JAERI-Review
98-013

原子力発電プラントにおけるディジタル計測制御系の安全性及び信頼性に関する課題と米国原子力規制委員会の対応（調査報告書）

1998年9月

渡辺憲夫・鈴土知明

日本原子力研究所
Japan Atomic Energy Research Institute

本レポートは，日本原子力研究所が不定期に公刊している研究報告書です。
入手の問合わせは，日本原子力研究所研究情報部研究情報課（〒319-1195　茨城県那珂郡東海村）あて，お申し越しください。なお，このほかに財団法人原子力弘済会資料センター〒319-1195　茨城県那珂郡東海村日本原子力研究所内）で複写による実費領布をおこなっております。

This report is issued irregularly.
Inquiries about availability of the reports should be addressed to Research Information Division, Department of Intellectual Resources, Japan Atomic Energy Research Institure, Tokai-mura, Naka-gun, Ibaraki-ken 319-1195, Japan.

編集兼発行　　日本原子力研究所

JAERI－Review 98－013

原子力発電プラントにおけるディジタル計測制御系の安全性及び信頼性に関する課題と米国原子力規制委員会の対応（調査報告書）

日本原子力研究所東海研究所安全性試験研究センター原子炉安全工学部
渡辺　憲夫・鈴土　知明

（1998年8月19日受理）

近年、各国において、原子力発電プラントの計測制御系にディジタル技術が導入されつつある。しかし、ディジタル技術の導入に伴い、設計、施工、安全及び許認可に関する新たな問題も生じている。特に、ディジタル系ではソフトウェアを使用するため、従来のアナログ系には見られなかった問題がある。従って、原子力発電プラントの安全性に関して現在の高いレベルを維持あるいは向上させるためには、規制側並びに産業界は、こうした問題に対処すべく、安全評価の方法や、技術基準、規制指針等の見直しを行うことが必要となる。

こうした背景の下、原研では、9年度より、「ディジタル計測制御系の信頼性に関する調査」研究を行っている。その一環として、現在は、米国を中心に、ディジタル系に対する設計評価、技術規準、規制プロセス等について調査・分析を進めている。

本報告書では、米国研究協議会(NRC : National Research Council)が実施した調査研究の結果と、そこで提示された勧告に対する米国原子力規制委員会(USNRC : U. S. Nuclear Regulatory Commission)の見解を紹介する。NRCによる調査研究では、ディジタル計測制御技術の適用に際しての重要課題として、6つの技術的課題（ディジタル計測制御技術の系統的特性、ソフトウェアの品質保証、共通原因によるソフトウェアの故障、ヒューマンファクタ及びマンーマシン・インターフェース、安全性及び信頼性の評価方法、民生用既製品のハードウェアとソフトウェアの利用）と、2つの施策的課題（ケースバイケースの許認可プロセス、技術基盤の適性）を摘出し、それぞれについて、USNRCがどう対応すべきかを勧告として提示した。これらの勧告についてUSNRCは自らの対応見解を示し、多くの勧告については同意している。

我が国においても、今後、アナログ機器の生産量が低下するに伴い、ディジタル機器の導入は避けられない状態になるものと予想される。その際に対処できるよう基準やガイダンス等の整備・検討を進める必要があると考えられるが、本報告書で紹介した技術的課題や施策的課題及びそれに対するUSNRCの対応見解は、その検討に有用になるものと思われる。

東海研究所：〒319-1195　茨城県那珂郡東海村白方白根2-4

Review Report :

Safety and Reliability Issues on Digital Instrumentation and Control Systems in Nuclear Power Plants and United States Nuclear Regulatory Commission's Dispositions

Norio WATANABE and Tomoaki SUZUDO
Department of Reactor Safety Research
Nuclear Safety Research Center
Tokai Research Establishment
Japan Atomic Energy Research Institute
Tokai-mura, Naka-gun, Ibaraki-ken

(Received August 19, 1998)

Recently, digital instrumentation and control (I&C) systems have been applied to nuclear power plants (NPPs) in various countries. Introduction of digital I&C systems, however, raises special issues on design, implementation, safety and licensing. In particular, the use of software in digital I&C systems might introduce problems specific to the digital technology that have not been observed in the conventional analog systems. The needs to develop and update the safety evaluation approaches, technical standards/criteria, regulatory guideline/guidance, etc. to deal with such problems emerge on both regulatory and industrial basis so that the current high level of plant safety is at least maintained and preferably increased.

Since FY 1997, the Japan Atomic Energy Research Institute has been carrying out a project, Study on Reliability of Digital I&C Systems, which includes extensive reviews of design approaches, technical standards, regulatory processes, especially, in the United States.

This report summarizes the results from the study of National Research Council (NRC) and the U. S. Nuclear Regulatory Commission's (USNRC's) responses to the recommendations made by the NRC's study. That study identified six technical key issues (system aspects of digital I&C technology, software quality assurance, common-mode software failure potential, safety and reliability assessment methods, human factors and man-machine interface, dedication of commercial off-the-shelf hardware and software) and two strategic key issues (case-by-case licensing process, adequacy of technical infrastructure) that arise from the introduction of digital I&C technology and then, made recommendations to the USNRC for coping with digital I&C applications.

The USNRC responded to each recommendation and showed their own dispositions in which the USNRC agreed with most of the recommendations.

In Japan, it is expected that introduction of digital I&C technology is inevitable in NPPs because the vendors are gradually discontinuing support and stocking of analog components. To cope with such situations, there is a need to develop and update the standards and guidelines applicable to digital I&C technology. The key issues and the USNRC's dispositions provided in this report is believed to be useful for developing and updating them.

Keywords : Digital Instrumentation and Control System, USNRC, Regulatory Guidelines, Technical Standards, Review Report, Safety and Reliability

This is a blank page.

目　　次

Contents

略語リスト

ABWR : advanced boiling water reactor（新型 BWR）
ACRS : Advisory Committee on Reactor Safeguards（原子炉安全諮問委員会）
AECB : Atomic Energy Control Board（カナダ原子力管理委員会）
AECL : Atomic Energy Canada Limited（カナダ原子力公社）
ANS : American Nuclear Society（米国原子力学会）
ANSI : American National Standards Institute （米国規準研究所）
ASIC : application-specific integrated circuit（アプリケーション固有型集積回路）
BTP : Branch Technical Position（部門技術見解）
CFR : Code of Federal Regulations（連邦規制規則）
CMF : common mode failure（共通モード／原因故障）
COTS : commercial off-the-shelf（民生用既製品）
DOE : Department of Energy（米国エネルギー省）
EMI : electromagnetic interference（電磁波干渉）
EPRI : Electric Power Research Institute（電力研究所）
FAA : Federal Aviation Administration（連邦航空管理局）
FDA : Food and Drug Administration（食物薬物管理局）
FPGA : field programmable gate arrays（フィールド・プログラマブル・ゲート配列）
GDC : general design criteria（一般設計基準）
HICB : Instrument and Control Branch（USNRC の計測制御部門）
IEC : International Eelectrotechnical Commission（国際電気技術委員会）
IEEE : Institute of Electrical and Electronics Engineers（電気・電子技術者協会）
ISA : International Society for Measurement and Control, formerly Instrument Society of America（国際計測制御学会、旧米国計測学会）
ISO : International Organization for Standardization（国際標準化機構）
KAERI : Korea Atomic Energy Research Institute（韓国原子力研究所）
KINS : Korea Institute of Nuclear Safety（韓国原子力安全解析所）
LER : licensee event report（設置者事象報告書）
MMI : man-machine interface（マン－マシン・インターフェース）
MTTF : mean time to failure（平均故障時間）
NASA : National Aeronautics and Space Administration（航空宇宙局）
NRC : National Research Council（米国研究協議会）
NRR : Office of Nuclear Reactor Regulation（USNRC の原子炉規制局）
NSRRC : Nuclear Safety Research Review Committee （原子力安全研究レビュー委員会）
NUSMG : Nuclear Utilities Software Management Group（原子力利用者ソフトウェア管

理グループ）

OECD/NEA-CSNI : Organization for Economic Cooperation and Development/Nuclear Energy Agency - Committee on Safety of Nuclear Installations（経済協力開発機構／原子力機関－原子力施設安全委員会）

PLC : programmable logic controller（プログラマブル・ロジック制御装置）

PPS : primary protection system（主保護系）

PRA : probabilistic risk assessment（確率論的リスク評価）

RES : Office of Nuclear Regulatory Research（ USNRC の規制研究局）

RFI : radiofrequency interference （無線周波数干渉）

RPS : reactor protection system（原子炉保護系）

SBWR : simplified boiling water reactor（単純化 BWR）

SRP : Standard Review Plan（標準レビュープラン）

TVA : Tennessee Valley Authority（テネシー渓谷開発公社）

USNRC : United States Nuclear Regulatory Commission（米国原子力規制委員会）

USQ : unreviewed safety question（未レビュー安全問題）

V&V : verification and validation （性能及び妥当性評価）

概 要

本報告書は、ディジタル計測制御系の安全性と信頼性に関する米国研究協議会の調査研究の内容とそれに対する米国原子力規制委員会の見解を紹介するものであり、その詳細は、後続の第2章から第5章に記載する。本概要(Executive Summary)は、本報告書の要約版であり、調査研究によって同定された技術的・施策的課題の具体的内容、提言された勧告、及び、それに対する米国原子力規制委員会の対応見解を簡潔にまとめている。

はじめに

近年、欧米諸国において、原子力発電プラントの計測制御系にディジタル技術が導入されつつある。特に、カナダ、フランス、イギリスでは、最新のプラントで完全なディジタルベースの計測制御系が導入されている。米国では、過去20年間新設のプラントはないが、新型炉の設計ではディジタル計測制御系の利用を前提としている。また、既存プラントでは、これまで使用してきたアナログ機器からディジタル機器への変更が行われている。我が国においても、柏崎・刈羽-6、7号機(ABWR)で安全系にディジタル機器が使用されている。しかし、ディジタル技術の導入に伴い、設計、施工、安全及び許認可に関する新たな問題も生じている。特に、ディジタル系ではソフトウェアを使用するため、従来のアナログ系には見られなかった問題がある。従って、原子力発電プラントの安全性に関して現在の高いレベルを維持あるいは向上させるためには、こうした問題を考慮して、安全評価の方法や、技術基準、規制指針等の見直しが必要となる。

原子力発電プラントにおいてアナログ機器からディジタル機器への移行が進む最大の理由は、製造業界によるアナログ機器・部品の供給が少なくなり、品質の良い交換部品の入手が困難となりつつあることにある。従って、今後ますますディジタル機器の利用が進み、その形態も多様化することが予想される。

こうした背景の下、原研では、9年度より、「ディジタル計測制御系の信頼性に関する調査」研究を行っている。この研究では、ディジタル系、特にソフトウェアに対する信頼性評価の手順や方法を確立することを最終的な目的としているが、その第1ステップとして、現在、米国を中心に、ディジタル系に対する設計評価、技術規準、規制プロセス等について調査・分析を進めている。本報告書では、米国原子力規制委員会(USNRC)が、米国研究協議会(NRC)に委託した調査研究の結果と、そこで提示された勧告に対するUSNRCの見解を紹介する。

アナログ計測制御系からディジタル計測制御系への移行

現在、米国では、109基の原子力発電プラントが運転されているが、これらは全てディジタル技術が普及する前に設計されたものであり、アナログ式の計測制御系を前提とした設計

となっている。アナログ計測制御系は、設計上の問題や環境による機能の低下等はあったものの、モニタリング、制御及び保護機能に関し良好な実績をあげてきた。しかし、その一方で、アナログ機器の経年劣化による機械的故障等が顕在化し、また、製造業界がディジタル技術の開発に力を注いできたためアナログ機器・部品の生産量が低下すると共に予備品も少なくなり、品質の良い交換部品の入手が困難となりつつある。製造業界がディジタル技術へ移行する理由は、アナログ機器に比べて大きな利点があることにある。即ち、ディジタル機器は、アナログ機器の弱点の1つであるドリフトがなく校正の手間が省けたり、精度や計算機能の向上が図れると共に、大量のデータを格納・処理でき、プラント運転状況の表示等も容易に行える。その結果、プロセス制御の改善や、プラントの安全性向上が期待される。このため、原子力発電プラントにおけるディジタル技術の導入は避けられない状況となっている。

こうした背景の下、多くのプラントで、計測制御機器のアナログーディジタル変更（レトロフィット）が行われているが、ほとんどは、レコーダやディスプレイ等比較的規模の小さい機器単位のレトロフィットである。しかし、1990年から1994年にかけて、幾つかのプラントでは、比較的規模の大きい系統レベルでのレトロフィットが行われている。こうしたディジタル系の原子力発電プラントへの導入に際しては、幾つかの問題点も生じている。

新技術導入に特有の不確定性： 原子力発電プラントのような安全上重要な産業においては、利用者、設計者及び規制当局は、現在の高いレベルの安全性を維持あるいは向上させるよう、潜在的な危険性を取り込まずにディジタル系の導入を行わねばならない。さらに、ディジタル系に関する設計、評価及び規制アプローチでは、安全裕度を評価する手段も提示しなければならない。

アナログ系の実績から得た既存技術基盤の移行： 原子力発電プラントの設計及び運転に関する経験の多くはアナログ技術に基づくものである。従って、ディジタル技術に起因する不確定性の取扱いに加えて、技術支援体制や規制の枠組も変更する必要がある。

ディジタル計測制御系の導入に伴う技術的問題： アナログ式とディジタル式の計測制御系における相違点により、ディジタル計測制御系の導入に際しては以下のような技術的課題が派生する。

- ソフトウェアの共通原因故障
- 民生用ハードウェア及びソフトウェアの利用
- 新技術に関するプラント内使用実績の欠如
- 構成管理
- 複雑さの増加によるプログラミングエラーや不正出力
- 標準的なソフトウェアツールの信頼性
- 環境耐性（電磁波干渉、周波数干渉、温度、接地、煙等）
- プラントの安全裕度への影響

許認可アプローチ上の問題： 一般に、新たな規制基準を策定し文書化するには長い期間を

要するため、規制プロセスに大きな負担となる。その結果、新たなディジタル計測制御系や既存システムの変更に対する規制レビューや承認の許認可プロセスは、困難で時間がかかり申請ごとに行うこと（ケースバイケースの許認可）が慣例となっている。このため、多くの電力会社は、変更の申請をためらっている。

USNRCと米国原子力産業界でのコンセンサスの欠如： 上記の課題について効果的に対処するために、コンセンサスを得ることが必要となる。これにより、安全性及び公衆の信頼を維持しつつ新技術の利点を最大限活用することができる。しかし、産業界と規制側は、こうした新技術に関する経験が少なく効果的にコンセンサスを得ることが困難である。コンセンサスが得られていないことにより、ディジタル計測制御系を利用することの利点が不利益に勝るか否かを不明瞭にしている。

以上の問題点に加えて、USNRCは、原子炉安全諮問委員会(ACRS)や原子力安全研究レビュー委員会(NSRRC)により下記の問題を指摘された。

・ディジタル計測制御技術に対する一貫性のある効果的なレビュープランの欠如：ACRS
・新技術に対する規制／承認プロセスを策定するためのストラテジーの必要性：NSRRC
・ソフトウェアの設計仕様、性能評価と妥当性評価、ハードウェアに対する環境影響、共通原因故障に対処するための多重性、及び、計測制御系の信頼性予測などの課題に対する基準策定の必要性：ACRS, NSRRC
・人工知能やニューラルネットワーク等の分野における技術開発をはじめとする技術の急速な進歩への対応：NSRRC

規制プロセスにおける標準的アプローチ

原子力発電プラントに対するディジタル計測制御の有する技術的な特徴は、化学プラントや航空機の場合と本質的に同じである。他産業との違いは、広範な状況において十分高い信頼性と安全性を確保しなければならないという点である。原子力発電プラントの事故は極めて大きな影響を及ぼし得るため、発生頻度の低い事象であっても、計測制御系によりその発生可能性を下げる必要がある。USNRCは、こうした高い信頼性と公衆の安全性を確保することを目的とした規制プロセスを確立してきた。現行の規制プロセスは、安全裕度の確保と重大なリスクのないことの確認に着目しており、そのために多くの標準的なアプローチを用いている。そこで、これらの方法の中から、ディジタル系の利用に関連する5つの項目が選定され、ディジタル系が新しい技術であり急速に進歩することによる影響が検討された。

深層防護(Defense-in-Depth)： 安全設備においては、多重にバリアを設け、1つのバリアの故障が他のバリアに影響を与えないよう設計される。ディジタル計測制御系については、自己チェック機能などを設けることで信頼性の向上を図ることができる。しかし、共通原因故障等、ある種の故障は広い範囲に及ぶ不具合をもたらし、その結果として、深層防護の複数のレベルが無効となる可能性がある。

安全裕度(Safety Margin Assessment)： 安全裕度の評価には、決定論的手法と確率論的手

法が用いれられるが、前者は、事故に対する安全系の性能を、後者は、設計上の弱点や、設計基準を超える事故の発生頻度、リスクを評価する。ディジタル計測制御系については、膨大な数の入出力や状態が想定され、構成要素も複雑に絡み合っていることから、安全裕度や信頼性の評価はかなり議論すべき問題である。さらに、ソフトウェアは、一般に、数学的に記述することが困難である。

環境に対する品質(Environmental Quality)： 安全系の機器については、使用環境において所定の機能を果たすことが示される。ディジタル計測制御系には光ファイバーや磁気／光ディスク等の新たな機器が使用されるが、こうした機器に対する環境影響が他の種類の機器と同様である場合も異なる場合もある。ディジタル系のハードウェアについては、アナログ系と同様、経年劣化を考慮する必要があるが、ソフトウェアは「疲労破損」等の状態に曝されることはなく、従って、従来のアナログ系に対する寿命試験方法を適用することはできない。さらに、ソフトウェアの致命的なエラーによる故障モードは検出が困難である。

要求される品質(Requisite Quality)： 体系的な品質管理／保証プログラムにより、安全設備が要求された品質を満たしていることを確認することとなっている。ディジタル系に対しては、ソフトウェアの品質管理／保証を体系的に行うための方法が幾つか有るが、その使用経験は少ない。従って、ディジタル系において要求された品質が確保されていることを確認することは困難である。

故障性(Failure Vulnerability)： 安全設備には、独立性、物理的分離、冗長性及び多様性が設けられている。しかし、ディジタル系については、故障モードとその影響が理解されていることを確認できないため、USNRCは、アナログ系より高いレベルの冗長性と多様性を要求しようとしており、その結果、ディジタル系の設計が複雑化する可能性がある。また、ソフトウェアの作成を独立に行って多様性を設けても故障の発生防止にはさほど効果はなく、高信頼性を確保するためには別のアプローチを用いるのが妥当であると示唆されている。

上記の検討により、安全性及び信頼性に関する疑問点と問題点が明らかになり、それらは6つの技術的課題と2つの施策的課題に整理された。

（技術的課題）

・ディジタル計測制御技術の系統的特性(system aspects of digital I&C technology)
・ソフトウェアの品質保証(software quality assurance)
・共通原因によるソフトウェアの故障(common-mode software failure potential)
・ヒューマンファクタとマンーマシン・インターフェース(human factor and man-machine interfaces)
・安全性及び信頼性の評価方法(safety and reliability assessment methods)
・民生用既製品のハードウェア及びソフトウェアの利用(dedication of commercial off-the-shelf hardware and software)

（施策的課題）

・ケースバイケースの許認可プロセス(case-by-case licensing processes)

・技術基盤の適性(adequacy of technical infrastructure)

これらの課題は、原子力発電プラントでのディジタル計測制御系利用に関する次の2つの主要テーマに関連している。即ち、技術的課題は、主に、ディジタル技術自体（テーマ1）に関連するが、施策的課題は、主として、最新技術の導入プロセス（テーマ2）に関係する。

1. ディジタル計測制御技術の特徴に関する取扱い
2. 既存プラントで使用されているディジタル技術より進歩している技術に関する取扱い（ディジタル技術は急速に進歩しており、原子力産業界ではその速度をコントロールできないが、その一方で、原子力産業の運用や規制には大きな影響を及ぼすものである）

技術的課題

(1) ディジタル計測制御技術の系統的特性(System Aspects of Digital I&C Technology)

課題： ディジタル計測制御系の導入に伴い、新たな故障モードも発生し得る。従って、ディジタル計測制御系の設計及び設置に関する系統的特性を正確に取り扱うことが要求される。

・このためには如何なる方法が必要か？

・ディジタル系の利用に関わる様々な技術者の経験をどのように集約し、原子力発電プラントに適用するか？

・将来、新しいディジタル計測制御技術や機器を導入する際、その方法やそれまでの経験を更新するために、如何なる手順を整備することができるか？

勧告とUSNRCの対応見解：

1) （米国内での大規模なディジタル計測制御系の設計や設置が困難な状況にあることから）USNRCは、提案された規制ガイダンス文書を米国外の原子力発電プラントのディジタル系に試行的に適用すべきである。特に、このレビューでは、改訂されたガイダンス文書がディジタル系の系統特性を適切に説明するのに必要なレベルの具体性を有しているか否かを評価することに着目すべきである。

→ USNRCは、規制ガイダンスを米国外の原子炉に適用することには同意していない。米国外への適用は、当事国の規制当局と電力会社の賛同と参加を得なければできないものであり、また、国によってディジタル系に対する要求が異なるためこうした適用が必ずしもガイダンスの有意義な評価になるものでもないと考えられる。しかしながら、一方で、米国外の機関による使用例もある。

・チェコ：Temelinにおけるウェスチングハウス(WH)社製ディジタル計測制御系のレビュー（標準レビュープラン(SRP)の7章を利用）

・韓国：独自のガイドラインを策定するためにSRPを参照

2) USNRCは、大規模なディジタル系を採用している化学プラントや航空機などの他産業における系統特性に関するガイダンス文書を同定・レビューすべきである。このレビュ

ーでは、それらのガイダンス文書とUSNRCが整備しているガイダンスを比較することに主眼を置くべきであり、特に、共通の問題点や適用にあたっての固有の差異に注意すべきである。

→ USNRCは、本勧告に同意している。規準やスタッフによる研究の策定や更新の際には、通常、本勧告に示されているようなタスクを行っている。SRPの7章を改訂する際にも、USNRCスタッフは産業界との討議の場を持って、ガイダンス策定に有用な情報を入手しており、こうした活動は継続して行うこととしている。例えば、規制ガイダンスでは、ボーイング社やソフトウェア生産協会からの情報や、国際電気技術委員会(IEC)、国際標準化機構(ISO)、電気・電子技術者協会(IEEE)などの規準を参考としている。さらに、今後、他産業におけるディジタル系の利用やUSNRCのガイダンスとの関係に関する調査をはじめとする活動を行うことを予定している。

3) 実践的な経験を積むために、USNRCは、大規模で安全上重要なディジタル計測制御系を規制・監督する他機関にスタッフを派遣すべきである。

→ USNRCは、本勧告を実施するに十分な人員が確保できないため、同意していない。他産業における規制機関とは、機関間会合などを通して、相互の情報交換を既に行っている。

4) USNRCは、特に系統特性に関連する技術についてスタッフのトレーニングを継続して行うべきである。

→ USNRCは、本勧告に同意している。スタッフは、ディジタル技術の様々な特性に関するトレーニングに参加してきている。現在進行中の内部トレーニングを継続して行う予定である。さらに、ディジタル計測制御系に関するスタッフの能力開発に対するガイダンス(NUREG/BR-0227)を策定しており、ディジタル系の問題に関する能力の開発と維持を図っている。また、スタッフを特別のプログラムに参加させ、ディジタル系に関する個人の専門知識の向上を図っている。

(2) ソフトウェアの品質保証(Software Quality Assurance)

課題： ソフトウェアの利用がアナログ系とディジタル系との大きな違いである。ソフトウェアの品質は、仕様が適切か否か、仕様通りに作成されているか否かを調べることによって確認される。しかし、ソフトウェアの作成過程を管理したり、出来上がったソフトウェア自体を検証するという従来の方法だけは、適切な品質管理は行えない。そこで、

・ディジタル計測制御系ソフトウェアの仕様、作成及び工程管理に関し、USNRCや産業界は、一般的に容認される技術的な解決法をどのようにして定義することができるのか？

勧告とUSNRCの対応見解：

1) 現在、USNRCは、種々の産業界規準を容認するために規制指針を策定する方針である。USNRCは、ソフトウェアの品質保証に対し、規範的な解決策よりもむしろ容認基準に着

目した独自のガイドラインを策定すべきである。カナダ原子力管理委員会(AECB)による規制指針のドラフト(C-138)がその典型的な例である。ガイドラインの策定にあたっては、(a)原子力産業界、(b)他の安全上重要な産業界、及び、(c)民間及び学術的なソフトウェア業界等の幅広い外部機関によるピアレビューを受けるべきである。

→ USNRCは、本勧告に同意していない。これまでの経験から、スタッフは、独自のガイダンスを策定するより、適用可能な産業界規準を承認し利用する方が適切かつ効率的であると考えている。但し、その際には、適用できない部分の明確化を図る必要がある。こうした方針をとることのメリットは、規制側だけでなく、ベンダー、設置者、学術界からの情報入手を一貫性のあるプロセスで行えることにある。規制指針は、一般に、規範的な解決策や要求を含むものではなく、規制要求に従うための方法を示している。規制指針やSRPなどのガイダンスに関する最終版を発行する前に、内部のスタッフやACRS等の委員会によるレビューを受けることになっている。また、産業界や学術界を含む一般公衆からのコメントを求める期間を設けることも義務づけられており、これらのコメントは最終版の発行に先立ち検討することとなっている。カナダのソフトウェアに関するドラフト規制指針については、AECBからの要請を受けて、規制指針C-138をスタッフがレビューし、その内容がスタッフの見解やSRPの7章の改訂内容、及び、新たな規制指針と一致している旨の文書を送付している。

2) 系統の要求項目(systems requirements)は、アプリケーション固有の属性と同様、一貫性や完全性といった一般的な属性を分析できるよう、正確な意味を有する言語で記述すべきである。プラント技師、規制当局、システム設計者、ソフトウェア作成者などの関係者がその言語を理解できるものとすべきである。

→ USNRCは、本勧告に同意している。スタッフは、安全上重要なソフトウェアの開発にあたって、システムに関する仕様を明確に記述することが重要であると考えている。但し、その仕様をどのように記述すべきであるかを義務づけることはないが、仕様の整合性、完全性、理解性及び明確化はスタッフの基準に盛り込まれる。ソフトウェアの品質レビューに対するガイダンスと容認基準は、計測制御部門(HICB)の部門技術見解(BTP) HICB-14（ディジタル計算機ベースの計測制御系に対するソフトウェア・レビューに関するガイダンス）及びスタッフの検査支援ツールに示されている。さらに、この問題については、要求仕様のフレームワークに関する研究プロジェクトにおいて、検討を行う予定である。

3) USNRCは、ソフトウェアの品質保証に関し、ソフトウェアのライフサイクル初期フェーズとコードレベルの課題（例えば、多様性を持たせるための異なる言語を用いたコーディング）の間でバランスを取りながら研究を進めるべきである。この初期フェーズがソフトウェアのエラー発生にしばしば関与することは経験により明らかである。

→ USNRCは、本勧告に同意している。具体的にはSRPの7章の付録に示されているように、ディジタル計測制御系の全体レビューにおいて設計開発の早期段階に着目している。さらに、上述したように、要求仕様のフレームワークに関する研究プロジェクトが開始されている。本研究プロジェクトの目的は、設計開発の初期フェーズにおいて発生するソフトウェアのエラーを最小限にするために幾つかのステップが踏まれていることを確認するためのレビューガイダンスを策定することである。

4) USNRCは、アプリケーション固有型集積回路(ASICs)、プログラマブル・ロジック制御装置(PLCs)及び他の類似の技術に対し、同等の品質保証プロセスを要求すべきである。

→ USNRCは、本勧告に同意している。スタッフは、PLCやASICについて、他の計算機ベース・システムと同様の方法でレビューを行っている。また、他のディジタル計測制御系に関するガイダンスや審査と同様のレベルの品質保証に関する活動を継続する予定である。

(3) 共通原因によるソフトウェアの故障(Common-Mode Software Failure Potential)

課題： アナログ系における共通原因故障(CMF)を評価するために多種多様な方法が開発されてきたが、

・これらの方法がソフトウェアに基づくディジタル系へ適用可能であるか、あるいは、別の方法が必要か？
・ソフトウェアの多様性とは何か？
・その多様性の実現や評価は可能か？
・計算機を含むCMFを評価するための方法は存在するか？
・許認可プロセスに対してソフトウェアの共通原因故障はどんな意味を持つか？
・冗長性や多様性はディジタル系の信頼性を確保するために最も有効な方法であるか？

勧告とUSNRCの対応見解：

1) USNRCは、ソフトウェアCMFが起こり得るものと仮定する見解を保持すべきである。

→ USNRCは、本勧告に同意しており、既に、改訂SRPの7章において明示している。

2) USNRCは、部門技術見解(BTP)ドラフト“新型及び既存プラントにおけるディジタル計測制御系”で述べているように、ディジタル計測制御系に多様性を持たせる必要があるという基本的な見解を維持すべきである。

→ USNRCは、本勧告に同意しており、既に、改訂SRPの7章において明示している。

3) USNRCは、適切な多様性が存在するか否かの評価に関するガイドラインを再検討すべきである。USNRCは、異なるプログラミング言語、同一機能の要求を満たすための異なる設計方法、異なる設計チーム、あるいは、異なる製造者による機器の使用（ネームプレート多様性）に頼るべきではない。むしろ、USNRCは、機能多様性、異なるハードウ

ェア、及び、異なる実時間オペレーティングシステムの利用など、より抜本的な方法に着目すべきである。

→ USNRCは、本勧告に同意している。多様性の評価は、1つの要因だけに基づいて行うわけではなく、機能多様性、ハードウェア多様性、システム多様性などを組み合わせて評価する。改訂SRPの7章では、ネームプレート、設計多様性及び機能多様性を考慮して容認可能な多様性を明確化するよう更新する予定である。

4) USNRCは、同一機能を果たす2つのソフトウェアの間の多様性を確立しようとして研究予算を執行することについて再度検討すべきである。ソフトウェア間の多様性を確立することができるとは考えられない。特に、Unravelツールに関するUSNRCの予算が、同ツールをソフトウェア間の多様性確保のために使用することを前提としているが、有用とは考えられない。

→ USNRCは、本勧告に同意している。しかし、Unravelがディジタル系の機能多様性を評価するためのツールではないことに注意されたい。Unravelは、ソフトウェアの品質を評価するために使用できるツールの1つである。Unravelの主たる目的は、エラーを見つけるためにソフトウェアのストリング・チェックを行う際に、スタッフによるレビューを支援することである。Unravelでは、コード全体にわたってストリングを組み合わせることにより、共通原因故障を引き起こす可能性のある共通のコーディング命令(coding instruction)を識別することができる。

(4) ヒューマンファクタとマンーマシン・インターフェース(Human Factor and Man-Machine Interfaces)

課題： 計算機に基づくマン.マシン・インターフェース(MMI)が運転員に及ぼす影響の評価方法については、USNRCと産業界の間で合意が得られていない。

・ヒューマンファクター及びMMIが適切に考慮されているかを確認するために、如何なる方法を用いるべきか？

勧告：

1) USNRCは、設計及びそのプロセスに対して適切なレビュー・ガイドラインがあれば、それを継続して使用すべきである。原子力及びその他の産業界の利用において知識が高まるにつれて、これらのガイドラインを更新する際には注意を要する。

2) USNRCは、レビューをガイドラインやチェックリストに限定しないものと仮定すべきである。 (a)設計の基となる運転員モデル、(b)マンーマシン相互作用に関する古典的な設計上の問題の記述方法、及び、(c)パフォーマンスに基づく評価に関して、設計を評価すべきである。さらに、評価では、代表的なタスク、実際のシステム挙動及び実際の運転を使用すべきである。

3) USNRCは、レビュー基準を拡張して、数多くの安全上重要な設備への利用において繰

り返し発生するマンーマシン相互作用の欠陥についてリストを作成すべきである。他産業における問題点や提案された解決策を理解することは、ディジタル技術の導入によって引き起こされるエラーが繰り返し発生するのを防止するために効率的な方法である。

