

安全確保に関する国際法規の枠組み

<機械・プラント等を中心に>

横浜国大 福田隆文・清水久二

1. はじめに

近年、食品産業や原子力発電、その他の産業において、安全問題への対応の拙さが社会的な大問題へと発展する事例が増えている。従来、科学技術教育において事故や不具合は一時的な人間のミスと扱われており、これを安全法規の枠組みの中で学問的に正式に取り上げるといふ事は遅れていた。この様な未熟な体験が前記の惨状に帰結したと思われる。

欧州ではセブン指令を以て「或る種の産業には危険性が存在する」ことを始めて公式に認めており、その為の安全法制や技術規格を年度的に整備してきた。欧州の先進的な安全規格は既に世界貿易に影響を与え始めている。本稿では特に化学プラントや一般機械産業、宇宙・船舶の分野において電気/電子的な手法を以て安全機能を実現する技術(SIS: Safety Instrumented System)に限定し、その安全法規の枠組みについて解説を試みる。最後に多重防護設計ツールの最近の動向についても簡単に触れておく。

2. 国際安全規格の包括化

(a) セブン指令以後の欧州法制の動き

EUはその前身であるECの頃より、域内での自由な製品流通が安全基準という非関税障壁によって阻害されるのを防ぐため、CEN(Comitee Europeen de Normalisation/CENELEC(Comitee Europeen de Normalisation Electro Technique)が中心となって加盟国相互の規格の整合化を推進してきた。この政策は欧州では旧アプローチと呼ばれている。しかし元来ECは英国、ドイツ、フランス等のように膨大な工業規格をもつ国の共同体であり、その整合化は遅々として進まなかった。1985年、ECはこの様な手詰まりを打開するために新アプローチという新しい政策を発表した。この政策の特徴は従来の各国の国内規格に代わるものとして、欧州閣僚理事会がEC指令としての約20種類の指令を発行し、定められた必須要求事項を製品が満足している限り、域内での製品の自由な流通を認めようとするものである。これに加えて1989年6月14日、閣僚理事会は加盟各国に対して、各国国内法において機械安全の法制を1993年1月を猶予限度として整備する様に閣僚理事会指令を出した。

以上の様な一連の政策の下で、国際標準化の分野でも安全に関する規格整合化の取り組みが急速に活発化した。例えば一般機械については1989年に欧州規格の審議機関であるCENがISOとの間で技術交換協定を結び、同様

の趣旨の協定が同年ISOとCENELECとの間で成立している。こうしてCENで作成された欧州規格はISOの舞台に移されることになり、機械安全に関する国際規格作成に向けて1991年にはISO/TC199(機械の安全性に関するISOの専門委員会)が設置された。この様なグローバルな標準化の動きはEUを中心とした欧州経済圏全域に敷衍される趨勢にある。ここでは話の順序としてまず機械指令について解説する。

(b) 機械指令(The Machinery Directive)

前述の国際安全規格の動向に関連して重要なのは欧州閣僚理事会の機械指令(1989年)が挙げられる。原版は89/392/EECであり、後に2度改訂された(91/368/EEC & 93/44/EEC)。この指令は機械の製造業者に対する指令であり、対になる指令として「労働の場における機械使用の指令」(The Use of Work Equipment by Workers at Work Directive)が良く引用される。これは使用者に対する規格であり、前者と密接な関係がある。EC及びEFTA域内の各国において機械の設計、製造、供給/購入、使用を行う場合、この指令の安全仕様に一致することが要求される。しかも現在ではEC加盟国の範囲は非常に広がった。

機械指令は新たな機械と安全要素(Safety elements)とに適用され、対象とする機械には主として金属工作、木工、運搬、作業、移動等の凡そ機械的イメージを有する機械全てが含まれる。除外される機械を下記に示す。

