制作：PA・FA 計測制御委員会 機能安全調査研究 WG
初版：2013 年 11 月

制作：PA・FA 計測制御委員会 機能安全調査研究 WG
初版：2013 年 11 月

1. はしがき

1.1 機能安全とは

従来我が国では、「安全とは事故がないこと」であるとの考え方が根強く、事故は人為的ミスや欠陥によって起こるとされ、いったん事故が発生すれば、原因追及よりもむしろ過失責任の追及に重点をおいた調査がされる傾向が強い。事故を起こさないためには、品質を含めた信頼性をひたすら高めることによって、異常事態が発生する可能性をゼロに近づけることが必要だとされ、構成要素に故障やバグがあることは前提としていない。日本の企業はこれまで、この考え方によって実績を積み上げてきた。「日本製品は壊れにくい」という評価は、正にこの結果といえる。信頼性は定量的で純技術的な概念であり、技術者にとって扱いやすい指標だったこともこの傾向が強くなった要因といえる。

しかし近年生産設備は大型化かつ複雑化し、またプラントの制御・安全に PLC（プログラマブル・ロジック・コントローラ）等のマイクロプロセッサをベースとした電子システムを使用することも多くなり、複雑な要因が絡み合って、予期しない事故や故障が発生する可能性も高まってきている。従来のような個別機器の安全性や、法律に基づく安全基準を満足するだけでなく、ソフトウェアを包含した、システム全体の安全性確保が必要となってきた。

我が国では 100%の安全が常に要求されてきたが､欧米では安全とは｢リスクが最小の状態であること」という安全工学に基づく、新しい枠組みによる安全性の評価がすでに一般的となっている。プラントの複雑度が増すにつれ、その安全性の重要度は増してくるが、リスクゼロの絶対的な安全はなく、多少のリスクは残存すると考えなくてはならない。このリスクは多重防護策を講じることにより、それを許容可能なレベルにまで低減させることができると考える。

従来、過去の経験による装置の改善・改良と、設備の信頼性を向上させることにより故障低減を進めてきた。しかしこの方法ではソフトとハードが複雑に絡み合って発生する未知の故障や突発的な事態に対処できないことが考えられる。そこで、このような異常事態は不可避であるという前提に立ち、そのような事態でも確率・統計学をベースとした、危険事象の発生するリスクが、許容可能なまで低減させるシステムを構築する必要があり、IEC 61508 のような安全規格が制定されてきた。

国際電気標準会議（IEC）が発行する国際安全規格 IEC 61508 によって定められている機能安全とは「EUC（被制御機器）および EUC 制御系の全体に関する安全のうち、電気・電子・プログラマブル電子（E/E/PE : Electrical/Electronic/Programmable Electronic）安全関連系、他技術安全関連系および他リスク軽減措置の正常な機能に依存する部分」と定義されている。言い換えると各種安全関連のシステムを正しく機能させることにより、リスクを軽減し許容できるレベルの安全を維持することである。

従来機械製品に対する安全規格はあったが、機械の構造規格が主になっていた。しかしマイクロプロセッサをベースとする電子システムに対し、構造規格を規定することは意味がない。したがって構造のいかんにかかわらず安全機能を高める性能規格の概念が必要となった。安全機能とは技術やコストなど

の理由で危険事象が起こる原因を完全に取り除けないような場合、危険事象が起きるリスクを極力減らし安全性を増す機能である。国際安全規格はこの安全機能の概念を導入し、安全システムを製造するメーカーだけでなく、そのシステムを利用する事業者およびユーザの管理にも及ぶものである。

プロセス産業分野においては、プラントやシステムのリスクを下げ、機能安全を実現するシステムとして安全計装システム（safety instrumented system、SIS）が生れた。日本国外では標準的に安全計装システムが導入されてきているが、単に機能安全 PLC を導入すれば良いということではなく、プラントに対する規制・規格に基づいてリスクアセスメントを行い、必要な部分には安全計装システムを導入し、安全ライフサイクルを実行し、各々の項目が正しく機能していることを監査し、維持することが求められている。

1.2 規格の歴史

1970 年代、世界的にプラントの重大事故により多くの人命と財産が失われた。1976 年セベソ（イタリア）で発生した事故[注 1)]をきっかけとして、当時の欧州委員会（EC：European Commission、現欧州連合 EU：European Union）では「特定産業活動の大事故災害に対する欧州閣僚理事会指令」としていわゆるセベソ指令（EC 指令）が 1982 年に発令された。これは加盟各国に対して危険物質を扱う産業活動に対してリスク解析を求めるものであった。更に欧州経済統合が進捗するにつれて、域内における製品の流通を円滑にするため、各国毎に制定されていた安全規格を統一する必要が生じた。

その後 1996 年にセベソ指令Ⅱとして改定され、加盟各国は大事故災害のコントロールを各国法規として強制し、その実現手段を準備することを求められた。2 年の準備期間を経て 1999 年に域内での強制となった。このセベソ指令Ⅱでは、安全管理システム（Safety Management System）と事故時の緊急計画を策定することが求められた。その結果イギリス、ドイツ、米国の各国でそれぞれ安全関連の法規制が制定され、機能安全規格 IEC 61508 に代表される国際規格につながった。

IEC 61508 の翻訳規格である JIS C 0508 は 2000 年に発行された。 現在、IEC 61508 の第 1 部～第 7 部は第 2 版（2010 年改正版）である。第 1 部、第 4 部はすでに日本語に翻訳され第 2 版と同一内容の JIS C 0508：2012－1、4 として発行されおり、引き続き第 2 部、第 3 部の発行準備を JEMIMA が（一財）日本規格協会と共同して行っている（2013 年 10 月現在)。また、IEC 61511 は 2003 年に発行され、その翻訳規格である JIS C 0511 は 2008 年に発行された。

我が国においても化学工場の爆発事故や放射能漏れ事故など、従来は考えられなかった事故も目立ち始め、自主保安を前提とした従来型の規制の強化のみでは事故を防止出来なくなりつつある。特にプラントは大型化、複雑化の度合いが高まっているほか、高度成長期に導入された設備の老朽化、さらには熟練技術者の不足に伴い、従来の人に依存した安全管理から、プラントのシステム全体の評価や安全計装機器導入によるリスクマネジメントへの転換が求められている。

注 1）セベソ事故

セベソ事故（Seveso disaster）とは、1976 年 7 月 10 日にイタリアのロンバルディア州、ミラノの 25km 付近に位置するセベソの農薬工場で発生した爆発事故である。代表的なダイオキシンである 2、3、7、8-テトラクロロジベンゾ-1、4-ジオキシンの 30kg～130kg が住宅地区を含む 1800 ヘクタール（新宿区に相当する）に飛散し、ダイオキシン類の暴露事故としては史上最大規模なものとなった。高汚染地区は居住禁止・強制疎開などの措置が取られた。周辺地域では鶏、兎、猫等の家畜が大量に死亡し、奇形出生率が高くなったことが報告されている。この事故を教訓として、EC は化学工場の安全規制を定めたセベソ指令を定めている。