4) 上記の勧告2を補足すると、ヒューマンファクタのレビューは慎重に（例えば、実際の状況や運転員によるパフォーマンス基づく方法を用いて）行うべきであるが、レビューの範囲や規模はディジタル機器への変更の特徴や規模と対応を取るべきである。

5) USNRCと原子力産業界は、定期的に公開討論会に参加すべきである。NUREG-0711に述べられているように、ヒューマンインターフェースに関する最新技術は、ヒューマンファクタ関連の新たな未解決問題を数多く導入する。USNRCが他産業における現在の研究や最善のプラクティスに遅れずに、自分たちの利用から得られた知見を研究や実践の遂行に貢献することは、困難である。

6). USNRCは、ハルデン研究プロジェクトに携わる研究者が国際的な研究活動に積極的に参加して成果を共有したり知見を得ることを奨励すべきである。

7) USNRCの規制研究局(RES)は、マンーマシンの統合、管理及び自動化についてより高度レベルの課題を検討するための研究を支援すべきである。こうした研究には、より効率的に設計を具体化するための運転員モデルなど、原子力発電プラントに適用するための設計手法を検討することも含めるべきである。さらに、広範な分野の研究を行って、原子力特有の技術的問題を明らかにしたり、他産業における経験と対比させる必要がある。こうした研究の成果は、繰り返し発生する欠陥のカタログに追加すると共に、提案された解決策とリンクさせることになる。

8) USNRCは、自身の研究プロジェクトを補完しながら、エネルギー省(DOE)との間での施設の調整を検討すべきである。こうした施設において、米国内の原子力産業界は提案された設計を具体化し評価することが可能である。ワークステーション技術がさほど高価でないことから、ワークステーションによる精度の高い制御室シミュレータの開発が可能である。他産業（例えば、航空機）では、ワークステーションによる部分的タスクのシミュレータが幅広く利用されている。

なお、上記の勧告に対し、文献(3)において、USNRCはその対応見解を提示していない。

(5) 安全性及び信頼性の評価方法(Safety and Reliability Assessment Methods)

課題： ディジタル計測制御系の安全性と信頼性を評価するために、効果的かつ効率的な方法が必要であるが、

・如何なる方法が用いられるべきか？

勧告とUSNRCの対応見解：

1) USNRCは、ソフトウェアの故障が系統全体の信頼性に及ぼす相対的な影響を、ディジタル機器を含む系統の確率論的リスク評価(PRA)において考慮するよう要求すべきである。

→ USNRCは、本勧告に同意している。ディジタル系を利用した新型炉の設計に

対するPRAでは、ディジタル系をアナログ系と見なしてモデル化している。アナログ系に比べると、ディジタル系に対する故障率データは限られており、潜在的に重要な故障モードも異なっているが、ディジタル系をモデル化したPRAでは、不確実さ解析を通してその重要度を調べることでリスク寄与度に関する知見を得ることができる。例えば、WH社のAP600のレビューにおいて、こうした評価が行われている。信頼性に関する要求が厳しくなるにつれて、データの不足により評価における確信度が低下する。例えば、希有事象に影響を及ぼす設計エラーに関するデータはほとんどない。しかし、スタッフがディジタル計測制御系の容認性について判断する際に数値的な信頼性基準にだけ頼るのではないことに注意されたい。

2) USNRCは、PRAでの使用を目的とし、民生用既製品(COTS)を含むディジタル系の故障確率を推定するための手法開発に力を注ぐべきである。これらの手法には、使用にあたっての容認基準、ガイドライン及び制限条件の他、必要とされる論理的根拠や正当化を含めるべきである。

→ USNRCは、本勧告に同意している。スタッフは、ディジタル系のリスク評価の分野で行われている活動を随時レビューすることとしている。また、プラント計算機システムの運転経験とリスク解析手法に関するデータベースを構築するために、経済協力開発機構／原子力機関(OECD/NEA)の原子力施設安全委員会(CSNI)による提案を支持している。計算機システム問題に関する最終報告書では、CSNIはソフトウェア並びにディジタル系の信頼性を評価するための手法開発を目的とした研究を随時レビューすべきであるとしている。現在進行中の研究プロジェクトの1つにおいて、ソフトウェアの信頼性を推定するための現行の方法を評価することとなっている。

3) USNRCと産業界は、それぞれの能力を評価し、確信を持ってディジタル化を行うための要求事項と定量的評価の限界を理解するのに十分な専門知識を構築すべきである。

→ USNRCは、本勧告に同意している。スタッフと産業界は、ディジタル系の導入が効果的に行われることを確信するために専門知識の向上を図っている。例えば、スタッフと産業界は、COTS、PLC及びASICの作成計画において相互交流を行っている。定量評価の限界については、米国内の原子力産業界はプロセス計算機の主たるユーザではないため、スタッフは、CSNIの活動などディジタル系の信頼性に関する研究活動を継続してレビューすることが適切であると考えている。ディジタル系の定量評価に関する専門知識を高めるために、スタッフはセミナーへの参加や手法に関する文献調査を行っている。

4) USNRCは、ディジタル系の（安全性／信頼性）解析を行うための新たな手法を開発することを目的とした研究計画を支援すべきである。この手法は、定量評価における不確実さを減らし確信度を上げるために用いることができるものと考えられる。

→ USNRCは、本勧告に同意している。USNRCの対応については上記2)及び3)を参照されたい。

(6) 民生用既製品のハードウェア及びソフトウェアの利用(Dedication of Commercial Off-the-Shelf Hardware and Software)

課題： 原子力発電プラントの安全系における民生用ディジタル計測制御系の利用を評価し容認するために、

・規制当局と設置者は、如何なる方法に対して合意を得るべきか？

勧告とUSNRCの対応見解：

1) USNRCは、電力研究所(EPRI)、原子力利用者ソフトウェア管理グループ(NUSMG)、IEEE及び国際計測制御学会(ISA：旧米国計測学会)のワーキンググループと協力することにより、 USNRCの関心や見解が議論され、これらのグループが策定する規準やガイドラインを速やかに承認することに繋がるという認識を持つべきである。

→ USNRCは、本勧告に同意している。COTSに関して、スタッフは、会合に参加したり産業界との相互交流を図っており、そのため、EPRIのCOTSガイダンス(EPRI TR-106439)の承認が速やかに行われるものと期待されている。

2) USNRCは、原子力発電プラントの安全系へのCOTS利用を容認するために如何なる研究が必要かを見極めるべきである。こうした研究は、全体の研究計画に取り込むべきである。

→ USNRCは、本勧告に同意している。スタッフは、COTSハードウェア及びソフトウェアの利用をサポートするための研究計画の策定を検討している。

3) COTS利用に関するUSNRCの規制ガイダンスは、基準や性能評価活動が利用形態の複雑さや安全上の重要性に対応しているという原則に基づくべきである。

→ USNRCは、本勧告に同意している。 スタッフが承認しようとしているEPRIのCOTSガイダンス(EPRI TR-106439)において考慮されており、改訂SRPの7章でこのガイダンスを参照している。

施策的課題

(1) ケースバイケースの許認可プロセス(Case-by-Case Licensing Processes)

課題：

・ディジタル計測制御系の規制をより効率的かつ効果的に行うために、規制プロセスにおいてどのような変更がなされるべきか？

・ディジタル計測制御技術が急速に進化するという特性に対応するためには、どのようにして規制プロセスに柔軟性を持たせるか？

・どのようにして規制プロセスの効率化を図ることができるか？

勧告とUSNRCの対応見解：

1) USNRCは、既設プラントへのディジタル系の導入に関するレビューと評価を行うために、一般に適用可能な枠組の構築を最優先して行うべきである。

→ USNRCは、本勧告に同意している。改訂SRPの7章では、こうした枠組やガイダンスを策定しており、当初から優先度の高いものとされてきた。

2) ディジタル技術の急速な進歩を考慮し、新技術の開発に遅れずに規制の枠組を更新するためのプロセスを確立すべきである。この枠組において他の安全上重要な産業における最善のプラクティスが考慮されていることを確認するために、外部や公衆によるレビューを受けることが強く望まれる。

→ USNRCは、本勧告に同意している。改訂SRPの7章は、必要に応じて定期的に更新する予定である。スタッフは、規準策定に継続的に参加したり他国や他産業分野との相互交流を行うことで、進歩する技術分野における新たな開発や現状に遅れずについていくこととしている。

3) USNRCは、ガイドライン策定プロセスを加速・簡素化することができるような新たな方法を検討すべきである。例えば、USNRC、産業界及び学術界からの代表を含めたタスクグループの設置を検討することが挙げられる。これらのグループは、ディジタル系の開発と利用において発生する安全上重要な問題を検討・解決するために、プロジェクト的に運営されるものとする。

→ USNRCは、本勧告に同意している。本件については、スタッフがUSNRCのコード・規準に関する会合において説明し、それに対して、規準承認のプロセスを加速化・合理化する方法を調べるよう指示され現在調査中である。安全上重要な未レビュー問題を提起するために産業界と学術界を含む諮問グループを利用することに関しては、現在、USNRC内部にACRSとNSRRCという2つの諮問グループがあり、安全問題や研究計画のレビューを行っている。スタッフは、効率的なガイダンス策定に対して、こうした監視体制と公衆からコメントを求めるというプロセスで十分であると考えている。さらに、産業界にとって重要な問題が生じた場合には、容認可能なガイダンスやアプローチの検討を行うために、スタッフと産業界の代表によるワーキンググループが組織されてきた。

4) 規制要求の策定にあたり、USNRCは、ディジタル系に特有の問題が生じた場合、それらが適切に対処されることを確認すべきである。一方、ディジタル系の導入によって生じる問題がアナログ系に対する問題と差異がない場合、これらの問題は矛盾が生じないように一貫して対処すべきである。 USNRCは、ディジタル系の導入に対するレビューと承認を行うにあたり、導入によって発生した問題が提案されたディジタル系の利用形態に固有のものでなければ、個々の設置者に新たな規制要求を課すべきではない。

→ USNRCは、本勧告に同意している。スタッフは、改訂SRPの7章及びディジタル系の検査ガイダンス(IP 52001&52002) が、ディジタル系への変更について一貫性のあるレビューを行う上で役立つものと考えている。委員会規則にお

ける新規項目あるいは追補項目によって生じた新たな要求を賦課したり、あるいは、規則の解釈に関して従来とは異なる規制スタッフ見解を賦課する場合があるが、これらは、10 CFR 50.109（バックフィッティング規則）に基づくものであり、新たな見解を賦課する前には、その妥当性を評価するための費用／効果解析を行うこととなっている。

5) USNRCは、電力会社、産業界および他の関連機関と早期に協力するための先行的な努力を行うべきである。さらに、原子力及び非原子力の分野におけるディジタル計測制御系の利用を幅広く理解することは、USNRCにとって大きな利益となる。こうすることにより、協力関係の基盤ができるものと考えられる。

→ USNRCは、本勧告に同意している。様々なトピックについて、EPRIや産業界のワーキンググループを通して先行的な活動を進めている。多くの場で、スタッフは、設置者に対して可能な限り早期に設備変更の議論を行うと伝えている。しかし、実際には、スタッフ及び設置者の人員に制約があり、個々の設置者と相互交流を図ることは必ずしも可能ではなく、また、設置者に対して、その計画をスタッフと議論するよう義務づけることもできない。10 CFR 50.90に従う設置変更が必要な場合に限り相互交流が要求される。

6) USNRCは、10 CFR 50.59との整合性を確認するために、Generic Letter (GL) 95-02及びEPRI TR-102348において提起された“システムレベル”の問題（システム、即ち、ディジタル系としての機能への影響はなくても構成する機器のレベルで未レビュー安全問題(USQ)が生じた場合の10 CFR 50.59の取扱い）を再検討すべきである。ディジタル技術を含む安全系の主要な変更と軽微な変更とを区別するという見解を維持及び具体化することは望ましい方向である。

→ USNRCは、本勧告に同意している。GL 95-02に述べたように、システムレベルに関するスタッフの見解は、10 CFR 50.59をレビューするためのプログラムの一部として、技術スタッフ及び法律スタッフにより再検討されてきた。その結果、GL 95-02の解釈は新たな不具合に関連するものであり、正しいと判断され、今後変更されることはないと考えられる。

7) USNRCは、ディジタル系の導入に関する50.59の評価をカタログ化するためのプロセスを確立すべきである。これにより、ディジタル系の導入を検討している電力会社が、ある特殊な変更によりUSQが発生したことが明らかになった場合について、過去の50.59の評価をレビューし検討することが可能となる。

→ USNRCは、本勧告に同意していない。10 CFR 50.59に基づく評価は設置者が行うものであり、USNRCにその結果を提出するよう要求されていない。設置者は、評価結果を纏めた年報を作成するよう要求されている。スタッフは、その報告書をレビューし、ディジタル系への変更ある場合、それに対する検査の必要性を検討することになる。ディジタル系への変更が行われる場合にUSQが

生じるか否かを判断するためのプラント設置基準をレビューするが、これは、プラントごとに設置基準が異なっているため個別に行われる。従って、スタッフは、50.59評価のカタログ化に多くの人員を投入することが、設置者にとって大きな利益を与えるとは考えていない。しかし、原子力産業界自体が、ディジタル系の導入によりUSQが生じるか否かを判断するためのガイダンスを整備することを目的に、ディジタル系の変更に対して50.59評価のカタログ化を行うことは可能であろう。なお、スタッフによるレビューを必要とするディジタル系のレトロフィットは、公開の安全評価において承認されるものと認識している。

(2) 技術基盤の適性(Adequacy of Technical Infrastructure)

課題： ディジタル計測制御技術の規制活動を支えるために、

・USNRCは、スタッフの構成、訓練及び研究プログラムにおいて変更を行うか？

・USNRCにとって適切なプログラムは何か？

・予算削減の中で、急速に進歩する技術に対応して同プログラムの有効性を維持するためには、プログラムをどのような構成にするべきか？

勧告とUSNRCの対応見解：

1) 技術の急速な動きと原子力産業界の沈滞にも拘わらず予算と人員が削減されていることにより種々の困難が生じてはいるが、USNRCは、現行のスタッフによるレビュープロセスの効率化を図るために様々な方法を模索しなければならない。

→ USNRCは、本勧告に同意している。SRPの7章を改訂するための努力を行っており、また、幾つかのプログラムに関して産業界と相互交流を図っている。

2) USNRCは、現行あるいは新規採用のスタッフに対して、最小かつ継続的な訓練の必要性を明確にすべきである。ソフトウェアの品質保証については特別な注意を払う必要がある。USNRCの訓練プログラムは適切な外部レビューを受けるべきである。専門家としてのレベルを証明することはUSNRCが検討したいと考えている1つの方法である。

→ USNRCは、訓練に関する勧告に同意している。内部の訓練諮問グループにより、ディジタル系のレトロフィットの検査に従事するスタッフの訓練と教育に関しガイダンスを整備している。NUREG/BR-0227には、ディジタル系のレビュースタッフに有用な訓練コースが示されている。こうした訓練は、ディジタル系ワークショップにより補完され、ディジタル系の問題や活動に関する最新のガイダンスを検査官に提供している。ディジタル系のレビュー及び検査に関する資格制度は、計算機システムの分野において資格認定の基準が十分に確立されていないため、現時点では実践的な選択ではない。

3) USNRCは、規制研究局(RES)及び原子炉規制局(NRR)によって行われる研究プログラムに対して施策的なプランを立てるべきである。このプランは、短期的な規制ニーズと長期的な研究ニーズとのバランスに着目すべきであり、研究目的を達成するために人員を有効的に活用する方策を取り入れるべきである。さらに、関連技術業界、EPRI、DOE、

米国外の原子力機関、及び、ディジタル計測制御問題を取り扱う他産業にも、より効果的にプランを拡げるべきである。この勧告を行うにあたり、当委員会は、ハルデン計画がこうした協力研究の例であると認識しているが、ハルデン計画における活動の多くは公開できず、従って、精密な検討による効果は得られない。

→ USNRCは、本勧告に同意している。ディジタル系に関する将来の研究に対し、本勧告の必要性を強調するような施策的なプランが策定されるであろう。同プランでは、規制項目の展開と調査研究とのバランス、他機関との関係、及び、ヒューマンファクタやディジタル計測制御に関する研究施設との協力などの問題に着目することになるであろう。

4) ディジタル計測制御に関する研究は長期にわたって行うべきものでると考えられるため、USNRCは、複数年の予算を計画・調整できるよう配慮すべきである。

→ USNRCは、本勧告に同意している。USNRCは、複数年ベースでプロジェクトに予算を付けることに合意しつつあるが、議会はUSNRCの予算を単年度ベースで認可している。特殊なタスクに対する研究プログラムは、ほとんどの場合、多数年にわたって計画される。

5) USNRCは、必要となる規準やガイダンス文書の作成・更新を促進するための方策を検討すべきである。特に、USNRCは、タスクグループの設置と利用を考慮すべきである。

→ USNRCは、本勧告に同意している。「ケースバイケースの認可プロセス」に関する勧告3)への対応を参照されたい。

まとめ

本報告書は、米国研究協議会(NRC)が、米国原子力規制委員会(USNRC)からの委託を受けて行った、ディジタル計測制御技術の原子力発電プラントへの適用に関する調査研究の結果と、その中で提示された勧告に対するUSNRCの対応見解をまとめたものである。

NRCによる調査研究では、ディジタル計測制御技術の適用に際しての重要課題として、6つの技術的課題と、2つの施策的課題を摘出し、それぞれについて、USNRCがどう対応すべきかを勧告として提示した。合計で42の勧告（技術的課題に関するものが30項目、施策的課題に関するものが12項目）がなされたが、USNRCは、これらのうち、ヒューマンファクタ及びマンーマシン・インターフェースに関する8つを除き、各々の勧告について自らの対応見解を示した。摘出された重要課題の多くが、既に、USNRCや、その諮問機関である原子炉安全諮問委員会(ACRS)や原子力安全研究レビュー委員会(NSRRC)により明らかとされていたものであることから、多くの勧告（30項目）についてUSNRCが同意している。残る4つの勧告については、同意していないが、これらは、USNRCの策定したガイダンスの米国外での適用、スタッフの他機関への派遣、ソフトウェアの品質保証に関する独自のガイドライン策定、ディジタル系導入時評価の設備変更規則(10 CFR 50.59)への登録、である。

1. はじめに

近年、欧米諸国において、原子力発電プラントの計測制御系にディジタル技術が導入されつつある。特に、カナダ、フランス、イギリスでは、最新のプラントで完全なディジタルベースの計測制御系が導入されている。米国では、過去20年間新設のプラントはないが、新型炉の設計ではディジタル計測制御系の利用を前提としている。また、既存プラントでは、これまで使用してきたアナログ機器からディジタル機器への変更が行われている。我が国においても、柏崎・刈羽-6、7号機(ABWR)でディジタル機器が使用されている。しかし、ディジタル技術の導入に伴い、設計、施工、安全及び許認可に関する新たな問題も生じている。特に、ディジタル系ではソフトウェアを使用するため、従来のアナログ系には見られなかった問題がある。従って、原子力発電プラントの安全性に関して現在の高いレベルを維持あるいは向上させるためには、こうした問題を考慮して、安全評価の方法や、技術基準、規制指針等の見直しが必要となる。

米国原子力規制委員会(USNRC : United States Nuclear Regulatory Commission)は、これまでに、多くのプラントについて、計測制御系のアナログーディジタル変更（レトロフィット）をレビューすると共に、新型炉の設計レビューを行ってきた。しかし、統一された適用基準がなかったため、各申請に対して、ケースバイケースのレビューが行われた。こうしたレビュー方法は、批判を浴びる結果となり、USNRCは、体系的かつ一般的な規制レビューと承認の方法を確立するための研究を実施している。一方、米国の産業界では、積極的にディジタル技術の導入を進めており、能率的な許認可のためのガイドラインを策定してきた。例えば、米国規準研究所(ANSI : American National Standards Institute)、電気・電子技術者協会(IEEE : Institute of Electrical and Electronics Engineers)及び米国原子力学会 (ANS : American Nuclear Society) が共同でディジタル計測制御系に対する設計基準(ANSI/IEEE/ANS 7-4.3.2-1993)を作成し、原子力発電プラントのディジタル計測制御系のレトロフィットに関する安全評価に用いてきた。USNRCは、最近、条件を課することによって、これらのガイドラインを部分的に承認したが、ディジタル系のレトロフィットをケースバイケースでレビューするという見解は維持している。なお、米国外でも、国際電気技術委員会(IEC : International Electrotechnical Commission)や英国防省が、同様の基準を作成している。

米国研究協議会(NRC : National Research Council)では、USNRCからの委託を受けて、ディジタル計測制御技術の原子力発電プラントへの適用に関する調査研究を行った。この研究は、2つのフェーズからなり、米国MPR社のDouglas M. Chapinを委員長とする委員会が調査を実施した。フェーズ1[1]では、ディジタル技術の導入により生じる安全性及び信頼性に関する課題を明らかにした。フェーズ2[2]では、ディジタル計測制御系のレビュー及び容認のための基準を識別すると共に、USNRCがディジタル計測制御技術に関する規制や許認可を行う際のガイドラインを「勧告」の形で提言した。 USNRCは、この提言に対して、自らの見解を示している[3]。

本報告書は、上記フェーズ1及び2における調査結果、並びに、フェーズ2の提言に対するUSNRCの見解を纏めたものである。第2章では、アナログ系からディジタル系への移行について経緯を簡単にまとめ、第3章では、主として、フェーズ1による検討結果を、第4章では、フェーズ2における検討結果のうち、米国内外における技術的動向や、USNRCに対する勧告の内容及びそれに対するUSNRCの対応見解をまとめる。第5章では、フェーズ1及び2の調査研究を通しての結論を示し、第6章で本報告書のまとめを記す。なお、第2章から第5章までは全て、原著の記載に沿ってその内容をまとめたものであり、また、これらの章における参考文献（{n}の形式で示す）は、原著において参照されている主要文献であることを注記する。なお、技術規準や指針、NUREGレポートについては付録Cを参照されたい。

2. アナログ計測制御系からディジタル計測制御系への移行

現在、米国では、109基の原子力発電プラントが運転されているが、これらは全てディジタル技術が普及する前に設計されたものであり、アナログ式の計測制御系を前提とした設計となっている。アナログ計測制御系は、設計上の問題や環境による機能の低下等はあったものの、モニタリング、制御及び保護機能に関し良好な実績をあげてきた。しかし、その一方で、アナログ機器の経年劣化による機械的故障等が顕在化し、また、製造業界がディジタル技術の開発に力を注いできたためアナログ機器・部品の生産量が低下すると共に予備品も少なくなり、品質の良い交換部品の入手が困難となりつつある。製造業界がディジタル技術へ移行する理由は、アナログ機器に比べて大きな利点があることにある。即ち、ディジタル機器は、アナログ機器の弱点の1つであるドリフトがなく校正の手間が省けたり、精度や計算機能の向上が図れると共に、大量のデータを格納・処理でき、プラント運転状況の表示等も容易に行える。その結果、プロセス制御の改善や、プラントの安全性向上が期待される。このため、原子力発電プラントにおけるディジタル技術の導入は避けられない状況となっている。

こうした背景の下、多くのプラントで、ディジタル技術を用いた計測制御機器のレトロフィットが行われているが、ほとんどは、レコーダやディスプレイ等比較的規模の小さい機器単位のレトロフィットである。しかし、1990年から1994年にかけて、幾つかのプラントでは、比較的規模の大きい系統レベルでのレトロフィットが行われている{1-6}。その例を以下に示す。

- Haddam Neck：原子炉停止系及び補助給水系
- Sequoyah：原子炉保護系（WH(Westinghouse)社製Eagle 21の導入）
- Zion：原子炉保護系（WH社製Eagle 21の導入）
- Diabo Canyon：原子炉保護系（WH社製Eagle 21の導入）
- Palo Verde：ATWS系
- Turkey Point：非常用電源系負荷シーケンサ
- Prairie Iskand：所内停電／電源保護機能

・San Onofre：放射線モニタ系

ディジタル系へのレトロフィットは、連邦規制規則10 CFR 50.59（変更、試験及び実験）に従って行われてきた。こうした設備や系統の変更により新たな未レビュー安全問題(USQ：unreviewed safety question)が派生しない場合にはUSNRCの事前承認を受けずに行うことが許されているが、USNRCには変更の内容やレビューのための文書等を提出する必要がある。一方、10 CFR 50.59が適用されない場合には、USNRCによる事前承認が要求され、さらに、10 CFR 50.90（許認可及び建設許可の改正申請）に従って変更を行うことが必要となる。これまでのディジタル系へのレトロフィットの多くは、10 CFR 50.59に定義されるようなUSQを伴うことなく実施されてきた。なお、USQが生じるか否かを判断するための基準は10 CFR 50.59(a)(2)に記されている。

上記のように、米国では、ディジタル計測制御系の原子力発電プラントへの導入が進められてきたが、その際に幾つかの問題点も生じている。

新技術導入に特有の不確定性

原子力発電プラントのような安全上重要な産業においては、利用者、設計者及び規制当局は、現在の高いレベルの安全性を維持あるいは向上させるよう、ディジタル系の導入を進めて行かねばならない。その際の課題は、潜在的な危険性を取り込まずにディジタル系の導入により得られる性能及び安全性の向上を図ることである。さらに、ディジタル系に関する設計、評価及び規制アプローチでは、安全裕度を評価する手段も提示しなければならない。

アナログ系の実績から得た既存技術基盤の移行

原子力発電プラントの設計及び運転に関する経験の多くはアナログ技術に基づくものである。従って、ディジタル技術に起因する不確定性の取扱いに加えて、利用に当たっては技術支援体制や規制の枠組も変更する必要性が生じ得る。

ディジタル計測制御系の導入に伴う技術的問題

アナログ式とディジタル式の計測制御系における相違点を表 2-1に示す。こうした違いにより、ディジタル計測制御系の導入に際しては幾つかの技術的課題が派生する。レトロフィットの実績に基づき、USNRCは次のような潜在的な問題点を同定した[7]。

・ソフトウェアの共通原因故障
・民生用ハードウェア及びソフトウェアの利用
・新技術に関するプラント内使用実績の欠如
・構成管理
・複雑さの増加によるプログラミングエラーや不正出力
・標準的なソフトウェアツールの信頼性
・環境耐性（電磁波干渉、周波数干渉、温度、接地、煙等）
・プラントの安全裕度への影響

これらと同様の問題は、他産業の分野においても発生している[8]。

許認可アプローチ上の問題

一般に、新たな規制基準を策定し文書化するには長い期間を要するため、計測制御系の進歩が速く規制プロセスに大きな負担を負わせてきた。その結果、新たなディジタル計測制御系や既存システムの変更に対する規制レビューや承認の許認可プロセスは、困難で時間がかかり申請ごとに行うことが慣例となっている。このため、多くの電力会社は、10 CFR 50.59に基づいて行うことができない変更の申請をためらっている。

表 2-1 アナログ系とディジタル系の比較

	アナログ系	ディジタル系
データ収集	連続的	周期的あるいは事象依存
データ転送	計測値、関数、コマンドそれぞれが専用のワイヤ回線を介して連続的に転送される	多数の計測値、関数、コマンドが共用のワイヤ回線や光ファイバー回線を介して転送される
制御ロジック	固定関数式の機器で表現される	プログラマブル関数式の機器で表現される
運転員インターフェース	制御室と現場のを結線した固定機能型ディスプレイ	プログラマブル制御ロジックに接続されたプログラマブル対話型ディスプレイ
信頼性	温度変化、湿度、煙、放射線及び経年劣化によって校正値ドリフトが起こる；バスタブ型の故障率を示す	温度変化、湿度、煙、放射線及び経年劣化による性能低下の可能性がある；ハードウェアはバスタブ型の故障率を示す；ソフトウェアはデバグにより故障が少なくなる傾向を示す
供用中試験(サーベランス)	運転員あるいは保守員による手動で実施される	ソフトウェアを用いたハードウェアの自己試験が自動的に行われる（一部は手動）
運転前試験	入出力機能試験とcycle-to-failure試験が行われる	停止系等の簡単なロジックについては入出力機能試験とcycle-to-failure試験が行われる；プロセス制御系等の複雑なロジックについては統計的な機能試験が行われる；ソフトウェアのエラーは検出が困難である

USNRCと米国原子力産業界でのコンセンサスの欠如

上記の課題について効果的に対処するために、コンセンサスを得ることが必要となる。これにより、安全性及び公衆の信頼を維持しつつ新技術の利点を最大限活用することができる。しかし、産業界と規制側は、こうした新技術に関する経験が少なく効果的にコンセンサスを得ることが困難である。コンセンサスの欠如はディジタル系を使用すること自体についてではなく、むしろ、特殊な問題（例えば、共通原因故障）に関するものである。こうした問題に関してコンセンサスが得られていないことにより、ディジタル計測制御系を利用することの利点が不利益に勝るか否かを不明瞭にしている。これは、米国内の原子力産業が厳しい規制を受けていることで更に困難となっている。その上、かなりの資本が投資されており、従って、問題の解決が遅れれば、費用は1日当たり数十ドル余分にかかる

ことになる。結果として、許認可基準の定義は、体系的な研究と評価、並びに、異なる技術的見解の集約に基づくものでなければならないが、容易に実行できるプロセスではない。本質的には、ディジタル技術により十分な安全性と信頼性を確保できることを認めるために、ディジタル計測制御系に対する系統的な規制レビュー及び承認の方法論を確立することが重要である。

以上の問題点に加えて、USNRCは、原子炉安全諮問委員会(ACRS)や原子力安全研究レビュー委員会(NSRRC)により下記の問題を指摘された[9, 10]。

・ディジタル計測制御技術に対する一貫性のある効果的なレビュープラン（容認基準を含む）の欠如（ACRS）
・新技術に対する規制及び承認プロセスを策定するためのストラテジーの必要性（NSRRC）
・ソフトウェアの設計仕様、ソフトウェアの性能評価と妥当性評価、ハードウェアに対する環境影響、共通原因故障に対処するための多重性、及び、計測制御系の信頼性予測などの課題に対する基準策定の必要性（ACRS, NSRRC）
・人工知能やニューラルネットワーク等の分野における技術開発をはじめとする技術の急速な進歩への対応（NSRRC）

3. 重要課題の同定

3.1 規制プロセスにおける標準的アプローチの検討

原子力発電プラントに対するディジタル計測制御の有する技術的な特徴は、設備、応答時間、入出力範囲、及び、精度であり、これらは、化学プラントや航空機の安全設備におけるディジタル系の特徴と極めて類似している。原子力発電プラントのディジタル系と他産業との違いは、広範な状況において十分高い信頼性と安全性を確保しなければならないという点である。原子力発電プラントの事故は極めて大きな影響を及ぼし得るため、発生頻度の低い事象であっても、計測制御系によりその発生可能性を下げる必要がある。USNRCは、高い信頼性と公衆の安全性を確保することを目的とした規制プロセスを確立してきた。このプロセスは公開審査を条件としている。現行の規制プロセスは、安全裕度の確保と重大なリスクのないことの確認に着目しており、そのために多くの標準的なアプローチを用いている。そこで、フェーズ1では、これらの方法の中からディジタル系の利用に関連する5つの項目が選定され、ディジタル系が新しい技術であり急速に進歩することによる影響が検討された。

(1) 深層防護(Defense-in-Depth)

安全設備においては、多重にバリアを設けることにより、1つのバリアの故障が他のバリアに影響を与えないよう設計される。ディジタル計測制御系については、自己チェック機能などを設けることで信頼性の向上を図ることができる。しかし、ある種の故障、特に共通原因故障は、広範な機器・設備の不具合を引き起こす可能性があり、深層防護の複数の

レベルを無効にする可能性がある。

(2) 安全裕度(Safety Margin Assessment)

安全裕度の評価には、決定論的手法と確率論的手法が用いれられるが、前者は、事故に対する安全系の性能を評価するものであり、後者は、設計上の弱点を同定すると共に設計基準を超える事故の発生頻度やリスクを評価するのに用いられる。ディジタル計測制御系については、膨大な数の入出力や状態が想定され、構成要素も複雑に絡み合っていることから、安全裕度や信頼性の評価はかなり議論すべき問題である。さらに、ソフトウェアは、一般に、数学的に記述することが困難である。

(3) 環境に対する品質(Environmental Quality)

