク問題に適用する上で、基本となるコアシステムは、DiD リスク状態推定・シナリオ生成器、プラント DiD リスクモニタ、信頼性モニタの 3 つであり、そこでの基本用語はそれぞれ次のように定義する。

(1)**DiD リスク状態**とは対象とするプラントがもたらしうるリスクをその厳しさと緊急度でランク付けし、いくつかのレベルに分ける。

(2)いくつかのレベルに分けた個々の**リスク状態平面**内ではリスク状態が拡大してより厳しい状況である DiD リスク平面に発展するのを防ぐため**防護すべき障壁**が存在する。

(3)信頼性モニタにいう**信頼度**とはあるシステム、サブシステム、ないしコンポーネントがその防護機能を発揮してより厳しいリスク状態に発展するのを防止できる確実さの程度を意味する。

次いでコアシステムの３つの要素のそれぞれの役割と具体的な方法の例示を以下に要約する。

①**DiD リスク状態推定・シナリオ生成器**・・・対象システムがある時点でどんなリスク状態にあるかを推定するとともに、その現在のリスク状態が内的, 外的な要因によって今後どのようなシナリオで変化していくかを予想する。なお様々な過渡的な状態遷移のシナリオは種々の過渡, 事故解析コードによるシミュレーションで導出しておく。

②**プラント DiD リスクモニタ**・・・人間系と機械系の相互作用がもたらすDiDリスク状態の動的遷移を追跡する。吉川、中川が開発の DiD リスクモニタソフト[3]を用いれば技術システムと人間組織の相互作用による状態遷移の分岐シナリオを生成し, 動的並列シミュレーションが実現できる。

③**信頼性モニタ**・・・対象システムが引き起こす不都合なリスク状態の発展を抑制するためのシステムおよびそのサブシステム, コンポーネントの動作の信頼度を推定する。システムの信頼度を定量的に求めるための典型的な方法である FTA/ETA や松岡の開発した GO-FLOW ソフト[4]が使用できる。

2.2　支援ツールキットの分類

2.1 では統合型 DiD リスク解析システムの３つのコアシステムを述べた. 多重防護リスク解析フレームはこれらの 3 つのコアシステムを含めて統合型 DiD リスク解析を実施するうえで有効な支援ツールには様々な方法や解析手段があり、リスク状態をもたらす要因やその影響度、リスク発生の防止対策を表形式で記述する定性的方法やリスク要因の属性の分類とデータベース化、さらには事故事象の生起と発展、環境への影響などを表現する数学モデルに基づいて詳細に数値計算する各種のシミュレーションコードが該当する。

2.3　多重防護リスク解析フレームによる研究例

吉川、楊明らは以下の研究成果を発表している。

（1）プラント DiD リスクモニタの開発と PWR シビアアクシデント発生時の構内緊急対応行動の検討[3]

（2）シビアアクシデント発生による環境放射能放出事態に対する日本の原子力防災体制の再検討[5]

（3）プラント DiD リスクモニタの AP1000 の SBLOCA 対応支援用インタフェースの設計への活用の検討[1]

３. 原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援

楊　軍は広東省の支援を得て原子力発電所の事故時安全管理へのリスク解析の適用をテーマに 2022-23 年の 2 年間『原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援のための要素技術の研究』に関する国際共同研究プロジェクトを主導し本論文の著者らが参加している。2023 年 5 月 21-26 日京都で開催の国際会議に概プロジェクトの中国側メンバーが来日した機会に 5 月 24 日に京都でワークショップを開催した。このワークショップの報告は既に公表している[6]が、本章では日中の研究者の発表 4 件を中心にその要点を述べる。

3.1　国際共同プロジェクトの全体紹介

楊軍は、その主導する 2 年間の国際共同プロジェクトの目的と主要テーマ、中国と日本の参加メンバー、成果として求められている具体的事項とその数値目標とこれまでの達成度、そして 2 年目の現在までの進捗を発表した。以下では 4 つのサブテーマのそれぞれの研究の進捗状況を要約する。

（1）安全性の監視と管理のためのリスクの多層化

リスク情報に基づく知的な意思決定支援システムを構

成する基本概念として、次の３つの要素を提起した。
①重要安全機能のモニタリングによりプラントの安全状態を俯瞰する
②成功する道の立案により極端な条件下で想定外の事象発生時の策を提供する
③運転のナビゲーションと監督により運転員に有効なタスク実行のための手順の案内を行うとともにプロセスに対応している運転員の対応状況を監督する

楊軍はとくに①について、どのように目標―機能の樹状図、成功の樹状図、状態の樹状図を組み合わせて重要安全機能モニタリングを構成すべきかを課題として挙げた。

（２）強化したモデリングと解析基盤の開発

楊軍は、①GO-FLOW モデルを自動的に生成するツール、②GO-FLOW の解析機能を強化するアルゴリズム、③GO-FLOW の基盤の強化と最適化を進めているとし、その内容は次の何展宇の講演で紹介すると述べた。そして強化した GO-FLOW 解析のアルゴリズムの導入の仕方を示し、修復可能な PMS システムの信頼性解析を例にしてどのような問題を解こうとしているのかを述べた。

（３）緊急対応管理のための「成功する道」の立案

楊軍は、「成功する道」の立案法として、次の２つのオプションを述べた。
①GO-FLOW チャートに対するグラフ横断解析で得た最小パスセットをもとに成功パスを追跡して立案する方法。これは機能実現と目標達成を高度な抽象レベルで達成する手順を求めたものであり、運転員には手順のステップごとのガイダンスを与える必要がある。
②フロー図の知識表現と推論を組み合わせた方法。こちらは GO-FLOW モデルとは関係ないプラントパラメタのオンラインモニタリングをもとに状況を診断して対応策を推論する知識処理であり、ボロン希釈事故に対する手動補填操作を対象にケーススタデイを行っている。

