巻頭論文

発電プラントを支える計装制御システム技術


武田保孝*　石原　鑑**

Instrumentation and Control System Technologies for Power Plant

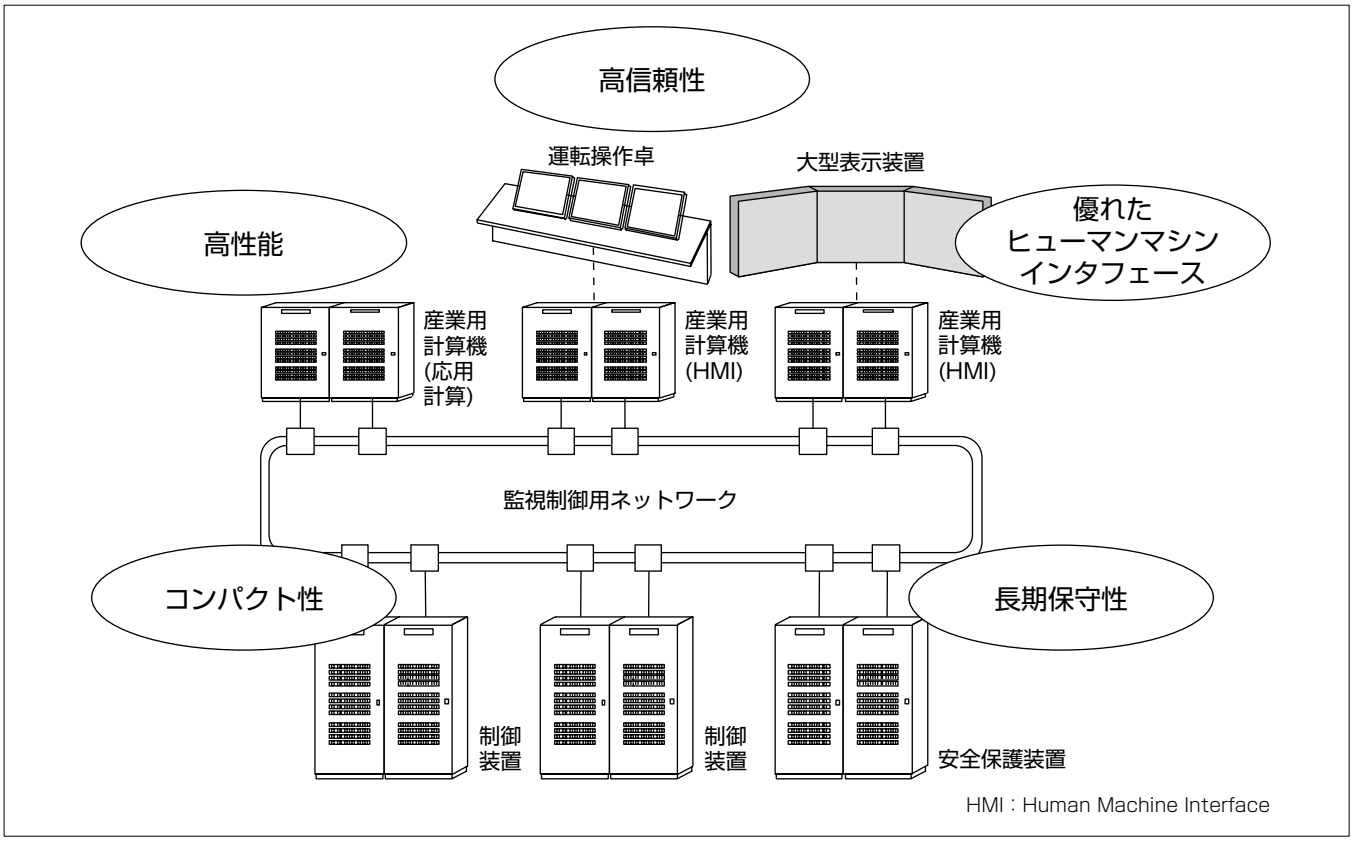
Yasutaka Takeda, Akira Ishihara

要　旨

生活水準の向上や高度情報化社会の進展によって，エネルギー消費全体における電気エネルギーの重要性は高まり続けている。電力供給に関わる計装制御システムは監視の連続性，制御の安定性等，電力安定供給に対する重要な役割を担ってきており，発電プラントの効率的運用が一層求められる中で，その果たす役割も拡大している。計装制御システムは発電所設備の一部として，堅牢(けんろう)，効率的かつ人に優しいシステムを実現することが必須となっている。