安全系に使用される機器については、その使用環境において所定の機能を果たすことが示される。ディジタル計測制御系には光ファイバーや磁気／光ディスク等の新たな機器が使用されるが、こうした機器に対する環境影響が他の種類の機器と同様である場合も異なる場合もある。ディジタル系のハードウェアについては、アナログ系と同様、経年劣化を考慮する必要があるが、ソフトウェアは「疲労破損」等の状態に曝されることはなく、従って、従来のアナログ系に対する寿命試験方法を適用することができない。さらに、ソフトウェアの致命的なエラーによる故障モードは検出が困難である。

(4) 要求される品質(Requisite Quality)

体系的な品質管理及び品質保証プログラムにより、安全設備が要求された品質を満たしていることを確認することとなっている。ディジタル系に対しては、ソフトウェアの品質管理や品質保証を体系的に行うための方法が幾つか有るが、その使用経験は少ない。従って、ディジタル系において要求された品質が確保されていることを確認することは困難である。

(5) 故障性(Failure Vulnerability)

安全設備には、独立性、物理的分離、冗長性及び多様性が設けられている。しかし、ディジタル系については、故障モード及びその影響が十分理解されていることを確認できないため、USNRCは、アナログ系より高いレベルの冗長性と多様性を要求しようとしており、その結果、ディジタル系の設計が複雑化する可能性がある。KnightやLevesonによれば、ソフトウェアの作成を独立に行って多様性を設けても故障の発生防止にはさほど効果はなさほど効果はなく、高信頼性を確保するためには別のアプローチを用いるのが妥当であると示唆されている[11]。

上記の検討により、安全性及び信頼性に関する疑問点と問題点が明らかになり、それらは以下の8項目（6つの技術的課題と2つの施策的課題）に整理された。

(技術的課題)

・ディジタル計測制御技術の系統的特性(system aspects of digital I&C technology)
・ソフトウェアの品質保証(software quality assurance)
・共通原因によるソフトウェアの故障(common-mode software failure potential)

・ヒューマンファクタとマン－マシン・インターフェース(human factor and man-machine interfaces)
・安全性及び信頼性の評価方法(safety and reliability assessment methods)
・民生用既製品のハードウェア及びソフトウェアの利用(dedication of commercial off-the-shelf hardware and software)

(施策的課題)

・ケースバイケースの許認可プロセス(case-by-case licensing processes)
・技術基盤の適性(adequacy of technical infrastructure)

これらの課題は、原子力発電プラントでのディジタル計測制御系利用に関する次の2つの主要テーマに関連している。即ち、技術的課題は、主に、ディジタル技術自体（テーマ1）に関連するが、施策的課題は、主として、最新技術の導入プロセス（テーマ2）に関係する。

1. ディジタル計測制御技術の特徴に関する取扱い
2. 既存プラントで使用されているディジタル技術より進歩している技術に関する取扱い（ディジタル技術は急速に進歩しており、原子力産業界ではその速度をコントロールできないが、その一方で、原子力産業の運用や規制には大きな影響を及ぼすものである）

なお、表3-1には、上記6つの技術的課題と標準的な規制アプローチとの関連をまとめる。

表3-1 ディジタル系の技術的課題による標準的規制アプローチへの影響

	規制アプローチ				
課題	深層防護	安全裕度評価	要求される品質	環境に対する品質	故障性
ディジタル計測制御技術の系統的特性	○	●	○	○	○
ソフトウェアの品質保証	○	○	●	NA	○
共通原因によるソフトウェアの故障	●	○	○	NA	○
ヒューマンファクタとマン－マシン・インターフェース	●	○	○	○	○
安全性及び信頼性の評価方法	●	○	○	○	●
民生用既製品のハードウェア及びソフトウェアの利用	○	○	●	○	○

注) ●：極めて重要、○：重要、NA：適用外

3.2 技術的課題

(1) ディジタル計測制御技術の系統的特性(System Aspects of Digital I&C Technology)

原子力発電プラントや他産業におけるディジタル系の利用実績から、その有用性は立証

されてきているが、その一方で、設計上あるいは設置上の問題（例えば、基本設計の変更が必要となる問題：フランスのN4プラントChooz-Bや英国のSizewell B[12, 13]、ソフトウェア変更の必要性：カナダのDarlington[14]）も生じている。これらの問題は費用の増加や建設・運転の遅れを招くだけでなく、複数の製造者から提供される部品で製作された、いわゆる、"open system"の利用を促すことになり、その結果、インターフェースの数が増え取扱いがより困難になる。

課題： ディジタル計測制御系の導入に伴い、新たな故障モードも発生し得る。従って、ディジタル計測制御系の設計及び設置に関する系統的特性を正確に取り扱うことが要求される。このためには如何なる方法が必要か？ ディジタル系の利用に関わる様々な技術者の経験をどのように集約し、原子力発電プラントに適用するか？ 将来、新しいディジタル計測制御技術や機器を導入する際、その方法やそれまでの経験を更新するために、如何なる手順を整備することができるか？

議論： ディジタル系における主要な特性としては、連続的動作、多重処理、メモリ共有、多様なデータ転送と保存媒体などがあるが、故障防止のためには、こうした特性を踏まえて、独立性、物理的・機能的分離及び多様性を確保することが必要となる。

（連続的動作）ディジタル計測制御系はデータを取り込みディジタル化して制御系プロセッサに転送する。こうした一連の制御シーケンス（パラメータの抽出や転送、制御コマンドの生成及び返送等）が、プロセス量の応答より速く行われるように設計しなければならない。ディジタル系では複雑な相互作用（送信チャンネルやメモリの共用、多重処理）があるため、こうしたタイミングに対する配慮が重要となる。

（多重処理）ディジタル計測制御系は、プロセス量や制御パラメータをサンプリングし、複数の共用の転送経路に伝達する。この多重処理は、上述したタイミングの問題にも関わっており、十分なバッファと伝達速度が必要となる。

（メモリの共用）ディジタル計測制御系は、設定データや基準値を用いて制御動作を行うなど機能を果たす。こうしたデータは多数のプロセッサからアクセス可能であるよう集中管理される。従って、メモリを共用する際には、あらゆる系統が一貫した正しい動作を行えるようデータを管理することが必要となる。

（データ転送及び記憶媒体）ディジタル計測制御系には光ファイバーや磁気ディスク等の媒体が用いられる。従って、こうした媒体がプラントの環境に対して十分な品質を維持できることを確認する必要がある。

新型炉、レトロフィットへの適用可能性： ディジタル系の特性を十分に活用することは、新型炉にもレトロフィットにも極めて重要な課題である。しかし、新型炉では大規模な系統が想定されるため、設計においては、系統構成やサブシステムの製作に自由度がある。これに対して、レトロフィットでは、変更対象が限定されるため、利用可能なディジタル系の特性も限られてしまう。また、一貫性のある変更を行うことも難しい。

(2) ソフトウェアの品質保証(Software Quality Assurance)

原子力発電プラントにおけるソフトウェアは、原子炉トリップ機能のような比較的単純な組合せ論理や、工学的安全施設作動回路やプロセス制御のような複雑なシーケンス論理を実行するために利用される。従来、これらの機能の幾つかは自動制御系により、また、その他は運転員により実行されてきた。いずれの場合も、必要とされる機能を実行したり、不必要なトリップを回避する上で、その信頼性は重要なポイントである。一方では、これまでに、Turkey Pointにおける電気負荷シーケンサの故障(LER 94-005-02)をはじめ、ソフトウェアの品質問題に起因するディジタル計測制御系の故障事例が数多く報告されている。

課題： ソフトウェアの利用がアナログ系とディジタル系との大きな違いである。ソフトウェアの品質は、仕様が適切か否か、仕様通りに作成されているか否かを調べることによって確認される。しかし、ソフトウェアの作成過程を管理したり、出来上がったソフトウェア自体を検証するという従来の方法だけは、適切な品質管理は行えない。では、ディジタル計測制御系ソフトウェアの仕様、作成及び工程管理に関し、USNRCや産業界は、一般的に容認される技術的な解決法をどのようにして定義することができるのか？

議論： ディジタル計測制御系に使用されるソフトウェアは、安全性及び信頼性の観点から品質の高いものでなければならない。特に、原子力発電プラントでは、単一の機能を実行するための簡単な論理制御や、トランジェントの検出及び原子炉停止系の作動など多数の装置を制御するものまで広範に利用される。従って、その品質保証は広範な適用と系統間相互作用を十分考慮して行わなければならない。ソフトウェアの評価は、その作成過程を調べること、あるいは、それ自身を評価することにより行うことができる。しかし、品質の高いソフトウェアの作成には、特殊な技術や工程が用いられており、その多くは訓練と経験を必要とするものである。従って、作成過程を調べるという方法を用いる際には、必要なレベルの専門知識がどのように担保されるかを示す必要がある。一方、ソフトウェア自体を評価する方法は、静的解析と動的解析に分類される。静的解析は、ソフトウェアの設計や試験結果等の検査に基づくものであり、動的解析は、ソフトウェアの動作に関する実験に基づくものである。しかし、ソフトウェアは、膨大な量の記述が不規則な構造をなしているため、試験や実験では極一部のみ調べられるものの、他の部分にエラーのないことを推論することは不可能である。また、当初は品質の高いソフトウェアが作成されても、新しいハードウェアを導入したり、新たな機能を設けたりする等の変更が行われるため、ソフトウェアのバージョンや変更部分の管理が問題となる。さらに、計算機技術の急速な発展に伴って、ソフトウェア開発の方法も急速に進歩し、評価方法の有効性に関する新しい知見も得られる。こうした発展に対応して、USNRCスタッフや産業界は引き続いて技術的知識を高めていく必要がある。

新型炉、レトロフィットへの適用可能性： ソフトウェアの品質保証は、新型炉にもレトロフィットにも同じように適用可能な課題である。

(3) 共通原因によるソフトウェアの故障(Common-Mode Software Failure Potential)

ソフトウェアに基づくディジタル系の信頼性を確保するための手段として、従来から用いられている冗長性の概念が提案されている。信頼性向上のために、冗長性と多様性を有するソフトウェアの利用が考えられるが、冗長性が必ずしも多様性を実現することにはならず、共通原因故障(CMF : common mode failure)を免れる訳ではない。勿論、既存のアナログ系も同様であるが、多様性に対する設計や試験を行うのはソフトウェアに比べて容易である。

課題： アナログ系におけるCMFを評価するために多種多様な方法が開発されてきたが、これらの方法がソフトウェアに基づくディジタル系へ適用可能であるか、あるいは、別の方法が必要か？ ソフトウェアの多様性とは何か？ その多様性の実現や評価は可能か？ 計算機を含むCMFを評価するための方法は存在するか？ 許認可プロセスに対してソフトウェアのCMFはどんな意味を持つか？ 冗長性や多様性はディジタル系の信頼性を確保するために最も有効な方法であるか？

議論： ハードウェアでは、冗長性や多様性を持たせることにより、故障の発生確率を低くすることができるが、KnightやLevesonの実験[11]等によっても示されているように、ソフトウェアでは、独立に作成された場合でも独立に故障するとは限らず、従って、単に独立のプログラマーを採用しても多様性は実現できない。さらに、独立に作成されたソフトウェアにおいてCMFを取り除くのは容易ではない。ソフトウェアの仕様の一部を共有することでCMFに繋がることがあり、また、これと同じような問題が、試験データの作成時にも存在する。同一の設計仕様に従って独立にプログラミングを行うことは、コーディング・エラーを防ぐのには有効であるが、その一方で、これまでの実績から、ほとんどの安全上の問題（エラー）はソフトウェアに対して要求される動作（機能）を誤解したことに起因していることが示されている。

新型炉、レトロフィットへの適用可能性： 共通原因によるソフトウェアの故障に関する課題は、レトロフィットにも新型炉にも適用すべきものである。しかし、新型炉の方がソフトウェアを広範に利用するため、重要性は高いと考えられる。レトロフィットに対しては、変更した系統におけるCMFの可能性をどう評価するかが重要となる。

(4) ヒューマンファクタとマンーマシン・インターフェース(Human Factor and Man-Machine Interfaces)

ディジタル計測制御系等の新しい技術を導入する際には、ヒューマンファクターとマンーマシン・インターフェース(MMI)を十分考慮する必要がある。特に、計算機技術、計算機に基づくインターフェース及び運転員支援の利用においては、運転員による操作、修理、維持管理に関連して重要な課題が生じる[15]。従って、ディジタル計測制御系を原子力発電プラントに使用する場合には、その設計や設置において人間の役割を適切に考慮しなければならない。

課題： 計算機に基づくMMIが運転員に及ぼす影響の評価方法については、USNRCと産

業界の間で合意が得られていない。ヒューマンファクター及びMMIが適切に考慮されているかを確認するために、如何なる方法を用いるべきか？

議論：　適切なヒューマン・パフォーマンスの確認は、アナログ系にもディジタル系にも同じように適用可能である。しかし、ディジタル系には、多くの特性がある。例えば、

(a)ディジタル系を利用した制御室及び制御盤は、従来のものよりかなりコンパクトになる傾向があり、その結果、多くの制御と表示の機能が並行して行われるため、良好なヒューマン・インタラクションが得られることを確認する必要がある。

(b)ディスプレイは、しばしば、集約的な表示形態となっており、情報は複数ページにまたがって保存される。従って、表示のロジック、情報量及び表示形式が重要な課題となる。

(c)多くの運転員は、アナログ系に基づいた大きな固定配置式の制御盤に慣れており、プラント状態の診断や必要機能の実行は“パターン認識”方法を用いて行っている。しかし、ディジタル系では、コンパクトな並行利用式であるため、こうした方法は利用できない。従って、設計においては、運転員のスキルを有効に利用しエラーを避けるよう運転員の特性等を配慮しなければならない。

(d)自動化を導入する際には、システムの運転モード、自動から手動への切替条件、運転員操作に関する制約、運転員操作の必要な状況、操作手順を運転員が認識できるようシステムを設計する必要がある。

(e)ディジタル系には、制御、警報及び表示の構成に柔軟性があり、警報の表示や制御操作の順序に優先度を設けることが可能である。しかし、その一方で、運転員が混乱してエラーを起こさないようシステムを設計することが要求される。

(f)保守、特に、ソフトウェアの保守は従来とは異なるため、保守の方法はかなり変更する必要がある。また、保守員には特殊なスキル（プログラミング、ディスプレイ設計、ソフトウェアの試験等）が要求されるため、保守方法の変更は、その妥当性を評価し、変更によるエラーの導入が無いことを確認する必要がある。

新型炉、レトロフィットへの適用可能性：　ヒューマンファクター及びMMIの問題は、新型炉にもレトロフィットにも適用可能であるが、その内容は異なる。新型炉におけるMMIはディジタル計測制御系を前提に設計、試験、評価される。これに対して、レトロフィットでは、プラント制御系の一部が影響を受けることとなり、変更部分をどのようにして既存の設備に統合するかを考慮して設計する必要がある。さらに、変更部分に関する技術や訓練を行う等の配慮も必要となる。

(5)　安全性及び信頼性の評価方法(Safety and Reliability Assessment Methods)

ディジタル計測制御系の容認性を確認する上で、その安全性及び信頼性を評価する方法は重要である。こうした方法は、信頼性の推定、安全裕度の評価、安全目標等の規制基準との比較等が可能であり、ディジタル系の導入が公衆の安全性向上に繋がることを示す上で有用なものでなければならない。

課題：　ディジタル計測制御系の安全性と信頼性を評価するために、効果的かつ効率的な

方法が必要であるが、如何なる方法が用いられるべきか？

議論： 安全性や信頼性を評価するための方法は、これまでに数多く開発されてきたが、これらをディジタル計測制御技術に適用することが難しい。確率論的評価は、ソフトウェアがあらゆる状況において正確かつ安全に動作することを確信するために、必ずしも最良の方法ではない。"symbolic logic"を用いた数学的な証明方法の方が、確率論的評価よりもソフトウェアには適していることが提案されている。既存の評価方法に頼れば、ディジタル系導入の度、ケースバイケースの評価及び許認可のプロセスが行われることになる。また、既存の方法では定量化が困難であり、公衆はディジタル系の安全性に疑問を抱く可能性が生じる。従って、USNRC、産業界及び公衆がディジタル系の導入による利点とリスクを評価できるだけの能力を有することが不可欠である。また、安全裕度の評価は規制プロセスの核であり、その評価方法を確立しなければならないが、そこでは、以下の要件を満たす必要がある。

- 決定論的及び確率論的な評価を含むこと
- 方法及び結果が理解できること
- 組み込まれている試験や診断機能の効果を評価できること
- 適切な専門家グループに容認されるものであること
- ある程度の経験的な試験を受けたものであること
- 複数の申請において一貫性のあるものであること
- 公衆が理解でき信用できるものであること
- ディジタル技術の急速な進化に対応可能であること

新型炉、レトロフィットへの適用可能性： この問題は、新型炉にもレトロフィットにも重要であるが、その内容は若干異なる。新型炉のディジタル計測制御系は、プラント全体の枠内で評価されるべきものであり、より一般的な方法を利用することができる。また、プラント設計の段階で試験や評価を十分に行う余裕がある。これに対して、レトロフィットでは、プラントあるいは計測制御系の一部だけに着目した評価方法となり、さらに、レトロフィットの評価は、全体設計に適用できない特殊の課題（レトロフィット部分と残りの部分とのインターフェース、運転員や保守作業等への影響）を示唆している。

(6) 民生用既製品のハードウェア及びソフトウェアの利用(Dedication of Commercial Off-the-Shelf Hardware and Software)

原子力発電プラントにおいては、民生用既製品(COTS：commericial off-the-shelf)型のハードウェア及びソフトウェアの利用が増えつつあるが、これは、原子力産業界における市場が小さくなっていることや、軍事等の他産業における民生品の実績が蓄積されていることによる。アナログ機器に対しては、その利用形態が確立されているが、ディジタル機器については、ソフトウェアの正確さの確認や故障モードの同定・評価を必要とすることから、民生品の利用形態は難しくなる。原子力発電プラントでの利用を前提として開発されるディジタル機器やソフトウェアに対しては、ソフトウェアの設計や作成過程を管理し、

その検証や性能評価を通して要求された品質が保証される。一方、民生品の場合には、一般に、こうしたプロセスを経ずに利用される。現時点で、民生用のディジタル計測制御機器及びソフトウェアの品質保証に関する問題を解決する方法について合意が得られていない。

課題： 原子力発電プラントの安全系におけるCOTS型ディジタル計測制御系の利用を評価し容認するために、規制当局と設置者は、如何なる方法に対して合意を得るべきか？

議論： ディジタル計測制御系へのCOTSの利用は、経済性の観点から重要な課題である。安全系への導入でなく産業界の性能基準を満足していれば、民生品の利用は可能である。しかし、プラントの安全性や許認可に影響を及ぼし得る系統への利用では、より高い基準を満足しなければならないし、規制当局も製品の性能や品質が許認可条件を満たしていることを確認しなければならない。従って、性能や品質の評価には規制側と産業界との合意が得られた方法が必要となる。この方法は、原子力発電プラント用に製作された製品に対する評価方法とは異なる。現在、COTS型ディジタル機器は、アドホック的に利用されているが、COTSを利用することによるメリットを示すためには、より明確に定義された方法が必要となる。そこで、解決すべき課題は、製品の故障モードにどう対処するかである。

新型炉、レトロフィットへの適用可能性： この課題は、新型炉及びレトロフィットの両方に同じように適用可能であるが、アナログ系機器の経年劣化に伴い民生品の必要性が高い既存プラントに対してはより重要な課題である。

3.3 施策的課題

(1) ケースバイケースの許認可プロセス(Case-by-Case Licensing Processes)

ディジタル計測制御技術を安全系に利用することにより、許認可及び規制の分野において特殊な問題が生じる。ディジタル技術は急速に進歩するため、機器のライフサイクルが許認可で要求される期間あるいは機器の保証期間より短くなる可能性がある。従って、安全性の観点から容認可能な方法でディジタル技術が利用されることを確認しつつ、規制レビュープロセスは、ディジタル機器の急速な進歩について行かねばならない。これまでのレビュープロセスは、ケースバイケースで行われてきた。電力会社もUSNRCも十分な経験を有しているわけではないため、ケースバイケースのプロセスにはメリットがあるが、数多くの問題点も生じている。例えば、ディジタル系への変更に対する明確な規準がなく、容認性を評価すること及び規制承認を得るために何が必要かを把握することが困難である。また、規準がないことにより一貫性のない規制レビューが行われ、アナログ系に要求される以上のものが要求されることもあり得る。さらに、ケースバイケースのアプローチには時間が掛かり、場合によっては、電力会社にとっても規制側にとっても多大な労力を要するプロセスとなる。最後に、ディジタル系への変更を行う際USNRCによる事前の承認が必要か否かを判断するために、10 CFR 50.59に従ってその変更を評価することになるが、その適用に関して、USNRCは一貫性のある方針を打ち出していないという問題がある。

課題： ディジタル計測制御系の規制をより効率的かつ効果的に行うために、規制プロセスにおいてどのような変更がなされるべきか？ ディジタル計測制御技術が急速に進化するという特性に対応するためには、どのようにして規制プロセスに柔軟性を持たせるか？どのようにして規制プロセスの効率化を図ることができるか？

議論： 新規プラントに対する許認可プロセスでは、USNRCと申請者がまず、品質保証と設計プロセスを規定し、設計上の制約、制限及び属性を定義する。これらが満足されれば設計が認可される。設計上の制約、制限及び属性に関する詳細が固まれば、USNRCは詳細設計をレビューし最終的な安全評価に至る。レトロフィットに対しては、USNRCは、まず、システムの特徴に関して申請者と合意を得るが、その後レビューのための詳細な情報を要求する。これまで、規制当局は、ディジタル制御計測技術を用いた設備変更によってUSQ（この内容は、10 CFR 50.59に定義されている）が生じると結論づけられた場合にはレビューを行うというアプローチを取ってきた。即ち、設備変更によってUSQが生じた場合には、プラントの運転開始前に承認を得る必要があり、さらに、許認可の条件にも影響を及ぼし得るため、レビュープロセスが必要となる。現行の規制構造はディジタル系の利用に対応していないため、規制レビューはアドホック的なものになりがちである。レビュープロセスに入る段階で、明確な容認基準の設定や、設備変更の容認性を立証するために必要な費用や労力の算定は困難である。従って、変更の際の要求項目が何であるか、また、変更部分の設計や品質についてどの程度の文書が要求されるのかがかなり不確かであるため、ディジタル計測制御系の導入に支障が生じることも考えられる。ケースバイケースのレビューが標準的な方法であるとしても、ディジタル技術が急速に進歩するという性質を踏まえ、レビュー経験から得られた試験を容易に反映させて、その基本プロセスを再考する必要がある。

(2) 技術基盤の適性(Adequacy of Technical Infrastructure)

アナログ系は長年の実績もあり、規制側も設置者側も十分理解しているが、ディジタル系に対する理解は十分ではない。さらに、ディジタル技術の進歩は急速であるため、その時点での最新の技術を習得し、その後の変更にも対応できるよう努力する必要がある。これは、規制側にも設置者側にも共通した問題である。

課題： ディジタル計測制御技術の規制活動を支えるために、USNRCは、スタッフの構成、訓練及び研究プログラムにおいて変更を行うか？ USNRCにとって適切なプログラムは何か？ 予算削減の中で、急速に進歩する技術に対応して同プログラムの有効性を維持するためには、プログラムをどのような構成にするべきか？

議論： USNRCは、その諮問機関であるACRSから、ディジタル技術に関する技術スタッフの育成と訓練が不十分であるとの批判を受けた[16]。その理由として、米国における新規プラントの建設が無いこと、原子力に興味を持つ技術系の学生が減少していること、USNRCの予算が削減されていること、等が挙げられる。また、USNRCの訓練センタにあるシミュレータがディジタル系によるレトロフィットに対応しておらず、訓練に対する予

算も削減されていることからニーズに応えられない状況にある。一方、研究プログラムについては、現在の研究が、直面している幾つかの規制上の課題を解決できるかもしれないが、それぞれが体系的に行われていないという問題がある。限られた財資を有効に利用し全ての課題に対する解決策を得るためには、より体系的で一貫性のある施策プランが必要となる。こうしたプランを立てることで、USNRC及び産業界での研究活動を調整し協力体制を整えることになる。現在の関心は主にレトロフィットにあるが、新型炉ではより広範にディジタル技術が利用される。さらに、ニューラルネットワーク、マルチメディア、光センサやデータハイウェイ等の新しい技術が提案、開発されつつあり、今後の規制及び技術支援体制では、こうした新技術への対応も要求される。

4. 重要課題の分析と米国原子力規制委員会の対応

4.1 技術的課題

(1) ディジタル計測制御技術の系統的特性(System Aspects of Digital I&C Technology)

(技術的動向)

米国内の原子力産業界： 米国では、過去20年間、新規プラントの建設は行われていない。しかし、GE(General Electric)社製のABWRやSBWR、WH(Westinghouse)社製のAP600、及び、ABB-CE(Asea Brown Boveri - Combustion Engineering)社製のSystem80+といった新型炉が設計されUSNRCによってレビューされてきた[17, 18]。これらのプラントは、ディジタル計測制御系の利用を前提として設計されている。USNRCは、こうした設計レビューを通して、現行の規制ガイダンス文書を改訂・更新する必要性を認識しており、そこでは、(a)ディジタル系の応答時間と詳細構造を確認するためのガイダンスを示した新規の部門技術見解(BTP：branch technical position)と、(b)データ通信やマルチプレクサに対する容認基準とレビューガイダンスを示した標準レビュープラン(SRP：Standard Review Plan)の7.9節（新規）を策定することとしている[19]。

一方、産業界では、費用効果性の高いディジタル系への移行が進むにつれ、データ通信や構造等ディジタル系の特性に関するガイダンスの整備を行ってきた[20]。

米国外の原子力産業界： 米国外では、英国のSizewell-B、フランスのChooz-B、カナダのDarlington、日本の柏崎-6において、完全なディジタルベースの計測制御系が導入された。Sizewell-B[21]では、制御及びデータ取得のためのディジタル系と保護機能を有するディジタル系が導入され、データ母線用のコンダクタの多重化や保護系の多様化等あらゆるレベルで多重性が設けられた。また、計算機ベースのシステムのバックアップとして、ハードワイヤ式の計測制御系が設置された。Chooz-B[22]では、3レベル構造が採用された。第1のレベルは、ディジタル保護系であり、炉心及び格納容器の健全性を維持しつつプラントを安全状態へ移行させる役割を果たす。第2のレベルでは、ホウ酸制御、圧力及び温度制御、並びに、二次系給水の監視等の機能を果たすために、在来のハードウェアが使用され

ている。第3のレベルは、制御室におけるマンーマシン・インターフェースであり、これには、ハードワイヤ式の制御系を使用し計測制御系の最下層に直接接続している。Darlington[23]では、制御系のほぼ100%と保護系の70%以上にディジタル系が使用されている。柏崎-6は、米国でレビュー中のABWR設計と同等であり、それに対する要求を満足している。このうち3基のプラントでは、系統特性に関する問題が発生している。具体的には、フランスのN4プラントChooz-Bや英国のSizewell Bでは、基本設計の変更が必要となる問題が発生し[12, 13]、また、カナダのDarlingtonでは、許認可プロセスにおいてソフトウェアのレビューを行った結果、使用には支障がないものの変更の必要性が生じたためソフトウェアの書き直しが必要であることが判明した[14]。柏崎-6では、制御系の一部に問題が生じたが起動計画において解決されたと報じられている。

他産業分野： 航空宇宙産業では、安全上重要な系統にディジタル系が幅広く使用されている。系統特性は種々の研究の対象となっているが、その結果、運転モードの自動変更が運転員の混乱を招くことの重要性が指摘された[24]。化学産業は、(a)類似の液体状態を扱うこと、(b)類似の回転機器を使用すること、及び、(c)種類は異なるがかなりの量のエネルギーを貯蔵することから、原子力産業とかなり似通っている。化学産業では、1970年代後半からディジタル系を広範に使用しており、重要な系統特性（プロセス制御系の健全性、プロセス・ハザード、制御ストラテジー、安全上の配慮、データ通信用媒体、等）に関する詳細を示したガイドラインを整備してきた[25]。

（議論）

系統特性を扱うにあたり、考慮すべき幾つかの重要な因子がある。第1に、3種類の新型プラントの設計レビューがUSNRCによって行われているが、次の数年間新規立地計画はなく、従って、米国におけるディジタル系の実績は、設計変更や限定された設備改善に限定される。第2に、系統特性の取扱いはUSNRCだけの責任ではない。これは、系統特性が安全系と非安全系の双方に当てはまるものであり、規制対象となるのは極く一部の計測制御系にすぎないためである。従って、産業界は、非安全系に対して系統特性が適切に扱われていることを確認しなければならない。米国外でのプラントで生じた問題やその経験から得られた教訓は、非安全系が問題を引き起こすことがあることを示している。例えば、Sizewell-BやChooz-Bで起こった問題は非安全系に関わるものであった。USNRCと産業界は、非安全系の故障がプラント設計に影響を及ぼすため、安全系をこうした影響に耐えられるよう適切に設計しなければならないとの認識を持っている。第3に、米国のプラントにおける現行の計測制御技術はアナログ機器に基づくものであり、ディジタル機器の系統特性に関する規制ガイダンスはほとんどない。

（結論と勧告）

結論

・ ディジタル計測制御の系統特性に対処するために、 USNRCと原子力産業界は継続的な努力を行う必要がある。

・ 大規模な計測制御系の設計・設置した実績が欠如しているため、 USNRCと原子力産業界が経験を活かして系統特性にどのように対処するかに関する基盤を確立することが困難である。
・ ディジタル計測制御技術の適用においてUSNRCは規制ガイダンスを改善しようとしているが、この意向を尊重すべきである。
・ 現行の規制ガイダンスは具体性に欠けているため、これを補うための改訂が必要である。

勧告

1) （米国内での大規模なディジタル計測制御系の設計や設置が困難な状況にあることから）USNRCは、提案された規制ガイダンス文書を米国外の原子力発電所のディジタル系に試行的に適用すべきである。特に、このレビューでは、改訂されたガイダンス文書がディジタル系の系統特性を適切に説明するのに必要なレベルの具体性を有しているか否かを評価することに着目すべきである。
2) USNRCは、大規模なディジタル系を採用している化学プラントや航空機などの他産業における系統特性に関するガイダンス文書を同定・レビューすべきである。このレビューでは、それらのガイダンス文書とUSNRCが整備しているガイダンスを比較することに主眼を置くべきであり、特に、共通の問題点や適用にあたっての固有の差異に注意すべきである。
3) 実践的な経験を積むために、USNRCは、大規模で安全上重要なディジタル計測制御系を規制・監督する他機関にスタッフを派遣すべきである。
4) USNRCは、特に系統特性に関連する技術についてスタッフのトレーニングを継続して行うべきである。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「規制ガイダンスの米国外プラントへの適用」に対して

USNRCは、規制ガイダンスを米国外の原子炉に適用することには同意していない。米国外への適用は、当事国の規制当局と電力会社の賛同と参加を得なければできないものであり、また、国によってディジタル系に対する要求が異なるためこうした適用が必ずしもガイダンスの有意義な評価になるものでもないと考えられる。しかしながら、一方で、米国外の機関による使用例もある。

・チェコのTemelinでは、WH社製のディジタル計測制御系のレビューにSRPの7章が用いられており、USNRCスタッフはチェコの規制当局と、レビュー結果に関する討議を継続的に行っている。
・韓国の規制当局(KINS)は、SRPの7章の適用に興味を抱いており、韓国原子力研究所(KAERI)が計算機ベース・システムの設計に対して独自のガイドラインを策定するためにSRPを参照している。

・NUREG-0700改訂版を、フランスのN4プラント制御室に関するヒューマンファクタの特性を評価する際に使用することが計画されている。

勧告2)「他産業におけるガイダンスのレビュー」に対して

USNRCは、本勧告に同意している。規準やスタッフによる研究の策定や更新の際には、通常、本勧告に示されているようなタスクを行っている。SRPの7章を改訂する際にも、USNRCスタッフは産業界との討議の場を持って、ガイダンス策定に有用な情報を入手しており、こうした活動は継続して行うこととしている。例えば、規制ガイダンスでは、ボーイング社やソフトウェア生産協会からの情報や、IEC、国際標準化機構(ISO：International Organization for Standardization)、IEEEなどの規準を参考としている。さらに、今後、他産業におけるディジタル系の利用やUSNRCのガイダンスとの関係に関する調査をはじめとする活動を行うこと予定している。

