平成 20 年度
組込みシステムにおける機能安全に関する調査研究

組込み系技術者のための安全設計入門

社団法人　組込みシステム技術協会

機能安全委員会

製品安全ワーキンググループ

はじめに

本報告書は、組込み系の安全性に高い関心をもつ JASA メンバーが集まり、機能安全をテーマに種々調査学習し、討議した内容を基に、組込み系の設計開発に必要と思われる基本知識を集め整理したものです。

近年、多くの製品にコンピュータが組込まれるようになりました。組込み系ソフトウェアの開発量も年々増加しています。その結果、社会インフラや家庭の製品等の利便性、快適性が向上し、社会も個人の生活もより豊かなものになってきました。しかしながら、一方で、製品の故障や想定外の使われ方などにより、思いもよらなかった危害や混乱を発生させる事例も増えています。

ところが、ソフトウェア技術者にとって、安全性確保は、信頼性確保のことである、と考える人がまだまだ多いようです。しかし、安全性と信頼性は、異なる概念です。利用者に危害を与えたり、システムに障害を発生させたりというケースをできるだけ回避するためには、品質を確保したうえで、安全にも配慮していく必要があります。

1998 年から 2000 年にかけて「機能安全」に関する国際規格 IEC 61508（JIS C 0508）が制定されました。IEC 61508 は、開発プロセス、ハードウェア、ソフトウェアの三つの視点から安全関連系に対する要求事項が提示されています。特にソフトウェアに対する要求事項が大きく取込まれた点が注目されます。

従来、「絶対安全」という言葉が、よく使われることがありました。本文中でも述べますが、絶対安全というものはありえません。また、すべての製品やシステムに対して「本質安全」を設計することもきわめて困難なことです。しかし、長い年月、社会通念として、絶対安全や本質安全が強調されてきて、合理的な議論の阻害にさえなってきました。

IEC 61508 の制定後、徐々にリスクを定量的に見る気運が一般にも拡がりだしたように思います。リスクを一定の許容範囲まで抑えるために必要な機能を付加するという「機能安全」という設計思想が注目されるようになって、やっと工学的な議論ができるようになってきたと思います。

製品開発過程で、安全性を確保するためには、まず、できるだけ本質的な安全を組込んでおくわけですが、それでも残存するリスクに対しては、利便性、経済性、使用環境の慣習などとのバランスを考慮しながら、機能的に安全を確保していくことになります。そのためには、信頼性、安全性、リスク分析、システム障害等といった用語や概念について、正しい基本認識が必要です。

本報告書は、組込み系の開発、特にソフトウェア開発に従事する方々にとって、安全設計入門の書となり、また安全性確保の議論のきっかけになればと考えて、編集しました。安全を技術で確保することに、多少なりとも役に立てば幸いです。

最後に、財団法人 JKA や、ご協力頂いた各位に感謝致します。

JASA 安全性向上委員会製品安全ワーキンググループ
主査　金田光範

目　　次

第 1 章　安全の基本

近年、ソフトウェアに起因するシステム障害がマスコミを賑わすようになった。ソフトウェアの安全性については誤解も多く、安全設計は普及徹底されているとは言えない。

本章では、安全にかかわる基本的な用語や考え方、設計手法について概観し、第 2 章以降の理解を容易にするための導入編としている。

第 1.1 節では、事故事例とソフトウェアの安全性について議論し、第 1.2 節では、安全に関する用語や概念について紹介し、リスクの捉え方を整理する。第 1.3 節では、障害と故障についての考え方を紹介し、リスク分析・評価を行う際の前提となる概念を整理する。第 1.4 節では、安全設計の実施方法の概略を紹介し、リスクを低減させるための設計手法や実践的対処法について紹介する。

1.1 事故は何故起きる

1.1.1 過去の事故事例

科学技術の発展によって、文化は大きく向上してきた。車や新幹線、ジェット機がどれほど便利かは多くの人が実感している。また、テレビや Web の情報は、居ながらにして世界中の情報に接することができる。しかし、生活の利便性の向上は、大事故の発生やプライバシーの侵害など、新たな問題も引起こしている。

文明の進歩により、平均寿命が延びていることは、病気や災害への不安が明らかに減っていることの証明でもあると思うのだが、それにもかかわらず、人々は、何かにつけ、不安を感じている。病気や自然災害への不安が減った反面、医療事故や鉄道・交通事故、テロへの不安が相対的に大きくなってきていると思われる。自然への不安よりも社会や産業への不安が大きくなってきている。

製品開発にあたって、その製品が利用者やその周囲の人に危害を与えることを望んでいるエンジニアは、犯罪者でもない限りまずいない。開発に参加するエンジニアは誰もが、利用者に喜ばれ、社会に貢献することを願っているはずである。それでも事故は起きている。事故は何故起きるのだろうか。

過去に発生した事故や失敗事例について、科学技術振興機構（JST）が失敗知識データベース推進委員会（JST 畑村委員会）を設置して 2006 年 3 月から、ネットに公開している（注 1）。その中から、ソフトウェアに関連した事例として、いくつかあげると以下のような事例がある。

1．アリアン 5 型ロケット打ち上げ失敗（制御不能）・・・1996 年 6 月 4 日　仏
2．ソフトのバグによるハイテク航空機の墜落事故・・・・2000 年 12 月 11 日　米
3．データ入力ミスで旅客機が山に激突　　・・・・1995 年 12 月 20 日コロンビア
4．オートドライブコンピュータの疲労（AT 車の暴走）・・1987 年 7 月 12 日　日
5．ソフトウェアの欠陥による放射線治療機事故　・・・・1986 年 3 月 21 日　米

また、最近、マスコミを賑わした国内の計算機トラブルでは、**図 1.1** に示すように、以下のようなものがある。

1．ANA 国内線予約システム障害　（2007 年 6 月 4 日）
2．自動改札機のトラブル　（2007 年 10 月 12 日）
3．東証のシステム障害再発　（2008 年 2 月 8 日、7 月 22 日）

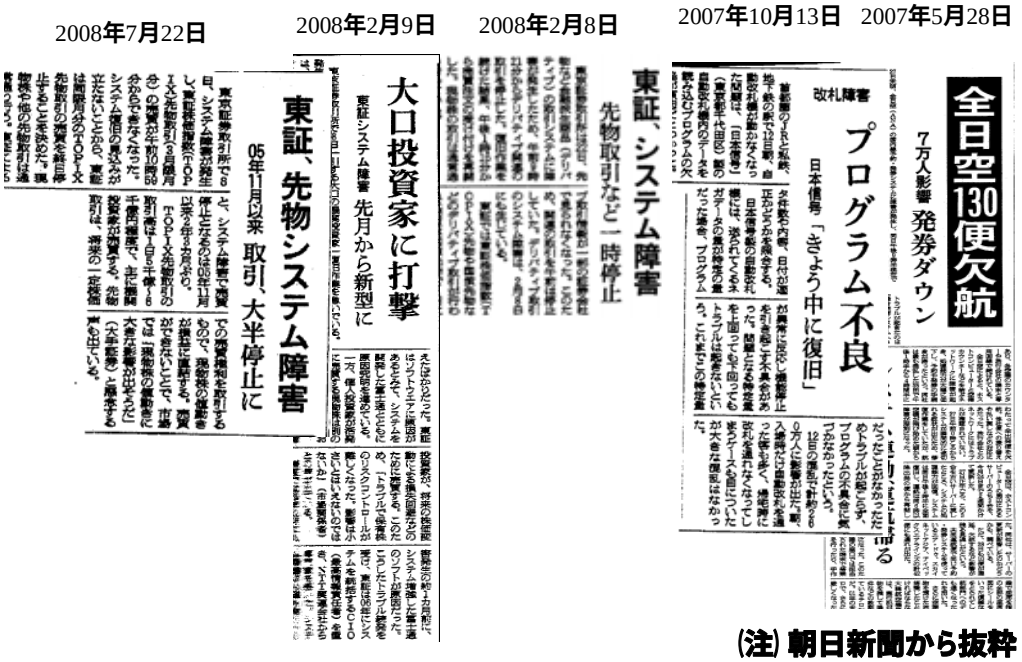


図 1.1　ソフトウェア起因のシステム障害事例

さらに、情報処理推進機構（IPA）の小冊子「組込みシステムの安全性向上の勧め」（注 2）にもソフトウェアのトラブル事例が掲載されている。

このようなソフトウェアに起因するトラブル増加の背景要因としては、計算機システムが大規模になり社会インフラのいたる所に組込まれるようになったこと、マイコンが身近な製品にも多用されるようになったことがあげられる。ソフトウェアの品質が最近低下してきたというより、元々試作段階に近いソフトウェアが急速にかつ大量に普及したため、ハインリッヒの法則（*1）によって大きな事故が目立ってきたものと思われる。これからは、小さなトラブルであっても真剣に撲滅していかないと、大事故を引き起こしかねない。

特に有名な事故事例として、被害額の大きかったアリアンロケット打ち上げ失敗の概要を図 1.2 に示す。

図 1.2　アリアン 5 型事故事例

この事例では、ソフトウェアのわずかなミスが、多大な被害額と多くの人の何年にも渡る準備を一瞬で無にしてしまったものである。ソフトウェアは、わずか一文字のミスでも、最悪の事態を引き起こす恐れがある。

1.1.2　組込み系ソフトウェアの安全性

ソフトウェアの信頼性向上策は、何十年にもわたっていろいろ講じられてきており、昔よりはずっと品質レベルは上がっているはずである。それでもトラブルが増大しているのは、前述の開発量増大だけでなく、安全の思想もしくは視点が開発設計の中に盛り込まれていなかったためと思われる。少なくとも過去のトラブル事例を見る限り、FMEA（failure mode and effects analysis）や FTA（fault tree analysis）を事前に実施しておけば回避できただろうと思われるケースがかなり多い。安全設計は機械設計や電機設計にはつきものであるが、何故かソフトウェア設計には抜けている。

発生した事故への反省や技術の進歩に合わせて、安全に関する法令・規格や種々のガイドラインは、過去に幾度となく整備改訂されてきた。世界中で安全に関する規格は数百件とも千件を超えるともいわれているが、進歩の激しいソフトウェアやマイコンに関しては、

安全設計の指針がほとんどなかった。現在、ソフトウェアの安全設計に詳細に触れている代表的な規格に、IEC 61508（JIS C 0508）（注 3）がある。

計算機の故障やソフトウェア障害に起因したトラブルが増えるに従い、この規格が注目されるようになってきている。過去に ISO 9000 が品質の管理マネジメントとして普及し、ISO 14000 が環境対策の管理マネジメントとして普及したように、これからは安全設計を実現することを目指して、IEC 61508 は徐々に普及していくと思われる。この規格の基本概念が「機能安全」という考え方であり、組込み系の安全設計を行う場合ベースとなる思想である。ただし、この規格は 400 頁近くあり、かつ難解な文章でもあることから、この規格を上位概念とした分野別・業種別の個別安全規格が発行されることによって、機能安全の考え方が普及していくのかもしれない。

1.2 安全に関する用語

1.2.1 安全に関する主な用語

安全に関しては、いろいろな誤解や社会通念の変化から、言葉の意味が業界によって、あるいは人によって異なっていることもしばしばである。安全に関する概念や用語を間違えていると、せっかく安全対策を行っても潜在リスクを残すことになりかねない。用語はいろいろな規格で定義されているが、ここでは、安全に関する事項を扱う場合の指針を規定している ISO/IEC Guide51（JIS Z 8051）（注 4）をベースに**表 1.1** に示す。

表 1.1　安全用語例

用語	概要
安全 (Safety)	**受容できないリスクがないこと。**
リスク (risk)	危害の発生確率及びその危害の程度の組合せ。
危害 (harm)	人の受ける身体的傷害若しくは健康傷害、又は財産若しくは環境の受ける害。
危険事象 (harmful event)	危険状態から結果として危害に至る出来事。
ハザード (hazard)	**危害の潜在的な源。**
	備考　ハザードという用語は、起こる可能性のある危害の発生源又は性質を定義するために用いることが一般的に認められている（例えば、感電、押しつぶし、切断、毒性によるもの、火災、おぼれなどのハザード）。
危険状態 (hazardous situation)	人、財産又は環境が、一つ又は複数のハザードにさらされる状況。
許容可能なリスク (tolerable risk)	社会における現時点での評価に基づいた状況下で受け入れられるリスク。
保護方策 (protective measure)	リスクを低減するための手段。
	備考　保護方策には、本質安全設計、保護装置、保護具、使用上及び据付け上の情報並びに訓練によるリスクの低減策を含む。
残留リスク (residual risk)	保護方策を講じた後にも残るリスク。

1.2.2　安全という概念

安全という言葉は多くの技術領域にまたがっており、あらゆる製品の規格で扱われていると考えられる。市場に提供される電気・電子製品の多くはソフトウェアが組込まれ、ますます高機能化・多様化しているが、利用者はソフトウェアが組込まれていることを意識することはほとんどない。「ユビキタス社会」という言葉があるが、便利に快適になるほど開発者は安全の視点に立った多様な設計配慮を求められることになる。

なお、「絶対に安全です」という言い方がよくある。「安全第一」という言い方も場合によっては誤解を生むことがある。実は、絶対的な安全というものはありえない。どんなに保護方策を講じてもある程度のリスクは必ず残る。その残ったリスク(残留リスク)が、利用者の価値観や社会通念に照らして許容可能なレベルまで低減されたと判断、または合意ができたときに、「相対的に」安全であるといえる。安全は、リスクを認識して始めて理解できるものである。

ISO/IEC Guide51（JIS Z 8051）では、安全という用語はリスクがないことを保証しているかのような誤解を与えるので、使用しないことが望ましいと明記している。例として、“安全ヘルメット”は“保護ヘルメット”と置き換えることを推奨している。

さらに品質は安全と同義語ではないので、品質の役割と安全の役割を混同しないことが望ましいとも述べている。

（相対的な）安全はリスクを許容可能なレベルまで低減させることで達成されるが、許容可能なリスクは安全という概念と、製品の利便性、目的適合性、費用対効果、社会の認識・慣習等、諸要件とのバランスで決まる。したがって、許容可能なレベルというのは、状況によって異なってくる。技術の進歩や社会通念の変化・進展に合わせて、経済性も考慮しつつリスクを最小化するような見直しが常に必要となる。

なお、本書では労働安全や食品安全の領域ではなく、電子機器に関する安全について議論していく。また、ヒューマンエラーと情報セキュリティの切り口での議論は他に譲る。

(1)　ハザードとリスク

人が何らかのリスク（危険、危害）にさらされるということは、危害をもたらす何かが存在するからであって、この何かをハザード（危険源）と言う（正確な定義は 1.2.1 参照）。システムが高度になるに従い、システム内の構造・特性をあまり認識することなく利用されているケースが多いが、このような状況ではシステムに内在するハザードも認識されにくい。安全設計を行うということは、リスク、つまり部品やシステムがもつ潜在的な危険性を明確にしてその対処策を講じるということになるが、リスクを明確にするためには、その製品に内在するハザードを特定しなければならない。

安全設計に着手するためには、ハザードの特定→リスクの見積・評価→リスク低減策決定というサイクルを回して、許容可能なレベルまでリスクを低減していく必要がある。このサイクルは、第 3 章を参照されたい。

ハザードの例としては、まず物理的な実体のあるものがあげられる。毒性のある薬品や化学物質、あるいは爆発の可能性のあるもの、可燃性物質、猛獣や病原菌などの生物もハザードである。事故を引き起こす可能性のある車、電車、エレベータ、エスカレータ、挟まれ事故を起こしかねないドア、溺死をもたらす大量の水も危険源である。

一方、例えば無理なジョギング、入浴時や起床時の卒倒など、人の行為が実体はないもののハザードである。その他、台風、落雷、地震などの自然現象や、不景気や集団パニックなどの社会現象もハザードになりうる。

つまり、ハザードはこの世界の至る所にあり、条件が整えばリスクとなる。ハザードが顕在化しない限り我々は意識しないので通常不安に陥ることはない。また顕在化しても、ハザードが遠方にあるか丈夫な物で隔離されていれば人はリスクを感じない。それは、リスクの発生確率が十分小さいと判断しているからである。また、ハザードが死にいたるようなものではなく運が悪くても小さな怪我で済むようなものなら、やはり人はリスクを感じない。それは、リスクが発生しても危害の程度が十分小さいと判断しているからである。このように、リスクは人の対応能力や価値観により、あるいは設置環境や社会環境によっても変わってくる。リスクは便宜上下記のような式で表現されるが、実際に起きる P と S の関係は単純な一次式ではない。

$$\text{リスク（R）} = \text{発生頻度（P）} \times \text{危害の程度（S）} \quad \Rightarrow \quad f(P,S)$$

リスクのイメージを**図 1.3** に示す。リスクは定量的なものであり、社会通念として無視しうるリスク（許容域のリスク）と社会通念として許されないリスク（非許容域のリスク）との間に、便益とのトレードオフとなる領域がある。それを ALARP（As low as reasonably practicable）領域という。機能安全の思想は、非許容域リスクと ALARP 領域のリスクを合理的に実行可能な範囲で、できるだけ低くしていき、許容域に押さえ込もうということである。機能安全の対策を実施した後も、残留リスクは存在していることに注意する必要がある。

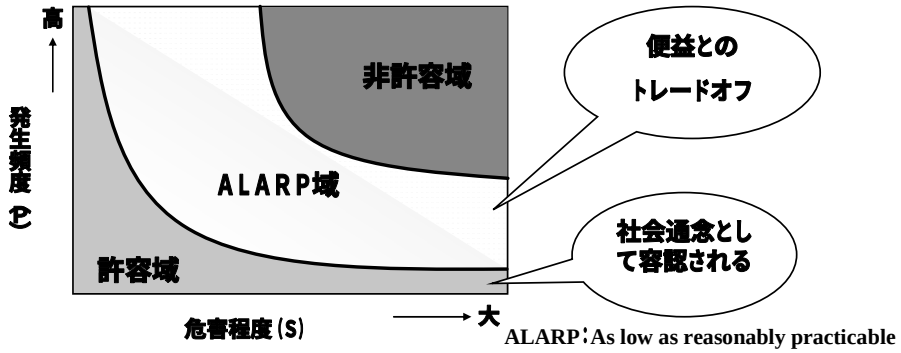


図 1.3　リスク

(2)　本質安全と機能安全

機能安全（functional safety）という言葉は、本質安全という言い方に対して相対的に安全を捉えようとして生まれてきた新しい用語であり、IEC 61508（JIS C 0508）で定義されている。

本質安全（inherent safety）は固有安全とも言い、システムの基本設計や運転特性に向けられた概念である。根源からリスクをなくして達成される安全のことである。それに対し、機能安全とは安全に寄与する保護システム（安全関連系など）や保護機能に向けられた概念で、（能動的に）付加された機能によって確保される安全のことである。

機能安全という概念は、先にも述べたが絶対安全はありえず相対的に安全であるに過ぎないという考え方から生じている。機能安全はリスクの評価を行い許容以下になるようにリスク軽減を実施するという考え方である。したがって、安全度合いを決めるための尺度がある。その尺度を安全度水準（SIL：Safety Integrity Level）という。

よく例に出されるのは立体交差と踏み切りの比較事例である（図 1.4 参照）。また隣家の耐火建築の家屋は一般に本質（的に）安全であるが、可燃性の木造家屋では本質安全とは言えない。しかし、そこに煙探知器を備えているとか、灯油やガスを使わない家であったら、隣家にとっては機能安全の水準が高いといえる。

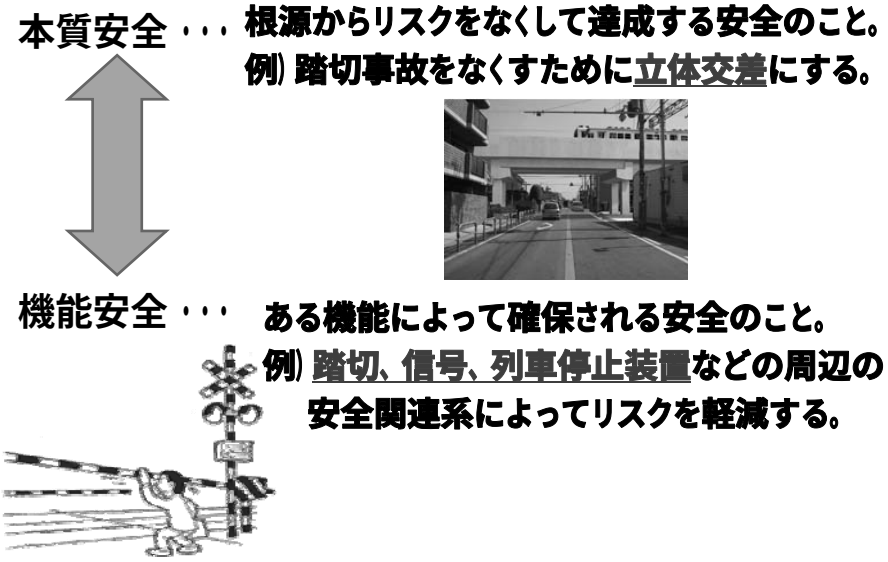


図 1.4　本質安全と機能安全

(3)　信頼性と安全性

ソフトウェアは機械や電気部品のような磨耗、経年劣化や故障がなく無体物なので、人や環境に直接的に危害を及ぼすとは考えにくい。そのためか、ソフトウェアの世界では、特に信頼性と安全性は混同されやすい。しかし基本的に異なる概念である。JIS Z 8115 信頼性用語では、信頼性と安全（性）を以下のように定義している。

・信頼性：（機器、設備などの）アイテムが与えられた条件のもとで、与えられた期間、要求機能を遂行できる能力。
・安全　：人への危害または資（機）材の損傷の危険性が、許容可能な水準に抑えられている状態。

つまり、信頼性とは製品寿命の期間内や使用条件の範囲内で要求された仕様をいかに満足しているかが問われているが、安全性は、製品寿命や仕様との適合性とは無関係に人（や環境）への危害がいかに低いかが問われている。言い換えれば、信頼性は、その製品の機能を実現する能力であるが、安全性は、その製品の機能とは無関係にリスクが低いことを示す概念である。

例えばよく故障する車があったとする。ただし、その故障が発進時によくエンストするようなものであれば、その車の信頼性は低いといえるが、安全性は低いわけではない。ま

た非常に稀であるが、あるタイミングになると急発進することがある車ならば、安全性に問題がある。つまり安全性の概念では、故障があっても危険側でなければ許容される。一方、信頼性の概念では、製品寿命期間内の故障発生率が設計目標以下であれば信頼性は確保されていることになる。そのときの故障が、安全側への故障か危険側への故障かは信頼性維持とは別の視点の問題になる。

安全性確保のためには信頼性の確保が必要条件であるが、信頼性と安全性は元々異なった概念である。

(4) ディペンダビリティとの関係

ディペンダビリティは、安全性とどのような関係にあるのだろうか。名古屋大学高田教授の解説を、**図 1.5** に示す。ディペンダビリティ（dependability）とは、広義の信頼性を指し、狭義の信頼性（reliability）、可用性（availability）、セキュリティ（security）、安全性（safety）を包含する概念であるとしている。元来の言葉は、「頼りがいのあること」を意味しており、システムがどの程度頼りになるものかを示す概念である。ただし、これらの用語は人によりコミュニティにより定義が異なるので注意が必要である。なお、情報セキュリティに関しては前年度報告書に詳細を述べているので、参照されたい（注 5）。

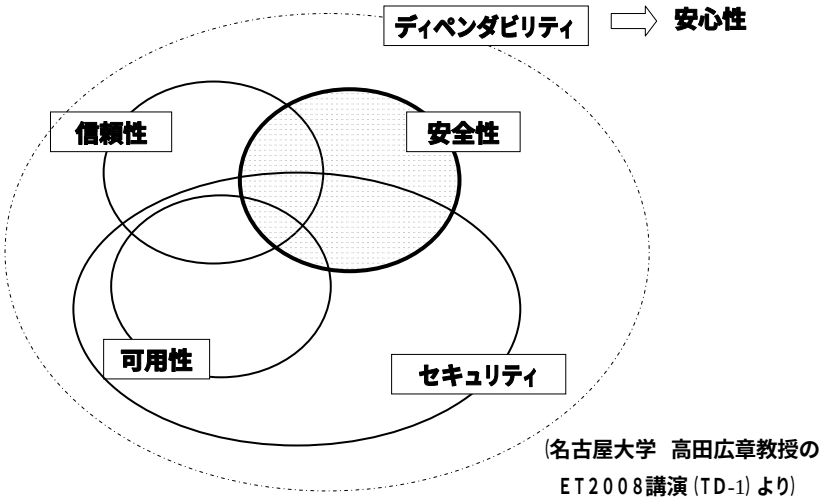


図 1.5　安全性にかかわる概念例

(5) 安全関連系

安全関連系（SRS：Safety Related System、安全関連システム）とは、制御の対象となる機器（EUC：Equipment Under Control）を安全な状態に移行、または維持するために必要な安全機能（safety function）を実行するサブシステムのことである。システム全体に要求される安全機能を実現するために、各安全関連系には、それぞれに必要な安全度水準（SIL）が割り当てられる。システムにおける安全関連系の位置付けを図 1.6 に示す。機能安全を実際に実現しようとするなら、ほとんどの場合この安全関連系の要求仕様を定め、設計することをいう。詳細は第 4 章以降を参照方。

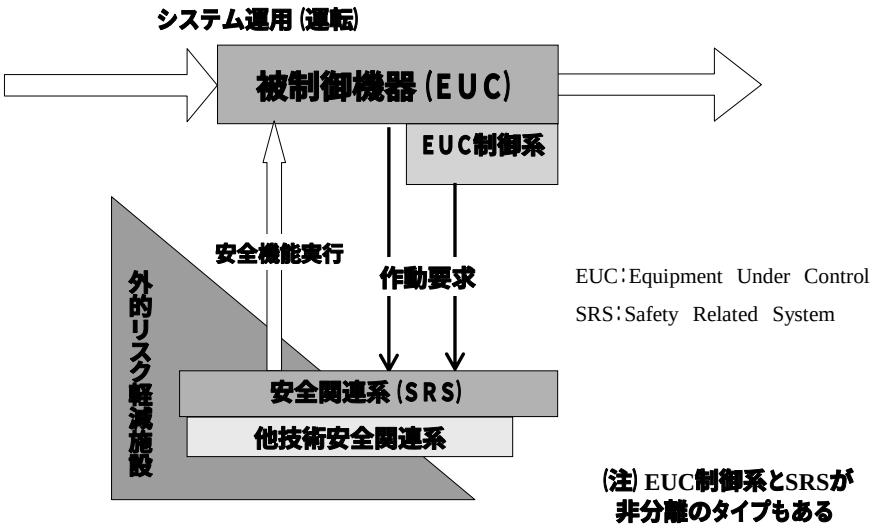


図 1.6　安全関連系

コラム1:セーフティとセキュリティ

「セーフティ」も「セキュリティ」も、日本語にすればともに「安全」と訳される。しかしながら、両者には微妙な使い分けが存在する。例えば、情報セキュリティとは言うが、情報セーフティとは言わない。それから、セーフティ・ネットとは言うが、セキュリティ・ネットとは言わない。

では、これらの違いはどこからくるのであろうか？手元の辞書には、以下の記載がある。まず、safe については、“Something that is safe does not cause physical harm or danger.”とある。また、secure については、“If you secure a place, make it safe from harm or attack.”とある。つまり、一部意味の重なりもあるようだが、セーフティとは危害を及ぼさないという性質のことであり、セキュアとは危害を及ぼされないという性質のことと解釈できる。

このことはソフトウェアの場合にも、同様に理解することができるだろう。つまり、ソフトウェアの不具合に起因して、衝突や爆発といった外界への危害が発生しないことが、ソフトウェア・セーフティであるし、逆に、外界から及ぶ改ざん等の危害からソフトウェアが保護されていることがソフトウエア・セキュリティである。

マルチタスクシステムや分散ネットワークシステムにおいては、あるタスクやノードの不具合が、システム全体の故障を引き起こさないようにしなければならない。そのためにはまず、一つのタスクやノードが、不慮の暴走やメモリアクセス等によって、他のタスクやノードに危害を及ぼさないことが求められる。さらには、そうした他者から及ぶ可能性のある危害から、タスクやノードが保護されていることも求められる。そこでは、セーフティとセキュリティが同居していると考えることができるだろう。

MI（水口 大知）

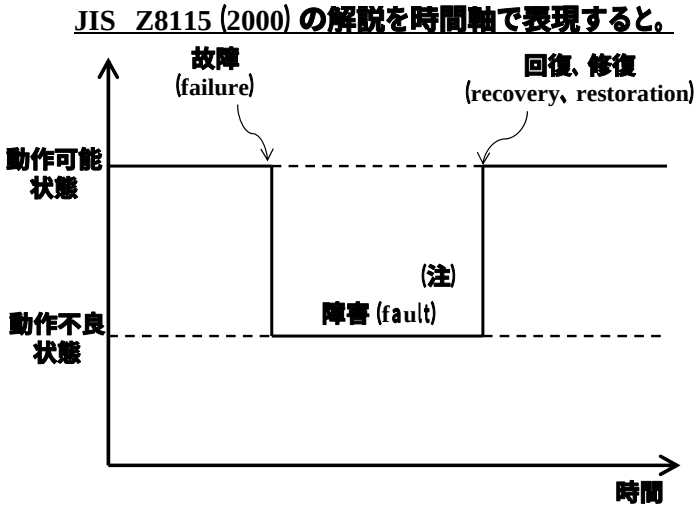
1.3 障害と故障

安全設計を実施する場合、特に重要になるのがシステム障害であり、どのような障害がありうるかを想定し、その予想される原因を分析しておくことは重要である。また、システム内の欠陥からどのような事故に至るのかを分析しておくことも必要となる。その際、障害と故障について明確に分離した定義をしておかないと混乱の元になりかねない。ところが、品質管理の現場では、故障、障害、不具合、不適合、エラーなどについて、定義を明確にして使い分けている例は少ないようである。業界やコミュニティによって言葉の使い分けが違っていることもある。規格によっても、障害と故障、あるいは fault と failure の使い方が異なっている(*2)ので、本書では以下のように定義しておく。

1.3.1 障害と故障の関係

東証のシステムに問題が発生した時、マスコミはシステム障害と表現しており、障害は実際に外部に現れたトラブルの状態を指していると思われる。また、システムに異常が発生したとき、その原因がメーカーが納入した機器やソフトウェアにあった場合、故障、不具合、あるいは欠陥という言い方をするが、原因が、操作ミスや火事などの災害や犯罪行為であった場合には、システムの故障、あるいはシステムの欠陥が発生したとはあまり言わない。そこで、本書では、「障害」は不具合・不適合と同義語と見なし、障害と故障の関係を図 1.7 に、障害の要因を図 1.8 に示す。

安全設計にあたっては、FMEA や FTA などの分析を行って障害の要因を洗い出し、対策を講じるわけであるが、システム障害に至る要因はソフトウェアの欠陥やハードウェアの故障だけではないことに注意する必要がある。



(注 : JIS Z8115 は「障害」とは言わず「フォールト」と言っている)

図 1.7 障害と故障

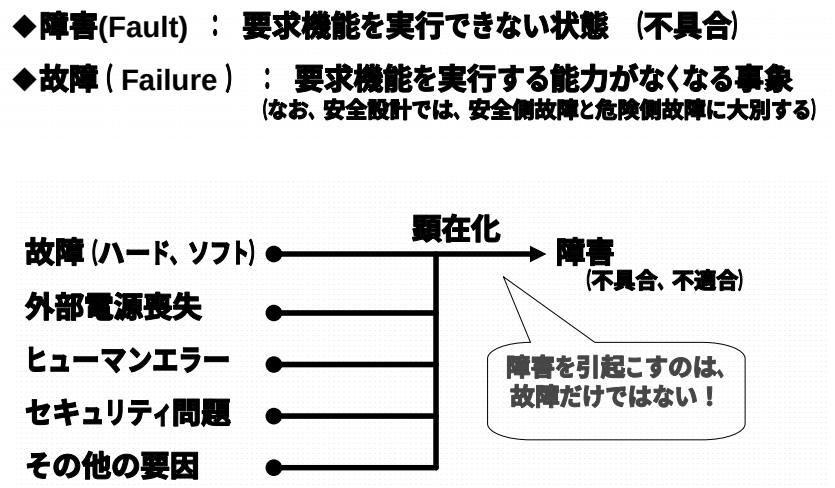


図 1.8　障害の要因

システムに何らかの障害（fault）が発生した場合、考えられる原因として第一に、構成要素の欠陥すなわち故障（failure）があげられる。

メモリを例にすると、欠陥があっても ECC（Error Correcting Code）機能が付加されていた場合、1 ビットのエラーは修復可能であり、その場合エラーがあっても故障ではない。2 ビット以上のエラーが起きると故障となる。ECC の代わりにパリティビットが付加されている場合、1 ビットのエラーは、即、故障となる。しかし、検出可能な故障なので、システムは一旦、障害を起こすが、再起動機能や異常部分を隔離する機能があらかじめ備わっていれば、ある時間後に自動復旧し障害はなくなっていく。パリティビットもない場合は原因不明の故障となり、原因を除去することが難しくなる。システムは障害に至った後、復旧に時間がかかるかもしれない。

システム障害の発生原因には、他に外部電源などエネルギー源の喪失や、操作ミスなどヒューマンエラー、ハッカーなどセキュリティ問題の発生などが考えられる。その他には、システムの能力を超える過大なアクセス、設計想定値を超える外部ノイズ、地震・洪水等の自然災害、火災、人為災害、改造・修理時の作業ミスなどが、システム障害の原因として考えられる。これらの障害や故障の中に安全性を脅かす問題が隠れている。

実際のシステムは、多くのモジュールや部材から構成されており階層構成をなしている。したがって、故障・障害の関係も階層構造をもつことになる（図 1.9 参照）。

製品開発の現場では狭義の信頼性確保は故障対策になるだろうが、広く信頼性確保というとヒューマンエラー対策や情報セキュリティ対策が含まれる。しかし、それだけでは安全確保には不十分なことが多い。FMEA（Failure Mode and Effect Analysis）等の手法を

用いて、考えられるすべての障害またはリスクをリストアップしてその要因を洗い出す必要がある。

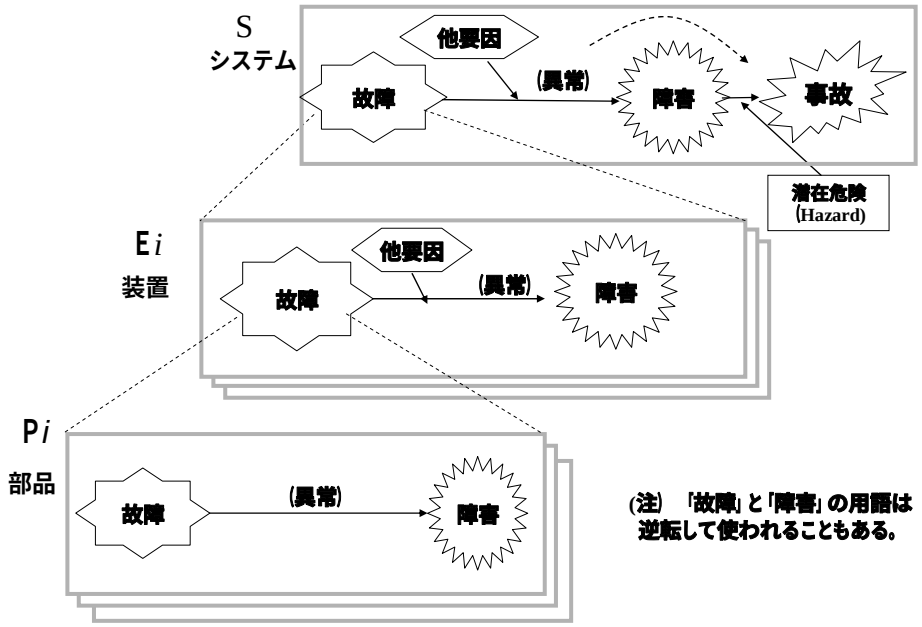


図 1.9　障害・故障の階層構造

(1)　安全側故障と危険側故障

故障発生時、故障のモードが複数ありうるが、安全側の故障モードになる確率が危険側の故障モードになる確率よりも著しく高い特性を非対称誤り特性という。故障が発生しても非対称誤り特性をもつ部品であれば、それを前提にシステムを設計することによりシステムの障害も安全側（になる確率が高い）にすることが可能となる。このように、故障が発生しても事故には至らないように設計するのがフェールセーフ設計である。

(2)　システム故障と部分故障

ある部分の故障がシステム全体に波及する場合と、部分限定で収まる場合とがある。開発にあたっては、できるだけ他に波及しないように設計すべきであるが、全体設計の時点では、システムダウンに至る故障と部分故障に至る故障は分類しておくことが望ましい。故障によっては積極的にシステムダウンさせるべきものと、逆に大きな故障でもシステムをできるだけ維持すべきものがあるはずである。故障や障害は与えられたものではなく、設計者の意思によっても定義できるものと考えた方がいい。

1.3.2　ハードウェアの故障とソフトウェアの故障

ハードウェアは全く同じ仕様で製作されても、品質にある程度のばらつきが避けられない。製造環境、動作時の周囲環境、利用頻度等、さまざまな影響により多様なメカニズムのもとで磨耗劣化する。性能がドリフトすることもある。ハードウェア故障の発生については、**図 1.10** 故障率曲線（バスタブカーブ）に示すように、初期故障期、偶発故障期、磨耗故障期と三つに分けられるといわれている。製品寿命の中で最も長い偶発故障期は、時間的に無秩序なランダム故障期であるとされている。

それに対して、ソフトウェアは基本的に磨耗劣化することはない（*3）。時間に関係なくランダムなエラーが発生することもない。従って、ソフトウェアの故障または障害については、設計・製造時の不具合や実行環境とのミスマッチが原因であり、決定論的原因故障（systematic failure）とされている。条件が整えば再現されうる故障である。

ソフトウェアとハードウェアでは故障の性格が異なるので、ソフトウェアに対しては従来のランダム故障に対するものとは別な対策の枠組みが必要になる。機能安全の考え方でもソフトウェアに対する安全要求事項が異なっている。

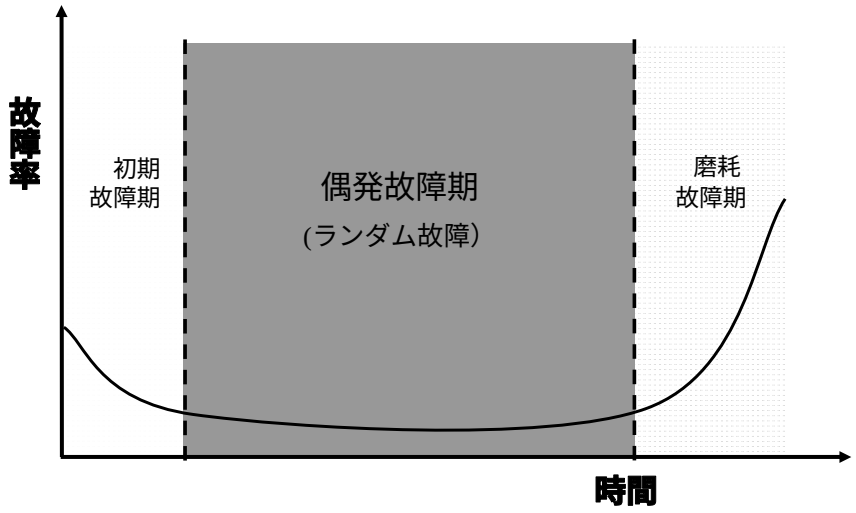


図 1.10　故障率曲線

(1) ソフトウェア障害発生に関する課題

電気・機械部品は一定の品質基準をクリアしたら出荷されるが、ソフトウェアは図 1.11 に示すように、一般的には計画したテストをすべて実施した後に、バグの新たな発見がなくなりすべてのバグに対策がうたれれば出荷している（はずである）。しかし、これはバグが発見されにくくなっただけで、ゼロになったということを意味するものではない。潜在的な欠陥は、潜在バグも含めて残っている可能性がある。

ソフトウェア開発は、品質管理プロセスの面でも多くの課題を抱えている。ソフトウェアは経年劣化せずランダム故障もないというメリットがある反面、一定の品質をクリアしているということを証明するのは、たいへん難しい。ハードウェアのような故障率を推定することは一般には困難である。ただしソフトウェアの故障率を定量的に推定可能という主張もある（注 6）。

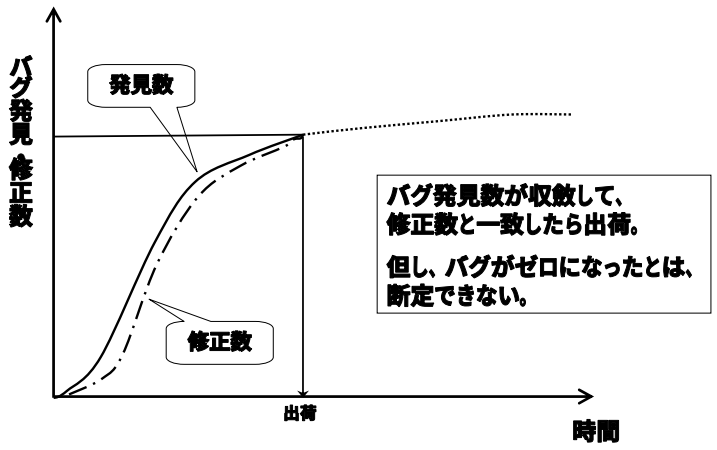


図 1.11　プログラムバグ曲線

システムの信頼性を高めるために、ハードウェアは、しばしば多重・冗長化するが、これはランダム故障特性を前提にしているからできることである（同時に故障することは確率的に極めて稀）。それに対してソフトウェアは、多重化してもエラーがあれば全く同じタイミングと状況のもとで障害が現れることになるので、単純な多重・冗長化は、ほとんど無意味である。

さらに、ソフトウェアは、開発過程でうまくいけば試作状態のプログラムがそのまま最終製品になることもしばしばである。ハードウェアは、試作品と製品を峻別しているが、ソフトウェアは、その本質があまり理解されていないためか、あるいは開発コストの節減や工程圧迫に晒されるためか（ソフトウェアは、しばしば製品開発のしんがりになる）、

構造的にしっかりしたものになっていないケースが大半のようである。品質にかかわる者であれば、ジャンパ線だらけのボードは試作品とは思っても、製品とは思わないだろう。にもかかわらず、ソフトウェアについては、スパゲティプログラムであっても、機能さえしていれば製品と見なしてしまうプロジェクトが多いのではないだろうか。

技術者配置についても、ハードウェアは、開発・製品化設計・製造・調達・試験と担当者が異なってくるが、ソフトウェアでは、開発から試験まで一人の技術者が担当することはよくある。工業製品の観点から見ればソフトウェアの管理方法は、改善すべきことが多い。

1.4 安全を設計するためには

これまで述べてきたように、安全を設計しようとするならリスクを明確にする必要がある。JIS Z 8051（ISO/IEC Guide51）では、リスク低減の方策としてリスクアセスメントを提示している。なお、リスクアセスメントを実施しても、そこに参加したメンバーだけで全てのリスクを抽出できるとは限らない。さらに低減策を立案するにしてもベストのプランを揃えることは難しい。従って、過去の先例に習うことは非常に重要である。できるだけ多くの安全に関する規格を参照すべきであるし、社内のトラブル事例やオープンされている失敗事例を参考にすべきである。以下、リスクアセスメントの概要、主なリスク分析手法、主な設計手法を簡単に述べる。詳細は後述の各章を参照されたい。

1.4.1 リスクアセスメント

リスクを許容可能なレベルまで低減するためのステップを図 1.12 に示す。

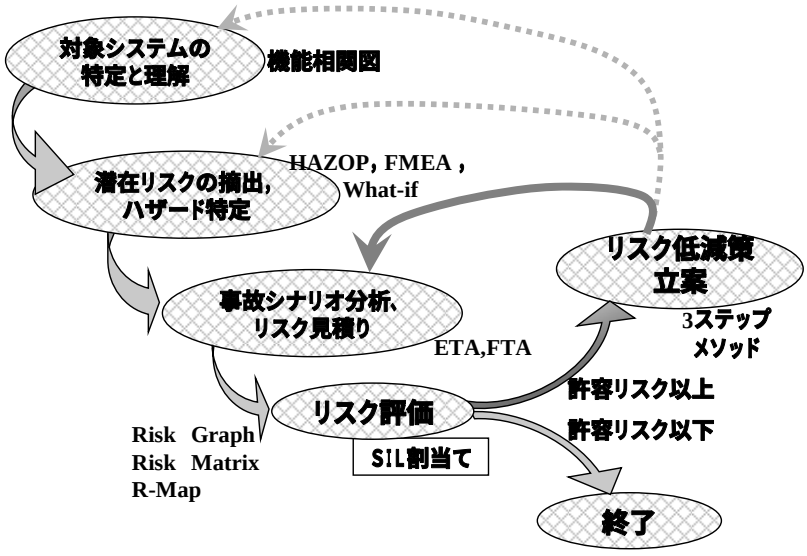


図 1.12　リスク評価の進め方

最初にシステムの目的、必要性、機能、構造･構成、利用期間、利用場所を明確にし、想定される使用者と接触者（子供、見学者など）を特定する。その場面で、想定される使用（意図される使用）を特定し、予想される誤使用例（合理的に予見可能な誤使用）を推定する。

次に、製品の全ライフサイクルの各段階で、あらゆる条件下で発生しうる各ハザードを特定する。

次に、ハザードが引起こすリスクを推定する。大規模な設備であれば事故シナリオを分析することになる。次にそれぞれのリスクについて、発生頻度、危害の程度を予想してリスクの程度を評価する。各リスクが許容可能かどうかを判断して許容可能でなければリスク低減策を立案し低減可能なレベルまで以上のサイクルを繰り返す。

リスク分析、評価に関する技法については、多々あるが、**表 1.2** に、主なものをリストアップする。詳しくは第 3 章を参照方。

表 1.2　主なリスクアセスメント関連技法

技法	概要
What-if	非体系的なブレインストーミング手法であり、手順として、悪い事態を仮定し、それによって起きる事故とその安全防御を考察する。
FMEA Failure Mode and Effect Analysis	製品および製造プロセスについて故障モードによる影響を分析して製品やプロセスの問題を解決する手法である。製品が使用される段階で起こりうる欠陥や異常な状態などを分析する。
HAZOP Hazard and Operability Study	通常状態からのズレ（設定の温度や濃度）が発生した場合にその原因と発生する結果の事象を特定する。
FTA Fault Tree Analysis	システムの特定故障を想定して、その発生原因を上位レベルから下位レベルまで論理的に展開し、最下位レベルのシステムの機能の故障発生率からシステムの特定故障の発生原因や発生確率を求める方法である。
ETA Event Tree Analysis	ある初期事象からスタートして、いろいろな経路をとることにより結果がどうなるかを明らかにする手法である。
Risk Graph	ツリー形式で示される方法で、想定される危害のひどさ、危険源／危険事象／危険状態にふらされる頻度、回避の可能性などがリスクパラメータとなる。
Risk Matrix	危害の発生頻度と危害のひどさを定性的に見積る手法である。それぞれの要素の分類は４分類する場合や６分類する場合など任意である。
R-Map	ルービックキューブの一面に似た、縦横３０の小間に、プロットした各々危害情報の安全度を表示する。それにより対象製品を客観的な視点、使用者の視点からデザインして見せる製品安全のツールである。(財）日科技連が推進している。

1.4.2　リスク低減の戦略と技法

リスクが明らかになったところで、関連規格や事例を参考に、リスクの低減方策を打ち立てていくことになるが、基本的な考え方と、設計のヒントになる主な手法を概説する。

(1)　3 ステップメソッド

設計段階で、リスク低減を策定する際の優先順位は、次の 3 ステップメソッドによる。詳しくは、第 4 章を参照方。

1．本質安全施策・設計
2．安全防護施策・設計（保護装置の設計、安全関連系の設計）
3．安全上の情報発信（警報、マニュアルなど）

上記のリスク低減策を講じても、なお製品完成後のリスクは残る。使用段階で、さらにリスクを低減するためには、(a）追加保護装置の設置、(b）訓練、(c）保護具の装着、（d）安全管理の体制　などを検討する必要がある。ただし、使用段階の改善策を設計段階でのリスク低減策の代替にしてはいけない。

(2)　安全規格が要求する設計技法

制御システムに関する代表的な規格としては、下記がある。

1．制御システムの安全関連規格　ISO 13849-1 （JIS B 9705-1）
2．機械の電気装置　IEC 60204-1 （JIS B 9960-1）
3．機能安全規格　IEC 61508 （JIS C 0508）

IEC 61508 では、リスクの程度に応じて安全度水準を決め、その安全度水準に応じた設計技法を推奨している。ソフトウェアの設計技法については､100 項目ほど提示している。詳細は**第 6 章**を参照方。

(3)　設計のための一般的戦略

基本的な戦略をあげると、以下がある。

●フォールトアボイダンス、フォールトレジスタンス

障害を回避する、あるいは、障害に対する抵抗力を高める構造・仕組みを考える。

●フォールトトレランス

障害が発現しても､リスクが低くなるような許容性を持たせたる構造・仕組みを考える。

●フォールトディテクション

障害発生時に的確な安全機能の実行ができ、障害発生後も確実に最低限の安全確保と迅速な事故対策、復旧対応ができるように、フォールトの検出・診断の仕組み・機能を考える。

