機能安全規格 IEC61508 と物流機械への応用

Functional safety IEC 61508 and it's application in the logistic machinery

正　加部隆史（NPO 安全工学研究所）
Takashi KABE, NPO The Safety Engineering Laboratory,
4-41-10 Minami Ogikubo Suginami-ku. Tokyo

Related to the ISO12100:Safety of machinery-Basic concepts, general principles for design, the position and the ripple effect of the IEC61508: Functional safety of electrical / electronic / programmable electronic safety-related systems is to be considered, when the software is applied to the control. Specially, the logistic system or the large-scale product system, such as the automobile industry and the semiconductor industry, the application of safe programmable controller should be required from the efficient viewpoint in future. Then, the safety management for all the life cycles and the product design meeting the functional safety should be necessary. After product has already been established logically and technically, it is authenticated by third party and applied to the actual working place. Because the functional safety standard is in the high level and the comprehensive scale, the proper consensus between the user side and the establishment side should be created at the introduction of each field.

Key words: machine safety ISO12100, functional safety, all the life cycles, third party certification

1．機能安全規格

電気・電子・プログラマブル電子安全関連系の機能安全：IEC61508 は全 7 巻に及ぶ包括的な規格であり、単一・個別の単なる構造規格とはその性格を全く異なったものとする。コンピューターに使われるＣＰＵ自体非常に便利なもので、日進月歩の進化を遂げているが、現時点での技術レベルは信頼性・安全性の観点からすると多くの問題点を含んだまま実用化されている。その為、これを工業用で安全関連信号に適用する為には、ISO12100 の機械安全での設計一般原則に加え機能安全を考慮したそれなりの安全方策が必要とされてくる。

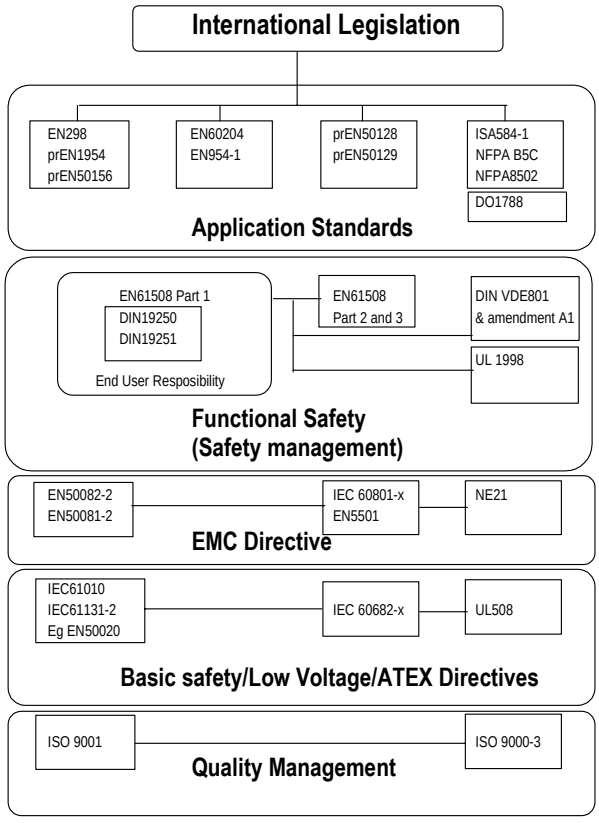
この機能安全 IEC61508 にたどり着く発端は、欧州での 1984 年最初のドラフトに遡り、1990 年のドイツ VED0801 及び DIN V 192050・19251 (AK1-8 のリスクグラフ)等でコンピューターの安全性及びリスク評価手法等が提示された事による。

その前段として 1982 年及び 1996 年のセベソ指令へのきっかけとなった 1976 年イタリア、セベソでのダイオキシン飛散による人畜への大被害や 1984 年インド、ボッパール農薬工場からの有毒ガス放散等の大事故教訓から、機械使用者には以下の責務が課せられた。「重大な事故を防止する為に証明書類を仕上げ、これを規定どおり実践できる事を実証しなければならない。機械使用者が見込む重大事故防止のコンセプトは適した方法・組織・マネージメントシステムにより、人と環境に対して高い保障水準を保証すべきものである（セベソ指令第 7 条 1 項)。

