機能安全の意味と基本的要求事項

■ 機能安全規格と対象製品群

1. 代表的な規格

IEC 61508-1
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
Functional safety of electrical/electronic/programmable electronic　safety-related systems
- Part 1: General requirements

2. 対象となる製品群

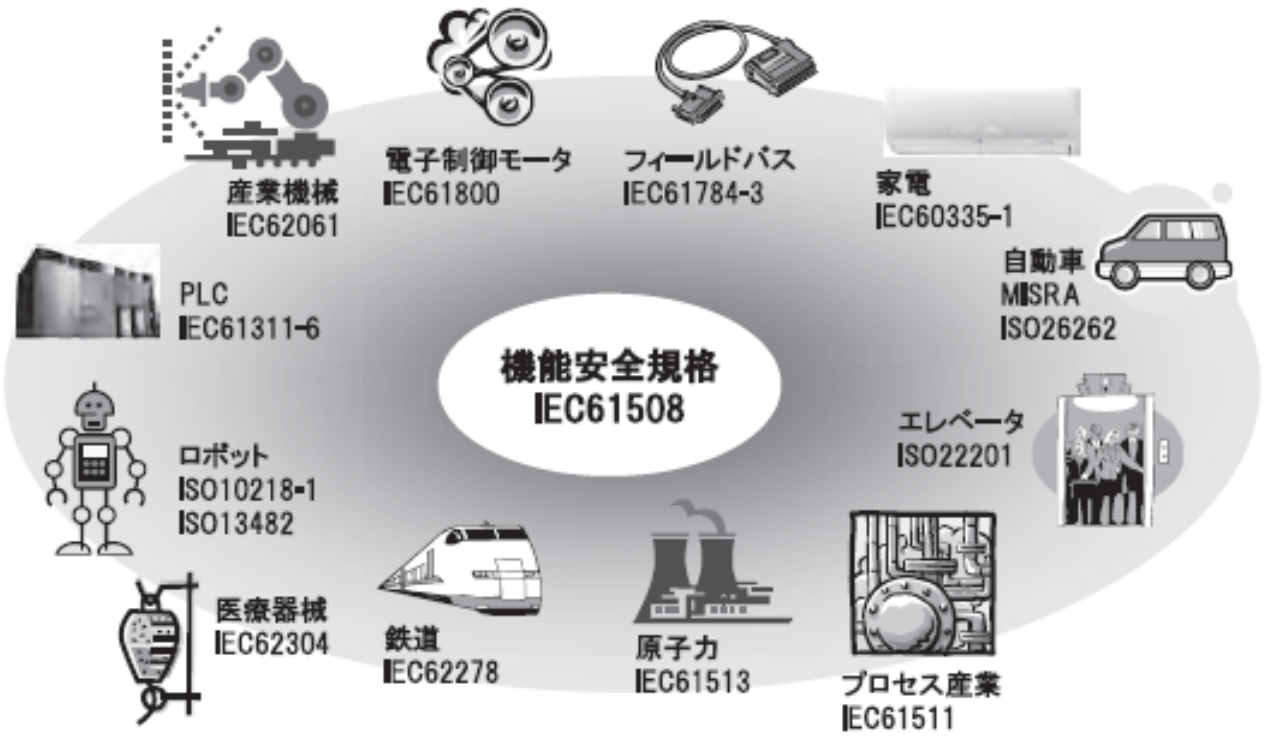
電気、電子機器で構成されるシステムは、安全機能を果たすために大きな役割を担っている。

プログラマブル電子系と呼ばれるコンピュータを用いたシステムは、あらゆる分野でその目的機能を達成するために用いられているが、機器（装置）、又はシステムに**安全機能を持たせることにも活用**されるようになってきた。

機能安全規格は、電気･電子･プログラマブル電子（E/E/PE）の要素から成るシステムが、安全機能を達成するための全ての電気的な安全関連系、安全ライフサイクルにわたって、**合理的かつ整合性がある技術指針の基に包括的に規定**している。

一般に安全性は、その**システムを構成する幾つかの機器（装置）が連携して動作**していて、複数の技術（機械、空気圧、電気･電子、プログラマブル電子技術等）に依存している。そのため安全対策については、個々のシステム（センサ、制御機器、アクチュエータ）の要素だけでなく、**全体システムを構成する安全関連系を考慮**しなければならない。
従って、機能安全は、電気･電子･プログラマブル電子安全関連系を対象とするが、更に制御システムの安全を含む安全関連系を対象としている。

今日、電気･電子･プログラマブル電子安全関連系を使用した機器（装置）、システムは、多岐にわたり、それらに**潜在的な危険、リスクが存在**する。そして、要求される**安全（達成）手段は、その適用に関わる多数の要因に依存**している。



