

人間信頼性分析手法との調和を考慮し
た人間工学設計開発手法の確立

2022年1月

真塩 健二

内容

第1章	序論.....	4
1.1	研究の現状と背景.....	4
1.2	論文の目的と構成.....	8
第2章	原子力発電所分野における人間工学を適用した制御室開発プロセスと ヒューマンエラー関連について.....	9
2.1	はじめに.....	9
2.2	人間工学を適用した制御室開発プロセスについて.....	10
2.3	原子力発電所分野におけるヒューマンエラー関連研究について.....	13
2.4	人間信頼性分析について.....	25
2.5	既存の制御室開発プロセスにおける課題.....	31
2.6	結果と検討.....	33
第3章	最新の認知リスク分析手法の想定を設計開発プロセスに取り込む手法 の開発とその実践適用.....	35
3.1	はじめに.....	35
3.2	リスクマネジメントを考慮した制御室設計統合化プロセスの検討.....	36
3.3	事例に基づく開発プロセスの詳細化と有効性評価.....	47
3.4	結果と検討.....	67
第4章	最新リスク分析をさらに網羅性あるシナリオ開発につなげる STAMP/STPA手法をベースとしたヒューマンコントローラモデルの適用.....	68
4.1	はじめに.....	68
4.2	STAMP/STPA分析との統合化プロセスの検討.....	69
4.3	結果と検討.....	75
第5章	決定論的手法に基づくトップダウン的マンマシン設計プロセスの導入 と効果の確認.....	76
5.1	はじめに.....	76
5.2	機能モデルと人間工学プロセスの関係.....	77
5.3	Success Pathの開発.....	80
5.4	Success PathのHSI設計への適用.....	81
5.5	結果と検討.....	85
第6章	運転シミュレータを用いたヒューマンパフォーマンス自動測定手法の 開発.....	86
6.1	はじめに.....	86
6.2	開発目標と開発プロセス.....	87
6.3	評価対象の選定.....	90

6.4	自動評価モデルの開発.....	91
6.5	プロトタイプ評価.....	103
6.6	結果と検討.....	112
第7章	結論.....	113
謝辞	116	
略語一覧	117	
参考文献	120	
研究業績	125	
付録A	：認知エラータイプからの設計方策の検討結果.....	130
付録B	：統合的な H/E 対処分析結果.....	141

第1章

序論

1.1 研究の現状と背景

原子力発電所の安全設計においては、設計想定や決定論的分析に基づく設計開発に加え、確率論的リスク分析によるリスク情報を活用したプラント系統機器の設計展開に関する研究が行われている。安全設計の観点では機器の信頼性設計のみならず、プラントの運転に携わる要員（運転員）のヒューマンエラーの発生を最小限化することが必須である。

すなわち、過去の原子力発電所における事故事象の分析においても、事故事象の発生や収束に人間の関与が必須であり、確率論的リスク分析においても人間信頼性の寄与、すなわち、ヒューマンエラーが大きな要因となるからである。

ヒューマンエラーを未然に防止する取り組みは、1979年にヒューマンエラーが主たる原因となった、米国スリーマイルアイランド2号機の炉心損傷事故の教訓反映から始まり、運転員の力量や運転組織体制を目的とした人的組織的な側面、すなわちシミュレータを用いた運転員訓練強化や安全文化の醸成の面だけでなく、原子力プラントの運転を司る原子炉制御室／制御盤（中央制御盤）システムの設計強化という側面からも研究が進められている。

中央制御盤システムは、原子力発電プラントの監視、操作を遠隔で集中的に行うシステムであり、プラント発電機能／安全機能の維持や事故時の対応として中心的役割を担う。また、原子力発電プラントの機能を維持する系統機器システムとこれらを監視、操作を行う運転員のインタラクションを司るマンマシンインタフェースとして、ヒューマンエラーを起こさないよう、人間工学を考慮した体系的な設計開発プロセス（人間工学プロセス）が適用されている。

人間工学プロセスは、人間工学分析結果を要件として、設計や検証を行い、検証／妥当性確認において十分なパフォーマンス評価が得られない場合は、分析の想定や設計の見直しを行う。

原子力発電所の設計や安全審査においては、確率論的リスク分析として、原子炉の炉心損傷に至るリスクを定量的に求め、当該リスク値（炉心損傷確率）を低減するよう、機器の信頼性設計へ展開している。当該リスク値の定量評価においては、機器の信頼性（故障率）だけでなく、ヒューマンエラーによる人的過誤率の寄与も大きいことから、上述の人間信頼性

分析として、事故時イベントにおける人的過誤率の推定を実施し、当該リスク値の計算に組み入れている。人間信頼性分析は、リスク値の分析を行って機器の信頼性設計に組み込む設計手法の開発当初（1980年頃）から、如何に正確に人的過誤率を推定するかという研究が行われ、様々な評価手法が開発されている。2020年頃に開発された最新（第三世代と言われる）の人間信頼性分析手法では、人間の認知行動のばらつきを如何に正確に、かつ、体系的に予測するため、人間の認知プロセスをマクロ化（標準化／巨視化）したマクログニティブモデルを適用している。

人間工学プロセスうち、ヒューマンエラー未然防止のための方策は、確率論的リスク分析の結果から、リスク上重要な人的操作を抽出して、当該人的操作については特別な注意を払うこと、すなわち、タスク分析等の人間工学分析を行い、中央制御室監視操作盤インタフェース設計、操作手順書の設計、運転訓練プログラムの設計への展開を行っている。

現状の枠組みでは、リスク上重要な人的操作を重要度指標といった閾値のみで抽出するが、その背後にある想定条件（ヒューマンエラー因子、行動形成因子）を考慮した体系的な設計プロセスフレームワークがなく、設計者の経験値や見識に依存するところが多いとの課題があった。この課題は、人的過誤率の算定を行う人間信頼性分析の手法が分析者の技量、経験に左右されない体系化された分析プロセスとして十分確立していないとの課題があること、また、人間信頼性分析の分析プロセスで得られるヒューマンエラーメカニズムを十分に設計改善のインプットとして設計プロセスに活用されていないなどの背後要因に基づく。

一方、上述したマクログニティブモデル適用による人間信頼性分析手法では、人的過誤率を求める過程において、想定条件（ヒューマンエラー因子、行動形成因子等）が体系的に得られることから、当該フレームワークを活用して、人間信頼性分析プロセスと人間工学プロセスの統合化を行い、認知プロセスレベルの影響因子を考慮したヒューマンエラーの未然防止策を体系的に中央制御盤システムの設計へ展開できると考えた。

また、最新の人間信頼性分析においても事故時イベントで生じるエラーモードについては、想定するシナリオや手法、或いは分析者の知識や経験により、分析結果についてばらつきが生じる可能性がある。そこで、当該人間信頼性分析を強化する観点から、STAMP/STPA手法をベースとしたヒューマンコントローラモデルを適用し、シナリオ選定の質や分析者の知識・経験を極力排除した体系的な手法を考案した。

一方、確率論的リスク分析での目標は、炉心損傷に至るイベントを洗い出し、炉心損傷を防止するための設備や手段の信頼性について評価することであり、決定論的な観点で炉心損傷を防ぐ安全機能を特定し、その安全機能を司る機器やその操作に着目してヒューマンエラーの防止を図ることが有効である。決定論的な観点でのヒューマンエラー防止は、既存のプロセスで段階的詳細化して設計を行うことで対応しているが、系統や機器が多数におよび複雑化する場合は、重畳的な観点で安全機能を直接機能、維持する機器やその操作手段に着目してこれをマンマシン設計に直接適用することが有効と考えたため、その手法について検討した。

また、人間信頼性分析による机上分析で不足する想定条件を補完するため、運転シミュレータを用いたパフォーマンス評価システムを導入し、当該評価システムから机上では想定していないエラーモードを確認するプロセスを統合した。なお、当該パフォーマンス評価システムは、先行研究があるが、強化されたリスク分析手法である、認知プロセスのエラー率を測定する場合は手動で評価することに限界があり、これを実践的にするものとして、自動的にパフォーマンス評価情報を取得して、評価を行うシステムを考案し、有効性を確認した。

以上を総括し、課題と本研究での効果について以下の通り纏める。なお、当該課題に対して、本論文で研究対象として取り扱う章番号を（）内に示す。

課題1：リスク上重要なヒューマンアクションは、リスク重要度評価指標を閾値として、特定される一方、その背景となるエラーモードや行動影響因子について設計への体系的な展開がされていない。

⇒人間信頼性分析から原子力発電所制御室設計への体系的な展開を検討し、また、事例に基づく適用効果を確認する。(第3章)

効果1：人間信頼性分析の想定条件をより具体的・体系的に制御室設計開発に展開できる。

課題2：人間信頼性分析においては、想定するシナリオや手法、或いは分析者の知識や経験により、分析結果についてばらつきが生じる。

⇒当該人間信頼性分析を強化する観点から、STAMP/STPA 手法をベースとしたヒューマンコントローラモデルを適用し、シナリオ選定の質や分析者の知識・経験を極力排除した体系的な手法を考案し、事例に基づく適用効果を確認した。(第4章)

効果2：分析者の技量に依存しない、分析の品質の向上が図れる。

課題3：確率論的分析手法の補完と決定論的分析手法からの設計展開の強化

⇒確率論的リスク分析での目標は、炉心損傷に至るイベントを洗い出し、炉心損傷を防止するための設備や手段の信頼性について評価することであり、決定論的な観点で炉心損傷を防ぐ安全機能を特定し、その安全機能を司る機器やその操作に着目してヒューマンエラーの防止を図ることが有効である。

⇒決定論的な観点でのヒューマンエラー防止は、既存のプロセスで段階的詳細化して設計を行うことで対応しているが、系統や機器が多数におよび複雑化する場合は、重畳的な観点で安全機能を直接機能、維持する機器やその操作手段に着目してこれをマンマシン設計に直接適用し、これにより得られる設計効果について確認した。(第5章)

効果3：決定論的な観点で炉心損傷を防ぐ安全機能に直接影響のある重要なタスク、系統機器のマンマシン設計強化による、確率論的分析手法による設計の補完、品質強化が図れる。

課題4：人間信頼性分析による机上分析で不足する想定条件を補完

⇒運転シミュレータを用いたパフォーマンス評価システムを導入し、当該評価システムから机上では想定していないエラーモードを確認するプロセスを統合した。なお、当該パフォーマンス評価システムは、先行研究があるが、強化されたリスク分析手法である、認知プロセスのエラー率を測定する場合は手動で評価することに限界があり、これを実践的にするものとして、自動的にパフォーマンス評価情報を取得して、評価を行うシステムを考案し、有効性について確認した。(第6章)

効果4：人間信頼性分析において机上では想定していないエラーモードの特定を行うことで、分析にフィードバックするとともに、運転員毎にパフォーマンス評価を行うことで、訓練へのフィードバックも可能となる。

以上の研究成果を中央制御盤システムの設計開発に展開することにより、プラントレベルで行われる決定論的分析／確率論的リスク分析の想定条件を、現実的な作業環境や中央制御盤という作業システムで起こりえるヒューマンエラーの側面から精緻化するとともに、その想定条件に基づく決定論的分析／確率論的リスク分析結果を活用することにより、有効なヒューマンエラー未然防止策を適用することができる。

1.2 論文の目的と構成

本論文では、原子力発電所の運転員の認知プロセスをマクロ化（標準化／巨視化）したマクログニティブモデル（Macro-cognitive function）に基づく第三世代人間信頼性分析手法の開発に注目し、人間工学設計開発プロセスの強化を目的とした。このため、第三世代人間信頼性分析手法での抽出される行動影響因子やヒューマンエラーモードを設計開発プロセスに取り込む手法の開発、第三世代人間信頼性分析手法をさらに網羅性あるシナリオ開発につなげる STAMP/STPA 手法をベースとしたヒューマンコントローラモデルの適用などの研究を行った。

本章以降の構成は以下の通りとした。

すなわち、第2章では原子力発電所分野における人間工学を適用した制御室開発プロセスとヒューマンエラー関連研究について、第3章では最新の間信頼性分析手法の想定を設計開発プロセスに取り込む手法の開発とその実践適用について、第4章では最新人間信頼性分析をさらに網羅性あるシナリオ開発につなげる STAMP/STPA 手法をベースとしたヒューマンコントローラモデルの適用、第5章では従来決定論的な段階的詳細化設計開発プロセスに重畳的に適用するトップダウン的マンマシン設計プロセスの導入と効果の確認、第6章ではリスク分析の想定シナリオの検証や想定しないエラーモード発掘のための、認知レベルでのヒューマンパフォーマンスを運転シミュレータの訓練を通じて自動的に評価するシステムの開発について記述し、第7章で結論とした。

第2章

原子力発電所分野における人間工学を適用した制御室開発プロセスとヒューマンエラー関連について

2.1 はじめに

分析で得られる潜在的ヒューマンエラーやその要因、また、実際に起こったヒューマンエラーや、当該ヒューマンエラーの要因分析から得られる背後要因に対して、未然防止や再発防止を行うため、ヒューマンエラーマネジメントとして、1980年代ごろから、認知的エラーのメカニズムを分析し、これを設計改善に活用している[5][6] [7] [8] [9] [10][11][12]。

原子力発電所分野におけるヒューマンエラー関連研究においては、確率論的リスク分析アプローチによるヒューマンエラー分析[2] [3]、また、1979年に起こった米国スリーマイルアイランド発電所2号機（Three Mile Island Unit-2, TMI）でのヒューマンエラーを起因とした事象の要因分析による再発防止を制御室設計開発のプロセスの中で担保する人間工学設計開発プロセスの研究[1][4]がある。当該研究は、米国にて実施され、日本でも米国の研究成果をフォローする形で、ガイドラインの導入が進められている。

本章では、まず、TMI事象を起因として研究開発がされ、現在、米国をはじめとした、日本を含む国際的なガイドとして導入が進められている、人間工学を適用した制御室の開発（人間工学プロセス）の概要を述べ（2.2章）、原子力分野におけるヒューマンエラー関連研究について整理し（2.3章）、確率論的リスク分析アプローチによるヒューマンエラー分析として実施している人間信頼性分析について述べたうえ（2.4章）、エラーマネジメントの視点から、現在の人間工学プロセスの課題について論じる。（2.5章）

2.2 人間工学を適用した制御室開発プロセスについて

原子力発電所では、安全で効率的な運転を実現すべく、人間工学を適用した制御室の設計開発を行っている。具体的には、プラント／系統機器の性能や制約条件のもと、制御室で監視操作タスクを行う運転員の体制や能力／限界を理解し、運転員のパフォーマンスを最大限に生かすよう、制御室の設計開発を行っている。

図 2.1 に人間工学を適用した典型的な制御室設計開発プロセス（人間工学プロセス）を示す[1]。

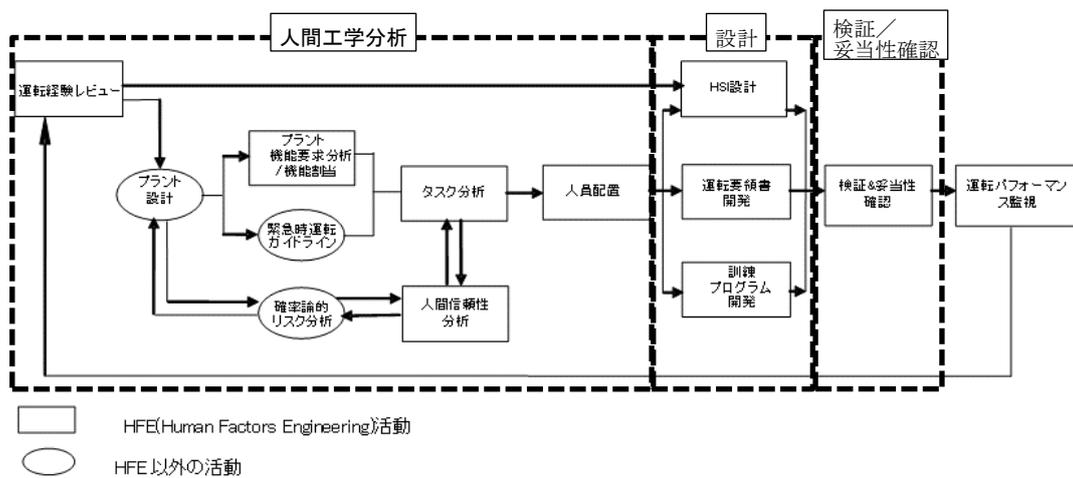


図 2.1 人間工学プロセス ([1]より作成)

人間工学プロセスは、プラント設計や安全解析をベースとして作成される緊急時運転ガイドライン、確率論的リスク分析をインプットとして、以下のようなプロセスから成り立っている。

- i) 人間工学分析：プラント機能分析／機能割当（人間と機械（自動化））、タスク分析、人員配置（対応人数、配置分析）などの人間の特性や行動の制約を考慮した人間工学的観点からの分析
- ii) 設計：人間工学分析結果を踏まえた、マンマシンシステム（Human-System Interface (HSI)）、運転要領書／手順書開発、訓練プログラム開発といった、ハードウェア／ソフトウェアの設計
- iii) 検証／妥当性確認：エルゴノミクス設計ガイドに適合していることの検証や、設計を統合した実際の運転環境条件を模擬したシミュレータ等を用いた運転員の

パフォーマンス評価。

人間工学プロセスは、人間工学分析結果を要件として、設計や検証を行い、検証／妥当性確認において十分なパフォーマンス評価が得られない場合は、分析の想定や設計の見直しを行う[34][35]。これを遂行する場合には、各分析、設計、検証／妥当性確認における各活動で発生した要件をトラッキングして、橋渡しを行うシステムが必要であり、設計開発支援システムとしてそのデータベースの構築をしている。

人間工学プロセスうち、ヒューマンエラー未然防止のための方策は、確率論的リスク分析 (Probabilistic Risk Analysis, 以下 PRA という) および人間信頼性分析 (Human Reliability Analysis, 以下 HRA という) の結果から、リスク上重要な人的操作 (Risk Important Human Action, 以下 RIHA という) を抽出して、RIHA については特別な注意を払うこと、すなわち、全ての RIHA についてタスク分析等の人間工学分析を行い、中央制御室監視操作盤インタフェース設計、操作手順書の設計、運転訓練プログラムの設計への展開を行っている。

RIHA はリスク重要度指標によって抽出される[25]。リスク重要度指標は、特定の事象 (機器の故障等) が生じた場合に、炉心損傷の至る確率 (Core Damage Frequency, 以下 CDF 値という) への寄与を測る指標であり、RIHA の抽出には、2つのリスク重要度指標(Risk Achievement Worth および Fussell-Vesely,以下それぞれ、RAW および FV という)により求める。すなわち、RAW は、 $RAW=(CDF(A=1)/CDF)$ と定義される。

ここで、 $CDF(A=1)$ とは、事象 A の発生率が 1.00 すなわち事象 A が必ず起こるとした場合の CDF 値を示す。FV は、全リスクに対する特定の事象の発生リスクの寄与を示し、 $FV=(CDF(A)/CDF)$ と定義される。ここで、 $CDF(A)$ とは、事象 A を含む各 CDF 値の和を示す。RIHA 抽出後人間工学を考慮した設計展開を行う際には、RIHA としてどのようなヒューマンエラー因子、行動形成因子があるかを分析し、このようなヒューマンエラーの要因を見極めた上で設計対策を考えていくことが必要となる。ところが、現状の枠組みでは、RIHA を重要度指標といった閾値のみで抽出するが、その背後にある想定条件 (ヒューマンエラー因子、行動形成因子) を考慮した体系的な設計プロセスフレームワークがなく、設計者の経験値や見識に依存するところが多いとの課題があった。

この課題は、ヒューマンエラー率 (Human Error Probability, 以下 HEP という) の算定を行う HRA の手法が分析者の技量、経験に左右されない体系化された分析プロセスとして十分確立していないとの課題があること、また、HRA の分析プロセスで得られるヒューマンエラーメカニズムを十分に設計改善のインプットとして設計プロセスに活用されていないなどの背後要因に基づく。

一方、近年、HEP の精度を高めることを目的に、HRA の分析プロセスのフレームワークの体系化が検討されたこと、また、HRA は HEP の算定が中心である一方、HEP

を算定するための想定条件（ヒューマンエラー因子、行動形成因子等）が得られることから、**HRA** をヒューマンエラー管理/分析としてとらえ、当該フレームワークを活用して、**HRA** での想定条件を体系的に既存の設計プロセス（人間工学プロセス）に取り入れられる可能性がある。

2.3 原子力発電所分野におけるヒューマンエラー関連研究について

原子力発電所分野におけるヒューマンエラー関連研究においては、大きく2つの潮流がある。この2つは共に米国において研究が開始され、日本においてもこれをフォローする形で開発プロセスに取り込まれている。

一つ目は、確率論的リスク分析アプローチによるヒューマンエラー分析である。もともと原子力発電所安全設計では決定論的なアプローチで安全設計や審査がされてきたが、1960年代初頭に、F.R. Farmerが、原因を制限した機器の信頼性を基に原子力の安全を考慮するアイデアを提案し、原子炉安全研究(WASH-1400)の中で、原子力発電所が、PRAを用いた体系的な形で分析できることが、1975年までに報告された。この研究報告をもとに、リスク分析を用いた安全評価のアプローチが開発され、安全設計や審査にも取り込まれている[2]。

当該リスク分析においては、人間信頼性分析(Human Reliability Analysis, HRA)として、人間が失敗する確率についても検討がされ、ヒューマンエラーを潜在的な人的過誤率(Human Error Probability, HEP)として定量化する試みがされている[3]。

二つ目は、ヒューマンエラーが原因となって炉心損傷事故を起こしたTMI2号機の事象を契機として、体系的な手法により、制御室の設計レビューを行うガイドラインが米国原子力規制局(NRC)から発行され[4]、後に、人的組織的な側面(運転体制、資質、運転手順書、訓練プログラム)も含めた体系的な制御室設計ガイドが制定され、人間工学設計開発プログラム(Human Factors Engineering Program, HFE) [1]として安全設計/安全審査に取り込まれている。

現在、米国原子力発電所の安全設計審査においては、上述の前者(リスク分析)は安全設計審査項目の第19章(Sever Accident)として、後者は、第18章(HFE)としてそれぞれ安全設計審査の要件となっている。また、とくにヒューマンエラーに関わる領域については、18章で体系的に審査をすることとしており、上述のHRAとのインターフェースについても18章側で審査がされる。

図2.2は、米国原子力発電所の安全設計審査における、HFE関連規制について纏めたものである。

TMI2号機事故分析に基づく、規制強化のアクションプラン(NUREG-0660、後にアクションプランの明確化を目的とした補遺版NUREG-0737)が米国原子力規制局(U.S. Nuclear Regulatory Commission, NRC)より発行され、さらに、NUREG-0737の付録(Supplement-1)として、既設原子力発電所中央制御盤の人間工学観点からのレビュー

基準が提起され、これに基づき米国発電所全てに対して中央制御室の人間工学的観点のレビューがされた。当該設計レビューは、2.2 節で述べた制御室開発プロセスと人間工学的設計観点／基準を纏めた設計ガイド (NUREG-0700) として纏められた。前者の制御室開発プロセスは、その後、新設炉プラント向け審査ガイド (後に改造工事を含む) として独立した技術ガイド (NUREG-0711) として分離され、また、NUREG-0700 は、設計ガイドに特化した形で最新の技術動向を反映した形で適宜改訂され、今日に至っている。

国際的にも、国際電気標準会議 (International Electrical Commission, IEC) から、制御室設計ガイド (IEC 60964) が発行され、国際原子力機関 (International Atomic Energy Agency, IAEA) から、人間工学設計開発プロセスに関するガイド (SSG-51) が 2019 年に発行された。

なお、我が国においても、当該 NRC のアクションプランに基づき、原子力安全委員会 (当時) から「我が国の安全確保対策に反映させるべき事項」として、設計や運用の対策強化を目的とした、52 個に渡る改善項目を発行しており、当該 52 項目の一つとして、制御室の人間工学的観点からの設計強化が指摘され、国内の制御室の設計が強化されてきた。また、2021 年 4 月には、原子力規制委員会から、「人間工学設計開発に関する審査および検査のガイド」として米国の制御室設計開発プロセスガイド (NUREG-0711) や IAEA SSG-51 を参考として審査・検査ガイドとして発行されている。

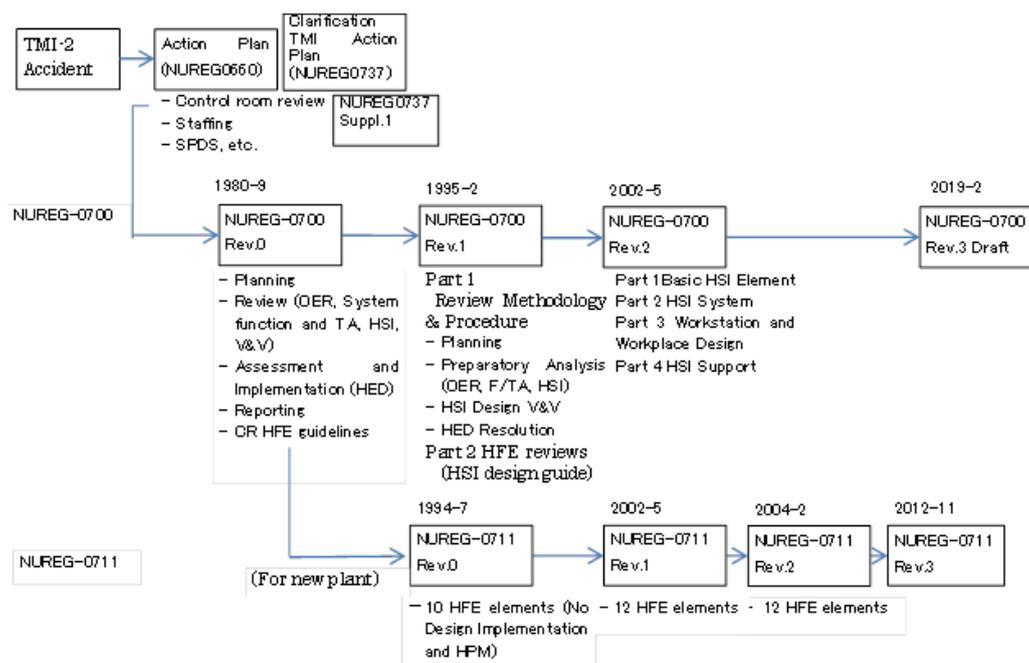


図 2.2 米国原子力発電所人間工学関連規制の動向

最近では、前者のリスク分析においては、HRA で分析される HEP の精度を高めるため、認知的タスクの体系的な HEP 算出の方法論について検討がされるとともに、後者

においては、デジタル HSI の取り扱いや段階的な検証手法の検討が進められている。

2.3.1 ヒューマンエラーマネジメントに関する関連研究について

本章では、原子力発電所分野におけるヒューマンエラー関連研究でも歴史的な基礎部分となっている、ヒューマンエラーメカニズムに関する関連研究、ヒューマンエラー分析、エラーマネジメントについて整理したものを示す。

2.3.2 ヒューマンエラーメカニズムに関する関連研究

ヒューマンエラーに関する認知的心理学的モデルとして著名なものは、1980 年初頭に発行された Rasmussen のスキル・ルール・知識 (SRK; Skill, Rule and Knowledge) モデル [5]、Norman のスリップ(Slip)モデル[6]がある。

図 2.3 に示す通り、SRK モデルは、決められた環境およびシステムにおける人間の行動様式を、スキルベース (Skill-based behavior)、ルールベース (Rule-based behavior)、知識ベース (Knowledge-based behavior) の 3 つに分類、定義したものである。スキルベースは、同じ入力に対して同じ反応や行動を示す自動化されたパターンにより、意識せずに、与えられた入力情報 (Sensory input) を基に、同じ反応や行動 (Signal Actions) を行う行動様式で、習熟した作業環境やシステムにおいて認知行動をバイパスして行う様式である。ルールベースは、習熟した作業環境やシステムにおいて、予期した入力情報に対して、手順書や決められたルールに基づき行動する様式である。この場合、行動計画は予め手順書で定められているため、作業者は入力情報を認知したうえ、どの手順に基づくかを特定し、その手順に基づいて行動する認知活動がされる。

知識ベースは、不慣れな作業環境やシステムにおいて、作業者本人が以前の経験やルールに基づかない行動様式であり、与えられた入力情報を特定し、特定された入力情報に対して、作業者が保有する知識や類似する成功失敗経験を総動員して、作業目標を達成する意思決定を行い、行動計画を立てたうえ、当該行動計画に対するタスク手順を決めて行動する。

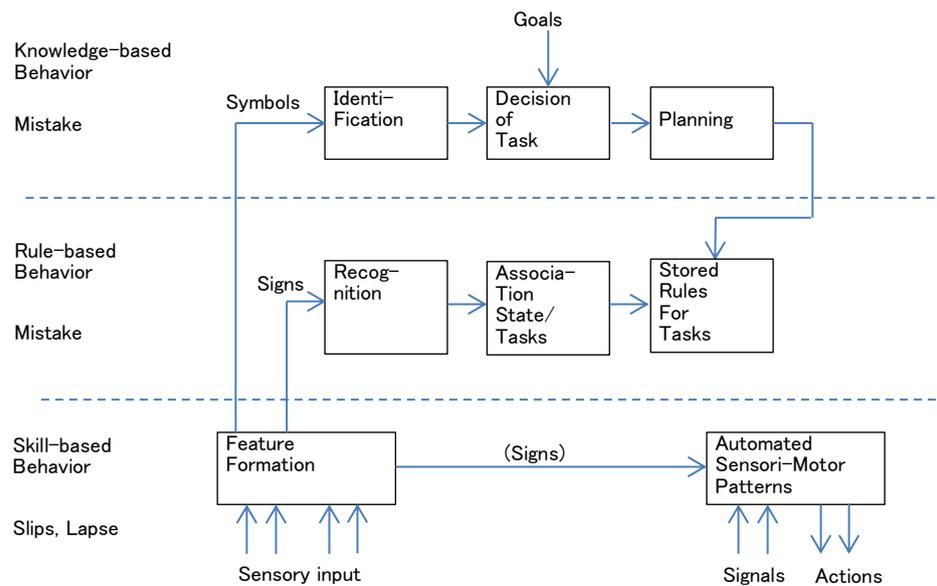


図 2.3 SRK モデル ([5]より作成)

Reason [7][9]は、Rasmussen のスキル・ルール・知識モデルを応用し、SRK の各段階における認知行動のプロセスと起こりえるヒューマンエラーについて包括的に整理し、物事の検知を行う段階のエラー (Slips と Lapse)、それに続く段階でのエラー(Mistake)に分類した。図 2.4 に示す通り、非安全行動 (UNSAFE ACTS) は意図しないものと意図したものに分類され、意図しないものには、スリップ/すり抜け (SLIP) および失念 (LAPSE) に、意図したものには、思い込み/ミステイク(MISTAKE)および違反 (VIOLATION) にそれぞれ分類される。スリップ/すり抜けは不注意のミス、失念は記憶のミスであり、SRK モデルでは Skill ベースの行動様式として当てはめることができ、思い込みは意図行動様式の失敗として、ルールベースまたは知識ベースの行動様式に特徴づけがされる。

また、違反を除く上記の 3つのタイプは基本的なエラータイプと分類付けをしている。

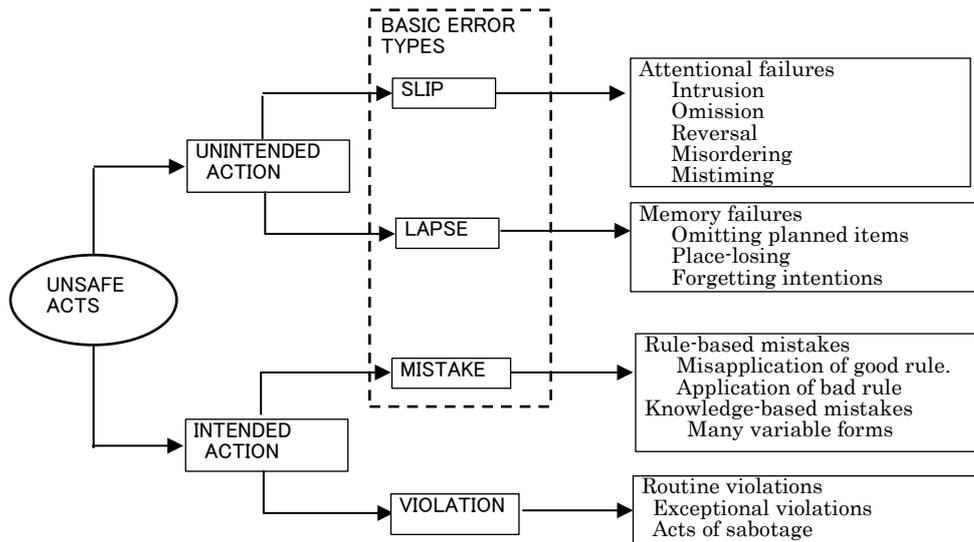


図 2.4 ヒューマンエラーの分類 ([7][9]より作成)

Card[8]らは、認知モデルを活用し、人間とコンピューターの関わりを工学的に分析する手法（GOMS, Goals, Operators, Methods, and selection rules for the methods）を提唱した。図 2.5 に示す通り、人間の情報処理モデルを、感覚プロセス、認知プロセス、運動プロセスなどのプロセスに分類し、各プロセスに要する時間を実験的に収集し、認知活動を時間的要素に展開して、ワークロードなどのパフォーマンス評価に用いるものである。

反応時間の構成

$$TS=TE+TP+TC+TM+TH$$

TS:反応時間

TE:①眼球運動

TP:②感覚プロセス

TC:③認知プロセス

TM:④運動プロセス

TH:⑤応答

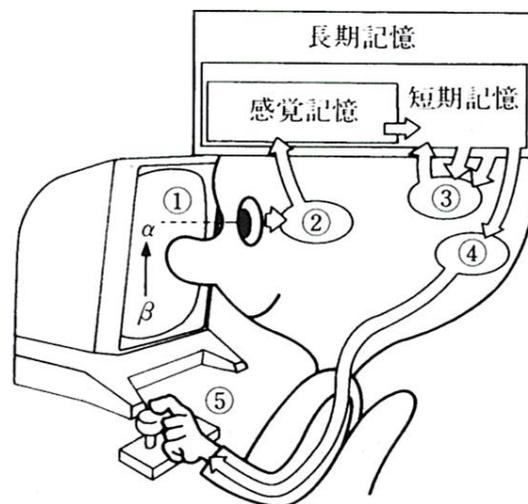


図 2.5 GOMS モデル ([8]より作成)

Reason は、深層防護のモデルとして、スイスチーズ(Swiss Cheese)モデルを提唱した[7]。あるシステムの危険源に対して、多重の防止策を講じているが、スイスチーズのように各防止策は完全ではなく危険源を防止できない穴があり、何らかのきっかけやタイミングにより、これらの多重の防止策の穴をすり抜けてエラーを引き起こすメカニズムを説明したものである。(図 2.6)

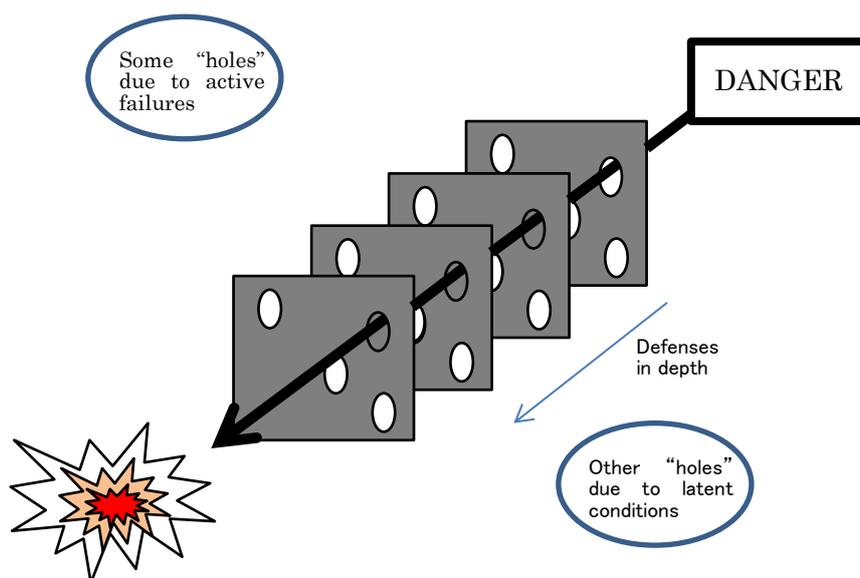


図 2.6 スイスチーズ・モデル ([7]より作成)

また、航空機システムにおける人間と機械のヒューマンファクター側面の関係性を説明するモデルとして、Hawkins 他[10]により、SHEL モデルが提唱された。本人(人間、Liveware)を中心として、本人に影響を与える要素をブロックとして表現し周囲に配置して、これらのそれぞれの要素とのインターフェースのゆがみ(波線で示したもの)により、エラーが発生するメカニズムを示したものである。(図 2.7)

図 2.7 に示す通り、本人(Liveware, L)を中心に配置し、本人に影響を与える要素である、ハードウェア(Hardware, H)、ソフトウェア(Software, S)、作業環境(Environment, E)および他者(Liveware, L)をその周囲に配置する。ヒューマンエラーは、本人(L)と作業を行う道具やマンマシンインターフェースであるハードウェア(H)、作業手順書などのソフトウェア(S)、照明や温度、騒音などの作業環境(E)、作業指示や協働して作業する作業者の影響により発生する(これを破線のゆがみで表す)としている。

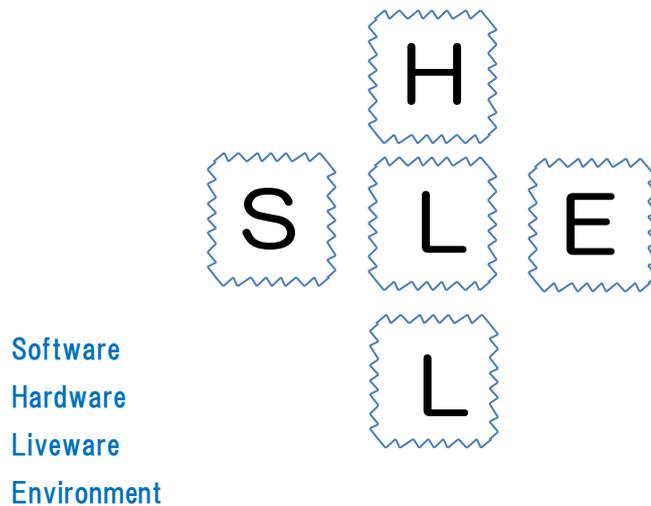


図 2.7 SHEL モデル ([10]より作成)

2.3.3 ヒューマンエラー分析、エラーマネージメントに関する関連研究

ヒューマンエラーマネージメント／ヒューマンエラー分析は、ヒューマンエラーの発生メカニズムを分析し、その発生を未然に防止すること、また、ヒューマンエラーが発生した場合はその影響を最小化することを目的としている。

(1) ヒューマンエラーマネージメント

ヒューマンエラーマネージメントは、他のエラーマネージメントと連携し、システム設計、運用のライフサイクルを通じて適用される。設計のフェーズでは、起こり得るヒューマンエラーを特定し、当該エラーを未然に防止し、また、エラー発生後の影響緩和を行うための設計方策を検討し、適用を図る。運用フェーズでは、設計方策に基づき、ヒューマンエラーを発生防止と発生した場合の影響緩和を実施していく。このことから、如何に完全かつ効果的に起こりえるヒューマンエラーを設計段階で特定し、これを未然に防止、もしくは、発生した場合の影響緩和対策について設計方策について検討し、設計施策として設計に展開していくことが重要である。

(2) ヒューマンエラー分析プロセス

ヒューマンエラー分析は、ヒューマンエラーを包括的かつ効果的に特定するための分析手法である。Kirwan ら[11][12]は、図 2.8 に示すような、全体的な分析方法のプロセスを

