機械・設備の安全関連系エンジニアリングにおける
機能安全認証の手引き

2009 年(平成 21 年) 5月 2 日 発行

社団法人日本電機工業会
PLC技術専門委員会
Safety PLC WG

まえがき

この資料は，PLC技術専門委員会傘下のSafety PLC WGの審議を経て作成した委員会資料である。

この資料の一部が，技術的性質を持つ特許権，出願公開後の特許出願，実用新案権，又は出願公開後の実用新案登録出願に抵触する可能性があることに注意を喚起する。社団法人日本電機工業会は，このような技術的性質を持つ特許権，出願公開後の特許出願，実用新案権，又は出願公開後の実用新案登録出願にかかわる確認について，責任をもたない。

来　歴

Ver.	日付	改訂箇所	改定内容
1.0	2009/05/25	全頁	新規作成
1.01	2009/06/24	全頁	編集上の修正を加えた（ヘッダ削除，誤字修正など）。

目　次

ページ

機械・設備の安全関連系エンジニアリングにおける機能安全認証の手引き

1　背景と目的

世界における機械・設備の安全性は，IEC/ISO規格に基づいた設計時のリスクアセスメントと本質安全設計に移行しつつある。特に欧州では機械指令への適合を宣言しなければならない。しかし，日本は法整備，審査制度，国際安全規格への関与など，多くの面で遅れをとっている。この状況が続くと，該当地域への輸出が困難になり，日本の機械・設備メーカは，海外市場を失う恐れがある。

このような背景のもと，JEMA Safety PLC WGでは，日本の機械・設備メーカ各位への参考資料として，「機械・設備の安全関連系エンジニアリングにおける機能安全認証の手引き」（以下，本書という。）を作成，公開することにした。

本書は，機械指令の機能安全整合規格であるIEC 62061（JIS B 9961）の第三者認証取得を前提とするが，自己宣言であっても，基本的な手順及び作成文書は同じである。ただし，安全関連系に対する具体的要求，信頼性や性能・機能要求までは言及せず，適合の手順と作成文書についてのみ述べる。

なお，本書は，各種安全規格を解りやすく解説することを目的としており，各種安全規格の厳密な定義などは必要に応じて原文を参照されたい。

本書が，機械・設備メーカ各位の機械指令や国際安全規格適合に多少とも役立つことができれば幸いである。

本書の作成には，社団法人 日本工作機械工業会，社団法人 日本包装機械工業会，社団法人 日本機械工業連合会，安全審査会社のテュフ ズード ジャパン株式会社，テュフ ラインランド ジャパン株式会社の協力を得て進められた。関係各位のご協力に深謝いたします。

2　用語及び定義

本書で用いる主な用語及び定義は，JIS B 9961，JIS B 9700-1及びJIS B 9705-1に基づく。

なお，2章における注記はJISからの引用であり，解説は本書独自の記述である。

2.1

機能安全(functional safety)

機械及び機械制御システムの安全の一部であって，SRECS，他技術安全関連システム[1)]及び外部のリスク低減設備[2)]の正しい動作に依存するもの。

注[1)]　他技術安全関連システムとは，例えば，油圧制御及び空圧制御の安全関連制御システム。

注[2)]　外部のリスク低減設備とは，例えば，防犯システム，防火システム，避難システムなど。

解説　安全制御にソフトウェアを使用する場合は，機能安全システムと見なされる。

2.2

リスクアセスメント(risk assessment)

リスク分析及びリスクの評価を含む全てのプロセス。

2.3

リスク(risk)

危険の発生確率と危害のひどさの組合せ。

2.4

安全インテグリティレベル（SIL） (safety integrity level)

SRECSに割り当てる安全機能の安全インテグリティを指定するために，数字で表す3段階のレベル。安全インテグリティレベル3(SIL3)が最も高い安全インテグリティに対応し，安全インテグリティレベル1（SIL1）が最も低い安全インテグリティに対応する。

注記　SIL4は，通常，機械類のリスク低減要求には必要でないため，JIS B 9961では扱っていない。SIL4に適用する要求事項に関してはIEC 61508-1及びIEC 61508-2を参照。

2.5

パフォーマンスレベルPL (Performance Level)

合理的に予見可能な状況下においてSRECSの安全機能実行能力の指定に使用する個別レベル。

2.6

カテゴリ(category)

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である。

2.7

安全関連電気制御システム［SRECS (safety-related electrical control system)］

機械の電気制御システムであって，それが故障するとリスクが直ちに増加することが有り得るもの。

注記　SRECSは，その部分が故障すると安全機能を低下又は喪失するようなすべての部分を含むものであり，電源回路と制御回路とで構成することができる。

2.8

安全側故障比率(safe failure fraction)

サブシステムの全故障のうち，サブシステムが危険側故障にならない故障の割合。

2.9

1 時間当たりの危険側故障確率(PFHd: probability of dangerous failure per hour)

SRECS 又はそのサブシステムが，1 時間の間に危険側故障を起こす平均確率。

2.10

妥当性確認(validation)

SRECSが特定アプリケーションの機能安全要求事項を満たすことを検査（例えば，試験，分析）によって確認すること。

2.11

安全関連制御機能(SRCF : safety-related control function)

機械の安全状態を維持するように，又はリスクが直ちに増加しないようにSRECS が実行する制御機能であって，指定の安全インテグリティレベルを持つ機能。

2.12

診断率(DC: diagnostic coverage)

自動的な診断テストによってSRECS又はサブシステムの危険側ハードウェア故障確率が減少する割合。

解説　危険側故障のうち，検出できる故障の割合。

2.13

共通原因故障(CCF: common cause failure)

一つ又は複数の事象に起因する故障であって，多重チャネルサブシステム（冗長系）の二つ以上のチャ

ネルに同時故障をもたらし，SRCFを故障に導くもの。

解説　設計時に混入したバグ・不具合，ランタイム時の外来ノイズ，高温条件などがある。

2.14

フォールトトレランス(fault tolerance)