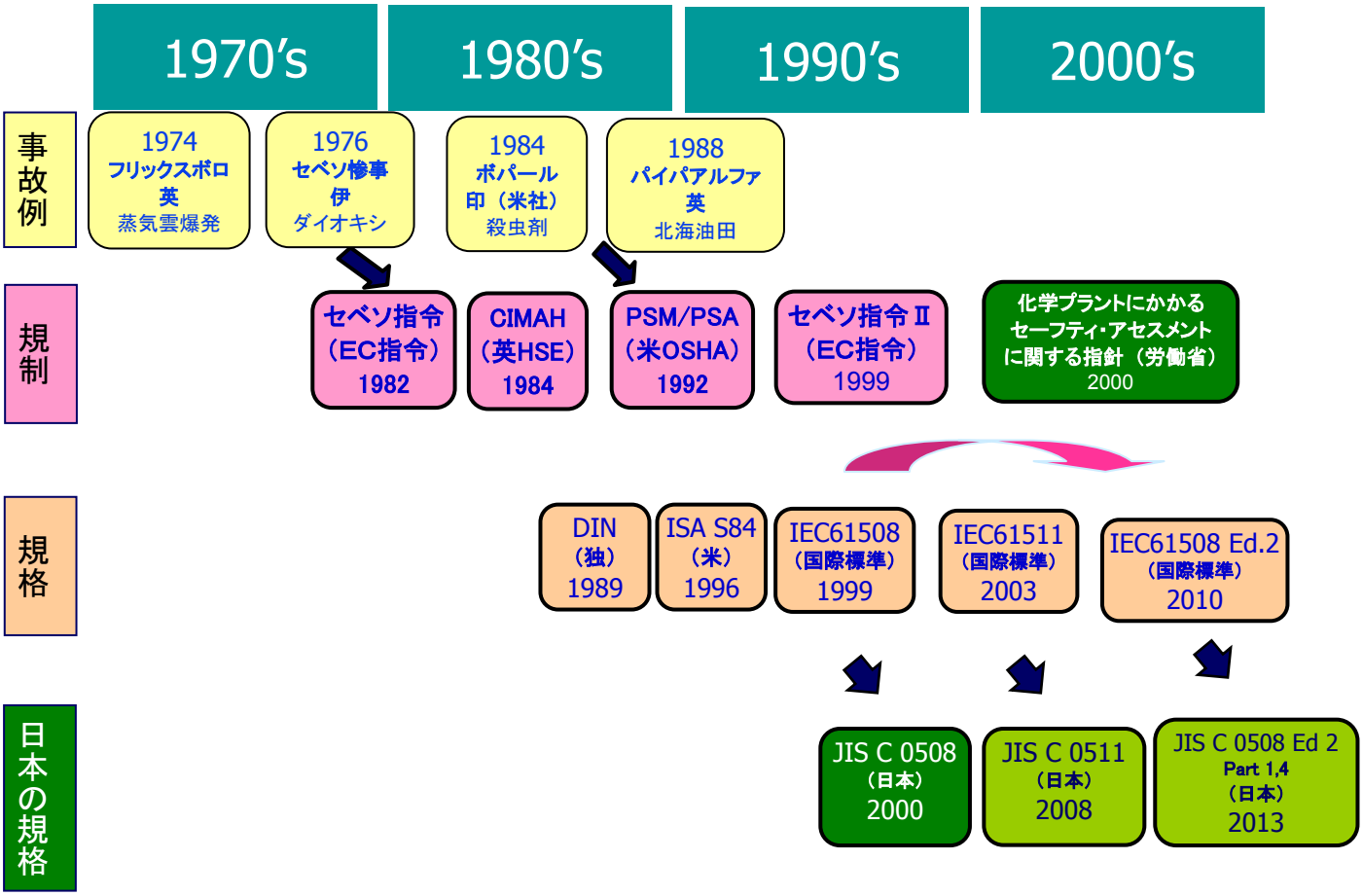


図 1.1　事故発生、規制、規格制定の歴史

2. 機能安全規格の適用範囲

機能安全の国際規格である IEC 61508 は
①全産業を対象としており、
②人命、環境、財産を保護するための安全関連系（安全関連システム）、および安全関連系において安全機能を実行するために使われる電気・電子・プログラマブル電子系（電気回路や電子回路やプログラム可能な電子回路を使ったシステム）に対する基本要求事項を定めており、
③安全関連系で使用する部品や機器の供給者、安全関連系のシステムインテグレータおよびエンジニアリング会社はもちろんのこと、安全関連系を利用するエンドユーザもこの規格の対象となる。

安全関連系の分かりやすい例としては、IEC 61511（JIS C 0511）が対象としているプロセス産業分野の安全計装システムがある。IEC 61508 が適用される安全計装システムと適用されない基本プロセス制御システムとの違いを図 2.1 に示す。

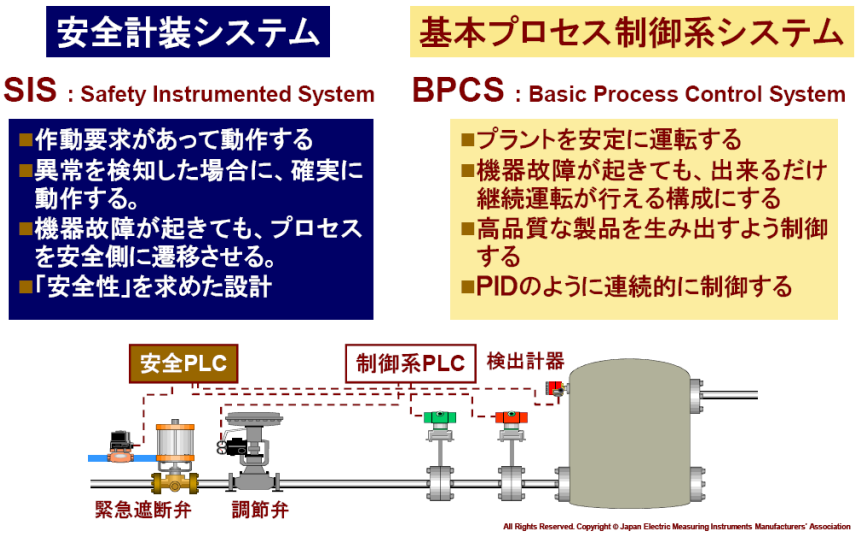


図 2.1　安全関連系と非安全関連系の例

IEC 61508 は、IEC ガイド 104 にしたがって制定された、IEC の規格体系で機能安全に関して最上位に位置する基本安全規格（Basic safety publication）であり、その主たる目的は、この規格にしたがって IEC の専門委員会（TC）にて、製品やアプリケーションの分野（Sector）毎に異なる機能安全要求事項を具体的に定める個別の国際規格を制定することである。IEC 61508 にしたがって具体的製品に対して制定された規格を（機能安全の）製品規格といい、具体的なアプリケーションの分野に対して制定された規格を（機能安全の）分野規格という。上述の IEC 61511 はプロセス産業における（機能安全の）分野規格である。

すなわち、IEC 61508 はすべての製品、アプリケーションの分野に適用できるように、膨大な一般要求事項を網羅しているので、どの要求事項を具体的な製品やシステムにどのように適用すれば良いかが、専門家でないと分かりづらいという面がある。したがって、現場で使いやすい製品規格や分野規格が必要になってくるということを前提として作られているともいえる。

とはいえ、機能安全の製品規格や分野規格がまだ制定されていない、あるいは、制定することが難しい製品カテゴリやアプリケーション分野に対しては、IEC 61508 をそのまま適用することになるし、それは認められている。また、ISO 規格など IEC 以外の規格に適用しても良い。

例えば、前述のプロセス産業において使われる温度伝送器には（機能安全の）製品規格はないので、安全計装システムで使われる温度伝送器の設計・製造は IEC 61508 にしたがって行うことになる。機能安全以外は他の規格を適用する。プロセス産業分野における IEC 61508 と IEC 61511 との関係を示したものが図 2.2 である。

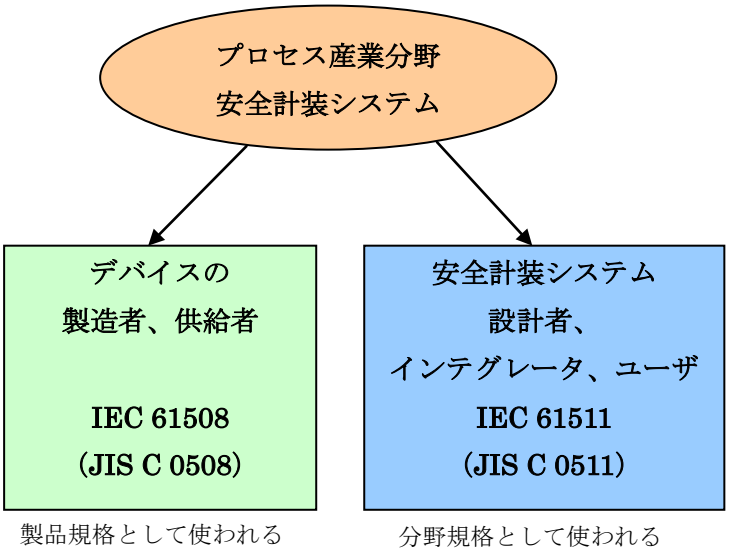


図 2.2　プロセス産業分野での規格の役割

現在、図 2.3 に示すように、機械、自動車、鉄道、原子力、その他の分野の規格への適用（製品規格、分野規格を含む）が広がっている。国際安全規格の体系における機能安全関連規格の関係を示したものが図 2.4 である。