- ・余りにも単純な機械：増力機構のない人力機械。
- ・非常に危険性の大きい機器類：可燃性/有害性物質の貯蔵タンクと導管類、海上石油採掘用プラットフォーム設備類、陸海空における乗客輸送用の交通機関、原子力発電関連機器類、医療機器類。
- ・軍事/防犯に関わる機器：小型銃器類、兵器類。
- ・特殊な保全を必要とする設備類：ケーブルカー、一部のエレベータとリフト類、遊園地の設備類、農業機械類。

また安全要素とは機能安全を実現するリレー、インターロック、光線式安全装置、ゴムマット式安全装置等を指す。これ以外の具体的規定はAnnexの中にある。全規定に適合する機械はCEマーキングの表示が許されるが、責任者による適合宣言書の添付が条件となる。

指令の発効日は、機械については1995年1月1日、安全要素については1997年1月1日であり、移行までの2年の猶予期間中は従来の国内法準拠でよい。

規格との適合性の確認作業はISO/IECガイド51(付録)の趣旨と一致する。その作業は特定機械の考えられる危険を全て洗い出し、その危険性を低減するための安全対策を施すといった内容である。但しここで危険性の把握に確率論に基づく定量化は要求されない。機械指令の狙いは機械安全の型式認定のための国際的枠組みを定めようとするものである。ここで型式認定であるから保全や改修後の処置に対する言及がないことに注意したい。つ

まり恒常的な保全を必要とする機械類を除外されている。

(c) EN292 <機械安全の欧州規格、後に ISO12100>

本規格は理事会指令が加盟各国の国内法に移植される場合各国間に不一致が生じるので、これを防ぐための具体的安全要件を成文化した欧州規格と理解される。これは機械指令の技術的内容を忠実に規格化したもので、その解説は成書に詳しい⁽¹⁾。これを中核とした衛星規格群の対応関係を図1に示す。後に述べる EN954 は安全要素として特に電気的な制御機能を使用した場合のカテゴリを定めた規格である。

機械制御システムのある部分はしばしば安全上の業務 (Safety Task) に割り当てられる。これらは安全関連系 (Safety related system) と呼ばれ、ハードとソフトとから構成されることもある。そして制御システムの安全機能 (Safety function) を提供する。

適用範囲：この欧州規格は、安全関連部分の設計に関する機能安全とその原理に関連して、区分 (カテゴリ) と要求事項を定める。この中で全ての機械及び関係安全装置に対するプログラマブルなシステムが含まれる。本規格は使用するエネルギーの種類、例えば電気、油圧、空気圧、機械的とを問わず、制御システムのあらゆる安全関連部分の設計、構築、プログラミング、運転、保守及び修理に対する安全要求事項、及び指針を提供する。さらに本規格は、産業用、及び個人用の目的を問わず全ての機械の用途に適用される。またこの規格は類似の危険状態を有する他の技術目的にも使用される。ここで機械安全のカテゴリ分類 (区分) に関して誤解が発生しやすい部分を解説する。

まずこの規格では、

カテゴリ B は制御システムの安全関連部分の安全機能に関する基本レベルの区分とされる。

カテゴリ 1 では主として部品の信頼性を改善することにより一層高い安全機能レベルが達成できる。つまりここでは故障率の小さな部品の選択が問題になる。

カテゴリ 2, 3, 及び 4 では、主として制御システムの安全関連系の構造を改良する事により一層高い安全機能レベルが達成される。

つまり二重系にした構造や、自己診断機能の組み込みが性能改善に寄与する。

これらの製作において、機械の制御システムの安全関連系は何れかのカテゴリの要求事項に適合しなければならない。安全関連系が複雑になるにつれ、カテゴリは異なる複数モジュールが混在するが、所定の換算方式により代表的なカテゴリに属すると見なされる。

(d) EN954 <後に ISO13849>

~ (安全装置として電機・電子系を使用する場合)。

矢継ぎ早に発行された機械の安全規格は「安全配慮の

原則」から言って拘束性は強まった。そして具体的には機械設備のリスクを低減する具体的方策として「安全装置」の組み込みを必須の条件として規定している。まず安全装置に制御の一部を使用する場合の基準がここに規定されている。