(4)運転のナビゲーションと監督

楊軍は、次の２つの方法で構成することを提案した。
①GO-FLOW のモデル、トレンドへのインパクト解析等から時々刻々変わる目標達成の観点でのその都度その都度の信頼度をはかる方法を導出する。
②不安全な行為の同定、手順に基づくナビゲーションと監督、手順にはないパスのガイド、運転上の使命達成度モニタリング、トレンドへの影響度の予測、運転上のハザードの分析の機能を統合した知的な運転状態監督システムの開発。

発表後の質疑討論では、全体として広範な機能開発に対してどのように開発した方法を検証しようとしているかについて議論があった。

3.2　GO-FLOW の改良

3.2.1　動的でリビング PSA に適用するための GO－FLOW の拡張

何展宇（華南理工大）は、まず GO-FLOW の機能拡張のために GO-FLOW の 14 個のオペレータを 4 種類に分類し、また対象システムに使われるコンポーネントを能動的コンポーネントと受動的コンポーネントに分類した後、①GO-FLOW の自動モデリング機能、②リビング PSA に適用するための GO-FLOW モデリングプラットフォームの拡張、③信頼性解析の改良を説明し結論として次の４つを述べた。
(1)コンポーネントモデルの分類表を導入してシステムのコンポーネントと GO-FLOW オペレータのマップ対応を容易にした。
(2)自動GO-FLOWモデリングツールによりP&ID図からGO-FLOWモデルを抽出できるようにした。
(3)新たなGO-FLOWプラットフォームは元来の機能を保持し、共通要因解析や成功パスの分析ができるようにした。
(4)NEA アルゴリズムの適用[7]により計算効率の改善と信頼性解析の精度を向上させた。

発表後の質疑討論では、NEA アルゴリズムは再帰的関係を取り扱うものならループ構造も取り扱えるのでないかとの質問があり、そうではないとの回答があった。

3.2.2　ループ構造のあるフェーズドミッションシステムの信頼性解析

松岡　猛は、表題の背景の説明から講演を始めた。

原子力発電所や航空宇宙システムなど高度化、複雑化したシステムの多くはフェーズド・ミッション・システム（PMS）と呼ばれ、異なるタスクを複数の連続した期間で実行するものとなっている。特に安全や事故防止といった重要なミッションをサポートするために設計された技術システムにはミッションの信頼性を正確に求めることが極めて重要である。

一般に、PMS の解析方法は、シミュレーションに基づく方法と解析的な方法の２ つに分類される。解析的手法はさらに、(1) フォルトツリー（FT）、バイナリ決定図（BDD）などの組合せ手法、(2) マルコフプロセス、ベイズネットワーク（BN）などの状態空間モデルベース手法、(3) 前二者の組み合わせであるモジュール手法の三つのグループに分けることができる。

ループ構造を持つシステムを非解析的に解くと、各フェーズで反復計算や数値計算が必要になる。そのため、ループ構造を持つPMS の解析では異なるフェーズ間の依存関係を扱うのが非常に困難となるためループ構造を持つPMS の信頼性解析の文献はほとんどない。信頼性解析やアベイラビリティ解析ではシステムに論理的ループがあるとそれを考慮して正しく解くことが困難な問題だった。その解決法として論理ループのサポートシステム間の依存関係が比較的弱い箇所で切断し、ループのない新しい論理を展開する試みが従来されてきた。例えば論理ループを解消するための反復法を提案したVaurio の方法は、ループ構造の再帰性を反復計算で考慮するため、非常に直感的であるが一つの解の可能性を与えるだけである。そこで厳密解を得るためのアプローチが松岡によって最近開拓された[8]。これは論理ループを持つブール代数関係に対して、任意の集合を持つ形式解を与える方法であり、論理的ループ構造を持たないこの解を、フォールトツリー（FT）や図形ベースの信頼性解析手法に適用すればループのあるシステムの解が求まる。

松岡は、提案した本解析方法を，簡便性，直接性，厳密性の観点から，図形ベースの信頼性解析手法の一つである GO―FLOWに適用してステムのモデル化を行った。具体的には実際のBWR 原子力発電所システムを取り上げ、形式的解析解における任意集合の決定方法を解説した。ループ構造の論理を厳密解の助けを借りてGO-FLOW チャート上に直接モデル化した。また、BWR・PMS をGO-FLOW 解析におけるPMSオペレータを用いて同じGO-FLOW チャート上にモデル化している。GO-FLOW 手法は解析的な組合せ手法であり、解析の初期段階で独立した構成要素に対して数値計算を行うため、ループ構造を持つ PMS の信頼性解析が容易に効率的に高速に行える。

松岡は以上の技術的要件を説明し、特徴的なPMSとなっているBWR プラント起動時の論理ループ構造を考慮した信頼性解析の実施例を紹介した。

発表後の質疑討論では、GO-FLOW の機能拡張を実施中の華南理工大学のチームから松岡が新たに提案したLOOP 構造を考慮した PMS の解法はどのように機能拡張に反映できるのか質問があり、今後検討するとの回答があった。

3.3 原子力発電所の緊急対応への DiD リスク解析フレームの適用

吉川榮和は、A.原発の緊急事態で動的に変動するリスクをどのようにモニタすべきかの考察から始めて、B.講演者らが 30 年前に取り組んだ「高速事故追跡システム」の研究[9]をもとに原発の緊急事態管理のための新たな知的支援システムのアイデアを提起した。