●深層防護、多重防護

特に潜在リスクの大きいシステムでは、リスク軽減施設や安全関連系などのバリアーを複数用意することになるが、3 層構造で、安全方策を考える。まず、異常状態を未然に「発生防止」することである。それが破られたときは、システム全体に波及しないようにする「拡大抑制」を考える。それも破られたときに備え、影響を最小限に留めるような「影響緩和」を考える。バリアーを単に複数用意することではなく、各層毎に他の層をあてにせず、異なった独立の思想で設計するという考え方である。

(4) 主な安全設計技法

IEC 61508 （JIS C 0508）には、多くの設計技法が掲示されているが、製造現場でよく使われていると思われるものを**表 1.3** にリストアップする。

表 1.3 主な安全設計技法

技法	概要
ゼロメカニカルステート（ＺＭＳ）設計	製品が保有している種々のエネルギーがすべてゼロになった**時、**安全性が最も高くなるという考え方を基本とした設計
フェールセーフ設計	故障が発生しても安全側になるよう配慮した設計
フールプルーフ設計	人の不適切な行為、過失があっても安全性が損なわれないように配慮した設計。チャイルドプルーフ、タンパープルーフ、ミステルーフ等も考え方は同じ。
ツーハンドコントロール	両手で同時に操作をしなければ、装置が動作しないように配慮した設計。安易な操作を避ける。
冗長設計	システムの構成要素や機能の実現手段を複数用意し、一部に故障が発生しても上位系の障害に至らないよう配慮した設計。
ディレーティング	部品に加わるストレスを軽減するために、定格値を下回る値で使用すること。
防御的プログラミング	不正な入力があっても、あるいは、実行環境に異常があっても、極力被害を被らないようにしたプログラム作成法

(5) 停止の概念

機械の運転制御や電気機器の制御を行う場合、異常発生時の対策として非常停止を設計に織り込んでおくケースが多い。ただし、中には非常停止を設けてもリスクが低減しない場合もあるので、注意が必要である。

「停止」には、非常停止を含めていろいろなケースがある。設計に当っては、自己診断機能・監視や制御アルゴリズムのバックグラウンド条件として、密接に関係してくるので、停止ケースをできるだけ明確に分類・定義しておくことが望ましい。以下、筆者が考えるケースを紹介する。

a.通常停止　：
運転状態における機能を終了した停止。手動停止と自動（終了）停止がある。
次の起動が手動で（利用者の許可がある状況で）開始することができる状態。

b.保安停止　：
関連する周囲機器からシステム的に切り離した状態での停止。運転用の動力源からも一般には切り離される。一般的には通常停止状態からのみ移行可能とする。保安停止状態からは、通常停止にのみ移行可能とする。

c.非常停止　：
インターロック系の動作または手動により、運転時の機能が未完了であっても人間の安全を損なわない状態で、緊急に運転を止める。非常停止は自己保持され、この状態の解除は、要因の除去と手動リセット操作に寄る。その後は通常停止状態となる（詳しくは 4.2.2 参照）。

d.制御停止　：
動力が供給されており、いつでも運転状態に移行できる状態での一時停止。外見は停止でも、制御上は運転状態であり「待機運転」でもある。

e.非制御停止：
動力源を遮断することによる停止。非常停止と同じ分類になると設計上はわかりやすいが、システムによっては、非常停止とは別扱いになるかもしれない。

f.故障停止：
システム内に異常が発生して、制御できなくなり結果として停止に至る場合。
非常停止と同じ分類になれば、設計上わかりやすい。

システム機能によっては、上記とは異なる定義も当然ありうるし、各状態間の遷移条件もいろいろありうる。上記の分類はあくまで参考である。

1.4.3　リスク低減の実践的対処法

実際の設計現場では、多くの場合、改良開発である。革新的新商品でも、あらゆる部分が新しいという新商品であっても、機能構成を分析すると、かなりの部分は既存の部材を利用していたり、他のモジュールを応用していたりしているものである。安全な製品を開発する場合は特に、できるだけ保守的になって実績を重視することは、重要な開発戦略である。

しかし、少しでも新規の開発が発生するなら、その新規部分を含めて、関連する部分全体をできるだけ広くシステム分析して、リスクを明確にするべきである。その後、各々のリスクに対して低減策を立てることになるが、全く新しい対策の場合は、その対策自体にリスクを抱えることになる。したがって、リスク低減策も実績に習うことは非常に重要である。それでも、新たな対策を必要とするケースが発生するので、その新規対策に、可能な限りのリソースを集中投資するのが望ましい。以下、対策を実施せざるを得ない場合の対処案を述べる。

(1)　安全認証取得製品の採用

システムの機能分析を行い、リスクと防護方策が決まったら、EUC と EUC 制御系、SRS に分ける。SRS が定義できたら、既に安全認証を取得した製品を組み入れて、SRS を構築すれば設計は格段に楽になる。少なくとも、SRS のハードウェアに SIL3 を取得した安全シーケンサを利用して、ソフトウェアを半形式手法で作成したら、安全性を実証する範囲は、大きく狭まることになる。第 8 章に SIL3 取得製品の調査結果を提示しているので参照してほしい。

(2)　制御用計算機の事例に学ぶ

1960 年代末から、1980 年代前半にかけて、制御用計算機システム（プロセスコンピューター：略称プロコン）が、盛んに各種産業分野で活躍した。たいへん高価であったが、プラントや工場設備の自動化・省力化に効果を発揮した。その後、マイクロプロセッサや PC に押されて姿を消したが、当時のハードウェアは、たいへん限られたリソース（例えば主メモリ 64KB と非常に小さかった）しかなく、しかも安定した品質をまだ確保できない状況であった。OS やコンパイラの能力も高くなかった。

それでも自動化のニーズは高かったので、年に何度かダウンする計算機であっても導入は進んだ。そのため、当時のプロコンは、故障が（必ず）起きるということを前提に、安全性確保、短時間復旧（MTTR の最小化）に開発の重点がおかれた。

プロコンが実施してきた安全対策は、巨大プラントの自動化への挑戦というビッグプロジェクトの中から生まれてきたものであり、20 年の実績もあって、今でも通用する方策が多々用いられていると思われる。

プロコンが実施してきた安全性・信頼性確保のための対策を参考にすることは、安全方策立案の近道になると思う。以下にプロコンの安全対策例を簡単にいくつか示す。

ａ．自動再起動機能の設置

CPU が異常を検出したときに、途中処理のタスクが、CPU 復旧後直ちに処理を続行できるよう最低限の情報を保存退避させ、その後、積極的にダウン・再起動をする機能。この保存退避機能は、パソコンのレジューム機能にあたる。

ｂ．実行環境への依存度をミニマム化

リアルタイム制御を担当するプログラムは、OS へのシステムコールをできるだけ行わずに単独実行するように設計する。OS への依存度を減らすことで、実行速度の確保と CPU 動作がランダムな動きになることを避ける。また、コンピュータの構成要素の中で最も故障しやすいのは、可動部をもつディスクとプリンタであるが、ディスクはシステム全体に影響を与えかねない。そのためディスクを必要とする一般の OS を用いる場合は、プログラムを主メモリに常駐化させ、ロールアウト・ロールインの他、ファイルのアクセスをしないよう設計するなど、リソースの利用範囲を極力限定する。利用する場合も時間的にランダムな動きにならないようにする。これは、トラブル発生時の原因絞り込みにも有効である。

ｃ．入力信号の信頼性確保

センサ信号一点毎に、故障状態、有効域逸脱状態、警報状態、正常状態など、5～8 の状態定義を行い、健全に使える状態を絞り込んでおく。こうすることで、センサ故障への対応処理が容易になり、センサ異常時の処理も明確になってくる。

ｄ．制御系の半形式手法表記

制御ロジックは、テーブル穴埋め表記など、DSL（Domain Specific Language）化して、基本的にすべての論理組合せを検証できるようにしておく。この方法は、図書と実行ベースのソフトを一致させることができ、検証・確認も容易になる。きめ細かい変更管理やロジックの再利用も可能になる。

ｅ．ダイバーシティの確保

共通故障モードによるシステムダウンを回避するために、電源系をお互いに異なった 2 系統にしたり、重要入力はアナログ信号とパルス信号の 2 タイプ用意したりというように、設計に多様性をもたせている。

フィードバック制御やプラントの性能計算など、計算アルゴリズムについては、半形式手法などの論理表現が難しい。しかも一般に専門性が高く、試験も設計から独立して行うことは難しい。このようなソフトウェアについては、アルゴリズム設計後のプラグラム作成段階から、2 チームが並行して独立に設計条件を相互に変えた形で開発させる。こうして開発された二つのソフトウェアは、同じ入力の組合せ（入力セット）に対しては、プラグラムの内部構造が異なっても、全く

同じ出力となるはずである。入力セットを何とおりも用意して、比較検証していけば、潜在バグもあぶりだされてくる。

(3) 失敗事例に学ぶ

安全に関する教訓を生み出したトラブルのほとんどが予想外のイベントや複数の障害・欠陥によって引起こされている。人は未経験のことを想像することが難しい。したがって開発設計においても、将来発生しうるリスクを事前に予測することは、非常に難しい。

そこで、過去の失敗事例に学ぶことが非常に有益になる。前述の畑村委員会による失敗知識データベース（注 1）は、その点で、たいへん参考となるものである。安全を考えるセンスを磨くためにも有用である。社内の過去のトラブル事例も更に参考になるだろう。類似システムのトラブル事例は、特に教訓として参考になる。一つのトラブルには、必ず三つ以上の改善策があるはずである。

1.5 本章のまとめ

本章では、以下の事項について概説した。

1）過去の事故事例から主にソフトウェアに関する事例を紹介。
2）ソフトウェアの安全性についての課題と動向を紹介。
3）安全に関する用語と概念について説明。
4）障害と故障について説明。
5）ハードウェア故障とソフトウェア故障の特徴を説明。
6）ソフトウェアの課題を概説。
7）安全設計の基本的な手順の紹介。
8）リスク低減の基本的な技法の紹介。
9）リスク低減のセンスを磨きかつ、即効的な対処法を説明。

以上、組込み系の安全設計に関する基本と思われる事柄を述べた。以降の章では、機能安全を中心に、規格の内容や設計手法について、解説していく。

＊＊＊＊＊＊　**第１章注記**　＊＊＊＊＊＊＊

（*1） ハインリッヒの法則 は、労働災害における経験則の一つ。一つの重大事故の背後は 29 の軽微な事故があり、その背景には 300 の異常が存在するというもの。

（*2） 障害と故障については、JIS Z 8115、JIS X 0014、JIS B 9700-1 を参照方。

（*3） ただし、バージョンアップせずに、長く利用すれば、CPU や OS、使用側の事情など、さまざまな実行環境の変化により、機能・性能ギャップが大きくなり、「磨耗劣化」はしないが、「陳腐化」は、進行する。

参考文献（第 1 章）

注 1） 科学技術振興機構（JST）失敗知識データベース推進委員会（JST 畑村委員会）
http://shippai.jst.go.jp/fkd/Search

注 2） 情報処理推進機構（IPA） 「組込みシステムの安全性向上の勧め」（機能安全編）2006 年 11 月

注 3） IEC 61508：1998 （JIS C 0508 : 1999） 電気・電子・ﾌﾟﾛｸﾞﾗﾏﾌﾞﾙ電子安全関連系の機能安全

注 4） ISO/IEC Guide51 ：1999 （JIS Z 8051 : 2004） 安全側面－規格への導入指針

注 5） 組込みシステム技術協会（JASA） 平成 19 年度組込みシステムにおける機能安全に関する調査研究～ネット社会における組込みシステム、二つの課題「情報セキュリティ」と「機能安全」～ 平成 20 年 3 月発行

注 6） 山田茂、藤原隆次；ソフトウェアの信頼性：モデル、ツール、マネジメント
プロジェクトマネジメント学会 2004 年 11 月

第2章　安全規格体系と概要

本章では安全規格の全体的な関係と、機能安全に関係するいくつかの安全規格の概要について述べる。

ISO などの国際規格は、そのカバー領域はかつては部分的であった。しかし最近は産業のあらゆる分野の標準化をはかり、無視できない存在になってきている。経済のグローバル化もまた国際規格の普及を促進する要因である。そのことは、いうを待たない。

本章では物づくりの中でも安全にかかわる規格に関して、いくつかの規格を取り上げ、その規格の特徴的な点を紹介し、安全規格の認識を高めることを目的とする。

2.1 節では、各国の安全規格と機構について概観する。国際安全規格が生まれた背景もうかがうことができる。

2.2 節では、ISO/IEC Guide51 について述べる。安全規格の中でこの規格の役割が述べられる。

2.3 節では、いくつかの国際規格の安全方策について述べる。ISO 12100、ISO 13849、IEC 60204、IEC 61508。

ISO 12100 は安全一般に関する基本概念や設計原則をのべた規格である。

ISO 13849 は機械の制御システムの安全関連部に関する規格である。

IEC 60204 は電気装置に関する安全規格である。

IEC 61508 は、電気・電子・プログラマブル電子の安全関連系を対象とする安全規格である。

これらの安全規格について、それぞれのリスクからの保護方策を説明する。リスクアセスメントなどリスク低減の方法などが語られる。またソフトウェアに関する安全についても、IEC 61508 にて語られる。

2.4 節では、国際安全規格を組込み系技術者や事業者がどう捉えるべきかの課題について若干ふれる。

2.1 各国の安全規格と機構

この節では ISO やその他の国際規格や機構の概略について説明する。

国際安全規格は欧州中心の規格であるが、欧州以外の地域にも同様な規格が存在する。国際安全規格とそれ以外の主要な地域の規格の関連につき図 2.1 にまとめる。

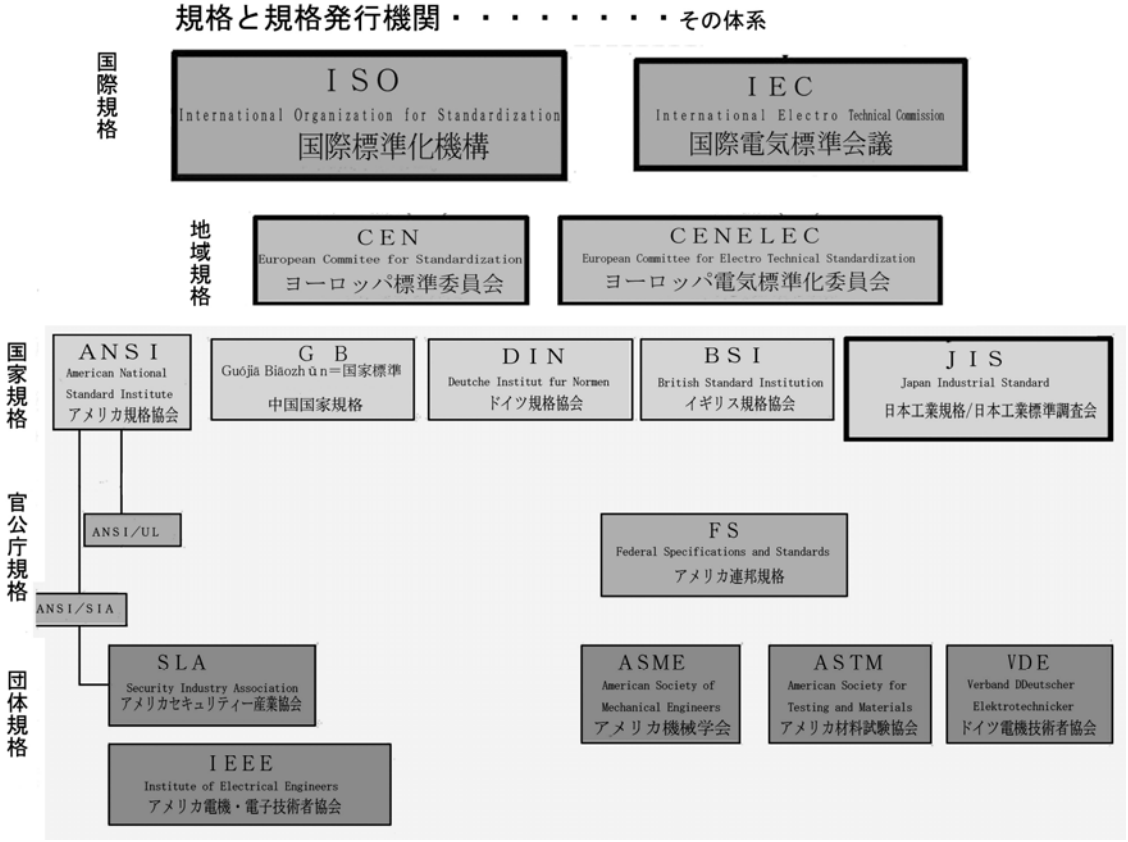


図 2.1　規格と規格発行機関

次に各規格発行機関の概要について説明する。

ISO　International Organization for　Standardization（国際標準化機構）

ISO は、サービスの国際交換を容易にし、知的、科学的、技術的及び経済的活動分野の協力を助長させるために、世界的な標準化及びその関連活動の発展を図ることを目的に、1947 年に発足した。非政府組織ではあるが、国連とその関連機関における諮問委員会的組織であり、通常の民間組織とは全く異なるオーソライズを有する。その会員数は、設立翌年は 25 カ国であったが、その後増加の一途をたどり現在では 100 カ国を超えている。加入

は各国の代表的標準化機関一つに限られている。

組織構造は、総会の下に評議会があり、全体の活動を監督している。国際標準化は評議会の下部機構である技術管理評議会が管理。活動範囲は、IEC の担当する電気・電子技術規格以外の分野の、すべての標準化を推進する。日本からは JIS の調査・審議を行っている JISC（日本工業標準調査会）が 1952 年から加盟している。

CEN　European Committee for Standardization（Comité Européen de Normalisation）（ヨーロッパ標準化委員会）

1961 年にヨーロッパ 18 カ国の標準化機関が参加して設立された地域標準化機関。現在のメンバーは 30 カ国であるが今後 EU に加盟を計画している複数の国が準会員となっている。EN（ヨーロッパ統一規格）は CEN のメンバー投票によって過半数の賛成によって決定され、規格は EN 規格として参加国に採用される。

CEN は ISO と密接に協調して業務を遂行している。規格制定当初の最大の目的は地域内の商品の安全を確保し、流通を円滑にすることにあった。欧州以外の国にも規格を広げる政策をとり、成立の経緯から ISO の骨格をなす。

また 1997 年からは JISC-CEN の定期協議が開催されており日欧の標準化に関する情報交換が行われている。

IEC　International Electrotechnical Commission（国際電気標準会議）

1904 年、アメリカのセントルイスにおいて開催された国際電気大会で批准され 1906 年に設立。中央事務局はスイスジュネーブに設置され、会員は準会員を含み 50 カ国以上。対象は電子、磁気、電磁気、電気通信及び、すべての電気技術が範疇に含まれている。またそれらの用語、記号、測定方法、性能信頼性、設計及び開発、安全、環境などの一般関連領域もその業務範囲に含まれている。IEC の使命は電気技術、電子技術及びその関連技術の分野で、電気技術の標準化に関するあらゆる問題解決と、規格への評価などさまざまな関連事項について、会員を通じて推進することにある。

IEEE　Institute of Electrical and Electronics Engineer（アメリカ電気・電子技術者協会）

1963 年にアメリカ電気学会（AIEE）と無線学会（IRE）が合併し組織された非営利の専門機関。発祥はアメリカであるが、会員は世界各国に及び、この種の団体では世界最大。パソコンと外部機器をつなぐインタフェースや、無線 LAN の規格などで馴染みが深い。対象とする分野は、通信・電子・情報工学とその関連分野に及ぶ。専門分野ごとに 39 の分科

会をもち、それぞれが会誌（論文誌）を発行。他に主な活動として規格の制定を行っている。

ANSI（アメリカ規格協会）

アメリカの工業的な分野の標準化組織であり、日本の日本工業規格（JIS）に相当する組織。ISO に加盟している。

アメリカの国内規格ではあるが ANSI 規格がほぼそのまま ISO 規格になることも多い。

規格の国際標準化の根拠

我が国の JIS 規格同様、欧米も独自の規格をもっている。しかし近年各国の規格は国際的な標準化へと向かっている。その根拠となる国際協定は、WTO-TBT 協定である。この協定は貿易の技術的障害（Technical Barriers to Trade、TBT）を取り除くためのものであり、これが規格の国際化・共通化を促す根拠となっている。この協定は、規格の国際整合に留まらず、適合性評価の手続き、その結果の相互認証、技術者の資格制度の整合化と相互認証など、広範囲に規定している。

JIS 規格と国際規格（ISO/IEC 規格）との整合性をとる歩みは、1995 年 1 月に WTO/TBT 協定が発効されるとともに開始された。

2.2 ISO/IEC Guide51 （JIS Z 8051）

この節では国際安全規格の基本となる ISO/IEC Guide51 の概略について説明する。

2.2.1 安全規格の階層構造

ISO/IEC Guide51 の正式名称は、“Safety aspects-Guidelines for their inclusion in standards”である。本書は“ガイドライン（指針）”という標題が示すように、さまざまの規格書を作る場合の指針書である。また“Safety aspects”とあるように安全面に関する規格書の指針である。

ISO/IEC Guide51 は、機械系（ISO）と電気系（IEC）の両者の上位に位置し、安全に関する規格書に関して両者が従うべきものである。“ISO/IEC”とあるように両組織が共同で開発・発行したものである。1990 年に初版が発行され、1999 年に改訂版が出されている。日本おいても JIS として 2004 年に“JIS Z 8051：2004 安全側面－規格への導人指針”が発行されている。JIS Z 8051 は ISO/IEC Guide51 と完全一致規格である。

ISO/IEC Guide51 は、安全規格を、基本安全規格（A)、グループ安全規格（B)、個別機械安全規格（C）の 3 種類の規格に分類している。かつ、これらの規格は、A、B、C の順で上位が下位を規定するようになっている。図 2.2 にこれらの階層関係が示されている。

各階層は次のように区分される。

(1) 基本安全規格（タイプ A 規格）：

安全一般に関する基本概念、設計原則、及び要求事項等から構成。

後に 2.3 節で述べる ISO 12100 はこのタイプ A に属する。

(2) グループ安全規格（タイプ B 規格）：

安全装置や安全距離等のように機械、システムに共通に用いられる規格である。

後に述べる（2.3 節）ISO 13849、IEC 60204、IEC 61508 はこのタイプ B に属する。

(3) 個別機械安全規格（タイプ C 規格）：

特定の機械に対する安全要求事項を定めた規格で具体的な機械､機器類が対象となる。

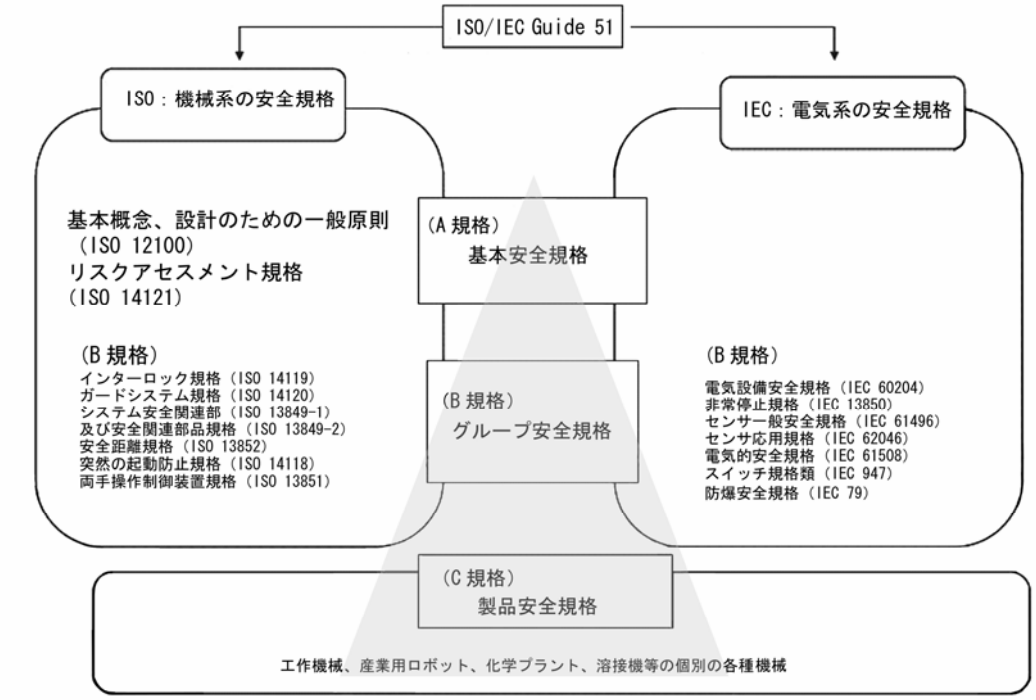


図 2.2　ISO/IEC Guide 51　安全規格の階層構造

この階層構造は、上位規格が下位規格を規定することを示している。製造しようとする特定の機械の安全規格が C 規格に定められていれば、C 規格に従って製造し、もし定められていなければ、A 及び B 規格に基づき、製造者が自己の責任において、その機械に必要な安全のための保護方策を定め実施することとなる。

2.2.2 ISO/IEC Guide51 の文書構成

本書の構成は以下である。

一般に規格書は、各項が「1.適用範囲、2.引用規格、3.用語の定義」と進み、4 項以降で、規格書の独自の項目立てを行っている。本書は指針の書であるが、同様の項目立てとなっている。内容的には上の説明と一部重複するが、規格書の構成を確認するために以下に述べる[1)]。

(1) “1.適用範囲”:(Scope)

本項には下記が書かれている。

本ガイドが規格を作成するためのものであること、
そのためには安全面（aspects）が何であり、それを盛り込むための方法、
本ガイドは人や財産、環境、またその組み合わせたものへ適用可能であること、
本ガイドは規格作成者のためのものであること、
発生するリスクの低減策としては、リスクアセスメントとリスク低減方策（保護方策）の二つが基本であること。

(2) “2.引用規格”:(Normative references)

本ガイドの規格を補完するために既存の規格や指針を引用している。色の安全性や公的標識の安全性、子ども器具の安全性など 9 つを引用している。

(3) “3.用語と定義”:(Terms and definitions)

安全、リスクなど 14 個の用語を定義している。その中のいくつかは第 1 章 1.2.2 項「安全という概念」にて述べられている。“安全”にアプローチする上でリスクという概念を用いることは、安全規格の基本である。

(4) “4.“安全”と“安全な”という用語の使用”:(Use of words “safety” and “safe”)

“安全”という用語はリスクがないことと誤解されるおそれがあるため、その用語を直接用いるのではなく、他の用語に置き換えることが必要とされている。

このことは第 1 章 1.2.2 節でもすでに述べている。安全壁→防御壁、安全靴→保護靴などの安全をもたらす目的や手段を表す用語が必要とされる。

(5) “5.安全という概念”:(The concept of safety)

安全の概念がリスクを用いて規定されており、リスクが残留しないことの根拠は無くしたがって「絶対安全」はありえないとされる（第 1 章 1.2.2 参照)。

(6) “6.許容可能なリスクの達成”:(Achieving tolerable risk)

許容可能なリスク達成のための一般的手順を規定している（第 1 章 1.2.2 参照)。

(7) “7.規格における安全面”:(Safety aspects in standards)

この項には“7.1 安全規格の諸タイプ”:(Types of safety standards）という節があり、安全規格の階層構造化の規定が記されている。

2.2.3　リスク低減プロセス

ISO/IEC Guide51 には、リスクはゼロには成らないゆえに、許容できるまでリスクを低減させるプロセスを行うべきことが規定されている。

このリスク低減プロセスは“リスクアセスメント”と“リスク低減方策（保護方策）”からなるとされる。このリスク低減プロセスは以下の工程をとる。

① 対象となる機械装置やその環境などを考え、危険を予見する。
② その際の危険の大きさなどを見積もり、評価査定し、リスク低減のための方策を講じる。
③ この方策により許容可能なリスク低減が達成されたとするなら、作業は終了。そうでない場合は①に戻り、作業を繰り返す。

この作業に内在する考え方は次のようなものである。

(1) 安全を考えるには、リスクにより考えること（上の①）。
(2) その手段としてリスクアセスメントを実施すべきこと（①、②）
(3) リスク低減方策を繰り返すべきこと（③）

リスクアセスメントやリスク低減方策の詳細は、第 3 章「リスク管理とリスクアセスメント」、第 4 章「安全設計の基本と 3 ステップメソッド」参照。

2.3　主な機械系安全規格と電気系安全規格

この節では機械系の安全規格である ISO 12100 と ISO 13849、電気系の安全規格である IEC 60204 と IEC 61508 について述べる。

2.3.1　ISO 12100 （JIS B 9700）

ISO 12100 は、安全規格の階層構造の中で、タイプ A に属し、下位のタイプ規格を規定する基本的な規格（基本安全規格）である。

安全一般に関する基本概念、設計原則、及び要求事項等から構成されている。JIS 規格では“JIS B 9700”である。

規格の基本的構成は、第一部（ISO 12100-1）と第二部（ISO 12100-2）の二部からなる。ISO 12100-1 は、基本用語を定義し、方法論を規定している。ISO 12100-2 は、技術原則を規定している。

ISO 12100-1 の基本用語は、機械の設計者向けに安全な機械を設計するためのものである。方法論はリスクアセスメントに基づいている。

ISO 12100-2 の技術原則は、機械の設計者向けである。機械類の安全性を達成するためのものである。その概要はリスクアセスメントに基づき保護方策を講じて、リスクを低減し、安全な機械を設計することからなる。

機械メーカーはこの規格をクリアしないと、海外への製品の輸出ができないことになっている[2), 3)]。

(1) ISO 12100 の文書構成

ISO 12100 は次のような文書構成となっている。

〈ISO 12100-1：2003（2003 年版）の構成〉

1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 機械類の設計時に考慮すべき危険源
5. リスク低減のための方法論

〈ISO 12100-2：2003 の構成〉

1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 本質的安全設計方策
5. 安全防護及び付加保護方策
6. 使用上の情報

これらの項目にみられるように、ISO 12100 では、

- 機械類の設計時に考慮すべき危険源
- リスク低減のための方法論
- 本質的安全設計方策
- 安全防護及び付加保護方策
- 使用上の情報

などが主要な課題となる。

これらの詳細は後の章に譲り、主なところを述べる。

(2)　リスク低減のための方法論、方策、情報

すでにのべたように、製造者は機械装置や使用環境のリスクを予見・特定し、見積もり、評価査定し、リスク低減の方策を講じて（リスクアセスメント）、それでももし許容不可能なリスクがあれば、さらにリスク低減の方策を繰り返すことが要求される。

ISO 12100 では、保護方策には、下記の①～③の順位が付けられている。リスクの低減はこの順位に基づいて行うことになる[4)]。

① 本質的安全設計：
　可能な限りリスクを除去・低減した設計を行う。

② 安全防護によるリスクの低減：
　除去できないリスクに対して安全防護策を講じる。

③ 情報によるリスクの低減：
　①、②の保護方策後に残る、残留リスクは操作マニュアル等でユーザーへ伝える。

この三つは、すでに第 1 章で触れたように、保護方策として 3 ステップメソッドとよばれるものである。ISO 12100-1 で規定されている。

保護方策は、設計者のみならず使用者によっても講じることができるが、ISO 12100-1 では設計者のための方策を規定している。

本質的安全設計の方策には、さらに次の規定がある。

① 設計上の各種処置方法を適切に選択し、できる限り多くの危険源の生成を防止し、低減する方法。

② 危険区域への進入の必要性を低減することにより危険源へさらされる機会を制限する方法。

安全防護方策には次の規定がある：

① ガード

② 保護装置

③ 付加保護方策（非常停止など）

情報によるリスクの低減方策には次の規定がある。

① 信号及び警報装置

② 表示、標識（絵文字）、警告文

③ 附属文書（特に、取扱説明書）

(3)　本質的安全設計方策

この中で第 1 ステップの設計方策は、危険源を除去し、リスクを最も効果的に低減することができる方策として、重要視されるものである。

この本質的安全設計は次のように定義されている（ISO 12100-1：2003）。

本質的安全設計方策（Inherently safe design measure）とは、「ガードまたは保護装置

を使用しないで、機械の設計または逆転特性を変更することによって、危険源を除去するまたは危険源に関連するリスクを低減する保護方策」とされている。

設計上の方策と人的対応方策とに分けられる（上述)。

〈設計上の方策〉

設計上の方策は危害の要因を取り除くか、あるいはその要因から生じる危害の程度が小さくなるようにする方法である。

規定内容は、

幾何学的及び物理的要素に関する配慮、

機械設計に関する一般的抜術知識の考慮、

機械的結合の安全原則、

人間工学原則の遵守、

制御システム設計上の安全原則、

安全機能故障の確率の最小化、

空圧／液圧設備の危険源防止、

電気的危険源の防止

などである[5)]。

〈人的対応方策〉

人的対応方策は危険なところに行かない、または行く頻度を減らせば危害にあうことが少ないという考えによる方策である。

規定内容は

設備の信頼性を上げることによって、修正等の介人の機会を制限する方法、

搬入（供給）または搬出（取出し）作業を機械化及び自動化することにより危険な個所への接近を制限する方法、

設定（段取り等）及び保全の作業位置を危険区域外とすることにより危険な個所への接近を制限する方法

などである[6)]。

リスク低減のための方策が講じられた後に残るリスクが許容可能であるかどうかは、その時代における社会の価値観や技術水準などを考慮して判断されるべきものとされる。加えて、その安全性の評価については、製造者自らの合理的な説明が求められる。

2.3.2 ISO 13849 （JIS B 9705）

ISO 13849 は、機械の制御システムの安全関連部に関する安全規格である。機械等装置の安全のためには、制御システムの安全にかかわる部分（Safety-related parts of control systems）のリスク低減が最も重要である。

ISO 13849 にはパート 1 と 2 がある。パート 1 である ISO 13849-1 には、設計の一般原則（General principles for design）、パート 2 である ISO 13849-2 には妥当性（Validation）に関する規格が記されている。

パート 2 はパート 1 の妥当性の確認を支援するための妥当性確認プロセスを規定し、また基本安全原則、十分吟味された安全原則、十分吟味されたコンポーネント、さらには障害リストを掲載している。以下においては特に断らない限り、パート 1、13849-1 について記すこととする[7]。

さらに技術報告書がある。ISO/TR 13849-100。これは ISO 13849-1 を適用するための指針（Guidelines for the use and application of ISO 13849-1）を記している。

ISO 13849 は、安全規格に関する階層構造（A 規格、B 規格、C 規格）のうち、タイプ B に属する。JIS 規格としては“JIS B 9705”である。

機械装置やシステム全体の一部である制御システムの安全関連部（SRP/CS：safety related parts of control system の略）に安全の規格が適用され理由は、制御部が安全の、重要な役割をもつからに他ならない。ここで安全関連部とは、入力信号を受け取り、それに応じて安全関連の信号を出力する制御システムの部分または付属的部分をさす。

このような規格を支える産業社会の動きがある。日本国内では 2006 年 4 月 1 日から、リスクアセスメントの努力義務化が施行された（改正労働安全衛生法）。これにより安全防護装置の活用が増加すると予測されている。

以上は ISO 13849-1 の概要と規格の背景である。規格の文書の構成は次のようになる。

〈ISO 13849-1：2006 の構成と規定内容〉

1. 適用範囲
2. 引用規格

   ISO 12100、ISO 61508-3、ISO 61508-4 など 7 つの規格が引用されている。
3. 用語、定義、記号及び略号

   SRP/CS、category、systematic failure、合理的に予見可能な誤使用、安全機能（safety function）、プログラマブル電子システム（PES:programmable electronic system）、性能レベル（PL）など 37 用語を規定している。
4. 設計上の考慮事項

この規格の大きな特徴は、安全の要求レベルを規定している点である。

以下、規定内容、適用範囲、事例などを踏まえ、順に述べる。

ISO 13849 は、SRP/CS の設計及び組込みの原則（ソフトウエアの設計を含む）に関する安全性要求事項を、構築されるべき安全機能がどのような要求性能レベルをもつかを含めて規定している。要求性能レベルなどの用語は後に説明する。

SRP/CS の適用範囲は、①システムの構造（ハードやソフトからなる制御部)、②コンポーネント・モジュール（ リレー、PLC などの制御用モジュール)、③制御システムの動力源（電気に限定されない油圧、空圧なども）である。使用する技術やエネルギーの種類、例えば、電気、油圧、空圧、機械的エネルギーを問わず、すべての機械類の SRP/CS に適用される[8)]。

SPR/CS に用いられる制御機器としては、スイッチやリレーがある。これらはハードウェアのみからなる。しかしソフトウェアやマイクロプロセッサにより構成されるものも増え、自己診断を行うなど威力を発揮している。例えばセーフティライトカーテンは、光電式の透過型センサであるが、産業用ロボットや機械設備の危険個所で働く作業員の人体検出に使われている。「進入、通過検知」用途に使用されている。プログラマブルロジッ クコントローラ（PLC）も安全関連部に利用される[9)]。

SRP/CS は要求性能レベルをもって安全が規定されるべき、となっていることが特徴であることはすでに述べたが、その方法は次のとおりである。

SRP/CS は要求性能レベル（PL_r）に応じて、カテゴリ（Cat)、コンポーネントの信頼性である平均危険側故障時間（$MTTF_d$)、診断範囲（DC）を採用する。これらの採用によって構築された性能レベル（PL）は、要求性能レベル（PL_r）と同等以上が要求されると規定されている。

〈用語〉

PL_r：Required Performance Level：要求性能レベル（要求安全遂行レベル）

$MTTF_d$：Mean Time to Dangerous Failure：平均危険側故障時間（危険側故障寿命）

DC：Diagnostic Coverage：診断範囲（自己診断率）

PL：Performance Level：性能レベル（安全遂行レベル）

以下、この要求性能レベルの設定等について、背景等から説明する。

〈背景〉

この規格は、どの程度のリスクにどの程度の安全を組み込めばよいのかについて、統一した原則を打ち立てるものである。この規格ができるまでは、一部の機械について定められている安全基準（構造規格など）を基に、類似設計をしていた。しかし、個々の安全基準が十分知られているわけではない。また、安全基準が設定されている機械と異なる業種においては、その基準の意味を知ることもなかなか困難である。結局、基本原則がなければ統一的な安全設計はできない。ISO 13849 によって、初めて統一した安全方策の適用基準ができあがった[10)]。

〈カテゴリ〉

「どの程度の安全を組み込めば」という安全性要求事項の基準となるのが、「カテゴリ」である。カテゴリは、要求性能レベル（PL_r）を満足するシステムを構築するための基本になる。カテゴリは、障害に対する耐性に関して、制御システムの安全関連部（SRP/CS）に要求される挙動を述べたものである。その内容を以下に記す[11)]。

カテゴリ B（Base）：

基本的カテゴリである。障害の発生は安全機能の喪失につながり得る。

カテゴリ 1：

このカテゴリにおいては障害に対する耐性の改善、主としてコンポーネントの選択及び適用により達成される。

カテゴリ 2、3 及び 4：

これらのカテゴリにおいては、特定の安全機能に関し、性能上の改善は、 主として制御システムの安全関連部の構造を改善することにより達成される。

カテゴリ 2：

このカテゴリにおいては、特定の安全機能が実行されていることを定期的にチェックすることにより安全機能の有効性が確認される。

カテゴリ 3 及び 4：

これらのカテゴリにおいては、単一の障害が安全機能の喪失につながらないことを確実にすることにより高い安全性が達成される。

カテゴリ（3 及び）4：

カテゴリ 4 において（及びカテゴリ 3 において合理的に実施可能な場合)、SRP/CS の障害は検出される。カテゴリ 4 では障害の蓄積に対する耐性をもつ。

これらのカテゴリの定義に基づき、各カテゴリへの要求事項と、その要求事項が満足されなかった場合の一覧を**表 2.1** として示す。

表 2.1　ISO 13849-1 におけるカテゴリ要求事項

カテゴリ	要求事項	異常時の安全確保
B	制御システムや保護装置の安全関連部は、想定される外的影響に耐えられるよう、適切な規格にしたがって設計、構成、選定及び組立がなされていること。	故障発生時、安全機能は失われる。
1	1)カテゴリBの要件を満たすこと。 2)十分吟味された、高い信頼性を示す部品を使用し、安全原則に従うこと。	故障発生時、安全機能は失われるが、その発生確率はカテゴリBよりも低い。
2	1)カテゴリBの要件を満たし、安全原則に従うこと。 2)安全機能が機械の制御システムにより適切な間隔でチェックされること。	チェックとチェックの間で故障した場合、安全機能は失われる。安全機能が失われていることがチェックによって検出される。
3	1)カテゴリBの要件を満たし、安全原則に従うこと。 2)安全関連部は以下の方針に従って設計されること。 1.単一故障では安全機能が喪失しないこと。 2.できる限り、単一故障は検出できること。	適切な間隔で安全機能がチェックされること。チェック回路自体が危険状態を引き起こさないこと。単一故障が発生した場合でも安全機能は常に維持さる。全ての故障が検出されるわけではなく、検出されなかった故障が蓄積した場合、安全機能は失われる。
4	1)カテゴリBの要件を満たし、安全原則に従うこと。 2)安全関連部は以下の方針に従って設計されること。 1.単一故障では安全機能が喪失しないこと。 2.次の安全機能が動作する時、またはそれ以前の単一故障が検出できること。それが不可能な場合、故障が蓄積しても、安全機能を喪失しないこと。	自動監視機能付きで、単一のコンポーネントの故障は検出され、安全機能を損なわないこと。これが、実施できないときはその故障は、次の安全機能実行時に検出されること。

〈リスク低減の反復プロセス〉

リスクアセスメントを行い、3 ステップメソッドを繰り返すなどはすでに述べたことと同様である。しかし、ISO 13489 では、リスクの低減が要求レベルに達しているか否かの妥当性を確認するステップが加わっている。2006 年版には 5 ステップの既述はないが、ISO 13489 における要求性能レベル（PL_r）やカテゴリの設定などを理解するために反復プロセスを既述する [12)]。

ステップ 1：危険源分析、リスクアセスメント

次の順序でリスクアセスメントを実施する。

① 械類の制限（使用条件など）の決定

② 危険源の同定

③ リスクの見積もり

④ リスクの評価

ステップ 2：リスク低減方策の決定

ステップ 1 の結果に基づいて、リスク低減方策を決定する。

① 本質的安全設計による

② 安全防護及び付加保護方策による

③　使用上の情報による

ステップ 3：安全要求事項の特定

ステップ 2 の結果に基づき安全機能特性を選択し，その実現方法を決定する。

安全要求性能レベル（PL_r）はここで決定される。PL_r と同等以上の安全性能レベル（PL）を構築するために、カテゴリ（Cat)、平均危険側故障時間（$MTTF_d$)、診断範囲（DC）などを選択し採用する。

ステップ 4：制御システムの安全関連部の設計

ステップ 3 で決定された安全性能レベルに適合するように、システマティック故障、コンポーネントの選択などを考慮して、SRP/CS を設計する。ソフトウェアについては、V（字）モデルに基づく手順によって設計する。設計された制御システムの安全性能レベルの達成度について評価する。

ステップ 5：達成された機能及びカテゴリの妥当性確認

達成された安全性能レベルが，ステップ 3 で決定された安全性能要求レベル（PL_r）を満足しているか検証する。検証方法には分析による場合と試験による場合がある。

・分析による妥当性確認

FMEA、FMECA、FTA などの分析手法による。

・試験による妥当性確認

通常条件及び予見可能な異常条件に対して安全システムの機能試験を実施する。

〈IEC 61508 の引用〉

引用規格に明示されているように ISO 13849 には IEC 61508 の考えが取り入れられている。安全性能レベル PL と IEC 61508(後述)の SIL(安全レベル)を危険側故障率(Probability of a Dangerous Failure）を介して関係づけると**表 2.2** となる[13)]。

表 2.2　安全性能レベル

PL	時間当たり平均危険側故障発生確率 (Average Probability of a Dangerous Failure per Hour（1／h）)	SIL
a	$10^{-5} \leqq PDF < 10^{-4}$	-
b	$3\times10^{-5} \leqq PDF < 10^{-5}$	1
c	$10^{-6} \leqq PDF < 3\times10^{-5}$	1
d	$10^{-7} \leqq PDF < 10^{-6}$	2
e	$10^{-8} \leqq PDF < 10^{-7}$	3

2.3.3 IEC 60204 （JIS B 9960）

IEC 60204 は機械の電気装置の安全に関する規格である。JIS 規格は“JIS B 9960”である。パート 1、2、11、31、32 がある。本書ではパート 1 について述べる。

〈IEC 60204-1:2005 の構成と規格内容〉

IEC 60204-1 は、電気装置が不意の割込み停止などをしないための規格であり、装置に対する一般的な安全要求事項が規定されている（Uninterruptible power systems （UPS） – Part 1: General and safety requirements for UPS)。ここでは、不意に割込み停止しない電気システムを“UPS”と略することとする。

1. 適用範囲と特殊なアプリケーション
2. 引用規格
   IEC、ISO から 48 の引用規格がある。感電保護、電線の色などによる識別、回転電気機械、建築電気設備などの規格が引用されている。
3. 用語と定義
   電気に関係する用語の他、システムやコンピュータ関係する UPS、回路、通信ネットワークの用語も定義されている。
4. 試験の一般条件
5. 基本的な設計要求事項
6. 配線、接続、電源供給
7. 物理的要求事項
8. 電気的要求事項と異常な条件のシミュレーション
9. 通信ネットワークへの接続

附属書 A 熱、火災への抵抗試験
附属書 B 異常な条件でのモーター試験
附属書 C ～0（附属書は 0 まで続き、電気関係の試験や測定の手引きなどが載っている)。

IEC 60204-1 の適用範囲は以下の三つである [14)]。

（1） 稼働中には手で運搬できない機械に用いる電気・電子・プログラマブル電子の装置及びシステムに適用する。連携して稼働する一群の機械も含む。なお、IEC 60204-1 においては、“電気の”という用語には、電気、電子、プログラマブル電子に関する事項を含む。
（2） 機械の電気装置の電源接続点から内側の部分について規定する。
（3） 公称電源電圧が交流 1000V 以下、直流 1500V 以下、公称周波数 200Hz 以下で作動する電気装置に適用する。

IEC 60204-1 の適用範囲は産業機械が主であるが、乗客運搬用機械、遊園地の乗り物も含む。ただし、屋外で用いる機械、爆発する可能性のあるものを使用・加工・製造する機械などには適用しない。

また機械への設計及び安全方策は、電源環境を考慮して行わなければならない。国及び地域によって、機械への供給電圧、周波数及び配電系統はまちまちであるからである[15)]。

このような電気装置を取り巻く事情を考慮しつつ、UPS が順調に稼働するためには、リスクの低減が必要である。危険状態は、次のようなことから発生する[16)]。

・感電又は電気火災を引き起こす制御回路の故障又は障害
・機械の機能不良を引き起こす制御回路の故障又は障害
・機械の機能不良を引き起こす電力回路の故障又は障害、ならびに電源の変動又は停電
・安全機能の故障を引き起こす滑り接触回路又は転がり接触回路の導通不良
・機械の機能不良を引き起こす電気装置の外部又は内部で発生する電気妨害（例：電磁妨害、静電気）
・蓄積エネルギーの解放（電気的又は機械的）
・騒音、表面温度

これらの保護方策は、電気装置供給者が設計段階で組み込むべきものと使用者が実施段階で取り組むべきものがある。

IEC 60204-1 の規格はこのように電気に関するリスク状態や条件を列挙している。組込みシステムの開発には直接関係しないが、組込みシステム開発者は、エンタプライズ系開発者と異なり、電気、電子に近いところで仕事を行う。参考までに以下を列挙する。電気装置の使用に関して使用者と供給者で合意を推奨している箇条と内容である[17)]。

各項目には、下記 4.3.1 のように“電源は、決められた条件で正常に作動するように設計しなければならない。同時に使用者も条件を満足する電源を準備しなければならない”などの規定が記されている。

・4.3.1 電源：使用者が指定する電源
・4.4.3 周囲温度
・4.4.6 汚染物
・4.4.7 電離性・非電離性の放射線
・4.4.8 振動、衝撃、バンプ（パルスの歪）
・4.5 輸送及び保管
・5.1 中性線の端子への表示ラベル
・7.2.2 電源導体のための過電流保護機器の設置

・7.3.2 過負荷保護
・9.2.7.1 ケーブルレス制御における停止
・9.2.7.3 停止
・10.2.1 押しボタンの色
・10.3.2 表示灯、表示器の色
・13.2.1 導体識別の方法
・15.1 特別なタイプのコンセントの必要性
・16.3 機能表示機能をもつ機器に、機器自体又はその近傍にマーキング
・17.1 必要情報の提供（技術文書で）
・17.3 使用者が準備する基礎に設置するダクト、寸法及び配置の情報
・17.4 使用者が準備するダクト、ケーブルトレイ、ケーブル支持物の寸法、種類、用途

〈制御回路や制御機能に関する規定〉

以上、電気に関係する規定を列挙したが、組込みシステムに関係する制御回路や制御機能に関する規定もある。規定はここでもソフトウェアではなく、電気に関する規定であるが、電気の接続法など回路の電源投入に関して苦い経験をもつ組込み開発者もおられるかもしれない。