安全業務はその性質と重要性とにおいて、本体システムの業務と異なっている。従って制御システムが考える安全機能、及び結果として採用される対策もまた異なる可能性がある。この規格の対象範囲は梱包機械、印刷機械、プレスの様な複雑な製造設備に至るまで、あらゆる種類の機械を対象としている。

適用範囲

この欧州規格は、制御システムの安全関連部分の設計において必要となる安全機能の考え、原理、及び仕様を定め、その特性を説明するものである。

安全対策の選定と設計手順は次に示す様なステップで行う。

(1) 危険状態の解析と危険度評価

EN292-1 等の危険度評価に従うことにより、機械寿命の各段階、並びに全ての動作モードにおいて機械に存在する危険状態を識別する。これら危険状態から派生する危険度を評価し、EN292-1 等に従ってその用途に応じた安全性の水準を判定する。

(2) 必要な安全性の水準まで危険度を低減するための要求事項を定める。

(3) 制御システムの安全関連系に必要とされる安全度水準を規定し、いかにそれを実現するかを決定する (ハードウェアのアーキテクチャの決定)。

(4) 設計

前項、及び目的 4.1 (安全機能に関する一般目的) で規定した仕様に従って安全関連系を設計する。

予見可能な故障を考慮に入れながら、各段階に応じて設計を検証する。

(4) 妥当性検証

前々項の規定に対して安全機能とその割当ての妥当性を検証する。

以上の五つのステップにより構成されるプロセスを必要があれば繰り返す。特にプログラム可能な電子系 (多重冗長性を有する PLC) を内蔵する安全関連系については別に定める IEC61508, or IEC61511 の国際規格に従う。

3 国際規格における安全の定義

安全とは事故や災害が起こらないことであり、これを回避するには正しい規範を厳格に守ることである。それでも起きてしまうのは、人間の過失や過誤に依るものである。これが過失責任主義の原則である。その結果全ての人的過誤を皆無にしようとする涙ぐましい努力が続けられた。この様な路線は安全が運転者の注意力のみに依存する交通機関の事故形態や、建設災害においては正解だろう。

しかし化学熱現象や材料の疲労・腐食現象など、自然科学では完全に捉えられない複雑な要因が関係するプラント事故の場合、人間の注意力に全面的に依存するのは酷というものであろう。そもそも人間の歴史そのものが人的錯誤の歴史と言ってもよく、人間は時代、時代に応じたその対抗処置としての防護策を考案してきたのである。そこで安全とは「危険な状態でないこと」という従来の定義を捨て、むしろ発想を逆転し、安全とは「危険が最小の状態であること」という新たな枠組みを構築すべきではなからうか。ここから危険を最小にする安全工学の方策と効果が具体化する。ここで導入されるのがリスクという概念である。EU法規でも安全管理の原則を「安全の管理」から「リスク管理」へと新たな転換を計った結果、幾つかの基幹的な指針が発行された。その最も有名なものは ISO/IEC ガイド 51 (付録) の規定であり、ISO/IEC が発行する全ての国際安全規格はこのガイドの精神に準拠する様に要請されている。いわゆるグローバルな安全規格の出現である。

4. 機能安全に関する国際規格

4.1 IEC61508, IEC61511

EN954 は ISO/IEC ガイド 51 の諸概念を継承し、安全装置の性能をリスクアセスメントにより評価し、その危険度を定性的に区分けする点で優れた規格であった。しかし化学プロセスの様な複雑な系では、多重防護の思想に基づいて安全の統合化が要請されている訳であり、定量的な評価が是非とも必要になる。特にセベソ指令に対応するにはリスク低減プロセスによって実現する包括的なリスクを数値的に計算する責務を求められていた。更に旧来の電磁リレーや機械的安全装置に代わるものとして、近年のマイクロプロセッサ技術の進歩を取り入れる舞台も要請されていた。と言うのは近年オランダを中心として、信頼性を飛躍的に改善した冗長性と自己診断機能の高い PLC が開発され、新時代の安全装置として既に成功を収めていたのである。この様な時代の要請に応える為、電気/電子/プログラム可能な電子系により機能安全を実現する場合、設計から設置、保守、廃棄に至る安全ライフサイクルに於いて行うべき手順を詳細に規定した規格 IEC61508 が発行された。