勧告3)「他規制機関へのスタッフ派遣」に対して

USNRCは、本勧告を実施するに十分な人員が確保できないため、同意していない。他産業における規制機関とは、機関間会合などを通して、相互の情報交換を既に行っている。

勧告4)「スタッフトレーニング」に対して

USNRCは、本勧告に同意している。スタッフは、ディジタル技術の様々な特性に関するトレーニングに参加してきている。現在進行中の内部トレーニングを継続して行う予定である。さらに、ディジタル計測制御系に関するスタッフの能力開発に対するガイダンス（NUREG/BR-0227）を策定しており、ディジタル系の問題に関する能力の開発と維持を図っている。また、スタッフを特別のプログラムに参加させ、ディジタル系に関する個人の専門知識の向上を図っている。

(2) ソフトウェアの品質保証(Software Quality Assurance)

（技術的動向）

米国内の原子力産業界： ソフトウェアの品質保証に対するUSNRCの規制基準は以下に示す通りである。

・10 CFR 50.55a(h)（規則及び規準：原子炉保護系）：IEEE 279-1971の使用を承認
・10 CFR 50, Appendix A, 基準1（品質規準及び記録）, 基準21（保護系の信頼性及び試験可能性）, 基準22（保護系の独立性）, 基準29（運転時の想定事象に対する保護）, Appendix B（品質保証基準）

さらに、ソフトウェアをレビューする際に、USNRCの規制指針1.152（安全関連系におけるディジタル計算機システム・ソフトウェアに関する基準）とANSI/IEEE/ANS-7-4.3.2-1982（安全系におけるディジタル計算機に関する基準）を使用している。また、参考資料として、IEEE 1012-1986（ソフトウェアの性能及び妥当性評価計画に関する基準）やASME NQA-2A-1990（計算機システムの利用に関する品質保証要求）等も用いている。

USNRCによる性能評価と妥当性評価(V&V : verification and validation)プロセスのレビューは徹底的に行われるものと考えられる。例えば、Zion-1,2に導入されたEagle 21原子炉保護系に対するV&Vプロセスのレビュー[26]では、ANSI/IEEE/ANS 7-4.3.2-1982との比較、V&V実施者の独立性確認、機能的要求の検討とその後のソフトウェア作成に関する文書のレビュー、ソフトウェアにおける問題点とその対処策のレビュー等が行われた。さらに、プラント・パラメータのサンプルを取り出し、要求検討からソフトウェア試験までの一連のプロセスをレビューすると共に、ソフトウェアとハードウェアとの間のタイミング問題についても調べた。また、408個の問題からランダムに56個を選び出した結果、その21%が要求との不整合やロジック欠陥によるものであることが明らかとなり、作成者による機能試験を拡充させるために厳格なV&Vが必要であるとされた。ディジタル技術の導入に対応して、SRPの7章の改訂が進められている。具体的には、2つの節（7.8節：計測制御系の多様性と7.9節：データ通信）が追加され、さらに、ソフトウェアの作成プロセスやプログラム式のロジック制御などに関する新たなBTPが取り込まれる。その一環として、下記の10種の産業界規準を容認するため規制指針の改訂も進められている。

・IEEE 7-4.3.2-1993：安全系のディジタル計算機に関する基準
・IEEE 603-1991：安全系に関する基準（IEEE 279-1971の続報）
・IEEE 828-1990：構成管理計画に関する規準
・IEEE 829-1983：ソフトウェア試験の文書化に関する規準
・IEEE 830-1984：ソフトウェアの要求仕様に関する指針
・IEEE 1008-1987：ソフトウェアの単体試験に関する規準
・IEEE 1012-1986：ソフトウェアの性能及び妥当性評価計画に関する規準
・IEEE 1028-1988：ソフトウェアのレビュー及び審査に関する規準
・IEEE 1042-1987：ソフトウェアの構成管理に対する指針
・IEEE 1074-1991：ライフサイクル策定に関する規準

さらに、安全系に使用されるプログラム言語の長所・短所の評価や故障事例の分析などの研究も進めている。

一方、産業界は、要求事項の分析と構成管理を強化することが高品質のソフトウェアを作成するために重要であるとの見解を示している。また、プラント設計では、安全系と非安全系のソフトウェアが同一の計算機上で走らないよう分離させているものの、安全系と非安全系のソフトウェアに対して要求事項の分析と構成管理を厳密に行うべきであると認識している。安全上重要な計算機上で稼働するソフトウェアには厳しい規準を適用しなければならないのは明らかであるが、非安全系でも安全系と同様の不具合が生じる可能性があるため、安全系と同等の要求を課すべきであると主張している。さらに、産業界は、V&Vの一部としてハザード解析を行うべきと考えており、実際、ある電力会社は、ハードウェアーソフトウェア間相互作用、ソフトウェアの作成プロセス、少数の機能に関する解析、及び、機器ベースの故障解析についてレビューを行った。

米国外の原子力産業界： 米国外（日本、英国、カナダ）の動向として、まず、日本（三菱重工業）では、ソフトウェアの品質保証をIEC 880（安全系における計算機ソフトウェア）の規準に準じて行っている。また、英国では、独自のガイドラインを策定しているが、Sizewell-Bの主保護系(PPS : primary protection system)の試験結果についてかなりの議論が起こった{27}。試験結果の大部分は、（予測モデルによる解析結果と試験結果とを比較するという）テストドライバーを用いることで自動的に確認できるものと想定されていたが、実際には、最初の50000回の試験の約半分しか自動的には確認できず、結局、試験の50%でPPSが故障する結果となった。PPSとテストドライバーとの間でタイミングの問題が生じたため、人手による試験結果の検査が必要であった。例えば、仕様上に問題があったため、時間遅れやその設定点におけるエラーが見つかった。この経験から得られた結論は、要求事項の完全性と構成管理に関する問題があったということであり、具体的には以下の通りである。

・PPSの応答時間を理解するには要求事項の他に設計に関する知識も必要である。
・履歴現象（磁力の変化に反応する時間遅れ）はオリジナルの機能仕様には含まれていたが、試験グループには伝えられていなかった。
・幾つかの入力に関するデフォルトの動作が仕様に記載されていなかった。

一方、カナダでは、原子力管理委員会(AECB)がDarlingtonにおける計算機利用の停止系を認可したが、最初は、安全上重要なソフトウェアに対する"good enough"が如何なるものかを明確に示していないことについて異論を提示した。そこで、設置者は、formal methodを用いてソフトウェアとその要求事項との間に整合性が取れていることを示すと共に、ランダムに試験を行って事故シナリオをモデル化しシステムの信頼性を実証した{28}。また、産業界は、ソフトウェア工学プロセスにおいて満足すべき要求規準OASESを策定してきたが、この規準では、ソフトウェア工学プロセスの他、プロセスの各ステップにおける手順と、どのようにソフトウェアの品質を決めるのかに関するガイドラインを定めている。さらに、AECBは、ソフトウェア評価のためのドラフト規制指針C-138（保護制御系におけるソフトウェア）を策定しており、この指針では、ソフトウェアの完全性、正確性及び安全性を第三者がレビューし理解するよう求めている。高品質のソフトウェアであることを示すためには、要求仕様、設計及び作成に関する体系的検査、試験、及び、作成プロセスとその管理等が重要であるとし、ドラフト規制指針において、下記の容認基準を示している。

・要求事項は、曖昧さがなく、一貫性があり、さらに、完全であるものとする。
・体系的検査には、ソフトウェアが課せられた機能を果たすことを実証するための機能的解析と、不安全な動作をしないことを確認するための安全解析が含まれるものとする。
・機能試験及びランダム試験を行うこととし、前者は通常状態及び境界条件におけるエラーを見つけるために行い、後者は特定の条件下で支障無く機能を果たすことを実証するために行うものとする。
・ソフトウェアの設計及び製作方法は、急速に進化しているため、ある種の方法を規定す

るのではなく、ソフトウェアがその開発及び品質保証プランに従って適切な技術者により作成されるよう明記する。使用した方法は完全性や整合性に関するレビューが可能であるものとする。

・構成管理により変更を管理することとする。変更点はレビューできるものとし、それに応じて設計や試験計画も更新するものとする。

(ソフトウェアの品質保証に関する問題：実事例の分析)

ソフトウェアの品質保証において如何なる問題が生じているかを理解するために、数多くの設置者事象報告書(LER)がレビューされた。Diablo Canyon(LER 92-028-00)、Salem(LER 92-107-00)及びTurkey Point(LER 94-005-02)の事例では、ソフトウェアの設計エラー、要求及び設計の不適切なレビュー、V&V手法としての試験への過剰な依存、及び、構成管理上の問題が明らかとなった。特に、Turkey PointのLERでは、非常用電源の負荷シーケンサに民生のプログラマブル・ロジック制御装置(PLC)を使用した際の問題が取り上げられている。民生のPLC導入に際しては、EPRI NP-5652（商用製品の安全系への利用に対するガイドライン）に示されるガイダンスに基づき品質を確認し、さらに、IEEE 1012-1986とUSNRCの規制指針1.152（ANSI/IEEE/ANS 7-4.3.2-1982を承認）に従ってV&Vを行って負荷シーケンサの冗長系に共通原因故障のないことを確認した。それにも拘わらず、ソフトウェア・ロジックの欠陥により4個のうちの幾つかの負荷シーケンサが安全注入(SI：Safety Injection)信号に反応しないというトラブルが発生した。具体的には、テスト・シナリオにSI信号が15秒以上継続した場合、テスト信号が解除されても禁止信号は保持されシーケンサの動作を妨げるというものであった。設計者と検証者はいずれも禁止ロジックとテストロジックの間に相互作用があることを認識できなかったのである。USNRCは、当該事例をレビューし、V&V手法として試験への依存度が高すぎるという欠陥があったものと結論づけた。

一方、USNRCとAECBは、原子力発電プラントにおけるデジタル系の故障事例の分析を行っている。USNRCの分析[29]では、79件のLERを対象に、根本原因別に事例を分類した。表4-1に示すように、30件はソフトウェアのエラーによるものである。また、AECBの分析[30]では、459件の事例を対象としており、そのうちの117件はソフトウェアに関わるものである（表4-2参照）。さらに、これら117件のうちの104件はアプリケーション・ソフトウェアに関するものであり、また、オペレーションシステムとデータベースに関わるものがそれぞれ5件である。

フェノール工場で使用されるPLC事例の分析[31]によれば、年2回の頻度でプロセッサの故障が発生しているとのことである。また、7年間の運転期間においてPLCが全て故障した事例もあるが、ソフトウェアのエラーに起因する故障はなかった。なお、フランスの原子力発電プラントでインターロックに使用されている冗長PLCについては、3年間で1,200の母集団に対して冗長PLCが両方とも故障したのは58件であった。これらのデータを評価した結果、システムの規模と複雑さが重要な因子であるとされた。また、システムによって

は、ソフトウェアのエラーによる故障が、ハードウェアの故障と同程度の頻度で発生し、システムの故障に対して重要な寄与因子であるものの、ソフトウェアのエラーは、異常な入力データの組合せが存在した場合にのみ顕在化するため、発生防止が困難であると結論づけられた。

表 4-1　1990-1993 年に米国で発生したソフトウェア関連事例[29]

事象原因	事象件数
ソフトウェア・エラー	30
マン－マシン・インターフェース上のエラー	25
電磁波干渉	15
機器のランダム故障	9

表 4-2　1980-1993 年にカナダで発生したソフトウェア関連事例[30]

事象原因	事象件数
ソフトウェアの問題	117
マン－マシン・インターフェース上の問題	130
ハードウェアの問題	220
外的要因（電磁波干渉など）	39
その他	37

（議論）

ソフトウェアの作成過程においてエラーが導入される確率を低減するために良好なエンジニアリング・プラクティスを利用し、さらに、エラーの検出確率を上げるために厳密な評価プロセスを経ることによって、品質の高いソフトウェアが得られる。しかしながら、良好なエンジニアリング・プラクティスの利用は容易ではなく、また、エラーを取り除くのではなく減らすにすぎない[32]。従って、ソフトウェアの評価は依然として重要な問題である。V&Vは、作成過程やソフトウェア自身のいずれかに着目して行うことが可能である。過程に着目したV&Vでは、一般的に、検査の実施と試験結果の評価が行われ、製品に着目したV&Vでは、作成過程には関係なく、最終的な製品であるソフトウェアの試験と評価を行う。作成過程を調べるという方法を用いる際には、必要なレベルの専門知識がどのように担保されるかを示す必要がある。現在、特殊な作成過程の提案や実験的検証が進められているが、こうした作成過程を採用することによって品質の高いソフトウェアが実際に作成できるか否か、また、どの程度の品質のものになるかについて、統一的な見解や確証は得られていない。一方、ソフトウェア自体（製品）を評価する方法は、幾つか有るが、これらは、静的解析と動的解析に分類される。静的解析は、ソフトウェアの設計や試験結

果等の検査に基づくものであり、動的解析は、ソフトウェアの動作試験に基づくものである。ソフトウェアの検査（静的解析）では、作成者チームが欠陥を見つけるために構造を調べることになる。欠陥を見つける上で検査が有効な方法であることは立証されている{33}。特に、要求事項に関する検査は、エラーが設計や製作に導入される前に検出することになり、修復のための費用も少なくて済む。また、設計に関わっていない複数の人によって検査を行うことも必要である。検査が成功するか否かは、実施者の経験とソフトウェア自体の質に依存し、また、レビュー者が文書をチェックできるよう要求事項が正確かつ明確に表現されているかどうかにも依る{34}。数学的手法を用いたformal methodによる性能評価では、ソフトウェアに関する詳細な記述と、その特性に関する概念的な記述とを比較するが、formal methodによるプログラムの特性評価は極めて困難であることが証明されており{35, 36}、さらに、数学的に立証されてもソフトウェアが正しく動作することが保証される訳ではない。従って、formal methodを用いて性能評価を行っても、試験によってその前提条件が妥当であることを示すことが必要である。ソフトウェアの動作試験（動的解析）は、プログラムの欠陥を見つけソフトウェアの信頼性を推定するのに用いられる。black-box試験は、ソフトウェアが要求通りに動作するか否かを調べるもので、入力と出力だけが対象となる。white-box試験は、ソフトウェアの内部構造を調べるものである。試験実施者は、ある状態に対してソフトウェアが正常に動作すれば他の場合にも同様に動作すると推測できるようなテストケースを決めようとするが、複雑なソフトウェアでは記述文が膨大で不規則な構造をなしているため、試験では一部のみ調べることになり、他の部分にエラーのないことを推論することは不可能である。要するに、プログラム試験は、バグの存在を示すのに用いるのであって、バグの無いことを示すのではない{37}。

この他に、信頼性成長モデル(reliability growth model)と信頼性モデル(reliability model)という方法が提案されており、前者は、作成段階における平均故障時間(MTTF：Mean Time to Failure)の予測、後者は、作成終了後におけるMTTFの予測に用いられる。しかし、これらの方法は、”ソフトウェアは修復される度に故障率が減少する”、及び、”MTTFはプログラムの大きさに依存しない”といった幾つかの疑わしい仮定に基づいている{38}。また、英国の防衛システム{39}に見られるような、安全管理及びソフトウェア工学に関する基準が提案されているが、その幾つかは、具体的な方法を示しているものの、一方では、メモリの動的割当、再帰法、人工知能技術等のソフトウェア特性の利用を妨げている。

ソフトウェアの規準は、容認可能なレベルの品質を達成する助けとなる。ソフトウェアの作成プラクティスは絶えず向上しているため、規準では作成者に対して特殊な方法を使用するよう規定すべきではない。しかし、規準には容認基準が明示されていることもあり、例えば、連邦航空管理局(FAA：Federal Aviation Administration)のガイドラインDO-178Bにはwhite-box試験を行うよう要求している。原子力発電プラントに対する安全上重要な系統の製作についても幾つかの規準が整備されている。例えば、IEC 880では、停止

系のためのソフトウェア作成に使用する方法が記されているが、特定の方法を使用することを義務づけているのではなく、ソフトウェアに関する要求事項を示しているのであって、この要求を満たすために如何なる方法を用いるかは作成者に任されている。また、IEEE 7-4.3.2-1993では、独立したレビュー、独立した立証、検査、解析、及び、試験といったV&Vを組み合わせて使用することを推奨している。このうちの幾つかは作成者が行うことを認めているが、それに引き続き独立したレビューを行わねばならない。検査方法としては、設計、コード及び試験結果を一通りレビューすることが望ましい。解析では、formal proof、ペトリネット等の解析手法を用いる。また、機能試験や構造試験を行うことも望ましい。

（結論と勧告）

結論：

- ソフトウェアの品質保証に関する手順は、製品の品質ではなく作成工程の管理をモニタすることである。特に、安全関連系のソフトウェアに対して一般的に容認されている評価基準がなく、むしろ、規準やガイドラインが最善のプラクティスを繰り返し行う際に有用となる。安全系に関連するソフトウェアの品質、例えば、保守性、正確さ及び保証は、ほとんどが直接図ることのできないものであるため、測定可能な変数と確認すべき品質との間にある種の関係が存在するものと仮定しなければならない。こうした制約に対処するために、ソフトウェアの品質を評価する際には、モデルの妥当性の検討及び測定値の適切さや正確さの確認に注意を払う必要がある。
- 特定のソフトウェアに関する事前の使用経験は、必ずしも、新たな適用における信頼性や安全性を確認するものではない。適切なレベルの品質を保証するためには、利用者や第三者によるレビュー、解析及び試験を行う必要があると考えられる。
- 試験は単なる品質保証方法であってはならない。一般に、実際の計測制御系を対象に徹底的な試験を行って、ソフトウェアが正確であることを担保しようとしてもうまくいかない。
- ソフトウェア作成時に用いられたV&Vプロセスに関するUSNRCのレビューは、徹底的に行うものと思われる。
- ソフトウェアの欠陥を明らかにすること、ソフトウェアの動作に関する信頼性を実証すること、及び、要求項目において意図していない機能や欠陥を見つけることは、異なった概念であり、以下に示すような技法を組み合わせて評価すべきである。
  ① 体系的検査や計画試験：系統の異なる部分からの代表的な入力を用いて行うが、ソフトウェアに欠陥が存在するか否かを決めることに役立つ。
  ② 機能試験：通常状態あるいは境界条件におけるエラーを見つけるのに有用であり、試験範囲も記録できる。
  ③ プログラムの動作プロファイルからランダムに選んだ多数の入力に基づく試験：ソフトウェアが特殊の条件下で異常となる可能性を評価するのに使用できる。

④ 第三者による要求項目の検査：ソフトウェアの作成に携わらなかった数人の経験者によって要求項目を検討・検査することは、ソフトウェアの欠陥を見つけるのに有効であるが、その有効性は、要求項目の品質にも依存する。

⑤ 系統全体のハザード解析：環境条件が重なった場合に事故に至るような状態を同定することができる。この解析は、ソフトウェアが系統のハザードに寄与していないことを確認するために、ソフトウェアの細部にわたって行うべきである。

- ソフトウェアの品質保証に関連するUSNRCの研究プログラムは、コードレベルの調査、例えば、多様性を持たせるための異なる言語によるコーディングや共通コードを含むロジックを識別するためのプログラム分割などの方向に偏重しているように見える。
- 変更が正確に設計・実施されていること、及び、異なるソフトウェア製品の間の関係が維持されていることを確認するためには、厳密な構成管理を行わなければならない。
- 設計が部分的に行われてきたため、ソフトウェアはさほど試験可能性の高いものではない。ソフトウェア設計と同等の技術、例えば、アプリケーション固有型集積回路(ASIC : application-specific integrated circuit)、プログラマブル・ロジック制御装置(PLC : programmable logic controllers)、フィールド・プログラマブル・ゲート配列(FPGA : field programmable gate arrays)、の利用にあたっては、同等の品質保証が要求される。

勧告：

1) 現在、USNRCは、種々の産業界規準を容認するために規制指針を策定する方針である。USNRCは、ソフトウェアの品質保証に対し、規範的な解決策よりもむしろ容認基準に着目した独自のガイドラインを策定すべきである。AECBの規制指針ドラフトC-138がその典型的な例である。USNRCのガイドラインは、(a)原子力産業界、(b)他の安全上重要な産業界、及び、(c)民間及び学術的なソフトウェア業界等の幅広い外部機関によるピアレビューを受けるべきである。

2) 系統の要求項目(systems requirements)は、アプリケーション固有の属性と同様、一貫性や完全性といった一般的な属性を分析できるよう、正確な意味を有する言語で記述すべきである。プラント技師、規制当局、システム設計者、ソフトウェア作成者などの関係者がその言語を理解できるものとすべきである。

3) USNRCは、ソフトウェアの品質保証に関し、ソフトウェアのライフサイクル初期フェーズとコードレベルの課題（例えば、異なる言語を用いたコーディング）の間でバランスを取りながら研究を進めるべきである。この初期フェーズがソフトウェアのエラー発生にしばしば関与することは経験により明らかである。

4) USNRCは、ASIC、PLC及び他の類似の技術に対し、同等の品質保証プロセスを要求すべきである。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「独自のガイドライン策定」に対して

USNRCは、本勧告に同意していない。これまでの経験から、スタッフは、独自のガイダンスを策定するより、適用可能な産業界規準を承認し利用する方が適切かつ効率的であると考えている。但し、その際には、適用できない部分の明確化を図る必要がある。こうした方針をとることのメリットは、規制側だけでなく、ベンダー、設置者、学術界からの情報入手を一貫性のあるプロセスで行えることにある。規制指針は、一般に、規範的な解決策や要求を含むものではなく、規制要求に従うための方法を示している。規制指針やSRPなどのガイダンスに関する最終版を発行する前に、内部のスタッフやACRS等の委員会によるレビューを受けることになっている。また、産業界や学術界を含む一般公衆からのコメントを求める期間を設けることも義務づけられており、これらのコメントは最終版の発行に先立ち検討することとなっている。カナダのソフトウェアに関するドラフト規制指針については、AECBからの要請を受けて、規制指針C-138をスタッフがレビューし、その内容がスタッフの見解やSRPの7章の改訂内容、及び、新たな規制指針と一致している旨の文書を送付している。

勧告2)「システム要求仕様の記述の明確化」に対して

USNRCは、本勧告に同意している。スタッフは、安全上重要なソフトウェアの開発にあたって、システムに関する仕様を明確に記述することが重要であると考えている。但し、その仕様をどのように記述すべきであるかを義務づけることはないが、仕様の整合性、完全性、理解性及び明確化はスタッフの基準に盛り込まれる。ソフトウェアの品質レビューに対するガイダンスと容認基準は、計測制御部門(HICB)の部門技術見解(BTP) HICB-14（ディジタル計算機ベースの計測制御系に対するソフトウェアのレビューに関するガイダンス）及びスタッフの検査支援ツールに示されている。さらに、この問題については、要求仕様のフレームワークに関する研究プロジェクトにおいて、検討を行う予定である。

勧告3)「ソフトウェアの品質保証に関する研究計画」に対して

USNRCは、本勧告に同意している。具体的にはSRPの7章の付録に示されているように、ディジタル計測制御系の全体レビューにおいて設計開発の早期段階に着目している。さらに、上述したように、要求仕様のフレームワークに関する研究プロジェクトが開始されている。本研究プロジェクトの目的は、設計開発の初期フェーズにおいて発生するソフトウェアのエラーを最小限にするために幾つかのステップが踏まれていることを確認するためのレビューガイダンスを策定することである。

勧告4)「ソフトウェア類似技術に対する品質保証要求」に対して

USNRCは、本勧告に同意している。スタッフは、PLCやASICについて、他の計算機ベース・システムと同様の方法でレビューを行っている。また、他のディジタル計測制御系に関するガイダンスや審査と同様のレベルの品質保証に関する活動を継続する予定である。

(3) 共通原因によるソフトウェアの故障(Common-mode Software Failure Potential)

(技術的動向)

米国内の原子力産業界： 多様性に関する規制要求では、安全機能を遂行するための代替手段を備えることを前提としているため、USNRCは、最近、ディジタル系の間で十分な多様性が確保されているか否かを評価するためのガイドラインを発行した[40]。同ガイドラインでは、以下のいずれかの場合に適切な多様性が確保されるとしている。

・プログラム言語、ハードウェア、機能、信号、設計が全て異なる場合、
・ディジタル系により異なる機能が備えられているが同じプログラム言語を用いて製作されており、さらに、ベンダーも同一である場合、
・ディジタル系のベンダーは異なるが同じ機能を果たす場合（ネームプレート多様性）、
・他の方法により多様性を実現させたためにケースバイケースのレビューが要求される場合

また、USNRCの規制研究局(RES)では、Unravelと呼ぶソフトウェア・ツールの開発を進めている。このツールは、プログラム分割(program slicing)というデバグ技法を用いているが、この技法では、プログラムの実行部分に到達する前にある変数の値に影響を及ぼし得るステートメントを取り出す。従って、ステートメントNにおけるエラーを修復しようとする場合に、他のどの部分が当該ステートメントにおける変数の値に影響を及ぼすかを調べる際に役立つ。USNRCは、このツールの有用性について、安全上重要なソフトウェアにおける機能多様性の評価や審査を行う際に役立つものと主張しているが、こうした技法を多様性の評価に利用できるという意見を聞いたこともなく、USNRCの主張は疑わしい。

米国外の原子力産業界： AECBのドラフト規制指針C-138には以下の見解が示されている。

> 要求されたレベルの安全性及び信頼性を達成するために、システム設計では、同一あるいは同様の機能を果たす機器を多重かつ多様に備える必要がある。例えば、AECBの規制書簡R-8及びR-10では、独立かつ多様性のある2系統の保護停止系を備えるよう要求している。多重に用意した機器において同種の機能を果たすためにソフトウェアを利用する場合には、設計多様性が担保されない可能性があることを認識すべきである。従って、設計では、機能多様性、センサーの独立性と多様性、タイミングの多様性といった他のタイプの多様性を考慮すべきである。

このように、ソフトウェアCMFの可能性とそれを低減するための対策の必要性に関し、AECBのドラフト規制指針はUSNRCの見解に一致している。しかし、AECBがソフトウェアCMFの対応策として義務づけてはいないものの機能多様性を容認しているのに対し、USNRCはベンダーが異なれば同一の機能を果たすディジタル系の使用を容認している。

他産業分野： 原子力以外の産業界では、安全性確保のアプローチが異なることから、ソフトウェアCMFに関する考え方も異なっており、単純に比較できるものではない。FAAのガイドラインDO-178Bは、ソフトウェアのライフサイクル・プロセスの目的、それを達成

するための活動と設計上の配慮に関する説明、そして、それが達成されていることを示す材料に関する記述から構成されているが、ソフトウェアに対する冗長性や多様性は要求していない。要するに、FAAは、ソフトウェアの多様性に関して、設計多様性により得られる相違や保護機能の程度は、通常、定量的に示すことができないため、要求されたレベル以上の保護機能を付加する必要があるという見解を有している。軍事及び航空産業では、MIL-STD-882C（システムの安全性プログラムに関する要求）あるいはそれに準拠する規準を使用しているが、これらの規準ではハザードの早期識別とリスクの低減を強調した安全性プログラムの利用を要求している。即ち、深層防護のような特定の安全設計アプローチや冗長性／多様性といった設計特性を規定するのではなく、ハザードの分析や安全性確認といったタスクと、定性的なリスク評価の実施などの基準を包含した安全性プログラムを策定するよう要求している。FAAや原子力産業界とは対照的に、ソフトウェア機器の重要性に関する格付けは無く、その作成手順も異なっているが、ハザード自体の評価が行われ、取り除かれたり管理されることになる。食物薬物管理局(FDA : Food and Drug Administration)のガイダンス[41]では、安全性に対する特殊なアプローチを規定しておらず、また、ソフトウェア作成や品質保証の手順について具体的なアプローチも規定していない。しかし、製品のレビュー文書に如何なる情報を含めるべきかを規定すると共に、レビュー時に如何なるタイプの質問が出されるかを明記している。また、提出物には、潜在的なハザードとその管理の方法、安全対策などを示したハザード解析を含めなければならない。どのように安全性を達成するかに関する規定がないため、冗長性や多様性に関するガイダンスも整備されていない。

（議論）

設計に関わる共通のエラーを回避するために、同一の機能を有する異なった設計の機器を使用することがある。これを設計多様性と呼ぶが、その例として、同等の要求仕様に沿って書かれた複数のバージョンのソフトウェアが挙げられる。即ち、機器の要求事項は同一であるがそれを満たすための方法が異なるというものである。もう一つの多様性として、機能多様性があるが、これは、全く異なった機能を果たす機器により達成されるものである。ここで重要なのは、機器に対する要求が異なっているという点である。機能多様性の典型的な例は、原子炉トリップのロジックであり、流量に対する原子炉出力高を利用した制御棒挿入と、冷却材温度高に対する原子炉出力高を利用したホウ酸水注入である。しかし、このようにシステムの動作が物理的に異なっていても、（原子炉スクラムに必要な信号を発する状態を検知する）保護機能が同じ場合には、ディジタル機器としては機能多様性を有するとは言えない。

以上をまとめると

・冗長性とは、単一故障に対して所定の機能を遂行するための代替手段を確保できるよう多重性あるいは多様性を持たせることである。

・冗長性は、動的なもの（全ての機器が同時に利用される）あっても静的なもの（一

部の機器は待機状態にあり故障が発生した場合にのみ使用される）であっても良い。

・多重性とは、物理的な劣化による独立故障に対処できるよう同種機器を多重に備えることである。

・設計多様性とは、設計は異なるものの同じ機能を果たす機器を複数利用することである。

・機能多様性とは、システムに対する要求の観点からは関連するものの異なる機能を果たすために複数の機器を利用することである。

・設計多様性及び機能多様性は、共通原因故障を防止するために用いられる。

（分析）

多様性を備えるためにディジタル機器が多重に設けられる場合、ソフトウェアCMFの可能性が存在するため、次の2つの問題を考慮する必要がある。

問題1： 独立に製作されたディジタル機器に対して故障の独立性を仮定できるか？、また、仮定できるとすれば如何なる状況においてか？ この問題を議論する際には設計多様性と機能多様性を区別する必要がある。

① 設計多様性

ケース1：ハードウェアとオペレーティングシステム(OS)

ハードウェアについては、極く少数のプロセッサと実時間OSしか一般には使用されていないため、単なるネームプレートによる多様性を仮定することは無意味である。即ち、製造メーカが異なっていても多くの計算機では同一の内部部品やOSを使用している。多様性を有するディジタル装置の故障が独立であるという仮定を否定できるだけのデータはないが、メーカの異なる同一機能のディジタル機器の故障に独立性を仮定するに当たって3つの問題がある。1つは、プロセッサで見つかるエラーの多くが、例えば、浮動小数点演算のように、類似の機能に関係することである。2つ目は、チップ設計が複雑化し試験を行うための能力が低下することである。3つ目は、共通の設計環境、ライブラリ及び製造施設を利用することである。ハードウェア設計におけるエラーが独立であると仮定できるか否かという疑問は、ソフトウェア故障の独立性に関する問題と深く関わりつつある。しかし、現時点では、設計が異なれば設計エラーによるハードウェア故障は独立であるという仮定を無視できる根拠はない。同様に、OSについても異なる設計であればその故障が独立であるという仮定を否定できるだけの根拠はほとんどない。しかし、実際には、異なるベンダーによるOSにおいてもソフトウェアCMFの可能性はある。例えば、異なるプログラム言語を使用して異なる国で作成され、長年にわたって使用されてきたプログラムパッケージにおいて、同種のエラーが見つかっている{42}。