制御機能に関しては、起動機能、停止機能、運転モードなどに関して、起動、停止、非常停止などの規定が記されている。

他の制御機能であるホールドツゥラン（Hold-to-run）制御、イネーブル制御、また両手操作制御についても規定されている。

IEC 60204-1 の規格は広範にわたる。日常生活の全領域に UPS が行き渡っていることを物語る。

2.3.4 IEC 61508 （JIS C 0508）

IEC 61508 は、制御システムの機能安全に関する規格である。“Functional safety of electrical/electronic/programmable electronic safety-related systems”に対する規格である。JIS 規格では“JIS C 0508”である。「電気・電子・プログラマブル電子安全関連系の機能安全」という規格である。

安全規格の階層構造からは B 規格である。B 規格はグループ規格であるため、下位の C 規格である個々の製品やシステムの安全規格に拘束的な役割を果たす。

IEC 61508 は特定の分野に適応する規格ではなく、広く多種多様な制御システムに適用される。かつ、対象のシステムは電気・電子・プログラマブル電子の機能をもつものをい

う。電気・電子・プログラマブル電子を E/E/PE（electric/electronic/programmable electronic）と略記する。よって、IEC 61508 は E/E/PE の制御システムの安全規格である。

規格書は 7 部構成である。構成の一覧を表 2.3 に掲げる。部の制定年、また IEC 61508 は大部の書であるため、参考までにその頁数も記載する。ただし頁数は仏文、英文並記であるため、倍の頁数となっている。

表 2.3 IEC 61508 の構成

部	表　　題	制定年	頁数
第 1 部	General requirements 一般的要求事項	1998	115
第 2 部	Requirements for electrical/electronic/programmable electronic safety-related systems 電気・電子・プログララマブル電子安全関連系への要求事項	2000	143
第 3 部	Software requirements ソフトウェア要求事項	1998	93
第 4 部	Definitions and abbreviations 用語の定義と略語	1998	53
第 5 部	Examples of methods for the determination of safety integrity levels 安全度水準を決定するための方法の事例	1998	57
第 6 部	Guidelines on the application of IEC 61508-2 and IEC 61508-3 第 2 部と第 3 部を適用する上でのガイドライン	2000	145
第 7 部	Overview of techniques and measures 技術と方法の概観	2000	229

なお、この 7 部の他に、第 0 部（パート 0）として、2005 年、IEC 61508 を簡単に概説する目的で 1 部追加された。“ Functional safety and IEC 61508 ”（機能安全と IEC 61508、2005 年、33 頁）である。テクニカルレポートであり、規格ではない。

〈本規格の適用分野〉

IEC 61508 は、すでにみたように ISO 13849（機械の制御システムの安全関連部に関する安全規格）に引用されている。その他、化学プラントなどのプロセス産業関連、原子力、医療機器、鉄道関連、自動車のエンジン制御などにも適用され、またこれらの規格もまた IEC 61508 に影響を与えている。

〈本規格の構成〉

本規格の構成も他の規格と同様に、「1.適用範囲、2.引用規格、3.用語の定義」と進み、それ以降の項に、当該規格の固有の規格内容が記述される。

ソフトウェアに関係するパート 3 をみると第 6 章に、ソフトウェアの品質管理システムの記述がある。また第 7 章には、すでにみたリスク低減のプロセスを思わせるような、ソ

フトウェアの開発のライフサイクルを回しながら、安全という要求項目の実現のために仕様の実装の検証や仕様の妥当性の検証するプロセスが述べられている。このことは後にあらためて述べる。

原文であるが、第3部「**ソフトウェア要求事項**」の構成の目次一覧をそのまま以下に記す。

1 Scope
2 Normative references
3 Definitions and abbreviations
4 Conformance to this standard
5 Documentation
6 Software quality management system
  6.1 Objectives
  6.2 Requirements
7 Software safety lifecycle requirements
  7.1 General
  7.2 Software safety requirements specification
  7.3 Software safety validation planning
  7.4 Software design and development
  7.5 Programmable electronics integration （hardware and software）
  7.6 Software operation and modification procedures
  7.7 Software safety validation
  7.8 Software modification
  7.9 Software verification
8 Functional safety assessment
Annex A （normative） Guide to the selection of techniques and measures
Annex B （normative） Detailed tables
Annex C （informative） Bibliograph

〈機能安全と関連する主な用語〉

規格 IEC 61508 は、“Functional safety：機能安全”に関するものであり、その対象はE/E/PE の制御つき装置システムである。IEC 61508 の第0部、P.13 を参考にし、機能安全規格の主な用語を整理すると次のようになる[18)]。

このシステムにどのような重大な潜在的な危険（hazards）があるのかを特定し、リスクを低減するプロセスは、すでにみたリスクアセスメントと3ステップメソッドによるリスク低減を反復的に行う安全規格と変わらない。

IEC 61508 では、危険の防護のために“機能安全”を設計に考慮する。機能安全は潜在

する危険を扱う単に一つの方法に過ぎず、本質安全（inherent safety）のように、潜在する危険をなくしたり、少なくしたりする他の方法がまず第一に重要であり、これは今までみてきたことと同様である。

このように機能安全とは、設計に考慮されるべき危険に対応する機能である。

安全機能（safety functions）とは、リスクが受容レベルに保たれていることを保証する機能である。**また、安全度水準（safety integrity）**は、水準が高ければ危険が少ないことを示す基準である。

したがって、機能安全がシステムに対して設計に考慮され、**システムが**安全機能と安全度水準がいずれも要求を満たしているとき、システムは**安全関連的（safety-related）**であるという。

端的にいえば、安全機能を実行するシステムは、どれも**安全関連系（safety-related system）**であるといえる。

また、安全関連系は、付属の装置制御システムとは分離可能な系かもしれない。

〈全安全ライフサイクル〉

システムの安全に関して、安全機能や安全度水準を設定し、それらを設計に盛り込むためのおおよそのプロセスは上に述べたが、安全は、システムの運用のみで終わるのではなく、保全、廃棄の全体までを対象としなければならない。

IEC 61508 は、このような全安全サイクルを考慮している規格である。すなわち、システムの概念設計段階から、安全要求事項、仕様の決定、仕様に基づいた安全装置の設計・開発、運用・保全、廃棄までのライフサイクル全体にわたって、安全を達成・維持するために必要な事項を規定している。

また、IEC 61508 は、規格の標題に“programmable”とあるようにソフトウェアを含む規格であるところに特徴がある。同時にソフトウェアに関する安全を取り扱う場合は、機械などの故障と異なり、システマティック故障 （systematic failure）という概念を導入し、部品の劣化などのランダムハードウェア故障（random hardware failure）と区別している。このことを第 1 章では「ハードウェアの故障とソフトウェアの故障」として論じている。

システマティック故障は因果的に発生すると理解される。そのためには原因を取り除くことが必要とされる。同様にリスク低減方策をはかる必要がある、かつこれらを全工程にわたって行う必要がある。IEC 61508 では、これらを全サイクルに関して行うことを規定している。これは「全安全ライフサイクル」と呼ばれ、図 2.3 に表した[19)]。

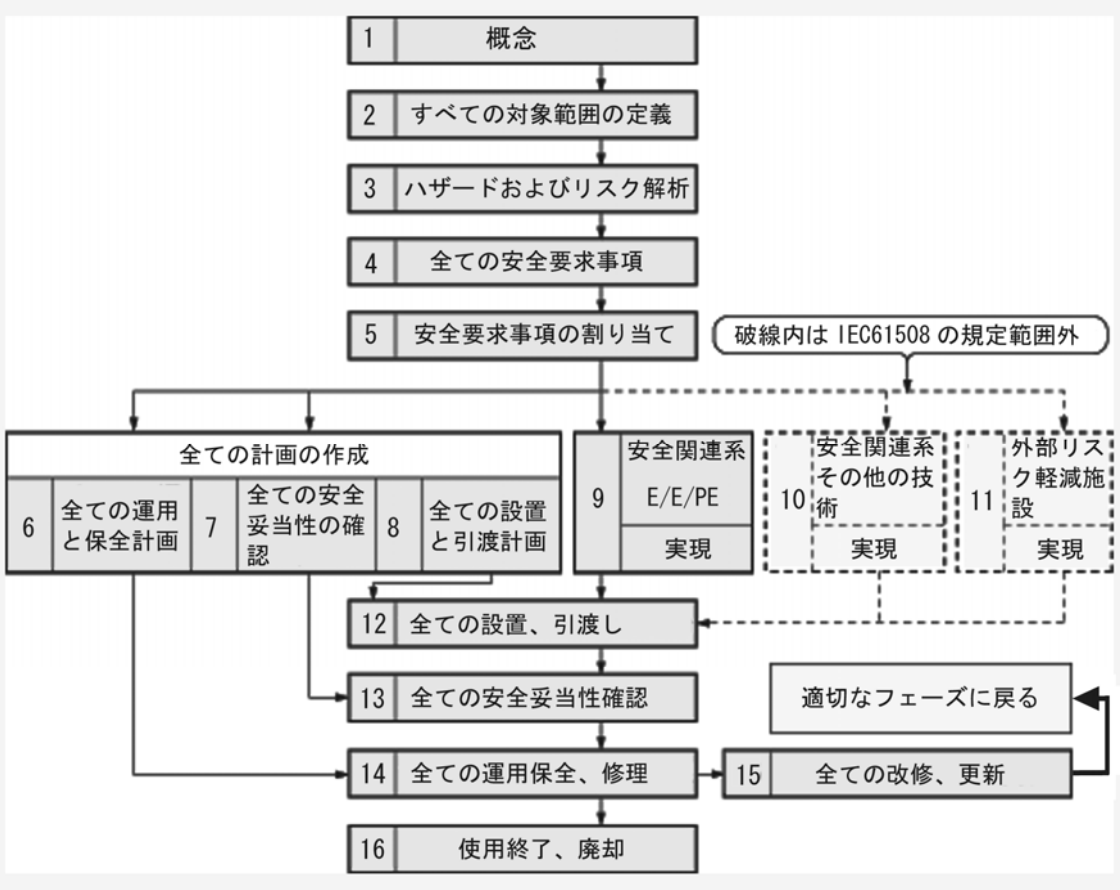


図 2.3　全安全ライフサイクル

〈全サイクルの概観〉

フェーズ 1〜4 では、制御系に異常があった場合のリスクを解析し、リスクを軽減するために必要な安全要求仕様を決定する。フェーズ 5 では、安全関連系の機器や施設に安全要求機能を割り当て、各安全機能に対して安全度水準（SIL）を割り当てる。フェーズ 6〜8 では、設置から保守に至る工程で、安全を維持するための計画を策定し、フェーズ 9〜11 では要求された SIL を実現する。フェーズ 12〜16 では、設置から廃棄に至る工程における安全を維持する。

各フェーズの詳細な内容は以下の通り。

フェーズ 1：概念の把握

対象システムの環境と関連法規等を理解し、ハザードや情報を把握する。

フェーズ 2：すべての対象範囲の定義

対象システムと制御系の境界を定め、潜在危険分析及びリスク解析の範囲を定義する。

フェーズ 3：潜在危険及びリスク解析

対象システムと制御系に対し、すべての運転モードで生じる潜在危険の分析及びリスク解析を行う。

フェーズ 4：すべての安全要求事項

E/E/PE 安全関連系、他技術安全関連系、外部リスク軽減施設（例えば防護壁など）に対して、安全機能要求事項及び安全度水準 SIL 要求値を、安全要求仕様書として作成する。

フェーズ 5：安全要求事項の割り当て

安全機能要求事項及び SIL 要求値を、E/E/PE 安全関連系、他技術安全関連系、外部リスク軽減施設に対して割り当てる。

フェーズ 6：すべての運用及び保全計画

E/E/PE 安全関連系の運用保全計画を作成する。

フェーズ 7：すべての安全妥当性確認計画

E/E/PE 安全関連系のすべての安全妥当性確認を実施するための計画を作成する。

フェーズ 8：すべての設置及び引き渡し計画

E/E/PE 安全関連系の設置計画及び引き渡し計画を作成する。

フェーズ 9：E/P/PE 安全関連系実現

E/E/PE 安全関連系の安全機能要求事項と SIL 要求値に適合する、E/E/PE 安全関連系を設計・製造する。

フェーズ 10：その他の技術安全関連系実現

E/E/PE 以外の技術で安全関連系を設計・製造する。

フェーズ 11：外部リスク軽減施設

外部リスク軽減施設によって、リスクを低減する。

フェーズ 12：すべての設置及び引き渡し

E/E/PE 安全関連系の設置及び引き渡しを行う。

フェーズ 13：すべての安全妥当性確認

E/E/PE 安全関連系が、すべての安全機能要求事項及び SIL 要求値を定めた安全要求仕様に、適合して妥当であることを確認する。

フェーズ 14：すべての運用保全及び修理

要求される安全機能を維持するよう、E/E/PE 安全関連系を運用、保全及び修理する。

フェーズ 15：すべての部分改修及び改造

E/E/PE 安全関連系の機能安全が、部分改修時や改造時、またその後も維持されるようにする。

フェーズ 16：使用終了または廃却

E/E/PE 安全関連系の安全機能が、対象システムの使用終了時や廃却中、またその後の環境で適切であるようにする。

《ソフトウェアの安全ライフサイクル》

リスクの低減を実現するためのフェーズはフェーズ 9 である。フェーズ 9 は E/E/PES とソフトウェアの安全ライフサイクルに分かれる。

“E/E/PES”とは、“Electrical/Electronic/Programmable Electronic System ”の略である。このE/E/PESは、システムであって、安全という概念は含まれていない。よって、フェーズ9.1の「E/E/PESの安全要求仕様」とは、「（ハード＆ソフト等からなる）任意のシステムの安全要求仕様を適切に決める」という意味である。

ソフトウェアの安全ライフサイクルにおけるフェーズ9.1に関しても、「ソフトウェアの安全要求仕様」とは、「任意のソフトウェアの安全要求仕様を適切に決める」という意味である。またソフトウェア制御による安全機能を決めると換言できる。

図は、システムとソフトウェアを別々に描いているが、同時に矢印で相互に関係すべき異を表している。システムの安全ライフサイクルを実行するためには、システムとソフトウェアの同期が必要である。このことを以下に**図2.4**で表す[20)]。

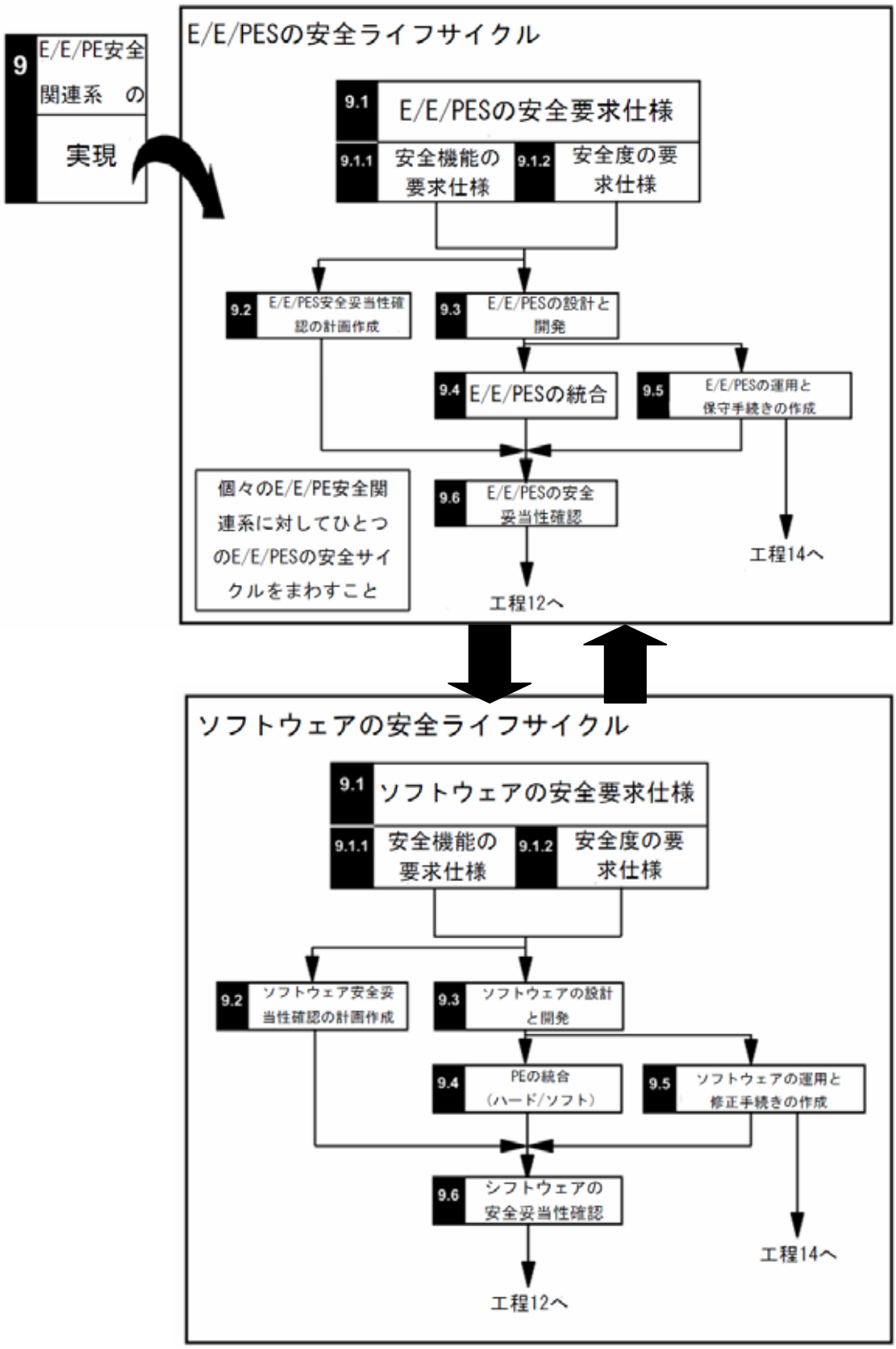


図 2.4　システムのソフトウェアの安全ライフサイクル

〈V モデル〉

以上のようなソフトウェア開発プロセスに関して、IEC 61508 では「ソフトウェア安全度と開発ライフサイクル」としてV（字）モデルが推奨されている。検証と妥当性確認をプロセスごとに行うことが重視される。

IEC 61508 では、評価認証の取得の制度もあり、開発が定石通りに行われたかが重視される。この過程は文書で示す必要があり、文書には、開発履歴がプロセス単位に明記されていなくてはならない。このことはプロセスが定石通り実行されていなくては困難である。

V モデルはソフトウェアの開発ライフサイクルとして、IEC 61508 に推奨されていることは組込み系開発企業として承知しておくべきことであろう。

V モデルを**図 2.5** に示した[21)]。

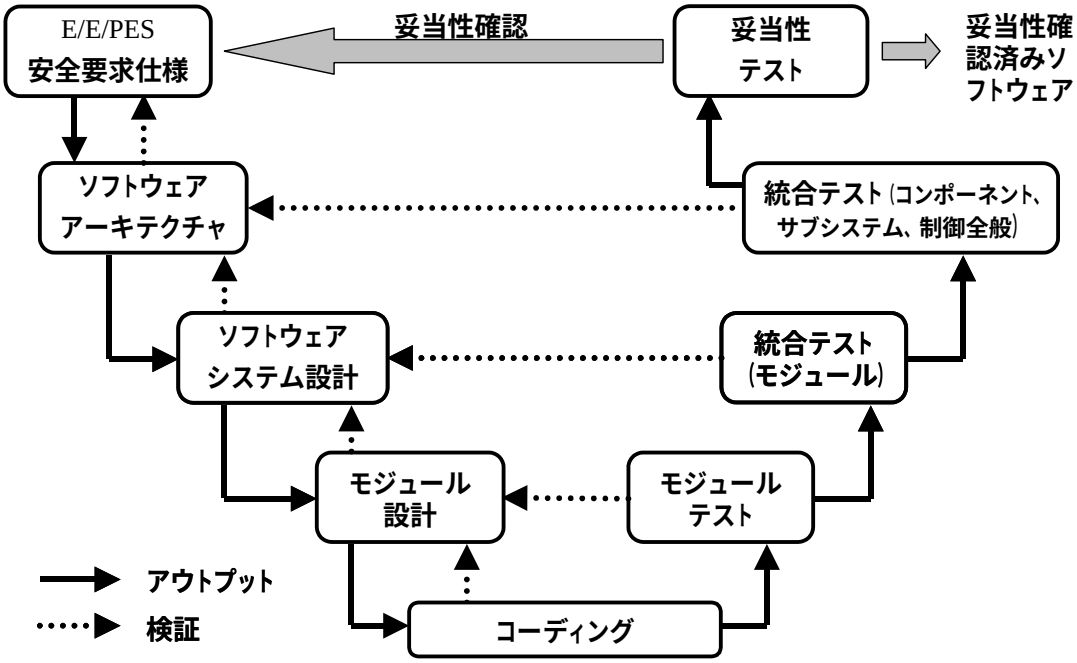


図 2.5　V モデル

〈安全度水準 SIL〉

図 2.3 フェーズ 4 では、リスクを受容できるまでに低減する安全機能をどのレベルのものにするかの選択がなされる。SIL の選択である。**図 2.4** のフェーズ 9.1.1 には「安全度の要求仕様」というフェーズが描かれている。これは SIL 実現のための安全機能に関する仕様である。どのような機能を安全のために実現するか、仕様を決め、実装する。

IEC 61508 においては、SIL は安全性能の低い順から SIL1～SIL4 の 4 段階で示され、SIL4 がもっとも高いものとなっている。また低需要運転モードと高需要運転モードにおける目

標故障限度が別に規定されている。低需要運転モードの SIL を**表 2.4** に示す。

低需要モードは稼働回数を基準にした安全度水準である。SIL3 であれば、1 万分の 1 回から千分の 1 回の間に故障しても、十分リスクが受容できる機械装置やシステムが当てはまる。高需要運転モードを含めた全体の表については第 6 章の表 6.6 を参照されたい。

表 2.4　安全度水準:低需要運転モード

SIL	低需要運転モード時の平均故障確率
4	$\geqq 10^{-5}$ ～ $< 10^{-4}$
3	$\geqq 10^{-4}$ ～ $< 10^{-3}$
2	$\geqq 10^{-3}$ ～ $< 10^{-2}$
1	$\geqq 10^{-2}$ ～ $< 10^{-1}$

2.4 国際安全規格と組込みシステム開発の課題

この節では各企業の国際安全規格への、実際の取り組みの実例を挙げ、規格化の国際的な動きについて述べる。

国際安全規格の採用は欧米のみではなくアジアでも始まっている。

台湾の新幹線システムを日本企業連合が国際落札した際に、鉄道信号機システムの部分を担った、ある会社では、当時としては耳慣れない SIL4 対応を迫られ、大変苦労したとのことである。

このように受注の可否に国際安全規格への対応が関わっており、日本の企業も数年前より IEC 61508 規格の認証の取得を行っている。特にこの 1、2 年は大手の電機メーカーがかなりの費用を投じて認証を取得するなど、国際安全規格への関心が高まっている。ネット検索をすることによってこのことは確認できよう。

このような動きの中で、組込みシステムの開発を行う立場としては、国際安全規格に関してどのような関わりをもつべきか､あるいは実際に何を行うべきか､ということになる。

国際安全規格が分野を超えて横断的に物づくりの現場に入ってきたことは近年の傾向である。その結果、物をつくるにあたり、世界の標準的な規格はどのようになっているのかを知らずして事に当たることはできなくなってきている。折に触れ、あるいは実際の事に当たり、安全規格をものにして行くことは必要であろう。

しかし同時に組込みシステムの開発を担う組込み系技術者、あるいは事業者としては、安全にかかわる技術の習得や事業の展開が関心事となる。

技術に関していえば、IEC61508 の第 7 部付属書 C で取り上げている「ソフトウェア安全

を達成するための技術と手法の概観」に取り上げられている事柄が参考になる。要求事項を明確にするためには、構造的手法が有効であり、そのいくつかが紹介されている。また信頼性や品質の高いソフトウェアの実現は、リスク低減のための重要な条件である。そのために形式手法が紹介されている。

形式手法は SIL4 を取得するために強く推奨されている方法であるが、高度な制御はむろんのこと、情報セキュリティのためのソフトウェアにとっても不可欠な技法とされている。次代の組込み系ソフトウェアの領域もこのあたりに存在すると明言する人も少なくない。

形式手法は、論理学や数学の証明論などの方法を基礎においた、仕様の内容やソフトウェアの記述を明晰にする方法である。仕様のモデル化やシミュレーション、また形式的な仕様記述言語の利用からプログラムの自動生成などが実用化され、徐々に現場に浸透しているようである。ソフトウェア規模が増大する中で、形式手法は威力を発揮することが期待されている。

また安全分析手法についていえば、技術者にとっては日頃の業務であるシステム分析の手法に類似のものも多い。違いなどを学び、自らの手法に取り入れることも可能であろう。

またリスク低減のプロセスも、システムの不具合を減らす過程と類似する。またソフトウェアの安全ライフサイクルを回すなどは、日頃の開発過程と類似である。しかしより厳密に品質水準などを付けながら、品質管理や仕様との適合性を検査する方法などがあるのかもしれない。

組込みシステムがその規模と複雑さを増して行く中での基本的な問題である。

2.5 本章のまとめ

本章では国際規格の発行機関について梗概し、国際化の進展と規格の増大とその横断的な広がり。従って規格を無視できないことを述べた。

また安全規格に関しては、ISO/IEC Guide51 の安全規格全体における位置づけが、他の安全規格の上位にある指針（ガイド）であることを確認し、その下位にある A 規格、B 規格に属する主な規格を述べた。

ISO 12100 は安全一般に関する基本概念や設計原則をのべた A 規格である。

ISO 13849 は機械の制御システムの安全関連部に関する B 規格である。

IEC 60204 は電気装置に関する安全規格である。規格である。

IEC 61508 は、電気・電子・プログラマブル電子の安全関連系を対象とする安全規格である。B 規格である。

C 規格は個別の製品規格であるが、本書では取り扱わない。

これらの安全規格については、それぞれの規格が担う機械装置や電気装置の受けるリスクを特定し、そのリスク保護方策を説明した。リスクの分析や特定、査定のリスクアセスメントと本質的安全の設計から行う 3 ステップメソッドが、リスク低減の基本であることを述べた。このことを反復的に繰り返すことの重要性も述べた。規格によってはこの 3 ステップに加え、対象システムに安全の水準値を設計として加え、その要求が実現されているかのステップも加えるものもある。このことも説明した。

さらに、安全制御の実現のためにソフトウェアが威力を発揮しているが、ソフトウェアの規格も規定している IEC 61508 についても述べた。この規格は、組込みシステムを担う技術者や事業者にとって、看過できない規格であろう。

最後に組込み系技術者や事業者は、安全の規格から学ぶところが多いと同時に、組込み制御分野に適した技術として、数学や論理学をベースにした形式手法に注目すべきではなかろうかと述べた。

参考文献（第 2 章）

注 1)　向殿政男監修、安全の国際規格 1「安全設計の基本概念」,pp.23-27,日本規格協会,
2007 年 5 月

注 2)　オムロンセーフティーテクニカル Guide 第三部　安全規格、オムロン株式会社,p.3,
http://www.fa.omron.co.jp/data_pdf/commentary/safety_technical_guide3.pdf

注 3)　向殿政男、機械システムの安全性,p.27,電子情報通信学会誌,Vol88 No.5,2005 年
5 月

注 4)　向殿政男監修、安全の国際規格 2「機械安全」,p.27,日本規格協会,2007 年 6 月

注 5)　向殿政男監修、安全の国際規格 2「機械安全」,p.36,日本規格協会,2007 年 6 月

注 6)　向殿政男監修、安全の国際規格 2「機械安全」,p.36,日本規格協会,2007 年 6 月

注 7)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.104,日本規格協会,
2007 年 9 月

注 8)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.105,日本規格協会,
2007 年 9 月

注 9)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.105,日本規格協会,
2007 年 9 月

注 10)　佐藤国仁、ISO 国際安全規格「内容と動向」,pp.13-14,ESPEC 技術情報 NO.31,
2002 年 10 月

注 11)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.150,日本規格協会,
2007 年 9 月

注 12)　向殿政男監修、安全の国際規格 3「制御システムの安全」,pp.114-117,
日本規格協会,2007 年 9 月

注 13)　佐藤国仁、ISO 国際安全規格「内容と動向」,p.14,ESPEC 技術情報 NO.31,
2002 年 10 月

注 14)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.26,日本規格協会,
2007 年 9 月

注 15)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.29,日本規格協会,
2007 年 9 月

注 16)　向殿政男監修、安全の国際規格 3「制御システムの安全」,pp.31-33,日本規格協会,
2007 年 9 月

注 17)　向殿政男監修、安全の国際規格 3「制御システムの安全」,p.34,日本規格協会,
2007 年 9 月

注 18)　IEC, TR-61508-0, Part0: Functional safety and IEC 61508, 2005-01, p.13

注 19)　IEC, 61508-1, Part1: General requirements, 1998-12, p.33

注 20)　IEC, 61508-3, Part1: Software requirements, 1998-12, p.25

注 21） IEC, 61508-3, Part1: Software requirements, 1998-12, p.27

引用はないが参考とした主な文献

注 22） 水口大知、長谷部浩二、ソフトウェアの安全性をめぐる課題について、
日本信頼性学会、Vol.157, No.5,2007
注 23） 水口大知、機能安全対応のためのソフトウェア安全分析手法、
エンベデッドフォーラム in グレーター・ナゴヤ（講演資料）、2008-1/29
注 24） 田辺安雄（株式会社日本機能安全）、機能安全の考え方と組み込みシステム、
財団法人組込みシステム技術協会「機能安全・セキュリティーセミナー」（講演資料）、
2007-7/10
注 25）財団法人日本船舶標準協会、船舶の安全システムの評価に関する基礎調査報告書、
平成 12 年度
注 26） 独立行政法人産業技術総合研究所システム検証研究センター、
機能安全規格と適合認証（61508 のさらなる理解に向けて）、2006
注 27） ソフトウェア安全設計概説　　株式会社レンタコーチ、
http://homepage2.nifty.com/rent-a-coach/text_safety_design.pdf
注 28） 機械安全規格について、株式会社キーエンス、
http://www.sensor.co.jp/worldsupport/index.html

第3章　リスク管理とリスクアセスメント

リスク低減の方法論としては、二つに分類される。一つは「リスクアセスメント」、もう一つは「リスク低減のための技術的保護方策」である。

この章では、リスクの低減を図ることによって、製品の安全を設計する（織り込む）場合に、最初に行う重要なプロセスであるリスクアセスメントの概要について述べる。特にリスクアセスメントを行うプロセスであるリスク分析、危険源の同定、そのリスクにおける見積り方法とそのリスクの評価方法に関してわかりやすく記載する。

また、実際にリスクアセスメントを実施した後のリスク管理のプロセスとしての安全設計手法（リスク低減のための技術的保護方策）については、第 4 章以降で解説を行う。

3.1 リスク管理

ISO/IEC の Guide51 の中では、リスクの定義は「危害の発生確率及びその危害程度の組合せ」となり、TR Q 0008（ISO/IEC GUIDE 73:2002）(*1）では「事象の発生確率と事象の結果の組合わせ」と表現される。本書のいうリスク管理（リスクマネージメント）とは、組織的、包括的に管理しハザード、損失などを回避もしくは低減をはかる体系的なプロセスのことである。

3.1.1 リスク管理

リスクマネージメントに関しては、標準情報として TR Q 0008 が制定されており、リスクは、低減、対応、コントロールするものであり、リスクへの対策は、ISO/IEC Guide51 などの安全規格より広い内容となっている。

ISO/IEC Guide51 と TR Q 0008 の違いを簡単に表現すると ISO/IEC Guide51 が、安全分野に特化しており、リスクから生じる結果はネガティブリスクとしてとらえているのに対し、TR Q 0008 は、リスクから生じるポジティブリスクも対象としている。

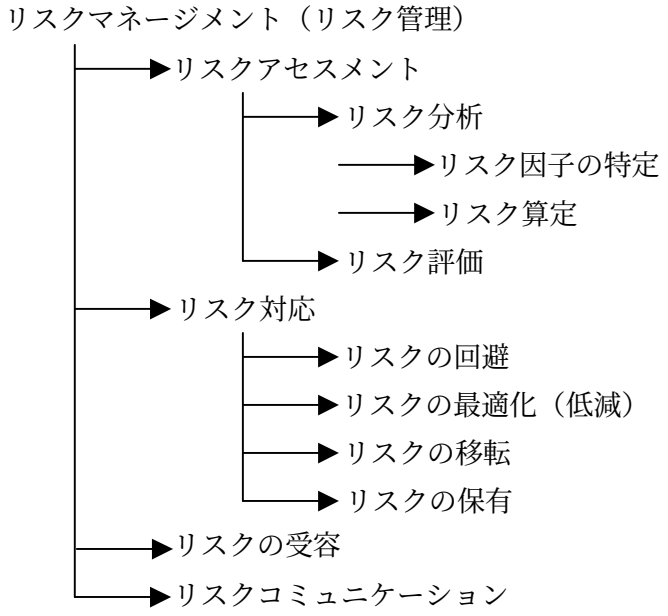


図 3.1　リスクマネージメントの構成　（TR Q 0008）

TR Q 0008 によるリスクマネージメント（リスク管理）は、**図 3.1** のように表現される。リスクマネージメントは「リスクアセスメント」、「リスク対応」、「リスクの受容」、「リスクコミュニケーション」を含み、さらに「リスクアセスメント」は「リスク分析」、「リスク評価」により定義される。

最初に、リスク分析は、「リスク因子の特定」と「リスク算定」により構成され、リスク因子の特定は、リスク因子を発見し特長を明確にすること、リスク算定は、リスク因子の発生確率と結果を設定することになる。次にリスク対応は、リスクを変更させるための方策を選択、実施することである。また、リスク評価の結果、リスク対応を実施することが決定したリスクについて、リスク回避、リスクの最適化、リスクの移転、リスクの保有の四つから選択することになる。さらに、リスクの受容については、リスクを受容する意思決定プロセスである。本章で述べるリスクアセスメントや第 4 章で述べる安全設計の基本と 3 ステップメソッドもリスク管理の一部として位置づけられる。

3.2 リスクアセスメント

リスクアセスメントは、安全性確保のための最も基本的な作業の一つであり、機械、化学、医療、電気などさまざまな分野で利用されている。特に機械の分野でのリスクアセスメントの原則は ISO 14121 として発行されており、リスクアセスメントは ISO 12100 シリーズで実施することが要求されていますが、すべての機械にはリスクが存在するという大原則に基づき、機械に存在する危険源を評価するための理論的なステップである。リスクアセスメントは機械ができあがってから行うものではなく、設計の段階で本質安全設計を行い、より安全で使いやすい機械を作るために必要不可欠なテクニックである。**図 3.2** にリスクアセスメントの手順を示す。

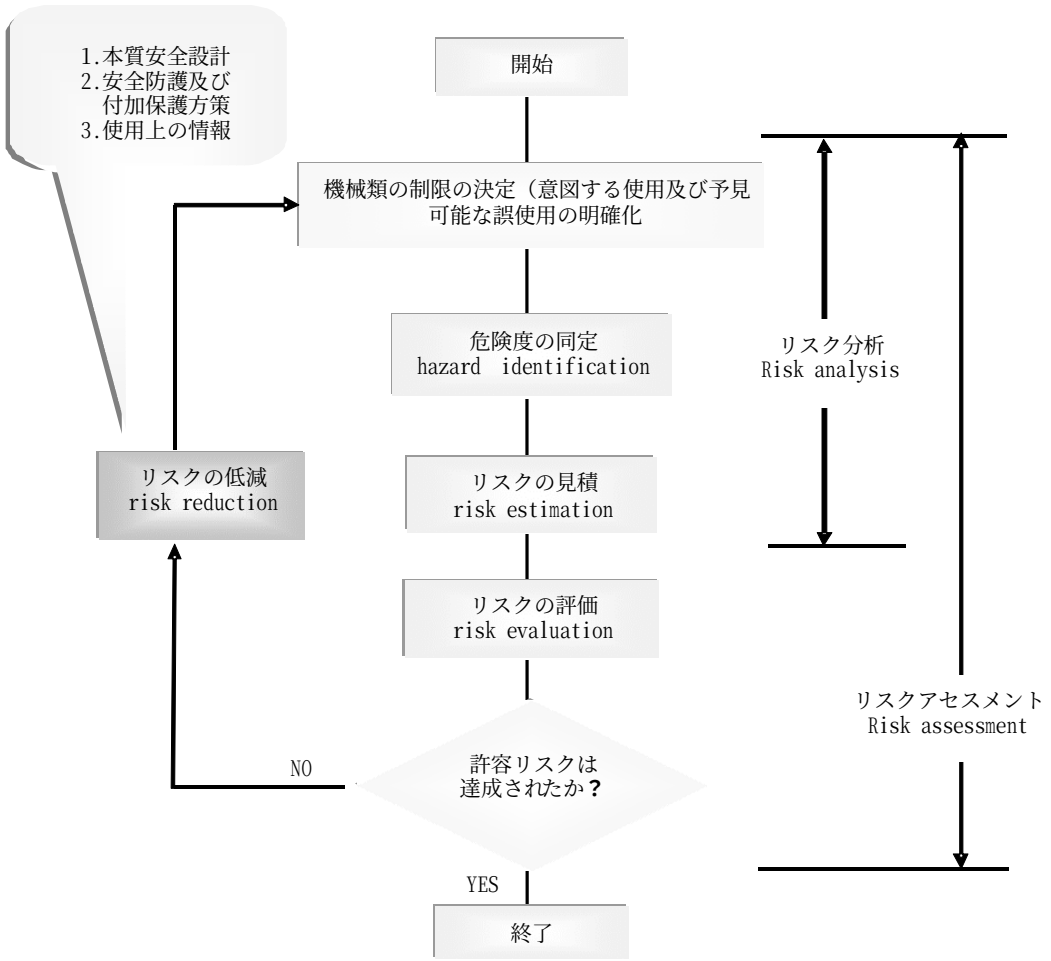


図 3.2　リスクアセスメントの手順

3.2.1　危険源分析方法（リスク分析）

（1）機械類の制限（使用及び予見可能な誤使用の明確化）

最初にやることは、対象装置（製品）の特徴を正確に把握し、使用目的・使用条件を明確にすること。永遠に使える装置はないので、有効期限は何年まで、こういう用途で使う、使用者はこういう条件を満たしていること、設置のための条件はこれこれと、整理することである。

次に「予見可能な誤使用」といって、普通の人（組み立て作業者、設置工事者、オペレータ、保守要員などに加え、清掃作業者や対象装置に近づく可能性のある第三者まで含める）だったら、こんなミスや本来の目的外での使用をするであろうと想像し、その「誤使用」まで、条件に加えるようにする。

このように機械安全規格では、「機械類の制限」を決定することが要求されている。

それには、「使用上の制限」、「空間上の制限」、「時間上の制限」に分類され、明確化することが要求される。

① 使用上の制限

使用上の制限は、「意図する使用」及び「合理的に予見可能な誤使用」を明確にすることを意味する。この制限を検討するうえで、考慮すべき要件として ISO 14121 では以下の四つが示されている。また、これらを加味した一般例を、**表 3.1** に示す。

a)　機械の各運転モード及びさまざまな介入手順
　通常運転、機能不良の修正、保全、修理など
b)　性別、年齢、利き手又は身体的能力の限界によって特定される人による機械の使用範囲
c)　機械使用者の訓練、経験、能力レベル
　オペレータ、保全要員又は技術者、見習い及び初心者、一般大衆
d)　機械類に付随する危険源に第 3 者が暴露されること
　－周辺地域で作業するオペレータ
　－周辺地域のオペレータではない被雇用者
　－周辺地域の被雇用者ではない人

表 3.1　使用上の制限要素例

制限要素例		
1	意図する使用	ライフサイクル上の相互作用
		機能不良に伴う相互作用
		対象とする人
2	合理的に予見可能な誤作用	・オペレータによる操作不能の発生 ・機能不良、事故発生時の人の反射的な挙動 ・集中力の欠如又は不注意による機械の操作誤り ・作業中での近道反応による被災 ・第三者の行動
3	予期しない起動	・制御システムの故障やノイズなど外部からの影響による起動指令で生じる軌道 ・センサや動力制御要素など、機械の他の部分での不適切な扱いにより生じる軌道 ・動力中断後の再復帰に伴う起動 ・重力や風力、内燃機関での自己点火など、機械への外部又は内部からの影響による起動 ・機械の停止カテゴリ（IEC 60204-1）

② 空間上の制限

空間上の制限とは、当該機械の可動範囲、機械の設置及び保全のための空間、オペレータと機械の間のインタフェース、機械と動力供給の間のインタフェースなどを決定することである。一般例を**表 3.2** に示す。

表 3.2　空間上の制限要素例

制限要素例		
1	機械の動作範囲	アクチュエータの可動範囲、及びその可動速度又は運動エネルギー
2	オペレーター機械間インタフェース	機械の大きさに適した使用場所、操作パネルの位置、オペレータの作業範囲、保守時の点検／修理スペース、点検部位へのアクセス、工具や加工物の放出、機械のレスポンスタイム
3	機械ー動力間インタフェース	機械可動部の過負荷対応、異常時のエネルギー遮断、蓄積エネルギーの消費、捕捉時の救出
4	作業環境	階段、はしご、手すりの設置、プラットフォーム

③　時間的な制限

時間上の制限とは、機械類やそのコンポーネントの寿命限界を考慮することである。一般例を**表 3.3** に示す。

表 3.3　時間的な制限要素例

制限要素例		
1	機械的制限	加工用の砥石やドリルなど工具の交換時期､可動部のベアリングや油空圧部品のシール寿命
2	電気的制限	絶縁劣化、接点寿命、配線被覆の磨耗、接地線の外れ

④　その他の制限

環境面、掃除レベル、処理材料の特性

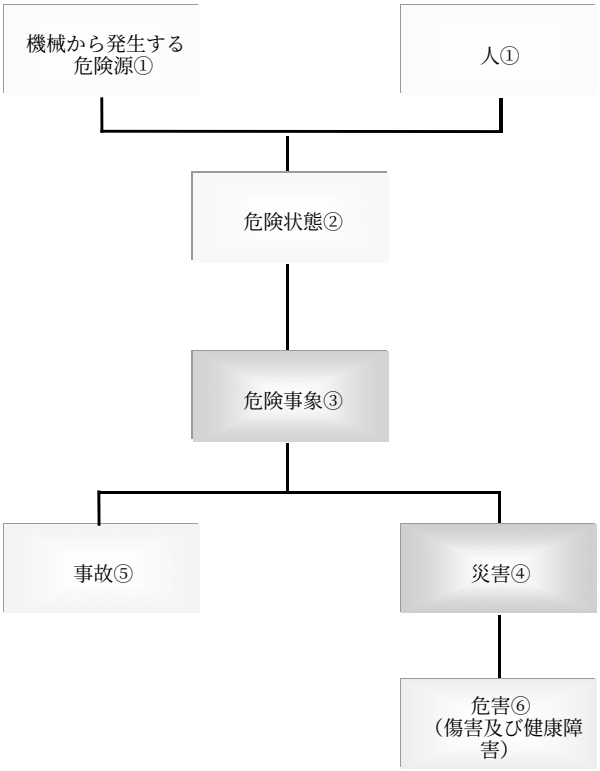
(2)　危険源の同定

この装置には、どういう危ない所があるかを全て洗い出し、リストとして整理する。この作業は、意外と難しい作業で、無意識の内に回避している危険源などを、つい見落とすことがある。この見落としを少しでも防ぐために、ISO 14121（JIS B 9702）「リスクアセスメントの原則」の附属書Aとして記載されている､「危険源、危険状態及び危険事象の例」が参考になる。

IEC 60204（JIS B 9960）など、あるいはCEマーキングの低電圧指令やEMC指令での要求項目が国際的にも通用する安全レベルと考えることができるので参考にすると良い。

①　危険源とは

危険源とは、危害を生じる可能性のある原因のことを示す言葉であり、危険源があるからといって、即、事故や災害が起こり危害が発生するということではない。すなわち、危険源が存在したとしても､そこに接近する人がいなければ､危害の発生に至ることはない。ここで､危害発生のプロセスを定義すると**図 3.3** のようになる。また、ISO 12100-1 では、「危険源」は、危害を引き起こす潜在的根源と表現されている。

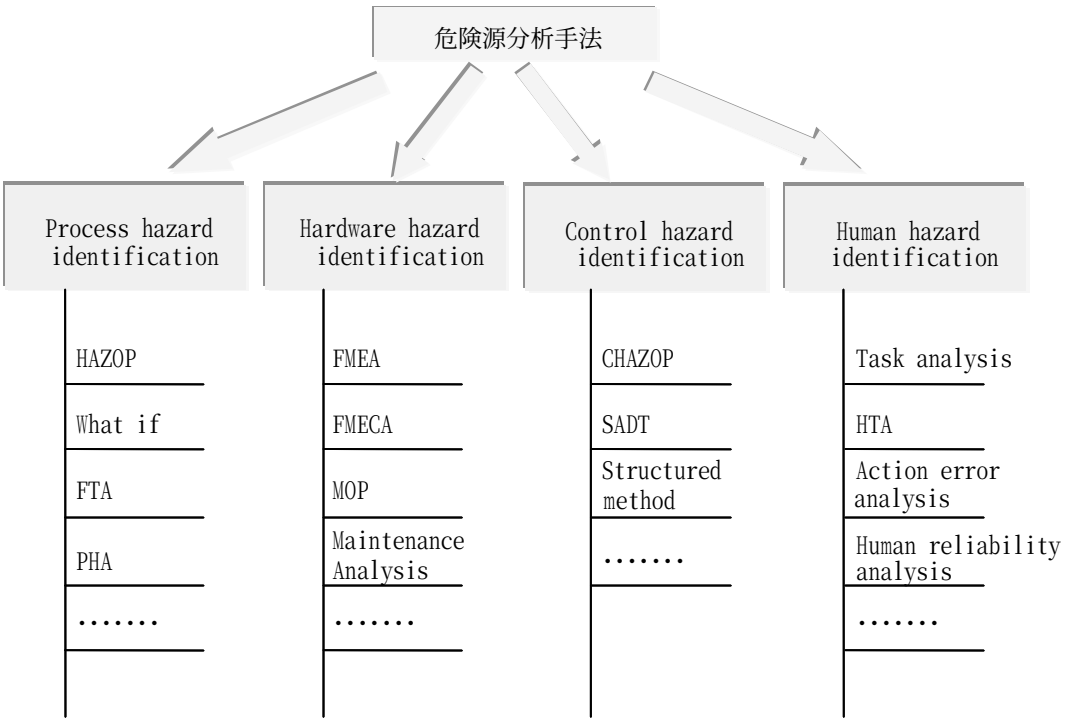


①：人及び機械が存在する
②：人及び機械が共存する（危険状態）
③：危険事象が発生する（hazardous event ）
④：傷害及び健康障害に至る場合がある（accident）
⑤：傷害及び健康障害に至らない場合がある（incident）
⑥：危害の発生確率とひどさの組合せがリスク

図 3.3　危害発生のプロセスの定義

② 同定

危険源の同定は、リスクアセスメントのステップの中でもっとも重要なステップである。これは、機械の通常運転中だけでなく、機械の製作、運搬、組立及び設置、検収、使用停止、分解及び安全上問題がある場合には廃棄処分のような機械の寿命上のすべての局面を考慮し、危険源から危害に至るシナリオを想定して、当該機械に付随するすべての危険源、危険状態及び危険事象を同定し、危険源リストを作成することが目的となる。また、危険源を同定する手法としては**図 3.4** のようなものがある。



手法の名称

- HAZOP(Hazard and operability study)
- FTA(Fault tree analysis)
- PHA(Preliminary hazard analysis)
- FMEA(Failure mode and effect analysis)
- FMECA(Failure modes, effects, and criticality analysis)
- MOP(Maintenance and operability study)
- CHAZOP(Computer hazard and operability study)
- HTA(Hierarchical task analysis)

図 3.4　危険源分析手法

表 3.4 に ISO 12100 で規定されている危険源を表す。危険源の例の詳細は ISO 14121 の附属書を参照されたい。

表 3.4　ISO 12100 で規定されている危険源

危険源	危険源の具体例
機械的危険源	可動する機械と直接人が接する、機械や装置に巻き込まれる、又ははさまれるなど、機械の動きが要因となり危害を生じる可能性がある危険源。 （例）：・ 機械又はその部分の回転運動 ・ スライド運動 ・ 往復運動 ・ これらの組合せ
電気的危険源	電気に起因して危害が生じる可能性がある危険源 （例）： ・直接接触 ・間接接触 ・充電部への人の接近 ・合理的に予見可能な使用条件下の不適切な絶縁 ・帯電部への人の接触等による静電気現象 ・熱放射 ・短絡もしくは過負荷に起因する化学影響のような又は溶解物の放出のような現象
熱的危険源	人間が接触する表面の異常な温度（高低）が要因となり危害が生じる可能性がある機権限 （例）：・極端な温度の物体又は材料との接触による ・火炎または爆発及び熱源からの放射熱 ・高温作業環境又は低温作業環境
騒音による危険源	機械から発生する騒音が要因となり、危害を生じる可能性がある危険源
振動による危険源	長い時間の低振幅または短い時間の強烈な振幅が要因となり危害を生じる可能性がある危険源