A では、原発の安全設計原理として核燃料、被覆、原子炉冷却水の圧力境界、格納容器の 4 つの障壁の多重防護の仕組みで放射性物質の環境への放出を防止すること、障壁の健全性は STOP, COOL および CONTAIN の 3 つの安全機能で保証する等の基本原則から始めて原子炉容器内、格納容器内および環境外への放射性物質放出影響の 3 段階のシビアアクシデントの発展段階とそれぞれの段階に適用される解析コードについて簡単に触れたうえで、①3 つの安全機能の組み合わせでリスクレベルを段階分けし、②個々のリスクレベルの中で動的に変化するリスクの程度をより厳しいリスクレベル段階に至るまでの余裕時間と施設の構造的健全度の２軸で定量化することを考察。
①については、楊軍氏の提起する個々の安全設備―重要安全機能―3 つの安全機能のツリー構造でプラント安全目標を表わす知識表現と、個々のクリテイカル安全機能の状態の４段階表現は、実際の原発の計装信号との対比関係を規定しさえすればプラントの安全度、言い換えれば“健全度”を常時監視する「ヘルスモニタ」を構成できる。しかし人間ドックと同様でこのような「ヘルスモニタ」の情報提供は、「どうしたら健康を回復できるか」という問題とは別物である。そのためにはどこがどの程度悪くなっているのかを詳しく知ったうえで、健康を回復するためにどの程度時間的余裕があるかを考えて適当な治療法を考える。これが上記の②の問題である。
吉川は、楊軍らの提起する知識表現モデルを更に一歩進めて②に挙げた問題に対応することも考えられるが、吉川らが30年前に取り組んだ研究を②の問題に適用できるのでないかと次の話題であるBに移った。

B では、吉川は「高速事故追跡システム」の３つの要素である①カルマンフィルタの組み合わせた診断的プラント分析器、②超実時間高速事故シミュレータ、③双**方を制御してトラブル発生検知、原因診断、将来予測、対**応操作を提案するAIマネージャの基本的考え方[9]を紹介した。これは現在のAI分野での「**データ同化**」と同じで、要するにプラント計装で観測できる計測データを取り込んだシミュレーションで観測できない原子炉内部の安全上重要な燃料温度などを精度よく推定できる、さらに吉川らの DiD リスクモニタソフト[3]と現代の進んだ AI ソフトを用いて全体をインテリジェントな緊急時対応支援技術として実現可能である、と提起した。

発表後の質疑討論では、カルマンフィルタによるパラメタ推定は現在の AI ソフトのパッケージに入っている、高速事故トラッキングはVRを応用してデイジタルツインとして実現できないかなどのコメントがあった。

４．京都ワークショップからの今後の展望

本プロジェクトは、ループ構造を考慮したPMS問題において、様々な故障事象生起の統計的性質や共通要因故障を考慮し、対象システムの動的モデルを基本的な図形オペレータによりグラフ表現してそれから動的計算アルゴリズムに変換してシミュレーションする機能を具備するGO-FLOW ソフトウエアを中核に、システムの安全機能の階層化モデルの知識表現とプラント計装信号の動的変動の観測をもとに、動的に変化するリスク状態を判断するリスクモニタの導入と、状況に応じてリスク状態を回避ないし軽減させる手順を生成する知的推論を統合し、それによる推論結果を運転員に適切に提示して運転員のヒューマンエラー防止を意図している。このような知的支援システムの開発では、その個々の要素の有効性や全体システム動作の時間的整合性を検証する上でプラントシミュレータを用いた開発システムの実験的検証が必須である。そのためにはどのようなタイプの原子炉のシミュレータを用いるかを検討することが本プロジェクトの次の段階へのプロジェクトの発展には必要である。また最近進歩の著しいＡＩ技術とＶＲシミュレータを融合させるデータ同化の方面からの接近も期待される。さらには人間機械協調系としてのインタフェース設計では NRC の推奨する人間工学設計基準[10]の適用が期待される。最近急激に進歩してきたAIの社会的影響が懸念され、G7においてもAIの適切利用の５原則が政府間レベルで論じられている。本研究はAI活用で原子力発電の安全管理の一層向上を目標にDFFT（信頼性のある自由なデータ流通）を原則に日中間の研究協力を進めている。

謝辞

This work was supported by Soft Science Research Project of Guangdong Province (Grand No. 2022A0505050007).

This work is also supported by the ZE Research Program IAE, Kyoto University (ZE2023B-29).

参考文献

[1]H.Yoshikawa, M. Yang: “Integrated Defence-ib Depth (DiD) Risk Analysis System for Safety Operation of Nuclear Power Plants”, ICONE26-82639, ICONE26, July 22-26, 2018, London, UK.

[2]IAEA, “Assessment of Defence in Depth for Nuclear Power Plants”, Safety Report Series No.46, 2005.

[3]シンビオ社会研究会ホームページ DiD Risk Monitor http://sym-bio.jpn.org/homepage.php.

[4]松岡猛: システム信頼性解析手法 GO-FLOW, CRC 総合研究所 (1996).

[5]H.Yoshikawa, M.Yang, Z.Zhang, “What should be level 5 defence layer in post-Fukushima nuclear safety”, Proc. ISSNP2015, Aug.24-28, Kyoto, 2015.

[6]吉川榮和、楊軍、楊明、松岡猛、“京都ワークショップ（より高度なリスク解析法の実現を目指して）報告”、Symbio News and Report、Vol.12, No.4, 2023.

[7]L.Zhang,X.Dai,J.Yang, M.Yang, H.Lu, “A flexible optimization algorithm for GO-FLOW methodology to deal with shared signals”, Annals of Nucl. Energ. 158(2021) 108-220.

[8]T. Matsuoka, “Procedures to solve mutually dependent Fault Tree(FT) with loops”, Reliability Engineering and System Safety, 214, 2020.

