国際規格 IEC61508 に適合した安全システム

IEC61508-compliant Safety System

赤　井　　創[*1]
AKAI Hajime

当社の安全システム ProSafe-RS は，安全関連系に関する国際規格 IEC61508 に適合すべく開発された。その適合性は第 3 者認証機関によって認証されている。この国際規格はリスク管理をベースとしたものであり，プロセス産業分野では世界に広く普及し，そのプラントの安全に役立てられている。ここでは，本特集号での各技術説明への導入として，国際規格IEC61508の骨子とリスク管理の概念，及び規格が求める安全システムの要件を述べる。

The ProSafe-RS Safety System has been developed in compliance with the IEC61508 international functional safety standard and has been certified by a third-party certification body as conforming to the standard. This international standard is based on risk management concepts and is widely accepted across the process industry for plant safety. In this artcle, we will discuss the main points of IEC61508, the concept of risk management and the standard's requirements for safety systems.

1. はじめに

最近の種々の産業事故，鉄道事故を目の当たりにするにつけ，“安全”がいかに第一優先でなければいけないことかを痛感する。安全第一といえば万人が納得し，これに異論をはさむ余地はない。しかしながら，実際にはその具体的達成目標が明確でなかったり，潜在危険の把握が十分でない場合があると感じる。

安全システムが規範としている国際規格 IEC61508 では，産業の安全に関して，リスク低減の定量的目標を決め，具体的手段によってそれを実現する指針を定めている。安全に関するこの考え方は，欧米に比べ日本ではその普及が遅れていたが，ここ数年の産業事故などを反省し，大きく注目を集めている。この規格が背景としている安全の考え方は，従来の安全＝「危険でない状態」に代わって，安全＝「許容できないリスクが無いこと」とする考えに基づいている。ある安全手段に欠点が無いことを仮定すると，その手段に欠点がないようにする努力は行うが，欠点が万が一あった場合に対する備えが疎かになる。一つの安全手段を講じても完全無欠のものはありえないので，そこで残るリスクに対して，その外側で別の安全手段を講じ，それでも残ったリスクがなお許容できる水準でなければ，更に外側に安全手段を講じるといった階層的防護の考えが必要となる。その中で各階層の安全手段は，明確にそのリスク低減の定量的目標が定められる。この特集で扱う安全システムにおいても，リスク低減に貢献するための定量的目標が定められており，それをどのように実現するかが，技術的要点である。

ここでは，以降の技術説明の導入として，安全システムが規範としている国際規格IEC61508の中で，リスクの扱いに関する部分と，安全システムの実現に関して規定している部分に焦点を当てて解説する。

2. IEC61508 とリスク低減

IEC61508 の表題は「Functional safety of electrical/electronic/programmable electronic safety-related systems」であり，これを翻訳して作成されたJIS C 0608 では，「電気・電子・プログラマブル電子安全関連系の機能安全」と訳されている。この規格は，その題名が示す通り，電気回路，電子回路あるいはプログラマブルな電子システム（E/E/PES：Electrical/Electronic/Programmable Electronic System）で，安全を実現する全ての場合に適用可能なものである。主要な適用産業として，プロセス産業，機械製造業，交通輸送，医療機器などが紹介されている。この中で，この規格を最も採用しているプロセス産業に対して，IEC61508 の傘下の規格として IEC61511（Functional safety：Safety Instrumented System for the process industry sector）が，2003 年に発行されている。この特集号の「安全システム」と並んで表現される「安全計装システム」の名前は，この Safety Instrumented Systemの訳であり，プラントの緊急遮断