一方で、機械設計者の責務としては 1985 年の欧州ニューアプローチ指令において、安全と健康を保障する為の自己責任による適合性評価手順が打ち出され、製造者は安全な機械のみ市場流通できるしくみである、いわゆる CE マーキング制度が打ち出された。それに続き 1989 年発令された欧州機会指令及びそれに伴い整備され始めた例示規格により、機械の安全性についてのシステムが確立した。これにより、機械設計者ならびに機械使用者は、予防措置（**prevention**）により ISO/IEC Guide 51 に謳われている受け入れ可能な範囲までリスク低減を実施し、安全の妥当性証明を立証する事を法的に求められるようになった。

その後機械安全用のリスクグラフ EN954-1 は確定論に基づき B-4 間での 5 段階の制御カテゴリーが導入された。、但し、1996 年に制定された本規格は信頼性を考慮していない為に、適応上数々の議論が持ち上がりコンピュータの急速な進歩と普及に鑑み信頼性を考慮の上定量的リスク解析手法として確率的要素が加わり安全度水準 **Sefety Integrecy Level (SIL)** が導入された。

本来機械安全に関する標準化は例えばドイツの VDE/DIN となりその後欧州規格ＥＮとなり、それからに IEC 規格として制定されるが、IEC61508 の場合 EN61508 が欠落している。主な理由は、機能安全と全ライフサイクルに亘る要求事項が高度な為、EU 加盟国のなかでこれは安全規格による貿易障害になるとの批判から EN 規格として未だ成立していないという政治的要因が関連している為である。



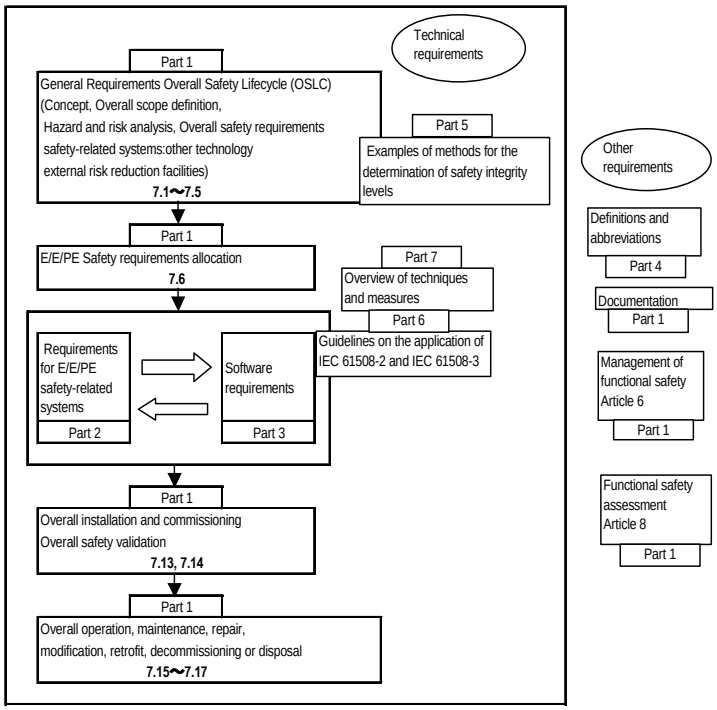
Pic.1.International Legislation of safety management system

2．具体的要求事項：技術ー人・組織

IEC61508（注 2）で要求されるのは先ず先立って、一般設計原則である ISO12100 の安全思想のみならず、それを全ライフサイクルに亘り保持すると言う要求から、基本的には ISO900 に基づく品質管理システムと自己責任に基づく適合性評価の実施が要求され、第三者認証の過程では、製品開発普及・設計・その後の設計変更に伴う文書管理及び責任体系の組織図が必須要件となってくる。同時に機能安全とは別に、電磁波による影響につき電磁両立性(EMC)試験が要求される（図 1、注 1)。