なお、医療機器の規格である IEC 60601 シリーズに適合するものには、IEC 61508 を基本安全規格としては用いないことになっている。

図 2.3　IEC 61508 が適用されている規格の例

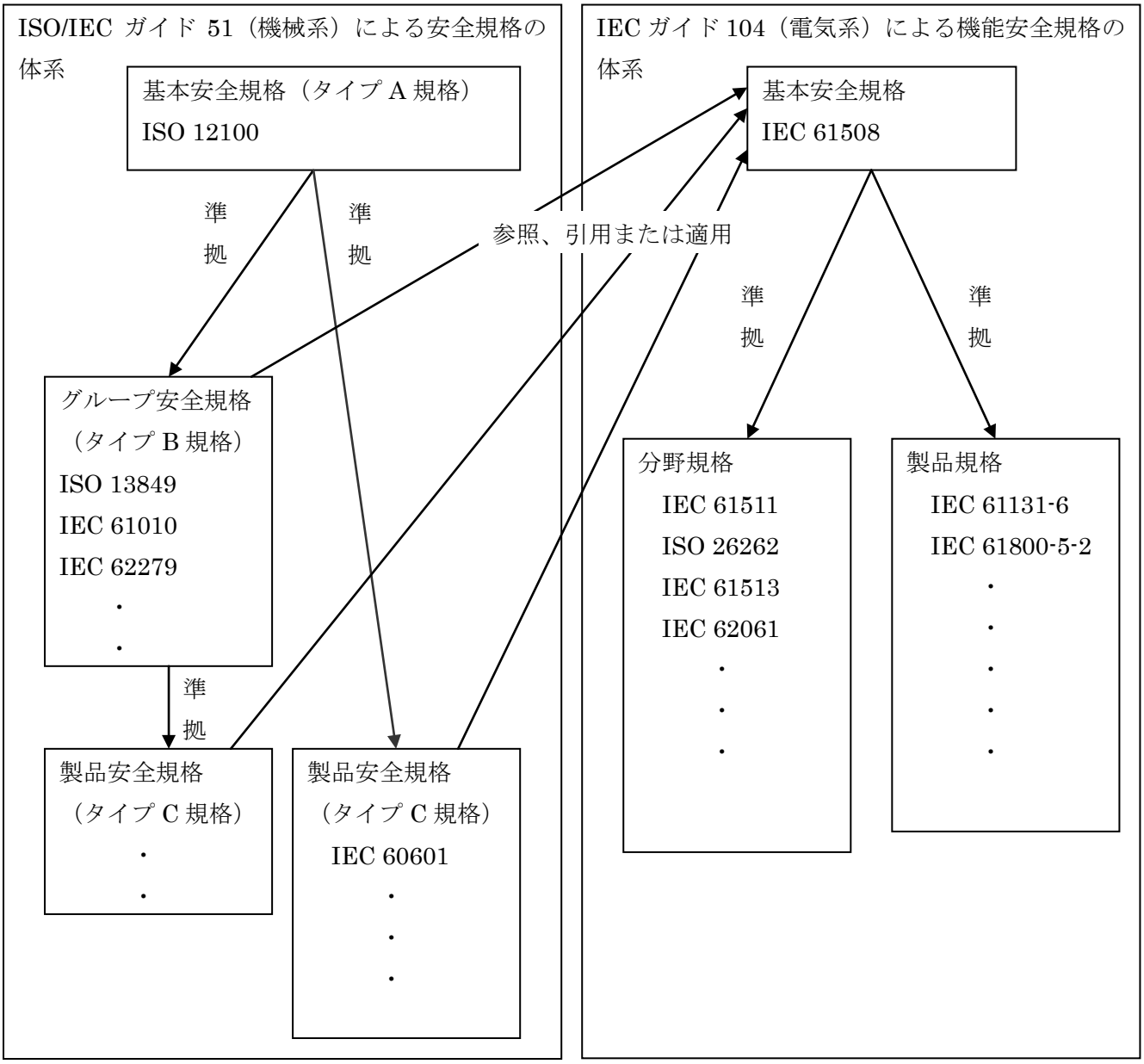


図 2.4　国際安全規格の体系における機能安全関連規格の関係

IEC 61508 には第 1 部から第 7 部までがあり、第 1 部から第 4 部までで製品規格や分野規格を制定するための要件として、それぞれ「一般要求事項」、「ハードウェア要求事項」、「ソフトウェア要求事項」、「用語の定義」を定めており、第 5 部から第 7 部は第 1 部から第 4 部の要件を満足するために用いることが可能なさまざまな設計手法、分析手法を網羅したガイドラインとなっている。

なお、第 1 部から第 4 部はそれぞれ独立した規格として、製品規格や分野規格以外の規格で個別に引用規格としても良い。

3. 用語の解説

3.1 本章で解説する用語について

本章では、IEC 61508 で使用される用語のうち、重要なものについて解説する。本章に記載する内容は、用語は JIS C 0508 に記載されているものであるが、その用語の解説であり JIS C 0508 に記載される定義ではない。

3.2 安全に関する用語

3.2.1 安全（Safety）

許容できないリスクが存在しないこと。

3.2.2 危害（harm）

人が被る身体の損傷や健康被害のこと。人に対する事象だけでなく、財産の毀損や環境の破壊も指す。

3.2.3 危害事象（harmful event）

危険状態または危険事象が発生した結果として、危害に至る事象のこと。

3.2.4 潜在危険（hazard）

潜在的に危害を引き起こす可能性がある物事。火災や爆発のような短時間に人に危害を与えるものの他に、毒性物質の放出といった長期にわたり健康へ影響を与えるものも含む。

3.2.5 危険事象（hazardous event）

結果として危害の生じるおそれがある事象。危険事象の結果として危害が生じるかどうかは、人、財産または環境が危害の生じるおそれがある危険事象に結果としてさらされているかどうかに左右される。人に対する危害の場合は、事象発生後に、危険事象にさらされた人が事象から逃れられるかどうかにも左右される。

3.2.6 危険状態（hazardous situation）

人、財産または環境が、一つまたは複数の潜在危険にさらされている状況。

3.2.7 リスク（Risk）

危害がもたらす好ましくない状況を表す指標であり、危害の発生確率とその危害の程度の組合せによって表現する。

3.2.8 許容リスク（tolerable risk）

現在の社会通念上、想定される状況下で許容されるリスク。

3.2.9 残存リスク（residual risk）

リスクを低減するための安全措置を取った後に、なお残っているリスク。

3.2.10ALARP（As Low As Reasonably Practicable、合理的に可能な限り低い）

ALARP は、許容リスクの達成を判定するための考え方の一つであり、リスクが現実的に実施できる最低限の水準になっていれば許容リスクを達成できたとする考え方である。現実的に実施できるとは、ある水準からさらにリスクを軽減する際に、現時点での技術や知見に基づいて、現実的な費用で実施できることを意味している。リスクが大きくて許容できない水準と、リスクが小さく問題とならない水準という 2 つの水準の間の水準を指す場合もある。

3.3 故障に関する用語

3.3.1 フォールト（fault）、故障（failure）、エラー（error）

一般的には、フォールト（fault）、機能喪失、機能失敗、故障（failure）、エラー（error）は、異常、故障などの意味で同じように使用することがあるが、機能安全では、それらの意味を個々に定義している。

3.3.2 フォールト（fault）

ある要求された機能を実行するための機能ユニットの能力が、部分的に機能しなくなる、あるいは全く機能しなくなるといった状況を引き起こす原因となりうる、異常な状態を指す。フォールトは、機能喪失や機能失敗（failure）に至る要因であり、機能喪失や機能失敗（failure）そのものではない。フォールト時に作動要求が発生すると機能喪失・機能失敗が起きる。作動要求時にフォールトが生じても、機能喪失・機能失敗が起きる。
本内容は JIS X 0014 と同様であるが、JIS Z 8115 に記載されている一般的な定義とは異なる。

3.3.3 機能喪失、機能失敗、故障（failure）

ある機能ユニットが持つ要求された機能を提供する能力の停止、あるいは要求された以外の方法での機能ユニットの稼働を指す。Failure（機能喪失、機能失敗、故障）は、ランダムハードウェア故障（random hardware failure）、または決定論的原因故障（systematic failure）のいずれかである。

3.3.4 エラー（error）

計算、監視、あるいは測定された値（または状態）と、真の、規定された、あるいは理論的に正しい値（または状態）との不一致を指す。エラーが、フォールトを引き起こす場合がある。

3.3.5 ランダムハードウェア故障（random hardware failure）

ハードウェアで時間に無秩序に起こりうる劣化メカニズムにより発生するハードウェア故障を指す。多くの構成要素から構成される装置では、個々の構成要素の故障率を元に装置の故障率を予測することは可能である。しかし、構成要素毎に劣化メカニズムは異なり、かつ各構成要素の稼働時間も様々であるため、故障の発生時刻は予測不可能（ランダム）である。

3.3.6 決定論的原因故障（systematic failure）

正しい知識や認識および対策の欠如などを原因とする故障。これらの故障は、設計の変更、あるいは製造プロセス、運用手順、文書またはその他の関連した要因を変更することによってのみ取り除くことができる。通常、変更を伴わない事後保全では、この故障原因を取り除くことはできない。その原因の一例は、安全要求仕様の誤り、ハードウェアの設計、製造、設定や運用における誤り、ソフトウェアの設計、実装等における誤り等、設計や製造における人的過誤（ヒューマンエラー）を含む。決定論的原因故障は、予測不可能である。決定論的原因故障がどのような事象を引き起こすかを簡単には予測することができないため、決定論的原因故障を原因とするシステム故障を統計的に定量化することはできない。

3.3.7 ソフトエラー（soft-error）

物理的な回路自体が故障したわけではないが、何らかの原因によって、回路が保持・処理するデータの内容に生じた誤った変更を指す。ソフトウェアのバグなどのプログラム作成エラーのことではない一過性のものである。宇宙線等によって、メモリ、デジタル論理、アナログ回路および伝送回線などで発生することがある。回路自体にはエラーは起きていないため、ソフトエラーの発生後にデータを再書込した場合、回路は本来の状態に回復する。ソフトエラー発生に関するデータは、例えば製造業者から入手できる場合がある。

3.3.8 共通原因故障（common cause failure）

単一の故障によって、複数の機器や装置の同時故障や機能喪失（機能失敗）を発生させる故障をいう。「多重チャネル系の二つ以上の個別チャネルが同時に故障し機能喪失（機能失敗）を引き起こし、その結果、システムの機能喪失（機能失敗）に至る故障」と定義されている。多重チャネルを持つ安全関連システムの機能失敗確率の計算などでは、ランダムハードウェア故障と共に考慮されるべき故障である。
安全関連系の機能失敗確率の計算では、共通原因故障による故障割合を β ファクター（ベータ・ファクター）として扱っている。β ファクターは、検出ができない危険側故障のうちの共通原因故障の割合で、% で表される。

3.3.9 共通モード故障（common mode failure）

「同様の誤った結果を引き起こす、2 つ以上のチャネルで同様に起きる故障」であり、主に設計やメンテナンスにおける品質の問題などによって引き起こされる故障である。単一の要因によって、冗長機器

の場合でも同じモードで同時に故障するので、この故障は多重化によっても軽減はできない。
注：本用語は、JIS C0511（IEC 61511）に記載されている用語であり、JIS C 0508（IEC 61508）に記載はない。