SRECS，サブシステム，又はサブシステム要素が，フォールト又は故障が存在する状況で要求機能の実行を継続できる能力。

2.15

プルーフテスト(proof test)

SRECS及びサブシステム内の，フォールト及び劣化を検出し，必要ならば，SRECS及びそのサブシステムを新品又は新品同様状態に修復するために実効するテスト。

注記　通常，プルーフテストによってサブシステムの残存寿命を新品同様に戻すことはできない。故障修復後のハードウェアの偶発故障確率を新品に近くすることは可能と考えられる。

2.16

安全機能(safety function)

故障がリスクの増加に直ちにつながるような機械の機能。

解説　安全機能はリスクを減少させるための機能であり，その故障は直ちにリスクの増加につながる。

3　安全規格の概要

3.1　CEマーキング，EC指令と第三者認証

CEマーキングとは，EU地域で販売される指定製品に添付を義務付けられているマークのことであり，EU理事会が出すEC指令に適合した製品であることを示す。特に多くの産業機械や装置は，低電圧指令，EMC指令及び機械指令に対応したことを示す適合宣言書とCEマーキングがないとEU域内に輸出することができないため，国内メーカもこれらの指令適合とCEマーキングへの対応が必要となる。指令に対する適合性を評価するために，製品種別ごとの安全要求を規定した整合規格を参照する。整合規格はEN規格であるが，ほとんどはISO/IEC規格と同一である。

(1)低電圧指令(2006/95/EC)

定格電圧AC50～1,000 V又はDC75～1,500 Vで使用される電気機器及びバッテリ搭載電気機器の安全性に関する指令であり，産業機器から家電品まで電気機器のほとんどを対象とする。また，電気的な面だけでなく，機械的要因や操作性など安全要求は多岐にわたる。最初の低電圧指令は1973年に制定され，現在のCEマーキングや各種EC指令の原型となった。2009年4月現在の最新版は，2006年に制定された2006/95/ECである。

(2)EMC指令(2004/108/EC)

電気及び電子機器は動作中に電磁波を発生するが，機器が電磁波によって誤動作や不動作等の悪影響を受けない，あるいは影響を与える電磁波を発生しないことを確認する指令である。EMCとは，電子環境両立性(Electromagnetic Compatibility)であり，EMC指令への適合は他の機器からの干渉に対する保護された，安全・確実な作動の保証を意味する。EMC指令(2004/108/EC)は2007年7月20日に施行され，2年で旧指令から移行することが決められている。

(3)機械指令(2006/24/EC)

少なくとも一個の可動部のある機械や機器が対象であるため，大型・小型を問わずほとんどの機械装置が含まれる。特に危険性の高い装置を付属書Ⅳ(表1)に定義し，これらの機械は公的認証機関に

よる整合規格への適合認証を取得することが義務付けられている。付属書Ⅳにない機械は，整合規格への適合を自己宣言できるが，規格適合性を自身で証明しなければならない。対象機械が幅広いため整合規格の種類も多く，通常，複数規格への適合が必要となる。

表1　機械指令2006/42/EC 付属書Ⅳ

1.回転鋸	13.手動積み込みのごみ収集車
2.手動送り平削り盤	14.取り外し可能な機械的搬送装置
3.片面平削り盤	15.機械的搬送装置のガード
4.バンドソー	16.車両リフト
5.上記1-4の組み合わせ	17.人用リフト(高さ3m以上)
6. 多軸ほぞ取り盤	18.可搬カートリッジ型の打付機械
7.回転式木材成形機	19.存在検出のための保護装置
8.可搬チェーンソー	20.インタロック付きガード
9.プレス(プレスブレーキ含む)	21.安全ロジックユニット
10.射出・真空プラスチック成形機	22.ロールオーバー保護構造
11.射出・真空ゴム成形機	23.落下物保護構造
12.地下工事機械工事機械	

3.2　機械安全の基本的な考え方－本質的安全と機能安全

ISO 12100-1／JIS B 9700-1(機械類の安全性-基本概念，設計のための一般原則―第1部)は，リスクアセスメント後の安全設計を以下の3つのステップで実施すると定めている。

(1)本質的安全設計方策（JIS B 9700-2　4章参照）

機械の動作速度を遅くする，あるいは制限する，高温部や鋭利な箇所をなくす，など設計又は運転特性を変更することで，危険源を除去する設計の実施。

(2)安全防護及び付加保護方策（JIS B 9700-2　5章参照）

JIS B 9700-2では，「本質安全設計により合理的に危険源を除去できず，リスクを十分に低減することができない場合，人を保護するためのガード及び保護装置」を設けることとしている。

安全防護及び付加保護方策のひとつとして，人が危険源の影響を受ける状況にならないよう危険源を停止させるか，機械や保護装置によって安全に制御するという考え方がある。この制御による安全方策を「機能安全」と呼ぶ。

(3)残留リスクに対する使用上の情報（JIS B 9700-2　6章参照）

上記ステップを実施してもリスクが残る場合，使用者に対し標識や文字列によって安全確保に必要な情報を提供する。

すなわち，まず機械自体から危険源をなくすこと，それで不十分ならガードや保護装置による安全関連制御よって対策し，それでも残留するリスクに対して使用上の注意として情報提供する。

例えば，道路と鉄道が交わらない立体交差にして踏み切りをなくすのが本質安全であり，踏み切りに遮断機や非常停止装置をつけて列車と車が同じ空間に存在しないようにするのが機能安全である。機械が高度かつ複雑になるに従い，本質安全設計だけでは機械の安全確保が困難になり，安全装置による対策が不可欠となってきている。そこで，安全関連制御用に設計された安全スイッチやセンサ，安全リレーユニットや安全PLC，などを使用した機能安全による安全装置が効果的な安全対策として広まりつつある。非常停止スイッチと安全リレーユニットによるモータの非常停止回路や，ライトカーテンと安全PLCによるパ