提唱している。以下の通り、分析プロセスについて述べる。

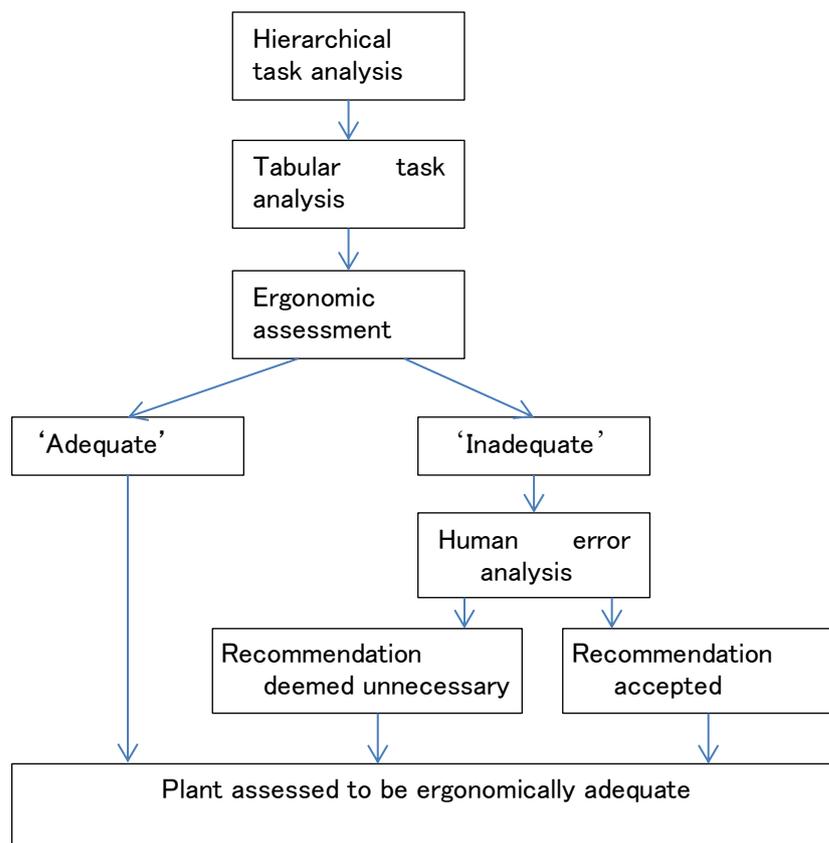


図 2.8 Overall 分析手法 ([11]より作成)

潜在的ヒューマンエラーを分析するためには、タスクの複雑さの特定、タスクの特徴の特定、運転員／オペレータのワークロード等を特定することが有効であり、これを分析するためにタスク分析手法が用いられる。

図 2.8 に挙げる、階層化タスク分析 (Hierarchical task analysis, HTA) は、あるタスクに含まれるサブタスク、アクティビティを詳細化するものである。表形式タスク分析 (Tabular Task Analysis, TTA) は、文字通り表形式を用いて HTA で展開した詳細化タスク／サブタスク或いはアクティビティ毎に、タスクの特徴 (例えばある操作を行うタスクに対してどのような操作器でどのように操作するかなど)、タスクを遂行するために必要な補助器具／手段／情報等 (例えば工具の使用や計算機の使用等) を分析していく。タスク分析は上記 2 つの他様々な分析手法が開発されている。

エルゴノミクス分析(Ergonomic assessment)は、エルゴノミクス設計標準 (例えば、色の識別性、一貫性、使用制限、文字の大きさ、可読性、一貫性、指示計／操作機器の配置条件など人間がヒューマンエラーを起こさない経験則や人間の特性データに基づく設計条件等) と比較することによる、人間に割り当てられたタスクやその特徴づけ (TTA 参照)

の制約や困難さを評価していく。

エルゴノミクス分析の結果タスク遂行が不十分な場合、ヒューマンエラー分析(Human error analysis)を行い、ヒューマンエラー要因を特定し設計改善を行う。ヒューマンエラー分析は、一般的には設計改善方策の検討を含む。すなわち、ヒューマンエラー分析により、どのタスクにおいてどのようなタスク遂行上の制約や困難さがあるかが明らかになることから、これを改善するための方策への展開が可能となる。

Kirwanら[11][12]は、ヒューマンエラー分析の一例として、表 2.1 に示すような例を提唱している。ヒューマンエラー分析は、人間工学評価の観点で設計が不十分な項目(Design inadequacy)を抽出し、当該設計仕様で起こりえるヒューマンエラー(Errors)やその原因(Possible consequence)、リカバリポイント(Recovery points)を特定する。これらの評価の結果、設計の改善策 (Remedial actions) を設計(Design)、教育訓練 (Training)、手順書 (Procedure) の視点で幅広く考察する。

ヒューマンエラーは合理的な発生可能性を主観的に俯瞰して見積もることで、かつ、設計面の改善点を図る観点から、定量的な値 (発生確率) の評価は必要ないとしている。

表 2.1 Human Error Analysis ([11]より作成)

Error No.	Design inadequacy	Errors	Possible consequences	Recovery points	Remedial actions		
					Design	Training	Procedure
1	The required updating of the pond contents on return to computer control	Incorrect input of the location of equipment, racks, etc.	Potential risk of equipment collisions	Notice error via observation of monitors	Improved feedback		Recording & checking of information
2	---	---	---	---	---	---	---
3	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---

なお、タスク分析を行うため、類似タスクの理解を深めること、また、ヒューマンエラー分析を行うため過去に発生した類似事象について理解を深めることはヒューマンエラー分析を網羅的、かつ、効果的に行うために極めて重要である。これは、人間工学プロセスの冒頭分析プロセスとして挙げている、運転経験レビューを通じて達成される。すなわち、運転経験レビューとは、参照プラントや類似プラントで発生したヒューマンエラーやこれに関連する事象について、良好な側面は積極的に設計に踏襲するとともに、ヒューマンエラーが行った要因やその影響因子については再度同じようなことが起きないように未然対策として設計に取り入れることを目的としたものであり、運転経験レビューを通じ類似タスクの理解が深まり、タスク分析の展開やヒューマンエラー分析が効果的に実施できる。

(3) ヒューマンエラー分析手法

ヒューマンエラー分析は、様々なものが提案され、原子力発電所制御室の設計をはじめ、他の産業でも適用されている[11]。

ヒューマンエラー分析において重要な点は、如何に失敗事象を網羅的かつ現実的に起こりえるものとして特定することである。

以下の分析手法が一般産業界で広く使用されている。なお、HRAについては、原子力産業では一般的に使用されているが、他産業への展開は限られている。

i) Failure modes and effects analysis (FMEA)

ii) Faults trees analysis (FTA)

iii) Hazard and operability analysis (HAZOP)

iv) System Theoretic Accident Model and Process/System-Theoretic Process Analysis (STAMP/STPA)

v) Human Reliability Analysis (HRA)

主要な手法としてここでは上記 i) から iv) について述べる。v) の HRA については、2.4 章で詳述する。

i) Failure modes and effects analysis (FMEA)

FMEA[13][14]は、システムにおけるハードウェアの故障の影響を評価するために開発されたが、タスクの失敗に対するシステムの影響評価として、ヒューマンエラー分析にも適用可能である。

表 2.2 に運転員のエラーに対する FMEA の例を示す[13][14]。分析手法はボトムアップアプローチとして実施され、タスクレベルでの起こりえるエラータイプを設定し、それに対するリカバリアクションやその認知的要因、当該失敗により起こりえる影響について評価し、その対策（推奨案）を検討する。

利点としてはタスクレベルでの起こりえるヒューマンエラーを個別に特定することで実際の作業環境やストレスレベルを想定したコンテキストレベルの評価が可能である一方、エラータイプの想定や抽出には分析者の能力に依存し、また、原子力発電所運転のような非常に幅広い運転モードや機器操作を分析するためにはどのタスクが重要であるかの絞り込みが必要になることから、原子力発電所の安全設計では、決定論的な安全評価とリスク分析により重要なタスクを絞り込んだのちに、FMEA に類似したタスク分析を行うこととしている。

表 2.2 運転員のエラーに対する FMEA の例 ([13][14]より作成)

Task Step	Error Type	Recovery Step	Psychological mechanism	Cause, consequences and comments	Recommendations		
					Procedure	Training	Equipment
51.1 Close supply valve	Action too late	No recovery	Place-losing error	Overfill of tanker, resulting in dangerous circumstances	Operator estimates time/records amount loaded	Explain consequences of overfilling	Fit alarm-timing/vol./tanker level
51.2.1	---	---	---	---	---	---	---
51.2.2	---	---	---	---	---	---	---
51.2.3	---	---	---	---	---	---	---

ii) Faults trees (FTA)

FTA[13]は失敗と成功を樹形図で示すことで、最終的な失敗（例えば原子力発電所で言えば炉心損傷や放射能放出）に至る機器やヒューマンエラーを特定するとともに、そこに信頼性確率（故障率や失敗確率）を当てはめることにより、システム全体の信頼性（最終的な失敗に至るシステム全体の確率）と改善点（信頼性が低い機器の高信頼性対策（多重化等））を図ることができる。

原子力発電所では、まず、FTAによりリスクの高いイベント（タスクや機器故障）を絞り、このイベントに対してさらに詳細分析を実施することにより、設計を評価し、改善点を見つけることとしている。

iii) Hazard and operability analysis (HAZOP)

HAZOP[13]は、システムの設計意図と運転意図（達成可能性）のギャップを設計の初期段階で取り除くため、システムの設計者や運転経験者などの関係者がワークショップにより、定められた手順（Property word/guide word）により起こりうるエラーを特定する手法であり、1970年代にICI(UK)にて開発された[15]。また、Whalley[16]らは、HAZOPをヒューマンエラー分析に適用した。HAZOPは、原子力プラントでは、2.4章で述べる人間信頼性分析（ATHENA[20]）で類似手法(Unsafe Action)としてヒューマンエラー分析として適用されている一方、適用範囲は人間信頼性分析の一手法にとどまり、大々的な適用はされていない。これは、2.4章で詳述するが、HAZOPによるヒューマンエラーモードの抽出を用いたATHENAを含め、評価者の知識や経験に基づくところが多く、分析結果にばらつきが出てくることが指摘されている[21]。

iv) System Theoretic Accident Model and Process/System-Theoretic Process Analysis (STAMP/STPA)

STAMP/STPAはHAZOPの一つとされるが、大規模/複雑なシステムにおけるエラー分析

が可能なよう、各サブシステム、コンポーネント間の相互作用（制御-被制御対象プロセス）に焦点をあてたものである[17]。ソフトウェアを組み込んだシステムの複雑化、高機能化に伴い、従来の手法ではハザードの特定が難しいとして、プロセスを通じてシステム間で発生する **Emergent properties (e.g., enforcing safety constraints)** を特定して、システム全体で発生する非安全アクションをハザード捉えてその要因や改善策を決定することを示した。具体的には、図 2.9 に示す通り、制御する側と制御対象（プロセス）間の相関図を作成し、この間に制御信号(**Control Actions**)や制御対象からのフィードバックの有無やタイミングを示した以下の4つの非安全制御アクション (**Unsafe Control Actions**)、を想定した場合に発生するシステム間の影響度合いを評価する。

- ①安全制御信号が与えられない(**Control commands required for safety are not given**)、
- ②非安全信号が発信される(**Unsafe ones are given**)
- ③安全制御信号発信が時間的／シーケンス的に早すぎる、または、遅すぎる(**Potentially safety commands given too early, too late (i.e. timing/sequence)**)
- ④安全制御の発信間隔が短すぎる、または、長すぎる(**Control stops too soon or applied too long (i.e., duration)**)

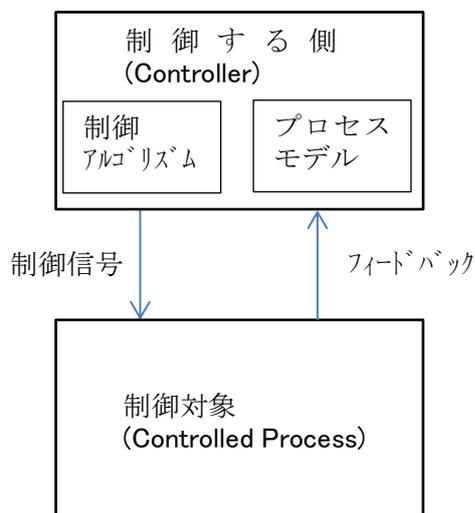


図 2.9 制御ループのプロセスモデル ([17]より作成)

2.4 人間信頼性分析について

2.3 節で述べた通り、原子力発電所では、確率論的リスク分析(Probabilistic Risk Analysis, PRA)の一部として、人間信頼性分析 (Human Reliability Analysis, HRA) を行い、ヒューマンエラーを人的過誤率として算出し、炉心損傷確率計算に組み込んでいく。

HRA は、定性分析においてヒューマンエラーイベント (Human Failure Event, HFEv) とこれに内在するヒューマンエラーと当該ヒューマンエラーの要因となる影響因子 (Performance Influence Factor, PIF) を特定し、定量分析において人的過誤率をこれらのヒューマンエラーのタイプや PIF による重みづけと積み重ねにて人的過誤率を計算する。

定性分析においては、タスク分析手法によりコンテキストの中でどのようにタスクを遂行し、その中でどのようなエラーを起こす可能性があるかを検討していくため、これらの分析結果は単に HEP を計算するためだけではなく、ヒューマンエラーを防止するための改善策にも適用することができる。

HRA は上述の通り、定性分析 (HFE と PIF を特定)、定量分析 (HEP として数量化) の組み合わせであるが、特に定性分析において、ヒューマンエラーをどのように特定するかについて多くの議論があり、また、多くの手法が開発された。

以下に代表的な HRA 手法を示す。

- THERP (Technique for Human Error Rate Prediction)[3]
- HEART (Human Error Assessment and Reduction Technique)[18]
- CREAM (Cognitive Reliability and Error Analysis Method)[19]
- ATHEANA (A Technique for Human Event Analysis)[20]
- IDHEAS (Integrated Decision-Tree Human Event Analysis System)[21] [22] [23]
- Phoenix (A Model-Based Human Reliability Analysis Methodology)[24]

THERP と HEART は第一世代 HRA に分類され、行動ベースのヒューマンエラー (例えば、指示計を読み取る HE 等) をベースとしているが、認知的タスクについては評価の限界がある。第二世代 HRA として、CREAM や ATHENA があるが、これは認知的タスクを含めた包括的なヒューマンエラーを評価する方法として開発されたが、評価者の能力に判断され、また、定性分析結果を定量分析 (HEP 値の算出) に展開するための明確なガイダンスが不足している。

第三世代 HRA (IDHEAS, Phoenix)では、認知タスクを巨視的認知モデル (マクロコグニティブモデルともいう、Macro-cognitive Model) として標準化して、評価者による

評価の偏りを少なくするとともに、定量分析への展開を容易にした。

図 2.10 に IDHEAS の HFE 事象を 5 つのタイプの認知タスクにブレークダウンした階層図を示す。最上位階層にあるシナリオ (Scenario) は、PRA で炉心損傷に至るシナリオを示す。第二階層で示す人的過誤事象 (Human Failure Events, HFEvs) は、シナリオに内在する人的アクションのうち、潜在的に人的過誤があると考えられる事象を示す。第三階層で示すクリティカルタスク (Critical tasks) は、HFEvs の中に包含する、様々なタスクのうち、人的過誤に関連する重要なタスクを示す。なお、タスクとは、人的アクションに対してさらにブレークダウンしたタスク、サブタスク、アクティビティを示す。最下層で示す認知タスクを構成する巨視的認知モデルは、それぞれのクリティカルに対して割り当て、巨視的認知モデルの構成要素 (検知 (Detection)、理解 (Understanding)、意思決定 (Decision-making)、実行 (Action execution)、チーム調整 (Inter-team coordination)) 毎に影響因子 (Performance Influence Factor, PIF) を分析する。

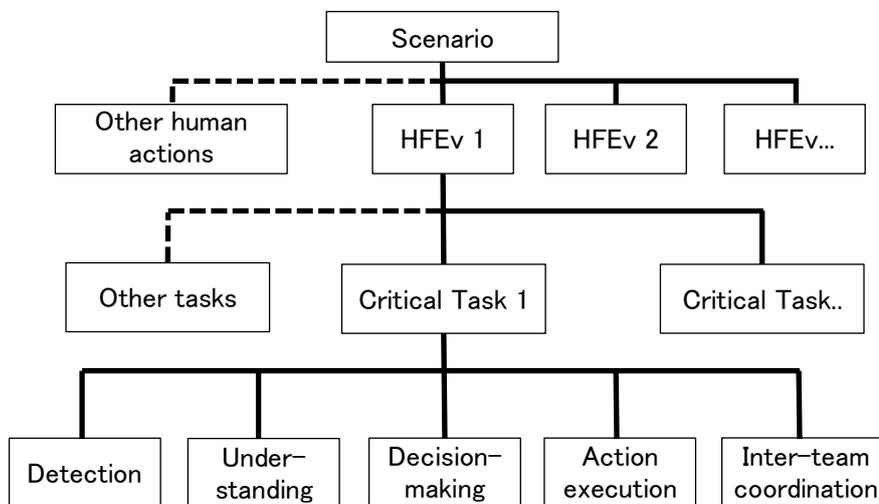


図 2.10 IDHEAS の 5 つのタイプの認知タスク ([22]から作成)

1. 認知的タスク分析に基づく行動影響因子の特定

認知的タスク分析においては、運転員のタスク/パフォーマンスに影響を与える因子 (PIF) を認知的タスクプロセスに対して分類し整理している。Phoenix および IDHEAS で使用している PIF を図 2.11 および表 2.3 にそれぞれ示す。

図 2.11 に示す通り、Phoenix では、巨視的認知モデルとして、3 つの認知タスク、すなわち、情報処理 (Information processing)、診断/意思決定 (Diagnosis/Decision making)、行動 (Action taking) を定義し、横軸に配置する。さらに、それぞれの認知タスクに対して起こりえるエラータイプを小分類としてリスト化する (例えば、情報処理

では、I1~I9の9分類を設ける)。また、縦軸に運転員の行動分類(監視(Monitor)、精査(Scan)等)を列挙する。表の中身は横軸の認知タスクレベルのエラー分類と縦軸で示す、それに対応する運転員の行動が当てはまるものに対して色識別する。(例えば、情報処理で起こりえるエラー分類は、茶色で識別する監視や精査については全てのエラータイプ(I1~I9)で起こりえるが、診断(Diagnosis)や計画(Plan)という運転員行動には当てはまらない)次に、表中で色識別した項目毎に行動影響因子(PIF)を設定して、分析の中でシナリオ中起こりえる運転員の行動とその行動影響因子を特定する。

一方、IDHEASにおいては、表2.3で示すように、図2.10で挙げた5つの巨視的認知モデル(Macro-cognitive function)/認知タスク分類(検知(Detection),理解(Understanding),意思決定(Decision-making),行動(Action execution),チーム調整(Inter-team coordination))を横軸に配置する。また、縦軸には、運転員の行動に基づくエラータイプを行動影響因子(PIF)として、シナリオの未習熟(Scenario Familiarity)や情報取得可能性と信頼性(Information Availability and Reliability)といった、15個の基礎的行動影響因子(Base PIF)と、各基礎的行動影響因子に対してエラータイプにより影響度合いの重みづけを行った付加的影響因子分類(全200種類)を配置する。基礎的行動影響因子は、表中の縦軸に太字で大項目として分類し、付加的影響因子は、それぞれの大項目で示す分類の中でエラータイプ/影響度合い毎に分類する。(例えば、シナリオの未習熟では、SF0が基礎的影響因子、SF1~SF-4が付加的影響因子に該当する。)表中の黄色部分(N/Aでない領域)は、各行動影響因子毎(縦軸)、巨視的認知モデル毎(横軸)に過去の実験データを基にエラー率を割り当てる。なお、N/Aの領域は、適用対象外であることを示す。(例えば、シナリオの未習熟では、検知においては、情報取得可能性と信頼性は基礎的行動影響因子のみが該当し、その他のエラータイプは起こりえないとする。)

ヒューマンエラー率(Human Error Probability, HEP)は、タスク毎に行動影響因子の特定とその行動影響因子に割り当てられたヒューマンエラー率を積算して算出する。

ヒューマンエラー率の計算は、定量分析として実施されるが、一旦行動影響因子を特定すれば、積算計算についてはどの手法も差異は無く、信頼性品質は確保されていることから、本論文では取り上げない。

なお、IDHEASでは、シナリオの認知(Scenario Familiarity)、情報の可用性と信頼性(Information Availability and Reliability)、およびタスクの複雑さ(Task Complexity)については、他の12個の基礎的影響因子(Base PIF)に比べて支配的(起こりえる確率が高い)であることから、基礎的影響因子(Base PIF)のヒューマンエラー率を、その他のPIFについては上記3つの基礎的影響因子(Base PIF)のヒューマンエラー率に重みづけを行いHEP値を調整することとしている。

すなわち、式に表すと以下のようなになる。

$$P_{cfm} = P_{cfm_base} \cdot (1 + \sum_{i=1}^n (w_i - 1)) \cdot \frac{1}{Re}$$

$$P_{cfm_base} = 1 - [(1 - P_{inf})(1 - P_{sf})(1 - P_{tc})]$$

Pinf : 情報の可用性と信頼性の基礎的影響因子に割り当てられるヒューマンエラー率

Psf : シナリオの認知の基礎的影響因子に割り当てられるヒューマンエラー率

Ptc : タスクの複雑さの基礎的影響因子に割り当てられるヒューマンエラー率

Pcfm_base: 上記3要素の基礎的影響因子に割り当てられるヒューマンエラー率

wi: 重みづけ因子。すなわち、基礎的影響因子に対する付加的影響因子の影響度合として、以下のように、定義される。

$$w_i = \frac{ER_{pif}}{ER_{pif_base}}$$

ここで、**ERpif** は、表 2.3 の付加的行動影響因子に割り当てられたエラー率（例えば、表 2.3 における、環境行動影響因子（**Environmental PIF**）で **ENV1** に示す値）、**ERpif_base** は、基礎的行動影響因子に割り当てられたエラー率（例えば、表 2.3 における、環境行動影響因子（**Environmental PIF**）で **ENV0** に示す値）。

例えば、付録 A に示すように、**ENV2-1**（5℃以下の環境）では、通常の場合と比べエラー率は 1.1 倍に重みづけする。

これらの付加的行動影響因子の重みづけを積算し、基礎的影響因子のエラー率に掛け合わせる。

Re は、ヒューマンエラー直後のリカバリ因子を示しているが、リカバリファクターがない場合（デフォルト）は 1 としている。（例えば、ダブルチェックを行う場合、**Re**>1 としてエラー率低減を評価する。）

Table 4-2: Relationship between types of Crew Activities, CFMs and IDA phases [5]

Types of crew activities	Human Response Model (IDA)																	
	Information Processing (I)									Diagnosis/Decision making (D)							Action Taking (A)	
	Noticing/ Detecting / Understanding									Situation assessment / Diagnosis			Decision making / Response planning				Action taking	
	I1	I2	I3	I4	I5	I6	I7	I8	I9	D1	D2	D3	D4	D5	D6	D7	A1	A2
Monitor																		
Scan																		
Detect / Observe																		
Identify																		
Communicate																		
Evaluate / Interpret																		
Record																		
Compare																		
Verify																		
Adapt																		
Adhere																		
Diagnosis																		
Decide																		
Plan																		
Coordinate																		
Execute																		
Regulate																		
Maintain																		
I1: Key Alarm not Responded to (intentional & unintentional)									D1: Plant/System State Misdiagnosed									
I2: Data Not Obtained (Intentional)									D2: Procedure Misinterpreted									
I3: Data Discounted									D3: Failure to Adapt Procedure to the situation									
I4: Decision to Stop Gathering Data									D4: Procedure Step Omitted (Intentional)									
I5: Data Incorrectly Processed									D5: Deviation from Procedure									
I6: Reading Error									D6: Decision to Delay Action									
I7: Information Miscommunicated									D7: Inappropriate Strategy Chosen									
I8: Wrong Data Source Attended to									A1: Incorrect Timing of Action									
I9: Data Not Checked with Appropriate Frequency									A2: Incorrect Operation of Component/Object									
									A3: Action on Wrong Component / object									

図 2.11 Pheonix に基づく PIF 分類

表 2.3 IDHEAS に基づく PIF 分類

PIF Attribute	Macro-cognitive function				
	Detection	Under- standing	Decision making	Action Exe- cution	Team Coordi- nation
Base PIF					
Scenario Familiarity					
SF0: No-impact					
SF1: Unpredictable dynamics in known scenarios					N/A
SF2: Unfamiliar elements in the scenario					N/A
SF3-1: Scenarios trained on but infrequently performed					N/A
SF3-2: Scenario is unfamiliar, rarely performed					N/A
SF3-3: Extremely rarely performed					N/A
SF4: Bias or preference for wrong strategies exists, mismatched mental models					N/A
Information Availability and Reliability					
Inf0: No impact - Key information is reliable and complete					
Inf1-1: Information is temporarily incomplete or not readily available	N/A			N/A	N/A
Inadequate updates of information					
Inf1-2: Information is moderately incomplete - a small portion of key information is missing	N/A			N/A	N/A
Inf1-3: Information is largely incomplete	N/A			N/A	N/A
Inf2-1: Low unreliable or uncertain	N/A			N/A	N/A
Inf2-2: Moderately unreliable or uncertain	N/A			N/A	N/A
Inf2-3: Highly unreliable	N/A			N/A	N/A
Inf3: Extremely unreliable	N/A			N/A	N/A
Task complexity					
C0: No impact					
C1: Detection overload with multiple competing signals		N/A	N/A	N/A	N/A
C2: Detection is moderately complex		N/A	N/A	N/A	N/A
C3: Detection demands for high attention		N/A	N/A	N/A	N/A
C4: Detection criteria are highly complex		N/A	N/A	N/A	N/A
C5: Cues for detection are not obvious		N/A	N/A	N/A	N/A

PIF Attribute	Macro-cognitive function				
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation
C6: No cue or mental model for detection		N/A	N/A	N/A	N/A
C10: No impact – straightforward diagnosis with clear procedures or rules	N/A		N/A	N/A	N/A
C11: Working memory overload (その他44件)	N/A		N/A	N/A	N/A
Weight factors					
Environmental PIFs					
ENV0: No impact – nominal weather and environmental factors	1	1	1	1	1
ENV1: Coldness on action execution Moderate cold (<5° C) – 1.5 Extreme coldness on manipulating instrumentation – 2 Extreme coldness on physically demanding execution – 5 Extreme coldness on high precision manipulations (e.g., connecting lines to pump, remove air from lines and pumps) – 20 他13件	N/A	N/A	N/A		N/A
System and I&C Transparency (5件)					
Human-System Interface (16件)					
Equipment and Tools (7件)					
Staffing (7件)					
Procedures, Guidance, and Instructions (8件)					
Training (14件)					
Teamwork and Organizational Factors (6件)					
Work Processes (8件)					
Multitasking, Interruption, and Distraction (11件)					
Mental Fatigue and Time Pressure and Stress (11件)					
Physical Demands (6件)					

2.5 既存の制御室開発プロセスにおける課題

一般的に、制御室設計プロセスでは他の設計プロセスと同様、決定論的な条件設定により、設計目標を定め、プラントの安全設計要件や機能要件を満足する制御室概念設計を行い、プラント機能分析、タスク分析などを実施し、具体的な要求を展開するとともに、経験的知見に基づくエルゴノミクス設計基準に適合するようにマンマシンインターフェース設計を進めて行く。原子力発電所安全設計においては、リスク分析により炉心損傷や放射能放出に対して影響度の高い機器やタスクを抽出して設計に展開していく。

上述の基本的な設計プロセスにおける変更はないが、現状のプロセスにおいて以下の課題がある。

1) リスク分析とのインターフェース

既存の制御室設計プロセスにおいては、リスク分析から、リスクへの影響度が大きいタスクの特定として、機器の故障による影響度の評価と同様、期待されるヒューマンアクション(HA)に対する重要度指標、すなわち、評価対象の HA が必ず達成する（失敗確率(HEP)を 0）とした場合、炉心損傷頻度がどの程度低下するか（Fussell Vesely, FV）、逆に、評価対象の HA が必ず失敗する（HEP を 1）とした場合に、炉心損傷頻度がどの程度増加するか(Risk Achievement Worth, RAW)として、これらの値がある閾値以上の場合、リスクの寄与（影響度）が高いものとして選定し、抽出された HA について、詳細なタスク分析等を進め、ヒューマンエラー防止の観点から制御室の設計考慮を重点的に行う。

上述のプロセスにおいては、一律にリスクの寄与が高い HA を特定ができ、これらの HA に対して未然防止を進めて行く面でメリットがある一方、どのような要因（分析上の想定）でエラーを引き起こす可能性があるかについて、明確でない場合が多く、また、制御室設計プロセスで行うタスク分析の想定との違いや重複（リスク分析で実施するヒューマンエラーイベントの特定には定性分析としてタスク分析がされる）が生じる。

2) 最新のエラーマネジメント手法との統合

ヒューマンエラーマネジメントとして潜在的なエラーを FTA, FMEA, HAZOP, STAMP/STPA など抽出し、これを設計に展開し、未然に防止することとしているが、当該エラーマネジメントプロセスが体系的なプロセスとして展開されていない。

3) 運転中の中央制御室システムのパフォーマンス管理と設計改善への施策

現状の制御室設計プロセスでは、運開後はパフォーマンスを評価していくのみとしており、どのようにパフォーマンスを評価していくか、また、パフォーマンス評価の結果を体系的に設計に反映していく仕組みがない。

2.6 結果と検討

本章では、原子力発電所分野における人間工学を適用した制御室開発プロセスとヒューマンエラー関連研究について纏めた。

人間工学を適用した制御室開発プロセスについて、ヒューマンエラー未然防止のための方策として、HRAの分析結果にから、リスク重要度指標を閾値として、リスク上重要な人的操作(RIHA)を特定し、当該RIHAに対して人間工学を考慮した設計考慮を行う現状の設計フレームワークを述べるとともに、HRAの想定条件を適切に体系的に設計プロセスに取り組むフレームワークが無いとの課題について明らかにした。

原子力発電分野におけるヒューマンエラー関連研究においては、2つのアプローチ、すなわち、確率論的リスク分析アプローチによるヒューマンエラー分析、および、人間工学的設計基準適用を含む人的組織的な側面(運転体制、資質、運転手順書、訓練プログラム)も含めた体系的な制御室設計開発プロセス、により制御室の設計開発の改善がされてきたことを纏めた。

また、原子力発電分野におけるヒューマンエラー関連研究の基礎となる、ヒューマンエラーメカニズムに関する関連研究について、RasmussenのSRKモデル、Reasonのヒューマンエラー分類、CardらのGOMSモデル、Reasonのスイスチーズモデル、HawkinsのSHELモデル、ヒューマンエラー分析/エラーマネージメントに関する関連研究として、Kirwanらによるヒューマンエラー分析をはじめ、各種のヒューマンエラー分析手法について纏めた。

ヒューマンエラーの未然防止を考える際に、人間のエラーメカニズムについてまず理解することが重要である。これを理解するために、人間の認知プロセスのモデル化を行い、どの認知プロセスにエラーの原因があるかを特定する仕組みが有効であり、RasmussenのSRKモデルや、Card氏らのGOMSモデルをはじめ、様々な認知モデルを検討して、認知プロセスのマクロ化(標準化/巨視化)をしたマクロコグニティブモデル(Macro-cognitive model)をHRAのプロセスに適用している。

また、ヒューマンエラーは、認知プロセスへのインプットとなる状況認知(Situation awareness, SA)と、物理的または精神的ワークロードとして表される、人間の処理能力即ちパフォーマンスに依存する。

すなわち、RasmussenのSRKモデルでいえば、状況認知は、SRKいずれに対してもインプット情報の品質を決定するものであり、S,R,Kどれを選択するかは当該状況認知次第で変化してしまう。また、間違った状況認知は、コミッションエラーを発生させ、状況認知の更新がない限りリカバリが難しい。また、パフォーマンスの限界を超える際に、Reasonのヒューマンエラーモデルでいう、LAPSEやSLIPという不注意行動、あるいは

は、作業制約の中で結果的に間違っただ判断、すなわち、MISTAKE を起こすリスクが高くなる。後者のパフォーマンスを改善するためには、SHEL モデルで表されるように、作業
者本人のパフォーマンスに影響を与える様々な影響因子（PIF）／背後要因をマンマシン
インタフェースといったハードウェアだけでなく、手順書に代表するソフトウェア、或い
は作業環境など多面的に考慮することが重要である。パフォーマンスは、S,R,K それぞれ
のプロセスの選択に影響を及ぼすだけでなく、各認知プロセスにおける判断や意思決定に
も影響を与える。例えば、与えられたタスクの要求が経験したこともなく、対応するガイ
ドや手順書もない場合（PIF でいう、シナリオの未習熟）は、知識ベースのプロセスへ選
択を余儀なくされ、また、その認知プロセスの中で行われる作業計画（Planning）も時間
プレッシャという影響因子があれば、考慮不足の作業計画がされかねない。

ヒューマンエラーが実際に起こった場合は、その影響因子について焦点を当てて原因を
分析（背後要因を特定）し、再発防止を考えるが、ヒューマンエラーを未然に防止するた
めには、上述した適切な状況認知の維持と、認知プロセスに与える影響因子の正確な特定
および、これを排除／低減する設計改善が効果的である。したがって、ヒューマンエラー
の認知プロセスレベルのパフォーマンス影響因子の特定し、これを体系的に HSI 設計へ展
開する枠組みは、ヒューマンエラー未然防止に大きな改善を図ることができるものといえ
る。

最後に、既存の制御室開発プロセスにおける課題として、3つの課題、すなわち、リス
ク分析とのインターフェース、最新のエラーマネージメント手法との統合、運転中の中央
制御室システムのパフォーマンス管理と設計改善への施策、を抽出した。

これらの課題については、3章以降の研究の中で、課題解決やその方策について検討を
進める。

第3章

最新の認知リスク分析手法の想定を設計開発プロセスに取り込む手法の開発とその実践適用

3.1 はじめに

2.5 節で整理した課題に対して、従来から実施している決定論的な条件設定に基づく制御室設計プロセスにおいて、リスク情報を活用したエラーマネジメントの考え方を適用した制御室設計統合化プロセスについて検討する。

なお、Boring ら[26]は、HRA を人間工学設計プロセスに展開する可能性や有効性について検討しているが、具体的な展開については論じていない。これは、従来の HRA の定性分析の体系的な確立がされていないため、具体的な展開はできなかったものと考えられる。

3.2 リスクマネージメントを考慮した制御室設計統合化

プロセスの検討

3.2.1 制御室設計プロセスにおけるヒューマンエラー分析適用検討

2.2 節で述べた人間工学を適用した制御室開発プロセス（人間工学プロセス）の中で、ヒューマンエラー分析に関わる部分について、2.3 節および 2.4 節で述べたヒューマンエラー分析の関係や改善点について述べる。

2.2 節で述べた人間工学プロセスの中で、ヒューマンエラー分析に関わる部分は、以下の実施項目である。

- (1) 運転経験レビュー
- (2) タスク分析
- (3) HRA

運転経験レビューは、過去に発生した類似のヒューマンエラーを防止し、また、ヒューマンパフォーマンスに好影響を与える設計要素を取り入れることを目的に、過去事例を分析する。運転経験レビューについては、その分析手法から単独での分析が適しており、その分析結果の設計開発への適用や管理に焦点を置くことでさらなる改善の余地は少ない。

人間工学で取り扱うタスク分析は、設計への展開を焦点にあて、タスクを遂行するための、タスク要求（すなわち、タスク遂行に必要な監視情報、制御／操作、人員など）を特定し、これらの結果を設計入力情報として使用する。タスク分析については、2.3 節、2.4 節で述べた通り、エラー分析の観点でも使用されており、統一化された手法による、体系的な活用が分析精度の向上や運用中に想定していなかったエラーが顕在化した際の逆解析への展開や要因の分析のためのタスク分析の活用が容易になる。

HRA は、2.5 節で課題として挙げた通り、十分に人間工学プロセスに統合されていない。すなわち、現状のプラクティスでは、リスク重要度指標により、RIHA を抽出し、そのタスクについて他の人間工学プロセスの中で考慮していくこととしているが、RIHA でのエラーメカニズムを体系的にどのように考慮していくかについて連携が十分でない。その一方で、ヒューマンエラー分析では、ヒューマンエラーのメカニズム、要因についても分析がされていることから、これらの分析で得られる様々な要因を体系的に人間工学プロセスに取り込んで設計展開を図れる可能性がある。

3.2.2 ヒューマンエラー分析の人間工学プロセス適用への有効性評価

ここでは、2.3 節で挙げた、代表的なヒューマンエラー分析手法とタスク分析を中心とした人間工学プロセスとの関係について述べる。

FTA は、PRA の中で既に展開されており、Fault-tree 形式で炉心損傷に至る起因事象（人的事象も含む）およびそれに影響を及ぼす機器故障、人的過誤事象(Human Failure Event, HFEVs) を特定し、これらの失敗確率により、炉心損傷確率（Core Damage Frequency, CDF) 値を求めている。また、人的過誤事象に内在する潜在的人的過誤率 (HEP) は HRA で分析する。

FMEA は、タスク分析の一手段として統合化、展開されている。すなわち、タスク分析は、サブタスクの分解とタスク特徴の特定を行い、運転員のタスクプロセスとしてタスクの複雑さ、並行タスクの有無などを評価している。なお、2.3 節でも述べた通り、タスク分析はヒューマンエラー分析でも用いられる根本的な手法であるが、人間工学プロセスにおいては、タスクの理解（複雑さ、ワークロード等）とタスク遂行に必要な監視制御情報、人数／力量の特定など設計開発に必要な設計入力情報の特定を主たる目的として使用しており、ヒューマンエラーの特定やその重要度評価までは目的としていない。

HAZOP と STAMP/STPA は設計フェーズでシステムのリスクや潜在的ハザードを特定する有効な方法であり、原子力発電所制御室設計におけるヒューマンエラーを特定するために用いる場合、評価すべき対象を絞るなど体系的なスクリーニングプロセスが必要である。

HRA は、人間工学プロセスと有機的に結合することでヒューマンエラーを起こすメカニズムや因子を考慮して、これを未然に防止する設計方策を考案する可能性がある。また、2.4 節でも述べた通り、従来の HRA は、HAZOP 手法も取り入れてヒューマンエラーリスクについて専門家（類似プラントの運転経験者や HSI 設計者等）の知見により抽出していたため、分析プロセスが評価者の力量によることか、分析プロセスが専門家の思考によることか多いため見える化や体系がされておらず、課題が多かったが、最新の HRA 手法である、第三世代 HRA (IDHEAS, Phoenix) [21] [22][23] [24]では、体系的に評価できるような手法に改善されているため、これをヒューマンエラーマネジメントとして活用することで、人間工学プロセスへ体系的に展開できる可能性がある。

上述の検討結果について、人間工学プロセスへの適用が有効なヒューマンエラー分析手法について表 3.1 に纏めた。

表 3.1 人間工学プロセスへの適用が有効なヒューマンエラー分析の評価結果

ヒューマンエラー分析手法	HFE プロセスにおける適用状況	HFE プロセスへの適用評価
FTA	○ ^a	—（適用済）
P-FMEA	○ ^b	—（適用済）
HAZOP	× ^c	○ ^e
STAMP/STPA	× ^c	○ ^e
HRA	△ ^d	○ ^f

注)

- a. HFEv を特定するために PRA の中で利用されている。
- b. タスク分析の中で実施。
- c. HAZOP や STAMP/STPA をエラーモード抽出に適用することで、包括的なエラーモードの抽出が可能。
- d. PIF/CFM を特定するために適用され、リスク重要度指標による RIHA として抽出しているが、HFE プロセスへの統合化までは至っていない。
- e. HAZOP としては体系的に取り込むためにはガイドワードの具体化が必要であり、HRA の中で一部適用している。HFE プロセスでは、HAZOP の一部の位置づけとして STAMP/STPA を適用。
- f. HRA の分析プロセスで得られる PIF/CFM の特定結果を体系的に活用可能。

上記の結果より、人間工学プロセスにおける HRA とのインターフェース改善について次章で検討を行う。また、STAMP/STPA の適用については、第 4 章でその展開について検討する。

3.2.3 HRA とのインターフェース改善

人的過誤事象やその失敗確率 (HEP) を分析し、算定するプロセスである、人間信頼性分析 (HRA) において、2.4 節で述べたように第三世代の HRA 手法が提案され、これを体系的にエラー防止メカニズムの特定とエルゴノミクスの観点からの改善に活用するとともに、既存の制御室設計プロセスとの有機的、体系的な統合化を検討する。

具体的には、第三世代 HRA の分析プロセス、また、関連する既存の制御室設計プロセスの一つとして、タスク分析プロセスについて、それぞれ検討を行い、その結果を基に統合化プロセスについて検討する。

(1) 第三世代 HRA の分析プロセス

IDHEAS, Phoenix 等の第三世代 HRA には、手法によって一部異なるが、概ね以下に示すようなステップでヒューマンエラー率(HEP)を算出する。(図 3.1)

- a. シナリオ／人的過誤事象 (HFEv) 分析
- b. クリティカルタスク分析
- c. タイムライン分析
- d. HEP 算出

シナリオ分析では、事故対処ガイドライン (Emergency Response Guideline, ERG) や過去の類似プラントにおける運転経験などから、シナリオを作成するとともに、パフォーマンスに影響を与えるコンテキスト (作業環境下におけるタスクの前後関係を示した記述) を作成し、必要に応じてタスクシーケンスやダイアグラム化してタスクの流れを分析することにより、人的過誤事象とこの中に内在するクリティカルタスクについて特定を行う。