3.3.10 安全関連系の故障（safe, dangerous, detected, undetected failure）

ランダムハードウェア故障から、機能喪失（機能失敗）確率を計算するために、故障率をベースとした数値を採用している。安全関連系が故障したとき安全機能状態が維持または安全機能が誤作動する故障を“安全側故障”といい、安全機能を喪失して動作できない故障を“危険側故障”と呼んでいる。安全関連系のランダムハードウェア故障の故障率では、全体の故障を安全側故障、危険側故障、検出できる故障、検出できない故障に分けて計４つの故障を扱う。
すなわち、全体の故障率（総故障率）をλとすると、以下の式となる。
$\lambda = \lambda_{SU} + \lambda_{SD} + \lambda_{DU} + \lambda_{DD}$
λ_{SU}（検出できない安全側故障）、λ_{SD}（検出できる安全側故障）、λ_{DU}（検出できない危険側故障）、λ_{DD}（検出できる危険側故障）である。

3.3.11 安全側故障（safe failure）

安全関連系において、安全状態に移行する、または安全状態を維持するように、安全機能が誤作動する故障を指す。安全関連系の故障率では、λ_{SU}（検出できない安全側故障）とλ_{SD}（検出できる安全側故障）の両方の和で計算される。
故障の発生時にシステムを安全側にするかは、システム構成やシステムのチャネル構成などにも依存する。“迷惑故障”、“擬似トリップ故障”、“誤トリップ故障”なども“安全側故障”と分類される。

3.3.12 危険側故障（dangerous failure）

安全関連系の安全機能を機能できなくなる状況に置く可能性のある故障を指す。安全関連系の故障率では、λ_{DU}（検出できない危険側故障）、λ_{DD}（検出できる危険側故障）の両方の和で計算される。
故障の発生時にシステムを危険側の状態にするかどうかは、システム構成やチャネル構成などにも依存する場合がある。冗長化システムにおいては、一つのハードウェアの危険側故障によって、システム全体が危険な状況または機能できなくなる状況に至る可能性を小さくすることができる。

3.3.13 安全側故障割合（safe failure fraction、 SFF）

装置のランダムハードウェア故障の全故障率に対する、全安全側故障率と検出可能な危険側故障率との和の比率を指し、以下の式で表される。
$SFF = (\lambda_{SU} + \lambda_{SD} + \lambda_{DD}) / \lambda$
SFF が大きいということは、「検出できない危険側故障（λ_{DU}）が少ないということで、万一故障が発生しても、安全関連システムが安全機能を実行できる割合が高い」ということを意味する。

3.3.14 診断カバー率（diagnostic coverage、 DC）

運転中に自動的に実行されるオンライン診断テスト機能を適用したサブシステムまたは構成部品の全危険側故障率に対する検出可能な危険側故障率の比率。オンライン診断機能が充実した製品は診断カバー率（DC）が高く、安全性が高いと言える。

3.4 機能安全に関する用語

3.4.1 安全関連系（safety-related system）

安全関連系（safety-related system）とは、制御される機器を安全な状態に移行させるまたは安全な状態を維持するためのシステムである。例えば、あるセンサで異常を検知して燃料などの緊急遮断弁を動作させるシステムなどが該当する。

3.4.2 機能安全（functional safety）

例えば化学プラントなどで、制御装置に付随してインターロックや緊急遮断などを実現する装置などを使用して、必要な安全の確保を行い、これら機能や装置が動作することによって達成される安全を「機能安全」と呼ぶ。装置自体を故障や事故が発生しないように考える本質安全とは異なって使用される。なお、「機能安全」は制御装置自体により実行される場合もある。

3.4.3 安全機能（safety function）

特定の危険事象に関し、装置の安全な状態を達成または維持する機能を呼ぶ。E/E/PE（電気・電子・プログラマブル電子）や、その他の技術による安全関連系または他リスク軽減措置によって実行される機能である。

3.4.4 安全要求仕様（safety requirements specification、 SRS）

安全関連系の実現において必要な要求事項をまとめ、すべての安全要求を記述した仕様書である。文章、フローダイアグラム、マトリックス、ロジックダイアグラム等を用いて、必要な機能が明確に記述される。

3.4.5 妥当性確認（validation）

検討段階または設置前後に、安全関連系が安全要求仕様を満たしていることを実証する業務で、確認と各種証明データが求められる。

3.4.6 適合確認（verification）

安全ライフサイクルの各フェーズにおける引継ぎ事項に対して、すべての観点から設定された目的と要求事項とに適合していることを、分析および試験によって確認することを指す。適合確認は、要求仕様

書で要求された事項の各フェーズにおける確認でもある。

3.4.7 安全計装システム（safety instrumented system、 SIS）

安全度水準（SIL）を要求される安全計装機能（SIF）を実行する計装システムで、検出端（センサ）、論理処理部、および操作端（アクチュエータ）を組み合わせて（ループとも呼ばれる）構成される。
制御系の人間による操作や判断が安全計装システム（SIS）の一部である場合、運転操作のアベイラビリティおよび信頼性は、安全要求仕様書（SRS）で規定され、この SIS の性能計算に含まれていなければならない。
注：本用語は、JIS C0511（IEC 61511）に記載されている用語であり、JIS C 0508（IEC 61508）に記載はない。

3.5 運用モードに関する用語

3.5.1 運用モード（mode of operation）

「低頻度作動要求モード」、「高頻度作動要求モード」、および「連続モード」の 3 つの運用モードに分類されている。IEC 61511:2003 では「作動要求モード」と「連続モード」の 2 つであったが、IEC 61508:2010（Ed.2）で、3 つの運用モードに分類された。ここでは、より新しい規格である JIS C 0508 （IEC 61508:2010）の内容で解説する。

(1) 低頻度作動要求モード（low demand mode）：作動要求が発生した時のみ、被制御機器（EUC）を安全な状態にする運用で、安全関連系への作動要求頻度が、1回／年より大きくない場合が該当する。
(2) 高頻度作動要求モード（high demand mode）：作動要求が発生した時のみ、被制御機器（EUC）を安全な状態にする運用で、安全関連系への作動要求頻度が、1回／年より大きい場合が該当する。
(3) 連続モード（continuous mode）：安全関連系へ、通常運転の一環として、連続的に安全状態を保持するような場合が該当する。

3.5.2PFD（probability of failure on demand、作動要求時の機能失敗確率）

安全関連系の運用モードが「低頻度作動要求モード（low demand mode)」のときに使われ、「安全機能が作動しようとした際に、安全機器やシステムが危険側に故障している確率」である。PFD（作動要求時の機能失敗確率）値は、装置や部品の故障率をベースとしている。

3.5.3PFDavg（average probability of failure on demand、作動要求時の機能失敗平均確率）

機能失敗平均確率とは、安全関連系の運用モードが「低頻度作動要求モード（low demand mode)」のときに使われ、安全機能が作動しようとした際に、機器やシステムが危険側に故障している確率の平均値である。装置や部品の故障率から算出される PFD（作動要求時の機能失敗確率）値は、時間の経過と共に増加する方向で変化する。プルーフテストによって、PFD 値の増加分はリセットされると仮定し、

安全関連系の計算では、機能失敗確率の平均値（PFDavg）で評価される。

3.5.4PFH（単位時間当たりの時間平均危険側故障頻度 average frequency of a dangerous failure per hour）

プロセスが、高頻度作動要求（high demand mode）と連続モード（continuous mode）の場合には、間欠的ではなく、連続的な作動要求が求められ、安全関連系の危険側故障率が直ちに設備の安全性を左右する。そのため、機能失敗確率（probability of failure）として、単位時間内おける危険側への故障頻度の平均値（PFH 単位時間当たりの時間平均危険側故障頻度）が、その安全度の単位となる。
通常のプロセス産業界では、制御系と安全関連系は独立しており、ほとんどの安全関連系が低頻度作動要求として分類されている。

3.6 安全度に関する用語

3.6.1 ハードウェア故障許容/ハードウェアフォールトトレランス（hardware fault tolerance、 HFT）

ハードウェアフォールトトレランスとは、ハードウェアに一つの以上の危険側故障が生じた場合でも、コンポーネントまたはサブシステムに要求される安全機能を継続して行う能力である。
センサ（検出端）、論理処理部および操作端（アクチュエータ）は、安全度水準に見合った最低限の HFT を持たなければならない。ハードウェアフォールトトレランス（HFT）が N とは、N+1 の故障で、システムの安全機能が失われることを意味する。例えば、二重化された論理処理部では、HFT は 1 で、1 台（シングル）の故障では安全機能を継続できるが、2 台（HFT+1）の故障で安全機能が失われる。ただし、二重化しても機能的に HFT は 1 とならない場合があるので、その構成については注意が必要である。

3.6.2 ハードウェア安全度（hardware safety integrity）

安全関連系の危険側のランダムハードウェア故障に関する安全度のひとつである。危険モードの故障に関連したハードウェアの故障で、安全機能の安全度を低下させる故障の程度を指す。