ケース2：アプリケーション・ソフトウェア

ソフトウェアの信頼性を向上させる際に設計多様性を持たせることの利点は、個別に作成された複数のバージョンのソフトウェアにおける故障が独立であるという仮定に基

づいている。この仮定は、ソフトウェアの設計多様性がUSNRCの多様性と独立故障に対する要求を満足しているかどうかを評価する際に重要である。これまでに、幾つかの実験的研究が行われてきたが、その結論は、同一の機能要求を満たすために個別に作成されたソフトウェアが独立に故障するという仮説を否定するものであった[43]。即ち、実験において観測された相関故障や、CMFの多くは偶発的ではないと結論づけられた。さらに、ある実験において、相関故障の原因となるプログラミング・エラーを調べた結果、ある場合には、複数のプログラマーが同等の論理エラーを犯すことが明らかとなり、また、見かけ上異なる論理エラーであっても完全に別のアルゴリズムにおける相関エラーを引き起こす場合があることも判明した[44]。別の実験においても同様の結論が導かれている[45]。結局、異なった開発ツールや方法を用いても、複数のソフトウェアにおける相関故障を引き起こすようなエラーを著しく低減できるものではなく、プログラマーや言語を異にして独立に製作したソフトウェアであっても同一の機能を要求される場合にはその故障が独立して起こると仮定することはできない。従って、現時点では、独立性確保のためのネームプレート多様性や設計多様性の採用を認めたUSNRCの見解を支持する科学的根拠はない。なお、FAAやAECB等の規制機関では、故障独立性の根拠としての設計多様性を容認していない。

② 機能多様性

設計多様性とは対照的に、機能多様性を採用した場合にコードの独立性は仮定されず、機能要求が独立かつ異なっているか否かについてのみ議論される。ここで問題となるのは、新たな故障モードが導入されるか否かを検討することを除けば、アナログ機器の場合と同様である。従って、機能多様性に関するUSNRCの見解は科学的根拠に裏付けられていると言える。

問題2： 独立に製作されたソフトウェアの独立性を立証できるか、即ち、ソフトウェアを含むディジタル機器が故障時の動作において適切な独立性／多様性を有していることを確認する方法があるか？

アナログ系に対しては、CMFの評価方法が開発されており、また、状態の数や動作の連続性により、完全な試験が可能である。これに対し、ディジタル系では、通常、極く少数の状態についてのみ試験が可能であり、連続性に欠けるため試験の対象外となる入力に対しソフトウェアの動作を仮定することができない。また、一般に、2つのアルゴリズムの間の多様性を確認することは不可能である。仮に、設計多様性の効果が確認できるのであれば、多様性が必要でなくなると考えられる。USNRCは、Unravelなるツールの開発を進めており、これによって機能多様性の評価ができるものと考えているが、一般に、Unravelのようなプログラム分割を行って、ある特殊の計算に関連するコードを識別するだけでは機能多様性を評価することはできない。独立に作成されたプログラムが同一のコードを含む可能性は極めて低く、ソフトウェアに多様性を持たせる場合には異なる変数やデータ構造及びアルゴリズムが使用される。さらに、実験によれ

ば、完全に異なるアルゴリズムを使用しプログラミングエラーにも相関がない場合でさえプログラムの異常動作には従属性があることが示されている。また、プログラム分割は、出力に影響を及ぼすステートメント及び出力に至るまでの全てのパスを識別するために、出力から後向きに辿っていくが、実行可能な(feasible)パスと実行不可能な(infeasible)パスとを区別することができない。従って、どのパスが検討対象であり、また、実行可能なパスなのかを決めるには、解析者による手作業が必要であり難しいタスクである。これに対して、別のアプローチである"symbolic execution"では、ある特定の入力から開始し実行可能なパスを識別できるため、当該パスに対して真となるべき部分を評価することになる。また、この方法と関連するが、Software Deviation Analysis{46}も、入力から開始して出力に及ぼす影響を調べるという前向きのアプローチを用いているが、入力値の偏差を使用して出力に異常が生じるか否かを調べるというものである。

（ソフトウェアに対する多様性の代替策）

冗長性及び多様性はディジタル系の信頼性を向上させる上で最も有効な方法か？　他に効果的な方法はないのか？

代替方法としては、幾つかあるが、その中で、数学的な性能評価方法は、プログラミングエラーを見つけるのには有効であるが、使用が難しく、また、これまで極く小さなプログラムにしか適用した経験がない。この方法は、カナダのOntario Hydro社がプラント保護系のソフトウェアに適用したが、それによれば、経費が掛かるとのことである。しかし、こうした数学的な方法は、ソフトウェア開発の最終段階で適用するよりも初期の段階から組み込む方が費用効果性の高いものであることも示されている。

ディジタル系には、実行時にハードウェアの故障やソフトウェアのエラーを検出するために自己チェック機能を備えることもできる。このアプローチは、ランダムなハードウェア故障に対しては有効であるが、ソフトウェアの設計エラーに対してはそうではない。ゼロ割など幾つかのプログラミングエラーに対する試験は容易であり、かつ、有効であるが、より細かなエラーに対するチェックは困難であり、新たなエラーを誘発する可能性もある。ある実験によれば、自己チェックにより検出されるエラーは殆どなく、逆に、それによって新たなエラーが導入される可能性が高いことが示されている{47}。

標準的なシステム安全解析方法{48}は、ソフトウェアにおけるハザードを同定、削除、管理するためのものであるが、全てのエラーが対象となるのではなく、危険性の高い事故を引き起こすようなエラーに限定される。従って、他の方法に比べて経費も掛からない。また、安全性能評価方法の1つであるソフトウェア・フォールトツリー解析が、カナダDarlingtonプラントの許認可の際に用いられたという実績もある{49}。

ソフトウェア工学の分野においては、冗長性や多様性よりも、ソフトウェアの高信頼性を達成するための費用効果性の高い方法があると考えられているが、まだコンセンサスは得られていない。

（結論と勧告）

結論：

・ ソフトウェアのCMFが発生すると仮定するUSNRCの見解は妥当であり、工学的なプラクティスにも整合しているため、この見解を保持すべきである。

・ USNRCの部門技術見解(BTP)ドラフト、“新型及び既存プラントにおけるディジタル計測制御系”に述べられているように、多様性に関するUSNRCの見解は妥当である。

・ USNRCは、適切な多様性が存在するか否かの評価に関するガイドラインを再検討すべきである。これらのガイドラインについて、(a)異なる機能を果たすディジタル系を用意することが多様性を確保するのに有効な方法であるという見解は妥当である。ソフトウェアの機能多様性の分析によって、系統レベルで独立性が維持されることやディジタル系の利用により新たな故障モードが発生しないことが示されるが、この分析は、アナログ系を含む設計や変更に対する分析と差異はない。(b)機能多様性が実証されている場合、異なるハードウェアや実時間オペレーティングシステムを利用することは多様性を実現するのに有効であると考えられる。(c)異なるプログラミング言語を用いたり、同一機能の要求を満たすために異なる方法によって設計したり、複数のチームにより設計したり、あるいは、同一機能を達成するために異なる製造者の機器を使用することが、多様性を達成する際に有効であるという見解は適切でない。即ち、これらの方法はいずれも故障の独立性を立証するものではなく、故障の従属性を立証する訳でもない。

・ 同一の機能を達成する2つのソフトウェアの間の多様性を評価するために利用可能で有効な方法はないと考えられる。表面的あるいは構文的な相違を持たせることや、同一機能を達成するために異なるアルゴリズムを用いることは、故障の独立性を意味するのではない。従って、設計多様性を評価するための研究は、USNRCの予算を執行するだけの正当な理由がないものと思われる。

・ ソフトウェア業界の多くは、多重性や多様性の確保に比べて、高信頼性を達成するための技術の方が費用効果性の高いと信じているが、これらの方法がどんなものであるかについては統一した見解はない。このうち最も期待できるのは、標準的な安全解析及び設計に関する技法をソフトウェアに適用することと、数学的な解析を使用することであると思われる。

・ ハードウェアの故障やソフトウェアのエラーを検出するために自己チェック法(self-checking)を利用することは有効であり取り入れるべきである。しかし、自己チェック法自体がエラーを招かないことの確認に注意を払う必要がある。

勧告：

1) USNRCは、ソフトウェアCMFが起こり得るものと仮定する見解を保持すべきである。

2) USNRCは、BTPドラフト“新型及び既存プラントにおけるディジタル計測制御系”に述べられているように、ディジタル計測制御系に多様性を持たせる必要があるという基本的な見解を維持すべきである。

3) USNRCは、適切な多様性が存在するか否かの評価に関するガイドラインを再検討すべきである。USNRCは、異なるプログラミング言語、同一機能の要求を満たすための異なる設計方法、異なる設計チーム、あるいは、異なる製造者による機器の使用（ネームプレート多様性）に頼るべきではない。むしろ、USNRCは、機能多様性、異なるハードウェア、及び、異なる実時間オペレーティングシステムの利用など、より抜本的な方法に着目すべきである。

4) USNRCは、同一機能を果たす2つのソフトウェアの間の多様性を確立しようとして研究予算を執行することについて再度検討すべきである。ソフトウェア間の多様性を確立することができるとは考えられない。特に、Unravelツールに関するUSNRCの予算が、同ツールをソフトウェア間の多様性確保のために使用することを前提としているが、有用とは考えられない。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「ソフトウェアCMFの発生を仮定する見解の保持」に対して

USNRCは、本勧告に同意しており、既に、改訂SRPの7章において明示している。

勧告2)「多様性を持たせることの必要性に関する基本的見解の維持」に対して

USNRCは、本勧告に同意しており、既に、改訂SRPの7章において明示している。

勧告3)「多様性の評価に関するガイダンスの再検討」に対して

USNRCは、本勧告に同意している。多様性の評価は、1つの要因だけに基づいて行うわけではなく、機能多様性、ハードウェア多様性、システム多様性などを組み合わせて評価する。改訂SRPの7章では、ネームプレート、設計多様性及び機能多様性を考慮して容認可能な多様性を明確化するよう更新する予定である。

勧告4)「多様性評価のための研究予算の再検討」に対して

USNRCは、本勧告に同意している。しかし、Unravelがディジタル系の機能多様性を評価するためのツールではないことに注意されたい。Unravelは、ソフトウェアの品質を評価するために使用できるツールの1つである。Unravelの主たる目的は、エラーを見つけるためにソフトウェアのストリング・チェックを行う際に、スタッフによるレビューを支援することである。Unravelでは、コード全体にわたってストリングを組み合わせることにより、共通原因故障を引き起こす可能性のある共通のコーディング命令(coding instruction)を識別することができる。

(4) ヒューマンファクタとマンーマシン・インターフェース(Human Factor and Man-Machine Interfaces)

（技術的動向）

米国内の原子力産業界： アナログ系主体の制御室に対するUSNRCのレビューは、SRPとNUREG-0700（制御室設計レビューに関するガイドライン）に従って行われてきた。こ

れらのガイダンス文書は詳細な設計レビューを行えるよう用意されたものであるが、計算機ベースのMMIが普及する前に策定されたものであるため、USNRCは既設炉に導入された新技術をレビューするためのガイダンスが必要となった。そこで、1995年に、NUREG-0700の改訂版（マンーシステム・インターフェース設計のレビューに関するガイドライン）を発行し、その中で、申請者によるマンーマシン・インターフェースの設計プランをレビューするための方法と、その導入をレビューするための詳細なガイダンスを示した。また、1997年には、SRPの改訂も行われた。一方、産業界では、非安全系に対するディジタル技術の適用を行ってきたが、その範囲を安全系へ拡げている。ディジタル系を適用することの最大の利点は、運転員により多くの情報を提示でき、運転員のニーズに合わせて表示情報を調整できることであると言われている。例えば、従来は、複数のディスプレイにより表示されていた異なるパラメータを集中して表示することができ、さらに、事態がクリティカルな状態にあるか否かを調べる際にもチャートや図表のある場所へ行く必要があったが、こうした労力もなくなり表示画面においてチェックできる。しかし、このような利点があるにも拘わらず、許認可の不確定性により更なる計算機システムの導入に躊躇する動きもある。

米国外の原子力産業界：　米国外では、ディジタル技術が幅広く利用されており、制御室も計算機ベースのインターフェースが導入されている。しかし、こうしたインターフェースの設計に対する新たな容認基準が十分には整備されていない。例えば、新型プラントの設計における運転員の役割について2つの相反する傾向がある[23]：日本とドイツは自動化を推進する傾向にあるが、フランスでは、運転員を支援するための計算機ベースのディスプレイを使用している。また、ハルデン計画においても新たな制御室設計と技術の試験及び評価研究が行われているが、現時点では、かなり模索的なものであり、実践的な利用に供するような結果は殆ど得られていない。

他産業分野：　化石燃料発電所、化学工場、鉄鋼や製紙産業、航空宇宙産業などでは、運転員支援や自動制御というように広範にディジタル技術を利用しており、改良も進められている。こうした産業界の中には、ヒューマンファクタ工学に関する良好なプラクティスを注視しているだけの分野もあれば、その一方で、独自のガイドラインを策定している分野もある[50, 51]。原子力を含む殆どの産業界はディジタル技術の利点を認めている。特に、航空宇宙産業では、改良すべき点はあるものの、ディジタル技術の導入により安全性と効率が向上するものと信じている[52]。コックピット自動化のレビューによりインターフェースの問題が認識されたが、パイロット、運行会社、製造会社、規制当局などの関係者で従来の技術に戻す必要があると主張するものはおらず、問題はあっても利点があるため、評価や改良を行うことによりデジタル技術が進歩するものと信じている。

（議論）

MMIに関しては、しばしば、2つの問題点（設計エラーを分類することの必要性と、運転員の役割及び作業の定義）が取り上げられる。前者については、計算機ベースの技術設

計における欠陥を同定し、それらが人間の認知・行動にどのような悪影響を及ぼすかが検討されている{53}。例えば、自動化が適切に設計されておらず軽い作業の際に自動化の効果が現れたり、作業量がピークであったり安全上あるいは時間的に余裕のない状態にあるにも拘わらず自動化に関連する負担が起こったりする。一方、多くの場合、人間の役割と機能は設計により細かく規定されているわけではなく、ハードウェアやソフトウェア等が明確化された後に検討される。運転員の役割は、ハードウェアやソフトウェアの制限によって生じるギャップを埋めるためのものである。従って、運転員に対して暗に定義された役割や機能が実際に効果的かつある程度の信頼度を持って果たされるか否かという疑問が生じる（例えば、ディスプレイは信頼できるか？　情報は容易にアクセスできるか？　意志決定に十分な情報が表示されるか？　情報の収集や取出し作業が運転員に対して過剰ではないか？）。こうした問題は設計上の問題であり、技術に固有の欠陥ではない。従って、効果的に新しい技術を取り入れて巧みに設計すれば、システムの安全性や効率は向上し、運転・操作も容易になる。

一方、MMIに関する幾つかのガイダンスが策定されているが、これらの適用範囲は限定されている。例えば、ノブやダイアルの設計といった次元の低い問題を対象にしているものもあれば、設計で取り入れるべき特性ではなく避けるべき特性を示すというような概念的なものもある。結局、計算機ベースシステムに対するヒューマンファクタの観点から適用可能なガイダンスは殆どないと言える。

（分析）

ディジタル計測制御系のヒューマンファクタに関して効果的な設計を担保する際、「データ量が多過ぎて運転員に過大な負担を掛からないようにすること」というような曖昧さがあるためガイドラインに頼ることができない。計算機技術が急速に進歩したり新たな研究が行われるため、ガイドラインの記載内容は時として現状を反映していないことになる。アナログ制御などでは、設計に対する容認基準は、ガイドラインに規定された規準に従うことであると定義されている。しかし、ディジタル系については、広く適用可能な基準を策定するのに時間が掛かる。UNREG-0700改訂版でも新しい技術を用いた運転員インターフェースに対して十分な基準を規定しているわけではない。また、他の産業界でもきちんとした基準を用いてきたわけではない。EPRIによれば、新型制御室に対するヒューマンファクタの容認基準をより完全に整備する計画はないとのことである。従って、設計は、信頼のあるガイダンスが示されているガイドラインに従って行うべきであるが、安全設計を担保するためにはガイドライン以上の要求を満たすことが必要である。

新技術に関するヒューマンファクタ問題は、計算機ワークステーションに関する人体計測学(anthropometrics of computer workstations)から、ディスプレイや制御装置に関する人間工学、人間－計算機相互作用、マン－システム統合化、監督管理、自動化へと続く階層構造を成している。計算機ワークステーションに関する人体計測学は、設備や空間の適正な大きさを決めるための科学である。これについては、作業場所の高さ、机の高さ、

フットレスト、文書ホルダー、視覚距離などを規定する計算機ベースのワークステーションに対する規準や勧告があり、これらの多くはNUREG-0700改訂版にも示されている。ディスプレイや制御装置に関する人間工学には、フォントの大きさ、色の利用、入力装置、ディスプレイのタイプ（例えば、視覚、音響）の問題が含まれる。広く認められたガイドラインは最新の研究成果と併用される。例えば、計算機の入力装置としてのマウスは導入当初数多くの論争を引き起こしたが、今日ではハードウェアにパッケージされるに至っている。しかし、マウスのボタンを幾つにするかは未だに議論が続いており、最良の設計はユーザ、タスク及び設計者の好みに依存するとされている。試行錯誤的な評価や模擬試験などの方法が必要であるが、これに関して、NUREG-0700改訂版には、標準的なガイドラインが示されている。人間－計算機相互作用は、最も研究が進んでいる分野である。これに関する問題には、ウィンドウの形式や管理、ダイアログのタイプ、メニューの形式が含まれる。ガイドラインでは、適用の方法に依存しない一般的なMMI特性を強調しており、その殆どは、適用の過程で期待されそうな、期待できる、あるいは、評価すべき属性を規定している。NUREG-0711では、現行のガイダンスの限界及び設計に関する知識の現状が論じられている。マンーシステム統合化については、人間の能力と限界、計算機ベースのワークステーションの特徴に関する問題がある。これらの問題は、計算機インターフェースの意味論(semantics) に関わるものであり、即ち、人間の能力を高めると共にその限界を補償するために情報の表示やシステムの制御をどのように設計するか、である{54}。運転員の取るべき判断と行動及びインターフェースの特徴の間には概念的な距離があり、この距離が大きければインターフェースは要求からかけ離れたものとなる。ある研究{55}では、運転員のモデルに基づいて設計されたディスプレイにより運転員のパフォーマンスが著しく向上する可能性があることを示しているが、最良のモデルに関するコンセンサスは得られていない{56}。監督管理とは、運転員の役割が手動制御から計算機制御系の監視、監督に移行することを指しており、これにより、人間のパフォーマンスに関する関心が高まっている。運転員の役割が監視という静的な行動に変わることで、人間の弱点とさせる分野でその能力に重荷を負わせる結果となる可能性がある。具体的な問題としては、自動化による安心感、ループから外れているという一種の疎外感、状況把握の欠如などがある。自動化による安心感については、古くから、航空機産業で関心が持たれているが、運転員が自動化や計算機制御に警戒心を抱き続けることを担保するための設計方法として合意の得られているものはない。過去20年にわたって監督管理が主たる範例になってきたため、計算機ベースのワークステーションでは知的ディスプレイや電子チェックリストといった様々な運転員支援を取り入れてきた。しかし、最近の研究{57}では、計算機ベースのチェックリストを使用することにより、従来のペーパー方式に比べてミスが多くなっていることが示され、必ずしも運転員支援として有用でないとの意見もある。原子力においても同様の実験結果が得られている。具体的には、事故シナリオにおいて、計算機ベースの手順書を用いることでエラーは少なくなるものの対応をとるまでの時間が長くなるという

ものである[58]。自動化については、手動制御から完全自動化への移行が進むにつれてシステム制御への運転員の寄与が著しく少なくなる。システムによっては、異常が発生するとシステムを安全側に移行させるため、人間はそれを知らされ自動制御の修復等を行うだけとなる。こうした完全自動化システムに関連した人間のパフォーマンス問題は数多くあるが、現在は、監督管理者あるいは自動管理者のいずれかに対して自動化をどのように定義し設計するかに議論が集中している。

マンーシステム相互作用のレビューは、注意深く段階を踏んで行うべきである。まず、適用可能なものがあればガイドラインを使用すべきである。しかし、新型インターフェース技術に関して最も重要な人間のパフォーマンス問題の多くは、現行のガイダンスでは適切に対応できない。さらに、新たなガイダンスが策定されるのを期待している間にディジタル技術の利点が活かされなくなる。レビューでは、運転員の役割や活動に関する詳細な仕様に基づいて設計されていることを確認すべきである。設計者は、古典的な設計上の欠陥に関して提案されるMMIの特性を評価する必要があり、さらに、提案された設計は、パフォーマンスに基づく方法で評価しなければならないが、この評価では、現実的なタスク環境や統計的に試験可能なパフォーマンスデータを用い、実際の利用者の協力を得るべきである。要するに、慎重にガイドラインを利用し、規範的な設計プロセスや現実的なモデルを用い、さらに、パフォーマンスに基づく評価を行うことで、運転員の有効性を高め共通の設計欠陥を防げるものと考えられる。

（結論と勧告）

結論：

- ディジタル技術は、MMI、さらには、運転員のパフォーマンスを向上させる可能性がある。ヒューマンファクタ及びMMIがディジタル計測制御系を導入するにあたって障壁とならないことは、十分に理解されている。
- ヒューマンファクタ及びMMIをレビューするためにUSNRCが採用している方法は、レビューにおける第1ステップである。設計及びそのプロセスに対する現行のUSNRCの手順は他産業のものと一致している。ガイドラインは、既に文献で公開されたり、特定の産業で策定されている数多くのものに基づいている。設計プロセスをレビューするための方法は、有効なヒューマンファクタの性能評価や妥当性検討と整合性の取れたシステムエンジニアリングの基本原則に基づいている。
- 適切な設計は、ガイドラインを卓越したものでなければならない。新技術及びヒューマンパフォーマンスに関するNUREG-0711の議論と、NUREG-0700改訂版の付録Aに論じられている設計の原則は、原子力産業界が設計を具現化し評価するための枠組を示している。設計がマンーマシン統合化に関する一般原則に従っておりヒューマンパフォーマンスの特性を考慮していることを実証することにより、幾分不明瞭ではあるが重要な概念を具体化した場合にその評価が可能となる枠組を形成することができる。
- 安全及び安全関連系に対して行われるディジタル技術の導入は、その範囲も規模も多

種多様である。ヒューマンファクタのレビューと評価の範囲を、変更の規模と対応させることが重要である。しかし、運転員が見る情報や制御入力に対する系統の応答に影響を及ぼすような変更は、新たな設計によりマン－マシン相互作用の有効性が損なわれないことを確認するために、経験的に評価しなければならない。

・ USNRCは、ヒューマンファクタに関する公開討論に積極的ではない。例えば、NUREG-0700改訂版のように、ヒューマンファクタに関して提案された手順や方針あるいはスポンサー付の研究は、定期的に公表されるわけではなく、また、米国内外のヒューマンファクタ関係者（米国のヒューマンファクタ及び人間工学学会、IEEE、システム・人間・サイバネティクス学会、計算機－人間相互作用に関する計算機特別検討グループなど）による定期的なレビューも受けていない。欧州における原子力関係のヒューマンファクタ研究者は、ヒューマンパフォーマンス問題に関する理解を深めるために、原子力発電プラントのヒューマンファクタ研究成果を利用してきた。宇宙、航空機及び軍事など米国内の安全上重要な産業界は、積極的に参加し、他分野におけるレビューと経験から教訓を得ている。

勧告：

1) USNRCは、設計及びそのプロセスに対して適切なレビュー・ガイドラインがあれば、それを継続して使用すべきである。原子力及びその他の産業界の利用において知識が高まるにつれて、これらのガイドラインを更新する際には注意を要する。

2) USNRCは、レビューをガイドラインやチェックリストに限定しないものと仮定すべきである。 (a)設計の基となる運転員モデル、(b)マン－マシン相互作用に関する古典的な設計上の問題の記述方法、及び、(c)パフォーマンスに基づく評価に関して、設計を評価すべきである。さらに、評価では、代表的なタスク、実際のシステム挙動及び実際の運転を使用すべきである。

3) USNRCは、レビュー基準を拡張して、数多くの安全上重要な設備への利用において繰り返し発生するマン－マシン相互作用の欠陥についてリストを作成すべきである。他産業における問題点や提案された解決策を理解することは、ディジタル技術の導入によって引き起こされるエラーが繰り返し発生するのを防止するために効率的な方法である。

4) 上記の勧告2を補足すると、ヒューマンファクタのレビューは慎重に（例えば、実際の状況や運転員によるパフォーマンス基づく方法を用いて）行うべきであるが、レビューの範囲や規模はディジタル機器への変更の特徴や規模と対応を取るべきである。

5) USNRCと原子力産業界は、定期的に公開討論会に参加すべきである。NUREG-0711に述べられているように、ヒューマンインターフェースに関する最新技術は、ヒューマンファクタ関連の新たな未解決問題を数多く導入する。USNRCが他産業における現在の研究や最善のプラクティスに遅れずに、自分たちの利用から得られた知見を研究や実践の遂行に貢献することは、困難である。

6). USNRCは、ハルデン研究プロジェクトに携わる研究者が国際的な研究活動に積極的

に参加して成果を共有したり知見を得ることを奨励すべきである。

7) USNRCの規制研究局は、マン－マシンの統合、管理及び自動化についてより高度レベルの課題を検討するための研究を支援すべきである。こうした研究には、より効率的に設計を具体化するための運転員モデルなど、原子力発電プラントに適用するための設計手法を検討することも含めるべきである。さらに、広範な分野の研究を行って、原子力特有の技術的問題を明らかにしたり、他産業における経験と対比させる必要がある。こうした研究は、繰り返し発生する欠陥のリストに拡充すると共に、それらを提案された解決策と結びつけることになる。

8) USNRCは、自身の研究プロジェクトを補完しながら、エネルギー省(DOE)との間での施設の調整を検討すべきである。こうした施設において、米国内の原子力産業界は提案された設計を具体化し評価することが可能である。ワークステーション技術がさほど高価でないことから、ワークステーションによる精度の高い制御室シミュレータの開発が可能である。他産業（例えば、航空機）では、ワークステーションによる部分的タスクのシミュレータが幅広く利用されている。

（USNRCの対応）

上記の勧告に対し、文献[3]において、USNRCはその対応見解を提示していない。

(5) 安全性及び信頼性の評価方法(Safety and Reliability Assessment Methods)

（技術的動向）

米国内の原子力産業界： USNRCによる承認を受けずにプラントの変更を行うための基準は10 CFR 50.59に示されている。その中で、変更に対する承認が必要か否かに関する基準は、安全解析書で既に評価されている安全上重要な設備の異常や事故の発生確率とその影響が大きくなるか否かである。USNRCは、確率論的リスク評価(PRA : Probabilistic Risk Assessment)を規則策定(rulemaking)活動に取り入れようとしているが、現時点では、ディジタル系の確率論的評価について明言されていない。1995年10月の時点でのUSNRCの見解は、「ディジタル計測制御系の信頼性及び安全性確保は設置者の責任であるが、設計のライフサイクルに関する活動により定性的・定量的な信頼性評価方法が容認されディジタル技術の進歩に十分対応できる」ということである。しかし、その一方で、USNRCは、「定量的な信頼性評価方法が、標準的なプラクティスとして容認できる程十分に成熟しているとは考えていない」と述べている。産業界は、ディジタル制御系の解析にフォールトツリーを用いて故障モードを考慮した例はあるものの、確率論的評価のディジタル系（特に、ソフトウェア）への適用については賛否両論である{59}。例えば、GE社のABWR解析{60}では、ソフトウェアの品質保証及びV&Vによりソフトウェア故障の問題が明示されると仮定しており、従って、PRAにおいてソフトウェアの故障を明確には含めていない。しかし、WH社のAP600における保護安全監視系のPRA{61}では、ソフトウェアのCMFによるアンアベイラビリティを、単一モジュールに対して1.1×10^{-5}、複数モジュールに対して

1.2×10^{-6}としている。

米国外の原子力産業界： AECBは、現在、新しい規制指針(C-138)においてソフトウェアの評価に対するアプローチの正式導入を進めている。AECBによるソフトウェアの評価は、要求仕様のレビュー、開発及び導入時の体系的検査、試験のレビュー、開発プロセスと管理に関する確認といった4つの側面に着目している。AECBのアプローチでは、プラントの安全性におけるソフトウェアの役割を評価するための解析を要求しているが、確率論的な評価は要求していない。英国では、Sizewell-Bにおいて原子炉保護系の安全解析の一環として、ソフトウェアの主要部分に関する動的解析が行われている。許認可において信頼性の評価は要求されていないが、研究開発の一環としてソフトウェアの信頼性を精度良く推定するための試験を継続することとした{62}。

他産業分野： 他産業では、決定論的方法が広く用いられており、確率論的方法については賛否両論である。例えば、FAAは、ソフトウェアの品質保証に対するガイドラインDO-178Bの使用を推奨しており、ソフトウェア故障に関する確率論的評価は行わないものとしている。鉄道制御の分野では、ハザード解析や故障モード影響解析、抽象モデル（ペトリネットやマルコフモデル）、故障導入実験など利用してきたが、PRAに基づく解析を取り入れようとしている{63}。ソフトウェア工学の分野では、開発プロセスの各段階でV&Vなどを行っているが、仕様分析にはデータ流れ図や状態遷移図などを使用し、定量評価にはフィールドデータを用いてソフトウェア故障のシステム全体の安全性に対する重要度を評価している。

（議論）

原子力発電プラントにおいて、信頼性や安全性の評価には、決定論的手法と確率論的手法が用いられているが、ディジタル系の評価におけるこれらの手法の適用可能性、及び、その適切な利用方法は重要な問題である。

ディジタル系に対する決定論的手法は、原子力産業界で用いられている設計基準事故の解析手法を一般化したものであり、これには、ハザード解析やformal methodが含まれる。決定論的手法の適用にあたってディジタル系に起因する故障モードを考慮することに注意を払っている限り、ディジタル系の解析に決定論的手法を用いることに異論はない。しかし、確率論的手法をディジタル系に適用するには議論の余地がある。以下では、確率論的手法の適用可能性について論じる。

物理的な故障に対して容認されている解析手法は幾つかあるが、設計上の欠陥に関する確率論的な解析には問題がある。ソフトウェアの故障は設計上の欠陥によるものと定義されるため、ソフトウェアを評価するための確率論的手法に着目して議論がなされている。ソフトウェア工学の分野では、ソフトウェアが故障するか、故障はランダムに発生するか、故障率の概念が存在するかについて論争がなされている。不正確な結果が生じた場合に物理的な変化が起こらないためソフトウェアは故障しないと主張する人もいれば、ソフトウェアは正常に動作するかしないかであるため、その信頼性は1か0であると主張する人も

いる{64}。また、ソフトウェアの故障を認める人でもそれを確率的にモデル化できるか否かに関しては意見が分かれる。ある人はソフトウェアを決定論的なものであるとしその動作は固定していると主張する。

ソフトウェアの信頼性を評価するための方法は幾つか提案されているが、故障確率が低いことを立証するために膨大な数の試験を行わねばならないという問題があり、いずれも直接適用できるものではない。また、故障確率が規定された上限値以下であることを確信するためにどれ程の試験を行うべきかを決める方法も提案されている{65, 66}。NUREG/CR-6113にも同様のアプローチが示されているが、そこでは、安全系の運転範囲が、安全状態と非安全状態との遷移領域にあると考えている。従って、この領域においてランダム試験を行うべきとされており、故障確率が十分低いことを統計的に示すために試験の回数を決める必要があるが、これには数学的なアプローチが用いられる。しかし、ランダム試験は、安全評価や品質保証活動の極く一部にすぎない。試験とformal methodは相互に補完するものであり、即ち、解析では試験対象とすべき状態を決める際に有用であり、また、試験は解析における主要な仮定を検証するのに役立つ。

運転実績から得られる故障データも利用可能であり、これまでに、事例の分析がなされてきた{59}。例えば、279の単一チャンネル故障と55の複数チャンネル故障を分析した結果が報告されているが、これによれば、55件の複数チャンネル故障のうちの9件がソフトウェア欠陥に起因するものであると示されている。また、こうした分析結果を用いたフォールトツリー解析は、アナログ系からディジタル系への移行を決める上で有用であるとされている{59}。

