日本語翻訳版

IAEA　安全基準

人と環境を防護するために

原子力発電所の計測制御系の設計

個別安全指針

No. SSG-39

国際原子力機関

２０２２年　３月

原子力規制庁　翻訳

本翻訳版発行に当たっての注記事項

A：本翻訳版は非売品である。

B：本翻訳版は、「Desgin of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide No. SSG-39」©International Atomic Energy Agency, (2016)の日本語訳である。本翻訳版は、原子力規制庁により作成されたものである。本翻訳版に係る IAEA 出版物の正式版は、国際原子力機関（IAEA）又はその正規代理人により配布された英語版である。IAEA は、本翻訳版に係る正確性、品質、信頼性又は仕上がりに関して何らの保証もせず、責任を持つものではない。また、本翻訳版の利用により生じるいかなる損失又は損害に対して、これらが当該利用から直接的又は間接的・結果的に生じたものかを問わず、何らの責任を負うものではない。

C：著作権に関する注意：本翻訳版に含まれる情報の複製又は翻訳の許可に関しては、オーストリア国ウィーン市 1400 ウィーン国際センター（私書箱 100）を所在地とする IAEA に書面により連絡を要する。

D：本翻訳版は、業務上の必要性に基づき、原子力規制庁が IAEA との合意に基づき発行するものであり、唯一の翻訳版である。

E：原子力規制庁は、本翻訳版の正確性を期するものではあるが、本翻訳版に誤記等があった場合には、正誤表と合わせて改訂版を公開する。また、文法的な厳密さを追求することで難解な訳文となるものは、分かりやすさを優先し、本来の意味を損なうことのない範囲での意訳を行っている箇所もある。

なお、本翻訳版の利用により生じるいかなる損失又は損害に対して、これらが当該利用から直接的又は間接的・結果的に生じたものかを問わず、原子力規制庁は何らの責任を負うものではない。

目次

１．はじめに

背景

1.1.　本安全指針は、IAEA 安全基準シリーズ No. SSR-2/1 (Rev. 1) 「原子力発電所の安全設計」[1]で定められた要件を満たすための、計測制御（I&C）系の設計に関する推奨事項を提示する。

1.2.　本刊行物は、2 つの安全指針、すなわち、IAEA 安全基準シリーズ No. NS-G-1.1[1]及び No. NS-G-1.3[2]の改訂及び統合であり、これらに置き換わる。この改訂は、2000 年及び 2002 年の旧安全指針の出版以降の I&C 系の開発を考慮に入れている。主な変更は、継続的なコンピュータ適用技術の開発及びこれらの安全、確実及び実用的な利用のために必要な手法の進展に関係している。加えて、人間工学の発展及びコンピュータ・セキュリティの必要性を考慮に入れている。本安全指針は、I&C 設計に関係する手引きを提示する他の IAEA 安全基準及び核セキュリティシリーズの刊行物を参照し、また、考慮に入れている。これらの中で代表的なのものは、IAEA 安全基準シリーズ No. GS-R-3「施設及び活動に関するマネジメントシステム」[2]、No. GS-G-3.1「施設及び活動に関するマネジメントシステムの適用」[3]、No. GS-G-3.5「原子炉等施設に関するマネジメントシステム」[4]及び GSR Part 4 (Rev. 1)「施設及び活動に関する安全評価 」[5]である。

1.3.　本安全指針が提示する新規又は最新化された指針の主な分野は以下である。

- GS-R-3[2]で定められた要件を遵守することに関する、I&C に固有の考慮事項
- I&C 系の設計基準策定時に考慮されるべき設計入力情報
- I&C 系の設計及び実装のためのライフサイクル、並びに、特に施設全体の一体化した I&C、個々の I&C 系及びソフトウェアに関するライフサイクルの相互依存的な性質、また、これらのライフサイクルへの人間工学及びコンピュータ・セキュリティの入力情報の統合の必要性
- コンピュータ、ハードウェア記述言語でプログラムされた装置及び機能を限定された産業用装置の利用、並びにそれらの正しい動作の保証を得る手段
- 発電所システムの設計に適用された深層防護の概念の支援を受けての、また、共通原因故障に対する防護として I&C 系自体の深層防護を確立する際の、I&C 全体構造
- 安全上重要な系統間でのデータ伝送、特にデータ送信側より受信側がより高位の安全クラスの系統である場合の考慮
- デジタル安全系のセキュリティを確保することに対する方策

---

[1] IAEA 安全基準シリーズ No. NS-G-1.1「原子力発電所における安全上重要なコンピュータに基づいた系統のためのソフトウェア」

[2] IAEA 安全基準シリーズ No. NS-G-1.3「原子力発電所における安全上重要な計測制御系」

－ 本安全指針又は間接的に前の安全指針 NS-G-1.1[3]で与えられた原則に由来する、設計、検証及び妥当性確認を含めた、コンピュータソフトウェアの開発に関係する活動

1.4. 本安全指針を通して、用語「I&C 系」は、IAEA 安全用語集[6]に定義されている安全上重要なあらゆる I&C 系を指す。用語「安全上重要な」は強調する場合を除き繰り返さない。推奨事項又は説明が、安全上重要な I&C 系及び安全上重要ではない I&C 系の両方に適用できる場合、このことは明確に記述される。

1.5. 本安全指針は、IAEA 安全基準シリーズ No.SSG-34「原子力発電所の電力系統の設計」[7] と密に関係しており、同基準は、電源供給、ケーブル系統、電磁障害に対する防護、設備と信号の接地及び I&C 系の満足いく運用に必要なその他の項目に関する推奨事項を提示している。

1.6. I&C 系、設備及びソフトウェアの設計と開発についての追加の手引きは、加盟国及び基準を策定している他の組織から入手できる。このような刊行物は、IAEA 安全基準として適切なレベルよりはるかに詳細を提示している。本安全指針は、詳細な産業界基準と併せて使われると想定されている。

目的

1.7. 本安全指針の目的は、I&C 全体構造について及び発電所の安全目標を満たすための原子力発電所の安全上重要な I&C 系についての手引きを提示することである。

1.8. 本安全指針は、発電所の機械、電気、原子力及び土木の工学的設計、発電所配置プロセス並びに安全解析からの、I&C の設計基準を定義するために、I&C 設計者にとって必要とされる入力情報を特定している。I&C 設計基準は、例えば、I&C によって達成されるべき機能要件、設備が動作することを要求される環境温度の極限値、I&C 設備が耐えることを要求される外部事象並びに自動停止を起こすことが要求される条件を提示することになる。

範囲

1.9. 本安全指針は、SSR-2/1 (Rev. 1)[1]の要件を満たすため、原子力発電所の安全上重要な I&C 系の設計、実装、性能保証及び文書化に関する手引きを提示する。本安全指針は、マネジメントシステム、試運転、設置、運転及び運転上の制限値と条件を対象とする安全指針など特定の他の安全指針の推奨事項を適用する際に関連する特定の I&C 系固有の問題も記述する。このような場合、本安全指針は、その他安全指針の関連する章を明示する。

1.10. 本手引きは、検出器から機械設備を起動、制御する装置まで全ての I&C 設備に適用する。この手引きには、例えば以下を対象とする。

---

[3] 脚注 1 を参照。

- 検出器
- 起動装置の制御装置
- 発電所設備の自動制御及び手動制御のための設備
- 運転員インターフェース

1.11. 本安全指針はまた、以下の I&C 設備を実装することに対する手段にも適用する。

- コンピュータシステム及び関連する通信連絡システム
- ソフトウェア
- ハードウェア記述言語を使用してプログラムされた装置（例えば、フィールドプログラマブルゲートアレイ）
- 限られた機能の産業用デジタル装置

1.12. 本安全指針は、冷却、潤滑及びエネルギー供給などの I&C 系の支援的な仕組みへの推奨事項を提示しない。電源供給に関する推奨事項は SSG-34[7]で提示される[4]。

1.13. 本安全指針は、人的因子及びコンピュータ・セキュリティの特定の側面が I&C と関係することから、それらを対象としているが、これらの領域についての包括的な手引きを提示していない。本安全指針の意図は、人的因子及びコンピュータ・セキュリティ活動との主要な取合いを特定すること、また、これらに影響する I&C 設計の仕組みについての推奨事項を与えることである。本指針において対象とされない人的因子及びコンピュータ・セキュリティの事例には、コンピュータ化された運転手順書及び情報技術セキュリティを含む。コンピュータ・セキュリティのより詳細な情報は参考文献[8]で提示されている。

1.14. 本指針は、新規の発電所のための I&C 系の設計、既設発電所の改造及び既設発電所の I&C の近代化に適用する。IAEA 安全基準シリーズ No.NS-G-2.3「原子力発電所の改造」[9] は発電所改造を取り扱っており、本安全指針の NS-G-2.3[9]との重複は最小限に抑えられている。

1.15. IAEA 安全用語集[6]は、安全上重要な I&C 系を、安全系の一部である I&C 系及びその機能不全又は故障が敷地の職員又は公衆の構成員の放射線被ばくに至る可能性がある I&C 系として定義している。本安全指針の第 5 章はさらに、用語「安全上重要な」及び安全分類に関係するその他の専門用語を説明している。本安全指針を適用することができる I&C 系の例は以下を含む。

- 原子炉保護系
- 原子炉制御系及び反応度制御系並びにそれらの監視系
- 原子炉冷却を監視及び制御するための系統
- 非常用電源供給を監視及び制御するための系統
- 格納容器隔離を監視及び制御するための系統
- 事故時監視のための計測装置

[4] 他の支援的な仕組みのための推奨事項を提示することになる補助系統の事項に関する安全指針草案は現在策定中である。

- 流出物の監視のための系統
- 燃料取扱いのための I&C 系

1.16. 本安全指針は、デジタルデータ通信とともに安全上重要な I&C 系で使用するためのコンピュータソフトウェアの開発についての推奨事項を提示する。本安全指針は、また、ハードウェア記述言語を使用して集積回路にプログラムされる I&C 機能に対して必要とされる対策を定義する。

1.17. 参考文献[10、11]は、本安全指針の基礎となる概念の概要を示しており、また、本指針で取り上げられる系統の例を挙げている。これら参考文献は、IAEA の手引きを提供するものではないが、一部の利用者のための有用な背景資料を提供する場合がある。

構成

1.18. 第 2 章は、GS-R-3[2]における要件の適用のための手引き並びに I&C 系の開発に特に関係している GS-G-3.1[3] 及び GS-G-3.5[4]の推奨事項を提示する。また、第 2 章はまた、I&C の開発のためのマネジメントシステムのプロセスを記述するためライフサイクルモデルの使用を示し、I&C 設計の共通プロセスについての手引きを提示し、また、特定の I&C 開発活動の実施についての手引きを提示する。

1.19. 第 3 章は、設計に必要な入力情報を特定し、また、I&C 系の設計基準に関する推奨事項を提示する。

1.20. 第 4 章は、発電所に関する I&C 全体の構造に関する手引きを提示する。

1.21. 第 5 章は、本安全指針の推奨事項を適用する機器等の安全上の重要性にしたがって当該推奨事項の適用を等級別けするために使用される安全分類体系を記述する。

1.22. 第 6 章は、安全上重要な I&C 系全てに適用可能な全般的な手引きを提示する。

1.23. 第 7 章は、原子炉保護系のような特定の系統、検出器などの特定の型式の設備並びにデジタルシステム及びハードウェア記述言語により設定された集積回路などに特有の推奨事項を提示する。第 2 章から第 6 章、第 8 章及び第 9 章の推奨事項は、第 7 章で検討された特定の系統にも適用する。

1.24. 第 8 章は、ヒューマンマシンインターフェースに関する推奨事項を提示する。第 8 章には、I&C に対する人的因子の原則の適用について、また、ヒューマンマシンインターフェースが持つべき特性についての手引きを含む。

1.25. 第 9 章は、コンピュータに基づいた安全上重要な I&C 系のためのソフトウェアの開発についての手引きを提示する。

1.26. 本安全指針は、独立した章の連続としてではなく、全体として適用されるべきである。例えば、第 9 章に提示されたソフトウェアについての手引きは、第 2 章で与えられたマネジメントシステム及びライフサイクルに関する手引きと併せて適用されることになる。

1.27. 添付資料は、本安全指針の主な事項に関してより詳細な手引きを提示する産業界規格のリスト、本安全指針が置き換わる 2 つの安全指針（NS-G-1.1[5]と NS-G-1.3[6]）に本安全指針を関連付ける情報及び加盟国によって実施方法が異なる分野の要約を含む。本安全指針に固有の定義に関するリストも提示される。

2. 計測制御設計のためのマネジメントシステム

全般

2.1. SSR-2/1 (Rev. 1)[1]の要件 6 は以下のように述べている。

「原子力発電所の設計は、必要な信頼性をもって安全機能を果たすことができること、発電所が設計寿命の全期間を通して運転上の制限値と条件内で安全に運転でき、安全に廃止措置ができること、また、環境への影響が最小にされることを確実なものとするために、発電所及び安全上重要な機器等が適切な特性を有するものであることを確実なものとしなければならない。」

2.2. SSR-2/1 (Rev. 1)[1]の要件 2 は以下のように述べている。

「設計組織は、発電所の設計に関して定められた全ての安全要件が設計プロセスの全ての局面で考慮され、実施されていること、また、これらの要件が最終設計で満たされていることを確実なものとするためのマネジメントシステムを確立し、実装しなければならない。」

2.3. GS-R-3[2]は、施設と活動のためのマネジメントシステムに関する要件を定めている。

2.4. GS-R-3[2]の 2.1 項は以下のように述べている。

「マネジメントシステムは、設定され、実装され、評価され、また継続的に改善されなければならない。これは組織の目標と協調していなければならず、また、これらの達成に寄与しなければならない。マネジメントシステムの主な狙いは、以下のことにより、安全を達成し、また、強化することでなければならない。

- 組織の管理に関する要件全てを首尾一貫した形で纏めること
- これらの要件が全て満たされているとの十分な確信を与えるために必要な、計画された体系的な活動を記述すること
- 安全に対して起こりうる悪影響を排除する手助けとするために、健康、環境、セキュリティ、品質及び経済上の要件が、安全要件とは別個に考慮されないことを

[5] 脚注 1 を参照
[6] 脚注 2 を参照

確実なものとすること。」

GS-R-3[2]の 4.2 項はさらに、「組織の情報及び知識は資源として管理されなければならない。」と述べている。

2.5. 安全を確保するために、安全上重要な I&C 系に関係する、設計基準に関する文書及び関連の情報又は記録は、I&C 系のライフサイクル全体を通して完全、明確、簡明、正確、整合しているように、適切な手順で管理されるべきである。マネジメントシステムは、設計基準文書及びそれに関連又は由来する情報又は記録が十分かつ適切であること、また、設計変更又は発電所の状態の変化を反映するために全期間で維持されることを確実なものとすべきである。これは、設計基準文書から導き出される場合がある文書及び情報並びにこのような系統の運転、保守又は改造に関係する手順書又はマニュアルのような安全に影響を及ぼす場合がある文書及び情報を含む。

2.6. マネジメントシステムは、安全要件を満たす I&C 系を開発するための資源（例えば、人材、設備、業務基盤及び作業環境）を特定し、割り当てるためのものも含めて、組織構成、組織文化、方針及び手順を含む。

2.7. I&C 系の開発活動に参画する各組織は、運転組織のマネジメントシステムの期待事項と整合したマネジメントシステムを持つべきである。

2.8. GS-G-3.1[3] 及び GS-G-3.5[4]は、施設及び活動並びに原子炉等施設に対する GS-R-3[2]で定められた要件の適用に関する手引きを提示する。

2.9. I&C 系の開発のためのマネジメントシステムは、GS-R-3[2]の要件を満たすべきであり、また、原子力発電所の全ての構築物、系統及び機器の開発に広く適用している GS-G-3.1[3] 及び GS-G-3.5[4]で提示された推奨事項に従っているべきである。I&C 系に必要とされる個々の開発プロセスを取り扱っている本安全指針は、これらの刊行物と併せて使用されるべきである。

I&C 系の開発に特に関係のある GS-R-3[2]の項目は次のとおりである。

- マネジメントシステム
- 安全文化
- 管理者の積極的関与
- 法令及び規制要件の遵守
- 組織の方針
- 計画立案
- 責任と権限
- 資源の準備
- 人的資源
- マネジメントシステムのプロセスの開発
- プロセス管理
- 文書、成果物（ツールを含む）及び記録の管理
- 購入
- 情報伝達
- 組織変更の管理
- 監視及び測定
- 自己評価
- 独立した評価
- 不適合並びに是正措置及び予防措置
- 改善

ライフサイクルモデルの使用

2.10. GS-R-3[2] の 5.1 項は以下のように述べている。

> 「目標を達成し、全ての要件を満たすために手段を与え、かつ組織の製品を提供するために必要とされるマネジメントシステムのプロセスが特定されなければならない、また、これらの開発は、計画され、実装され、評価され、継続的に改善されなければならない。」

2.11. 原子力発電所の近代的な I&C 系は、古い系統に一般的に適用されるもの以上に設計及び性能保証に様々な手法が必要である複雑な存在である。前の世代の I&C 系の機能上の特性及び性能は、たびたび、物理原則に基づくモデル及びこれらの妥当性を確認した試験によって特性付けられていた。

2.12. 近代的な I&C 系、特に、その機能性がソフトウェア又はハードウェア定義言語に依存しているデジタルシステムは、それらの挙動が論理により決定され、外部の物理法則により規定されないという点で、より古い系統とは基本的に異なっている。したがって、設計及び実装における小さな過誤が、デジタルシステムが予期されない挙動を示す原因となりうる。

2.13. デジタル I&C 系においては、最終製品がその目的に適合していることの実証は、設計要件の規律が取れた仕様と具体化を備える高品質な開発プロセスの使用に非常に強く依存するが、これだけではない。検証及び妥当性確認の活動は、最終的な製品が使用に適していることを保証するために必要である。しかし、全範囲の条件におけるデジタル I&C 系の正確な性能は、ハードウェアにのみ依存する系統に対して実施可能な同程度の試験及び物理学モデルの組み合わせから導くことはできない。したがって、近代的な系統の正確さの確信度は、純粋にハードウェアのみで実装されている系統の場合よりも開発プロセスの規律に、より強く由来する。

2.14. この状況に対応して、航空宇宙など他の安全に重きを置く領域と同様に、原子力発電の領域において、電子系統の開発に関する活動及びこれらの活動間の関係について説明する､一般にライフサイクルモデルとして代表される開発プロセスが適用されてきている。これらの一般に受け入れられている慣行は、I&C 系の開発のためのプロセスに関する広範囲な手引きを提示する原子力標準において正式なものとされている。通常、与えられた開発工程に関係する活動はライフサイクルの同じ段階にグループ分けされている。

2.15. 十分に文書化された開発プロセスは、独立した評価者及び規制機関が最終製品の目的適合性に確信を得ることができる証拠も産み出すことになる。

2.16. この章で提示されているライフサイクルプロセスに対する推奨事項は、第 9 章に記述されているライフサイクル活動にも適用する。この章におけるライフサイクルプロセスについての手引きは、GS-R-3[2]の要件並びに GS-G-3.1[3]及び GS-G-3.5[4]の推奨事項を、これらが I&C 系の開発に適用されているので、補足している。

2.17. I&C 系の開発を記述するために、ライフサイクルの 3 つの基本レベルが必要とされる。

(a) I&C 全体構造のライフサイクル
(b) 1 つ以上の個々の I&C 系のライフサイクル
(c) 1 つ以上の個別機器のライフサイクル。機器のライフサイクルは一般的にプラットフォームの開発の枠組みにおいて管理され、全体構造のレベル及び個別のシステム

レベルのライフサイクルとは独立である。デジタルシステムに関する機器のライフサイクルは通常、ハードウェアとソフトウェアの開発に関する個別のライフサイクルに分割される。

2.18. 時として、I&C 系の開発と関係しない他の活動が、I&C 系に対する要件及びその設計に対し重要な影響を持つことになる。人間工学及びコンピュータ・セキュリティはこのような活動の例である。このような活動は、I&C 系設計の支援より広範な目的を有しているが、I&C 開発に強い影響を持つことになる。さらに、設計段階において人的因子及びセキュリティ上の仕組みを考慮に入れることは、より容易でコスト効率もより良い。設計段階後は、変更は実施するのに非常に難しいか又は不可能であることも有り得る。

2.19. 図 1 に、I&C 開発ライフサイクル並びに人間工学及びコンピュータ・セキュリティプログラムから受け取られる主要な入力情報の例を示す。

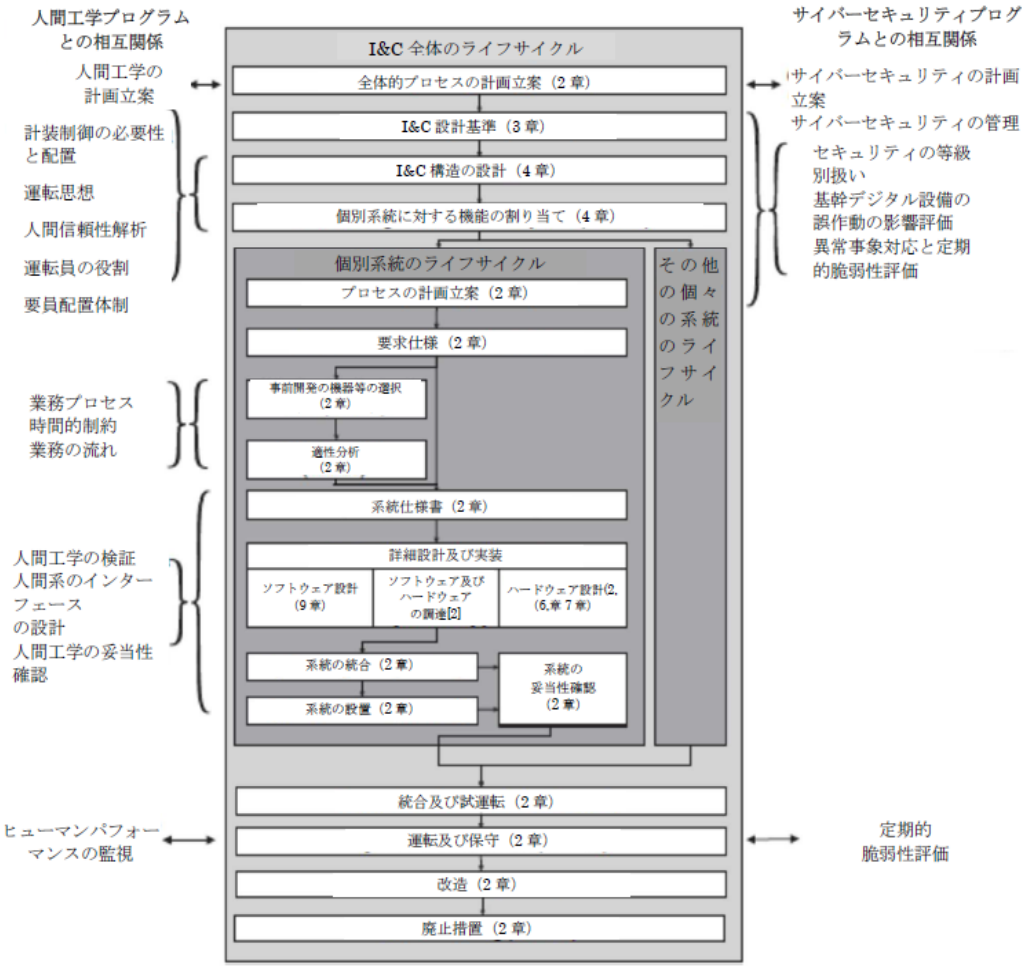

図 1. 典型的な I&C 開発ライフサイクル活動並びに人間工学及びコンピュータ・セキュリティプログラムとの取り合い

2.20. 図 2 に示されている「V モデル」は、開発ライフサイクル例の有用で別形式での表示である。このモデルは、要求仕様、設計、統合及び系統の妥当性確認並びに開発に関係する検証及び妥当性確認の活動との間の関係を図示している。図 2 は、デジタルとアナログの両方の系統に適用する。ソフトウェアがない場合はこの活動は当然不必要である。

2.21. ライフサイクル中のいかなる時点においても、得られた経験から、その前の段階で実施された作業を変更する必要性に行き着くことがある。その結果、これらの変更分が流れに入り、介入を受けた段階からの作業に影響することになる。単純化のため、図 1 及び図 2 はこのような反復経路を示していない。

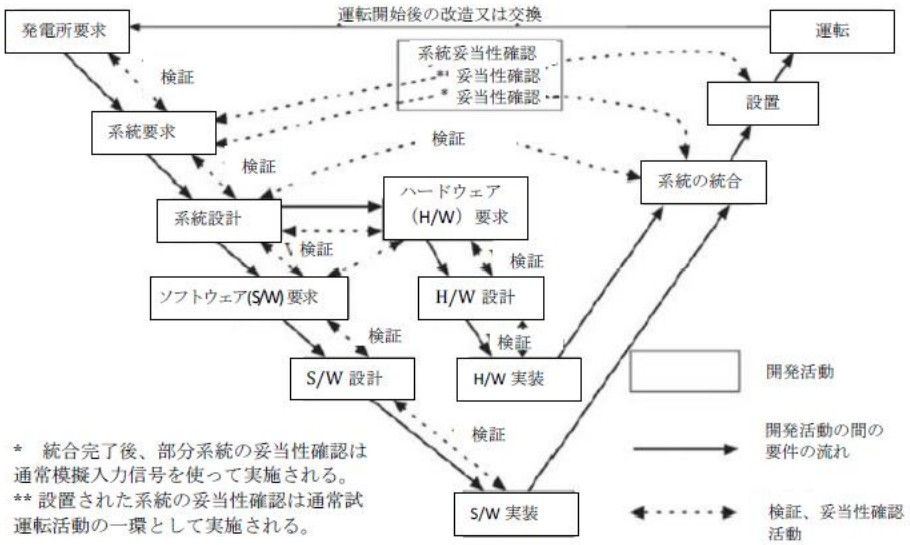

図 2. I&C 開発ライフサイクルプロセスと検証及び妥当性確認活動との間の典型的な関係。

2.22. I&C 全体構造、個々の I&C 系及び I&C 系の機器[7]の開発、実装及び運転に付随する全ての活動は、文書化された開発ライフサイクルの枠組みの中で実施されるべきである。

2.23. 各 I&C 系とその機器のライフサイクルは、その要件の導出から始まり、それらが発電所の安全のために要求されなくなる時に終わる期間を対象とするべきである。

プロセスの計画立案

2.24. あらゆる技術的な活動を開始する前に、その活動に必要な入力情報並びにその活動の成果物及びプロセス、並びに他の活動との関係を特定する計画が、マネジメントシステムに対する要件にしたがって作成され、承認されるべきである。

2.25. I&C 系の開発のための計画は、I&C に固有の事項及び I&C の開発が特別な処理を必要とする場合がある事項を取り扱う。一般的に、I&C の開発に固有の計画は、以下に与えられる事項を取り扱うために作成されることになる。

- ライフサイクルモデル
- 構成管理
- 不適合の特定、管理及び解決
- ハザード分析
- 検証及び妥当性確認
- 確率論的安全評価からの洞察の使用
- I&C 系に固有の安全解析
- 要求工学
- 構造の設計

[7] I&C 機器は、ハードウェア、応用ソフトウェアとファームウェアなどのソフトウェア及びハードウェア記述言語を含む。

- 事前開発機器の選択及び受け入れ
- 設計
- 実装（例えば、ハードウェアの製造及びソフトウェアのコード作成又はハードウェア記述言語を使用するコード作成と合成）
- 統合
- 系統の妥当性確認
- 設置
- 試運転
- 設備の性能保証
- ツールの性能保証と使用
- 保守性
- 旧式化の緩和
- 運転
- 訓練
- ソフトウェアの保守

2.26. これらの項目の幾つかのための計画は、一つの計画に纏められる場合がある。

2.27. I&C 系の開発は、以下のような I&C 開発に固有でない活動の計画にも依存する。

- 品質保証
- 安全上重要な機器等の分類
- 購買
- 製造
- 文書の作成と維持

2.28. 全ての I&C 開発活動は、適用可能な承認された計画にしたがって実施されるべきである。

人間工学活動及びコンピュータ・セキュリティ活動との協調

2.29. 人間工学及びコンピュータ・セキュリティに関係するライフサイクルにわたるモデルは、本安全指針に含まれないが、このようなプロセスは I&C 開発に要求される情報を提供する。図 1 は、これらのプロセス間の関係と取合いを図示している。これらは以下のことを含む。すなわち、人間工学に固有の要件を作成する活動、人間工学に関係する検証及び妥当性確認活動の成果、技術的なセキュリティ対策及びコンピュータ・セキュリティ要件である。

2.30. I&C 系の開発は、人間工学活動及びコンピュータ・セキュリティ活動と調和しているべきである。

2.31. I&C 系の開発において、人間工学プログラムから生じる要件は、以下のことを含めて考慮に入れられるべきである。

- 運転要員の役割と責任及びその他の要員配置要件の仕様
- ヒューマンマシンインターフェースについての構築物、系統及び機器の安全分類
- 事故状態及び事故後の状態に対処するために要求される一群の指示装置及び制御装置を定義することに関する考慮事項を含めた、情報の必要性の仕様
- 制御の必要性、自動及び手動による制御機能及び適切な場所への制御装置の配置についての仕様
- 業務プロセス、時間的制約及び運転員の手順並びに分析（すなわち、業務分析；8.78 項を参照）により特定される情報に関係する要件

- 状況に基づく告知に関する方針。状況に基づく告知は、例えば、起動時と過渡時にメッセージが「溢れる」ことを回避する。
- I&C 系の欠陥の報告に対する要件
- I&C 系の保守性を支援する方策
- 安全解析（すなわち、人間信頼性解析）における人的過誤の可能性を考慮することがもたらす洞察

2.32. 人間工学に関係する検証及び妥当性確認の活動は、以下であるべきである。

- 人間工学及びヒューマンマシンインターフェース設計の分析時に特定された欠陥に関係する推奨事項の解決策を検証すべきである、
- I&C 系が人間工学に関係する適用可能な設計手引きに適合していることを検証すべきである、
- 設計が I&C 系、他の設備及び運転員に対して、指定された業務を実施する際に運転員を支援するために適切な支援を提供していることを検証すべきである、
- 人的因子の設計が、信頼できる運転要員行動のために十分な時間を許容することを含めて、通報意図に対して、適切な運転員の応答を引き出していることを検証すべきである、
- I&C 系のいくつかの部分が、例えば保守又は試験実施の目的のためのような認められた理由により供用から外れているときを含めて、系統が機能すると予定されている全ての状態において、運転要員が I&C 系を用いて自身の機能を実行できることを、性能に基づく尺度を用いて、確認すべきである。

2.33. 人間工学についての要件の作成並びに人間工学の活動の検証及び妥当性確認は、通常、人間工学プログラムの一部として実施される。人間工学プログラムは、I&C ライフサイクルプロセスとの取合いを除き、本安全指針でこれ以上に詳細に記述されていない。

2.34. 発電所の I&C 全体は、コンピュータ・セキュリティ計画により割り付けられたセキュリティ対策を実装すべきである。

2.35. コンピュータ・セキュリティ計画は、I&C 全体構造及び個々の I&C 系を考慮に入れて必要に応じて更新されるべきである。

2.36. I&C の開発は、安全及び核セキュリティに関する責任者間の対話により、又は技術、手順及び管理に関するコンピュータ・セキュリティ計画の要件を満たす開発環境において、安全及び核セキュリティの担当者の合同チームにより実施されるべきである。

2.37. 原子力施設のコンピュータ・セキュリティの実装についての追加情報は、参考文献[8]に提示されている。

全てのライフサイクル期間に共通な活動

構成管理

2.38. GS-R-3[2] の 5.12 項、5.13 項、5.18 項及び 5.19 項は以下のように述べている。

「5.12. 文書を管理しなければならない。文書の利用者が、適切で、正しい文書を承知しており、これを使用していることが確実なものとされなければならない。」

「5.13. 文書への変更は、審議しなければならず、記録しなければならず、文書自体と同じレベルの承認を受けなければならない。」

「5.18. 管理は、製品が要求される検証活動をバイパスしていないことを確保するために使用しなければならない。」

「5.19. 製品は、これらの適切な使用を確保するために特定されなければならない。追跡可能性が要件である場合、組織は、製品の固有の識別を管理し、記録しなければならない。」

2.39. GS-R-3[2]において、これらの項目は、文書の管理、製品の管理及び記録の管理の表題の下に記述されている。工学的な活動については、文書及び製品の管理は、より一般的には構成管理の表題の下に分別される。一部の記録は構成管理の体制とは別個に管理される場合があるが（例えば、別個の記録管理体制により）、記録の管理に対する GS-R-3[2]の要件は、構成管理の下の文書にも適用される。GS-G-3.1[3]及び GS-G-3.5[4]は、2.38 項に示された 4 つの項目についての追加の推奨事項を提供している。

2.40. I&C 系のライフサイクルにわたる構成管理の目的は以下を含む。

- 構成管理が要求される全ての機器等の特定、すなわち、文書、I&C 製品及び付随する記録の特定
- 構成機器の確実な保管及び検索に対する方策
- 構成管理の下にある機器等の間の依存性及び関係の特定
- 構成管理の下にある機器等の全ての変更の特定
- 構成管理の下にある機器等の不注意及び無許可での改造の防止
- 設計基準に継続的に適合していることを確保すること
- 構成に関するベースラインの仕様、すなわち、構成管理の下での構成の全ての階層的レベルにおいて、ある個別機器に関する相互に両立性があり、整合性がある機器の構成の仕様[8]
- 実際の発電所と技術文書との間の整合性を確保すること
- 構成管理の下にある機器等の現在の状況の仕様（例えば、それらの審査若しくは承認又は妥当性確認の状況）

2.41. 構成管理は、変更の影響を分析すること、変更を承認すること、型版が正確に組み合わされていることを保証すること、使用のための設計文書及びソフトウェアを発行すること並びに年代順の記録を確立し及び維持することに対する技法及び手順を含むべきである（例えば、設計における特定の時点でツールのどの型版が使われることになるのか）。

2.42. 全ての I&C 機器等及びそれらに付随する文書は、指定され、固有の識別子を与えられ、また、構成管理の下に置かれるべきである。

2.43. I&C 機器等は、配備された I&C 系、その系統を補助する又はその系統が意図されたとおりに動作するために必要な、個別に設置されたあらゆる機器等、これらの機器等全てを規定する文書及びファイル並びにそれらの品質に影響を及ぼすことがあるソフトウェアツールを含む。