クリティカルタスク分析では、そのタスクの認知タスクに着目して、どのようなヒューマンエラーモードが起こりえるかについて分析を行い、認知タスクプロセスにおける失敗モード（Crew Failure Mode, CFM）とその行動影響因子（PIF）について特定し、CFM および PIF による固有の失敗確率を累積計算することで、HEP(HEP_c)を求める。

タイムライン分析では、そのタスクが設計上時間制約を含む場合は、その設計想定時間（Tavail）とタスク遂行に必要な時間（Treqd）を見積り、その差（時間余裕）に基づく HEP(HEP_t)を算出する。

HEP の算定では、HEP_c と HEP_t を加算することで冒頭特定した人的過誤事象毎の HEP を計算する。

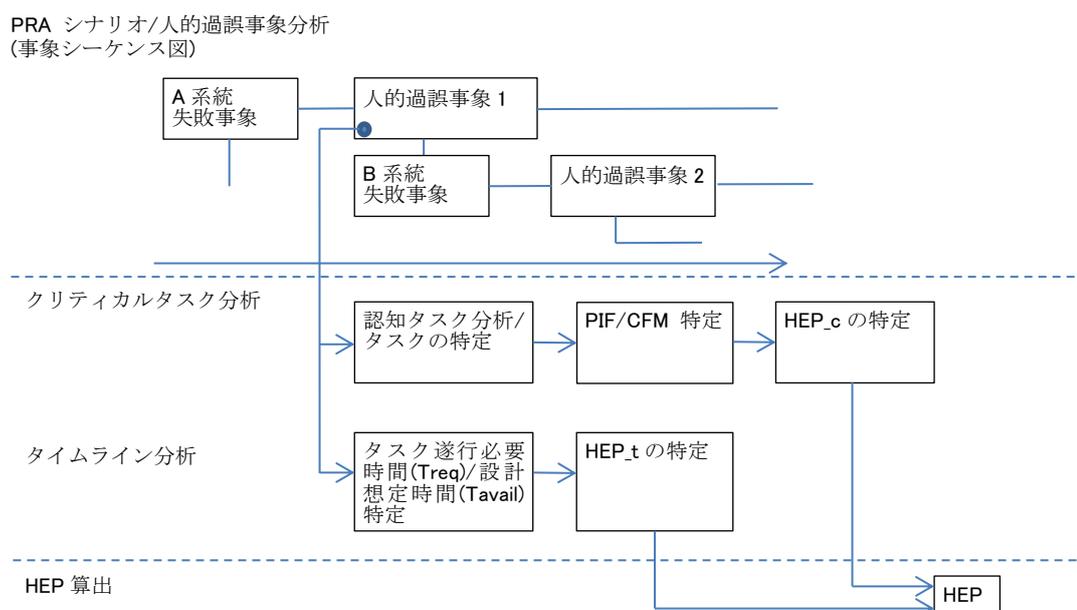


図 3.1 HRA におけるヒューマンエラー率の算定プロセス([23]より作成)

(2) タスク分析

制御室開発プロセスにおいて、タスクレベルでそのタスクに必要な運転人数、監視、操作情報を特定するために分析を行うプロセスとしてタスク分析がある。制御室設計プロセスで行うタスク分析は、リスク分析の観点のみならず、プラントの目標（安全停止や発電）達成するために必要な主たる機能を機能要求分析で特定し、さらに機能分配により人間のタスクとして割り当てられた手動操作機能、安全機能／安全解析で決定論的にクレジットをとるタスク、PRA の評価で従来実施している重要度指標（FV/RAW）で一定の閾値でリスクに寄与するタスク、または運転経験レビューにより過去の人的過誤事象と類似するタスク等に対して包括的にタスク分析を進めて行く点において異なる。また、タスク分析の目的が上述の通り、制御室設計に必要な運転人数、監視、操作情報等を特定または評価する点に

において異なる。

タスク分析は、一つの手法だけではなく、複数の手法を組み合わせで行う。典型的なプロセスについて図 3.2 に示す。

- a. タスク記述開発（どのようにタスクを遂行するかについてシナリオを記述, **Task descriptions**）
- b. 階層化タスク分析（**Hierarchical task analysis, HTA**）
- c. 目的別タスク分析（c1. シーケンス分析、c2. タイムライン分析、c3. 認知タスク分析、c4. ワークロード分析）
- d. タスク遂行に必要な監視パラメータ、警報、制御器、人員、知識の特定

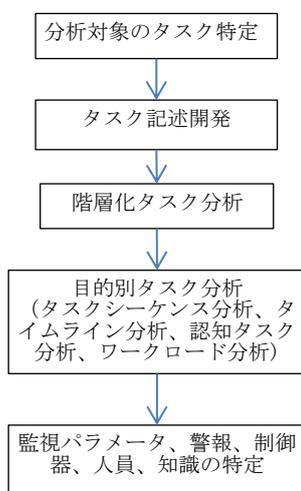


図 3.2 タスク分析プロセス

a. タスク記述開発では、インプットとなる選定したタスクに関連する情報（ERG や設計仕様）或いは過去の類似プラントにおける運転経験から、制御室における運転員の作業状況を踏まえて、タスクの流れについて記述していく。机上だけでなく、関係者との **Talk-through** やモックアップなどや類似プラントの設備を用いた **Walkthrough** もタスク記述を具体化するうえで有効である。

b. タスクの階層化分析（HTA）では、そのタスクに含まれるサブタスクやアクティビティを樹形図で示すことにより、タスクの構成について明らかにする。同時にそのタスクを行うための要件（サブタスクやアクティビティで要求される監視パラメータや操作器、その他のタスクサポートツール等）を明らかにする。

次の段階では、タスク記述や階層化分析の結果を基に、複数のタスク分析手法を目的に応じて選択して実施する。

c1. 運転シーケンス分析は、タスク間（HTA で明らかにしたサブタスク、アクティビティも含む）の繋がりや前後関係を明らかにするため、各タスク間の前後、或いは並行して行うタスクをシーケンス図で表現し、分析を行う。c2. タイムライン分析では、各タスクの実行する時間について分析、見積もり、運転シーケンス図で連関するタスクの繋がりを累積して、あるタスクの開始から完了時間を見積もる。なお、時間の見積りについては、実証データ（Walkthrough）や GOMS モデルなどを用いて見積もる。

c3. ワークロード分析では、HRA でも実施しているような、設計上のタスク遂行想定時間(Tavail)と上述の Timeline 分析で見積もったタスク遂行必要時間(Treqd)を比較して、このマージンが少ないほどワークロード（要は急いでタスクを完遂することが強いられる）が高いと評価する。

d. 認知タスク分析では、HRA で実施しているような認知タスクのタイプを明らかにする。手法は Walkthrough/Talk-through、プロトタイプシミュレータによるシナリオ実施後運転員のインタビューや観察を通じて評価する。ただし、設計で用いる認知タスク分析は GOMS のようなタスクの実行時間に置き換えてワークロード評価に用いたり、設計のポイント（状況認識が適格に行えるかなど）の確認が中心であり、HRA のようなエラー分析を主たる観点としていない（少なくとも体系化されていない）。

ワークロードの結果は、運転員の要件（数や訓練（資質）、自動化（FRA/FA へのフィードバック）、HSI によるタスクサポート（HSI 改善）などに活用する。

その他、各タスクの順番を上から下に表形式で並べ、上述のタスク分析のタスクの特徴づけを行い、HTA で特定したタスク要件を補完し、同様に設計要件（制御室の監視、操作情報の割り当て、手順書、訓練プログラム開発）に活用していく。

(3) HRA のヒューマンエラー分析結果からエルゴノミクス評価への展開

(1)(2)で検討した通り、HRA は HEP の算出のため、CFM と PIF を特定し、さらに、時間余裕を見積もる一方、制御室開発プロセスで実施するタスク分析は、タスク遂行のための設計要件（運転員の数／資質／訓練要件、HSI での機能（監視、操作情報、警報など）、運転要領書等）を特定する。また、HRA ではリスク分析からリスク上影響の高いヒューマンエラーイベントに注目してヒューマンエラーの可能性やタイプについて分析をしていく一方、タスク分析では、制御室機能を定めるべく、包括的に実施する。

このような目的／範囲に違いがあるが、HRA で分析しているヒューマンエラーの可能性のあるタスクやその影響因子についてはヒューマンエラー未然防止の観点から、エルゴノミクス評価を行い、設計に予め取り込むことが可能である。

ここでは、HRA でのヒューマンエラー分析からエルゴノミクス評価に展開し、設計に展開するプロセスについて検討する。

a. 認知エラータイプのレビューからの設計方策分類

(1)で述べた通り、HEP 算定については認知タスクに対する PIF を定義し、それぞれに失

敗率データを当てはめたテーブルから、各失敗率を抽出し、累積加算し、全体 HEP を求める。

PIF 特性に応じて、包括的に改善すべき事項を抽出し、対策として当てはめることが考えられる。

例えば、“Scenario Familiarity”に関しては訓練の強化、“Task complexity”に対しては、「HSI については自動化の検討／タスクサポートをするための HSI 機能強化」また、「運転手順書に対しては、タスクステップの整流化」等の一般的／包括的改善が考えられる。

当該改善点の抽出には、良好事例を集約し一般化したエルゴノミクス設計ガイドから適切な方策を抽出することができ、これを当てはめていく。

上述の手順により、各 PIF の特性表に応じて、改善すべき領域を制御盤 I/F、環境改善 (HSI)、運転要領書改善(Procedure)、運転員体制／技量改善 (Training) に分けて、それぞれの設計領域での対応改善施策についてマッピングし、設計の改善に役立てる。(表 3.3 参照)

なお、各 PIF で失敗率や重みづけが異なり、HFEvs/CFM 全体での HEP は、各失敗率／重みづけの掛け合わせとなることから、支配的な CFM の PIF を表 3.2 に示すように、PIF のエラー率に応じて設定した重要度閾値(Human Error 閾値, H/E 閾値)によって識別、特定する。

すなわち、表 3.2 の重要度閾値に従い、表 3.3 において、影響度の高い PIF に対して色識別し、HFEvs/CFM の中でも特にヒューマンパフォーマンスへの影響の高く設計の改善が必要なものに対して優先順位付けを行った。なお、表 3.3 は、IDHEAS に基づく PIF 分類表(表 2.3)にエラー率を IDHEAS の文献[23]から抽出したものである。また、当該表の右側に設計対策欄 (Design countermeasure) を設け、マンマシンインタフェース (HSI)、手順書 (Procedure) および教育訓練 (Training)の観点からヒューマンエラー防止策、改善策を特定する。なお、全てのエラーモードに対して対策立案を行うことは現実的ではないことから、表 3.2 に示す重要度に応じて対策の優先順位付けを行う。

表 3.2 PIF の影響度に基づく識別

重要度	配色	PIF H/E 閾値 (SF, Inf, C)	PIF H/E 閾値 (左記以外)
高	赤色	>1E-1	>10
中	橙色	>1E-2	>5
低	黄色	上記以外	上記以外

表 3.3 IDHEAS-ECA に基づく PIF 分類

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Execution	Team Coordination	HSI	Procedure	Training
Base PIF								
Scenario Familiarity						(Confirm HSI to consider the scenarios)	(Confirm Procedures to cover the scenarios)	Enhance frequency of training
SF0: No-impact	1E-4	1E-3	1E-3	1E-4	1E-3			
SF1: Unpredictable dynamics in known scenarios	6.6E-4	6.6E-3	6.6E-3	6.6E-4	N/A			
SF2: Unfamiliar elements in the scenario	5E-3	5E-2	5E-2	5E-3	N/A			
SF3-1: Scenarios trained on but infrequently performed	1E-3	1E-2	1E-2	1E-3	N/A			
SF3-2: Scenario is unfamiliar, rarely performed	1.2E-2	1E-1	1E-1	3.3E-2	N/A			
SF3-3: Extremely rarely performed	3.3E-2	3E-1	3E-1	3.5E-1	N/A			
SF4: Bias or preference for wrong strategies exists, mismatched mental models	N/A	2.6E-2	2.6E-2	N/A	N/A			
Information Availability and Reliability						Improve information qualities		
Inf0: No impact - Key information is reliable and complete	1E-4	1E-3	1E-3	1E-4	1E-3			
Inf1-1: Information is temporarily incomplete or not readily available Inadequate updates of information	N/A	5E-3	5E-3	N/A	N/A			
Inf1-2: Information is moderately incomplete - a small portion of key information is missing	N/A	5E-2	5E-2	N/A	N/A			
Inf1-3: Information is largely incomplete	N/A	2E-1	2E-1	N/A	N/A			
Inf2-1: Low unreliable or uncertain	N/A	1E-2	1E-2	N/A	N/A			
Inf2-2: Moderately unreliable or uncertain	N/A	5E-2	5E-2	N/A	N/A			
Inf2-3: Highly unreliable	N/A	1E-1	1E-1	N/A	N/A			
Inf3: Extremely unreliable	N/A	3E-1	3E-1	N/A	N/A			
Task complexity						Enhance automation/improve HSI to support tasks	Improve task step alignments	(Enhance training)
C0: No impact	1E-4	1E-3	1E-3	1E-4	1E-3	Improve situation	-	(Enhance training)

b. HFEvs/CFM における状況因子を踏まえたヒューマンエラー防止策

a 項の措置に加え、或いは a 項の一般的措置だけでは規範的なもので具体化が図れないものが生じること、また、コンテキストにより組み合わせられる PIF が異なることから、コンテキストや HFEvs/CFM 全体のエラーモードから影響する PIF をその設計改善方策のプロセスについて検討する。

コンテキストやクリティカルタスク分析で抽出したタスクの特長付け等を調査し、a.項で定めた一般的設計改善方策も考慮しながら、具体的な設計改善方策を決定していく。

(4) 統合化プロセスの検討

本項では、(1)(2)(3)の検討を踏まえて統合化プロセスについて検討を行う。

まずプロセス自体の統合化については、リスク分析の観点から抽出されたタスクには、タスク分析の対象としているタスクの中にも含まれる場合があるが、HRA での分析はヒューマンエラーの可能性やその影響因子を特定することを目的としていることから、タスク分析とは独立して重畳的に行うことが望ましい。

ただし、HRA およびタスク分析で類似するプロセスを実施することから、これらを体系的に連携したプロセスとすべく表 3.4 のように整理する。すなわち、タスク記述開発 (Context,シナリオ開発) は、HRA とタスク分析で共通し、また、HRA で実施するクリテ

イカルタスクを特定するプロセスやワークロードでは、タスク分析の HTA や種々のタスク分析手法（Operation Sequence Analysis, OSA/Time Line Analysis, TLA, Cognitive Analysis など）を活用することでより精緻化ができ、また、分析する際の重複や不一致を生じる可能性を減らすことができる。

表 3.4 HRA とタスク分析の関係

	HRA	タスク分析
タスク記述開発	実施	実施
HEP_c	Human Failure Events analysis, Critical tasks analysis,	HTA, OSA, TLA, Cognitive
HEP_t (Treqd/Tavail の算定)	実施(*)	X(**)

*初期データは、訓練シミュレータのデータや運転員インタビューで取得

** タイムライン分析 (TLA) で取得

3.2.4 制御室設計統合化プロセス

図 3.3 に HRA の手法を用いたヒューマンエラー分析と STAMP/STPA プロセスを統合したプロセスを、ヒューマンエラーモード/要因に基づく体系的な設計展開手法として示す。図の左側点線枠で示すプロセスは、決定論的な設計要求と条件に基づく現存する制御室設計検証プロセスであり、右側枠外のプロセスは、HRA およびヒューマンエラー (Human Error, H/E) 分析に基づく、リスク情報に基づく追加的な設計プロセスである。

HRA のなかで、定性分析として実施される領域は、タスク分析と統合した形で示したものである。すなわち、コンテキスト分析はタスク分析、HRA とともに前提として必要なものであり、また、タスク分析の対象とされる HTA シーケンス/タイムライン分析、ワークロード分析は、HRA で実施される認知タスク分析と並行または共有化して実施する。さらに、重要なタスクに対しては、CFM/PIF を考慮して、上記に述べた方策で未然防止策を追加的に考慮する。この点について、H/E 分析と対策として、包括的に分析を達成すべく、STAMP/STPA を追加的に適用する。STAMP/STPA の適用については、4 章で述べる。

プラント機能要求分析から得られるプラント安全機能とその自動/手動の配分情報に基づき、タスク分析に基づかないトップダウン的設計考慮について 5 章で述べる。

HRA や H/E 分析の結果から得られる設計情報の設計や検証プロセスへの展開手法について 3.3 節で述べる。

3.2.5 節で述べるが、検証プロセスやヒューマンパフォーマンス監視の中で得られる定量的なデータは、PIF 毎の実証的 H/E 率として整理され、設計や HRA の PIF データベースの更新に活用される。

ヒューマンパフォーマンスデータを認知タスクレベルの PIF 毎の H/E 率として定量的

のパフォーマンス評価を行う際に実施される。また、プラント運転中の作業システムの有効性としても用いられる。

3.2.3 節で述べた通り、タスク要件（タスク分析結果や証跡）や PIF テーブルを基に、ISV で運転検証として評価するシナリオを作成し、また、評価を行うことにより、プラントの目標（安全性、発電等）やリスク面で考慮すべき手動操作を含む運転員タスクを網羅することができ、また、設計段階で事前に設計改善や設計入力情報として使用していることから、設計の最終段階で実施される ISV で生じる運転パフォーマンス上の問題点を最小限化でき、また、問題点が生じた場合の設計展開も容易となる。

また、設計や検証段階で収集したタスク要件や PIF テーブルを基に運転訓練などで運転員の行動観察や動作記録を基に収集したパフォーマンスデータと比較評価を行い、タスク要件や PIF または HEP 値を見直すことで、これらの情報の精緻化が図れるとともに、その情報に基づく設計へのフィードバックが可能である。さらに、設備の更新に伴う、HSI の変更、運転手順書の変更に伴う作業システムへの影響を評価する場合にも、上記テーブルや分析結果を用いることで影響を受けるタスク、プラント運転機能を追跡することが可能となり、影響評価が容易かつ確実になる。当該実践的手法については、第 6 章で述べる。

3.2.6 結果と検討

ヒューマンエラー分析の原子力発電所中央制御室設計への体系的な設計展開について検討した。すなわち、従来はリスク重要度指標にて抽出したリスク上重要な人的操作について、どのように設計対策に結び付けるかについて体系的な手法がないことから、HRA におけるヒューマンエラー分析と人間工学プロセスにおけるタスク分析プロセスについて関連性を明らかにし、ヒューマンエラー分析で実施されるヒューマンエラーモード／要因に基づき、設計対策立案を行う体系的な設計展開手法を考案した。更に、HRA で抽出されるヒューマンエラーモードを体系的に抽出するため、STAMP/STPA を補完的に適用することで、分析者が包括的にエラーモードを抽出できるプロセスについて検討した。なお、当該 STAMP/STPA の適用について、4 章で詳述する。

HRA で行われるヒューマンエラー分析プロセスを人間工学プロセスにおけるタスク分析に統合化を行うことにより、同じ情報またはコンテキスト分析に基づき、タスク分析で実施しているタスク要件や特徴を踏まえた CFM/PIF を特定し、また、STAMP/STPA を補完的に適用することによって、分析者が包括的に CFM/PIF を抽出することで、分析者の力量や知識経験に依存しない CFM/PIF の特定と、これらを未然に防止する設計対策案を設計要件として人間工学プロセスにフィードバックするプロセスを構築することが可能となる。

3.3 事例に基づく開発プロセスの詳細化と有効性評価

本章では、3.2 節で検討した制御室開発プロセスについて事例に基づく開発プロセスの詳細化と有効性評価を行う。また、3.2 節図 3.3 制御室開発プロセスのリスク評価結果の制御室設計、検証プロセスの展開とその有効性について述べる。

3.3.1 事例の選定

事例では、第三世代 HRA の手法との共通点／差異の確認や展開の仕方の違いを明らかにするため、IDHEAS の具体的手法である、IDHEAS-ECA(Event and Condition Assessment, ECA)[23] の適用事例としている軽水炉加圧水型原子力発電所 (PWR) の事故事象の一つである蒸気発生器細管破断 (Steam Generator Tube Rapture, SGTR) を採用する。

3.3.2 リスク分析とのインターフェース改善の展開

3.2.3 節で検討した結果を踏まえ、HRA の制御室設計への展開ステップについて述べる。

HRA の観点から追加した制御室設計における、分析／設計／評価手順を図 3.4 のように定める。

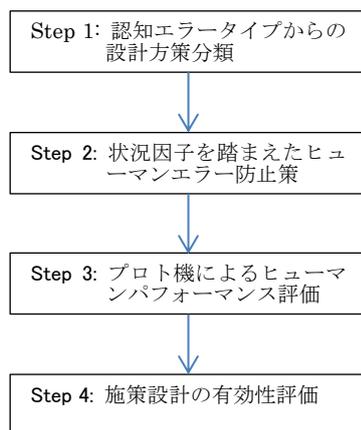


図 3.4 制御室開発プロセス

以下、各ステップにおける評価内容／手順について検討する。

Step 1. 認知エラータイプからの設計方策分類

Step1 では、3.2.3 章で検討した通り、表 3.3 で掲げた PIF 分類に基づき、改善すべき領域

を制御盤 I/F、環境改善 (HSI) , 運転要領書改善(Procedure), 運転員体制/ 技量改善 (Training) に分けて、それぞれの設計領域での対応改善施策についてマッピングする。また、PIF の数も多く、設計対策の適用制約も考慮し、エラーへの影響因子の大きいものをヒューマンエラー率の閾値で識別して優先順位の検討を行う。

これらの改善策については、今までの実験、経験から得られたエラープルーフ方策でカバーできるものもあることから、エラープルーフ策を纏めた HSI 設計ガイドをと比較して、過不足について評価し、不足するものがあれば、新たな設計考慮事項として設計に適用するデザインガイド (Style Guide) に反映する。

Step 2. 状況因子を踏まえたヒューマンエラー防止策

3.2.3 章で述べた通り、個別の影響因子に対する画一的な対応ではカバーできない、エラー因子に対して、タスク分析の結果 (コンテキスト、タスクの特徴) を評価してエラー防止策を検討する。具体的にはコンテキストやタスク手順をベースにエラー率を詳細に評価するとともに、特に繰り返し操作の要求されるタスクについては一回で終了するタスクに比べてエラー率やワークロードも高くなることから (ワークロード因子も PIF に含めているが、一連のタスクの中でさらに複数回の操作が要求されるものについて差別化するために)、各 CFM/PIF の HEP に対して、操作回数の因子を重みづけする。

なお、ヒューマンエラー防止策を考慮するうえで、医療分野で抽出された、図 3.5 に示す 5 つの原理[27][28]については、制御室におけるヒューマンエラー防止対策においても適用可能であり、発生防止の観点および波及防止の両方の観点包括的な対策の検討を行う。

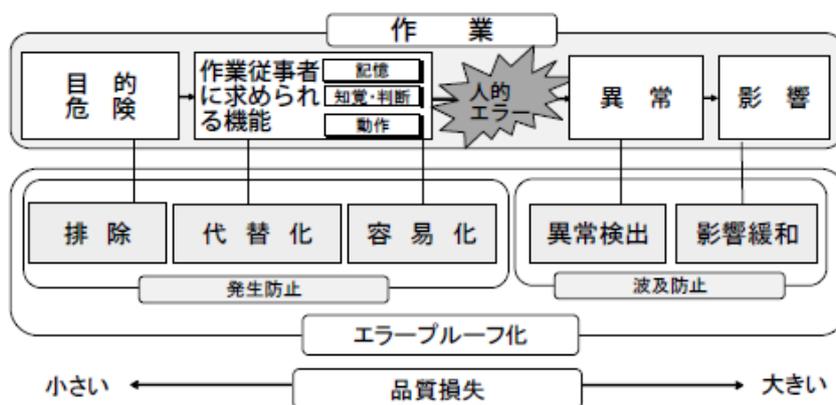


図 3.5 エラープルーフ化の原理([27][28]より作成)

まず、発生防止の観点からは、「排除」「代替化」については、「原子炉の制御を行う」ことから、危険源 (炉心損傷、放射能放出、人災のリスクがあること) (排除) はできない。「代替化」については、人間工学プロセスにおける機能分析および機能配分 (Function Requirement Analysis and Function Allocation, FRA/FA) においてシステムの制約条件や

人間の特性も考慮して手動への分配を分析している。したがって、「容易化」すなわち運転員の行うタスクを以下に容易化しサポートするか (Task Support) を設計上考慮していく。

具体的には、タスクサポートを支援する機能として、マンマシンインタフェース (Human Machine Interface, HSI) 設計の改善 (状況認知、ワークロード低減、インタロックなどの動作制限によるエラー防止支援)、運転要領書への反映や明確化 (記憶、判断の支援)、訓練 (事象判断、手順への順応や HSI の使用への順応) が主たる対応施策として考えられる。その他作業環境、スタッフ数/体制 (m-SHEL モデルでいう、E や L または m) も考えられるが、作業環境は中央制御室全体の作業環境設計として想定する全てのプラントモードで同一の環境条件を適用し (タスクや運転モードに依存しない)、スタッフ数や体制は別途人間工学プロセスにおける要員の配置および体制の分析 (Staffing and Qualification, S&Q) で評価し、これも画一的に定めていることから対象外とする。ただし、特別な作業環境の考慮 (重大事故事象など) する場合はこれらも評価対象とする。

波及防止の観点からは、以下が考えられる。

- ① 異常検知：全運転タスクに対する、運転要領書/訓練によるエラー防止作業管理 (手順書へのチェックマーク、3 ways communications, 指差し呼称等) の他、リスクの重要度に応じて追加的な方策 (警報、計算機機能による運転支援) が考えられる。特に、コミッションエラー (Error of Commission, EOC) については、中央制御室における運転管理者/当直長などの第三者、計算機機能による運転支援等による運転クルー以外の状況判断支援が有効である。
- ② 波及防止：波及防止には、プロセスの状態 (異常) 検知によるリカバリー動作が考えられるが、原子力プラントでは (限られた安全機能の維持以外は) 手動優先の設計思想があり、EOC の状態が続くとさらに状況を悪化させる可能性があり、波及防止よりも異常検出 (特に EOC の防止) が非常に重要となってくる。

Step 3 プロト機によるヒューマンパフォーマンス評価

Step 1,2 で検討した施策が有効かについて、プロトタイプやシミュレータ等を用いて、実際の状況でヒューマンパフォーマンスを確認する。Step 1,2 で用いた PIF に割り当てられたヒューマンエラー (Human Error, H/E) 率は過去の実績データに基づくものであるが、これらは当然使用する HSI や運転手順書、訓練の質により変化するものである。設計プロセスにおける当該評価で取得できるデータ数は限りがあり、H/E 率に影響を与えるほどの母集団を収集することは難しいが、Reference Plant の同型のシミュレータなどによる H/E 率の蓄積により適用する制御室システムにおける H/E 率を精緻化していくことができる。

Step 4 施策設計の有効性評価

決定論的な設計条件においては、設計条件や要求を満足することを達成度により評価可能であるが (例えば、あるポンプを中央制御室から操作するためのスイッチの設置等)、H/E

率を低減させるための施策設計においては、達成度評価では有効性を確認できない。

一方、デジタル HSI ではソフトウェアの改造が比較的容易であり、また、早期の設計段階でリスクの高いタスクに対する有効な設計方策を絞り込むことは重要である。

そこで、施策設計を入れた場合と入れない場合で Step3 のパフォーマンス評価を行い、母数は少ないがその際の H/E 率の発生率の差を評価する（代替設計方策がある場合その発生率の差で相対評価を行う）ことで、有効性の確認が可能である。また、H/E が認知タスクにより起こることから、インタビューや行動観察も補完的にを行い、そのチェックリストの評価結果を複合的に用いて評価することもできる。

3.3.3 事例によるプロセスの具体化とプロセスの有効性評価

本章では、3.3.2 節で検討した具体的な分析、設計、評価プロセスを事例に基づき展開し、実現可能性や有効性について評価する。なお、以下 Step 1-4 は、3.3.2 節での開発ステップに対応する形で具体化する。

なお、引用する HRA の情報源（参考文献[23]）が英語文献のため、原文との比較／邦訳による意味合いの変化の排除のため、必要に応じて原文を併記することとする。

(1) Step 1

認知エラータイプからの設計方策の検討結果を付録 A に示す。なお、当該付録 A で抽出した PIF は、参考文献[23]に基づく。

一般的な運転員パフォーマンス影響因子（Performance Influence Factor, PIF）のレビューでは、一部の例外を除き、PIF の H/E 率の大小に関わらず、PIF のタイプ毎に共通した対策が当てはまること、また、PIF レベルでの記述では具体的な人間工学設計ガイドが当てはまらない場合があるため、この場合は概ね対応できる領域を記述することとし、H/E 率の高い項目（赤、橙）ではなく各 PIF タイプのカテゴリ（No Impact としている各 PIF タイプの最初の行）に対応策を記載した。設計対応（“Measure treatment area”）は、HSI,手順書(Procedure),訓練 (Training) に分けて、それぞれ考慮事項を記載した。なお、黄色でハッチングしている部分は主たる考慮事項を、括弧書きは補助的な考慮事項として識別した。

Step1 で得られた結果について以下纏める。

- ・ PIF の H/E 率の大小に関わらず、PIF のタイプ毎に共通した対策が当てはまる。
- ・ これらの対策は、既に人間工学設計ガイドで取り扱っているものでカバーできることを確認した。
- ・ PIF レベルでの記述では具体的な人間工学設計ガイドが当てはまらない場合があり、したがって、具体的な対策が明確にならないことが多い。
- ・ PIF の H/E 率の大小による重要度識別は、PIF タイプ毎のレビューよりも、シナリオと結びつけた場合に有効な対策や優先順位を特定する場合に有効である。

(2) Step 2

事例に基づき具体化し、また、HRA の評価との差異を識別するため、IDHEAS-ECA[23]の事例の一つである加圧水型原子力プラントの蒸気発生器細管破損事象 (Steam Generator Tube Rapture, SGTR) の事例 (同文献[23] Appendix C) にて検証を行う。

HRA では、以下のプロセスとしている。

- ① シナリオ分析：事象記述、Timeline 分析から人的過誤事象(Human Failure Events, HFEvs)を特定、コンテキスト記述から初期 PIF の特定を実施。
- ② HFEvs 分析：タスクダイアグラム (運転シーケンス) 分析から、Critical Task の特定を実施。
- ③ クリティカルタスクについて認知タスクの分析を行い、適用される運転員失敗モード (Crew Failure Mode, CFM) を特定。また、タスクの特徴付けを実施し、PIF を特定。
- ④ 各クリティカルタスクに含まれる CFMs/PIFs の HE 率から各クリティカルタスクの HEP を計算し、各 HFEvs に含まれるクリティカルタスクの HEP から各 HFEvs 毎の HEP を計算する。

一方、H/E 対処分析として以下のプロセスを上記 HRA プロセスに対して重疊的に追加する。

- ① HRA では PIF として HSI の要因もカテゴリで出てくるが、あくまでも影響因子の取り扱いであり、H/E 率に影響の大きい、HFE、CFM の分析比重が高いため、H/E 対処分析としては、HRA の分析プロセスに対して、特に作業システムに関わる PIF の適用 (すなわち、HSI,手順書、訓練などの PSF) に重点を置いて追加的な分析を行う。
- ② 操作回数分析：コンテキスト、タイムライン分析、運転シーケンス分析から、必ずしも出てこない、操作回数分析 (プロセス手動制御に伴うもの) を重疊的に実施し、潜在的人的過誤率 (Human Error Probability x, HEPx) 操作回数を算出し、H/E 対処の観点から、重点的に対策を行うタスクの抽出を行う。操作回数による重みづけを行う観点としては、一回で完了するタスクに対して複数回行うタスクに対する H/E の発生確率の差別化や、特に認知的タスクに対して、操作タスクには物理的ワークロードも伴うことから特に HSI や手順書の要因を考慮するうえで重要になるからである。
- ③ 発生防止 (未然防止) /波及防止 (異常検出) の観点から、対策を検討する。
未然防止については、Step 1 で検討した通り、HSI,手順書(Procedure),訓練 (Training) の観点 (状況によりその他の考慮も考えられることからその他も追加)、異常検出については、運転クルー以外の独立した異常検出機能として、運転管理者 / 当直長等の第三者、或いは計算機による診断機能を設け、それぞれの面から検討する。また、事象が進展し条件が確立することによって、設計上運転員に期待するタスク (決定論的に重要なタスク) および確率論上重要なタスク (リスク重要度指標からスクリーニングしたタスクや HEPx 操作回数からクリティカルタスクの中でも H/E 対処の観点から重点的に対

応すべきタスクについて、期待される操作や注意喚起のための識別等を記述する。

これらの統合的な H/E 対処分析を行った結果を以下示す。

① シナリオ分析

PRA のイベントツリーより以下のタスクが HFE として特定：

HFE1: 破損 SG の隔離失敗 (Fail to isolate the ruptured SG.)

コンテキスト分析の結果以下の PIF を特定：

タスクの複雑さ (Task complexity), 手順(Procedures), マルチタスク/中断
介入/注意をそらす(Multitasking / interruption / distraction), ストレス/時間
制限(Stress and time pressure)

② 人的過誤事象 (HFEvs) 分析

図 3.6 に示すタスクダイアグラムを作成し、2つのキータスクを特定。最初のタスクは、自動バックアップ (自動トリップ) があることから、クリティカルタスクとして以下を特定。

HFE1-T1: 事故時手順書-3 (SGTR 事象対応手順) に入り、当該手順書に基づきタスクを遂行 (Enter and perform EOP (Emergency Operating Procedure)-3)



図 3.6 HRA でのタスクダイアグラム

③ 認知タスク分析

認知タスク分析を行い HFE1-T1 に対して以下の 3つの CFM を特定：

T1-CFM1: 検出の失敗(Failure of Detection)

T1-CFM2: 理解の失敗 (Failure of Understanding)

T1-CFM4: アクションの失敗 (Failure of Execution)

タスクの特徴付けとして以下を特定(No impact は除く)：

特記要求事項 – 破損蒸気発生器の隔離を行い、1次系圧力を破損SG圧力以下に加圧器逃がし弁にて手動制御すること。

タスク順序(Cue) – タスクは、2次系の放射線モニタ警報から開始される。

人員 (Personnel) – 習熟訓練された運転員

手順書 (Procedure) –EOP-0 (原子炉トリップ/安全注入/事象判別)とEOP-3

(SGTR事象対応手順) がシミュレータ訓練でされている。手順書は訓練のフィードバックを受けて最適化されている。

タスク特徴も分析し、以下の PIF を特定(特定した理由は、引用した IDHEAS-ECA 文献[23]に記載されているため省略)；

T1-CFM1

タスクの複雑さ (Task complexity) : C0 – No impact.

手順書 (Procedures) : P0 – No impact.

マルチタスク (Multitasking) : MT0 – no need for multitasking.

精神的疲労、ストレス、時間制限 (Mental Fatigue, stress and time pressure) : FS0 – No impact.

T1-CFM2

タスクの複雑さ (Task complexity) : C30 – No impact.

手順書 (Procedures) : PG0 – No impact.

マルチタスク (Multitasking) : MT0 – no need for multitasking.

精神的疲労、ストレス、時間制限 (Mental Fatigue, stress and time pressure) : FS0 – No impact.

T1-CFM4

タスクの複雑さ (Task complexity) : C42 – EOP-3は複数の並行操作手順が含まれ、いくつかの手順は制御タスクがある。(EOP-3 has multiple proceduralized steps and some steps need control manipulation)

手順書 (Procedures) : P0 – No impact.

マルチタスク (Multitasking) : MT0 – no need for multitasking.

精神的疲労、ストレス、時間制限 (Mental Fatigue, stress and time pressure) : FS0 – No impact.