（分析）

安全性及び信頼性に関する決定論的評価の方法は容認されており、ディジタル系への適用も可能である。確率論的評価を検討するに当たっては、3つのオプションがある。1つは、最も良く知られているデータやランダム試験の結果を用いてソフトウェアを含むディジタル系の故障確率を推定することである。2つ目は、ソフトウェアは故障しないか、あるいは、常に故障するかのいずれかを仮定することである。前者の仮定は、フォールトツリーにソフトウェアの故障を含まないことに等しい。3つ目は、確率論的評価を断念することであるが、このオプションは、PRAが原子力発電プラントの安全解析における重要な部分であり効果的に利用されているため、実践的ではない。しかし、従来のフォールトツリー解析を用いるのであれば、ディジタル系に関する故障モードをモデル化することに限界があることを認識しなければならない。他のモデルとしては、マルコフモデルがあるが、このモデルは、ディジタル系の解析には適していると言われているものの、原子力での利用実績は少ない。マルコフモデルは、フォールトツリーに比べて柔軟性があり、シーケンスの従属性や共通原因故障のモデル化に有用であるが、モデルが大きくなると困難さが増したり膨大な時間が掛かるという欠点がある。最近では、動的フォールトツリーや動的フローグラフなどの方法が提案されている{67, 68}。

（結論と勧告）

結論：

・ 設計基準事故の解析やハザード解析といった決定論的評価方法は、ディジタル系に適用可能である。

・ ソフトウェアに対して精度良い故障確率を評価することが可能か、また、ソフトウェアの故障がランダムに発生するかに関し、ソフトウェア業界内で議論がある。しかし、ディジタル系の故障が系統全体に及ぼす相対的な影響を調べるためにPRAを行うことを目的として、ソフトウェアの故障確率を用いることができるという見解は妥当である。原子力発電プラントのPRAにおいてソフトウェアの故障を考慮することは、ソフトウェアの故障を無視した場合よりも明らかに望ましい。

・ ソフトウェア（及びディジタル系）に対する故障確率を割り当てることは、希有事象に対する確率の取扱いと本質的な差はない。良好なソフトウェアの品質保証は、ソフトウェアの故障確率を推定するための基盤を確立する際の前提条件である。PRAにおける不確実さ解析や感度解析は、評価結果が不確実さを有するパラメータに過度に依存していないことを確認するのに役立つ。他のPRA計算と同様、ソフトウェアの故障確率はランダム試験や専門家の判断を含むプロセスによって推定することが可能である。

・ 確率論的解析は、理論的には、COTSに対しても適用可能であるが、実際には難しい。例えば、故障確率を評価するために現場での実績を使おうとすると、その実績が同等であるか否かという点において困難が生じる。プログラム内蔵の装置に対しては、ソフトウェアの故障確率がその利用形態によってユニークであると考えられる。しかし、厳密な試験を行うことで、故障確率の限界値を推定することは可能であろう。各分野での長年にわたる良好な実績も、専門家の判断を引き出す際に有用であろう。

勧告：

1) USNRCは、ソフトウェアの故障が系統全体の信頼性に及ぼす相対的な影響を、ディジタル機器を含む系統のPRAにおいて考慮するよう要求すべきである。

2) USNRCは、PRAでの使用を目的とし、COTSを含むディジタル系の故障確率を推定するための手法開発に力を注ぐべきである。これらの手法には、使用にあたっての容認基準、ガイドライン及び制限条件の他、必要とされる論理的根拠や正当化を含めるべきである。

3) USNRCと産業界は、それぞれの能力を評価し、確信を持ってディジタル化を行うための要求事項と定量的評価の限界を理解するのに十分な専門知識を構築すべきである。

4) USNRCは、ディジタル系の（安全性／信頼性）解析を行うための新たな手法を開発することを目的としたプログラムの支援を考慮すべきである。この手法は、定量評価における不確実さを減らし確信度を上げるために用いることができるものと考えられる。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「PRAにおけるソフトウェア故障の考慮」に対して

USNRCは、本勧告に同意している。ディジタル系を利用した新型炉の設計に対するPRAでは、ディジタル系をアナログ系と見なしてモデル化している。アナログ系に比べると、ディジタル系に対する故障率データは限られており、潜在的に重要な故障モードも異なっているが、ディジタル系をモデル化したPRAでは、不確実さ解析を通してその重要度を調べることでリスク寄与度に関する知見を得ることができる。例えば、WH社のAP600のレビューにおいて、こうした評価が行われている。信頼性に関する要求が厳しくなるにつれて、データの不足により評価における確信度が低下する。例えば、希有事象に影響を及ぼす設計エラーに関するデータはほとんどない。しかし、スタッフがディジタル計測制御系の容認性について判断する際に数値的な信頼性基準にだけ頼るのではないことに注意されたい。

勧告2)「ディジタル機器の故障率推定手法の開発」に対して

USNRCは、本勧告に同意している。スタッフは、ディジタル系のリスク評価の分野で行われている活動を随時レビューすることとしている。また、プラント計算機システムの運転経験とリスク解析手法に関するデータベースを構築するために、OECD/NEAのCSNIによる提案を支持している。計算機システム問題に関する最終報告書では、CSNIはソフトウェア並びにディジタル系の信頼性を評価するための手法開発を目的とした研究を随時レビューすべきであるとしている。現在進行中の研究プロジェクトの1つにおいて、ソフトウェアの信頼性を推定するための現行の方法を評価することとなっている。

勧告3)「ディジタル機器に関する専門知識の構築」に対して

USNRCは、本勧告に同意している。スタッフと産業界は、ディジタル系の導入が効果的に行われることを確信するために専門知識の向上を図っている。例えば、スタッフと産業界は、COTS、PLC及びASICの作成計画において相互交流を行っている。定量評価の限界については、米国内の原子力産業界はプロセス計算機の主たるユーザではないため、スタッフは、CSNIの活動などディジタル系の信頼性に関する研究活動を継続してレビューすることが適切であると考えている。ディジタル系の定量評価に関する専門知識を高めるために、スタッフはセミナーへの参加や手法に関する文献調査を行っている。

勧告4)「解析手法開発の支援」に対して

USNRCは、本勧告に同意している。USNRCの対応については上記2)及び3)を参照されたい。

(6) 民生用ハードウェア及びソフトウェアの利用(Dedication of Commercial Off-the-Shelf Hardware and Software)

(技術的動向)

米国内の原子力産業界： USNRCによれば、COTS型のハードウェア及びソフトウェアに対する規制の基本は、他の一般商用製品の利用に対する規則にあるとしており、商用製品の調達に対する改訂規則(10 CFR 21)を発行している。しかし、この規則は、ディジタル機器やソフトウェアを安全系に適用するにあたって十分に注意すべきである。即ち、設計・製作のプロセスが終了した後に全ての機器を適切に導入できるわけではないというUSNRCの見解が同規則には反映されているのである。また、この規則は、ディジタル系について具体的に言及しておらず、従って、USNRCはディジタル系に対する新たな規則を適用することを検討している。一般的な規則を適用する際の具体性を示すために、SRPの改訂版においてCOTS型のディジタル機器の利用が論じられることとなっている。このSRP改訂版では、EPRIのドラフト・ガイドライン（EPRI TR-106439：民生用機器の安全系への適用評価及び容認に関するガイドライン）の適用が承認されると考えられる。USNRCは、COTS型のディジタル機器の利用に関するEPRIのワーキンググループ等産業界の活動やハルデン研究計画にも参加し現状の理解に努めている。また、国立研究所でもUSNRCがスポンサーとなって研究を進めており、SRPの改訂のために研究成果のレビューが行われている。

一方、産業界では、EPRIのワーキンググループが、実時間プロセス監視、制御及び保護（安全）機能に対するCOTS型のディジタル機器を導入する際に費用効果性の高い評価を行うためのガイドライン策定を進めている（そのドラフトがTR-106439である）。この策定は、既存のガイドラインEPRI NP-5652に基づいているが、その中に示されている規準をディジタル機器に対する新たな問題にどう適用するかを明確にしようとしている。例えば、NP-5652では、商用製品の特性を確認するために4つの方法（特別な試験と検査、供給者に関するサーベイ、オリジナル部品の性能評価、及び、供給者／製品の実績に関する記録）を示している。しかし、ソフトウェアを含むディジタル機器に対しては、最終的な製品の試験や検査が十分であるとは言えそうにない。EPRIのワーキンググループもこれを認めており、単一の方法に頼るのではなく上記の方法を組み合わせてディジタル系の評価を行う必要があると考えている。1996年に発行されたEPRIのドラフト・ガイドライン(TR-106439)には、COTS型のディジタル機器を適用する際の安全上の重要性に適切な基準と性能評価方法を用いたアプローチが提案されている。USNRCが以前から安全系へのCOTS型ディジタル機器の利用に関して容認をためらってきたことから、EPRIのワーキンググループは、まず、どのようにしてCOTS型ディジタル機器の利用が容認されるかに関しUSNRCと産業界との間でコンセンサスを得るためのガイドラインを策定しようとしている。同時に、そのガイドラインを実現させるための方法について詳細なガイダンスの策定を行うこととしている。EPRIのワーキンググループは、ベンダーによる開発、組立、試験及び構成管理のプロセス（商用グレード）を、10 CFR 50のAppendix B（原子力グレード）と比較している（図4-1参照）。そして、他の因子で相違が相殺できるか否かを評価する。これらの因子には、運転履歴や実績のレビュー、V&Vの追加実施、特別な試験と（故障あるいは

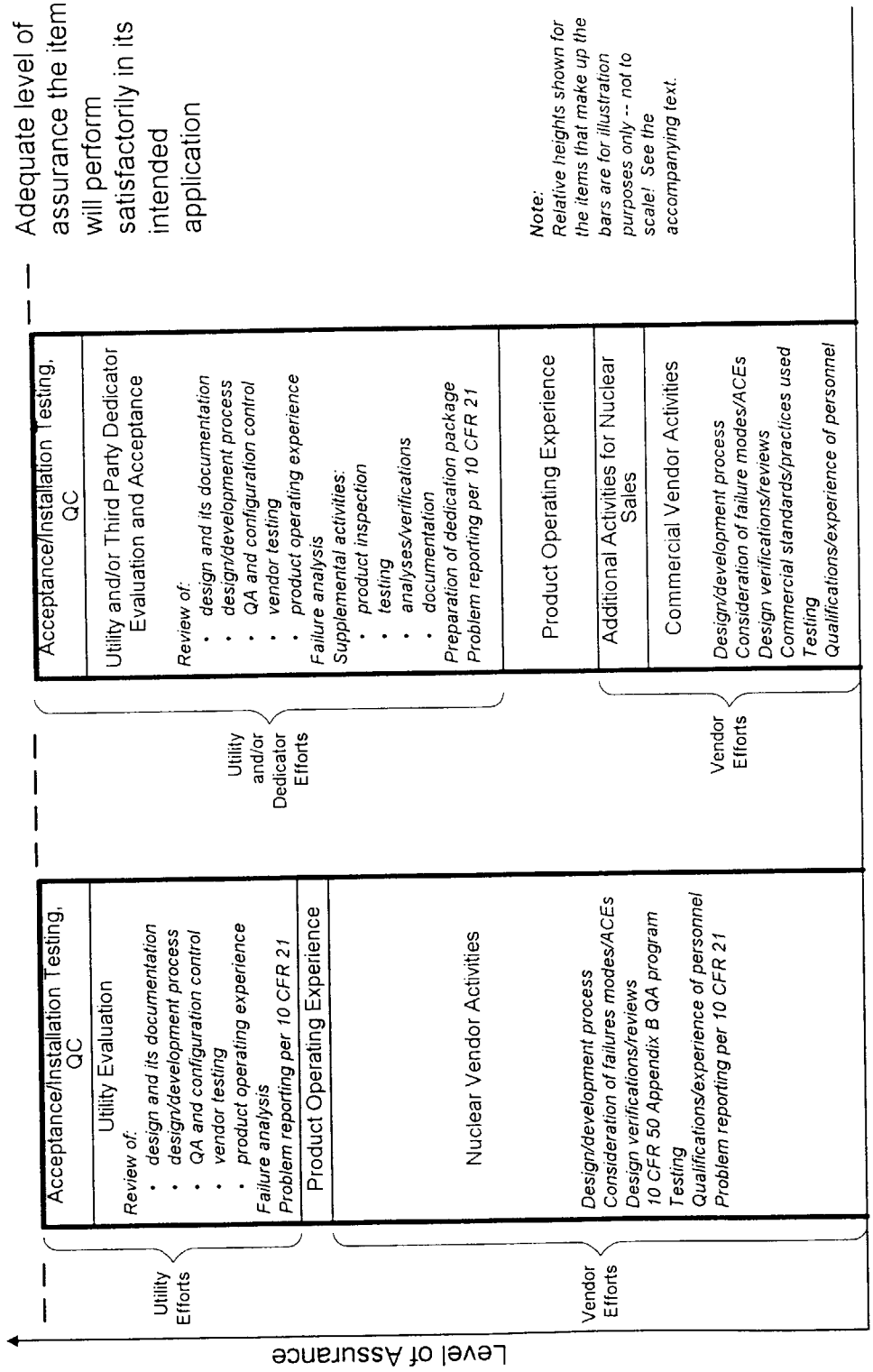

図 4.1 原子力グレードと商用グレードのディジタル機器に対する品質保証レベル（原典：EPRI TR-106439, Figure 3-2）

ハザード）解析の実施が含まれる。こうしたEPRIのアプローチの最終目的は、商用グレードと原子力グレードの機器のいずれに対しても同等の品質を確保することにある。原子力利用者ソフトウェア管理グループ(NUSMG)は、COTS型ソフトウェアの利用に関するガイダンス{69}を策定してきた。NUSMGのアプローチは、機能要求と容認基準のレビュー、ベンダーによるサーベイの審査、過去の顧客に関するサーベイ、類似の運転履歴、ソフトウェア相違点のレビュー、ベンダー及びそれと独立した試験、及び、故障解析に依存するものである。IEEE 7-4.3.2は、ディジタル計測制御系の品質保証に対する主要な規準であり、試験及び確認すべき安全要求を具体的に示している。その付録には、ベンダーの開発プロセスに関する技術的な問題が論じられているが、これを除く部分は、USNRCの規制指針1.152で承認されている。同規準については、更新の作業が進められており、民生用機器等に関する規準の充実化が検討されている。

米国外の原子力産業界：　カナダOntario Hydro社のOASES規準には、COTSの評価、ソフトウェアの品質保証プロセス、及び、保守プロセスに関するガイダンスが含まれている。故障モード解析により、COTSの利用に制約が生じることがあり、また、確証を得るために付加的な性能評価試験やレビューを行うこともあり得る。一方、英国でもCOTSの利用に関する研究が進められている。日本では、許認可上の制限はないもののCOTSは安全系に利用されていないが、ABWRの安全系に利用しているディジタル機器の幾つかは、非原子力産業界における良好な実績を基にその品質を確認しているように見受けられる。

他産業分野：　EPRIのワーキンググループがCOTSに関して策定したガイドライン(EPRI TR-106439)は、他産業分野での利用から得られた知見に基づいている。例えば、NASAによれば、 COTSの利用により80万ドルが節約でき、技術的及び機能的な要求も満足されたとのことである{70}。鉄道業界もスイッチ信号設計にCOTSの利用を開始している{63}。国際計測制御学会(International Society for Measurement and Control, 旧ISA : Intrument Society of America)のワーキンググループでは、COTSの安全制御、保護、監視機能への適用問題について検討を進めており、そこでは、ERPIのガイドラインを参考にCOTSに関する規準やガイドラインの策定が計画されている。1994年、国防省は、軍事仕様への依存を縮小しCOTSの利用を進めるための活動に着手した{71}。同様に、カナダの国防省もCOTSの利用に関する研究に資金を投じている。しかし、現時点では、これらの活動により、COTSの評価に対する具体的なガイダンスは策定されていないものと考えられる。

（議論）

民生用ディジタル計測制御系の利用は、経済性の観点から重要な課題である。アナログ系が廃れてきており、その製造規模も縮小されているため、ディジタル系への移行は避けられない。一般に、利用しようとする民生品が産業界の性能基準を満足していれば、その非安全系への導入は可能である。しかし、プラントの安全性や許認可に影響を及ぼし得る系統への利用では、より高い基準を満足しなければならないし、規制当局も製品の性能や品質が許認可条件を満たしていることを確認しなければならない。従って、性能や品質の

評価には規制側と産業界との合意が得られた方法が必要となる。この方法は、原子力発電プラント用に製作された製品に対する評価方法とは異なる。現時点で、COTS型ディジタル計測制御機器の導入は、幾つかの電力会社における個々のプロジェクト単位で行われる傾向にあり、従って、民生品を利用することによるメリットを示すためには、しっかりと規定されたアプローチが必要である。しかし、ディジタル機器やソフトウェアの品質保証に関する問題を解決する方法については合意が得られていない。解決すべき重要な問題は、故障モード、特に、ハードウェアあるいはソフトウェアの故障に起因する予想外の結果にどう対処するかであり、具体的には、故障モードを同定したり、試験によりこれらの故障モードが検出されその頻度が明らかとなることを確認したり、また、プラントシステムや運転員の手順書及び訓練がこうした故障モードに対応できることを確認することである。

（分析）

現時点で、COTS（ディジタル機器及びソフトウェア）の安全系への適用に対するガイダンスはない。産業界のグループがガイダンスや規準の策定を進めているが、USNRCは、その結果の承認を前提としてグループに参加すると共に動向を見守っている。しかし、承認に当たっては幾つかの問題も生じ得る。例えば、複数のグループにより得られた結果に整合性があるか？　規制ガイダンスの整備に間に合うか？　前者の問題については、EPRI TR-106439のレビューにより、一貫性をとるためのグループ間調整が非公式ではあるが十分に行われているものと判断されている。EPRIのワーキンググループが発行したドラフト・ガイダンスは他のグループの検討に役立っている。さらに、USNRCスタッフの参加も整合性をとる際の手助けとなっている。第2の問題（各グループの検討結果は、USNRCが規制ガイダンスを策定する際に参考とできるか否か）については、USNRCが検討の早い段階でグループに参加したことで公式な承認をスムーズに行われることが期待される。USNRCにとって、産業界のグループとの意見交換は、国立研究所で行っている研究をレビューするのに重要な役割を果たしており、産業界のガイドラインとの相違点を認識するのに役立っている。例えば、NUREG/CR-6421と EPRI TR-106439は、いずれもCOTSの容認アプローチを提案したものであるが、両者には、以下の相違点があることが明らかとなっている。

- NUREG/CR-6421のアプローチは、ERPI TR-106439に比べて、より詳細なものであるが、現行の規準に大きく依存している。
- NUREG/CR-6421は、安全上の重要性のみ考慮しIEC 1226の規準に従っているが、EPRIのアプローチは、機器に関して安全性の分類と複雑さの両面を考慮している。
- それぞれが策定した基準は異なった方法で示されているが、両者とも対象機器が必要規準を満たしているかを調べる際に工学的判断に基づくとしている。EPRIのガイダンスでは、このプロセスに関する具体的な方法について、例が示され、より詳細になるものと考えられる。
- NUREGレポートの方が若干規範的である。

こうした相違点を解消することに関連して、COTS利用に関するガイダンスにおいて、ハードウェア及びソフトウェアが有すべき属性を明確にする必要があると考えられている。こうした属性が定義されれば、それらが適切に備えられているか否かを評価するための方法も具体化されるであろう。さらに、評価方法が決まれば経験も蓄積され確信度も増すことになる。FAAのDO-178Bは、要求される属性を定義することを基本としており、これら属性がCOTSにより満足されることを確認するためのガイダンスを示している。USNRCと産業界のグループは、このFAA文書を検討すべきである。

既設の計測制御系の老朽化が進む中で、近代的な設備の利用が拡がることにより、COTSの利用は極めて有用であるが、その一方で、特に安全系への導入においては適切な費用で要求される品質を確保することが重要である。対象とする利用形態がこれまでの利用形態とかなり類似しているか、また、信頼性などの重要な属性を適切に確保する際に利用実績がどのように効果的であるかを評価することが重要なポイントであるため、民生品の利用には、従来ベンダーから提供されてきた以上の多くの情報が必要となる。ベンダーによっては、開発や試験の手順、利用実績などの情報を提供することに抵抗を感じるかもしれない。さらに、電力会社及びUSNRCは、先を見通して必要情報を蓄積する手段を見つけなければならない。民生のディジタル機器の利用が費用効果性の高いものであるか否かは不確実さのある重要な問題であるが、その答えは経験からのみ得られるものと考えられる。

（結論と勧告）

結論：

- 技術的に適切な利用プロセスが確立されていて費用面での利点を活かせるのであればCOTS型ハードウェア及びソフトウェアの利用は、原子力産業界にとって魅力的な方法である。
- EPRIのワーキンググループが最近策定したドラフト・ガイドラインEPRI TR-106439は、COTS問題について産業界とUSNRCとの間でコンセンサスを得るための基盤を提示していると考えられる。従って、ガイドライン及びそれに続く（第2段の）ガイダンスでは、ディジタル計測制御系の利用にあたって必要かつ十分な条件がハードウェア及びソフトウェアの両面から定義されていることを保証すべきである。一旦これらの条件がきちんと定義されれば、その妥当性を評価するための種々の方法が比較的容易に見つけられ使用されることになり、経験も増えていく。適切な方法の例として、EPRIワーキンググループとUSNRCは、FAAのガイドラインDO-178Bを検討すべきである。このガイドラインには、COTSに関するガイダンスが含まれている。
- ソフトウェアの品質保証と、安全性及び信頼性評価の手法は、COTSに強く関連している。標準化されたソフトウェアが類似のシステムで利用される場合、COTSの利用プロセスが適切であることを立証すべきである。
- USNRCは、EPRI、NUSMG、IEEE及びISAのワーキンググループと協力しているが、

こうした協力は有意義であり、COTS問題を論ずるためのガイダンス策定に役立つものと考えられる。

・ COTSの利用にあたっては、ある固有の利用形態に関する複雑さや安全上の重要性に見合った基準を用い、性能評価活動を行う必要がある。例えば、記録計や表示計といった小規模な交換に適用した性能評価活動は、原子炉保護系の大規模な交換に適用すべきものと同等ではない。

勧告：

1) USNRCは、EPRI、NUSMG、IEEE及びISAのワーキンググループと協力することにより、 USNRCの関心や見解が議論され、これらのグループが策定する規準やガイドラインを速やかに承認することに繋がるという認識を持つべきである。

2) USNRCは、原子力発電プラントの安全系へのCOTS利用を容認するために如何なる研究が必要かを見極めるべきである。こうした研究は、全体の研究計画に取り込むべきである。

3) COTS利用に関するUSNRCの規制ガイダンスは、基準や性能評価活動が利用形態の複雑さや安全上の重要性に対応しているという原則に基づくべきである。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「産業界との協力」に対して

USNRCは、本勧告に同意している。COTSに関して、スタッフは、会合に参加したり産業界との相互交流を図っており、そのため、EPRIのCOTSガイダンス（EPRI TR-106439）の承認が速やかに行われるものと期待されている。

勧告2)「COTS利用の容認に関する研究計画の策定」に対して

USNRCは、本勧告に同意している。スタッフは、COTS型ハードウェア及びソフトウェアの利用をサポートするための研究プログラムの策定を検討している。

勧告3)「規制ガイダンスにおける基本原則」に対して

USNRCは、本勧告に同意している。 スタッフが承認しようとしているEPRIのCOTSガイダンス（EPRI TR-106439）において考慮されており、改訂SRPの7章でこのガイダンスを参照している。

4.2 施策的課題

(1) ケースバイケースの許認可プロセス(Case-by-Case Licensing Processes)

（ディジタル系への移行に対する規制上の枠組）

一般に、USNRCは、予め定められた設計基準を用いて、原子力発電プラントの許認可及び規制において設計上の適性を評価する。計測制御系に関する設計基準は、アナログ式かディジタル式かを明示しておらず、これまではアナログ式に着目して適用されてきた。し

かし、近年のディジタル系導入の動きに合わせて、そのレビューや承認を行うために規制上の枠組を構築することが急務となっている。プラントの設備変更は10 CFR 50.59に従って、評価、レビュー、承認されるが、この規則では、USNRCによる事前承認を受けずに変更ができる条件として、USQ が生じないことを規定している。この規則をどのように解釈し適用するかが重要であり、また、一貫性のある規制を行うことが重要であるとの考えから、産業界は10 CFR 50.59の適用に関するガイダンス（NSAC-125：10 CFR 50.59対応の安全評価に関するガイドライン）を策定してきた。このガイダンスはUSNRCの承認を得ていないが、NSAC-125におけるガイドラインの有用性は認められている[72]。

長年にわたって、ディジタル技術が非安全系及び限定された範囲の安全系に利用されてきたが、原子炉保護系(RPS : Reactor Protection System)や工学的安全施設起動系(ESFAS : Engineered Safety Features Actuation System)など安全運転に核となる部分への導入は最近まで行われなかった。しかし、マイクロプロセッサ利用のディジタル技術の発展に伴い、また、アナログ機器の入手が困難になりつつあるという状況に応じて、RPS等の安全系への利用に関心が集まってきた。1987年にHaddam NeckにおけるRPSへのディジタル系の導入が申請された。電力会社は、10 CFR 50.59に従って評価を行い、その結果、USQはないものと判断した。しかし、USNRCは電力会社による評価をレビューして、新しい設備に関する電気的な環境がベンダーによる品質保証試験に含まれていることが立証されていない旨の結論を出し、その結果、電力会社に対して、解析、試験及び問題解決のためのスケジュールを提出するよう要求した[73]。さらに、従来の設備とは異なるタイプの機器を使用していることから、その機器の故障はUSQであるとの見解を示し、ディジタル系の導入に関して新たなガイダンスを策定する意向のあることを明らかにした。1992年8月、USNRCは、ディジタル系の導入に関してGeneric Letter(GL)のドラフトを発行し、その中で、ディジタル系の導入は、USQであり、USNRCスタッフによるレビューを行う必要があり、さらに、10 CFR 50.59に従って行うことはできないとの見解を示した。これにより、安全関連系へのディジタル系の導入は全てUSNRCスタッフによる事前承認が必要となり、また、一般的に適用可能な規制基準がないためにケースバイケースで判断されるという一貫性のない規制プロセスとなった。電力会社の中には、ディジタル系への移行を延期したり、アナログ系の利用を継続すると決定したところもある。

産業界は、10 CFR 50.59の適用可能性に関してより具体的なガイダンスの策定を開始したが、その一方で、USNRCは上記のGLドラフトを撤回した。1993年12月に、産業界はガイダンス文書EPRI TR-102348（ディジタル系への許認可変更に関するガイドライン）を発行し、また、1995年4月に、USNRCはGL 95-02を発行した。このGLでは、以下の2つの点を除き、EPRI TR-102348を承認している。

・ディジタル系への移行により従来とは異なったタイプの事故や故障が発生するか否かを評価する際に、考慮すべきシステムレベルは導入対象とするディジタル系である。
・変更によりUSQが生じないことを示す根拠を安全評価レポートに纏める際、それに用い

た工学的判断や論理を実用可能なレベルまで掘り下げて記述すべきである。

(分析)

ケースバイケースの許認可に関する問題には、次の2つの基本的な疑問点がある。

① ディジタル系の導入に適用する規制規準は何か？ 一貫性のある規制上の枠組を構築するための規準を策定できるか？

② USNRCによる事前のレビューや承認を受けずにディジタル系への変更が認められるような条件とは何か？

以下では、これら2つの疑問点について論じる。

ディジタル系に関するガイダンスは幾つかあるが、いずれも申請者やUSNRCのレビュー者にとって分かり易い規制要求や手引きを示すものとはなっていない。ある種の技術を初めて適用する場合に、その申請を評価するためにUSNRCが一般的な規制上の枠組をきちんと整備しておくことを期待するのは非合理である。実際、対処すべき問題に関して経験を積むにはケースバイケース的なアプローチが効果的であるという意見にも一理ある。しかし、こうしたアプローチには、一貫性のない結果となる可能性があり、レビュー者の質や考え方に依存するため、場合によってはより厳しい規制要求が課せられたり、レビューに必要な相互連絡を図るために電力会社や申請者の人員構成が予測できないなどの問題も生じる。USNRCは、SRPの改訂をはじめ、ディジタル計測制御系の導入に関してそのレビューを行うためのガイドラインの策定を進めている。

10 CFR 50.59では、申請した変更によりUSQが生じるか否かを設置者が個別に評価するよう求めている。しかし、USNRCは、EPRI TR-102348に関し、10 CFR 50.59の解釈を、「ディジタル系への移行により従来とは異なったタイプの事故や故障が発生するか否かを評価する際に、考慮すべきシステムレベルは導入対象とするディジタル系である」としており[72]、この解釈は、「システムレベルの機能が影響を受けなくても機器レベルでの新たな故障モードがUSQを構成する可能性がある」ことを示唆していると考えられる。USNRCは、ESFAS等主要な安全系に対する機器レベルでの検討を制限することによりEPRI TR-102348の解釈を精緻化しようとしているが、主要な安全系への導入とあまり主要でない安全系への導入とを区別することは重要である。結局、USNRCによる事前レビューが必要な事例と要求されない事例を示すなど、10 CFR 50.59の判断をより具体的に提示するためのプロセスを確立することが有用であろう。こうすることで、10 CFR 50.59の適用に関する一貫性が示されるものと考えられる。

(結論と勧告)

結論：

- ディジタル系の導入を監督する際の規制側の役割は重要である。特に、ディジタル計測制御系などの分野では、技術が急速に進歩し原子力への適用が慎重に議論されているため、規制側による監督役割は、ディジタル系の導入に対して貴重な見解をもたらし得る。

・ ディジタル計測制御系の開発と原子力発電プラントへの導入に対する規制側の対応が、導入に際しての適用可能な規制要求と手順上の枠組に関し、設置者にある種の混乱と不確定性をもたらしてきたものと考えられる。この不確定性とそれに伴う費用の増加は、電力会社がディジタル系の導入をためらう大きな要因である。

・ ディジタル系の導入に対して一般に適用可能な規制要求が欠如しているため、ケースバイケース的なレビュー方法が用いられてきたが、これにより、混乱と不確定性が生じてきた。この方法は、ディジタル系への移行の初期段階においては必要であったかもしれないが、現在では、USNRCは十分な経験を有しており、また、米国外や他産業の経験による裏付けもあることから、ディジタル系の導入に関するレビューや承認について、一般に適用可能な規制の枠組を確立することができる。

・ 10 CFR 50.59では、設置者が事前にUSNRCのレビューや承認を受けずに変更を行うことができる場合を定義しているが、そのプロセスは、基本的に、健全かつ必要なものであり、公衆の健康と安全を守るというUSNRCの責任と整合が取れている。特に、設置者にとって、USNRCによる事前レビューと承認を受けずに許認可基準と矛盾しない施設の変更を行うことが実際上必要であると認識されている。さらに、そのプロセスは、設備変更における重要性の程度と、それに応じたUSNRCの役割を適切に反映している。USNRCにとって、ディジタル系の導入が（USQを伴うような）重要な場合とそうでない場合とを区別し、その程度に応じた方法で規制レビューの範囲と詳細を調整することが重要であると考えられる。

・ 1992年8月発行のGLドラフトに述べられているように、安全関連系へのディジタル技術の導入が全てUSQを生じるものであると定義することは10 CFR 50.59の基本的考え方に矛盾すると考えられる。

・ 規制当局は、ディジタル系の導入に関し10 CFR 50.59の下で行われる判断を明記するための公式なプロセスを有していない。こうした情報は、特定の変更がUSQをもたらすか否かを判断するにあたり、USNRCと電力会社の双方にとって有用である。

・ 申請者とUSNRCの間での早期の相互連絡は、重要な課題を同定し具体化するのに極めて有用である。こうした先行的な相互連絡が行われた場合、その後の規制レビューがより効率的となり、さらに、焦点が絞られるため、電力会社とUSNRCにおける必要人員を最小限に抑えることが可能となる。

勧告：

1) USNRCは、既設プラントへのディジタル系の導入に関するレビューと評価を行うために、一般に適用可能な枠組の構築を最優先して行うべきである。

2) ディジタル技術の急速な進歩を考慮し、新技術の開発に遅れずに規制の枠組を更新するためのプロセスを確立すべきである。この枠組において他の安全上重要な産業における最善のプラクティスが考慮されていることを確認するために、外部や公衆によるレビューを受けることが強く望まれる。

3) USNRCは、ガイドライン策定プロセスを加速・簡素化することができるような新たな方法を検討すべきである。例えば、USNRC、産業界及び学術界からの代表を含めたタスクグループの設置を検討することが挙げられる。これらのグループは、ディジタル系の開発と利用において発生する安全上重要な問題を検討・解決するために、プロジェクト的に運営されるものとする。