2.44. I&C 機器等には、通常、例えば、以下のものを含む。

- 調達された機器等、再使用された機器等及び新たに開発された機器等
- ソースコード及び演算コードなどのソフトウェア構成要素、ハードウェア記述言語、フィールドプログラマブルゲートアレイ形式の構成データ（「ビットストリーム」と

[8] 構成のベースラインが確立されている機器等には、個々の機器、系統又は I&C 系全体を含む場合がある。あらゆる個別機器のベースラインは、その個別機器から成る系統及び機器の全てを網羅することになる。

して知られている）並びに応用ソフトウェア、オペレーティングシステム及び支援ソフトウェアを含む、発電所設備に組み込まれたソフトウェア
- ハードウェア構成要素及び当該構成要素の交換可能な要素
- ファームウェア
- 仕様書、設計文書、製造用の図面及び指示書、据付用の図面及び指示書、ソフトウェア並びにハードウェア記述言語などの開発文書
- 設備の構成データ及び構成ファイル（例えば、安全運転制限値、警告又は警報の制限値、設定点及び較正定数）
- I&C 機器等を製造、管理、構成、検証又は健全性確認するために使用される実務ツール及びソフトウェアツール。このようなツールを採用したときに使用されるパラメータ設定値を含む。

2.45. 構成管理データは、I&C 機器等が正確に組み立てられ、物理的及び位相空間的に正確な場所に設置されていること並びに意図された型版のソフトウェアが正確に組み込まれていることを検証するために使用されるべきである。

2.46. GS-R-3[2]の 5.21 項は「記録は、プロセス文書において指定されなければならず、また、管理されていなければならない、全ての記録は、判読可能であり、完結しており、特定可能であり容易に検索可能でなければならない。」と述べている。

2.47. ライフサイクルプロセス記録は、構成管理の下に置かれるべきである。

2.48. ライフサイクル記録の構成管理プログラムは、I&C 製品に使用されるものとは異なる場合がある。

2.49. 構成管理の下に置かれるライフサイクル記録は、系統の安全解析がそれに依存しているか又は運転時若しくは保守時に安全に影響を及ぼす可能性がある、いかなる情報も含む。例えば以下である。

- ライフサイクル活動の計画及び手順書
- 安全実証計画
- 解析文書
- 安全の実証及びその裏付け証拠を文書化した加工物又は記録であって、例えば、保証、検証（解析及び試験実施を含む）、妥当性確認（要件の妥当性確認を含む）、プロセスの評価及び監査、確実性、健全性並びに追跡可能性に関する人工物又は記録
- 検証及び妥当性確認の活動の記録
- 試験仕様書、手順書、計画及び結果
- 安全系の制限値設定及び安全系の制限値設定を確立することに関する方法論
- システムの統合に関係する手順、計画及び結果
- プロセスの審査及び監査に関係する文書
- 要件の追跡可能性を提供する配列
- 保守及び運転の手順書
- 設備及び予備品のための購入仕様書の技術的側面
- 性能保証記録
- I&C 系及び機器の文書化（2.90 項を参照）

2.50. 構成管理の下にある機器等の特定は、改訂番号を含んでいるべきである。

2.51. 構成管理は、I&C 系の最初の開発、開発時になされた変更及びこれらが供用に付された後の改造に適用されるべきである。

2.52. 構成管理プロセスは、構成管理の下にある各個別機器に対する関連情報を維持すべきである。

2.53. 記録されることがある情報は以下のものを含む。すなわち、いつその機器が完成していると最初にみなされたか、適切な場合には様々な報告書を含めて様々な型版にどのような変更が組み入れられたか、構成管理の下にある他の機器等に対する依存性、その機器の現在の承認状況並びにそれを作成、審査及び承認することに関する責任者を含む。

2.54. I&C 設備に組み込まれたソフトウェアの属性及び構成データの値は、I&C 設備自体から取り出せるべきである。

2.55. 設置された機器等の属性及び構成データの値を取り出すことができることは、装置が適切に構成されていることの検証を支援することになる。自動点検の仕組み又はソフトウェアツールの組み込みはこの検証を支援する場合がある。

計測制御系に関するハザード分析

2.56. I&C 全体構造に関して、ハザード分析は、深層防護又は発電所設計の多様性の方針を損ねることがある条件を特定するために実施されるべきである。

2.57. 各安全系に関して、ハザード分析は、系統の安全機能の性能を劣化させることがある条件を特定するために実施されるべきである。

2.58. 考慮されるべきハザードは、内的ハザード及び外的ハザード、発電所設備の故障及び I&C の故障又はハードウェアの故障若しくはソフトウェアのエラーによる偽動作を含む。望まれない相互作用による外因性ハザードも考慮されるべきである。

2.59. I&C 系に対するハザード分析は、異なる運転モード間の移行を含め、全ての発電所の状態及び運転モードを考慮すべきである。また、劣化状態も含まれるべきである。

2.60. I&C 系全体に関する設計基準が完成する前に、I&C 系のハザード分析の最初の結果が利用可能であるべきである。

2.61. ハザード分析は、I&C 全体構造の設計並びに安全系に対する要件の指定及び安全系の設計、実装、設置及び改造を含め（しかし、これに限定されない)、開発ライフサイクルにわたる全ての期間で更新されるべきである。

2.62. ハザード分析を更新する意図は、I&C 安全系の特殊な特性、I&C 安全系と発電所との間の相互作用、及びそれらの安全分類に関係なく I&C 安全系とその他の I&C 系との相互作用によって引き起こされる場合があるハザードを特定することである。

2.63. 系統機能の性能を劣化させる可能性があると特定されたハザードの影響を除去、回避又は緩和するための対策が講じられるべきである。

2.64. ハザードの影響を除去、回避又は緩和するための対策は、例えば、I&C 系の要件、設計若しくは実装に対する変更又は発電所設計に対する変更の形を取ることがある。

2.65. ハザード分析のために選ばれた方法は、分析される個別機器にとって適切であるべきである。

検証及び妥当性確認

2.66. I&C 系のライフサイクルの各段階は、前の段階に開発された情報を使用し、その後の段階の入力として使用される結果を提供する。

2.67. ライフサイクルの各段階の結果は、前の段階に設定された要求事項に対して検証されるべきである。

2.68. 要件の追跡可能性の配列は、要求事項がライフサイクルの各段階において申し分なく満たされていることか又は要求事項が満足いくほど満たされていないところには適切な行動が取られたことの確認を文書化するために使用できる。

2.69. I&C 全体、各 I&C 系及び各 I&C 機器は、全ての要件（機能要件及び非機能的要件の両方）が満たされていることを確認するために、かつ、何らかの望ましくない挙動が存在しているかどうかを判断するために検証されるべきである(2.128 項～2.142 項を参照)。I&C 全体、各 I&C 系及び各 I&C 機器を定義している要件は、それらが意図されたとおりに果たされていることを確認するために妥当性確認されるべきである。

2.70. 検証及び妥当性確認は、設計者及び開発者から独立した個人、チーム又は組織的なグループにより行われるべきである。

2.71. 検証及び妥当性確認の独立性の確立は通常、検証及び妥当性確認を行うチーム、個人又は組織的なグループが以下であることを保証することを含む。

- 適切な技術的な力量と知識を有していること
- 彼ら自身の範囲を設定できること
- 開発者からの圧力にさらされないこと
- 審査の全範囲を完了することを妨げるおそれのある予算の削減又はスケジュール面での制約事項にさらされないこと
- 開発グループからの反対圧力なく管理者に指摘事項を提出することが許されていること

2.72. 検証及び妥当性確認の独立性の範囲及び種類は、関係する系統又は機器の安全クラスに対して適したものであるべきである。検証及び妥当性確認は、独立の様々なレベルにおいて並行して起こる場合がある（例えば、元来の開発組織の開発者から独立した試験者により行われる検証及び妥当性確認、また、別の組織により行われる追加の独立した検証及び妥当性確認)。

2.73. 検証及び妥当性確認の活動は、検知された逸脱及びこれらの解決の記録を含めて文書化されるべきである。検証及び妥当性確認の段階で逸脱が検知された場合、結果として生じる設計変更及びこれらの実装は、前に実施されたものと同じ検証及び妥当性確認のプロセスに付されるべきである。

2.74. 検証及び妥当性確認チーム、系統統合チーム、試運転チーム並びに系統設計者及び開発者の間の技術的な情報伝達は文書化されるべきである。

確率論的安全解析からの洞察の使用

2.75. SSR-2/1 (Rev. 1)[1]の 5.76 項は以下のように述べている。

> 「設計は、停止を含めて、全ての運転モード及び全ての発電所状態に対する発電所の確率論的安全解析を、特に以下のことを参照して十分に考慮しなければならない。
>
> (a) ある特定の仕組み又は想定起因事象が全体のリスクに対して不釣り合いに大きい寄与をすることがないようにするか又は全体のリスクに大きな不確かさの寄与を生じたりすることがないように、また、実行可能な範囲で深層防護の各階層が独立しているように、均衡の取れた設計がなされていることを確立すること
> (b) 発電所パラメータの僅かな変動が発電所の状態に大きな変化を引き起こしうる

状況（クリフエッジ効果）が防止される保証を提示すること
(c) 解析の結果とリスクの容認基準が特定されている場合はそれとを比較すること」

2.76. 確率論的安全評価から得られた洞察は、I&C 系の設計において考慮されるべきである。

2.77. 設計時の確率論的安全評価及び確率論的安全評価からの結果の使用に関する詳細情報は、関連する IAEA 安全基準[12、13]で見ることができる。

安全評価

2.78. I&C の安全評価は、GSR Part 4 (Rev. 1)[5]の要件並びに IAEA 安全基準シリーズ No. SSG-3「原子力発電所に関するレベル 1 確率論的安全評価の開発と適用」[12]及び No. SSG-2「原子力発電所に関する決定論的安全解析」[14]の推奨事項にしたがって実施されるべきである。

2.79. 設計解析並びに検証及び妥当性確認は、I&C 全体構造及び個々の I&C 系についての全ての設計基準要件が満たされていることを確認するために実施されるべきである。

2.80. 3.14 項は I&C 全体構造及び全ての I&C 系に対して設計基準要件において考慮されるべき事項を推奨している。3.15 項は安全系に対して設計基準要件において考慮されるべき追加の事項を推奨している。

2.81. 典型的な設計解析、検証及び妥当性確認の技法は以下を含む。

- 追跡可能性解析。追跡可能性解析は、一般的に、要件の具体化及び妥当性を確認するために使用される。
- 故障モード影響解析。故障モード影響解析は多くの場合、単一故障基準の遵守を確認するため及び全ての既知の故障モードが計画された試験により自ずと明らかになるか又は検知可能であることを確認するために使用される。
- 深層防護及び多様性の解析。深層防護及び多様性の解析は、共通原因故障に対する安全系の脆弱性を調査する手段の 1 つである（このことに関する追加情報を提示する参考文献[11]を参照）。
- 信頼性解析。信頼性解析は、系統又は機器の信頼性を予測するために統計的方法を使用する。一般に用いられる信頼性解析の技法は、部品点数法、部品ストレス解析法、寿命データ解析（例えば、ワイブル解析）、信頼性ブロック図及びフォールトツリー解析を含む。
- 妥当性確認。妥当性確認の試験は、決定論的な技法を含み、また、統計的手法を含む場合がある。
- セキュリティ試験。セキュリティ試験は、通常、脆弱性評価からの入力を必要とし、セキュリティにおける良好事例の使用を確認するために使用される。
- 機器等が信頼性対応設計されていることを確認するための分析。このような分析は、設計が、多重性、単一故障基準の遵守、試験可能性、フェールセーフ設計及び厳格な性能保証などの高い信頼性を促進するために知られている仕組みを組み込んでいることを確認するために使用される。[9]
- I&C 系の様々な運転モードに関する機能要件の確認。これは、停電、リスタート又

[9] I&C 系では、定性的解析、定量的解析及び試験の組み合わせが信頼性要件の遵守を検証するために通常必要とされる。

は再起動、その他の移行時期の期間中とその後の系統の正しい挙動の分析を含む。暦時間の変更（例えば、夏時間と閏年）はその他の移行時期の例である。

2.82. 解析において使用される各々の仮定は明記されるべきであり、また、仮定の使用は正当化されるべきである。

2.83. 実施されたあらゆる解析の方法論は、解析への入力情報、解析からの結果及び解析自体と共に徹底的に定義され、文書化されるべきである。

2.84. 最高の品質基準に従って仕様指定され、また、設計されている個々の系統に対する現在の最新技術を前提に、仕様、設計、製造、設置、運転環境及び保守実務に伴う全ての潜在的な故障原因（サイバーセキュリティに関連する故障原因を除く。）が考慮に入れられたとき、10^{-4}～10^{-5} のオーダーの故障／作動要求の値は、確率論的安全解析において要求される場合がある、信頼性に載せる全体の適切な制限値である場合がある。この値は、系統の多重性を有するチャンネルにおける共通モード故障のリスクを含める必要がある場合があり、検出器から出力の処理を経て起動される設備までの系統全体に適用される。これより高い信頼性の要求は排除されないが、取り上げられた全ての要因を考慮に入れた特別な正当化を必要とすることになる。

2.85. I&C 系に対するあらゆる信頼性要求は実体化されるべきであり、正当な制限値内にあるべきである（添付資料 III は一部の加盟国において容認された制限値を示している）。

2.86. 設計及び実装のプロセスの期間において、各 I&C 系の発電所との相互関係は、発電所の安全要件及び SSR-2/1 (Rev. 1)[1]の要件に対して定常的に審査されるべきである。

2.87. これらの要件とのいかなる矛盾でも見出された場合には、設計及び実装は適切に是正されるべきである。

文書

2.88. I&C 系の文書は以下であるべきである。

- 設計プロセスの様々な段階の間での及び設計プロセスに含まれる様々な関係者の間での、情報伝達の手段を提供するべきである。
- 全ての要件が、設置された系統において正確に解釈され、履行されていることを示す記録を提示すべきである。
- 発電所運転要員に運転上必須の情報及び安全設計関連情報を伝達すべきである。
- 発電所及び I&C 系の保守並びに将来的な設計の改訂の可能性に関する根拠を提供すべきである。
- I&C のライフサイクル期間を通じて追跡可能であるべきである
- 構成管理体系の下で管理されるべきである。
- 対象の読者（例えば、分野の専門家、安全技術者及びソフトウェア設計者）にとって曖昧さがなく、完全で、整合的で、十分に構築され、読み易く、理解し易くものであるべきであり、また、検証可能で維持可能であるべきである。

2.89. 適切な文書は、発電所及び技術支援の職員の訓練と共に、系統の運転、サーベイランス、不具合処理、保守、将来の改造又は近代化を促進することになる。

2.90. 運転組織は、少なくとも以下の事項を対象とする I&C の系統及び機器に関する文書を作成するか、又は提供されるべきである。

- 設計要件
- 機能及び機能設計

- 運転の原則
- 全体的な発電所構想における系統の役割
- 安全上重要な仕組みの特定を含む設計の仕組み
- 竣工時の設計及び構成文書
- 検出器及び起動装置を含む、系統及び主要機器の竣工時の配置
- 他の発電所の系統との取合い及び依存性
- サーベイランス、試験、診断、保守及び運転に関する施設と要件
- 試験手順書及び結果
- 設備の性能保証
- 設計及び開発プロセス並びに設計で従うことになる品質要件
- 試運転を含め、試験の全ての段階に関する方針
- 検証及び妥当性確認の方法の設計及び開発並びに結果
- 全ての通常運転の状態及びモードに対する運転手順書
- 想定事故シナリオ及び設計拡張状態を対象とする非常時運転手順書及び重大事故の手引き
- 予備品及び機器の準備のための推奨事項並びに購買仕様書
- セキュリティ設計の仕組み及びそれらの適用[10]

2.91. 入手及び供給、設計、製造活動、ソフトウェアコード並びに検証及び妥当性確認のためのプロセス及び要件に関する文書は、運転組織、規制機関又はこれらの組織の代理を務める独立した第三者による評価のために利用可能であるべきである（9.100 項～9.103 項を参照のこと）。

ライフサイクル活動

要件の仕様

2.92. I&C 全体、個々の I&C 系及び I&C 機器についての要件は、適切な形式で文書化されるべきである。

2.93. 個々の I&C 系のすべてについての要件の組み合わせは、I&C 系全体に対して定められた設計基準を果たすべきである。

2.94. I&C 系全体及び個々の I&C 系についての要件は、I&C 設計基準から導出されるべきである。

2.95. 第 3 章では I&C 全体の設計基準の導出及び内容を議論する。

2.96. 系統及び機器の要件は、適用できる場合は、以下を指定すべきである。

- 個々の I&C 系又は機器が行うべきこと
- 各発電所状態及び各発電所運転モードにおける各機能の入出力情報間の関係
- 測定、制御機能及び表示装置についての最小精度及び正確さ並びに最大応答時間
- 系統の取合い（例えば、系統と運転員との間及び他の系統との間）

[10] 設計が、運転組織の運転上のセキュリティ方針と慣行（コンピュータ・セキュリティに関係する方針と慣行を含む）に関する仮定を利用しているのであれば、これらは使用者に情報伝達されるべきである。それらの配布がその他の系統の情報よりも更に限定できるように、そのような説明の要素を別の文書に含むことが適切であることがある。

- 要求される時間的な性能（欠陥検出時間及び復旧時間を含め）を含む自己観察の仕組み
- 自己観察の手段による欠陥の検出があったときの I&C 系によって講じられる措置
- セキュリティ上の仕組み（有効性点検、固有のコンピュータ・セキュリティ管理及び系統がその環境下でセキュリティ管理を引き継ぎ、また、立ち入る権利を引き継ぐことを許容する仕組み）
- 達成されるべき信頼性及び稼働性の程度並びにこれが達成されることを確保するために必要なあらゆる支援要件[11]
- 保守のために要求される施設及び仕組み
- 設計制約事項[12]
- 特別の故障モードに対する安全応答
- 発電所の通常状態及び事故状態並びに予測可能な内的ハザード及び外的ハザードに付随する運転環境の全範囲に対する頑強性

2.97. 設計制約事項が必要な箇所では、制約事項が指定され、正当化され、また、追跡可能であるべきである。

2.98. デジタルシステムに対するセキュリティ設計要件は、セキュリティリスク評価の結果を考慮に入れるべきであり、また、運転組織のセキュリティ方針の特性と整合しているべきである。

2.99. ライフサイクルを通じて要件を管理するため、また、全ての要件が履行され、検証され、妥当性確認され及び実装されていることを確実なものとするために、特定のプロセスが使用されるべきである。

2.100. 要求工学は、I&C 系の安全目標が設計によって取り組まれることを確保する特定のプロセスである。

2.101. 要件は、系統の安全上の重要性に相応した技法の事前に決められた組み合わせを使用して、設定され、文書化されるべきである。

2.102. 要件を設定し文書化する技法は、明確に定義された構文と語義を有する仕様言語、モデル、分析並びに審議の使用を含む。

2.103. 可能な限り、要件は、どのように設計され実装されるべきかという観点よりは、何が達成される必要があるかという観点で書かれるべきである。

2.104. 要件は全ての関係者（例えば、許可取得者、供給者及び設計者）が理解し得る用語で記述されるべきである。

2.105. 要件についての文書は、要件が対象とする読者に要件が十分に理解されることを確保するため必要な範囲で、例えば、特定の要件に関する背景情報、リスク考慮事項、機能又は安全の仕組みの設計に対する推奨事項といった追加情報を参照し、含み、又はそれらによって補足されるべきである。

2.106. 安全に対し潜在的な影響を有している要件は、その旨特定されるべきである。

2.107. 全ての要件の起源及びこれらに関する論理的根拠は、検証、妥当性確認、より高位

---

[11] 信頼性と稼働性の程度は、例えば、上記で参照された補助的要件、すなわち、特定の信頼性方針の実現のための要件、開発プロセスの特性に関する要件又は指定された標準の遵守に関する要件のような補助的な要件の観点で定量的又は定性的に定義されることがある。

[12] 設計制約事項の例は、独立性又は多様性の要件を裏付けるための制約事項を含む。

文書への追跡可能性及び全ての関連する設計基準要件が考慮に入れられた実証を容易にするように、明示されるべきである。

事前開発機器の選択

2.108. 事前開発機器は、6.78 項～6.134 項で与えられた手引きにしたがって、適切に性能保証されるべきである。

2.109. 事前開発機器は、ハードウェア装置、事前開発ソフトウェア、商用の既製品装置、ハードウェア及びソフトウェアの両方から構成されるデジタル装置、ハードウェア定義言語で構成されたハードウェア装置又はハードウェア記述言語において使用可能な事前開発の機能的ブロックを含む。

2.110. 参考文献[11]は、商用の既製品装置の使用に関してより詳細を提供している。

2.111. I&C 安全系を実装する際に使用されない事前開発機器のいかなる機能も、系統の安全機能に対して容認できない干渉をしないことが示されるべきである。

2.112. 実現可能な場合、事前開発機器は、使用されない機能が使えないように構成されるべきである。

2.113. 多くの場合、選択された事前開発機器は、商用の既製品装置である。商用の既製品装置の使用は、コスト及び設計業務を軽減することがある。さらに、原子力発電所用に特化して利用可能な装置がない場合があり、また、十分に実証された商用製品の使用は、新しい機器の開発より効果的又はより安全である可能性がある。

2.114. 商用の既製品装置は、より複雑である傾向があり、意図しない機能を持っている場合があり、また、多くの場合、短期間で旧式になる場合がある。これらは、しばしば、原子力発電所での適用には不必要な機能を有している。商用の開発プロセスが本安全指針に記述されているものよりも透明性がなく、また管理されていない場合があるので、商用の既製品装置の性能保証はより困難となる可能性がある。性能保証は、多くの場合供給業者の協力なしでは不可能である。商用の既製品装置の受け入れに付随する困難さは、多くの場合、品質と信頼性を実証するための情報が利用できないところにある場合がある。

2.115. 商用の既製品装置を使用するか否かを判断するプロセスにおいて、許可取得者は発電所のライフサイクル中の、それらの性能保証の維持を検討すべきである。

2.116. 例えば、構成部品の変更、新しい型版のファームウェア、新しい製造プロセス又は新しい型版のソフトウェアのような、生産ラインの頻繁な設計変更があることがある。これは、特に I&C の保守及び予備品管理に関して、このような変更を適切に特定する際の発電所の構成管理とともに供給業者に困難な問題を課する場合がある。ある場合には、運転組織は、特定の機器又は型版が購入できなくなる可能性を回避するために、特定の型版の予備品の「ライフサイクル中の供給」を約束している。

2.117. 事前開発機器は、I&C 系におけるこれらの使用の必要な情報を与える文書を有しているべきである。

計測制御系の設計及び実装

2.118. I&C 全体構造及び個々の I&C 系の設計は、要求される機能にその他の要件を加えた、体系的で段階的な分解からもたらされるべきである。

2.119. I&C 系によって満たされるべき系統要件は、ハードウェア、ハードウェア記述言語で構成される装置及び（存在する場合）ソフトウェアの適切な組み合わせに割り当てられるべきである。

2.120. ハードウェアは、特定の適用対象に固有の集積回路を含むことがある。ソフトウェアは、オペレーティングシステム、開発予定のソフトウェア、事前開発ソフトウェアから作成されるソフトウェア、などの既存のソフトウェア及びファームウェアを含むことがある。また、精緻化された要求事項は、例えば、起動される装置の型式と性能など I&C 系の外部部品に関してなされた下位レベルの設計上の決定を考慮に入れなければならないことがある。

2.121. 安全上重要でない要件の具体化には、安全上重要な機能に干渉しないことが示されるべきである。

2.122. 各 I&C 系の内部論理が検証及び妥当性確認に耐えられることを保証するために、設計規則が定められるべきである。

2.123. 設計は、運転中に構成可能であること又は検証及び妥当性確認されることを必要とする I&C パラメータを考慮に入れるべきであり、また、そのようにするための手段（例えば、原子炉保護系のトリップ設定、較正定数及びソフトウェアの構成設定）を備えるべきである。

システムの統合

2.124. システムの統合は、以下であるべきである。

- ハードウェアとソフトウェアとの間又はソフトウェアモジュール間など、統合される構成要素間の全ての取合いに対処すべきである
- 系統の様々な構成要素間の取合いに対する要求事項が満たされていることを確認すべきである
- 範囲外の値、例外の取扱い及び時間合わせを含む要求事項を含め、系統が規定された要求事項を満たすことを可能とするため、統合された系統において構成要素、下位組立て品及び下位系統が設計されたとおりに動作することを確認すべきである

2.125. 検証済みのモジュール（ハードウェア及びソフトウェア）の整合性を持った構成が、システム統合の開始前に可能になっているべきである。

2.126. ソフトウェアツールは、通常、系統の構成要素への組込みのためのモジュールの問題を管理するため及び系統の妥当性確認に使用される既成ソフトウェアを管理するために使用される。また、ソフトウェアツールは、構成管理及び組み込まれた構成要素と健全性確認された構成要素との間の追跡可能性を容易にするために、運転中に所内で使用される。

2.127. 文書化された追跡可能性解析は、システム統合が系統設計仕様に関して完全であること及び 2.124 項の目的が満たされていることを実証するために使われるべきである。

系統の妥当性確認

2.128. 系統の妥当性確認は、個々の I&C 系に対して及び統合された一連の I&C 系に関して実施されるべきである。

2.129. 本安全指針の目的に関して、系統の妥当性確認は、発電所への系統の設置が完了した時点で終了する。系統が発電所に設置された後に系統の妥当性確認のうちのいくつかの

追加要素が実施される必要があれば、これらは試運転時の試験に含まれる場合があるが、それは、その結果が健全性試験の記録に含まれていること、また、2.71 項及び 2.72 項に定義されているとおり、独立性が設計チームと妥当性確認チームとの間で維持されていることを前提とする。

2.130. 妥当性確認の目的のために試験に付される系統は、敷地における I&C 系の最終構成配置を代表するものであるべきである。

2.131. 系統の妥当性確認に付されるソフトウェアは、運転中に使用されることになるソフトウェアと同一であるべきである。

2.132. 系統の妥当性確認は、系統が、全ての想定しうる取合い条件及び全ての想定しうる負荷条件の下で、全ての要件を満たすことを実証するべきである。

2.133. 系統の妥当性確認の期間中に容易に試験できない可能性のある、運転モード並びに I&C 系と発電所との間の相互作用は、試運転時に試験されるか又は補完的な分析を通じて妥当性確認されるべきである。

2.134. 系統の妥当性確認は、以下を対象とするべきである。

- 系統の全ての部品
- 範囲外の値を含め、取合い信号の全範囲[13]
- 例外の取扱い
- 設定点の精度及びヒステリシス
- モード間の移行を含む、発電所及び系統の運転の全てのモード
- 電源故障後の復旧
- 時間合わせ
- 頑強性及び耐障害性

2.135. 系統の妥当性確認試験は、全ての入力情報の変動を含むべきである。すなわち、動的試験が用いられるべきである。

2.136. 動的試験は、I&C 系への作動要求となる発電所パラメータの変動を代表する、また、想定しうる発電所シナリオの分析に基づく、現実的なシナリオを使用すべきである。

2.137. 機能試験は、機能要件により許されている全ての挙動を含むように設計されるべきである。機能試験の構造的な包含範囲は、機能要件を考慮に入れて正当化されるべきである。

2.138. 統計的手法を使用する妥当性確認の試験が検討されるべきである。

2.139. 系統の妥当性確認のためにシミュレータの使用が検討されるべきである。

2.140. 系統の運転マニュアル及び保守マニュアルの適切な部分は、系統の妥当性確認時に可能な限り最大範囲で妥当性確認されるべきである。

2.141. 文書化された追跡可能性分析は、系統の妥当性確認が系統要件の仕様に関して完全であること及び 2.132 項と 2.134 項の目的が満たされていることを実証すべきである。

2.142. 試験文書の完全な一式は、繰り返し試験及び以前は満足した試験のあらゆる試験に対して、整合した満足な結果が得られるとの確信を持って、試験プロセスが繰り返され

[13] 取合い信号は、例えば、他の系統、検出器、作動装置及び運転員インターフェースへの入力又はこれらからの出力を含む。

ることを可能にするために十分なものであるべきである。

設置、全体的な計測制御の統合及び試運転

2.143.　I&C 系は、承認された設計にしたがって発電所に設置されるべきである。

2.144.　設備は、系統及び機器が輸送中に損傷を受けていないことを検証するため、受け入れ時に検査されるか又は試運転による試験が行われるべきである。

2.145.　以下の項は、I&C 系に関する IAEA 安全基準シリーズ No. SSG-28「原子力発電所の試運転」[15]の手引きを実施する際の考慮事項を示している。

2.146.　試運転では、I&C 系を、他の構成要素及び他の発電所機器等と徐々に統合するべきであり、また、それらが設計仮定にしたがっていること並びに機能上の判断基準及び性能上の判断基準を満たしていることを検証すべきである。

2.147.　発電所環境内での試験は、試運転の重要な部分である。

2.148.　試運転は、外部システムとの取合いの検証及び取合い設備と正しく動作することの確認に特別の注意を払うべきである。

2.149.　試運転の期間に、全ての I&C 系は、可能な限り供用中の状態を代表する運転、試験及び保守の条件の下で、延長された時間の間、運転されるべきである。

2.150.　試運転が完了する前に、運転マニュアルについて及び保守マニュアルの適切な部分についての妥当性確認は完了されるべきである。

2.151.　I&C 系が運転可能と宣言される前に、関連するライフサイクルの計画された活動は完了されるべきであり、追跡可能性は設置された系統に対する要件から確立されるべきであり、また、それらの建設文書及び設計文書は完全であり、その時点における構成配置を反映しているべきである。

運転及び保守

2.152.　I&C 系の保守及びサーベイランスは、IAEA 安全基準シリーズ No. NS-G-2.6「原子力発電所における保守、サーベイランス及び供用期間中検査」[16]の手引きに従って実施されるべきであり、この基準は、I&C 系についての較正を含め、保守及びサーベイランスの計画立案、組織的側面及び実装についての手引きを提供している。

2.153.　以下の項（2.154 項～2.156 項）は、I&C 系に関する NS-G-2.6[16]の手引きを具体化する際の考慮事項を示している。

2.154.　I&C 系のパラメータの変更は、適切な手段を用いて行われるべきである。

2.155.　I&C 系の運転及び保守におけるヒューマンパフォーマンスは、人的過誤を低減するための改造の必要性を示す場合がある運転経験を文書化するために監視されるべきである。

2.156.　適切な量の予備品は、意図された供用寿命を通して、運転及び保守のために利用可能であるべきである（例えば、I&C 設計、機器の信頼性並びに交換機器及び供給業者の支援の将来的な入手可能性に基づいて）。

改造

2.157. 以下の項は、I&C 系に対して NS-G-2.3[9]の手引きを具体化する際の考慮事項を示している。

2.158. I&C に対する改良及び改造の設計は、以下を考慮すべきである。

- I&C 系に対する設計の選択肢を実効的に制限する、設置された発電所の物理的特性から生じる制限
- 交換設備の設計と既存 I&C 設備との間の整合性を維持することの想定しうる必要性。これは、例えば、全体的な運転員インターフェース及び発電所保守業務の複雑さを低減するためである。
- 市販で入手可能な設備に関しての又は設備の設置寿命期間中の製造業者又は第三者によるこのような設備及び技術の支援を確保することの見通しに関しての、実務的な考慮事項
- 既存の設計文書を更新する必要性[14]

2.159. I&C 系が改造されるか又は改良の一部であるとき、変更を正当化し、実行する際に適用される厳格さの程度は事前に設定されるべきである。

2.160. 厳格さの程度は、作業後の運転において以前の状態のままである既存の系統と連携して、原子力発電所の安全を確保するに際し影響を受ける系統の役割及び機能に基づくべきである。これは、ソフトウェアツールに対する変更にも適用する。

2.161. I&C 系の改造又は改良の展開は、指定されたライフサイクルに従うべきである。

2.162. 改造に必要とされるライフサイクルプロセスの複雑さは、改造の複雑さ及び安全上の重要性に関係づけられる。

2.163. 最も単純な変更に対してさえライフサイクルは、各 I&C の改造後の検証及び妥当性確認を含め、少なくとも図 2 に示されている個々の系統のライフサイクルの諸段階を含むべきである。

2.164. 新しい I&C と既存の I&C との間の移行を表わすヒューマンマシンインターフェースの暫定的な構成は、暫定的な設備又は手順書の使用に適応するために、人間工学の観点からの更なる分析を必要とすることがある。運転員とのインターフェースの強化は、変更後暫くの間は、運転員及び保守員による過誤の増加につながることがある。場合によっては、訓練の変更が必要になることがある。

2.165. I&C 系が交換される場合、試用期間の間、すなわち、新しい系統の妥当性について十分な信頼が得られるまで、古い系統と並行して新しい I&C 系を稼働させることに配慮されるべきである。並行運転に相当するものとして、1 つの系列に同時に新しい多重性を有する設備を設置することができることがある。

2.166. I&C 系の並行運転を検討する場合、運転上の問題及び複雑さの不利益は、信頼性の利得に対して比較検討されるべきであり、また、リスクが評価されるべきである。

2.167. 最初の開発時と改造時との間におけるソフトウェアツールの更新又は変更の影響は重大である場合があり、それらの影響が評価されるべきである（例えば、コンパイラの

[14] 古い系統に関する設計文書は、不完全又は不正確であることがある。したがって、このような系統に対する規模の大きい改造又は交換は、当初の設計基準及び仕様書を再生するために、ある程度の「リバース・エンジニアリング」を要求することがある。

改良は以前の分析結果又はコンパイラの健全性に関する検証を無効にする可能性がある)。

3. 計測制御系の設計基準

計測制御機能の特定

3.1. SSR-2/1 (Rev. 1)[1]の要件 4 は以下のように述べている。

> 「原子力発電所に対する次の基本的な安全機能の達成は、すべての発電所状態に対して確実なものとされなければならない。すなわち、(i) 反応度の制御、(ii) 原子炉及び貯蔵燃料場所からの熱の除去、並びに (iii) 事故による放射性物質の放出の制限に加えて、放射性物質の封じ込め、放射線遮蔽及び計画的な放射性物質の放出の管理。」

3.2. SSR-2/1 (Rev. 1)[1]の 4.1 項は以下のように述べている。

> 「基本的な安全機能を達成するために必要な安全上重要な機器等を特定することに対して、また、すべての発電所状態において基本的な安全機能を達成することに寄与し又は影響を与える固有の仕組みを特定することに対して、体系的な方法が取られなければならない。」