危険源	危険源の具体例
放射による危険源	次のような種類の放射が要因となり危害が生じる危険源。短時間で影響が現れる場合もあれば、又は長期間を経て影響が現れる場合もある （例）：・電磁フィールド（例えば、低周波、ラジオ周波数、マイクロ波域における） ・赤外線、可視光線、紫外線 ・レーザー放射 ・X 線及びγ線 ・α線、β線、電子ビーム又はイオンビーム、中性子
材料及び物質による危険源	機械の運転に関連した材料や汚染物、又は機械から放出される材料、製品、汚染物と接触することにより危害が生じる可能性がある危険源 （例）：・有害性、毒性、腐食性、はい（胚）子奇形発生体、発がん（癌）性、変異誘発性及び刺激性などをもつ流体、ガス、ミスト、煙、繊維、粉じん、並びにエアゾルを吸飲すること、皮膚、目及び粘膜に接触すること又は吸入すること ・生物（例えば、かび）及び微生物（ウイルスまたは細菌）
機械設計時における人間工学原則の無視による危険源	機械の性質と人間の能力のミスマッチから危害が生じる可能性がある危険源 ・不自然な姿勢、過剰又は繰り返しの負担による生理的影響（例えば、筋・骨格障害） ・機械の“意図する使用“の制限内で運転監視又は保全する場合に生じる精神的過大若しくは過小負担、又はストレスによる心理・生理的な影響 ・ヒューマンエラー
滑り、つまずき及び墜落の危険源	床面や通路、手すりなどの不適切な状態、設定、設置により生じる可能性がある危険源
危険源の組合せ	上に揚げた危険源がさまざまに組み合わされることにより生じる可能性がある危険源。個々には取るに足らないと思われても、重大な結果を生じるおそれがある。

3.2.2　リスクの見積もり

危険源の同定の後は、個々の危険源についてリスクの大きさを見積もる必要がある。見積もりの際には、危害のひどさ、危害の発生確率の二つの要素を考慮する（**図 3.5** 参照）。また同時に、リスクの見積もりの際には、**表 3.5** に示す側面にも、配慮する必要がある。

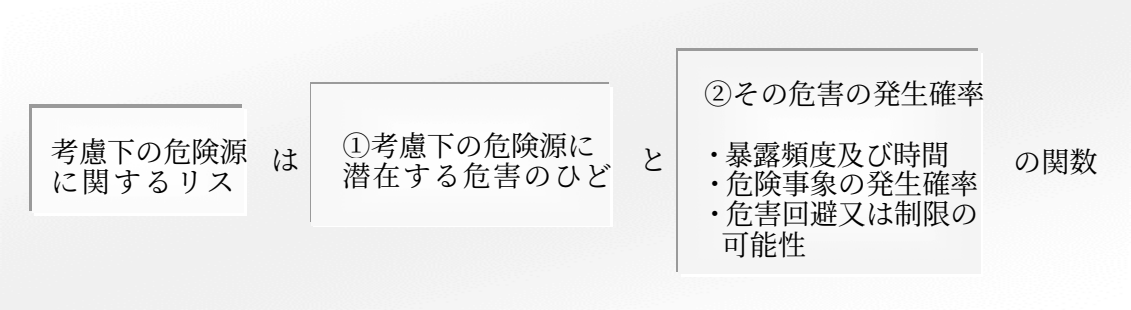


図 3.5　危険源によるリスクと、発生し得る危害との相関関係

①は、ある危険源が顕在化したときに、人が被る危害の程度を意味している。例えば、一人死亡するのか、あるいは腕や手がなくなってしまうのか、脚が動かなくなるか、またはかすり傷程度で済むものなのかなどである。

②は、危害の起こる頻度を意味しており、例えば、その危害は 100 年に 1 回起こるか、10 年に 1 回起こるのか、あるいは 1 年に 1 回起こるものなのかなどを意味している。この危害の発生確率を見積もるためには、暴露の頻度、危険事象の発生確率、危害回避又は制限の可能性の 3 要素を考慮することが必要とされる。

暴露の頻度とは、ある危険な状態に人がさらされる回数と時間のことであり、さらされる回数とは、1 時間に 1 回か、8 時間に 1 回か、10 日に 1 回か、あるいは全くさらされることはないのかということを意味しており、さらされる時間とは、瞬間的か数十秒程度、数分程度の比較的短時間か、あるいは数時間、数ヶ月、数年間など長期にわたるものなのかということを意味している。

危険事象の発生確率とは、故障等により、実際に危害に至る出来事がどのくらいの頻度で起こるのか（危険側故障率）を意味している。

危害の回避の可能性とは、危険事象が発生した際、危害にいたらないように回避できる可能性をいい、危害にあう人が熟練者でなくても、その人の身体的能力により（俊敏性や反射的動作など）回避できる可能性もある。また、非常停止が有効な場合など危害を回避できる可能性がある。

表 3.5　危害のひどさ及び発生確率並びにその要件

		考慮すべき要件
①考慮下の危険源に潜在する危害のひどさ		①保護対象の性質（人、財産、環境） ②傷害または健康障害のひどさ（軽い、重い、死亡） ③危害の範囲（個別機械の場合、一人、複数）
②危害の発生確率	・危険源にさらされる頻度及び時間	①危険区域への接近の必要性 ②接近の性質 ③危険区域内での経過時間 ④接近者の数 ⑤接近の頻度
	・危険事象の発生確率	①信頼性及び他の統計データ ②事故履歴 ③健康障害履歴 ④リスク比較
	・危害回避又は制限の可能性	①誰が機械を運転するか ②危険事象の発生速度 ③リスクの認知 ④危害回避又は制限の人的可能性 ⑤実際の体験及び知識による

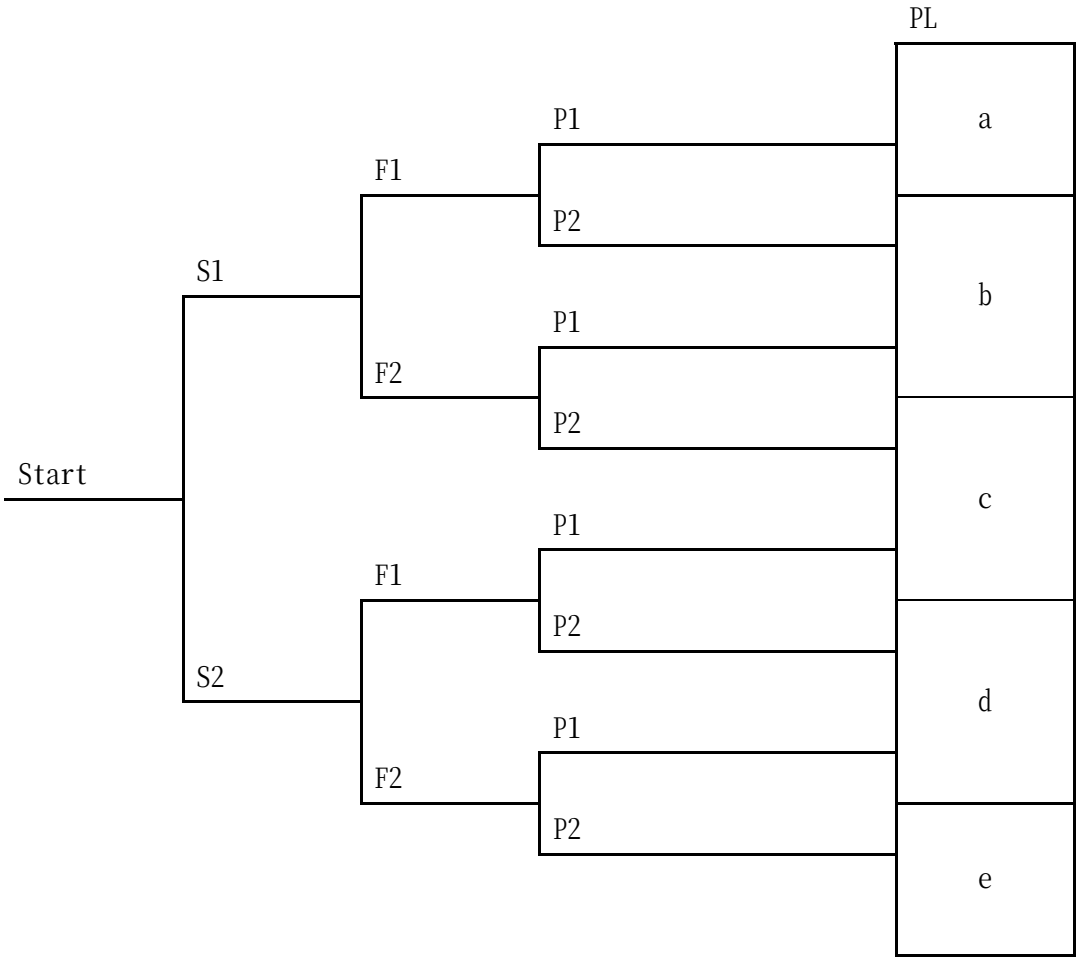
リスクの見積りには、いくつかのツールが利用可能であり、代表的なものを**表 3.6** に示す。危害の発生頻度と危害のひどさを定性的に見積る手法である。それぞれの要素の分類は 4 分類する場合や 6 分類する場合など任意である。

表 3.6　リスクマトリックス

頻度	被害のひどさ			
	無視可能 negligible	軽微な marginal	重大な critical	破局的な catastrophic
信じられない incredible	1	1	1	1
起こりそうにない improbable	1	1	2	2
あまり起こらない remote	1	2	2	3
たまに起こる occasional	2	2	3	4
かなり起こる probable	2	3	4	4
頻繁に起こる frequent	3	4	4	4

リスクの大きさ
1: 無視可能なリスク
2: 許容可能なリスク
3: 受け入れられないリスク
4: まったく受け入れられないリスク

図 3.6 で表されるような、ツリー形式で示される方法では、想定される危害のひどさ、危険源／危険事象／危険状態にふらされる頻度、回避の可能性などがリスクパラメータとなる。



危害の程度	危険源にさらされる頻度又は時間	危険源の回避可能性、又は危害を抑える可能性
S1：軽微	F1：まれから低頻度又はさらされる時間が短い	P1：ある条件では可能
S2：過酷	F2：高頻度から連続又はさらされる時間が長い	P2：ほとんど不可能

図 3.6　リスクグラフ

表 3.7　危害のひどさ（SS）のスコアリング

	危害のひどさ（SS）のスコア
致命的	SS ≧ 100
深刻	99 ≧ SS ≧ 90
中程度	89 ≧ SS ≧ 30
軽微	99 ≧ SS ≧ 0

表 3.8　危害の発生確率（PS）のスコアリング

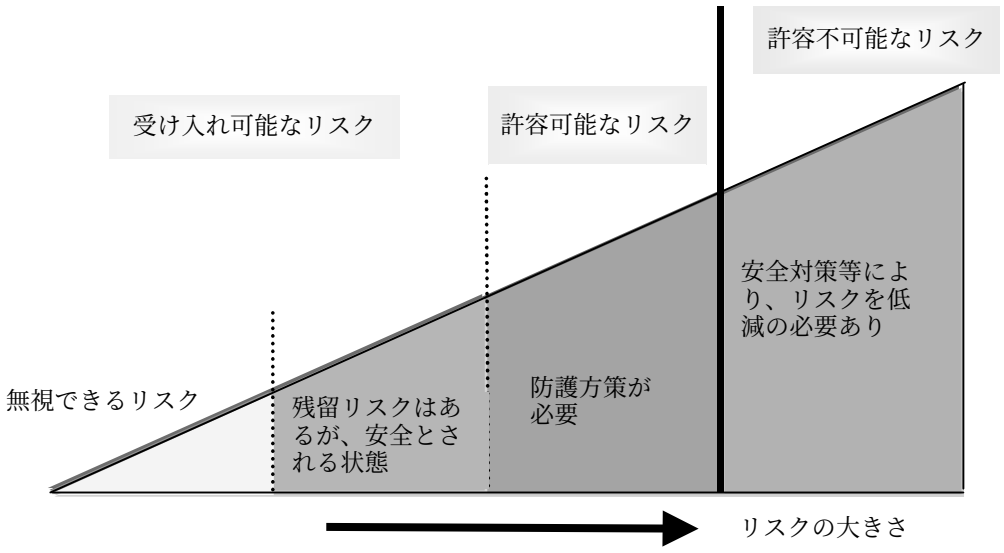
	危害の発生確率（PS）のスコア
確定的	PS ≧ 100
起こり得る	99 ≧ PS ≧ 70
起こりそうに無い	69 ≧ PS ≧ 30
起こり得ない	29 ≧ PS ≧ 0

表 3.9　リスクスコア（Score）

	リスクスコア（Score）
高	Score > 160
中	159 > Score > 120
低	119 > Score > 90
ネグリジブル	89 >Score > 0

前述のリスクマトリックスやリスクグラフと同様の方法であるが、リスクレベルを数字で表現する方法である。**表 3.7**、**表 3.8**、**表 3.9** のように危害の発生確率のスコアに危害のひどさのスコアを加算（あるいは乗算）し、出たリスクスコアによりリスクレベルを表す。危害の発生確率とひどさのパラメータは、定性的な判断により決定される。

3.2.3　リスク評価



受け入れ可能なリスク：Acceptable risk

図 3.7　許容可能なリスクと安全

リスクの評価は、リスク見積もりの後、許容可能リスクが達成されているかどうか、適切にリスクが低減されているかどうか、判断基準となるリスクレベルに基づいて、決定するために要求される。その評価の結果、許容可能リスクが達成されている、あるいはリスクが適切に低減されていればよいが、リスク低減が必要とされた場合には、適切な保護方策を選定し、リスクアセスメントの手順を反復しなければならない。(**図 3.7** 参照)

許容可能なリスクの定義（ISO/IEC Guide 51:1999）

→社会における現時点での評価に基づいた状況下で受け入れられるリスク

許容可能なリスクとは、ISO/IEC Guide51 では、上で示す定義に加え、このリスクを説明するために、「絶対的安全という理念、製品、プロセス又はサービスと使用者の利便性、目的適合性、費用対効果、並びに関連会社の慣習のように諸要因によって満たされるべき要件とのバランスで決定される」と説明している。つまり、許容可能なリスクは、統一的に、普遍的な一定の基準として決められるものではなく、限りなくリスクがゼロになることを目指し（絶対的安全)、製品などを使用する人の利便性、製品がその本来の使用目的と適合していること、費用対効果、ある社会の文化・慣習などのさまざまな要因によって決定されるものとしている。

3.2.4　リスク低減方策の決定

リスク評価の後、リスクが許容可能なレベル以下にない場合、ISO 12100 でいえば、適切にリスク低減がなされていない場合、許容可能レベル、適切なリスク低減を達成するために必要とされる方策を、リスク低減方策又は保護方策という。

ISO/IEC Guide51 では、保護方策を「リスクを低減するための手段」と定義しており、本質安全設計、保護装置、保護具、使用上及び据付け上の情報（設計者による方策）並びに追加保護方策、訓練、保護具、組織など（使用者による方策）による保護方策を指している。

ISO 12100 では、一般的に保護方策を「リスク低減を達成することを意図した方策」としており、設計者による方策と使用者による方策に分けている。設計者による方策は、「本質的安全設計方策」、「安全防護及び付加保護方策」、「使用上の情報」であり、使用者による方策は、「組織による安全作業手順、監督、作業許可システム」、「追加安全防護物の準備及び使用」、「保護具の使用」、「訓練」などとなっている。

3.2.5　リスクアセスメントの記録

図 3.2 には表していないが、リスクアセスメントの重要な構成要素として、リスクアセスメント結果の記録が定義されている。その内容については以下のものを含むことが重要である。

使用したツール、方法

(1) 評価した機械類、関連して想定した仮定

(2) 同定した危険源並びに危険状態、及び査定時に考察した危険事象

(3) リスクアセスメントの際に用いた情報（使用したデータ及びデータ源、使用データに付随する不明確さ、及び影響力）

(4) 保護法策によって達成される目標

(5) 同定した危険源の除去、又はリスク低減のために実施した保護方策

(6) 機械類に付随する残留リスク

(7) リスクアセスメントの評価結果

3.3 本章のまとめ

本章では、次のような事項について解説した。

1） リスク管理

2) スクアセスメント

・リスク分析

・リスクの見積り

・リスクの評価

・リスク低減方策の決定

・リスクアセスメントの記録

リスク管理とリスクアセスメントは製品の安全設計を行う上で非常に重要なステップである。「リスクアセスメント」については、具体的方法論を、**表 3.9** に一覧掲載した。また、第 4 章では、「実際にリスクを低減する方策」として 3 ステップメソッドについて述べる。

表 3.9　リスクアセスメント手法一覧

No	手法	主な適用分野	目的	概要
1	FTA（Fault Tree Analysis）	プロセスプラント 原子力 航空宇宙産業 電子産業 等	発生原因特定 発生確率算定	システムの特定故障を想定して、その発生原因を上位レベルから下位レベルまで論理的に展開し、最下位レベルのシステムの機能の故障発生率からシステムの特定故障の発生原因や発生確率を求める方法である。
2	ETA（Event Tree Analysis）	プロセスプラント 原子力 航空宇宙産業 電子産業 等	結果事象特定	ある初期事象からスタートして、いろいろな経路をとることにより結果がどうなるかを明らかにする手法である。
3	TBQ（Taxonomy-Based Risk Identification Questionnaire）	ソフトウェア開発	リスク特定	リスクをクラス、要素、属性の三つのレベルに分類する。リスクの同種側面の集まりを「クラス」、それを構成するものを「要素」、要素に属する性質を「属性」といい、この属性に関するチェックリスト作成する手法である。元々はソフトウェア開発のリスクを特定するために開発された。

No	手法	主な適用分野	目的	概要
4	HAZOP（Hazard and perability Studies）	化学プロセス	発生原因特定 結果事象特定	リスクシナリオ分析手法の一つで、化学プロセスにおける複数の独立した事象が複雑に絡む故障を取り扱うために開発された手法。 特に設計仕様（例えば、温度、圧力、PH、攪拌、反応）から逸脱した運転を行なった際の、設計からのズレが発生する個所及びそこで発生するハザードとその原因を解析し、それぞれの原因から危険事象への進展を阻止するための防護機能と改善すべき対策を調査する手法として用いられる。 設計仕様を逸脱する運転状態になった場合に発生するハザードを確認し、その操作上の問題点を分析するためにガイドワードによって質問を設定し、その回答を求めていく。手順としては、プロセス系統図であるエンジニアリング・フローシートなどの分析のための必要な情報とデータ等を準備した上で各設計仕様の項目、ズレ、原因、ハザード、防護機能、対策などのマトリックス表を作成する。系統的に危険なシナリオが把握しやすい。

No	手法	主な適用分野	目的	概要
5	PHA（Preliminary Hazard Analysis）	製品設計 プロセス設計 施設設計 等	事象発生可能性特定 被害の程度の定性的な評価 可能な改善措置の特定	これまでのハザードまたは故障の経験、知識を、将来、危害やハザードを招くおそれのある事象の特定を行い、さらに現時点で与えられている生産活動、施設、製品、システムの条件下でそれらが発生する可能性を特定する手法である。PHA は開発プロジェクトの初期段階で、設計の詳細や操作手順について情報がほとんどない場合に一般的に用いられる。
6	FMEA（Failure Modes and Effects Analysis）	製品設計 マネジメントシステム	影響分析 対応策検証	製品及び製造プロセスについて故障モードによる影響を分析して製品やプロセスの問題を解決する手法である。製品設計においては製品を設計する上で安全性を確保することや信頼性を確保することであり、製品が使用される段階で製品の欠陥の検出や異常な状態などを検出することにある。FMEA を設計段階で適用すれば、システムの設計について信頼性ブロックを用いて設計の信頼性や安全性の問題を検討することにより、試作前の段階で設計変更点を明確にできる。

No	手法	主な適用分野	目的	概要
7	相対危険度評価法	プロセスプラント	危険度定量的評価	プロセスの持つ危険性について、指標値を用いて各種のプロセスプラントを相対的比較評価する定量的評価技法を総称して、米国化学技術者協会AIChE（American Institute of Chemical Engineers）では、Relative Ranking Techniquesと呼んでいる。 この手法の代表的なものが、Dow方式と呼ばれる手法であり、英国ICI社Mond方式、日本の労働省通達「化学プラントのセーフティ・アセスメントに係る指針」もこの分類に入る。 Dow方式は、米国のダウケミカル社で考案された方法で、プラントをユニットに分け、ユニット毎に火災爆発指数を用いて、相対的に危険度の評価を行うと共に、防災対策選定のガイド値としても使われる。

No	手法	主な適用分野	目的	概要
8	シミュレーション法	原子炉 気象予測 等	被害予測	モデルを作り、コンピュータを使って予測する。例えば気象予測の例では、ハリケーンの被害予測を、風速の増幅に大きな影響を与える火山地形図、地域独特の建築習慣などをデータ化し、ハリケーンの中心気圧や暴風圏、進路の変化による規模の変動と地域に与える影響などをシミュレートする例がある。

No	手法	主な適用分野	目的	概要
9	ブレーンストーミング法	汎用	リスク洗い出し	複数のメンバが自由にアイデアを出し合い、互いの発想の異質さを利用して、連想を行う事によってさらに多数のアイデアを生み出そうという集団思考法・発想法である。 1940 年前後にアメリカの広告業界で創案されたが、その狙いは""つまらないアイデアでも、ほかの出席者には別の素晴らしいアイデアをひらめかせるかもしれない""というもの。提唱者と言われる A.F.オズボーンは「討論参加者の 1 人がアイデアを出すと、彼はほとんど自動的に別のアイデアに対する創造力をかき立てる。それと同時に彼のアイデアは他の参加者全員の連想の電源を刺激する」と述べている。
10	シナリオライティング法	汎用	予測シナリオ策定	仮説に従い将来の定性的な情景を時間や分野を区別して予測を記述し、複数の代替案を作成する。 組織の外部環境に生じるさまざまな出来事を論理的に積み上げ、現在の状況から将来どのような状況が生まれるかを示すものである。 社会調査の手法としてアンケートやヒアリング情報と組み合わせて使う。
11	デルファイ法	汎用	リスク予測	米国の研究機関ランドコーポレーションが開発した、多くの専門家がそれぞれ独自に意見を出し合い、それを相互に参照し再び意見を出し合う、という作業を繰り返し行うことで、意見を収斂させ、未知の問題に対し確度の高い見通しを得るための方法。

No	手法	主な適用分野	目的	概要
12	パターン分類方式	汎用	影響の分類 脅威の分類	経営者や顧客への影響、脅威の大きさを分類する。脆弱性対策のガイドラインを定め、管理策が必要な脅威や弱点を分析する。
13	クロスセッション法	汎用	将来像予測	時間と空間を超え、似たような状況を探す。先行した指標を読む。対象を切断、輪切りにした状態で判断する。
14	コートニィ理論	汎用	リスクの定量化	1992 年英国のリチャード・コートニィにより提唱されたリスク分析手法である。 以下の算出式により、リスクを定量的に示す。 リスク＝脅威の発生頻度×被害の大きさ
15	GMITS（Guidelines for the Management for IT Security）	セキュリティ	リスクの定量化	ISO/IEC TR13335 が紹介しているセキュリティの分析手法である。 以下の算出式により、リスクを定量的に示す。 リスク＝資産価値×脅威×脆弱性
16	DISC PD 3000 方式	セキュリティ	リスクの定量化	GMITS の情報資産の範囲を IT から一般の情報資産にまで拡大したアプローチを取る。 管理基準をチェックリストとし、基準からの差異（GAP）に基づき脆弱性を分析する。 以下の算出式により、リスクを定量的に示す。 リスク＝資産価値×脅威×脆弱性
17	JRMS（JIPDEC Risk Analysis Method 2002）	セキュリティ	脆弱性認識	脆弱性分析をベースとし、ネットワークを前提とした情報環境を認識し、さらに情報リスクが経営の根幹を握るという局面も考慮した視点も手法に取り入れられている。**→次ページへ続く**

No	手法	主な適用分野	目的	概要
				組織の脆弱性を認識するには、関係者のリスク認識の度合いについて JRMS の質問項目を通して把握し、それにより現状を捉える。
18	CRAMM（CCTA Risk Analysis and Management Methodology）	セキュリティ	脆弱性認識	英国大蔵省（CCTA）と英国規格協会（BSI）が共同開発した資産の識別、資産評価を質的技法と量的技法を併用し、脅威、脆弱性を分析する。
19	ALE	セキュリティ	リスクの定量化	米国標準技術院（NIST）が推奨する定量的リスクアセスメントの手法であり、年間の予想損失額 ALE（Annual Loss Exposure）を求めることができる。 ALE＝F × I F：年間に損失が発生する予想頻度 I：１回あたりの予想損失額
20	定性的リスク分析	プロジェクトマネジメント	リスクの優先順位付け	識別したリスクに対するリスクの発生確率を考慮した優先順位付けを行う。 リスク発生時のプロジェクト目標に及ぼす影響だけでなく、コスト、スケジュール、スコープ、品質などのプロジェクトの制約条件に対するリスク許容度などの要因を査定する。
21	感度分析	プロジェクトマネジメント	リスクの定量化	どのリスクがプロジェクトに最も影響を与える可能性があるかを明らかにする。 他の全ての不確実な要素をベースライン値に固定した状態で、プロジェクトの個々の不確定要素が、検討対象となっている目標に与える影響の度合いを調べる。

No	手法	主な適用分野	目的	概要
22	デシジョン・ツリー分析	汎用	リスクの定量化	想定シナリオの発生確率とコストにより、どのアクションを講じるかの意思決定をする際に使用する。 「どのような意思決定が発生するか」、「意思決定項目の間に不確実要素はないか」を整理し、将来発生するシナリオの全体像を理解する。
23	R-Map	プロジェクトマネジメント	リスクの定量化	縦軸が「危険の発生頻度」、横軸が「危害の程度」のマトリクスを使用してリスクの大きさを表現、判断、評価して行く手法である。「危険の発生頻度」をより低く、「危害の程度」をより軽微にする対策を、対象とする事象に対して施すことによって、リスクが許容リスクの範囲領域内に軽減されていく経過を、対象事象のリスクの大きさを示すマトリクス上のセルの位置の移動として視覚的に追いながら機能安全性を評価して行くことができる。それにより対象事象（対象製品）を客観的な視点、使用者の視点からデザインして行くツールとなっている。
24	What-if	汎用	予測シナリオ策定	What-if は、評価チームのメンバーそれぞれの気付きにより、「ポンプが故障で停まったら」、「バルブが閉まったら」、「不純物が混入したら」といった異常の引き金事象を想定し、それが発生した際のプロセスへの影響の検討、安全策の妥当性を評価する手法です。

＊＊＊＊＊＊＊　**第 3 章注記**　＊＊＊＊＊＊＊＊

（*1）：TR Q 0008（ISO/IEC GUIDE 73:2002）とはリスクマネジメントシステムにおいて、使われる用語を統一するために作られた用語集です。この中では、リスクという用語の定義が、事象、発生確率、事象の結果の組み合わせと定義されており、不確実性を伴うインシデントのことをさし、マイナス因子だけではなく、プラスの因子もリスクに含むと定義されているのが特徴です。

参考文献（第 3 章）

注 1）　向殿政男監修、向殿政男、宮崎浩一共著「安全設計の基本概念」安全の国際規格第 1 巻 2007 年 5 月 21 日 日本規格協会発行

注 2）　向殿政男監修、向殿政男、宮崎浩一共著「機械安全」安全の国際規格第 2 巻 2007 年 6 月 25 日 日本規格協会発行

注 3）　向殿政男監修、井上洋一ほか著「制御システムの安全」安全の国際規格第 3 巻 2007 年 9 月 25 日 日本規格協会発行

注 4）　独立行政法人原子力安全基盤機構　規格基準部 成果報告書 2006 年度（平成 18 年度）「ディジタル安全保護系規制要件調査等」

http://www4.jnes.go.jp/katsudou/seika/2006/kikaku/07kihi-0005.pdf

第4章　安全設計の基本と3ステップメソッド

前章でリスクアセスメントに関して紹介したが、リスクアセスメントを実施した結果、リスクの低減が必要となった危険源に対して、リスク低減方策を検討し実施することになる。リスク低減方策としては、設計者が講じるものと使用者が講じるものがあるが、ここでは設計者が講じる方策について述べる。

設計者が講じるリスクを低減するための手法として、3 ステップメソッドがある。この方法論に関しては、ISO-12100／JIS-B 9700 に記載されている。

3 ステップメソッドは、設計の段階で事故が起きないように危険を排除する設計を行うための「本質的安全設計方策」、それでも十分低減できないリスクから人を保護するために、安全防護物や非常停止手段等によって保護を行うための「安全防護及び付加保護方策」、以上二つの方策を行ってもまだ残ってしまう残留リスクに関して、その情報を使用者に伝え、さらにリスクを低減させる方策としての「使用上の情報」の三つから成る。

また方策実施にあたっては優先順位があり、「本質的安全設計方策」をステップ 1、「安全防護及び付加保護方策」をステップ 2、「使用上の情報」をステップ 3 とすると、ステップ 1＞ステップ 2＞ステップ 3 の順となる。こうした安全設計のためのステップや考え方は、機器の組込みシステムを設計するうえでも重要である。

4.1 では、「本質的安全設計方策」として、設計上の各種処置方策を適切に選択することや、設計を工夫することで、危険源を除去し、またリスクを低減する方策について述べる。大きく分類すると制御手段と非制御手段による方策がある。制御手段による方策としては、制御システムで故障、不具合を生じないようにすることで、人に危害を生じる動作を防止する対策等について述べる。非制御手段による方策としては、危険な個所をなくす方策や、オペレータの精神的、肉体的疲労などを低減する方策について述べる。

4.2 では、「安全防護及び付加保護方策」として、ガードや保護装置によりリスクを低減する方策、非常停止などの付加的なリスク低減方策について述べる。ガードは危険な個所へ接近することを防止する方策で、保護装置は、機器の危険な動作を停止させる方策について述べる。

4.3 では、「使用上の情報」として、専門あるいは一般の使用者が安全かつ正しい使用を確実に行えるようにするため、残留リスクについて必要な情報を伝えることと、本来「本質的安全設計方策」、「安全防護、付加保護方策」を適切に使用すべきところに安易に「使用上の情報」で適用すべきではないことも含めて述べる。また、「使用上の情報」は、大きく三つに分類され、(1) 機器の状態変化や異常状態を知らせるための信号や警報装置、(2) 機器を正しく使用するために必要な表示等、(3) 機器の運転や保全等に必要とされる情報について述べる。

4.1 本質的安全設計方策

4.1.1 本質的安全設計とは

設計者による保護方策（3 ステップメソッド）の実施にあたり、最初に実行すべき最も重要な位置付けにあるのが本質的安全設計方策であり、IS012100-1:2003 3.19 の中で「ガード又は保護装置を使用しないで、機械の設計又は運転特性を変更することにより、危険源を除去する又は危険源に関連するリスクを低減する保護方策」と定義されている。これは大きく分けて次の二つの考え方に基づいている。(1)「設計の段階から各種処置方策を適切に選択することで、可能な限り危険源の生成を防止し、低減させること」と、(2)「作業員が危険区域内に入る必要性を可能な限り少なくすることで、人の危険源への暴露を制限すること」である（図 4.1 参照)。

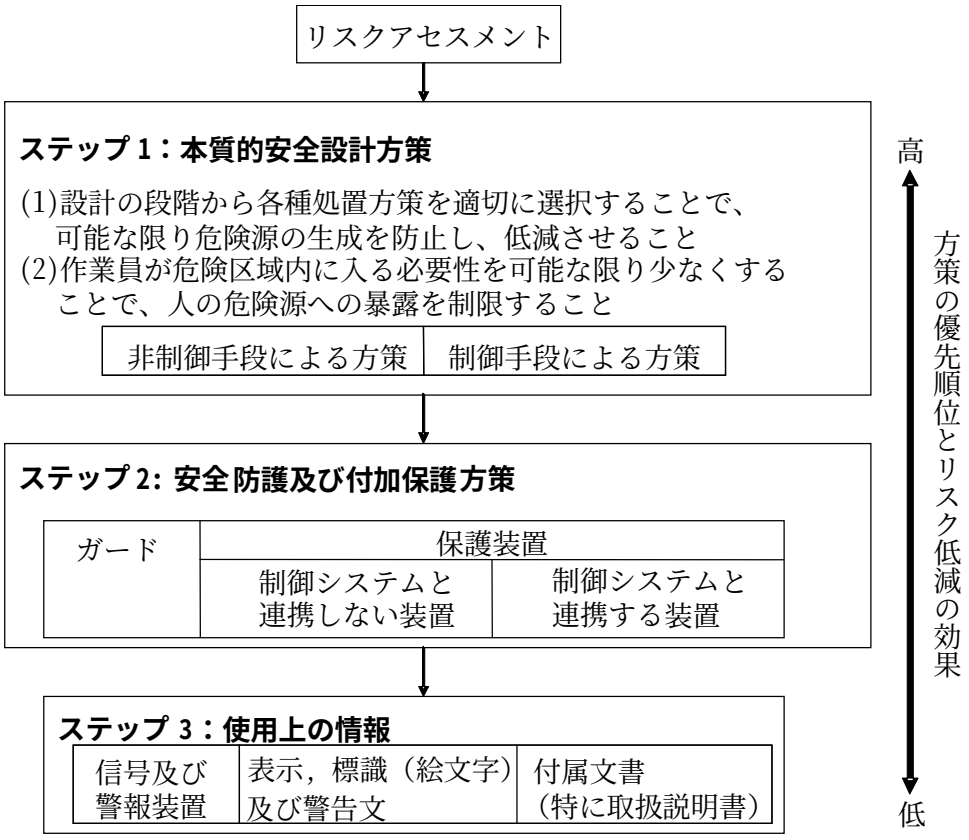


図 4.1　ISO 12100-2 で規定されるリスク低減方策（出典：安全の国際規格第二巻機械安全）

（1)「設計の段階から各種処置方策を適切に選択することで、可能な限り危険源の生成を防止し、低減させる」は、危害の要因を取り除く、あるいはその要因から生じる危害の程

度が小さくなるように設計処置を行うことである。そのための規定内容として、以下の事項などがある。

・幾何学的及び物理的要素に関する配慮
・機械設計に関する一般的技術知識の考慮
・機械的結合の安全原則
・人間工学原則の遵守
・制御システムへの本質的安全設計の適用
・安全機能の故障の確率の最小化
・空圧及び液圧設備の危険源の防止
・電気的危険源の防止

また、(2)「作業員が危険区域内に入る必要性を可能な限り少なくすることで、人の危険源への暴露を制限する」は、危険なところには行かない、あるいは行く頻度を減らせば危害にあう確率が減るという考え方に基づく方策である。そのための規定内容として、以下の事項などがある。

・設備の信頼性を上げることにより修正等の介入の機会を制限する方法
・搬入または搬出作業を機械化及び自動化することにより危険な個所への接近を制限する方法
・設定（段取り等）及び保全の作業位置を危険区域外とすることにより危険な個所への接近を制限する方法

（1）の規定内容の中で非制御手段による方策としての「人間工学原則の遵守」と制御手段による方策としての「制御システムへの本質的安全設計の適用」の二つについて、簡単に紹介する。特に制御手段に基づく安全設計のための考え方は、組込み機器の制御関連システムを設計するうえでも重要である。

・「人間工学原則の遵守」

人間にミスはつきものであり、ミスを完全に無くすことはできない。そこで設計段階から人間の精神的、身体的ストレス及び緊張を低減するための方策を組み込んでおけば、ヒューマンエラーの多くの部分が回避できるものと思われる。IS012100-2:2003 4.8 の中には、オペレータの精神的、身体的ストレスや緊張を低減することで安全性を確保するための方法が規定されている。特に、人体部位の寸法、年齢、力の強さと姿勢の関係といった身体的特性，騒音レベルといった使用環境から始まって、オペレータと機械とのインターフェースに関する種々の心理的特性や設計時の検討項目に至るまで述べられている。例えば、

「オペレータの作業リズムを自動運転のサイクルに無理に合わせない」ように規定している。これは、オペレータ自身が危険源の原因となる可能性のあるものはいかに自動化による環境改善効果があるといっても行うべきではなく、オペレータの精神的ストレスを低減するための改善方策を優先すべきとして明記されている。組込み機器等で制御関連システムを設計する場合においても、こうした人間工学的観点からの方策は参考になると思われる。

・「制御システムへの本質的安全設計の適用」

制御システムは、機械安全の重要な位置づけとなっている。制御システムの設計に誤りや不適切な部分があったり、構成部品に故障が発生したり、動力源が変動・故障したりすると、以下の事項などが生じて、危害が人間に及ぶ可能性がある。そうしたことを踏まえ、組込み機器の制御関連システムを設計するにあたっても重要である。

① 意図しない・予期しない機械の起動
事例：動力復帰後にオフラインから運転モードや保全のためのテストモードに切替えた際、プログラムミス等で本来動作しないはずの機械が起動してしまう場合。
② 無制御状態の速度変化
事例：制御システムが不能となり回転数速度が制御できず回転数が上昇（下降）してしまう場合。
③ 運動部分の停止不能
事例：運動部分の制御システムが不能となり、停止できなくなる場合。
④ 加工物等の落下や放出
事例：上記同様に加工物等を固定している制御システムが不能となり、固定できなくなる場合。
⑤ 保護（安全）装置の機能停止
事例：制御設計の誤りで安全装置が機能しなくなる状態が存在する場合。

これらを防止するための制御設計上の安全原則として、IS012100-2 では主として、以下の事項などが規定されている。

① 機構運動の起動または停止
事例：起動時は電圧（エネルギーレベル）が低い方から高い方に切替えることで起動し、停止時は電圧が高い方から低いほう方に切替えることで停止するように設計する。
② 動力中断後の再起動防止
事例：動力中断後に再起動すると機械が自動的に再起動し、危険源になるため、例えば自己保持のリレーを使用する等の設計をする。

③ 動力供給の中断

事例：安全のために常時運転を必要とする装置（例えば、ロックシステム、パワーステアリング等）は安全を維持するための装置を備える設計とする。

④ 自動監視の使用

事例：安全に稼動しているかを監視システムで常時監視し、異常を検知する設計とする。

⑤ 手動制御器の安全原則

事例：

・人間工学の原則に従って設計しているか。

・停止制御装置は起動制御装置の近くに配置されているか。

・一つの機械を複数の制御器で起動できる場合は、稼動時はそのうちの一つが有効となるような制御設計になっているか。

・無線通信による制御の場合は、制御信号が受信されない場合は自動停止となる設計となっているか。

⑥ 制御モード及び運転モードの選択

事例：人によるマニュアル運転、システムによる自動運転といったモードが存在するような制御機器では、安全のためにモード切替え装置を備える設計とする。

こうした制御設計上の安全原則を基に制御システムの安全関連部の設計（**図 4.2** 参照）にあたっては、概略以下の 5 ステップに従って行う。

ステップ 1：危険源分析、リスクアセスメント

IS012100-1 及び IS014121 に基づいてリスクアセスメントを行う。

ステップ 2：リスク低減方策の決定

ステップ 1 の結果に基づいて、リスク低減の方策を決定する。リスク低減の方策が制御システムによる方策か非制御手段による方策のいずれが適しているかを決定する。

ステップ 3：安全要求事項の特定

制御システムに備えるべき安全機能特性（設計原則、人間工学原則、停止機能等）を選択する。

ステップ 4：制御システムの安全関連部の設計

ステップ 3 の要求事項に適合するように制御システムの安全関連部を設計する。

ステップ 5：達成された機能及びカテゴリの妥当性確認

達成された安全機能等が、ステップ 3 で作成した安全要求事項に適合しているか検証する。

カテゴリとは IS0 13849-1 の規定によると、不具合（障害）に対する抵抗性（フォールト・レジスタンス）及び不具合（障害）条件下の挙動に関する制御システムの安全関連部の分類を意味する。なおフォールト・レジスタンスとは、たとえ不具合（障害）が起きても安全機能に限っては維持する能力のことである。

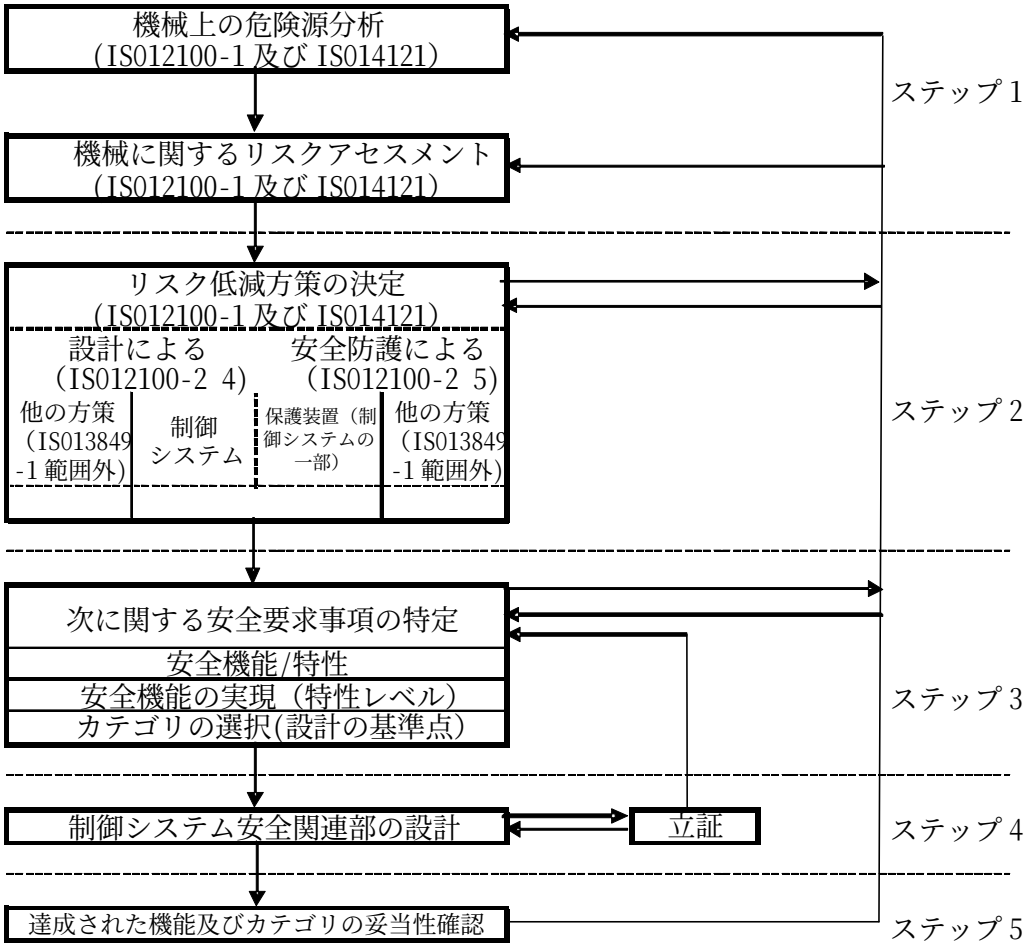


図 4.2　ISO 13849-1 での制御システムの安全関連部の設計プロセス（JIS B 9705-1:2000 図 1）

4.2 安全防護及び付加保護方策

4.2.1 安全防護とは

ガード及びセンサなどの保護装置は、安全防護と呼ばれ、IS012100-1:2003，3.20 の中で「本質的安全設計方策によって合理的に除去できない危険源、または十分に低減できないリスクから人を保護するための安全防護物の使用による保護法策」と定義されている。

さらに追加設備（例えば、非常停止設備）を含む付加保護方策を使用しなければならない場合もある（IS012100-1:2003，5.4)。

また、安全防護物は、IS012100-1:2003，3.24 の中で「ガード又は保護装置」と定義されている。ガードは保護するために機械の一部として設計された物理的な障壁であり、固定式ガードや可動式ガードなどがある。保護装置は、人の侵入や存在を検知するセンサ、インターロック装置などの制御装置やくさび、車止めといったものであり、制御システムと連携する装置としない装置に分類される。制御システムと連携する装置は、インターロック装置、両手操作制御装置やイネーブル装置等であり、侵入・存在検知装置としては、危険区域への人の侵入と存在を検知するライト（光）カーテンや圧力マット等がある。以下に上記保護装置の概要と事例を示す。

装置概要と事例：

・インターロック装置：

危険な運転状態となることを防ぐことを目的とした機械式､電気式等の装置である。代表的なものとして制御式インターロックと動力式インターロックがある｡制御式は、インターロック装置からの停止信号を機械側の制御システムで受けて、機械のアクチュエータへのエネルギー供給を中断するかアクチュエータと稼動部を切り離すことで機械の稼動を止めるものである。動力式は、インターロック装置からの停止命令により機械のアクチュエータへのエネルギー供給を直接遮断するかアクチュエータと稼動部を切り離すことで機械の稼動を止めるものである。リミットスイッチやキースイッチ等のスイッチを利用してインターロック装置を構成しているものが多い。

・両手操作制御装置：

例えば危険な装置を操作するその人のための保護手段となるものであり、危険な機械に対し起動開始命令を出し、かつ維持するために、両手で同時にスイッチを押す等の同時操作を少なくとも必要とする制御装置。

・イネーブル装置：

機械の危険な動きを制御するための手動制御操作装置であり、継続的に運転した場

合に、機械を運転可能とする装置。例えば 2 ポジション型の場合、ボタンを押していないと機械の駆動部は起動しない。ボタンを押していると駆動部が起動するといったもの。

・ライト（光）カーテン：
　侵入禁止区域に人が侵入した際、危険区域の境界に設置したライトカーテンの光がさえぎられたことを検出して機械に停止信号を送信する保護装置。

・圧力マット：
　圧力を検出するセンサから成り、人などがその上に立つと危険な駆動部を停止させる保護装置。

各種のガード及び保護装置は，IS012100-1:2003,3.25 及び 3.26 に定義されている。ある種の安全防護物は、数種の危険源への暴露を回避するために使用してもよく、例えば、機械的危険源が存在する区域に接近することを防止するための固定式ガードは、騒音レベルの低減またはエミッション（騒音、振動、危険物質など）の回収にも使用することができる。

4.2.2　付加保護方策とは

機械の「意図する使用」及び合理的に予見可能な機械の誤使用によって必要なとき、本質安全設計方策でなく、安全防護でもなく、使用上の情報でもない保護法策を付加保護法策という。特に非常停止に関しては、組込み機器のシステム設計においても考慮すべきである。
付加保護法策とは下記が規定される。

(1) 非常停止

危険になったプロセスまたは運動を停止させる非常動作の方策であり、組込み機器のシステム設計においても考慮すべき重要事項である。
人が異常に気づき、非常停止装置を押すと非常停止動作を開始し、停止状態となる。その後、リセット信号が入力されるまで停止状態が維持される（**図 4.3** 参照）。
また、非常停止はすべての機能の中で最優先されるものであり、非常停止信号がリセットされるまでその機能を持続しないといけないものである。

非常停止機能を下記する。

・ 非常停止機能は、機械のすべての運転モードよりも優先される。
・ リセットされるまで他のすべての起動信号も有効になってはならない。
・ 他の安全機能の代替手段として用いてはならない。
・ 非常停止機能は、他の保護装置または他の安全機能を持つ装置の有効性を損なってはならない。
・ 非常停止装置の動作後、非常停止機能は別の危険を発生させることなしに安全に機能を停止させるものである。

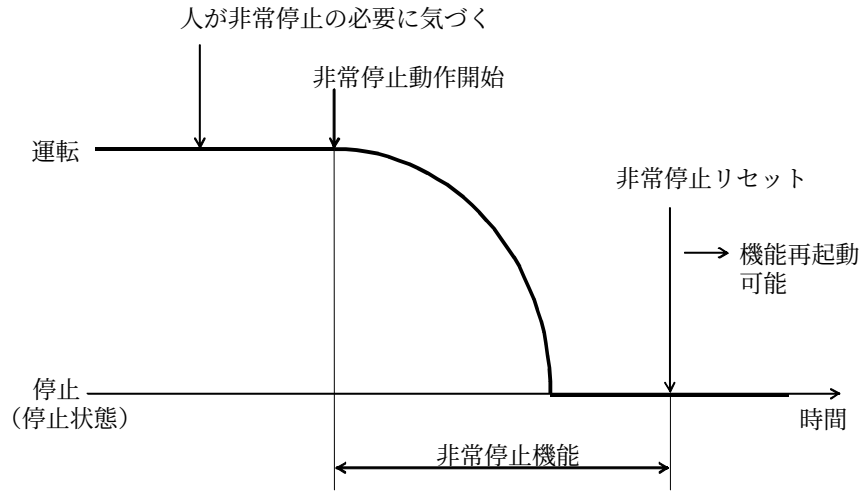


図 4.3 非常停止機能（JIS B 9703:2000 図 1）

(2) 捕捉された遮断及びエネルギーの消散に関する方策

危険区域内で作業を行う場合の安全確保のために、予期しない起動の発生を防止する必要があり、以下の装置を用いた方策がある。

① 動力源の遮断装置
② 蓄熱エネルギーの消散または制限装置

(3) 人の脱出及び救助のための方策

脱出及び救助のための方策としては、以下の事項などがある。

① オペレータが捕捉される危険源を生じる設備での脱出ルート及び避難場所
② 非常停止後に特定の要素を手で動かすための手段
③ 特定の要素を逆転させるための手段

④ 下へ降りる装置をつなぎ止めるための係留具
⑤ 捕捉された人が救助を求めることができる伝達の手段

(4) 機械及び重量構成部品の容易、かつ安全な取り扱いに関する準備

手で移動または運搬ができない機械やその構成部品については、つり上げ装置による運搬のための適切な付属用具を備えておくか、または付属用具を取り付けることができるようにする方策。