[9]J.Wakabayashi, H.Yoshikawa, A.Gofuku, “Diagnostic Plant Analysis for Nuclear Power Plant Emergencies”, Proc. Intern’l Conf. on Man-Machine Interface in the Nuclear Industry (Control and Instrumentation, Robotics and Artificial Intelligence), 15-19, Feb. 1988, Tkyo, Japan.

[10]J. O’Hara, J.Higgins,” Human Factors Engineering Program Review Gide (NUREG-0711), Rev.3: Updated Methodology and Key Revisions”, BNL-96812-2012-CP(2012).

原子力発電所緊急対応の知的支援のための多重防護リスク解析フレームの適用研究

○吉川　榮和(京都大学)　楊　軍(華南理工大学)

楊　明(深圳大学)松岡　猛(宇都宮大学)

発表の構成

１．はじめに

２．統合型多重防護リスク解析フレームについて

３．原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援に関するプロジェクトについて

４．原子力発電所の緊急対応へのDiDリスク解析フレームの適用

５．結び

1．はじめに

- 中国華南理工大学電力学院の楊軍准教授主導の『原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援のための要素技術の研究』プロジェクト（2022-23）に日本から吉川，松岡が協力している。
- 本発表では、発表者らの提唱した多重防護を考慮したリスク解析フレームを用いて、想定外事象の重畳でシビアアクシデント事態に至る可能性のある緊迫した状況下、原発を運転する人間組織が適切に対応できるように、人間と機械システムで構成される総合システムの環境と手段を整備し、かつ運転員を知的支援するための研究状況を報告する。

2. 統合型多重防護リスク解析フレームについて

2.1　統合型多重防護リスク解析システムとは

2.2　コアシステムの定義と役割

2.3　支援ツールキットの分類

2.4　適用研究例

2.1　統合型多重防護リスク解析システムとは

〇多重防護（DiD：Defense-in-depth）とはIAEA提唱の原子力施設の5つの防護層である。

〇緊急時対応ではとくに第4層（シビアアクシデント防止）と第5層（環境への放射線影響の軽減）が対象

〇統合型多重防護リスク解析システムは、３つのコアシステムと付随する種々の支援ツールキットで構成

2.2コアシステムの定義と役割

コアシステムは、DiDリスク状態推定・シナリオ生成器、プラントDiDリスクモニタ、信頼性モニタの3つで、そこでの基本用語を以下のように定義する。

(1)DiDリスク状態とは対象とするプラントがもたらしうるリスクをその厳しさと緊急度でランク付けし、いくつかのレベルに分ける。

(2) そしていくつかのレベルに分けた個々のリスク状態平面内で、リスクが拡大してより厳しい状況のDiDリスク平面に発展しないための防護壁の存在を考慮してリスクの動的変化を追跡するものです。

(3)信頼性モニタはあるシステム、サブシステム、ないしコンポーネントがその防護機能を発揮してより厳しいリスク状態に発展するのを防止できる確実さの程度（信頼度）を求めるものです。

2.3　コアシステムの役割と具体的な方法

名称	役割	具体的方法の例示
DiDリスク状態推定・シナリオ生成器	対象システムがある時点でどんなリスク状態にあるかを推定、現在のリスク状態が内的，外的な要因によって今後どのようなシナリオで変化していくか予想。	様々な過渡的な状態遷移のシナリオを種々の過渡，事故解析コードによるシミュレーションで導出
プラントDiDリスクモニタ	人間系と機械系の相互作用がもたらすDiDリスク状態の動的遷移を追跡する。	吉川、中川の開発したリスクモニタにより技術システムと人間組織の相互作用による状態遷移の分岐シナリオを生成し，動的並列シミュレーションを実現
信頼性モニタ	対象システムが引き起こす不都合なリスク状態の発展を抑制するためのシステムおよびそのサブシステム，コンポーネントの動作の信頼度を推定する。	システムの信頼度を定量的に求めるために」FTA/ETAや松岡のGO-FLOWを使用

2.4支援ツールキットの分類

- **統合型DiDリスク解析では、3つのコアシステム（(FT/ETA、リスクモニタ、GOーFLOW)以外に支援ツールとして以下のような方法を用いる.**
- リスク状態をもたらす要因やその影響度、リスク発生の防止対策を表形式で記述するFMEAのような定性的方法
- リスク要因の属性分類と生起確率などのデータベース化
- 事故事象の生起と発展、環境への影響などを表現する数学モデルに基づいて詳細に数値計算する各種のシミュレーションコード

2.5　適用研究例

（1）プラントDiDリスクモニタの開発とPWRシビアアクシデント発生時の構内緊急対応行動の検討

シンビオ社会研究会ホームページ　DiD Risk Monitor　http://sym-bio.jpn.org/homepage.php.

（2）シビアアクシデント発生による環境放射能放出事態に対する日本の原子力防災体制の検討

H.Yoshikawa, M.Yang, Z.Zhang, “What should be level 5 defence layer in post-Fukushima nuclear safety”, Proc. ISSNP2015, Aug.24-28, Kyoto, 2015.

（3）AP1000のSBLOCA対応支援用インタフェース設計へのリスクモニタ活用の検討

H.Yoshikawa, M. Yang: “Integrated Defence-in Depth (DiD) Risk Analysis System for Safety Operation of Nuclear Power Plants”, ICONE26-82639, ICONE26, July 22-26, 2018, London, UK.

原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援に関するプロジェクトについて

3.1 全体概要

3.2 安全性の監視と管理へのリスクの多層化

3.3 強化したモデリングと解析基盤の開発

3.4 緊急対応管理の「成功する道」の立案

3.5 運転のナビゲーションと監督

３．１　全体概要

- 楊　軍は中国広東省の支援を得て原子力発電所の事故時安全管理へのリスク解析の適用をテーマに2022-23年の2年間『原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援のための要素技術の研究』に関する研究プロジェクトを主導している。以下では、同プロジェクトの４つの課題の状況を報告する。

参考文献　吉川榮和、楊軍、楊明、松岡猛、“京都ワークショップ（より高度なリスク解析法の実現を目指して）報告”、Symbio　News　and Report、Vol.12, No.4, 2023.