④ HEP 見積

表 3.5 に示す通り、HFE1 に対して包含するクリティカルタスク(HFEv1-T1)について整理し、各 PIF にアサインされるノミナル PIF を累積し、HEP を算出する。

表 3.5 クリティカルタスク (HFEv1) HEP 見積

HFEv1: 破損 SG 隔離失敗かつ 1 次系圧力制御失敗		
クリティカルタスク	適用する運転員失敗モード (CFMs)	各 CFM に適用する PIF
事故時手順書-3(SGTR 事象対応手順)に入り、当該手順書に基づきタスクを遂行	T1-CFM1: 検出の失敗	No impact (基礎的 PIF)
	T1-CFM2: 理解の失敗	No impact (基礎的 PIF)
	T1-CFM4: アクションの失敗	タスクの複雑さ(付加的 PIF) C42 –複数の並行操作手順と制御操作

一方、H/E 対処分析として分析した結果、引用 IDHEAS-ECA 文献[23]では評価されない、特にマンマシン関係のエラーモード (CFM) について追加的に特定した。

結果を以下に示す。(詳細分析結果は、付録 B に示す。)

- ① (決定論的) 設計プロセスに基づくタスク分析 (従来の FRA/FA から手動へ割り当てたタスクに対するタスク分析) から、抽出されたタスク記述、タスク要件 (**Controllers, Indicators, and other equipment to perform tasks**) を基に、主要なタスクに対する運転員失敗モード (CFM) に対して、HSI などの影響因子を考慮して評価を実施。

以下の HFEvs および CFM/PIF について追加的に特定した。;

- a. 原子炉トリップおよびタービントリップの確認(**Check reactor trip & turbine trip**)

CFM1:PIF- C1, HSI2,3,5, EVN7, FS6, SF0, Inf0

※上記の付加的影響因子を特定した理由:EVN7(大きなノイズの影響、Loud or burst noise), FS6 (長い期間低いワークロードから高いワークロードへの急激な増加/Sudden increase in workload from a long period of low to high)としたのは、原子炉トリップ時多くの警報が多発し(EVN7)、原子炉トリップが発生した時点で長い期間ワークロードが低い状態から高い状態に突然遷移するため(SF6)、検知タスクに影響と評価した。HSI は、起こりうる HSI 設計 (警報、指示計の配列) の影響因子 (2: 隣接する情報源からの技術的差異を示す兆候無し/No sign or indication of technical difference from adjacent sources (meters, indicators)、3:タスクに関連する情報表示が分散し/組織化されず、または同時にアクセスできない。/Related information for a task is spatially distributed, not organized, or cannot be accessed at the same time, 5: 混雑した複数の情報表示の中で目標となるパラメータ、警報が目立たない。/Poor salience of the target (indicators, alarms, alerts) out of the crowded background) を選択。ただし、エルゴノミクス設計ガイド適用により事前に除去できる因子 (例えば、HSI6: 一貫していない形態、単位、シンボル、表形式/Inconsistent formats, units, symbols, or tables 等) は Step 1 や当該プロセス以外で対策実施済として除外) なお、ヒューマンエラー率の計算では最も影響の高い HSI5 を選択。

CFM4:PIF- C31, HSI2,3,5, EVN7, FS6, SF0, Inf0

※上記の付加的影響因子を特定した理由: C31(多くのステップを持つ単純な手順書タスクステップの遂行/**Straightforward Procedure execution with many steps**)としたのは、E0 (原子炉トリップ手順書) においては多くの手順書に基づく操作 (確認操作も含む) があるため。EVN7, FS6, HSI5 の選択は、CFM1 の評価と同じ。

- b. 安全注入状態の確認 (Check Safety Injection (SI) status)

CFM1: PIF- C1, HSI2,3,5, EVN7, FS6, SF0, Inf0

CFM4: PIF- C31, HSI2,3,5, EVN7, FS6, SF0, Inf0

※上記の付加的影響因子を特定した理由：SGTR 事象の場合、a.事象とほぼ同時に起こることから、EVN7, FS6 を選択。HSI の影響因子の選択も a. 事象と同様。

- c. 緊急給水弁のラインナップ確認 (Check Emergency Feedwater (EFW) valve alignment)

CFM1: PIF- C31, HSI2,3,5, FS6, SF0, Inf0

※上記の付加的影響因子を特定した理由：c.以降は警報の多発はない状態のため、EVN7 の因子はないと評価。なお、c.項は a.b.からの一連のタスクとして FS6 があると評価。その他は a.の評価と同様。

CFM4: PIF- C31, HSI2,3,5, SF0, Inf0

- d. 蒸気発生器水位の制御 (Control SG level)

CFM1: PIF- C0, HSI2,3,5, FS8, MT1, SF6, Inf0

CFM4: PIF- C31, HSI2,3,5, FS8, MT1, SF6, Inf0

※上記の付加的影響因子を特定した理由：c.以降は警報の多発はない状態で、また、突然のワークロードの増加から一定時間経過しているため、EVN7, FS6 の因子はないと評価。ただし、FS 因子は突然のワークロードの変化 (FS6) から、感情的なストレス (anxiety, frustration) に変化するとして、FS8:感情的ストレス/Emotional stress (e.g., anxiety, frustration)を残した。その他は a. の評価と同様。MT1(注意を向ける必要がある他の並行タスクによって注意がそれる/Distracton by other ongoing activities that demand attention)は、SG 水位手動制御操作は SGTR 事象を通じて、注意を向けながら、他の対応操作と並行して行うため選択した。

- e. 蒸気発生器破損の診断(Diagnose SG tube rapture)

CFM1: PIF- C3, HSI2,3,5, FS8, SF0, Inf0

※上記の付加的影響因子を特定した理由：C3 (高い注意喚起のための検出要求/Detection demands for high attention)は、検知タスク (CFM1) として、事象判別のため、タスク要求 (Cue) となる、放射線モニタ警報 (Secondary radiation alarm) の発信を注意深く監視し検知することが要求されるため選択した。なお、本タスク以降は、HRA で実施した HFE1-T1 に相当する。

CFM4: PIF- C31, HSI2,3,5, FS2, FS8, SF0, Inf0

※上記の付加的影響因子を特定した理由：FS2 (感覚的時間制限対応によるプレッシャ/Time pressure due to perceived time urgency) は SGTR 事象が発生した場合 (診断時)、設計で要求された時間制限以内に隔離操作が要求されることから、選択した。

f. 破損蒸気発生器の隔離 (Isolate flow from ruptured SG)

CFM4: PIF- C31, HSI2,3,5, FS2, FS8, SF0, Inf0

※上記の付加的影響因子を特定した理由：e.事象と同様。

g. 1次冷却材温度および圧力のクールダウン (Cool down Reactor Coolant System (RCS) temperature & pressure)

CFM1: PIF- C0, HSI2,3,5, FS8, MT1, SF0, Inf0

CFM4: PIF- C31, HSI2,3,5, FS8, MT1, SF0, Inf0

※上記の付加的影響因子を特定した理由：d. の評価と同様。破損 SG 隔離後のため、FS2 はないものと評価。一方、MT1 は、サブクールに注意しながら、RCS 温度調整 (主蒸気逃し弁(Main Steam Relief Valve, MSRV)操作)、加圧器逃がし弁(PROV)による1次冷却材 (RCS) 圧力調整を並行して他の作業と並行して操作間隔を空けて実施するため選択した。

② ①のタスクのうち、d.およびg.のタスクは事象進展中操作間隔を空けてパラメータに注意を向けながら頻繁に行うため、10回とした。その他は1回で終了するため、1を設定した。

③ ①の各操作に対して未然防止および波及防止 (異常検出) の観点で対策を考案した。図 3.7 に a. 原子炉トリップおよびタービントリップの確認および e. 蒸気発生器破損の診断 (HRA の HFE-T1 の最初のタスク (Enter EOP-3) に相当) に対する対策検討結果を例として示す。

例えば、a. 事象における未然防止策として、原子炉トリップまたはタービントリップの確認に必要なしゃ断器、パラメータの情報を集約した画面をタスクサポート画面として予め設計し、中央制御室の監視操作画面に取り込んで HSI2, 3 の影響を無くす (この場合、HSI5 については、原子炉トリップ/タービントリップ警報は他の警報と識別して表示することとしており HSI-5 も無くす)。また、C3 (多くのパラメータ監視、検知が要求される情報の多くの表示形態または表示分類/Monitor many parameters, Many types or categories of information to be detected) の影響も低減できる。

波及防止に関しては、運転員監督者 (当直長) が運転員の判断を検証可能とするために、役割を絞って (安全機能維持や運転クルーのクリティカルタスクの遂行や判断の妥当性の確認)、運転員に提供する上記と類似の情報を提供することで、運転員のストレス (その他の運転対応要領の準備等クリティカルタスクや事象の判断に影響を与えるディストラクションが考えられる) からくる EOC を低減するため、第三者による妥当性の判断や、また、計算機により、原子炉トリップまたはタービントリップの機器ステータス状態 (あるべき姿) と自動チェックした結果を運転員に提示することで、HE の確率を下げる (リカバリー効果) を期待できる。

	未然防止	運転支援 (Recovery action 支援)
a. 原子炉トリップおよびタービントリップの確認	タスク支援画面の提供 (原子炉トリップおよびタービントリップ確認を行うためのパラメータ/機器状態の集約画面)	計算機で原子炉トリップ状態を確認するために必要なパラメータ/機器状態をチェック 確認用チェックリストとチェック対象パラメータ/機器状態の表示 / 運転管理者への上記情報の提供
e. 蒸気発生器破損の診断	EOP-3 への移行条件を判定するパラメータ (放射線モニタ警報) の目立つ位置への表示 (大型表示画面への表示)	パラメータ/機器の状態が移行条件に合致するかを計算機で判定し、運転員へ提供 確認用チェックリストとチェック対象パラメータ/機器状態の表示 / 運転管理者への上記情報の提供

図 3.7 対策検討

なお、上記の設計施策は、プロトタイプシミュレータによる運転検証（以下 Step3）や先行プラントの運転経験レビューにより、状況認知(Situation Awareness, SA)やワークロードの改善点として特定され、既に設計に取り込まれているが、H/E 対処分析の観点からもリスク上重要なクリティカルタスクに対する設計考慮として確認ができ、また、第三者チェックとしてこれらのクリティカルタスクを特定し、第三者への提示（確認）や計算機支援による状態チェック/告示機能の追加することにより、異常検出の改善を図るうえで、H/E に対するリカバリ効果が期待できる。図 3.8 にリスク上重要なクリティカルタスクまた、決定論的に運転員に期待するタスクをリスト化し、関連パラメータとともに集約表示した画面を示す。

このような画面を、第三者（運転管理者等）が状況を確認し、そのタスク前後において、運転員のタスク進行をサポートすることにより、実際の運転状況における注意喚起を行い、異常検出を高めることができる。

クリティカルタスクリスト (EOP-3)			
Step#	クリティカルタスク	関連機器状態/	タスク目標 (基準)
3-14	破損 SG 隔離	MSIV(VXXX) 開 MSRV(VXXX) 開	全閉 全閉
3-20	RCS 減温および減圧	... RCS サブクール XXX°C	... RCS サブクール 減温率 xx°C/hr

図 3.8 対策検討

(3) Step 3

プロトタイプ機（モックアップ、シミュレータ）を用いて、設計施策を取り入れない場合と取り入れた場合に対してパフォーマンス評価および HE 率の算定を実施する。

一般的に、原子力発電所制御室のような大規模、複雑なシステムにおける、HSI システムのパフォーマンスを評価するうえで、運転員のワークロードと状況認知(SA)が、システムの運転に影響を与え、エラーを発生させる要因として重要とされている[29]。

状況認知は、認知タスクの **Detection** や **Understanding** に直接影響を及ぼすとともに、この認知プロセスを基に行う後続のプロセス (**Decision Making** や **Action**) に対して間違った反応 (**EOC**) を及ぼすため、この点を詳細にモニタし、評価することが重要である。

また、ワークロード、特にメンタルワークロードは認知タスク全般に渡り影響を与え、状況認知にも影響を及ぼす。図 3.9 にワークロードと状況認知の関係を示す[29]。ワークロードがある程度までは状況認知レベルは一定であるが、ワークロード(**Internal workload**)が許容値を超えると、ワークロードに比例して状況認知レベルが下がる。

さらに、**External Workload** と **Internal Workload** の関係性を評価することで、**Base PIF** として経験上 HE 率に大きく寄与する、シナリオ親和性 (**Scenario Familiarity**) やタスクの複雑さ (**Task Complexity**) の設定を評価することが可能である。(すなわち、評価者により **External Workload** と自身の経験に基づきタイプを設定するが、**Internal Workload** を測ることで当該作業システムにおけるより正確な設定が可能)。

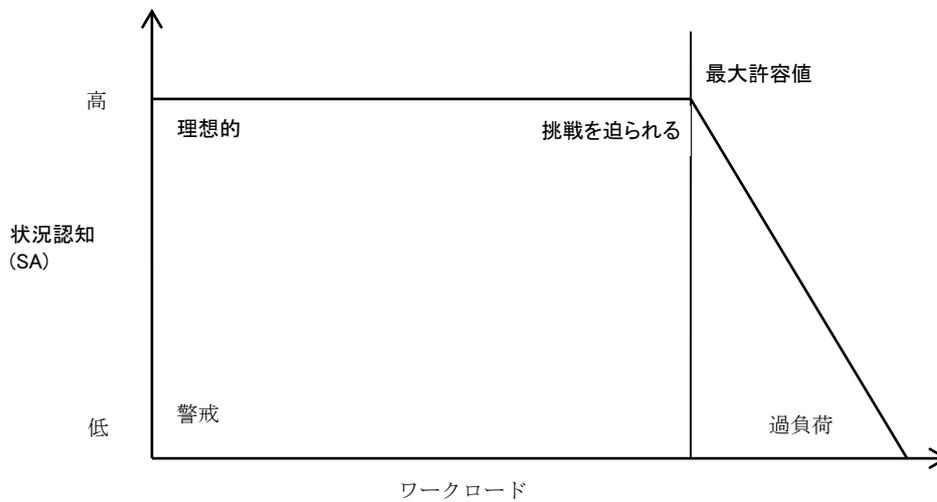


図 3.9 状況認知とワークロードの関係([29]より作成)

状況認知およびワークロード評価については多くの測定方法が提案されている。

以下代表的なものを示す。

状況認知(SA):

- Subjective techniques[30][31]

被験者または観測者によって主観的評価により実施。そのため、評価者のバイアスがかかる可能性がある。測定対象（アンケートで聞く内容）やレート数は異なるが、基本的に Low から High に並べた Likert rating score で判定する。

- Questionnaires

注目すべき評価項目に対して、評価者が被験者に対して、質問形式で詳細に被験者の SA について確認することにより実施する。インタビューのタイミングはシナリオ終了後、シナリオ遂行中行う。（各タスクの状況認知(SA)状況は、短期記憶として直ぐに忘却してしまう可能性があり、重要なタスクの SA 評価についてはあえてシミュレータを止めて確認する場合もある。）最もメジャーな測定方法の一つとして、Situation Awareness Global Assessment Technique (SAGAT)がある[32]。

SAGAT は、状況認知(SA)について、特定のアクション直後にシミュレータを止めて、Level 1(Perception of data=認知モデルでいう、Detection), Level 2 (comprehension of data=認知モデルで言う、Understanding), Level 3 (projection of data=認知モデルで言う、Decision Making)、という、包括的な認知モデルの3つの観点から測定するものである。Bias のかからない状態で客観的なデータを取得するメリットがある一方、シミュレータを止めて評

価を行うことから、包括的なワークロードやパフォーマンスを測定するデメリットも生じる。一方で、昨今の生態計測データ（Eye tracking, Motion capture）やクルー会話ログ、デジタル HSI となったことによる、画面タッチ操作ログの履歴データとの照合により、また、電子化手順書システムの操作完了ログを確認することで特定ができると考えられ、当該手法を用いた制御室運転員パフォーマンス評価を 6 章において検討する。

- Performance Measure

Performance Measure はシミュレータによる運転員のタスク遂行において、予め評価すべき運転員のふるまい（プラントパラメータの監視、診断或いは操作など）を設定し、シナリオ終了後客観的な情報（ある注目すべき監視パラメータやプラント状況の確認を運転員の会話記録から判定したり、あるタイミングに的確に操作したかを観察やシミュレータログから確認する）から判定する。Performance Measure は、状況認知(SA)評価だけでなく、その他の評価（達成度評価）にも適用できる。

- ワークロード(Work Load, WL) :

様々な評価手法があるが、最も広く使用されているものの一つとして米国航空宇宙局（NASA）で開発された、NASA-Task Load Index (TLX)[33]がある。

タスク終了後、表 3.6 に示す評価項目について、0-10 段階の評価シートおよび 6 つの評価項目の 2 つを取り上げてどちらが支配的かについて、それぞれ被験者に記入してもらい、Rating（絶対尺度）と Importance weighting(重要度重み)および Overall Workload(全体的な負担)を算定する。

表 3.6 NASA-TLX 評価項目

項目	説明
精神的要求/ 知的・知覚的欲 求	<u>どの程度、精神的・知覚的な活動が必要でしたか？</u> (例:考える、意思決定をする、計算する、記憶する、観察する、検索する等) 作業は容易でしたか、それとも困難でしたか。単純でしたか、それとも複雑でしたか。 苛酷でしたか、それとも寛大でしたか。
身体的要求	<u>どの程度、身体的活動が必要でしたか？</u> (例:押す、引く、回す、操作する、動き回る等) 作業は容易でしたか、それとも困難でしたか。ゆっくりしていましたか、それともきびきびしていましたか。ゆるやかでしたか、それとも努力を要するものでしたか。落ち着いたものでしたか、それとも骨の折れるものでしたか。

項目	説明
忙しさ/ 時間切迫感	<u>作業や要素作業の頻度や速さにどの程度、時間的切迫感を感じましたか？</u> 作業ペースはゆっくりしていて暇でしたか、それとも急速で大変でしたか？
作業達成度	<u>参加メンバー(あなた自身を含む)によって設定された作業の達成目標の遂行について、どの程度成功したと思いますか？</u> この目標達成における作業成績にどのくらい満足していますか？
努力	あなたの作業達成レベルに到達するのにどのくらい一生懸命(精神的および身体的に)作業を行わなければなりませんでしたか？
不満度	作業中、どのくらい、不安、落胆、いらいら、ストレス、不快感、あるいは安心、喜び、満足、リラックス、自己満足を感じましたか？

以上より、状況認知およびワークロードの測定を通じて、認知タスクの達成度の評価をクリティカルタスクに対して実施する。なお、状況認知については、被験者への質問表によるインタビューやパフォーマンス観察により評価を行う。

H/E 率測定、上記のパフォーマンス評価を基に、認知タスクの成功、失敗についてクリティカルタスク毎、CFM 毎に実施する。

例として、状況認知については 5 段階の Likert Scale で評価項目（例えば、“プラントの状況理解”、“プラント安全機能”）を平均で示し、ワークロードについては、包括的ワークロードと支配的な要素（Weighting factor）について規格化した値を表 3.7 のようにクリティカルタスク毎に、設計施策を適用する前後で評価する。

例として、a.と e.のクリティカルタスクについて評価した例を表 3.7 に示す。

なお、状況認知やワークロードの分析内容はクリティカルタスクに含まれる各 PIF のどの因子と因果関係があるか、また、この因子の影響を排除するのに寄与する HSI 機能や手順書機能について被験者へのインタビューや行動観察からの特記事項があれば関連性を明らかにするために、“設計改善”の欄の対応設計項目に該当する改善 PIF を記載し、また、“CFMs/PIFs”の欄には該当する PIF にマーク（表の例ではアンダーライン）を行う。

表 3.7 対応設計前後のパフォーマンス評価の例

クリティカルタスク	CFMs/PIFs	状況認知 (5 pt. scale)	ワークロード (TLX-Overall/ Major weight)	設計改善
a. 原子炉トリップおよびタービントリップの確認	CFM1:PIF-C1, <u>HSI2.3.5</u> , <u>EVN7</u> , FS6, SF0, Inf0 CFM4:PIF-C31, <u>HSI2.3.5</u> , <u>EVN7</u> , FS6, SF0, Inf0	改善前: 3.1※ 改善後: 4.0※	改善前: 68%※ 改善後: 50%※	未然防止: タスク支援画面の提供 (原子炉トリップおよびタービントリップ確認を行うためのパラメータ/機器状態の集約画面) 運転支援: 計算機で原子炉トリップ状態を確認するために必要なパラメータ/機器状態をチェック 確認用チェックリストとチェック対象パラメータ/機器状態の表示/運転管理者への上記情報の提供
e. 蒸気発生器細管破断の診断	CFM1: PIF-C3, <u>HSI2.3.5</u> , FS8, SF0, Inf0 CFM4: PIF-C31, <u>HSI2.3.5</u> , FS2, FS8, SF0, Inf0	改善前: 2.6※ 改善後: 3.2※	改善前: 61%※ 改善後: 52%※	未然防止: EOP-3 への移行条件を判定するパラメータ (放射線モニタ警報) の目立つ位置への表示 (大型表示画面への表示) 運転支援: パラメータ/機器の状態が移行条件に合致するかを計算機で判定し、運転員へ提供 確認用チェックリストとチェック対象パラメータ/機器状態の表示/運転管理者への上記情報の提供

※注: 状況認知、ワークロードの値は例として入れた。対象物に対して設計改善前後の値を、状況認知、ワークロードに関する各種手法で評価を行う。

なお、パフォーマンス評価は、制御室の統合システム検証 (Integrated System Validation: ISV) で実施するが、特に、安全設計や H/E 対処分析で抽出されたクリティカルタスクについては、設計施策の有効性を設計の早い段階で確認するため、シナリオやシミュレータの模擬範囲もそのエリアに絞って行うことで、設計開発 PJ 上のリスクの低減にも効果がある [34][35]。

(4) Step 4

Step 3 で実施した、設計施策適用前後の SA, WL の比較評価の結果、改善が見られない場合は、想定した PIF の影響を排除できない、或いは、そもそも異なった PIF の影響がある可能性があり、状況認知やワークロード評価の内容を詳細に分析し、適用する PIF や CFM 或いは設計施策方案を見直す。また、見直した PIF や CFM、或いは、Recovery Factor に基づき HE 率について再計算を行い、HEP の見直しを行う。

3.3.4 結果と検討 (制御室開発プロセスの見直し)

3.3.2 節、3.3.3 節では、制御室設計開発プロセスの中で、HRA で得られるリスク評価を H/E 分析の中で設計要求として展開する具体的手法を事例に基づいて述べた。ここでは、最終的な見直し結果について検討する。

図 3.10 に制御室設計開発プロセスのうち HSI 設計プロセスについて、ヒューマンエラー分析と対策(Human Error Analysis, H/E 分析)経由でリスク評価結果を HSI 設計情報として取り入れる前後のプロセスを示した。図 3.10 では、HSI 設計インプットとして、「運転コンセプト/HSI コンセプト⇒エルゴノミクス設計ガイド」と簡略的に記載したが、実際は、運転コンセプト/HSI コンセプトは、規制要件 (Regulatory Requirement) とともに、HSI 設計における基本要件事項として HSI 設計の中で考慮される。また、タスク分析 (TA) のアウトプットである、図 3.10 で示した、タスクを遂行するために必要な監視操作情報、警報、人員配置の特定 Tavail 特定は、タスク支援要求(task support requirement)として HSI 設計のインプットとなる。HSI エルゴノミクスガイドは設計ルール(Style guide)として HSI 設計全般に適用される。そのほか、HSI 設計を実装する計測制御装置 (I&C System/HSI Platform) やプラントの系統設備の動作情報が HSI 設計の入力情報となる[36][37]。

ヒューマンエラー分析および対策プロセス統合後の人間工学プロセスにおいては、HRA で抽出された HFEvs やクリティカルタスクについて分析したリスク情報に基づく設計考慮が、タスク要求として追加される。ただし、人間工学プロセスで実施されるタスク分析は、分析する対象範囲が HFEvs やクリティカルタスク以外に対しても実施されるため、並行して実施されるプロセスとして位置づけた。

さらに、3.3.2 節、3.3.3 節で検討したヒューマンエラー分析および対策の詳細分析評価ステップ(Step1~4)における HRA と人間工学プロセスとのインターフェースについて図 3.11 に示す。

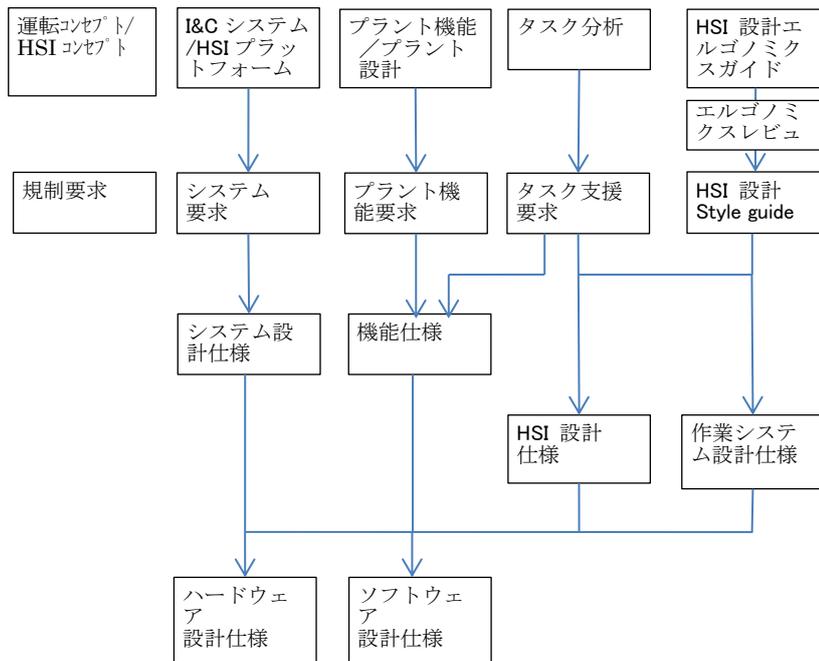
HSI 設計ガイド (HSI Design Style Guide) は、主に制御室運転設計概念、システム要件やその他の要件から、設計仕様のベース (例えば、VDU 画面の適用サイズ、表示画面上の機器のシンボル、色、大きさ等) をエルゴノミクスガイドに適合した形で定めるものであり、HFE プロセスの中で設計されるが、Step1 のエルゴノミクスレビュー結果は、HSI 設計ガイドとの比較や HSI 設計エルゴノミクスガイドなどを参照し、追加すべきものがあれば HSI 設計ガイドに追加を行う。

Step 3 のヒューマンパフォーマンス評価については、ヒューマンエラー分析および対策からのタスクサポート要求に応じた設計施策の他、リスク上重要なタスク (RIHA) 以外のタスク分析の結果、評価すべきタスクやタスクサポート要求に応じた設計施策も統合して設計段階で必要に応じて実施する。

なお、図 3.3 の検証および妥当性確認プロセスでは、パフォーマンス監視およびヒューマンパフォーマンスデータ収集として独立させたが、ヒューマンパフォーマンス評価として検証および妥当性確認プロセスに含めた。また、図 3.3 にはタスクサポート評価を含めていない。これは、図 3.3 では、パフォーマンスデータ収集⇒PIF へのフィードバックを簡略的

に記載したが、ここでは、ヒューマンパフォーマンス評価(Step4)を経て、PIF/CFMの要素の改訂やその前提が正しい場合はタスクサポート要求の見直しなど、詳細プロセスを明らかにしたためである。

(現状)



(ヒューマンエラー分析統合後)

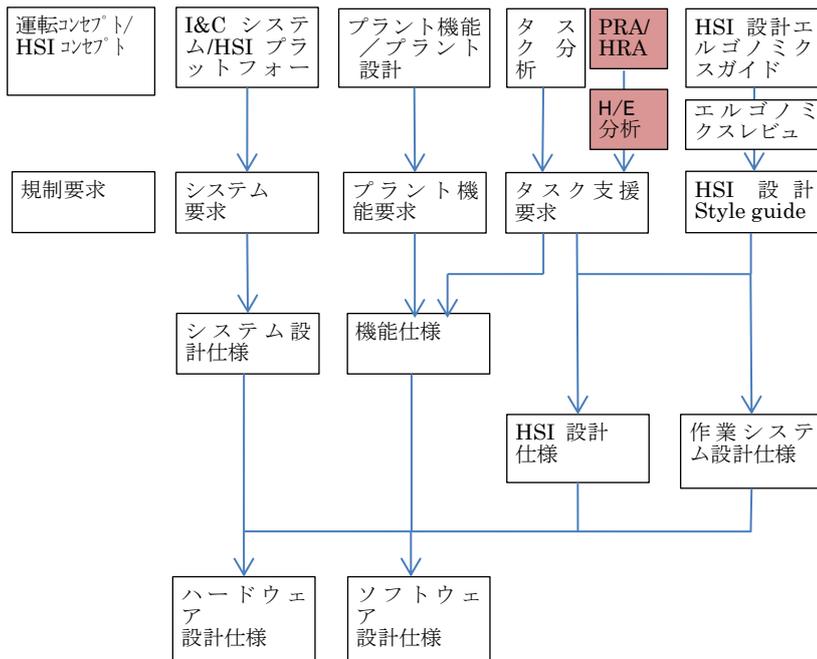


図 3.10 制御室開発プロセス (ヒューマンエラー分析統合)

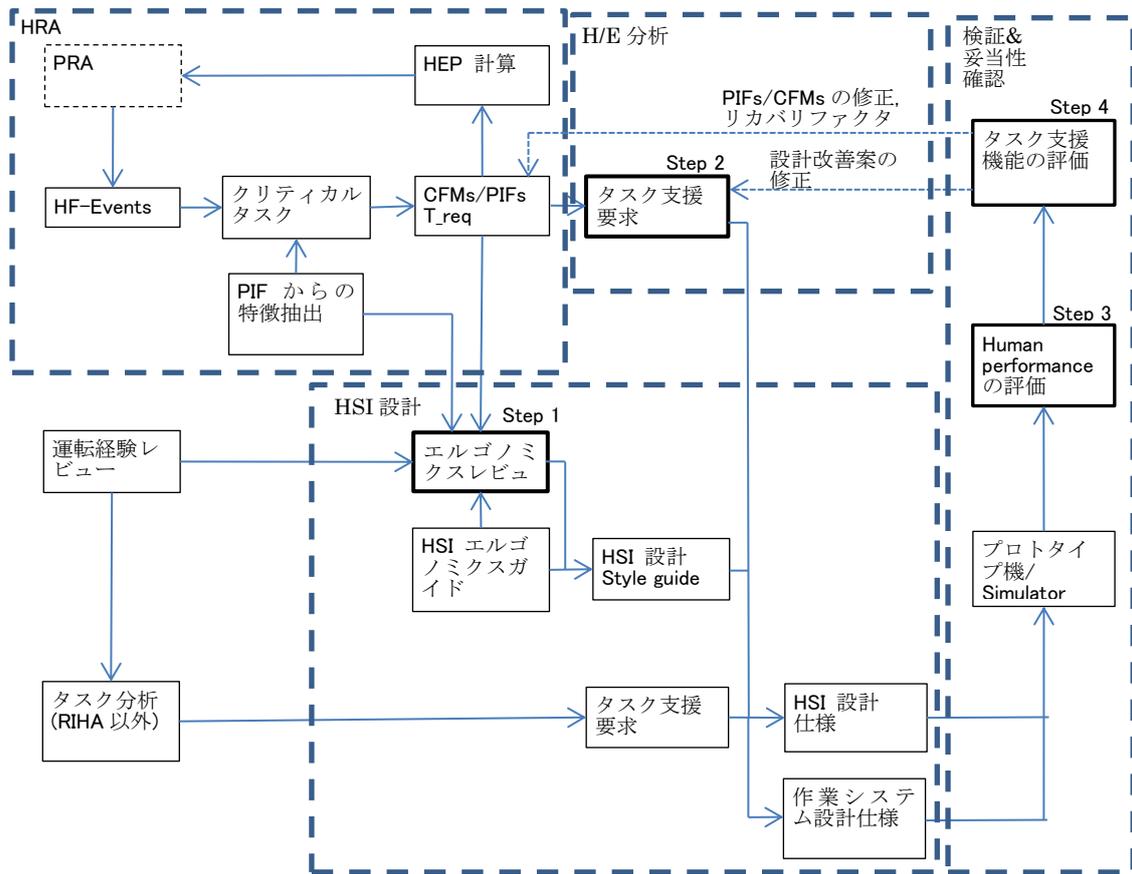


図 3.11 HRA と人間工学プロセスとの統合化プロセス
(HSI 設計検証における詳細プロセス)

3.4 結果と検討

本章では、リスクマネジメントを考慮した制御室設計統合化プロセスの検討を行った。具体的には、既存のヒューマンエラー分析の人間工学プロセスへの適用状況の整理と追加的な枠組みについて検討し、第三世代 HRA の分析プロセスを人間工学設計適用の観点でレビューを行うとともに、従来の課題とされた、HRA の想定条件を人間工学プロセスへ体系的に取り入れる設計開発統合プロセスを開発した。

さらに、第三世代 HRA で実施している事象シナリオを基に、当該プロセスを実行し、リスク情報を考慮した設計要求事項の取得と設計改善への応用を具体事例として示し、当該統合化プロセスの有効性について確認した。

第4章

最新リスク分析をさらに網羅性あるシナリオ開発につなげる STAMP/STPA 手法をベースとしたヒューマンコントローラモデルの適用

4.1 はじめに

2.4節で述べた通り、IDHEAS[23]に代表される第三世代HRAでは、体系的な分析プロセスにより、分析者の知識や経験に依存しないよう評価を行うようにし、また、第3章で述べた通り、第三世代HRAの体系的プロセスを人間工学プロセスへ取り込むことにより、HEPの計算だけでなく、HRAの分析結果から得られるリスク評価情報に基づく、体系的な設計プロセスの開発に応用することができた。

ところが、第三世代 HRA においても、定性分析である、タスク分析の領域においては、分析手順が確立されているものの、人的過誤事象 (HFEvs) で起こりえる、シナリオ開発や運転員のエラーモード (CFM) の特定については、分析者の知識や経験に基づく想像力に依存するところがある。

分析者の知識や経験に基づく想像力は分析には必要である一方、エラーモードを網羅的かつ体系的に抽出するプロセスのサポートがあれば、その評価結果については偏りがなく安定的なものにすることができる。

本章では、STAMP/STPA に基づいて、人間とシステム間の相互作用を俯瞰してそのエラーモードを探求することで、起こりえるシナリオや CFM をトップダウン的に抽出し、エラーモードを網羅的かつ体系的に抽出するプロセスの方策について述べる。なお、当該プロセスの実効性について検証を行うため、3.3.3 節で検討した事例に基づいて検討を行う。

4.2 STAMP/STPA 分析との統合化プロセスの検討

2.3章で述べた通り、STAMP/STPAは、注目すべき制御対象と非制御対象の相互作用に着目して、起こりえるエラーモードを網羅的かつ体系的に特定する手法である[17]。

STAMP/STPAの原子力プラントへの適用について、原子力プラントの主要系統に絞って試行的に実施される先行事例[38]やデジタルI&Cシステムへの適用検討やプラン[39]があるが、多くの系統、機器、プロセスが複雑に作用し、また、制御対象、非制御対象の組み合わせも非常に多いことから、本格的な導入に至っていない。

ここでは、人間とシステムの相互作用、すなわち、ヒューマンエラーモード (CFM) の特定に焦点を絞り込むこと、また、PRAの中で実施する炉心損傷に至るFTAで抽出される、リスク上重要な人的過誤事象 (HFEvs) に絞り込みを行い、かつ、HRAの定性分析で実施されるシナリオ開発やCFMの特定や網羅性の確認を検証するという、補完的目的に焦点を置くことで、より実用的な使用が可能にすることを目的とした。

3.3.3節で検討した通り、以下のクリティカルタスクが特定された。

- a. 原子炉トリップおよびタービントリップの確認(Check reactor trip & turbine trip)
- b. 安全注入状態の確認 (Check SI status)
- c. 緊急給水弁のラインナップ確認 (Check Emergency Feedwater (EFW) valve alignment)
- d. 蒸気発生器水位の制御 (Control SG level)
- e. 蒸気発生器破損の診断(Diagnose SG tube rupture)
- f. 破損蒸気発生器の隔離 (Isolate flow from ruptured SG)
- g. 1次冷却材温度および圧力のクールダウン (Cool down RCS temperature & pressure)

このうち、監視、確認、診断に関する認知タスク (a, b, c, e)は3.3.3章で詳細に分析しており、また、このエラー防止に対する対策も実施済である。また、STAMP/STPAでは、制御側非制御側のインタラクションの観点で分析するため、これらの認知タスクに対しては有効ではない。また、1回で完結する操作(f)については制御側(人間)から制御対象への単発1方向への信号の有無やタイミングは時間シーケンス分析でWLの影響も踏まえて評価済であり、STAMP/STPA適用による新たな効果は期待できない。

一方、事象対応中のプロセスの制御(d, g)については、多くのインタラクションが発生し、起こり得る非安全信号について分析する価値がある。

したがって、dおよびgのタスクについて以下分析をする。

STAMP/STPAでの分析プロセスを図4.1に示す。

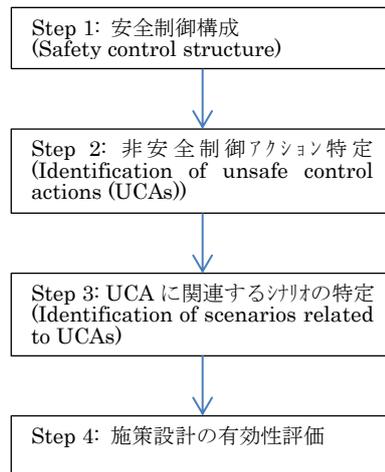


図 4.1 STAMP/STPA 評価プロセス

Step 1 安全制御構成 (Safety control structure) の構築

d.および g.の制御タスクを纏めた安全制御構成 (Safety control structure, SCS)を図 4.2 に示す。RCS 温度制御および RCS 圧力制御はプロセス制御として相関関係があるため、同一の SCS として纏めた。なお、d.および g.の制御タスクは破損 SG の2次系側圧力まで RCS 温度圧力をサブクール度を維持しながら、クールダウンする操作であり、自動制御系は介在しないため、自動制御系が搭載される制御装置 (Distributed Control System, DCS) は単に信号をスルーだけのものとして簡略化した。

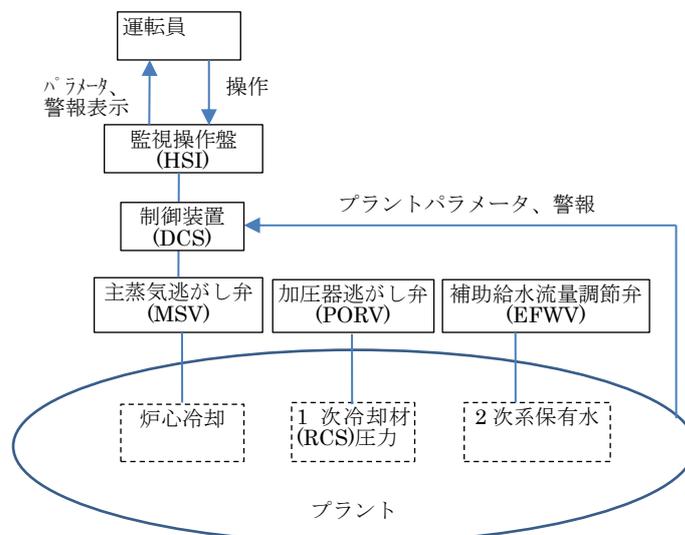


図 4.2 安全制御構成の構築

Step 2: 非安全制御アクション(unsafe control actions , UCAs)特定

4つのガイドワード (Not providing causes hazard, Providing causes hazard, Too early/too late or wrong order, Stopped too soon/applied too long) に従い、各制御アクションに対して非安全制御アクション (制御アクションがハザードを引き起こす状況) を特定する。

表 4.1 に評価結果を示す。

表 4.1 非安全制御モード

制御アクション	アクションモード	制御アクションが無いことによるハザード発生	制御アクション提供によるハザード発生	制御アクションが早すぎる、遅すぎる、順番が違う	制御アクションが早期に停止、長期に適用
MSV	開	RCS 温度が増加しているときに開せず、炉心冷却がされない。	RCS 温度低下による RCS サブクール (炉心飽和状態) となる。	開操作が遅れた結果、炉心冷却が遅れる。	閉状態が短すぎる結果、炉心が冷却されない。開状態が長すぎる結果、RCS サブクール (炉心飽和状態) となる。
	閉	開状態のまま放置 (閉止しない)、RCS 温度低下による RCS サブクール (炉心飽和状態) となる。	RCS 温度が増加し、炉心が冷却できない。	開⇒閉のタイミングが早すぎ、RCS 温度が減少せず、炉心冷却が遅れる。開⇒閉のタイミングが遅れ、RCS サブクール (炉心飽和状態) となる。	閉状態が短すぎる結果、RCS サブクール (炉心飽和状態) となる。閉の状態が長期渡り、開操作が行われない結果、炉心冷却がされない。
PROV	開	RCS 圧力が上昇している場合を開せず、破損 SG への RCS 流体を拡散。	RCS 減圧が継続し、RCS サブクール (炉心飽和状態) となる。	RCS 減圧が遅れ、破損 SG への RCS 流体を拡散	RCS 減圧が十分でなく、破損 SG への RCS 流体を拡散。RCS 減圧が継続し、RCS サブクール (炉心飽和状態) となる。
	閉	開状態のまま放置 (閉止しない) し、RCS 減圧が継続し、RCS サブクール (炉心飽和状態) となる。	開ができず、RCS 圧力が上昇し、破損 SG への RCS 流体を拡散。	開⇒閉のタイミングが早すぎ、RCS 減圧せず、破損 SG への RCS 流体を拡散。開⇒閉のタイミングが遅れ、RCS サブクール (炉心飽和状態) となる。	閉状態が短すぎる結果、RCS 減圧が過剰となる。閉の状態が長期渡り、開操作が行われない結果、破損 SG への RCS 流体を拡散。
EFWV	開	SG への保有水供給がされず SG 除熱ができない。	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。
	閉	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。	無負荷水位を維持できず、健全 SG への保有水バランスが失われる。

Step 3: UCA に関連するシナリオの特定 (Identification of scenarios related to UCAs)

非安全制御アクションに関連するシナリオを特定する。制御側が人間の場合、図 4.3 に示すモデルが提案されている[40]。

当該ヒューマンコントローラモデル(Human Controller Model, HCM)[40]は、STAMP/STPA の手法を踏襲しつつ、制御側が人間に適用可能なように開発されたモデルであり、当該文献では航空機コックピット向けのヒューマンエラーモードの特定に使用された。

HCM は、航空機コックピットの属性はなく、人間をコントローラとしたマンマシンシステム一般に応用可能なため、原子力プラントの人間工学プロセスへの展開を考慮して以下のように検討した。

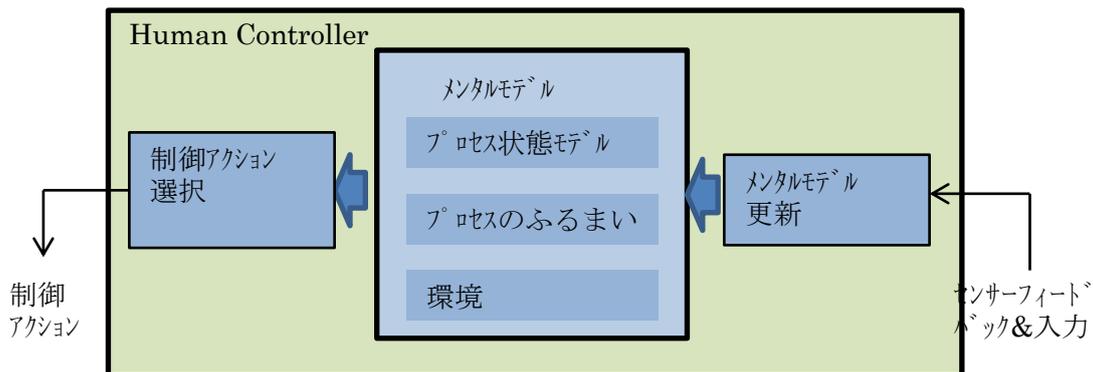


図 4.3 Human controller model ([40]より作成)

HCM の各要素の説明は、表 4.2 に整理される。なお、3.3.3 節で検討した CFM との関連付けを行うため、対応する Macro cognitive function を付記する。

Macro cognitive function のマッピングに対しては、Human controller model と必ずしも一対一の対応関係にはならず、他の整理の仕方也被考えられるが、メンタルモデルに対して表 4.2 のように対応付けを図った。すなわち、“プロセス状態モデル”を Detection/Understanding に、“プロセスの振舞い”を Understanding/Decision making を含め、“環境”は別の系からの影響を与える cognitive function として Detection/Understanding が対応し、また、“メンタルモデル更新”は、Detection/Understanding/Decision making 全てに影響を与えるものとして対応関係を考える。なお、Macro cognitive function における Team coordination は、本人以外の別の系からの影響を受けるものとして”環境”に対応付けた。

表 4.2 非安全制御モード

項目	定義/説明	対応する Macro cognitive function
制御アクション選択	なぜ特定の制御アクションが、ゴールや（優先順位として対処する）その他のタスクなどの要因を考慮して選ばれるかを説明する。	アクション実行
メンタルモデル	外界に関する様々な人間の考えを捉える。以下3つのモデルで構成する。	-
プロセス状態モデル	ソフトウェアモードの運転員の認知や運転の状況認識を反映する。間違っメンタルモデルは自動運転モードの変化からくるかもしれないし、制御されたプロセスの進行が、運転員へのフィードバック無しに進行することからくるかもしれない。	検出/理解
プロセスの振舞い	どのようにシステムが特定の運転モードやステージで振舞うかに対する運転員の期待値を表現する。これは、運転員の行動とシステムのふるまいの間の因果関係を含む	理解/意思決定
環境	運転員の制御外の因子、その他の制御器のふるまいや、環境の変化などを含む。	検出/理解/