(5) 機械類への安全な接近に関する方策

機械類への安全な接近に関する方策としては、以下の事項などがある。

① 運転や保全などの作業を地上レベルで行えない場合の方策として、プラットフォームや階段などを設置する。
② 機械類の高所へ接近するための手段としての階段やはしごには、ガードレール等を設置する。
③ 歩行区域に関する要求事項として、作業時にすべらないような材料で歩行面を製作する。

4.3 使用上の情報

4.3.1 使用上の情報とは

使用上の情報は、専門・一般の使用者に、安全でかつ正しい使用を確実にするためのものである。そのための必要な情報を与えるために、文章、語句、標識、信号、記号、図表またはそれらの組合せによる伝達手段で構成される。

使用者に使用上の正しい情報を伝えることは、3 ステップメソッドの 3 ステップ目に位置づけられる事項である。ステップ 1、ステップ 2 の方策の実施ではリスクが除去、低減されない場合の最終手段である。したがって、機構設計での安全の作り込みを行わず安易に情報の提供に頼ることは望ましくないし、他の保護方策のように方策自体でリスクを除去、低減できるものではない。ただし多くの場合、本質安全設計や安全防護を行ってもどうしても残ってしまうリスクがあるので、これらを適切に伝えることは、機器が安全に使用されるために重要なことである。組込み機器のシステムにおいても機器が安全に使用されるという観点で考慮すべき事項である。

使用上の情報は、次の 2 タイプに分類される。

(1) 信号及び警報装置

危険であることを警告するために使用される視覚信号（点滅灯等）及び聴覚信号（サイレン等）といったもの。

① 危険事象が発生する前に発せられること。
② 曖昧な警告でないこと。
③ 明確に知覚でき、他の信号と識別できること。

(2) 表示、標識（絵文字)、警告文

機器等を明確に識別するために要求されるもの。

① 製造業社の名前及び住所。
② シリーズ名または型式名。
③ 製造番号。
④ マーキング。
⑤ 文字での表示等。

(3) 付属文書（取扱い説明書）

機器等の取扱いにあたって必要とされる提供すべき情報。

① 機械の運搬、取扱い、保管に関する情報。
② 機械の設置及び立ち上げに関する情報。
③ 機械自体に関する情報等。
④ 機械の使用に関する情報。
⑤ 保全に関する情報。
⑥ 使用停止、分解、及び廃棄処分に関する情報。
⑦ 非常事態に関する情報。

4.4 本章のまとめ

設計者が講じるリスクを低減するための手法として、3 ステップメソッドがある。

3 ステップメソッドとは下記の 3 ステップである。こうした安全設計のためのステップや考え方は、機械類の組込みシステム（特に、組込み機器で用いられる制御関連システム等）を設計するうえでも同様で重要である。

①ステップ 1「本質的安全設計方策」: 設計の段階で事故が起きないように危険を排除する設計を行うための方策

②ステップ 2「安全防護及び付加保護方策」: ①でも十分低減できないリスクから人を保護するために、安全防護物や非常停止手段等によって保護を行うための方策

③ステップ 3「使用上の情報」: ①、②の二つの方策を行ってもまだ残ってしまう残留リスクに関して、その情報を使用者に伝え、さらにリスクを低減させる方策

また方策実施にあたっては優先順位があり、ステップ 1＞ステップ 2＞ステップ 3 の順とする。

参考文献（第 4 章）

注 1)（財）日本規格協会編、向殿政男監修、宮崎浩一、向殿政男共著、安全の国際規格第二巻、機械安全、2007 年 6 月

注 2） JIS B 9700-1;2004 機械類の安全性－設計のための基本概念,一般原則－第一部：基本用語，方法論

注 3） JIS B 9700-2;2004 機械類の安全性－設計のための基本概念,一般原則－第二部：技術原則

注 4） JIS B 9705-1:2000 機械類の安全性－制御システムの安全関連部－第一部:設計のための一般原則

注 5） ISO12100-1:2003 Safety of machinery-Basic concepts, general principles for design-Part1：Basic terminology, methodology

注 6） ISO12100-2:2003 Safety of machinery-Basic concepts, general principles for design-Part2：Technical principles

注 7） ISO14121:1999 Safety of machinery-Principles of risk assessment

第5章　機能安全ハードウェア設計手法概要

本章はIEC/CDV 61508-2:1998の内容を変更することなくJIS化した日本工業規格JIS C 0508-2:2000 の「電気・電子・プログラマブル電子安全関連系に対する要求事項」に基づいている。

この中で特にハードウェアに関係する部分―安全サイクル上ではフェーズ 9―を主体に述べる。以下JIS C 0508-2:2000を「規格書」という。なお、CDVとは「投票用委員会原案：Committee Draft for Voting」の意味である。また、以下の記述で、ハードウェアをHW、ソフトウェアをSWと略記する。

5.1 国際規格 IEC 61508 の概要

IEC 61508 規格の適用分野のうち、主に **IEC 61508** シリーズに記述される電気・電子プログラマブル電子（以下 E/E/PE という）安全関連系のハードウェア面から見た場合の機能安全について述べる。**IEC 61508** 規格は、全 7 部で構成され、ハードウェアに関しては**第 2 部 IEC 61508-2** の「**E/E/PE 安全関連系の要求事項**」と**第 6 部 IEC 61508-6** の「**第 2 部及び第 3 部の適用指針**」**附属書 A～B** に述べられている。本規格は、基本的には電気的／電子的／プログラマブル電子に基づくシステムを安全関連制御システムに適用する場合の枠組みを定めたもので、プロセス制御装置や鉄道など輸送設備等に適用される。IEC 61508 規格の適用事例は、**図 5.1** に示すように各種分野に拡大しつつある。

ただし、ISO 26262 は車載電子製品の機能安全規格であり、2008 年中に作成予定であったが、現時点ではまだ国際標準化に至っていない。

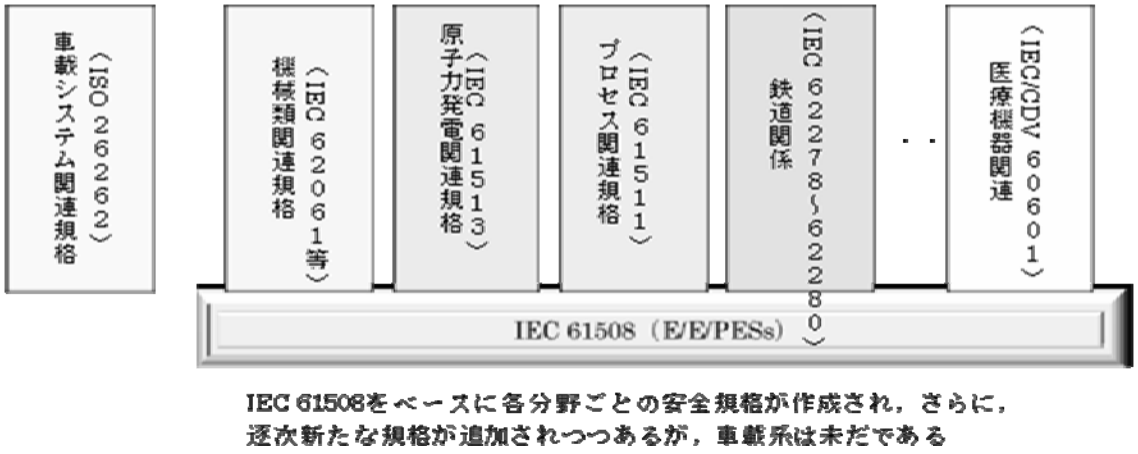


図 5.1　国際規格 IEC 61508 の適用例

5.2 IEC 61508 規格関連用語

規格書 IEC 61508-2 で使われる主な専門用語の説明を**表 5.1** にまとめてみた。

表 5.1　主な用語の説明

（参考：向殿政男監修「制御システムの安全」第 3 巻の表 4.5 及び表 4.6）

No.	日本語	英　語	説　明
1	故障	Failure	システムの障害・誤りによる指定性能からの逸脱。故障は事象であり、障害（状態を示す）の結果である
2	系統的故障	systematic failure	設計変更、製造工程、運転手順、文書変更によってのみ除去可能な決定的故障
3	偶発的 HW 故障	random hardware failure	HW の劣化による偶発的な故障
4	障害	fault	システムの誤りに至る異常状態で、偶発的または系統的である
5	系統的障害	systematic fault	システムの仕様、設計、製作、設置、運用、保守における本質的障害
6	偶発的障害	random fault	予知不可能な障害
7	安全サイクル	safety life cycle	設備の企画から廃棄までの安全確保作業の流れ図（図 6.3 はその一部）
8	フェーズ	phase	安全サイクル上のブロックに対応する諸活動で、必ずしも時系列で実施されない
9	安全機能	safety function	EUC を安全な状態に移行もしくは安全な状態に維持するために必要な機能
10	安全関連系[1]	safety-related systems	E/E/PE システムの安全に関わる部分
11	サブシステム	subsystem	センサやアクチュエータなど E/E/PE を構成する機能要素
12	ランダム故障	random failure	構成部品・機器などが多様な劣化のメカニズムのもとで時間的に無秩序に発生する故障

[1] 「安全関連系」は、「安全関連システム」ともいう。

No.	日本語	英　語	説　明
13	システマティック故障[2]	systematic failure（決定論的故障ともいう）	設計過程、製造過程、運転手順、文書化などに直接関わり、これらの中に故障原因が入り込むことで必然的に発生する故障
14	安全側故障	safe failure	安全関連系を危険状態、機能喪失状態にするような可能性を有しない故障
15	危険側故障	dangerous failure	安全関連系を危険方向すなわち故障状態にする可能性を持つ故障
16	整合性	integrity	情報が完全で、変更されていない状態
17	安全整合性	safety integrity	ある安全関連系が所定期間やすべての所定条件下で、要求される安全機能を果たす確率
18	HW 安全整合性	hardware safety integrity	安全整合性のうち危険側故障モードの偶発的 HW 故障部分
19	系統的安全整合性	systematic safety integrity	安全整合性のうち危険側故障モードの系統的故障部分
20	系統的故障整合性	systematic failure integrity	システムに同定の危険側誤りとその原因が不在であることの程度
21	偶発的故障整合性	random failure integrity	システムに危険側の偶発的障害が不在であることの程度
22	安全整合性水準	safety integrity level（SIL）[3]	安全関連系に特定される安全整合性要求事項の四つの水準、安全度水準ともいう
23	被制御設備	equipment under control（EUC）	製造、プロセス、輸送等の活動に用いられる設備
24	被制御設備制御系	EUC control system	プロセスやオペレータの入力信号に応答して EUC を望ましい方法で運転するための出力信号を生成するシステム。EUC の一部を構成し、入力装置や最終要素も含む

[2] JIS 規格では「システマティック故障」を、{決定論的故障} ともいう。
[3] 本章末に掲載のコラム２を参照。Safety integrity とは、safety な設計をする integrity があるということ。

No.	日本語	英　語	説　明
25	目標機能失敗尺度	target failure measure（TFM）	安全整合性要求事項で達成される**危険側故障モード**の発生確率で、以下の運用モードで決められ、**目標故障限度**ともいう -**低頻度作動要求モード**：作動要求当たりの設計機能実行に対する機能失敗平均確率 -**高頻度作動要求モード**：単位時間当たりの危険側故障発生確率
26	故障モードとその影響の解析	failure modes effects analysis（FMEA）	潜在的な故障・不具合の防止を目的としたボトムアップの体系的な分析手法
27	診断範囲（自己診断率）	diagnostic coverage（DC）	自動的診断試験により実現する危険側 HW 故障逓減率、**自己診断率**ともいう
28	論理系	logic system	論理機能を行うシステム内のセンサ及び最終要素（アクチェータ等）を除いた部分
29	安全側故障率比	safety failure fraction（SFF）	全故障率に対する安全側故障率と検出可能な危険側故障率の和の比率
30	プルーフテスト	proof test	安全関連系の故障状態を見つけるために実施される定期的な試験
31	妥当性確認	validation	仕様上の要求事項の審査・確認
32	検証	verification	要求事項の調査・確認
33	フォールト・トレランス	fault tolerance	障害または誤りの存在下で、要求される機能を遂行し続ける機能ユニットの能力

5.3 IEC 61508-2 における E/E/PE の安全関連系の要求事項

全 16 フェーズからなる**安全ライフサイクル**のうち、**フェーズ 9**(**E/P/PE 安全関連系実現**)は、E/E/PE 安全関連系の安全機能要求事項と **SIL** 要求値に適合することを要求している。このフェーズは、E/E/PES 安全関連系のハードウェアに対する安全ライフサイクルと、ソフトウェアに対する安全ライフサイクルから構成されているが、ここでは主に前者の要求事項について述べる。

5.3.1 E/E/PE 安全関連系の要求事項ライフサイクルの実現フェーズ

IEC 61508-2 の規定は、**IEC 61508-1** の一般的な要求事項に加えて、E/E/PE の主に HW について追加の要求事項を規定したもので、**安全ライフサイクル**上で適用するものである。

安全性要求事項仕様書はシステムを構成する要素と人との係り合い方を示す仕様書である。E/E/EP システムの安全性確保には、システムの設計段階でその方法を仕込む必要がある。この仕込みは、**IEC 61508** では安全計画書と呼ばれ、安全性要求事項仕様書は安全計画書の主要部をなす。ここで重要なのは安全ライフサイクルの実現フェーズ全体に渡って要求事項を確実にアウトプットに織り込むことである。　総合的な安全サイクルのうち安全機能の実現フェーズであるフェーズ 9 の詳細を**図 5.2** に示す。全体として、9.1～9.5 の五つのフェーズから構成され、E/E/PE システムの実現過程に当たる。各フェーズには安全要求事項及び先行フェーズの出力結果が入力情報として入力される。特に、9.4 の E/E/PE 統合フェーズには、設計結果のプログラマブルな HW・SW の統合及び統合テスト計画が引き渡される。

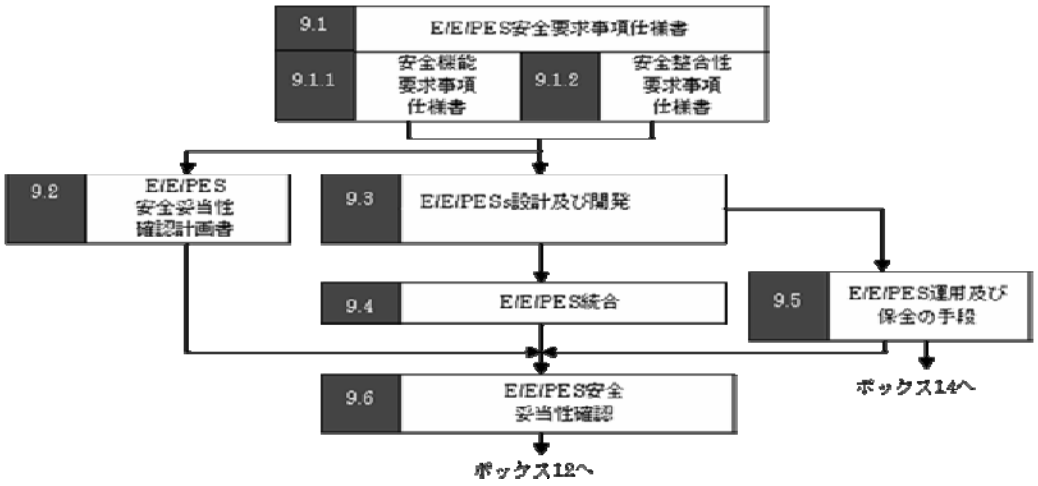


図 5.2　安全性ライフサイクル（参考：JIS C 0508-2:2002 図 2）

図 5.2 のうち、E/E/PE 安全関連系の 9.3 設計・開発フェーズは SW も含み、HW 部分と SW

部分に分けて詳細化したものが次の**図 5.3** である。なお、9.1 の E/E/PE 安全関連系の安全要求事項仕様書は、安全機能要求事項仕様書と安全整合性要求仕様書からなる。

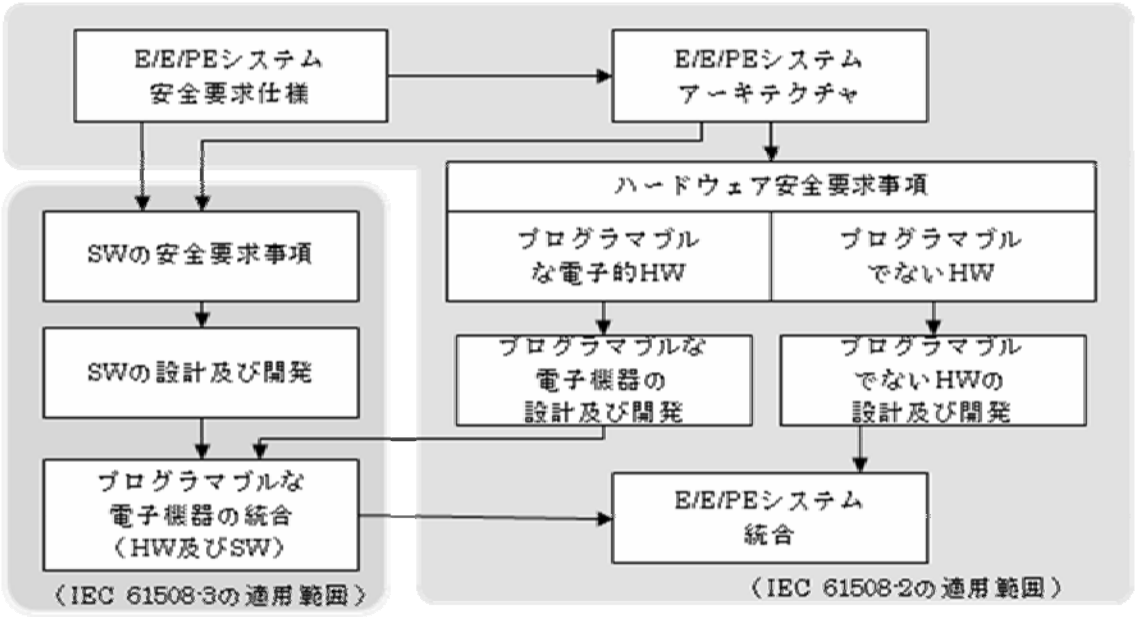


図 5.3　IEC 61508-2 と IEC 61508-3 の関係と適用範囲（参考：JIS C 0508-2:2000 図 3）

5.3.2　IEC 61508-2 E/E/PE 安全関連系の要求事項例

E/E/PE システムの安全要求事項仕様書と安全妥当性確認計画書、設計及び開発について安全ライフサイクルフェーズ上の要求事項の例を **IEC 61508-2** の条項に沿って**表 5.2**、**表 5.3**、**表 5.4** 及び**表 5.5** にまとめる。これらの表は、規格書の **7.2.3.1～7.7.2.7（pp.8～26）**に記述されているものを要約したもので、E/E/PE システムの安全機能に係る要求事項として包含すべきものを挙げてある。なお、表中の**白抜きの数字**は、**図 5.2 安全性ライフサイクルのボックス番号**である。

表 5.2　E/E/PE システム安全サイクル要求事項例（1）

（参考：向殿政男監修「制御システムの安全」第 3 巻 p.210 表 4.18）

9.1E/E/PE システム安全要求事項仕様書		
(A) 9.1.1 **安全機能要求事項仕様書への記入事項例（規格書 7.2.3.1）**	**(B) 9.1.2** **安全整合性要求事項仕様書への記入事項例（規格書 7.2.3.2）**	**（C）9.2** **E/E/PE システム安全妥当性確認計画書作成上の考慮事項例（規格書 7.3．2.2）**
a） E/E/PE システム安全関連系設計上の要求事項詳細、非制御設備（EUC）の安全性達成／維持方法 b） システムの処理速度 c ） E/E/PE システム安全関連系と運転員のインタフェース d） 機能安全に係るすべての情報 e） E/E/PE システム安全関連系ト他のシステムとのインタフェース f） EUC のすべての運転モード g） E/E/PE システム安全関連系の故障時の挙動や反応 h） HW/SW 間の相互作用・制約の文書化 i） E/E/PE システム安全関連サブシステムの最悪ケースの解析（タイミング、環境条件等） j） E/E/PE システム安全関連系の起動／再起動手順 k） 安全サイクルに遭遇しそうな環境条件の上下限 l） 運転中遭遇しそうな電磁現象	a） 安全機能に対する SIL b） 目標機能失敗尺度の運転モード等への適用 c） プルーフテストに対する要求事項、制約、機能、設備 d） 製造から運転、保守に至るまでの最悪環境状態 e） 電磁イミュニティ（EMI 電磁環境耐性）[4]の限界値は、電磁両立性[5]や SIL を考慮する **仕様書作成上の参考資料として附属書 B 表 1** E/E/PE システム安全要求仕様（pp.40）による適切な技術／手法を適用 **（規格書 7.2.3.3）**	a） EUC 関連のモード仕様 b） E/E/PE システム安全要求事項との照合 c） 各安全機能の実行証明に対する手順及び試験の合否基準 d） 各安全機能の安全整合性証明に対する手順及び試験の合否基準 e） 試験実施上の環境（ツール、校正を含む） f） 試験評価手順（要正当化） g）電磁イミュニティ（EMI）試験手順／性能基準 h） 故障解決指針と手順

[4]電磁雑音（電子機器が放射する電磁波ノイズ）に対する耐久度。EMI の強度が規制値を超えていた場合には、回路設計の工夫、電磁シールド板の採用、EMI フィルタの挿入、電波吸収シートの張り付けなど対策がとられる。EMI 規制の国際基準は、IEC の特別委員会である CISPR（国際無線障害特別委員会）が定めている。国・地域別では、米国の FCC（米国連邦通信委員会）や欧州の ETSI（欧州電機通信標準化機構）、日本の VCCI（情報処理装置等電波障害自主規制協議会）などが、それぞれ EMI 規制値を定めている。

[5] 電磁両立性とは、電磁的な耐性と不干渉性のことであり、不干渉性とは、電磁的な耐性により発生する電波や高周波電流を抑えることをいう。医療機器などには特に高い電磁両立性が求められる。安全関連系の電磁両立性に係る指針は、IEC 61000-1-2 ”電磁両立性（EMC）”第 1 部“一般―第 2 章の電気・電子系の機能安全の達成”に述べられている。

表 5.2 の（**A**）欄では、被制御設備（**EUC**：equipment under control）の安全性は、E/E/PE システム安全要求仕様に含まれるので、同欄内の a）はこれを、また b）以下は詳細例を記述している。

（**B**）欄では、安全機能に対する安全整合性水準、従って目標機能失敗尺度（目標故障限度）が示される。同欄の a）はこれを、b）以下は安全整合性水準決定の条件を表す。

（**C**）欄は、E／E／PE 安全関連系による安全性の妥当性確認を計画する。このフェーズは、通常 E／E／PE システムの設計及び開発に併行して実施され、（A）、（B）の実現結果に対する論証手順、試験、合否基準が不可欠となっている。

表 5.3　E/E/PE システム安全機能・安全度に係る要求事項例（2）

（参考：向殿政男監修「制御システムの安全」第 3 巻 p.211 表 4.19）

※（ ）内の数字は規格書の条項番号

9.3 E/E/PE システム設計と開発（規格書 7.4）		
（G）一般的要求事項（規格書 7.4.2）	**（Rf）　偶発的 HW 故障の抑制（規格書 7.4.3）**	**（Hf）　HW 機能失敗確率の推定（規格書 7.4.4）**
G1E/E/PE システム安全の設計は以下による a）E/E/PE システム安全要求仕様への準拠（規格書 7.4.2.1） b）安全機能と非安全機能の独立性[6]の達成方法とその正当性の文書化（規格書 7.4.2.2） **G2** 安全機能は非安全機能から分離することが望ましい（7.4.2.3） **G3** 異なる安全度水準の安全機能からの独立が証明できない場合、各構成要素は最高安全度水準として扱う	**Rf1** HW アーキテクチャ上の制約(HW の SIL の決定) **Rf2** HW 安全度に対して各サブシステムの構成方法、事故診断技法を選定する（個性方法、自己診断率、プルーフテスト間隔、診断試験間隔等の決定） **Rf3** しすてまてぃっく決定論的安全度に対して決定論的フォールトの制御方法を選定する **Rf4** 決定論的安全度に対して決定論的フォールトの回避技法を選定する	**Hf1** HW 機能失敗確率推定の手順 **Hf2** 構成方法のモデルを作成（規格書 7.4.4.2） a）E/E/PE システム安全機能の個別選定 b）サブシステムの要素（センサや最終要素）の特定（数、タイプ等） c）E/E/PE システム安全系のサブシステムと要素の関係と相互干渉について検討する **Hf3** E/E/PE システム安全関連系のパラメータを定める（7.4.4.3） a）E/E/PE システム安全系のサブシステムと要素における平均故障確率を決定する d）自動検出不可のフォールトについてのプルーフテスト間隔を定める e）検出可能フォールトの修理時間を定める

[6]独立しているとは、安全機能以外のいかなる不履行も安全に関連する機能に影響しないということである。履行上十分な独立性の証明は、安全関連部と非安全関連部の従属故障の確率が安全度水準に比べ十分小さいことで行われる。

（規格書 7.4.2.4） **G4** E/E/PE システム安全系の設計では、安全サイクル上で必要な技法／方策を文書化する（規格書 7.4.2.7） **G5** 安全度水準を満たす集合体に適用した技術／方法について文書化しておくこと （規格書 7.4.2.8）	**（Fa）故障回避（規格書 7.4.7）**	f） 自己診断率、自己診断テストの間隔を定める **Hf4** 目標安全度水準に適合させる（規格書 7.4.4.4） a） E/E/PE システム安全関連系に対する信頼性モデル（FTA 等）を作成する b） 信頼性予測結果と目標機能失敗尺度と比較する c） 標機能失敗尺度を達成しない場合、適用可能な改善手段を選定・履行 **Hf5** 自己診断率を次の原則で決定 a） 自己診断率のチェックや外部励起によるテスト等による達成 b） 自己診断の対象となるのは、すべてのサブシステムや要素 c） 自己診断試験を実施数部分は、フォールト検出後、EUC の復帰、故障サブシステムの切離し等を自動的に行う **Hf6** 自己診断理率の特定（7.4.4.6） a） フォールトモード影響解析の実施 b）フォールトモードが、安全側か危険側か分類する c） 安全側故障と危険側故障に相当する故障確率の比を求める d） 自己診断試験で検出されるフォールトモードを特定する e）検出された危険側故障率を総計する g） 検出された危険側故障率を全危険側故障率割ってサブシステムの自己診断率を
	Fa1 障害回避の技法／方策を規約書附属書 B 表 B2 に示す（7.4.7.1） **Fa2** 要求安全度水準に従った設計方法の選定（規格書 4.7.1.2） a） 明瞭性、モジュール性 b） 機能性、同時性等の明瞭かつ正確な表現 c） 情報の文書化と伝達 d） 適合及び妥当性の確認 **Fa3** 保全に関する要求事項の早期決定（7.4.7.3） **Fa4** 自動テスト手法、統合的開発手法の適用（7.4.7.4） **Fa5** 統合テスト計画の文書化（7.4.7.5） a）試験種と手順、 b）環境、手法、形態、計画表の策定 c）合否基準を定める	
	（Pt）プルーフテスト・自己診断試験（規格書 7.4.6）	

	設計にはプルーフテスト、自己診断試験を実施する手段を含むべき（規約書附属書 A 参照） プルーフテスト頻度、自己診断試験間隔、故障～修理の時間には次を含む複数の要因が関係する(規約書附属書 B 参照) a）目標機能失敗尺度 b）アーキテクチャ c）自己診断率	求める **Hf7** 解析のための情報（7.4.4.7） a） 自己診断試験の詳細な記述 b） E/E/PE システム安全系の詳細なブロックダイヤグラム c） HW サブシステムの HW 図 d） 70%以上の統計的信頼水準を有する部品（群）の故障確率 e） 要素（群）のフォールトモード・故障確率の全故障確率に占める割合（%）

表 5.4 E/E/PE システム安全機能・安全度に係る要求事項例（3）

※（ ）内の数字は規格書の条項番号

9.3 E/E/PE システム設計と開発**（規格書 7.4）**	
（Df）システマティック故障の抑制（規格書 7.4.8）	**（Ee） E/E/PE システム履行（規格書 7.4.9）**
Df1 次の事項に対する耐性を持つべき（規格書 7.4.8.1） a） HW における残存する設計フォールト（附属書 A 表 16 参照） b） 電磁環境を含む環境負荷（附属書 A 表 17 参照） c） EUC 運転員の誤り（附属書 A 表 18 参照） d） SW における残存する設計フォールト **Df2** 保守・試験は、設計、開発業務において検討される（7.4.8.2） **Df3** すべてのインタフェース設計は、人間工学に従うとともに、運転員の熟度や意識に適応する（7.4.8.3）	**Ee1** 設計は各サブシステムまたは部品への分解に基づく（規格書 7.4.9.1） **Ee2** 設計･開発業務において HW 及び SW の干渉については、同定・査定し、文書化する（7.4.9.2） **Ee3** E/E/PE システム安全関連系は、設計に従って履行されるべき（7.4.9.3） **Ee4** 附属書 A 表 1 は自己診断率達成のため検出すべきフォールト／故障を提示（7.4.9.4） **Ee5** すべてのサブシステム及び部品は安全関連の有無と次を宣言すべき（7.4.9.5） a) 新規／既存／独占特許品か b) 前もって正式に評価したことがあるか **Ee6** 既開発のサブシステム／部品を安全機能として

a） 運転員や保全要員による予見可能な過誤を防止・除去することは、設計上望ましい b） 運転員や保全要員によるある種の過誤は、E/E/PE システム安全関連系によって対処できないかもしれない	使う場合、同定・文書化すること。使用の正当化は、次に基づく（4.7.9.6） a） 類似の適用での満足できる運用の証明 b） 要求事項に適合することの例証 **Ee6** ディレーティング（設計余裕：JIS C 0508-7:1998 附属書 A の A.2.8 参照）[7]は、すべての E/E/PE システム要素に対して可能な限り使用すべき（7.4.9.6）

表 5.3 及び**表 5.4** は、ともにフェーズ 9.3 に相当するもので、E／E／PE 安全関連系に対して定められた安全機能及び安全度に係る要求事項に適合するように、当該安全関連系のハードウェアを設計し開発を行う。G、Rf、Hf、Fa、Pt、Df 及び Ee の各欄は、E／E／PE 安全関連系の設計・開発の詳細要求事項を示す。このフェーズでは多くの要求があり、そのすべてを説明できないため、以下に一部を紹介する。

- 設計の文書化
- 自己診断率、プルーフテスト間隔の決定
- **SIL** に応じた検出できない危険側故障の割合
- **FMEDA**（Failure Modes、Effects and Diagnostic Analysis）による故障解析

IEC 61508 規格の特徴として機器の故障は、**ランダムハードウェア故障**（random hardware failure）と**システマティック故障**（systematic failure）に分けられる。ランダムハードウェア故障は部品の劣化などによる偶発的な故障であり、**システマティック故障**はシステムの仕様や運用方法に起因する必然的な故障である。**ランダムハードウェア故障**に対しては故障確率によって定量的に、**システマティック故障**に対しては安全ライフサイクルに基づいた手順と文書化により定性的に対処する。

表 5.5 E/E/PE システムの統合、運用と保全、安全妥当性確認に係る要求事項例（4）

※（ ）内の数字は規格書の条項番号

E/E/PE システムの統合、運用と保全、安全妥当性確（規格書 7.5～7.7）		
（In） 9.4 統合（規格書 7.5）	**（Om） 9.5 運用と保全（規格書 7.6）**	**（Sv） 9.6 安全妥当性確認（規格書 7.7）**
In1 E/E/PE システム安全関連系は設計に従って統合、	**Om1** E/E/PE システムの運用・保全のために用意すべきも	**Sv1** E/E/PE システム安全関連系の安全に係る安全妥当性確認は、計画

[7] Derating:ディレーティングは、故障率を少なくするため定格より低い負荷で使用することで、信頼性設計の重要な要素である。安全余裕を与えて偶発的な過大ストレスによる故障の可能性を低減するという効果を持ち、信頼性の向上に寄与する。ディレーティングは他の要因 （主に大きさとコスト） とのトレードオフの関係にあることから、個々の部品の特性や製品に必要な信頼性を充分に理解したうえで、適切な判断を行なうことが必要。

テストすべき（7.5.2.1） **In2** 全モジュールが意図した通り設計されていることを示すこと（7.5.2.2） **In3** E/E/PE システムへの安全 SW の統合は、C-058-3:2000 の 7.5 に従う。(7.5.2.3) **In4** 統合テスト実施の文書化は、テスト結果及び設計・開発基準への合否を宣言する（7.5.2.4） **In5** テスト期間中のE/E/PEシステム安全関連系のすべての改修・改造を影響分析の対象とすべき（7.5.2.5） **In6** 統合テストにおける文書化（7.5.2.6） a） テスト仕様の説明 b） テストの合格基準 c） テスト対象の説明 d） 公正データ付装置・機器 e） テスト結果 f） 期待値と結果の不一致 g） 不一致の場合のテスト続行／改造要請かの解析と決定 **In7** 統合間のフォールト回避のための技法の選択（附属書 B 表 3 参照）（7.5.2.7）	の（7.6.2.1） a） 機能安全保持のための定常的業務 b） 不完全な状態の防止／被害軽減のための業務と制限 c） E/E/PE システム安全関連系の故障率と作動要求率の保持と文書化 d） 監査とテスト結果の保持と文書化 e） フォールト／故障発生時の保全手順 f） 保全実施の報告手順 g） 保全・再適合確認に必要なものとその保全手順 **Om2** 運用・保全手順の監査・テスト結果に基づく更新（7.6.2.2） **Om3** 定常的な保全業務は、次のような系統的な方法で決定すべき（7.6.2.3） a） フォールトツリーの検討 b） 故障影響分析 c） 信頼性規範の保全 **Om4** 運用・保全手順における EUC への影響度の評価（7.6.2.4） **Om5** フォールト／故障の回避のための技法群の選択（附属書 B 表 4 参照）（7.6.2.5）	に従い実施（7.7.2.1） **Sv2** すべてのテスト計測機器に対しても妥当性確認を実施（7.7.2.2） **Sv3** E/E/PE システムの安全機能、運用・保全手順は、テスト／解析によって妥当性確認を実施(7.7.2.3) **Sv4** 安全妥当性確認のためのテストについて次を文書化（7.7.2.4） a） 安全妥当性確認計画の説明 b） 要求事項及びテスト（解析）される安全機能の詳細な説明 c）校正データとともに使用する道具・機器 d） 各テスト結果 e） 予想と実際の不一致 **Sv5** 予想と結果の不一致を生じた安全妥当性確認のテストの文書化（7.7.2.5） a） 解析結果 b）テスト続行か改造要求を出してテスト開始段階に戻るかの決断 **Sv6** E/E/PE システムの供給者／開発者は、EUC（制御系）の開発側が安全妥当性確認テスト結果を利用出来るようにする（7.7.2.6） **Sv7**安全妥当性確認中のフォールト／故障の回避のための技法群の選択（附属書 B 表 5 参照）（7.7.2.7）

表 5.5 は安全ライフサイクルのフェーズ 9.4～9.6 に相当し、それぞれ In、Om、Sv の各欄において要求事項例を示す。

フェーズ 9.4 では、フェーズ 9.3 で定められた E／E／PE システム設計に従って統合し、また定められた統合テストに従って試験を行う。ここでは、統合テストの文書化が要求され、当該テスト結果及びフェーズ 9.3 設計・開発の目的と基準に適合しているかどうかを明示する必要がある。

フェーズ 9.5 では、E／E／PE 安全関連系に要求する機能安全が、運用と保全の期間中に保持されることを確実にするための手順を確立する。

フェーズ 9.6 では、E／E／PE 安全関連系が、要求する安全機能及び安全度について、安全要求事項に適合している妥当性を確認する。この安全妥当性確認は、フェーズ 9.2 であらかじめ準備した計画に従って実施する必要がある。

5.4 ハードウェア故障率評価の技法

5.4.1 故障率算定基準

機能安全は、本質安全と対比される用語で、安全機能によってリスクを許容リスク以下に軽減することにより安全を確保することである。**IEC 61508-2** が対象とする E/E/PE 安全関連系は、**図 5.4** に示すように、HW と SW からなる論理回路とセンサやアクチュエータなどのサブシステムから構成される。

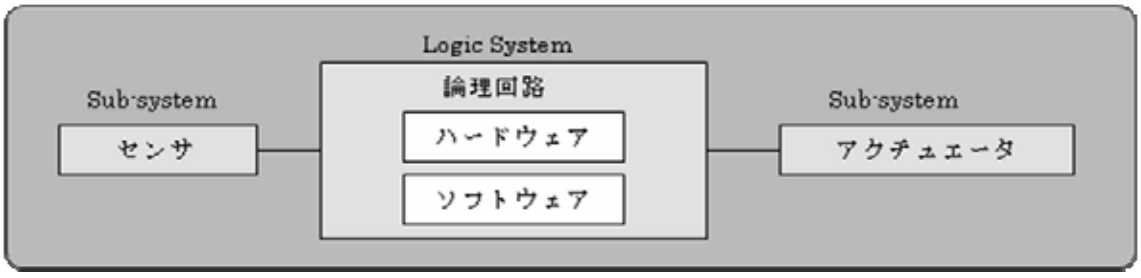


図 5.4　典型的な E/E/PE システム安全関連系の構成（参考：IEC/CDV 61508-2:1998Figure B.2）

論理回路は、プロセッサのほか走査装置が、センサ部分にはセンサのほか入力調整回路、アクチュエータ部分にはアクチュエータのほか出力調整回路等の最終要素が含まれる。

5.4.2 故障に対する SIL の割り当て

安全性ライフサイクルにおける**フェーズ 9**（E/E/PE システムの安全要求事項仕様書作成フェーズ）に先行する**フェーズ 5** では、**フェーズ 9** 以降で実現される E/E/PE システムに対して安全要求仕様に含まれる安全機能を割り当て、各安全機能に対して **SIL** を割り当てる。

許容リスクを表す指標が **SIL** であり、その四つのレベルに対して**表 5.6** に示すように、**低頻度作動要求モード**と**高頻度作動要求モード**（または**連続モード**）の 2 種類の運用モードにおける、**目標機能失敗尺度**[8]（**TFM**：target failure measure）が規定されている。これは E/E/PE 安全関連系の機能安全が IEC 61508 の要求事項に適合するかどうかの機能安全評価尺度[9]であり、運用モードにおける低頻度要求モードとは、作動要求が 1 年に 1 回以下程度、高頻度要求モードは、1 時間当たりや 1 日当たり何回も作動するということになる。例えば自動車の安全システムでは、低頻度作動要求モードがエアバッグに相当し、高頻度作動要求モードがブレーキに相当する。

表 5.6 の左欄に示す**低頻度作動要求モード**における**目標機能失敗尺度**は、作動要求があった際に安全関連部が動作しない確率（**機能失敗平均確率**）という意味である。また右欄の**高頻度作動要求モード**時の**目標機能失敗尺度**は、単位時間当たりの**危険側故障**の回数（**危険側故障確率**）となる。

表 5.6　E/E/PE 安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

（参考：JIS C 0508-1:1999 の PP.24 表 2 及び表 3、及び IPA・SEC 編「組込みシステムの安全性向上の勧め（機能安全編）」pp.55 の付表 2）

SIL	**低頻度作動要求モード運用時の TFM**（作動要求当たりの**機能失敗平均確率**）	**高頻度作動要求モード運用時の TFM**（単位時間当たりの**危険側故障確率**［1／時間］）
4	$10^{-5} \leqq TFM < 10^{-4}$	$10^{-9} \leqq TFM < 10^{-8}$
3	$10^{-4} \leqq TFM < 10^{-3}$	$10^{-8} \leqq TFM < 10^{-7}$
2	$10^{-3} \leqq TFM < 10^{-2}$	$10^{-7} \leqq TFM < 10^{-6}$
1	$10^{-2} \leqq TFM < 10^{-1}$	$10^{-6} \leqq TFM < 10^{-5}$

5.4.3　平均機能失敗確率の算定手順

表 5.6 の**低頻度作動要求モード**における**目標機能失敗尺度**を、低頻度作動要求時の機能失敗確率 **PFD**（Probability of Failure on Demand）と定義し、その平均値を PFD_{AVG} と表す。つまり PFD_{AVG} は、作動要求があったときに安全制御機能が作動しない平均確率（必要な時に働かないという危険側に倒れる平均確率）を意味する。

故障は**図 5.5** に示すように分類できるが、PFD_{AVG} を算出するために、各分類に従って、故障率（作動時間内に故障を起こす割合、故障数／作動時間）を図中に示したように定義する（λ_{SD}、λ_{SU}、λ_{DD}、λ_{DU}）。

[8]目標機能失敗尺度とは、安全度水準に係わる機能失敗尺度で、ハードウェアの安全度に関してだけ定量化可能。当該機能失敗尺度の妥当性評価において信頼性予測技術の適用が同意されている。決定論的原因安全度に係わる目標機能失敗尺度に適合するための必要な予防策に関しては、定性的な手法を用いて判断を行わなければならない。

[9] 機能安全尺度により、任命された 1 名以上の評価者が、IEC 61508 の要求事項に照らして「受容」「条件付き受容」「拒否」など判定することによって機能安全評価が行われる。

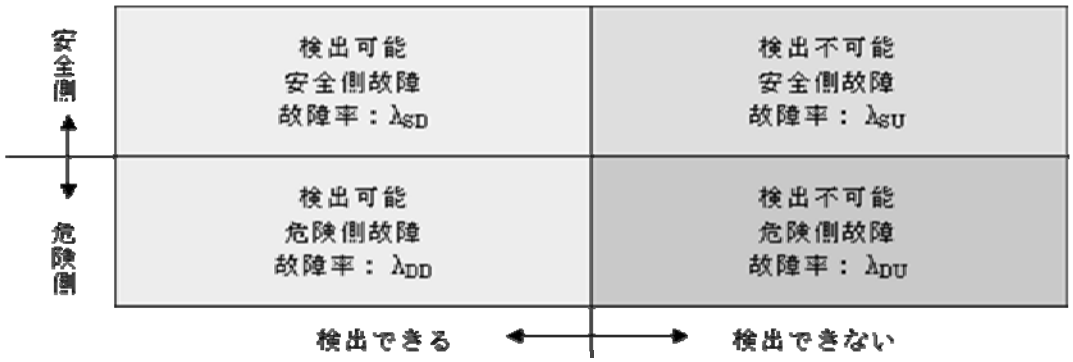


図 5.5　故障の分類

（参考：安藤忠明ほか「安全計装システムと ProSafe シリーズの診断機能」横河技法 Vol.43, No.4, 1999）

また、PFD_{AVG} の計算式として、**図 5.6** に示すような最も単純なシステム、すなわちセンサなどの入力が一つかつアクチュエータなどの出力が一つで、単一チャネルの場合の PFD_{AVG} は次の式で求められる。

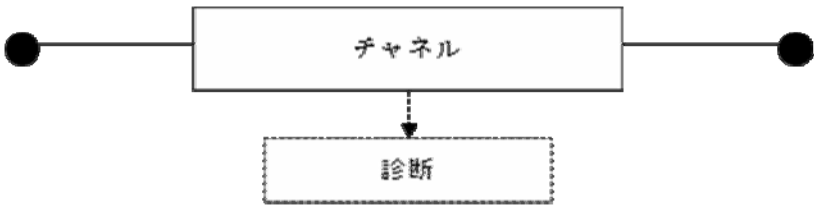


図 5.6　シングルチャネルの物理ブロックダイアグラム

（参考：向殿政男監修、井上洋一ほか著「制御システムの安全」安全の国際規格第 3 巻、PP.258 表 4.40**）**

$$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD})\, t_{DE}$$

$$\text{平均故障時間：} t_{DE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

次に上式に使われているパラメータは以下のとおりである。

- **t_{DE}（時間）：平均故障時間**
- **T_1（時間）：プルーフテスト間隔（Proof test period）**
  安全関連系の機能が正しく動作しているかどうかを確認するために行う機能確認試験をプルーフテストといい、この機能確認試験を実施する時間間隔をプルーフテスト間隔という。1 か月、3 か月、6 か月、1 年、2 年、10 年から選択。
- **MTTR（時間）：平均修理時間（Mean time to Restoration）**
  E/E/PE システムの故障発生から修復までの平均時間で、通常 8 時間。

・**λ（λ_S、λ_D、λ_{DD}、λ_{DU}、λ_{SD}、λ_{SU}）**：1 時間当たりの**故障率（Random hardware failure rate）**で、0.1×10^{-6}、1.5×10^{-6}、 5×10^{-6}、 10×10^{-6}、 50×10^{-6}から選択される。

PFD を求める必要から故障率**λ**を次のように分類している（図 5.5 参照）。

安全側故障発生率：λ_S

危険側故障発生率：λ_D（$=\lambda_{DD}+\lambda_{DU}$）

検出可能な安全側故障率：λ_{SD}

検出不可能な安全側故障率：λ_{SU}

検出可能な危険側故障率：λ_{DD}

検出不可能な危険側故障率：λ_{DU}

安全度水準（SIL）は、低頻度作動要求モードで運用された場合、 E/E/PE 安全関連系のプルーフテスト間の平均作動要求時機能失敗確率（PFD_{AVG}）により与えられる。

なお、機能安全の理解に必要なパラメータとして、診断範囲（自己診断率ともいう）**DC** がある。

・**DC（%）：診断範囲（自己診断率）（diagnostic coverage）**

危険側ハードウェア故障に対して自己診断テストがカバーする割合のこと。検出可能な危険側の故障率をλ_{DD}、検出できない危険側の故障率をλ_{DU}とすると診断範囲（自己診断率）**DC** は次式で表すことができる。

$DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU}) = \lambda_{DD} / \lambda_D$

機能安全では、危険側故障が少ないほど、また危険側故障が潜在していても自己診断で検出できるならば、「安全度が高い」と評価される。

5.5 E/E/PE 安全関連系のハードウェアの安全性評価

E/E/PE の安全関連部に対する技術的要求を **SIL**（**safety integrity level**）で定量的に評価するが、 **SIL** は主に HW で発生する全故障率に対する**安全側故障比率**（**SFF**：**safe failure factor**）によって決まる。**1）**安全側に故障するか、**2）**危険側に故障が予測されても E/E/PE 安全関連系自身がそれを把握でき、被災を回避できるか、**3）** 危険側に故障しても別途 HW が代行する（フォールト・トレランス）か、を**安全側故障率**というが、**SFF** とはこの安全側故障の発生率が、全故障発生率に対してどのくらいの比率であるかを示すもので、1 に近づくほど安全ということになる。

5.5.1 安全側故障率比 SFF の算定方法

上記 1)、2）に対応する **SFF** の算定手順を以下の（a）～（h）に示す（参考：規格書の附属書 C)。

(a) センサやアクチュエータなど E/E/PE 安全関連系のサブシステムの構成要素であるコン

ポーネント（またはそれが複数集まったコンポーネントグループ）に対して効果を確認するため、以下の（b)、(c）により、**FMEA**（故障モードとその影響解析）を実施して障害モード及び障害率、安全側／危険側故障発生率に対する割合を定める。

(b) 故障モードには、次の二つがあり、その各々について FMEA を行う。

① 安全側故障モード：E/E/PE システム安全関連系の安全整合性を低下させない、または安全整合性に影響しないような故障。

② 危険側故障モード：E/E/PE システム安全関連系が機能しなくなったり、安全整合性が低下するような故障。

(c) 各コンポーネント（グループ）に関する故障発生率の見積もりと FMEA の結果から安全側故障発生率 λ_S、と危険側故障発生率 λ_D を算定する。

(d) 各コンポーネント（グループ）に関して診断試験等により検出される危険側故障率 λ_{DD} を見積もる。

(e) サブシステムに関して、以下の値を定量化する。

① サブシステム全体に関して、全側故障発生率 λ_S、と危険側故障発生率 λ_D、危険側故障率 λ_{DD} を算定する。

② サブシステムの**診断範囲 DC** を $DC = \Sigma\lambda_{DD} / \Sigma\lambda_D$ として算定する。

③ サブシステムの**安全側故障率 SFF** を、$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$ として算定する。

(f) 上記②と③の式から、サブシステムの**診断範囲 DC** と**安全側故障率 SFF** の関係は、次式で与えられる。

$$SFF = \frac{\frac{\Sigma\lambda_S}{\Sigma\lambda_D} + DC}{\frac{\Sigma\lambda_S}{\Sigma\lambda_D} + 1}$$

(g) コンポーネントの安全側故障率 λ_S と λ_D の比 $\Sigma\lambda_S / \Sigma\lambda_D$ は、非対象故障率（人の誤りを含む場合は非対象誤り率）と呼ばれ、この比を η（イータ）で表すと、安全側故障率 SFF は、次式で示される。

$$SFF = \frac{\eta + DC}{\eta + 1}$$

(h) 通常半導体装置では $\eta = 1$ なので、$SFF = 0.5 + 0.5DC$ となる。なお通常診断範囲 **DC** は、$1 > DC \geqq 0$ の範囲にある。