３．２
第1の課題：安全性の監視と管理へのリスクの多層化

- リスク情報に基づく知的な意思決定支援システムを構成する基本概念として、次の3つの要素を提起。

①重要安全機能のモニタリングによりプラントの安全状態を俯瞰する

②成功する道の立案により極端な条件下で想定外の事象発生時の策を提供する

③運転のナビゲーションと監督により運転員に有効なタスク実行のための手順の案内を行うとともにプロセスに対応している運転員の対応状況を監督する

- 楊軍はとくに①について、どのように目標—機能の樹状図、成功の樹状図、状態の樹状図を組み合わせて重要安全機能モニタリングを構成すべきかを課題として挙げた。

3.3 第2の課題：強化したモデリングと解析基盤の開発

- ①松岡らが開発のGO-FLOWモデルを自動的に生成するツール、②GO-FLOWの解析機能を強化するアルゴリズム、③GO-FLOWの基盤の強化と最適化を進めている.
- 楊軍の指導学生何展宇は強化したGO-FLOW解析のアルゴリズムを示し、修復可能なPMSシステムの信頼性解析を例にどのような問題を解こうとしているのかを述べた。
- 松岡猛は、フェーズドミッションシステムにLOOP構造が存在する場合へGO－FLOWの解析法を拡張し、適用例を示した。

3.4 第3の課題
緊急対応管理の「成功する道」の立案
（「成功する道」の立案法として2つのオプションを提起）

①GO-FLOWチャートに対するグラフ横断解析で得た最小パスセットをもとに成功パスを追跡して立案する方法ーこれは機能実現と目標達成を高度な抽象レベルで達成する手順を求めるもので、運転員には手順のステップごとのガイダンスを与える必要がある。

②フロー図の知識表現と推論を組み合わせた方法ーこれはGO-FLOWモデルとは関係はなく、プラントパラメタのオンラインモニタリングをもとに状況を診断して対応策を推論する知識処理（ボロン希釈事故に対する手動補填操作を対象にケーススタデイを実施）

3.5 第4の課題：運転のナビゲーションと監督
（2つの方法で構成することを提案）

①GO-FLOWのモデル、トレンドへのインパクト解析等から時々刻々変わる目標達成の観点からその都度その都度の信頼度を計る方法を導出する。

②不安全な行為の同定、手順に基づくナビゲーションと監督、手順にはないパスのガイド、運転上の使命達成度モニタリング、トレンドへの影響度の予測、運転上のハザードの分析の機能を統合した知的な運転状態監督システムを開発する。

4. 原子力発電所の緊急対応へのDiDリスク解析フレームの適用

4.1　診断，予測と対策の主要な課題とは，ヘルスモニターと適切な治療法の選択である

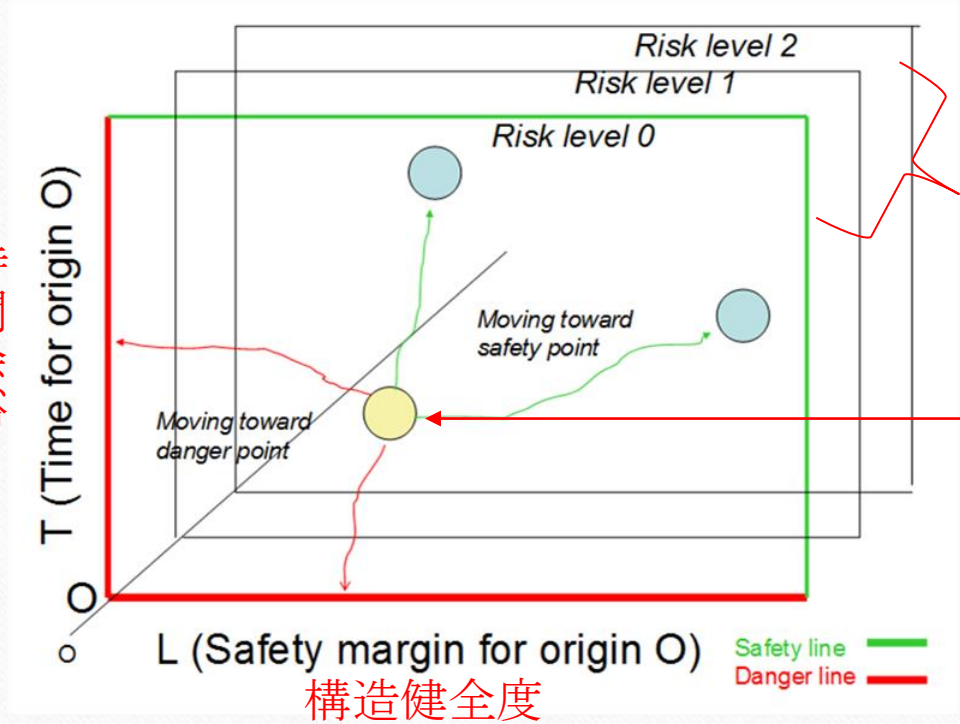
4.2　AIによるデータ同化として高速事故追跡システムを再構成する

4.1診断，予測と対策の主要な課題とは ヘルスモニターと適切な治療選択ーその１

- まず、原発の安全設計原理では4つの障壁（核燃料、被覆、原子炉冷却水の圧力境界、格納容器）の多重防護の仕組みで放射性物質の環境への放出防止、障壁の健全性をSTOP,COOLおよびCONTAINの3つの安全機能で保証しています
- そこで，①3つの安全機能の組み合わせで**リスクレベルの段階分け**、②個々のリスクレベルの中で動的に変化するリスクの程度をより厳しいリスクレベル段階に至るまでの**余裕時間**と施設の**構造的健全度**の2軸で定量化することを提起します。