そのため，発電プラント向け計装制御システムには安定した連続運転を実現する，高いシステム信頼性，処理性能等が要求され，プラントを運転する人間が使いやすい優れたヒューマンマシンインタフェース設計が求められる。加えて，20年を超えるプラント寿命に対応した計装制御システムの長期保守性，装置のコンパクト性等も求められる。三菱電機では，これらの要求を満たす発電プラント向け計装制御システムの開発を進めている。

この特集号では，火力発電プラント向け計装制御システム“MELSEP5”，発電プラント向け新計装制御システムプラットフォーム，原子力発電プラントの新規制基準に対応した技術開発，米国や中国の原子力発電プラント向け計装制御システム等，具体的な開発事例を通じて当社の取組みについて述べる。



発電プラント向け計装制御システム

重要な社会インフラ設備である発電プラントの計装制御システムには，高性能，高信頼，優れたヒューマンマシンインタフェース，長期保守性，コンパクト性等の要求がある。計装制御システムを構成する個々のコンポーネントである，制御装置，監視制御用ネットワーク，産業用計算機にはこれらの要求を実現するための様々な技術が実装されている。

*先端技術総合研究所 システム技術部門 部門統括　**同研究所 ソリューション技術部長(博士(工学))

1. まえがき

電力は我々の社会，経済活動を支える重要なインフラである。資源エネルギー庁の電力調査統計では，2012年度の発電量実績は約8,200億kWhであり，原動力別で火力，原子力，水力でその99%以上をカバーしている。したがって，電力の安定供給のためには，発電プラントの安定した稼働が必要不可欠である。

発電プラントは，燃料から熱エネルギーを取り出す熱源機器(ボイラ，原子炉)，熱などのエネルギー源を機械エネルギーに変換する原動機(ガスタービン，蒸気タービン)，機械エネルギーを電気エネルギーに変換する発電機などの機器と，発電プラントの神経網としてこれらの機器を監視制御する計装制御システムから構成される。発電プラントは社会インフラ設備として連続した安定運転が要求されるため，その設備の一部である計装制御システムにも高い信頼性が要求される。またプラントを運転する人間に対しても使いやすく，ヒューマンエラーに配慮したヒューマンマシンインタフェース設計が求められる。

経済産業省などの予測では，我が国のエネルギー需要は今後緩やかに頭打ちとなるとされている。発電プラント向け計装制御システムを発展させていくためには，国内だけでなく海外でのビジネス展開が必要になると考えられる。海外市場では，当該国の基準，規格に加え国際的な基準，規格への適合が求められ，要求事項に対応した取組みが必要となる。

本稿では，これらの種々の要求を満たすための発電プラント向けの計装制御システム技術の動向を概観し，当社の取組みについて述べる。

2. 計装制御システム技術の動向

2.1 計装制御システムの進化

計装制御システムは，プラントから温度，圧力，流量等に代表されるプロセス情報を収集し，ポンプ，弁等の機器の制御を行う。加えて，運転員へプラント監視，操作のための機能を提供する，いわばプラントの神経系統をつかさどるシステムである。

現在の計装制御システムは，1970年代に開発された分散型制御システムDCS(Distributed Control System)を原型としている。DCSは分散された機能間を通信によって結合するという概念を実現したシステムであり，プラント機器の監視制御を行う制御装置，データの加工，ロギング，性能計算等を行い，運転員へ監視操作機能を提供する産業用計算機，及びこれらを結ぶ制御用ネットワーク等から構成される。

制御装置，産業用計算機のキーコンポーネントであるマイクロプロセッサは1970年以降現在に至るまで高性能化が進んでいる。マイクロプロセッサのアーキテクチャ及び集積技術の進歩に伴い，演算で一度に扱えるデータ量は8ビット，16ビット，32ビット，64ビットと増加している。近年では，2つ以上のプロセッサコアを1つのパッケージに集積したマルチコア型のマイクロプロセッサが主流となりつつある。メモリ容量もKバイトオーダーからGバイトオーダーに大容量化し，システムの実行速度を決めるクロック周波数もMHzオーダーから数GHzオーダーへと高速化している。これらコンポーネントの進化に伴い制御装置，産業用計算機ともに高性能化しており，制御装置の性能向上に伴う装置台数の削減，装置のコンパクト化，システムの多重化による信頼性向上等が進んでいる。