5.5.2　ハードウェア安全度に関するアーキテクチャ（構成）上の制約

E/E/PE システム安全関連系のサブシステムについての最大の安全整合性基準（**SIL**）は、サブシステムの HW のフォールトレランス[10]によって制限される。サブシステムは安全側故障比 **SFF** の以下の三つの算定条件によって、**タイプ A** と**タイプ B** の二つに分類される。

a)　すべてのコンポーネント（サブシステムの構成要素）の故障モードを定義できる。

b)　障害条件下でサブシステムの挙動が完全に決定できる。

c)　要求される目標故障尺度に適合していることを示すに十分な、現場経験に基づく信頼できるデータがある。

この 3 条件をすべて満たすサブシステムが**タイプ A**、一つでも満たさないサブシステムを**タイプ B** と呼ぶ。この両タイプは論理的に否定の関係にある。式で表すと、

A-type=¬B-type（¬は否定を示す）である。

表 5.7 に安全整合性基準（**SIL**）と安全側故障率比（**SFF**）の関連を示す。網掛け部分がタイプ B のサブシステムついてであり、それ以外がタイプ A である。

なお、SFF＜99%で同一の SFF の値に対する SIL の値が 1 ランク異なることに注意する必要がある。

表 5.7　サブシステムのアーキテクチャ上の制約（参考：規格書 PP.17-18、表 2-表 3）

※SIL の欄は、網掛けの無い部分はタイプ A の場合、網掛け部分はタイプ B の場合

安全側故障率（SFF）	ハードウェアのフォールト・トレランス（N）					
	0		1		2	
SFF<60%	SIL1	許されない	SIL2	SIL1	SIL3	SIL2
60%≦SFF<90%	SIL2	SIL1	SIL3	SIL2	SIL4	SIL3
90%≦SFF<99%	SIL3	SIL2	SIL4	SIL3	SIL4	SIL4
99%≦SFF	SIL4	SIL3	SIL4	SIL4	SIL4	SIL4

5.6　E／E／PE 安全関連系に係る故障回避及び抑制のための技法

E/E/PE 安全関連系の故障には、安全ライフサイクル上、システムの設置前に内包されているフォールト（HW 的には製造段階のものや部品選定の誤りなど）によるものと、設置後のフォールト（ランダムハードウェア故障[11]や誤使用等のヒューマンエラー）とがある。フォールトによる故障を回避または抑制するために、多くの手段があり、安全ライフサイ

[10] HW フォールトレランス（N）は、偶発的 HW 故障によって引き起こされるが、危険側故障にまではいかない最大の障害発生数を意味する。従って、N=0 は単一障害が危険側故障を引き起こすことを意味する。必ずしも冗長構成を意味するものではないが、N=1～2 の場合は冗長構成を想起すると理解しやすい。

[11] E/E/PE システムの構成部品・機器などの劣化メカニズムのもとで偶発的あるいは時間的に無秩序に発生する故障。

クル上の各フェーズにおいて故障を回避する技法（附属書 B）及び運用時に故障を抑制する技法（附属書 A）が挙げられている。

5.6.1　E/E/PE 安全関連系の安全要求事項仕様書作成上の錯誤回避の技法及び方策

表 5.2 下欄にある附属書 B の表 1 参照（規格書 7.2.3.3）とは、IEC 61508-7 の E/E/PE 安全関連系の安全要求事項仕様書作成する際の錯誤回避の技法及び方策のことであり、**表 5.8** に目的例を含めて示す。網掛けの欄は、いずれか一つを選択する。なお、規格書第 7 部の欄は、規格書 IEC 61508-7 内の説明番号である。

表 5.8　E/E/PE 安全関連系の要求事項仕様での錯誤回避の技法／方策

（参考：向殿政男監修「制御システムの安全」第 3 巻 PP.213、表 4.20 及び規格書の附属書表 B.1）

錯誤回避の技法／方策	目的例	規格書第 7 部	SIL1	SIL2	SIL3	SIL4
プロジェクト管理	組織のモデル化	B.1.1	HR（L）	HR（L）	HR（M）	HR（H）
文書化	安全評価の容易化	B.1.2	HR（L）	HR（L）	HR（M）	HR（H）
安全関連系／非安全関連の分離	安全評価の容易化	B.1.3	HR（L）	HR（L）	HR（M）	HR（H）
構造化仕様	要求事項の階層化	B.2.1	HR（L）	HR（L）	HR（M）	HR（H）
仕様検査	仕様の不完全性回避	B.2.6	—（L）	HR（L）	HR（M）	HR（H）
半形式手法による	仕様の一貫性	B.2.3	R（L）	R（L）	HR（M）	HR（H）
チェックリストによる	要求事項の包括的適用	B.2.5	R（L）	R（L）	R（M）	R（H）
計算機支援の仕様ツール	形式的手法の適用	B.2.4	—（L）	R（L）	R（M）	R（H）
形式手法[12]	仕様の一貫性	B.2.2	—（L）	—（L）	R（M）	R（H）

※HR、R、—はそれぞれ「強く推奨する」、「推奨する」、「反対はしない」を表す。また、（ ）内の H、M、L はそれぞれ高、中、低を表す。

[12]形式手法（formal methods）とは、 数学を基盤とした SW／HW システムの仕様記述、開発、検証の技術で、高度な安全性やセキュリティが求められるシステムでは特に重要。開発工程でエラーが入り込まないことを保証するので、要求仕様レベルや機能仕様レベルで効果的であり、実装レベルでも形式主義的開発が可能。半形式的手法とは、機能ブロック、原因／結果図、シーケンス図等の SW の設計・開発技法を使うもので、リスク分析結果を複数にランク付けする方法なども含まれる。（参考: フリー百科事典『ウィキペディア（Wikipedia）』）

5.6.2　E／E／PE 安全関連系に係る故障回避の技法

表 5.3 の中欄 Fa1 の障害回避の技法／方策を規約書附属書 B 表 B2 に示す（規格書 7.4.7.1）**とは、**最終製品における機能安全を確立するため、不注意などによる故障回避を目的とする設計と開発における技法／方策の例のことで、これを**表 5.9** に示す。網掛け部分は、少なくともいずれか一つが採用される。

表 5.9　E/E/PE システムの設計・開発での故障回避の技法／方策

（参考：規格書の附属書 B 表 2 及び向殿政男監修「制御システムの安全」安全の国際規格第 3 巻）

回避の技法／方策	目的例	規格書第 7 部	SIL1	SIL2	SIL3	SIL4
指針及び規格の遵守	利用分野別規格参照	B.3.1	HR_m	HR_m	HR_m	HR_m
プロジェクト管理	組織のモデル化	B.1.1	HR（L）	HR（L）	HR（M）	HR（H）
文書化	安全評価の容易化	B.1.2	HR（L）	HR（L）	HR（M）	HR（H）
構造化設計	検証の簡略化	B.3.2	HR（L）	HR（L）	HR（M）	HR（H）
モジュール化	サブシステム間の複雑化制限	B.3.4	HR（L）	HR（L）	HR（M）	HR（H）
吟味されたコンポーネントの使用	未検出障害の低減	B.3.3	R（L）	R（L）	R（M）	R（H）
半形式手法による	仕様の一貫性	B.2.3	R（L）	R（L）	HR（M）	HR（H）
チェックリストによる	要求事項の包括的適用	B.2.5	R（L）	R（L）	R（M）	R（H）
計算機支援設計ツール	設計手順の系統化	B.3.5	—（L）	R（L）	R（M）	R（H）
シミュレーション	機能の系統的検査	B.3.6	—（L）	—（L）	R（M）	R（H）
ハードウェアの検査、またはウォークスルー	仕様と実現の間の不一致の検査	B.3.7 B.3.8	—（L）	R（L）	R（M）	R（H）
形式手法	仕様の一貫性	B.2.2	—（L）	—（L）	R（M）	R（H）

※HR、R、—はそれぞれ「強く推奨する」、「推奨する」、「反対はしない」を表す。また、（ ）内の H、M、L はそれぞれ高、中、低を表す。

故障を回避する手段は、当該安全ライフサイクルにおいて実行される。ただし、手段が強制でない場合は、他の手段でもよい。

5.6.3　安全関連系のハードウェア故障の抑制に関する技法

IEC 61508-2:2000 附属書 A の表 1 にある「検出される故障またはフォールト」は、EUC（被制御設備）の運転中に検出される故障またはフォールトの例を示している。**表 5.10** には規格書の附属書 A 表 1 に挙げられた事例のうち、HW について自己診断率を達成するため検出すべきフォールトを抜粋して掲げてある。

表 5.10　EUC 運転中に検出されるハードウェア故障またはフォールト（抜粋：規格書の附属書 A 表 1）

構成要素の例	診断範囲（DC：自己診断率）に対する要求事項		
	低（60%）	中（90%）	高（99%）
(A) CPU（レジスタ、内部バスを含む）	データ／アドレスの固定故障	データ／アドレスの直流化障害モデル	データ／アドレスの直流化障害モデル、メモリセル間の動的干渉、アドレス化なし／アドレス化誤り／マルチアドレス化
(B) バス（一般）	アドレスの固定故障	タイムアウト	タイムアウト
(C) 割込み処理	割込みなし／連続割込み	割込みなし／連続割込み／割込み干渉	割込みなし／連続割込み／割込み干渉
(D) クロック（クォーク）	低調波／超高調波	低調波／超高調波	低調波／超高調波
(E)　定数メモリ	データ／アドレスの固定故障	データ／アドレスの直流化障害モデル	メモリ内のデータに影響するすべての障害
(F)　可変メモリ	データ／アドレスの固定故障	データ／アドレスの直流化障害モデル	データ／アドレスの直流化障害モデル、メモリセル間の干渉、アドレス化なし／アドレス化誤り／マルチアドレス化
(G) センサ	固定故障	直流化障害モデル（ドリフト及び発信）	直流化障害モデル（ドリフト及び発信）
(H) 最終要素	固定故障	直流化障害モデル（ドリフト及び発信）	直流化障害モデル（ドリフト及び発信）

この表で、(E) ～ (H) の HW に対する固定障害は、出力が論理値 1 または 0 をとる故障モードで、struck at 0 or 1 とも呼ばれる。(A)、(E) ～ (H) の直流化障害モデルとは、固定故障に回路の断線故障と短絡故障を加えたもの。(G)、(H) のドリフトとは電源変動や環境変化による出力レベル変動、発振はフィードバック回路の正帰還故障による出力レベ

ル変動や電源回路故障に伴う交流出力の発生等を意味する。

このほか附属書 A には、表 2～表 19 に自己診断テストに係る技法、運用上の故障抑制手段など様々な故障の抑制技法が勧告されている。

5.7 本章のまとめ

本章は、国際標準で言えば、主に **IEC 61508** シリーズの第 2 部を中心にハードウェアの安全性について述べた。具体的には機能安全の「ゆりかごから墓場まで」と俗にいわれる「安全ライフサイクル」の流れのうち、1）フェーズ 9　E/E/PE システムの**安全要求事項**を中心に、各フェーズについての求められる **SIL** を満足する要求事項について詳述した。また、安全度の定量的評価法の一環として、2）危険側の**平均目標機能失敗尺度**（**PFD**）の計算方法、3）**安全側の故障率比**（**SFF**）の算定方法について言及した。また、4）ハードウェアの安全度が、そのフォールトレランスによって制限され、その時の **SIL** と **SFF** の関係を A、B の二つのタイプについて述べた。最後に IEC 61508 シリーズの第 2 部の附属書 A、B で勧告している、5）故障の回避と抑制についてその技法を規格書から抜粋して挙げた。

なお、組込みシステムの場合、SW と HW が連携してシステムが成り立っている場合が多いので、設計時から HW と SW の融合した安全機能を組み込んでおくことが重要である。

コラム 2： 故障と故障モード

（参考：客観説 TQM 研究所の信頼性・安全管理研修セミナー「特性要因図」）

例えば、電源キーの先に作動レバーがあって電源スイッチをオンにする場合、何かの原因でそのレバーが曲がって電源キーに届かなくなったとすれば、レバーの「曲がり」という事象と「電源が入らない」という 2 つの事象が存在する。前者を故障モード､後者を故障と呼ぶ(同旨:久米均､「設計開発の品質マネジメント」日科技連 P.141)。ここで、電源断、停止、油漏れ、騒音・振動、・・・等々のような機能障害が**故障**であり、ひび割れ、欠け、腐食、磨耗、曲がり、折れ、断線、破裂などの物理・化学的な変化（システムの破壊）を故障モードと呼ぶ。つまり機能障害を起こす可能性のある事象（必ずしも機能障害に至らない場合もある）が故障モードであり、故障モードが機能障害という結果につながったときの事象を故障と呼ぶ。従って、FMEA は「故障モード影響解析」と和訳されるが、これは「システムがどんな原因で「故障モード」をひき起こし、 その影響がどう出るか」という意味になる。

S（済賀 宣昭）

参考文献（第 5 章）

注 1） 向殿政男監修、井上洋一ほか著「制御システムの安全」安全の国際規格第 3 巻 2007 年 9 月 25 日 日本規格協会発行
注 2） JIS C 0508-1:1999「電気・電子・プログラマブル電子安全関連系の機能安全―第 1 部：一般要求事項」日本工業標準調査会 1999 年 7 月 20 制定、日本規格協会発行
注 3） JIS C 0508-2:2000「電気・電子・プログラマブル電子安全関連系の機能安全―第 2 部：電気・電子・プログラマブル電子安全関連系に対する要求事項」日本工業標準調査会 2000 年 2 月 20 制定、日本規格協会発行
注 4） JIS C 0508-6:2000「電気・電子・プログラマブル電子安全関連系の機能安全―第 6 部：第 2 部及び第 3 部の適用指針」日本工業標準調査会 2000 年 2 月 20 制定、日本規協会発行
注 5） IPA・SEC 編「組込みシステムの安全性向上の勧め（機能安全編）」2006 年 11 月 10 日、オーム社
注 6）安藤忠明、安藤進清「安全計装システムと ProSafe シリーズの診断機能」横河技報、Vol.43、No.4、1999
注 7） 宮脇信芳「産業分野における『機能安全』の潮流（安全の定性的評価から定量的評価へ）JTEKT Engineering Journal No.1005（2008）
注 8） 山田陽慈「ロボットの安全―『規格・認証』の現状と課題」産総研知能システム研究部門技術講演会レポート「次世代ロボット産業化基盤技術」2008 年 10 月 21 日
注 9）エム･システム技研「計装豆知識『機能安全と IEC 規格 61508 について』」MS Today2007 年 12 月
http://www.m-system.co.jp/mstoday/plan/mame/2006-2007/0712/index.html
注 10） 池田博康ほか「コンピュータを用いるプラント設備の安全制御手法と安全性評価」産業安全研究所特別研究報告　NIISOSRR-No.27 （2002）

第6章　機能安全ソフトウェア設計手法概要

本章は前章と同様にJIS C 0508-2:2000の「電気・電子・プログラマブル電子安全関連系に対する要求事項」に基づいて説明する。この中で特にソフトウェアに関係する部分を主体に述べる。IEC61508の第3部には、ソフトウェア開発のライフサイクルフェーズ毎に、安全装置のソフトウェアへの適用が推奨される技法・方策が安全度水準に応じて示されている。

6.1 ソフトウェアの要求事項

6.1.1 ソフトウェア安全ライフサイクル

図 6.1 に IEC61508 の第 3 部で示される安全性ライフサイクルの構成を示す。ソフトウェアに対する安全性ライフサイクルは、第 5 章でのハードウェアに対する解説と同様に、ソフトウェア安全要求事項仕様書 9.1 に始まり、9.2 ソフトウェア安全妥当性確認計画書、9.3 ソフトウェア設計及び開発、9.4 E/E/PES 統合（ハードウェア／ソフトウェア）、9.5 ソフトウェア運転と変更（保守）手続き、9.6 ソフトウェアの安全妥当性確認のフェーズからなる。

さらに 9.1 ソフトウェア安全要求仕様書は、E/E/PES 実現のために必要なソフトウェアに関する 9.1.1 安全機能要求事項仕様書と、9.1.2 安全整合性要求事項仕様書からなっている。

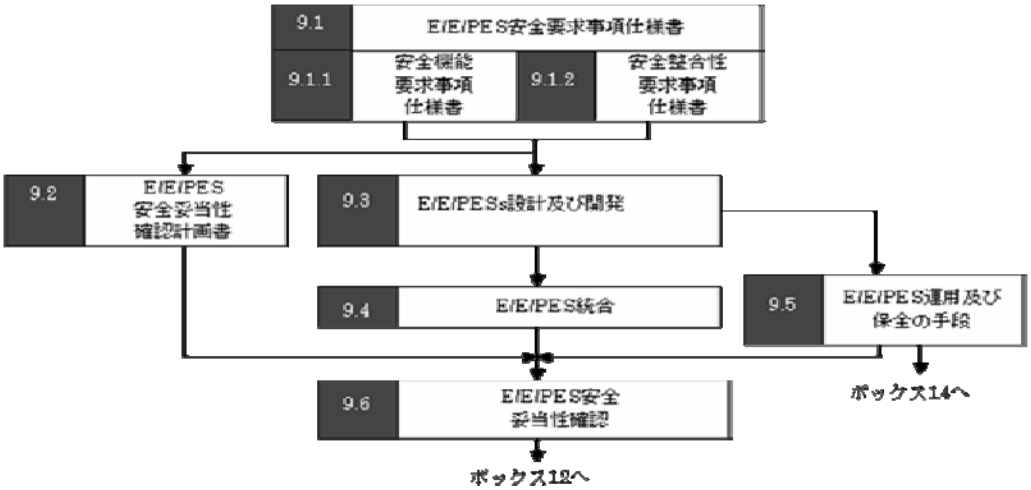


図 6.1　安全性ライフサイクル（参考：JIS C 0508-2:2002 図 2）

第 5 章で解説したハードウェアと本章で解説するソフトウェアの関係との適用範囲は**図 6.2** のように示される。ソフトウェアについても、**図 6.2** の IEC 61508-3 の適用範囲において全体としての E/E/PES 安全要求事項をもとに、そこで必要となる安全要求事項仕様書の作成から始まる。

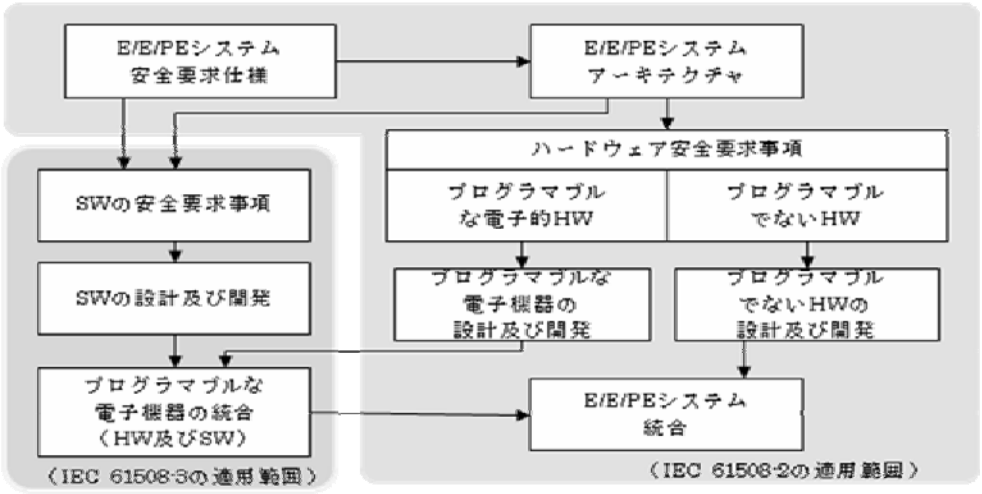


図 6.2 IEC 61508-2 と IEC 61508-3 の関係と適用範囲（参考：JIS C 0508-2:2000 図 3）

図中の略語　SW：ソフトウェア、HW：ハードウェア

しかし、ソフトウェア開発では、プログラムコード自体が文書の側面をもっており、修正や変更も容易であるため、より厳格な文書管理が必要とされる。また、開発プロセスの各フェーズの作業結果としての出力文書を次のフェーズの入力とすることと、作成されたソフトウェアについても各フェーズ毎に試験する必要がある。この関係を明確に表すために、図 6.3 のソフトウェア安全性ライフサイクルモデルが必要となる。

さらに、ソフトウェアは、バグなどによって生じる危険を確率的に表すことが困難であるため、安全整合性水準に応じてとるべき技法・方策を決定する形が必要となる。

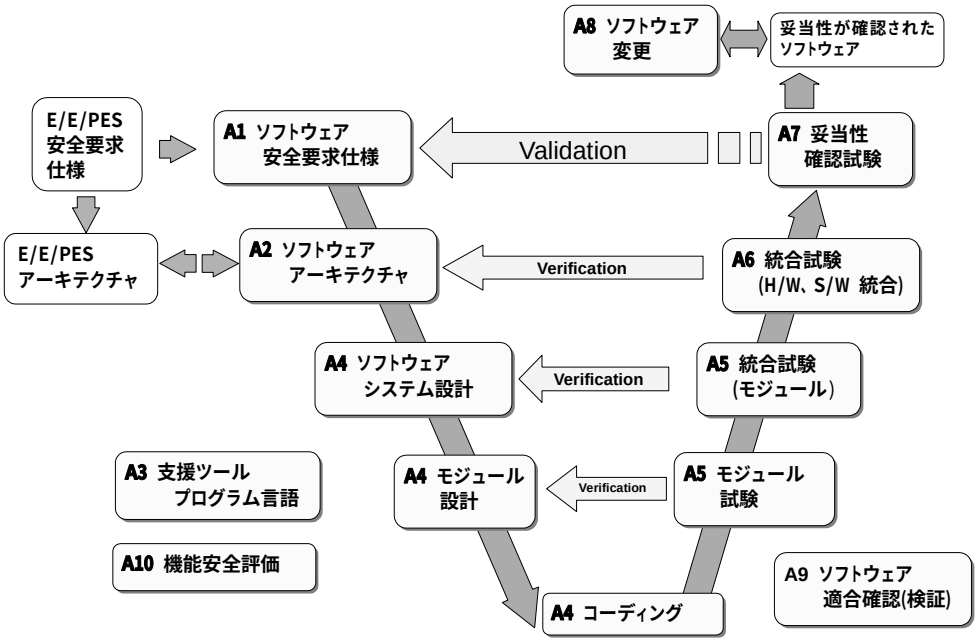


図 6.3　ソフトウェア安全性ライフサイクルモデル（V-モデル）

6.1.2　ソフトウェア安全ライフサイクルフェーズ要求事項

(1)ソフトウェア安全要求事項仕様書及び安全妥当性確認計画書フェーズでの要求事項

図 6.1 で表したように、9.1 ソフトウェア安全要求事項仕様書は、9.1.1 安全機能要求事項仕様書と 9.1.2 安全整合性要求事項仕様書からなる。

9.1.2 ソフトウェア安全整合性要求事項仕様書では、9.1.1 安全機能要求事項仕様書の中の安全機能に対して、ソフトウェアに対する安全整合性水準を振り当てるだけの作業となる。これは、リスクアセスメントの結果として定まったハードウェアにおける安全整合性水準に整合しなければならない。

ソフトウェア安全機能要求事項仕様書と安全妥当性確認計画書フェーズでの記入事項の例を**表 6.1** に示す。

表 6.1 ソフトウェア安全要求仕様書及び安全妥当性確認計画書への要求事項例
（参考：向殿政男監修「制御システムの安全」第 3 巻 p.231 表 4.29）

(A) ソフトウェア安全機能要求事項仕様書への記入事項例 (7.2.2.11)	(B) ソフトウェア妥当性確認計画書作成上の考慮事項例 (7.3.2.2)
a)EUC 安全状態の達成／維持方法 b)PE ハードウェア、センサアクチュエータの故障検出とその管理方法 c)ソフトウェア自体の故障検出とその管理方法 d)オンライン、オフライン定周期テスト e)PES の安全な変更方法 f)非安全関連系とのインタフェース g)容量、時間応答性 h)ソフトウェアと PES のインタフェース i)EUC の運転モード j)ハードウェアとソフトウェアの関係と制約	a)妥当性確認の実施期間、実施担当者 b)EUC の運転モード（異常状態を含む） c)ソフトウェアの識別 d)妥当性確認の為の技術的方策、技法、手順 e)ソフトウェア安全要求事項への参照 f)妥当性確認実施時の環境 g)合否判定基準 h)妥当性確認の結果、特に不合格の場合の方針と手順

ソフトウェア安全要求事項仕様書は、E/E/PES 安全関連システムの安全要求事項及び機能安全計画の要求事項である安全整合性水準に応じたソフトウェアの調達、開発、統合、検証、妥当性確認、変更の手順の明確化から導かれることになる。

(2)ソフトウェアの設計及び開発に関する要求事項

図 6.3 の V-モデル図上でソフトウェアの設計プロセスは、A2 のソフトウェアアーキテクチャから A4 のコーディングの実行までのフェーズとなる。しかし、実際には、ソフトウェアの開発は、A5 のモジュールの試験、モジュール統合試験を伴う。要求事項例としては、以下に説明する。なお、()内は IEC 61508 の条項番号である。

要求事項の「ソフトウェアアーキテクチャ設計」に対する要求事項例では、設計上での記述事項として、次の項目が示されている。（7.4.3.2）

1）：ソフトウェア安全要求事項仕様の安全整合性水準を満たす技法／方策を選択し、結果を正当化すべきこと、これには、フォールトトレラント及びフォールトアボイダンスの戦略を含めること。
2）：コンポーネント／サブシステムは区分化すること、これらには、ソフトウェア安全整合性水準とともに、新規／既存品か、検証済か否か、安全関連か否かを示すこと。
3）：ソフトウェア／ハードウェア間の相互作用、及びその重要性評価の記述。
4）：アーキテクチャの表現は明確に定義された表記法に基づくこと。
5）：すべてのデータについて安全整合性が維持されることを示すこと。
6）：ソフトウェアアーキテクチャ統合試験を規定すること。

次に「詳細設計及び開発」の要求事項では、詳細設計上での前提として、①ソフトウェア安全要求事項仕様書、ソフイトウェアアーキテクチャ設計及びソフトウェア安全妥当性確認計画書により(7.4.5.2)、②モジュール化、試験可能／安全変更可能な設計とすべきことが要請され（7.4.5.3）、さらに③統合を含む試験方法が示されるべきとされる。

要求事項の「コーディングの実行」に対する要求事項では、ソースコードの要求事項として、
a)読み、理解、試験可能で、
b)ソフトウェアモジュール規定の要求事項及びコード標準を満たし、
c)安全計画時の安全関連要求事項を満たすことが要求される。

次の「モジュール試験」に関する要求事項例は、「ソフトウェア統合試験」と相当の部分が共通するので後で述べる。要求事項の「一般的要求事項」(7.4.2)は、設計及び開発上で考慮すべき一般的要求事項である。この欄の「設計方法選択」(7.4.2.2)は、詳細事項の a)抽象化、モジュール化、複雑管理、b)表現、c)設計と理解、d)検証と妥当性確認にどの程度効果があるのかの考慮事項である。特に b)の「表現」には、IEC 61508 では機能性、

コンポーネント間の情報フロー、シーケンス／時間、タイミングの制約、同時性、データ構造、設計全体への表現の効果を挙げている。また「ソフトウェア変更容易化構造とする」(7.4.2.4)はモジュール化、情報隠蔽、カプセル化等のソフトウェア自体に対する変更の容易化構造を意味し、「最終的に、試験／安全な変更を可能にする」(7.4.2.3)は安全に関する試験／変更の容易化構造を意味する。「明瞭な定義の表記法による」(7.4.2.5)、「安全関連のソフトウェアの最小化」(7.4.2.6)、「独立性のない非安全関連ソフトウェアは安全関連とみなす」(7.4.2.7)、「ソフトウェアの独立性なしでは最高のソフトウェア安全整合性水準で扱う」(7.4.2.8)は、安全関連ソフトウェアの複雑性防止方策でありまた更にこれは、ソフトウェアが異なる安全整合性水準をもつ安全機能を扱う場合の処置であり、「プルーフテスト、診断試験、制御／データフローの自己診断機能はソフトウェア安全整合性に基づく」（7.4.2.9-10）は、高レベルの安全整合性への処置を示している。

「支援ツール及びプログラミング言語」に対する要求事項では、「プログラミング言語」(7.4.4.3)はプログラミング言語の決定の選択事項で、詳細事項の a)妥当性確認認証所有又は適合査定による、b)曖昧でない、c)アプリケーションへの適正、d)プログラミングミスの検出に基づく、「コーディング基準」で「不安全言語」とは、未定義言語の使用や未構造化設計による場合を意味する。「ソフトウェア統合試験」に関する要求では、「ソフトウェア統合試験規定事項」(7.4.8.2)は、試験に際しての用意すべき要求事項である。さらに、「全てのソフトウェアモジュール／構成要素・サブシステムが意図する機能を実行し、意図しない機能を実行しないことを示す」(7.4.8.3)は、安全関連試験の特別要求事項である。

(3)ソフトウェア設計及び開発後のフェーズに関する要求事項

ソフトウェア設計及び開発後における要求事項には、「プログラマブル電子装置統合の要求事項」(7.5.2)、「ソフトウェア変更に対する要求事項」(7.8.2)、「ソフトウェア運転及び変更手順に関する要求事項」(7.6.2)、「ソフトウェア妥当性確認の要求事項」(7.7.2)、「ソフトウェア検証に関する要求事項」(7.9.2)等が規定されている。

次の表 6.2 に、「プログラマブル電子装置統合の要求事項」(7.5.2)及び「ソフトウェア妥当性確認の要求事項」(7.7.2)に関する要求事項例を示す。

表 6.2 プログラマブル電子装置統合及びソフトウェア妥当性確認に関する要求事項例

（参考：向殿政男監修「制御システムの安全」第 3 巻 p.235 表 4.31）

(P) プログラマブル電子装置統合の要求事項例 (7.5.2)	(V) ソフトウェア妥当性確認の要求事項例(7.7.2)
P1: HW と SW の両立性確保の統合試験を規定のこと (7.5.2.1) P2: 統合試験規定 (7.5.2.2) a) 統合水準へのシステムの分割 b) 試験事例及び試験データの明示 c) 試験の形式 d) 試験環境、ツール、構成、プログラムの確認 e) 試験の完了判定の為の試験基準 P3: 作業種の区分の要求 a) 試験場所が開発側かユーザ側かの区分 (7.5.2.3) b) SW の HW への合体 (7.5.2.4) c) E/E/PE 統合（インタフェースの適用） d) EUC と E/E/PE 安全関連システムの総合統合 P4: ソフトウェア統合でのソフトウェアの修正、変更は、影響分析を行うこと (7.5.2.6) P5: 試験事例及びその結果は、その後の分析の為に文書化を行うこと (7.5.2.7) P6: 試験結果は試験目的及び試験評価基準を満たすことを（不合格の場合は理由）を文書化する (7.5.2.8)M	V1: E/E/PE 安全関連系でソフトウェア安全要求事項適合の場合、妥当性の再確認は不用 (7.7.2.1) V2: 妥当性確認は確認計画書に基づく (7.7.2.2) V4: 全ての安全機能は以下の文書化要 (7.7.2.4) a) 妥当性確認活動の日付記録 b) 妥当性確認計画書のバージョン c) 対象とする安全機能 d) 使用ツール及び機器、校正データ e) 妥当性確認の結果 f) 予想と実際の結果の不一致 V5: 結果不一致の場合、その処置の文書化要 (7.7.2.5) V6: 妥当性確認での要求事項 (7.7.2.6) a) 主要な確認方法はテストによること b) ソフトウェアシミュレーション： - 通常運転の入力信号で - 予想事象で - システム動作の望ましくない状況で c) 開発者は必要文書を入手可能とする V7: 妥当性確認でのソフトウェアツールは、目的に適合し、国際規格、国内規格、又は、十分に認識された手順によること (7.7.2.7)

(4)ソフトウェア安全ライフサイクルに関わる安全性向上のための要件

図 6.1 の安全性ライフサイクルの各要求事項に沿って、それぞれの安全性向上のための要件を、以下、**表 6.3** にまとめた。

表 6.3 ソフトウェア安全ライフサイクルに関わる安全性向上の為の要件の整理結果

（参考　独立行政法人原子力安全基盤機構　「ディジタル安全保護系規制要件調査等に関する報告」）

Phase No.	IEC61508	安全性向上の為の要件	適用技法
9.1	【SW 安全要求事項仕様書】		1: コンピュータ支援仕様書作成ツール
	SW 自己診断 [P3-7.2.2.9, 11]	SW 自己監視機能を備えること。SW 故障に対する検知／警報／管理機能備えること。	
	HW、センサ、アクチュエータの監視 [P3-7.2.2.9, 11]	プログラマブル電子装置 HW、センサ、アクチュエータの監視機能を備えること。プログラマブル電子装置 HW の故障に対する検知／警報／管理機能を備えること。	
	安全機能試験性 [P3-7.2.2.9, 11]	安全機能の定期試験に関わる機能を備えること。	
9.1	SW の容量と応答時間性能 [P3-7.2.2.9, 11]	要求される SW の容量と応答時間性能を定めること。	
9.2	SW 安全妥当性確認計画 [P3-7.3.2]	SW 安全妥当性確認計画を作成すること。SW 安全妥当性確認計画は、開発、設計、製作、検査に携わった者とは、独立した部門または組織が作成すること。	
9.3	【SW 設計及び開発】		
	アーキテクチャ [P3-7.4.3.2]	SW 安全要求事項仕様書を満足すること。要求される安全レベルに応じて、SW の冗長性及び多様性を考慮した SW アーキテクチャを定めること。	1: コンピュータ支援仕様書作成ツール 4: 故障検出及び診断 6: 異常断定プログラム

Phase No.	IEC61508	安全性向上の為の要件	適用技法
9.3	支援ツール [P3-7.4.4.2]	要求される安全レベルに応じて、プログラミング言語、コンパイラ、構成管理機能、自動試験機能（必要に応じて）を備えた SW 開発支援ツールを選択すること。	20: 適切なプログラミング言語 22: 認定されたツール及び認定された変換プログラム
9.1	【SW 安全要求事項仕様書】		1: コンピュータ支援仕様書作成ツール
9.3	プログラミング言語 [P3-7.4.4.3]	プログラミング言語のトランスレータ／コンパイラは、要求される安全レベルに応じて、国内もしくは国際規格に対する妥当性確認認定を受けるか、用途への適合性評価を行うこと。	20: 適切なプログラミング言語
	コーディング基準[P3-7.4.4.5]	コーディング基準を用いて、SW 開発を行うこと。	20: 適切なプログラミング言語
	SW システム／モジュール設計 [P3-7.4.5.3]	SW のシステム設計は、モジュール性、試験可能性、変更可能性など考慮して実施すること。	31: コンピュータ支援設計ツール 33: モジュール化手法 35: 構造化プログラミング 65: コーディング基準 69: 割込みの使用制限 71: 再帰の使用制限
	SW ソースコード設計 [P3-7.4.6.1]	SW ソースコード設計は、判読容易性、理解容易性、試験可能性などを考慮して実施すること。	31: コンピュータ支援設計ツール 33: モジュール化手法 35: 構造化プログラミング 65: コーディング基準 69: 割込みの使用制限 71: 再帰の使用制限
	SW モジュール試験 [P3-7.4.7]	SW モジュール試験を実施すること。SW モジュールが意図した動作を実現し、意図しない動作をしないことを確認すること。	45: 機能試験 53: データ記録及び分析 80: プロトタイピング／アニメーション 96: なだれ／ストレス試験

Phase No.	IEC61508	安全性向上の為の要件	適用技法
9.3	SW 統合試験 [P3-7.4.8]	SW 統合試験を実施すること。全ての SW モジュール、SW 構成要素／サブシステムが意図した動作を実現し、意図しない動作をしないことを確認すること。	45: 機能試験 53: データ記録及び分析 80: プロトタイピング／アニメーション 96: なだれ／ストレス試験
9.4	HW と SW の統合及び試験 [P3-7.5]	HW と SW を統合して、HW と SW の適合性を確認する統合試験を実施すること。	80: プロトタイピング／アニメーション 96: なだれ／ストレス試験
9.5	SW 変更手順 [P3-7.8]	SW 構成管理で定めた手続きに基づき、SW 変更とその管理を実施すること。	52: SW 構成管理 53: データ記録及び分析
9.6	SW 安全妥当性確認 [P3-7.7]	SW 安全要求事項の全てが正しく実現され、SW システムが意図しない動作をしないことを確認する。	45: 機能試験 80: プロトタイピング／アニメーション
-	SW 検証 [P3-7.9.2.7]	SW 安全ライフサイクルで、以下のものについて検証活動を実施すること。 SW 安全要求事項作成、SW アーキテクチャ設計、SW システム／モジュール設計、SW ソースコード設計、SW 設計データ検証、SW モジュール試験、SW 統合試験、HW と SW の統合試験、SW 安全妥当性確認試験	

6.2 ソフトウェア安全ライフサイクルモデル

ソフトウェア開発のプロセスを表現するモデルとして**図 6.3** に示す V-モデルがある。この V-モデルは、開発プロセスにおける各フェーズ間の入出力が明確になるとともに、必要な試験、検証、妥当性確認の位置づけが明確になるメリットがある。

さらに、E/E/PES 安全要求事項から開発プロセスの各フェーズの上流のアウトプットが下流のフェーズに反映することにより、仕様レベルの検証が確実に実施できることになる。

第 5 章で述べたハードウェアに対し、ソフトウェアでは、バグなどによって危険な事象が発生するかどうかを定量的に扱うことは困難である。このような性質をもつ故障を、IEC 61508 では決定論的故障として扱っている。ソフトウェアにおいては、ソフトウェアライフサイクルにおける各フェーズの安全整合性に応じて推奨される技法／方策が与えられる。**表 6.4** ～ **表 6.22**（注 4）に、これらの技法／方策を示す。

表中の各フェーズ内の連続した網掛け部分において同一安全度水準推奨度であれば、いずれかの項目を適用することである。以下に安全度水準の推奨度を示す。

HR：技法／方策は強く推奨される。もしこの技法／方策を用いない場合には、安全計画時にその理由について詳細を示し、アセッサーの合意を得ること。
R ：技法／方策は推奨されるが、HR の推奨に比べればその推奨度は低い。
－：技法／方策の適用にあたって推奨も反対もない。
NR：技法または方策の適用は強く否定される。この技法または方策が用いられる場合、安全計画時にその理由について詳細を示し、アセッサーの合意を得ること。

なお、HR に分類される技法は、R に分類される技法よりも、より効果的にソフトウェア開発において決定論的な不具合が入り込むことの防止ができるか、またはソフトウェアに残存し、実行中に明らかになる不具合をより効果的に制御できると考えることになる。

また、これらの表に次いで、**表 6.23**（注 4）には、各技法／方策の概要を掲載した。

表 6.4 ソフトウェア安全要求仕様書

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
1	コンピュータ支援仕様書作成ツール	R	R	HR	HR
2	半形式手法 （表 6.20 参照）	R	R	HR	HR
3	形式手法：例えば、CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM 及び Z	―	R	HR	HR

表 6.5 ソフトウェア設計及び開発：ソフトウェア・アーキテクチャ設計

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
4	故障検出及び診断	―	R	HR	HR
5	エラー検出及びコード修正	R	R	R	HR
6	異常断定プログラム	R	R	R	HR
7	安全バッグ	―	R	R	R
8	ソフトウェアの多様性	R	R	R	HR
9	リカバリ・ブロック	R	R	R	R
10	後退回復	R	R	R	R
11	再試行障害回復機構	R	R	R	HR
12	実経路の記憶	―	R	R	HR
13	グレースフル・デグラデーション	R	R	HR	HR
14	人工知能－故障修復	―	NR	NR	NR
15	動的再構成	―	NR	NR	NR
16	構造化技法：例えば、CORE, JSD, MASCOT, SADT, 及び yourdon	HR	HR	HR	HR
17	半形式手法（表 6.20 参照）	R	R	HR	HR
18	形式手法：例えば、CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM 及び Z	―	R	R	HR
19	コンピュータ支援仕様書作成ツール	R	R	HR	HR

表 6.6 ソフトウェア設計及び開発：サポート・ツール及びプログラム言語

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
20	適切なプログラム言語	HR	HR	HR	HR
21	強固なプログラム言語	HR	HR	HR	HR
22	言語サブセット	—	—	HR	HR
23	認定されたツール及び認定された変換プログラム	R	HR	HR	HR
24	ツール：使用による信頼性向上	HR	HR	HR	HR
25	証明付きトランスレータ（翻訳機能）	R	HR	HR	HR
26	トランスレータ：使用による信頼性強化	HR	HR	HR	HR
27	信頼できる又は、検証済みソフトウェア・モジュール及び構成要素のライブラリ	R	HR	HR	HR

注：No.23，24 のいずれか、No.25，26 のいずれか。

表 6.7 ソフトウェア設計及び開発：詳細設計

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
28	構造化技法：例えば、CORE，JSD，MASCOT，SADT，及び yourdon	HR	HR	HR	HR
29	半形式手法（表 6.20 参照）	—	R	R	HR
30	形式手法：例えば、CCS，CSP，HOL，LOTOS，OBJ，temporal logic，VDM 及び Z	—	R	R	HR
31	コンピュータ支援設計ツール	R	R	HR	HR
32	防御プログラム	—	R	HR	HR
33	モジューラー・アプローチ（表 6.22 参照）	HR	HR	HR	HR
34	設計及びコード化規格（表 6.14 参照）	R	HR	HR	HR
35	構造化プログラム	HR	HR	HR	HR
36	信頼できる又は、検証済みソフトウェア・モジュール及び構成要素の使用（可能ならば）	R	HR	HR	HR

表 6.8 ソフトウェア設計及び開発：ソフトウェア・モジュール試験及び統合

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
37	確率的試験	—	R	R	HR
38	動的解析及び分析（表 6.15 参照）	R	HR	HR	HR
39	データ記録及び分析	HR	HR	HR	HR
40	機能及びブラックボックス試験（表 6.16 参照）	HR	HR	HR	HR
41	性能試験（表 6.19 参照）	R	R	HR	HR
42	インタフェース試験	R	R	HR	HR

表 6.9 プログラマブル電子機器統合（ハードウェア及びソフトウェア）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
43	機能及びブラックボックス試験（表 6.16 参照）	HR	HR	HR	HR
44	性能試験（表 6.19 参照）	R	R	HR	HR

表 6.10 ソフトウェア安全妥当性確認

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
45	確率的試験	—	R	R	HR
46	シミュレーション／モデル化（表 6.18 参照）	R	R	HR	HR
47	機能及びブラックボックス試験（表 6.16 参照）	HR	HR	HR	HR

表 6.11 ソフトウェアの修正

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
48	影響度分析	HR	HR	HR	HR
49	変更ソフトウェア・モジュールの再検証	HR	HR	HR	HR
50	影響を受けたソフトウェア・モジュールの再検証	R	HR	HR	HR
51	完全システムの再健全性確認	—	R	HR	HR
52	ソフトウェア・コンフィグレーション管理	HR	HR	HR	HR
53	データ記録及び分析	HR	HR	HR	HR

表 6.12 ソフトウェアの適合確認

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
54	形式的な証明手法	—	R	R	HR
55	確率的試験	R	R	R	HR
56	静的解析（表 6.21 参照）	R	HR	HR	HR
57	動的解析及び試験（表 6.15 参照）	R	HR	HR	HR
58	複雑度指標	R	R	R	R

表 6.13 機能安全評価

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
59	チェックリスト	R	R	R	R
60	決定表（真理値表）	R	R	R	R
61	複雑度指標	R	R	R	R
62	異常解析（表 6.17 参照）	—	R	HR	HR
63	ダイバース・ソフトウェアの共通要因故障分析 （ダイバース・ソフトウェア使用時）	—	R	HR	HR
64	信頼性ブロック・ダイアグラム	R	R	R	R

表 6.14 設計及びコード化規格（表 6.7 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
65	コーディング基準	HR	HR	HR	HR
66	動的オブジェクトの不使用	R	HR	HR	HR
67	動的変数の不使用	—	R	HR	HR
68	動的変数生成時のオンラインチェック	—	R	HR	HR
69	割込みの使用制限	R	R	HR	HR
70	ポインタの使用制限	—	R	HR	HR
71	再帰の使用制限	—	R	HR	HR
72	高級言語プログラムにおける無条件ジャンプなし	R	HR	HR	HR

表 6.15 動的解析及び試験（表 6.8 及び 表 6.12 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
73	境界値解析からの試験ケース実行	R	HR	HR	HR
74	エラー推定からの試験ケース実行	R	R	R	R
75	エラー・埋め込みからの試験ケース実行	—	R	R	R
76	性能モデル化	R	R	R	HR
77	等価クラス及び入力分類試験	R	R	R	HR
78	構造に基づく試験	R	R	HR	HR

表 6.16 機能及びブラックボックス試験（表 6.8, 表 6.9 及び 表 6.10 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
79	因果関係ダイアグラム	—	—	R	R
80	プロトタイピング／アニメーション	—	—	R	R
81	境界値での分析	R	HR	HR	HR
82	等価クラス及び入力分類試験	R	HR	HR	HR
83	プロセスシミュレーション	R	R	R	R

表 6.17 異常解析（表 6.13 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
84	因果関係ダイアグラム	R	R	R	R
85	イベント・ツリー分析	R	R	R	R
86	FTA	R	R	HR	HR
87	FMECA	R	R	HR	HR
88	モンテカルロ・シミュレーション	R	R	R	R

表 6.18 シミュレーション／モデル化（表 6.10 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
89	データ・フロー・ダイアグラム	R	R	R	R
90	有限状態機械／状態遷移図	—	R	HR	HR
91	形式手法	—	R	R	HR
92	性能モデル化	R	HR	HR	HR
93	タイムペトリネット	—	R	HR	HR
94	プロトタイピング／アニメーション	R	R	R	R
95	構造ダイアグラム	R	R	R	HR

表 6.19 性能試験（表 6.8 及び 表 6.9 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
96	なだれ／ストレス試験	R	R	HR	HR
97	応答タイミング及びメモリー制約	HR	HR	HR	HR
98	性能要求事項	HR	HR	HR	HR

表 6.20 半形式手法（表 6.4, 表 6.5 及び 表 6.7 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
99	機能ブロック・ダイアグラム	R	R	HR	HR
100	シーケンス・ダイアグラム	R	R	HR	HR
101	データ・フロー・ダイアグラム	R	R	R	R
102	有限状態機械／状態遷移図	R	R	HR	HR
103	タイムペトリネット	R	R	HR	HR
104	決定表（真理値表）	R	R	HR	HR

注１： 機能ブロック・ダイアグラムは IEC61131-3:2003 による。

表 6.21 静的解析（表 6.12 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
105	境界値解析	R	R	HR	HR
106	チェックリスト	R	R	R	R
107	制御フロー解析	R	HR	HR	HR
108	データ・フロー・ダイアグラム	R	HR	HR	HR
109	エラー推定	R	R	R	R
110	Fagan 検査	—	R	R	HR
111	組込み回路解析	—	—	R	R
112	シンボル実行	R	R	HR	HR
113	ウォークスルー／デザインレビュー	HR	HR	HR	HR

表 6.22 モジューラー・アプローチ（表 6.7 に引用）

No.	技法／方策	SIL1	SIL2	SIL3	SIL4
114	ソフトウェア・モジュール・サイズ制限	HR	HR	HR	HR
115	情報隠蔽／カプセル化	R	HR	HR	HR
116	パラメータ番号制限	R	R	R	R
117	サブルーチン及び機能における一つのエントリー／一つの exit	HR	HR	HR	HR
118	完全定義インタフェース	HR	HR	HR	HR

表 6.23　技法／方策の概要

No.	技法／方策	技法／方策の概要
A.1 ソフトウェア安全要求仕様		
1	コンピュータ支援仕様書作成ツール	コンピュータを用いた仕様書作成ツール
2	半形式手法	B.7 参照
3	形式手法： CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM, Z	CCS: 同期通信プロセスのシステムの挙動について記述し、論証する手法 CSP: 並列ソフトウェアシステム、即ち並列して動作する通信プロセスシステムの使用規定のための技法（他、割愛）
A.2 ソフトウェア設計及び開発： ソフトウェアアーキテクチャ設計		
4	故障検出及び診断	アサーションプログラミング、N バージョンプログラミング、安全バッグ技法、エラー検出コードなど
5	エラー検出及びコード修正	ハミングコード、多項式符号など
6	異常断定（アサーション）プログラム	アサーションプログラミング技法は、一連のステートメントを実行する前後に、事前条件と事後条件のチェックを行う。何れかの条件が満たされていなければ、エラーと判定され、処理が停止する。
7	安全バッグ	独立したコンピュータでの監視手法
8	ソフトウェアの多様性	多様なソフトウェアを使用する手法
9	リカバリ ブロック	同一の処理を行う複数の部分のプログラムを用意しておき、順番に適用する方法
10	後退回復	障害が検出された場合、前もって一貫性が証明されている初期状態にリセットする手法
11	再試行障害回復機構	障害やエラーが検出された場合、同一コードを再実行して状態を回復するよう試みる手法
12	実経路の記憶	許されない経路を実行しようとした場合、ソフトウェアを強制的かつ安全に機能停止させる

