プラント DiD リスクモニタの多用途応用の展望

A prospective review on multi-purpose application of plant DiD risk monitor

シンビオ社会研究会	吉川　榮和	Hidekazu YOSHIKAWA	Member
プライムシステム研究所	中川　隆志	Takashi NAKAGAWA	Nonmember
System P&A	寺下　尚孝	Naotaka TERASHITA	Nonmember
哈爾濱工程大学	馬　戦国	Zhanguo MA	Nonmember

Abstract: A new risk monitor system has been under development which can be applied not only to prevent severe accident in daily operation but also to serve to mitigate radiological hazard just after severe accident happens. The system is composed by plant DiD (Defence-in Depth) risk monitor and reliability monitor. The plant DiD risk monitor can describe versatile scenarios of human-machine interaction in accident situation by utilizing UML (Unified Modeling Language) so as to serve as a useful tool of accident management. The employed methods in the plant DiD risk monitor are briefly explained first and then typical applications of the plant DiD risk monitor are introduced: one is the simulation of emergency procedure for managing severe accident in conventional PWR plant in Japan, and the other is the designing of digital HIS to monitor plant state in SBLOCA in passive safety PWR of AP1000.

Keywords: DiD, risk monitor, unified modeling language, severe accident management, PWR, AP1000, SBLOCA

1．　はじめに

2011 年 3 月東日本大震災の際東電福島第一発電所では想定外の自然災害の重畳に巧く対応できず、結果として 4 つの原子炉でシビアアクシデントの連鎖が生じた。さて事故後 6 年を経た今日、日本ではようやくシビアアクシデント対策設備を強化した PWR プラントが再稼働し始めた。そこではシビアアクシデント対策設備の強化だけでなくハードを適切に使ってシビアアクシデントをもたらさないためのソフトウエア対策の向上が課題とされている。

著者らは複雑な機械システムの操作安全性に関わり、人間―機械相互作用のモデリング手法であるプラント DiD リスクモニタ[1]と動的信頼性解析法の GO-FLOW [2]を組み合わせた新たなリスクモニタシステムを提唱している[3]。本稿では、まずプラント DiD リスクモニタのソフトウエア構成法の概要を紹介する。次いでそのソフトウエアの 2 つのシビアアクシデント対策への応用（緊急時対応における組織連携行動のシミュレーションと人間―自動系相互作用の設計評価法）について紹介する。

連絡先：吉川榮和、〒606-8202 京都市左京区田中大堰町 49（公財）応用科学研究所内　シンビオ社会研究会
E-mail: yosikawa@kib.biglobe.ne.jp

2．　プラント DiD リスクモニタのソフトウエア構成法

2.1 2 層構成のリスクモニタシステム

著者の提唱する 2 層構成のリスクモニタシステムを Fig. 1 に示す。

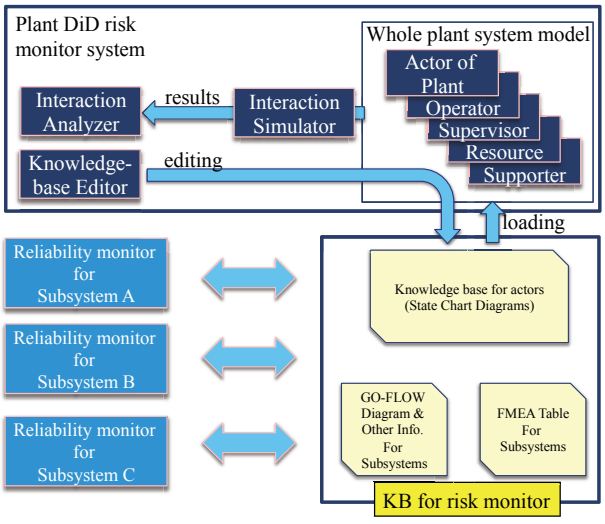

Fig. 1　Configuration of two-layer risk monitor system

著者のリスクモニタシステムは、システム全体に対するプラント DiD リスクモニタといくつかの信頼性モニタで構成されている。信頼性モニタは安全系を構成する個々のサブシステムについて所与の状況と条件下でサブ

システムが果たすべき機能が損なわれる可能性と機能発揮に失敗したときの影響を定性評価するFMEAとその動的信頼性を定量評価するGO-FLOWで構成されている。一方、プラントDiDリスクモニタは安全設備の全体とそれらを操作する人々の組織の全体について、人と機械の個々の要素をアクターとし、特定の状況下での個々のアクター間の相互作用の全体の振舞いを状態遷移モデルを用いて表現して起こりうる様々なリスク状態を解析評価する。

2.2 プラントDiDリスクモニタ

プラントDiDリスクモニタは、プロセスシステムの状態遷移をモデル化するカラーペトリネットの一種を採用しており、基本的には様々なシステムに適用可能である。ここでは原子力プラントの安全問題に応用するために展開した方法と応用ソフトウエアを述べる。

2.2.1 プラントの運転モード

プラントDiDリスクモニタによるリスク解析評価の対象としての原発の運転モードの分類をTable 1 に示す。表中のAは、原発の設計基準として考慮すべき定常および過渡状態として運転モードであり、一方、Bは設計基準では想定外の緊急事態である。

Table 1. Classification of operation modes for nuclear power plant

A. Design basis	Normal operation	Start-up, Steady state operation, Power change and shutdown
		Refueling and maintenance testing
	Off-normal	Anticipated transient, accident
	Design basis severe accident	
B. Imaginary emergency situation		

2.2.2 プラントの運転モードと人間の行動モードとの関係

Table 1中の設計基準内の運転モードAと設計想定外のBは、ヒューマンファクタの領域での3つの人間行動モード（Skill-base, Rule-Base, およびKnowledge-base）と対比すると、Aに対してはSkill-baseおよびRule-base行動で対応できるように運転要員には運転手順書を整備し、様々な研修訓練によって一定水準以上の熟練度が要求される。一方、Bに対しては、福島第一事故後、たとえ想定外の事象に遭遇しても運転員は自分の習得した知識と発見的な問題解決によってできるだけ事態を悪化させないように対応できる知識ベースの対応能力を強化するよう教育訓練することが要請されるようになった。