制御用ネットワークは，信頼性，リアルタイム性の要求を満たしつつ制御装置と産業用計算機間のデータ伝送を行う。制御用ネットワークの通信速度は，汎用ネットワーク技術をベースに数kbpsから100Gbpsへと高速化が進んでいる。制御用ネットワーク独自の信頼性，性能要求を満たすための機能として，ネットワークの二重化，リアルタイムデータ伝送等の手法が発達してきている。

2.2 計装制御システムへの要求

発電プラント向け計装制御システムには，高性能，高信頼性，長期安定性，コンパクト性，運用・メンテナンスの容易性，使いやすいヒューマンマシンインタフェース等が求められ，近年ではサイバーセキュリティへの対策も求められている。

発電プラントでは，数万点のデジタル情報，アナログ情報を数ミリ秒から数100ミリ秒で処理することが求められる。運転員に対してはプラント運転状態，警報等の情報提供，プラント機器に対してはPID(Proportional Integral Derivative)制御などを行う。これらの処理をプラント運転中は間違いなくかつ連続して行うため，システム全体として高い信頼性が求められる。また，装置が故障しても影響が広がらない独立性の確保などが求められる。

一般に発電プラント自体の寿命は20年以上であり計装制御システムの長期の安定性が求められるとともに，ICT(Information and Communication Technology)機器の寿命などを考慮して容易にシステム・装置の更新が行えることが求められる。また計装制御システムの設置スペースの問題から装置のコンパクト性も求められる。

プラント運転では，運転員の情報の誤認識，誤操作がプラント運転に重大な影響を与える可能性がある。また計装制御システムの効率的な運用を支援するためには，制御システム全体，ネットワーク，装置個々の動作状態の可視化機能が必要となる。そのため，人間にとって分かりやすく使いやすい，ヒューマンマシンインタフェースが必要とされる。

発電プラント向けの計装制御システムは，通常ルータや

ファイアウォールなどのセキュリティ機器によって外部のネットワークからは遮断されているが，コンピュータウイルスStuxnetの出現[1]によって，サイバーセキュリティへの対策が求められている。Stuxnetはウイルス伝播（でんぱ）の形態として，ネットワークだけでなくUSB（Universal Serial Bus）メモリによっても媒介され，スタンドアロンのネットワークに対しても侵入可能である点が脅威である。そのため，計装制御システムにおけるサイバーセキュリティの必要性が強く認識された。

2.3 計装制御システム技術と当社の取組み

2.3.1 全体システム構成

代表的な発電所向け計装制御システムの構成を**図1**に示す。計装制御システムを構成する装置としては大きく2種類に分けることができる。1つは制御・安全保護装置で，プラントの監視制御に必要なプロセス情報をセンサから取り込み，プラントを制御するための演算処理を行い，種々のアクチュエータ，プラント機器へ動作指令を出力する。制御装置は，通常の発電プラント運転に必要な圧力制御や流量制御といったプラントの制御を行い，安全保護装置は発電プラントを安全に停止させる。

もう1つは産業用計算機と呼ばれるもので，プラントから収集したデータの加工，ロギング，性能計算等，種々の応用計算処理を行う。さらに，産業用計算機は運転員へのプラント監視情報の提供，プラント機器操作等のヒューマンマシンインタフェースをつかさどる。

制御・安全保護装置と産業用計算機を接続し，相互のデータ通信を行うために監視制御用ネットワークが設けられている。また，計装制御システムの保守，メンテナンスを行うために保守用ネットワークが設けられている。

これらが計装制御システムの基本構成である。個々の制御・安全保護装置，産業用計算機はそれぞれの果たす機能の重要度に応じ，シングル構成，二重化構成，複数分散構成等がとれるようになっている。次に計装制御システムの主要な構成要素とエンジニアリング環境，ヒューマンマシンインタフェース，サイバーセキュリティについて述べる。