レット搬送の安全関連制御などが挙げられる。

3.3　機械安全の基本的な考え方ーリスクレベル

機械の安全性の一般原則は，ISO 12100-1／JIS B 9700-1（機械類の安全性-基本概念，設計のための一般原則―第1部）おいて定義されている。リスクアセスメントによって機械の危険源を同定及びリスクの見積・評価を行い，そのリスクが許容できるレベル以下になるように本質安全設計，保護方策を実施する。

安全機能をSILで示す方法と，PLで示す方法がある。SILはIEC 61508／JIS C 0508(電気/電子/プログラマブル電子安全関連系の機能安全)で定義され，IEC 62061／JIS B 9961(機械の安全性−安全関連電気/電子/プログラマブル電子制御システム)でも使われている。リスクアセスメントによるSILの決定方法を**表2**に示す。危険源から発生する危険事象の結果，潜在危険領域にさらされる頻度，潜在危険事象回避の可能性，望ましくない事象の生起確率によってSIL1～4に分類される。なお，機械系ではSIL 4は適用されない。

表2　リスクアセスメントによるSILの決定方法

(JIS B 9961:2008附属書Aより)

危害のひどさ:Se		SILクラス:Cl=Fr+Pr+Av				
		3~4	5~7	8~10	11~13	14~15
回復不可能 致死，目・四股の喪失	4	SIL2	SIL2	SIL2	SIL3	SIL3
回復不可能 四股骨折，指の喪失	3		(OM)	SIL1	SIL2	SIL3
回復可能 医師の手当て	2			(OM)	SIL1	SIL2
回復可能 応急処置	1				(OM)	SIL1

OM:安全関連電気制御システム（SRECS）以外の手段を推奨
*危害への暴露間隔が1時間を超え，かつ暴露の継続時間が10分未満の場合は，Frを1ランク下げてよい。

危害への暴露間隔:Fr		危険事象の発生頻度:Pr		回避の可能性:Av	
≦1時間	5	頻繁	5	不可能	5
>1時間 ≦1日	5*	かなり	4		
>1日 ≦2週	4*	時々	3	まれには可能	3
>2週 ≦1年	3*	まれに	2		
>1年	2*	無視	1	かなり可能	1

リスクレベルとしては，EN/ISO 13849-1(機械類の安全性-制御システムの安全関連部)においてPLを用いる手法が定義されている。SILとPLの関係を**表3**に示す。ただし，**表3**はSILとPLの相対関係の目安であり，読み替えとしては利用できないので注意が必要である。

表3　SILとPLの関係

SIL(IEC 61508)	PL(EN/ISO 13849-1)
-	a
1	b
	c
2	d
3	e
4	-

3.4　本書が対象とする製品範囲

機械指令への適合のためには，参照規格であるIEC 62061／JIS B 9961又はISO 13849-1／JIS B 9705-1に従って安全関連制御系を構築しなければならない。機械の機能安全の関連規格を**図1**に示す。ここで，図中のふたつの規格のどちらを選択すればよいのか，あるいはSILとPLのどちらに基づくべきだろうか。

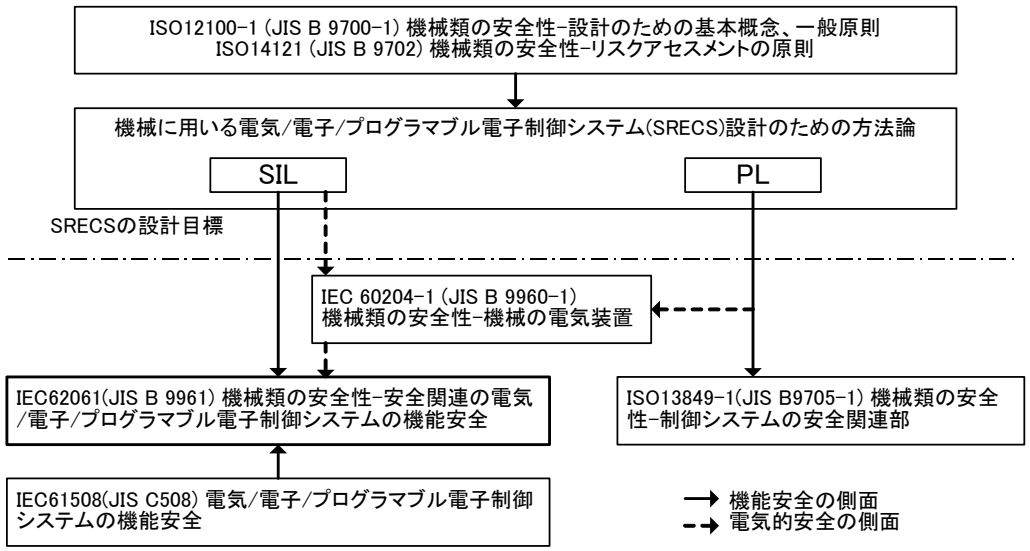

図1　機械の機能安全の関連規格(IEC 62061／JIS B 9961より)

表4が示すように，IEC 62061とISO 13849-1は，安全関連制御技術に対するカバー範囲が異なっており，例えば非電気的な安全制御技術(機械式や油圧系)を採用する場合は，IEC 62061に記載がないためISO 13849-1に適合しなければならない。一方，安全PLCに代表される安全プログラマブル機器を使用する場合，ISO 13849-1はPL=dまでしか適用できないので，PL=eすなわちSIL3はIEC 62061を適用しなければならない。さらに，PL=d以下であっても，安全ソフトウェアに関する要求事項はIEC 62061を参照するので，安全プログラマブル機器を使用する場合はIEC 62061への適合が必要となる。