Two stage visualization of dynamically changing risk

動的に変化するリスクの2次元平面での可視化



時間余裕

構造健全度

リスクレベルを段階分け

個々のリスクレベルの中で動的に変化するリスクの程度をより厳しいリスクレベル段階に至るまでの余裕時間と施設の構造的健全度の2軸で定量化

Difference of risk level by different plane
Quantification of risk by two factors in the same risk level;
- Time margin to reach the point of no return
- Degree of physical damage no more to be recovered

4.1診断，予測と対策の主要な課題とは ヘルスモニターと適切な治療選択-その2

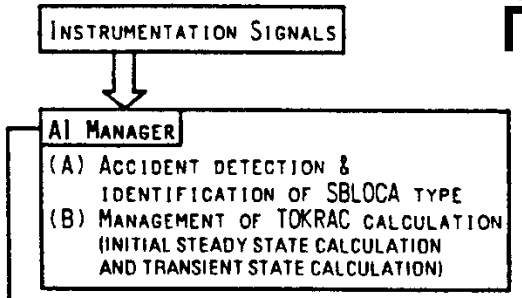
- 楊軍提起の**プラント安全目標を表わす知識表現**（個々の安全設備―重要安全機能―3つの安全機能のツリー構造）と、個々の**クリテイカル安全機能の状態の４段階表現**に、実際の原発の計装信号との対比関係を規定すればプラントの安全度、言い換えれば“健全度”を常時監視する「**ヘルスモニタ**」を構成できる。
- しかし人間ドックと同様でこのような「ヘルスモニタ」の情報提供は、「どうしたら健康を回復できるか」という問題とは別物である。
- そのためには**どこがどの程度悪くなっているのかを詳しく知った**うえで、**健康を回復するためにどの程度時間的余裕があるか**を考えて適当な治療法を選択して処置する。**これをどのようにしたらよいか？それは次の４．２**

4.2　AIによるデータ同化として高速事故追跡システムを再構成する

- 福島事故当初、東電は水位計では原子炉上部まで水があるから燃料は溶けていない，と発表していた．実際は水位計は正しくなかった。
- それなら燃料の温度を直接計るセンサーをつければよい．しかし燃料破損実験ならできても実用原発では無理．ではどうする？
- そこで参考になるアイデアがＡＩ分野での『データ同化』（プラント計装で正しく観測できる計測データを取り込んだシミュレーションで観測できない原子炉内部の安全上重要な燃料温度を精度よく推定する）
- その実例として「高速事故追跡システム」の3つの要素①カルマンフィルタの組み合わせた診断的プラント分析器、②超実時間高速事故シミュレータ、③双方を制御してトラブル発生検知、原因診断、将来予測、対応操作を提案するAIマネージャの基本的考え方を紹介

J.Wakabayashi, H.Yoshikawa, A.Gofuku, “Diagnostic Plant Analysis for Nuclear Power Plant Emergencies”, Proc. Intern’l Conf. on Man-Machine Interface in the Nuclear Industry (Control and Instrumentation, Robotics and Artificial Intelligence), 15-19, Feb. 1988, Tokyo, Japan.

高速事故追跡システムの3つの要素



AIマネージャ

次の診断的プラント分析器と超実時間事故シミュレータを制御し、事故の検知、事故の種類の診断、PWR一次系内部の詳細な予測と事故の将来予測を行う

(A)

IDENTIFICATION RULES FOR SBLOCA TYPE					TYPE OF SBLOCA	KALMAN FILTER MODELS NEEDED			
PP DECREASING	LP DECREASING	PC	PT	IR		MODEL (A)	MODEL (B)	MODEL (C)	MODEL (D)
RAPID	RAPID		INCREASING	CONSTANT	PORV STUCK OPEN				◎
RAPID	RAPID	INCREASING	CONSTANT	CONSTANT	PRIMARY PIPE BREAK	YES	YES	YES	◎
SLOW	SLOW	CONSTANT	CONSTANT	INCREASING	SGTR				○

PP : PRESSURIZER PRESSURE
LP : PRESSURIZER WATER LEVEL
PC : CONTAINMENT PRESSURE
PT : PRESSURIZER RELIEF TANK PRESSURE
IR : RADIATION MONITOR

◎ : QUICK-RESPONSE CHARACTERISTIC
○ : LOW-NOISE CHARACTERISTIC

診断的プラント分析器

プラント計装信号の実時間処理でSBLOCAの種類(PORV開固着、一次系破断、SGTR)の診断とカルマンフィルターにより漏洩量のような測定不能な安全上重要なパラメタを推定。これらの結果は超実時間シミュレータの入力ないし境界データとして利用する

(B)

CALCULATION CONTROL	INITIAL S.S. CALCULATION	TRANSIENT CONDITION
ESTIMATED RESULTS BY KALMAN FILTERS	TOKRAC : DETAILED DIAGNOSTIC RESULTS OF PRIMARY LOOP THERMAL-HYDRAULICS CONDITION	

超実時間事故シミュレータ

PWR一次系だけを対象に模擬
(1)実時間で事故を追跡する
(2)それを基に将来予測する

FIG. 5. Roles and functions of AI manager as required for effective computerized diagnostic plant analysis.