No.	技法／方策	技法／方策の概要
13	グレースフル　デグラデーション	より重要度の低い機能を停止させることで、重要度の高い機能を維持する手法
14	人工知能による故障修復	人工知能(AI)に基づくシステムによって、障害予測（トレンド計算）や障害復旧、保守、監視動作を効率よくサポートする手法
15	動的再構成	ハードの故障を検出すると、機能し続けている制限されたハードに、再度マッピングする手法
16	構造化技法：CORE, JSD, MASCOT, SADT, yourdon	CORE: 要求事項を明確に表現する手法 JSD: 逐次プロセス間の通信に着目して、モデル化、機能表現、実現する方法（他、割愛）
17	半形式手法	B.7 参照
18	形式手法： CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM, Z	（前述に同じ）
19	コンピュータ支援仕様書作成ツール	（前述に同じ）
A.3 ソフトウェア設計及び開発： 支援ツール及びプログラミング言語		
20	適切なプログラミング言語	完全かつ一義的に定義された等の特徴をもつ言語
21	強固なプログラミング言語	コンパイラでチェック可能な言語
22	言語サブセット	あるプログラミング言語のある機能について、いくつかの小さなセットに分割する手法
23	認定されたツール、認定された変換プログラム	独立機関が基準に照らして認定したもの
24	ツール利用による信頼性向上	動作検証されたツールの利用
25	証明付きトランスレータ（翻訳機能）	独立機関が基準に照らして認定したもの
26	トランスレータ利用による信頼性強化	動作検証されたトランスレータ利用
27	信頼できる又は、検証済のソフトウェアモジュール及び、構成要素のライブラリの利用	充分な実績のあるモジュール、ライブラリの利用

No.	技法／方策	技法／方策の概要
A.4 ソフトウェア設計及び開発： モジュール設計、コーディング		
28	構造化技法：CORE, JSD, MASCOT, SADT, yourdon	（前述に同じ）
29	半形式手法	B.7 参照
30	形式手法： CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM, Z	（前述に同じ）
31	コンピュータ支援設計ツール	コンピュータを用いた設計支援ツール
32	防御プログラム	特異な制御フロー、データフロー、データ値を検出して、事前に定められた、許容可能な方法で対処する方法
33	モジュール化手法	B.9 参照
34	設計及びコード化規格	B.1 参照
35	構造化プログラミング	実行せずに解析できるよう、制御フローの単純化、モジュール化を考慮する手法
36	信頼できる又は、検証済のソフトウェアモジュール及び、構成要素のライブラリの利用	（前述に同じ）
A.5 ソフトウェア設計及び開発： ソフトウェアのモジュール試験と統合試験		
37	確率的試験	確率的試験や運転経験に基づいた検討手法
38	動的解析、試験	典型的な入力をプロトタイプに与えて試験を行う手法。 B.2 参照
39	データ記録と分析	検証、妥当性確認、評価、保守の容易化の為、全てのデータ、根拠等を文書化する方法。
40	機能試験、ブラックボックス試験	機能試験：特徴的な運転データを与えて試験を行うもの。 ブラックボックス試験：仕様書から入力データ（許容範囲内外データ、境界値、限界値、極端な値のデータ）を求めておき試験を行う。 B.3 参照
41	性能試験	B.6 参照
42	インタフェース試験	サブプログラム間インタフェース確認の為、全モジュール組合せ、境界値、限界値データを用いて試験をするもの

No.	技法／方策	技法／方策の概要
A.6 プログラマブル電子機器の統合試験		
43	機能試験、ブラックボックス試験	（前述に同じ）
44	性能試験	（前述に同じ）
A.7 ソフトウェア安全妥当性確認試験		
45	確率的試験	（前述に同じ）
46	シミュレーション／モデル化	B.5 参照
47	機能試験、ブラックボックス試験	（前述に同じ）
A.8 ソフトウェアの変更		
48	影響度分析	ソフトウェア変更前の事前影響評価
49	変更ソフトウェアモジュールの再検証	変更ソフトウェアモジュールの再検証
50	影響を受けたソフトウェアモジュールの再検証	変更の影響を受けたソフトウェアモジュールの再検証
51	完全システムの再健全性の確認	変更後のシステム全体の健全性を再確認
52	ソフトウェアコンフィギュレーション管理	構成管理手法を適用するもの
53	データ記録と分析	（前述に同じ）
A.9 ソフトウェアの適合確認		
54	形式的な証明手法	プログラムを実行せず、ロジック上のモデル、ルールを使って、正当性、妥当性を検証するもの
55	確率的試験	（前述に同じ）
56	静的解析	データフロー整合性、制御フロー、インタフェースが正しいか、文書上で解析する。B.8 参照
57	動的解析、試験	（前述に同じ）
58	複雑度指標	ソフトウェア自体の特性と、開発／試験の経過履歴より、複雑度を予測する手法

No.	技法／方策	技法／方策の概要
A.10 機能安全評価		
59	チェックリスト	チェックリストを用いた評価方法
60	決定表（真理値表）	全入出力結果を表にして評価をする方法
61	複雑度指標	（前述に同じ）
32	異常解析	B.4 参照
63	ダイバースソフトウェアの共通要因故障分析（ダイバースソフトウェアの利用時）	多重チャネル間の共通要因故障に着目して故障の分析を行う。これに伴ったレビュー、検証、試験などを行う。共通要因故障には、内外の原因を含める。
64	信頼性ブロックダイアグラム	対象をブロック、線、論理結合からなる成功経路として表現し、最低１つの成功経路があれば正しく動作すると判断する方法
B.1 設計及びコード化規格		
65	コーディング基準	モジュールのインタフェース、言語の制限、割込み制限等、コーディング規則を明確化する方法
66	動的オブジェクトの不使用	実行状態に依存して変数等のメモリを割当てる方式を不使用とする
67	動的変数の不使用	66 に同じ
68	動的変数生成時のオンラインチェック	実行状態に依存して変数等のメモリを割当てる方式で、メモリ番地を事前にチェックする方式
69	割込みの使用制限	分岐が複雑となる割込みを制限する手法
70	ポインタの使用制限	ポインタによる参照番地不都合を回避する為に、メモリの使用を制限する方法
71	再帰の使用制限	サブルーチンのなかで、再度そのサブルーチンを呼び出しすることを制限する手法
72	高級言語プログラムに於ける無条件ジャンプの制限	無条件ジャンプによる複雑化を回避するために、使用を制限する方法

No.	技法／方策	技法／方策の概要
B.2 動的解析、試験		
73	境界値解析からの試験ケース実行	データの限界地、境界値で試験を実施
74	エラー推定からの試験ケース実行	エラーが発生しそうなケースの試験実施
75	エラー、埋め込みからの試験ケース実施	故意にエラーを埋め込んで試験を実施し、エラーが発見できるか否かを検討してみる方法
76	性能モデル化	システムプロセスと相互作用のモデル化を行い、それに必要とされるリソースを計算し、設計と照合チェックする手法
77	等価クラス及び入力分類試験	入出力を適宜分割し、それら全てに対しての試験を行う方法
78	構造に基づく試験	プログラム解析結果から、可能な限りのプログラムを実行するようにした試験方法
B.3 機能試験、ブラックボックス試験		
79	因果関係ダイアグラム	システム内で起こり得る事象シーケンスをダイアグラムでモデル化し、機能を確認する方法
80	プロトタイピング／アニメーション	システムの一部をツールを利用してプロトタイプとして作成し、機能確認をして行く方法
81	境界値解析	境界値や極端な値、条件での試験の実施
82	等価クラス及び入力分類試験	（前述に同じ）
83	プロセスシミュレーション	システムと同等な機能を有した模擬システムと、シミュレータを使って、機能を確認する方法
B.4 異常解析		
84	因果関係ダイアグラム	（前述に同じ）
85	イベントツリー解析	イベントツリーを使用してシステムの機能確認をする手法
86		
87		
88		

No.	技法／方策	技法／方策の概要
B.4 異常解析		
84	因果関係ダイアグラム	（前述に同じ）
85	イベントツリー解析	イベントツリーを使用してシステムの機能確認をする手法
86	FTA	フォルトツリーを使ってシステムの機能確認をする手法
87	FMECA	故障モード、影響解析手法
88	モンテカルロ　シミュレーション	乱数によるシミュレーションをする方法
B.5 シミュレーション／モデル化		
89	データフロー ダイアグラム	データフローをダイアグラムの形で表し、機能を確認する手法
90	有限状態機械／状態遷移図	システムの構造をモデル化し、全状態、全入力での動作確認をする手法
91	形式手法	数学的論理に基づいた厳密なプログラムの記述方法
92	性能モデル化	（前述に同じ）
93	タイムペトリネット	タイムペトリネットとは、状態（プレース)、処理（トランディッション）とそれらの関係を表す図を使って、システム機能等を単純化して表現し、これを数式に置き換えて全体の挙動等の解析に用いる手法
94	プロトタイピング／アニメーション	（前述に同じ）
95	構造ダイアグラム	プログラムの構造を図形で表し、機能の関連付けを表現したもの。動作順序は表現しない。
B.6 性能試験		
96	なだれ／ストレス試験	作業負荷に対する性能を試験するもので、例外的に高い負荷を与える試験
97	応答タイミング、メモリ制約	応答時間、メモリ制約を確実にする為に、平均、最悪の条件下で解析をする手法
98	性能要求事項	実証可能な性能要求を確立する為に、要求仕様の分析と性能計測法を検討、解析する。

No.	技法／方策	技法／方策の概要
B.7 半形式手法		
99	機能ブロック ダイアグラム	プログラムを機能ブロック図で表し、機能を検討するもの
100	シーケンス ダイアグラム	プログラムをシーケンスで表し、機能を検討するもの
101	データフロー ダイアグラム	データの流れをダイアグラムの形に表し、機能を検討するもの。
102	有限状態機械／状態遷移図	（前述に同じ）
103	タイムペトリネット	（前述に同じ）
104	決定表（真理値表）	（前述に同じ）
B.8 静的解析		
105	境界値解析	（前述に同じ）
106	チェックリスト	（前述に同じ）
107	制御フロー解析	プログラムの実行順序を解析し、不正を見つける手法
108	データフロー ダイアグラム	（前述に同じ）
109	エラー推定	エラーが生じそうなケースを考えて試験実施する手法
110	Fagan 検査	活動又はプロセスに対して、開始／終了に対する基準を設けて文書を検査する手法
111	組込み回路解析	組込み回路の意図しない動作を検知する為の解析。構成要素の関連付けに関する質問のチェックリストを利用して実施する
112	シンボル実行	プログラム変数を記号で表し、仕様から抽出され得るべき表現と比較する方法
113	ウォークスルー／デザインレビュー	ウォークスルー／デザインレビュー

No.	技法／方策	技法／方策の概要
B.9 モジュール化手法		
114	ソフトウェア モジュール サイズの制限	ソフトウェアをモジュール化して、モジュール単位のプログラムサイズに制限をつける手法
115	情報隠蔽／カプセル化	ソフトウェアへアクセス可能なデータは、予期せぬ変更があり得る。これを防止する為に、データ構造を隠蔽し、定められた手順でのみ、当該データへのアクセスを可能としておく手法
116	パラメータ番号制限	モジュールでの共通のパラメータを使用する場合、充分に構造化と管理をする手法
117	サブルーチン（機能）の lentry/ lexit 化	サブルーチンへの入力、出力を１つのみにする手法
118	完全定義インタフェース	モジュールの全てのインタフェースを完全に定義する手法

コラム 3：SIL の訳語

Safety Integrity Level の邦訳語については、諸説あるようだ。そもそも integrity とは、訳しづらい単語である。手元の辞書には、以下の記載がある。integrity については、まず第 1 に、"If you have integrity, you are honest and firm in your moral principles."とあって、正直とか誠実とか高潔とかいう訳語が与えられている。であるから、SIL とは、安全機能の実行がどの程度「誠実」に為されるかを表す指標であり、安全機能に対するディペンダビリティの指標を与えるものと考えてよいだろう。

また、あるイギリス人からは、integrity という単語には、何かをする能力がある／可能であるという語感があって、SIL とは安全を達成する力がどの程度あるかを示すものであり、というわけで、safety level とはしないのだ、という説明を聞いたことがある。

こうしてみると、JIS で採用されている「安全度水準」という訳語は、integrity の意味の込められ具合が若干物足りない感じがするし、「度」と「水準」がだぶついている感もある。

JIS 以外のところでは、「安全整合性水準」という訳語をあてている書物もある。IEC 61508 では、インテグリティをランダム故障に対するインテグリティと、システマチック故障に対するインテグリティに分けて考えているが、どちらに対しても統一的に SIL という指標を用いることで、この 2 つの世界の橋渡しを試みている。この意味であれば、安全整合性水準とは、的を射た翻訳である。だが、本来の「誠実さ」の感じが欠けるし、IEC 61508 の外では必ずしも整合性が問題にならないことも考えられる。

そもそも安全の「全」には integrity の意味が込められているのだから、ずばり「安全水準」と訳せばよいのである、という説も耳にしたことがある。どうにも訳しきれないので、そのまま「安全インテグリティレベル」としている記述もみかける。何かよい訳語はないものかと思うが、そのためには、まず SIL の概念を体得して納得する必要があるのかもしれない。

MI（水口 大知）

6.3 本章のまとめ

本章では、IEC 61508 に沿って、ソフトウェアの機能安全設計方法について概略を解説してきた。しかしながら、ソフトウェアの特質として当初の目的、用途に対する設計において安全設計を実施していたとしても、その目的や用途、使用される環境が変わってしまった場合は、いかに当初、機能安全設計を施した製品であっても、そのソフトウェアにおける安全は保障されなくなることを考慮しておく必要がある。また、安全度水準の決定についてもソフトウェアは定量的な評価が困難なこともあり、本章で述べたようにソフトウェアのライフサイクル上で推奨される技法／方策におけるベストプラティクスによって与えられることになる。

参考文献（第 6 章）

1)向殿政男監修、向殿政男、宮崎浩一共著「安全設計の基本概念」安全の国際規格第 1 巻 2007 年 5 月 21 日 日本規格協会発行

2)向殿政男監修、向殿政男、宮崎浩一共著「機械安全」安全の国際規格第 2 巻 2007 年 6 月 25 日 日本規格協会発行

3)向殿政男監修、井上洋一ほか著「制御システムの安全」安全の国際規格第 3 巻 2007 年 9 月 25 日 日本規格協会発行

4)独立行政法人原子力安全基盤機構　規格基準部 成果報告書 2006 年度
「ディジタル安全保護系規制要件調査等に関する報告」
http://www4.jnes.go.jp/katsudou/seika/2006/kikaku/07kihi-0005.pdf

第7章　機能安全の動向

本章では、機能安全規格の出てきた背景、我が国における取組みの現状を振り返り、機能安全の今後の動向を考察する。規格のみかけの表現にとらわれるだけではなく、その本質的な意味を理解して用いるための啓蒙活動の重要さと、機能安全に配慮した開発ツールの重要さを指摘する。

7.1 機能安全規格の背景

近代技術の急速な発展に伴って、従業員や地域住民への危害を与える大きな事故が起こっている。このような事故に対し、従来は、事故が起こってから対策するという事後対応型となっていたが、これでは別の形で発生する新たな事故の発生は防ぐことはできないと考えられるようになり、事前にリスクを評価し、事故を予防することが求められるようになってきた。欧米では、これらの事故を分析し、事故が起きる要因として、技術的要因、組織的要因、個人的要因の 3 要素を総合的に考慮した規定を設けなければ安全は守れないという考え方にいたっている（**図 7.1**）。このような、安全に関する体系的な考察から、リスクの事前評価に関する規格 ISO 14121 や、機械安全に関する規格 ISO 12100、電気系の安全にかかわる機能安全規格 IEC 61508 などが、欧米で制定されてきている。品質・環境規格に続く第 3 の波としての安全規格の登場である。これは、安全を守るという観点で重要な規格であるが、各国の文化に応じて異なった捉え方をされ得る規格でもある。IEC61508 の例でいうと、その規格の一部に、国によって意見の相違があり、場合によっては、ある種の関税障壁となってしまうことも懸念されている。別の見方をすると、製品の安全性に絶対的な価値判断の基準があるわけではないことから、規格の解釈に任意性が生じることを意味している。つまり、このような規格を順守していることと、本来の製品の安全性は必ずしも一致はしないということである。しかしながら、安全に関する社会の要望が大きくなり、事故が起こった際の説明責任も非常に重要になっている昨今の事情を考えると、各国が同意する規格が望まれることも確かである。

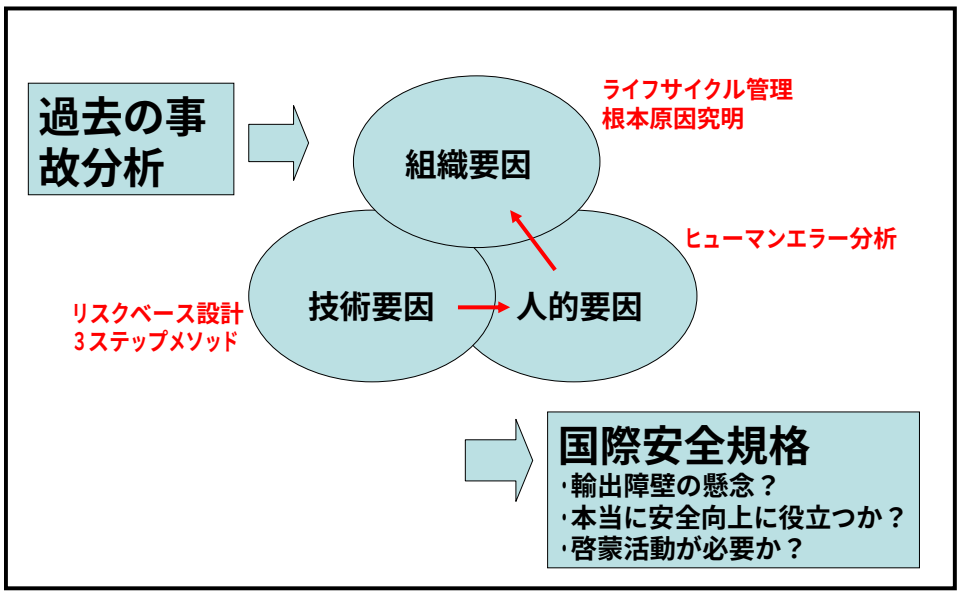


図 7.1　国際安全規格の成立の背景

7.2 我が国の状況

我が国では、自動車や電機産業のように、機械・電機製品を組み合わせた「ものつくり・摺り合わせ技術」の優秀さによって世界的競争力を維持している分野がある。近年のデジタル技術の進展によって、これらの製品の多くは、計算機を内蔵した組込みシステムになっており、顧客の要求に応えるため、高機能化・複雑化が進んでいる。しかしながら、多くの自動車リコール・不具合事象[1)]や、最近では、JR の改札機トラブル[2)]のように、サービスを提供する組込みシステムのバグや不具合は、多大な経済的損失をもたらすばかりでなく、場合によっては、人身事故をもたらす可能性もある。このような背景から、複雑化する組込みシステムの安全性を担保する技術が強く求められるようになってきた。しかしながら、組込みシステムの開発ニーズの急増、開発期間の短期化、人手不足の深刻化などのため、不具合の可能性も増大する一方の状況になっている。また、グローバル化に従って､欧米からの機能安全に対する要求やアジアへのオフショア開発等が急速に増えている。そのような情勢の中で、世界標準規格に合わせた製品開発が強く望まれるようにもなってきている。

社会の成熟に伴って、今後、工学的製品への安全・安心への要求はますます強くなることが想定されるが、これは、安全性の担保だけでなく、不安全事象が起こった際の説明責任の増大も同時に意味することになる。また、製造物責任は、製品のライフサイクルにわたった管理を要求することになる。さらに、ビジネスのグローバル化は、従来の暗黙値に基づいた擦り合わせ技術的な製品ではなく、世界標準規格に基づいて明示的に安全を主張できる製品を求めるようになる。

このような環境から、国内でも機能安全を取り込んでいる会社が近年増えている。組込みシステムの機能安全に関する製品認証を受けた企業、機能安全認証の製品開発に用いることのできる汎用 OS を提供している企業､機能安全認証のためのコンサルテーション活動をしている企業などである。また、欧州とのビジネスの中で、機能安全規格の理解の必要性を感じ、ごく最近になって機能安全の規格の習得へ取り組み始めているところもある。これらの動向は、安全そのものの大事さだけでなく、認証を受けることの大事さやビジネス上の利点への理解が、わが国でも進みつつあることを示している。特に、今後、欧州とのビジネスに関係している会社では、機能安全に関するニーズは著しく増えていくものと思われる。

7.3 啓蒙活動と開発ツールの重要さ [3,4)]

機能安全の中で、特に、ソフトウェアの安全とは何かということに関して、まだ誤解も多く、戸惑っているエンジニアも多いと思われる。機能安全に関するセミナーに多くの人が集まることがその根拠である。日本のメーカーとしては、欧米の規格に不必要に流され不利益にならないようにするためにも、規格の意味を理解し、「自社の技術を、それぞれの規格要求事項にどのようにマッピングさせるか」という知識とノウハウをもつ人材が必要となる。現在、機能安全規格を体系的に学習し、その本質的内容を理解・把握している技術者は少なく、OJT により欧州からの要求に対応しているのが実状といえる。

また、より安全な設計であっても、世界の標準規格に対応項目がないため、その規格そのものにとっては意味がない場合もある。このような規格にない、日本メーカー独自の安全に関する工夫・ノウハウが多くあり、これらが、日本の製品の品質と安全を高めているともいえる。それらをどのように整理して標準規格に反映・提案するか、どのように一般化した知識・ノウハウとして整理し国内に広げるか、アジア諸国へのオフショア開発において安全システムの開発管理にどのように活用するか、といったことは緊急な課題となっている。そのために、ノウハウ・経験の整理や企業間の連携・交流によって、日本全体の機能安全のレベルや提案力をあげ、国際競争力を向上することが不可欠である。

このような独自の安全規格や安全思想を立ち上げるために望まれることは、教育機関や独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター（IPA/SEC）のような独立行政機関が、企業の営利目的から一定の距離をもって音頭をとり、規格化を推進するための努力をすることである。具体的には、機能安全の規格論だけではなく、現場で実用的に使えるマニュアルの作成や演習や実例を含む機能安全教材の作成、それらを普及するための人材の育成などが必要である。

RTOS として機能安全の SIL3 認証を得た会社が海外に複数社あるが、認証のために多大な努力をしている [3)]。また、国内でも、名古屋大学付属組込みシステム研究センターで自動車の制御を想定した SIL3 対応の RTOS 開発プロジェクトが進行中である。これらは、あくまで、SIL3 対応の応用システムを作るための一部品ではあるが、それらの基盤技術(API や使用マニュアル）を使えば、機能安全対応可能なミドルウェアやアプリケーションシステムがより確実に開発できる。これは、ソフトウェア信頼性と安全性だけでなく、開発期間・コストの低減、認証コストの低減に役立つ。これは、安全システム開発に対応できる開発ツールといえるが、現状、欧米で開発されたものしかなく、日本では、まだ本格的に活用する会社は少ない。それは、機能安全に対する認識がまだ広がっていないことも原因であるが、慣れない開発ツールの使用によるトラブルへの不安、コスト高への不安も原因の一つと考えられる。しかし、事故等が発生し、ニュースになるたびに、社会や利用者からの信頼を失い、企業自身に大きな負担・損害をこうむる最近の社会状況を考えると、安

全に対してさらなるコストを払う決心をする必要があり、そこには、日本版の規格や開発ツールの開発と普及が含まれるといえよう。

国内では、機能安全に対する認知度は徐々に増えているものの、まだまだ低い状況である。しかしながら、前述の安全に対する要求のグローバル化を考えると、必然的に、安全規格に基づいた透明性を持った製品の開発が必要になり、さらに、それを支援する日本型の開発ツールの必要性がさらに増えるものと考えられる。海外では安全認証のために多くのコンサルテーション会社が活躍しているが、そこでは、認証のための支援ツールが必須とされている（**図 7.2、7.3**）。日本独自のこのようなツール（**図 7.4**）も存在するが、まだ、その普及は十分ではなく、今後、企業の壁を超えた協力体制による開発が望まれる。また、国内型の、形式手法・半形式手法ツールなどの開発も重要である。企業内に蓄えられた製品開発のための開発ツールやコーディングガイドを汎用化し、社会に提供することも、今後大切になる。コーディングガイドについては、C 言語は MISRA 規格が確立されていたが、最近（2008 年）、C++についても同様の規格が公開された。情報公開によるデファクトスタンダード化やオープンソース戦略が、多くの成功を収めているように、安全に関する汎用ツールを開発し、社会に提供していくことが、今後ますます大事になると考えられる。さらに、これらを支えるために、大学での教育体制の整備や啓蒙活動、国の機関による規格化、標準化支援体制などが重要になってくる。

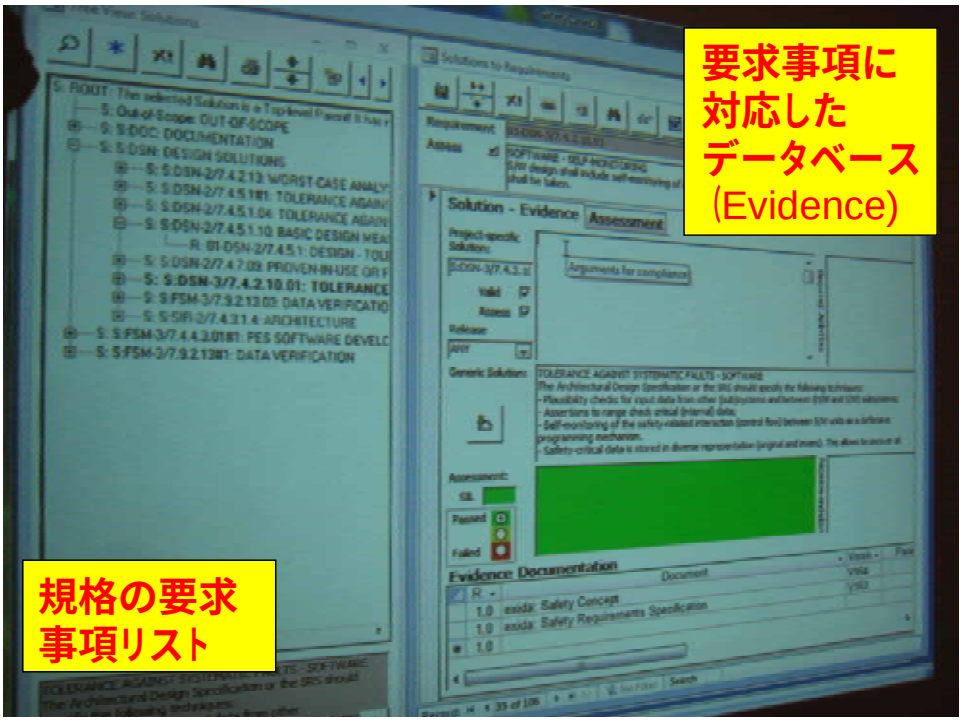


図 7.2　開発ツールの例（SAFETY CASE DATABASE/Exida 社）

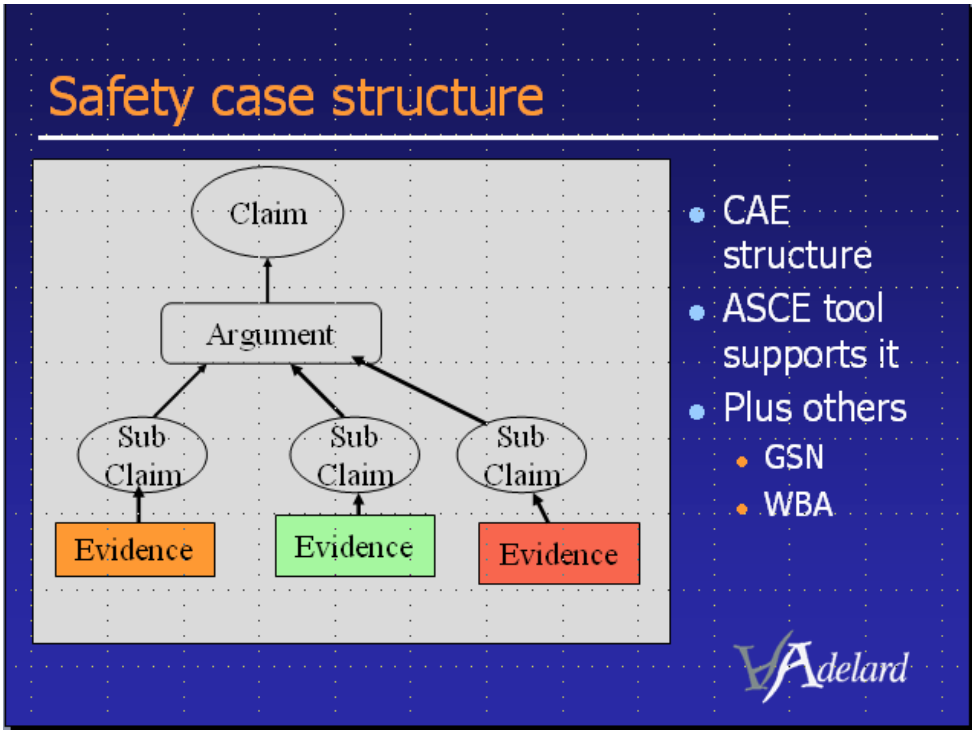


図 7.3　開発ツールの例（SAFETY CASE Environment/Adelard 社）[5)]

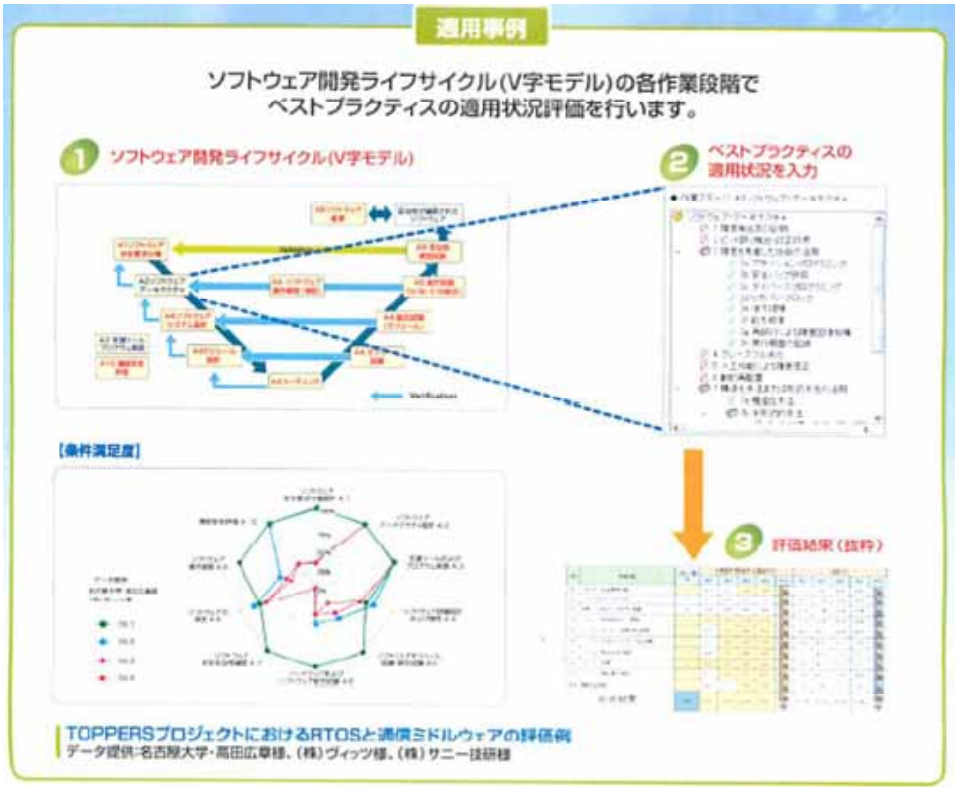


図 7.4　開発ツールの例（安診太郎™/東芝システムテクノロジー（株））

7.4 今後の課題

機能安全に関する啓蒙活動、国の機関による規格化・標準化支援体制、実用的な開発ツールの重要さは、上記で指摘したとおりであるが、これと平行して、企業内や企業間、企業と利用者の間で、安全規格・安全思想・安全文化を共有化し、安全意識を向上することは非常に重要と考えられる。この観点から、メーカーだけではなく、サービスの業者（運転者）や利用者も含めて、安全対応の資格と能力が求められ、常に安全に関する教育を受け、自らレベルを向上することが重要になってくる。このような活動を活性化するためには、今後、下記のような各分野の検討が必要と考えられる。

1) 安全設計の事例研究

各産業分野の安全設計の事例を学び、共有化する仕組みを確立する。また、安全認証を取得した製品の継続的な調査も望まれる。

2) 安全解析・安全評価にかかわる技法・手法の研究

組込みシステムに適用可能な HAZOP、FTA、FMEA などの故障解析技法を調査し、その実用性を検証する。例えば、引用文献では、Software のための HAZOP 解析[6]、制御系も含めた化学プラントのための潜在故障自動解析法の研究[7,8]などの試みが紹介されている。これらの潜在リスク分析支援ツールの実用性の調査、組込み系への適用可能性の検証などが望まれる。

3) 安全設計技法、リスク低減手法の研究

形式手法、半形式手法、自己診断技法など、組込み系に有効と思われる各技法・手法について調査し、その実用性を検証する。また、前記の安診太郎™や、SAFETY CASE DATABASE などの認証支援ツールの有効性の検証も望まれる。

4) 安全性向上のためのモデル契約書の検討[9,10]

ソフトウェアの信頼性を向上するためのモデル契約書として、「情報システム・モデル取引・契約書〈第一版〉(2007 年 4 月)」が発行されている。基本事項をほぼ網羅しており、価値高い文書であるが、これには、組込み系はまだ考慮されていない。また、情報セキュリティと機能安全の確保については、特段の言及はなく、今後の課題となっている。前記のツールや手法の整備とあわせて、安全性への考慮、契約や開発プロセスなどの取引フレームまで含めた、組込み系のモデル契約書の検討が望まれる。特に、規制－ユーザー（事業者）－メーカーの各組織の間での安全にかかわる認証や、契約にかかわる考え方の整理は、国によっても異なるため、我が国の実情だけでなく、国際ビジネスを考慮して標準的な考え方を整理しておくことが望まれる。

7.5 本章のまとめ

本章では、以下の事項について議論した。

(1)機能安全規格の背景

(2)我が国の状況

(3)啓蒙活動および開発ツールの必要性

(4)今後の課題

組込みシステムの高機能化・複雑化に伴って、機能安全規格は、今後ますます重要になる。その本質的な意味を理解して用いるためにも、啓蒙活動や開発ツールの活用、モデル契約書の概念などが今後重要になろう。

引用文献

1)自動車のリコール・不具合情報、国土交通省
http://www.mlit.go.jp/jidosha/carinf/rcl/recall.html

2)産経ニュース、2007 年 10 月 12 日
http://sankei.jp.msn.com/affairs/disaster/071012/dst0710120736001-n1.htm

3)IPA-SEC 調査報告、「機能安全に関する先行研究(1)」(会津大学)、2008 年 3 月

4)IPA-SEC 調査報告、「機能安全に関する先行研究(2)」(会津大学)、2009 年 3 月

5) Assurance and Safety Case Environment (ASCE™)、Adelard LLP.
http://www.adelard.com/web/index.html

6)F.Redmill, M.Chudleigh and J.Catmur, “System Safety; HAZOP and Software HAZOP”, John Wiley and Son, 1999.

7)N.L. Rossing, et al., “A Goal Based Methodology for HAZOP Analysis”, Proceeding of Joint International Symposium of ISSNP2008/CSEPC2008/ISOFEC2008, Harbin, China, Vol.2, pp.3-10, 2008.

8)A.Gofuku and A.Ohara, “Fault Tree Analysis of Chemical Plants based on Multi-Level Flow Modeling”, Proceeding of Joint International Symposium of ISSNP2008/CSEPC2008/ISOFEC2008, Harbin, China, Vol.2, pp.3-10, 2008.

9)情報システム信頼性向上のための取引慣行・契約に関する研究会」最終報告書
http://www.meti.go.jp/policy/it_policy/keiyaku/

10)モデル取引・契約書<第一版>(PDF 版)
http://www.meti.go.jp/policy/it_policy/keiyaku/model_keiyakusyo.pdf

第8章　SIL3取得関連製品の現状

規格認証機関から SIL3 認証を得ている製品の現状を調査した。システム又はソフトウェアを構成するコンポーネント、並びに開発を支援するツールに分けて調査を行った。システム製品は、完成品として顧客に直接提供されるから、この調査からは除外した。調査方法の概要を**表 8.1** に示す。

製品を機能面から分類するため、製品区分を定義した。安全関連系は、センサ、コントローラ、アクチュエータ、ネットワークから構成されるから、製品区分はそのどれかに対応する。製品区分のシステム構成における対応づけは、**図 8.1** に示す。

製品区分と調査した製品数は**表 8.2** のとおり。調査対象の製品一覧を**表 8.3** に示し、各製品の概要をそれ以降に掲載する。

表 8.1　調査方法の概要

調査期間	2008 年 12 月から 2009 年 2 月。
調査対象	ET2008 等の展示会、ネット検索等を利用して抽出した。なお、既に認証を取得しているものだけでなく、今後、認証取得を予定している製品、又は認証取得を支援する製品も含めた。
調査票の作成	製品カタログ、ホームページに公開されている資料等を参照し、一部、販売元の協力を得て調査票を作成。

※この章に記載している会社名、製品名等は、それぞれの会社の登録商標または商標です。
※SIL3 関連製品の調査については、本書の執筆委員が分担して行った。

また、各製品の詳細調査と編集作業は、株式会社レンタコーチ中村氏に委託した。

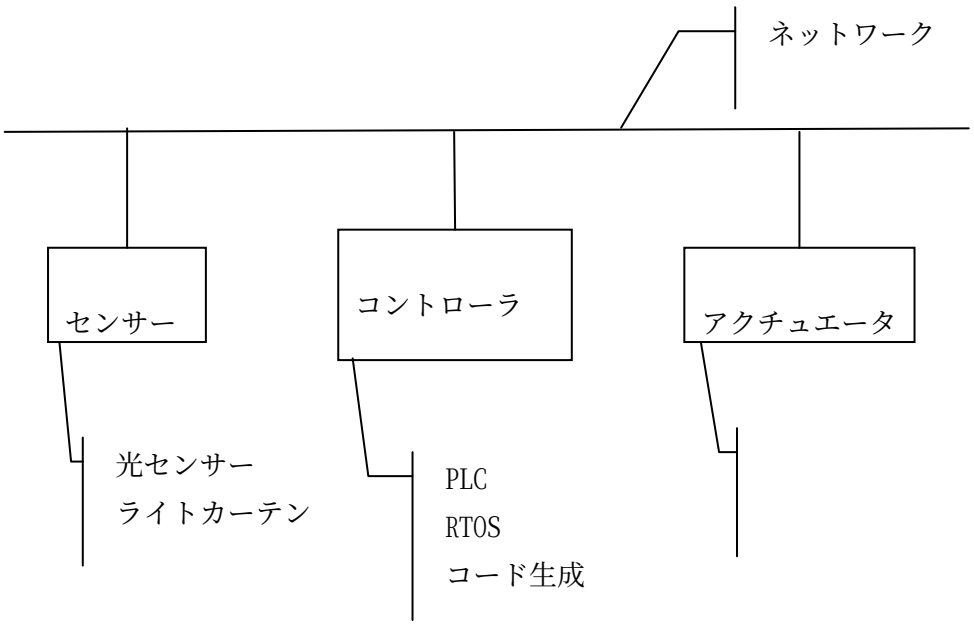


図 8.1　システム構成における製品区分の対応付け

表 8.2　種別と製品区分

種別	製品区分	製品数
システムコンポーネント	PLC	8
	ネットワーク	1
	光センサー	1
	ライトカーテン	1
ソフトウェアコンポーネント	RTOS	2
ツール	コード生成	2
	安全性評価	1

表 8.3　SIL3 取得関連製品一覧

番号	開発元/販売元	製品名	製品区分
1	Green Hills Software/ アドバンスドデータコントロールズ	INTEGRITY	RTOS
2	ETAS/ イータス	ASCET	コード生成
3	Wind River/ ウィンドリバー	VxWorks	RTOS
4	オムロン	セーフティネットワークコントローラ NE1A-SCPU シリーズ	PLC
5	オムロン	フレキシブルセーフティユニット G9SX	PLC
6	キーエンス	セーフティライトカーテン SL-V シリーズ	ライトカーテン
7	キーエンス	セーフティコントローラ SC シリーズ	PLC
8	光洋電子工業	KOSTAC　Safety　AZ-C1	PLC
9	サンクス	小型ビームセンサ ST4	光センサ
10	Esterel Technologies/ シーディアダプコジャパン	SCADE Suite	コード生成
11	ジェイテクト（JTEKT）	TOYOPUC-PCS	PLC
12	東芝システムテクノロジー	安診太郎	安全性評価
13	日本 AS-i 協会会員	AS-Interface Safety at Work	ネットワーク
14	シュナイダーエレクトリック/ 富士電機機器制御	Preventa　XPS　MC シリーズ	PLC
15	三菱電機	安全シーケンサ MELSEC safety	PLC
16	Rockwell Automation/ ロックウェルオートメーションジャパン	GuardPLC システム	PLC

備考:　記載順は、販売元の五十音順。

SIL3 関連製品調査票（1）

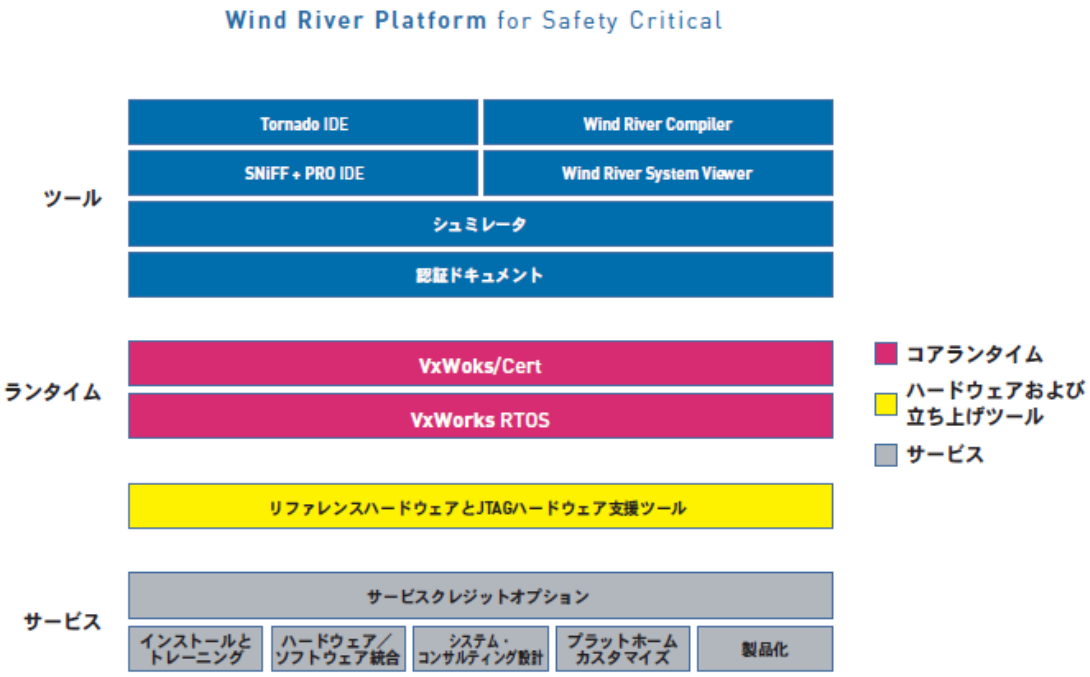
種別		ソフトウェアコンポーネント	
製品名		INTEGRITY	
製品区分		RTOS	
特徴	主要機能	● 仮想アドレス空間を使ってカーネルとタスクのメモリ空間を分離し、かつタスク間のメモリ空間を分離。 ● タスクごとにメモリとプロセサ時間の割当てを保証。 ● 高速な割り込み処理によって極小の割込遅延時間（約 200ns）を達成。 ● POSIX、VxWorks、μITRON 向けの API を提供。 ● 静的解析ツール等を有する統合開発環境 MULTI を備え、最新のモデルベース開発ツールとの協調連携が可能。	
	動作条件/ 動作環境	● ハードウェアによるメモリ保護機構が必要。 ● X86、ARM、OMAP 等のアーキテクチャをサポート。	
規格	適合規格	SIL3	DO-178B（レベル A）
	取得時期	2006 年 6 月	
	認定機関	TUV	
開発元		米国 Green Hills Software http://www.ghs.com/	
販売	販売元	アドバンスドデータコントロールズ http://www.adac.co.jp/	
	価格		
	販売時期	販売中	
	製品情報	http://www.adac.co.jp/products/integrity/details/page01.html	
利用ガイド		● 航空宇宙、防衛等の分野で使用されていて、強いリアルタイム性を必要とする FA 分野等に利用可能。 ● SIL の異なるアプリケーションが混在するとき、それらを分離して相互干渉を防止するために使うことができる。 ● SCADE との連携が可能である。 ● 認証取得のためのコンサルティングや支援サービスを利用できる（提供は Exida 社）。	

SIL3 関連製品調査票（2）

種別		ツール
製品名		ASCET
製品区分		コード生成
特徴	主要機能	● ASCET は自動車用 ECU ソフトウェア開発を支援するツールセット。モデリング、プロトタイピング、コード生成等を支援する。 ● ASCET-SE はモデルから各種マイクロプロセサをターゲットとする量産用 ECU コードを自動生成するツール。 ● AUTOSAR 準拠の開発を支援できる。 ● MATLAB/Simulink モデル及び UML 表記からの変換が可能。 ● XML 形式でデータを保存し、要件管理、構成管理等のツールとの連携が可能。 ● 対応するマイクロプロセサは、日立、NEC、Motorola、Infineon、TI 等。 ● 生成されたコードは、MISRA-C に準拠し、SIL3 に適合する。
	動作条件/動作環境	
規格	適合規格	SIL3
	取得時期	
	認定機関	TUV
開発元		ETAS（ドイツ） http://www.etas.com/ja/about_etas.php 車載 ECU 用ソフトウェア開発ツールの専門メーカであり、2004 年から AUTOSAR のプレミアムメンバになっている。
販売	販売元	イータス http://www.etas.com/ja/index.php
	価格	
	販売時期	販売中
	製品情報	http://www.etas.com/ja/products/ascet_software_products.php
利用ガイド		● 1997 年のリリース以来、生成されたコードは数千万もの量産用 ECU で使用されている。 ● 車載用のソフトウェアの開発、あるいはモデルベース開発を行うときに利用できるツールである。

SIL3 関連製品調査票（3）

種別		ソフトウェアコンポーネント	
製品名		VxWorks	
製品区分		RTOS	
特徴	主要機能	● 航空宇宙、船舶等の分野に適用できる高い応答性を有している。 ● 認証取得のための開発プロセスを規定。 ● 認証が取れる API サブセット VxWorks/Cert を規定。 ● 取得に必要な膨大なドキュメントを提供する。	
	動作条件/ 動作環境		
規格	適合規格	SIL3（認証可能）	DO-178B（レベル A、認証可能）
	取得時期		
	認定機関		
開発元		Wind River（米国） http://www.windriver.com/	
販売	販売元	ウィンドリバー http://www.windriver.com/japan/	
	価格		
	販売時期	販売中	
	製品情報	http://www.windriver.com/japan/products/vxworks/index.html	
利用ガイド		認証取得を支援するために、Wind River Platform for Safety Critical というソリューションを提供している。その概要は図 8.2 を参照。	