表4　IEC 62061とISO 13849-1が対象とする安全技術

安全制御技術	IEC 62061	ISO 13849-1
非電気的(機械式，油圧等)	-	○
電気機械又は単純電気(リレー等)	SIL3まで	PL=eまで
複雑電気系(プログラマブル)	SIL3まで	PL=dまで ソフトウェアはIEC 62061を参照

本書では，普及が進んでいる安全プログラマブル機器を使用することを前提として，IEC 62061に対する適合の進め方について説明する。

4　IEC 62061機械類の機能安全

4.1　機能安全規格の要求事項

機能安全の考え方は，安全スイッチやセンサを入力として機械や防護装置の動力や状態を事故が起こらないように制御することにある。そのための安全装置は，設計不具合や故障発生による不動作があってはならないが，現実的に不具合も故障もない装置はありえない。従って，機能安全規格は，安全装置について設計ミスや不具合が混入しにくい開発プロセスや検証体制，動作中故障でも誤不動作しないための多重化や診断手法の実装を規定し，SILのレベルごとに診断率や故障率の数値目標を定義している。IEC 62061が安全装置に要求する項目の主なものを以下に示す。

(1)構造・機能要求

アーキテクチャを二重化や三重化として，単一故障で安全機能が損なわれない構成とする。I/O，CPU，メモリ，電源等など全ての部品について，十分な診断率を備えた診断機能を実現する。診断回路自身も診断しなければならない。故障検出時には安全となるように機械を停止し，安全制御機器をシャットダウンしなければならない。また，SILに応じて採用すべき技術が規定されているので，

その対応が必要である。

(2)信頼性の定量的要求

故障を安全側故障と危険側故障に分け，さらに危険側故障を，検出できる危険側故障と検出できない危険故障に分ける。「安全側故障比率(SFF)=安全側故障率＋検出できる危険故障率」がSIL指定の値以上(SIL3は概して90%以上)であること。時間当たりの危険側故障確率 (PFHd)がSIL要求値(10^{-8}～10^{-7})を達成すること。

(3)開発検証体制

設計と検証が独立した人，組織であること。独立した組織とは，設計の責任者(検認者) と評価の責任者(検認者) が異なることを意味する。詳細はIEC 61508-1を参照。

(4)開発プロセス

開発プロセスの安全規格対応(機能安全ライフサイクル)と文書管理。

上記，1)，2)に関しては技術的内容が多いため，本書では説明しない。規格を参照するか，技術コンサルタントに相談してほしい。上記4)については，次節で述べる。

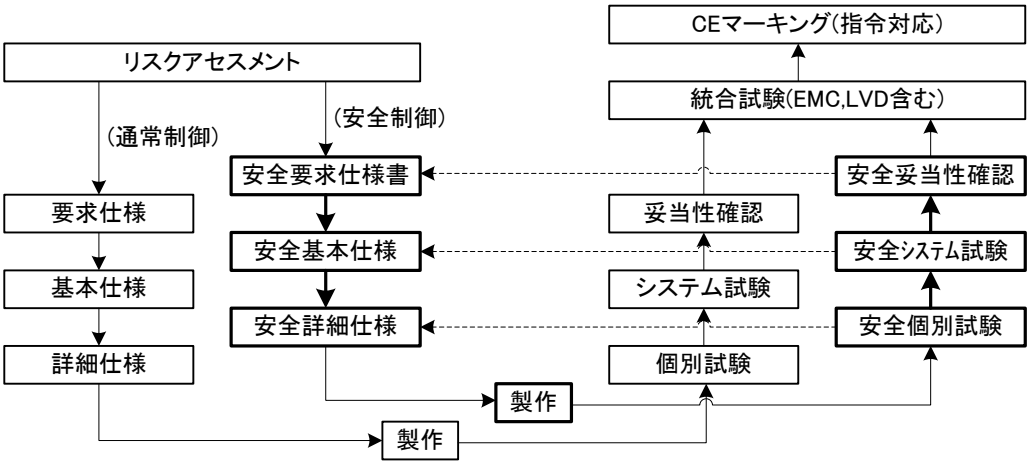

図2　通常制御と安全制御を持つ機械の設計プロセス例

4.2　機能安全の開発プロセス

通常制御と安全制御を含む機械の開発プロセスを，**図3**を用いて説明する。安全制御系の開発プロセスに対する規格の要求は，Vモデルに基づく段階的詳細化設計と設計フェーズに対応する試験である。図3において，実線は作業フェーズの移行，点線は試験・確認を意味する。H/W及びS/Wを段階的に設計し，サブモジュールごとにレビュー・試験を行うのは，通常制御でも広く実施されているので，このVモデルの導入が従来の開発プロセスに与える影響は大きくないだろう。ただし，規格で要求する項目を追加する場合がある。

従って，規格が要求する文書化要求及び記載事項を，通常の開発プロセス及び文書にどう反映するかが残された課題である。安全関連で特徴的な文書として，安全関連部の開発・検証の体制や手法などを記載する機能安全計画書がある。この文書は，開発計画や体制を記載するという点において，一般的な製品開発における製品企画書あるいは開発計画書に相当する。そして，開発の後半の詳細設計や個別試験，システム試験となると，通常の開発と同様の記載内容になる。例えば，評価仕様と評価成績書は，安全機能も通常機能も区別することなく試験を実施するなら，通常と同じ様式でよい。

H/WとS/WとアプリケーションS/Wを持つ機械の一般的な開発フェーズをもとに，安全関連開発を行う

場合の相違点を**図3**に示す。この図では，安全特有の用語をできるかぎり使わずに，安全関連開発が通常の開発と大きく違わないことを示している。各文書において，安全関連として追記すべき内容については次章で述べる。