出典: 日本機械学会誌　2014. 11　Vol. 117 No.1152〔神余浩夫　三菱電機（株）〕

■機能安全規格の基本的要求事項と導入効果

1. 基本的要求事項

1) 安全度水準　SIL (Safety Integrity level)

システム全体の安全を確保するためにその被害規模と事故確率からリスク見積を行い、その対策に必要な安全レベル(SIL)を決定する。

2) 電気・電子・プログラマブル電子の安全技術

体系的故障(設計ミス･バグ)のない開発プロセスと安全関連の品質管理を行うことが要求される。

3) ハードウエアの信頼性

故障モードとしての安全側故障はフェイルセーフの考え方で、また危険側故障(安全機能不全)は、安全水準(SIL)要求に従って定量的な要求がある。

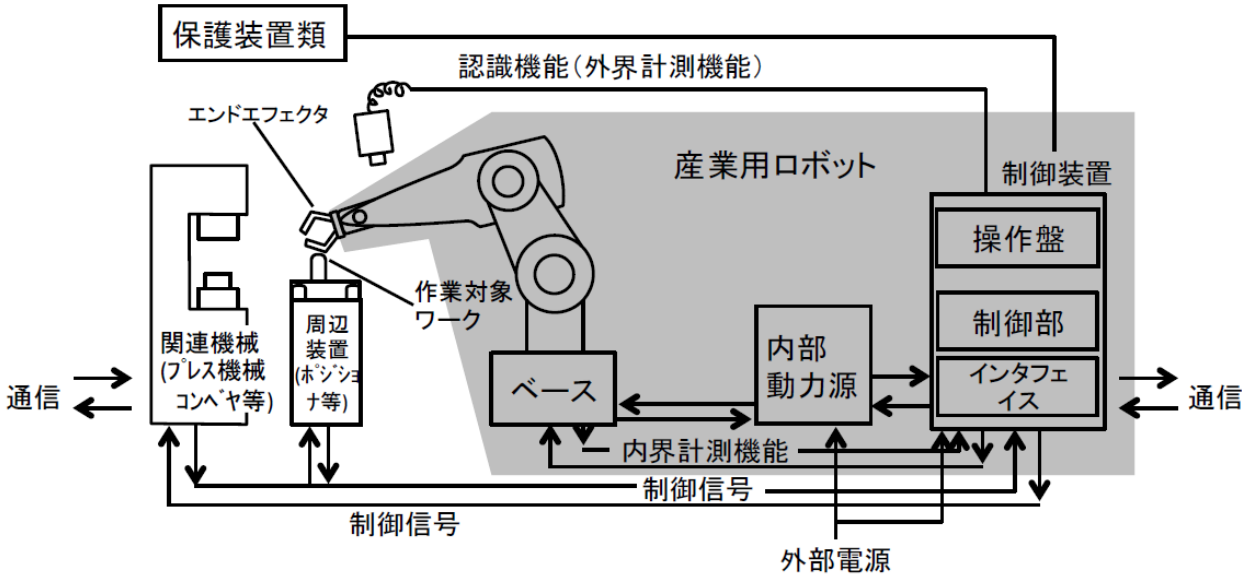
4) ソフトウウェアによる診断

安全水準(SIL)の定量的な要求に対応するためにそのSIL水準ごとに安全回路の診断手法が決められている。

5) 安全機能マネッジメント

全ての産業に適用した安全ライフサイクル活動が基本となる。本来、機能安全は、個々の機器（装置）の認証をする目的ではないが、顧客の要求としては、コンポーネント、サブアッセンブリ単体の認証要求がある。

※全体システム(装置)の機能安全を実現するための個々のコンポーネント、サブアッセンブル製品への要求は、現実的には対象が個別要素（汎用･専用スペック、メーカー別　等）で成り立っているため**全体最適の機能安全**を実現することが難しい。



産業用ロボットシステムの構成例

出典: 機能安全活用実践マニュアル(産業ロボット編)〔中央労働災害防止協会〕

2. 機能安全技術の導入

機能安全を実現する制御のプログラム化は、機械（装置）に内蔵される安全装置のコンパクト化と省コスト化を達成して、安全装置の高性能化による製品の高性能化、運転効率向上などの生産性の工場に寄与することが期待されている。
そして、現在、**機能安全技術の活用により安全性と生産性を両立できるメリットがあるため、機械設備を初めとした多くの分野で機能安全の導入は注目**されている。