それ故、機能安全を達成しようとする場合、単に製品を開発し単品認証で販売するという事では済まずに、技術・人・組織に亘り、かつ全ライフサイクルに渡る管理体制が一貫して完備している事が要求される。図 2 に本規格の全体構成を示すが、その詳細については本規格を参照していただきたい。

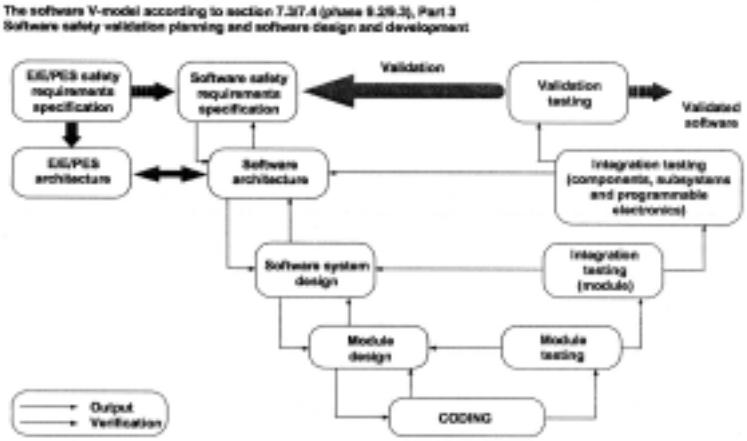
本規格の対象は電気 (E)，電子 (E) 及びプログラマブル電子システム (PES) ―E:Electric / E:Electronic / PES:Programmable Electronic System(s) (E/E/PES) である。



Pic.2.Framework of IEC61508

包括的な内容と妥当性確認手法

製品作りにおいては、先ず安全要求仕様を明確にし詳細な安全コンセプトに安全性を達成する手法・考え方・引用規格などを詳細に明示し、アーキテクチャーの設計を行う。第三者認証の場合、この基本設計での安全性確保についての詳細な吟味が先ず行われる為に、完成品を第三者機関に持ち込んで合否を問うという方法ではなく、開発の初期段階から第三者機関と相談しながら進めるのが一般的である。その後に、ソフトウェア及びハードウェアの設計を行い、ソフトウェアについては V モデル（図 3）という開発手法を適用し妥当性確認を繰返し実施する。



Pic.3.　Development of software (V-Model)

トランジスタ、キャパシタ、リレー、コンタクタ、抵抗等各部品の評価目安として、

MTTFd　Mean Time to Dangerous Failure
DC　Diagnostic Coverage（見積もりに FMEA を使用）
CCF　Common Course Failure

等が用いられ、定量的手法として代表的には冗長性の信頼性については数学的手法であるマルコフモデルやペトリネット等が用いられ、その統合結果リスクレベルを **SIL(Safety Integration Level)**として SIL-4 の四段階に適合させる。危険事象を発生させる故障は、ランダム・ハードウェア故障（random hardware failure）と決定論的原因故障（systematic failure）とに分類され、かつ高頻度モード及び低頻度モードの割り当てがある（注３）。

機械安全は、SIL3 迄のレベルで、SIL4 は基本的に該当しない。この場合、従来の EN954-1 は確定的手法による制御カテゴリーの分類の為、これを確率的手法に基づく SIL と比較する事は一概に出来ないが、ひとつの目安としては、例えば安全 PLC 等の場合に制御カテゴリー4 対応のものは SIL3 対応と言う事ができる（図 4)。EN954-1 の改訂版である ISO13849 においては、この信頼性の概念を考慮し、従来の制御カテゴリーから **Performance Level(PL)** a,b,c,d,e の区分けが追加される。

機能安全規格は、全ライフサイクルに亘る安全性確保を要求している事から、製品のみならず、リスクアセスメント・文書化及びその管理が継続的に実施される事を要求している（**Assessment-Documentation-Management**)。