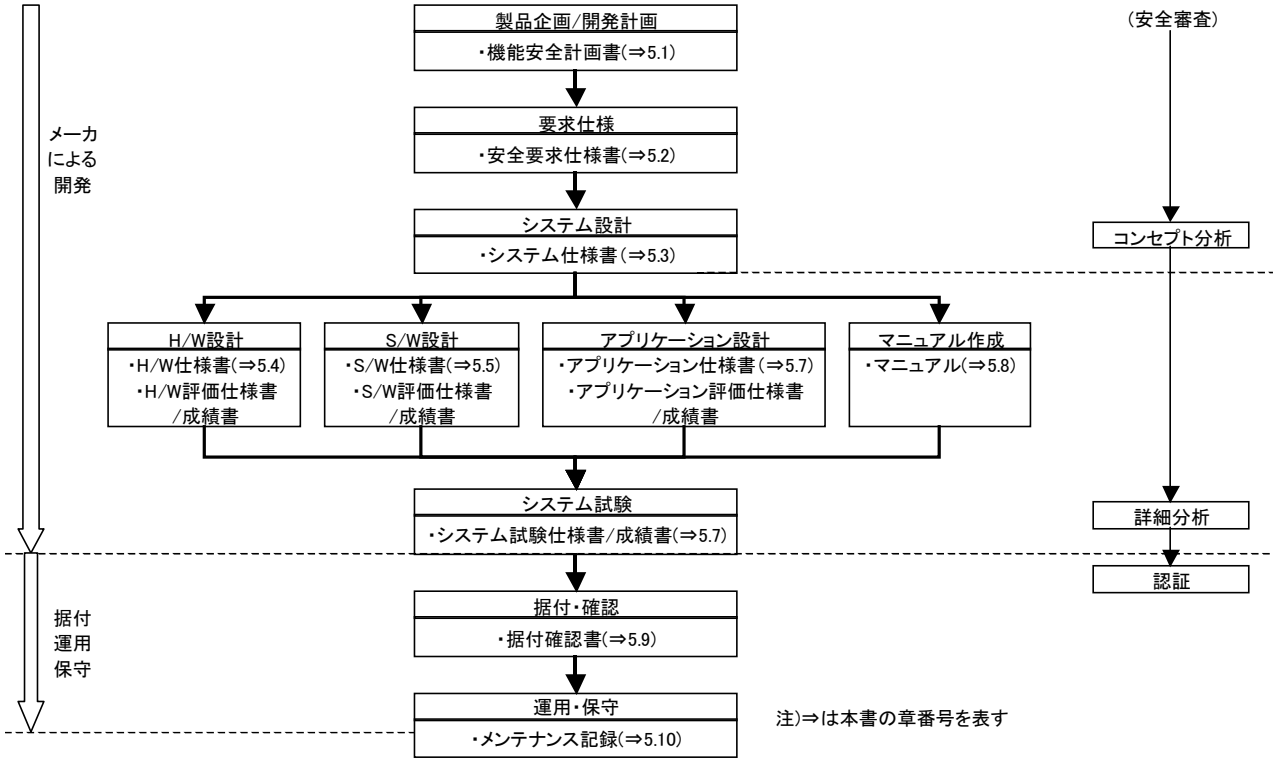

図3　機能安全開発フェーズと関連文

5　機能安全関連の記載内容

5.1　機能安全計画書(Validation and Verification Plan)

【IEC 62061 4.機能安全の管理】参照。

通常の製品開発における開発計画書に相当し，開発における全てのフェーズ(計画からシステム試験まで)の活動を明確にする。また，プロジェクトの特徴(プロジェクトの大きさ，複雑度，新規性，標準化度合いや故障の影響度など)に応じた内容とする。以下の内容を記述する。

表5　機能安全計画書の記載内容

	内容	備考
a	開発における全てのフェーズの内容	
b	機能安全要求事項を達成する方針及び方策	安全システム仕様書に記載してもよい
c	機能安全を達成する方策	アプリケーション，試験，統合試験，及び妥当性確認
d	開発における各フェーズを実行又はレビューする体制と要員	
e	安全システムに関係する情報を記録，保存する手順及び要員	危険源同定結果とリスクアセスメント結果，安全制御機能を実行するために用いる装置，機能安全の維持に責任を持つ組織，機能安全の達成・維持に必要な手順など
f	構成管理の方針(組織構成等)	
g	検証計画	検証の実施時期，検証の体制，方針及び技術の選定，試験装置，合格基準，検証結果の評価方法など
h	妥当性確認の計画	確認の実施時期，確認に供する機械の運転モード，確認対象の要求事項，技術方針，合格基準，不合格時の措置

ISO 9000等の品質管理基準を擁する組織であれば，通常の開発プロセス及び体制について記述し，それにb)，c)等の安全特有の内容を追記すればよい。

5.2　安全要求仕様書(SRS: Safety Requirement Specification)

【IEC 62061 5.2.SRCFの要求仕様作成】参照。

安全要求仕様書とは，リスク低減手法を用いて必要な安全機能を決定し，安全制御に関する機能要求仕様(IEC 62061 5.2.3)とSIL要求仕様(IEC 62061 5.2.4)を作成する。これらを作成するために，機械の運転特性(運転モード，サイクルタイム，応答時間性能，環境条件，機械への人の介入)及び，安全システムの設計に影響する関係情報(制御する機械の動作，複数の安全システム間又は他機能とのインタフェース，安全制御の故障対応機能など)を明確にする。

また，安全要求仕様書は不足や矛盾がないようにチェックリスト(IEC 61508-7 B.2.6参照)によって検証する。

安全制御の機能要求仕様には実行する安全制御の詳細を記述し，SIL要求仕様では機械に対するリスクアセスメントに基づく安全制御のSIL要求を記述する。例えば以下が挙げられる。