項目	定義/説明	対応する Macro cognitive function
		チームワーク
メンタルモデル更新	このモデルは、分析者がメンタルモデルの源（メンタルモデルがどのように形成され、変化に対応してどのように変化するかを含む）を考慮することを必要とする。顕著な変化や運転員の期待などの因子は、どれくらいその変化が敏感に反応するかに影響を与える。この因子は、時間プレッシャーや不注意などの因子が、どのようにして不完全さや不正確さのメンタルモデルを形成するかについても考える。	検出/ 理解/ 意思決定（アップデート）

STPA では、UCA を基に一連の非安全シナリオを考察していくが、HCM を用いて非安全シナリオを考察することにより、より包括的に非安全シナリオを特定することができる[40]。図 4.4 に考察した非安全シナリオを示す。

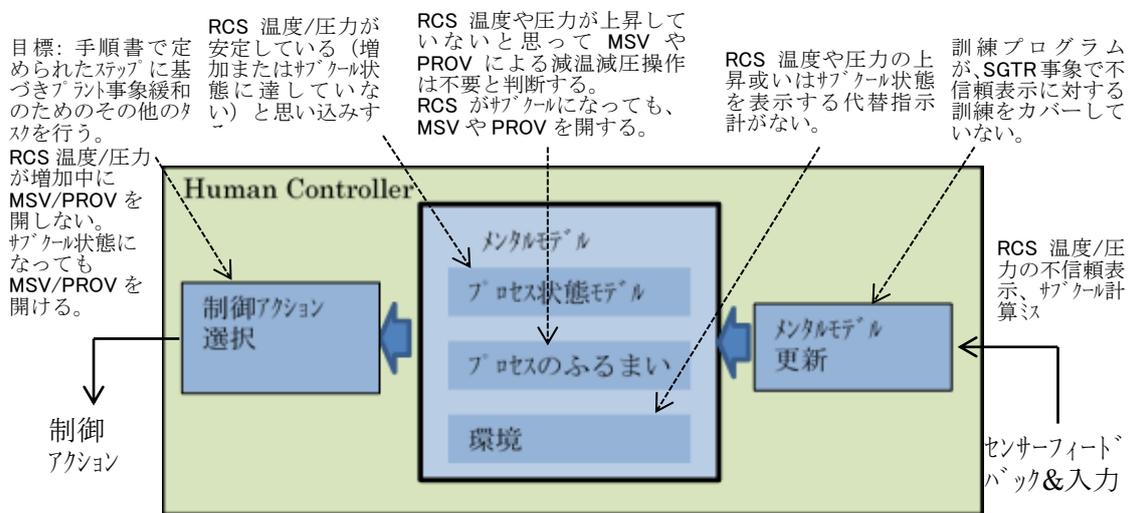


図 4.4 原子力プラント運転員の HCM

Step 4 施策設計の有効性評価

ここでは、Step 3 で抽出した非安全シナリオからこれを防止する設計方策を検討し、これを後続の人間工学プロセスで（例えば、非安全シナリオを適用してシミュレータを用いた運転検証を行い）、その有効性を確認する。図 3.11 でのプロセスに追加的に図示すると図 4.5 のようになる。Step 4 は分析結果を用いたエラーマネージメントの領域（非安全シナリオを防止するための設計方策(Task support requirement)を検討して有効性を確認する）に該当し、これは他の HFE プロセスの中で統合的に取り扱う。

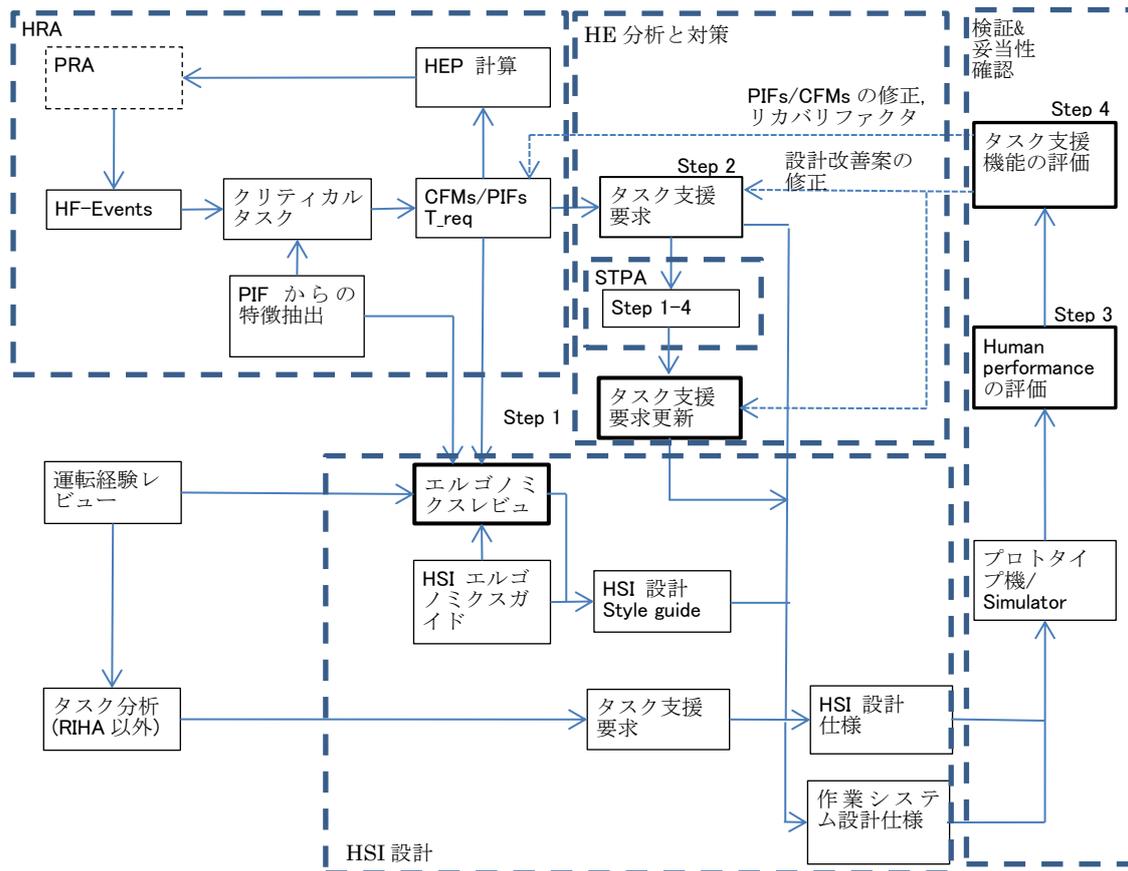


図 4.5 HRA と人間工学プロセスとの統合化プロセス
(HSI 設計検証における詳細プロセス) (STAMP/STPA)

4.3 結果と検討

HCM で有効なものは、非安全シナリオを制御側／非制御対象間のインタラクションプロセスを考慮して可能性のある事象として体系的に捉えられることである。

HRA では、手順書をベースとして各種の PIF の適用を考察していくが、例えば、指示計が正しく指示されなかった場合の波及的影響（例えば、操作をしないという結果）や因果関係（なぜ操作をしなかった）を捉えて現実的に起こりえるものとして評価が可能である。HRA ではこのような影響を演繹的に評価して初めて具体的な PIF を当てはまれるが、当該想像力が乏しいと適切な（起こりえる）PIF の当てはめが難しくなる（抜け漏れや見落としが発生する。）特に類似プロセスがないような新設計を評価する場合には有効となる。

この例では、HRA において、“Information Availability and Reliability”という Base PIF に対して“Inf0”すなわち“No impact”という前提で評価していたが、仮にプロセスを監視するキーとなる指示計（ここでは RCS 圧力、RCS 温度、或いは Subcool の計算）が可用性でない場合において、ほぼ起こりえる波及的な影響を想像することが可能となる。（そもそも、RCS 圧力、RCS 温度、或いは Subcool の信頼性が確率的に低いかな否かの議論は別として）決定論的な設計思想では信頼性を高く（例えば 2 重化などをして）対応を図るが、リスクの観点から、インタラクションプロセスに対する万一の障害に対するキーパラメータの抽出とその故障に対する影響に対して代替的な対策を見つけ出すためには有効な分析と言える。

この例では、RCS 圧力や温度については安全系として多重化等信頼性の向上を実施しているが、（設計想定では考えない）万一の多重故障において運転員がどのように RCS 温度、圧力の上昇について気づかせるかについて考えさせるトリガーとなる。この対策としては、シナリオで抽出した非安全人的モデルを修正するような強化（例えば、このような状態を起こした場合の訓練強化や代替監視パラメータでの安全機能低下の指示など）を対策として取ることが考えられる。

なお、これらのリスク面における非安全シナリオに対する、決定論的な設計プロセスによる設計方策の有効性の確認をすることも可能である。例えば、HFE プロセスにおいては、FRA/FA において安全機能を定義し、これをサポートする系統、機器を特定していることから、これらの機器の状態や系統のラインナップ、プロセスの状態を集めて、安全機能毎にグルーピング化し、安全器機能毎に健全性を表示する監視モニタがある。RCS 圧力、温度計器の同時喪失まではカバーできないが、一部のパラメータ不良により、安全機能の健全性表示が異常となることから、これらの代替監視モニタにより、安全性機能の異常（ここでは RCS Integrity や Secondary Heatsink への影響）が運転員に確認され（運転員は当該安全機能健全性モニタは事故時には特に注意を向けるよう訓練される）、その原因を詳細に探ることで異常を特定することができ、当該監視モニタの有効性が確認可能である。

第5章

決定論的手法に基づくトップダウン的マンマシン設計プロセスの導入と効果の確認

5.1 はじめに

本章では、人間工学プロセスにおける、決定論的手法に基づくトップダウン的マンマシン設計プロセスの導入と効果の確認について述べる。

具体的には、機能モデル(Function model, FM)[41]を用いた、プラント安全機能を維持、達成するために不可欠なプラント系統機器群系統 (Success Path, SP) モデルを HSI 設計入力情報として直接 HSI 設計に適用し、制御室運転員の安全機能の状況認知 (Situation Awareness, SA) を向上させる。これにより、タスク分析やリスク情報から得られるヒューマンエラー対策 (ボトムアップ的対策) では得にくい、コミッションエラー (Error of Commission, EOC) に対する対策を図ることができる。

5.2 機能モデルと人間工学プロセスの関係

機能モデル(FM)[41]は、システムに内在する機能を構造的に表現する手法として、工学分野では広く適用されている。原子力プラントや航空機制御のような複雑、かつ、多様な系統からなるシステムを機能面から体系的に整理することで、システムに内在する相互作用を俯瞰することができ、システム全体としての安全性を分析することができる。

機能モデルを、複雑なシステムの相互作業の分析に応用するため、FRAM (functional resonance analysis method)[42]など改良されたモデルが開発され、航空機分野などで適用されている[43]。

機能モデルは、システムに内在する機能（インプット、アウトプット、プロセス、相互作業を含む）をフロー線図などで表現し、各機能の働きや関係性を明らかにする。典型的な機能モデルには2つのタイプとして、機能フロー線図（Function Flow Diagram, FFD）および機能分解（Function Decomposition, FD）がある[41]。

図 5.1 は、FFD の例を示す。各機能はボックスで表され、各機能へのインプット(Input)、各機能から出力されるアウトプット(Output)、制御信号 (Controls)、メカニズム（機能を達成するための補助ツールや手法）が矢印として表される。

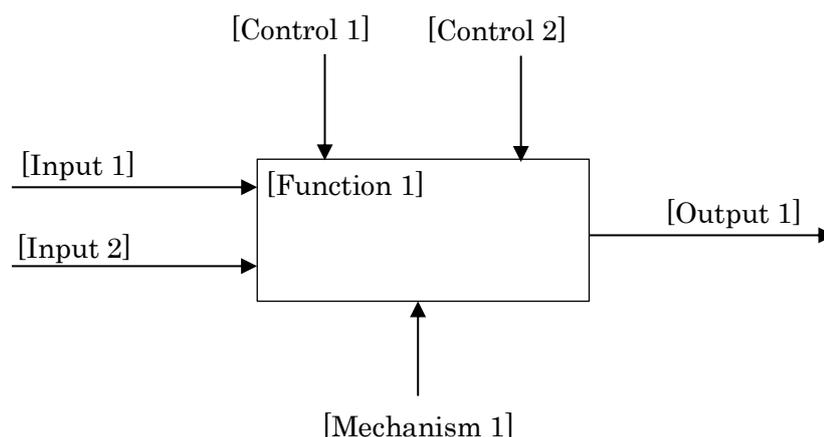


図 5.1 FFD の例 ([41] から作成)

図 5.2 は、FD の例を示す。FD は、システム全体の機能や、システムに内在する各機能を構成するサブ機能の関係を明らかにするために分析対象とするシステムや上位機能を頂点とした機能階層図（樹形図）でモデルを表現する。

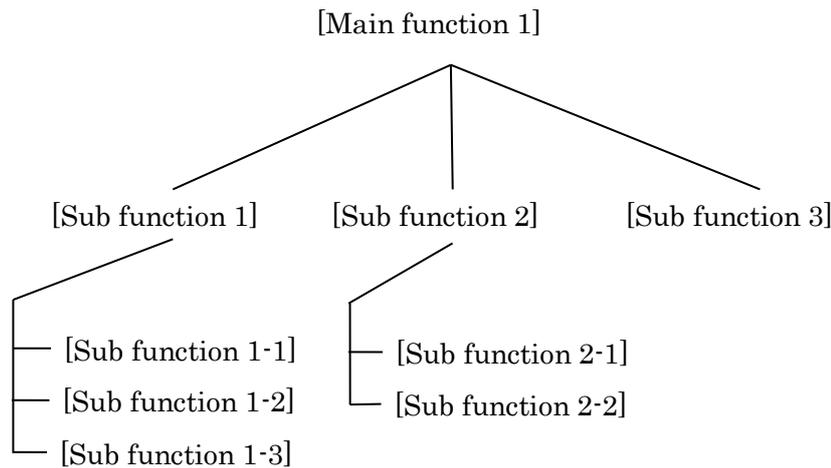


図 5.2 FD の例 ([41] から作成)

人間工学プロセスでは、機能モデルに関連する分析アプローチとして、プラント機能分析および配分 (Function Requirement Analysis/Function Allocation, FRA/FA) およびタスク分析 (Task Analysis, TA) が実施されている。

以下、その関係性を明らかにするため、FRA/FA および TA で現状実施される、プロセスを述べる[1][44]。

i. FRA/FA

FRA は、プラントの安全目標を頂点として、その安全目標を維持、達成するための上位安全機能(High level function)、上位安全機能を維持、達成するための、サブ機能、さらに、当該上位安全機能およびサブ機能を構成する系統機器を、樹形図を用いて明らかにする。ここで、各上位安全機能-サブ機能-系統-機器が機能階層構造を司る成功経路 (success path, SP) がプラント安全機能の維持、達成のための重要な情報となる。

FA では、各 SP 毎に自動、手動、またはその組み合わせの配分を運転員 (人間) の特性 (作業負荷/負担、パフォーマンス) を考慮して配分する。

FRA で実施される分析は、FD を用いた例として組み込まれている。

ii. TA

TA については、3 章で詳述したので、ここでは、FRA/FA との関係について明らかにする。

すなわち、TA は FRA/FA の後続プロセスとして位置づけられ、FA で手動に配分された機能に対して、さらに、階層化分析 (Hierarchical Task Analysis) で当該 SP に内在するタスクを明らかにし、また、タスクシーケンス分析 (Operation sequence analysis, OSA) やタイムライン分析 (Time line analysis, TLA) でタスク間の関係や SP の機能達成するためのメカニズムを明らかにする。

OSA や TLA は手動にアサインされた SP の機能の関係を明らかにするために採用されて

いる。

TAの結果は、タスクサポート要求として HSI 設計のインプットとしている。

表 5.1 に、人間工学プロセスにおける機能モデル適用関係を整理した。

表 5.1 人間工学プロセスにおける機能モデル適用関係

機能モデルタイプ	目的/成果物	人間工学プロセスでの適用	
		Analysis	Design
機能フロー線図 (FFD)	各機能へのインプット(Input)、各機能から出力されるアウトプット(Output)、制御信号(Controls)、メカニズム(機能を達成するための補助ツールや手法)を明らかにする	タスク分析 (TA)	HSI 設計/運転手順書開発へのインプット
機能分解(FD)	目的を達成するための機能構成/成功経路 (success path)を明らかにする。	プラント機能分析 (FRA)	N/A

現状の人間工学プロセスでは、手動に割り当てられた SP に対してタスク分析を行い、その結果を HSI 設計のインプットとしている一方、各 SP 毎、また、タスク毎に詳細化されるため、運転員があるシナリオの中でコミッションエラー(EOC)をした場合、これをリカバリーする方法は現状の設計プロセスでは設計情報として提供する限界がある。

一方表 5.1 に示す通り、FD で分析した SP 情報を HSI 設計にトップダウン的に適用し、自動に配分された SP を含め、各 SP の状態を制御室運転員へ提供することで、事故時シナリオでの運転員のプラント安全維持達成において、コミッションエラー (EOC) を是正するために有効となる。

例えば、ある事故時シナリオの収束は、現状の設計プロセスでは、タスク分析に基づく想定にて手順書が整備され、また、監視操作機能に必要な画面も当該タスクを遂行するために用意された個別系統画面を用いることとしており、運転員にバイアスが生じ、タスク分析では想定していなかった事象や当該事故シナリオで想定する SP が故障などで機能しない場合、対応する手順書が用意されておらず、リカバリアクションとして事故時のストレス状況下において正しい判断がされず、EOC に至る可能性がある。特に、重大事故などの設計想定外シナリオでは、タスク分析によりボトムアップ的なアプローチに限界が生じる。

そこで、各安全機能の状態や SP の状態を運転員に提供することで、現在遂行している対応操作が間違っていることやその対応手段(SP)が適用できない(安全機能の状態が悪くなることが SP の情報で得られる)ことに認知でき、迅速にリカバリ手段の特定(別の SP の特定)が可能となる。

そこで、FRA で得られる SP の情報を HSI 設計に直接適用することを検討した。

5.3 Success Path の開発

図 5.3 は、PWR 型原子力プラントの FRA の結果の例を示す。FRA では、2.2 節で述べた通り、プラントの安全目標を頂点として、その安全目標を維持、達成するための上位安全機能(High level function)、上位安全機能を維持、達成するための、サブ機能、さらに、当該上位安全機能およびサブ機能を構成する、系統機器を樹形図を用いて明らかにする。また、ここでは、さらに、各系統機器を制御する HSI（ここには、安全系 HSI(Safety HSI)や非安全系 HSI (Non-Safety HSI)または、安全系/非安全系 HSI が同時に喪失した場合の深層防護として設置する代替 HSI (Diverse Action system HSI)) まで特定する。

図 5.3 で太字で図示したのは、SP の例である。この例では、Safety Goal-Reactor Coolant System (RCS) inventory control-RCS pressure control-Pressurizer Relief Operation Valves (PROVs)-Non-safety HSI が SP の一つとなる。

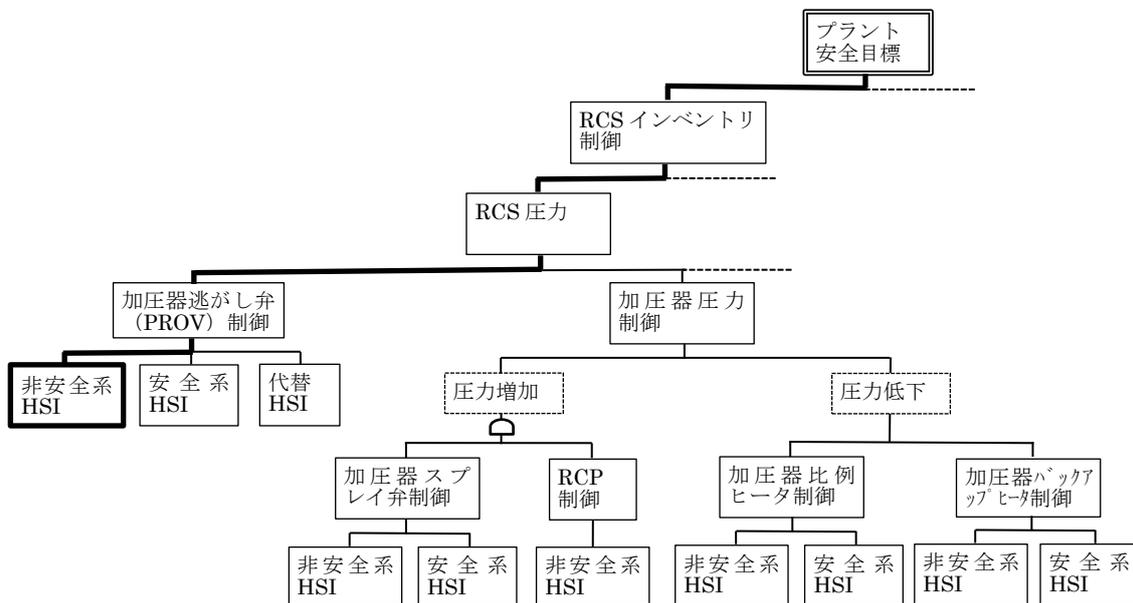


図 5.3 プラント機能分析(FRA)の結果と SP の例

5.4 Success Path の HSI 設計への適用

現状の人間工学プロセスでは、タスク分析の結果を用いて、手動に配分された SP を制御するために必要監視操作情報などのタスクサポート要件を特定し、これを HSI 設計の入力情報として、HSI ハードウェア設計、手順書の設計を行っている。

図 5.3 に示す通り、上記現状の設計プロセスに加え、2.3 節で FRA の分析結果の一部である、SP を直接的に HSI 設計へ適用する。安全機能を維持、達成する SP の情報をリアルタイムで制御室運転員に提供することにより、タスク分析で個別の想定する事故収束シナリオには依存しない、HSI 設計考慮が可能となり、重大事故などの設計想定外の事象や予期しない SP 劣化時の代替手段の特定を迅速、かつ、効率的に行うことが可能となる。

このような迅速、かつ、リアルタイムの SP 情報の提供は、運転員の適時対応手順書による対応の成否を予測することが可能となり、認知バイアスや EOC による誤った監視操作の是正を図ることが可能となる。

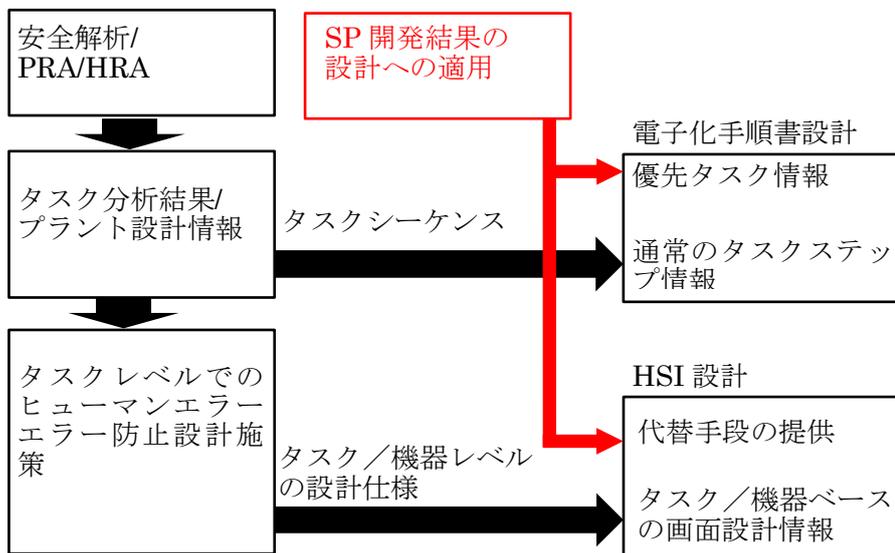


図 5.3 SP を HSI 設計情報として追加した設計プロセス

図 5.4 は、SP を設計情報として活用した、運転手順書の例を示す。実線は、現状の設計プロセスによるもの、点線は、SP を HSI 設計情報として追加的に適用したプロセスをそれぞれ示す。現状の手順書開発は、タスク分析結果とそのベースとなる想定した SP (Normal SP) に基づく情報による。手順書での代替ステップは、機器故障などにより通常そのステップが遂行できない場合を想定し、タスクイベントレベルで考慮されるが、システム全体の

SPの可用性を考慮した観点で代替ステップが考慮されていない。

ここに、使用できる（可用な）SPを、プラント計算機でプラントの機器の状態とチェックし、リアルタイムで提供し、通常のSPが使用不能になった場合の代替SPによる達成手段を提供することで、運転員に迅速かつ効率的にプラント安全機能の維持やリカバリ操作の判断をすることができる。運転手順書は、デジタル化された制御盤では電子化手順書とすることができ、図5.4で太字で示す情報は代替可能なSPで対応する各種手順への手順書番号を示す。

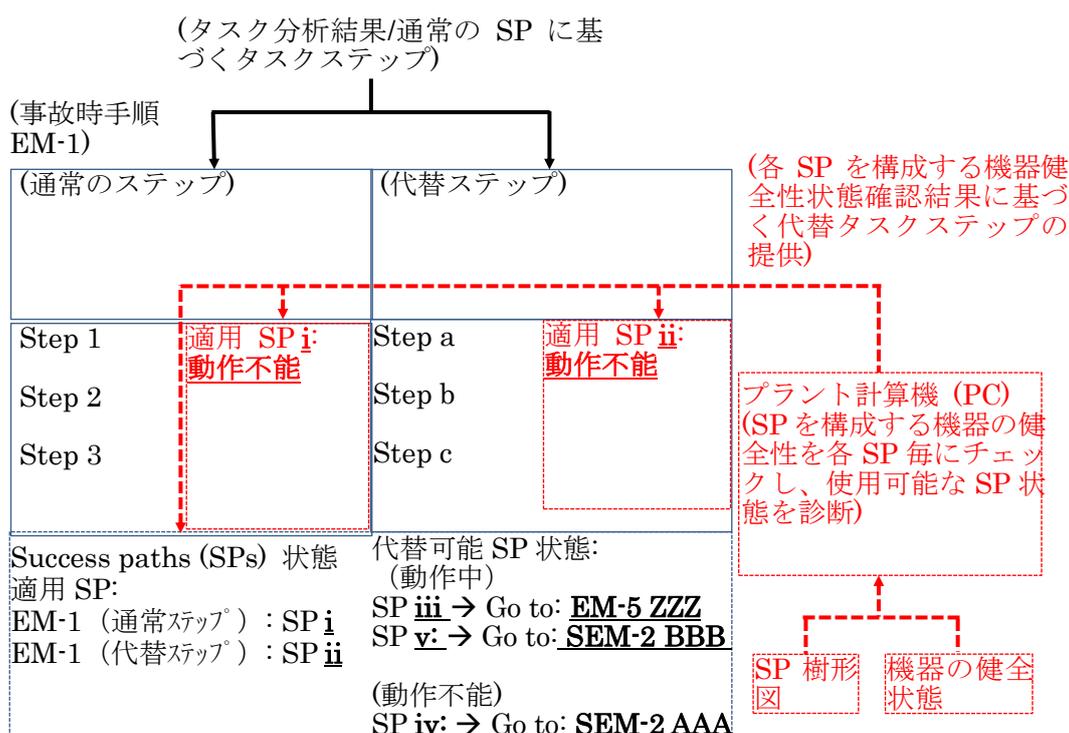


図 5.4 SP 情報を考慮した HSI 設計（運転手順書）の例

図 5.5 は、SP 情報を制御室の監視操作画面に適用した例である。点線は、SP を HSI 設計情報として追加的に適用したプロセスをそれぞれ示す。手順書と同じように、使用できる（可用な）SP を、プラント計算機でプラントの機器の状態とチェックし、リアルタイムで提供し、通常の SP が使用不能になった場合の代替 SP による達成手段を提供し、運転手順書とともに状況認知とその対応（代替 SP による手順の遂行）を迅速にすることができる。

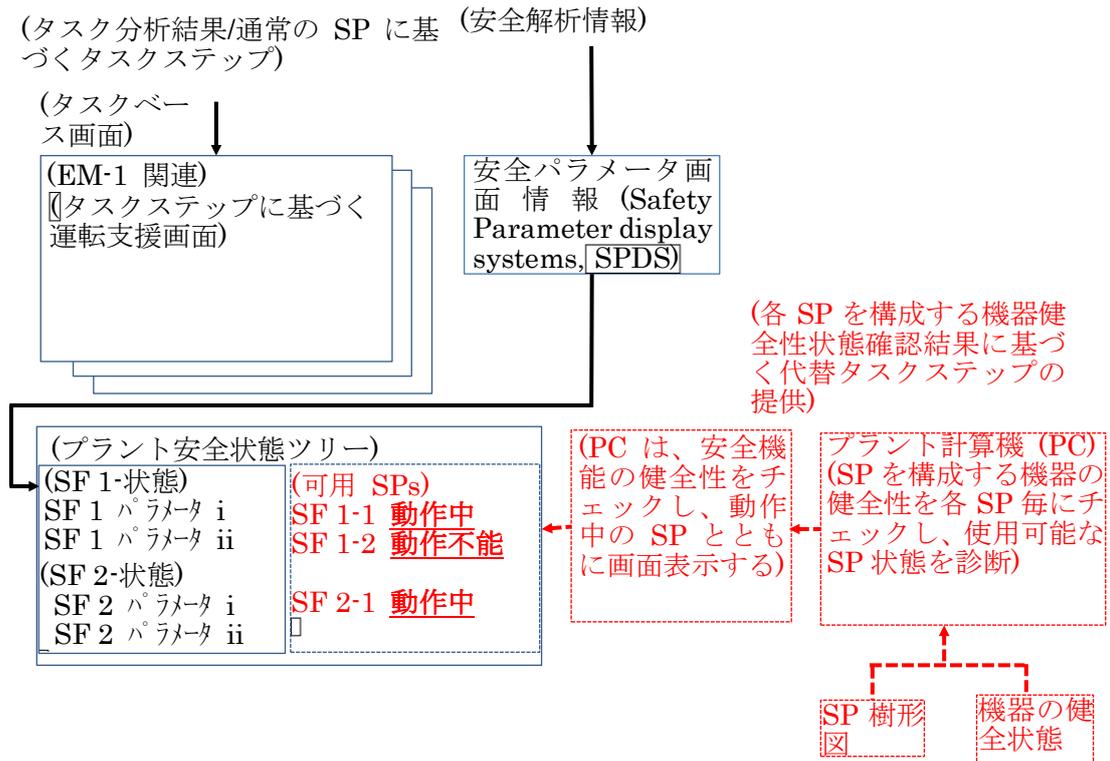


図 5.5 SP 情報を考慮した HSI 設計 (画面設計) の例

設計改善効果について検証した結果を図 5.6 および図 5.7 にそれぞれ示す[52]。検証は、米国発電所運転員を被験者として、制御室シミュレータを用いて、延べ8クルーの運転員にて、7つの異常事故シナリオを実施した。

図 5.6 および図 5.7 の評価項目は、状況認知 (Situation Awareness, SA) ワークロード (Work load, WL)、エラーの特定と対応(Error Tolerance, ET)、チームワークなどの運転員パフォーマンスに関わる事項とその影響因子に対して、運転員アンケートによる 5 point-Likert scale スケールで設計改善前後の効果について評価した。1A Test は設計改善前、1B Test は設計改善後のスコアをそれぞれ示す。

検証の分析は、米国人間工学専門家により独立した観点で実施し結果を纏めた。

設計改善は、SP 情報(中央制御室監視画面である大型表示装置 (Large Display Panel, LDP) に安全機能 (Critical Safety Function, CSF) として表示)の追加の他、LDP へのパラメータトレンド情報の表示、運転管理者/当直長エリアへの画面表示装置(Visual Display Unit, VDU)追加など、いくつかの改善点を含むが、SP 情報の表示は、他の設計改善点では得られない、SA や ET の向上に大きな寄与をしていると考えられる。

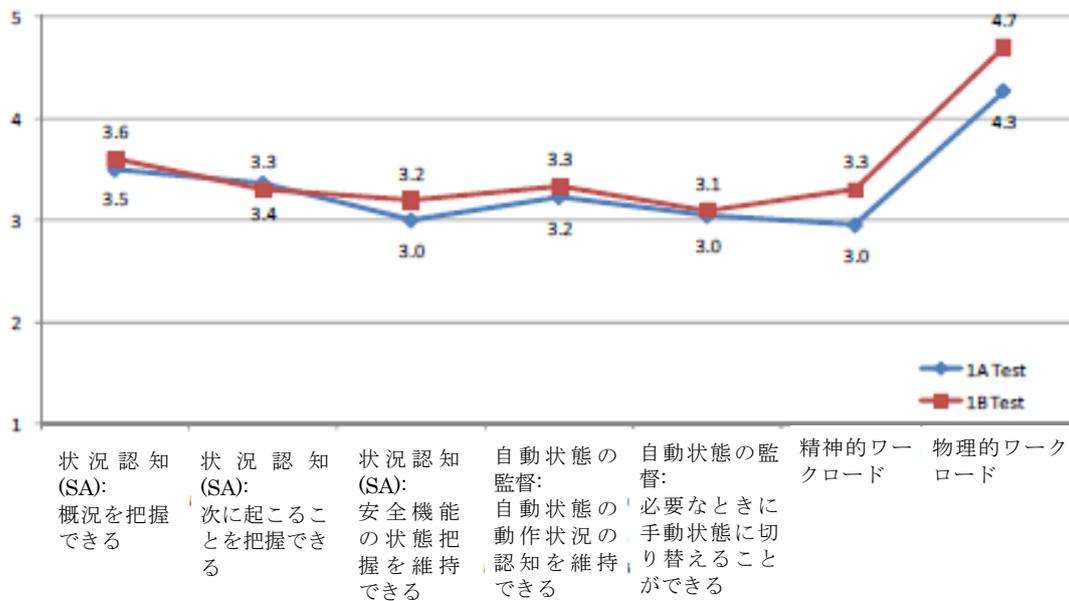


図 5.5(a) 米国運転員によるアンケート集計結果に基づく評価結果[52]

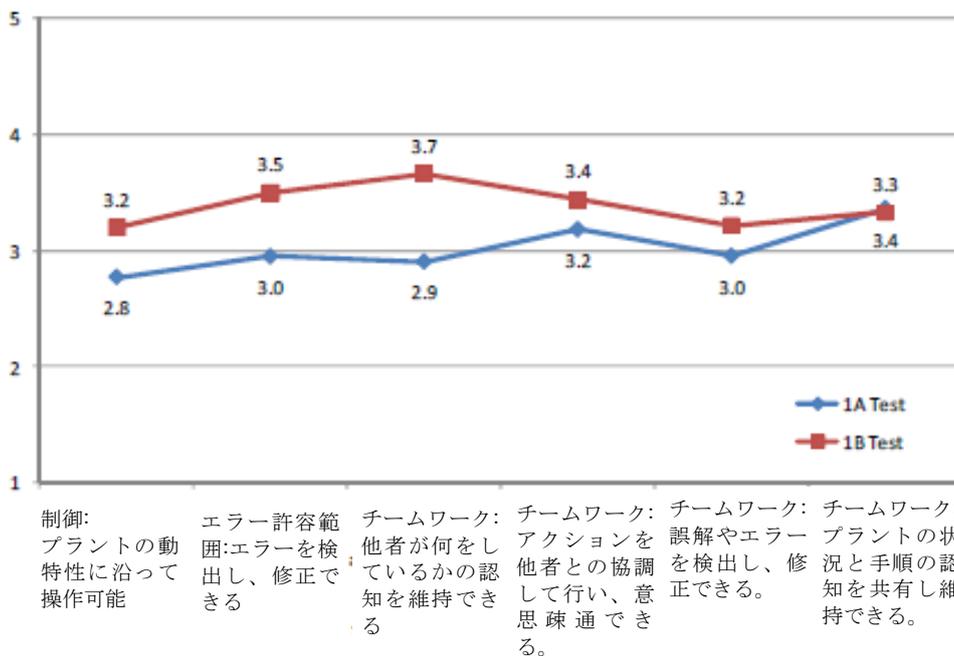


図 5.5(b) 米国運転員によるアンケート集計結果に基づく評価結果[52]

5.5 結果と検討

人間工学プロセスにおける、決定論的手法に基づくトップダウン的マンマシン設計プロセスの導入と効果の確認について検討した。

現在の人間工学プロセスにおいては、FRA/FA から TA を経由してタスクレベルでの分析を通して、HSI 設計入力情報を特定するが、このようなボトムアップ的アプローチにおいては、重大事故シナリオなどの設計想定外事象において、タスク分析で想定しえないエラーモードに対する対処を行う場合には限界があり、FRA におけるプラントの安全機能分析の結果得られる、SP の情報をオンラインで制御室運転員へ提供することで、状況認知 (SA) やエラーの特定と対応 (ET) において改善効果があることを確認した。

第6章

運転シミュレータを用いたヒューマンパフォーマンス自動測定手法の開発

6.1 はじめに

HRAにおける人的過誤率（Human Error Probabilities, HEP）を、分析者による分析結果のばらつきを無くし、かつ、信頼性を高めるべく、IDHEAS[23]に代表される第三世代HRA手法では、Macro-cognitive手法を用いて、リスク分析（PRA）における人的過誤事象（Human Failure Events, HFEvs）に対して適用している。

すなわち、運転員の知識プロセスを（検出-理解-意思決定-アクション）として形式化（細分化）し、これを個別のタスクに当てはめて、個別タスクや作業環境、作業場／インタフェースに対する影響因子を設定し、それぞれの影響因子を考慮したヒューマンエラー率を積み上げて、HFEvsに対するHEPを算定する。

一方、机上評価において、HEP算定のベースとなる、運転員のエラーモード（Crew Failure Mode, CFM）やその影響因子（Performance Influence Factor, PIF）を網羅的に予測することには限界があり、実機を模擬した運転訓練シミュレータによる運転訓練の結果のパフォーマンス評価を基にCFM/PIFの特定と机上分析への見直しを図るプロセスが検討されている[46]。

本研究は、運転訓練におけるパフォーマンス評価を認知レベルでヒューマンエラー率を測定、自動評価が可能とするよう、評価者が行う評価を基に、運転員の行動をパターン化して自動評価ロジックを構築し、オンラインで評価が可能なプロトタイプ機を製作し、その有効性について確認した。

6.2 開発目標と開発プロセス

HRAにおける人的過誤率（Human Error Probabilities, HEP）を、分析者による分析結果のばらつきを無くし、かつ、信頼性を高めるべく、IDHEAS[23]に代表される第三世代HRA手法では、Macro-cognitive手法を用いて、リスク分析（PRA）における人的過誤事象（Human Failure Events, HFEvs）に対して適用している。

Macro-cognitive手法では、人間の認知プロセスを標準化（Macro化）し、その認知プロセスのそれぞれの要素について、人的過誤事象（Human Failure Events, HFEvs）のシナリオで考慮すべきクリティカルタスクに対して、運転員のエラーモード（Crew Failure Mode, CFM）やその影響因子（Performance Influence Factor, PIF）を特定し、その掛け合わせとして、人的過誤率（Human Error Probabilities, HEP）を算出する[21][22][23]。

図 6.1 は、Macro-cognitive手法を用いたCFM/PIF特定の全体プロセスを示す。また、人間の認知プロセスを標準化（Macro化）した例は、図 2.9 で示した認知タスクがその例である。

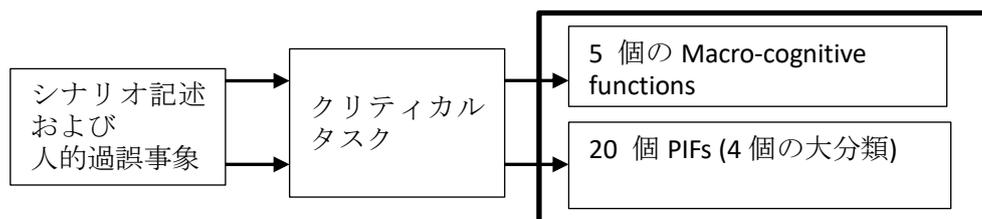


図 6.1 全体プロセス（[22]から作成）

現状のアプローチにおいては、PIF 毎に定義されたヒューマンエラー率(Human Error Rate)（当該エラー率は、30-40 年以上の前のアナログタイプのマンマシンインタフェースをベースに、HSI タイプに係わらず、様々な失敗率のデータを混在させたもの）を参照することとしている[22][23]。

これは、そもそもヒューマンエラー率を算定するためには膨大なデータが必要であり、個別の HSI タイプ毎に詳細化する場合その母集団が少ないことが要因として挙げられる。

Porthin[47]らは、アナログ計器やハードウェア操作器を主体とした在来型の制御盤と、監視操作をVDU（Visual Display Unit）で行うデジタル型制御盤では、PIFそれぞれのヒューマンエラー率に誤差があり、原子力プラントで導入が進むデジタル型制御室のヒューマ