超実時間事故シミュレータ TOKRAC
（PWR一次系 のSBLOCA 事故模擬）

- PWR一次系の主要機器の接続をノード・ジャンクション法で考慮し、事故時核熱流力挙動を均質二相流モデルで計算
- TOKRAC への様々な外部入力を下図に示す

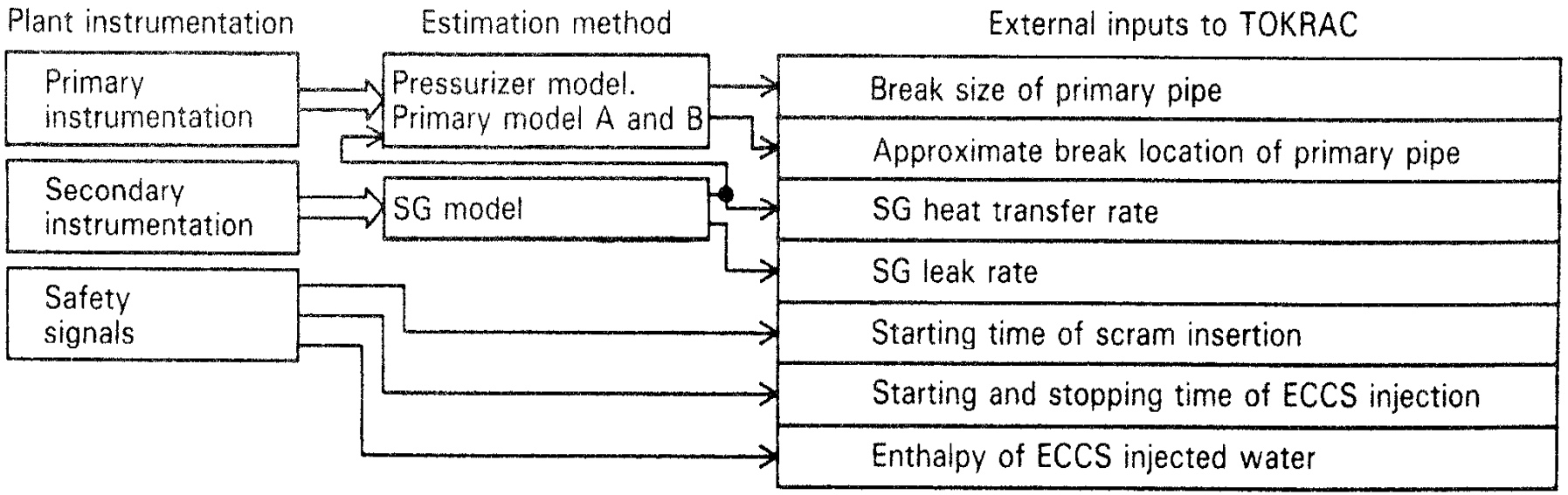
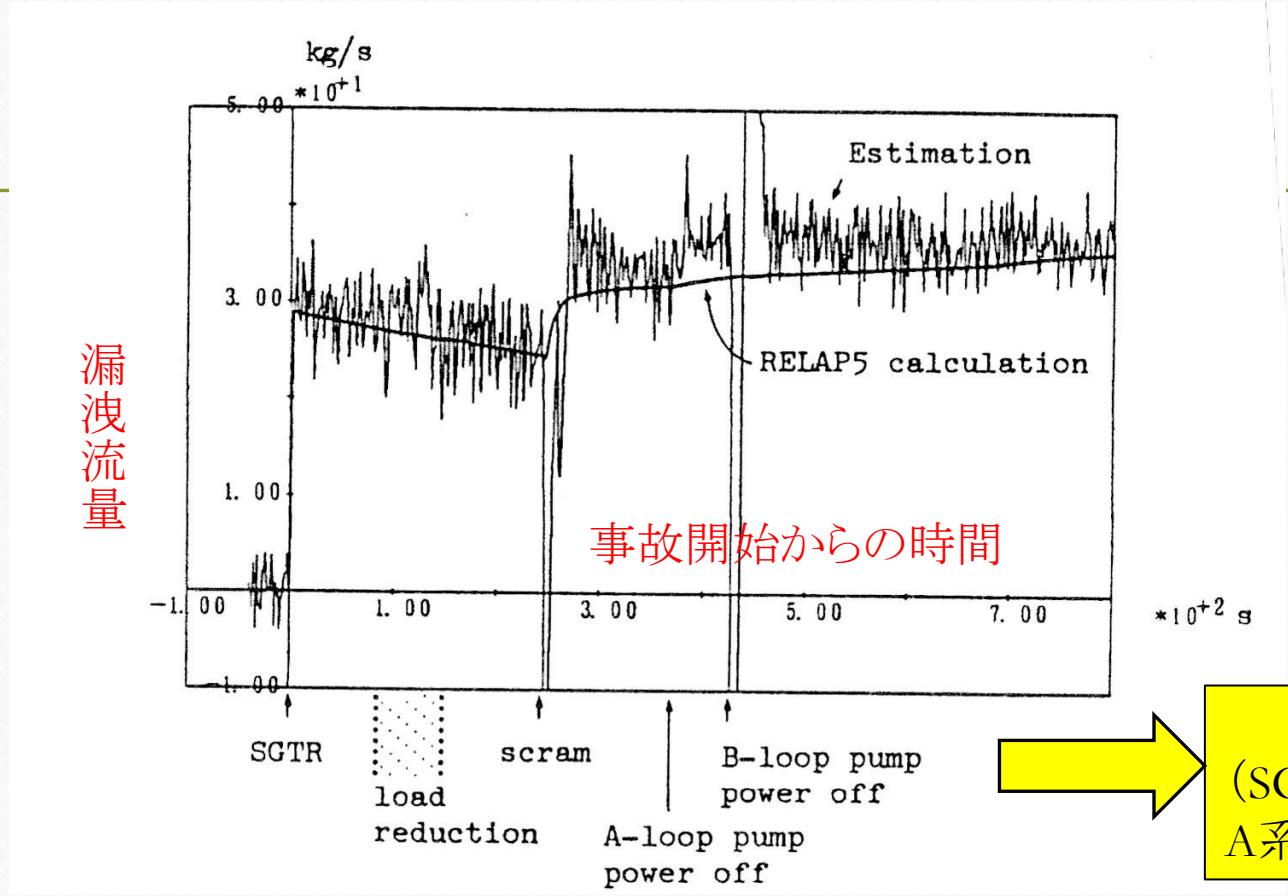


Fig. 3. Relationship between external input to TOKRAC and observed signals from plant instrumentation.