表6　安全要求仕様書の記載内容

	内容	備考
a	安全制御を作動又は不作動にして運転する機械の条件	例えば，運転モード
b	相容れない動きを起こす機能が同時に作動したときの優先順位	
c	各安全制御の作動頻度	
d	各安全制御の要求応答時間	
e	他の機械機能とSRCF とのインタフェース	
f	(例えば，入出力機器の)要求応答時間	
g	各安全制御の説明	故障反応機能の説明，及び最初の故障反応が機械を止めることである場合は，再起動又は運転継続に対する制約などの説明
h	運転環境の説明	例えば，温度，湿度，ちり，化学物質及び機械的振動衝撃
i	試験及びその関連装置	例えば，試験装置及び試験アクセスポート
j	安全制御の目的に用いる電気・機械複合部品の作動頻度及び／又は使用カテゴリ	
k	電磁イミュニティ，電磁妨害への性能基準	
l	安全制御系の要求SIL値	
m	SFF，PFHd目標値	

5.3　安全システム仕様書

【IEC 62061 6.安全関連電気制御システム(SRECS)の設計及び統合】参照。

安全関連制御機能は機能毎のブロックに分解され，その構造，各機能ブロックの安全要求事項(機能要求及びSIL要求)，各機能ブロックの入出力の定義が行われる。各機能ブロックの入出力は，転送する情報(例えば，スピード，ポジション，運転モードなど)である。機能ブロックは，安全関連制御機能を表すものであって，安全システムの診断機能は含まない。この規格では，診断機能は安全関連制御機能とは異なる構造を持つ別機能と考える。

安全システム仕様設計は，一般的なシステム設計と同様，要求仕様をサブシステムの各ブロックにどのように分割・割り当てを行うかの設計である。ただし，診断や故障反応機能など安全特有の視点による機能設計が行われる。なお，機能安全計画書において，機能安全要求事項を達成する方針を明確にするとあったが，その方針は安全システム仕様設計において明確になるため，本書にその内容を記述することが現実的である。また，安全関連制御系のFMEAやPFHd算出等も，本書で概略を示すことができる。

認証機関によるコンセプト分析では，ここまでの「機能安全計画書」，「安全要求仕様書」及び「安全システム仕様書」の3つの資料に基づいて審査が行われる。安全システムが安全規格に従ったリスク分析と安全対策が行われているか，安全関連制御が適切であるか，安全システムは安全要求仕様を満足するか，開発プロセスは機能安全ライフサイクルに従っているか，等が確認される。

表7　安全システム仕様書の記載内容

	内容	備考
a	市販のSRECSを選定した場合，その要求事項(6.5)	・SRECSの故障によるSIL低下，誤起動防止 ・SRECSの系統的ハードウェア故障防止 ・非安全関連系とSRECSとの独立性及びSILを維持する方策
b	SRECS一般要求事項(6.2)	・ハードウェア要求SIL，PFHd ・系統的ハードウェア故障の防止 ・オペレータインタフェース ・保全及び試験方法 ・設計，試験文書
c	SRECS故障時の動作要求(6.3)	・オンライン修理におけるSIL低下防止 ・SIL低下時の安全な停止 ・誤起動防止
d	SRECSの系統的ハードウェア故障回避(6.4)	・機能安全計画に基づく設計 ・仕様書範囲内での使用 ・ノイズなどによる共通原因故障(CCF)防止 ・設計レビュー(DR) ・シミュレーション ・電源断時の安全状態維持 ・SRECSサブシステムの一時的故障による影響回避 ・データ通信における異常で生じる影響回避 ・電磁イミュニティレベル（高耐ノイズ）⇒附属書E
e	SRECSの設計及び開発(6.6)	・SRSに従った設計と，設計過程の構造化，文書化 ・SRECSの独立性確保とSILを維持する方策 ・機能ブロック構造への分解と入出力の定義 ・SRECSサブシステムへの機能ブロック割り当て

5.4　ハードウェア仕様書/試験成績書(サブシステム仕様書)

【IEC 62061 6.6.2.1.7サブシステムのSRS】参照。

規格ではサブシステムをハードウェアと明確に規定していないが，記述内容がハードウェアを指向していること，後述のソフトウェア仕様と区別するために，ここではハードウェア仕様として記述する。

ハードウェア設計では，以下の情報を入手しなければならない。

表8　ハードウェア仕様書の記載内容

	内容	備考
a	安全制御を実行するハードウェアの機能及びインタフェースの仕様	
b	安全システムの危険側故障を招くすべての故障モードでの推定故障率	ハードウェアの偶発故障による
c	ハードウェアに関する次の制約	偶発故障率の推定値が妥当性を持つための環境条件。 偶発故障率の推定値が妥当性を持つために，これを超えて使用してはならないハードウェアの寿命時間。
d	試験及び／又は保全の要求事項	
e	DC 及び診断間隔(T2)	必要な場合
f	診断による故障検出後の平均修復時間(MTTR)を導くために必要なすべての追加情報	例えば，修理時間
g	アーキテクチャによる制約に基づくSIL	SRECS に用いるサブシステムのSFF を導くために必要なすべての情報(例：サブシステムのハードウェアフォールトトレランス)
h	系統的故障を回避するためのサブシステム使用上の制限	
i	サブシステムを用いるSRCF に対して付与できる最も高い安全インテグリティレベル	次のことを考慮すること ・サブシステムのハードウェア及びソフトウェアの設計及び実現の段階において，系統的フォールトの誤入を防止する方策及び技術。 ・サブシステムが系統的フォールトに耐えるようにする設計技術。
j	安全システム の構成管理を可能にするために，サブシステムのハードウェア及びソフトウェアの構成識別に必要な情報	
k	該当する場合は，デジタルデータ伝送における危険側伝送誤りの確率	