3.3. SSR-2/1 (Rev. 1)[1]の 4.2 項は、「必要な安全機能が達成されることを確実なものとするために発電所の状態を監視する手段が設けられなければならない。」と述べている。

3.4. 要求される安全機能は、原子力発電所の設計プロセスより導出され（SSR-2/1 (Rev. 1)[1]の第 4 章を参照)、また、発電所の構築物、系統及び機器にこれらの機能を割り当てるために従う体系的な方法が要求される。

3.5. I&C 系の要求される機能（並びに安全、セキュリティ及び時間的制約のような特性に関する非機能的要件）は、原子力発電所に対する設計プロセスの一環として決定されるべきである。

3.6. I&C 系に割り当てられた機能は、運転状態の様々なモード及び事故状態における発電所の運転に関連する情報及び制御能力を提供する機能を含む。深層防護の概念に対応するこれらの機能の目的は以下である。

- 通常運転からの逸脱を防止すること
- 故障を検出し、異常運転を制御すること
- 発電所の設計基準内の事故を制御すること
- 設計拡張状態における影響を制御すること
- 事故の放射線上の影響を緩和すること

計測制御系の設計基準の内容

3.7. SSR-2/1 (Rev. 1)[1]の要件 14 は以下のように述べている。

「安全上重要な機器等の設計基準は、原子力発電所の存続期間にわたって具体的な容認基準を満たすために、関連する運転状態、事故状態並びに内的ハザード及び外的ハザードから生じる状態に対して必要な能力、信頼性及び機能性を定めなければならない。」

3.8. SSR-2/1 (Rev. 1)[1]の 5.3 項は以下のように述べている。

「安全上重要な個々の設備の設計基準は、体系的に根拠付けられ、文書化されなければならない。この作成文書は、事業者が発電所を安全に運転するために必要な情報を提供しなければならない。」

3.9. I&C 全体構造及び各 I&C 系は、文書化された設計基準を持つべきである。

3.10. I&C 全体構造は発電所の I&C 系の組織的な構造である。原子力発電所の I&C 全体構造は、各々が特定の役割を果たす多数の I&C 系を含む。

3.11. 設計基準は、I&C 全体及び個々の I&C 系に関する機能、条件及び要件を特定している。その上で、この情報は機能を区分し、これらを適切な安全クラスの系統へ割り付けるために使われる。[17]。

3.12. いくつかの事例においては、I&C 系の要件は原子力発電所の設計及び設計基準が開発されるとともに特定されることになる。したがって、I&C 系の設計基準の完全な内容は、プロジェクトの最初の時期には利用できないことがある。

3.13. I&C 設計基準の策定は、発電所の安全設計基準文書から導出されるべきであり、また、以下の情報を提供すべきである。

- 発電所の深層防護の概念
- 備えられるべき安全機能（3.11 項を参照）
- 安全区分並びに安全上重要な発電所機能の機能要件及び性能要件
- 自動で開始される操作と手動で開始される操作との間の優先順位及び一つまたは複数の系統が装置又は機能を起動できる自動操作間の優先順位に関する原則
- I&C 系の許認可に対する国の要件
- I&C の安全分類に対する国の要件
- 運転上の要件に関する国の要件
- 発電所における安全機能及びセキュリティ機能に不可欠なデジタル I&C 系の分析及び特定
- コンピュータ・セキュリティに対するリスク評価及び影響解析
- 情報及び制御の必要性及び配置
- 発電所における運転の思想
- 人間信頼性解析
- 運転要員の役割
- 職員配置のレベル

3.14. I&C 系の設計基準は、I&C 全体及び個々の I&C 系のために必要な能力、信頼性及び機能性を規定すべきであり、以下を含む。

- 全ての機能要件、例えば以下である。
  - 各 I&C 系が要求される発電所の運転状態
  - 各 I&C 系が動作可能であるべき様々な発電所の構成配置

・ 各発電所状態、発電所の各運転モード及び長期間停止に対する機能要件[15]
・ 要求される各 I&C 機能の安全上の重要性
・ 系統が対応すべき想定起因事象
・ I&C 全体構造の中での、深層防護概念における個々の I&C 系の役割
・ 監視されるべき変数又は変数の組み合わせ
・ 自動、手動又はその両方で実施されるべき操作の細目を含む、要求される制御機能及び保護機能並びに制御装置の場所
・ 要求される範囲、変化率、精度、デジタル表現の定量化、計算の正確さ及び各 I&C の安全機能の応答時間

－ 必要なレベルの信頼度及び稼働率を達成するために課される全ての要件、例えば以下である。

・ 安全機能の独立性の要件
・ 定期試験、自己診断及び保守の要件
・ 定性的又は定量的な信頼性目標及び稼働率[16]目標
・ プロセスの故障時の挙動に関する要件

－ 必要なレベルのセキュリティを達成するために課される全ての要件。例えば以下である。

・ 設計において監視されるべきセキュリティ上の制約事項及び運転上の制約事項
・ 実装されるべきセキュリティ対策

－ 設備が適切に性能保証されていることを保証するために必要な全ての要件、例えば以下である。

・ I&C 系が遵守すべき標準の仕様を含む、設計判断基準
・ 系統がその機能を実施する際の性能を劣化させる可能性を伴う発電所条件及び必要な能力を保つためになされるべき方策
・ 系統が安全上重要な機能を実施することを要求される内的ハザード及び外的ハザード（自然現象を含む）の範囲
・ 系統が安全上重要な機能を実施することを要求される、発電所の環境状態[17]の範囲
・ 使用される材料に対する制限事項
・ 設備の位置、ケーブルへの接近及び電源についての制約事項を含め、発電所の物理的な設計及び配置により課される制約事項
・ 設備の物理的位置及び設備間の取合い

3.15. 3.14 項に示されている推奨事項に加えて、安全系に関する設計基準は、以下を規定すべきである。

－ 安全系を起動するために要求されるパラメータの制限値（解析制限値、6.209 項及び 83 頁の図 3 を参照）

---

[15] 機能要件は、例えば、入力情報の出力情報への変換及び取られるべき操作を定義している。

[16]系統及び機器に関する信頼度及び稼働率の制限値は、確率論的な判断基準、決定論的な判断基準（例えば、単一故障基準又は特定の手順書及びソフトウェアに関する検証方法の順守）又はその両方を使用して規定される場合がある。

[17] ここでいう発電所の環境状態は、通常状態、異常状態、また、設計基準事故、内部事象又は外部事象の時に I&C 設備が経験することがある極端な状態を含む。I&C 系間のあらゆる相互作用、特に異なる程度で性能保証された機器間の相互関係は、全面的に考慮に入れられない場合、深層防護に関する要件を損なう場合がある。

- 運転員が系統の保護機能の動作を確認することができるように表示されるべき変数及び状態
- 自動で開始されないあらゆる安全操作の正当化。これには以下を含む。
  - 手動制御が許容される状況、異常事象、継続時間及び発電所の状態
  - 手動措置のみによる、開始を認めることの正当化又は開始後の制御
  - 運転状態及び事故条件において運転員が手動操作を取ると予想されるときの運転員周囲の環境条件の範囲
  - 手動操作を実施するときに、運転員が考慮に入れるべき情報が適切な場所に表示されていること、また、この情報が運転員の操作を支援するために必要な性能特性を持っていることの確認
- I&C 安全機能のバイパスが許されることになる条件
- 起動された保護系統がリセットできる前に満たされなければならない条件
- 共通原因故障の影響を緩和するための多様な機能に関する要件

3.16. 上記の機器等は、I&C 全体の設計基準又は個々の系統の設計基準のいずれかにおいて規定される場合がある。一部の機器等については、I&C 全体の設計基準において汎用的な要件を規定し、個々の系統に関する設計基準においてさらに詳細を提示することが適切であることがある。いずれの場合においても、I&C 全体に対する設計基準及び個々の系統に対する設計基準は、互いに整合しているべきであり、また、様々な設計基準間の取合いは容易に理解できるべきである。

4. 計測制御の構造

構造の設計

4.1. I&C 系全体についての構造の設計は以下を設定している。

- 全体的な構造を構成する I&C 系
- これらの系統の組織
- これらの系統に対する I&C 機能の割り当て
- I&C 系を跨ぐ相互接続並びにそれぞれの割り当てられた及び禁止された相互作用
- 全体構造に割り当てられた設計制約事項（禁止された相互作用及び挙動を含む）
- 様々な I&C 系間の境界の定義

4.2. 個々の I&C 系についての構造の設計は以下を設定している。

- 分割不可能な個々の機器に至るまで全ての統合レベルを通しての構成－分割の関係
- 各統合レベルでの各機器への I&C 機能、挙動、制約事項及び（導出された）品質要件の割り当て
- ひとつの統合レベルでの挙動の構成が、次のより高い統合レベルで要求される挙動を満足させていること、及びこれが他の挙動を誘起しないことの保証を提供するための構成可能性と構成の規則
- 各統合レベルにおける及び各統合レベルを跨ぐ機器等の相互接続、並びに割り当てられた及び禁止されたそれぞれの相互作用
- 個々の I&C 系に割り当てられた設計制約事項（禁止された相互作用及び挙動を含む）

4.3. 最新の I&C 系は、より相互接続しており、分析することがより困難である（したがって、安全の保証は以前の世代の I&C 系の場合より困難である）。適切に設計された I&C 系構造は、これらの仕組みが発電所の安全の確保をより難しくすることのないように、深層防護及び多様性を確保することになり、また、系統の仕組みを分析する困難さを限定し、封じ込めることになる。

4.4. I&C 全体構造及び個々の I&C 系構造は、系統の取合いに関する要件並びに安全、セキュリティ、検証性、解析可能性及び時間的制約のような特性に関する要件を含む、発電所の要件を満足させるべきである。

4.5. SSR-2/1 (Rev. 1)[1]の要件 7 は、「原子力発電所の設計は、深層防護を取り入れなければならない。深層防護の階層は実行可能な限り独立したものでなければならない。」と述べている。

4.6. 参考文献[18、19]は、深層防護の概念を説明しており、また、深層防護の階層を記述している。

4.7. I&C 系全体構造は、発電所の設計の深層防護の概念及び多様性の方針を損なうべきではない。

4.8. I&C 系全体構造は、I&C 全体の中で適用される深層防護の概念及び多様性の方針を定義するべきである。

4.9. I&C 系全体構造の設計はまた、発電所の深層防護の概念の様々な階層及び多様性を支援する I&C 系間の独立性のレベルも設定している。

4.10. I&C 系全体構成内の深層防護は、1 つの防護線の故障が、次に続くものにより補われるように、独立した防護線により達成される。

計測制御全体構造の内容

4.11. I&C 系全体構造は以下であるべきである。

- 発電所の設計基準を果たすために必要な全ての I&C 機能を含んでいるべきである。
- 全ての I&C 系にわたって、整合性を持って扱われるべき事項を特定すべきである[18]
- 以下のために、I&C 系全体構造に含まれる個々の I&C 系を特定すべきである
  - 発電所で適用される深層防護の概念及び多様性を支援するため
  - I&C 全体に対する独立性に関する設計基準要件を支援するため
  - 異なる安全クラスの系統及び異なる安全区分の機能を十分に分離するため
- 個々の I&C 系の間の取合い及び情報伝達手段を定義すべきである。
- I&C 全体構造に割り当てられた、各安全機能の信頼性要件を果たすために適用される設計方針を設定すべきである。[19]
- 安全グループによる単一故障基準の遵守を支援すべきである
- 運転又は事故管理のために情報が必要とされる、中央制御室、補助制御室及びその

---

[18] 全ての I&C 系に渡って整合性をもって考慮されるべき事項は、例えば、発電所の運転の概念の適用、ヒューマンマシンインターフェースに関する設計標準の適用、ケーブル配線に対する制約事項、接地の実践及び警報管理の考え方を含む。

[19] 信頼性要件を判断することに関する方針は、単一故障基準、多重性、多重性を有する機能間の独立性、フェールセーフ設計、多様性及び検証可能性（解析可能性及び試験可能性を含む）の順守を含むことがある。第 6 章は、信頼性を達成するための方針を具体化する際の考慮事項を記している。

他の区域において必要な情報を提供すべきである。
- 運転又は事故を管理するために制御装置が必要とされる、中央制御室、補助制御室及びその他の区域において必要な運転員の制御装置を備えるべきである。
- プロセスの変数を、それらが安全系の能力を超えないように、指定された運転範囲内に維持、制限するために、また、故障及び通常運転からの逸脱の影響を制限するために必要な自動制御装置を備えるべきである。

4.12. I&C 系を実装するために使用される I&C プラットフォームの特性は、I&C 全体構造の設計と相互作用する場合があり、また、I&C 全体構造は、I&C プラットフォームに対し、機能上及び性能保証上の要件を課すことになる。したがって、一般に、I&C 系全体構造の定義と合わせて、I&C プラットフォームが選定されることが望ましい。安全系に対する機能上及び性能保証上の要件は制御系のものとは通常異なっている。このこと及び多様性の理由から、I&C 全体は通常 2 つ又はそれ以上のプラットフォームを含むことになる。

個々の計測制御系の構造の内容

4.13. 個々の I&C 系の構造の設計は以下であるべきである。

- I&C 全体構造の設計において、それに割り付けられた役割を果たすために必要な全ての I&C 機能を提供するべきである。
- 適切な場合には、系統を多重の区分に分割すべきであり、このような区分間の独立性についての要求される程度を規定すべきである。[20]
- 多重性を有する区分に含まれる I&C 機器等を規定すべきである
- 各 I&C 機器に対する、I&C 機能の割り当て及びその他の系統の要件を記述すべきである。
- 系統内の I&C 機器等の間の取合い及び情報伝達手段を定義すべきである。
- 主要な機器等及びデータリンクに適用される主要な設計上の仕組みを定義すべきである。

独立性

4.14. I&C 全体構造内の独立性は、系統間の故障の伝播を防止すること、また、可能なところでは共通原因故障の同一原因に複数の系統がさらされることを避けることが意図されている。このような共通原因故障の原因の例は、内部事象、外部事象及び共通の支援的な補助系統の故障を含む。

4.15. I&C 全体構造は、安全系の区分の独立性を損なうべきでないし、発電所において適用される深層防護の異なる階層の独立性も損なうべきではない。

4.16. 完全な独立性があることを要求される I&C 機能は、独立したハードウェア系又は機器等に割り付けられるべきである。

4.17. 安全系は、より低い安全クラスの系統から独立しているべきである。

4.18. 安全系内の多重性を有する区分は、要求された時に全ての安全機能が達成できることを確保するために必要な範囲で互いに独立しているべきである。例えば、論理照合の目

[20] 通常、安全系は単一故障基準を順守するために多重性を有する区分で構成されることになる。より低い安全クラスの系統は安全の理由で多重性を有する要素を持つ必要がないことがあるが、通常運転時の信頼性を改善するために多重性を有することがある。

的又は部分的なトリップを可能にするために多重性を有する区分間の情報伝達が必要な箇所では、電気的及び物理的な分離並びに情報伝達の独立性を確保するための十分な対策があるべきである。論理照合のための情報伝達は、安全を危険にさらす可能性がある偶発故障により引き起こされる偽起動を制限することができる。

4.19. 運転員インターフェースは、多重性を有する一つまたは複数の区分の安全機能を同時に抑えるべきではない。

4.20. 安全制御拠点は、6.55 項の推奨事項を遵守する優先機能を用いて、自分自身の区分外の安全設備の機器を操作する場合がある。

4.21. 安全系統又はその機器は、安全系による作動要求が装置を作動させるための優先度を有している場合にのみ、より低い安全クラスの運転員制御装置から操作される場合がある。

4.22. 安全系からの情報は、6.25 項～6.56 項の推奨事項が満たされている場合、より低い安全クラスの制御拠点に提示される場合がある。

4.23. 安全系統及びその機器は、事故状態又はそれらの対応が必要である内的ハザード若しくは外的ハザードにより生じる状態の影響にさらされられるときに、これらの安全機能を実施する能力を維持するべきである。

4.24. I&C 安全系の支援設備の故障又は誤操作は、安全系の多重性を有する部分間、安全系とそれより低い安全クラスの系統との間又は発電所において適用される深層防護の概念の異なる階層間の独立性を損なうべきでない。

共通原因故障の検討

4.25. SSR-2/1 (Rev. 1)[1] の要件 24 は以下のように述べている。

> 「設備の設計は、多様性、多重性、物理的分離及び機能の独立性の概念が、必要な信頼性を達成するためにどのように適用されなければならないかを判断するため、安全上重要な機器等の共通原因故障の可能性について十分に考慮しなければならない。」

4.26. IAEA 安全用語集[6]は「共通原因故障」を「単一の特定の事象又は原因による 2 つ又はそれ以上の構築物、系統及び機器の故障」として定義している。

4.27. 共通原因故障は、人的過誤、開発又は製造プロセスにおける過誤、保守における過誤、開発において使用されるソフトウェアツールにおける過誤、系統若しくは機器の間の故障の伝播、又は内的ハザード若しくは外的ハザードに対する不適切な仕様、それに対する不適切な性能保証若しくはそれに対する不適切な防護、によって発生することがある。

4.28. I&C 全体構造は、発電所における深層防護の諸階層を実際的な範囲で独立しているようにするために、採用されるべき構造概念を定義すべきである。

4.29. 発電所における深層防護の階層間の独立性を保持するために、I&C は、系統内及び系統間の共通原因故障に対する防護を備えて設計されるべきである。これを達成するために、様々な系統及び系統の要素に対する機能の割り当ては、十分に検討されるべきであり、系統間の適切なレベルの独立性が具備されるべきであり、また、安全系内で共通原因故障を防護するために方針が規定されるべきである。

4.30. 1 つ又はそれ以上の基本的安全機能を損なう全体 I&C 内の共通原因故障の可能性は評価されるべきである。

4.31. この評価において考慮されていない、特定されたあらゆる共通原因故障に対する正当性が提示されるべきである。

4.32. 各想定起因事象の影響についての解析は、保護系がその必要な安全機能を実施することを妨げるおそれのある共通原因故障と組み合わせて、安全解析の範囲内で行われるべきである。

4.33. 深層防護の概念及び多様性の分析は、4.32 項に記述されている解析を実施する 1 つの方法である。2.81 項を参照。

4.34. 4.32 項に記述されている解析が、保護系の共通原因故障と組み合わされた想定起因事象が容認し難い影響をもたらすと判断しているのであれば、設計は変更されるべきである。

4.35. 共通原因故障に対する I&C 系及びその構造の脆弱性すべての完全排除は達成可能ではないが、特定されたあらゆる脆弱性を受け入れることに対する正当性は提示されるべきである。

多様性

4.36. IAEA 安全用語集[6]は、「多様性」を「特定された機能を実施するための 2 つ以上の多重性を有する系統又は機器の存在であって、ここでは、異なる系統又は機器が共通モード故障を含めた共通原因故障の可能性を低減させるよう異なる属性を有している。」として定義している。

4.37. 多様性は、要件、設計、製造又は保守における過誤から生じる共通原因故障に対する脆弱性を低減する方法であり、また、指定された信頼性レベルを実証する難しさを補うための保守性を含める方法でもある。

4.38. 保護系における共通原因故障の影響を緩和するものとして多様性が機能保証されている場合、その多様性の仕組みが、要求されている共通原因故障の影響の緩和を実際に達成しているとの正当性が提示されるべきである。

4.39. 多様性を有する I&C 系が設けられているとき、多様性を有する系統は、仕様、設計、製造又は保守において同じ過誤に服するべきではない。

4.40. 確率論の研究[21]は、安全上重要な I&C 系の機器等を完全に独立している[22]として扱うべきではない、ただし、それらが多様性をもち、また、本安全指針で提示される、機能の独立性、電気的な隔離、情報伝達の独立性、環境性能保証、耐震性能保証、電磁気的性能保証、物理的分離及び内部事象に対する防護、に関する推奨事項を満たしていれば、この限りではない、

5. 計測制御の機能、系統及び設備の安全分類

[21] 確率論的研究は、例えば、信頼性解析及び確率論的安全評価を含む。
[22] 確率論的研究では、系統は、単純にその個々の故障確率の積を取ることによって、完全に独立しているとして扱われる。

5.1. SSR-2/1 (Rev. 1)[1] の要件 18 は以下のように述べている。

「原子力発電所の安全上重要な機器等に対する工学的設計規則は、原子力技術との関連を十分に考慮して指定されなければならず、また、関連する国内又は国際的な規格基準及び実証された工学的慣行に適合していなければならない。」

5.2. SSR-2/1 (Rev. 1)[1]の要件 22 は、「すべての安全上重要な機器等は特定されなければならず、また、それらの機能とそれらの安全上の重要度に基づいて分類されなければならない。」と述べている。

5.3. SSR-2/1 (Rev. 1)[1]の 5.34 項は以下のように述べている。

「安全上重要な機器等の安全上の重要度分類の分類方法は、以下の因子に十分に配慮をして、主として適宜決定論的方法に基づいて、必要な場合は確率論的手法で補完して行われなければならない。

(a) 機器等によって実施されるべき安全機能
(b) 安全機能を実施できなかった時の影響、
(c) 機器等が安全機能を実施するために起動要求される頻度、
(d)想定起因事象が発生してから安全機能を実施するために機器が起動要求される時間又はそのための期間 」

5.4. SSR-2/1 (Rev. 1)[1]の 5.36 項は、「複数の機能を実施する設備は、その設備によって実施される最も重要な機能と整合する安全クラスに分類されなければならない。」と述べている。

5.5. IAEA 安全基準シリーズ No. SSG-30「原子力発電所の構築物、系統及び機器の安全分類」[17]は、SSR-2/1 (Rev. 1)[1] 及び GSR Part 4 (Rev. 1)[5]において定められた、安全上重要な構築物、系統及び機器の特定のために、また、それらの機能及び安全上の重要度に基づく分類のために、定められた要件をいかにして満たすかについての推奨事項及び手引きを示している。

5.6. SSG-30[17]において推奨されている安全分類プロセスは、SSR-2/1 (Rev. 1)[1]で設定された深層防護の概念と整合している。深層防護の様々な階層において実施される機能が検討されている。

5.7. 特定の原子力発電所に関して、分類プロセスは主として以下のことを考慮している。

- 発電所の設計基準及びその固有の安全の仕組み
- SSR-2/1 (Rev. 1)[1]の要件 16 で要求されているように、全ての想定起因事象のリスト、発電所の設計基準で考慮されている想定起因事象の発生頻度が考慮に入れられるべきである。

5.8. 想定起因事象のリストを設定する場合、安全上重要な機器等の故障若しくは誤操作が直接的に想定起因事象を引き起こす場合がある可能性又は安全上重要な機器起動要求に対応できないことが想定起因事象の影響をより悪くする場合がある可能性が考慮されるべきである。

5.9. SSR-2/1 (Rev. 1)[1]の要件 4 において定義されている、主要な安全機能を達成するために必要な全ての I&C 系の機能及び設計方策は、通常運転の全てのモードを含む様々な発電所状態に対して特定されるべきである。

5.10. 全ての I&C 系の機能は、安全上の重要性に基づき以下の 3 つの要因を考慮に入れて区分されるべきである。

(a) 機能を実施できないことの影響
(b) 機能が作動要求されることになる想定起因事象の発生頻度
(c) 機能が実施されることを要求されることになる想定起因事象後の時間又はその継続期間

5.11. 安全区分において割り付けられた各機能を実施する I&C 系及び機器は、特定され、分類されるべきである。それらは、主として、それらが実施する機能に割り付けられた区分にしたがって分類されるべきである。

5.12. 安全分類を割り付けるときには、代替措置を講ずることができる適時性と信頼性及び I&C 系におけるいかなる故障も検知、修復できる適時性と信頼性が考慮されるべきである。

5.13. SSG-30[17]においては、機能に対して 3 つの安全区分が並びに構築物、系統及び機器に対して 3 つの安全クラスが、加盟国の経験に基づいて推奨されている。しかし、より多いか少ない区分数及びクラス数が、SSG-30[17]の 2.12 項及び 2.15 項に提示されている手引きに沿っていることを条件に、使われる場合がある。

6. 安全上重要な全ての計測制御系に対する全般的推奨事項

全般

6.1. I&C 系は、その設計基準についての要件を完全に満たすべきである。

6.2. I&C 安全系の設計において、不必要な複雑さは避けられるべきである。

6.3. I&C 安全系の全ての仕組みは、それらの安全機能に有益であるべきである。

6.4. I&C 安全系の設計の複雑さは、他の設計原則（例えば、独立性、多重性又は多様性）の妨げにつながるべきでない。

6.5. 複雑さを避けることの意図は、I&C 系を可能な限り単純に保つことであるが、それでも安全要件を完全に満たすことである。避けられるべき複雑さの例は、I&C 系の安全機能又はその信頼性に寄与しない機能を含むこと、十分な分析又は検証に適していない設計特性及び実装時の特性の使用並びに安全の適切な実証の実施に対して複雑すぎる実装用プラットフォームの使用である。したがって、採用される構造は、単純な相互作用及び単純な情報伝達リンクを有するべきである。注意深い文書作成及び各要件に対する合理性の検討は、不必要な複雑さを避ける 1 つの効果的な手段である。

信頼性設計

6.6. SSR-2/1 (Rev. 1)[1] の要件 23 は、「安全上重要な機器等の信頼性は、それらの安全上の重要度に相応していなければならない。」と述べている。

6.7. SSR-2/1 (Rev. 1)[1] の要件 62 は以下のように述べている。

「原子力発電所における安全上重要な機器等に対する計測制御系は、遂行されるべき安全機能につり合った機能上の高い信頼性と定期的な試験可能性を有するものとして設計されなければならない。」

6.8. SSR-2/1 (Rev. 1)[1]の 6.34 項は以下のように述べている。

「安全機能の喪失を防止するために、実施可能な範囲で、必要であれば自己診断能力を含む試験可能性、フェールセーフ特性、機能上の多様性並びに機器設計及び運転構想における多様性のような設計手法が使用されなければならない。」

6.9. I&C 系の設計において、機能的な信頼性を具備するために使用される仕組みの例は以下を含む。すなわち、偶発故障に耐える能力、設備及び系統の独立性、多重性、多様性、共通原因故障に対する耐性、試験可能性及び保守性、フェールセーフ設計並びに高品質設備の選択、である。

単一故障基準

6.10. SSR-2/1 (Rev. 1)[1] の要件 25 は 、「単一故障基準は、発電所の設計に取り入れられた安全グループ毎に適用されなければならない。」と述べている。

6.11. SSR-2/1 (Rev. 1)[1]の 5.39 項は、「ある安全設備グループ又は安全系に単一故障基準を適用する場合、誤操作は、故障モードの一つであると見なされなければならない。」と述べている。

6.12. 通常、多重性、独立性、試験可能性、連続監視、環境性能保証及び保守性などの概念は、単一故障基準の遵守を達成するために採用される。

6.13. 各安全グループは、安全系内のいかなる単一の故障の存在下であっても想定起因事象に対応するために要求される全ての措置を、以下のことと組み合わせて、実施すべきである。

- 検知不可能なあらゆる故障、すなわち、定期的な試験、警報又は異常表示により検出できないあらゆる故障
- 単一の検知失敗及び検出不可能な故障により引き起こされる全ての故障
- 安全グループに影響を与える可能性がある想定起因事象を引き起こすか又はその想定起因事象により引き起こされる、全ての故障及び系統誤作動
- 発電所の運転上の制限値及び条件により認められている試験又は保守のため、安全系の一部の供用からの取り外し又はそれのバイパスをすること

6.14. 設計、保守、運転又は製造における過誤がもたらす故障は、単一故障基準の遵守の解析に含まれていない。既知の過誤は、マネジメントシステムの手段により適切に取り組まれるべきである。未知の過誤の影響は予想することができず、したがって、単一故障基準は安全グループにおけるこのような過誤の影響を理解するための有用なツールではない。このような過誤による共通原因故障の潜在的な影響を評価するための解析は第 4 章で検討される。

6.15. 単一故障基準の不遵守は、例外的な場合にのみにされるべきであり、設計文書において特定されるか、安全解析で明確に正当化されるべきである。

6.16. 単一故障基準の不遵守を正当化するための、外的ハザードなどの頻度の低い事象の解析では十分な注意が必要である。安全系の運転及び監視のために必要な電気系及びその

他の支援系の長期的な利用可能性の確保のために、特別な考慮がなされるべきである。

6.17. 信頼性解析、確率論的評価、運転経験、工学的判断又はこれらの組み合わせは、単一故障基準を適用するときに特殊な故障を考慮から除外することに対する根拠を設定するために使用される場合がある。

6.18. 保守、補修及び試験の活動は、単一故障基準が満たされない状況においても発電所の運転上の制限値及び条件と整合しているべきである。

6.19. 単一故障基準の遵守が信頼性要件を満たすのに十分でない場合、系統が信頼性の要件を満たしていることを保証するために、追加の設計上の仕組みが提供されるべきであるか又は設計に対する変更がなされるべきである。

多重性

6.20. I&C 系は、I&C の信頼性に対する要件及び単一故障基準を満たすために必要な程度の多重性を有するべきである。

6.21. 多重性は、単一故障基準への適合を含め、系統に対する信頼性目標を達成するために I&C 系で一般に使用される。多重性は多重性の要素も独立していない限り、十分に効果的でない。一般に、多重性は信頼性を増加するが、誤操作の確率も増加する。多重性信号の同時一致（「選択論理」）又は偽信号拒絶の仕組みは、信頼性と誤操作のないこととの適切な均衡を得るために一般的に使用される。

独立性

6.22. SSR-2/1 (Rev. 1)[1]の要件 21 は以下のように述べている。

> 「安全系間の干渉又は系統の多重的要素間の干渉は、適宜、物理的分離、電気的隔離、機能的独立性及び通信（データ転送）の独立性のような手段により、防止されなければならない。」

6.23. SSR-2/1 (Rev. 1)[1]の 5.35 項は以下のように述べている

> 「設計は、安全上重要な機器等同士のいかなる干渉も防止されること、及び、特に、低い安全クラスの系統における安全上重要な機器等のいかなる故障も、より高い安全クラスの系統に伝播しないことを確実なものとしなければならない。」

6.24. IAEA 安全用語集[6]は独立した設備を以下のように定義している。

> 「以下の特性を両方とも有する設備、
>
> (a) 要求される機能を実施する能力は、他の設備の運転又は故障により影響されない
>
> (b) 機能を実施する能力は、これが機能することを要求される想定起因事象から生じる影響の発生により影響されない。」

6.25. 独立性は、故障、内的ハザード又は外的ハザードが、安全系の多重性を有する要素に影響を及ぼすことを防止するために設定される。また、これは、故障又はハザードが深層防護の異なる階層を提供する諸系統に影響を及ぼすことを防止するために設定される。考慮されるべき故障プロセスは、以下を含む。すなわち、設計基準事故から生じる故障、同一ハザードにさらされること、系統間又は多重性を有する区分間の電気的接続、及び系

統間又は多重性を有する区分間のデータのやり取り並びに設計、製造又は運転、保守における共通的な過誤である。

6.26. 独立性を提供するための手段は、以下の仕組みを含む。すなわち、物理的分離、電気的隔離､機能上の独立性及び情報伝達の過誤の影響からの独立性である(第 7 章を参照)。設備の性能保証及び多様性も独立性を支援する場合がある。これらの事項は、本章で追って検討される（6.77 項～6.134 項)。一般にこれらの仕組みの組み合わせは独立性の目標達成するために採用されるべきである。

6.27. 隔離を確保するための装置が、異なる安全クラスの系統間で使用されるとき、これらはより高い安全クラスの系統の一部であるべきである。

6.28. 様々な物理的な影響、電気的障害及び情報伝達の過誤から隔離するための対策は、必ずしも保護されている装置内に組み込まれる必要はない。様々な異なる種類の脅威から系統を隔離するための特性は、物理的に同じ装置内に組込まれる必要はなく、又は回路内の同じ場所に配置される必要はない。また、単一の影響に対する隔離機能は、一つまたは複数の装置により共有される場合もある。例えば、データ通信における過誤に対する隔離はバッファメモリーにより提供されることがあり、これは、データが妥当性、正確性及び信憑性の判断基準を満たしていない限り、バッファーからデータが読まれないことを確保するため、異なる装置のプロセッサにより提供される妥当性チェックを伴って、データがある一つの区分によって他の区分に直接書き込まれることを防止するためである。

6.29. 独立性の要件を満たすために備えられる設計の仕組みの妥当性は、正当化されるべきである。

物理的分離

6.30. 物理的分離の使用は以下にあげられる。

- 物理的分離は、内的ハザードの影響による共通原因故障に対し防護する。当該の内的ハザードは、火災、飛来物、蒸気噴射、配管のむち打ち、化学爆発、溢水及び隣接した設備の故障を含む。
- 物理的分離は、通常状態、異常状態若しくは事故状態における共通原因故障、事故（全ての設計基準事故を含む）の影響又は内的及び外的ハザードの影響に対して保護するために使用される可能性がある[23]。
- 物理的分離は、影響を局所化させる外部事象（例えば、航空機衝突、竜巻又は津波）の結果として、共通原因故障の確率を減少させる場合がある。
- 物理的分離は、多重性を有する設備の運転時又は保守時の、不注意な過誤の確率を減らす。

6.31. 安全系の一部である機器等は、より低い安全クラスの系統の機器等から物理的に分離されるべきである。

6.32. 安全グループの多重性を有する部分は、互いに物理的に分離されるべきである。

6.33. 検出器又は起動装置がともに近接して配置される場合、制御棒駆動機構又は炉内計装の場合には、多重性を有する機器等の間の完全な物理的分離は非実用的である場合があ

[23] 例は、電磁干渉の影響を弱めるための空間、異なるレベルで性能保証されている系統と機器との間の分離を含む。また、環境性能保証、耐震性能保証及び電磁気性能保証は、事故、内的ハザード又は外的ハザードの影響に対して保護するために、機器等自身によって又は物理的分離に併せて使用される場合がある。

る。

6.34. 設備又は配線の集中のため、困難さが存在することがある一部の区域は以下のとおりである.