3.6.3 実績による使用（proven in use）

安全関連系のハードウェア構築で、機器の選択と構成を確定するために、使用する機器のアーキテクチャや安全度の確認がなされ、目標の安全度レベル（SIL）を満足しているかどうかが確認される。そのときのパラメータの一つで、安全度故障割合（SFF）によらず、実績の有無や過去に使用した経験に基づいた（“proven in use”）選択ができる。部品の使用経験に基づき、この部品が安全関連系の構成要素としての使用に適切であるという証拠の存在がデータや文書による評価によって示されている必要がある。具体的には、該当機器の運用実績数、運用実績期間、故障データ、使用経験などが揃っていることによって妥当性が判断される。

3.6.4 安全度（safety integrity）

定められた期間以内に、定められた条件下で、安全関連系が必要な安全機能を十分に実行できるであろう確率で、安全度水準（SIL）を算出して安全機能は評価される。

安全度の決定では、危険側に導く故障（ランダムハードウェア故障と決定論的原因故障の両方）のすべての原因を含んで査定する。ただし、（ハード、ソフトの）設計、製造過程、運用手順、文書またはその他の関係した要因に起因するような故障（決定論的原因故障）などは、正確には定量化が困難で、定性的に検討した結果だけで評価される。

安全機能の安全度は 4 つのレベルに等級化され、SIL が高くなるにつれ、より高い安全性能が求められる。

3.6.5 安全度水準（safety integrity level、 SIL）

安全関連系に割り当てられる安全機能の安全度要求事項を規定する（4 段階の）水準があり、安全関連系が担うべきリスク軽減の度合いである。安全度水準 4 が安全度の最高水準、安全度水準 1 が最低水準となる。各レベルに対して、機能失敗平均確率が割り当てられている。

3.6.6 プロセスセーフティタイム（process safety time）

被制御機器（EUC）制御系に危険事象を引き起こす可能性のある故障が発生してから、当該危険事象が起きないように被制御機器の処置を完了するまでの許容時間である。

検出端（センサ）や操作端（アクチュエータ）の応答時間、また論理処理部の検知時間と応答時間の全部の合計がプロセスセーフティタイム以内であることを保証しなければならない。プロセスセーフティタイムは、アプリケーションの要求、また、適用される工業規格によって異なる。

4. 安全ライフサイクル

4.1 全安全ライフサイクルの概要

4.1.1 全安全ライフサイクルの構成

図 4.1 に全安全ライフサイクルの構成を示す。全安全ライフサイクルは、E/E/PE 安全関連系の構想から設計、実現、廃却に至るまでの全ての業務を系統的に取り扱うための枠組みである。また、全安全ライフサイクルを通して、安全関連系の重要な情報を記録として残すことも目的としている。

全安全ライフサイクルの業務内容は 16 のフェーズに分けられている。各フェーズに対して要求事項があり、その要求事項に適合する必要がある。また、全安全ライフサイクルを通して、機能安全の管理、機能安全評価に関する業務を行う必要がある。

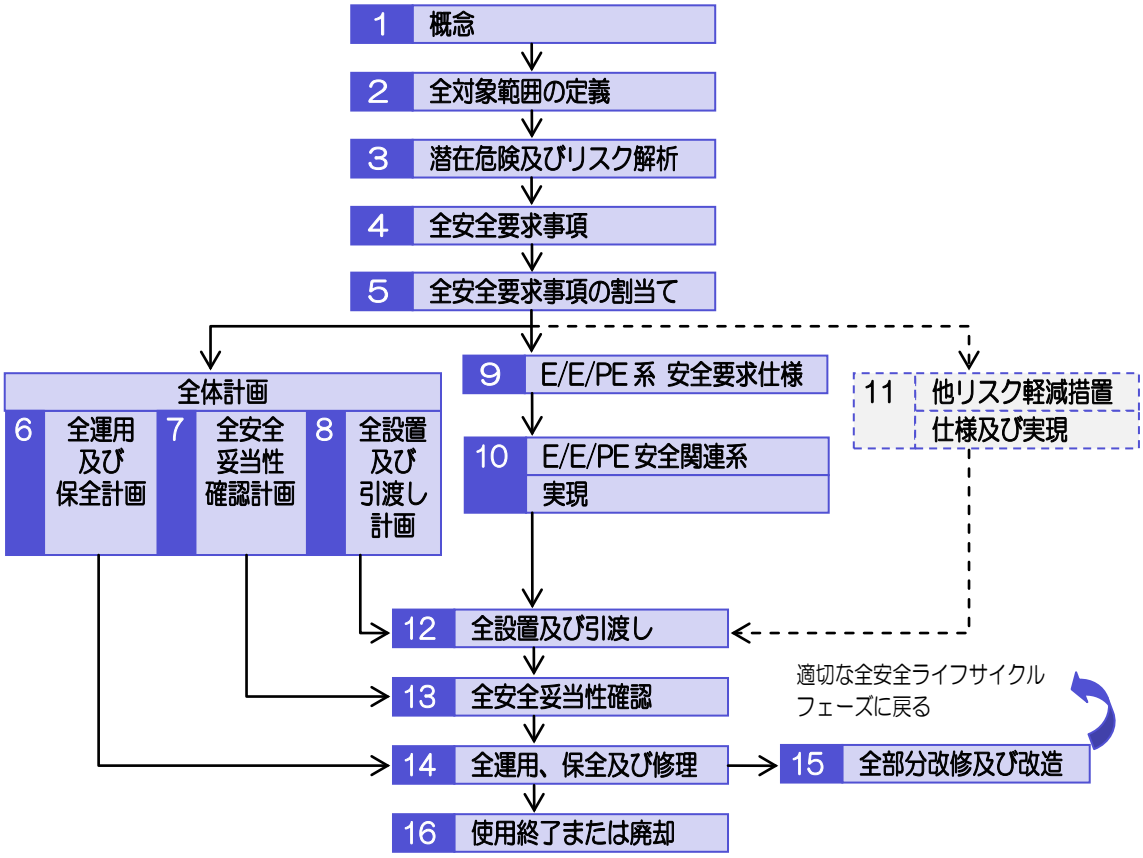


図 4.1　全安全ライフサイクル

4.1.2 全安全ライフサイクルの各フェーズの内容

全安全ライフサイクルの各フェーズの内容を表 4.1 に示す。

表 4.1　全安全ライフサイクルのフェーズとその内容

フェーズ		内容
1	概念	装置の置かれている環境、法規制などを十分に把握し、潜在危険、危険状態、危害事象を明確化する。
2	全対象範囲の定義	リスク解析を実施するにあたり、装置の範囲、及び潜在危険の範囲を決定する。
3	潜在危険及びリスク解析	装置の潜在危険、危険状態、危害事象を明らかにし、リスク解析を実施する。
4	全安全要求事項	リスク軽減手段と安全機能の仕様を決定する。また、定量的な方法、定性的な方法を用いて安全度水準を決定する。
5	全安全要求事項の割当て	リスク軽減を達成するために、安全関連系に対して安全機能を割り当てる。また、安全度水準を用いて、安全機能に対する目標機能失敗尺度を決定する。
6	全運用及び保全計画	安全機能が維持されるような、運転、検査、停止などの各運用時の業務手順や制限事項を決定する。
7	全安全妥当性確認計画	安全機能が安全要求を満たしていることを確認する、妥当性確認の手順、技法などを決定する。
8	全設置及び引渡し計画	設置及び引渡しの手順、担当などを決定する。
9	E/E/PE 系安全要求仕様	応答特性、運用モード、耐用年数、環境条件などを考慮して、割り当てられた安全機能の仕様を明確化する。
10	E/E/PE 安全関連系：実現	E/E/PE 系安全要求仕様を満たす安全関連系を作る。
11	他リスク軽減措置：仕様及び実現	安全要求仕様を満たす E/E/PE 安全関連系以外の設備を作る。（※ このフェーズは規格の対象外である。）
12	全設置及び引渡し	E/E/PE 安全関連系の設置、引渡を計画通りに実行する。
13	全安全妥当性確認	E/E/PE 安全関連系の妥当性確認を計画通りに実行する。
14	全運用、保全及び修理	安全機能が維持されるように、運用及び保全を計画通りに実行する。
15	全部分改修及び改造	安全機能が部分改修や改造の期間中も維持されるように、計画及び実行する。
16	使用終了または廃却	使用終了や廃却中、またその後においても安全が適切に維持されるように、計画及び実行する。

4.2 全安全ライフサイクルの詳細

全安全ライフサイクルが安全に関係する全業務を含む枠組みであることは、4.1 章でも記載した。安全を確保する対象がプラントのような大規模なものである場合には、全業務の範囲は単一の企業で収まらずに、ユーザ、エンジニアリング、コンポーネントサプライヤなどの複数の企業が関係してくることになる。そのため、全安全ライフサイクルを理解する上では、大まかな内容を把握し、担当する業務範囲を理解することが第一となる。

以降では、全安全ライフサイクルの全容をつかむために、いくつかのフェーズにまたがる内容をひとまとめにして記載する。詳細な内容については、JIS C 0508：2012（IEC 61508：2010）の第 1 部を参照のこと。

4.2.1 リスクアセスメントとリスク低減（フェーズ 1～5）

全安全ライフサイクルを通じて実施するのは、特定された危険源のリスク低減、リスク低減の実現、実際の運用、これらを実施することにより危険源のリスクを目標リスクまで低減することである。