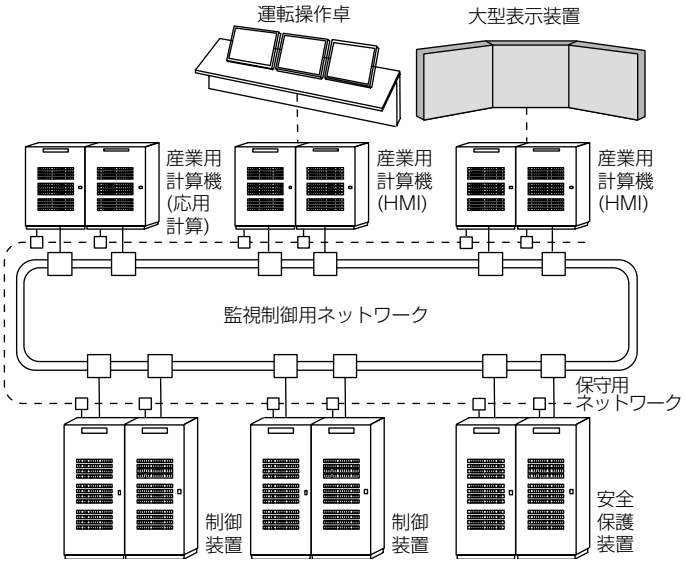


図1．発電所向け計装制御システムの構成

なお，当社最新の火力発電プラント向け計装制御システムの全体像は，この特集号の“火力発電プラント向け計装制御システム“MELSEP5””（p.7）で詳しく述べている。

2.3.2 制御・安全保護装置

制御・安全保護装置は，プラントからの種々のデータを取り込み，産業用計算機からの設定に基づいた制御演算を行い，制御指令をアクチュエータへ出力する装置である。

制御・安全保護装置は，計算処理を行うCPUカードとプラント側に設置されたセンサやアクチュエータとの入出力を行うIOカード等で構成する。それぞれのカードは，装置の重要度から要求される信頼性を実現できるように，シングル構成，二重化構成等がとれるようになっている。また信頼性確保のためにRAS（Reliability Availability Serviceability）機能が搭載されている。

当社の最新型の制御装置では，CPUとして初めてマルチコアプロセッサを採用し高性能化を図っている。マルチコアを有効に活用するため，1台の制御装置の中で仮想的に複数の制御装置が動作できるように制御用モニタを新たに開発した。制御用モニタ上ではOS（Operating System），アプリケーションである制御演算ロジックを，リソースを意識することなく，複数台分動作させることが可能となっている。また，制御装置内のシステムバスも従来のパラレルバスからシリアルバスへの変更を行い性能向上を図っている。

さらに，信頼性向上策の一環として一過性異常に対するリカバリー機能を強化している。一過性異常は，メモリ上のデータが宇宙線などによってデータ反転を起こすSEU（Single Event Upset）現象や外来ノイズ・静電気等によって，システム内のデータが一時的に異常になる現象である。リカバリーの対象としたのはメモリとシステムバスである。メモリは，ECC（Error Checking and Correction）による自動修復，CRC（Cyclic Redundancy Check）値／チェックサム値等によるデータ健全性のチェックとエラー検出時のデータ再送等の方法を採用している。システムバス上のデータは，シリアルバス上のデータパケット単位でのCRC値チェックと再送機能を実装することでリカバリーを実現している。リカバリー機能を強化することで一過性異常が発生しても，待機系へ切り替えることなく制御装置の運転が継続できるようになっている。

2.3.3 産業用計算機

発電プラントなど社会インフラ設備の監視制御に適用されるコンピュータは産業用計算機と呼ばれ，パソコンと比較して高品質，高信頼，故障解析の容易性といった要求を

実現するため，ハードウェア及びソフトウェア面での様々な強化が図られている。当社では，OSレベルでの故障解析を容易化するため，OSとしてリアルタイム処理などを強化したLinux(注1)や制御用RTOS(Real Time Operating System)を採用している。信頼性を高く保つためにRAS機能を持たせている。さらに，マルチコアCPUを適用する際にも単に処理性能を高めるだけでなく，信頼性を強化する方式を組み込んでいる(2)。

(注1) Linuxは，Linus Torvalds氏の登録商標である。

2.3.4 監視制御／保守用ネットワーク

発電プラントの計装制御システムでは，リアルタイムにプラントの監視制御を行うための監視制御用ネットワークと制御装置や産業用計算機の保守，メンテナンス用に使用される保守用ネットワークの2つがある。