- 格納容器貫通部
- モーターコントロールセンター
- 開閉所区域
- ケーブル敷設室
- 機器室
- 中央制御室及びその他の制御室
- 発電所のプロセスコンピュータ

6.35. 適切な物理的分離が不可能な場所では、分離は実際に達成可能な限り備えられるべきであり、また、例外事項は正当化されるべきである（6.43 項を参照)。

6.36. 物理的分離は、距離、障壁又はこれらの 2 つの組み合わせによって達成される。

6.37. IAEA 安全基準シリーズ No. NS-G-1.7「原子力発電所の設計における内部火災及び爆発に対する防護」[20]及び No. NS-G-1.11「原子力発電所の設計における火災及び爆発以外の内的ハザードに対する防護」[21]は、火災及びその他の内的ハザードに対する防護に関する追加手引きを提示している。

電気的隔離

6.38. 電気的隔離は、1 つの系統での電気的故障が、接続されている系統又は系統内の多重性を有する要素に影響を及ぼすことを防止するために使用される。

6.39. 安全系統及び機器は、より低い安全クラスの系統及び機器から電気的に隔離されるべきである。

6.40. 安全グループの多重性を有する部分は、互いに電気的に隔離されるべきである。

6.41. 電気的隔離を提供する装置は、保証できる最大の過渡的な電圧又は電流、地絡、断線及び装置の片側に生じた短絡が、接続されている安全回路の運転に許容できない劣化を生じることを防ぐべきである。

6.42. 電気的隔離のための方策の例は以下を含む。すなわち、電気的な接続がないこと、隔離を提供する電子的装置、光学的隔離を提供する装置（光ファイバーを含む)、リレー、距離による分離及び内部における機械的構造又はこれらの仕組みの組み合わせである。

随伴回路

6.43. 安全回路と安全クラスがより低い回路との間の適切な物理的分離又は電気的隔離を備えることが実際的でない場合、安全クラスがより低い回路（ここでは「随伴回路」とする）は、以下であるべきである。

- 随伴回路はそれがつながる安全クラスの回路に許容できない劣化をもたらさないことを実証するために解析又は試験されるべきである。[24]

[24] 例えば、解析又は試験は、安全回路が耐えうる電圧との比較で随伴回路内の最大電圧を考慮する場合がある。

- それがつながる安全区分の一部に指定されるべきである。
- それがつながる安全区分の回路と同じ程度に他の機器から物理的に隔離されるべきである。

機能の独立性

6.44. 機能の独立性とは、ある系統の要求された機能の成功裏の完了が別の系統の故障若しくは通常動作を含むあらゆる挙動とは関係ないとき又は別の系統に由来するあらゆる信号、データ若しくは情報とは関係ないときに存在する状態である。機能の独立性は、ある系統の別系統からの隔離を達成する一つの手段である。機能の独立性は、多重性を持つ設備間の隔離を達成する方法としても使うことができる。

6.45. 機能の独立性は、構造の設計及び機能間で共有されるデータの注意深い取扱いにより支援される。構造の考慮事項は第 4 章に記載される。共用データの扱いは以下で議論される。

6.46. より低い安全クラスの I&C 系からの入力情報は、安全系がその安全機能を実施する能力に悪影響を及ぼすべきでない。

6.47. しかし、安全系は、例えば、保守、ソフトウェア更新、試験を実施する系統、構成データを設定する系統など、安全分類されない保守用の系統からの入力情報に依存している場合もある。通常、そのような入力情報は、影響を受ける区分を切り離して作成され、データが入力された後に検証される。

6.48. 安全クラスがより低い監視系統は、その監視系統が安全系を乱すことができないことが実証されていることを前提に、安全系に接続される場合がある。安全系が、安全クラスがより低い保守用系統に接続される場合、影響を受ける区分若しくはチャンネルが切り離し状態であるとき､保守用系統からのデータの使用が特定の目的に限定されているとき、又は保守用系統の接続がコンピュータのセキュリティプログラムに適合しているときにのみ接続がなされるべきである。

6.49. チャンネルレベルでの保守が認められる状況では、単一の区分に対し共通しているチャンネル間の十分な隔離がなされるべきである。

6.50. 保守用系統が接続される場合がある発電所の運転モードは指定されるべきである。

6.51. 安全系と安全クラスがより低い系統との間のデータの転送は、安全クラスがより低い系統で発生しうる故障が、接続されている安全系の安全機能の遂行を妨げることのないように設計されるべきである。

6.52. 安全グループの多重性を持つ要素間のデータの通信は、送信側要素で発生し得る故障が、接続されている要素がその要件を満たすことを妨げることのないように設計されるべきである。

6.53. コンピュータシステムにおいて、より高い安全クラスのコンピュータに基づく系統が、より低い安全クラスの系統にデータを提供する場合、一方向の広域データ通信が多く使われる。一方向の仕組みを強いるハードウェア特性は、そのような一方向通信を保証する手段とみなされるべきであり、例えば、安全クラスがより高い系統の発信装置のみに、また、安全クラスがより低い系統の受信装置にのみ接続された連絡回線の使用である。

6.54. 正当化された場合には、以下の条件の下に、個々のアナログ又は二値信号回線を経由してより低い安全クラスの系統から、より高い安全クラスの系統に信号が送られる場合がある。

－　6.51 項の推奨事項がなお満たされていること。
－　安全クラスの機器の偽起動を引き起こす可能性がある、安全クラスがより低い系統での故障の可能性が、評価され、容認できることが示されること。

6.55.　安全系の起動装置が、より低い安全クラスの系統を含む他の系統からの情報により動作するとき、他の系統からの誤ったデータが安全機能を抑制できないことを保証する方策が講じられるべきである。多くの場合、これは安全系の内部からのデータ及び作動命令を優先する優先論理の使用により達成される。

6.56.　7.52～7.59 項は、保護系及び制御系が共通の入力信号を使う場合の追加の推奨事項を提示する。

多様性

6.57.　コンピュータに基づくシステム又は複雑なハードウェア機能、複雑なハードウェア論理若しくは複雑な電子機器を使うシステムの信頼性を実証する際に難しさが生じることがある。I&C により実施される機能について十分な信頼性を実証することができない場合、多様性のある I&C 設備が、基本的な安全機能が果される確信度を高めるために使用されることがある。様々な加盟国で、期待される多様性の種類に大きな違いがある。

6.58.　設計基準事故の条件の下で基本的な安全機能を達成する際に多様性を使うか否かの決定は、正当性が示されるべきである。

6.59.　共通原因故障の可能性に対処するために多様性が使われる場合、2 種類以上の多様性の使用が検討されるべきである。

6.60.　様々な種類の多様性の事例には以下のものを含む。

－　設計の多様性。これは、同一の又は類似の問題を解決するために、異なる設計手法を使うことによって達成される。
－　信号の多様性。これは、異なる発電所パラメータの値に基づいて安全動作が開始される場合がある系統によって達成される。
－　設備の多様性。これは、異なる技術を採用したハードウェア（デジタル設備に対するアナログ設備、電磁気型設備に対する半導体設備又はフィールドプログラマブルゲートアレイに基づく設備に対するコンピュータに基づく設備）によって達成される。
－　機能の多様性。これは、同じ安全目的を達成するために様々な動作を取る複数の系統によって達成される。
－　開発プロセスにおける多様性。これは、異なる設計組織、異なる管理チーム、異なる設計と開発のチーム及び異なる実装と試験のチームを使うことによって達成される。
－　論理の多様性。これは、異なるソフトウェア又はハードウェア記述言語、異なるアルゴリズム、論理機能の異なる時間調整及び論理機能の異なる処理順位付けの使用によって達成される。

6.61.　多様性が備えられる場合、使われる多様性の種類の選択が、求められる共通原因故障の緩和を達成することが実証されるべきである。

6.62.　分離した系統に多様性を適用することは必ずしも必要ではない。例えば、機能の多様性と信号の多様性が、単一の系統内で適用されることがある。

6.63.　多様性の具備は、多様性の適用において、類似の材料、類似の機器、類似の製造プロセス、類似の論理、動作原理のわずかな類似性又は共通の支援設備のような、潜在的共

通性のある領域を避けることを含む。例えば、異なる製造者が同じプロセッサを使っているか又は同じオペレーティングシステムの使用許諾を受けており、そのために共通故障モードを含んでいることがある。この可能性を考慮しないで製造者の名称又は型式番号の違いに基づいて多様性の主張の根拠とするのは不十分である。

故障モード

6.64. SSR-2/1 (Rev. 1)[1] の要件 26 は、「フェールセーフ設計概念は、適宜、安全上重要な系統及び機器の設計に取り込まれなければならない。」と述べている。

6.65. あらゆる I&C 機器への電源の喪失又は既知で文書化されたあらゆる故障モードの I&C 機器の故障は、系統を安全上容認できると実証された事前決定された状態下に置くべきである。

6.66. 故障しても系統を安全な状態に置くことを確保する方法には、電源が切られた場合に系統が安全な状態に行くような設計又は設備がもはやその設計機能を実施していないことを検知し、その系統を安全な状態に置くための「ウオッチドッグタイマー」の使用がある。

6.67. そのような行為が適用された場合、6.65 項の手引きを適用するときにフェールセーフ設計の仕組みそれ自体の故障が検討されるべきである。

6.68. I&C 機器及び系統の非系統的故障モードは周知され、文書化されるべきである。

6.69. 系統へのフェールセーフ概念の適用においては機器の故障モードに関する知識が重要である。それはまた、制御系統の故障が安全解析の範囲外の事象を引き起こさないことを確認する際にも重要である。

6.70. ソフトウェアのエラーから生じることがある故障は予測することが難しい。そうであっても、装置の端末で見られる想定しうる故障状態を判断するために、ソフトウェアがどのように故障するかを知ることは必要ではない。一つの選択肢は、想定しうる故障モードを特定し、管理できる可能性群にグループ分けすることである（たとえば、間違った出力、出力の遅延及び出力のフリーズ）。

6.71. ハードウェア又はソフトウェアの設計に含まれる体系的な原因から発生する可能性が最も高い故障モードは本質的に予測不能である。したがって、そのような原因から発生する故障を扱うには、フェールセーフ設計の概念は効果的ではない。そのような原因の数を減らし、残るそのような原因の影響に対処することについては、統制された開発プロセス（第 2 章参照）、ハザード分析（2.56～2.65 項を参照）、深層防護の概念の適用（第 4 章参照）及び多様性の適用（6.57～6.63 項を参照）がより効果的なツールである。

6.72. I&C 機器の故障は、定期的な試験若しくは自己診断によって検知可能であるべきであるか又は警報若しくは異常指示によって自己表示できるべきである。

6.73. 故障は自己表示できることが望まれる。欠陥が自己表示できる仕組みにより、系統を安全でない状態におくべきでなく、又は安全系の偽起動にならないようにすべきである。

6.74. 定期的な試験、警報又は異常指示によって検知できない、あらゆる特定された故障は、単一故障基準との適合性を評価するときには、単一故障と併せて存在すると仮定されるべきである。自己試験機能、自己診断機能又は自己警報機能自体の故障が検知され明らかにされるべきである。

6.75. 実施可能な限り、機器の故障は安全系の誤作動を引き起こすべきではない。

6.76. I&C 安全系又は機器への電源を再起動又は復旧する際、有効な安全信号に対応中のものを除いて、出力はあらかじめ決められた安全な状態に初期化されるべきである。

設備の性能保証

6.77. SSR-2/1 (Rev. 1)[1] の要件 30 は次のよう述べている。

> 「原子力発電所の安全上重要な機器等が、設計寿命を通して、必要なときに及び代表的な環境条件下で、意図した機能を果たすことができることを検証するために、保守及び試験期間中の発電所状態を十分に考慮して、それらの機器等の性能保証プログラムが実行されなければならない。」

6.78. I&C 系及び機器は、その供用寿命期間中にわたる意図された機能に対して性能保証されるべきである。

6.79. I&C 機器の性能保証は、そのソフトウェア、ハードウェア記述言語及びプロセスの取合いがあれば、それを含むべきである。

6.80. 性能保証は、系統又は機器の安全上の重要性に見合った水準の確信度を提供すべきである。

6.81. 性能保証プログラムは、所定の機能に対する各々の系統又は機器の適性に影響を及ぼす全ての事項に対応するべきであり、これには以下を含む。

- 機能及び性能の適性及び正確さ
- 環境性能保証
- 内的及び外的ハザードの影響に対する性能保証
- 電磁気性能保証

6.82. 設備の性能保証は、下記の方法からの選択に基づくべきである。

- 認められた標準に適合した工学的プロセス及び製造プロセスの使用
- 信頼性の実証
- 類似の用途における過去の経験
- 型式試験
- 供給された設備の試験
- 試験結果又は関連する条件の下での運転経験を外挿することに関する分析
- 製造者の製造プロセスの評価
- 製造期間中の機器の検査

6.83. 上記の方法の全てを適用することは一般的に必要ではない。選択された方法の特定の組合せは、検討対象の系統又は機器に依存することになる。例えば、既に存在している機器等の性能保証では、設計中及び製造時の完全に文書化された検証及び妥当性確認の不足を補うように、過去の経験及び分析に対し、より重点が置かれることがある。

6.84. 設備の性能保証に使われる方法又は方法の組み合わせは、正当化されるべきである。

6.85. 設備の性能保証を支援するために運転経験が用いられる場合、提案される使用に対して適切であり、また、対象物適用の環境に対して適切であることが示されるべきである。

6.86. 安全系については、運転経験に基づく性能保証の証拠は、不十分であり、したがって、型式試験及び供給された設備の試験並びに製造者の製造プロセスの評価又は製造期間中の機器の検査と組み合わされるべきである。

6.87. 設備の性能保証に関する証拠の一部である分析には、使用された方法、原理及び仮定の正当性根拠を含むべきである。

6.88. 例えば、設備の性能保証に使われた数学モデルの有効性は、実験データ、試験データ又は運転経験に基づいて正当化されることがある。

6.89. 追跡可能性は、設置された安全上重要な系統及び機器の各々と性能保証についての適用できる証拠との間で確保されるべきである。

6.90. これには、機器自体の追跡可能性だけでなく、性能保証された構成と設置された構成との間の追跡可能性も含む。

適性及び正確さ

6.91. 設備の性能保証プログラムは、I&C 系及び機器の設計が、I&C 系及び機器ついての設計根拠及び設備仕様に含まれる、全ての機能要件、性能要件及び信頼性要件を満たしていることを実証すべきである。

6.92. 機能要件の例には、用途によって要求される機能性、系統又は設備の運転性を支援するために要求される機能性、運転員インターフェースに関わる要件及び入出力の範囲に関連する要求事項を含む。

6.93. 性能要件の例には、精度、分解能、範囲、データ採取頻度及び応答時間を含む。

6.94. 信頼性要件の例には、最小平均故障間隔に関する要件並びにフェールセーフ挙動、独立性、故障検知、試験可能性、保守性及び供用寿命に関する要件を含む。

6.95. 設備の性能保証プログラムは、実際の設計並びに実際に設置された I&C 系及び設置された機器が、性能保証された設計を正確に実装していることを実証するべきである。

環境性能保証

6.96. 本安全指針では、環境性能保証は、機器の適切な機能実行に影響を及ぼす、温度、圧力、湿度、化学ばく露、照射、浸水、電磁現象及び経年変化メカニズムに対する、当該条件下での性能保証である。

6.97. 系統及び機器は、機能することを要求される、通常運転、予期される運転時の事象及び想定される事故に付随する環境条件の影響に順応するように設計されるべきであり、また、その環境条件と両立できているべきである。

6.98. 機器は、指定された環境条件の範囲にさらされたとき、全ての要件を満たしていることが示されるべきである。

6.99. 設備の性能保証要件、プロセス及び方法の詳細は参考文献 [22] で与えられる。

穏やかな環境にのみさらされる機器

6.100. 事故時の供用環境条件が通常運転時の条件より大幅に厳しいことがけっしてない（いわゆる「穏やかな環境」）I&C 機器の環境性能保証は、所定の環境条件の下で機器がその要求された機能を実施することを示す供給者からの認証又は個別の評価とともに、発電

所の運転状態に伴う特定の環境条件に対する機能要件についての明確な仕様に基づく場合がある。

過酷な環境にさらされる機器

6.101. どの時間帯でも通常運転時の条件より大幅に厳しい供用環境条件（いわゆる「過酷な環境」）のなかで機能することを要求される機器の環境性能保証は、機器が、その性能保証寿命の終わりにおいて、指定された供用条件の全範囲の下でその安全機能を実施する能力があることを実証するべきである。

6.102. 機器がその性能保証寿命の終わりに要求に応じて機能することができることの実証には、性能保証寿命の終わりにおいても要求された機能性が維持されていることを示すために、顕著な経年変化の影響（例えば、放射線及び熱による経年変化）に対処していることを含む。これには通常、予期できない経年変化メカニズムを許容するために、適切な場合は更なる保守性を含む。

6.103. 設備の性能保証プログラムの仕様の中で、供用条件間の相乗効果を含め、供用環境条件の想定しうる最悪の組み合わせも取り組まれるべきである。

6.104. 様々な環境条件について別々に試験することが必要であれば（例えば、放射線と温度の影響についての個別試験）、当該の試験が行われる順序は、組み合わされた環境によって引き起こされる劣化を適切に模擬する試験としての正当性が示されるべきである。

6.105. 環境性能保証に対する最も厳格な方法は、安全分類された機器にのみ適用される必要がある場合がある。

6.106. 過酷な環境の下で作動することを要求される安全分類された機器の環境性能保証は、型式検査を含むべきである。

6.107. 想定しうる環境影響から設備を隔離するための防護障壁が設けられるときは、障壁自身がその妥当性を確認するために性能保証プログラムの対象とされるべきである。

内的ハザード及び外的ハザード

6.108. 発電所の設計基準及び発電所の安全解析は、発電所が運転に対する耐性を持っていることを要求されるか又は発電所が安全に耐えることを要求されており、また、それに対して防護又は系統性能保証が必要とされる、火災、溢水及び地震事象などの内的ハザード及び外的ハザードを特定することになる。また、発電所の設計基準及び発電所の安全解析は、安全機能の劣化につながる可能性がある、工学的決定又は不備などの体系的な原因によってもたらされるハザードも特定することになり、対応する系統の制約事項が安全機能の劣化を防ぐために特定されるべきである。

6.109. I&C 系及び機器は、NS-G-1.7[20]の手引きにしたがって火災及び爆発の影響に対して防護されるべきである。

6.110. I&C 系及び機器は、NS-G-1.11[21]の手引きにしたがって他の内的ハザードの影響に対して防護されるべきである。

6.111. I&C 系及び機器は、IAEA 安全基準シリーズ No. NS-G-1.6「原子力発電所の耐震設計及び耐震性能保証」[23] の手引きにしたがって、地震ハザードに耐えるために設計され、

性能保証されるべきである。

6.112. I&C 系及び機器は、IAEA 安全基準シリーズ No. NS-G-1.5「原子力発電所の設計における地震以外の外部事象」[24] の手引きにしたがって、他の外的ハザードに対して防護されるべきであるか又はそれに耐えるために設計され、性能保証されるべきである。

電磁気性能保証

6.113. 電磁両立性は、その環境中においていかなるものに対しても、耐えられない電磁気妨害をもたらすことなく、電磁環境の中で十分に機能する系統又は機器の能力である。電磁干渉に対する機器の感受性及び電磁環境に対する電磁干渉の寄与（電磁波の放出）は、電磁両立性の両面である。

6.114. 電磁干渉は、無線周波数干渉を含み、また、本安全指針で使われているように、電気サージ、例えば回路開閉時の過渡現象から生じる電圧スパイクを含む。

6.115. 電気系及び電子系の系統及び機器の外乱を受けない作動は、それらの作動環境との機器の電磁両立性、すなわち、周辺の機器又は接続された機器によって引き起こされる外乱に耐える機器の能力に依存する。

6.116. 電磁干渉の顕著な発生源は、開閉器、回路遮断器又はヒューズの作動による故障電流の遮断、無線発信機によって引き起こされる電場、落雷又は太陽嵐などの自然の発生源、及び発電所内外でのその他の人為的な発生源を含む。

6.117. I&C 系及び機器の電磁気性能保証は、I&C 機器に対する電磁ノイズの結合を最小限にするための系統及び機器の設計の組み合わせに依存し、また、予想されるレベルの電磁気放射に機器が耐えられることを実証するための試験及び電磁波放出が許容レベル内にあることを実証するための試験に依存する。

6.118. 電磁ノイズの発生及び結合を最小にする手法は、以下を含む。

- 発生源での電磁ノイズの抑制
- 電力ケーブルからの I&C 信号ケーブルの分離及び隔離
- 磁気放射及び電磁放射の外部発生源からの設備及びケーブルの遮蔽
- 感受性の高い電子回路に電磁ノイズが結合する前の電磁ノイズのフィルタによる除去
- 電子設備の接地電位差の解消又は隔離
- 電気設備及び I&C 設備、電線管、筐体、機器並びにケーブル遮蔽体の適切な接地

6.119. これらの方策の適切な適用及び有効性の継続には、適切な設置及び保守の実施が必須である。

6.120. 電磁両立性に対する詳細な要求事項は、安全系統及び機器に対して決定されるべきであり、要求事項に対する適合性は実証されるべきである。

6.121. 産業環境での電磁両立性に関する国際標準は、より要求の多いことがある発電所固有の電磁両立性の必要性を網羅するために必要な場合に補完されるのであれば、要求事項の根拠として役立つ場合がある。電磁両立性に関する要求事項の決定には、繰り返される過渡現象（例えば、誘導負荷の回路開放及びリレーの閉作動）及び高エネルギーサージ（例えば、電源障害及び落雷）に I&C 機器がさらされることになる可能性についての考慮を含む。

6.122. 原子力発電所の各号機の I&C 機器の電磁環境の設定は、一般的に各号機特定の分析を含む。これら分析は、各 I&C 機器の電磁両立性の妥当性を判断するために使われる。

6.123. 安全上重要な設備及び系統は、付随するケーブルを含め、それらが配置される場所の電磁環境に耐えるように設計、設置されるべきである。

6.124. I&C 系及び機器の設計において考慮されるべき電磁干渉に関する側面は次のものを含む。

— 電磁妨害の発生及びそれに対する耐性
— ケーブルを介した電磁妨害の発生及び伝播
— 静電放電
— 回路開閉の過渡現象及びサージ
— 発電所で使われる無線による系統及び装置[25]並びに修理、保守及び測定装置の電磁波放出特性

6.125. ある感受性の高い設備の近傍では、無線装置及び他の可搬式の電磁干渉源（溶接装置など）の操作が制限される除外区域が設定されるべきである。

6.126. 設備の性能保証プログラムは、電磁干渉及び耐サージ能力に関する作動限界範囲によって定められた制限値にさらされたときに、安全分類された I&C 機器がその安全機能を実施する能力があることを実証するべきである。

6.127. 全ての発電所設備について、放射及び誘導された電磁波放出に関する制限値が設定されるべきである。

6.128. 発電所のいかなる電気設備又は電子設備も電磁環境に影響を与えることになる。したがって、電磁波放出を制限する必要性は、安全上重要と分類された設備のみでなく、全ての発電所設備に適用するべきである。

6.129. 個々の機器に課された放出制約は、モード又は状態を跨ぐ切り替え及び劣化した条件を含む、系統及び機器の全てのモード及び状態において作動環境中で結果的に発生する電磁波放出が、全ての機器の電磁干渉に関して安全な（ハザードのない）上限範囲内にあるべきである。

6.130. 設備の性能保証プログラムは、全ての発電所設備の電磁波放出が定められた制限値内にあることを実証するべきである。

6.131. 設備及び系統は、付属するケーブル及び電源を含めて、発電所設備間での電磁干渉の（放射及び伝導の両方による）伝搬を適切に制限するように設計、設置されるべきである。

6.132. いくつかの I&C 系が同じ電源に接続されているときには、電磁気性能保証は、電磁干渉の伝達経路を評価すべきである。

6.133. 計測ケーブルはツイストペアであるべきであり、また、電磁干渉及び静電気干渉を最小化するため遮蔽されるべきである。

6.134. SSG-34 [7] は、電磁干渉の発生及び伝播を低下させるための接地、ケーブルの選択並びにケーブル配線に関する推奨事項を提示している。

[25] 無線システムと装置は、例えば移動電話、トランシーバー、無線データ通信ネットワークを含む。

経年変化及び旧式化に対処するための設計

6.135. SSR-2/1 (Rev. 1)[1] の要件 31 は次のように述べている。

> 「原子力発電所において安全上重要な機器等の設計寿命が決定されなければならない。安全上重要な機器等が設計寿命を通して必要な安全機能を果たす能力を確実なものとするために、経年変化、中性子脆化及び摩耗のメカニズム並びに潜在的な経年変化による劣化の可能性を十分に考慮し、設計では適切な安全余裕が与えられなければならない。」

6.136. SSR-2/1 (Rev. 1)[1] の 5.51 項は次のように述べている。

> 「原子力発電所の設計は、試験、保守、保守停止時、想定起因事象の発生時の発電所状態及び発生後の発電所状態を含めて、機器が保証されるべき全ての運転状態において経年変化及び摩耗の影響を十分に考慮しなければならない。」

6.137. SSR-2/1 (Rev. 1)[1] の 5.52 項は次のように述べている。

> 「設計段階で予測される経年変化のメカニズムを評価するために、また、発電所の予期しない挙動又は供用中に生じることがある劣化の識別を支援するために、監視、試験、試料採取及び検査のための措置が講じられなければならない。」

6.138. 電気及び電子系及び機器の性能保証された供用寿命は、発電所の寿命に比べてかなり短いことがある。

6.139. 過酷な環境条件の下で機器が機能する能力を損なう経年変化関連の劣化は、通常条件下での機器の機能上の能力が顕著に影響を受けるより前、十分に早い時期に発生することがある。

6.140. I&C 機器に大きな影響を与える可能性がある経年変化メカニズム及びこれらのメカニズムの影響を追跡調査する手段は、設計期間中に特定されるべきである。

6.141. 経年変化による影響の可能性の特定は、最初に、様々な I&C 機器に対して関連する経年変化現象についての理解を伴う。

6.142. I&C 機器の経年変化は、ほとんどの場合、熱又は放射線にさらされることによる。それでもなお、6.140 項の手引きを適用するときには、他の現象（例えば、超小型回路中の電子による金属移動、錫メッキ表面の繊維状ヒゲの形成、機械的振動又は化学的劣化）が特定の機器に関連していることがあるという可能性が考慮されるべきである。

6.143. 保守プログラムは、設備がその安全機能を実施できなくなる原因となる可能性のある前兆事象の検知を含めて、あらゆる劣化（経年変化）傾向の特定のための作業を含むべきである。

6.144. 監視手法の例は以下を含む。

- 経年変化が性能の劣化に影響を与える代表的な発電所機器又は代表的な機器群の適正な時間間隔での試験
- 目視検査
- 運転経験の分析

6.145. 経年変化の影響に対処する手段の例は以下を含む。

- 性能保証寿命の終了前の機器の交換
- 経年変化の影響に対処するための機能特性の調整（再較正など）
- 経年変化プロセスを遅くする効果がある保守手順書又は環境条件への変更

6.146. 過酷な環境の下で安全機能を実施することが要求される安全分類された機器の性能保証寿命は決められるべきである。

6.147. 安全分類された機器は、その性能保証寿命の終了前に交換されるべきである。

6.148. 実施中の性能保証は、機器の性能保証寿命が有効とされること、又は機器の性能保証寿命が試験の実施、分析若しくは経験により判断された性能保証寿命と異なっていると表示されること、を示すことがある。実施中の性能保証からの情報は機器の性能保証寿命を延長又は短縮するために用いられる場合がある。

6.149. I&C 系及び機器の予期される供用寿命並びに予期される旧式化は、設計期間中に特定されるべきであり、また、運転組織に伝えられるべきである。

6.150. I&C 系及び機器の供用寿命の推定及び旧式化の予想される時期は、運転組織に対し、供給者との長期的な契約を結ぶこと、余分の予備部品の取得の計画を立てること及び旧式化した機器等の適切な時期の交換を計画することを必要とするとの情報を提供する。

6.151. 経年変化又は旧式化が、一部の I&C 系の供用寿命を、発電所の存続期間に比べて大幅に短くしてしまう場合があることが予測される。したがって、交換用系統の設置及びそれへの切り換えを促進することになる仕組みを備えることが適切であることがある。そのような施設は、新しい設備及び付随するケーブルの設置用に予定された場所を含むことがある。

6.152. IAEA の安全基準シリーズ No. NS-G-2.12「原子力発電所の経年変化管理」[25] は、経年変化管理及び旧式化管理に関する追加的な手引きを提示している。それは、設備の性能保証プログラムと経年変化管理プログラムとの間の取合いの説明を含んでいる。

安全上重要な系統への立入りの管理

6.153. SSR-2/1 (Rev. 1)[1] の要件 39 は次のように述べている、すなわち、コンピュータのハードウェア及びソフトウェアを含む安全上重要な機器等への無許可の立入り又は妨害は、防止されなければならない。

6.154. 参考文献 [26～28] は、原子力発電所のセキュリティ及び安全と核セキュリティとの調和に関する手引きを提示している。

6.155. I&C 系の設備への立ち入りは、無許可の立ち入りの防止のために及び過誤の可能性を低減するために制限されるべきである。

6.156. 効果的な方法は、管理面の対策と物理的セキュリティとの適切な組み合わせ（例えば、筐体の施錠、部屋の施錠、筐体の扉の警報など）を含む。

6.157. 特に懸念される分野は、運転又は保守の過誤による系統の性能劣化を防止することの重要性から、設定値調整、較正による調整及び構成データへの立ち入りである。

6.158. 7.103～7.130 項は、デジタルシステムへの電子的立入りの制御に対する追加的な手引きを提示している。

運転時の試験及び試験可能性

6.159. SSR-2/1 (Rev. 1)[1] の要件 29 は次のように述べている。

「原子力発電所における安全上重要な機器等は、設計基準で規定された全ての状態に

おいて、それらの機能を果たす能力を確実なものとし、それらの健全性を維持するために要求されたように、較正、試験、保守、修理又は交換、検査及び監視されるべく設計されなければならない。」

6.160.　SSR-2/1 (Rev. 1)[1] の 6.35 項は次のように述べている。

「安全系は、発電所が運転中に、多重性の故障と喪失を検出するためにチャンネルを独立して検査できる可能性を含めて、安全系の機能性を定期的に検査できるように設計されなければならない。設計は、測定器、入力信号、最終段の起動装置及び表示装置に対する機能検査の全ての側面を可能としなければならない。」

試験装備

6.161.　I&C 系は、試験実施用の装備を含むべきである。

6.162.　安全系に恒久的に接続されている試験装備は、6.25～6.56 項に記された独立性に関係する推奨事項を満たさない限り、それら自体が安全系である。

6.163.　出力運転を含む全ての通常運転モードの下で、安全系が安全機能を果たす能力が保持されつつ、安全系の設備の試験及び較正が可能であるべきである。

6.164.　通常、発電所運転期間中の定期的な試験は、安全系に要求される信頼性を達成するために必要である。しかし、この試験が発電所の安全を危険状態に置くおそれがある場合は、出力運転中の試験実施を避けることが望ましいときもある。出力運転中の試験実施及び較正の利点は、発電所の安全に対して引き起こす場合がある不利な影響との釣り合いが取られるべきである

6.165.　出力運転中に安全系又は機器を試験する能力が備えられていない場合は、下記が確保されるべきである。

- 影響を受ける機能の信頼性が試験間隔を超えて容認できると示されるべきである。
- 試験されない機器の精度及び安定性が試験間隔を超えて要件を満たしていると示されるべきである。
- 試験されない計測チャンネルの測定値を他の装置と比較する（例えば中性子出力と熱出力を比較する）手段の具備に考慮が払われるべきである。
- 試験されない系統又は機器を停止期間中に試験する能力が備えられるべきである。

自動試験、自己観察及び監視

6.166.　I&C 系は、継続的で正しい動作の定常的な確認をできる、自己観察又は監視の仕組みを有するべきである。

6.167.　そのような仕組みは、入力情報の合理性を点検する手段を含むべきである。

6.168.　デジタル安全系は、ウオッチドッグタイマーなどの安全状態用の仕組みを含むべきである。

6.169.　故障が自己表示されるようにする系統又は機器の設計は、6.166 項の推奨事項を達成する 1 つの手段である。

6.170.　試験施設は、試験の実施及び関連する試験の一連操作を、手動で開始されるか自動的に開始されるかに関係なく、実施するために備えられるハードウェア及びソフトウェアを含む。

6.171. 安全系の多重性の喪失を示す警報装置が設けられるべきである。

6.172. 系統又は設備の欠陥が自己観察によって検知されたときは、あらかじめ決められた措置が取られるべきである。

試験実施中に計測制御系機能を維持すること

6.173. SSR-2/1 (Rev. 1)[1] の 5.46 項は次のように述べている。

> 「安全上重要な機器等が出力運転中に較正、試験又は保守されるように計画されている場合には、それぞれの系統は、安全機能の実施信頼度において有意な低下を招くことなくその業務を実行するように設計されなければならない。停止期間中での安全上重要な機器等の較正、試験、保守、修理、交換又は検査に対する方策は、こうした業務が安全機能の遂行の信頼度の面で有意な低下を招くことなく実施され得るように、設計に含められなければならない。」

6.174. I&C 系のための試験装備（手動装備と自動装備の両者）は、試験の実施が、I&C 系がその安全機能を実施する能力に悪影響を及ぼさないことを確保するように、また、安全動作の擬似的な開始の可能性及び試験による発電所の稼働性への他の悪影響を最小化するように、設計されるべきである。

6.175. 試験実施のための準備は、安全系の独立性を損なうべきでなく、また、共通原因故障の可能性を持ち込まないようにすべきである。

6.176. 試験のための準備は、手順書、試験の取合い、設置された試験設備及びあらかじめ組み込まれた試験施設を含む。

試験の取合い

6.177. SSR-2/1 (Rev. 1)[1] の 5.45 項は次のように述べている。

> 「発電所の配置は、較正、試験、保守、修理又は交換、検査及び監視の作業が容易であり、また、関連の国内及び国際的な規格基準にしたがって実施されるようであらねばならない。こうした作業は、果たされるべき安全機能の重要度に見合ったものでなければならず、また、作業者が過度の被ばくを受けることなく実施されなければならない。」

6.178. I&C 系及び機器を試験するための装備は、以下の特性を持つべきである。

- 当該の装備は、適切な試験の取合い[26]及び状態表示の手段を有するべきである。
- 当該の装備は、設備の欠陥が容易に検知できるよう作動するべきである。
- 当該の装備は、無許可の立ち入りを防止する仕組みを有するべきである。
- 当該の装備は、試験実施職員及び試験設備にとって容易に近接できるべきである。
- 当該の装備は、試験を支援するために必要な情報伝達施設を有しているべきである。
- 当該の装備は、試験の実施又は試験実施場所への近接が、運転要員を危険性のある環境にさらすことがないように配置されるべきである。[27]