2.2.3 プラントDiDリスクモニタ構成上の基本的仮定

著者らのプラントDiDリスクモニタの構成ではTable1中のAのうち設計基準シビアアクシデント時の想定安全設備を用いて緊急時対応人的組織がシビアアクシデントに対応する際の機械システムと人的組織との相互作用を以下の考え方で解析する。

(1) 全体のプラントシステムは、機械システムとプラント運転に関わる運転員、当直長およびその他の要員をアクターとし、それぞれのアクターの機能モデルの組み合わせで相互作用のシナリオをモデル化する。

(2) 全体のプラントシステムの動的振舞いはこれらのアクター間の相互作用で模擬される。

(3) それぞれのアクターはそれぞれのシナリオデータを持ち、このシナリオデータに基づいて振舞う。このようなシナリオデータを直感的にかつ容易に作成するため、ソフトウエア工学の分野でコンピュータの動作を記述するため広範に用いられているUnified Modeling Language (UML) Ver.2 [4]で定義されている“State Chart Diagram”を用いる。

(4) プラントDiDリスクモニタの機能として、模擬したプラント挙動が望ましいかどうか、相互作用は望ましいかどうか、またそれが望ましくないときに何がその原因になっているのかを分析できるようにする。

2.2.4 プラントDiDリスクモニタのソフトウエア構成

上述の機能を実現するプラントDiDリスクモニタは次の3つのサブシステムで構成している。

(1) 知識ベースエデイタ（Knowledge base editor）ーアクターのシナリオデータをState Chart Diagramとして編集する。

(2) 相互作用シミュレータ（Interaction simulator）ーすべてのアクターをシナリオデータに応じて駆動することによって全体プラントシステムの振舞いをアクター群の振舞いとして模擬する。

(3) 相互作用アナライザ（Interaction analyzer）ー相互作用シミュレータによって得られたそれぞれのアクターの振舞いの結果を、State Chart Diagram同様、UML[4]で定義されている、Sequence diagramによって図示する。

これらの3つのサブシステムは統合開発環境Eclipse[5]とグラフィカル編集フレームワークGEF[6]によってPlug-inソフトとして作成され、platformに依存しないオブジェクト指向プログラム言語Javaでプログラムしているので Window—PCでもMac-PCでも使用できる。

2.2.5 知識ベースエデイタ

事故のシナリオとは、起こった事故に応じてプラントの利用可能な機器を適宜用いて各々の対応組織が行う事故収束のために行う作業の流れの全体である。これを State chart diagram と呼ぶ状態遷移モデルで表現する。様々なアクターの知識ベースを表現するうえで State chart diagram を用いると次の２つのメリットがある。

(1) 抽象的で概略的な表現から具体的で詳細にわたるまで異なった抽象レベルで動的振舞いを容易に表現できる。
(2) 状態の定義、異なった状態の間の遷移、状態の遷移をもたらす事象の生起の 3 つを簡単に記述できる。

Fig. 2 は知識ベースエデイター—の一場面である。図中、画面中央部のキャンバスは、“運転員が機械の状態を確認する”というタスクの State Chart Diagram である。利用者は状態やラベルを右側中央にある Component ボックスから選択し、キャンバス内の適当な場所にドラッグする。状態間の“遷移線”は同じく右上のパレットにある Connection tool によって引くことができる。遷移線は矢印の線で始めの状態を目標とする状態へ結合するが、この遷移を引き起こすことは複数の事象ハンドラー—で定義できる。事象ハンドラーは、ある特定の事象を受け取ると状態遷移を引き起こすコマンドシーケンスを実行する。利用者は Java プログラムでこれらのコマンドシーケンスを記述して、次の 4 つのタイプの事象ハンドラーを定義できる。

(A) Actor external event：他の actor に働きかける
(B) Actor internal event：一つの actor 内部での通信
(C) Primary event：ある状態が生起ないし消失したときにそれを知らせる
(D) Timer event：ある時間に達すると事象を起こす。

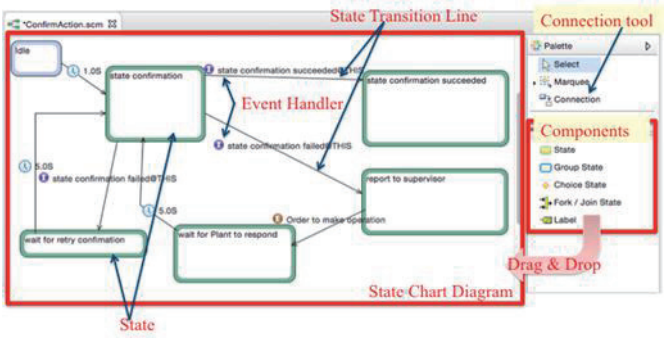

Fig. 2 Snapshot of knowledge-base editor

Fig. 2 に示した State Chart Diagram は、ある機械がある要求された状態に達したかどうかを確認するというタスクをモデル化したものである。このような確認タスクはプラントの運転員が頻繁に行う共通のタスクであるのでこれを知識ベース（ソフトウエア要素）として繰り返し使用できるようにしておけば効率的である。このような基本的タスクモデルを State Chart Diagram の形で要素化するには、特定の対象を表す情報（たとえば機械の名称、達成すべき目標など）は分離したほうが良い。そこでそのような特定データは、対象に依存する情報を与えるパラメタ領域に指定できるようにすれば、このような state chart diagram は計算機プログラムのサブルーチンのように共通的に用いるソフトウエア要素にすることができる。

様々な要素タスクをこのようなソフトウエア要素にしておけば、一般ユーザは、これらを必要に応じて選択して適当な順序に配列していくだけで“シナリオデータ”を簡単に構築できる。要するに煩雑なプログラミング能力がなくても、プラント DiD リスクモニターを容易に利用できるようになる。著者らのプラント DiD リスクモニタではこのようなソフトウエア要素として機械システムの監視制御にあたる人的組織が行う基本的なタスクを抽出して、Fig. 3 に示すようなソフトウエア要素を用意している。