本規格の対象範囲は

- ・プロセス機器 (例えば緊急遮断系、火災及びガス検出系、燃焼制御系)。
- ・製造機器 (工業用ロボット、数値制御式工作機械等)
- ・輸送用機器 (鉄道信号、自動制御系、航空管制機器)
- ・医療用機器 (各種電子医療器具、レントゲン撮影装置等)。

などが具体例として挙げられている。なお原案作成作業に参画した技術専門家は英国、米国、ドイツの主要な化学プラントの技術者、英国の HSE(Health and Safety Executive)の担当官、機能安全用 PLC のメーカーの技術者、

フランスのソフトウェア会社の技術者である。

IEC61508 の特徴を EN954 と比較すると

(a)保守作業までを管理する安全ライフサイクル。

(b)ソフトウェア安全性の検査方式。

(c) 定量的尺度である安全統合度 (SIL: Safety Integrity Level)。

等の導入であろう。これにより安全関連系の優劣を比較する尺度が設定されて、相互比較することが可能になった。また IEC61511 はこれを化学プロセスへ適用する場合のより具体的な規格である。現在国際規格作成の最終段階に入っている。

5. 機能安全の設計 < IEC61508 の考え方 >

5.1 その概要

本国際規格は EN954 の概念を更に前進させ、リスク低減要求に応じたプラント設備や機器に装置された E/E/PES(電気、電子、プログラム可能な電子系)による機能安全を数値的に規定するものである。この概念の普遍性から鑑み、化学プラントに限らず高度の安全性が要求される他の機械システムへの適用が期待される。既にオランダ・シェル社等の国際的に有力な企業が採用している。なお翻訳 JIS は JIS C 0508 である。全体は 7 部より構成される。

第 1 部は規格の基本事項である。

第 2 部は主として計装系のハードウェアに対する。

第 3 部は計算機ソフトウェアに対する要求事項。

第 4 - 7 部は上記の技術的解説である。

他の規格にはない独自の概念は安全ライフサイクル、4 段階の安全度(SIL)規定(表 1)であろう。機能安全に要求される安全度はプラントハザードをどの程度に低減させるかの多重防護の方策に依存する。そこでまず許容リスクから解説を始める。

a. リスクの定義と変換

あるプラントの爆発・火災等の災害(ハザード)を考える場合、その脅威として 1 方では災害の重大性、例えば修復費用や操業停止による損失、或いは環境汚染に対する補償など、いわば貨幣価値に換算し得る要因がある。さらに他方ではその災害がどれほどの確率(或いは頻度)で発生するか、の要因がある。リスクとは拙著⁽¹⁾で解説した通り、この重大性(Consequence 或いは損害額) C とその確率(或いは単位時間当たりの頻度) F との積である。

$$R = C \times F$$

多様な災害に応じてこのリスク R 一定の直線を描くと、図 2 の様な曲線になる。重大性 C はプラントの形態や立地や生産種別によって相対的に変わるから、C の絶対尺度を決めることは出来ない。具体的にある国で C が決められれば、それに応じて頻度 F_p が決まる。