---

[26] 例えば、模擬プロセス条件又は模擬電気信号を取り入れる能力を備えた試験の取合い

[27] 試験用の装備の場所を決める際の考慮事項例には次のものがある。
- 試験及び較正がその場で実施できるような検出器の場所

6.179.　試験される設備が危険性のある区域に設置されている場所では、危険性のある区域の外から試験が制御されるような備えがなされるべきである。

試験プログラム

6.180.　I&C 系の設計は、関連する IAEA 安全指針 [16 及び 29～31] で示された推奨事項の適用を支援する試験及び較正プログラムの仕様を含むべきである。

6.181.　I&C 系試験プログラムは、通常、以下を含む。

- プログラムの目的の説明
- 試験されるべき系統及びチャンネルの仕様
- 個々の試験の頻度及び実施順序
- 行なわれるべき試験及び試験間隔の理由及び正当性根拠
- 要求される文書及び報告書の説明
- 試験の合否判断基準及びそれら判断基準に対する不適合の処理プロセス
- 試験プログラムの有効性の定期的な見直しに関する要件
- 試験の実施を管理するために使われることになる個々の試験手順書についての仕様

6.182.　試験及び較正の範囲及び頻度は、機能要件及び稼働性要件に一致していると正当化されるべきである。

6.183.　試験プログラムは、試験中及び試験後に、下記の条件が満たされていることを確認すべきである。

- 系統の全体的な機能上の能力が劣化されてないこと
- I&C 安全系がその機能要件及び性能要件を満たし続けること

6.184.　試験プログラムでは、試験は他の機器又は系統の更なる試験なしで、試験中の系統又は機器の全体的な状態が直ちに評価できるような順序で準備されるべきである

6.185.　試験プログラムの実施は、いかなる発電所の機器についても、設計で決められた以上の劣化を生じないようにすべきである。

6.186.　試験プログラムの実施時に及び機器の性能保証寿命の終りに達する時点についての判断に至る際に、例えば、試験することによる摩耗及び経年変化を考慮することが必要である場合がある。

6.187.　試験プログラムは、次の事項を提示するべきである。

- 系統又は機器の状態に関する客観的な情報
- 機器の劣化に関する評価
- 劣化を検知する際に役立つ傾向に関するデータ
- 系統内の初期故障の兆候
- 失敗した試験の繰り返しが運転性を設定するものとして正当化される前に行われる

- 試験される設備に便利な区域内の試験装置と試験設備の場所
- 試験される機器の場所へ試験設備を持ち込むことを困難にする可能性のある発電所の仕組み又は管理面の仕組み。例えば、狭い通路に沿って又は汚染区域を出入りして設備を移動する必要性
- 機器及び試験接続の状態表示の利便性

べき評価に関する要件[28]

6.188. 試験プログラムは、定期的な試験及び較正のための以下のプロセスを定めるべきである。

- 検出器から起動装置までの安全機能の全面的な点検を規定するプロセス
- その場で実施できるプロセス
- 設備の機能要件及び性能要件が満たされていることを確認するプロセス
- 系統信頼性に関する要件及び機能要件を満足させために必要な範囲で、警報装置、指示計、制御動作及び起動用の装置の運転などの入出力機能を試験するプロセス
- 各試験の期待される結果を定めるプロセス
- 試験中の発電所の安全性を確保するプロセス
- あらゆる安全動作の擬似的な開始の可能性を最小化する、また、試験による発電所稼働性へのその他のあらゆる悪影響を最小化するプロセス
- その場しのぎの試験設定の使用、一時的なジャンパー又はコンピュータコードの一時的な変更を禁止するプロセス[29]
- 構成パラメータが前もって点検用パラメータと特定されていない限り、発電所機器の構成パラメータの変更を禁止するプロセス
- 設備が供用から外される時間間隔を最小化するプロセス
- 実際にできる範囲で、各検出器を個々に試験するプロセス

6.189. 6.188 項の推奨事項に加えて、安全系の定期的な試験及び較正に対して定められたプロセスは、

- 単一のオンライン試験であるべきである[30]。
- 各チャンネルの検出機能、命令機能、実行機能及び支援機能に関する、機能要件及び性能要件を単独に確認すべきである。
- 発電所の継続的な通常運転を損なうことなく、試験の下で、実際にできるだけ多くの機能（検出器と起動装置を含む）を含むべきである。
- 可能なところはどこでも、運転の一連操作を含めて、実際の又は模擬の運転状況の下で遂行されるべきである。
- 安全系のための特定の信号を生成するために変数の組み合わせが使われる場合は、使われる全ての変数を試験し、較正すべきである。
- 多重性を持つ設備の欠陥を検知できるべきである[31]。

6.190. 単一のオンライン試験が実施できないときには、試験プログラムは、試験の目的を達成するために、重複する試験を組み合わせる場合がある。安全系のチャンネルのために単一のオンライン試験が行われない場合、重複する試験の使用に対する正当化文書が提示されるべきである。

6.191. 正当化は一般的に、重複する試験が完全に網羅していること、より長い試験間隔があっても設備の信頼性が容認できること、また、オンラインで試験が行われなかったいか

---

[28] 繰り返し試験の結果が、当該の系統又は機器の作動性を実証するために使用される前に、失敗した試験についての理由、その根本原因及びその後に取られた措置の評価及び文書化が通常は必要である。是正措置は、機器の保守若しくは修理又は試験手順の変更を含む場合がある。是正措置が不要と判断された場合は、理由が文書化されることになる。

[29] 試験設備は、試験される設備が当該試験設備の接続のために特別に設計された施設を持つ場合、一時的に発電所設備に接続される場合がある。定期的な試験又は較正のために一時的な接続が要求される場合には、そのような設備の接続及び使用は適切な運営管理に従うことになる。

[30] そのようなオンライン試験は、試験用の接続をする必要なく又は制限された時間以上にオンライン設備若しくはその動作を妨害せずに、特定の欠陥をその発生時点で直接特定できることになる。

[31] 多重な設備は、多重な区分内の設備又は 1 つの区分内の多重な設備であることがある。

なる機器も発電所の停止時に試験が行われること、を実証ことになる。

保守性

6.192. I&C 系の設計は、全ての系統及び機器に関する保守計画を含むべきである。

6.193. I&C 系及び機器は、運転要員に対するリスクを最小化するように、また、必要な予防保全、不具合対応及び時宜にかなった修理を容易にするように、設計され、配置され、組み立てられるべきである。

6.194. 保守、不具合対応及び修理を容易にする設計は次のことを含む。

- 発電所の通常運転時に極端な温度又は湿度条件が予想される区域に設備を置くことを避けること。
- 高い放射線レベルのリスクがある区域に設備を置くことを避けること（IAEA の安全基準シリーズ No. NS-G-1.13「原子力発電所の設計の放射線防護面」[32] を参照）。
- 保守作業の実施において、人の能力と限界を考慮に入れること。
- 通常の作業条件の下で保守職員が業務を実施できることを確実なものとするために設備の周りに十分な空間を残すこと。

6.195. 機器が近接できない場所に置かれている場合、故障に対処する他の方針の例は以下のものを含む。

- 予備の多重装置の設置
- 遠隔保守のための施設
- 設備が故障し、迅速かつ容易に修理又は交換ができないのであれば、出力を下げての発電所の運転に対する計画立案

6.196. I&C 系の保守に備えられる手段は、発電所の安全に対するいかなる影響も容認できるように設計されるべきである。

6.197. そのような手段の代表例は、いくつかの多重区分を持つ系統の 1 つの区分を切り離すこと又は代替の手動操作を実行する装備である。

試験の実施又は保守のための供用除外の方策

6.198. 試験実施又は保守のための施設の使用が I&C 機能を損ない得るのであれば、試験する系統又は保守する系統との相互作用が手動による慎重な介入なしには可能でないことを確実なものとするために、取り合い箇所は、ハードウェアによるインターロック設置の対象であるべきである。

6.199. 設計は、系統が知らないままに試験又は保守の構成で放置されることがないことを確実なものとするべきである。

6.200. 安全系のいずれかの単一機器又は多重系のいずれかの区分の供用からの取り外しが要求される最低限の多重性の喪失につながらないようにすべきである。ただし、容認できる信頼性のある系統運転が適切に実証できる場合はこの限りでない。

6.201. SSR-2/1 (Rev. 1)[1] の 6.36 項は次のように述べている。

> 「安全系又は安全系の一部が試験のために供用から外されなければならない場合は、試験又は保守活動の間に必要とされる保護系のバイパスの全てを明確に表示するのに十分な対策が取られなければならない。」

6.202. 安全系の機器若しくは区分の不作動又はバイパスは制御室に表示されるべきである。

6.203. 頻繁にバイパスされる又は頻繁に動作不能にさせられる機器等については、これらの表示は自動的であるべきである。

6.204. NS-G-2.6 [16] は、試験又は保守の後の系統及び設備の供用状態への復旧に関する手引きを示している。

設定値

6.205. SSR-2/1 (Rev. 1)[1] の 5.44(b) 項は、「この要件並びに原子力発電所の設計で定められた運転上の制限及び条件は、……安全系に関する制限の設定……を含まなければならない。」と述べている。

6.206. 安全な運転のための運転上の制限値及び条件は、安全系に関する I&C の設定値を含む。

6.207. 安全系に関する I&C の設定値の決定は、通常、次の値を考慮する。

- 安全限界値。運転パラメータの限界値[32]であって、発電所の運転はその範囲内で安全であると示されるもの。
- （設定値の）解析上の限界値。安全解析によって設定された変数の測定値又は計算値の限度[33]であって、安全限界値が超過されていないことを保証するためのもの。
- トリップ設定値。保護動作を開始するため、最終設定値装置の起動のためにあらかじめ決定された値。
- 許容値。定期的に試験されるときに設定値がとり得る限界の値であって、超えた場合は適切な操作が必要になる値。ある設定値がその許容値を超えていることを見つけると、そのチャンネルが設定値解析の仮定範囲内で動作していなかったことを意味する場合がある。この場合は、運転上の制限値と条件の違反があったかをどうかを、また、もし何らかの違反があれば、そのチャンネルを作動状態に復旧するためにどういう措置が必要とされるかを判断する必要がある。
- 安全系の限界設定値。予期される運転時の事象又は事故状態の発生時に、安全限界値が超過するのを防止するために、保護装置が自動的に起動されるレベル[34]。

6.208. 定期的な試験中に測定された設定値は、前回の設定からの変動幅が、不確かさ解析において用いられる予想値と整合していることを確認するために評価されるべきである。許容値の違反に到らない過大な変動幅（例えば、保守的な方向への変動）は、そのチャンネルが期待どおりに振る舞っていないこと及び設備が修理される必要があるか又は解析が改訂される必要があるかのいずれかであるとの表示であることがある。

6.209. 図 3 は、これらの用語とトリップ設定値及び許容値の根拠を確定する際に通常考慮される測定の不確かさ及び動作点設定の種類との相互関係を図示している。

---

[32] 安全制限値は I&C 系によって直接測定可能でないパラメータで与えられることもある。

[33] 解析上の制限値と安全限界値との間の余裕は、計測チャンネルの応答時間及び当該の事故による過渡現象の範囲を考慮に含める。

[34] 「安全系の限界設定値」は「安全系設定値」又は「限界安全系設定値」とも呼ばれ、いくつかの加盟国では法律用語になっている。これらは、トリップ設定値、許容値又はその両方として表されることもある。IAEA の安全基準シリーズ No. NS-G-2.2「原子力発電所の運転制限値及び条件並びに運転手順書」[29]は、安全系の設定値の確定及び実装に関する追加手引きを提示している。

6.210.　設定値は、固定値であるか又は他の発電所パラメータ若しくは条件に依存する可変値である。

6.211. 安全動作を開始するために使われるトリップ設定値は、監視されている変数が解析上の限界値に達する前に、要求される緩和動作が起きることを確実なものとするために選定されるべきである。

6.212.　安全系に関する限界設定値は、測定用の動作点設定、チャンネル動作点設定、不確かさ及び時間の経過に伴って生じるこれらのあらゆる変化を考慮に入れるために、トリップ設定値と解析上の限界との間に十分な余裕を与える、文書化された方法を用いて計算されるべきである。

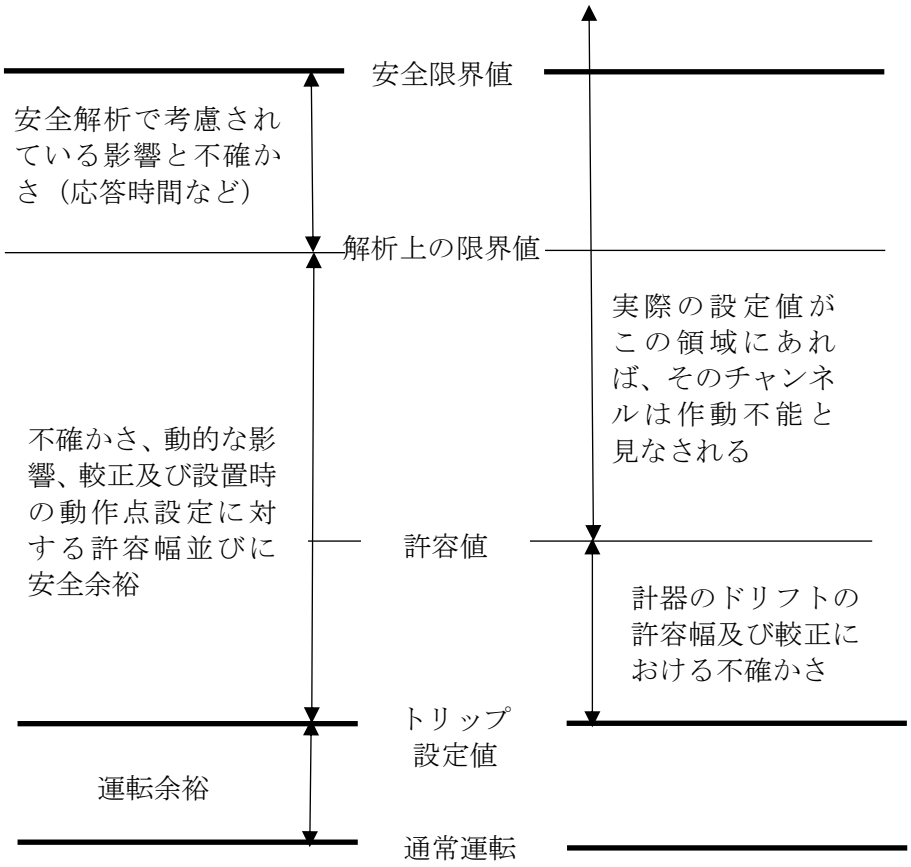

図3　設定値に関する用語と設定値の決定の際に考慮されるべき誤差

安全上重要な機器等の標識と識別確認

6.213.　全ての I&C 系機器を命名及び識別することについての、また、ヒューマンマシンインターフェースの記述的表題として使うための、整合性があり、一貫性があり、かつ理解されやすい方法が、決定され、発電所の寿命期間中の設計、設置及び運転の段階にわたって守られるべきである。

6.214.　適切な識別方法は、図面、マニュアル又は他の資料の頻繁な参照を要するべきでない。

6.215.　系統及び機器の一貫性があり理解されやすい命名及び識別は、制御装置、表示装置及び指示装置の標識付けの際の使用と同様に、技術職員、保守職員及び建設職員にとって重要である。

6.216.　発電所の I&C 機器は、一般に、それらの識別情報で標識付けられるべきである。設備若しくは集成物の内部に取り付けられた機器又はモジュールについては、それ自身の識別を必要としない。そのような機器、モジュール及びコンピュータソフトウェアの識別の維持のためには、一般的に、構成管理で十分である。

6.217.　安全の異なる区分に属する機器は、互いに、及び、より低い安全クラスの機器から、容易に区別できるべきである。

6.218.　機器の明確な識別は、正しくないチャンネルに対する、保守、試験、修理又は較正の不注意な実施の可能性を減らす。

6.219. 識別は、タグ付け又は色彩による識別の形をとる場合がある。

7. 個別の計測制御系及び設備に対する設計手引き

検出装置

7.1. 発電所の変動量の測定は、I&C 系及び発電所に対する設計基準の要件と整合しているべきである。

7.2. 発電所の変動量の測定は、測定範囲内での変数の現在値の測定及びリミットスイッチ、補助リレーの接点位置並びに温度、圧力、流量又は水位のスイッチによって検知されるような離散的な状態の検出の両者を含む。

7.3. 発電所の変動量の測定は、直接測定又は複数の測定に基づく計算若しくは目的の変数との関係が既知の他のデータの測定に基づく変数の値の決定などの間接測定によりなされる場合がある。

7.4. 実行可能な範囲で、発電所の状態は、間接測定に基づいて推定されるより、直接測定によって監視されるべきである。

7.5. 各監視対象変数の検出器及びその測定範囲は、検出器からの情報が必要とされる全ての発電所状態で変数を監視するために必要な、精度、応答時間、動作環境及び範囲に基づいて選択されるべきである。検出器及び起動装置の設計に際して、設計余裕が考慮されるべきである。

7.6. 検出器の共通原因故障の影響は 4.30～4.34 項に記された分析に含まれるべきである。

7.7. 検出装置の共通原因故障に対する特定された脆弱性が、運転員が事故を制御し、その影響を緩和するために必要とする情報及びパラメータを与えられない可能性がないようにすべきである。

7.8. 監視対象の変数の全範囲を網羅するために 2 つ以上の検出器が必要であれば、信号応答曲線における信号の飽和又は折り重ねの影響が要求される機能の実施を妨げないことを保証するため、一つの検出器から別の検出器への移行点ごとに合理性のある重複範囲が備えられるべきである。

7.9. 変数の測定において空間依存性（変数の測定値が検出器の位置に依存すること）が I&C 機能上重要であれば、検出器の必要最小数及び設置位置が識別されるべきである。

制御系

7.10. SSR-2/1 (Rev. 1)[1]の要件 60 は、「関連するプロセス変数を定められた運転範囲内に維持及び制限するために、原子力発電所に適切で信頼性のある制御系が設けられなければならない。」と述べている。

7.11. 主要なプロセス変数を運転制限値内に維持する自動制御は、発電所の深層防護の一部であり、したがって、関連する制御系は、通常、安全上重要な系統となる。

7.12. 制御系は、自動制御モード及び手動制御モードとの間の円滑な移行及び自動モード時に使用中プロセッサと予備プロセッサとの切り換えが発生した場合の円滑な移行に備え

るべきである。

7.13. 制御機能への電源喪失は、予備設備への円滑な移行又は警報を伴う起動装置の現状保持停止及び運転員による手動制御につながるべきである。

7.14. 自動制御系の故障の影響が、設計基準事故に対して設定された容認基準又は想定を超える状態を作りだすべきではない。制御系の複数の偽動作のような故障モードも、そのような故障の可能性が特定の系統設計に対して存在する場合は検討されるべきである。細分化構成などの適切な設計対策は、制御系の複数の偽動作発生可能性を排除する手段又はそれらの発生可能性を容認できるレベルにまで下げる手段として使うことができる。

保護系

7.15. SSR-2/1 (Rev. 1)[1] の要件 61 は次のように述べている。

> 「安全でない発電所状態を検知する能力及び安全な発電所状態を達成し維持するために必要な安全系を作動するために、自動的に安全措置を開始させる能力を備えた保護系が原子力発電所に設けられなければならない。」

7.16. 保護系は、発電所パラメータを設計基準事故に対して定められた制限値内に維持するように、発電所の変動量を監視し、指定された制限値からの変数の逸脱を検知すべきである。

7.17. 保護系全体はいくつかの系統を含む場合がある。

自動的な安全操作及び手動による安全操作

7.18. SSR-2/1 (Rev. 1)[1] の 6.33(b) 項は次のように述べている。

> 「[保護系の] 設計は、‥‥予期される運転時の事象又は事故状態の開始から正当化された期間内は、運転員の操作が必要とならないように、安全系を起動するための様々な安全操作を自動化しなければならない。‥‥」

7.19. 手動操作だけが正当と認められているもの以外は、保護系の全ての安全動作を自動的に開始し、制御するための手段が備えられるべきである。

7.20. 通常、保護系のほとんどの機能に自動的な開始が備えられることになる。

7.21. 手動操作のみが正当と認められることがある状況の例は、以下を含む。

- 自動操作手順の完了後の一定の安全タスクの開始
- 事故後、長期間にわたって発電所を安全な状態にするための制御操作
- 想定起因事象の後、相応な時間が経過するまで要求されない安全動作の開始

7.22. 手動操作のみが容認されることを正当化するためは、次の要件が適用され、これら要件が満たされていることが実証されるべきである。

- 安全系は、明確に提示され、かつ、要求される安全動作を開始する必要性について運転員が合理的な判断をできるのに十分な情報を運転員に提供すべきである。
- 運転員は、安全タスクに関する書式の手順書及び訓練を提供されるべきである。
- 運転員は、要求される操作を実施するために十分な発電所制御の手段を提供されるべきである。
- 操作を行う運転員の間の通信リンクは、運転員による操作が正しく完遂されること

を確保するのに適切であるべきである。

- 想定起因事象のそれぞれについて発電所の状態が推奨される容認基準内に維持できることを保証するために適した人間工学解析が実施されるべきである。
- 運転員は、発電所の状態を評価するため、また、要求される操作を完了するため十分な時間を認められるべきである[35]。関連するタイミング解析は、利用可能な時間及び運転員の必要な各々の操作のために要求される時間を考慮に入れるべきである。タイミング解析は安全余裕を決定し、また、安全余裕が減少するのに応じて、これらの時間の差を推定する際の不確かさが適切に考慮されるべきである。

7.23. 機械的な安全系及び自らの安全機能の実施を開始し、制御するために必要な個々の機器を手動で開始するための手段が提供されるべきである。

7.24. 機械的な安全系の安全機能を開始するための手動信号は、実用的にできる限り最終の起動用の装置に近いところで投入されるべきである。

7.25. 安全操作の手動開始は、予期される運転時の事象及び事故状態に対する深層防護の一形態を提供しており、また、事故後の発電所の長期的な運転を支援する。

7.26. 機械的な安全系は、例えば、制御棒の個々の区分、非常用給水、非常用炉心冷却又は格納容器隔離である。

情報の表示

7.27. SSR-2/1 (Rev. 1)[1] の 6.33(c) 項は、「[保護系の]設計は、‥‥‥自動操作の影響を監視するために、運転員に関連情報を利用できるようにしなければならない。」と述べている。

7.28. 保護系は、発電所運転員に対し、保護系の機能に用いられる各入力パラメータの測定値、区分ごとの各停止機能及び起動機能の状況並びに各系統の開始の状況を利用できるようにするべきである。

保護系の検出器と設定値

7.29. 保護系に信号を提供する検出器は、適切な緩衝装置及び隔離装置を通してのみ他の系統に信号供給するべきである。

7.30. 保護系の機能喪失を防止するために、機能面の多様性、多重性及び信号の多様性などの設計手法は実用的に可能な範囲で使用されるべきである。

7.31. 保護系の機能のために（例えば出力の上昇又は降下に対して許容するために）複数の設定値が必要とされる場合には、設計は、発電所の状態が制限の少ない設定値の使用に対して適さなくなったときに、より制限された設定値が自動的に使用されるか又は管理的手段によって課されることを確実なものとするべきである。

7.32. 特定の運転モード又は運転条件の組合せに対して適切な保護を達成するために複数の設定値を設けることが時には望ましいことがある。

7.33. 設計が可変設定値を使用しているか又は保護系が動作可能であることを要求され

[35] 新しい設計又は大幅な改造の場合には、設計基準事故発生後の最初の 30 分間は発電所パラメータを決められた制限値内に維持するための運転員による操作が必要ないように発電所を設計することが望ましい。

ているときに設定値を変更する能力を備えているのであれば、設定値を可変とするか又は変更するために使われる装置は、保護系の一部であるべきである。

7.34. 保護系は、保護系の各チャンネルの設定値を決めるための手段を備えるべきである。

運転時バイパス

7.35. 特定の発電所の状態時に保護系機能の起動を抑止するため、運転時バイパス又はトリップ条件ロジックが必要になることがある。例えば、起動中に原子炉出力を制限するトリップは、低出力トリップ設定値を超えて出力上昇を許容するために、ある点でバイパスされることは運転上の必要性である。

7.36. 運転時バイパスが必要な場合、運転時バイパスが作動される必要がある状態に発電所が近づきつつあるときに、運転員は適切な警告又は警報を提供されるべきである。

7.37. 運転時バイパスの状態の表示は制御室に備えられるべきである。

7.38. 保護系は、発動された運転時バイパスに対する条件が満たされていないのであれば、次の操作のうちの 1 つを自動的に実行すべきである。

- 発動された運転時バイパスの撤回
- 運転時バイパスが許される状態に発電所を置くこと、又は
- 適切な保護操作の開始

保護系機能の自己保持性

7.39. SSR-2/1 (Rev. 1)[1] の 6.33(a) 項は次のように述べている。

> 「[保護系の] 設計‥‥‥運転状態及び事故状態において、保護系の有効性を損なう可能性のある運転員の操作を防止しなければならないが、事故状態において正しい運転員操作を無効にしてはならない。」

7.40. 保護系によって開始された操作は、一旦それが開始されたときは、開始したときの状態が終わってしまっても継続するように自己保持されるべきである。

7.41. 保護系によって開始された操作の自己保持は、通常は発電所設備に対する起動信号のレベルで実装される。個々の測定チャンネルの「封鎖」は必要ない。

7.42. 保護系の機能が一旦開始されたときは、その機能によって実施される全ての操作が完遂されるべきである。

7.43. 7.42 項の手引きは、保護系によって起動された安全設備を電気的に保護するために設けられた装置の動作を制限することは意図されてない。SSG-34 [7] は、安全上重要な機器等の電気的な保護に関する推奨事項を提示している。

7.44. 保護系の機能がリセットされたときには、起動された設備は、特別で慎重な運転員操作によらない限り、通常状態に戻すべきでない。

7.45. 安全機能をリセットするための装備は、安全系の一部であるべきである。

擬似的な開始

7.46. 保護系の設計は、実行可能な範囲で、保護系の擬似的な開始又は動作の可能性を最小化するべきである。

7.47. 保護系の機能の擬似的な開始は以下をもたらす可能性がある。

- 設備に対する不必要な応力と発電所寿命の短縮
- 他の安全動作の必要性
- 設備に対する運転員の信頼の低下。これはその後の運転員による有効な信号の無視につながる可能性がある。
- 発電所の発電能力の損失

7.48. 保護系の擬似的な開始は、発電所を不安全な状態にするべきではない。

7.49. 保護系の擬似的な開始又は動作が、保護機能が引き続き要求される発電所の状態に落ち着く可能性があるのであれば、そのときは、擬似的な起動と関係のない、また、それに影響されない保護系の一部又は他の安全系によって開始され、実行される操作によって安全な状態が維持されるべきである。

保護系と他の系統との相互作用

7.50. SSR-2/1 (Rev. 1)[1]の要件 64 は、「原子力発電所の保護系と制御系の間の相互干渉は、分離の手段により、接続を避けることにより、又は適切な機能上の独立性によって防止されなければならない。」と述べている。

7.51. SSR-2/1 (Rev. 1)[1] の 6.38 項は次のように述べている。

> 「保護系とどの制御系の間でも信号が共用される場合、(適切な切り離しのような)分離は確実なものとされなければならず、また、信号系は保護系の一部として分類されなければならない。」

7.52. 保護系は、保護系及び制御系によって共用されている、あらゆる機器又は信号の故障が生じている状態の下で、信頼性、多重性及び独立性に関する全ての要件を満足させるべきである。

7.53. SSR-2/1 (Rev. 1)[1] の 6.32(a) 項は 、「保護系は、制御系の非安全動作を無効にできるように、・・・設計されなければならない。」と述べている。

7.54. 想定起因事象が、保護系の機能の開始を要求する発電所状態をもたらす制御系の動作を引き起こすことができる場合、同一の想定起因事象は、必要な保護系機能を提供する安全系の適切な動作を妨げるべきではない。

7.55. 保護系の故障それ自体が、保護系が必要となる制御系の動作の引き金となる想定起因事象である可能性は無視されるべきではない。

7.56. 制御系と保護系との間の干渉が誤った運転を引き起こすことを防止するために用いられる対策の例は、以下を含む。

- 保護用及び制御用に分離した計測チャンネルの備え付け
- 干渉の可能性に対処するため安全グループへの追加の設備
- 想定起因事象によって生じる損傷を限定するために、発電所内に障壁若しくは代替物配備、又は
- 安全グループ及び発電所設計が発電所の状態を容認限界値内に維持するのに十分であるようなこれらの要素の組み合わせ

7.57. 7.52、7.54 及び 7.55 項に記された推奨事項は、そのような故障の発生時に、保護系がその要件を継続して完全に満たすことを確実なものとすることを狙いとしている。満たされるべき信頼性要件は、単一故障基準への適合性を含む。

7.58. ある装置が保護系又はより低い安全クラスの系統のいずれかによって起動されるときには、保護系による保護機能の開始に対するあらゆる作動要求は、装置を起動する優先権を持つべきである。

7.59. 例えば、起動信号は、通常運転のために制御系から送られることがあるか又は保護系によるあらゆる作動要求が制御系からの命令に優先するのであれば運転要員が同一の取合点から全ての系統要素の通常運転を制御できるようにするために制御系から送られる場合がある。

電力の供給

7.60. I&C 系のための電力供給は、その種類（電力源、空気圧源及び水力源など）とは関係なく、それらが供給する I&C 系の信頼性要件と一致した、安全クラス、信頼性条項、性能保証、隔離、試験可能性、保守可能性及び供用除外表示に関する要件を持つべきである。

7.61. 運転状態又は設計基準事故状態の下で常に使える状態にあることを要求される I&C 系は、I&C 系の設計基準によって指定された許容範囲内の電力を系統に供給する、無停電電源に接続されるべきである。

7.62. I&C 系は、その機能が電力源における付随的な中断に耐えられることを条件として、運転状況によって必要とされるときに手動操作又は自動切り替え操作によって、通常電源から予備電源に移行される場合がある。通常、移行系統は、電源供給系の一部として扱われるべきであり、それが支える I&C 系と同じ安全クラスのものとなる。

7.63. いくつかの近代的 I&C 系は、直流電源から直接に受電できる。このことは、電力系統のインバーター、電動発電機又は電力変換装置の必要性をなくすことから、無停電電源を必要とする系統にとって利点である。

7.64. 電源は、I&C 系の外部で生じるか又は同じ電源に直接的若しくは間接的に接続された他の I&C 系から発生することがある電磁障害の伝播経路になり得る（6.132 項を参照）。

7.65. SSG-34 [7] は電力の供給及び付随する配電系統に関する推奨事項を提示している。また、他の形での動力の供給（空気圧の供給、水力の供給、機械力の供給など）に関する推奨事項は、IAEA の安全基準シリーズ No. NS-G-1.8「原子力発電所の非常用電源系の設計」[33] に提示されている[36]。

デジタルシステム

7.66. デジタルシステムは、例えば、コンピュータに基づく系統及びハードウェア記述言語でプログラムされた系統を含む。

7.67. SSR-2/1 (Rev. 1) [1]の要件 63 は次のように述べている。

> 「原子力発電所の安全上重要な系統がコンピュータを基にした設備に依存する場合、系統の供用期間、特にソフトウェアの開発期間を通して、コンピュータのハードウ

[36] 原子力発電所の補助系及び支援系の設計に関する安全指針も作成中である。

ェアとソフトウェアの開発と試験実施に対する適切な基準及び手法が制定され、実施されなければならない。また、開発全体が、品質マネジメントシステムの対象とされなければならない。」

デジタルシステムの機能

7.68. I&C 機能へのデジタルシステムの使用は、複雑な機能を提供するための柔軟性、改善された発電所監視と運転員とのインターフェース、自己試験及び自己診断能力、強固なデータ記録能力に基づいた運転経験の反映を促進するためのより優れた環境、物理的に小さい寸法及びケーブルの必要性の少なさを含む、利点を提供する。デジタルシステムは、信頼性を改善する試験機能及び自己点検機能を持つことができる。

7.69. I&C 機能はデジタルシステムにおいては、アナログシステムで実現される方法とは異なる方法で実現される。デジタル技術では、機能が 1 つ又はそれを超える数の処理装置の中で組み合わされる。処理装置の中で組み合わされた機能は、分析が非常に難しい状態につながる可能性があり、ある処理装置の故障が複数の機能の同時故障をもたらすことになる。また、ある機能が、欲しない相互作用を通して別の機能の性能を（なんらかの特定できる「故障」なしに）低下させる場合がある。

7.70. そのような複雑な機器の十分な検証及び妥当性確認は、正しく設計されていない場合は非常に難しいか又は事実上不可能である可能性がある。特定されない誤りが存在することがあり、これらが全ての多重な機器において複製されるか又はソフトウェアモジュール､プログラムされた装置若しくはライブラリは全てに共通である可能性があることから、同一のプラットフォームに基づく他のシステムへ広がることがある。

7.71. デジタルシステムでは、入力情報は離散時間間隔で採取される。信号は、一定時間ごとにシステム要素間で伝送され、出力も一定時間ごとに作られる。その結果、そのようなシステムが正しく設計されていない場合、デジタルシステムの処理負荷又は通信負荷の変化が、通信速度と応答時間に影響を与える可能性がある。処理負荷又は通信負荷の変化は、発電所パラメータの変化、様々な系統の運転若しくは発電所状態又は設備の故障によって発生することがある。

7.72. 参考文献 [11]は、デジタルシステムの特別な性質に関するより詳細な情報を提示している。

7.73. デジタル I&C 系の設計は､指定された全ての運転状態及び想定しうる全てのデータ負荷条件の下で、系統が応答時間及び精度に関する要件にしたがって、その安全機能を実施することを確保すべきである。

7.74. I&C 安全系は、機器の仕様の範囲内のいかなる入力シーケンスも常に同じ出力及び応答時間を生み出すことになるという点で、確定的な挙動を有するように設計されるべきである。すなわち、入力誘因と応答の間の時間遅れは保証された最大値及び最小値を持つことである。

7.75. 確定的な応答時間を確実なものとすることは、次の事項を含むことがある。

- プロセスに関係する割込みを避けること。これは、発電所状態が、I&C 系が扱わなければならなくなる割込みの発生率に直接影響を及ぼすことができないようにするためである。
- 設計時に静的に資源を割り当てること
- 事前に定義された制限値によって設定されるループの反復に枠をはめること