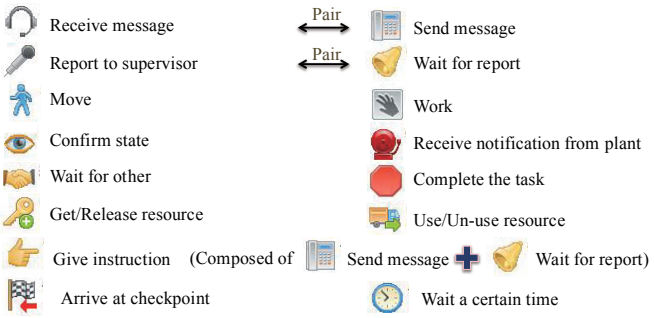

Fig. 3 Component list for all basic tasks

Fig. 3 に示すような基本的なソフトウエア要素を適宜用いて“シナリオデータ”を作成する事例を Fig. 4 に示す。図中、キャンバス上に 4 つの“状態”を左から右に配置し、それぞれの状態の間を“遷移線”で結んでいる。右側にあるウインドウから適当な“ソフトウエア要素”を選び、それぞれ対応する“状態”に落とす。そしてそれぞれのソフトウエア要素に与えるべきタスクを完了させるのに必要な時間や、人数などのパラメタ値をそのソフトウエア要素のパラメタ設定欄に書き込む。

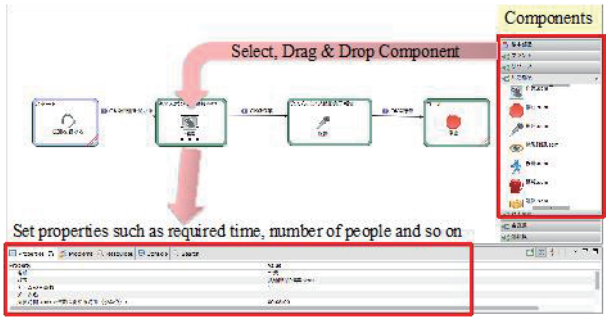

Fig. 4 Creation of scenario data using component data

次にユーザはこれらの“遷移線”に対して、“事象ハンドラー”を設定する。事象ハンドラーの具体的な設定方法を Fig. 5 に示す。図中左側の State-A で示された“Open Valve”というタスクは、“性質”に指定された条件が満たされたら“OK”という名前の”アクタ内部事

象“が完了する。(”アクタ内部事象“は、”Event Name”@“Generate Place Name of Event”という文法で与えられる。)

Fig.5 でのState Aから State Bへの遷移線に設定されている OK@OpenValve という アクタ内部事象はその性質で規定されているバルブ開という名前の仕事を開始して2分経過すると、事務所に移動するというタスクに変わるという意味である。

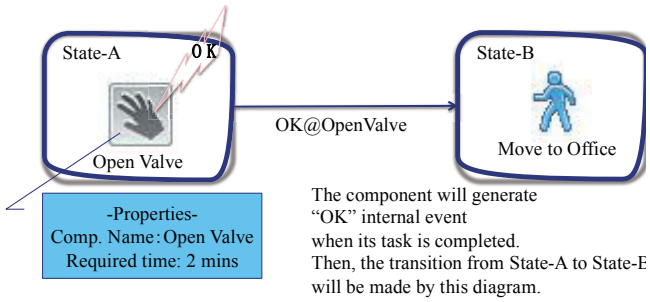

Fig.5 Method of setting event handler

2.2.6 相互作用シミュレータ

所与の事故シナリオに対応するすべての知識ベース情報が一群の State Chart Diagram に変換されると、ユーザは相互作用シミュレータを起動することによってアクター間の相互作用シミュレーションを行うことができる。著者らの相互作用シミュレータでは、個々の基本タスクの実行時間は次の5つの要因により決定される。

(A) 基本タスクに対する”要素”は、それを実行するのに要する時間が”変数”として与えられている。この変数をタスク完了のための実行時間として定める。

(B) 移動時間 : アクターが人間の場合、目標とする場所への移動に要する時間を加味する。移動時間はそこまでの距離を歩いていくか車で行くかの移動手段を計算する。

(C) 必要な人数 : そのタスクを実行するのに要する人数。必要な人数がそろえば実行できるが、そろわなければ人数が集まるまで実行は延期される。

(D) 待ち合わせ時間 :他人の助けや他のタスク完了が必要な場合はそれがそろうまで待つことになる。

(E) 資源の準備時間 :タスクを実行するのに車が必要とか道具が必要とか準備が必要な場合はそれらがそろうまで待つ。

2.2.7 相互作用アナライザ

相互作用シミュレーションの結果は、評価目標に照らして分析評価することになるが、著者らによる相互作用アナライザを用いる上での評価の3つの観点と評価結果に基づく対策の立て方を以下にまとめる。

(A) シミュレーション結果が期待外れの場合 :相互作用シミュレーションの結果が期待外れ、ないしシナリオの途中でシミュレーションが停止するような場合、シナリオデータの設定に誤りや正確さを欠くと考えて、データの設定などの試行錯誤を行って役割分担などのシナリオを見直すことで解決を図る。

(B) シナリオの重要な局面を制限時間内にクリアできない場合 : たとえば緊急時対応手順にはその実行の途中段階に時間的制約がある。このような事件制限を超えるような場合にその原因を考えてシナリオの立て方、人数や資源の不足を改善する。

(C) シミュレーション結果が望ましくない状況を予測させる場合 : シナリオ通りに実行しても結果が望ましくない場合としてたとえば炉心溶融事故になってしまえば環境への放射能放出が避けられなくなる。この場合炉心溶融事故を絶対に起こさないようにシナリオのあり方や対策の強化を図るというような場合である。