対象となる装置によっては一つの設備に対して複数の潜在危険源が存在する場合がある。各潜在危険に対して、目標リスクを定めて、リスクの低減を実施することが必要である。

リスク低減の参考手順を右図に示す。

手順 1：機器やプロセスの想定される使用方法、使用者、使用時間などを明確化する。また、意図される使用を特定し、予見可能な誤使用を見積もる。

手順 2：使用（設置、保全、修理、廃却含む）の全段階で想定される潜在危険を列挙する。性質（毒性・腐食性・爆発性等）・量・時間。

手順 3：列挙された潜在危険の危害の程度と発生頻度をもとに、リスクを見積もる。

手順 4：見積もられたリスクとリスク低減手段を考慮して残存リスクを見積もる。

手順 5：残存リスクが許容可能なレベル（目標リスク）まで到達しているか判断する。

手順 6：許容可能なレベルに到達していない場合は、追加のリスク低減手段を用いる。

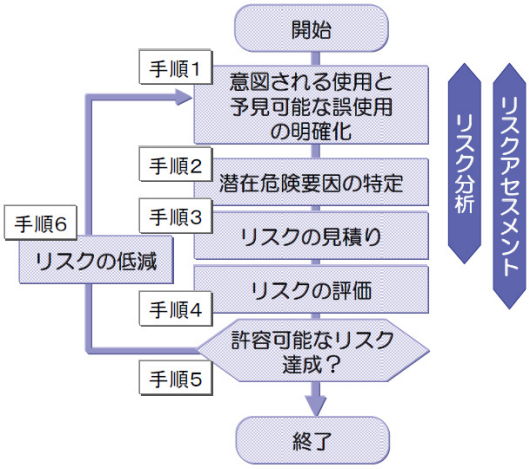


図 4.2 潜在危険、リスク評価の一般的な流れ

4.2.2 安全要求事項の実現（フェーズ 9～10）

リスク分析・評価により決定された安全機能及び安全度水準（SIL）に関して具体的な要求事項をまとめたものが安全要求仕様（SRS: Safety Requirements Specification）となる。SRS は実際の設計・開発における入力情報となる。

SRS には、次のような主な要求事項を盛り込まなければならない。

- 処理能力や反応時間といった機能的要求事項
- PFDavg やSIL など安全度に関する要求事項
- 運用に関する必要条件と運用限界に関する事項

安全要求仕様書に基づいて、ハードウェア設計、ソフトウェア設計を実施する。ハードウェア設計では必要な安全度水準を達成するための機器を調達し、それらを組合せてシステム構築を行う。ソフトウェア設計では、ソフトウェア開発ライフサイクルにしたがって開発する。詳細な内容については、IEC 61508：2010の第2部、第3部を参照のこと。

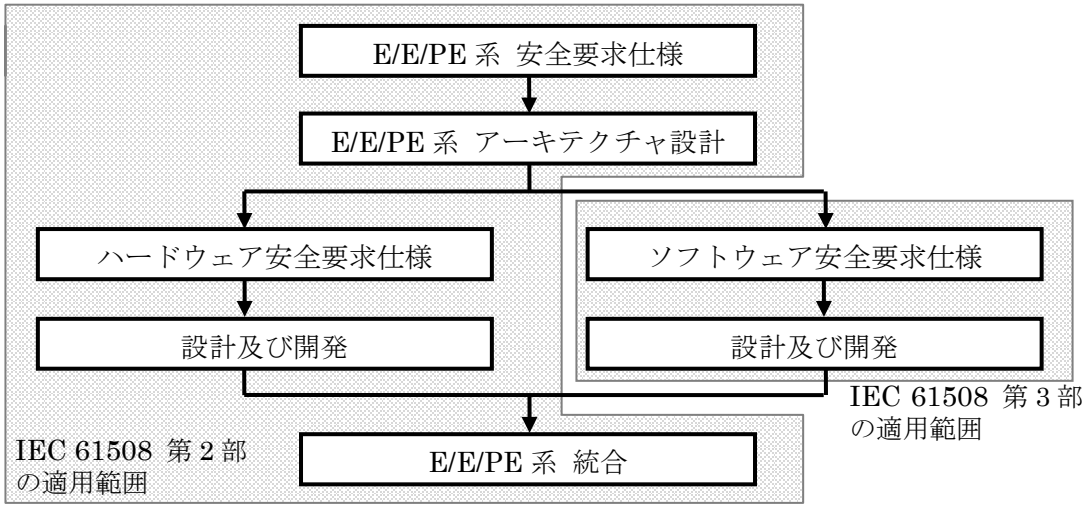


図 4.3 ハードウェアとソフトウェアの実現と第 2 部、第 3 部の適用範囲

(1) ハードウェア

ハードウェアの設計・開発に際しては、ランダムハードウェア故障、及び決定論的原因故障を考慮する必要があり、以下のような要求事項への適合が必要となる。

- ハードウェア安全度要求事項
- 決定論的安全度の要求事項
- 異なるチャンネル間の独立性の達成
- フォールト検出時の挙動の要求事項
- データ通信プロセスの要求事項

ハードウェア安全度要求事項、決定論的安全度の要求事項に適合するためは、各々いずれかのルートを選択し、その要求事項に適合する必要がある。

ハードウェア安全度の要求事項

ルート 1_H ： HFT＝0の要素の主張できる最大の SIL を表から求める。（表 4.2 を参照）
アーキテクチャを整理し、直列要素は最大値から SIL を求め、並列要素は和から SIL を求め、最終的に安全関連系全体の主張できる SIL を決定する方法。

ルート 2_H ： 目標安全度水準と運用モードから、サブシステムに必要とされる最小の HFT を表から求める。（表 4.3 を参照）
ランダムハードウェア故障の定量化の際、信頼性データとして類似のアプリケーションでの使用経験において、IEC 60300-3-2 または ISO 14224 に基づいて収集されたデータを評価して使用する。

決定論的安全度の要求事項

ルート 1_S ： 適合開発を行う。設計・開発の間、決定論的原因フォールトの回避のために、目標安全度水準に応じた適切な技法を使用する必要がある。また、設計の残存フォールト、電磁外乱、環境ストレス、ヒューマンエラー、通信エラーなどの保全性、試験性を考慮する必要がある。
ソフトウェアに関しては、第３部に従った開発が必要となる。

ルート 2_S ： 使用実績による証明。機能が明確に限定されており、危険な決定論的原因故障の可能性が十分に低い場合にのみ適用できる。運用経験の解析と適合性解析、及び試験による証拠文書を準備する必要がある。

ルート 3_S ： 非適合開発を行う。既存のソフトウェアにのみ適用できる手法。安全マニュアルの準備、ソフトウェア安全要求仕様の準備、安全性の検討結果、設計資料、テスト結果の文書化、適合確認、妥当性確認の結果などの対応が必要。

図 4.4 ハードウェア設計・開発におけるルートの選択

ハードウェア安全度の要求事項の達成手順は、以下のような手順となる。

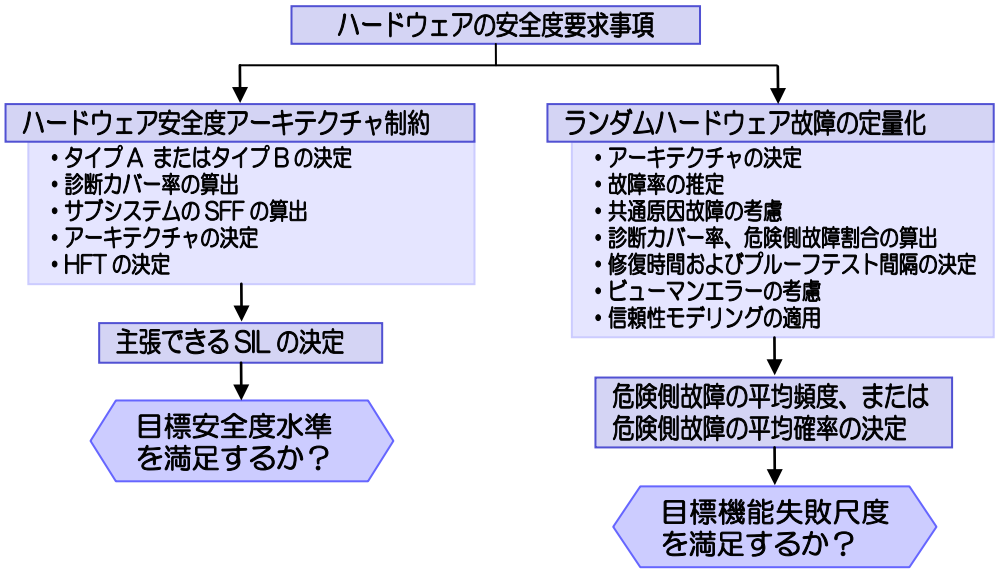


図 4.5 ハードウェア安全度要求事項の達成手順

表 4.2 主張することのできる安全機能の最大許容安全度水準

(1) タイプ A の安全関連要素

安全側故障割合（SFF）	ハードウェアフォールトトレランス（HFT）		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% ～ <90%	SIL 2	SIL 3	SIL 4
90% ～ <99%	SIL 3	SIL 4	SIL 4
≧99%	SIL 3	SIL 4	SIL 4

(2) タイプ B の安全関連要素

安全側故障割合（SFF）	ハードウェアフォールトトレランス（HFT）		
	0	1	2
<60%	許容しない	SIL 1	SIL 2
60% ～ <90%	SIL 1	SIL 2	SIL 3
90% ～ <99%	SIL 2	SIL 3	SIL 4
≧99%	SIL 3	SIL 4	SIL 4