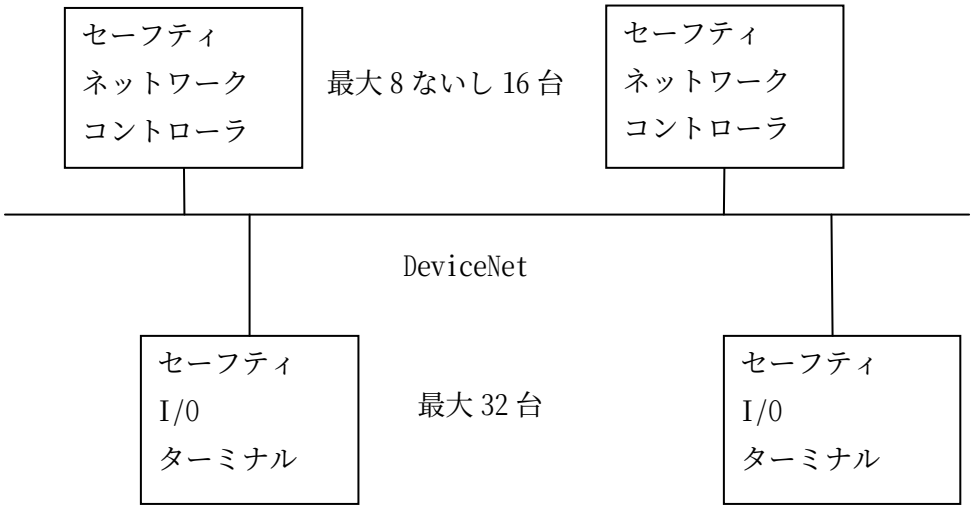


出典:ウィンドリバー社の製品カタログから引用

図 8.2　認証可能な COTS ソリューションの体系図

SIL3 関連製品調査票（4）

種別		システムコンポーネント	
製品名		セーフティネットワークコントローラ NE1A-SCPU シリーズ	
製品区分		PLC	
特徴	主要機能	● 従来、リレーを組合わせていた安全制御回路のプログラマブル化を実現。用意されているファンクションブロックを選択、組み合わせてプログラムを作成できる。 ● マルチベンダネットワーク DeviceNet に接続でき、DeviceNet Safety システムを構成できる。システム構成図は図 8.3 を参照。 ● 1 台のコントローラは、12 ないし 16 入力可能。ネットワークに 16 ないし 8 台までのコントローラを接続可能。 ● I/O ターミナルは、最大 16 点の入出力可能で、32 台までネットワークに接続可能。 ● 標準コントローラからも安全システムのモニタリングが可能。	
	動作条件/動作環境	ネットワークとして DeviceNet を使用できる。	
規格	適合規格	SIL3	ISO13849-1（カテゴリ 4）
	取得時期		
	認定機関	TUV	
開発元		オムロン http://www.omron.co.jp/r_d/index.html	
販売	販売元	オムロン http://www.fa.omron.co.jp/index.html	
	価格	ネットワークコントローラ NE1A-SCPU01-V1:　20 万円 I/O ターミナル DST1-ID12SL-1:　9 万円	
	販売時期	販売中	
	製品情報	http://www.fa.omron.co.jp/product/family/1625/index_p.html http://www.fa.omron.co.jp/product/family/1626/index_p.html	
利用ガイド		リレーで構成していた安全制御回路を PLC に置き換え、かつ、マルチベンダネットワーク DeviceNet での接続を実現できる。	



コントローラとターミナルはそれぞれ安全入出力を有する。

図 8.3　DeviceNet Safety システムの構成図

SIL3 関連製品調査票（5）

種別		システムコンポーネント	
製品名		フレキシブル　セーフティユニット G9SX	
製品区分		PLC	
特徴	主要機能	● 従来のリレーに比べて、多入力、多出力の複雑な安全制御回路を柔軟に構成できる。 ● 論理接続機能によって拡張が容易。	
	動作条件/動作環境		
規格	適合規格	SIL3	IS013849-1（カテゴリ 4）
	取得時期		
	認定機関	TUV	
開発元		オムロン http://www.omron.co.jp/r_d/index.html	
販売	販売元	オムロン http://www.fa.omron.co.jp/index.html	
	価格	G9SX-AD322-T15-RT: 47,000 円	
	リリース時期	販売中	
	製品情報	http://www.fa.omron.co.jp/product/family/1524/index_p.html	
利用ガイド		装置をユニットごとに停止させたり、装置の構成変更が多い安全制御回路に適用できる。	

SIL3 関連製品調査票（6）

種別		システムコンポーネント	
製品名		セーフティ　ライトカーテン SL-V シリーズ	
製品区分		ライトカーテン	
特徴	主要機能	● 機器の存在が見える表示灯内蔵。 ● スリムタイプだけでなく、堅牢・防水タイプもラインアップ。	
	動作条件/ 動作環境	● スリムタイプ保護構造 IP65 ● 堅牢・防水タイプ IP67/65	
規格	適合規格	SIL3	IS013849-1（カテゴリ 4、PLe）
	取得時期	2007 年 3 月	同左
	認定機関	TUV	同左
開発元		キーエンス http://www.keyence.co.jp/index.jsp	
販売	販売元	キーエンス	
	価格	65,000 円から	
	販売時期	2007 年 3 月から販売	
	製品情報	http://www.keyence.co.jp/switch/safety/sl_v/index.jsp	
利用ガイド		危険区域への侵入検知に利用。	

SIL3 関連製品調査票（7）

種別		システムコンポーネント	
製品名		セーフティコントローラ SC シリーズ	
製品区分		PLC	
特徴	主要機能	● ユニット増設によってフレキシブルに安全 I/O を増設可能。 ● 部分停止/全停止やロボットティーチング制御にも対応可能。	
	動作条件/動作環境	保護構造 IP20（制御盤内での使用）	
規格	適合規格	SIL3	IS013849-1（カテゴリ 4、PLe）
	取得時期	2007 年 8 月	同左
	認定機関	TUV UL	同左
開発元		キーエンス http://www.keyence.co.jp/index.jsp	
販売	販売元	キーエンス	
	価格	28,000 円から	
	販売時期	2007 年 8 月から販売	
	製品情報	http://www.keyence.co.jp/switch/safety/sl_v/index.jsp	
利用ガイド		安全機器制御実施時に利用。	

SIL3 関連製品調査票（8）

種別		システムコンポーネント	
製品名		KOSTAC　Safety　AZ-C1	
製品区分		PLC	
特徴	主要機能	● プログラミングとして、ファンクションブロック機能とラダー機能を用意している。 ● 安全及び非安全の制御を１台で実行できる。 ● S/N インターフェイス機能（各種オープンネットワーク接続用 I/F　別途ゲートウェイモジュールが必要） ● 安全ラダ-回路チェック機能	
	動作条件/動作環境	● 電源　DC24V　2A ● 周囲温度　0-55 ℃ ● 相対湿度　30-85% RH（但し結露なきこと）	
規格	適合規格	SIL3	IS013849-1（PLe）
	取得時期	2008 年	同左
	認定機関	TUV BGIA（ドイツ労働安全技術研究所）	
開発元		ジェイテクト http://www.jtekt.co.jp/index.html ステアリング装置（自動車用）と駆動部品、各種ベアリング、各種工作機械、制御機器を製造、販売。	
販売	販売元	光洋電子工業 http://www.koyoele.co.jp/	
	価格		
	販売時期	2009 年 3 月販売開始予定	
	製品情報	問い合せ先は次の通り: 光洋電子工業株式会社 東京都小平市天神町１－１７１ サポートセンタ Tel　042-349-7700 Fax　042-345-7994 mail　info@koyoele.co.jp	
利用ガイド		● 従来の安全制御回路のプログラム化を実現。 ● ファンクションブロック機能による安全回路の標準化。	

SIL3 関連製品調査票（9）

種別		システムコンポーネント	
製品名		小型ビームセンサ ST4	
製品区分		光センサ	
特徴	主要機能	● LED ビームを用いて、1 センサヘッドあたり最長 15m の範囲を感知できる。 ● 1 コントローラに最大 6 センサヘッドを取り付け可能。 ● 最大 3 コントローラまで無干渉で構成できる。	
	動作条件/動作環境		
規格	適合規格	SIL3	IS013849-1（カテゴリ 4、PLe）
	取得時期		
	認定機関		
開発元		サンクス http://sunx.jp/japanese/company/profile/technology.html センシング技術とレーザ技術をコア技術として、FA 化に貢献している。	
販売	販売元	サンクス http://sunx.jp/index.html	
	価格	● センサヘッド: 19,800 円から ● コントローラ: 39,800 円から	
	販売時期	販売中	
	製品情報	http://sunx.jp/japanese/products/safety/st4/index.html	
利用ガイド		危険区域における侵入検知に利用する。	

SIL3 関連製品調査票（10）

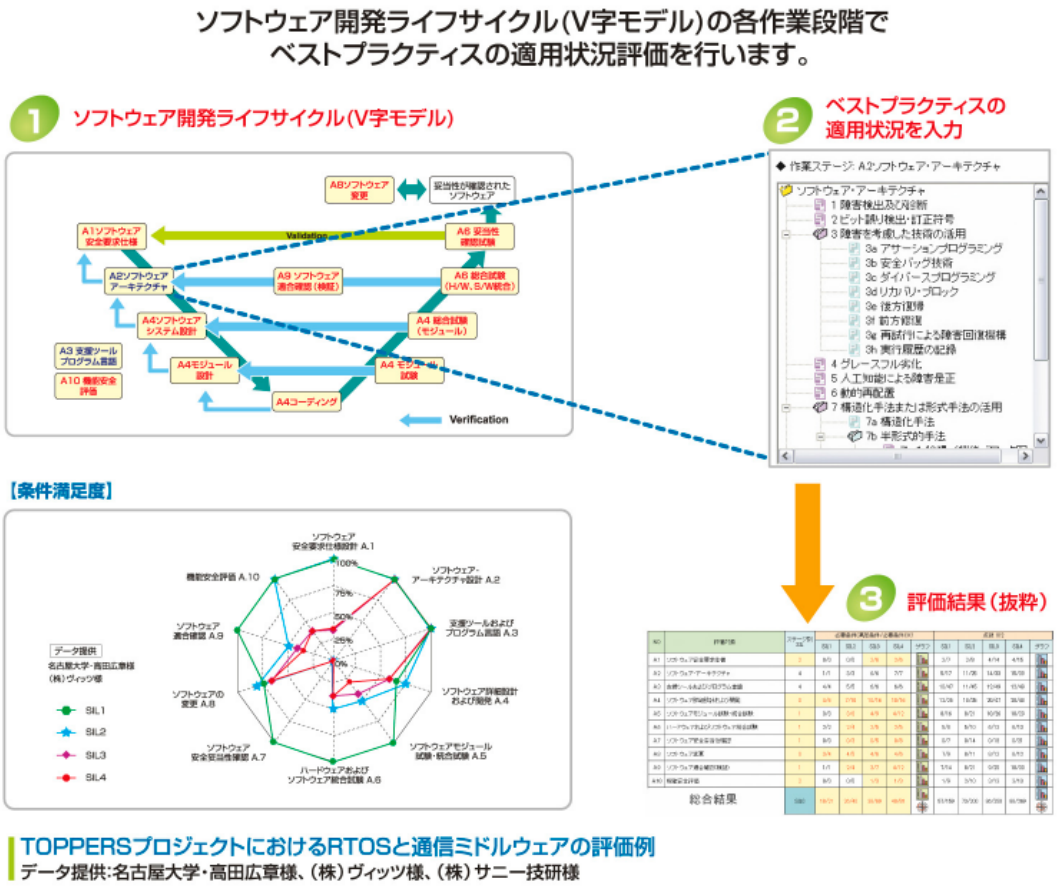
種別		ツール	
製品名		SCADE Suite	
製品区分		コード生成	
特徴	主要機能	● 要件管理機能によるトレーサビリティ管理 ● システム設計ツールとのインターフェース（SysML/UML、アルゴリズム設計ツール） ● SCADE 言語によるモデリング（データフロー/制御フローの自由な構造） ● モデルレベルでの検証支援（セマンティックチェック、モデルシミュレーション、モデルカバレッジ、形式検証、ワーストケース実行時間見積り、コンパイラ検証キット） ● 認証可能な C コードの自動生成 ● 設計モデルに対するレポートの自動生成	
	動作条件/動作環境	対象 OS は、Windows XP、Windows VISTA	
規格	適合規格	SIL3/ EN-50128（SIL4）	DO-178B（レベル A）
	取得時期	2008 年 11 月（SCADE6.0 版）	製品版ごとで認証取得
	認定機関	TUV	
開発元		Esterel Technologies（フランス） http://www.esterel-technologies.com/	
販売	販売元	シーディー・アダプコ・ジャパン http:://www.cdaj.co.jp/	
	価格	450 万～ （モジュール構成で価格は変わる）	
	販売時期	販売中	
	製品情報	http://www.cdaj.co.jp/product/070000scade/index.html	
利用ガイド		● 要件管理からソフトウェア設計、検証、自動コード生成、ドキュメント生成までの工程を１ツール環境でサポートできる。 ● 民間航空・宇宙・防衛の分野で主に使用されていて、DO-178B レベル A 認証プロジェクトでの適用実績あり。IEC-61508/EN-50128 認証プロジェクトにも適用中。 ● 生成コードは、MISRA-C 準拠、ANSI-C 準拠。 ● RTOS（INTEGROTY, VxWorks）統合コード生成可能。 ● 認証取得のためのコンサルティングや支援サービスを利用できる（各規格に対するハンドブック提供）。	

SIL3 関連製品調査票（11）

種別		システムコンポーネント	
製品名		TOYOPUC-PCS	
製品区分		PLC	
特徴	主要機能	● プログラミングとして、ファンクションブロック機能とラダー機能を用意している。 ● 安全フィールドバス機能 ● S/N インターフェイス機能（各種オープンネットワーク接続用 I/F　別途ゲートウェイモジュール必要） ● 安全ラダー回路チェック機能	
	動作条件/動作環境	● 電源　DC24V　2.5A ● 周囲温度　0-50 ℃ ● 相対湿度　30-85% RH（但し結露なきこと）	
規格	適合規格	SIL3	IS013849-1（PLe）
	取得時期	2004 年	同左
	認定機関	TUV BGIA（ドイツ労働安全技術研究所）	
開発元		ジェイテクト http://www.jtekt.co.jp/index.html ステアリング装置（自動車用）と駆動部品、各種ベアリング、各種工作機械、制御機器を製造、販売。	
販売	販売元	ジェイテクト	
	価格	営業に問い合せ（0566-25-5140）	
	販売時期	販売中	
	製品情報	http://www.jtekt.co.jp/products/toyopuc/toyopuc-pcs/index.htm	
利用ガイド		● 従来の安全制御回路のプログラム化を実現。 ● ファンクションブロック機能による安全回路のスリム化および標準化。 ● 安全フィールドバス機能による大規模システム対応。	

SIL3 関連製品調査票（12）

種別		ツール
製品名		安診太郎
製品区分		安全性評価
特徴	主要機能	● IEC61508 に基づいてソフトウェアの機能安全性を総合的に評価する。 ● 開発プロセスに照らして、各フェーズごとに安全度の達成度をグラフ、表を用いてわかりやすく表示する。適用事例として図 8.4 を参照。
	動作条件/動作環境	対象 OS は、Windows2000/XP Professional
規格	適合規格	
	取得時期	
	認定機関	
開発元		東芝システムテクノロジー http://www3.toshiba.co.jp/tst/
販売	販売元	東芝システムテクノロジー
	価格	
	販売時期	販売中
	製品情報	http://www3.toshiba.co.jp/tst/product/anshintaro.htm
利用ガイド		● 現状の開発プロセス、開発技術力を評価し、目標とする安全度水準との差異を分析するために利用する。 ● ツールに関するコンサルティングも利用可能。

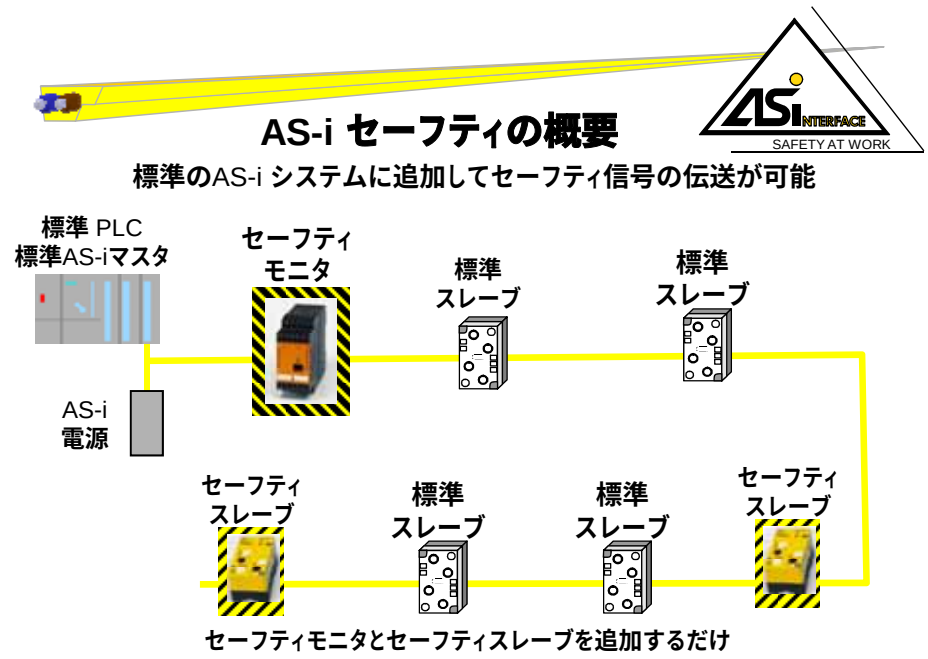


出典:東芝システムテクノロジーの製品カタログから引用

図 8.4　安診太郎の適用事例

SIL3 関連製品調査票（13）

種別		システムコンポーネント	
製品名		AS-Interface Safety at Work	
製品区分		ネットワーク	
特徴	主要機能	● 標準 AS-i システムに非常停止スイッチ等のセーフティ機器を接続することを可能とする。 ● セーフティ信号伝送のために、標準 AS-i システムにセーフティモニタとセーフティスレーブを追加する。スレーブからモニターへの最大応答時間は、40ms。 ● AS-i システムとは、制御システムにセンサー、アクチュエータを接続するネットワークである。システム構成概念図は図 8.5 を参照。	
	動作条件/ 動作環境	● ﾄﾎﾟﾛｼﾞｰ ；トリー，ライン，スターの配線 ● 使用電線；２線式配線で電源と信号を重畳	
規格	適合規格	SIL3	IS013849-1（カテゴリ 4）
	取得時期	2006 年	1999 年
	認定機関	TUV	TUV BGIA（ﾄﾞｲﾂ法令労災保険協会）
開発元		AS-International Association http://www.as-interface.net AS-Interface を普及、促進すること及び、IEC62026-2（AS-Interface を規定）の改定・技術ｻﾎﾟｰﾄをする団体。日本 AS-i 協会は、各国にある協会の一つで、日本国内への普及拡大と各種要望を取りまとめて提出する団体。	
販売	販売元	日本 AS-i 協会会員会社。 （シーメンス／ピーアンドエフ／IDEC／富士電機機器制御等） http://www.as-i.jp/	
	価格		
	販売時期	2006 年	
	製品情報	http://www.as-i.jp/prd_sms1.html	
利用ガイド		制御ネットワークに AS-i を使用していれば、非常停止スイッチ等のセーフティ機器を追加するために利用できる。	



セーフティモニタは、AS-i マスタとセーフティスレーブ間の通信を監視し、異常検出時に安全リレー等を作動させることができる。

出典:日本 AS-i 協会の資料から引用

図 8.5　AS-i セーフティのシステム構成概念図

SIL3 関連製品調査票（14）

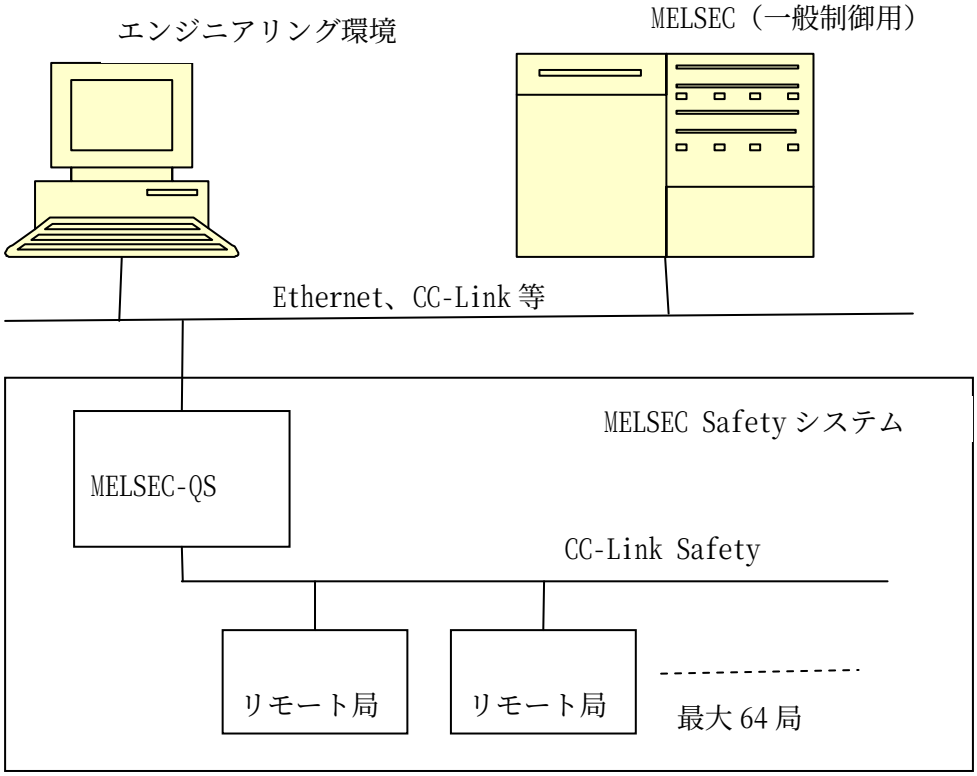
種別		システムコンポーネント	
製品名		Preventa XPS MC シリーズ	
製品区分		PLC	
特徴	主要機能	● それぞれ独立した安全機能を制御できる。その選択と構成は、PC 上のソフトウェアを使って設定できる。 ● 安全入力は 16 ないし 32 点、出力は独立した 8 点までの安全出力が可能。 ● 安全マットのモニタ等、安全機能は 30 種類用意され、すべて認証済み。 ● 通信として、CANopen、Profibus、Modbus に対応できる。	
	動作条件/動作環境	設定用のソフトウェアは Windows 上で稼働する。	
規格	適合規格	SIL3	ISO13849-1（カテゴリ 4）
	取得時期	2005 年 1 月	
	認定機関	TUV	
開発元		シュナイダーエレクトリック（フランス） http://www.schneider-electric.co.jp/index.html	
販売	販売元	富士電機機器制御 http://www.fujielectric.co.jp/fcs/jpn/index.html	
	価格	171,000～277,000 円	
	販売時期	2007 年 12 月	
	製品情報	欄外参照。	
利用ガイド		現在のシステムで複数のリレー装置を使っていれば、省スペース、省配線のために活用できる。	

製品情報の URL:
http://www.fujielectric.co.jp/fcs/jpn/f/f_SE_h02-PreventaXPSM_Series.html

SIL3 関連製品調査票（15）

種別		システムコンポーネント	
製品名		MELSEC Safety	
製品区分		PLC	
特徴	主要機能	● 従来のシーケンサ MELSEC をもとにして、規格に適合させた。 ● 安全規格が要求する診断機能や安全機能をを備えた MELSEC-QS と、安全フィールドネットワーク CC-Link Safety を含む。システム構成概念図は、図 8.6 を参照。 ● 非常停止スイッチ、ライトカーテンなどを接続して、非常停止などの安全制御を実行する。 ● 自己診断機能を持ち、故障検出時に安全出力を強制的に OFF にできる。 ● 最大入力 8 点、出力 4 点のリモート局を最大 64 局接続可能。 ● プログラミングツールは MELSEC と同様で、PC 上の GX Developer にてパラメータ設定、プログラミングする。	
	動作条件/動作環境	プログラミングツールは、PC 上で稼働する。	
規格	適合規格	SIL3	IS013849-1（PLe）
	取得時期	2008 年 3 月	同左
	認定機関	TUV	同左
開発元		三菱電機 http://www.mitsubishielectric.co.jp/corporate/tech/index.html	
販売	販売元	三菱電機 欄外参照。	
	価格		
	販売時期	販売中	
	製品情報	http://wwwf2.mitsubishielectric.co.jp/plcq/safety/index_j.htm	
利用ガイド		● リレー回路からのプログラマブル化を実現。 ● リモート局との接続がネットワーク化しているから、省配線、大規模対応を実現できる。	

販売元の URL:
http://www.mitsubishielectric.co.jp/business/industry/equipment/index.html



GX Developer ツールはエンジニアリング環境で稼働する。

図 8.6　MELSEC Safety システム構成概念図

SIL3 関連製品調査票（16）

種別		システムコンポーネント
製品名		GuardPLC システム
製品区分		PLC
特徴	主要機能	● コントローラ、I/O、プログラミング・構成ツールから構成されている。 ● プログラミング・構成ツールは Windows 上で動く。
	動作条件/動作環境	
規格	適合規格	SIL3
	取得時期	
	認定機関	
開発元		Rockwell Automation（米国） http://www.automation.rockwell.com/
販売	販売元	ロックウェルオートメーションジャパン http://www.automation.rockwell.co.jp/
	価格	
	販売時期	
	製品情報	欄外参照。
利用ガイド		

製品情報:

http://www.automation.rockwell.co.jp/applications/gs/ap/gsjp.nsf/pages/GuardPLC

あとがき

本報告書は、機械安全と機能安全に関する規格を基に、組込み系の設計開発に必要と思われる基本知識を整理してみたものです。現場で使える実践的ガイドには、まだ不足かもしれませんが、機能安全に関する基本知識の習得と安全設計の手がかりになって欲しいと願って活動してきました。

最初は、組込み系を対象に検討してきましたが、内容的には組込み系にとどまらず、一般ソフトウェアの安全設計にも十分参考になるものと思われます。ただし、システムの安全性を確保するためには、さらに情報セキュリティの確保とヒューマンエラー（組織エラーも含めて）対策が必要ですが、本報告書では、議論に含めておりません。

本報告書をまとめる過程で、用語に関して、規格間のずれや不整合も見えてきました。安全の問題に関しては、古く産業革命にまでさかのぼることができます。それ以降、先人達によって法令や規格が整備されてきました。安全対策は、産業分野、技術分野ごとにさらにきめ細かく制定・改良されてきたわけですが、産業を横断して急速に発展してきた組込み系技術分野において、いざあらためて安全の問題を取り上げようと思った時、分野ごとに用語の使い方が違い、とまどってしまったという経験があります。今回も“ fault ”と“ failure ”の違いや混用が議題となりました。

しかしこのような問題があるとしても、第 7 章「機能安全の動向」にも記載していますが、デジタル機器や制御システムは今後とも発展・進化を続ける以上、機能安全は、ますます重要になって来ます。現場で使えるガイドや教材の整備、また人材の育成が必要になってきます。便利な機能の優れたものへ対価を支払うばかりではなく、機能の安全性を確保してくれるものへも対価を支払う時代が本格的に来たのかと、委員各位もあらためてその感を強くしました。

本委員会は、限られた期間の活動でもあったので、まだまだ調査や議論の不足している部分もあると思われます。今後も、委員会活動を継続し、SIL3 製品の調査や、より実践的な安全設計手法の検討を進めていき、情報発信も行っていきたいと思います。有識者の皆様のご意見・ご指導を頂ければ有難いと思っております。

平成 21 年 3 月

JASA　安全性向上委員会　　委員長 漆原憲博
製品安全ワーキンググループ 主査　金田光範

附録

アンケート調査『情報セキュリティ対策実施状況』の結果報告

当ワーキンググループでは、昨年度の情報セキュリティ研究の成果を踏まえ、組込み業界の情報セキュリティ対策に関して、簡易で実質的な制度を目指して検討しておりますが、この度、実態に即したものにするためにアンケート調査を実施しました。

組込み業界として、JASA 会員企業（アンケート依頼時点での JASA 正会員 201 社／事業所）を対象としました。

その結果が出ましたのでここに報告します。

アンケートにご協力をいただいた各社様に感謝を申し上げます。

2009 年 3 月

ＪＡＳＡ 安全性向上委員会

ｾｷｭﾘﾃｨﾜｰｷﾝｸﾞｸﾞﾙｰﾌﾟ

主査 漆原憲博

目次

1．アンケートの実施概要

（1）目的

組込み業界が、情報セキュリティ対策をどのように行っているかの調査。

（資料1「アンケート依頼文書」参照）

（2）アンケートの対象

JASA 協会参加企業正会員 201 社または事業所（アンケート依頼時点）

（3）アンケート回答数

77 社（有効回答 76，アンケート回収率 37.8%）

（4）アンケートの実施期間

2009 年 1 月 6 日～1 月 31 日

（5）アンケートの方式

文書での選択肢への回答方式。

ISMS 認証取得サイト（企業、組織など）は独自調査。

（6）アンケート実施機関

JASA 安全性向上委員会ワーキンググループ

（漆原憲博、済賀宣昭、三輪一義）

2．アンケート結果と評価

（1）情報セキュリティに対する認識

「情報セキュリティが必要」であると回答した会社が 100%であった。

何らかの対策を実施している企業が 81.6%であった。

〈解釈／評価〉

必要が 100%は業界としては当然かもしれない。しかし実施が 80%台であることが業界として高いと評価できるかは意見が分かれるところである。

表1　情報セキュリティに対する認識

		Yes	%
問1	ISMS 第三者認証制度をご存知ですか。	70	92.1%
問2	情報セキュリティ監査制度をご存知ですか。	64	84.2%
問3	**情報セキュリティ対策が必要と思いますか。**	**76**	**100.0%**
問4	情報セキュリティ対策を実施していますか。	62	81.6%

（2）情報セキュリティを進める上での課題

「予算不足、人材の不足、実務の負担が大きい、投資効果が見えづらい」が回答の比率が最も高い項目となっており、40～50%超となっている。

〈解釈／評価〉

必要であるが、効果には確信のない様子がうかがえる。

情報セキュリティへの対策を向上させてゆくためには、この点を踏まえた業界や行政等の施策である必要があろう。

表2　情報セキュリティを進める上での課題

	数	%
1. 内部統制、法的対応等への対応が困難	21	27.6%
2. 取引先の要求への対応が困難	10	13.2%
3. セキュリティ対策予算の不足	**33**	**43.4%**
4. セキュリティ対策推進人材の不足	**39**	**51.3%**
5. どこまで対策すべきか不明	21	27.6%
6. 投資対効果が見えづらい	**33**	**43.4%**
7. 取引先にコスト負担が出来ない	22	28.9%
8. 経営陣の理解が得られない	2	2.6%
9. 教育・訓練が行き届かない	18	23.7%
10. 従業員の意識が低い	13	17.1%
11. 実務上の負担が大きい	**32**	**42.1%**
12. 最適なツールや相談するところがない	5	6.6%

（3）対策実施状況を説明する有効な手段

情報セキュリティ対策の実施状況を対外的に説明するためには、ISMS 認証取得やセキュリティ監査などが必要になる。

業界共通のチェックリストや実施状況確認のフォーマットの要望が大きい。

情報セキュリティポリシーの設定も必要という結果となっている。

〈解釈／評価〉

費用を掛けずに効果を、ということであろう。

表３　対策実施状況を説明する有効な手段

	数	%
1．情報セキュリティポリシーの設定	**50**	**65.8%**
2．セキュリティレベルを証明・確認する業界共通のチェックリスト	**50**	**65.8%**
3．情報セキュリティ対策実施状況確認のための業界共通のフォーマット	**41**	**53.9%**
4．情報セキュリティのためのリスク分析	25	32.9%
5．情報セキュリティ対策ベンチマーク	23	30.3%
6．情報セキュリティ監査	23	30.3%
7．ISMS(ISO/IEC 27001:2005, JIS Q 27001:2006）認証取得	36	47.4%
8．プライバシーマーク（JIS Q 15001）認証取得	27	35.5%
9．情報セキュリティ格付	12	15.8%

（４）ISMS 認証取得状況（資本金別）

アンケートとは別に、JASA 会員企業の資本金規模別の ISMS 認証取得率を調べた。
取得企業の割合は全体で 8.7%である（17 社／全体 196 社）。
資本金別に分類すると資本金１億円以下の認証企業は 4.1%（６社／146 社）。
１億円以上の企業は 18.3%である（11 社／50 社）。

※ISMS 認証とは，情報セキュリティマネジメントシステム ISO/IEC 27001:2005（日本工業規格では，JIS Q 27001:2006）に対応する認証であり，企業の中の事業所（例えば支店）単位での取得も可能である。

表４　ISMS 認証取得率（資本金別）

			ISMS 認証企業		
資本金（百万円）	社数	%	数	取得率 A	取得率 B
10 以下	53	27.0	1	1.9%	―
100 以下	93	47.4	5	5.4%	**4.1%**
1,000 以下	37	18.9	9	24.3%	―
1,001 以上	13	6.6	2	15.4%	**18.3%**
計	196	100.0	17	8.7%	

（５）ISMS 認証取得状況（社員数別）

アンケートとは別に、JASA 会員企業の社員規模別の ISMS 認証取得率を調べた。
取得企業は全体で 8.5%（17 社／200 社）。
社員数 100 人以下で 1.5%（2 社／133 社）、
100 人以上で 22.4%（15 社／67 社）である。

〈〈解釈／評価〉

社員数が少なく、自社で情報セキュリティ管理のための専任要員を手当てできないことなども要因であろうかと思われます。

表５　ISMS 認証取得率（社員規模別）

			ISMS 認証企業		
社員数（人）	社数	%	数	取得率 A	取得率 B
～10	43	21.5	0	0.0%	―
～50	50	25.0	1	2.0%	―
～100	40	20.0	1	2.5%	**1.5%**
～300	40	20.0	6	15.0%	―
～1,000	13	6.5	4	30.8%	―
1,000～	14	7.0	5	35.7%	**22.4%**
	200	100.0	17	8.5%	

３．まとめと今後の課題

ISMS 認証取得を、情報セキュリティ対策の、外部に向けて客観化できるための合格ラインと考えた場合、この合格ラインは企業の資本金や社員数など、企業の規模に依存するという結果が出たといえる。

もちろん、企業の考えにより積極的に取得しないということも可能性としては考えられるが、回答企業の 100%が情報セキュリティ対策は必要と考えていることから、積極的に取得しない理由は現実的ではない。

取得する、あるいは取得しなくてもそれに代る有効な手段はないか、が、アンケート結果の最も期待されるところであろう。上の項目の「（３）対策実施状況を説明する有効な手段手段」の回答結果にそのようなことがうかがわれる。費用対効果、要員の不足などが問題のようである。

今後の課題としては、調査結果にもみられるように、組込み業界の多数を占める小規模企業（資本金１億円以下、社員数 100 人以下の企業）の情報セキュリティ対策がどうあるべきか、業界共通の課題としてどう取り組むべきか、また実情に即した簡易な制度が可能なのかなどが、関係諸機関と連携を取りながら検討されなければならないと考えられる。

資　料

資料１．アンケートの依頼文

会員企業各位殿

2009.1.吉日
社団法人 組込みシステム技術協会
安全性向上委員会セキュリティ WG
委員長　漆原　憲博

御社における『**情報セキュリティ対策実施状況**』アンケートのお願い

新年あけましておめでとうございます。
旧年中は当協会の活動にご協力を賜り厚くお礼申し上げます。
本年もよろしくお願いします。
さて、当委員会では組込みシステムにおける情報セキュリティの問題を昨年来研究して参りましたが、その一環として会員企業各位に、アンケートをお願いしたいということになりました。アンケートは標記の通りです。
よろしくご協力のほどお願いします。
なお調査票（３枚）は恐れ入りますが、2009 年１月 31 日までにご返送をお願いします。

《調査の背景》
当委員会では研究の成果として昨年度末、報告書『ネット社会における組込みシステム、2 つの課題「情報セキュリティ」と「機能安全」』を出させていただきました（会員各位には配布済み）。研究会は主に技術的な観点からアプローチしていますが、研究の途上「技術論もさりながら、いったいそもそも各社は情報セキュリティの管理にどんな体制で臨んでいるのだろうか、取引先からは情報セキュリティの組織管理体制を設けるように、といわれていないだろうか」ということが話題に上りました。
業界を取り巻く大きな流れは、組織のセキュリティ管理体制を整えよ、という方向と思われ、そのためには情報セキュリティ認証制度 ISMS（ISO/JIS 27001）の取得が一般的と思われます。しかし、その取得費用、維持費用、また要員費用等の負担が**費用対効果**から考えても問題があるとの指摘がありました。
そこで、何か**簡易で実質的な制度**は作れないものか、そのためにも業界の実情を踏まえるべきである、ということになり、会員企業各位に対しアンケート調査を実施させていただくことになりました。
調査の背景は以上であります。なにとぞご協力のほどお願いします。

《注釈》
景気の大変思わしくない中、管理費用を増大させるような調査。お叱りを受けそうですが、こういう状況でこそ、“組織管理の質を高める分野”での**新規事業の創出**につながればと期待するものです。

ご記入頂きました個人情報は本件調査にのみ使用し他の目的には使用いたしません。
なお、調査の結果はご協力いただいた企業様へはお知らせします。

資料２．アンケートの集計結果

以下、回答結果を各項目ごとに集計し、グラフ化した表を記載します。

表 2.1　情報セキュリティに対する認識

		Yes	%
問１	ISMS 第三者認証制度をご存知ですか。	70	92.1%
問２	情報セキュリティ監査制度をご存知ですか。	64	84.2%
問３	**情報セキュリティ対策が必要と思いますか。**	**76**	**100.0%**
問４	情報セキュリティ対策を実施していますか	62	81.6%

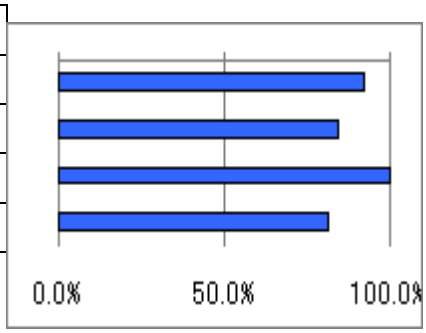


表 2.2　発注元からの質問・調査

問５	発注元から質問または調査がありましたか	数	%
1.	各種認証・制度の取得証明書の提示	24	31.6%
2.	**チェックシート等による対策状況の確認**	**63**	**82.9%**
3.	IPAno ベンチマークによる確認	7	9.2%
4.	内部監査人等による監査の実施	21	27.6%
5.	情報セキュリティ監査法人の報告書の確認	9	11.8%
6.	経営者の署名入りの確認書の提示	20	26.3%
7.	質問も調査もなかった	11	14.5%

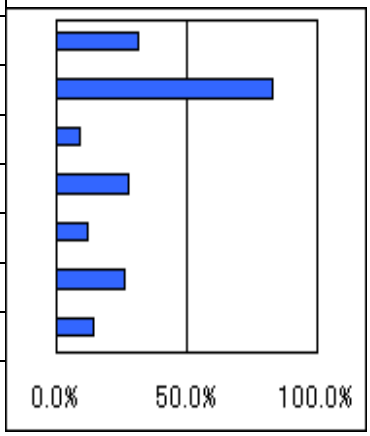


表 2.3　実施している情報セキュリティ対策

問６	実施している情報セキュリティ対策	数	%
1.	情報セキュリティに対する組織的な取り組み		
a.	情報セキュリティポリシーを作成し実施	56	73.7%
b.	従業員との契約	52	68.4%
c.	職務の分離	38	50.0%
d.	従業員教育	54	71.1%
2.	物理的セキュリティ対策	62	81.6%
3.	運用管理：通信ネットワーク及び情報システム	62	81.6%
4.	アクセス制御：通信ネットワーク及び情報	65	85.5%
5.	ログの蓄積：セキュリティ事故対応の記録	56	73.7%
6.	再委託先管理：委託先選定基準の有無等	41	53.9%
7.	情報の廃棄管理	62	81.6%
8.	その他	0	0.0%
9.	何もしていない	2	2.6%

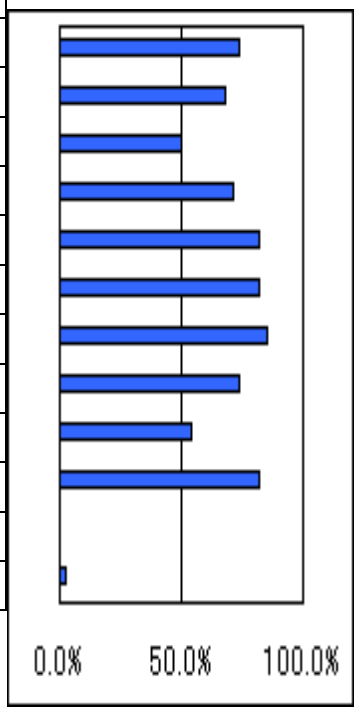


表 2.4　発注元が調査時の要求項目

問７	発注元の調査時の要求項目	数	%
1.	情報セキュリティに対する組織的な取り組み		
a.	情報セキュリティポリシーを作成し実施	43	56.6%
b.	従業員との契約	32	42.1%
c.	職務の分離	18	23.7%
d.	従業員教育	40	52.6%
2.	物理的セキュリティ対策	44	57.9%
3.	運用管理：通信ネットワーク及び情報システム	33	43.4%
4.	アクセス制御：通信ネットワーク及び情報	37	48.7%
5.	ログの蓄積：セキュリティ事故対応の記録	25	32.9%
6.	再委託先管理：委託先選定基準の有無等	36	47.4%
7.	情報の廃棄管理	40	52.6%
8.	その他	1	1.3%
9.	調査はあったが要求された事はない	6	7.9%

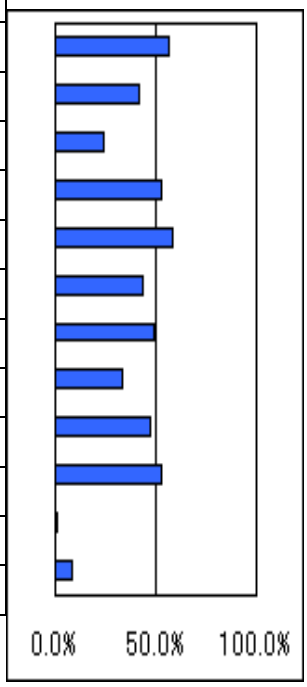


表 2.5　発注元から調査時に対応不足時の要求事項

問８	発注元の確認時の条件	数	%
1.	取引停止	9	11.8%
2.	追加対策	25	32.9%
3.	信用失墜（取引継続/停止を検討）	12	15.8%
4.	その他	1	1.3%
5.	いずれもない	27	35.5%

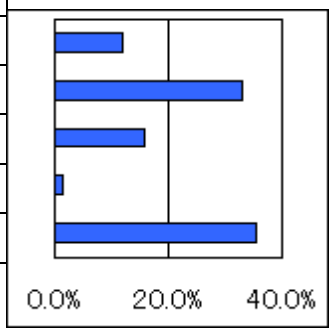


表 2.6　再委託先の管理

問９	再委託先の情報セキュリティ対策状況の確認	数	%
1.	発注元が、直接状況確認を行っている	4	5.3%
2.	自社が発注元の基準に準じた管理をしている	30	39.5%
3.	自社の基準により管理を行っている	45	59.2%
4.	契約時、再委託は認められていない	10	13.2%
5.	確認していない	10	13.2%

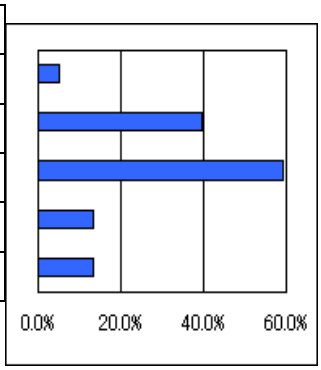


表 2.7　発注元から委託されている重要な情報

問１０	発注元から委託されている重要な情報	数	%
1.	取引先の従業員に関する個人情報	28	36.8%
2.	取引先の顧客に関する個人情報	36	47.4%
3.	取引先の経営に関わる情報	21	27.6%
4.	製造方法、仕様書、部品等に関する技術情報	58	76.3%
5.	金型、生産設備等に関する技術情報	18	23.7%
6.	最終製品に関する情報	40	52.6%
7.	取引先の入退館カード	44	57.9%
8.	取引先の知的財産	34	44.7%
9.	ビジネスに関わるノウハウ等	31	40.8%
10.	重要な情報は委託されていない	5	6.6%

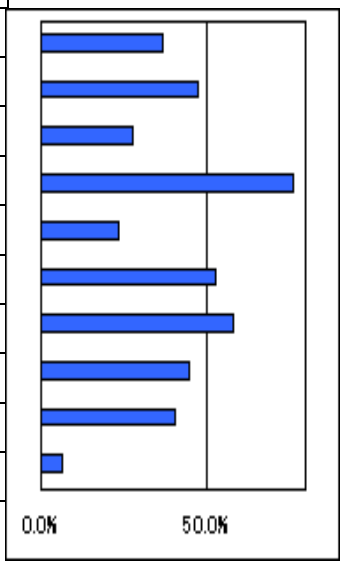


表 2.8　情報セキュリティを進める上での課題

問１１	情報セキュリティを進める上での課題	数	%
1.	内部統制、法的対応等への対応が困難	21	27.6%
2.	取引先の要求への対応が困難	10	13.2%
3.	**セキュリティ対策予算の不足**	**33**	**43.4%**
4.	**セキュリティ対策推進人材の不足**	**39**	**51.3%**
5.	どこまで対策すべきか不明	21	27.6%
6.	**投資対効果が見えづらい**	**33**	**43.4%**
7.	取引先にコスト負担が出来ない	22	28.9%
8.	経営陣の理解が得られない	2	2.6%
9.	教育・訓練が行き届かない	18	23.7%
10.	従業員の意識が低い	13	17.1%
11.	**実務上の負担が大きい**	**32**	**42.1%**
12.	最適なツールや相談するところがない	5	6.6%

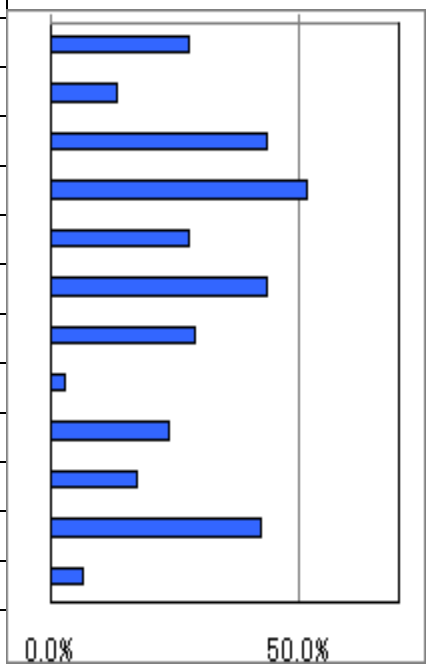
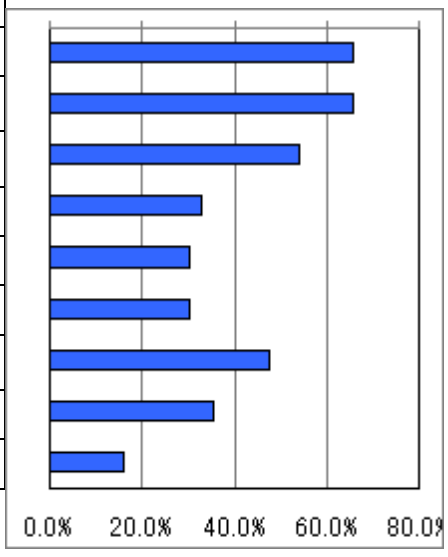


表 2.9　対策実施状況を説明する有効な手段

問１２	対策実施状況を説明する有効な手段	数	%
1.	情報セキュリティポリシーの設定	50	65.8%
2.	を証明・確認する業界共通のチェックリスト	50	65.8%
3.	状況確認のための業界共通のフォーマット	41	53.9%
4.	情報セキュリティのためのリスク分析	25	32.9%
5.	IPA のセキュリティ対策ベンチマーク	23	30.3%
6.	情報セキュリティ監査	23	30.3%
7.	ISMS 認証取得	36	47.4%
8.	プライバシーマーク認証取得	27	35.5%
9.	情報セキュリティ格付	12	15.8%



＊＊＊　　報告書の執筆者一覧　　＊＊＊

第 1 章　安全の基本	金田 光範
第 2 章　安全規格体系と概要	漆原 憲博
第 3 章　リスク管理とリスクアセスメント	大塚 悦生
第 4 章　安全設計の基本と 3 ステップメソッド	入月 康晴
第 5 章　機能安全ハードウェア設計手法概要	済賀 宣昭
第 6 章　機能安全組込みソフトウェア設計手法概要	大塚 悦生
第 7 章　機能安全の動向	兼本　茂
第 8 章　SIL3 取得関連製品の現状	委員分担調査

ＪＡＳＡ　安全性向上委員会　製品安全ワーキンググループ委員表

漆原　憲博	（委員長）	株式会社ジェーエフピー
金田　光範	（WG主査）	東芝システムテクノロジー株式会社
大塚　悦生	（ 委員 ）	東芝システムテクノロジー株式会社
入月　康晴	（ 委員 ）	地方行政独立法人 東京都立産業技術研究センター
済賀　宣昭	（ 委員 ）	東海ソフト株式会社
那須　誠	（ 委員 ）	株式会社ジェーエフピー
八谷　祥一	（ 委員 ）	株式会社ガイア・システム・ソリューション
大地　秀二	（ 委員 ）	株式会社コア
高橋　重眞	（事務局）	社団法人組込みシステム技術協会（JASA）
前澤　敏昭	（事務局）	社団法人組込みシステム技術協会（JASA）
兼本　茂	（アドバイザー）	会津大学　コンピュータ理工学部　教授
水口　大知	（アドバイザー）	独立行政法人 産業技術総合研究所
門田　浩	（アドバイザー）	IPA－SEC／日本電気株式会社

平成 20 年度

組込みシステムにおける機能安全に関する調査研究

組込み系技術者のための安全設計入門

平成 21 年 3 月
社団法人　組込みシステム技術協会
〒103-0007　東京都中央区日本橋浜町 1-8-12
電話　03-5821-7973
FAX　03-5821-0444
http://www.jasa.or.jp