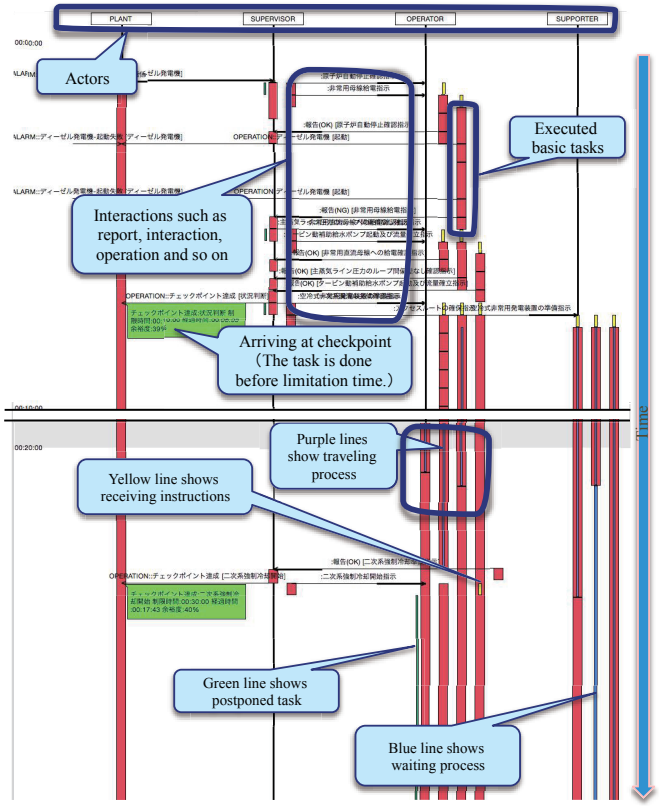

Fig.6 Example of sequence diagram

相互作用シミュレータによる結果を、Fig.6 に示すような”シーケンスダイアグラム”を用いて図式表示すると、相互作用の結果の多角的な観点での分析と対策の検討が効率的に行える。ここでは詳細は割愛するが、Fig.6 では横軸方向にすべてのアクターを並べ、縦軸方向に時間の進展とともに生じる各アクターのアクションの種別、開始、終了の時点を図示している。アクター間を結ぶ横線

はいわゆるアクター外部事象のやり取りを示している。制限時間を超える逸脱や遅滞などの問題点は自動的に色分け表示されるので問題点の発見も容易である。そしてそのような部分を右クリックするとState Chart Diagramの内容が表示されるので、シナリオデータの修正などを行って再度シミュレーションを実行すれば問題点解決のための検討が容易に実施できる。

３．原発シビアアクシデント時緊急対応の組織連携シミュレーション

3.1 背景

事故や災害の発生など緊急事態の収拾に対応する人たちには事故発生した工場などの当事者以外に警察、消防などの行政機関の人たちも関わっている。このような人たちは予め想定している事象だけでなく、想定外の事象でもその場で対処できる高い対応力が求められる。そのような職務に携わる人たちには緊急事態に適切に対応できるように研修訓練があり、それぞれの役割に応じて対応行動をするためのマニュアルが整備され、また対応組織全体が正しく行動できるように想定訓練が行われている。しかし無数の可能性のある事態に適切に対応するために実地訓練をすることは不可能であり現実的でもない。そこでコンピュータで多様な人的構成、多様な事態に巧く対応できるかどうかをシミュレーションさせて問題点を発見し、その解決策を見出しておくようにすれば大掛かりな実地訓練を繰り返すより効率的であろう。こういった目的にプラントDiDリスクモニタの適用が期待できる。

3.2 国内PWRの全交流電源喪失事故時の緊急対応の組織連携シミュレーション

日本の原子力界では2011年3月発生の東電福島第一発電所事故以降、原子炉規制基準の改正によってシビアアクシデント対策が強化された。ここでは最近再稼働されたPWRを例に所内全交流電源喪失事故時に代替発電機の起動と消火用エンジン車による海水注水により炉心冷却を行ってシビアアクシデントを回避する緊急対応シナリオの成立性を検討する。

そのベースケースとして、プラント内緊急対応チームの構成としてSupervisor 2名、運転員8名にプラント外から駆けつける助勢チーム17名とし、緊急事態進展中のcheck pointとして事故の判断を10分以内、2次系後備冷却開始30分以内、代替発電機の起動による給電開始1時間以内、代替炉心注入開始2時間20分以内、温態停止到達4時間以内、海水の補助給水タンク供給11時間、海水のCV再循環系と高圧注入系の供給51時間を満たすべくプラントDiDリスクモニタでシナリオ成立性の検討を行った。解析作業に要した時間ではシナリオデータの編集時間に1-2時間を要した。これには知識ベースエディタのデバッグ機能が作業実施に役に立った。その後シナリオ開始から終了まで一貫した相互作用シミュレーションが可能になるまでに1-２時間を要した。ラン中のデバックを効率化するため実際時間より100倍の高速シミュレーションをできる機能がデバッグに役にたった。

Table２のCase１はベースケースの結果で、チェックポイントに到達した時間を記載し、制限時間を満たしているかどうかを表示している。Case1では代替炉心注水が2時間44分24秒になって制限時間の2時間20分より遅れる。そこでCase2ではsupervisorのうち1名が運転員のほうに回ることで2時間17秒に改善し、一方Case3ではsupervisorのタスク配分を変えてさらに1時間38分11秒と大幅に改善を図っている。

Table 2 Result of case study

Checkpoints & Limitation time	Case 1 Supervisors: 2 Operators: 8	Case 2 Supervisors: 1 Operator: 9	Case 3 Supervisor: 2 Operator: 8
Judge the accident (0:10:00)	0:06:10	0:07:29	0:06:07
Start forced cooling of 2nd system (0:30:00)	0:18:04	0:19:43	0:18:00
Supply electricity from alternative generator (1:00:00)	0:37:12	0:38:51	0:37:09
Start alternative water injection into core (2:20:00)	2:44:24	2:00:17	1:38:11
Hot shut down status (4:00:00)	2:44:24	2:33:34	2:33:41
Able to supply seawater to aux feed water tank (11:00:00)	5:00:18	5:01:58	5:00:17
Able to supply seawater to CV recirculation unit (51:00:00)	6:28:39	6:30:19	6:28:38