*1 IA事業部システム事業センター 安全システム部

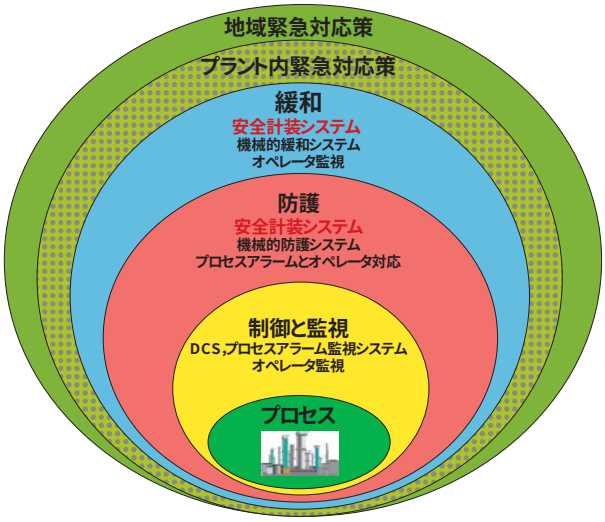

図 1　プラントの階層的防護と安全計装システム（SIS）

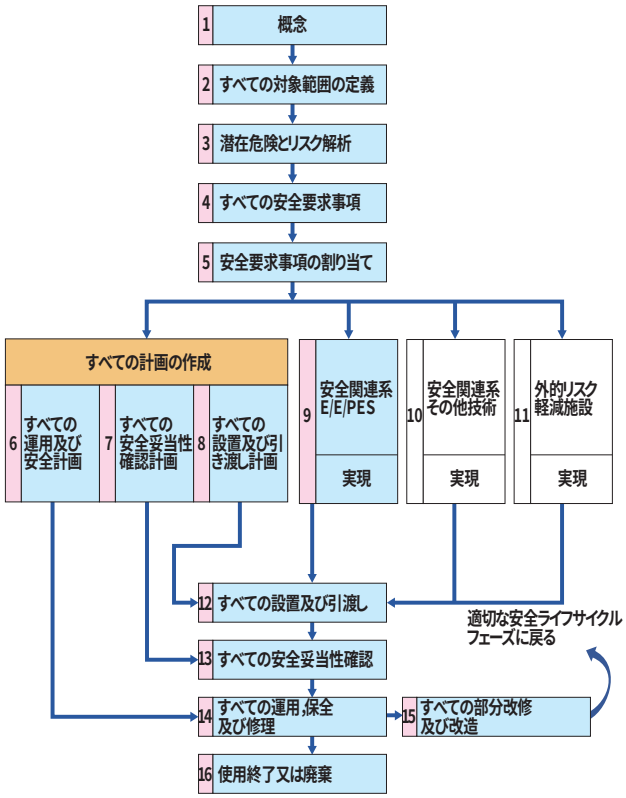

図 2　安全ライフサイクル

装置や防消火施設などに適用されている。安全計装システムは，プロセスの異常を検出するセンサ，センサからの情報を用いて予め設定された演算を行い，遮断弁などアクチュエータを起動するロジックソルバー，及びアクチュエータで構成される。この特集で扱う安全システムは，このロジックソルバーに位置付けられる機器である。**図1**に，「プラントの安全」を実現するための階層的防護の考え方と安全計装システムの位置付けを示す。この内容は，IEC61511で規定されているものであり，それを和訳して示したものである。

IEC61508においては，冒頭に述べたように，リスク低減に関して定量的指標を定めており，安全関連系をライフサイクルで管理することを規定している。以降のIEC61508の解説では，これをプロセス産業に適用された場合，すなわち安全計装システムの場合を例にとって説明する。**図2**に，IEC61508の安全ライフサイクルを示す。IEC61508の中で大変重要な位置付けとなるのが，3番目の枠で示される「潜在危険とリスク解析」である。ここでは，プラントとその制御装置（DCSなど）に生じる潜在危険及び危険現象の明確化を行うことを規定している。その中では，潜在危険の除去方法の考慮，危険事象の発生し易さの査定，危険事象に関して起こり得る被害の明確化を求め，プラントのリスクの推定及び査定（リスクアセスメント）を行う。リスク解析のための手段は限定されておらず，HAZOP スタディ（Hazard and Operability study）などいくつかの手法が規格の中で紹介されている。

そして次に，「すべての安全要求事項」で，上記で把握した危険事象に対して必要なリスク低減対策を決定する。リスクを低減する手段としては，安全計装システムの他，他の安全関連系（安全弁など）及び外的リスク軽減施設があり，それぞれに対して安全機能仕様を定める。安全計装システムの場合には，例えば，ある箇所の温度，圧力あるいはレベルの異常を検出した時に，遮断弁を閉じるというものである。また，この安全機能仕様と共に安全度要求を定めることが規定されている。安全度要求とは，プラントのリスクを低減する程度を定量化した要求仕様である。IEC61508 の表題にある「機能安全」とは，以上に示したリスク低減手段によって実現される安全のことを言う。

リスクは危害の大きさと危害の発生する頻度の掛算で表されるが，安全計装システムは危害が発生する頻度を低減する役目を担う。この規格では，安全度要求の表現方法として，安全度水準（Safety Integrity Level ＝ SIL）が導入された。安全度水準は，**表1**に示されるように，4等級（SIL1 ～ SIL4）にクラス分けされている。IEC61508では，安全関連系に対する作動要求の頻度から，低ディマンドモード（概略説明としては，作動要求が1年に1回以下）と高ディマンド／連続モードとに分けて安全度水準を扱っているが，プラントに設置される安全計装システムは，低ディマンドモードに分類される。低ディマンドモードにおける安全度水準の尺度は，PFD（Probability of Failure on Demand）である。このPFDは，作動要求時に安全計装システムが故障などにより働かない確率のこと

表 1　安全度水準（SIL）

安全度水準（SIL）	低ディマンドモード（PFD）
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

であり，この確率が小さいほど安全度水準が高くなる。

安全度要求の観点でこの安全度水準を見てみると，例えば，導入する安全計装システムに安全度要求として SIL3 を定めることは，SIL3 の PFD は 10^{-4} 以上 10^{-3} 未満であるので，元の危険な状態が発生する頻度を1/1000以下に低減することを安全計装システムに求めていることを意味する。つまり，例えば，何も対処されていないプラントでは10年に1度の危険な事象が発生し得るところを，安全計装システム導入によって，1万年に1度以下の頻度への改善が実現できることになる。