つまりリスク R ($\$/x 1/year$) の代わりに頻度 (1/year) を

新しい危険性の尺度としている。これを本書においては頻度リスクと呼称する。更にリスク曲線を段階化し判読し易い様に変換したのが表2であるが、これは経験技術的産物である。

b. 許容可能なリスク

多重防護の思想は、必要な機械・電気的手段でこのプラントのハザードを許容し得るリスク R_i まで低減しよとするものである。新しく導入された尺度を使えば、 F_i が許容し得る頻度リスクの目標値である。さてプラント危険 (EUC Risk) がリスク頻度 F_{np} で推定され、これを許容し得る量 F_i まで低減するために安全関連系を使う場合この系の機能の信頼性 (或いは確実性) が問題となる。安全関連系にも絶対確実と言うのはあり得ないので、その非信頼度を機能失敗確率 PFD と称する。システムが複数チャンネルが構成される場合はその平均値を意味する avg を添書きする。

プラント・ハザードのリスク頻度と安全関連系の機能失敗確率の積が残留リスク頻度である。即ち

$$PFD_{avg} * F_{np} = F_1$$

が必要条件である。

F_{np} は安全関連系に対する EUC 側からの作動要求 (ダイヤモンド) と解釈されるので、 PFD_{avg} は物理的には作動要求に対応する機能に失敗する確率である。その原因は主に機能安全のハード、ソフトの欠陥によるものである。換言すれば化学熱力学的な不確実性を電気・電子的な不確定に代替したと解釈される。

上式の両辺の対数を取れば

$$\log(PFD_{avg}) + \log(F_{np}) = \log(F_1)$$

となり、左辺のマイナスが増大し、リスク頻度の低減量を与える。各種のアーキテクチャで安全関連系を構成した時、その統合された PFD_{avg} を安全度水準 (Safety Integrity Level: SIL) と称する。与えられたプラント危険性の下でこの SIL をどの様に決定して行くかが、安全関連系の設計課題である。

6. ソフトウェアの安全規格⁽³⁾

6.1 始めに

ESA (Europe Space Agency: 欧州宇宙機構) が 1996 年に打ち上げたロケット・アリアン 5 が、発射後まもなく空中で爆発、落下した事故は当時テレビで多くの人が目撃した。しかしその原因が飛行制御用のコンピュータ・ソフトウェアの欠陥であったことを関係者以外で知る人は少ない。それ以来、欧州では ESA 加盟国を中心にソフトウェアに対する安全要求の国際規格作りが精力的に続けられている。特に英国は HSE や民間航空局を中心に非常に完成度の高い規格を既に作成し、一般に推奨している。

筆者は ISO/IEC TC65/SC65/MG9, 10 の国内対策委員会の主査としてこの問題に関わっており 特に IEC61508 制定後

の規格改訂作業委員会 (MT-12) に 2 度ほど出席している。現在の規格周辺の動向を紹介しておきたい。

現在の改訂作業委員会の委員達の問題意識は、

・産業界で日々開発されるソフトウェアの量は指数関数的に増大している。

・それらのソフトウェアは既存のソフト部品の組み合わせで構築されることが多く、過去の不確定な要素が蓄積される傾向にある。

ことであり、これが「潜在リスクの主要原因」になっていると指摘する。

これらに対処すべく一部の第三者検査機関では安全機能用ソフトの認定業務を検討しており、未来技術におけるコンピュータが果たす役割の重要性に鑑み、この様な動向が国際的な産業活動の中枢に影響を与える可能性もある。

6.2. アリアン 5 の爆発事故

1996 年 6 月 4 日の朝、アフリカの ESA 宇宙センターの空は快晴であり 打ち上げに天候上の障害は無かった。所定の時刻に打ち上げられたアリアン 5 は、点火シークエンス後 4.0 秒にして高度 3700m に達したが、その後突然軌道を外れ分解、爆発した。事故後直ちに加盟各国の専門家を網羅した原因調査委員会が組織され、事故原因の究明に当たった。事故の連鎖記録を詳細に分析した結果、慣性標定装置に指令を与えるコンピュータソフトに明らかなミスが認められた。即ちアリアン 5 の飛行制御システムに対する認定 (qualification) 手順は以下の標準の方式によっていた。

- ・装置認定 (Equipment qualification)
- ・ソフトウェア認定 (搭載コンピュータのソフトウェア)
- ・ステージの統合
- ・システム確認試験 (validation test)