４．人間－自動系相互作用の設計評価法

4.1 背景

計算機技術の進歩により、デイジタル制御と情報処理技術の統合によって全デイジタル型計装制御中央制御盤の導入が進んでいる。そこでは1980年代から90年代にかけてTMI-2事故やチェルノビル事故を契機にプラント運転操作からできるだけ人間を除外してヒューマンエラーを防止するという意図から自動方式の多用を指向している。また計測系がセンシングした結果を用いて能動的に安全系を動作させる方式は能動的な要素の存在が信頼性を損なうとの考えから、原発の安全系の構成を従来の能動安全系（Active safety system）から自然の物理原理を活かして全体システムが自然に安全側に状態を変えるという受動安全系（Passive safety system）の研究が進展して最近では受動安全系を積極的に採用する新型の軽水炉原子力発電プラントが実用化されている。

しかしコンピュータを多用した自動系や受動安全系の登場はプラントの運転員のするべき仕事の性質に変化をもたらし、これが新たなヒューマンエラーの発生につながるという、いわゆる supervisory control の問題点が懸念されるようになった。要するに自動機械には普段人間にはすることがないから機械がブラックボックス化する。しかしそれでは機械が故障し、人間が代わりに対応しないといけないような状況になると人間はうろたえるだけで適切に対応できなくなる。それではだめだと、滅多に起こらないのに万一の自動系故障の事態発生に備えて運転員はいつも訓練しなければならない。ironies of automation という言葉で 1980 年代の欧州の応用認知心理学者たちが指摘した問題である。その後プロセスシステムの認知工学という名前で認知科学の応用が 90 年代以降世界中で大きく取り組まれた。

認知工学には多様な側面があるが、ここではあらゆる運転モードに対してどのように自動支援系を組み込めば人的要因の観点からより望ましくなるかについて、最近進展の著しい高度情報技術の活用に着目した。具体的には現場運転員自身が日常的にそのような IT 技術を活用して使命を達成できるにはどのような支援技術が求められるのかを研究課題とした。本稿ではその第一歩として、人間―自動系相互作用の新たな設計評価法としてプラントの事故解析シミュレーションとプラント DiD リスクモニタとの統合を検討した。

4.2 人間―自動系相互作用の新たな設計評価法

人間―自動系相互作用の新たな設計評価法創出の第 1 歩として、ここでは特にプラント事故時の運転員支援のための異常監視・診断・対応操作教示機能を持つヒューマンインタフェースシステムを具体的対象に、プラントの事故解析シミュレーションとプラント DiD リスクモニタとを統合した人間―自動系相互作用の設計評価環境の構成を検討した。

4.2.1 その構成手順

異常監視・診断・対応操作教示機能を持つヒューマンインタフェースシステムは、概念的には Fig. 7 のように図示できる。図中、左側上部にはプラント計装系のセンサー信号がプラント状態を監視・診断するための入力処理部(ブロック A) とモニタした信号の表示と制御操作のための出力処理部 (ブロック B) に送信される。ブロック B では運転員への監視信号の表示、操作指示情報の提示、運転員からの操作入力を取り扱うヒューマンインターフェース部以外にプラント制御安全装置を直接制御する信号を生成する。そしてブロック A とブロック B の間がプラントの状態診断と対応手順の対応およびヒューマンインタフェースへのメッセージ生成にかかわる高度情報処理の中枢部である。

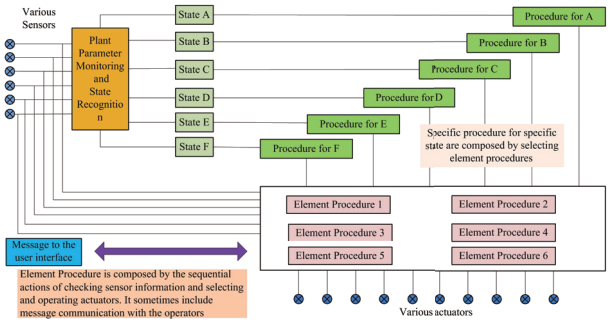

Fig. 7 Basic scheme of digital I&C + HIMT system

一方、原子力発電所の営業運転開始から最終的には廃炉処分に至るまでのプラントの全生涯で運転モードの変遷を Fig. 8 に示した。プラントの監視診断対応操作は、起動操作・出力運転・停止操作だけでなく、停止時にも必要である。また停止時に行う燃料交換や出力運転の継続に伴って炉心状態も変わるため、監視診断対応操作の仕方も調節が必要であり、トラブルや事故が発生したときにの対応の仕方もそれらの変化要因まで考慮しなければならない。

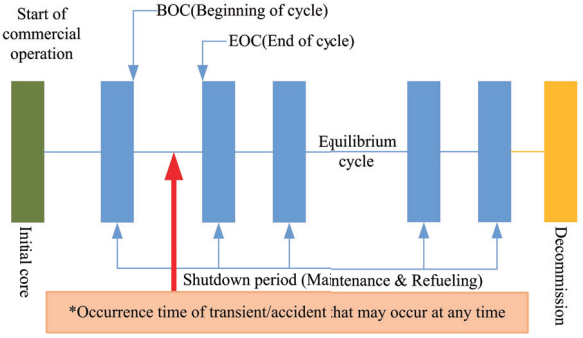

Fig. 8 Different stages of plant operation in the whole plant life

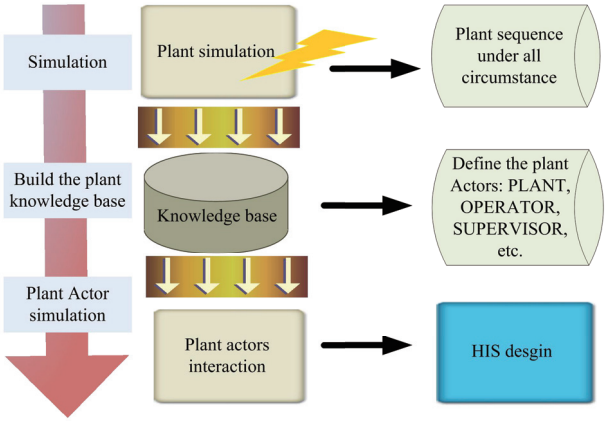

Fig. 9 Framework of integrating the simulation and knowledge based information processing