4) 規制要求の策定にあたり、USNRCは、ディジタル系に特有の問題が生じた場合、それらが適切に対処されることを確認すべきである。一方、ディジタル系の導入によって生じる問題がアナログ系に対する問題と差異がない場合、これらの問題は矛盾が生じないように一貫して対処すべきである。 USNRCは、ディジタル系の導入に対するレビューと承認を行うにあたり、導入によって発生した問題が提案されたディジタル系の利用形態に固有のものでなければ、個々の設置者に新たな規制要求を課すべきではない。

5) USNRCは、電力会社、産業界および公衆と早期に協力するための先行的な努力を行うべきである。さらに、原子力及び非原子力の分野におけるディジタル計測制御系の利用を幅広く理解することは、USNRCにとって大きな利益となる。こうすることにより、協力関係の基盤ができるものと考えられる。

6) USNRCは、10 CFR 50.59との整合性を確認するために、GL 95-02及びEPRI TR-102348において提起された“システムレベル”の問題（システム、即ち、ディジタル系としての機能への影響はなくても構成する機器のレベルでUSQが生じた場合の10 CFR 50.59の取扱い）を再検討すべきである。ディジタル技術を含む安全系の主要な変更と軽微な変更とを区別するという見解を維持及び具体化することは望ましい方向である。

7) USNRCは、ディジタル系の導入に関する50.59の評価をカタログ化するためのプロセスを確立すべきである。これにより、ディジタル系の導入を検討している電力会社が、ある特殊な変更によりUSQが発生したことが明らかになった場合について、過去の50.59の評価をレビューし検討することが可能となる。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「既設プラントへの導入に対する一般的なレビュー・評価の枠組の構築」に対して

USNRCは、本勧告に同意している。改訂SRPの7章では、こうした枠組やガイダンスを策定しており、当初から優先度の高いものとされてきた。

勧告2)「規制枠組の更新プロセスの確立」に対して

USNRCは、本勧告に同意している。改訂SRPの7章は、必要に応じて定期的に更新する予定である。スタッフは、規準策定に継続的に参加したり他国や他産業分野との相互交流を行うことで、進歩する技術分野における新たな開発や現状に遅れずについていくこととしている。

勧告3)「ガイドライン策定プロセスの簡素化」に対して

USNRCは、本勧告に同意している。本件については、スタッフが委員会に説明し、

それに対して、規準承認のプロセスを加速化・合理化する方法を調べるよう指示され、現在調査中である。安全上重要な未レビュー問題を提起するために産業界と学術界を含む諮問グループを利用することに関しては、現在、USNRC内部の諮問委員会ACRSとNSRRCが、安全問題や研究計画のレビューを行っている。スタッフは、効率的なガイダンス策定に対して、こうした監視体制と公衆からコメントを求めるというプロセスで十分であると考えている。さらに、産業界にとって重要な問題が生じた場合には、容認可能なガイダンスやアプローチの検討を行うために、スタッフと産業界の代表によるワーキンググループが組織されてきた。

勧告4)「ディジタル系特有の問題への対処と確認」に対して

USNRCは、本勧告に同意している。スタッフは、改訂SRPの7章及びディジタル系の検査ガイダンス(IP 52001&52002) を発行したことで、ディジタル系への変更について一貫性のあるレビューが行われることを確認する際に役立つと考えている。委員会規則における新規項目あるいは追補項目によって生じた新たな要求を賦課したり、あるいは、規則の解釈に関して従来とは異なる規制スタッフ見解を賦課する場合があるが、これらは、10 CFR 50.109（バックフィッティング規則）に基づくものであり、新たな見解を賦課する前には、その妥当性を評価するための費用／効果解析を行うこととなっている。

勧告5)「産業界及び公衆との早期交流」に対して

USNRCは、本勧告に同意している。様々なトピックについて、EPRIや産業界のワーキンググループを通して先行的な活動を進めている。多くの場で、スタッフは、設置者に対して可能な限り早期に設備変更の議論を行うと伝えている。しかし、実際には、スタッフ及び設置者の人員に制約があり、個々の設置者と相互交流を図ることは必ずしも可能ではなく、また、設置者にその計画をスタッフと議論するよう義務づけることもできない。10 CFR 50.90に従う設置変更が必要な場合に限り相互交流が要求される。

勧告6)「“システムレベル”問題の再検討」に対して

USNRCは、本勧告に同意している。GL 95-02に述べたように、システムレベルに関するスタッフの見解は、10 CFR 50.59をレビューするためのプログラムの一部として、技術スタッフ及び法律スタッフにより再検討されてきた。その結果、GL 95-02の解釈は新たな不具合に関連するものであり、正しいと判断され、今後変更されることはないと考えられる。

勧告7)「ディジタル系導入に関する評価のカタログ化」に対して

USNRCは、本勧告に同意していない。10 CFR 50.59に基づく評価は設置者が行うものであり、USNRCにその結果を提出するよう要求されていない。設置者は、評価結果を纏めた年報を作成するよう要求されている。スタッフは、その報告書をレビューし、ディジタル系への変更ある場合、それに対する検査の必要性を検討するこ

とになる。ディジタル系への変更が行われる場合にUSQが生じるか否かを判断するためのプラント設置基準をレビューするが、これは、プラントごとに設置基準が異なっているため個別に行われる。従って、スタッフは、50.59評価のカタログ化に多くの人員を投入することが、設置者にとって大きな利益を与えるとは考えていない。しかし、原子力産業界自体が、ディジタル系の導入によりUSQが生じるか否かを判断するためのガイダンスを整備することを目的に、ディジタル系の変更に対して50.59評価のカタログ化を行うことは可能であろう。なお、スタッフによるレビューを必要とするディジタル系のレトロフィットは、公開の安全評価において承認されることを認識している。

(2) 技術支援体制の適性(Adequacy of Technical Infrastructure)

(技術的動向)

米国内の原子力産業界： 原子炉規制局(NRR)は、原子力発電プラントの設計、建設及び運転に関連する許認可と検査の責務を担っている。規制研究局(RES)は、規制上の意志決定をサポートするための情報の提供、安全問題を解決させるための研究の実施、及び、技術的な規制と規準の策定を行うこととなっている。1996年、NRRスタッフ(650人)のうちの10人と、RESスタッフ(212人)のうちの6人がディジタル計測制御系関連の業務に携わった。USNRCスタッフはディジタル計測制御系に関する経験を有しているが、新たに専門家を雇ったり外部機関による訓練を受けることで知識の向上を図ろうとしている。1996年には、16,000ドルの予算が外部機関による訓練費用に充てられた。一方、USNRC内部の訓練プログラムの強化も図られており、訓練部門スタッフの30人のうちの1.5人がディジタル系関連のプログラムに割り当てられ約4万ドルの予算が投じられた。USNRCにおける研究として、ソフトウェアのV&V、高健全性ソフトウェアの作成、規制指針の策定、ソフトウェア言語の評価、ディジタル機器の環境性能などが行われている。1996年には、約3万ドルの予算がディジタル系関連の研究に割り当てられた（この年のRESの研究予算総額は68万ドル、NRRの研究予算総額は14万ドルである）。

一方、電力会社の中には、ソフトウェア工学に関して独自の訓練プログラムを用意し、ディジタル系の導入時に備えているところもある。また、別の電力会社では、計測制御系を計算機システムから切り離している現状の組織構成に問題があり、これが知識の向上や専門家の育成の障害となっていると指摘している。EPRIとテネシー渓谷開発公社(TVA：Tennessee Valley Authority)は、新型の計測制御技術に関する研究を行うために専門の技術センターを設立し、技術の蓄積と移転を押し進めている。

米国外の原子力産業界： カナダ、日本、英国、フランスを対象とした調査により、スタッフ配置、訓練、研究計画に関する具体的な情報は得られなかった。日本では、電力会社と協力して、ベンダーが社内で研究活動を行っているが、ディジタル系への変更はさほど関心を集めていないとのことである。

他産業分野： 他産業についての調査により、スタッフ配置、訓練及び研究計画に関する具体的な情報は入手できなかった。しかし、鉄道及び医療機器の分野では規制側の専門知識に関して類似の関心を抱いている。航空宇宙産業では、FAAがスタッフ能力を補うために産業界から技術者を指名し活用している点に注目すべきである。殆どのベンダーは社内に技術部門を有し大学との共同研究を行っている。

（分析）

適切かつ有効な規制プログラムを確立・維持するために、USNRCには、(a)レビューを行うのに十分な数のスタッフ、(b)スタッフに対する訓練とディジタル計測制御専任のスタッフの雇用、及び、(c)規制ニーズを支援するための研究プログラムが必要である。USNRCスタッフは、ACRSから、ディジタル技術に関する知識レベルと訓練が不十分であるとの批判を受けてきたが、その理由は、米国における新規プラントの建設が無いこと、原子力に興味を持つ技術系の学生が減少していること、USNRCの予算が削減されていること、等である。また、これらの理由により、計算科学やソフトウェア工学の優秀な技術者の雇用も困難な状況にある。さらに、ディジタル系によるレトロフィットはUSNRCによるレビューを受けなければならず、このプロセスでは、USNRCからの質問に対応するために6ヶ月も余分に掛かり、かなりの人員を投入することになる。その結果、設備変更の内容を変えることもある。従って、十分なUSNRCスタッフがディジタル系の分野に割り当てられているか、また、レビュープロセスをより効率的にできないかという疑問が湧いてくる。さらに、USNRC内部の組織構造にも問題があり(例えば、NRRとRESの分離)、これによって内部での議論が不十分であったり、研究が重複したり、短期的・長期的な研究のバランスが悪く、結果的にレビュープロセスが遅れる原因になっているように思われる。

規準やガイダンスに関しては、USNRCは産業界や学術界に依存しており、それらの文書をレビューして承認を行っている。こうした規準策定プロセスは時間がかかり、急速に進歩する技術に追いつけないため、結果的に、非効率なアプローチとなっている。

ディジタル計測制御系の規制では、ハードウェア、ソフトウェア、マンーマシン・インターフェースなどに関する技術能力が要求されるため、訓練においては、ヒューマンファクタ関連の知識とディジタル計算機やソフトウェアに関する知識とを組み合わせた内容にすべきである。USNRCは、1995年から新たな訓練プログラムを作成し内部で評価してきたが、同プログラムは外部レビューを受けるべきと考えられる。さらに、スタッフの訓練を論じる際に考慮すべき因子として、NRRのレビュー者と地方局の検査官との間に技術的な知識の相違があることである。この相違により、レビューが遅れたり不適切な結果を招いたりする可能性がある。

一方、分野によっては、所定のレベルの技術能力を有する個人を"certified"、"qualified"、あるいは、"licensed"と認めて資格を与え、これにより、新技術の進歩に対処するための継続的な教育と現状把握を行っている。ソフトウェア工学に関しては、こうした資格制度に対して議論の余地はあるものの、FAAのように外部専門家の活用プログラムなどの方法も

ある。ANSIやIEEEなどの機関が、USNRCスタッフ（あるいは電力スタッフ）に対して専門家を派遣できれば、規制レビューにおける不整合な問題を軽減できる可能性がある。

（結論と勧告）

結論：

- USNRCは、原子力発電プラントにおけるディジタル計測制御技術の規制をサポートするために、スタッフ配置、訓練及び研究プログラムを変更すべきである。
- 適切な技術支援体制に関する問題は、USNRCだけでなく、原子力産業界全体にも適用可能である。USNRCに対する勧告の多くは、原子力産業界にも当てはまる。
- USNRCは、ディジタル計測制御技術の発展により技術支援体制が影響を受けることを想定しなければならない。近い将来の許認可は、ディジタル系の導入による設備変更と新規プラントの承認に着目している。USNRCは、ディジタル技術の利用が拡がり洗練されて行くにつれて技術支援体制の整備を継続しなければならない。
- 規準や産業界ガイドラインを策定するためのプロセスに固有の問題、特に、急速に進歩するディジタル技術に関する問題がある。規準や産業界ガイドラインの策定にUSNRCが初期の段階で関与することにより、規制ガイダンスや容認基準がタイムリーに利用できるようになるものと考えられる。
- ディジタル計測制御系の利用に関するUSNRCの研究プログラムには施策的なプランが必要である。現行の研究プログラムは、ストラテジーのない研究の集まりであり、ある場合には価値があるかどうかが疑わしい問題を追求している。現行のUSNRCスタッフの構成は、NRRとRESとに分かれており、RESスタッフがNRRのニーズに応えることを義務づけており、これが、短期的な規制上の意志決定と長期的な研究とのバランスをとるようなプランの障害となっている。USNRCの研究プログラムが定期的な外部レビューを受けることにより、的を得た課題が議論されていることが確認でき、共同研究の分野が明確になる。現行のNSRRCによる活動は効果的であり、好ましいと認識されている。しかし、より公式な外部レビューがあればさらに有用であると考えられる。おそらく、これは、人員削減のために、他機関と人員交換を行うことを基本として実施できるものであろう。

勧告：

1) 技術の急速な動きと原子力産業界の沈滞にも拘わらず予算と人員が削減されていることにより種々の困難が生じてはいるが、USNRCは、現行のスタッフによるレビュープロセスの効率化を図るために様々な方法を模索しなければならない。
2) USNRCは、現行あるいは新規採用のスタッフに対して、最小かつ継続的な訓練の必要性を明確にすべきである。ソフトウェアの品質保証については特別な注意を払う必要がある。USNRCの訓練プログラムは適切な外部レビューを受けるべきである。専門家としてのレベルを証明することはUSNRCが検討したいと考えている1つの方法である。
3) USNRCは、RES及びNRRによって行われる研究プログラムに対して施策的なプラン

を立てるべきである。このプランは、短期的な規制ニーズと長期的な研究ニーズとのバランスに着目すべきであり、研究目的を達成するために人員を有効的に活用する方策を取り入れるべきである。さらに、関連技術業界、EPRI、DOE、米国外の原子力機関、及び、ディジタル計測制御問題を取り扱う他産業にも、より効果的にプランを拡げるべきである。この勧告を行うにあたり、当委員会は、ハルデン計画がこうした協力研究の例であると認識しているが、ハルデン計画における活動の多くは公開できず、従って、精密な検討による効果は得られない。

4) ディジタル計測制御に関する研究は長期にわたって行うべきものであると考えられるため、USNRCは、複数年の予算を計画・調整できるよう配慮すべきである。

5) USNRCは、必要となる規準やガイダンス文書の作成・更新を促進するための方策を検討すべきである。特に、USNRCは、タスクグループの設置と利用を考慮すべきである。

（USNRCの対応）

上記の勧告を受けて、USNRCは以下のような見解を示している。

勧告1)「現行スタッフよるレビュープロセスの効率化」に対して

USNRCは、本勧告に同意している。SRPの7章を改訂するための努力を行っており、また、幾つかのプログラムに関して産業界と相互交流を図っている。

勧告2)「スタッフ訓練の必要性」に対して

USNRCは、訓練に関する勧告に同意している。内部の訓練諮問グループにより、ディジタル系のレトロフィットの検査に従事するスタッフの訓練と教育に関しガイダンスを整備している。NUREG/BR-0227には、ディジタル系のレビュースタッフに有用な訓練コースが示されている。こうした訓練は、ディジタル系ワークショップにより補完され、ディジタル系の問題や活動に関する最新のガイダンスを検査官に提供している。ディジタル系のレビュー及び検査に関する資格制度は、計算機システムの分野において資格認定の基準が十分に確立されていないため、現時点では実践的な選択ではない。

勧告3)「研究プログラムの施策的プラニング」に対して

USNRCは、本勧告に同意している。ディジタル系に関する将来の研究に対し、本勧告の必要性を強調するような施策的なプランが策定されるであろう。同プランでは、規制項目の展開と調査研究とのバランス、他機関との関係、及び、ヒューマンファクタやディジタル計測制御に関する研究施設との協力などの問題に着目することになるであろう。

勧告4)「複数年予算の計画・調整」に対して

USNRCは、本勧告に同意している。USNRCは、複数年ベースでプロジェクトに予算を付けることに合意しつつあるが、議会はUSNRCの予算を単年度ベースで認可している。特殊なタスクに対する研究プログラムは、ほとんどの場合、多数年にわたって計画される。

勧告5)「ガイダンス文書作成・更新の迅速化」に対して

USNRCは、本勧告に同意している。「ケースバイケースの認可プロセス」に関する勧告3)への対応を参照されたい。

5. 米国研究協議会の調査研究における結論

原子力発電プラントにおけるディジタル計測制御系の利用に関して2つの主要なテーマがある。

- ディジタル計測制御技術の特性に関する取扱い（テーマ1：技術的課題）
- 既設炉において幅広く利用されている技術よりも進んでいる技術に関する取扱い（テーマ2：施策的課題）

このうち、テーマ1、即ち、ディジタル技術については、特に、以下の4つの項目が重要なポイントである。

1. 注意して使用する限りにおいて、設計基準事故解析やハザード解析などの決定論的評価手法をディジタル系に適用することは可能である。
2. ソフトウェアに対する故障確率を正確に評価することが可能か否か、また、ソフトウェアがランダムに故障するか否かについては議論の余地がある。しかし、ディジタル系の故障がシステム全体に及ぼす影響を相対的に調べるために、ソフトウェアの故障確率をPRAに使用できるものと考えられる。ソフトウェアの故障を無視するより、PRAにおいて明確にモデル化する方が望ましい。
3. ディジタル系を、ハードウェアあるいはソフトウェアの観点からのみ論じるべきではない。ハードウェアもソフトウェアも纏めて1つのシステムとして取り扱うべきである。例えば、ソフトウェアのCMFはソフトウェア自体の枠を超えてシステム全体として取り扱うことにより解決できるものであり、また、システムの複雑さに関する問題は、ソフトウェアを単純化するだけでは解決できない。
4. 最も実用的なディジタル計測制御系は完全に試験できるわけではなく、従って、エラーが存在しないことを示すことは不可能である。しかし、適切な方法が存在し実用的な範囲で適用できるものと考えられる。

ディジタル計測制御技術は、原子力産業界内外で幅広く利用されており、強力な機能を生み出すものであるが、原子力発電プラントの安全性に影響を及ぼし得るためその適用にあたっては十分注意を払う必要がある。しかしながら、新型炉及び既設炉にディジタル計測制御系を利用することは適切であり、望ましい方向である。特に、既設炉については、ベンダーからの支援がなくなる旧式のシステムや機器に代わってディジタル機器を利用する必要がある。

原著における主要な参考文献

{1} USNRC : "Safety Evaluation Report by NRR Related to Amendment No. 84 to

Facility Operating License No. DPR-80 and Amendment No. 83 to Facility Operating License No. DPR-82: Eagle 21 Reactor Protection System Modification with Bypass Manifold Elimination: Diablo Canyon Power Plant," Docket Nos. 50-275 and -323, October 7, 1993.

{2} USNRC : "Safety Evaluation Report Related to Amendment No. 127 to Facility Operating License No. DRP-48: Zion Nuclear Power Station, Unit 2," Docket No. 50-304, June 9, 1992.

{3} Turkey Point : "Safety Evaluation Report by NRR of the Load Sequencers in the Enhanced Power System at Turkey Point Plant, Unit 3 and 4, Amendment to Operating Licenses DRP-31 and -41," Docket Nos. 50-250 and -251, November 5, 1990.

{4} Palo Verde : "NRC Inspection Report 50-528, 50-529 and 50-530/93-07 Related to Amendment to Operating Licenses No. NPF-41, -51 and -74, Implementation Inspection for Anticipated Transients Without Scram (ATWS) Systems: Palo Verde Nuclear Generating Station Units 1. 2 and 3," Docket Nos. 50-528, -529 and -530, April 9, 1993.

{5} Prairie Island : "Supplemental Safety Evaluation by NRR: Revision 1 of Design Report for Station Blackout/Electrical Safeguards Upgrade Project, Amendment to Facility Operating License No. DRP-42 and -60: Prairie Island Nuclear Generating Plant Units 1 and 2," Docket Nos. 50-282 and -306. January 4, 1993.

{6} ACRS : "Minutes of ACRS Subcommittee Meeting on Computers in Nuclear Power Plant Operations: Quantitative Software Assessment and Analog-to-Digital Industry Experience," February 9, 1993.

{7} J. Mauck : "Regulating Digital Upgrades," Presentation to the Committee, January 31, 1995.

{8} T. Kletz : "Computer Control and Human Error", Gulf Publishing, 1995.

{9} ACRS : "Proposed National Academy of Sciences/National Research Council Study and Workshop on Digital Instrumentation and Control Systems," Letter to I. Selin, Chairman, USNRC, July 14, 1994.

{10} NSRRC : "Summary of April 29, 1992, Meeting," Letter to E. Beckjord, USNRC, November 16, 1992.

{11} J. Knight and N. Leveson : "An Experimental Evaluation of the Assumption of Independence in Multiversion Programming," IEEE Trans. on Software Engineering SE-12(1): 96-109, 1986.

{12} Nucleonics Week : "British Support French I&C System That EDF Has Abandoned for Its N4," January 10, 1991.

{13} S. Watts : "Computer Watch on Nuclear Plant Raises Safety Fears," London Independent, October 13, 1991.

{14} P. Joannou : "Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety," December 1995.

{15} NRC (National Research Council) : "Human Factors Research and Nuclear Safety," National Academy Press, 1988.

{16} H. Lewis : "Digital Instrumentation and Control Systems," Letter to I. Selin (USNRC Chairman), December 11, 1992.

{17} USNRC : "Digital Computer Systems for Advanced Light Water Reactors," SECY-91-292, 1991.

{18} USNRC : "Final Safety Evaluation Report: Related to the Certification of the System 80+ Design," NUREG-1462, Vols. 1-2, 1994.

{19} USNRC : "USNRC Staff (J. Wermeil) Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety," October 1995.

{20} A. Machiels, R. Torok, J. Naser and D. Wilkinson : "The Digital Challenge, An Update on EPRI's I&C Upgrade Initiative," Nuclear Engineering International 40 (489):44-46, 1995.

{21} D. Boettcher : "State-of-the-Art at Sizewell-B," Atom 433 (mar-Apr):34-38, 1994.

{22} Nucleonics Week : "Outlook on I&C: Special Report to the Readers of Nucleonics Week, Inside the N.R.C. and Nuclear Fuel," September and October, 1995.

{23} J. D. White : "Comparative Assessments of Nuclear Instrumentation and Controls in the United States, Canada, Japan, Western Europe, and the Former Soviet Union," JTEC/WTEC Annual Report and Program Summary 1993/94, 1994.

{24} Aviation Week and Space Technology : "Automated Cockpits: Who's in Charge?," January 30 and February 6, 1995.

{25} Center of Chemical Process Safety : "Guidelines for Safety Automation of Chemical Processes," American Institute of Chemical Engineers, 1995.

{26} USNRC : "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 138 to Facility Operating License No. DPR-39 and Amendment No. 127 to Facility Operating License No. DPR-48," June 1992.

{27} W. D. Ghrist III : personal communication to the committee, May 1996.

{28} P. Joannou : "Experience for Application of Digital Systems to Nuclear Power Plants," NUREG/CP-0136, pp.61-77, September 13-14, 1993.

{29} E. Lee : "Computer-Based Digital System Failures," AEOD/T94-03, July 1994.

{30} H. Ragheb : "Operating Maintenance Experience with Computer-Based Systems in Nuclear Power Plants," Presentation at International Workshop on Technical Support for Licensing of Computer-Based Systems Important to Safety, March 1996.

{31} H. M. Paula : "Failure Rates for Programmable Logic Controllers," Reliability Engineering and System Safety 39:325-328, 1993.

{32} D. L. Parnas : "Software Aspects of Strategic Defense Systems," Communications of the Association for Computing Machinery 28(12):1326-1335, 1985.

{33} M. E. Fagan : "Design and Code Inspections to Reduce Errors in Program Development," IBM Systems Journal 15(3):182-211, 1976.

{34} A. Porter, H. P. Sly and L. G. Votta : "A Review of Software Inspections," pp.40-77 in Software Process, Advances in Computers 42, M. V. Zelkowitz (ed.), Academy Press, 1996.

{35} J. Rushby and F. von Henke : "Formal Verification of the Interactive Convergence Clock Synchronization Algorithm Using EHDM," SRI-CSL-89-3R, SRI International, August 1991.

{36} J. Rushby and F. von Henke : "Formal Verification of Algorithms for Critical Systems," IEEE Transactions on Software Engineering 19(1):13-23, 1993.

{37} E. W. Dijkstra : "Structured Programming," pp.84-88 in Software Engineering Techniques, J. N. Buxton and B. Randall (eds.), Scientific Affairs Division, NATO, 1970.

{38} D. Hamlet : "Are We Testing for True Reliability?," IEEE Software 9(4): 21-27, 1992.

{39} Ministry of Defense : "Defense Standard 00-55: The Procurement of Safety Critical Software in Defense Equipment," April 1991.

{40} USNRC : "Draft Branch Technical Position on Defense-in-Depth and Diversity," 1996.

{41} FDA : "Reviewer Guidance for Computer Controlled Medical Devices Undergoing 510(k) Review," 1991.

{42} B. P. Miller, L. Fredrikson and B. So : "An Empirical Study of the Reliability of UNIX Utilities," Communications of the Association for Computing Machinery 33(12):32-44, 1990.

{43} S. Brilliant, J. C. Knight and N. G. Leveson : "Analysis of Faults in an N-Version Software Experiment," IEEE Transactions on Software Engineering 16(2):238-247, 1990.

{44} J. C. Knight and N. G. Leveson : "An Experimental Evaluation of the Assumption

of Independence in Multi-Version Programming," IEEE Transactions on Software Engineering 12(1):96-109, 1986.

{45} R. K. Scott, J. W. Gault and D. F. McAllister : "Fault Tolerant Reliability Modeling," IEEE Transactions on Software Engineering 13(5):582-592, 1987.

{46} J. D. Reese : "Software Deviation Analysis," Ph. D. dissertation, University of California, January, 1996.

{47} N. G. Leveson, S. S. Cha, J. C. Knight and T. J. Shimeall : "The Use of Self Checks and Voting in Software Error Detection: An Empirical Study," IEEE Transactions on Software Engineering 16(4):432-443, 1990.

{48} N. G. Leveson : "Safeware: System Safety and Computers," Addison-Wesley, 1995.

{49} W. C. Bowman, G. H. Archinoff, V. M. Raina, D. R. Tremaine and N. G. Leveson : "An Application of Fault Tree Analysis to Safety-Critical Software at Ontario Hydro," Presentation at Conference on PSAM, April 1990.

{50} NASA : "Space Station Freedom Human-Computer Interface Guidelines," NASA USE-100, 1988.

{51} NASA : "User Interface Guidelines for NASA Goddard Space Flight Center," NASA DSTL-95-033, 1996.

{52} FAA : "The Interfaces Between Flightcrews and Modern Flight Deck Systems," 1996.

{53} D. D. Woods, L. J. Johannesen, R. I. Cook and N. B. Sarter : "Behind Human Error: Cognitive Systems, Computers, and Hindsight," Wright-Patterson AFB, Crew Systems Ergonomics Information Analysis Center, 1994.

{54} J. Rasmussen and L. P. Goodstein : "Information Technology and Work," pp.175-202 in Handbook of Human-Computer Interaction, M. Helander (ed.), North-Holland, 1988.

{55} D. A. Thurman and C. M. Mitchell : "A Design Methodology for Operator Displays of Highly Automated Supervisory Control Systems," Proceedings of the 6th IFAC/IFIP/IFOR/SEA Symposium on Analysis, Design, and Evaluation of Man Machine Systems, June 27-29, 1995.

{56} K. J. Vicente and J. Rasmussen : "Ecological Interface Design: Theoretical Foundations," IEEE Transactions on Systems, Man, and Cybernetics 22(4):589-606, 1992.

{57} E. A. Palmer and A. Degani : "Electronic Checklists: Evaluation of Two Levels of Automation," pp.178-183 (Volume 1) in Proceedings of the 6th International Symposium on Aviation Psychology, April 29-May 2, 1991.

{58} S. A. Converse : "Evaluation of the Computerized Procedures Manual II (COPMA

II)," NUREG/CR-6398, 1995.

{59} H. M. Paula, M. W. Roberts and R. E. Battle : "Operational Failure Experience of Fault-Tolerant Digital Control Systems," Reliability Engineering and System Safety 39:273-289, 1993.

{60} B. Simon : "Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety," February 28, 1996.

{61} Westinghouse/ENEL : "Simplified Passive Advanced Light Water Reactor Plant Program-AP600 Probabilistic Risk Assessment," DE-AC03-90SF18495, Prepared for U. S. Department of Energy, 1992.

{62} P. Marshall : "NE Tries for Quantification of Software-based System," Inside the N.R.C. 17(20):9, 1995.

{63} J. Profetta : "Presentation to the Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety," April 16, 1996.

{64} N. D. Singpurwalla : "The Failure Rate of Software: Does it exist?," IEEE Transactions on Reliability 44(3):463-466, 1995.

{65} R. W. Butler and G. B. Finelli : "The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software," IEEE Transactions on Software Engineering 19(1):3-12, 1995.

{66} D. Parnas, A. J. van Schouwen and S. P. Kwan : "Evaluation of Safety-Critical Software," Communications of the Association of Computing Machinery (33)6:636-648, 1990.

{67} L. L. Pullum and J. Bechta Dugan : "Fault Tree Models for the Analysis of Complex Computer Systems," pp.200-207 in Proceedings of the 1996 Annual Reliability and Maintainability Symposium, January 22-25, 1996.

{68} C. J. Garrett, S. B. Guarro and G. Apostolakis : "The Dynamic Flowgraph Methodology for Assessing the Dependability of Embedded Software Systems," IEEE Transactions on Systems, Man, and Cybernetics 25(5):824-840, 1995.

{69} NUSMG : "Guidance for the Dedication of Commercial Grade Computer Software (Revision 5)," January 4, 1995.

{70} Loral Space Information Systems : "Mission Control Center Upgrade at NASA Johnson Space Center," Loral Corporation Press Release, 1996.

{71} Defense Science Board : "Acquiring Defense Software Commercially," 1994.

{72} USNRC : "Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrade, in Determining the Acceptability of Performing Analog-to-

Digital Replacements under 10 CFR 50.59," Generic Letter 95-02, 1995.

{73} USNRC : "Safety Evaluation Report by the Office of Nuclear Reactor Regulation, Reactor Protection System Upgrade (Phase One)," Connecticut Yankee Atomic Power Company, Docket No. 50-213, March 21, 1990.

6. おわりに

米国研究協議会(NRC : National Research Council)は、米国原子力規制委員会(USNRC : United States Nuclear Regulatory Commission)からの委託を受けて、ディジタル計測制御技術の原子力発電プラントへの適用に関する調査研究を行った。この研究は、2つのフェーズからなり、フェーズ1では、ディジタル技術の導入により生じる安全性及び信頼性に関する課題を明らかにした。フェーズ2では、ディジタル計測制御系のレビュー及び容認のための基準を識別すると共に、USNRCがディジタル計測制御技術に関する規制や許認可を行う際のガイドラインを提言した。なお、この提言に対して、USNRCは自らの見解を示している。

本報告書は、上記フェーズ1及び2における調査結果、並びに、フェーズ2の勧告に対するUSNRCの対応見解を纏めたものである。

NRCによる調査研究では、ディジタル計測制御技術の適用に際しての重要課題として、6つの技術的課題と、2つの施策的課題を摘出し、それぞれについて、USNRCがどう対応すべきかを勧告として提示した。合計で42の勧告（技術的課題に関するものが30項目、施策的課題に関するものが12項目）がなされたが、USNRCは、これらのうち、ヒューマンファクタ及びマンーマシン・インターフェースに関する8つを除き、各々の勧告について自らの対応見解を示した。摘出された重要課題の多くが、既に、USNRCや、その諮問機関である原子炉安全諮問委員会(ACRS)や原子力安全研究レビュー委員会(NSRRC)により明らかとされていたものであることから、多くの勧告（30項目）についてUSNRCが同意している。残る4つの勧告については、同意していないが、これらは、USNRCの策定したガイダンスの米国外での適用、スタッフの他機関への派遣、ソフトウェアの品質保証に関する独自のガイドライン策定、ディジタル系導入時評価の設備変更規則(10 CFR 50.59)への登録、である。

我が国においても、今後、アナログ機器の生産量が低下するに伴い、ディジタル機器の導入は避けられない状態となり、新設のプラントは勿論のこと、既設のプラントにおいても、レトロフィットが行われるものと予想される。我が国において、レトロフィットが規制の対象となるか否かは定かでないが、そうなった場合に対処できるよう基準やガイダンス等の整備・検討を進める必要があると考えられる。本報告書にまとめた、技術的課題や施策的課題及びそれに対するUSNRCの対応見解は、その検討に有用になるものと思われる。

参考文献

[1] National Research Council : "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues," National Academy Press, 1995.