5.5ソフトウェア仕様書/試験成績書

【IEC 62061 6.10ソフトウェアSRS，6.11ソフトウェアの設計及び開発】参照。

ソフトウェア仕様書には，表8の内容を含む。また，IEC 61508-3の要求事項に適合しなければならない。

ソフトウェア上のパラメータ設定は，安全システムの専用ツールを用いて行わなければならない。パラメータ設定ツールは，例えば，パスワードの使用によって，無許可の変更を防止しなければならない。ソフトウェア上のパラメータ設定の文書化においては，用いたデータ(例えば，事前に定義したパラメータセット)，及び，安全システム関連のパラメータ，パラメータ設定者，パラメータ設定日付などの関連事項を識別するために必要な情報を示さなければならない。ソフトウェア上のパラメータ設定に対して，表8に示す検証を行わなければならない。

構成管理，シミュレーション，及び試験に用いるものを含め，適切なツールセットを選定しなければならない。安全システム の使用期間にわたって関連サービスを行う適切なツール(必ずしも最初のシステム開発に使われるものではない)を入手できるように配慮しなければならない。ツールの適切性の説明を文書化しなければならない。

表9　ソフトウェア仕様書の記載内容

	内容	備考
a	そのサブシステムに割り当てたすべての機能ブロックの論理(機能)	
b	各機能ブロックに割り当てた入力及び出力のインタフェース	
c	入力及び出力データのフォーマット及び数値の範囲，及びそれらと機能ブロックとの関係	
d	各機能ブロックの限界値を示す関連データ	例えば，最大応答時間，有り得ない数値を確認するための限界値。
e	そのサブシステムが安全システム内の他の装置(例えば，センサ及び最終要素)を診断する機能	
f	機械が安全状態を達成又は維持できるようにする機能	
g	故障の検出，通知，及び処理に関連する機能	
h	オンライン又はオフラインの安全制御周期テストに関連する機能	
i	無許可の安全システム変更を防止する機能	
j	非安全関連機能とのインタフェース	
k	受容能力及び応答時間性能	
l	パラメータ設定	－ 各安全関連パラメータが正しく設定されたことの検証(最小値，最大値，及び代表値)。 － 安全関連パラメータの有効性が確認をされたことの検証(例えば，無効データの検出によって)。 － 安全関連パラメータの無許可の変更が防止されていることの検証。 － パラメータ設定のためのデータ･信号の生成及び処理が，フォールトによってSRCF が失われない仕組みになっていることの検証。
m	ソフトウェア構成管理	－ 要求のソフトウェア安全インテグリティの達成に必要なすべての作業が実施されたことを確認して保証する。 － SRECS の安全インテグリティを維持するために必要な構成品目に関連するすべての文書を，正確に，固有の識別を付けて，維持する。
n	ツールの適切性	

5.6　アプリケーション仕様書/試験成績書

【IEC 62061 6.11.3 アプリケーションソフトウェアの設計及び開発】参照。

アプリケーション言語の使用手順には，良好な構成手法を規定しなければならない。不安全な汎用ソフトウェアの特徴(例えば，定義されていない言語要素，階層化されていない設計など)を追放し，構成上の誤りを検出できる確認法を明確にして，アプリケーションプログラムを文書化する手順を規定しなければならない。最小限，次の情報をアプリケーション仕様書に含めなければならない。

表10　アプリケーション仕様書

	内容	備考
a	法人名	例えば，会社，作成者など
b	説明	
c	アプリケーション機能要求事項へのトレーサビリティ	
d	標準ライブラリ機能へのトレーサビリティ	
e	入力及び出力	
f	構成管理	

アプリケーションソフトウェアモジュールの試験結果は，次のことを文書化しなければならない。

表11　アプリケーションモジュール試験成績書の記載内容

	内容	備考
a	入出力点の構成の確認	データが正しいアプリケーションロジックにマッピングされていることを確認するために，各入出力点の構成を，レビュー，試験，又はシミュレーションによって確認しなければならない。
b	各ソフトウェアモジュールの単体試験結果	意図した機能が正確に実行され，意図しない機能は実行されないことを判断するために，各ソフトウェアモジュールを，レビュー，シミュレーション，及び試験のプロセスによって確認しなければならない。
c	各ソフトウェアモジュールの試験結果	試験は，指定の試験対象モジュールに適し，次のことを保証できなければならない。 － すべてのブランチアプリケーションソフトウェアが確実に働く。 － 領域データが正しく使われる。 － シーケンスが正確に実行される(関連する同期条件を含めて)。
d	試験不合格時の措置	試験に失敗(不合格)した場合は，失敗の理由及び実施した修正を試験成績書に含めなければならない

アプリケーションソフトウェアの統合中にソフトウェアの変更又は修正を行った場合は，安全影響解析を実施し，影響を受けるすべてのソフトウェアモジュール及び，必要となる再検証及び再設計の活動について文書化すること。

5.7　システム試験成績書

【IEC 62061 6.12.1.3 SRECS統合試験の文書化】参照。

安全システムの統合試験は，適切に文書化しなければならない。試験結果並びに設計開発段階で指定した目的及び基準が満たされたかどうかを記述しなければならない。試験に失敗(不合格)した場合は，失敗の理由を文書化し，修正を行い，再試験しなければならない。

SRECS 統合試験の段階では，次のことを文書化しなければならない。

表12　システム試験成績書の記載内容

	内容	備考
a	用いた試験仕様書のバージョン	
b	統合試験の合格基準	
c	供試SRECS のバージョン	
d	用いたツール及び設備(校正データと共に)	
e	各試験の結果	
f	期待値と実現結果との不一致	
g	不一致があったとき，実施した分析，及び試験を続けるか変更要求を出すかの決定	