しかし実際上Fig.8に示したすべての運転モードに対してFig.7に示したdigital I&C+HMITシステムを開発することは難しい。本研究では特定の原発の定常出力運転時に特定の異常事象が生じた場合の異常監視・診断・対応操作教示機能をAI手法で構成するための手順としてFig.9に示すように,プラント事故シミュレーションと知識情報処理を組み合わせた方法として(A)事故シミュレーションの実施、(B)プラント知識ベースの作成、(C)プラントのアクター間相互作用をもとにしたHISの設計、の3段階の手順を提起する。以下それぞれの要点を説明する。

(A)事故シミュレーションの実施

原発のすべての運転モードを示したTable 1のうちシビアアクシデントは設計基準事故に含められた。そのためシビアアクシデントに至ってもプラント周辺に放射能放出に至らないように対応手順の検討の強化が求められるようになった。しかしシビアアクシデントに至りうるシナリオは無数にあり、それらを実際のプラントで試験するわけにいかない。したがってどのように事故がシビアアクシデントに進展しうるかを調べるには精度の保証された安全解析コードによる事故シミュレーションによることとなる。その際にはTable 3に示すような定常および外乱条件を考えることとなる。これを見れば特定の事故形式を考えても定常運転での炉心状態、事故が起こる際の外部要因や人的要因、共通原因要因を考慮するとそれだけでも無数のシナリオを考えた対応手順を考えねばならぬことが予想される。

Table 3 Specific aspects of plant simulation for both initial and disturbance considerations.

Assumed conditions	Selection of occurrence time for transient/accident	Remark
Initial condition	Initial Plant condition	Plant configuration based on state of plant
	Initial core condition such as fuel rod, reactor power shape, coolant condition, reactivity feedback condition, etc.	Result of SS irradiation calculation
Disturbance condition	Type of transient/accident scenario	LOF, TOP, LOCA, ATWS, etc.
	Influential factors to be assumed	External factors, human factors, common cause factors,

ここでは炉心溶融事態には発展しない範囲でシビアアクシデントを収めることに限定して多様な事故シミュレーションを実施するため多様な形式の冷却材喪失型事故を精度よくシミュレーションできるRELAP５MOD４コード[7]を用いる。

(B)プラント知識ベースの作成

プラント知識ベースの作成とは、ここではプラント事故時のマンマシン相互作用による様々な状態遷移の全体諸相をモデル化して蓄積し、情報処理することを意味する。これは(A)による多数の事故シミュレーション結果をもとに様々なマンマシンシステムの状態遷移のシナリオを、プラント自動系と人間の様々なアクター間のインタラクションの状態遷移モデルの全体系を本稿２に述べた著者らの提唱するプラントDiDリスクモニタ[8]を用いて知識ベースシステム化することに他ならない。

しかし著者らのプラントDiDリスクモニタでは人間要素の行動記述に重きを置いているので、プラント系の動作を連続系として模擬する事故シミュレーションをプラントDiDリスクモニタと連携させるには、プラントDiDリスクモニタ側にさらに次のような事項を取り扱えるように機能を追加する必要がある。

(1) プラントシステムの機能、構造に着目した階層表現（プラントアクタの階層システム化）
(2) プラントに設備された計測センサからデータ入力、アクチュエータの起動停止、人間系とのインタフェースへの入出力を取り扱う機能の追加。

上述の（１については既存のプラントDiDリスクモニタでプラントのアクタモデルを機能に応じて多重階層化すればよいが、(2)についてはオフラインでのRELAP5MOD4による計算結果の時系列データをプラントDiDリスクモニタに”実時間で”取り込むための新たな機能の追加を必要とする。

本研究では一般のオンライン系との実時間データ入出力にも対応可能なように、Fig.10に示すようなソケットインタフェースを追加して、プラントDiDリスクモニ内の種々のState Chart diagramから共通に外部とデータ授受できるようにした。

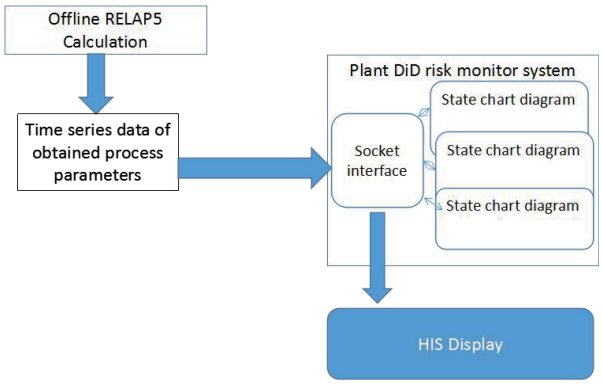

Fig. 10 Integrating accident simulation and knowledge-based information processing by plant DiD risk monitor software

(C)プラントのアクター間相互作用をもとにしたHISの設計

事故シミュレーションデータをもとにプラントアクタ間の相互作用を、ソケットインタフェースを追加したプラントDiDリスクモニタで実行させるには、とくにRELAP5MOD4コードによって得られた不均一な時間刻み幅のプロセス時系列データを、時間刻み幅が一定した実時間センサーデータに変換して用いるために次のような前処理が必要である。

(1) RELAP5MOD4コードによる計算データを一定時間幅のデータに変換したものを“真のプロセスパラメタ”とする。

(2) その”真のプロセスパラメタ”をセンサが測定してセンサーデータとしてモニターされる部分では、さらに計測系の原理や構成によって生じる時間遅れ効果やノイズ成分の重畳、運転持続によって生じるセンサードリフトを補正する必要がある。

(3) プロセス制御安全系が生成するWarningやAlarmメッセージさらには自動スクラムの動作は、プラントの運転状態の危険度に応じて設定されている閾値にセンサー値が達すると発出されるようになっている。プラントDiDリスクモニタでもプラント運転条件に応じてこれらの閾値設定を調整する必要がある。

次にHISの設計では、画面の目的、用途に応じて誰にどれだけ情報提示するべきか、予め考慮する必要がある。とくにヒューマンエラー防止のため、人間要素の排除をうたい文句にした受動安全や自動系を多用するプラントは、その設計が効果を発揮すれば発揮するほど、何が起こっても機械が自分で対処してくれるという妙な依存心を人間に植え付けるので、その結果として運転員全体のsituation awarenessを劣化させる恐れがある。Endsleyは、運転員がPerception, Recognition, projectionの３つのレベルのsituation awarenessを維持することの重要性を指摘した[9]が、本研究ではこのsituation awarenessの維持向上の観点から如何にHISを設計すべきか、が大きな課題と考えた。