文書管理は、小規模システムの場合 1 冊の集合体で済ますことが出来るが、物流システム等大規模システムの場合以下の分類が必要となる；

エンジニアリング用集合
製造者用集合
引き渡し用集合
保安用集合
運転用集合

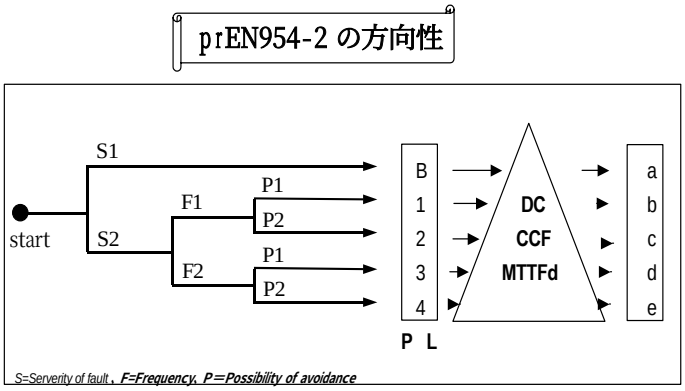
IEC61508 は、あまりにも包括的・専門的・難解である為に、機械安全用には IEC62061、プロセス産業用には IEC61511 としてアプリケーションに適合した案を作成中である。又、以下の規格のなかで機能安全規格が引用或いは条件とすべく検討されている。

機能安全は法的強制力により実施すると言うよりも、特定ユーザーが仕様書上あるいは第三者機関が運転開始時の立会い検査で規格適合性を要求或いは確認するもので、それ故各製造者の自己責任・自主的対応が重要となってくる。

3．第三者認証の役割

製品＋品質管理体制が全ライフサイクルに亘り問われる。

欧州のみならず、米国でも要求される。米国の場合、NFPA79:1997 では緊急停止はハードワイヤリングのみが許容されていたが､IEC60204 がソフトウェアを許容した事により、それを受け NFPA79:2002 ではソフトウェアが許容された(9.4.3.項)。同時に、製品認証の際 11.3.4.項にて NRTL に登録された試験機関での認証がソフトウェアの安全性につき要求されている。UL1998 では software programmable components の安全性の要求があり、IEC61508 と共に認証の条件となっている。



Performance Level (PL) の導入により、low risk (a) ―high risk (e) とする。
PLは、以下の要因により構成される; 定量的手法ではマルコフモデル、GSPN等が使われる。

MTTFd mean time to dangerous failure
DC diagnostic coverage （この見積もりにはFMEA等が使われる）
CCF,β common cause failure

IEC61508:Relation with SIL
PL a no safety requirements
PL b,c SIL 1
PL d SIL 2
PL e SIL 3

characteristics	MTTFd value	DC value
none		0-60%
low	**3-10 years**	60-90%
medium	10-30 years	90-99%
high	30-100 years	99%<DC

Pic.4.Revision of EN954-1

安全の妥当性確認については、基本は欧州の場合自己宣言であり、型式検定が法律で義務付けられているわけではないが、実質的にはユーザーが、前述米国の例にもあるように第三者認証書を要求する傾向にある。事故が発生し、製造者責任を追及された場合、例えば欧州では 2 週間以内に、安全の妥当性確認に関する図書（技術・品質管理・安全管理等）を法廷に提出することが要求されるために、そこで製造者自ら説明し第三者を納得させるか或いは事前に第三者機関によりその妥当性を確認済であるかは大きな違いが出てくる。第三者機関の役割は、基本的にその時代の科学及び技術の知見に基づき最高の技術が適用され勝つ適切に管理されているかを検証するもので、その実績は特に欧州の場合既に歴史的に実証された権威付けがなされている。人々の健康と安全を確保すると言う基本的人権に端を発し、過去の事故例から導き出され改善を繰り返してきた妥当性確認の手法が最近では ISO 及び IEC という任意の国際規格により支えられ、これら既存規格を適用する事により、妥当性確認に必要な時間を迅速化している。