表 4.3 安全関連系の各サブシステムの最小ハードウェアフォールトトレランス制限

要求される安全度水準	SIL 4	SIL 3	SIL 2		SIL 1
運用モード	全モード	全モード	高頻度又は連続モード	低頻度モード	全モード
最小ハードウェアフォールトトレランス	2	1	1	0	0
備考：タイプ B 要素は、最低限 60%以上の診断カバー率を持たなければならない。					

(2) ソフトウェア

ソフトウェアの設計・開発に際しては、決定論的原因フォールトの回避と管理に関する適切な技法や手段を使用することで対応する必要がある。IEC 61508：2010 の第 3 部には、ソフトウェア安全ライフサイクルのフェーズ毎に推奨される技法の一覧が記載されており、その中から選択する。

ソフトウェア安全ライフサイクルは、新規の大規模なシステム開発に適した内容となっているため、小規模なシステムにおいては、目標安全度及び複雑さに応じて V モデルを適切に修正し、ライフサイクルモデルとして適用しても良い。

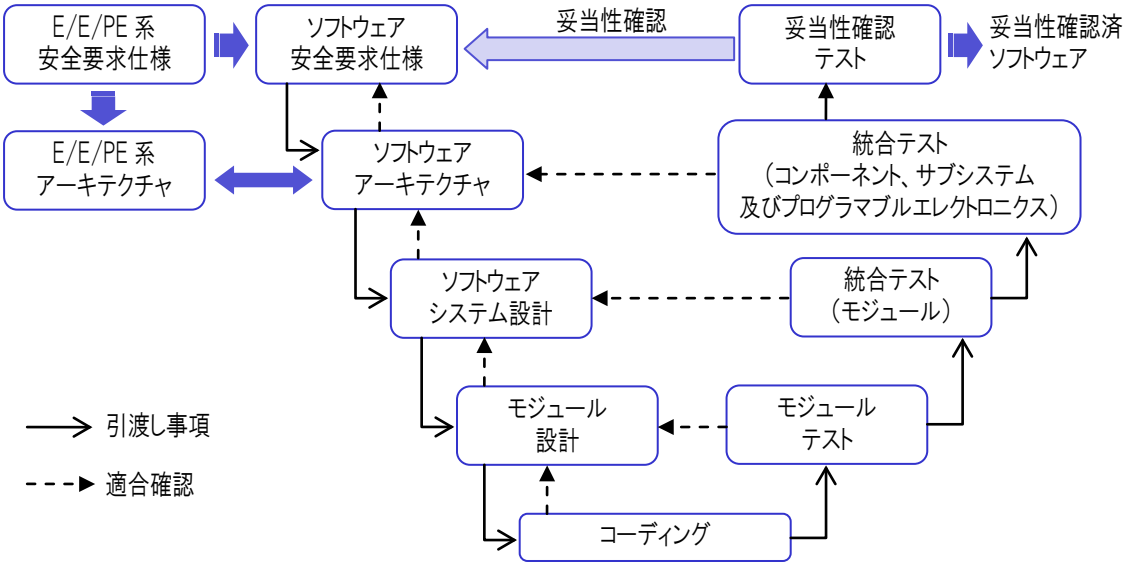


図 4.6 ソフトウェアの開発ライフサイクル（V モデル）

4.2.3 設置・試運転（フェーズ 7～8、12～13）

設置及び引渡しは、機能安全の達成が保証できるように計画を立てて実施する。設置・引渡しのいずれも業務記録を残す。

実際の据付けが設計情報に適合しないことがわかった場合は、安全性への影響を予測しなければならない。不適合が安全性に影響を及ぼさないと判明した場合は、設計情報を実際の状態に書き換える必要がある。それ以外の場合は、設計の要求事項に合わせて据付けを変更しなければならない。

4.2.4 運用及び保全計画（フェーズ 6、14～15）

通常運転、及び保全（コンポーネントの修理、交換、プルーフテストなど）の間、適切な安全機能が確保されるように、計画を立てて実施する。通常の運転稼働状態だけでなく、立ち上げ作業、定期点検作業、故障時などの定常運転状態ではない状態においても安全機能が確保されるように手順を立てて実施する。実施に際しては、その記録を残す。

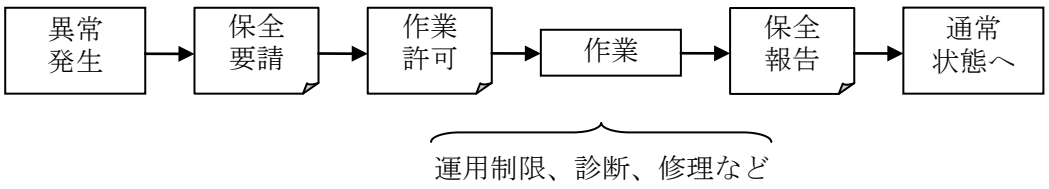


図 4.7　保全業務の流れ

決定論的原因フォールトが見つかった場合や、装置の部分改修などに伴い、安全機能の部分改修を行う必要が出た場合には、部分改修の間やその後に確保されるように、計画を立てて実施する。

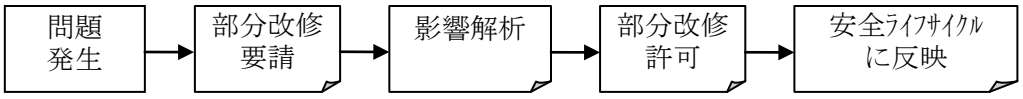


図 4.8　部分改修要請の流れ

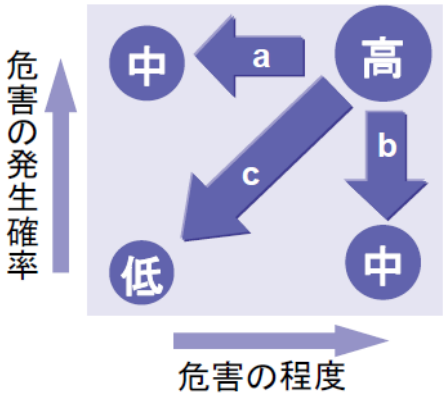
4.2.5 使用終了（フェーズ 16）

使用終了、廃却業務に伴って、作業中・作業終了後において適切な安全が確保されるように、計画・実施する。計画を立てる際には、影響解析を実施する必要がある。使用終了・または廃却の実施可否は、影響解析結果に基づく。また、作業結果については記録を残す。

4.3 リスク評価

4.3.1 リスクと危害

リスクの大きさは「危害の発生確率」と「危害の程度」の組合せで決まる。「危害の発生確率」は、例えば、ある期間内で 1 回または複数回発生する確率であり、「危害の程度」は、例えば、想定される被害者数などで表わされる。



a ：危害の程度を下げてリスクを小さくする
b ：発生確率を下げてリスクを小さくする
c ：複合でリスクを小さくする

図 4.9　リスクの大きさの概念

リスクは潜在危険によって存在し、この潜在危険の解消が根本的なリスク解消につながる。しかし、潜在危険はなんらかの形で存在するので、結果としてリスクがゼロになることはない。この時の残ったリスクが残存リスクとなる。潜在危険が有ったとしてもそこに人がいなければ危害を受けることはない。つまり、潜在危険に対して人が存在しているときに危険状態が生まれる。この危険状態を無くすために保護方策を実施するが、この保護方策が正しく働かなかったときに危険事象が発生した場合に「危害」が生まれる。

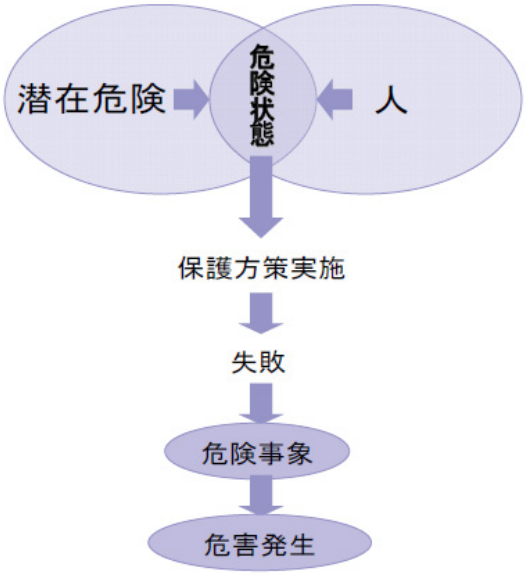


図 4.10　潜在危険と危害発生のかかわり

4.3.2 リスク評価の手法

潜在危険およびリスク評価に使用される代表的なツールを下図に示す。
使用する手法は考えられる適用業務によって選定する。

表 4.4　リスク評価の代表的なツール

ツール名		概要	リスク分析	ハザード	
				特定	分析
FMEA	Failure Mode and Effect Analysis	システムを構成する各機器の故障が、プラント全体にどのように影響するかを系統的に検討する	◎	◎	
FTA	Fault Tree Analysis	望ましくないﾄｯﾌﾟの事象から始めて、この事象が発生するあらゆる原因を見つけ出す	◎	◎	◎
ETA	Event Tree Analysis	事故の引き金となる事象をSTARTとして、その事象が伝搬して潜在的結果に至るまでをﾓﾃﾞﾙ化	◎		◎
HAZOP	Hazard And Operability	ｶﾞｲﾄﾞﾜｰﾄﾞを使い、設計とのズレを仮定して、ﾊｻﾞｰﾄﾞを系統的に見つけ出していく	◎	◎	
LOPA	Layer of Protection Analysis	保護ﾚｲﾔｰに重点を置いたｲﾍﾞﾝﾄﾂﾘｰ解析。事故に至るﾊｻﾞｰﾄﾞの頻度を設定するのに効果	◎		
RISK MATRIX	-	危害の頻度、影響の度合いの大きさによって、リスクのレベルを分類する手法	◎		
RISK GRAPH	-	いくつかのパラメータの組み合わせによって、リスクのレベルを分類する手法	◎		