4.2.2 AP1000のSBLOCA時自動安全系のHIS設計への適用性検討

本節では受動安全概念と自動系を積極的に採用した3.5世代PWRであるAP1000[10]をケーススタデイの対象とする。Fig.11に安全系を含めたAP1000のプラント構成を示す。AP1000は現在米国および中国で建設中であり、いずれもデイジタル計測制御系を採用している。中央制御室の要員構成ではとくに重大事故時のプラント運転の指揮は、世界標準になっているShift technical adviser (STA)ないし安全技術者が行うものとして、STA用の重大事故時運転支援用HISの設計問題を、ここでのプラントDiDリスクモニターの応用対象とする。

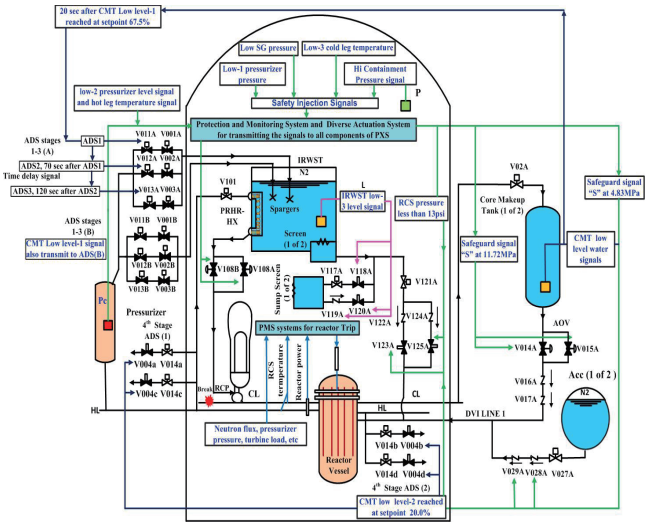

Fig.11 Plant configuration of AP1000

ここではフィージビリテイスタデイとしてA炉心溶融事態に発展しうるAP1000の小破断冷却材喪失事故(SBLOCA)に対する事故シミュレーションをRELAP5/MOD4コードにより行った。SBLOCA事故時に順次自動的に起動する安全系がすべて起動条件通りに正しく作動する場合をシナリオ１とし、一方、シナリオ１の進行中にそれぞれの安全系が故障する場合を含めて全部で８通りの事故シナリオをRELAP5 MOD4で計算した。[11]Fig.12にその８通りの事故シナリオを示す(注:特定の安全系が作動しないシナリオでは、その後の安全系は故障せずに作動するとしている)。これらの８つのシナリオのうち原子炉停止系が作動しないシナリオ２ (ATWS)とADS１～３が開かないシナリオ５では作動が回復しないと炉心溶融事態に発展する恐れがある。

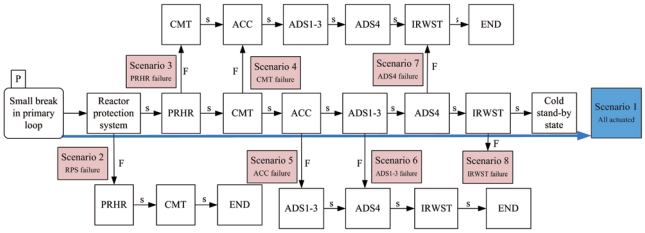

Fig.12 8 scenario of SBLOCA in AP1000

Fig.13にはSBLOCA時にすべての安全系が想定通り作動して安定に事故が収束できるシナリオ1と、SBLOCA時に炉停止系が不作動のATWSシナリオ2の場合の原子炉圧力値の時間変化計算値を示す。シナリオ2ではSBLOCAによる初期の急速減圧事態でCMTによる注水は働くが炉圧が上昇し、すべての注水機能が作動できずに高圧を維持されたままで炉心は急激に溶融事態に向かう。

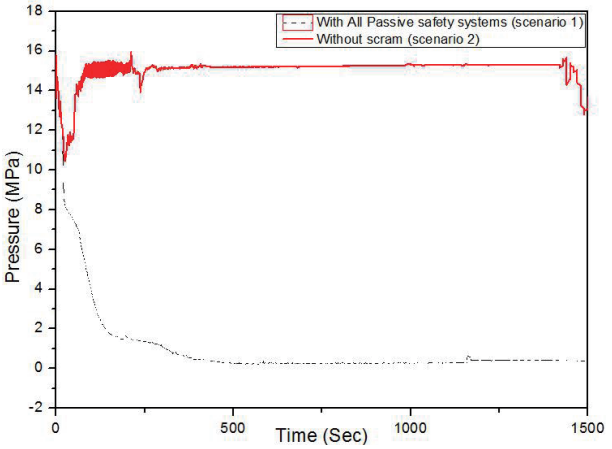

Fig. 13　Time changes of reactor pressure both in scenario 1 and 2.

さてここで注意すべきは、SBLOCA の RELAP5MOD4 コードによる事故シミュレーションはSBLOCA の発生場所と大きさを仮定して過渡計算を行ない、事故中に作動する各種安全系作動の有無も仮定した計算であって、実際のプラントでの事故発生事態とは全く違っている。実際のプラントでは、大抵は正しく運転を保っていて、いつ SBLOCA が起こるかわからない。そもそも決められた時間にきちんと事故が起こるわけでない。また事故があってもなにも SBLOCA だけが起こるわけでないし、たとえ SBLOCA が起こっても同じ場所で同じサイズの破断が起こるわけでない。

従って STA 用の HIS には、まず正常の運転状態であることがきちんと知らされ、そこに正常ではない事態が生じたとしてその後各種のアラームなどが出されてついには安全系が次々と動き出す様子を正しく知らせてくれることが期待される。これによって STA は異常事態になったという第一のレベルの perception が働くのである。そして次々に続く報知によっていったい何が起こったのかを理解できるようになる。これが situation awareness のレベル２の understanding である。それから次にこの事態を放置していたら一体どういう事態に至るかを先読みして、事態をさける手段をとるようにする。これが situation awareness のレベル３である。