7.76. デジタルシステムの応答時間と精度は、サンプル率と処理サイクル時間に機能的に

依存する。正しく設計されなかったシステムでは、これらのパラメータもプロセッサの速度に依存する可能性がある。

7.77. デジタルシステムの設計及び分析は、個々の機器（コンピュータのプロセッサなど）の故障が、容認されるシステム挙動の予測範囲内に留まるようになされるべきである。

7.78. デジタルシステムの電源喪失又は再起動は、構成データ又はソフトウェアの望ましくない変更をもたらさないようにすべきである。

デジタルデータ通信

7.79. 安全系に関するデータ通信は、一定の伝送時間を持つように設計されるべきである。

7.80. 一定の伝送時間を確保する方法は、以下のものを含む。

- 時間に基づくあらかじめ決められた挙動、すなわち、データ通信システムの動作は、その依頼機器側により決められるのはなく、時間スケジュールに基づいて、設計によってあらかじめ決められること
- あらかじめ決められたデータ通信負荷、すなわち、通信負荷が常にデータ通信システムの伝送容量に見合うように、決められたどの時間においても、伝送されるメッセージの大きさは設計によってあらかじめ決められること
- あらかじめ決められたデータ通信パターン、すなわち、決められたどの時間においても、送信されるメッセージの送信者と宛先は設計によってあらかじめ決められていること

7.81. デジタルデータ通信は、6.25～6.56 項の推奨事項に従うべきである。

7.82. デジタルデータ通信を介して送受信される各メッセージは、自動的に点検され、もしエラーが特定された場合は警告信号が出されるべきである。

7.83. エラーは、損傷したデータ、無効なデータ（計画外のメッセージ）、不正なメッセージ（予期されない発信源からのメッセージ）を含むことがある。

7.84. 通信システムがデータを暗号化するか又は専用のプロトコルを使うのであれば、これらの仕組みがエラーの検出を妨げないようにすべきである。

7.85. データ通信でエラーが検出されたときに取られるべき操作は、あらかじめ定められるべきである。

7.86. エラーが検出されたときに取られることがある操作は、無効若しくは不正なデータの自動的な排除、可能であれば損傷したデータの修正又は損傷したデータの排除を含む。

7.87. 設計は、データ伝送及びデータ通信設備の故障が検知されること、運転員に対して適切な警報装置が備えられること並びに性能分析のために記録が作られることを確実なものとすべきである。

7.88. デジタルデータ通信におけるある種のエラーの存在は、このようなエラーは予期されており、また、通信プロトコルがある種のエラー及び一定の範囲のエラー発生率に対処するように設計されているため、それ自身ではシステムの故障を構成しない。したがって、7.87 項の手引きの適用は、何がデータ伝送の故障を構成するのかの仕様を含む。判断基準は、例えば、成功した送信間の許容可能最大間隔又はエラーの最大発生率を指定することである。

7.89. エラーの検出及び修正の仕組みは、信号伝送の信頼性を改善する。

7.90. エラーの処理及び通信故障の検出に使われる方法の範囲は、データの使用に対して適切であり、データを使用する機能への作動要求の頻度に対して適切であり、また、持ち込まれる複雑さに対して釣り合いが取られているべきである。

安全系内の情報伝達の仕組み

7.91. 安全関連のデータの通信が何らかの機能不全した場合、安全系は、その安全機能を実施し続けるか又は安全な状態に移行すべきである。

7.92. 多くの場合、この推奨事項は、共有メモリへの注意深く制御された入出力を介してデータを共有する 2 つのプロセッサを使用することによって達成される。1 つのプロセッサは安全機能を実施することに専用使用され、他はデータ通信業務に専用使用される。計算及び論理機能の、通信及び割り込み機能からの分離は、通信及び割り込み機能におけるエラーが安全性計算又は論理機能の確定的な挙動及び時間設定を乱すことを防止する。バッファリングと呼ばれることもあるこの分離は、区分の外部で発生した通信の障害及び故障が安全機能を実行するプロセッサまで伝播することを防止しようとするものである。

7.93. あらかじめ決められたメッセージのみが、受け取り側の安全系によって処理されるべきである。

7.94. 予め定められるべきメッセージの具体的な要素は、メッセージプロトコル、メッセージ形式及び一群の有効メッセージを含む。

データ通信の独立性

7.95. この節は、デジタルシステム内のデータ通信に特有な手引きとともに、6.25～6.56 項の手引きを補足する。

共通原因故障の回避

7.96. データ通信ネットワークの接続形態及びメディアへの出入り管理は、安全系の共通原因故障を避けるように設計され実装されるべきである。

安全区分間の通信

7.97. 通信のエラー又は故障を含めて、安全区分内の通信は、接続された安全区分側がその安全機能を実施することを妨げるべきでない。

7.98. 7.97 項の推奨事項の意図は、区分間での故障の伝搬を防止することである。通常、データの妥当性確認（7.82～7.94 項を参照）とバッファリングとの組み合わせが採用される。

7.99. 複数の安全区分からの通信が単一のリンクを介して伝送される中央ハブ又はルーターを使った構造は、使われるべきではない。

異なる安全クラスの系統間の通信

7.100. デジタルシステムと異なる安全クラスの装置との間のデータ通信は、6.25-6.56 項の手引きに従うべきである。保護系機能の開始に対する作動要求は、装置を起動することへの優先権を持つべきである。

コンピュータ・セキュリティ

7.101. 参考文献 [8] は、原子力施設におけるコンピュータ・セキュリティプログラムを実装することに対する懸念事項、要件及び方針に関する手引きを提示する。本章は、参考文献 [8] の指針を補足する。

安全とセキュリティとの相互関係

7.102. SSR-2/1 (Rev. 1)[1] の要件 8 は次のように述べている。

> 「原子力発電所における、安全対策、核セキュリティ対策及び核物質の計量・管理に対する加盟国の対処方策は、互いにそれぞれの機能を損なうことがないように、統合された形で設計され、また、実施されなければならない。」

7.103. あらゆるコンピュータ・セキュリティの仕組みの運用又は故障のいずれも、系統がその安全機能を実施する能力に悪影響を与えるべきでない。安全とセキュリティとの間に対立があればそのときは、セキュリティリスクに対処する解決策が追求されることを前提に、安全を確保するために行われる設計配慮事項が維持されるべきである。セキュリティ解決策がないことを受け入れることは、強く推奨されず、厳格なケースバイケース基準にもとづき、かつ、完全な立証及びセキュリティリスク分析によって支持される場合のみに考慮される場合がある。

7.104. コンピュータ・セキュリティの仕組みの故障モード及びこれら故障モードの I&C 機能への影響は認識され、文書化され、また、系統のハザード分析で考慮されるべきである。

7.105. コンピュータ・セキュリティの仕組みがヒューマンマシンインターフェースの中で実装される場合、その仕組みは運転員が発電所の安全を維持する能力に悪影響を与えないようであるべきである。

7.106. 実施可能な場合、安全上の便益を提供しないセキュリティ対策は、I&C 系から分離された装置に実装されるべきである。

7.107. I&C 系へのセキュリティ機能の追加は、その系統の複雑さを増加させ、安全機能を確実に実施する能力を危うくするか又は誤操作の可能性を増すおそれのある、潜在的な故障モードをその系統に持ち込むことがある。

7.108. I&C 系に含まれるコンピュータ・セキュリティの仕組みは、本安全指針の第 2 章の推奨事項に沿って開発されるべきであり、その仕組みが組み込まれる系統と同じレベルで性能保証されるべきである。

7.109. デジタルシステム又は機器の開発プロセス、運用及び保守は、コンピュータ・セキュリティを達成する手段を指定し詳述するコンピュータ・セキュリティ計画に従って実行されるべきである。

7.110. コンピュータ・セキュリティ計画は、I&C 系の開発中に実装される適切な物理的、論理的及び運用的管理を含むべきである。

7.111. デジタルシステムの開発環境並びにそれに続くデジタルシステムの設置、運用及び保守は、意図的若しくは意図的でない侵入又はソフトウェア若しくはデータの破損、悪質なコードの導入、外部ネットワークへの正しくない接続及びハッキング攻撃を防止することに適した対策を持つべきである。

安全上重要なデジタルシステムへのアクセス管理

7.112. 系統及び機器への全てのデータ接続装置は、筐体内に置かれるべきであり、その筐体については、筐体への接近及びその筐体の内部への接近の両方が 6.156 項にしたがって管理されている。

7.113. データ接続装置は、ネットワーク接続装置、外部記憶装置用の接続装置並びにメモリスティック、フラッシュカード及びデータディスクなどの携帯媒体への出入りを含む。

7.114. 使われていないデータ接続は無効にされるべきである。

7.115. 一時的な使用のために必要とされる接続、例えば保守用コンピュータの接続は、使用されていない時は無効にされるべきである。

7.116. 使われていない接続を無効にする形態は、取り外し、物理的な対策又は論理的な対策を含む。

7.117. データ接続を無効にする手段として論理的な対策が使われる場合、追加の対策は、接続が無効な状態を維持することを確保するためか、又は接続の構成若しくは状態のあらゆる変化が検知され、システムの操作性への影響について評価されることを確保するために提供されるべきである。

7.118. ソフトウェア又は構成データの変更及び変更自体を許容する機能へのアクセスは監視され、記録されるべきである。

7.119. 監視すること及び記録することは、管理手順書によって自動又は手動で実施される場合がある。

7.120. 使用される方法は、安全機能の性能と干渉することなく必要なセキュリティを提供するものとして正当化されるべきである。

7.121. 7.118～7.120 項は、設計により制御室の運転員によってできる構成データの変更に対しては適用しない。

緊急時施設との情報伝達のセキュリティ

7.122. 発電所内の I&C 系からのデータは、緊急時対応を支援する、発電所敷地内にある他の場所（例えば、技術支援センター）及び発電所敷地の外（例えば、緊急事態対応組織）に伝送される場合があるが、I&C 系がこれらの接続によって悪影響を受けないことが前提である。

7.123. 発電所と技術支援センターとの間及び発電所と緊急事態対応組織との間の通信回線は、人間のコミュニケーションに使われるものを含めて、その目的専用のものとされるべきであり、また、不正な変更から防護されるべきである。

7.124. データ通信は、基本的な安全機能の状態に関する情報及び緊急事態の管理を支援する他の情報を含むことがある。

運用面のセキュリティのための仕組み

7.125. コンピュータ・セキュリティの脅威を検知し、その影響を緩和することに対して、能動的なコンピュータ・セキュリティ上の仕組みの使用が検討されるべきである。

7.126. I&C 系に対する能動的なコンピュータ・セキュリティ上の仕組みが安全上重要な機能に悪影響を及ぼさないようにすべきである。

7.127. 能動的なコンピュータ・セキュリティ上の仕組みは、系統の複雑さを増し、系統資源の使用に関して競合し、偽作動の可能性を増加し、又は新しい故障モードを導入することがある。受動的なコンピュータ・セキュリティ上の仕組みの適用が常に考慮されるべきである。

7.128. 能動的なセキュリティ上の仕組みを適用することは、系統が切り離された状態のときにのみ望ましい。I&C 系については、切り離し状態でスキャン機能を実施することが望ましい。

7.129. コンピュータシステムは、コンピュータ・セキュリティ上の仕組みが適切に構成され、適切に作動していることの、定期的な検証及び保守後の検証のための装備を含むべきである。

7.130. コンピュータのセキュリティ監視から得られた結果を検討し、それに基づき行動することに対する手順書が制定されるべきである。

ハードウェア記述言語で構成された装置

7.131. ハードウェア記述言語で構成された装置は、特定の機能を提供するために I&C 開発者によって特別注文された論理構造を提供するプログラム可能な電子モジュール（ゲートとスイッチの配列など）である。フィールドプログラマブルゲートアレイは、この種別の装置の一般例である。

7.132. この特別注文には、これらの機能を実装するための要件を形式的に記述する特別なソフトウェアツールを伴う。

7.133. ハードウェア記述言語で構成された装置に関連する本章の手引きは、第 2 章のライフサイクルに関する手引き、本章で提示されるデジタルシステムに対する手引き及び第 9 章で提示されるソフトウェアに対する手引きと合わせて適用されるべきである。それは、安全機能を直接実装する装置に適用できる。

7.134. プログラムされたハードウェア装置を用いたアプリケーションの開発は、事前に定義された、第 2 章の推奨事項を満たすライフサイクルに従うべきである。

7.135. 開発計画は、第三者が理解できるやり方で個々の技術的な決定の正当性を求めるべきである。

7.136. プログラムされたハードウェア装置の実装計画は、製作された各部品が設計に適合していることを保証するための手段を指定すべきである。

7.137. プログラムされたハードウェア装置に関する設計要件は、ゲート遅延及び準備時間の要件など、時間調整要件を含むべきである。

7.138. プログラムされたハードウェア装置並びにそれに付随する、ライブラリ、最終製品に組み込まれる知的所有物の核心部及びハードウェア定義言語などの品目の選択は、その適性を保証するために、定義され、文書化されたプロセスに従うべきである。

7.139. 知的所有物核心部は、以下の条件が満たされる場合にのみ使われるべきである。

- 使われる知的所有物核心部は、厳格な工学的プロセス、明確に定義された有用な文書及び統合の容易さを含む知的所有物の核心部に対する高品質な開発プロセスに従

う、資格のある供給業者から取得されるべきである。
- ハザードの持ち込みがないことを保証するために評価が実施されるべきである。

7.140. 受け入れをするするために事前開発品目の改造が必要な場合、その改造は、受け入れ審査前に仕様作成され、設計され、実装され、また、検証されるべきである。

7.141. 選択されたプログラムされたハードウェア装置が補助的な仕組み（組み込まれた自己試験など）を含む場合、安全機能の性能への寄与におけるその装置の適性は、開発プロセス（及び検証プロセス）及び設計を含む、様々な要素の評価によって判断されるべきである。

7.142. 性能保証され、互換性があるソフトウェアツールを備えた標準化ハードウェア記述言語が、プログラムされたハードウェア装置のプログラム作成に選択されるべきである。

7.143. プログラムされたハードウェア装置の設計は、以下であるべきである。

- プログラムされたハードウェア装置の挙動は確定的であることを保証するべきである。確定的な設計は、例えば、内部同期設計を使うことによって達成される場合がある。同期設計は、正確さ（準安定性問題の回避）及び試験可能性に優れており、また、設計及び検証のためのソフトウェアツールの最大限の活用を可能とする。
- 明確に定義された具体性及び動作特性を持つプログラムされたハードウェア装置構成のみを使うべきである。明確に定義された具体性及び動作特性を達成する方法は、レジスタ転送レベルの記述、厳密な意味及び構文規則の使用、ハードウェア記述言語の「安全」セットの使用並びにあらかじめ定められた言語及びコード作成規則の使用のような、装置の形式化された記述の開発を含む。
- 実現可能な範囲で、数学的な定理の証明に基づいた検証手法の使用を支援するべきである。
- 想定しうる全ての論理ケース並びにリセット、電源投入及び通常動作のような、プログラムされたハードウェア装置の全ての動作モードを明示的に扱うべきである。
- 供給電圧、温度及び超小型電子プロセッサの境界での変化に起因する、想定される全ての時間的な状況に対して正確であるべきである。
- プログラムされたハードウェア装置の中に実装される各機能が試験可能であることを保証するべきである。

7.144. 事後の経路分析は、設計の供給者によって定義された技術規則及び実装用のソフトウェアツールを使って、装置の設計及び実装の適合性を実証するために使われるべきである。

7.145. プログラムされたハードウェア装置の設計プロセスは I&C 系の全体開発プロセスに結合されるべきである。

7.146. 検証及び妥当性確認は、下記であるべきである。

- プログラムされたハードウェア装置の機能遂行に影響を与える、指定外の機能がプログラムされていないことを確認するために用いられるべきである。
- プログラムされたハードウェア装置内の全ての信号経路の試験を含むべきである。
- プログラムされたハードウェア装置に特有なシステムの側面に対処するべきである。
- 時間合わせについての解析及びシミュレーションを含むべきである。

7.147. 環境性能保証及び環境分析は、事前開発機器又は補助的な仕組みを含むことが安全上重要な系統がその安全機能を実施する能力を低下させないことを実証するために使われるべきである。

ソフトウェアツール

7.148. ソフトウェアツールは、使用を通じて利益が生じ、かつ、使用可能である場合に、I&C 開発ライフサイクルの全ての面を支援するため使用されるべきである。

7.149. 適切なソフトウェアツールの使用は、I&C 開発時に欠陥を取り込むリスクを減らすことができ、点検、検証及び妥当性確認の間に欠陥が発見される確率を高めることができる。その結果、ソフトウェアツールの使用は、I&C 開発プロセスの健全さを向上でき、それによって機器の信頼性を高めることができる。ソフトウェアツールの使用はまた、系統、機器及びソフトウェアを製作するために要求される時間及び人の作業量を減らすことができるため、経済的な利点も持つことができる。ソフトウェアツールは、作成規則及び標準への遵守状況を自動的に点検するために、標準様式での適切な記録と一貫した文書を作成するために、また、変更管理を支援するために使うことができる。ソフトウェアツールはまた、試験に要求される作業量を減らすこともでき、自動化された記録履歴を維持することもできる。また、いくつかの特定の開発方法は、ソフトウェアツールの使用を要求している。

7.150. I&C 系の開発に使われるソフトウェアツールは次のものを含む。

- 要件マネジメントシステム又は統合開発環境などの作業基盤及び開発支援システムを提供するソフトウェアツール
- 自動回路及び配線計画ソフトウェア
- コード作成、コンパイラ、論理合成器及びテキスト又は図表をある抽象化レベルで、通常はより低い他の抽象化レベルへ変換するツールなどの変換ソフトウェアツール
- 電子設計を自動化するソフトウェアツール
- 静的コード分析器、自動回路試験器、試験対象範囲モニター、論理証明補助、電子回路シミュレータ及び発電所全体シミュレータのような、検証及び妥当性確認のためのソフトウェアツール
- 系統構成データ作成用のソフトウェアツール
- 構成管理及び管理のためのソフトウェアツール
- 既知及び未知の脆弱性を検知するセキュリティ試験のためのソフトウェアツール

7.151. 統合プロジェクト支援環境の重要な要素は、適切な管理及び整合性を確保することである。ソフトウェアツールが利用できないのであれば、新しいソフトウェアツールの開発に考慮が払われるべきである。

7.152. ソフトウェアツールを使用することの利点及びリスクは、ソフトウェアツールを使わない場合の利点及びリスクに対して調整されるべきである。

7.153. 重要な取り組み方は、エラーをすること及び欠陥を持ち込むことの機会を制限するが、欠陥を避けるか又は検知する機会を最大にするソフトウェアツールを選択することである。系統開発は、いくつかの方法で、ソフトウェアツールの使用によって悪影響受けることがある。例えば、設計用ソフトウェアツールは、間違いの多い出力の生成によって欠陥を持ち込むことがあり、又は検証ツールは、ある種の欠陥若しくは欠陥の形式を明らかにし損なうことがある。

7.154. システムの全供用期間にわたって利用可能であり続けるソフトウェアツールが選択されるべきであり、システム開発の間に使われる他のソフトウェアツールと両立性があるべきである。

7.155. 全てのソフトウェアツールの機能性及び適用限界は特定され、文書化されるべきである。

7.156. ソフトウェアツール及びその成果物は、事前の正当化なしに、宣言された機能性又

は適用限界を超えて使用されるべきではない。

7.157. 例えば、ソフトウェアツールは、判断が要求されるときは、人に置き換えることはできない。場合によっては、ソフトウェアツールによる支援がプロセスの完全自動化よりもより適切である。

7.158. ソフトウェアツールは、ソフトウェアツールの信頼性に関する要件、ソフトウェアツールの種類、ソフトウェアツールが欠陥を持ち込む又は存在する欠陥を使用者に知らせ損なう可能性、また、系統の多重な要素又は多様性系統にソフトウェアツールが影響する場合の範囲に従って検証され、評価されるべきである。

7.159. 必要な検証及び評価の程度に影響する可能性がある状況の例は以下に示される。

- 欠陥を持ち込む能力のあるソフトウェアツールは、その能力がないと実証されているソフトウェアツールより厳格に検証されるべきである。
- 存在する欠陥を使用者に知らせることができないソフトウェアツールは、その能力がないソフトウェアツールより厳格に検証されるべきである。
- ソフトウェアツールの成果物が系統的かつ独立に検証されるときは、ソフトウェアツールに対する検証は必要ではない。
- ソフトウェアツールのあらゆる潜在的な欠陥の影響の緩和に対する方策が施されているのであれば（例えばプロセスの多様性又は系統設計によって)、ソフトウェアツール検証の厳格さをいくらか下げることが容認できる場合がある。

7.160. ソフトウェアツールの検証及び評価は、開発者の経験及びソフトウェアツールが使われるプロセスから得られた経験を含め、先行使用の経験を考慮に入れるべきである。

7.161. ソフトウェアツールの選択、検証及び評価は、正当化され文書化されるべきである。

7.162. 全てのソフトウェアツールは適切な構成管理の下に置かれるべきである。

7.163. ベースライン設備の開発、検証又は妥当性確認の間に使われたソフトウェアツールの設定、ソフトウェア及びハードウェア記述言語で構成された装置は、開発記録に文書化されるべきである。

7.164. そのような文書化は、最終ソフトウェアの整合性を保証することに有用なだけではなく、ソースコード、ソフトウェアツール又はソフトウェアツールの設定に存在することがある欠陥の発生源を評価するのにも役立つ。使用されるツールの設定に関する情報は、ソフトウェアツールに起因する共通原因故障の可能性を評価する際に重要な場合がある。

機能が限定された産業用デジタル装置の安全系適用に関する性能保証

7.165. 本章は、原子力発電所の安全系で使用されることになるが、そのような用途での使用のために特別に開発されてこなかった、機能が限定された産業用デジタル装置の性能保証に関する手引きを提示する。この手引きは、この分類の装置に関する 6.78～6.134 項の性能保証に関する推奨事項を遂行する方式を記すものである。

7.166. 機能が限定された装置は次の特性を持っている

- あらかじめ開発されたソフトウェア又はプログラムされた論理を含む。
- 自律的であり、製造者によって定められ、使用者によって変更できない 1 つの概念的に単純な主要機能のみを実施する。
- 再プログラムできるように設計されていない。
- 再構成可能な場合、その構成可能性は、監視若しくは制御されているプロセスとの

両立性、又は接続されている設備との取合いに関連するパラメータに制限されている。

7.167. 他の全ての装置は「機能が限定された産業用デジタル装置」ではない。すなわち、それらは次の特性を持っている。

- 当該の装置は、市販のコンピュータ（個人用コンピュータ、産業用コンピュータ又はプログラム可能な論理制御器）を用いている。
- 当該の装置は、I&C プラットフォーム用に開発されている。又は
- 当該の装置は、原子力産業用に特別に開発されている。

7.168. 機能が限定された産業用デジタル装置のその目的とする機能に対する、適性及び正確さの確認は、以下に対する証拠を作成すべきである。

- 装置の主要機能が適用に関する機能要件を満たしていること
- 主要機能以外の機能[37]の動作又は故障のいずれもが、主要機能の不安全な動作となりえないこと
- 装置は、互いに多重性があり、又は多様性のある I&C 系の要素に類似の装置が設置されている場合、ほとんど同時の共通原因故障を引き起こす可能性が高い系統的な欠陥が存在しないこと
- 開発プロセスが系統的で、本安全指針の第 2 章に記された一般的な原則に従っていること
- 製造に関わる品質保証が、後で製造される同一又は類似の型式の装置を受け入れる根拠を提供するのに十分であること

7.169. 他の産業での安全目的での性能認定期間中に作成された情報が、装置の性能保証を支援する証拠として使われる場合がある。認定証だけでは不十分であり、むしろ、価値があるのは認定プロセスによって作成された情報である場合がある。

7.170. 上記 1 つ又はそれを超える数の推奨事項が満たされない場合、適性及び正確さの証拠の不備な点に直接的に対処する補完的な証拠が提示されるべきである。

7.171. このような補完的な証拠は以下のようであるべきである。

- 立証しようと意図する要件に直接対処すべきである。
- 問題の装置に適用できると示されるべきである。

7.172. 補完的な証拠を提示する手法の例は、次のものを含む。

- 意図する適用のために適切な装置固有の補完的業務及び正確さの証拠の他の要素
- 適用可能で信頼できる運転経験の評価
- 設計結果の検証
- 統計的試験

7.173. 使用者は、装置を目的とする用途に適したものにするためにその装置を構成設定する場合がある。そのような変更は、設計の正確さと文書化に対する本安全指針の判断基準を満たすべきであり、また、性能保証で認められた従前の運転経験又は試験を無効にすべきでない。

7.174. 目的とする用途での装置の安全使用のために観察されるべき制約条件が特定され

[37] 主要機能以外の機能には、例えば、装置を維持するため又は構成を設定するために使われる機能及び目的とする用途のためには必要とされない機能を含む。

るべきである。

7.175. そのような制約条件は、例えば、次のものを含む。

- その装置が性能保証されている用途に関する制約事項
- 有効又は無効にされるべき、特定の選択肢及び使用されない機能
- 動作環境及び動作寿命に対する制限事項
- 運転、試験及び保守の際に監視されるべき対策

8. ヒューマンマシンインターフェースに関連する考慮事項

制御室

中央制御室

8.1. SSR-2/1 (Rev. 1)[1] の要件 65 は次のように述べている。

「原子力発電所では、全ての運転状態において発電所が自動又は手動で安全に運転できるように、並びに予期される運転時の事象及び事故状態が発生した後に、発電所を安全な状態に維持するか又は安全な状態に復旧するための対策が取れるように、制御室が設けられなければならない。」

8.2. SSR-2/1 (Rev. 1) [1]の要件 59 は次のように述べている。

「発電所の安全で信頼性の高い運転に必要な情報を得るために、事故時の発電所の状態を判断するために及びアクシデントマネジメントのための判断をするために、原子力発電所における核分裂プロセス、原子炉の炉心の健全性、原子炉冷却系及び格納容器に影響を与える全ての主要な状態値を測定するための計装設備が設けられなければならない。」

8.3. SSR-2/1 (Rev. 1) [1] の 5.57 項は次のように述べている。

「運転員には、次の事項のために必要な情報が提供されなければならない。
(a) 発電所のいかなる運転状態においても全般的な状態を評価するため
(b) 発電所の系統及び設備に付随するパラメータについて指定された制限（運転上の制限と条件）内で発電所を運転するため
(c) 安全系の起動のための安全動作が、必要な時に自動的に開始されること及び関連する系統が意図したとおりに機能していることを確認するため
(d) 指定された安全動作の手動開始の必要性及び時間を決定するため」

8.4. I&C は、発電所を制御し安全を維持するために必要な各機能を、制御室の運転員が手動で開始又は制御することを許容すべきである。

8.5. 制御室には、発電所の状態、その安全状態及び重要な発電所パラメータの傾向を含め、安全上重要な全ての機能を監視するために、十分な数の表示装置があるべきである。

8.6. 安全分類された指示装置及び制御装置は、緊急時運転手順書及び重大事故マネジメント指針を具体化するために備えられるべきである。

8.7. 8.6 項の手引きは、緊急時運転手順書及び重大事故マネジメント指針の目標を満足させるために適切な他の手段を使う選択肢を排除することは意図されていない。

8.8. 発電所を制御し安全を維持するために要求される系統又は系統の一部が、故障又は意図的に動作不能にされた場合、この状態は、制御室に及びその情報が運転員に伝えられる必要がある場所に表示されるべきである。

8.9. 安全系の状態の変化は広く知らされるべきであり、この情報が運転員によって必要とされる場所に、その状態が表示されるべきである。

8.10. 警報を出す必要がある系統の状態の変化には、通常運転限界からの逸脱、安全系の利用可能性の喪失、又は故障、保守若しくは試験による待機設備の使用不可能な状態を含むことがある。

8.11. 警報系統の機能の進歩は、発電所で運転員が効果的に監視すること及び事象に対して対応することを支援する警報の処理、警報の優先順位付け及び警報の制御と管理など、望ましい仕組みが実装されることを可能にした。

8.12. 中央制御室及び補助制御室の設計は、火災、内的ハザード又は想定起因事象が運転員の基本的安全機能を履行するのを妨げることのないようであるべきである。

補助制御室

8.13. SSR-2/1 (Rev. 1) [1] の要件 66 は次のように述べている。

> 「原子力発電所内において制御室から物理的、電気的及び機能的に分離した場所、できれば一箇所（補助制御室）で、計測制御設備が利用できるように維持されなければならない。補助制御室は、制御室で重要な安全機能を果たすことができなくなった場合、原子炉が停止状態に置かれ、その状態で維持され、崩壊熱が除去され、また、発電所の重要なパラメータが監視されるように装備されなければならない。」

8.14. いくつかの発電所の設計は、2 つ以上の補助制御室を持つ場合があるか又は補助制御室内ではない補助制御場所が設けられる場合がある。

8.15. 補助制御室は、中央制御室からの退避を要する状況から生じる場合がある事象に対する対応を支援するために、必要に応じて、発電所の状態を監視する情報表示装置を収納するべきである。

8.16. 補助制御室は、運転員が発電所を安全な状態に持ちこみ、安全な状態が到達され維持されることを確認するために、また、発電所の状態及び重要な発電所パラメータの傾向を監視するために、十分な制御装置、指示装置、警報装置及び表示装置を収納するべきである。

8.17. 8.16 項の推奨事項を果たすために必要とされる全ての制御装置を補助制御室内に設置することが現実的でない場合、現場の制御場所にある制御器が使われる場合がある。

8.18. 中央制御室が放棄されるときはいつでも、優先される制御を新しい場所へ移動することに関して、中央制御室外での適正な方策が講じられるべきである。

事故の監視

8.19. SSR-2/1 (Rev. 1)[1] の 6.31 項は次のように述べている。

> 「枢要な設備の状態及び事故の経過を監視するために、また、設計で意図した場所から放出される放射性物質の放出場所と量を予測するために、さらに、事故後の解析のために、それぞれに対する必須の情報を利用できることを確実なものとするように計

装設備と記録設備が設けられなければならない。」

8.20.　発電所内の事故状態を監視する情報表示は、適切な場所（すなわち、中央制御室及び補助制御室）で、運転要員の役割及び責任に沿って提供され、表示されるべきである。

8.21.　事故状態を監視する一連の表示装置は、通常、「事故監視系統」又は「事故時監視系統」と呼ばれる。そのような表示装置は、別の系統の一部として備えられるか又は個々の計測チャンネルを集めたものである場合がある。

8.22.　事故監視系統は、以下を可能とするため、事故状態下での発電所の運転員によって必要とされる変数の値を表示すべきである。

(a)　発電所を安全な状態に持ち込むためにあらかじめ計画された手動操作をとること
(b)　基本的な安全機能が果たされているか否かを判断すること
(c)　核分裂生成物の放出を防止する障壁（燃料被覆管、原子炉冷却材圧力バウンダリ及び格納容器）の破損の可能性又は実際の破損の存在を判断すること
(d)　設計基準事故及び設計拡張状態の時に影響を緩和し、発電所を安全な状態に持ち込むために必要な発電所の諸系統の状況及び性能を判断すること
(e)　放射性物質の放出から公衆を防護するための行動を開始する必要性を判断すること
(f)　発電所における重大事故マネジメント指針を実行すること

8.23.　8.22 項の項目 (a) から (d) に挙げられた表示機能を実施する計測設備は、安全クラスとされるべきであり、設計基準事故状態及び設計拡張状態の下で実施できる I&C 設備によって備えられるべきである。

8.24.　「安全系」としての分類は、安全グループに関する単一故障基準への適合を含め、第 6 章の判断基準を完全に適用する必要に至ることになる。

8.25.　重大事故監視用の計測設備は、予想される環境条件の全域に対して設計され、性能保証されるべきである。

8.26.　経験することがある、考えられる最悪の条件に対して重大事故監視用計装の型式検査を完全に行うことは、必ずしも実現可能だとは限らない。そのような場合には、6.82 項に記した方法（ただしそれに限定されるものではない）を含め、他の方法で試験は補完されることがある。

8.27.　重大事故マネジメント指針の実行を支援する事故監視機能は以下であるべきである。

(a)　重大事故監視計装の一部ではない I&C 設備の作動、故障又は誤作動によって能力が損なわれるべきでない。
(b)　外部電源に頼らないか又は発電所の電力系統以外の電源から給電されるように設計された能力を有するべきである。

8.28.　8.22 項の項目 (a) から (c) 及び (f) に挙げられた機能を実施する計測設備の単一の表示チャンネルの故障が不明瞭な指示となる可能性がある場合には、運転員がその不明瞭さを解決することができる手段が備えられるべきである。

8.29.　1 つの表示チャンネルの故障が 1 対の多重的表示が一致しないことを引き起こすことがある。不明瞭さを解決する手段には、追加のチャンネルを設けること、又は不明瞭な指示値を問題の指示値との関係がわかっている別の変数と比較する手順を含む。

8.30.　事故監視用に設けられた計測設備は、事故状態の下で達する場合があるパラメータ値の全域を範囲とするべきである。

8.31. 事故監視変数の表示装置は、容易にそれと認識できるものであるべきである。

8.32. 電子的な運転員支援（「安全パラメータ表示系」など）は、運転員が発電所の状態を迅速に把握する際に、事故監視チャンネルの動作を確認する際に、それらの指示値の妥当性を確認する際に、また、直接的な測定値から間接的に測定される変数の値を判断する際に、支援するために設けられるべきである。

8.33. コンピュータによる手引きは安全を強化し、正しい措置が取られているとの確実性をより高くできる場合がある。

8.34. 近代の制御室の設計では、安全パラメータ表示系統及び事故監視系統の機能は、多くの場合、通常の運転員用ヒューマンマシンインターフェースに統合される。助言は、特定の運転若しくは事故シナリオに限定される場合があるか、又は起動時及び通常の出力運転時を含む全ての運転を対象とする場合がある。

8.35. 電源に依存しない運転員支援が、8.22 項の項目 (a) から (c) 及び (f) で与えられた表示機能を実施する計測設備にも利用できるべきである。

運転員の通信連絡システム

8.36. SSR-2/1 (Rev. 1)[1] の要件 37 は次のように述べている。

> 「あらゆる通常運転モードで安全運転ができるようにするために、また、全ての想定起因事象の後及び事故状態においても利用することができるために、原子力発電所全体にわたる効果的な通信連絡設備が設けられなければならない。」