監視制御用ネットワークには，リアルタイム性，高信頼性，対故障性が要求される。そのため当社では，通信の物理媒体としては光ファイバを用い，通信プロトコルとしては定期的にデータ伝送を行うサイクリック通信方式を基本方式としている。また，故障時に短時間でのシステム復旧を実現するため，IEEE802.17 RPR(Resilient Packet Ring)などの技術を適用している(3)。保守用ネットワークとしては，リアルタイム性が要求されないため，一般産業用途で広く使われているTCP/IP(Transmission Control Protocol/Internet Protocol)プロトコルなどを採用している。

2.3.5 エンジニアリング環境

制御装置に搭載する制御ロジックは，POL(Problem Oriented Language)と呼ぶ図的な形式の言語を使用し，個別の制御機能を持つ要素を図的に結合することで記述している。制御ロジック図の作成，プログラムやデータへの変換は専用ツールで行い，これを制御・安全保護装置へローディングして使用する。また，産業用計算機のソフトウェアは，構造としてOS層の上にミドルウェアと呼ぶアプリケーションソフトウェアの共通的な機能を集めた層があり，その上でアプリケーションソフトウェアが動作する形となっている。アプリケーションソフトウェアは基本的にはプラントごとには改変をなるべく行わず，プラントごとの差異はデータ部分で吸収するような構成となっている。アプリケーションソフトウェアの一部は，制御装置用のPOLと同様に図的な形式でその処理を記述している。

これら計装制御システム用のプログラムやデータを構築するツール群を総称してエンジニアリング環境と呼んでいる。データの構築を効率的に行うため，エンジニアリング環境のツール群はWindows(注2)を搭載したパソコン及び産業用計算機上で動作するようにしている。エンジニアリング環境内のツールは，ソフトウェア開発のV字モデルに適合するように，仕様の策定，詳細化，製作，単体試験，組合せ試験等のフェーズを連携してカバーする。

当社の最新型の監視制御システムでは，制御装置向けのPOLと産業用計算機向けのPOLのエンジニアリング環境を統合し，統合データベースによってシステム全体の情報を一元管理し，ツール間の相互連携を図っている。また，監視制御システム自体の構成も図的に定義してシステム管理を行うツールを提供している。さらに，プラント運転時にシステム運用を支援するためのツールとして，制御装置の制御ロジックの動作状態を表示するロジックモニタ，監視制御システム自体の動作を表示するシステムモニタ等の機能を実装している。

(注2) Windowsは，Microsoft Corp. の登録商標である。

2.3.6 ヒューマンマシンインタフェース

発電プラントの制御室に設置される計装制御システムのヒューマンマシンインタフェースとしては，個人用に複数のディスプレイ，運転チーム全体での情報共有用に大型表示装置を設置し，入力デバイスとしてはタッチパネル，マウス等を用いたシステムが標準的な構成となっている。

大規模プラントでは，監視操作のための対象が非常に多く，直接オペレータが把握することは難しい。そのため，計装制御システムの大きな役割の一つが，プラントの情報を集約しオペレータに提供すること，またオペレータ指示をプラントに伝えることである。

当社では，様々な観点から計装制御システム向けのヒューマンマシンインタフェースの研究開発に取り組んでいる。一例として，これまでの計装制御システムでは，制御室でプラントの運転操作を直接担当する運転員への支援が中心であったが，制御室で運転員を統括・管理する監督者の支援が必要であると考え，監督者支援のため，運転員の操作履歴を状況に対応した詳細度で提示するインタフェースを提案している(4)。また，コンピュータやスマートフォン等のICT機器の普及によって，ユーザーのコンピュータリテラシが向上しており，モバイル機器の発電プラントでの利用，ユニバーサルデザインのヒューマンマシンインタフェース設計への反映等を進めている。

なお，**2.3.2項**から**2.3.6項**までで述べた技術の当社の最新状況はこの特集号の“発電プラント向け新計装制御システムのコンセプト”(p.11)，“発電プラント向け新計装制御システムの要素技術”(p.15)で詳しく述べている。

2.3.7 サイバーセキュリティ

発電プラント向けの計装制御システムは，一般的に外部のネットワークからは遮断されている。それでも，プラントの安全をつかさどる安全保護システムを始めとした計装制御システムを構成する装置は，考えられる侵入手段から確実に保護されなければならない。サイバーセキュリティの観点からは，これらの装置に対する正当なアクセスを保証することと権限のない不正なアクセスを阻止することが必要となる。

サイバー攻撃における脅威としては，次の4つのカテゴリーを考慮するべきであるとされている。

(1) 情報への権限のないアクセス
(2) 情報，ソフトウェア，ハードウェアの遮断や改変
(3) データの伝送回路の遮断・システムの中断
(4) データ通信システムや計算機への権限のない侵入