4.3.3 多層防護によるリスク軽減の考え方

推定したリスクに対して、目標の許容リスクを達成するためにリスク軽減を行う必要がある。図 4.3.3.1 に、目標の許容リスクを達成するためのリスク軽減の一般的な概念を示す。

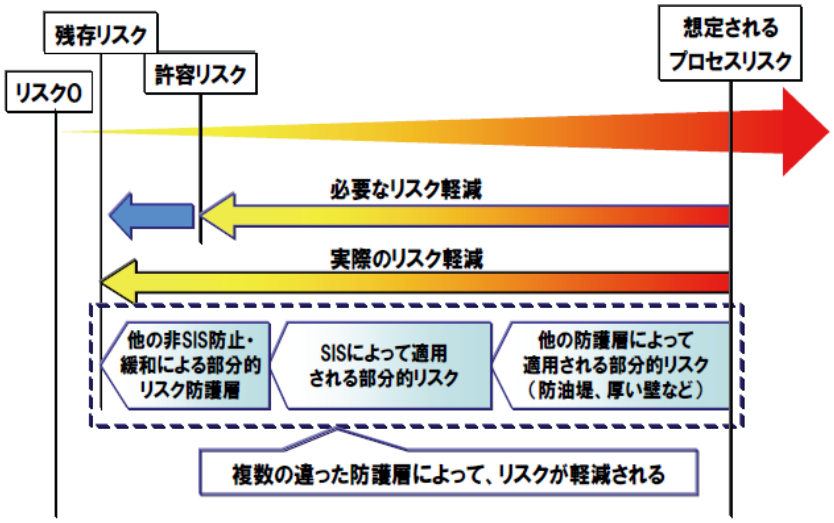


図 4.11　リスク軽減の一般的概念

必要なリスク軽減は、許容リスクを満たすために、達成されなければならないリスク軽減の最低水準である。それは、複数の異なる防護層の組合せによる多層防護で達成することが可能である（図 4.3.3.2）。それぞれの防護層が全体のリスク軽減に対してどのくらいになるかを定性的または定量的に分析し、安全機能の割り当てを行い、それぞれの安全機能に対する安全度水準（SIL）を決定する必要がある。
各防護層は、制御、予防または緩和によってリスクを軽減する任意の独立した機構で、電気系によらない他リスク軽減措置や、避難手順などの行政手段、システムの運用や組織、教育・訓練なども防護層の一つとして考えられる。これらの対処手段は、自動化されても、または人間によって開始されてもよい。防護層間での独立性、防護層の多様性、異なる防護層間での物理的な分離などが求められる。他リスク軽減措置には、安全排出装置、防火壁または堤防（ダイク）などが含まれ、広義においては、緊急放送・連絡設備や非難手順なども含まれる。

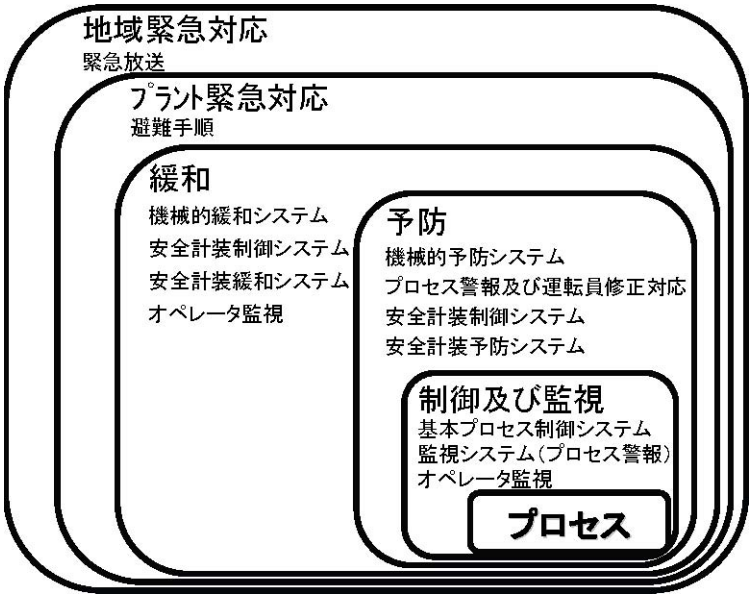


図 4.12　多重防護層（Protection layers）

4.4 機能安全の管理

4.4.1 機能安全の管理とは

機能安全の要求事項が全ライフサイクルにおいて確実に計画・実行するために必要な管理作業を機能安全の管理と呼び、次のことが求められている。

- 各ライフサイクルフェーズ、または全ライフサイクルにおける個人、および組織の責任について文書化し、規定すること
- 実行されるべき業務について、文書化し、規定すること

次にあげるような項目を確実に実施できるように、手順を規定する必要がある。

- 潜在的危険およびリスク解析
- 機能安全評価
- 適合確認業務（Verification）
- 妥当性確認業務（Validation）
- 構成管理（安全ライフサイクルの各フェーズにおける、実現した機能を構成する要素の管理）
- インシデント報告および解析

例えば安全計装システムに関して言えば、それに係わる安全ライフサイクルの取り組みを実行するのに必要な技能や知識を確認することが望ましく、それぞれの技能には、必要な能力レベルを定義することが望ましい。下記に必要な技術や知識を示す。

- プロセス分野に適した工学上の知識、訓練および経験
- 使用される対応技術（例えば、電気、電子またはプログラマブル電子）に適した工学上の知識、訓練および経験
- 検出端と操作端とに適した工学上の知識、訓練および経験
- 安全工学の知識（例えば、プロセス安全分析）
- 法的および安全規制上の要求事項の知識
- 安全ライフサイクル業務の役割に適した十分な管理能力および指導力
- ある事象に関して起こり得る結果に対する理解力
- 安全計装機能（SIF） の安全度水準
- アプリケーションおよび技術の新規性および複雑性

4.4.2 文書化

安全ライフサイクルの全フェーズ、とくに機能安全、適合確認、機能安全評価などの諸業務の管理が効果的に実行できるように文書化すべき必要な情報について規定している。文書化においては、つぎの要求事項が記載されている。

- 正確で簡潔であること
- 文書利用者が容易に理解できること
- 意図した目的に適していること
- 利用しやすく、保全が可能であること
- 文書の版を識別ができること
- すべての関連文書は改訂、修正、見直し、承認がなされること

4.4.3 機能安全評価

機能安全評価とは、安全ライフサイクルの各段階で、独立した機能安全評価実施者による検査や監査を実施することである。「独立した」とは、設計に関与しなかった担当者または担当組織が、機能安全評価を実施することを指す。独立性の最低基準は、被害の程度、安全度水準に応じて規定されている。被害の程度に応じた独立性の最低現の水準をつぎの表に示す。表中の HR、NR の定義は下記のとおり。

HR: 特定された被害、安全度水準に対して、最低限要求される独立性の水準。HR1、HR2 がある場合は、HR2 の適用が望ましい。

NR: 特定された被害、安全度水準に対して、不十分とされる独立性の水準。

表 4.5 独立性の最低限の水準（安全ライフサイクルフェーズ 1-8 および 12-16）

独立性の最低水準	被害の程度			
	A	B	C	D
独立した人員	HR	HR1	NR	NR
独立した部門		HR2	HR1	NR
独立した組織			HR2	HR
被害の程度	A: 一時的な機能喪失 B: 1 名以上の深刻な永久障害、または 1 名の死亡 C: 数名の死亡 D: かなり多数の人命損失			

表 4.6　独立性の最低限の水準（安全ライフサイクルフェーズ 9 およびソフトウェア安全ライフサイクルの全フェーズ）

独立性の最低水準	安全度水準			
	1	2	3	4
独立した人員	HR	HR1	NR	NR
独立した部門		HR2	HR1	NR
独立した組織			HR2	HR

機能安全評価では次の事項を確認しなければならない（安全計装システムにおける例）。

a) 潜在危険およびリスク評価が行われている。

b) 安全計装システムに適用された潜在危険およびリスク評価から得られた勧告が実施されているまたは問題が解決されている。

c) プロジェクト設計変更手順が整備され、かつ、適切に実行している。

d) 先行した機能安全評価から得られた勧告を実施している。

e) 安全要求仕様にしたがって、安全計装システムが設計され、組み立てられ、かつ、設置されている。また、安全要求仕様と異なる部分が特定され、かつ、問題解決がされている。

f) 安全計装システムに関係した安全、運用、保全および緊急時の手順を整備している。

g) 安全計装システム妥当性確認計画が適切で、かつ、妥当性確認業務が完了している。

h) 要員の訓練が終了し、かつ、安全計装システムについて適切な情報を保全および運転要員に提供している。

i) 更なる機能安全評価を履行するための計画または戦略を整備している。