機械設備の場合、従来は危険回避のために非常停止(EMS)で機械(装置)の制御盤全体の電源遮断により安全確保することが一般的であったが、安全PLC（Safety Programmable Logic Controller）を用いた安全制御が導入することによって人に危害を与える箇所だけを電源遮断すれば、安全確保が可能となっている。

PLCのような安全デバイス(Safety Device)を用いることで作業性に寄与しない無駄な設備（装置）の停止を抑制して作業を中断するような非常停止からの復旧を迅速に対応することが出来る。更に機能安全適合の安全センサや安全駆動装置との組合せによって、**よりきめ細かい安全制御を低コストで実現することが可能**になって来ている。

■機能安全ー第1部:一般要求事項

※以下、IEC 61508-1:2010 (JIS C 0508-1:2012)の規格(序文)を筆者が解釈して記載

1. 安全機能を達成するための設計、実装、運用、及びメンテナンスを含めて廃棄に至る全ての**電気・電子・プログラマブル電子系、及びソフトウェアの安全ライフサイクルの各段階を考慮**している。

2. 規格は、進歩する技術を念頭において作成され、その**将来の展開に対応できる包括的な内容**となっている。

3. 電気・電子・プログラマブル電子安全関連系について, 適用分野の製品規格などを開発することが出来る。
同時に、これらの規格によって開発する対象となる機器(装置)は、**適用分野間の基礎となる原理、原則、用語などに整合性を持った一貫性のあるものとして、安全性、及び経済性に寄与**する。

4. 電気・電子・プログラマブル電子安全関連系に対して要求される**機能安全の達成に必要な「安全要求仕様」**を開発する方法論を提供する。
<備考>**「安全要求仕様」とは、ユーザー(使用者)の使用環境において安全を確保するために必要な性能/機能をまとめた仕様書で機械の保有すべき生産に必要な性能/機能をまとめた「設備仕様書」と共にメーカーに提示する。**

5. 安全性、及びその程度に関して、対象の機器(装置)の**リスク低減を基本とした方法論**を提供する。

6. 電気・電子・プログラマブル電子安全関連系の安全機能に対して、開発設計における安全性の目標を特定するための**安全度水準の考え方、リスクに基づいた概念的枠組み、及びその技法の事例を提供**する。

7. 電気・電子・プログラマブル電子安全関連系が実現する安全度水準に対応した**「目標機能失敗尺度」**を設定する。
<備考> **目標機能失敗尺度とは、安全機能を満足に実行する確率で、、安全に関わる故障は、確率論的なランダムハード ウェア故障と決定論的原因故障とに分類され、安全インテグリティレベルSIL(Safety Integrity Level)で示す**。. E/E/PE安全関連系に割り当てられる安全機能に対する安全機能の作動要求と解釈される。

8. 単一の電気・電子・プログラマブル電子安全関連系が実現する**安全機能に対して、「目標機能失敗尺度」の最小値を設定**している。それらは、**運用モードに応じて次による**。

   1) **低頻度作動要求モード**の場合、最小値を作動要求時の危険側機能失敗時間平均確率(PFDavg)10^{-5}とする。
   2) **高頻度作動要求モード、又は連続モード**は、最小値を単位時間当たりの時間平均危険側故障頻度(PFH)10^{-9} [1/h]に設定する。