ンエラー率の精度向上が必要であると指摘している。

一方、Hsien ら[48]は、運転訓練シミュレータを用いた運転訓練中の運転員のパフォーマンスデータを取得するシステムの開発を行っている。当該システムで収集したパフォーマンスデータを基に、実際の作業環境や個別の HSI タイプを考慮した、PIF の特定やヒューマンエラー率の算定が可能であり、また、訓練生毎にパフォーマンス評価を行うことができ、訓練生毎のパフォーマンス向上／改善に向けた個別フィードバックが可能となる。

当該システムを用いて、マクロログニティブモデルによる PIF やヒューマンエラー率のフィードバックを行うためには、図 2.9 に定める各認知プロセス毎のパフォーマンスデータの収集が必要となり、現在は、訓練生（運転員）の訓練中の観察や訓練終了後の訓練生インタビュー（Debriefing）により、これらパフォーマンスデータを収集することとしている。

ところが、実際にパフォーマンスデータを収集する場合には、特に、PRA で想定する人的過誤事象（HFEVs）における、クリティカルタスクを含む事故時シナリオにおいては、短時間で多くの運転員タスクが要求され、認知プロセスレベルでのパフォーマンスデータの収集は困難となる。

Ujita ら[49]は、運転員のパフォーマンス評価システムを開発しているが、これは、ベテラン運転員の知識ベースや運転操作ログを基に、訓練生の失敗や不足点を特定することとしているが、認知レベルでの PIF やエラー率を取得するものではなく、また、ベテラン運転員の操作ログをベースとしたものであり、ベテラン運転員自体の評価を絶対的な評価基準で評価するものではない。（例えば、ベテラン運転員のコミッションエラーやその原因となる HSI 設計の良否を判定することはできない。）

本章では、運転員のパフォーマンスデータを運転訓練シミュレータによる訓練中に自動的に取得し、かつ、オンラインで、自動的に評価するシステムの開発を行う。

当該システム開発プロセスについて、図 6.2 に示す。

6.3 節では、評価する対象である、HSI システム、炉型、シナリオの選定について述べる。

6.4 節では、マクロログニティブモデルをベースに本システムで用いる認知モデル（Cognitive model）を検討し（6.4.1 節）、認知モデルに基づきパフォーマンスデータの自動測定手法の選定をし（6.4.2 節）、自動評価モデルの開発を行った（6.4.3 節）。

6.5 節では、プロトタイプ機による評価を行い、その有効性について確認した。

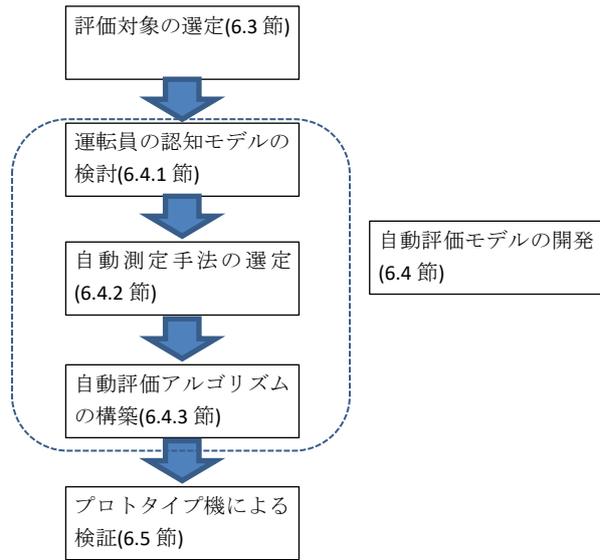


図 6.2 開発プロセス

6.3 評価対象の選定

6.3.1 HSI システム

最新型 PWR デジタル制御盤を対象として選定した[50]。

デジタル制御盤は、運転コンソール、当直長コンソール、大型表装置 (LDP) から構成される。制御室運転員(は運転コンソールに、運転管理者／当直長 (Supervisor) は当直長コンソールにそれぞれ配置し、運転員は、運転コンソールの背後に配置された当直長コンソールに座る運転管理者／当直長の指示のもとに、プラントの監視操作タスクを遂行する。大型表示装置には、プラント全体の状況を表示し、運転員および運転管理者／当直長がその状況を共有できるように、運転コンソール、当直長コンソールの前方に配置される。監視操作は運転コンソールに配置される、監視操作 VDU にてタッチオペレーション方式で行われ、その情報は、当直長コンソールでも確認ができる。

運転手順書は、紙ベースおよび電子化ベースいずれかで提供される。電子化手順書 (Computer-based procedure, CBP)が適用される場合は、電子化手順書は、運転コンソールの VDU として設置される。

6.2.2 評価対象者

PWR 型制御室運転員および運転管理者／当直長(制御室運転クルー)が評価対象である。ただし、運転パフォーマンスは、運転クルー自体のパフォーマンスだけでなく、HSI システムや運転手順書の仕様もパフォーマンスに大きく影響することから、評価対象は、HSI システムや運転手順書も対象となる。

6.2.3 適用施設およびシナリオ

PWR 型運転訓練シミュレータがプロトタイプ試験で使用される。

また、プロトタイプ試験のみならず、自動評価モデルの開発に当たっては、運転員のタスクを網羅的に評価可能なよう取り込むため、典型的な事故シナリオである、蒸気発生器細管破断 (Steam Generator Tube Rapture, SGTR) を選定した。SGTR は、PWR 型原子力プラントの想定事故収束シナリオの中でも、手動操作の判断やワークロードが高く、運転員パフォーマンスを確認するために訓練の中でも広く行われるシナリオである。

6.4 自動評価モデルの開発

6.4.1 運転員の認知モデルの検討

図 6.3 に示す運転員の認知プロセスを設定した。図 6.3 のモデルは、IDHEAS-ECA[23]での認知プロセスモデルをベースに以下の変更を加えたものである。

すなわち、一般的には、人間の認知プロセスは、知覚器による検出、検出した情報から状況を認知、認知した情報に基づく行動をとるための計画策定／意思決定、意思決定に基づくアクションから形成される。なお、原子力発電所運転員は単独の状況認知、意思決定を行うことはなく、中央制御室内で上級運転員や運転管理者／当直長によるチームとしての状況認知、意思決定を行うことから、認知プロセスのうち、特に、状況認知および意思決定において、他のチーム員の状況認知、意思決定により影響が及ぼされる。したがって、IDHEAS-ECA[23]での認知プロセスモデルのうち、状況認知、意思決定プロセスにおいて他のチーム員の状況認知、意思決定プロセスの影響を表すべく矢印で示すこととした。なお、このプロセスは状況認知や意思決定が相互の状況認知の共有化や意思決定の調整を経て統一化されることから、相互に影響を及ぼすものとして双方向矢印とした。

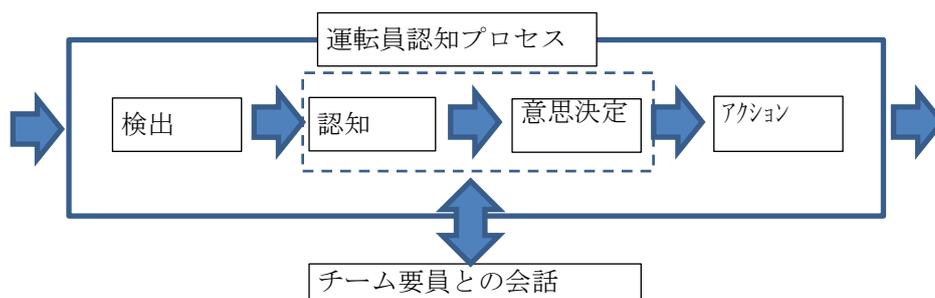


図 6.3 運転員認知プロセスモデル

6.4.2 自動測定手法の選定

6.4.1 で定めた運転員の認知プロセスに対して、評価データを自動で測定するための計測方法を図 6.4 で示すように定めた。

すなわち、検出については、人間の知覚器としては、視覚、聴覚、嗅覚、触覚があるが、プラントの中央制御室で主に使われるものは、中央制御室内火災など特定の事象を除き、視覚および聴覚が大きな比重を占めている。なお、聴覚器にインプットを与える中央制御室の機能としては、警報音などがあるが、事故時には多数の警報は発信され、聴覚器よりも、視覚による検出が大きな比重を占めている。また、今回評価対象とした制御盤は

デジタル式マンマシンシステムとすることから、どの画面のどの情報を見ていることを検出することがより重要になる。したがって、視覚器による検出に焦点を当てることとし、これを計測するものとして視点計測（eye-tracking system）を適用した。

次に、認知、意思決定プロセスについては、運転員が思考している内容であり直接的な計測は困難であるが、6.4.1節で述べた通り、制御室運転員は制御室の他の運転員との情報共有や意思決定を醸成していくことから、運転員間の発話内容を記録し、その内容を評価エビデンスや判定条件として用いることとした。

アクションについては、運転訓練シミュレータを用いて評価を行うことで、操作ログとして記録することができる。また、デジタル化中央制御盤の操作においては、全ての操作を画面操作により行うことから、実際のプラントのログとして記録される補機や弁の状態だけでなく、画面の切り替えや操作器の呼び出しなどの画面の操作ログも記録することで、運転員の全ての操作に対して評価が可能である。

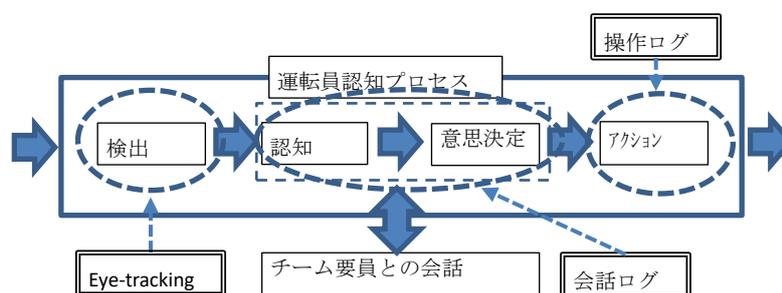


図 6.4 運転員認知プロセスにおける計測手法

6.4.3 自動評価アルゴリズムの構築

6.4.1節の運転員の認知モデル、6.4.2節の自動測定手法から得られる情報を基に、パフォーマンス自動評価するアルゴリズムを構築する。構築ステップを図 6.5 に示す。

まず、視点計測、会話ログ、操作ログのそれぞれの異なった情報を時系列データとして統一化し、次に、当該データに基づき、評価者がどのように評価を行うかについて評価プロセスを検討し、これをロジック化する。

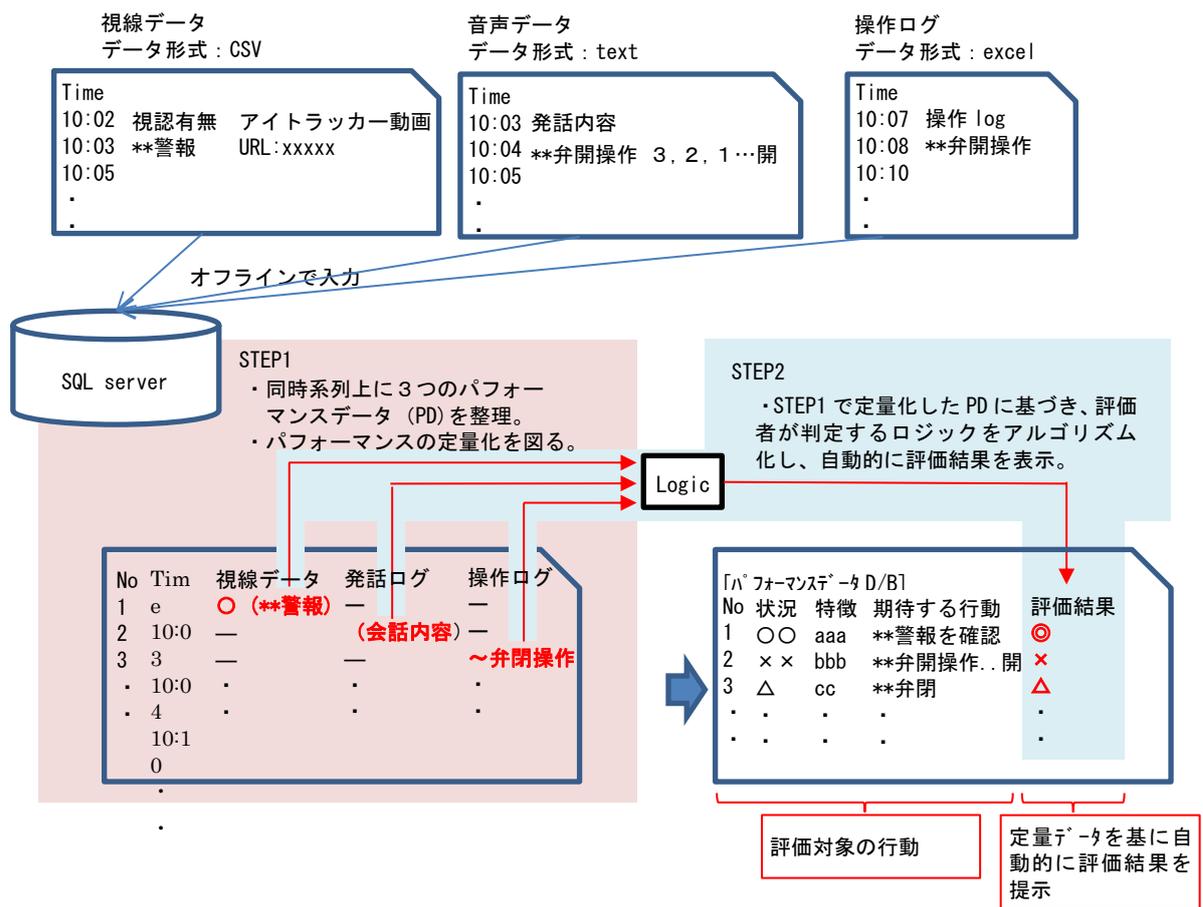


図 6.5 自動評価構築ステップ

以下に、自動評価構築ステップについて詳述する。

6.4.3.1 自動測定データ収集とデータベース化

時間軸をキーとして、視点計測、会話ログ、操作ログの収集データを1つのデータベースに統合する。これにより、時間軸をキーとして、いつ何を見て、どのように認知と意思決定を行い、何を操作したかの情報が収集可能である。なお、通話記録は、テキスト形式の電子情報として変換することで、特定のキーワードと照合が可能ないように変換する。

6.4.3.2 判定ロジックの構築

評価者が行う判定プロセスに基づき評価判定ロジックを構築する。

中央制御室の運転員のタスクは、以下の3つのタスクに集約される。さらに、プラント状態監視とプラント操作については、それぞれ2つのサブタスクがある。なお、運転員のタスクは、プラント運転に係るものを対象として、業務報告、引継ぎ、サーベランス等の間接業務は対象外とする。

- a. プラント事象判断
- b. プラント状態監視
 - b-1. プラントパラメータ・状態表示灯監視
 - b-2. 警報確認
- c. プラント操作
 - c-1. ポンプ、ON-OFF 弁などの ON-OFF 操作
 - c-2. 制御弁、調節弁などによるプロセス制御操作

それぞれのタスクに対して、評価者がどのように評価を行うかについて検討し、かつ、運転員認知モデルの各プロセスの判定を 6.4.3.1 節で収集したデータとの紐づけを行うことで、自動評価ロジックを構築した。以下、各タスクに対するロジックについて述べる。

a. プラント事象判別／判断

プラントの事象判別／判断は、他のタスク(b-1, b-2 および c)に比べ、状況認知や意思決定における個人の知識ベースの活用の領域が大きくなるものの、図 5 に挙げる認知プロセスモデルでロジックの構築ができる。

評価者は、シミュレータで模擬した事象について、運転員が、その事象の兆候を示すプラントパラメータや状態表示灯、警報等から、正しく事象を特定できたかについて、運転員チームの会話や対応操作の観察によって判定する。

上記評価者の評価プロセスに対して、適用される認知プロセスについては、「検出-認知-意思決定」となる。

検出については、その事象の兆候を示すプラントパラメータ、状態表示灯、警報について予め認知のための検出として必要な情報領域を画面毎にマッピング化し、そのマップ上に視線がある時間滞在した場合はそのパラメータ、状態表示灯、或いは警報を検出したものとみなすこととした。(図 6.6 参照) 図 6.6 は大型表示装置の画面上に表示されるパラメータ、補機状態のマップ化の例であるが、各パラメータ毎、補機毎の視線滞在の判別も可能な視点分解能があることから、パラメータ毎、補機毎に領域を設定した。また、運転コンソール上の各画面においても同様にパラメータ毎、補機毎に視覚検出領域を設定した。(図 6.7)

Card ら[8]によれば、知覚プロセスとして 100msec 程度なので、アイトラッキングによる視点位置がある特定の領域に 100msec 以上滞在する場合を検出として判断する。

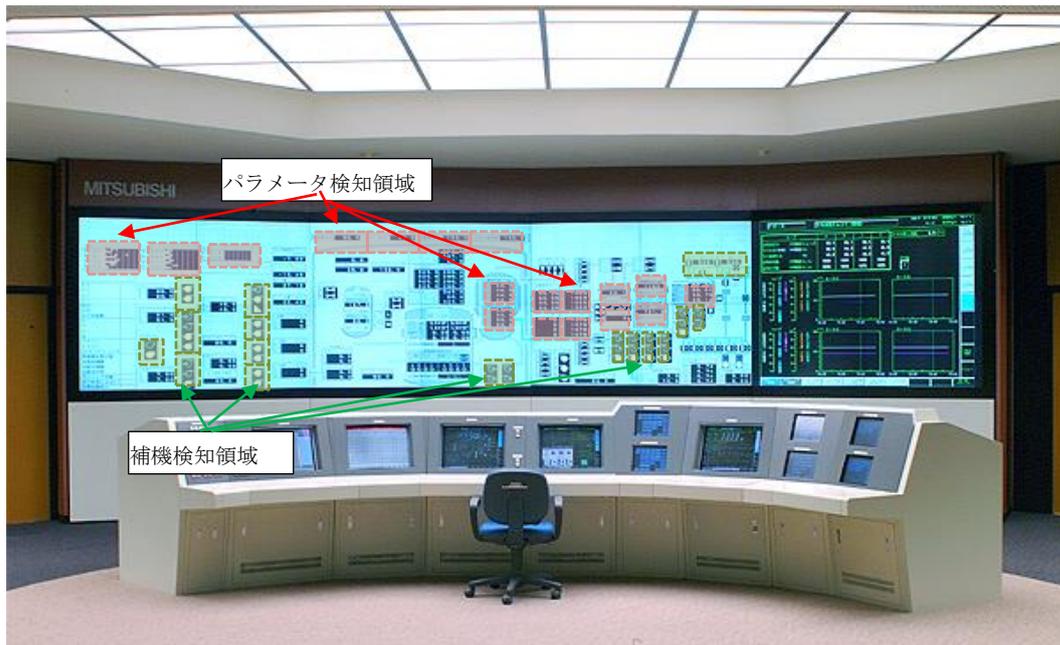


図 6.6 視覚検出領域の設定（大型表示盤の例）

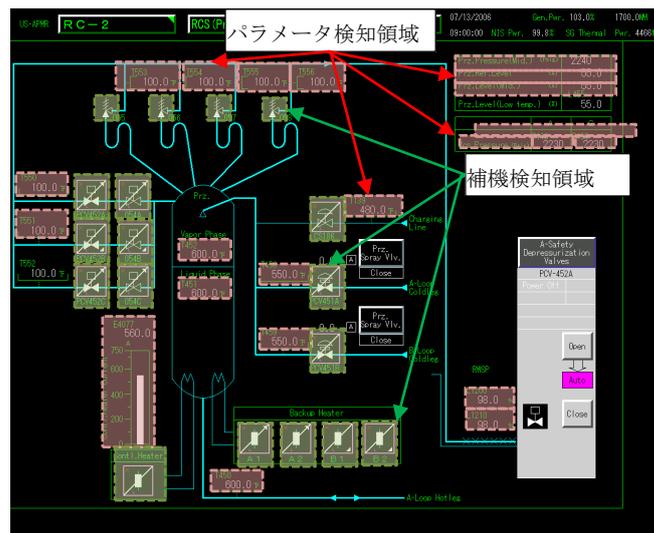


図 6.7 視覚検出領域の設定（個別監視画面の例）

認知-意思決定については、その事象の兆候を示すプラントパラメータや状態表示灯、警報等の予め認知のために必要な情報セット（基本的には検出と同じパラメータセット）を特定し、この情報セットと、事象そのものの名称、および対応運転手順書の番号を会話データと照合し判断する。さらに、デジタル化中央制御盤において、電子化手順書を導入し

ている場合には、当該手順書への画面切り替え操作情報を計算機で記録していることから、この情報と設定した事象を照合することで確実な判定が可能となる。

事象判別においては、プラントに対する、補機や弁の操作はないことから、認知プロセスにおける「アクション」は無しとしたが、b.で述べる通り、パラメータの確認、警報の確認のため、画面の切り替えなど操作はあることから、画面切り替え操作ログと切り替えた画面の注視エリア（当該画面での視覚検出領域）の特定によりどのパラメータや警報を確認したかについて判定要素として含める。

なお、パフォーマンス評価においては、0または1の判定だけでなく、目的は達成しているが一部不十分な部分があるとの判定も実施しており、このような判定を可能にすべく、部分的達成を示すロジックも設定した。すなわち、上述のように、認知プロセス全てにおいて達成している場合は「◎」、認知プロセスにおいて認知・意思決定は問題ないが、検出について不足する場合は「○」、検出、認知・意思決定とも全て満足していない場合は「×」とするロジックとする。

図 6.8 にロジック図を示す。

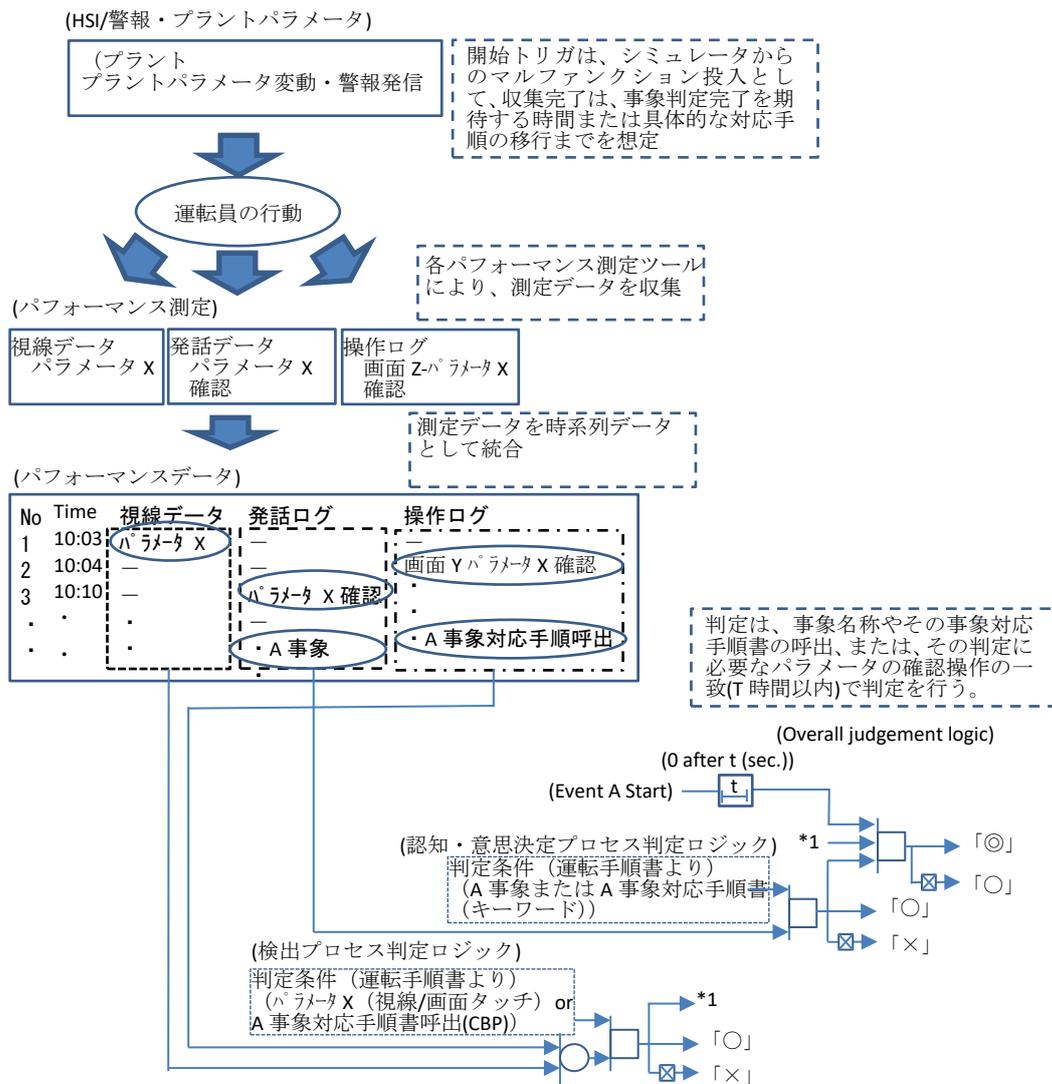


図 6.8 自動評価判定プロセス (事象判別)

プラント事象判別においては、運転手順書に必ずしも基づかず、運転員の知識、スキルにより、判断する場合がある。このような場合でも、運転手順書にある事象判別のためのキーパラメータを用いて行うこと、また、事象判別はある訓練シナリオでそれほど多くないことから、自動評価判定に用いる時系列データを、例えばシミュレータの模擬事象設定からある時間 (数十分) にする時限設定を入れることや具体的な対応運転手順書への移行までとして、評価判定用データ入力数を絞ることとする。

b. プラント状態監視

b-1. プラントパラメータ・状態表示灯監視

b-2. 警報確認

プラント状態監視については、現状のプラクティスでは個別プラントパラメータ、警報、機器の確認作業が一つの訓練シナリオの中においても多数に及ぶことから、評価者が短時間にこれらの運転員の確認作業について一つ一つ確認することは現実的ではなく、結果として、事象判別に用いられるようなプラント兆候に直接関連のあるパラメータの確認に焦点があてられる。

運転員のパフォーマンス自動測定、評価を適用することにより、運転員の個別監視操作タスクに対して、評価が可能である。

評価の仕方については、プラント事象判定後、或いは、ある目的を達成するため、特定の運転手順書で定められる操作手順に従って、監視操作を行うことになることから、a.で検討した評価プロセスと同様の評価プロセスを適用し、インプットについては運転手順書の各ステップに置けるタスク要求を設定する。（図 6.9）

なお、プラント状態監視タスクについては、プラントの補機を操作するというアクションはなく、適用される認知プロセスについては、「検出-認知-意思決定」となるが、以下のような、HSI システムに対する確認操作が発生する。

①警報確認：警報発信したことを認知し、警報音の停止と点滅表示を点灯表示とする確認行為

（デジタル型 HSI では警報画面の確認ボタンを押す操作）

②パラメータ・補機状態・状態表示確認：デジタル HSI ではオンデマンドで所望の画面にアクセスし、当該画面に表示されたパラメータ等を確認する。

これらの確認のための HSI 画面操作については、確認したことの確実なエビデンスともなることから、評価ロジックにはこれらの情報も取り入れることとする。

なお、パラメータ・状態表示灯監視、警報確認においては、上述のような、特定の目的や手順に従った対応操作以外にも、プラント異常時の初動対応など運転手順書に基づかない応急対応がある。この場合については手順書での対応移行前後操作として、識別化を図り、また、a.の事象判別対応の一つとして取り扱うこととした。

なお、プラント状態監視タスクのうち、「b-1. プラントパラメータ・状態表示灯監視」と「b-2. 警報確認」のサブタスクに分割したのは、警報確認については、警報専用のVDU 画面で警報確認操作を行うことから、b-1 と自動評価ロジックが異なるため、別のものとして識別した。

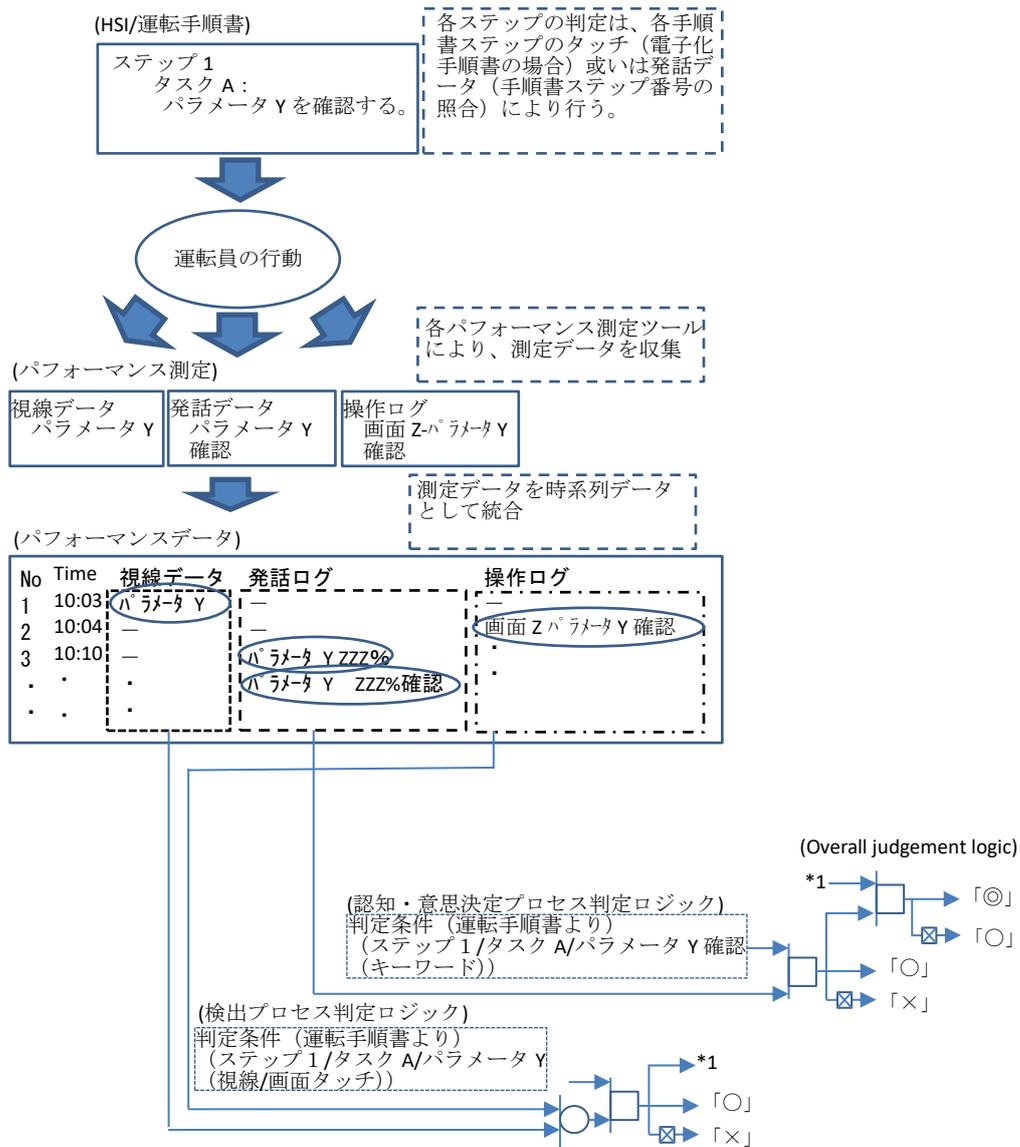


図 6.9 自動評価判定プロセス（プラント状態監視）

c. プラント操作

- c-1. ポンプ、ON-OFF 弁などの ON-OFF 操作
- c-2. 制御弁、調節弁などによるプロセス制御操作

プラント操作タスクについては、プラント状態監視タスクと同様、現状のプラクティスでは、個々の操作が、一連のシナリオ中で多数に及ぶことから、評価者が短時間にこれら

の運転員の個々の補機や弁操作作業について一つ一つ確認することは現実的ではなく、結果として、プラントの安全停止に対して重要なタスクの確認に焦点があてられる。

運転員のパフォーマンス自動測定、評価を適用することにより、運転員の個別監視操作タスクに対して、評価が可能である。

なお、従来収集できなかったこれらのタスクの達成度を個別に評価することにより、重要なタスクの遅れや不実施に対する因果関係の調査に決定的なエビデンスが得られることができ、インタフェースや訓練の改善など特定の問題の抽出や改善に効果が得られる。

プラント操作タスクは、認知プロセスでは、アクションが主となるが、その前段として特定の操作を行う前のプラント系統状態、対象操作補機／弁の状態や当該系統のプロセス状態、ラインナップ状態の確認など、操作対象補機、弁の状態に対する認知、目的とする操作可否を行う意思決定が必要となる。そのため、適用される認知プロセスについては、

「検出-認知-意思決定-アクション」となる。ただし、目的のアクションがなければ、「検出-認知-意思決定」が成功しても、目的を達成しないため評価は「×」となる一方、「検出-認知-意思決定」が不十分（未達成）の場合でアクションが成功した場合は、目的のタスクは成功したので、評価は「○」とする。（この場合、取得データの信頼性の問題か、意思疎通の問題、検出の問題など、◎と出来なかった理由については事後検討・レビューできるように識別を図る意義がある。）

評価の仕方については、プラント状態監視タスクと同様、プラント事象判定後、或いは、ある目的を達成するため、特定の運転手順書で定められる操作手順に従って、監視操作を行うことになることから、a.で検討した評価プロセスと同様の評価プロセスを適用し、インプットについては、b.と同様、運転手順書の各ステップに置けるタスク要求を設定する。（図 6.10, 図 6.11）

なお、プラント操作タスクのうち、「c-1. ポンプ、ON-OFF 弁などの ON-OFF 操作」「c-2. 制御弁、調節弁などによるプロセス制御操作」に分割したのは、表 6.1 に示す通り、操作の目標およびタスクの種類に違いがあるからである。

表 6.1 操作と制御の違い

	タスクの目標	操作方法
c-1	補機または弁を目的の状態（開／閉、起動／停止）にする	プラント系統状態、対象操作補機／弁の状態や当該系統のプロセス状態、ラインナップ状態の確認などの事前準備後、操作器を操作（1アクション）
c-2	プロセスを目標値に調整する。	プロセス値を数値やトレンドグラフなどで確認しながら、制御器の出力を調整する。（プロセスのフィードバックを得ながら、複数回操作）

すなわち、c-1 は補機や弁の状態や系統の状態を確認した後、一回の操作であるのに対し、c-2 は、プロセス値を数値やトレンドグラフなどで確認しながら、人間が制御ループの一役を担い、制御器の出力を調整する操作の違いがあることから、評価ロジックもその違いを表すようロジックを分けることとした。

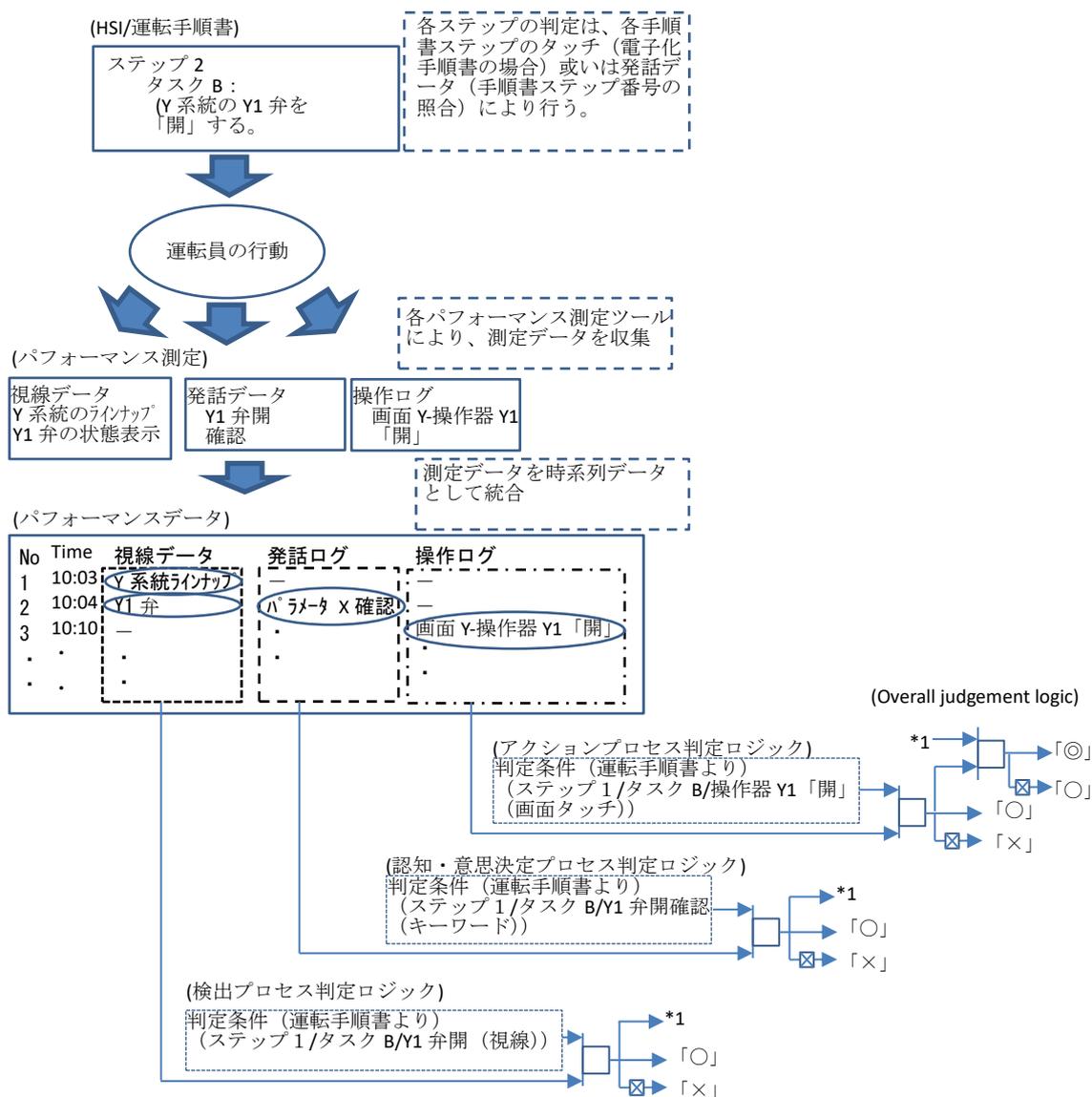


図 6.10 自動評価判定プロセス (プラント操作 (c-1 の場合))

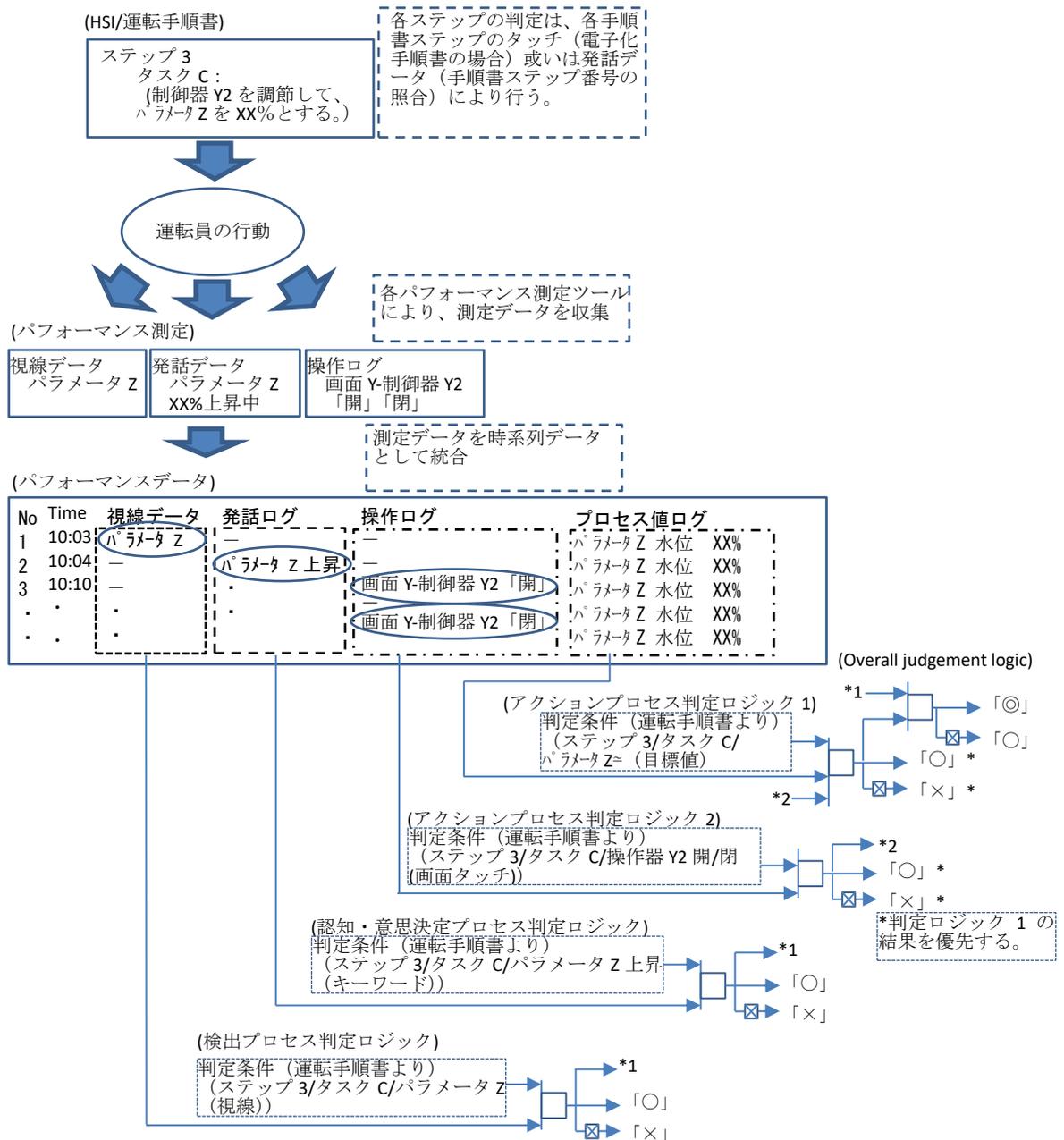


図 6.11 自動評価判定プロセス（プラント操作（c-2 の場合））

評価者は、シミュレータで模擬した事象について、運転員が、その事象の兆候を示すプラントパラメータや状態表示灯、警報等から、正しく事象を特定できたかについて、運転員チームの会話や対応操作の観察によって判定する。

上記評価者の評価プロセスに対して、適用される認知プロセスについては、「検出-認知-意思決定」となる。

6.5 プロトタイプ評価

6.4 節で作成した、ヒューマンパフォーマンス評価計測手法および自動評価手法の有効性を確認するため、プロトタイプ機による評価を行った。

6.5.1 プロトタイプ機のシステム構成と適用シナリオ

プロトタイプ機のシステム構成図を図 6.12 に示す。

プロトタイプ機は、パフォーマンス測定装置（視線計測器、発話記録システム（テキスト変換を含む）、操作ログ）、パフォーマンスデータ収集システムおよび自動パフォーマンス評価システム（アプリケーションソフトウェア）からなる。

運転コンソール VDU のディスプレイタッチログやシミュレータイベントログは、シミュレータ側で収集し、パフォーマンスデータ収集システムに転送する。

収集したパフォーマンスデータは、パフォーマンスデータ収集システムで、時系列データとして統合化され、一定のフォーマットで再整理される。

これらのデータは、自動パフォーマンス評価システムへ転送される。自動パフォーマンス評価システムには、6.4.3 節で構築した自動評価ロジックが搭載され、運転員のタスクタイプ毎に転送されたデータをインプットとして自動判定が行われる。

検証は、日本の発電所運転エキスパートを運転員として実施した。

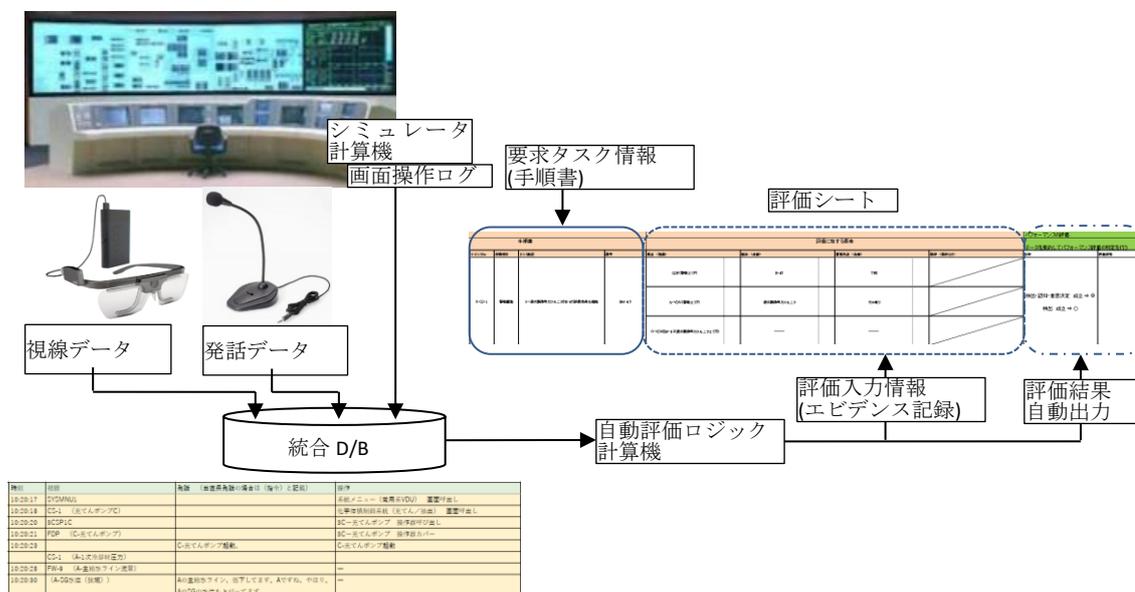


図 6.12 プロトタイプ機システム構成

シナリオは、SGTR およびその前段階事象となる蒸気発生器細管漏えい（Steam Generator Tube Leakage, SGTL）をシミュレータで模擬した。

当該事故時シナリオでは、一般的に以下の運転員アクションが行われる。（括弧書き欄は、6.4.3 の運転員の各タイプ記号(type a. b. c.)を示す。）

- i. 警報、プラントパラメータ、機器状態の確認による、異常状態の確認(type b.)
- ii. プラント診断 (type a.)
- iii. 運転手順書に基づく、事故対応と緩和操作(type b. または type c.)