サイバーセキュリティにおける課題は，計装制御システムが複雑になることによって，重要な脅威を取り込んでしまう可能性が排除できなくなることである。

当社では，脅威を識別して障壁を構築するツールとして，侵入検知やウイルススキャン，暗号化などのツールや，セキュリティ上安全が保証される領域の設定，アプリケーションやセキュリティ管理システム，セキュア・ゲートウェイとしてデータダイオード方式を適用したシステムを構築することで，発電プラント向けのサイバーセキュリティの確立に努めている。サイバーセキュリティへの当社の最新の取組み状況は，この特集号の“原子力プラントの安全対策に向けた技術”(p.19)，“米国原子力プラント向けデジタル計装システムの規制対応活動”(p.23)で述べている。

2.4 グローバル化に向けた当社の取組み

計装制御システム事業を海外展開するためには，当該国で定めている関連規格への対応が必要となる。当社では，2007年から原子力発電プラント向けの安全保護装置及び中央制御室のヒューマンマシンインタフェース設計を対象として，米国での設計認証取得活動を進めている。認証取得でキーとなる規格基準としては，産業用計算機のヒューマンマシンインタフェース設計が関連する制御室設計と，制御・安全保護装置に関するものがある。

制御室設計では，米国の規格であり国際的にデファクトスタンダードとなっている米国原子力規制委員会が定めるNUREG-0700[5]，NUREG-0711[6]がある。NUREG-0700は中央制御室におけるヒューマンマシンインタフェース仕様の審査指針を定めたものであり，NUREG-0711は中央制御室に設置される計装制御システム全体の設計，開発，評価，実装の全ライフサイクルにわたる開発プロセスの要求事項を定めている。

計装・安全保護装置関連では，原子力発電所の計装制御システム全体の標準審査指針を定めたNUREG-0800[7]の7章がある。そこでは，原子炉停止システム，工学的安全システム等，安全上重要な個別システムが満たすべき要件を定めるとともに計装制御システムの製品ライフサイクル全般にわたる要求も規定している。

具体的な認証取得活動としては，審査で要求される種々の申請資料を整備し提出，規制当局の承認を受ける。特にヒューマンマシンインタフェース設計では，米国内に検証設備を構築し，米国電力の運転クルー協力のもと，プラントシミュレータと組み合わせ動的な検証評価を行い，評価結果を申請資料として提出している[8]。

米国向け計装制御システムの最新の状況は，この特集号の“米国原子力プラント向けデジタル計装システムの規制対応活動”(p.23)で述べている。また，計装制御システムの中国向け仕様策定，規制・規格準拠活動は“中国CPR1000型原子力発電所向け計装制御設備の実現”(p.27)で述べている。

3. むすび

発電プラントを支える計装制御システム技術の動向を概観し，当社における取組みの概要について述べた。具体的な取組みの詳細については，この特集号の各論文を参照いただきたい。

発電プラント向け計装制御システムには堅牢で，効率的かつ人に優しいシステムを実現することが求められる。今後もシステム技術とヒューマンファクタの観点から，より優れた計装制御システムを構築するための研究開発を進める。

参考文献

(1) (独)情報処理推進機構(IPA)セキュリティセンター：2010年度 制御システムの情報セキュリティ動向に関する調査報告書，IPA報告書（2011）
(2) 井登純一，ほか：産業用計算機のマルチコアCPU適用，三菱電機技報，**84**，No.10，562～565（2010）
(3) 増濱和生：発電プラントにおける監視制御用ネットワーク，三菱電機技報，**81**，No.10，708～711（2007）
(4) Kagimoto，M.，et al.：Development of a shift supervisor support system for power plants，Proceedings of first international symposium on socially and technically symbiotic systems，36_1～36_6（2012）
(5) US-NRC：Human-system interface design review guidelines，NUREG-0700 Rev. 2（2002）
(6) US-NRC：Human factors engineering program review model，NUREG-0711（Rev. 2）（2004）
(7) US-NRC：Standard review plan for the review of safety analysis report for nuclear power plants：LWR edition，NUREG-0800，Chapter 7，Rev.5（2007）
(8) 北村雅司，ほか：米国向け中央計装運転検証設備及び型式認証活動，三菱電機技報，**84**，No.10，542～545（2010）