科学及び技術の知見は、特に情報通信産業の分野では著しい進歩をと出る為に、日夜追加変更される国際規格の体系並びに設計に必要な個別規格の現状、変更の予定等を網羅して把握する事は至難の業である。それ故、これらを認証作業の一環としてサービス産業として成立している第三者機関を情報源として活用する事が、有益となってくる。

特に、機能安全においては複数の電子関連部品から構成される製品の安全妥当性を立証してゆくのは、製造者のみで行うのは実質的に可能性が非常に限られており、通例として第三者機関の認証が行われている。

図 5 に示される様な複合化した生産システムの場合は、ISO11161 によると危険源を含んだ複数の機械を結合してひとつのシステムとして完成させたシステムインテグレーター（SI）が製造者責任を担う事になる為、SI は個々の機械、安全関連機器の妥当性確認の証を各製造者から事前に入手する事が得策となってくる。

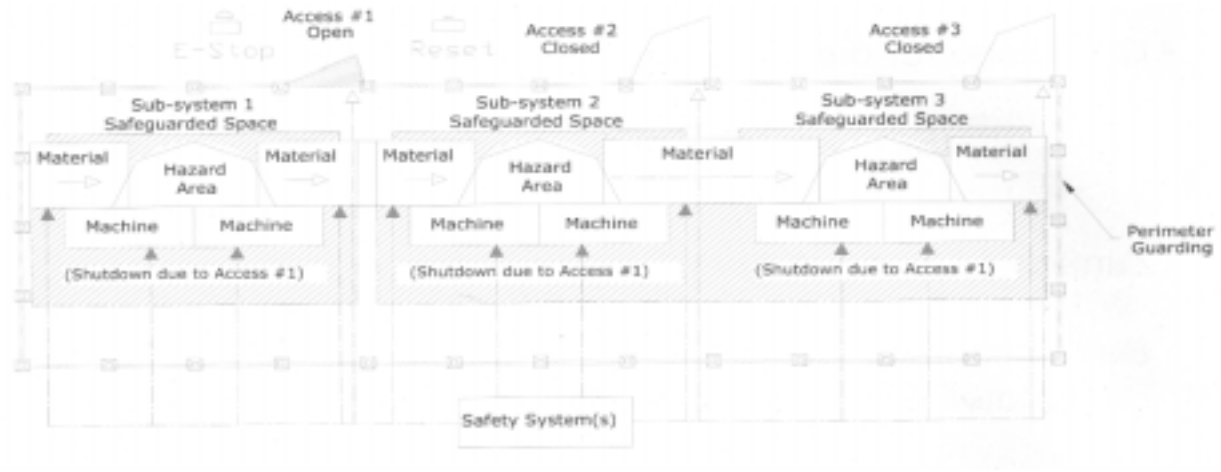
4．適応例

安全な E/E/PES 対象となりうる適用範囲として以下の分野があげられる（ドラフト段階を含む）；

EN50129 鉄道の安全 (Safety related electronic systems for signaling、安全についてのシステム定義、品質管理、安全管理、技術図書等機能安全の全ライフシステムを配慮した包括的な規格で、既に入札条件で示された例がある)
IEC61511 プロセス産業 (シャットダウンシステム等で適用済)
IEC62061 産業機械 (自動車産業などでの安全 PLC･通信･等複数の実績有り)
EN81-1 エレベーター(検討中)
IEC61513 原子力
IEC61800 回転機
その他、医療機器分野でも実質的に要求が出始めている。

機能安全規格 IEC61508 の適用例として、安全センサ、安全 PLC，安全フィールドバス・コントローラー、大規模プラントのシャットダウン・システム等があり、これらは既に実用化され複数の現場に設置されている。