6.5.2 評価結果

6.5.1 で述べたプロトタイプ機およびシナリオにてプロトタイプ試験を実施した。図 6.13 に、自動評価システムによって作成された結果の例を示す。

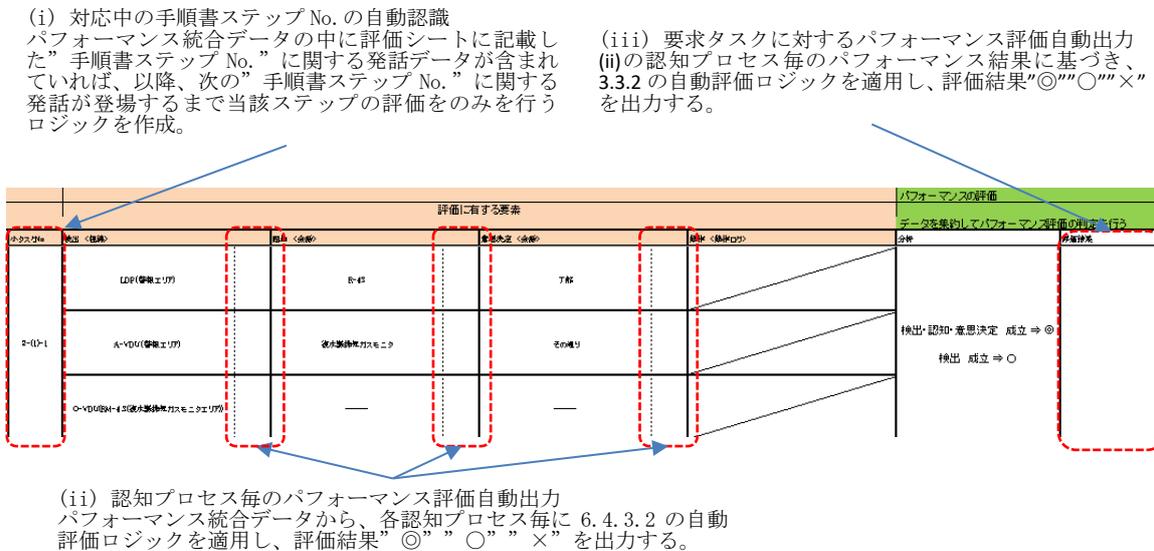


図 6.13 評価シート出力結果の例

図 6.13 に示す通り、要求タスク毎の開始、終了トリガは、6.4.3 節の自動評価ロジックを適用する。すなわち、事象判別以外は、運転手順書ステップの画面領域エリアのタッチ（電子化手順書の場合）或いは発話（紙ベースの手順書の場合）とし、事象判別タスクについては、シミュレータ計算機のマルファンクション投入後一定期間または具体的な対応手順書の移行まで（具体的な手順書移行は上記のロジックと同様）とする。

評価シートには想定通り評価結果の自動出力ができたことを確認した。

次に、自動評価結果の妥当性を確認するため、従来ベースの手動による評価（すなわち、運転員のタスク遂行の観察やシナリオ終了後のインタビューで同様のチェックリストで判定する手法）との比較を行った。手動では、認知プロセスレベルのパフォーマンスデータ（運転員がどの情報を検知したかなどの各タスク毎の行動データ）を収集することは

難しいことが判明した。すなわち、当該 SGTL/SGTR 事象では、はじめの 10 分間程度で 100 個近い手順書に基づく、監視操作タスクが発生し、これをリアルタイムで収集することは困難であった。

表 6.2 および表 6.3 に、自動評価と手動評価の比較結果を示す。表 6.2 および表 6.3 は、それぞれ、6.4 章で分類した「プラント監視」、「プラント操作(c-1)」のタスクの例を示す。自動評価結果の右側に手動で評価した結果を示す。3 人の評価者 (A,B,C) で運転員の訓練中の行動を観察し、運転手順書で要求されるタスクを実施したことを確認した場合は、手動評価欄に“○”を記入した。“Check if each task is performed”欄のブランクは、評価者が要求されたタスクを遂行したか特定できなかったことを示す。

SGTL/SGTR シナリオ全 70 ステップを評価対象とした。当該 70 ステップは、6.4 章で分類したタスクタイプで分類でき、かつ、全てのタスクタイプを含んでいる。表 6.2 および表 6.3 は、当該 70 ステップのうちの一部を示したものである。

手動評価では、全 70 ステップのうち、27 ステップのみ評価できた。その他のステップは、運転員のプラント運転タスクが早く評価が追いつかなかったことによる。また、手動評価では、どのパラメータを検出したかの認知プロセスレベルの確認はできず、各タスクレベル（当該タスクができたか）の評価のみチェックシートに「○」「×」またはブランク（評価不能）を記載するのみとなった。

したがって、自動評価で特定できた箇所に対する手動評価で特定できた箇所の割合は、70 ステップのサンプルに対して、39% (=27/70) であった。

タスクレベルでの自動と手動の評価の一致について、比較可能な上記 27 ステップについて確認したところ、全て一致していることを確認した。なお、当該 27 ステップには、6.4 章で分類した全てのタスクタイプが含まれている。

一方、自動評価の効率性については、表 6.2 および表 6.3 の形式で、全てのタスクについて、認知プロセスレベルの判定が自動で行われ、また、そのエビデンス（評価データ）がタスクステップ毎に記録されるため、事後的に当該自動ロジックの検証を行う上でも有意である。一方、手動評価においてはタスクレベルのチェックでも抜け漏れが発生し、また、エビデンスとの照合をシナリオ終了後に行う必要がある。

以上より、自動評価プロセスでは、手動評価結果と一致していることを確認するとともに、手動評価では認知プロセスレベルでのエビデンス取得が難しいことが実証した。さらに、自動評価による有効性について確認した。

表 6.2 自動評価結果と手動評価結果の比較 (プラント監視の例)

Step #	Task target	Procedure				Evaluation evidence	
		Sub-task#	Item	Descriptions	VDU #	Detection (Eye tracking)	
2-(1)	Confirmation of Radiation Monitoring System Interlock a. Check radiation high alarm and interlock signal initiations (Condenser RMS-XX and SG Blowdown RMS-YY)	2-(1)-1	Alarm Acknowledgement	Acknowledge condenser RMS-XX high alarm	RM-ZZ	LDP-1 (Alarm area)	×
						A-VDU (Alarm area)	×
						O-VDU (RM-ZZ (Condenser area))	○
		2-(1)-2	Alarm Acknowledgement	Acknowledge Steam Generator Blowdown RMS-XX high alarm	RM-ZZ	LDP-1 (Alarm area)	×
						A-VDU (Alarm area)	×
						O-VDU (RM-ZZ (SG Blowdown area))	×
		2-(1)-3	Parameter monitoring	Confirm interlock activations by monitoring interlock check display (Check white bold line on interlock signals)	RM-ZZ	O-VDU (RM-ZZ (Interlock area))	○
						——	×
						——	×

(下表へ)

Performance evaluation			Manual evaluation		
Action (operation log)	Analyses	Results	Evaluators	Check if each task is	Remarks/Comments
	Embedded logic = IF(D8="Alarm", "Detection-Understanding-DecisionMaking) OK ⇒ ◎	×	A	○	
			B	○	Acknowledge RXX alarm
			C		
	(Omitted)	×	A		
			B		
			C		
Select RM-ZZ Display page	×		A		
——	×	(Omitted)	×	B	
——	×		C		

(自動判定アルゴリズム)

(上表から)

表 6.3 自動評価結果と手動評価結果の比較 (プラント操作(c-1)の例)

Step #	Procedure				Evaluation evidence		
	Task target	Sub-task#	Item	Descriptions	VDU #	Detection (Eye tracking)	
4-(1)	Isolation of damaged SG. The actuators (A) and (B) of the 3A-main steam isolation valve (3V-MS-528A) of the damaged SG are closed.	4-(1)-5-1	Operation ON/OFF	Confirmation of operation target	FW-ZZ	—	×
						—	×
						—	×
		4-(1)-5-2	Operation ON/OFF	Select FW-ZZ display page	FW-ZZ	O-VDU(FW-ZZ)	○
						—	×
						—	×
		4-(1)-5-3	Operation ON/OFF	Display actuator(MS-528A) buttons	FW-ZZ	O-VDU(FW-ZZ)	×
						—	×
						—	×

(下表へ)

Action (operation log)	Performance evaluation		Manual evaluation		
	Analyses	Results	Evaluators	Check if each task is performed.	Remarks/Comments
—	×	(Omitted)	A		
—	×		B		
—	×		C		
Select FW-ZZ Display page	○	(Omitted)	A	○	
—	×		B		
—	×		C		
Display actuator(MS-528A) buttons	○	(Omitted)	A	○	
—	×		B		
—	×		C		

(上表から)

(自動判定アルゴリズム)

プロトタイプ試験で得られた結果として、自動でのパフォーマンスデータ収集とこれに基づく評価は、認知モデルベースで PIF を特定し、そのヒューマンエラー率を蓄積していくうえで必須の支援ツールであることが確認できた。

また、当該自動評価システムは、従来の運転訓練で実施される評価（最終目的（例えば、SGTR であれば、破損した SG を特定し、破損 SG を隔離し、プラントを安全停止状態レベルまで減温減圧操作すること）だけではなく、タスクステップ毎の認知プロセスレベルの達成度確認を行うことができ、個別操作の達成度が低い場合の原因究明と評価まで行うことができる。

これによって、例えば、どの運転クルーもあるタスクに対して同じ失敗を行う場合には、訓練の問題だけではなく、マンマシン設計の問題や運転手順書の記載不備などの問題など、HSI 設計の改善点を特定することが可能となる。

自動評価と手動評価の比較評価において、上記の通り問題ないことは確認できた一方、自動評価結果をエビデンスと詳細に比較した結果、以下 2 つの技術的改善点を特定した。

1 点目は、会話ログからのテキストの変換とキーワードマッチング率が低い問題である。会話ログからの機械的なテキスト変換とキーワードマッチングは、手動により、評価者の耳で、運転クルーの会話を聞いた情報を評価者の判断で文脈を読み取り、判定して運転手順書に記載されたタスク要求とマッチングさせるよりも悪い傾向がみられた。

これは、運転手順書に記載されたタスクや注意事項などの補足内容も限定されており、運転員は発話を大きな声で、明瞭に行うように訓練された状態で行っているにも関わらずそのマッチング精度は低い。

表 6.4 に実際に修正したログを示す。会話ログからテキストに自動変換した結果（2 列目）、キーワードマッチングによる自動判定がうまくいかず、人間が会話録音記録を基に 2 列目と照合して訂正した結果（3 列目）、人間による校正要否結果（○は問題ないもの×は修正を要したもの）（4 列目）をそれぞれ示す。

修正を要した点（×）の修正をする前全項目に対する割合は 34%であった（全 70 ステップのうち会話ログは 106 あり、そのうち 36 個について修正を要した）。自動判定ロジック自体は問題ないが、その前段となるテキスト変換の精度向上が必要である。

要因と改善点としては、大きく 2 つある。一つ目はキーワードマッチングの照合データを増やすことである。例えば、アルファベット A や a の発話は、誤認防止の観点から運転員は「アルファ」と発話する。このように運転で使用される発話慣習にキーワードを合わせることがあげられる。2 つ目は、文脈からのキーワードマッチング手法の取り込みである。例えば、表 6.3 の 2 行目にある「キュー」を 9 と自動変換されたように、文脈から判断すれば「急」（上昇）であることは明らかであり、これは前後の文脈を考慮した、最新のデータマイニング技術で改善は可能と考えられる。

ただし、当該課題については、以下の理由により、校正が容易であること、また、タスクレベルでの評価については影響がないことから、大きな影響はないと言える。

- i. 全ての会話ログは、テキストデータとして変換され、表 6.2 および表 6.3 の定型フォームに記録され、事後的に確認する際にも、修正が容易である。
- ii. 会話データの校正をしない場合は、認知プロセスレベルでの評価データの信頼性は低下するが、タスクレベルでの判定（◎か○かの判定はできないが、×かそれ以外（◎か○）の判定）は可能である。

表 6.4 会話テキスト変換データの校正例

Time	Operating procedure steps	Conversations	Conversations (Note: () indicates "supervisor".)	o means matches (no changes required.) x means no-matches. (correction required.)
0:03:02	SGTL(ECCS作動無し) 「ステップ1 関連パラメータの確認」 English notes) SGTL (no ECCS) Step 1: Acknowledge associated parameters	緊急。エヌ十六モニタ係数率高。アルファです、あるふあ えす。 English notes) Emergency. N-16 monitor high alarm. This is Alpha. Alpha es.	緊急。N-16モニタ係数率高。Aです、A-SG。 English notes) Emergency. N-16 monitor high alarm. This is <u>A</u> . <u>A-SG</u> .	×
0:03:11		指示9、上昇。 English notes) Parameter g increasing.	指示急上昇。 English notes) Parameter rapidly increasing.	×
0:03:16		アルファですね。(指令) English note) This is alpha.	アルファ (A-高感度型主蒸気モニタ) ですね。(指令) English note) This is alpha (A-high sensitive MS RMS monitor). (Supervisor)	○
0:03:19		その通り。 English note) Correct.	その通り。 English note) Correct.	○
0:03:26		関連パラメータ確認します。 English note) I will check associated parameters.	関連パラメータ確認します。 English note) I will check associated parameters.	○
0:03:29				
0:03:30		加圧器の状態はどうでしょう？ (指令) English note) How about Pressurizer condition?(Supervisor)	加圧器の状態はどうでしょう？ (指令) English note) How about Pressurizer condition?(Supervisor)	○
0:03:34		加圧器、ええ English note) Pressurizer?	加圧器、ええと。 English note) Pressurizer?	○

自動評価と手動評価の比較評価による、改善点 2 点目は、運転員の状況認知 (SA) の精度と効率性の問題である。すなわち、視線検出器の設定範囲外に視点がある場合でも運転員が警報情報を検知して、発話データより当該警報発信の認知をしたことが明らかになった。この点については以下の 2 点の要因と改善点が考えられる。

一点目は、現在の視線検出器の感度は、文字、シンボル、色に係わらず一定の範囲に設定しているのが原因と考えられる。

Medical Research Council [51]によれば、色、シンボル、文字の順で検知する視野角が異なることが分かっている。(図 6.14 参照)

したがって、図 6.15 に示すように、視線検出器の感度も、検知する対象に応じて設定を変更させることである (例えば、警報であれば色で判定させる等)。

2 つ目は、視野以外の知覚情報 (警報音など) により重要な情報を検知している可能性がある。運転員熟練者ほどその傾向を示すことが定性的にわかっており、運転員の SA の検知精度についてより感度を上げるための追加的実験が必要と考えられる。

ただし、本課題の発生確率は非常に低く、今回の例でいえば、全 70 ステップのうち 1 ステップのみ発生した (1.4%)。

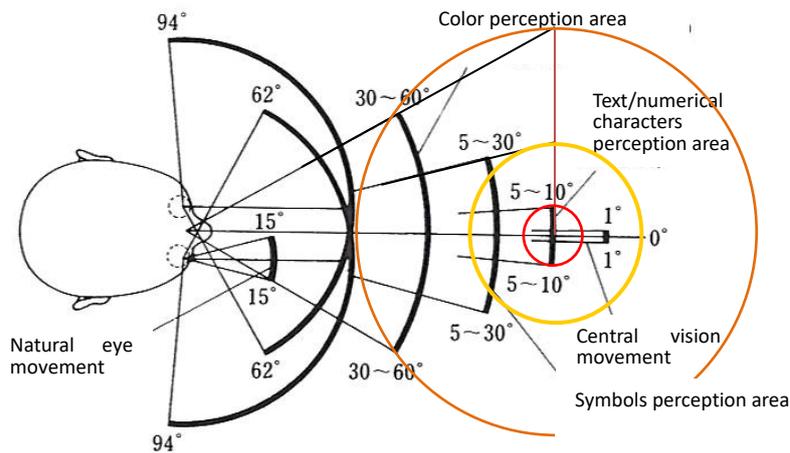


図 6.14 検知対象と視野角の関係 ([51]より作成)



Red circle: Textual/numerical character detection area
 Yellow circle: Symbols detection area
 Orange circle: Color detection area

図 6.15 視点検知閾値の多段階設定

表 6.5 に自動、手動評価の比較と、自動評価における課題（改善点）が自動／手動評価の比較結果に影響するかについて纏めたものを示す。

表 6.5 自動評価と手動評価の比較結果

	i. 評価ステップ (70 steps)	ii. 適合率(自動評価結果／手動評価結果)	iii. 会話校正有無に対する ii.適合率への影響度	iv. 視野検誤差に対する ii.適合率への影響度
手動評価	27 (39%)	-	-	-
自動評価	70 (100%)	100% (27 of 27 Steps)	None*	None*

*手動評価は認知プロセスレベルでできないため。なお、会話校正をしない場合は、一部の認知プロセス（Understanding/Decision-making）については信頼性として 34%程度低下する。

*手動評価は認知プロセスレベルでできないため。なお、視野校正については、非常に低い確率(今回の例では 1.4%)である。

以上の結果、自動評価結果と手動評価結果について適合していること、手動評価では、認知プロセスレベルでの評価はできず、また、タスクレベルでの評価であっても、全てのタスクステップを評価することは難しいこと、評価の効率性の観点からも客観的なエビデンスが定型フォームに自動で収集される点など様々なメリットがあることを確認した。

6.6 結果と検討

認知レベルでの PIF の特定やヒューマンエラー率への定量データのフィードバック、また、訓練へのフィードバックや HSI 設計の改善を行うため、マクロログニティブモデルによる認知モデルに基づき、図 6.2 に示す開発プロセスに従い、運転員パフォーマンス自動評価システムを開発した。なお、当該自動評価システムは、未だ、開発されたことがなく、本研究では、その有効性を確認するため、プロトタイプ機による、手動評価と自動評価の比較を行い、有効性を確認した。

自動評価を行うため、制御室運転クルーのマクロログニティブモデルを検討するとともに、制御室運転員のタスクタイプについて分類し、それぞれの分類に対して自動評価ロジックの作成を行った。

プロトタイプ機によるその有効性について確認を行った。手動による評価では認知レベルでの運転員パフォーマンスデータの収集や評価は困難な一方、自動評価での有効性と手動評価と比較した妥当性について確認した。

一方、手動評価と比較した際の、会話データからの判定や運転員の状況認知感度などの改善点について検討した。

当該システムを運転訓練シミュレータによる運転訓練において、各訓練生のパフォーマンスデータを収集することで、実際の作業環境や制御盤、手順書による現実に即した PIF の特定やヒューマンエラー率の算定が可能となり、マクロログニティブモデルを使用した第三世代 HRA へのフィードバックが可能である。

また、従来の訓練評価では得られなかった、訓練生毎のタスクレベルや認知レベルのパフォーマンス評価と再訓練へのフィードバックがより精度よく、効率的に行うことが、可能となる。

さらに、タスクレベルや認知レベルのパフォーマンス評価による、トレンドを分析することにより、訓練生の訓練向上だけでなく、具体的な HSI 設計や手順書不備などの改善点を把握することが可能となる。

第7章

結論

本論文では、第三世代 HRA の体系的手法に着目し、当該 HRA のプロセスで適用する、原子力発電所の運転員の認知プロセスをマクロ化（標準化／巨視化）した、マクロコグニティブモデル（Macro-cognitive Model）を人間工学プロセスでも適用し、HRA の想定条件を有機的に制御室設計プロセスに展開する検討を行った。

具体的には、当該マクロコグニティブモデルの中で考慮される行動影響因子やヒューマンエラーモードを設計開発プロセスに取り込む手法の開発、第三世代 HRA をさらに網羅性あるシナリオ開発につなげる STAMP/STPA 手法をベースとしたヒューマンコントローラモデルの適用などの研究を行った。

第2章では、本研究の対象である、原子力発電所分野における人間工学プロセス、HRA の開発経緯を纏めるとともに、関連するヒューマンエラー分析、関連研究について整理するとともに、現状の人間工学プロセスの課題について纏めた。

第3章では、第三世代 HRA の想定を人間工学プロセスに取り込む手法の開発とその実践適用について検討した。具体的には、マクロコグニティブモデルの中で考慮される行動影響因子やヒューマンエラーモードを設計開発プロセスに取り込む手法について検討し、また、具体的なシナリオを用いて、その実践的有効性について検証した。

第4章では第三世代 HRA をさらに網羅性あるシナリオ開発につなげる STAMP/STPA 手法をベースとしたヒューマンコントローラモデル(Human Controller Model, 以下 HCM という)の適用について検討した。HCM で有効なものは、非安全シナリオを制御側／非制御対象間のインタラクションプロセスを考慮して可能性のある事象として体系的に捉えられることを示し、HRA での行われるシナリオベースでは網羅的に得られないヒューマンエラーの抽出を補完することに効果があることを示した。

第5章では従来の決定論的な段階的詳細化設計開発プロセスに重畳的に適用するトップダウン的マンマシン設計プロセスの導入と効果について検討した。具体的には、Function model を用いた、プラント安全機能を維持、達成するために不可欠なプラント系統機器群系統 (Success Path, 以下 SP という) モデルを HSI(Human System Interface, 以下 HSI という)設計入力情報として直接 HSI 設計に適用し、制御室運転員の安全機能の状況認知 (Situation Awareness, SA) を向上させる。これにより、現状の人間工学プロセスで行わ

れるタスク分析やリスク情報から得られるヒューマンエラー対策（ボトムアップ的対策）では得にくい、コミッションエラー（Error of Commission, EOC）に対する対策を図ることができることを確認した。

第6章では、現在の机上評価では得られないヒューマンエラーモードや特定の制御室仕様や作業環境下で発生する、精密なヒューマンエラー率を特定するため、運転訓練シミュレータを用いた運転員訓練において、運転員のパフォーマンスを定量的な手段により測定し、その測定データから、認知プロセスレベルで、達成度やヒューマンエラー率を自動的に評価するシステムを開発し、プロトタイプ機を作成し、PWR型原子力発電所のシミュレータ、運転シナリオによる検証を行った。評価は、従来の手動による評価と比較し、従来は定量的な測定が難しい認知プロセスレベルについて精度よく測定できたこと、また、自動判定結果が、手動による評価と一致していることを確認し、当該自動評価システムの有効性について確認した。また、このシステムを活用し、ヒューマンエラー率を実践的データとして蓄積し、HRAへフィードバックすることで、より信頼性のあるヒューマンエラー分析と設計への改善が図れる。

従来は、HRA、人間工学プロセス、運転訓練がそれぞれ独立に行われており、リスク評価の精緻化、ヒューマンエラー発生リスクを高精度に予測して低減を図る制御室設計への展開について改善する余地があった。

人間工学プロセスは、実践的工学プロセスとして、人間とシステムの相互作用の中に発生するヒューマンエラーリスクを設計段階で予測し、設計へ展開し、未然防止を図ることとしているが、当該目的をさらに高い領域で達成させるため、ヒューマンエラーリスク分析、すなわち、HRAの想定条件の精緻化、訓練データをHRAや人間工学プロセスへ定量的データとして活用する、実践的手法について研究成果を纏めた。

本研究で開発した人間工学プロセスを実機設計や実訓練へ展開し、実務レベルでの有効性について確認すること、また、中長期的に訓練データからヒューマンエラー率を取得することで、中央制御盤のタイプや適用する手順によってどのような差異や特徴が得られるかを分析して、その中に潜在するヒューマンエラーの原因について探求していくことが、今後の課題および研究の方向性と捉えている。

第1章で述べた通り、ヒューマンエラーを未然に防止する取り組みは、米国スリーマイルアイランド2号機の炉心損傷事故の教訓反映から始まり、安全文化の醸成や運転員の訓練強化といった人的組織側面の他、運転員の状況認知や作業負荷低減といった、中央制御盤システムの設計強化により改善が実施されてきた。

本研究は、上述の中央制御盤システムの設計強化を目的に、分析者や設計者による想定範囲を超えたところでヒューマンエラーは発生し得ることに着目し、実際の作業環境や事象シナリオを模擬した訓練シミュレータを用いた運転訓練の中で起こりえるヒューマンエラーを最新の人間信頼性分析手法に取り込み、この結果を設計開発プロセスへ展開する仕組

みとその効果について有効性を確認したものである。

ヒューマンエラーの多くは、設計想定外の領域で起こりえることが過去の事故事例が示すところであり、当該設計想定を正確なものとするのが、ヒューマンエラーを起こしにくくする中央制御盤システムの設計品質向上への中核となる。

したがって、本研究は、当該設計想定を現実の現場作業で発生し得る領域まで拡張し、ヒューマンエラー発生メカニズムの正確な把握と設計フィードバックの枠組みを与えるものである。

このような取り組みを今後実務における中央制御盤システムの設計開発へ展開していくことにより、不適合事象の多くの原因となっている、ヒューマンエラーを低減した制御室設計開発に貢献していきたいと考えている。

謝辞

鳥取大学大学院工学研究科博士課程において本論文を作成および発表するにあたり、主指導教員の伊藤 弘道教授に御指導並びに御支援を賜りました。心から御礼申し上げます。

また、学位論文を作成するにあたり御指導いただきました鳥取大学大学院工学研究科の山田 茂名誉教授／特任教授、太田 隆夫教授、小柳 淳二准教授、南野 友香准教授に深く感謝し、厚く御礼申し上げます。

米国アイダホ国立研究所 R. Boring 博士、J. Joe 博士から、人間信頼性分析、人間工学プロセスについてヒューマンファクタ研究動向や国際的な視点についてアドバイスを賜り心より感謝申し上げます。

岡山大学工学部機械システム系学科 五福明夫教授から、Function Modeling, マンマシンシステム研究動向についてアドバイスを賜り心より感謝申し上げます。

三菱重工業の高浦勝寿氏、棚橋裕樹氏、徳永英昭氏、佐竹秀和氏には研究活動に対する理解と激励を賜りましたこと心より感謝申し上げます。

同伊藤広二氏、仲谷尚郁氏、花田聡、野田英介、塚原啓介氏には、人間工学研究に関する知見を賜り、心より感謝申し上げます。

同井手陽介氏には、航空機分野における人間工学研究、ヒューマンエラー分析に関する知見を賜り、心より感謝申し上げます。

同山下茂司氏には、飛翔体設計製作における人間工学研究、ヒューマンエラー分析に関する知見を賜り、また、同研究室の社会人枠学生として、切磋琢磨し、また、助け合いながら研究を進めることができ、心より感謝申し上げます。

鳥取大学大学院工学研究科経営システム研究室の皆様には、新型コロナウイルス禍の中オンラインでの研究が主となり、一緒に研究を進めることは困難でしたが、学会発表で研究成果を共有でき、また、知見を賜り心より感謝申し上げます。

また、研究を進めるにあたり、ご支援ご協力を頂きながら、ここに名前を記すことが出来なかった多くの方々に心より感謝申し上げます。

最後になりますが、本研究活動を温かく支援し続けてくれた妻 晶子に心からの感謝の意を示します。

略語一覽

ATHEANA	A Technique for Human Event Analysis
CBP	Computer-based procedure
CDF	Core Damage Frequency
CFM	Crew Failure Mode
CREAM	Cognitive Reliability and Error Analysis Method
CSF	Critical Safety Function
DCS	Distributed Control System
ECA	Event and Condition Assessment
EFW	Emergency Feedwater
EFWV	Emergency Feedwater Valve
EOC	Error of Commission
EOP	Emergency Operating Procedure
ERG	Emergency Response Guideline
ET	Error Tolerance
FA	Function Allocation
FD	Function Decomposition
FFD	Function Flow Diagram
FM	Function model
FMEA	Failure modes and effects analysis
FRA	Function Requirement Analysis
FRAM	Functional Resonance Analysis Method
FTA	Faults trees analysis
FV	Fussell-Vesely
GOMS	Goals, Operators, Methods, and selection rules for the methods
HAZOP	Hazard and operability analysis
HCM	Human Controller Model
H/E	Human Error
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HFE	Human Factors Engineering Program

HFEv(s)	Human Failure Event(s)
HRA	Human Reliability Analysis
HSI	Human-System Interface
HTA	Hierarchical task analysis
IAEA	International Atomic Energy Agency
IDHEAS	Integrated Decision-Tree Human Event Analysis System
IEC	International Electrical Commission
ISV	Integrated System Validation
LDP	Large Display Panel
MSIV	Main Steam Isolation Valve
MSRV	Main Steam Relief Valve
MSV	Main Steam Valve
NRC	U.S. Nuclear Regulatory Commission
OSA	Operation Sequence Analysis
Phoenix	A Model-Based Human Reliability Analysis Methodology
PIF(s)	Performance Influence Factor(s)
PRA	Probabilistic Risk Analysis
PROV	Pressurizer Relief Operation Valve
PWR	Pressurized Water Reactor
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RIHA	Risk Important Human Action
SA	Situation Awareness
S&Q	Staffing and Qualification
SCS	Safety control structure
SG	Steam Generator
SGTR	Steam Generator Tube Rapture
SI	Safety Injection
SP	Success Path
SRK	Skill, Rule and Knowledge
STAMP	System Theoretic Accident Model and Process
STPA	System-Theoretic Process Analysis
TA	Task Analysis
THERP	Technique for Human Error Rate Prediction
TLA	Time Line Analysis
TLX	Task Load Index

TMI	Three Mile Island
TTA	Tabular Task Analysis
UCA(s)	Unsafe Control Actions
VDU	Visual Display Unit
WL	Work Load

参考文献

- [1] J.M. O’Hara, J.C. Higgins, S.A. Fleger and P.A. Pieringer, ”Human Factors Engineering Program Review Model”, NUREG-0711, Rev.3, pp.44, U.S. Nuclear Regulatory Commission, 2012.
- [2] The community of The American Nuclear Society and The Institute of Electrical and Electronics Engineers, ”PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Chapters 1–8”, NUREG/CR-2300, Volume 1, U.S. Nuclear Regulatory Commission, 1983.
- [3] A. D. Swain and H. E. Guttman, “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications”, NUREG/CR-1278/SAND80-0200, U.S. Nuclear Regulatory Commission, 1983.
- [4] J.M. O’Hara, and S.A. Fleger, ”Human-System Interface Design Review Guidelines”, NUREG-0700, Rev.3, U.S. Nuclear Regulatory Commission, 2020.
- [5] J. Rasmussen, “Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models”, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 13, Issue: 3, 1983.
- [6] D.A. Norman, “Categorization of action slips. Psychological Review”, 88(1), 1–15, 1981.
- [7] J. Reason, “Human Error”, Cambridge University Press, 1990.
- [8] S.K. Card, T.P. Moran and A. Newell, “The Psychology of Human-Computer Interaction”, L. Erlbaum Associates, 1983.
- [9] J. Reason, “Human error: models and management”, BMJ, 2000
- [10] F.H. Hawkins and H.W. Orlady, “Human factors in flight”, Avebury Technical, 1993.

- [11] B. Kirwan and L.K. Ainsworth, "A GUIDE TO TASK ANALYSIS", Chapter 9, pp.267-287, Taylor & Francis, 1992.
- [12] B. Kirwan and J. Reed, "A Task Analytical Approach for the Derivation and Justification of Ergonomics Improvement in the Detailed Design Phase", Proc. Ergonomics Society Annual Conference, 36-43.
- [13] B. Kirwan and L.K. Ainsworth, "A GUIDE TO TASK ANALYSIS", Chapter 5, pp.184-201, Taylor & Francis, 1992.
- [14] E.J. Henley and H. Kumamoto, "Reliability Engineering and Risk Assessment", Prentice-Hall, 1981.
- [15] D. Limb, "HAZOP Studies – A NEW APPROACH?", Symposium series No.155, Hazards XXI, IChemE, 2009.
- [16] S.P. Whalley and B. Kirwan, "An Evaluation of Five Human Error Identification Techniques", Paper at 6th International Loss Prevention Symposium, Norway, 1989.
- [17] N. Leveson, "Engineering a Safer World", The MIT Press, 2012.
- [18] J.C. Williams, "HEART – A proposed method for achieving high reliability in process operation by means of human factors engineering technology", Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society (SaRS), 1985.
- [19] E. Hollnagel, "Cognitive Reliability and Error Analysis Method", Elsevier, 1998.
- [20] S.E. Cooper, A.M. Ramey-Smith, J. Wreathall, G.W. Parry, D.C. Bley, W.L. Luckas, J.H. Taylor, and M.T. Barriere, "A Technique for Human Error Analysis (ATHENA)", NUREG/CR-6350, U.S. Nuclear Regulatory Commission, 1996.
- [21] A.M. Whaley, J. Xing, R.L. Boring, M.L. S.M.L. Hendrickson, J.C. Joe, K.L. LeBanc, S.L. Morrow, "Building a Psychological Foundation for Human Reliability Analysis", NUREG-2114, U.S. Nuclear Regulatory Commission, 2016.
- [22] J. Xing, Y.J. Chang and J. DeJesus, "The General Methodology of humane vent analysis system (IDHEAS-G)", NUREG-2198 (Draft), U.S. Nuclear Regulatory Commission, 2019.
- [23] J. Xing, Y.J. Chang and J. DeJesus, "Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA)", RIL-2020-02, U.S. Nuclear Regulatory Commission, 2020.

- [24] N.J. Ekanem and A. Mosleh. “Phoenix – A Model-Based Human Reliability Analysis Methodology: Qualitative Analysis Overview”, Probabilistic Safety Assessment and Management (PSAM) 12, 2014.
- [25] J.C. Higgins, J.M. O’Hara, P.M. Lewis, J.J. Persensky, J.P. Bongarra, S.E. Cooper, and G.W. Parry, “Guidance for the Review of Changes to Human Actions”, NUREG-1764, Rev.1, U.S. Nuclear Regulatory Commission, 2007.
- [26] R.L. Boring and A. Bye, “Bridging human factors and human reliability analysis”, Human Factors and Ergonomics Society 52nd Annual Meeting, USA, September, 2008.
- [27] 中條 武志, “人間信頼性工学：エラー防止への工学的アプローチ”, 中央大学理工学部研究成果公開「医療におけるエラー対策普及用テキスト」
- [28] 中條武志、T.G. Clapp and A.B. Godfrey, “医療におけるエラープルーフ化 “、医療と社会, 16 卷(2006)1 号, pp.127-137, 2006.
- [29] S.G. Charlton and T.G. O’Brien, “Handbook of Human Factors Testing and Evaluation”, Chapter 9, CRC Press, December, 2001.
- [30] R.M. Taylor, “Situational Awareness Rating Technique (Sart): The Development of a Tool for Aircrew Systems Design”, Situational Awareness, 1st Edition, pp.18, Taylor & Francis Group, 2011.
- [31] M.A. Vidulich, “The Use of Judgment Matrices in Subjective Workload Assessment: The Subjective Workload Dominance (SWORD) Technique”, Proc. of the Human Factors and Ergonomics Society Annual Meeting, October, 1989.
- [32] M.R. Endsley, “Situation Awareness Global Assessment Technique (SAGAT)”, Proceedings of the IEEE 1988 National Aerospace and Electronics Conference: NAECON 1988.
- [33] S. G. Hart and L. E. Staveland, “Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. Advances in Psychology 52”, North Holland Press, pp 139-183, 1988.
- [34] K. Mashio, “Test Scenarios and Test Design”, Proc. of OECD/NEA Expert Workshop, Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications (Appendix B), February 2015.
- [35] OECD/NEA, “Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications”, OECD/NEA Human Aspects of Nuclear Safety, 2019.