5.8　ユーザーマニュアル

【IEC 62061 6.6.1.8 SRECSのメンテナンスマニュアル】参照。

安全システムの使用上の情報には，安全システムの有効寿命期間にわたってSILを維持するために必要な技法及び方策を明記しなければならない。定期点検表，寿命部品表，交換手順書などを含む。

5.9　妥当性確認試験仕様書

【IEC 62061 7.2据付，使用及び保全のための文書化】参照。

文書には，安全システムの据付け，使用及び保全のための情報を提供するために，次の事項を含めなければならない。

表13　妥当性確認試験仕様書の記載内容

	内容	備考
a	装置，据付け，組立てについての包括的な説明	
b	安全システムの意図する使用，及び合理的に予見できる誤使用を防止する手段の説明	
c	ブロック図	必要であれば
d	回路図	
e	プルーフテスト間隔又は寿命	
f	安全システム機能と機械の非安全関連電気制御システムとの間の相互作用の記述	
g	安全システム機能を機械の非安全関連電気制御システム機能から確実に分離するために必要な処置の説明	
h	安全システム機能を停止する必要があるときの安全維持を目的として備えた手段及び防護手段の説明	
i	必要であれば，プログラミングに関する情報	
j	安全システムに適用する保全要求事項の記述	・機械の保全履歴を記録するためのログ。 ・安全システムの機能安全を維持するために実行するべきルーチン作業。 ・安全システムに障害又は故障が起きたときにとるべき保全手順。 ・保全及び再立上げに必要なツール，並びに保全するための手順。 ・周期テスト，予防保全及び事後保全の仕様

各安全制御に対し，安全システムの妥当性確認試験を適切に文書化しなければならない。次のことを記述しなければならない。

表14　妥当性確認試験仕様書の記載内容

	内容	備考
a	用いた安全システム妥当性確認計画書のバージョン及び試験に供した安全システムのバージョン	
b	試験(又は分析)対象の安全制御	
c	用いた設備及びツール	校正データも付ける
d	各試験の結果	
e	期待値と実現結果との不一致	期待値と実現結果との不一致が発生した場合は，必要ならば，修正及び再試験を実施して，文書化しなければならない

5.10 保守記録(SRECS構成管理記録)

安全システムを変更する場合，次のことを考慮に入れて，構成管理手順を機能安全計画に従って実行しなければならない。特にハードウェア及びソフトウェアのバージョン，機器のシリアルナンバー等の構成管理は確実に行うこと。

表15　保守記録の記載内容

	内容	備考
a	各変更過程の計画	
b	意思決定過程及び安全システムに関する決定事項の文書化	ハードウェア及びソフトウェアのバージョン，機器のシリアルナンバー等の構成管理
c	変更要求手順の時系列的文書化(例えば，ログブック)	・安全システムの変更が影響すると考えられる危険源。 ・変更要求の記述(ハードウェア及び／又はソフトウェア)。 ・変更要求の理由 ・意思決定事項(及び各決定の承認)。 ・変更の影響解析。 ・(各段階の)再検証及び再妥当性確認。 ・変更要求活動から影響を受けるすべての文書。 ・変更段階で実行した活動及びそれらに対する責任者及び責任組織。
d	変更後の監査に必要となる情報の文書化	構成状況，工程間引渡し状況，すべての変更の正当性確認及びその承認，変更の細目など

6　認証取得の審査手順

認証取得が必要ならば，開発開始の頃から安全審査機関に審査依頼を申し込むべきである。コンセプト分析は基本設計段階で行うため，製品の出荷間際になって審査を始めても指摘の是正で多くの手戻りが発生する。

安全審査機関による機能安全の審査手順概要は，大きく3つのフェーズからなる。開発フェーズと認証フェーズの対応は，図3の右側に示されている。

(1)コンセプト分析

機械に対する安全要求事項についてどのような安全対策を実施するのかどのような体制・プロセスで評価を行うのかについて審査を行う。システムの基本設計完了時点での実施となるが，安全関連部についてはFMEA，診断手法や故障率が必要なのでH/W設計，S/W設計まで完了している必要がある。指摘があれば是正しなければならない。

提出文書：機能安全計画書，安全要求仕様書(SRCF仕様書)，安全システム仕様書(SRECS仕様書)

(2)詳細分析(本審査)

ほぼ完成した機械について，故障挿入試験，EMC/環境試験やソースコード審査により安全機能が仕様通りに実現されているか動作するかを確認する。また，開発が機能安全ライフサイクルに従って行われたかを文書により確認する。マニュアルの記述についても確認する。指摘があれば是正しなければならない。

提出文書：H/W仕様書，S/W仕様書，評価仕様/成績書，各種議事録，マニュアル

(3)認証

安全審査機関による認定証とテストレポートの発行であり，機械メーカが実施する仕事はない。

7　おわりに

機械指令において自己宣言が認められている機械であっても，機能安全による安全方策を使用していればIEC 62061に従った開発フェーズと文書管理が必要である。機能安全規格への適合は難解かつ大変だと言われているが，通常の開発フェーズにおける文書記載内容の追加で十分対応できる。ただし，本書は安

全制御のアーキテクチャ，診断手法及び数値的要求への対応に関しては言及していないので，それらに関しては関連規格を参照してほしい。

本書が機械の安全対応に役立つことができれば幸いである。

本資料の最新版の入手は・・・

本資料の最新版は，電子データダウンロードにて入手が可能です。JEMAのウェブサイトのオンラインストアにおいて無償公開出版物としてダウンロードが可能です。

JEMAウェブサイトURL：http://www.jema-net.or.jp/

本資料の内容に関するお問合せは・・・

社団法人 日本電機工業会　技術部　技術課
TEL　　03-3556-5884／FAX 03-3556-5892

平成21年5月25日 発行　　〒102-0082　東京都千代田区一番町17番地4
発 行 所　　社団法人 日本電機工業会

技09-03