[2] National Research Council : "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Final Report," National Academy Press, 1997.

[3] USNRC : "Disposition of National Research Council/National Academy of Sciences Final Report on Digital I&C Systems in Nuclear Power Plants," 1997.

付録 A
米国原子力規制委員会によるディジタル計測制御技術の許認可[1, 2]

ディジタル計測制御技術の規制に関し、米国原子力規制委員会(USNRC)は、既設炉のレトロフィットと新型炉への導入を検討してきた。

（既設炉）

これまでに、USNRC は、既設炉に対する数多くのレトロフィットを承認してきた。これらのレトロフィットは、個々の機器の取替という小規模なものから、原子炉保護系(RPS)全体の交換といった大規模なものまで含んでいる。最初に RPS 全体の交換が行われたのは、1991 年の Haddam Neck 炉である。その後、Sequoyah、Zion、Diablo Canyon、D.C.Cook において行われた。 USNRC は、これらのレトロフィットを評価し、プログラム式のディジタル機器を冗長性のある安全系に適用することによりプラント保護系の冗長性や独立性を損なうようなソフトウェアの共通原因故障(CMF)の可能性が導入されると結論づけた。その結果、今後行われる全てのレトロフィットにより 10 CFR 50.59 で定義される USQ が生じ得るとの結論に至った。未レビュー安全問題(USQ)が生じる場合には 10 CFR 50.59 に従って公式の許認可プロセスを踏むことになり、その結果、レビュープロセスや公開ヒアリングなどが要求される。さらに、こうした手続きに時間と費用が余分にかかるため、電力会社がレトロフィットへの移行を躊躇する要因となっている。USNRC は、問題の認識と USNRC の見解に関してより良い理解を得るために、何故レトロフィットによって USQ が生じ事前承認を受けずに手続きを進めることができないかを説明した Generic Letter のドラフトを発行した。しかし、産業界は、殆どのレトロフィットが USQ を伴うものであるとは考えておらず、こうした見解の相違を解決させるために、USNRC の協力を得てガイドラインを策定した。USNRC は、このガイドラインを承認したが、その一方で、未解決な問題も残されているとの見解を示した。

（新型炉）

USNRC は、新型炉の設計をレビューしてきたが、この中には、GE (General Electric) 社の ABWR や SBWR、WH (Westinghouse)社の AP600 及び ABB-CE (Asea Brown Boveri - Combustion Engieering)社の System 80+が含まれている。これらの新型炉の計測制御系は全てディジタル式となっている。軽水炉の設計は産業界のガイドラインに従っており、USNRC は同ガイドラインを評価したが、ディジタル計測制御技術の適用に関わる問題の多くを完全には解決しなかった。USNRC は、2 つの新型炉設計に関して最終設計承認を行ったが、その認可は現在進行中である。新型炉においては、実際のプラント機器（ソフトウェアを含む）がレビューできない状態にあるため、USNRC による設計レビューは設計プロセスのみを対象としている。従って、ディジタル計測制御技術に関する認可問題が解決されなければ、新型炉の設計に関する最終認可も困難であると考えられる。

（規準策定）

USNRCは、産業界や専門家と協力して、ディジタル計測制御技術の適用に対する規準の策定を進めてきた。既に、USNRC のガイドラインや産業界の規準が整備されているが、USNRCは、新たなガイダンスの策定を継続して行ってきた。また、ディジタル技術の評価や規制に関わる問題についての研究も進めてられているが、現時点では結論を出すには至っていない。

（最近の動向）

最近のUSNRCの見解によれば、USNRCは、要求事項と容認規準の明確化を図ろうとしている。USNRCは、深層防護の立証を要求するであろうが、単一の故障による影響を受けない設備の多様性によって同一の安全機能を果たすことができればCMFによる安全機能の喪失は容認されるであろう。さらに、USNRCは、ディジタル式あるいはアナログ式の非安全系の利用と運転員操作によるバックアップの組合せによる多様性の実現を認めるであろう。また、最近、USNRCは、ベンダーによる性能及び妥当性評価(V&V : verification and validation)を事前に審査し、その結果に基づいてソフトウェアの信頼性が適切であることを認めることになるとの見解も示している。しかしながら、現時点では、一般的なガイドラインが十分に整備されていないため、事前承認については依然としてケースバイケース的なアプローチが不可欠である。

付録 B
ディジタル計測制御系の特徴[2]

ディジタル系の主要な特徴としては、実時間処理、データ通信、シーケンシャル動作、多重通信、多重タスク処理、メモリ共用、データ転送・記憶媒体などがあり、各々について以下に記す。

（実時間処理）

実時間システム(real time system)とは、応答の正確さが計算の結果のみならず結果を得る時間にも依存するシステムであると定義される。このシステムには、制御する系統（制御系）と制御される系統（被制御系）が含まれる。制御系は、定期的に被制御系とその環境に関する情報を受け取り処理し、それに応じて被制御系に対して制御コマンドを発信する。この動作を安定させ性能要求を満たすために、制御系と被制御系との間のタイミング上の関係は、完全な制御シーケンス（パラメータサンプリング、伝送処理、制御コマンドの生成とプロセスへの伝送）が制御されるプロセスの応答時間より速く処理されるよう、設定しなければならない。重要なシステムに対しては、制御系のタイミング解析において通信の遅れや実行時間に関し最悪の値を考慮する。この最悪の値により設計上の制約が課せられる。即ち、実時間システムでは最悪の事態に対して応答を保証しなければならない。また、実時間システムの故障モードには、制御系の故障モードが含まれており、これは、タイミングエラーにより増幅される。タイミングエラーは打ち切り時間が履行されない場合に発生し、また、その結果は制御プロセスに依存する。複数の打ち切り時間が履行されなくても実時間システムが機能する場合があるが、殆どの場合は、その打ち切り時間の数に制限がある。

原子力発電プラントのような大規模なシステムへ適用する際には、実時間システムは、通常、最初から一般目的の計算機を用いて記述されることはない。むしろ、多くのベンダーは幅広く利用されている民生品の適用を提案する。その結果、プロセス制御用に設計される実時間システムは、多数のマイクロプロセッサ・モジュールを通信ネットワークにより相互に接続したものとなり、これにより、プロセス制御機能を実行することになる。データ取得やプロセス変数の制御等には関数モジュールが用意されている。こうした民生用のプロセス制御系のプログラミングでは、ライブラリから関数ブロックを選んで相互に繋ぐことになるが、通常、この相互作用はシステム設計者によりプログラミングされる。こうした特定目的のプロセス制御系を利用することによってある種の制約が課せられるため、最初から実時間システムを作成する場合に生じ得る多くの問題は避けられる。例えば、特定目的のプロセス制御系は、予め定義された標準的な関数モジュールに依存するため、一般目的のソフトウェア言語でプログラミングする必要はない。さらに、実時間オペレーティングシステムを利用することで、タイミング解析が簡素化され予測性の確認にも役立つ。

（データ通信）

プロセス制御系では、制御ノードをリンクするために、信頼性の高い通信ネットワークが

必要となり、この通信システムでは、負荷が大きい場合にもある程度のレベルの性能を保証し、メッセージの喪失やエラーの際に検出及び修復を行うことができなければならない。通信システムに関して重要なポイントは、データ・ハイウェイ通信ネットワーク用のアーキテクチャー（及びプロトコル）を構築することである。アーキテクチャーは産業によって多種多様であるが、token passing ring-based, broadcast-based, cluster-based といった３つ体系が共通に使用されている。これら各タイプのネットワークに対しては、既に、明確なアーキテクチャーとアルゴリズムが構築されている。

通信システムに関連した故障モードとしては、(a)メッセージの遅れや喪失、(b)メッセージの間違い、(c)送信後のメッセージの孤立（エラーが起こったために送信プロセッサが既に保存されたチェックポイントに戻ることによってメッセージの意味が失われる）、(d)メッセージの矛盾（これにより、複数の受取側が一貫性のない動きをすることがある）などがある。共用資源に関連する故障モードも考慮しなければならない。伝送終点でデータを取り出し結合させるマルチプレクサと受信終点で信号のデコードを行うマルチプレクサは、多重信号を順次処理するため、システムにおける弱点となる。

（シーケンシャル動作）

ディジタル系におけるマイクロプロセッサは、ソフトウェアのコマンドを順次実行する。シーケンシャル動作には、以下の項目が含まれる。

1. 制御ループのモジュールにおけるシーケンシャル処理能力は、ループ制御の応答がプロセス応答時間より数倍速くなるようにする必要がある。これは、閉ループ制御の安定性理論に基づくものである。ディジタル系では、高優先度の中断や先行処理が行われるため新たな時間遅れが生じ得る。従って、閉ループ制御アルゴリズムは、こうした不測の中断や先行処理によるタイミングの不確実さを伴わずに予測可能な方法で実行されるよう整備すべきである。
2. 閉ループ制御、制御・警報インターフェース、及び、性能計算に対して、専用の分離した母線を使用することは極めて好ましい。これにより、不必要な時間遅れが制御ループに導入される可能性が小さくなる。

（多重通信）

ディジタル系は、複数のプロセスパラメータを取り出し、単一の通信チャンネル上のメモリに伝送することができ、同様に、多重のコマンド制御信号をプラントプロセスに同時に伝送することもできる。従来、多重通信とは、こうしたタイプのプロセスパラメータの信号伝送に用いられてきた言葉であるが、ディジタル計測制御系における通信リンクでも様々な性質の情報（性能解析結果、時系列データファイルや表示データファイルなど）を伝達する。こうした多重通信機能は情報の伝送経路を共用し、また、多重通信自身もシーケンシャルな装置である。多重通信は、全てのデータの取得と利用が一貫性のある方法で行われるようプラント全体を通して調整しなければならない。プラントの性能や保護に重要な時間感受性の高いデータの多重通信は、決定論的なデータブスやデータリンクを介して最も良く処理され

る。なお、データブスやデータリンクは、設計レビューや試験においてV&Vを行うに際に容易な予測可能な方法でデータを処理する。さらに重要なのは、安全系に利用されるような独立チャンネルに関する多重通信が独立性を無効にする場合もあるため回避しなければならないということである。これに関するガイダンスは、NUREG/CR-6082（データ通信）に示されている。

（多重タスク処理）

多重タスク処理では、進行中のタスクを中断させ、優先度の高い別のタスクを開始させることができる。実際、この機能はソフトウェアの特徴であるが、ディジタル系の性能に影響を及ぼす可能性がある。時間感受性の高いシステムでは、優先処理的な多重タスク処理により時間遅れが生じ得るためその適用は望ましくない。こうした場合、決定論的な方法でタスクを処理する方が望ましく、重要なタスクが常に実施されることになる。一般に、多重タスク処理は、時間感受性が高くなく、また、そうした機能に相互干渉を持たない機能適用可能である。例えば、多重タスク処理は、時系列データの分析や診断計算などのオフライン機能には有用であると考えられる。

（メモリ共用）

ディジタル系では、制御動作、性能計算及び表示を行うために、時系列データを利用するが、これらのデータは、多重のプロセッサがアクセスできるよう保存される。あるプロセッサは、プラントプロセスから取り出したデータをメモリ上に記憶するが、その一方で、別のプロセッサはこれらのデータを利用する。例えば、1つのプロセッサによりタンクの水位を定期的に取り出してメモリ上に記憶させるが、別のプロセッサはその保存データを用いて水位制御のためのドレン弁を開閉させる。さらに、3番目のプロセッサは同じデータを用いて別のタンクに水を移送させ、4番目のプロセッサは制御室にその水位を表示させる。メモリを共用するには、データが常に正しくなるように、メモリからのデータの流れを管理・保護する必要がある。

（多様性のあるデータ伝送・保存媒体）

ディジタル信号は、アナログ系とは異なったタイプの媒体上で保存・伝送される。例えば、データは異なるタイプの磁気媒体上に保存することができ、光データ・ハイウェイを通して伝送することができる。しかし、賛否両論があることを認識する必要がある。例えば、光信号の伝送媒体がしばしばディジタル系に使用されるが、光学媒体は従来の電導体よりも強健で、あらゆる電磁干渉に対して免疫があり、電気回路での地絡による影響を受けない。光学ケーブルは、完全に電気絶縁することができ、殆どの化学物質に対する抵抗力がある。さらに、発生するノイズは相対的に小さく、信号の減衰も小さい。しかし、光ファイバーケーブルの設置には、特別な訓練と道具が必要となる。ディジタル計測制御系において、伝送・保存媒体に多様性を持たせることは、現時点で克服できない課題ではない。媒体は使用環境に対する品質を保証しなければならないが、その方法は、アナログ機器やディジタル機器に対してこれまでに行ってきた品質保証の方法と同様である。

付録 C
ディジタル計測制御系に関する技術基準、規制指針、NUREGレポート等

本付録では、ディジタル計測制御系に関連する技術規準、規制指針、NUREG レポートなどを示すが、以下では、本報告書で参照していないものも含めている（＊付の文献は、本報告書で参照されていないものを表わす）。

技術規準

ANSI/IEEE/ANS 7-4.3.2-1993 : Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations（安全系におけるディジタル計算機に関する基準）, ANSI/IEEE/ANS 7-4.3.2-1982 (Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations)の改訂版, 1993.

ASME NQA-2A-1990. Part 2.7 : Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications（原子力施設への計算機システムの利用に関する品質保証要求）, 1990.

IEEE 603-1991 : Standard Criteria for Safety Systems in Nuclear Power Generating Stations（安全系に関する基準）, IEEE Standard 279-1971 の続報, 1991.

IEEE 730.1-1993* : Software Quality Assurance Plans（ソフトウェアの品質保証計画）, 1993.

IEEE 730.2-1993* : Guide to Software Quality Assurance Planning（ソフトウェアの品質保証計画立案に関するガイダンス）, 1993.

IEEE 828-1990 : Standard for Configuration Management Plans（構成管理計画に関する規準）, 1990

IEEE 829-1983 : Standard for Software Test Documentation（ソフトウェア試験の文書化に関する規準）, 1983.

IEEE 830-1984 : Guide for Software Requirements Specifications（ソフトウェアの要求仕様に関する指針）, 1984.

IEEE 1008-1987 : Standard for Software Unit Testing（ソフトウェアの単体試験に関する規準）, 1987.

IEEE 1012-1986 : Standard for Software Verification and Validation Plans（ソフトウェアの V&V 計画に関する基準）, 1986.

IEEE 1016-1987* : Software Design Descriptions（ソフトウェア設計に関する記述）, 1987.

IEEE 1028-1988 : Standard for Software Reviews and Audits（ソフトウェアのレビュー及び審査に関する規準）, 1988.

IEEE 1042-1987 : Guide for Software Configuration Management（ソフトウェアの構成管

理に対する指針），1987.

IEEE 1058.1-1987* : Software Project Management Plans（ソフトウェアのプロジェクト管理計画），1987.

IEEE 1059-1993* : Guide for Software Verification and Validation Plans（ソフトウェアのV&V計画に関するガイダンス），1993.

IEEE 1074-1988 : Standard for Developing Software Life Cycle Processes（ソフトウェアのライフサイクル策定に関する規準），1988.

IEEE 1228-1994* : Software Safety Plans（ソフトウェアの安全性プラン），1994.

IEC 880 : Software for Computers in Safety Systems of Nuclear Power Stations（安全系における計算機ソフトウェア），1986.

IEC 987 : Programmed Digital Computers Important to Safety for Nuclear Power Stations（安全上重要なディジタル計算機），1989.

USNRCの規制指針

Regulatory Guide 1.152 : Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants（安全関連系におけるディジタル計算機システム・ソフトウェアに関する基準），IEEE 7-4.3.2-1993を承認，1996.

Regulatory Guide 1.153* : Criteria for Power, Instrumentation, and Control Portions of Safety Systems（安全系の駆動力、計測及び制御に対する基準），IEEE 603-1991を承認，1996.

Regulatory Guide 1.168 (Draft DG-1054)* : Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants（安全系のデジタル計算機ソフトウェアに対する検証、性能評価、レビュー及び監査），IEEE 1012-1986及びIEEE 1028-1988を承認，1997.

Regulatory Guide 1.169 (Draft DG-1055)* : Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants（安全系のデジタル計算機ソフトウェアに対する構成管理プラン），IEEE 828-1990及びIEEE 1042-1987を承認，1997.

Regulatory Guide 1.170 (Draft DG-1056)* : Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants（安全系のデジタル計算機ソフトウェアに対する試験文書化），IEEE 829-1983を承認，1997.

Regulatory Guide 1.171 (Draft DG-1057)* : Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants（安全系のデジタル計算機ソフトウェアに対する単体試験），IEEE 1008-1987を承認，1997.

Regulatory Guide 1.172 (Draft DG-1058)* : Software Requirements Specifications for

Digital Computer Software Used in Safety Systems of Nuclear Power Plants（安全系のデジタル計算機ソフトウェアに対する要求仕様），IEEE 830-1993を承認, 1997.

Regulatory Guide 1.173 (Draft DG-1059)* : Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants（安全系のデジタル計算機ソフトウェアに対するライフサイクルの策定），IEEE 1074-1995を承認, 1997.

NUREGレポート

NUREG-0800 : Standard Review Plan (SRP)（標準レビュープラン），1984 (Revised 1997)

NUREG-0700 : Guidelines for Control Room Design Reviews（制御室設計レビューに関するガイドライン），1981.

NUREG-0700, Rev.1 : Human-System Interface Design Review Guideline (a draft for comment)（マンーシステム・インターフェース設計のレビューに関するガイドライン），1995.

NUREG-0711 : Human Factors Engineering Program Review Model（ヒューマンファクタ工学プログラムのレビューモデル），1994.

NUREG/CR-6101* : Software Reliability and Safety in Nuclear Protection Systems（原子炉保護系におけるソフトウェアの信頼性と安全性），1993.

NUREG/CR-6113 : Class IE Digital Systems Studies（クラス1Eディジタル系に関する研究），1993.

NUREG/CR-6263* : High Integrity Software for Nuclear Power Plants（原子力発電所のための高健全性ソフトウェア），1995.

NUREG/CR-6293 *: Verification and Validation for High Integrity Systems（高健全性システムに対する性能及び妥当性評価），1995.

NUREG/CR-6421 : A Proposed Acceptance Procedure for Commercial Off-the Shelf (COTS) Software in Reactor Applications（民生既製品ソフトウェアの原子炉への適用に対する容認手順の提案），1996

NUREG/CR-6463, Rev. 1* : Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems（原子力発電所の安全系への利用に対するソフトウェア言語に関するレビューガイドライン），1996.

NUREG/CR-6465* : Development of Tools for Safety Analysis of Control Software in Advanced Reactors (authored by S. Guarro, M. Yau and M. Motamed)（新型炉における制御用ソフトウェアの安全解析ツールの開発），1996.

NUREG/BR-0227 : Guidance for Professional Development of NRC Staff in Digital Instrumentation and Controls（ディジタル計測制御系に関するUSNRCスタッフの能力開発に関するガイダンス），1996.

USNRC計測制御部門の技術見解(BTP : branch technical position)

HICB-14 : Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems（ディジタル計算機ベースの計測制御系に対するソフトウェアのレビューに関するガイダンス），1996.

HICB-16* : Guidance on the Level of Detail Required for Design Certification Applications under 10 CFR Part 52 （10 CFR 52に基づく設計認可申請に要求される詳細レベルに関するガイダンス），1996.

HICB-17* : Guidance on Self-Test and Surveillance Test Provisions （自己試験及びサーベランス試験規定に関するガイダンス），1996.

HICB-18* : Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumenation and Control Systems（ディジタル計算機ベースの計測制御系におけるプログラマブル・ロジック制御装置の利用に関するガイダンス），1996.

HICB-19* : Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumenation and Control Systems（ディジタル計算機ベースの計測制御系における深層防護及び多様性の評価に関するガイダンス），1996.

HICB-21* : Guidance for Digital Computer Real-Time Performance （ディジタル計算機の実時間性能に関するガイダンス），1996.

USNRCによる規制関連書簡

Generic Letter (GL) 95-02 : Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-Digital Replacements under 10 CFR 50.59（10 CFR 50.59に基づくアナログーディジタル変更の容認性検討におけるTR-102348の利用），1995.

連邦規制規則(CFR)

10 CFR 50.59 : Changes, Tests and Experiments 変更、試験及び実験

10 CFR 50.90 : Application for Amendment of License or Construction Permit 許認可及び建設許可の改正申請

10 CFR 50.55a(h) : Codes and Standards (Protection Systems)規則及び規準（原子炉保護系），IEEE Standard 279-1971の使用を承認

10 CFR 21 : Procurement of Commercial Grade Items by Nuclear Power Plant Licensees 原子力発電所の設置者による商用製品の調達

10 CFR 109 : Backfitting バックフィッティング規則

原子力産業界のガイダンス

NSAC-125 : Guidelines for 10 CFR 50.59 Safety Evaluations（10 CFR 50.59対応の安全評価に関するガイドライン），1988.

EPRI NP-5652 : Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications（商用製品の安全系への利用に関するガイドライン），1988.

EPRI TR-106439 : Guideline on Evaluation and Acceptance of Commercial Grade Equipment for Nuclear Safety Applications（民生用機器の原子力安全系への適用評価及び容認に関するガイドライン），1996.

EPRI TR-102348 : Guideline on Licensing Digital Upgrades（ディジタル系への許認可変更に関するガイドライン），1993.

他産業界のガイダンス

DO-178B（連邦航空管理局(FAA)の規準）: Software Considerations in Airborne Systems and Equipment Certification（空輸システム・設備の認可におけるソフトウェアの考慮），1992.

MIL-STD-882C : System Safety Program Requirements（システムの安全性プログラムに関する要求），1993.

カナダ(AECB)における規制指針

Regulatory Draft Guide C-138 : Software in Protection and Control Systems（保護制御系におけるソフトウェア），1996.

Regulatory Document R-8 : Requirements for Shutdown Systems for CANDU Nuclear Power Plants（CANDU 炉の停止系に対する要求項目），1996.

Regulatory Document R-10 : The Use of Two Shutdown Systems in Reactors（2 系統の停止系の利用），1996.

用語解説

アナログ技術(Analog technology)：連続変数量でデータが表現される装置

連邦規制規則(Code of Federal Regulations) 10 CFR 50, 10 CFR 50.59：10 CFR 50は、米国内における原子力発電プラントの許認可の法則基準である。10 CFR 50.59は、許認可されている原子力発電プラントにおいて設備変更を行う際に、事前にUSNRCの承認を得る必要があるか否かを判断するための基準を示している。10 CFR 50の付録Aには、原子力発電プラントの設計、建設及び運転において従うべき「一般設計基準(general design criteria)」が示されている。

ソフトウェアの共通モード／原因故障(Common-mode software failure)：多重性を有するソフトウェアが同じように故障すること

構成管理(Configuration control/management)：構成要素の機能的・物理的な特徴を識別して文書化し、その特徴の変更を管理し、変更の進捗状況や実施状況を記録・報告し、さらに、所定の要求を満足していることを確認するための、技術的かつ運用上の指導及び監視

(民生品の) 利用(Dedication)：民生品の安全系への適用が提案された場合に、10 CFR 50の付録Bに示される品質保証プログラムに従って作成された機器と同等レベルの品質であることを確認するために行われる品質管理プロセス

ディジタル技術(Digital technology)：0あるいは1などの離散値の組合せでデータが表現される装置

多様性(Diversity)：同一機能を果たすために相互排他的な複数の手段を利用すること。設計多様性、機能多様性、ネームプレート多様性がある。設計多様性は、同一機能を果たすために内部設計の異なる複数の機器を利用することである。機能多様性は、より高度なレベルの機能及び要求の観点からは関連があるものの異なる機能を達成するために複数の機器を利用することである。ネームプレート多様性は、同一機能を果たすために製造者の異なる機器を利用することである。

環境に対する品質保証(Environmental qualification)：想定される環境条件で機器の動作を確認するための試験及び検証プロセス

フォーマル・メソッド(Formal methods)：数学的に定義された意味論(semantics)による設計仕様及びこうした仕様に対して定義された数学的な解析手法

多重性(Redundancy)：個々の機器故障時に、所定の機能を果たす代替手段を確保するために同一あるいは同種の機器を利用すること。多様性を有しない場合にもランダム故障や疲労性故障に対処するための方策として使用される。

ソフトウェア品質保証(Software quality assurance)：所定の品質を有するソフトウェアの作成プロセスと規準

ソフトウェア設計仕様(Software specification)：設計及び導入に当たっての基準となるソフ

トウェア各部の記述

標準レビュープラン、部門技術見解、規制指針(Standard Review Plan, Branch Technical Positions, Regulatory Guides)：USNRC レビュー者用のガイダンスで、提案された設計の適性を評価するために設置者が提出すべきもの、あるいは、許認可要求に従っていることを示すための方法を規定している。部門技術見解、規制指針及び産業界規準では、さらに詳細なガイダンスが示されている。

静的解析(Static analysis)：ソフトウェアを実行せずに潜在的なエラーを検出するために行うソフトウェアの手動あるいは自動的な解析

筋道審査(Thread audit)：ソフトウェアの入力から出力まで一貫して調べるためのソフトウェアのレビュー方法

未レビュー安全問題(Unreviewed safety question)：プラントの安全解析において未解析な故障モード

性能及び妥当性評価(Verification and validation)：性能評価(verification)は、設計の各段階における成果（製品）がそれ以前の段階で課せられた要求を満たしているか否かを確認するためのプロセスである。妥当性評価(validation)は、システムに対する所定の機能、性能、及び、インターフェースに関する要求項目を満足していることを確認するための試験及び設計評価である。

国際単位系 (SI) と換算表

表 1　SI 基本単位および補助単位

量	名称	記号
長さ	メートル	m
質量	キログラム	kg
時間	秒	s
電流	アンペア	A
熱力学温度	ケルビン	K
物質量	モル	mol
光度	カンデラ	cd
平面角	ラジアン	rad
立体角	ステラジアン	sr

表 2　SI と併用される単位

名称	記号
分，時，日	min，h，d
度，分，秒	°，′，″
リットル	l，L
トン	t
電子ボルト	eV
原子質量単位	u

1 eV = 1.60218 × 10^{-19} J

1 u = 1.66054 × 10^{-27} kg

表 5　SI 接頭語

倍数	接頭語	記号
10^{18}	エクサ	E
10^{15}	ペタ	P
10^{12}	テラ	T
10^{9}	ギガ	G
10^{6}	メガ	M
10^{3}	キロ	k
10^{2}	ヘクト	h
10^{1}	デカ	da
10^{-1}	デシ	d
10^{-2}	センチ	c
10^{-3}	ミリ	m
10^{-6}	マイクロ	μ
10^{-9}	ナノ	n
10^{-12}	ピコ	p
10^{-15}	フェムト	f
10^{-18}	アト	a

表 3　固有の名称をもつ SI 組立単位

量	名称	記号	他の SI 単位による表現
周波数	ヘルツ	Hz	s^{-1}
力	ニュートン	N	m·kg/s^2
圧力，応力	パスカル	Pa	N/m^2
エネルギー，仕事，熱量	ジュール	J	N·m
工率，放射束	ワット	W	J/s
電気量，電荷	クーロン	C	A·s
電位，電圧，起電力	ボルト	V	W/A
静電容量	ファラド	F	C/V
電気抵抗	オーム	Ω	V/A
コンダクタンス	ジーメンス	S	A/V
磁束	ウェーバ	Wb	V·s
磁束密度	テスラ	T	Wb/m^2
インダクタンス	ヘンリー	H	Wb/A
セルシウス温度	セルシウス度	℃	
光束	ルーメン	lm	cd·sr
照度	ルクス	lx	lm/m^2
放射能	ベクレル	Bq	s^{-1}
吸収線量	グレイ	Gy	J/kg
線量当量	シーベルト	Sv	J/kg

表 4　SI と共に暫定的に維持される単位

名称	記号
オングストローム	Å
バーン	b
バール	bar
ガル	Gal
キュリー	Ci
レントゲン	R
ラド	rad
レム	rem

1 Å = 0.1 nm = 10^{-10} m

1 b = 100 fm^2 = 10^{-28} m^2

1 bar = 0.1 MPa = 10^5 Pa

1 Gal = 1 cm/s^2 = 10^{-2} m/s^2

1 Ci = 3.7 × 10^{10} Bq

1 R = 2.58 × 10^{-4} C/kg

1 rad = 1 cGy = 10^{-2} Gy

1 rem = 1 cSv = 10^{-2} Sv

（注）

1. 表 1 − 5 は「国際単位系」第 5 版，国際度量衡局 1985 年刊行による。ただし，1 eV および 1 u の値は CODATA の 1986 年推奨値によった。
2. 表 4 には海里，ノット，アール，ヘクタールも含まれているが日常の単位なのでここでは省略した。
3. bar は，JIS では流体の圧力を表わす場合に限り表 2 のカテゴリーに分類されている。
4. EC 閣僚理事会指令では bar，barn および「血圧の単位」mmHg を表 2 のカテゴリーに入れている。

換算表

力	N(=10^5 dyn)	kgf	lbf
	1	0.101972	0.224809
	9.80665	1	2.20462
	4.44822	0.453592	1

粘度　1 Pa·s(N·s/m^2) = 10 P(ポアズ)(g/(cm·s))

動粘度　1 m^2/s = 10^4 St(ストークス)(cm^2/s)

圧力	MPa(=10 bar)	kgf/cm^2	atm	mmHg(Torr)	lbf/in^2(psi)
	1	10.1972	9.86923	7.50062 × 10^3	145.038
	0.0980665	1	0.967841	735.559	14.2233
	0.101325	1.03323	1	760	14.6959
	1.33322 × 10^{-4}	1.35951 × 10^{-3}	1.31579 × 10^{-3}	1	1.93368 × 10^{-2}
	6.89476 × 10^{-3}	7.03070 × 10^{-2}	6.80460 × 10^{-2}	51.7149	1

エネルギー・仕事・熱量	J(=10^7 erg)	kgf·m	kW·h	cal(計量法)	Btu	ft·lbf	eV
	1	0.101972	2.77778 × 10^{-7}	0.238889	9.47813 × 10^{-4}	0.737562	6.24150 × 10^{18}
	9.80665	1	2.72407 × 10^{-6}	2.34270	9.29487 × 10^{-3}	7.23301	6.12082 × 10^{19}
	3.6 × 10^6	3.67098 × 10^5	1	8.59999 × 10^5	3412.13	2.65522 × 10^6	2.24694 × 10^{25}
	4.18605	0.426858	1.16279 × 10^{-6}	1	3.96759 × 10^{-3}	3.08747	2.61272 × 10^{19}
	1055.06	107.586	2.93072 × 10^{-4}	252.042	1	778.172	6.58515 × 10^{21}
	1.35582	0.138255	3.76616 × 10^{-7}	0.323890	1.28506 × 10^{-3}	1	8.46233 × 10^{18}
	1.60218 × 10^{-19}	1.63377 × 10^{-20}	4.45050 × 10^{-26}	3.82743 × 10^{-20}	1.51857 × 10^{-22}	1.18171 × 10^{-19}	1

1 cal = 4.18605 J(計量法)
= 4.184 J　(熱化学)
= 4.1855 J　(15 °C)
= 4.1868 J(国際蒸気表)

仕事率　1 PS(仏馬力)
= 75 kgf·m/s
= 735.499 W

放射能	Bq	Ci
	1	2.70270 × 10^{-11}
	3.7 × 10^{10}	1

吸収線量	Gy	rad
	1	100
	0.01	1

照射線量	C/kg	R
	1	3876
	2.58 × 10^{-4}	1

線量当量	Sv	rem
	1	100
	0.01	1

（86 年 12 月 26 日現在）

原子力発電プラントにおけるディジタル計測制御系の安全性及び信頼性に関する課題と米国原子力規制委員会の対応（調査報告書）