SGTR漏洩流量のカルマンフィルタによる予測とRELAP5による計算の比較



主な事象発生の説明
（SGTR発生、負荷減少、スクラム、A系ポンプ停止、B系ポンプ停止）

5. 結び

- 本発表では，楊　軍氏が中国広東省の支援を得て進めている『原子力安全と緊急時対応のためのリスク情報に基づく知的意思決定支援のための要素技術の研究』プロジェクトに，著者が取り組んだ研究が如何に活用できるかを中心に紹介した.
- 全体をデータ同化問題としてDiDリスクモニタと現代の進んだAIソフトとVRによるデイジタルツインによりインテリジェントな緊急時対応支援技術が実現可能と期待している.

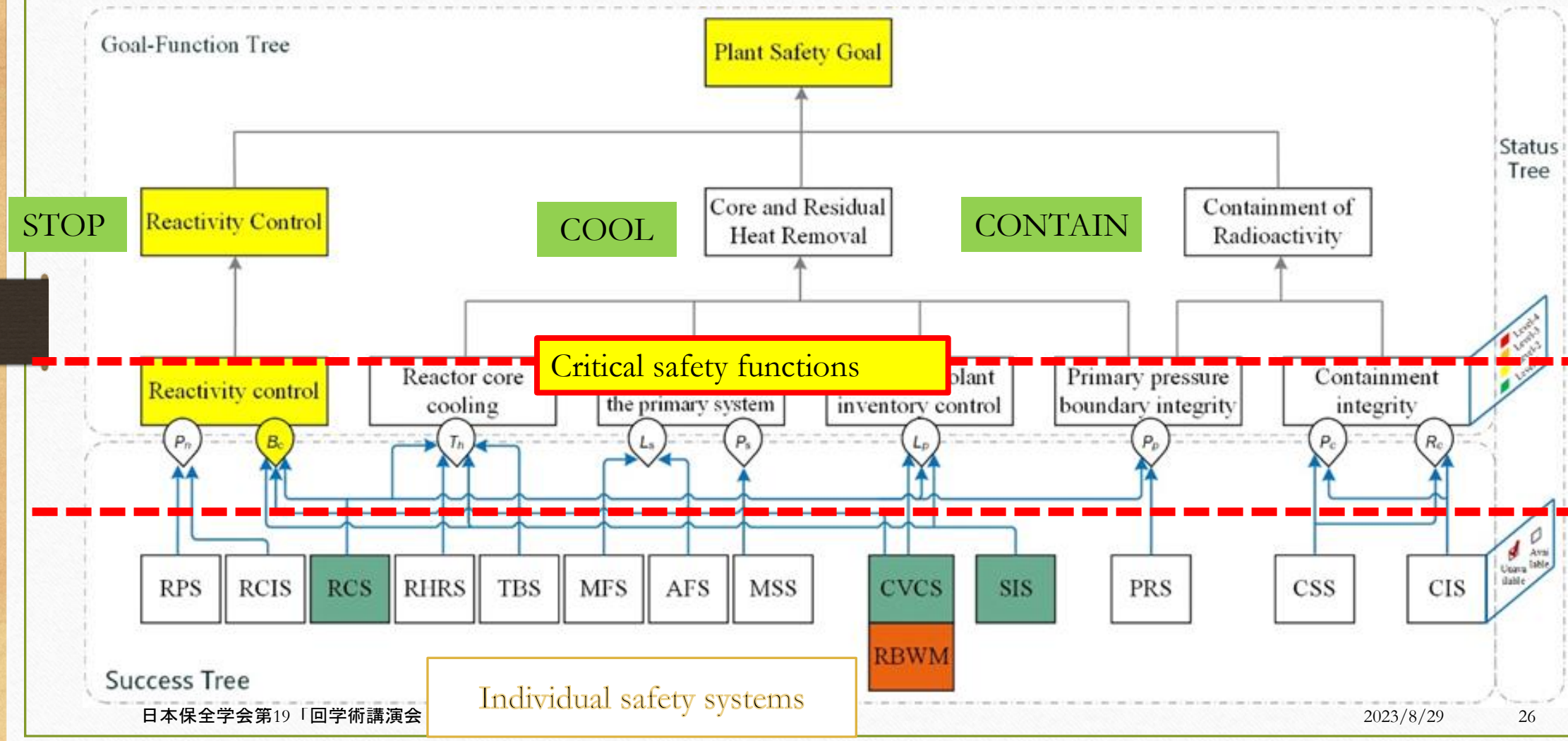
以上で発表を終わります。ご清聴ありがとうございました。

Acknowledgements

This work is supported by Soft Science Research Project of Guangdong Province（Grand No. 2022A0505050007）.

This work is also supported by the ZE Research Programme IAE, Kyoto University (ZE2023B-29)

プラント安全目標を表わす知識表現（個々の安全設備―重要安全機能―3つの安全機能のツリー構造）



個々のクリテイカル安全機能の状態の４段階表現

State	Description	Alarm Priority/Severity Level
Negligible	The critical safety function is operational.	1
Moderate	The critical safety function is partially degraded.	2
Critical	The integrity of a critical safety function is severely damaged.	3
Catastrophic	The integrity of a critical safety function is completely lost.	4