適用された論理は、それ以前に達成されなかった問題を各段階毎にテストすることであり、この様にしてそれぞれのサブシステムと統合されたシステムの全てのテストを網羅していた。しかし打ち上げ直後の過渡期の IRS (Inertial Reference System) の挙動を確認する試験は省略された。その理由は IRS を飛行環境においてブラックボックスの状態を試験することが物理的には不可能であった。つまり加速度センサーの出力信号を取り入れた再現試験は地上では原理的に出来ないという点にある。さらに IRS のシステム仕様には運転上の制約が記載されていなかった。

事故調査委員会が得たその他の膨大な知見は省略するが、直接的な原因はアリアン 4 で使用されたソフトウェアの有るプログラム要素には implicit な定義のものが含まれており、それが 5 では見逃され誤動作した、ということである。

7. 最新の安全管理手法 LOPA について⁽²⁾

7.1 LOPA とは何か

国際機能安全規格は安全ライフサイクル全般の行為規範を規定したもので、具体的にプラント側がこれを実行するにはやや複雑な面が多い。そこでこれを HAZOP(Hazard and Operability Study) のような目的指向の意思決定手法として単純化したものが LOPA(Layer of Protection Analysis)である。LOPA とは複数の独立防護層(IPL) を幾つか重ね併せて多重的な安全対策を設計するためのリスクベースの意思決定の為のツールであるが、防護層の概念図は図3に示される FMEA(Failure Mode and Effect Analysis), HAZOP 等の他のツールとの比較模式図を図4に示す。この図を見ると、左端に定性的分析があり、右端には定量的分析がある。LOPA はそれらのほぼ中間に位置し、複雑なプロセスに関して半定量的に有効な防護対策が決定されると言う点に特徴がある。その有効性と独立性とは実際には Audit によって確認する。

7.2 LOPA の歴史

歴史的に化学プラントでは多種類の安全技術が開発され多重防護層として採用されてきた。これらの防護層の有効性が設計や保守部門において度々議論の対象となったが、事故は発生頻度の低い事象であるから、その議論が感情的なものになることも少なくなかった。そこでその有効性を客観的、合理的に評価するリスクベースの手法の開発が求められるにいたった。

1) 1980 年代：米国の化学品製造業者協会はプロセス安全に関する実務コード(規定)を出版したが、この中に防護層への記述が見られる。

2) 1993 年：CCPS は"Guideline for Safe Automation of Chemical Process" を出版したが、この中で SIF の SIL の実務的決定方法の一つとして LOPA の名を挙げている。この出版に刺激を受け、各企業では LOPA の開発に傾注し、その多くの成果は 1997 年の「リスク解析に関する国際会議(CCPS:Center for Chemical Process Safety 主催)」で総括された。これらの作業と平行して ISA S84.01, IEC61511 の規格作成委員会は SIF の構造と設計上の手法として LOPA に注目したが、後者の国際規格の第3部の原案が発表されるのに及び LOPA は広く注目される様になった。そして各企業が分担執筆して専門書⁽²⁾が CCPS より出版された。

参考文献

- 1) 清水久二・福田隆文「機械安全工学」、養賢堂、2000
関口隆・佐藤吉信「機械安全・機能安全実用マニュアル」、日刊工業新聞社、2001
渡辺昭一「電気機器安全規格導入ガイド」、日刊工業新聞社、2002
- 2) CCPS: Layer of Protection Analysis, AIChE 2001

3) <http://www.bsk.ynu.ac.jp/~shimizulab>

付録：ISO/IEC ガイド 51：

本ガイドは「安全に係わる」規格を作成する場合、その規格の体系を提供するものであり、安全が関連する全ての項目に適用される。ここでよく既発の ISO 9000 等と内容が混同されることがあるが、品質と安全とは同義語ではなく、品質規格と安全規格とのそれぞれ固有の役割を混同すべきではない。