物流システムなどの場合、小規模な複合生産システム或いは、物流倉庫での非常停止、安全スイッチ、安全ライトカーテン等の安全関連信号を制御面で処理する場合に、従来の有接点・ハードワイヤリングでやるかソフトで対応するかは制御版の設計とその設置において大きな違いが生じてくる。安全関連信号の総数が多ければ多いほど、安全ＰＬＣさらには安全フィールドバス・コントローラー等で処理をすると、反応速度や処理能力の面で大きなメリットが生じてくる。基本的に、安全関連信号を受ける安全リレーユニットを使用している場合に、その個数が 5―７個以上になると、経済的には安全 PLC 或いは安全フィールドバス・コントローラーが該当してくる。



Pic.5　Example of　machinery system with safety relevant signals

５．日本での対応

総括すると、大部分の産業機械・結合機械及び大規模システム等に不可欠な安全関連信号の処理系等をソフト化そしてさらに通信で結合する為の重要な要素である E/E/PES が機能安全の対象となり、部品・製品の開発・設計・保守等全ライフサイクルに亘る安全管理が必要となる事。そして、各部品・製品においてはその安全の妥当性確認を第三者認証にゆだねる事。

日本国内では、この機能安全規格が法規制の元に要求される見通しは殆ど無いが、グローバル社会ではユーザーが実際に特定分野においては要求し始めており、この要件を満たさない場合、海外案件への入札に支障をきたす場合が出てくる。

しかしながら、機能安全を達成する為の具備要件を満たしてゆく事の負荷は、大手企業にとっては人材及び資金の面で時間をかければ克服できるが、多くの中小企業にとってはグローバル企業活動を実践する上で、結構な負担になってくる。それ故、その運用を円滑に進める事ができる社会システムが必須要件となってくる。

同時に、機械安全及び機能安全の規格がますます包括化・体系化してゆく中で、ものづくりをになう事業者は万国共通に安全性のほかに経済性を追求する。その為、安全性の導入により生産性に支障をきたす事は極力避けなければいけない。多くの場合、それを回避する為に安全機器が無効化されたり、外されたりする事が度々あるが、生産性の観点から無効化を必要としない現場の技術に密着した安全方策のあり方は、未だ多々改善の余地を残している。つまり、正等論としては安全をやる事で生産性も向上する事が望まれる。特に、日本国内は安全規制のあり方が見直しを余儀なくされている中で、これらを考慮したあり方を考えてゆく必要がある。

さらに高齢者用の福祉ロボット或いは、レスキューロボット等これから開発・実用化が進むものなどについては、危険源であるロボットと人が柵なしで共存・協働し制御面での暴走の可能性がある為に、ここにどこまで機能安全の手法を適用してゆくか等についても、機能性・安全性等の兼ね合いからこれから議論のうえ整合性が取られてゆく必要がある。

最後に、製造設備の関連各社の安全責務のありかたと進め方を以下の通り整理したい；

● 機械使用者（事業者）

人の健康と安全を確保する製造現場を達成する為に、安全配慮義務をになっており、設置される機械が、機械安全並びに機能安全の要件を満たしている事を配慮する。さらに、機械の設置後の保守・設備拡張等のさいにも同様の配慮を行い、安全専門家による管理を実施する。

● 機械製造者（設計者）

国際機械安全及び機能安全の規格での要求事項を把握し、自ら製造する機械が科学及び技術の知見（state of the arts）に合致している事を技術者としての最低要件とし、自己責任に則り、安全の妥当性の立証を万が一の場合に直ぐできる為の図書作りを徹底する。第三者認証については、製品に応じ極力実施した方が後で有利になる。

又、科学及び技術の知見を最新情報に基づき理解できるべく学術動向も踏まえ、配慮する。

● 行政

急速に発展する科学技術社会において、国内のみならずグローバル時代に合致した、適切な安全規制・技術基準のありかた並びに国際標準化活動の促進加速化、安全の責任体制及び社会システム構築についての配慮義務。

参考文献：

（1） TUV mapping of standards and regulation/Technical Brief-09/Tony Simmons/13.10.2000/UK

（2） IEC61508. Functional safety of electrical / electronic / programmable electronic safety-related systems（JIS C 0508）

（3） 「機械安全・機能安全実用マニュアル」関口隆・藤義信監修、2001 年日刊工業新聞社