- [36] K. Mashio, “Human Factors Engineering & HSI Design in the US-APWR”, 18th Annual Joint ISA POWID/EPRI Controls & Instrumentation Conference, 2008.
- [37] IAEA, “Human Factors Engineering Aspects of Instrumentation and Control System Design”, IAEA Nuclear Energy Series, No. NR-T-2.12, 2021.
- [38] R. Torok and B. Geddes, “Systems Theoretic Process Analysis (STPA) Applied to a Nuclear Power Plant Control System”, MIT STAMP Workshop, March 26-28, 2013.
- [39] R. Torok, B. Geddes, J. Thomas, and D. Blanchard, “Update on Digital Instrumentation & Control Projects - Failure Modes – Hazard Analysis Methods - Operating Experience Review - PRA Insights”, ACRS Subcommittee on Digital Instrumentation & Control Systems, September 19, 2013.
- [40] M. France and J. Thomas, “Engineering for humans: A new extension to systems theoretic process analysis”, International Symposium on Aviation Psychology, 2017.
- [41] Department of Defense Deputy Assistant Secretary of Defense (Information Management) Records Management Task Force, “The Department of Defense Records Management Function and Information Models”, U.S. Department of Defense, October 1995.
- [42] E. Hollnagel, “Barriers and Accident Prevention”, CRC Press, 2004.
- [43] W. Tian and C. Caponecchia, “Using the Functional Resonance Analysis Method (FRAM) in Aviation Safety: A System Review”, October 2020.
- [44] Mitsubishi Heavy Industries, “Design Control Document for the US-APWR Chapter 18 Human Factors Engineering”, 2011.
- [45] K. Mashio, T. Hotta, A. Gofuku and K. Ito, “Development of Online Performance Evaluation System of Nuclear Power Plant System”, Journal of Nuclear Science and Technology, October 2021
- [46] Y. Hsien and J. Chang, “SACADA A Data Collection Tool for Simulator Training”, U.S. NRC’s Web-based ADAMS at <https://adams.nrc.gov/wba/> with the access number of ML17053B558, Feb, 2017.
- [47] M. Porthin, M. Liinasuo, and T. Kling, “HRA of digital control rooms - Literature review”, Research Report, VTT-R-00434-16, VTT, Finland, August 2016.

- [48] Y. Hsien and J. Chang, “SACADA A Data Collection Tool for Simulator Training”, U.S. NRC’s Web-based ADAMS at <https://adams.nrc.gov/wba/> with the access number of ML17053B558.
- [49] H. Ujita, M. Fukuda and R. Kubota, “Plant operator performance evaluation system”, *Journal of Nuclear Science and Technologies*, 26[6], pp 591-606, June 1989.
- [50] K. Mashio, “Human Factors Engineering & HSI Design in the US-APWR”, 18th Annual Joint ISA POWID/EPRI Controls & Instrumentation Conference, 2008.
- [51] Medical Research Council (Great Britain)/Royal Navy Personnel Research Committee. Operational Efficiency Sub-Committee, “Human Factors for Designers of Naval Equipment”, Medical Research Council (U.K.), 1968
- [52] E.M. Roth, J. Easter, R.E. Hall, L. Kabana, K. Mashio, S. Hanada, T. Clouser, G. W. Remley, “Person-in-the-Loop Testing of a Digital Power Plant Control Room”, *Proc. of Human Factors and Ergonomics Society, Annual Meeting*, September 2010.
- [53] J. Kawai and Y. HORIUCHI, “Enhancement Framework for Human Factors Engineering Review Model on Beyond-Design Basis Events Conditions”, Eleventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2019, USA, February 2019.
- [54] M. Modarres, M. P. Kaminskiy, and V. Krivtsov. “Reliability Engineering and Risk Analysis: A Practical Guide, 3rd ed.”, CRC Press, USA, 2017.
- [55] G. W. Parry, A. J. Spurgin, P. Moieni, and A. Beare, “An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment”, Electric Power Research Institute, TR-100259, 1992.
- [56] E. Hollnagel, “Cognitive reliability and error analysis method”, Elsevier Science Ltd., Amsterdam, Netherlands, 1998.
- [57] 林 喜男, “人間信頼性工学 -人間エラーの防止技術-“, 海文堂出版, 1984.
- [58] 人間工学教育研究会編, “人間工学入門”, 日刊工業新聞社, 1983.
- [59] 浅井 喜代治, “現代 人間工学概論”, オーム社, 1980.
- [60] A.J. Spurgin, “Human reliability assessment – theory and practice”, Taylor and Francis Group, LLC, 2010

研究業績

・学位論文に関係した研究業績

	題目	雑誌名
第2章 (2.2章)	ヒューマンファクターエンジニアリングを通じた HRA の原子力発電所設計への展開と課題	講演会資料、日本原子力学会「2019年春の年会」企画セッション, 2019
	原子力発電所向け人間工学設計支援システムの開発	講演会資料、日本保全学会、第17回学術講演会、2021/7/6-2021/7/8, 2021.
第2章 (2.3章)	HFE (人間工学) ガイドに係る国際動向	講演会資料、日本原子力学会 HMS 研究部会「2019年夏期セミナー」
第3章 (3.2章)	Human Factors Engineering Enhancement integrated with human reliability analysis for control room design of nuclear power plant	Proc. of ANS NPIC&HMIT 2021
第3章 (3.3章)	Application of integrated human error management in human factors engineering process to nuclear power plant design	International Journal of Mathematical, Engineering and Management Sciences, Vol. 6, No. 4, 1186-1198, 2021/ Proc. of 4th Proc. of ICMTEA 2020
第4章	Application of top-down approach to human factors engineering process for control room design of nuclear power plants	Proc. of 26th ISSAT RQD 2021

第5章	Application of top-down approach to human factors engineering process for control room design of nuclear power plants	Proc. of 26th ISSAT RQD 2021
	Application of functional modeling for human-system interaction in nuclear power plant system	Workshop of IWFM 2020
	Development of Information System to Support Decision Making in Emergency Conditions	Proc. of ANS NPIC&HMIT 2019
第6章	Development of Online Performance Evaluation System of Nuclear Power Plant System	Journal of Nuclear Science and Technology, 2021
第7章	—	—

・研究業績 -学術論文-

- (1) 真塩健二, “ヒューマンファクターエンジニアリングを通じた HRA の原子力発電所設計への展開と課題”, 日本原子力学会「2019 年春の年会」 企画セッション, 2019.
- (2) 真塩健二, “HFE (人間工学) ガイドに係る国際動向”, 日本原子力学会 HMS 研究部会「2019 年夏期セミナー」, 2019.
- (3) K. Mashio, “Human Factors Engineering Enhancement integrated with human reliability analysis for control room design of nuclear power plant”, American Nuclear Society, 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), July 14-16th, 2021.
- (4) K. Mashio and K. Ito, “Application of integrated human error management in human factors engineering process to nuclear power plant design”, 4th International Conference on Mathematical Techniques in Engineering Application (ICMTEA 2020), December 4-5, 2020.
- (5) K. Mashio and K. Ito, “Application of integrated human error management in human factors engineering process to nuclear power plant design”, International Journal of Mathematical, Engineering and Management Sciences, Vol. 6, No. 4, 1186-1198, 2021.

- (6) K. Mashio and K. Ito, “Application of top-down approach to human factors engineering process for control room design of nuclear power plants”, International Society of Science and Applied Technologies (ISSAT), 26th ISSAT International Conference on Reliability and Quality in Control (RQD 2021), August 5-7, 2021.
- (7) K. Mashio, “Application of functional modeling for human-system interaction in nuclear power plant system”, 5th International Workshop on Functional Modeling for Design and Operation of Engineering Systems (IWFM 2020), October 26-28, 2020.
- (8) K. Mashio, T. Hotta, A. Gofuku and K. Ito, “Development of Online Performance Evaluation System of Nuclear Power Plant System”, Journal of Nuclear Science and Technology, October 20, 2021
- (9) K. Mashio, “Human Factors Engineering & HSI Design in the US-APWR”, 18th Annual Joint ISA POWID/EPRI Controls & Instrumentation Conference, 2008.
- (10) 真塩健二、” 原子力発電所向け人間工学設計支援システムの開発”, 日本保全学会、第17回学術講演会、2021/7/6-2021/7/8, 2021.
- (11) R. Boring (INL, Chair), D. Desaulniers (NRC), T. Ulrich (INL), N. Lau (Virginia Tech), K. Mashio (Mitsubishi), C. Poresky (UC Berkeley) and S. Massaiu (IFE), “What’s Next for Nuclear Energy? A Human Factors Perspective–Panel”, American Nuclear Society, 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (11th NPIC&HMIT 2019), 2019.
- (12) K. Mashio, S. Hanada, E. Noda, M. Kasamatsu, T. Oka, “Development of Information System to Support Decision Making in Emergency Conditions”, Proc. of American Nuclear Society, Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019), 2019.
- (13) S. Hanada (Mitsubishi), K. Mashio (Mitsubishi Nucl), M. Hirahatake, K. Takahashi (Mitsubishi Electric), “U.S.-APWR Human System Interface System Verification and Validation Program for Digital I&C Design”, Proc. of American Nuclear Society, 2010 Winter Meeting and Nuclear Technology Expo, 2019.
- (14) C. Rivere, K. Mashio and D. Martinez-Pellegrini, “ATMEA1 Nuclear Power Plant: Overview of the Human Factors Engineering Program”, Proc. of 23th International Conference on Nuclear Engineering (ICONE23-1654), Vol.23, 2015.
- (15) K. Mashio, “Test Scenarios and Test Design”, Proc. of OECD/NEA Expert Workshop, Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications (Appendix B), February 2015.

(16) K. Ito, S. Hanada and K. Mashio, “Mitsubishi’s computerized HSI and digital I&C system for PWR plants”, Progress of nuclear safety for symbiosis and sustainability: Advanced digital instrumentation, control and information systems for nuclear power plants, January, 2014.

(17) S. Hanada, K. Ito (Mitsubishi Heavy Industries, Ltd.), K. Mashio (Mitsubishi Nuclear Energy Systems), M. Hirahatake (Mitsubishi Electric), T. Clouser (Luminant Power), R.E. Hall (REH Technology Solutions), “Application of Computer-Based Operating Procedure to the US-APWR Human-System Interface,” Proc. of American Nuclear Society, 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2012), July 22-26th, 2012.

(18) E.M. Roth, J. Easter, R.E. Hall, L. Kabana, K. Mashio, S. Hanada, T. Clouser, G. W. Remley, “Person-in-the-Loop Testing of a Digital Power Plant Control Room”, Proc. of Human Factors and Ergonomics Society, Annual Meeting, September, 2010.

(19) 山田雄介、真塩健二、” 新型中央制御盤の概要と異常時・事故時運転支援システムの適用”, 火力原子力発電大会論文集 平成20年度(2009年)

・研究業績-受賞歴

・ International society of Automation (ISA), Power Industry Division (POWID), 18th Annual Joint ISA POWID/EPRI Controls & Instrumentation Conference, 2008: Technical Award (Third Place)

・研究業績-研究報告-

(1) 真塩健二、” ヒューマンエラー分析に基づく体系的な原子力発電所制御室設計展開手法の検討”, 令和2年度 日本オペレーションズ・リサーチ学会、中国・四国支部確率モデリングシンポジウム (2020 Operations Research Society of Japan, Chugoku and Shikoku Branch Symposium on Stochastic Modeling) , December, 2020.

(2) 真塩健二、” 原子力発電所設計プロセスへのヒューマンファクタエンジニアリングの適用”, 日本人間工学会 会報・人間工学専門家認定機構 Vol.47 2016.

(3) 緒方 善樹、川中子 信二、稲積 義則、高浦 勝寿、真塩 健二、二井田 晋次、”US-APWR における電気計装設備の新技術 (新型中央制御盤及び非常用ガスタービン発電機の検証)”, 三菱重工技報 Vol.46 No.4 , 2009.

(4) OECD/NEA Human Aspects of Nuclear Safety 2019, “Multi-Stage Validation of

Nuclear Power Plant Control Room Designs and Modifications” 2019 (Contributor/Panel Expert)

(5) J.C. Joe, L. Hanes and C. Kovesdi, “Developing a Human Factors Engineering Program Plan and State Vision to Support Full Nuclear Plant Modernization”, INL/EXT-18-51212, Idaho National Laboratory, August 2018 (Contributor)

(6) IAEA, “Human Factors Engineering Aspects of Instrumentation and Control System Design”, IAEA Nuclear Energy Series, No. NR-T-2.12, 2021 (Contributor to drafting and review)

(7) IEEE Standard Association, NPEC, “IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities”, IEEE-std. 1023-2020,2020 (Contributor)

付録 A : 認知エラータイプからの設計方策の検討結果

3.3.3 章 (1) Step 1 で検討した、各 PIF タイプ毎の設計方策の検討結果を付録資料として掲載する。なお、PIF 分類と”Macro-cognitive function”欄にあるエラー率は参考文献[23] Appendix B から抽出し、再整理したものである。

Red(Bold line): Need to improve (more than 1E-1) for Base PIF, more than 10 for Weight factors

Orange (Dotted line): Nice to improve (more than 1E-2), more than 5 for Weight factors

*Worst case

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under- standing	Decision making	Action Exe- cution	Team Coordi- nation	HSI	Procedure	Training
Base PIF								
Scenario Familiarity						(Confirm HSI to consider to execute the scenarios)	(Confirm Procedures to cover the scenarios)	Enhance frequency of training
SF0: No-impact	1E-4	1E-3	1E-3	1E-4	1E-3			
SF1: Unpredictable dynamics in known scenarios	6.6E-4	6.6E-3	6.6E-3	6.6E-4	N/A			
SF2: Unfamiliar elements in the scenario	5E-3	5E-2	5E-2	5E-3	N/A			
SF3-1: Scenarios trained on but infrequently performed	1E-3	1E-2	1E-2	1E-3	N/A			
SF3-2: Scenario is unfamiliar, rarely performed	1.2E-2	1E-1	1E-1	3.3E-2	N/A			
SF3-3: Extremely rarely performed	3.3E-2	3E-1	3E-1	3.5E-1	N/A			
SF4: Bias or preference for wrong strategies exists, mismatched mental models	N/A	2.6E-2	2.6E-2	N/A	N/A			
Information Availability and Reliability						Improve information qualities		
Inf0: No impact – Key information is reliable and complete	1E-4	1E-3	1E-3	1E-4	1E-3			
Inf1-1: Information is temporarily incomplete or not readily available Inadequate updates of information	N/A	5E-3	5E-3	N/A	N/A			
Inf1-2: Information is moderately incomplete – a small portion of key information is missing	N/A	5E-2	5E-2	N/A	N/A			
Inf1-3: Information is largely incomplete	N/A	2E-1	2E-1	N/A	N/A			
Inf2-1: Low unreliable or uncertain	N/A	1E-2	1E-2	N/A	N/A			
Inf2-2: Moderately unreliable or uncertain	N/A	5E-2	5E-2	N/A	N/A			
Inf2-3: Highly unreliable	N/A	1E-1	1E-1	N/A	N/A			
Inf3: Extremely unreliable	N/A	3E-1	3E-1	N/A	N/A			
Task complexity						Enhance automation/improve HSI to support tasks	Improve task step alignments	(Enhance training)
C0: No impact	1E-4	1E-3	1E-3	1E-4	1E-3	Improve situation	-	(Enhance training)

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
						awareness		
C1: Detection overload with multiple competing signals	3E-1	N/A	N/A	N/A	N/A			
C2: Detection is moderately complex	1E-3	N/A	N/A	N/A	N/A			
C3: Detection demands for high attention	1E-3	N/A	N/A	N/A	N/A			
C4: Detection criteria are highly complex	1E-2	N/A	N/A	N/A	N/A			
C5: Cues for detection are not obvious	5E-2	N/A	N/A	N/A	N/A			
C6: No cue or mental model for detection	1E-1	N/A	N/A	N/A	N/A			
C10: No impact – straightforward diagnosis with clear procedures or rules	N/A	1E-3	N/A	N/A	N/A	Provide diagnosis support information/cue alignment information	Check clear direction of procedure	(Enhance training)
C11: Working memory overload	N/A	3E-1*	N/A	N/A	N/A			
C12: Relational complexity (Number of uncheckable topics or relations in one understanding task)	N/A	3E-1*	N/A	N/A	N/A			
C13: Understanding complexity – Requiring high level of comprehension	N/A	1E-2	N/A	N/A	N/A			
C14: Potential outcome of situation assessment consists of multiple states and contexts	N/A	1E-2	N/A	N/A	N/A			
C15: Ambiguity associated with assessing the situation	N/A	1E-1	N/A	N/A	N/A			
C16: Conflicting information, cues, or symptoms	N/A	1E-1	N/A	N/A	N/A			
C20: No impact – simple, straightforward choice	N/A	N/A	1E-3	N/A	N/A	Provide support information whether criteria is met	Provide clear criteria for decision making	(Enhance training)
C21: Transfer step in procedure –integrating a few cues	N/A	N/A	4.5E-3	N/A	N/A			
C22: Transfer procedure (Multiple alternative strategies to choose) – integrating multiple cues	N/A	N/A	1.2E-2	N/A	N/A			
C23: Decision criteria are intermingled, ambiguous, or difficult to assess	N/A	N/A	1E-2	N/A	N/A			
C24: Multiple goals difficult to prioritize, e.g., advantage for incorrect strategies	N/A	N/A	3.3E-2	N/A	N/A			
C25: Competing or conflicting goals (e.g., choosing one goal will block achieving another goal, Low preference for correct strategy, Reluctance & Viable Alternative)	N/A	N/A	1.4E-1	N/A	N/A			
C26: Decision-making involves developing strategies or action plans	N/A	N/A	5E-2	N/A	N/A			
C27: Decision-making requires diverse expertise	N/A	N/A	1E-1	N/A	N/A			

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
distributed among multiple individuals or parties who may not share the same information or have the same understanding of the situation								
C28: integrating a large variety of types of cues with complex logic	N/A	N/A	1.7E-1	N/A	N/A			
C30: No impact – Simple execution with a few steps	N/A	N/A	N/A	1E-4	N/A	Study automation possibility, Provide task displays	Provide straightforward /simplified procedure steps	(Enhance training)
C31: Straightforward Procedure execution with many steps	N/A	N/A	N/A	1E-3	N/A			
C32: Non-straightforward Procedure execution	N/A	N/A	N/A	5E-3	N/A			
C33: Simple continuous control that requires monitoring parameters	N/A	N/A	N/A	3.4E-4	N/A			
C34: Continuous control that requires manipulating dynamically	N/A	N/A	N/A	2.6E-3	N/A			
C35: Long-lasting action, repeated discontinuous manual control (need to monitor parameters from time to time)	N/A	N/A	N/A	2E-2	N/A			
C36: No immediacy to initiate execution – time span between annunciation (decision for execution made) and operation	N/A	N/A	N/A	5E-3	N/A			
C37: Complicated or ambiguous execution criteria	N/A	N/A	N/A	1E-2	N/A			
C38: Action execution requires close coordination of multiple personnel at different locations – transport fuel assemblies with fuel machines	N/A	N/A	N/A	5E-2	N/A			
C39: Unlearn or break away from automaticity of trained action Scripts	N/A	N/A	N/A	1E-1	N/A			
C40: No impact – Clear, streamlined, crew-like communication and coordination	N/A	N/A	N/A	N/A	1E-3	Provide support display to share within the teams	Provide clear role to execute steps within the teams	Enhance communication scheme within the teams
C41: Complexity of information communicated –	N/A	N/A	N/A	N/A	1E-1*			
C42: Complex or ambiguous command-and-control	N/A	N/A	N/A	N/A	1E-2			
C43: Complex or ambiguous authorization chain	N/A	N/A	N/A	N/A	1E-2			
C44: Coordinate activities of multiple diverse teams or organizations	N/A	N/A	N/A	N/A	1E-2			
Weight factors								
Environmental PIFs								
ENV0: No impact – nominal weather and environmental factors	1	1	1	1	1	Improve environmental	-	-

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
						factors (temperature, humidity, background noise, wears, etc..)		
ENV1: Coldness on action execution Moderate cold (<5° C) – 1.5 Extreme coldness on manipulating instrumentation – 2 Extreme coldness on physically demanding execution –5 Extreme coldness on high precision manipulations (e.g., connecting lines to pump, remove air from lines and pumps) – 20	N/A	N/A	N/A	20*	N/A			
ENV2-1: Moderate coldness (<5° C) for nonexecution	1.1	1.1	1.1	N/A	1.1			
ENV2-2: Extreme coldness for non-execution	2	2	1.1	N/A	2			
ENV3: Heat (>33° C) or high humidity	1.1	1.1	1.1	1.5	1.1			
ENV4: Poor lighting, low luminance (L=0.15, compared to no impact L=1.5) for reading information or execution	2	N/A	N/A	2	N/A			
ENV5: Strong ambient light, glare, reflection	2	N/A	N/A	1.5	N/A			
ENV6: Very low visibility (e.g., heavy smoke or fog) for detecting targets or execution	5	N/A	N/A	5	N/A			
ENV7: Loud or burst noise	1.7	1.1	1.1	1.1	1.1			
ENV8: Wearing heavy protective clothes and/or gloves	N/A	N/A	N/A	1.5	N/A			
ENV9: Slippery surface (e.g., icing)	N/A	N/A	N/A	1.5	N/A			
ENV10: Strong winds, rain, or objects close to road on physically demanding tasks	N/A	N/A	N/A	1.5	N/A			
ENV11: Strong winds, rain, or objects close to road impeding vehicle movement	N/A	N/A	N/A	2	N/A			
ENV12: High or chaotic traffic impeding vehicle movement	N/A	N/A	N/A	1.5	N/A			
ENV13: Unstable or vibrating surface or work site	N/A	N/A	N/A	2	N/A			
System and I&C Transparency								
SIC0: No impact	1	1	1	1	N/A	Provide system/I&C Condition status, especially conditions not to reset as intended	Provide clear criteria /conditions for executions/reset	Enhance training to understand executions/reset criteria /conditions
SIC1: System or I&C does not behave as	1.1	1.1	1.1	1.1	N/A			

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
intended under special conditions								
SIC2: System or I&C does not reset as intended	1.1	1.1	1.1	10	N/A			
SIC3: System or I&C is complex or nontransparent for personnel to predict its behavior	N/A	2	N/A	N/A	N/A			
SIC4: System or I&C failure modes are not transparent to personnel	N/A	2	N/A	N/A	N/A			
Human-System Interface								
HSI0: No impact – well designed HSI supporting the task	1	1	1	1	1	Improve/check ergonomics design consideration, (labels, consistency, action status, etc..)	Clear directions to harmonize HSI functions/behavior	Understand HSI functions/behavior
HSI1: Indicator is similar to other sources of information nearby	1.5	N/A	N/A	N/A	N/A			
HSI2: No sign or indication of technical difference from adjacent sources (meters, indicators)	3	N/A	N/A	N/A	N/A			
HSI3: Related information for a task is spatially distributed, not organized, or cannot be accessed at the same time	1.5	2	N/A	N/A	N/A			
HSI4: Un-intuitive or un-conventionnel indications	2	N/A	N/A	N/A	N/A			
HSI5: Poor salience of the target (indicators, alarms, alerts) out of the crowded background	3	N/A	N/A	N/A	N/A			
HSI6: Inconsistent formats, units, symbols, or tables	5	N/A	N/A	N/A	N/A			
HSI7: Inconsistent interpretation of displays	N/A	5.7	N/A	N/A	N/A			
HSI8: Similarity in elements – Wrong element selected in operating a control element on a panel within reach and similar in design in control room	N/A	N/A	N/A	1.2	N/A			
HSI9: Poor functional localization – 2*5 displays / panels needed to execute a task	N/A	N/A	N/A	2	N/A			
HSI10: Ergonomic deficits	N/A	N/A	N/A	3.38	N/A			
HSI11: Labels of the controls do not agree with document nomenclature, confusing labels	N/A	N/A	N/A	5	N/A			
HSI12: Controls do not have labels or indications	N/A	N/A	N/A	10	N/A			
HSI13: Controls provide inadequate or ambiguous feedback,	N/A	N/A	N/A	4.5	N/A			
HSI14: Confusion in action maneuver states (e.g., automatic resetting without clear indication)	N/A	N/A	N/A	10	N/A			
HSI15: Unclear functional allocation (between	N/A	N/A	N/A	9	N/A			

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
human and automation)								
Equipment and Tools								
TP0: No impact – tools & parts are well maintained under proper administrative control	1	1	1	1	1	Improve equipment/tools usability and check dependability	Provide operation manuals	(Enhance training)
TP1: Tools / parts are complex or difficult to use	1.1	N/A	N/A	1.1	N/A			
TP2: Failure modes or operational conditions of the tools are not clearly presented (e.g., ranges, limitations, and requirements)	1.1	N/A	N/A	1.1	N/A			
TP3: Tool does not work properly due to aging, lack of power, incompatibility, improper calibration etc.)	1.1	N/A	N/A	1.1	N/A			
TP4: Document nomenclature does not agree with equipment labels	2	N/A	N/A	2	N/A			
TP5: Personnel are unfamiliar or rarely use the tool / parts	2	N/A	N/A	2	N/A			
TP6: Tools or parts lack of proper administrative control	2	N/A	N/A	2	N/A			
Staffing								
STA0: No impact – adequate staffing	1	1	1	1	1	-	-	Enhance staffing coordination
STA1: Shortage of staffing	1.1	1.1	1.1	1.1	1.1			
STA2: Lack of backup/lack of peer check or cross-checking	1.1	1.1	1.1	1.1	1.1			
STA3: Ambiguous or incorrect specification of staff roles and responsibilities	1.1	1.1	1.1	1.1	1.1			
STA4: Inappropriate staff assignment	1.1	1.1	1.1	1.1	1.1			
STA5: Key decision maker's knowledge and ability are inadequate to make the decision	1.1	1.1	1.1	1.1	1.1			
STA6: Lack of administrative control on fitness-for-duty	1.1	1.1	1.1	1.1	1.1			
Procedures, Guidance, and Instructions						-	Improve procedure writing forms/ descriptions	-
PG0: No impact – well validated procedures like most EOPs	1	1	1	1	1			
PG1: Procedure design is less than adequate (difficult to use) - Requires calculation (e.g., unit conversion) - No placeholders	1.2	1.1	1.1	1.2	1.1			

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
- Graphics or symbols not intuitive - Inconsistency between procedure and displays								
PG2: Procedure requires judgment	1.6	1.6	1.6	3	1.1			
PG3: Procedure lacks details	2.2	2.2	2.2	2.2	1.1			
PG4: Procedure is ambiguous, confusing	1.5	5	5	3	5			
PG5: Mismatch – Procedure is available but does not match the situation (e.g., needs deviation or adaptation)	1.1	17	17	1.1	10			
PG6: No verification in procedure for verifying key parameters for detection or execution	20	N/A	N/A	20	10			
PG7: No guidance to seek confirmatory data when data may mislead for diagnosis or decision-making	N/A	30	30	N/A	10			
Training								
TE0: No impact – professional staff have adequate training required	1	1	1	1	1	-	-	Improve training frequency and programs
TE1: Inadequate training frequency / refreshment	5*	10*	10*	10*	5*			
TE2: Inadequate training practicality – no hands on training · Not drilled together · Training on parts, not whole scenario together	1.5	1.5	1.5	1.5	1.5			
TE3: Inadequate training on procedure adaptation: Training focuses on procedure-following without adequately training personnel to seek alternative interpretations, evaluate the pros and cons of alternatives, and adapt the procedure for the situation	1.1	2	2	2	N/A			
TE4: Inadequate amount of training – no qualification exam	1.8	3	3	6.1	N/A			
TE5: Operator inexperienced (e.g., a newly qualified tradesman, but not an “expert”)	3	3	3	3	N/A			
TE6: Poor administrative control on training (e.g., not included in the Systematic Approach of Training Program)	2	2	10	10	N/A			
TE7: Inadequate training or experience with sources of information (such as applicability and limitations of data or the failure modes of the information sources)	14	N/A	N/A	N/A	N/A			
TE8: Inadequate specificity on urgency and the criticality of key information such as key alarms	20	N/A	N/A	N/A	N/A			

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
TE9: Not trained to seek confirmatory information when dismissing critical data	N/A	10	10	N/A	N/A			
TE10: Premature Termination of Critical Data Collection in diagnosis due to inadequate training on system failure modes	N/A	15	N/A	N/A	N/A			
TE11: Poor training on assessing action margin in deciding implementation delay	N/A	N/A	5	N/A	N/A			
TE12: Poor training on interpreting procedure in the context of the scenario for decision-making	N/A	N/A	11	N/A	N/A			
TE13: Poor training on the importance of data in frequently checking data for execution	N/A	N/A	N/A	10	N/A			
Teamwork and Organizational Factors								
TF0: No impact – adequate, crew-like teams	1	1	1	1	1	-	-	Enhance team coordination
TF1: Inadequate team	2	2	2	2	2			
TF2: Poor command & control	1.5	1.5	1.5	1.5	1.5			
TF3: Poor information management in multiple-team tasks	N/A	N/A	N/A	N/A	2			
TF4: Poor communication capabilities between teams	N/A	N/A	N/A	N/A	2			
TF5: Competing resources available for multiple teams	N/A	N/A	N/A	N/A	1.5			
Work Processes								
WP0: No impact – licensed personnel with good work practices	1	1	1	1	1	-	Incorporate work process policy in procedure	Develop and enhance work process
WP1: Lack of practice of self- or cross verification (e.g., 3-way communication)	10	1.1	1.1	10	1.1			
WP2: Lack of or ineffective peer checking/supervision	10	1.1	1.1	10	1.1			
WP3: Poor work prioritization, scheduling	1.1	1.1	1.1	1.1	1.1			
WP4: Lack of or ineffective instrumentation (e.g., pre-job briefing) for personnel to be aware of potential pitfalls in performing the tasks	1.1	1.1	1.1	1.1	1.1			
WP5: Lack of or ineffective instrumentation (e.g., supervision) for safety issue monitoring and identification	1.1	1.1	1.1	1.1	1.1			
WP6: Lack of or ineffective instrumentation for safety reporting	1.1	1.1	1.1	1.1	1.1			
WP7: Hostile work environment	1.1	1.1	1.1	1.1	1.1			
Multitasking, Interruption, and Distraction								
MT0: No impact	1	1	1	1	1	Design avoiding/reducing concurrent	Improve procedure to make good	Enhance training

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
						tasks (e.g., visual and auditory detections, etc.,)	alignment to execute concurrent tasks	
MT1: Distraction by other ongoing activities that demand attention	2.8*	1.1	1.1	2.8*	2.8*			
MT2: Interruption taking away from the main task	4*	1.7*	1.7*	4*	4*			
MT3: Concurrent visual detection and other tasks	10*	N/A	N/A	N/A	N/A			
MT4: Concurrent auditory detection and other tasks	20*	N/A	N/A	N/A	N/A			
MT5: Concurrent diagnosis and other tasks	N/A	30*	N/A	N/A	N/A			
MT6: Concurrent Go/No-go decision-making	N/A	N/A	2	N/A	N/A			
MT7: Concurrently making intermingled complex decisions / plans	N/A	N/A	5	N/A	N/A			
MT8: Concurrently executing action sequence and performing another attention/working memory task	N/A	N/A	N/A	2.3	N/A			
MT9: Concurrently executing intermingled or interdependent action plans	N/A	N/A	N/A	5	N/A			
MT10: Concurrently communicating or coordinating multiple distributed individuals or teams	N/A	N/A	N/A	N/A	5			
Mental Fatigue and Time Pressure and Stress								
FS0: No impact	1	1	1	1	1	Introduce automation for long-term or time pressure demanding tasks	-	Introduce staffing shift or additional resource to support long-term or time pressure demanding tasks
FS1: Sustained (>30mins) high demanding cognitive activities requiring continuous attention (e.g., procedure-situation mismatches demand constant problem-solving and decision-making; information changes over time and requires sustained attention to monitor or frequent checking.)	2.5	1.1	1.1	2.5	1.1			
FS2: Time pressure due to perceived time urgency	2	2	1.1	3	1.1			
FS3: Lack of self-verification due to needs to rush the task completion (speed-accuracy trade-off)	10	2	2	10	2			
FS4: Reluctance to execute an action plan due	N/A	N/A	N/A	2	N/A			

PIF Attribute	Macro-cognitive function					Design countermeasures		
	Detection	Under-standing	Decision making	Action Exe-cution	Team Coordi-nation	HSI	Procedure	Training
to potential negative impacts (e.g., adverse economic impact, or personal injury)								
FS5: Long working hours (greater than 4hrs) with high cognitively demanding tasks	1.5	1.5	1.1	1.5	1.1			
FS6: Sudden increase in workload from a long period of low to high	1.2	1.2	N/A	1.2	1.2			
FS7: Sudden decrease in workload from high to normal	1.8	1.1	N/A	1.8	1.2			
FS8: Emotional stress (e.g., anxiety, frustration)	1.2	1.2	1.2	1.2	1.2			
FS9: Physical stress or fatigue (e.g., long hours exposure to ambient noise, disturbed dark and light rhythms, air pollution, disruption of normal work sleep cycles, ill health)	1.1	1.1	1.1	1.1	1.1			
FS10: Sleep deprivation	2	1.2	1.1	2	1.2			
Physical Demands								
PD0: No impact	1	1	1	1	1	Design HSI to avoid exceeding physical limits	-	Enhance training
PD1: Physically strenuous – possibly exceeding physical limits (e.g., lifting heavy objects, moving heavy things, opening / closing rusted or stuck valves)	N/A	N/A	N/A	1.5	N/A			
PD2: High spatial or temporal precision	N/A	N/A	N/A	2	N/A			
PD3: Precise motor coordination of multiple persons	N/A	N/A	N/A	2	N/A			
PD4: Unusual, unevenly balanced loads (e.g., reaching high parts)	N/A	N/A	N/A	5	N/A			
PD5: Loading or unloading objects using crane/hoist	N/A	N/A	N/A	10	N/A			

付録 B : 統合的な H/E 対処分析結果

3.3.3 章 (1) Step 2 で検討した、統合的な H/E 対処分析を行った結果を付録資料として掲載する。

本文の追加的分析結果として追加されたタスク(a, b, c...)は、以下表中 HFEvs 欄に 1,2,3 に対応する。

Case 1: Major tasks in SGTR scenario (E0+E3)

HFE- vs	Tasks descriptions	Controllers, Indicators, and other equipment to perform tasks	PIFs				HEP	操作回数	HEPx 操作回数	Improvement factors (未然対策)				Recovery Factors (異常検出) (in case of actions not taken)			
						Descriptions				HSI	Procedure	Training	Others	Independent reviewer (person)	Independent reviewer (computer)	Deterministic	Probabilistic
1	Check reactor trip & turbine trip	E0 Reactor trip Procedure	CFM1	C1	3E-1	Monitor many parameters. Many types or categories of information to be detected	CFM1(D): Pcfm1_base=3.2E-3 Pcfm1=3.2E-3*(1+4+0.7+0.2) =1.9E-2 Pinf=E-4, Psf=E-4, Ptc=3E-1 w1=5(HSI5), w2=1.7(ENV7) w3=1.2(FS6)	1	1.9E-2	Provide task support display (e.g. reactor trip check display)	Provide step-by-step procedure to avoid distractions	Simulator training	-	Check parameters to meet criteria.	Check parameters to meet criteria.		Provide possible CFMs. Obtain personnel's behavior/performance data Update CFs actually taken and
		Reactor trip breaker: open (indication/switch)		HSI2,3,5 EVN7 FS6	2x3x5 1.7 1.2												
		Shutdown/control rod: bottom (indication)		SF0	1E-4	No impact											
		Neutron flux: decreasing (indication)		Inf0	1E-4	No impact											
		Turbine stop valves: closed (indication/switch)	CFM4	C31	1E-3	Straightforward Procedure execution with many steps	CFM4(E): Pcfm4_base=1.2E-3 Pcfm4=1.2E-3*wi =7.1E-3 Pinf=E-4, Psf=E-4, Ptc=1E-3 w1=5(HSI5), w2=1.7(ENV7) w3=1.2(FS6)	1	7.1E-3								
		Power to class 1E buses		HSI2,3,5 EVN7 FS6	2x3x5 1.7 1.2												
				SF0	1E-4												
2	Check SI status	ECCS actuation signal: lit (indication)	CFM1	C1	3E-1	Monitor many parameters. Many types or categories of information to be detected	CFM1(D): Pcfm1_base=3.2E-3 Pcfm1=3.2E-3*wi =1.9E-2 Pinf=E-4, Psf=E-4, Ptc=3E-1 w1=5(HSI5), w2=1.7(ENV7) w3=1.2(FS6)	1	1.9E-2	Provide task support display					Check lineup		
		Safety injection pump: running (indication)		HSI2,3,5 EVN7 FS6	2x3x5 1.7 1.2												
		RHR (Residual Heat Removal) pump: running (indication)		SF0	1E-4	No impact											
		Safety injection/RHR lineup (Outlet flow, valves) (indication)		Inf0	1E-4	No impact											
			CFM4	C31	1E-3	Straightforward Procedure execution with many steps	CFM4(E): Pcfm1_base=1.2E-3 Pcfm1=1.2E-3*wi =7.1E-3 Pinf=E-4, Psf=E-4, Ptc=1E-3 w1=5(HSI5), w2=1.7(ENV7) w3=1.2(FS6)	1	7.1E-3								

HFE- vs	Tasks descriptions	Controllers, Indicators, and other equipment to perform tasks	PIFs			HEP	操作回数	HEPx 操作 回数	Improvement factors (未然対策)				Recovery Factors (異常検出) (in case of actions not taken)					
					Descriptions				HSI	Procedure	Training	Others	Independent reviewer (person)	Independent reviewer (computer)	Determinis tic	Probabilistic		
				HSI2,3,5 EVN7 FS6	2x3x5 1.7 1.2													
				SF0	1E-4													
				Inf0	1E-4													
3	Check Emergency Feedwater (EFW) valve alignment	Emergency feedwater flow (indication) EFW pumps/valves: open (indication)	CFM1	C0	1E-4	No impact	CFM1(D): Pcfm1_base=3.0e-4 Pcfm1=3e-4*wi =1.6E-3 Pinf=E-4, Psf=E-4, Ptc=E-4 w1=5(HSI5), w2=1.2(FS6)	1	1.6E-3	Provide task support display (lineup check)				Secondary Heatsink	Check lineup			
				HSI2,3,5 FS6	2x3x5 1.2													
				SF0	1E-4	No impact												
				Inf0	1E-4	No impact												
			CFM4	C31	1E-4	No impact	CFM4(E): Pcfm1_base=3.0E-4 Pcfm1=3E-4*wi =1.6E-3 Pinf=E-4, Psf=E-4, Ptc=E-4 w1=5(HSI5), w2=1.2(FS6)	1	1.6E-3									
				HSI2,3,5	2x3x5													
				SF0	1E-4													
				Inf0	1E-4													
4	Control level	SG EFW control valve (switch) SG levels (indication)	CFM1	C0	1E-4	No impact	CFM1(D): Pcfm1_base=3.0E-4 Pcfm1=3E-4*wi =2.1E-3 Pinf=E-4, Psf=E-4, Ptc=E-4 w1=5(HSI5), w2=1.2(FS8) w3=2.8(MT1)	10	<u>2.1E-2</u>					Secondary Heatsink				
				HSI2,3,5 FS8 MT1	2x3x5 1.2 2.8													
				SF0	1E-4	No impact												
				Inf0	1E-4	No impact												
			CFM4	C31	1E-4	No impact	CFM4(E): Pcfm1_base=3.0E-4 Pcfm1=3E-4*wi =2.1E-3 Pinf=E-4, Psf=E-4, Ptc=E-4 w1=5(HSI5), w2=1.2(FS8) w3=2.8(MT1)	10	<u>2.1E-2</u>									
				HSI2,3,5 FS8 MT1	2x3x5 1.2 2.8													

HFE- vs	Tasks descriptions	Controllers, Indicators, and other equipment to perform tasks	PIFs				HEP	操作回数	HEPx 操作 回数	Improvement factors (未然対策)				Recovery Factors (異常検出) (in case of actions not taken)			
						Descriptions				HSI	Procedure	Training	Others	Independent reviewer (person)	Independent reviewer (computer)	Determinis tic	Probabilistic
		Valve (PORV) (controller) RCS temperature RCS pressure Subcooling		C33	3.4E-4	Simple continuous control that requires monitoring parameters	Pinf=E-4, Psf=E-4, Ptc31=E-3, Pct33=3.4E-4 w1=5(HSI5), w2=1.2(FSS) w3=3(FS2) w4=4(MT2)										