本研究では、はじめはシナリオ１の想定通りに進行していたが ADS1~3 が開いていないと運転員から STA が聞いて、運転員に ADS１～３の弁開を命じたことで炉心溶融の恐れのあるシナリオ５に行かずにもとのシナリオ１でおさまった時の、プラント DiD リスクモニタが生成した相互作用の結果をシーケンスダイアグラムとして Fig. 14 に示した。

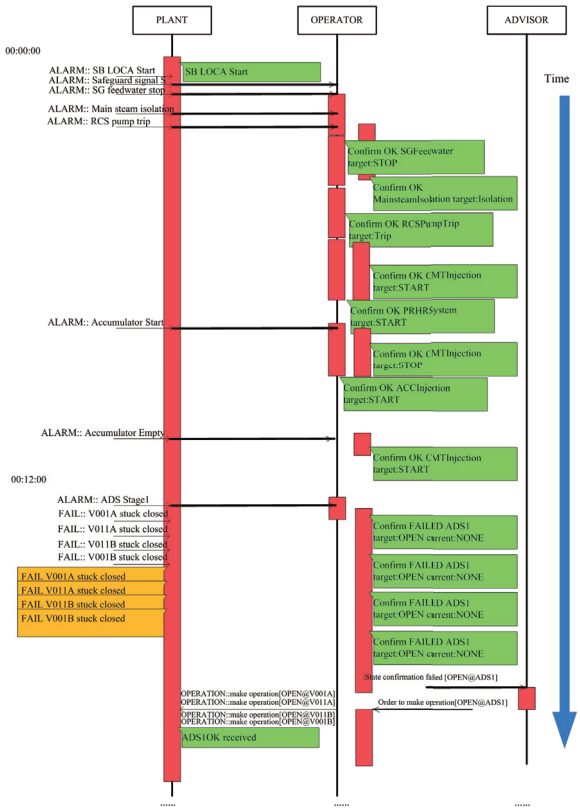

Fig. 14　Result of sequence diagram for scenario 1

Fig 14 のシーケンスダイアグラムでは、STA は運転員から ADS１～３が開いていないという報告を聞いてそれはまずい、閉めなさい、と命じて事なきをえたわけだが、STA には Fig. 15 に示すようなデイスプレイでプラント DiD リスクモニターの分析した状況を一覧できるならオペレータからの報告がなくても多様な事態へ的確な対応ができるだろう。もちろんそのためには莫大な事故シナリオに対する RELAP5MOD４コードによる事故シミュレーションを実施してそれをもとに実効的な実時間プラント DiD リスクモニタにするためには特段の工夫が必要であり、これが本テーマの実用化で最も大きな課題である。

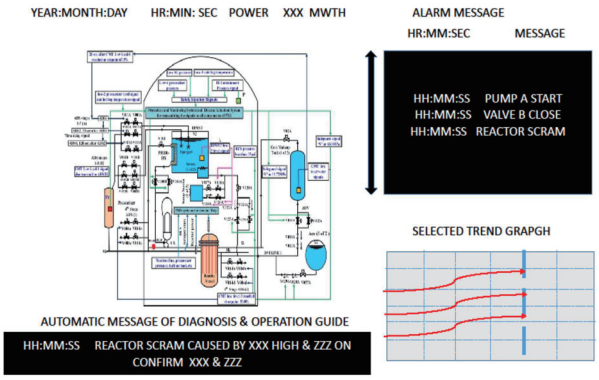

Fig. 15 Condensed information display for STA.

５．結論

本稿では著者らの開発したプラントDiDリスクモニタの基本的概念とソフトウエア構成を紹介し、とくに原発のシビアアクシデント対応に関するその応用事例としてプラント緊急事態対応シナリオの分析への応用を紹介するとともにAP1000の事故時対応のための支援インタフェース構成への応用を将来展望した。

参考文献

[1] YOSHIKAWA, H. and NKAGAWA, T.: Software system development of NPP plant DiD risk monitor -basic design of software configuration-, (ICONE23-1312) Proceedings of the 23th International Conference of Nuclear Engineering (ICONE23), May 17-21, 2015, Chiba, Japan, 2014.

[2] MATSUOKA, T.: System Reliability Analysis Method GO-FLOW for probabilistic Safety Assessment, CRC Sogo Kenkyusho, 1996. (In Japanese).

[3] YOSHIKAWA, H., *et al.* A new functional modelling framework of risk monitor system, Nuclear Safety and Simulation, Vol. 4, No. 3, pp.192~202, 2013.

[4] Object Management Group: UML Version 2.4 Specification, http://www.omg.org/spec/UML/2.4, November 201

[5] Eclipse foundation: Eclipse IDE for Java Developer Version: Luna (4.4.1), http://www.eclipse.org, 2014.

[6] Eclipse foundation: GEF(Graphical Editing Framework) Release 3.9.101, https:// eclipse.org/gef, 2014.

[7] RELAP5 Code Development Team, RELAP5/MOD3.3 Code Manual: NUREG/CR-5535, US Nuclear Regulatory Commission, Washington, DC, USA, 2001.

[8] YOSHIKAWA, K., NAKAGAWA, T. Development of plant DiD risk monitor system for NPPs by utilizing UML modeling technology, USB Proc. IFAC HMS 2016 in Kyoto, August 30-September 2, 2016, Kyoto, Japan.

[9] Endsley MR, Kaber DB, Level of automation effects on performance, situation awareness and workload in a dynamic control task. Ergonomics. 1999; 42: 462-492.

[10] Westinghouse Electric Company LLC., http://www.westinghousenuclear.com/New-Plants/AP1000-PWR/Safety/Passive-Safety-Systems (Accessed on May 18, 2017)

[11] Nawaz A, Yoshikawa H, Yang M, Hussain A: Comparative analysis of AP1000 reactor during SBLOCA with and without reactor SCRAM using RELAP5 MOD4, 8th International Symposium on Symbiotic Nuclear Power Systems for 21st Century, September 26-28, 2016, Chengdu, China.