8.37. SSR-2/1 (Rev. 1)[1] の 5.66 項は次のように述べている。

> 「運転状態及び事故状態において、原子力発電所内及び敷地内にいる全ての人が警告及び指示を与えられるように、適切な警報系及び通信連絡手段が設けられなければならない。」

8.38. SSR-2/1 (Rev. 1)[1] の 5.67 項は次のように述べている。

> 「原子力発電所内及び隣接地域内の安全のため並びに所外の関係機関との連絡のために必要な、適切で多様性のある連絡手段が設けられなければならない。」

8.39. 運転要員が監視、制御を行うと予測される I&C 系から離れる必要なく、彼らが発電所内部及び外部の場所と確実に取り交わす通信連絡システムが備えられるべきである。

8.40. 運転要員が相互間で及び敷地外緊急時支援部隊と連絡するために設けられたシステムは、いかなる個人防護装備、想定起因事象又は単一の悪意のある行為によっても無力なものとされるべきでない。

8.41. I&C 設備の特性は、運転要員間の情報伝達を不能にするべきではない。

8.42. 例えば、I&C 設備が無線通信を妨害する場合、無線通信が I&C 設備を妨害する場合、又は個人防護装備が電話の使用を妨げる場合には、他の方式の情報伝達が必要である場合がある。

8.43. 中央制御室、補助制御室及び技術支援センターは、下記との間に少なくとも 2 つの多様な情報伝達方法を持つべきである。

(a) 予期される運転事象又は事故状態の際に情報伝達が必要とされる区域
(b) 技術支援センターなどの緊急時対応施設及び緊急時対応組織

(c) 関連施設[38]

8.44. 多様な情報伝達方法の例は、電子メール、データ転送、ファックス、ビデオリンク、地上通信、衛星電話及び携帯電話並びに携帯型無線装置を含む。

8.45. 8.43 項及び 8.44 項に特定された多様な情報伝達リンクは以下であるべきである。

(a) それらのいずれもが同じ故障、内的ハザード、外的ハザード又は想定起因事象によって影響を受けないように設計されるべきである。
(b) 発電所の電力系統及び敷地外の電力系統の両方から独立して動作可能であるべきである。

8.46. 敷地内及び発電所内の全ての要員に聞こえる通知を行なうための通信連絡システムが備えられるべきである。

計測制御系の人間工学に関わる一般的な原則

8.47. SSR-2/1 (Rev. 1)[1] の要件 32 は次のように述べている。

> 「人的因子に関する体系的な検討は、ヒューマンマシンインターフェースを含めて、原子力発電所に対する設計プロセスの初期の段階で実施されなければならず、また、設計の全プロセスを通して継続されなければならない。」

8.48. SSR-2/1 (Rev. 1)[1] の 5.55 項は次のように述べている。

> 「運転要員が自らの責任を達成し、また、その業務で成果が出るのを支援するように設計されなければならず、また、運転上の誤操作の安全に対する起こり易さ及び影響を制限するように設計されなければならない。設計プロセスは、全ての運転状態において運転要員と発電所との間の相互作用を容易にするために、発電所の配置及び設備の配置並びに保守及び検査の手順を含む手順類に対して適切な配慮を払わなければならない。」

8.49. SSR-2/1 (Rev. 1)[1] の 5.56 項は次のように述べている。

> 「ヒューマンマシンインターフェースは、判断や行動に必要な時間に応じて、運転員に包括的であるが容易に扱いやすい情報を提供できるように設計されなければならない。運転員が行動する意思決定をするために必要な情報は、平易にかつ曖昧さのないように提示されなければならない。」

8.50. ヒューマンマシンインターフェースの設計は、参照設計に付随する肯定的な仕組みを保持すべきであり、できの悪い運転経験をもたらしてしまう問題を避けるべきである。

8.51. 安全系の監督管理に要求されるヒューマンマシンインターフェースの設計は、深層防護の原則を適用すべきである。

8.52. I&C 系は、系統状態の変化を検知するため、状況を診断するため、(必要なときに)系統を運転し、手動又は自動操作を検証するために必要な情報を運転員に提供すべきである。

8.53. 満足な設計は、運転員の認知処理能力とともにプロセスに関わる時間的制約事項を

---

[38] 関連施設には、原子力発電所の各号機の運転による影響を受けることがある他の施設(例えば、同一敷地にある別の号機など)を含む。

考慮に入れる。

8.54. 設計は、何らかの制御器を操作してから制御系によって入力が認識されるまでに要する最長の時間が運転員に容認できるものであることを確実なものとすべきである。

8.55. I&C 系の設計は、系統要件によって指定された時間内に運転員のタスクが実施できることを確実なものとすべきである。

8.56. 速すぎる又は遅すぎる情報の伝達速度及び制御動作は、運転員の能力を減じる可能性がある。

8.57. 操作が正しくない方法で行われるか又は不適切な発電所構成の下で行われることがある場合、可能なところでは、I&C 系は、運転員の過誤を防止し、検知するように設計されるべきである。これは、制御系、監視系及び保護系の設定値変更の妥当性確認を含む。

8.58. I&C 系は、検知可能な運転員の過誤に関する簡潔で理解しやすい通知を提供すべきであり、また、復旧のため簡単で効果的な方法を利用できるようにするべきである。

8.59. 単一の運転員の過誤が原子炉の制御の喪失につながらないようにすべきである。

8.60. ヒューマンマシンインターフェースは、以下であるべきである。

(a) 実行可能な限り、系統に関わると予想される多くの職種の運転要員の異なる役割と責務に合わせるべきである。
(b) 設備の安全な運転に責任を負う運転員の役割に最大限の注意を払って設計されるべきである。
(c) 制御室要員チームに共通の状況認識の形成を支援するべきである。例えば壁掛けされた大型の発電所状態表示装置。
(d) 発電所の状態に関する効果的な概要を提供するべきである。
(e) 実行可能な限り、機能及びタスク要件と整合する最も簡単な設計を適用するべきである。
(f) 運転員の訓練に対する依存度を最小限にするように設計されるべきである。
(g) 運転員によって素早く認識、理解できるように情報を表示するべきである。[39]
(h) 制御操作の重大な中断なしに、アナログ及びビデオ表示装置の故障に適応させるべきである。
(i) 人の生理学的特性[40]、人の運動制御特性及び人体測定学に関する考慮を反映するべきである。

8.61. ヒューマンマシンインターフェース、手順書、訓練体制及び訓練は、互いに整合性のあるものであるべきである。

8.62. 情報の表示は、発電所の状態及び発電所を制御するために必要な活動についての運転員の理解を最適化する調和のとれた配列にまとめられるべきである。

8.63. ヒューマンマシンインターフェースの運用及び外観は、情報間で並びに制御装置の位置及びプラットフォームを通して整合しているべきであり、高度な標準化に反映するべきである。

8.64. 全ての記述式の識別票及び標識に対して、単一の言語及び互換性のある表記文字の

[39] 容易に理解される形での情報の表示は、運転員の認識作業負荷を低減する。この手引きを満たすヒューマンマシンインターフェースの設計は、例えば、運転員が暗算と変換を行い、再現メモリを使う必要性を最小化する。
[40] 人の生理学的特性には、例えば、視覚／聴覚及び生体力学（届く範囲及び運動）を含む。

使用が検討されるべきである。

8.65. I&C 系の全ての面（制御装置及び表示配列を含む）は、運転員によって使われるメンタルモデル及び確立された慣例と整合しているべきである。

8.66. メンタルモデルは、運転員の理解及び系統がどう振る舞うかの予測を組み入れている。そのようなモデルは、訓練、手順書の使用及び経験を通じて作成される。

8.67. 各種の制御及び表示に対する慣例は、設計において決められ、しかる後に、制御装置及び発電所状態の表示装置の特定、配置及び配列において全面的引き継がれる。

ヒューマンーオートメーションの相互作用の検討事項

8.68. 人と I&C 系に対する I&C 系機能の適切な割り付けの決定手法は、体系的であるべきであり、また、整合的に適用されるべきである。

8.69. 人と機械の間での機能の割り付けに影響を与えることがある要因は、以下を含む。

- 全ての運転モードにおける人の潜在的な作業負荷
- 精度と反復性に対する要件
- 時間的要因
- 必要とされる意思決定及び行動論理の種類及び複雑さ
- 環境要因
- 人間の生理学及び人体測定学

8.70. SSR-2/1 (Rev. 1)[1] の 5.59 項は以下のように述べている。

> 「運転員が短時間の間に介入する必要性は最小限に留められなければならず、また、運転員が行動を意思決定するための十分な時間及び行動するための十分な時間を持っていることが実証されなければならない。」

8.71. 運転員が信頼をもって時宜にかなった適切な手動操作をできないとき又は手動制御への依存が運転員に合理的でない負荷を与えるおそれがあるときは、I&C 系は自動操作を提供すべきである。

8.72. I&C 系は、それぞれの自動機能を監視するのに必要な情報を運転員に提供すべきである。

8.73. I&C は、自動操作を検証するために複数の手段を運転員に提供すべきである。

8.74. 自動機能を監視するために提供される情報は、運転員が効果的に監視できる速度と詳細さ（例えば、目的物若しくは目標の特定又は検証の機会）で表示されるべきである。

8.75. I&C は、運転員が発電所を制御し、安全を維持するために必要なそれぞれの機能を手動で開始又は制御できるようにすべきである。

計測制御系のタスク設計に関する検討事項

8.76. 運転員の役割は、要員が発電所に関しての精通度を維持し、行動に負の影響をそれほど及ぼさないが注意力を維持するのに十分な水準の作業負荷を維持することができる、目的を持った有意義なタスクで構成されているべきである。

8.77. I&C は、タスク分析によって必要と特定された全ての特性を持つべきである。

8.78. タスク分析は、全ての発電所状態、全ての発電所の運転モード及び運転要員の全てのグループ、例えば、原子炉運転員、タービン運転員、当直監督者、現場運転員、安全技術者並びに運転及び保守職員を考慮すべきである。タスク分析は、表示情報の正確さと精度、系統応答時間、物理的配置、制御装置の型式、表示装置及び警報装置並びに情報表示装置内のソフト制御の統合などの I&C の特性に関する設計入力を提供すべきである。

8.79. ヒューマンマシンインターフェースは、タスクの実施に利点を提供する場合は、ビデオ表示装置上の表示装置及び制御装置がそのタスクにとって最も便利な構成で形式化されることを許容すべきである。

8.80. このような構成化が有益である場合の例は、様々な構成が様々な水準の運転員経験とより適切に順応できることがある場合又は様々な構成が様々な運転モードにおいてより有効であることがあるような場合を含む。

8.81. ヒューマンマシンインターフェースの全ての面（形式、専門用語、順序付け、グループ化及び運転員に対する意志決定支援装置）は、タスク要求事項に基づく明白な論理又は一部ではその他の恣意的でない理論的根拠を反映すべきである。

8.82. 関連するタスク及び機能に対する、それぞれの表示、制御及びデータ処理支援との関連性は明確であるべきである。

8.83. ヒューマンマシンインターフェースは、タスク分析の結果と整合した方式及び形式で、情報を運転員に示すべきである。

8.84. I&C は、タスク分析によって特定された潜在的な運転員の行動の範囲を対象とする制御上の選択肢を提供すべきである。

8.85. I&C は、運転員に行動を行うための複数の手段を与えるべきである。

8.86. I&C は、運転員が最小数の行動でタスクを完了できるようにするべきである。

接近性及び作業環境に関する検討事項

8.87. SSR-2/1 (Rev. 1)[1] の 5.61 項は、「運転要員の作業場所と作業環境の設計は、人間工学の概念にしたがっていなければならない。」と述べている。

8.88. 運転要員が発電所の系統を監視し、制御することが予測される区域においては、作業環境において適した条件を確保し、危険性のある状態から保護するために必要な方策が取られるべきである。

8.89. 考慮されるべき作業環境の通常の側面には、照明、温度、湿度、騒音、振動を含み、また、連続監視が要求される場合は休憩場所及び洗面所などの施設を含む。

8.90. 考慮されるべきハザードは、大気中の放射線、煙及び有毒物質を含む。

8.91. SSR-2/1 (Rev. 1)[1] の 5.60 項は、以下のように述べている。

> 「発電所に影響を与えるような事象の発生後、制御室内又は補助制御室内及び補助制御室への立入り通路の上の場所における環境条件によって運転要員の防護と安全を損なわないことを確実なものとするよう設計されなければならない。」

8.92. ヒューマンマシンインターフェースの拠点が分散されているときには[41]、運転員は、安全で時間内にこれら様々な場所に立ち入る手段を持つべきである。

8.93. 適した立ち入り手段を設定する一つの方法は、補助制御場所及び運転員操作が発生すると予測されるその他の現場へ、潜在的な内的ハザード又は外的ハザードから保護するための方策を備えた、適格性が保証された経路を提供することである。

過去データの記録作成

8.94. ヒューマンマシンインターフェースは、過去の情報を記録、保管及び表示する能力を備えるべきであり、このような表示装置が、運転要員がパターンと傾向を特定し、系統の過去又は現在の状態を理解し、異常事象発生後の分析を実施し、又は将来の進展を予測することを助けることになる。

9. ソフトウェア

全般

9.1. 本章における推奨事項は、安全上重要な I&C 設備の中で適用又は安全上重要な I&C 設備自体への適用のための全ての種類のソフトウェア、例えば、オペレーティングシステム、事前開発のソフトウェア若しくはファームウェア、特定計画用に特別に開発されたソフトウェア又は既存の事前に開発された一連のハードウェア若しくはソフトウェアモジュールから作成されるべきソフトウェアに適用する。

9.2. デジタルシステムは、信頼性の評価に関してアナログシステムと異なる取り組み方を要求する。信頼性は、作成活動の品質の評価並びに検証及び妥当性確認の結果から推定される。ソフトウェアは、その性質及び中身によって、(電気的又は機械的な) ハードウェアよりもはるかに大きな設計余地を許容する。体系的に制約されなければ、それは瑕疵となりやすく、かつ検証不可能なものとなりうる。ソフトウェアの具体化における複雑さは、設計における追加の欠陥を作りだすことができ、欠陥を検知し、是正する際の困難さを増加させることができ、より単純な設計では存在しない故障モードと影響をもたらすことができ、また、独立性、試験可能性及び信頼性などの安全系の設計判断基準の遵守のあらゆる実証における確信度を低下させることができる。

9.3. 第 2 章で提示されているマネジメントシステム及びライフサイクルプロセスに関する手引きは、対象範囲とされている活動がソフトウェアの効果的な開発に必要であるため、特にソフトウェアに関連している。

9.4. SSR-2/1 (Rev. 1)[1] の要件 63 は、以下のように述べている。

「原子力発電所の安全上重要な系統がコンピュータを基にした設備に依存する場合、

[41] 分散されたヒューマンマシンインターフェースの拠点の事例には、補助制御室及び運転員の操作が生じると予想されるその他の現場を含む。

系統の供用期間、特にソフトウェアの開発期間を通して、コンピュータのハードウェアとソフトウェアの開発と試験実施に対する適切な基準及び手法が制定され、実施されなければならない。また、開発全体が、品質マネジメントシステムの対象とされなければならない。」

9.5. 系統用のソフトウェアの開発は、事前に定義されたライフサイクルに従い、正式に計画され、文書化され、また、徹底した検証及び妥当性確認を含むべきである（第 2 章を参照）。

ソフトウェア要件

9.6. I&C 系の要件を満足させるために必要な全てのソフトウェアは、再使用されたコード又は自動的に作成されたコードを含めて、本章における推奨事項に適合する適切な形式で文書化された要件を持つべきである。

9.7. ソフトウェア要求事項は、系統の安全上の重要性に見合った、事前に定められた技法の組み合わせを使用して設定されるべきである。

9.8. 要件を設定する技法は、明確に定義された構文と語義を有する仕様言語、モデル、分析並びに審議の使用を含むことがある。

9.9. ソフトウェア要求事項の開発者は、第 3 章に記された系統に対する基礎的な設計基準についての適切な理解を持っているべきである。

9.10. 系統設計基準を理解することは、ソフトウェア要求事項が系統の必須な特性を適切に満足させることを保証するために必要である。関連のある課題は以下を含む。

- 潜在的な故障条件
- 運転モード
- 安全目的のための監視
- 自己観察
- 故障の検出
- 検知されたが復旧不可能な故障の発生時に達成されるべき安全状態
- その他のフェールセーフ挙動
- 安全に関連する入力と出力の関連性

9.11. ソフトウェア要求事項についての仕様は以下であるべきである。

(a) 個々のソフトウェア品目が何をすることを要求されているか、また、それが系統の他の機器等とどのように相互作用することになるかを定義すべきである。
(b) I&C ライフサイクルの関連プロセス（以前の分析で特定された系統のハザードの検討を含む）を元に、また、例えば人間工学及びコンピュータ・セキュリティ活動のような、I&C ライフサイクルと取り合いのあるプロセスを元に作成されるべきである（12 頁の図 2 を参照）。
(c) 可能な限り、どのように設計され、実装されるかより、何が達成される必要があるかについて記述されるべきである。
(d) 完全で、曖昧さがなく、整合的で、読み易く、対象者（例えば、特定分野の専門家、安全技術者及びソフトウェア設計者）にとって理解可能で、検証可能であり、かつ追跡可能であるべきである。
(e) 品質要件を含め、ソフトウェア品目に割り当てられた系統要件を満足させるべきである。

(f) 必要に応じて、要求される最低限の正確さ、数値的精度、取合いの説明[42]、演算実行経路の独立性、自己観察、時間的性能[43]及びセキュリティ[44]について規定すべきである。
(g) 達成されるべき必要なレベルの信頼性及び稼働性[45]を含むべきである。
(h) コンピュータ、ソフトウェアツール及び既存の類似のシステムが、ソフトウェア要求事項が実現できることを保証する能力を可能とすべきである。
(i) 対象使用者に対して適用可能な追加情報、例えば、特定の要件に関する背景情報、機能若しくは安全の仕組みの設計に関するリスクの検討事項若しくは推奨事項などの追加情報を、対象使用者に理解可能であることを保証するために必要な範囲で引用するか、それらを含むか、又はそれらによって補完されるべきである。
(j) ソフトウェアが実施しない、特別に重要なあらゆる機能、挙動又は相互関係を定義すべきである。

9.12. 設計上の制約事項が必要なところでは、それらは、指定され、正当性化され、追跡可能であるべきである。

9.13. 全てのソフトウェア要求事項の根源は、検証、妥当性確認、より高位文書への追跡可能性及び全ての関連要件が取り組まれたとの実証を容易にするために十分に文書化されるべきである。

9.14. 要件の追跡システムは、開発プロジェクトの設計、実装、統合及び妥当性確認の段階を通じてソフトウェア要求事項が追跡できるように使用されるべきである。

9.15. 安全上重要なソフトウェア要求事項は、そうであると特定されるべきである。

ソフトウェア設計

9.16. 完了したソフトウェア設計は、曖昧さがなく、ソフトウェア要求事項に関して正確かつ実証面で完全で、整合性があり、よく構築され、読み易く、対象者（例えば その分野の専門家、安全技術者及びソフトウェア設計者）に理解可能で、検証可能で、妥当性確認が可能で、追跡可能で、保守が可能で、文書化されているべきである。

9.17. ソフトウェア設計は、系統の安全上の重要性に見合った、技法の事前に決められた組合せを使用して確立され、最新の状態に保持されるべきである。

9.18. このような技法には、説明書、明確に定義された構文及び語義を有する論理図及び図形表現、モデル、分析並びに審議を含むことがある。

9.19. ソフトウェア設計は、安全要件の根源についての理解を持って開発されるべきである。

9.20. ソフトウェア設計の部品は、設計を通じて要件の有用な追跡性を可能にするために、十分に区別されるべきである。

9.21. 安全系向けのソフトウェアの設計は、全体構造、外部との取合い、モジュール間の

---

[42] 取合いの事例には、ソフトウェアと運転員との間の、検出器と起動装置との間の、コンピュータハードウェアと他のソフトウェアとの間の及びシステムの間の取合いを含む。
[43] 時間的性能には、故障検出及び復旧時間を含む。
[44] セキュリティの事例には、妥当性点検及び立ち入り権である。
[45] 信頼性と稼働性のレベルは、9.11 項の(a)～(f)に引用されている支援的ソフトウェア要件及び作成プロセス(標準の遵守)のような形で、定量的に又は定性的に定義されることがある。

内部取合い及び詳細設計を含む全ての階層で単純さを最大化すべきである。

9.22. 設計における単純さは、安全を達成し実証することの主要な手段であるが、常に、例えば、機能、柔軟性及び所要経費との得失を含むことになる。9.21 項の推奨事項は安全系統にのみ適用するが、単純さは、より低い安全クラスの系統のソフトウェアに対する有益な目標である。より低い安全クラスの系統に関しては、安全と複雑さとの間のつり合いは異なるものであり、より高い複雑さが受け入れられる場合がある。

9.23. ソフトウェア設計の構造は、将来の改造、保守及び改良を可能にするよう構成されるべきである。

9.24. ソフトウェアの構造は、等級付けされた抽象化レベルを備えるために階層的であるべきである。

9.25. 情報を見えなくする技法の使用は、可能なところでは、部分ごとの審査及び検証を可能にし、改造を支援するために奨励される。

9.26. ソフトウェア設計は、ソフトウェアとその外部環境との間の取合いを含むべきである。

9.27. ソフトウェア設計は、全てのソフトウェアモジュールの詳細設計を含むべきである。

9.28. ソフトウェアモジュールの説明は、その機能、他のモジュールとの取合い及び全体ソフトウェアの中での機能の関連性を完璧に定義すべきである。

9.29. 類似の機能を実施するソフトウェアモジュールは、整合性のある構造を持つべきである。

9.30. モジュールの取合いは、整合しているべきである。

9.31. モジュール間の各取合いの相対する両側は一致すべきであり、モジュールの入力及び出力の取合いの変数名の使用は整合しているべきであり、また、可能な限り、再帰呼出しは避けられるべきである。

9.32. システムが多数のプロセッサを含み、ソフトウェアがこれらの中で分散されているのであれば、ソフトウェア設計は、どのソフトウェアプロセスがどのプロセッサ上で動いているか、また、データと表示装置がどこに配置されるかを定義すべきである。

9.33. ソフトウェア設計は、安全系の確定的な挙動及び時間設定を支援すべきである。

9.34. 情報伝達プロトコルは、7.79 項 ～ 7.94 項の推奨事項を遵守すべきである。

9.35. 設計が精緻化されるにしたがって、欠陥検出及び自己観察のための追加的な仕組みの必要性が検討されるべきで、これはソフトウェア設計に含まれるべきである（6.166 項 ～ 6.172 項を参照）。

9.36. 故障の検出時に、系統が安全な状態に維持されていることを確保するために、復旧、手順書の中断並びに過誤の情報提供及び記録履歴の点でのソフトウェア要求事項を満たすために、適切な行為が取られるべきである。

9.37. ソフトウェア設計文書は、設計段階期間中に、守られることを必要とする実装に関する制約事項を含むべきである。

9.38. 実装時におけるこのような制約事項は、多様性並びにプログラム言語、コンパイラ、サブルーチン・ライブラリ及びその他の支援用ソフトウェアツールについての特殊な属性を確実なものとするあらゆる必要性を含む場合がある。

9.39. このような制約事項は、正当化されるか又はより高位の要件若しくは制約事項に対して追跡可能であるべきである。

9.40. 安全系統以外の系統に関しては、独自仕様のシステムに対する実装時の制約事項が供給者から提供された標準文書に対して追跡できることが十分である場合がある。

9.41. ソフトウェア設計の構造は、多様性を適用するための決定から生じることがある、モジュール及び取合いに対する制約事項を考慮に入れるべきである。

9.42. ソフトウェア設計は、情報セキュリティに関しては、マルウェア又はハッカーによる悪用が容易でかつ復旧が困難な、設計による脆弱性の発生を避けるために、最良事例を考慮に入れるべきである。

9.43. ソフトウェア設計は、適切な場合は、ピアレビューを受けるべきである。

ソフトウェアの実装

9.44. ソフトウェアの実装は以下であるべきである。

- ソフトウェア要求事項に関して正確かつ完全であり、また、設計に関して完全であり、良く構成されており、読み易く、検証可能で、追跡可能で、保守可能で、適切に文書化されているべきである。
- 言語、ソフトウェアツール、コード作成の実践、分析、審議及び試験実施を対象とする、系統の安全上の重要性に相応した技法の事前に決められた組み合わせを用いて確立されるべきである。
- 全てのソフトウェア要求事項及びソフトウェア設計に実証的に取り組むべきである
- プログラム作成の容易さを優先しつつ、読み易さ及び保守性を伴う単純で容易に理解可能であるべきである。
- ソースコードと演算コードの読み易い方式、装置取合い試験とモジュール取合い試験の結果及びコード仕様に関するコードの正確さを検証するための十分な文脈情報を含むべきである。

9.45. 全てのコードは、適切に文書化されるべきである。

9.46. 安全系に関しては、コードの全ての部品に関する文書の利用可能性（演算時間支援コード及び欠陥監査機能を含む）が、本安全指針の試験実施手引きが満たされることを可能にすることになる。

9.47. コード作成規則は、コード作成が始まる前に規定されるべきであり、また、規則の遵守が検証されるべきである。

9.48. データの構成及び命名の慣例は、整合性をもって適用されるべきである。

9.49. ソフトウェアの実装は、以下に従っているべきである。

- 変更管理用に定義された手順書（影響分析を含む）
- 構成管理
- 全ての変更結果に対して適切な試験範囲を確保すること

9.50. 使用されるプログラム言語（又は言語セット）は、表現力、セキュリティがない状態の回避、抽象化のレベル、モジュール化及び情報の非表示の支援、コンパイル及び演算時間の点検並びにエラーの取扱いに関して適切であるべきである。

9.51. 安全系に使用されるプログラム言語は、単純な実装を支援すべきである。

9.52. 使用されるプログラム言語及び機能の定義方法（論理図又は図形表現のような）の選択は、関連するプロセスの機能性及び健全性に関する要件の体系的評価に基づくべきである。

9.53. 安全系に関しては、プログラム言語の選択は、正当化され文書化されるべきである。

9.54. 安全系に関しては、言語の構文と語義は完全で、利用可能で、また、厳密に定義されるべきである。

9.55. ソフトウェア関数は、特定の業務を実施するプログラム作成の要素である。これらは、ライブラリに含まれるか又は事前に別途開発されたプログラム言語に固有のものであることがある。

9.56. ソフトウェア関数は、単純さを最大化する目的を持って使用されるべきであり、また、特定され、よく定義された取合いを持ち、常にこれらの使用に関して関連する制限事項にしたがって呼び出されるべきである。

9.57. オペレーティングシステムが使用されているのであれば、それは、徹底的にかつ満足いくまで試験されるべき又はされているべきであり、目標とする適用に対する適正さが正当化されるべきである。

9.58. 安全系に関しては、あらゆるオペレーティングシステムのソフトウェアは、本安全指針の全ての推奨事項を遵守すべきである。

9.59. 実装のための適正な一連のソフトウェアツールは、エラーを最小化する目的で選択されるべきである。関連する推奨事項については、7.148 項 ～ 7.164 項を参照のこと。

9.60. 本章の推奨事項は、コード生成と古典的なソフトウェアの開発の使用についての想定しうる全ての組合せに適用する。

9.61. ソフトウェアの多様性（すなわち、独立した開発チームの使用及び／又は異なる方法、言語、時間設定、機能の順序若しくはアルゴリズム）は、ソフトウェアにおける共通原因故障の発生可能性及び影響を低減させる手段と見なされる場合がある。しかし、ソフトウェアの多様性は、それ自体が新たな故障に繋がり得る設計制約事項を導入しうる。

9.62. 異なる深層防護階層を支援する系統間における独立性が、オペレーティングシステム、ネットワークの情報伝達、又は他の演算支援ソフトウェアなどの同一のソフトウェアの使用によって損なわれないことを保証するために、予防措置が取られるべきである。

9.63. ソフトウェアを実装するチームは、保証された開発技法について訓練されるべきである。

ソフトウェアの検証及び分析

9.64. ソフトウェアの要件、設計及び実装は、I&C 系の要件の仕様に対して検証されるべきである。

9.65. 追跡可能性の検証は、欠落ができるだけ早く取り組まれ、それにより必要な変更が実行できることになっていることを確実なものとするための継続的な活動であるべきである。

9.66. ソフトウェアのライフサイクルにおける各段階の結果は、前の諸段階によって設定された要件に対して検証されるべきである。

9.67. 以下のことを文書化したソフトウェア検証計画が作成されるべきである。

(a) 使用されるべき検証技法
(b) その対象と深さを含め、各技法を適用する際に使用されるべき手順書の詳細又は参考文献
(c) 非機能的要件及び制約事項が満たされていることがどのように実証されることになるか
(d) 前段階の出力に関する完全性及び機能試験の構造的な範囲に対する目標を含め、十分な検証がいつ行なわれたか、また、これらがどのように実証されることになるかを判断する基準
(e) 結果が記録されることになる手段
(f) 不履行及び欠陥が記録され、また、解決されることになる手段
(g) 検証を実施する単独又は複数のチーム及びこれらのチームがソフトウェア設計者から独立していること
(h) ソフトウェアツールがどのように使用されるべきかに関する予想及び制限を含む、あらゆる検証用ソフトウェアツールの機能性（例えば、領域、言語及びプロセス）
(i) 上記の（a）～（h）項に列挙された各要素に関する論理的根拠及びこれが適用される安全クラスの系統のソフトウェアのための検証が十分となることの正当性。

9.68. 検証は、以下の技法を含むべきである。

- 審議、実地検証、検査及び監査などのマニュアルの詳細調査
- ソースコードの静的分析
- 動的分析

9.69. 静的分析は、ソフトウェアの最終版で実施されるべきである。

9.70. 使用される静的分析技法は、系統の安全上の重要性に従って異なることになる。静的分析は、設計及びコード作成標準の遵守、管理の分析、データ及び情報の流れ、代表入力による性能確認並びに公式なコード検証などの技法を含む。

9.71. ソフトウェアの中に実装された全ての非機能的要件は検証されるべきである。

9.72. 関連する運転経験は、是正対象の逸脱を特定するために、また、ソフトウェアの信頼性に対して更なる確信を提供するために使用されるべきである。

9.73. 関連する運転経験は、他の検証技法を補足することはできるが、代替はできない。

9.74. 7.148 ～ 7.164 項は、ソフトウェアの検証及び分析のためのツールの使用に関連した手引きを提示する。

9.75. ソフトウェア実装の検証及び妥当性確認に関して、試験方針（例えば、ボトムアップ又はトップダウンの方針）が決定されるべきである。

9.76. 試験ケースの仕様書は、以下についての試験の適切な実施を保証すべきである。

- 取合い（モジュール間の取合い、ソフトウェアとハードウェア間の取合い、システム境界の取合いなど）
- データ通過メカニズム及び取合いプロトコル
- 除外条件
- 各入力変数の全範囲（同等クラスの分割及び境界値解析などの技法を使用して)
- システムの運用の全モード

9.77. 回帰試験を容易にするため、試験計画は、試験が繰り返し可能であること及び試験結果が記録されていることを確実なものとすべきである。

9.78. 反復試験に要求される人間の介入を最小化することも望ましい。

9.79. GS-G-3.1 [3]は、試験に使用される測定及び試験設備の適切性を確保することに関する手引きを提示する。

9.80. 試験ケースの仕様書及び試験の有効性は、審議されるべきであり、また、検証計画における目標に対するあらゆる未達事項は、全て解決されるか又は正当化されるべきである。

9.81. 検証は、設計者及び開発者から独立したチーム、個人又は組織されたグループによって行われるべきである。

9.82. コードは、自動化されたソフトウェアツールを使用して、ソフトウェアのセキュリティ上の脆弱性を点検するために審査され、また、コードの最重要部分についての人手による審査によって補完されるべきである（例えば、入出力の取扱い及び例外の取扱い）。

9.83. I&C 系の全ての出力は、検証期間中を通じて監視されるべきであり、また、予想された結果からのあらゆる逸脱は調査され、文書化されるべきである。

9.84. 検証計画（例えば、試験の実施範囲というような）に対する検証結果におけるあらゆる欠落は、解決されるか、正当化されるべきである。

9.85. 検知されたあらゆるエラーは、原因を分析されるべきであり、また、合意された変更手順及び適宜回帰試験実施によって修正されるべきである。

9.86. エラーの分析には、I&C 系の他の部分への適用可能性の評価を含むべきである。

9.87. 発見された逸脱の件数及び種類の記録は、維持され、開発プロセスに対する知見のために再検討され、また、現在及び将来のプロジェクトの便益のため適切なプロセスの改善を具体化するために使用されるべきである。(GS-G-3.1 [3] の 6.50 項 ～ 6.77 項及び GS-G-3.5 [4] の 6.42 項 ～ 6.69 項を参照)

9.88. 検証及び分析の文書は、開発プロセスの生成物が完全で、正しく、かつ整合性があるとの首尾一貫した一連の証拠を提示すべきである。

9.89. 試験記録を含む検証結果は、文書化され、維持され、また、品質保証監査及び第三者評価のために利用可能な状態に保たれるべきである。

9.90. 設計文書の追跡可能性は、ライフサイクル各段階の文書と機能要件との間の連続的な関連性を含むべきである。

9.91. 試験結果の文書は、試験ケースの仕様書と相互に追跡可能であるべきであり、また、どの結果が期待事項を満たさなかったか及びこれらが如何に解決されたかを示すべきである。

9.92. 試験の対象範囲は、明確に文書化されるべきである。

9.93. 安全系に関しては、ソフトウェアの要件、設計、実装及び試験の間のつながりを示す追跡可能な配列を使用して、各々の試験ケースを追跡することが可能であるべきである。

9.94. 安全系に関しては、結果として生じたアプリケーションは、コンピュータ・セキュリティ（侵入試験などの）を確保するために、共通的なセキュリティの脆弱性が検知困難であることを確認するために、また、ソフトウェアの設計及び実装の継続的な改善を可能にするために、試験実施に供されるべきである。

9.95. 試験文書は、同じ結果が達成されることになるとの確信をもって試験プロセスが繰り返されることを可能にするために十分であるべきである。

事前開発のソフトウェア

9.96. 安全系に関しては、I&C 安全系で使用される事前開発ソフトウェアは、その適用のために特別に記述されたソフトウェア向けのものと同程度の性能保証を有しているべきである。

9.97. 事前開発されたソフトウェア関数は、2.108 項 ～ 2.117 項の推奨事項を遵守すべきである。

9.98. 安全系ではない安全上重要な系統に関しては、事前開発ソフトウェアは、以下を記載する使用者文書を有するべきである。

(a) 具備される機能
(b) 役割、種類、形式、範囲並びに入力、出力、除外信号、パラメータ及び構成データに課された制約事項を含む取合い
(c) 該当するものがあれば、挙動の異なるモード及び対応する移行の条件
(d) 事前開発ソフトウェアを使用するときに満たされるべきあらゆる制約
(e) 事前開発ソフトウェアが、上述の（a）～（d）項の使用者文書の記述に関して正確であることの正当性
(f) 機能が I&C 系に対して適していることの正当性

ソフトウェアツール

9.99. ソフトウェアツールに関する推奨事項は、7.148 項 ～ 7.164 項に提示されている。

第三者評価

9.100. 安全系ソフトウェアの第三者評価は、ソフトウェアの開発プロセスと同時に行なわれるべきである。

9.101. このような第三者評価の目的は、系統及びそのソフトウェアの妥当性に関する見解を提供することであり、その見解は、系統とソフトウェアの一方か両方の供給者及び運転組織の両者から独立しているものである。このような評価は、規制機関によって又は規制機関の容認する組織によって実施される場合がある。

9.102. 第三者評価を可能とするためにソフトウェアの作成者と適切な取り決めがなされることが重要である。

9.103. この評価は、以下の詳細調査を含むべきである。

- 開発プロセス（例えば、計画書、ソフトウェア仕様書及び試験活動の全体範囲などの、ライフサイクル文書の詳細調査を含む、品質保証監査及び技術検査を介して）
- 最終的なソフトウェア（例えば、静的分析、検査、監査及び試験を介して）。これにはその後のあらゆる改造を含む。

参考文献

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006). (A revision of this publication is in preparation, to be issued as GSR Part 2.)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Modifications to Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.3, IAEA, Vienna (2001).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, IAEA, Vienna (2010).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Commissioning for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-28, IAEA, Vienna (2014).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.6, IAEA, Vienna (2002).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[18] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[19] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-

1.7, IAEA, Vienna (2004).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.12, IAEA, Vienna (2009).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, The Operating Organization for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.4, IAEA, Vienna (2001).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Conduct of Operations at Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.14, IAEA, Vienna (2008).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.13, IAEA, Vienna (2005).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004)

.