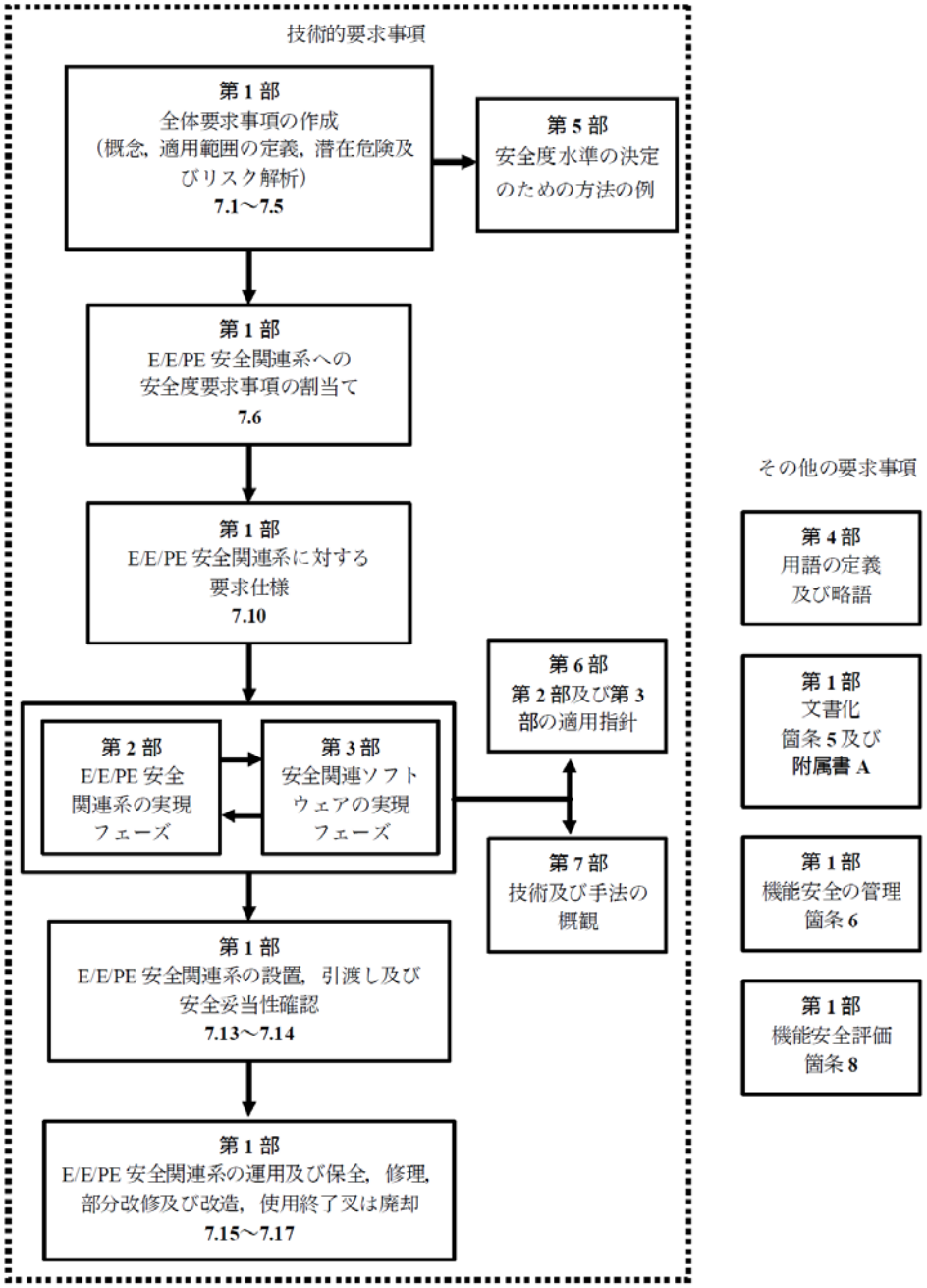
   〈注記〉**単一の電気・電子・プログラマブル電子安全関連系とは、必ずしも単一チャネル構成を意味するものはない。複雑でないシステムは、目標安全度をより小さな値で安全関連系の設計をすることが可能であるが、これらの限界値は、比較的複雑なシステム(例 プログラマブル安全関連系)に対して達成できるものとみなされている。**

9. **安全機能が損なわれる要因(決定論的原因フォールト)**は、実際の経験に基づく専門的な判断に基づいて解析、対策されるが、それらの**回避、及び制御の方法を設定**している。

   また、**決定論的原因故障の発生確率**は、一般的に数値化が困難であるが、**安全機能に関連した「目標機能失敗尺度」は, この規格に規定する要求事項を全て満たしている場合は, 達成しているとみなしてもよい**。

10. 決定論的安全度は、特定の安全度水準の要求事項に適合する信頼に対応する要素を提供するもので、**決定論的対応能力を考慮に入れた安全設計が要求**される。

11. 電気・電子・プログラマブル電子安全関連系に対して、**機能安全を達成するために多岐にわたる原理・技法、及び手段を適用するが、「フェールセーフ」の概念は明示的には使用しない**。
但し、**「フェールセーフ」、及び「固有(本質)安全」の原理**は、この規格の関連する**要求事項に適合することを条件として適用してもよい。**



機能安全規格群の枠組み

出典: JIS C 0508-1:2012 (IEC 61508-1:2010)

■ 参考情報

1. **機能安全活用テキスト (中央労働災害防止協会)**
   https://www.jpa.gr.jp/about/safety/pdf/kinoanzenkatsuyo_2017_text.pdf

2. **機能安全が可能にする機械の安全確保 (中央労働災害防止協会)**
   http://www.mhlw.go.jp/file/06-Seisakujouhou-11200000-Roudoukijunkyoku/0000117706.pdf

3. **経済産業省 ロボット導入実証事業**
   http://www.robo-navi.com/intro.html

4. **ロボット活用事例**
   http://www.robo-navi.com/Cases/index

5. ロボット活用の基礎知識
   http://www.robo-navi.com/webroot/document/robokiso.pdf