添付資料 I

国際的な計測制御標準の参考文献

I-1.　SSR-2/1 (Rev. 1)[I-1] の要件 9 は、「安全上重要な機器等の設計基準は、原子力発電所の存続期間にわたって具体的な容認基準を満たすために、関連する運転状態、事故状態並びに内的ハザード及び外的ハザードから生じる状態に対して必要な能力、信頼性及び機能性を定めなければならない。」と述べている。

I-2,　本安全指針は、IAEA 加盟国の間で広く受け入れられている高水準の推奨事項を提示している。IAEA によって提示される手引き以上に、SSR-2/1 (Rev. 1)[I-1] の遵守を裏付ける設計方法及び系統特性についてのより詳細な推奨事項を与える多数の国内標準及び国際標準が存在する。設計者、使用者及び規制機関は、これらの標準の中の情報を活用することが期待されている。

I-3.　原子力発電所において計測制御（I&C）に対して国際的に使用されている標準の大部分に対しては、2 つの標準作成組織が責任を負っている、すなわち、(a) 国際電気技術委員会（IEC）の小委員会 45 及び（b）電気電子技術者協会（IEEE）の原子力技術委員会である。各組織は、多数の標準を策定した。両組織は、SSR-2/1 (Rev. 1)[I-1] の要件及び本安全指針の推奨事項の基礎となる共通の原則に対応する標準を作成している。したがって、一連の標準のいずれもが、本安全指針の推奨事項をさらに解釈するために使用することができる。

I-4.　本添付資料は、読者が本安全指針と IEC 及び IEEE の標準との間の関係を理解する上で助けとなることを意図したものである。表 I-1 は、本安全指針の推奨事項と緊密な関係がある IEC 及び IEEE 標準を列挙している。表 I-1 は、これらの標準の完全なリストではない。しかし、これは、IEC 及び IEEE の基準への手掛かりを特定するものである。

I-5.　表 I-2 は、これらの記載標準が、本安全指針の主要な主題の分野とどのように関連しているかを示している。

表 I-1　本安全指針と緊密な関連を持つ国際標準

IEC 60515	原子力発電所 － 安全上重要な計測 － 放射線検出器 － 特性と試験方法
IEC 60568	原子力発電所 － 安全上重要な計測 － 発電用原子炉内の中性子フルエンス率（中性子束）測定のための炉心計測
IEC 60671	原子力発電所 － 安全上重要な計測制御系 － サーベイランス・試験の実施
IEC 60709	原子力発電所 － 安全上重要な計測制御系 － 分離
IEC 60737	原子力発電所 － 安全上重要な計測 － 温度検出器（炉心及び一次冷却回路） － 特性及び試験方法
IEC 60780	原子力施設 － 安全上重要な電気設備 － 適格性性能保証
IEC 60880	原子力発電所 － 安全上重要な計測制御系 － カテゴリー A の機能を実施するコンピュータベースシステムに関するソフトウェアの側面
IEC 60964	原子力発電所 － 制御室 － 設計
IEC 60980	原子力発電所に関する安全系統の電気設備の耐震上の適格性性能保証に関して推奨事項されたプラクティス
IEC 61226	原子力発電所 － 安全上重要な計測制御 － 計測制御機能のクラス分け
IEC 61468	原子力発電所 － 炉内計測 － 自己出力形中性子検出器の特性及び試験方法
IEC 61500	原子力発電所 － 安全上重要な計測制御 － カテゴリーA 機能を実施するシステム内のデータの情報伝達
IEC 61501	原子炉計測 － 広範囲な中性子フルエンス率メートル － 平均平方電圧法
IEC 61513	原子力発電所 － 安全上重要な計測制御 － システムに関する一般的要件
IEC 61772	原子力発電所 － 制御室 － 視覚的表示装置（VDU）の適用
IEC 61839	原子力発電所 － 制御室の設計 － 機能の分析と割付け
IEC 61888	原子力発電所 － 安全上重要な計器 － トリップ設定値の確定及び保守
IEC 62003	原子力発電所 － 安全上重要な計測制御 － 電磁適合性試験の実施要件
IEC 62138	原子力発電所 － 安全上重要な計測制御 － カテゴリーB 又は C の機能を実施するコンピュータベースシステムのソフトウェア側面
IEC 62241	原子力発電所 － 中央制御室 － 警報の機能と実演
IEC 62340	原子力発電所 － 安全上重要な計測制御系 － 共通原因故障（CCF）に対する対処要件

IEC 62397	原子力発電所 ー 安全上重要な計測制御 ー 抵抗温度検出器
IEC 62566	原子力発電所 ー 安全上重要な計測制御 ー カテゴリー A 機能の実施システムのために HDL をプログラムされた集積回路の開発
IEC 62671	原子力発電所 ー 安全上重要な計測制御 ー 機能が制限された産業用デジタル機器の選択と使用
IEEE Std. 1023	原子力発電所及び他の原子力施設の系統、設備及び施設への人間工学の適用に関する IEEE 推奨事項のプラクティス
IEEE Std. 308	原子力発電所の 1E クラス電源系統に関する IEEE 基準の判断基準
IEEE Std. 323	原子力発電所の 1E クラス設備の適格性性能保証のための IEEE 基準
IEEE Std. 338	原子力発電所の安全系統の定期的サーベイランスと試験実施の判断基準に関する IEEE 基準
IEEE Std. 344	原子力発電所設備の耐震上の適格性性能保証に関する IEEE 基準
IEEE Std. 379	原子力発電所の安全系統に対する単一故障判断基準の適用に関する IEEE 基準
IEEE Std. 384	1E クラスの設備と回路の独立性に関する IEEE 基準の判断基準
IEEE Std. 497	原子力発電所の事故モニタリング計器に関する IEEE 基準の判断基準
IEEE Std. 603	原子力発電所の安全系統に関する IEEE 基準の判断基準
IEEE Std. 7-4.3.2	原子力発電所の安全系統のデジタルコンピュータに関する IEEE 基準の判断基準
IEEE Std. 1012	ソフトウェアの検証及び妥当性確認に関する IEEE 基準
IEEE Std. 1074	ソフトウェアのライフサイクルプロセス開発のための IEEE 基準
ISO/IEC 15288	システムとソフトウェア工学 ― システムのライフサイクルプロセス
ISO/IEC 12207	システムとソフトウェア工学 ― ソフトウェアのライフサイクルプロセス

注記： ISO： 国際標準化機関。

表 1-2. 本安全指針と緊密な関連を持つ国際標準

本安全指針	国際的に使用されている 計装制御系の基準
1. はじめに	
2. I&C 系設計のためのマネジメントシステム	IEC 61513, IEEE 7-4.3.2
— ライフサイクルモデルの使用	IEC 61513, IEEE 7-4.3.2, ISO/IEC 15288
3. I&C 系の設計基準	IEC 61513, IEEE 603
— I&C 機能の特定	IEC 61226
— I&C 系の設計基準の内容	IEC 61513
4. I&C 構造	IEC 61513, IEC 62340
5. I&C の機能、系統及び設備の安全分類	IEC 61226
6. 安全上重要な全ての I&C 系に関する全般的推奨事項	
— 全般	IEC 61513, IEC 60709, IEEE 379, IEEE 384
— 設備の性能保証	IEC 60780, IEC 980, IEC 62342, IEEE 344、 IEEE 323, EC 2003
— 経年変化と旧式化に対処するための設計	
— 安全上重要な系統への立ち入りの管理	IEC 61513
— 運転時の試験と試験可能性	IEC 60671, IEEE 338
— 保守性	IEC 61513
— 試験又は保守のために供用除外の方策	IEC 61513
— 設定値	IEC 61888
— 安全上重要な機器等の標識と識別確認	
7. 個別の I&C 系及び設備の設計手引き	
— 検出装置	IEC 60515, IEC 61501, IEC 60568, IEC 61468, IEC 60737
— 制御系	
— 保護系	IEEE 603
— 電力の供給	IEC 61225, IEEE 308

— デジタルシステム	IEC 61513, IEEE 7-4.3.2, IEC 61500, IEC 62671
— ハードウェア記述言語で構成された装置	IEC 62566
— ソフトウェアツール	IEC 60880, IEC 62138
8. ヒューマンマシンインターフェースの考慮事項	
— 制御室	IEC 60964, IEC 61772, IEC 62241, IEEE 576
— 補助制御室	IEC 60965
— 事故の監視	IEEE 497
— 運転員の通信連絡システム	
— I&C 系の人間工学に関わる全般的原則	IEC 61839, IEC 61772, IEEE 1023, IEEE 1082
— 過去のデータの記録	
9. ソフトウェア	IEC 60880, IEC 62138, IEEE 7-4.3.2, IEEE 1012, IEEE Std. 1074, ISO/IEC 12207

I-6. 本安全指針の推奨事項と IEC 及び IEEE 規格との間の対立点を回避するために協調作業が行われた。本安全指針の策定に参加した IEC と IEEE の両規格委員会の委員と両標準機関は、対立点の特定と解消を手助けするために草案を審議した。

I-7. それにも拘らず、使用者は、IEC 及び IEEE 規格との間には重要な差があるという事実を認識し、それを考慮に入れる必要がある。

I-8. IEC 規格は、その規格策定のための基本的な入力情報として IAEA の安全要件及び安全指針を採用している。結果として、IEC 規格は、安全上重要な機器等に取り組み、全般的推奨事項の元として IAEA により提供された I&C 系に関する手引きを採用している。

I-9. IEEE 規格は、安全機器に大きく重点を置いており、したがって、その手引きは、本安全指針が行っているよりも、より小さな一連の機能、系統及び設備に直接的に適用される。そうであっても、IEEE の手引きは、等級別扱いを使用して、安全関連の機器等（安全系統ではない安全上重要な機器）に適用できる。

I-10. IEEE 規格は、本安全指針を参考文献として採用していない。IEEE 規格 603（表 I-1 参照）は、IEEE 規格の枠組みの中では本安全指針と同等のものである。そうであっても、本安全指針と IEEE 規格は、I&C 系の設計に関する一連の同じ原則に対応している。IEEE 規格は多くの場合、用語「安全」、「安全関連の」及び「1E」を、IAEA 用語「安全」と同等なものとして使用することに注意すべきである。IEEE には、IAEA によって使用されるような「安全関連の」と同等な用語はない。

I-11. 参考文献 [I-2] には、I&C 系の設計に関する標準のより広範な文献が含まれている。

資料Ⅰの参考文献

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
[I-2] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

添付資料 II

本安全指針と IAEA 安全基準シリーズ No. NS-G-1.1 及び NS-G-1.3 との間の相関関係

II‐1. 本添付資料では、先行の安全指針、NS-G-1.1[46]及び NS-G-1.3[47]で対象とされている主題が本安全指針のどこにあるかを示す表を提示している。

表Ⅱ-1. IAEA 安全基準シリーズ No. NS-G-1.1 と本安全指針の関連

IAEA 安全基準シリーズ No. NS-G-1.1	本安全指針
1. はじめに	1. はじめに
2. コンピュータベースシステムに関する技術的検討	2. I&C 設計のためのマネジメントシステム 9. ソフトウェア：全般
3. コンピュータベースシステムの安全についての設計管理に関する要件の適用	2. I&C 設計のためのマネジメントシステム 9. ソフトウェア：第三者評価
4. プロジェクトの計画立案	2. I&C 設計のためのマネジメントシステム
5. コンピュータシステムの要件	2. I&C 設計のためのマネジメントシステム
6. コンピュータシステムの設計	2. I&C 設計のためのマネジメントシステム 6. 安全上重要な全ての I&C 系に関する全般的推奨事項 7. 個別の I&C 系及び設備の設計に対する手引き 8. ヒューマンマシンインターフェースに関連する考慮事項
7. ソフトウェア要求事項	9. ソフトウェア：ソフトウェアの要件
8. ソフトウェア設計	9. ソフトウェア：ソフトウェアの設計
9. ソフトウェア実施	9. ソフトウェア：ソフトウェアの実施
10. 検証と解析	9. ソフトウェア：ソフトウェアの検証及び分析
11. コンピュータシステム	2. I&C 設計のためのシステム。

[46] IAEA 安全基準シリーズ No. NS-G-1.1「原子力発電所における安全上重要なコンピュータに基づいた系統のためのソフトウェア」

[47] IAEA 安全基準シリーズ No. NS-G-1.3「原子力発電所における安全上重要な計測制御系」

の統合	
12. コンピュータシステムの妥当性確認	2. I&C 設計のためのシステム。
13. 設置及び試運転	2. I&C 設計のためのシステム。
14. 運転	2. I&C 設計のためのシステム。
15. 引渡し後の改造	2. I&C 設計のためのシステム。
添付資料：既存のソフトウェアの使用と妥当性確認	2. I&C 設計のためのシステム。 9. ソフトウェア：事前開発ソフトウェア

表Ⅱ-2. IAEA 安全基準シリーズ No. NS-G-1.3 と本安全指針の関連

IAEA 安全基準シリーズ No. NS-G-1.3	本安全指針
1. はじめに	1. はじめに
2. 安全上重要な I&C 系	参考文献 [II-1] を参照
— I&C 系の特定	3. I&C 系の設計基準
— I&C 系の分類	5. I&C の機能、系統及び設備の安全分類
3. 設計基準	3. I&C 系の設計基準
4. 全般的設計手引き	
— 性能要件	2. I&C 設計のためのマネジメントシステム：ライフサイクル活動：要件の仕様
— 信頼性設計	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：信頼性設計
— 独立性	4. I&C 構造；独立性 6. 安全上重要な全ての I&C 系に関する全般的推奨事項：信頼性設計-：独立性
— 故障モード	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：信頼性設計：故障モード
— 設備への立入り管理	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：安全上重要な系統への立入りの管理 7. 個別の I&C 系及び設備の設計に対する手引き：デジタルシステム：コンピュータ・セキュリティ
— 設定値	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：設定値

— ヒューマンマシンインターフェース	8. ヒューマンマシンインターフェースに関連する考慮事項-
— 設備の性能保証	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：設備の適格性性能保証
— 品質	2. I&C 設計のためのマネジメントシステム。
— 電磁気的適合性に関する設計	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：設備の性能保証：内部及び外的ハザード：電磁気性能保証
— 試験と試験可能性	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：運転時の試験と試験可能性
— 保守の可能性	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：保守性
— 文書	2. I&C 設計のためのマネジメントシステム：全てのライフサイクル時期に共通の活動：文書
— 安全上重要な機器等の特定	6. 安全上重要な全ての I&C 系に関する全般的推奨事項：安全上重要な機器等の標識と識別確認
5. 系統特融の設計手引き	
— 安全系 — 保護系	7. 個別の I&C 系及び設備の設計に対する手引き：保護系
— 電力	7. 個別の I&C 系及び設備の設計に対する手引き：電力の供給
— デジタルコンピュータシステム	7. 個別の I&C 系及び設備の設計に対する手引き：デジタルシステム
6. ヒューマンマシンインターフェース	8. ヒューマンマシンインターフェースに関連する考慮事項
7. 安全上重要な I&C 系の設計プロセス。	2. I&C 系設計のマネジメントシステム：ライフサイクル活動：改造

資料 II の参考文献

[Ⅱ-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011)

添付資料 III

加盟国の慣行が異なる分野

はじめに

III-1. 計測制御（I&C）の安全に関する設計判断基準を裏付ける学術的な根拠又は工学的慣行が、全ての加盟国によって広範に受け入れられていない多くの分野がある。本添付資料では、本安全指針の策定期間中にこのような差異が特定された分野を論じている。加盟国の慣行が時間と共に進展することが期待される場合がある。

デジタルシステムに関する信頼性の判断

III-2. 複数の多重部分において同一のソフトウェアが使用されている場合、ソフトウェアのエラーは、多重性を有するデジタルシステムにおいて共通原因故障につながる場合がある。したがって、デジタルシステムの信頼性を推定するためには、ハードウェアの故障及び一部の加盟国ではソフトウェアのエラーによるシステム故障の確率を推定することが必要である。その他の加盟国に関しては、（ソフトウェアのエラーを含む）設計の誤り及びこれらの影響は、構造及び設計の定性的分析によってのみ適切に処理される。

III-3. 一部の加盟国では、I&C設計基準を策定するとき、安全上重要な各々のI&C系に対する明確な信頼性数値目標を維持することによって、I&C系の信頼性要件と確率論的安全解析との間の整合性を確保している。したがって、これらの加盟国は、デジタルシステムの信頼性の数値上の推定値を、信頼性実証のために必要な要素であると見做している。

III-4. ソフトウェアに対して数値による信頼性を適用している加盟国に関しては、ソフトウェアの高い信頼性の要求は、現時点では、実証可能でない。したがって、単一のコンピュータに基づくシステムが、ソフトウェアに関して 10^{-4} よりも低い、作動要求当たりの故障確率（pfd）を達成することを要求する設計は、注意して扱われる必要がある。

III-5. デジタルシステムに関して数値による信頼性推定値を利用している一部の規制機関は、彼らが I&C 系に関して正当化ができると見なしている信頼性レベルの限度を確立している。例えば、共通のプラットフォームに基づくあらゆる I&C 系に対する信頼性の要求は、使用される技術に関係なく、10^{-5} pfd に制限されており、また、共通のコンピュータベースのプラットフォームに基づくあらゆる個々の I&C 系に対する信頼性の要求は、本安全指針に記述された方針（例えば、多重性）が採用される範囲に関係なく、10^{-4} pfd に制限されている。

III-6. 一部の加盟国では、ソフトウェアの信頼性を判断することに対して定性的な手法を使用している。このような定性的手法は、全面的な検証及び妥当性確認を可能にするために、一般的に、ソフトウェアの確定的挙動に関する堅固な要件に基づいている。全面的な検証及び妥当性確認を可能にする堅固な設計要件の組合せが、ソフトウェアの信頼性面で高い確信度を与えている。

安全系統における共通原因の脆弱性の評価

III-7. 本安全指針の 4.32 項は、以下を推奨している。

> 「各想定起因事象の影響についての解析は、保護系がその必要な安全機能を実施することを妨げるおそれのある共通原因故障と組み合わせて、安全解析の範囲内で行われるべきである。」

この点については、一般的な合意があるが、解析の範囲、安全系統内の共通原因故障と共に想定起因事象が発生した場合に容認される放射線の影響、又は放射線の影響を確定するときに使用される解析方法の種類に関する一般的な合意はない。

解析の範囲

III-8. 規制機関が 4.32 項に記述されている解析に対して期待する範囲には、以下の事例を含む。

- 予期される運転時の事象及び設計基準事故状態であると見做される想定起因事象と併せての安全系統における共通原因故障の解析
- 1 年当たり 10^{-3} より大きい発生頻度を持つ想定起因事象と併せて、安全系統の共通原因故障の解析

容認可能な影響

III-9. 想定起因事象が安全系統における共通原因故障と併せて発生したときに、規制機関が容認できる影響の事例には以下のものを含む。

- 原子炉保護系における共通原因故障と併せて起きる予期される運転時の事象の影響であって、以下をもたらさないもの。
  - 核分裂生成物の放出開始後に 2 時間にわたって非居住区域の境界上のあらゆる地点にいるあらゆる個人、又は核分裂生成物放出の全継続期間にわたって低人口区域の境界にいるあらゆる個人であって、25 mSv を越える全身線量又はヨウ素により甲状腺に 300 mSv を越える線量を受ける個人。又は
  - 一次冷却材系統の設計限界を越えること。
- 原子炉保護系における共通原因故障と併せて起きる設計基準事故の影響であって、以下をもたらさないもの。
  - 核分裂生成物の放出開始後に 2 時間にわたって非居住区域の境界のあらゆる地点にいる個人、又は核分裂生成物放出の全継続期間にわたって低人口区域の境界にいる個人であって、0.25 Sv を越える全身線量又はヨウ素により甲状腺に 3 Sv を越える線量を受ける個人。又は
  - 一次冷却材系統又は格納容器の設計限界を越えること。
- 原子炉保護系における共通原因故障と併せて起きる設計基準事故後において、残り

の安全系統は、以下のことが可能であること。

- 規制機関と許認可取得者との間で同意された線量限度が満たされていることを保証すること。
- 超過圧力による一次熱輸送系の故障を防止すること
- 燃料の過大な温度を防止すること
- 燃料破損を防止すること
- エネルギーの発生率及び全エネルギーの発生を格納容器の健全性が損なわれない範囲内に制限すること
- 原子炉の未臨界を確保するための代替手段を提供するために十分長い期間にわたって未臨界を維持すること

－ 共通原因故障の影響を防止又は緩和するために備えられた多様性及びその他の手段が、十分に高い系統機能信頼性を確保している。

― 安全系統が故障した場合、設計基準事故の影響が、容認可能な線量限度を越えない。

解析手法

III-10. 4.32 項に記述された解析の一部として影響について判断をする際に、一部の規制機関は、保守的な方法の使用を期待しており、他の機関は、最良推定方法の使用を認めている。IAEA 安全基準シリーズ No. SSG-2「原子力発電所に対する決定論的安全解析」[III-1] では、保守的手法及び最最適評価手法を論じている。

多様な作動システム

III-11. 保護系機能を実装するためにデジタルシステムが使用されるとき、デジタル保護系内の共通原因故障が共通原因故障と想定起因事象との一定の組合せに対して容認できない影響をもたらすことがあるということを分かるということは、4.32 項に記述されている解析では珍しいことではない。この状況に遭遇した場合、多くの場合、多様な作動システムが保護系をバックアップするために備えられる。

III-12. 多様な作動システムが保護系の想定される共通原因故障と併せての特定の想定起因事象の影響を効果的に緩和する場合があるとの一般的合意がある。しかし、安全分類、デジタル保護系をバックアップするための多様的デジタル作動システムの使用及び保護系の共通原因故障の影響を緩和するための手動起動操作の使用に関しては、様々な方式がある。

安全分類

III-13. 一部の規制機関は、多様性を有する作動システムは安全系統として分類されることを期待している。一部の規制機関は、これらをより低い安全クラスの系統であることを認めている。一部の規制機関は、多様性を有する作動システムに対してなされる信頼度要求を期待される安全クラスの基礎としている。

多様な作動システムの技術

III-14.　一部の規制機関は、多様な作動システムが配線接続の系統になることを期待している。一部の規制機関は、デジタルシステムの使用を抑制するが、しかし禁止していない。一部の規制機関は、十分な多様性が実証される場合には、デジタルシステムの使用を認めている。

多様な作動に関する手動操作の使用

III-15.　一般に、手動起動は、保護系のための多様なバックアップとして受け入れられる場合があるが、手動起動が機能保証される条件は色々である。容認された実施例の範囲には以下を含む。

— 手動操作が 30 分以内には必要でなく、また、人間工学分析が、その時間以内に適切な決定が行われかつ実装できることを確認した場合に、手動操作は機能保証できる。
— 手動操作が 20 分以内には必要でない場合には、その手動操作は機能保証できる。
— 手動操作は、工学的安全設備の起動に関して機能保証できるが、原子炉トリップに関しては機能保証されない。
— 手動操作は、制約なしに機能保証できる。

III-16.　上記のものは、諸規制機関における実施例の範囲を例示したものであるが、規制機関は、提案された特定の状況に基づいて様々な手法をとる場合がある。

添付資料 III の参考文献

[Ⅲ-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

定 義

以下の定義は、本刊行物に固有のものであり、IAEA 安全用語集：原子力安全及び放射線防護において使用される専門用語（2007 年版）IAEA、Vienna (2007 年)に提示されていないか又はそれとは異なるものである。

http://www-pub.iaea.org/books/IAEABooks/7648/IAEA-Safety-Glossary

記号””は、IAEA 安全用語集で提示されているものとは異なる定義を示す。*

構造　安全上重要である発電所の計測制御系の体系的構成

利用可能性（稼働性）*　必要な外部資源が提供されているという前提の下に、所定の瞬間又は所定の時間間隔において、所定の条件の下で要求される機能を実施する状態にある機器の能力。

較正*　測定計器若しくは測定系統によって表示される諸量の値又は物質の測定若しくは参照物質によって表される値と、標準によって実現される対応する値との関係を、指定された条件の下で確定する一連の操作。

構成要素（又は機器）*　系統を構成する部品の 1 つ。構成要素（機器）は、ハードウェア又はソフトウェアであり、また、他の構成要素（機器）に細分される場合がある。

注記:　用語「設備」、「構成要素（機器）」 及び「モジュール」は、多くの場合、互換可能に使われる。これらの用語の関係はまだ標準化されていない。

構成のベースライン　機器のライフサイクル中の特定の時点で、公式に指定かつ固定された一連の構成機器等。

確定的な挙動　系統又は機器の特性であって、機器の仕様書の範囲内にある所定のあらゆる入力シーケンスが、常に同じ出力を生成するようなもの。

確定的な時間設定　系統又は機器の特性であって、誘起要因と応答との間の時間的遅れが、保証された最大値と最小値を持っているようなもの。

多様性*　特定された機能を実施する 2 つ以上の多重の系統又は機器の存在であって、そこでは、共通モード故障を含む共通原因故障の可能性を低減するように、異なる系統又は機器が異なる属性を持っている。

注記 1：　用語「多様性」が追加的属性を伴って使用されるとき、多様性という用語は、一般的な意味の「指定された目的を達成する 2 つ以上の異なる方法又は手段の存在」を示す一方で、その属性は、例えば、機能的多様性、設備の多様性、信号の多様性のような、適

用される異なる方法の特性を示す。

注記 2： IAEA の安全用語集の「機能的多様性」の見出し語も参照のこと。

区分　相互接続を含む機器等の集積であって、多重の系統又は安全グループの 1 つの多重性を形成するものである。区分には、多重チャンネルを含む場合がある。

フィールドプログラマブルゲートアレイ　計測制御製造業者によって現場でプログラムをすることができる集積回路。これには、プログラムが可能な論理ブロック（組み合わせ型及び連続型）、プログラムが可能なこれらの間の相互接続並びに入力及び／又は出力用のプログラム可能なブロックを含む。この結果、機能は、回路製造業者によってではなく、計測制御設計者によって定義される。

ファームウェア　ソフトウェアが組み込まれているハードウェア特性と緊密に組み合わされるソフトウェア。

機能要件　個別機器の要求される機能又は挙動を規定する要件。

ハードウェア記述言語　文書化、シミュレーション又は合成のための、電子機器の機能及び／又は構成を公式に記述することを可能にする言語。

プログラムされたハードウェア装置　これは、ハードウェア記述言語及び関連ソフトウェアツールを用いて構成された（原子力発電所の計測制御系用の）集積回路である。

ハザード（ハザード）　危害の潜在性

外因性ハザード　危害の潜在性に寄与する因子。

ハザード分析　固有のハザード及び外因性ハザードを特定し、また、これらを除去し、防止し又は制御するための要件及び制約事項を特定するために、系統をそのライフサイクル全体を通じて詳細調査するプロセス。

注記：　ハザード分析の範囲は、異常事象を含めること及び劣化した設備と発電所系統での発電所運転を含めることにより、発電所の設計基準事故を越えて拡大する。

ヒューマンマシンインターフェース　運転職員と、計測制御系及び発電所に連結されたコンピュータシステムとの間の取り合い。このインターフェースには、表示装置、制御装置及び運転員支援系との取り合いを含む。

非機能的要件（品質要件としても知られている）　要求される機能及び挙動以外の機器の固有の性質又は特性を規定する要件。事例としての特性には、解析可能性、保証可能性、

監査可能性、利用可能性、互換性、文書化、健全性、保守性、信頼性、安全、セキュリティ、使用可能性及び検証可能性を含む。

事前開発ブロック　　ハードウェア記述言語において使用可能な事前に開発された機能的の塊。事前開発ブロックには、例えば、ライブラリ、複数処理体又は知的所有物核心部を含む。事前開発ブロックは、プログラムされたハードウェア装置に組み込まれる前に、かなりの作業を必要とする場合がある。

事前開発機器　　すでに存在している品目は、商業用製品又は企業所有製品として利用可能であり、計測制御系での使用について検討されている。事前開発機器には、ハードウェア装置、事前に開発されたソフトウェア、市販の商用装置、ハードウェアとソフトウェアの両方で構成されるデジタル装置又はハードウェア定義言語若しくは事前開発ブロックで構成されたハードウェア装置を含む。

要求工学　　一連の要件を策定し、文書化し、また、維持することに関連する活動を含む工学的プロセス。

静的分析　　系統又は機器の形状、構成、内容若しくは文書に基づく系統又は機器の分析。

型式試験　　製品の代表的な 1 つ以上の機器等に対して行なわれる適合性試験。

妥当性確認*　　系統が意図された要件仕様を全体として果たしていることの、詳細試験による及びその他の証拠の提供による確認。

検証*　　活動の結果が、その活動に関して規定された目的及び要件を満たしているとの、詳細試験による及び客観的証拠の提供による確認。

基準案の作成と査読の協力者

Alpeev, A.	Scientific and Engineering Centre of Rostechnadzor, Russian Federation
Alvarado, R.	Nuclear Regulatory Commission, United States of America
Asikainen, S.	Teollisuuden Voima Oyj, Finland
Babcock, B.	Ontario Power Generation, Canada
Benitez-Read, J.	National Institute for Nuclear Research, Mexico
Bicer, C.	Turkish Atomic Energy Authority, Turkey
Boeva, T.	Kozloduy Nuclear Power Plant, Bulgaria
Bouard, J. P.	Electricité de France, France
Bowell, M.	Office for Nuclear Regulation, United Kingdom
Curtis, D.	Consultant
Debor, J.	Consultant
Duchac, A.	. International Atomic Energy Agency
Edvinsson, H.	Vattenfall, Sweden
Eriksson, K. E.	Oskarshamn Nuclear Power Plant, Sweden
Faya, A.	Federal Authority for Nuclear Regulation, United Arab Emirates
Fichman, R.	Ontario Power Generation, Canada
Furieri, E. B.	National Nuclear Energy Commission, Brazil
Gassino, J.	Institute for Radiological Protection and Nuclear Safety, France
Gonchukov, V.	Rostechnadzor, Russian Federation
Göring, M.	Vattenfall, Germany
Harber, J.	Atomic Energy of Canada Limited, Canada
Hohendorf, R.	Ontario Power Generation, Canada
Johnson, G.	International Atomic Energy Agency
Karasek, A.	CEZ, Czech Republic
Kawaguchi, K.	Nuclear Regulation Authority, Japan
Kim, B. Y.	Korea Institute of Nuclear Safety, Republic of Korea
Klopkov, V.	Rostechnadzor, Russian Federation
Lee, J.	Korea Atomic Energy Research Institute, Republic of Korea
Li, H. S.	Nuclear Regulatory Commission, United States of America
Lindskog, U.	Oskarshamn Nuclear Power Plant, Sweden
Mangi, A.	Pakistan Nuclear Regulatory Authority, Pakistan
Ngo, C.	Candesco, Canada
Odess-Gillett, W.	Westinghouse, United States of America
Park, H. S.	Korea Institute of Nuclear Safety, Republic of Korea
Parsons, A.	AMEC, United Kingdom
Piljugin, E.	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH, Germany
Poulat, B.	International Atomic Energy Agency
Régnier, P.	Institute for Radiological Protection and Nuclear Safety, France
Santos, D.	Nuclear Regulatory Commission, United States of America

Seidel, F.	Federal Office for Radiation Protection, Germany
Shumov, S.	Specialized Scientific Research Institute for Instrumentation Engineering, Russian Federation
Sjövall, H.	Teollisuuden Voima Oyj, Finland
Stattel, R.	Nuclear Regulatory Commission, United States of America
Svensson, C.	Oskarshamn Nuclear Power Plant, Sweden
Takala, H.	Radiation and Nuclear Safety Authority, Finland
Takita, M.	Nuclear Regulation Authority, Japan
Tate, R.	Office for Nuclear Regulation, United Kingdom
Thuy, N.	Electricité de France, France
Welbourne, D.	Consultant
Yastrebenetsky, M.	State Scientific and Technical Centre for Nuclear and Radiation Safety, Ukraine
Yates, R.	Office for Nuclear Regulation, United Kingdom
Zeng, Z. C.	Canadian Nuclear Safety Commission, Canada

※この協力者一覧は、正本に記載のあるものを転記したものであり、これらの協力者は日本語翻訳版の作成には一切関係はありません。