安全度水準（SIL）の決定に際しては，社会的な“安全”の指標を参照する。これは，IEC規格の範囲外の内容である。冒頭に述べたように，安全＝リスクが十分小さく許容できる限度未満であるという考え方が，これらの決定に大きく影響していることが分かる。欧米の例などを見ると，一人の人の事故による年間死亡確率を 10^{-5}〜10^{-6} の値を目標とする例が多い。日本での交通事故死の確率が年間で約 10^{-4} であるが，この平均値よりは更に低いことを目指している。これらのことから，上記の欧米での指標は納得できるものと考えられる。

さて，この「すべての安全要求事項」では，制御システムとの関連についても示している。**図 1** には，安全計装システムのプラント安全管理の上での位置付けが示されている。制御対象であるプロセスとそれを制御する制御装置が何らかの異常を来たした時に，安全計装システムは危険事象の発生を防ぐ役割を果たす。また，安全計装システムは，出火や毒性のガス突出の事態に対して，その影響を緩和するための防消火施設（F&G：Fire and Gas Protection System）にも適用される。ここに示されるように，各階層でそれぞれの安全機能が発揮されてはじめて，全体の安全が実現できるとの考え方である。

この考え方に基づき，規格の中では，安全計装システムと制御システムを分離しなければいけないことを述べている。これは，例えば同じプロセス変数を観測するからといって，センサを共用してはいけないことを意味する。なぜなら，一つのセンサの故障により，制御機能も安全機能も同時に喪失する可能性があるからである。また，制御システムは SIL1 未満の安全度水準と見なして，安全計装システムへの作動要求を見積もらねばならないことを述べている。これは，信頼性が高い制御システムを使用する場合にも，それを期待して安全計装システムに要求する安全度水準を簡単に低減させてはいけないことを意味している。

3. IEC61508 に適合した安全計装システムの実現

安全計装システムの具体的な構築は，IEC61508の安全ライフサイクル（**図 2** 参照）の中で，「安全関連系：E/E/PES」という枠で扱われている。安全度水準に合致する安全計装システムの設計に対して，規格では機器に使用される部品の「偶発故障（ランダムハードウエア故障）」への対応と，機器の仕様ミス，設計ミス，運用ミスなど「システマティック故障」と規格で呼ぶものの防止対策とを求めている。

(1) ランダムハードウエア故障への対応

安全度水準（SIL）の指標となっている PFD は，作動要求が発生した時に機器が故障により機能を失っている確率であるので，機器の不稼働率と捉えることができる。制御システムなどの場合には，機器の故障を，自己診断で故障検出できる部分と自己診断では検出できない部分に分類して扱うが，安全計装システムでは，更にそれぞれについて，安全側故障（出力がプラントを停止させる方向に導かれるか無影響）か危険側故障（プラントを停止させる出力機能を喪失）かで分類する。すなわち，安全側検出可能故障，安全側検出不能故障，危険側検出可能故障および危険側検出不能故障に分類される。危険側検出可能故障は自己診断で故障を知ることができるので，出力を別の手段で安全側に導くことが可能である。問題となるのが，危険側検出不能故障である。この故障は自己診断では見付けられないため，定期点検で行う動作試験（プルーフテスト）のみによって検出できる。非冗長機器の場合，このプルーフテスト間隔を T で表した時の PFD は，次式で表される。

$$PFD = \lambda_{DU} \times T/2 \cdots\cdots\cdots\cdots\cdots (1)$$

λ_{DU}：検出不能危険故障率

最近の機器は，デジタル集積回路を使用したマイクロプロセッサ応用製品であり，機器は高度な自己診断の徹底により，要求された PFD を実現している。特に注意すべきことは，安全計装システムの動作環境は，ほとんどの場合，その入出力信号に変化がないことである。従って，全ての信号には通常は変化がないことを前提に，自己診断回路を実現する必要がある。

それでは，実際にどれくらいの自己診断を実現することが求められるか，SIL3に適合する安全システムを例題として取り上げる。安全計装システムは，先に述べたように，センサ，安全システム（ロジックソルバー），及びアクチュエータで構成されており，

システム全体の PFD(sys)は,

PFD(sys)＝ PFD(センサ)＋ PFD(安全システム)＋ PFD(アクチュエータ)・・・・・(2)

で表される。実際のエンジニアリング上は，安全コントローラの場合，PFD(安全システム)はこの全体の PFD のうち 15% 未満であることが期待されている。残りはセンサとアクチュエータに割り振られる。すなわち，SIL3 の場合，PFD(sys)は 10^{-3} 未満，10^{-4} 以上であるので，PFD(安全システム)は 1.5×10^{-4} 以下であることが必要になる。一方，プルーフテスト間隔に関しては，日本国内でも 4 年連続運転を行っているプラントがあり，海外では更に長期間無停止運転が行われていることから，短い間隔でのプルーフテストは受け入れられない。そこで，プルーフテスト間隔を 10 年(簡単のため 10 万時間とする)として考察すると，危険側検出不能故障の値は式(1)を用いて，3×10^{-9}/h(3fit)以下であることが求められる。3fitというのは，一つの部品の故障率にも満たない小さな値であるので，ほぼ100%の自己診断カバー率を実現しないと達成できないレベルであることが分かる。経済性とのバランスを意識している一般の高信頼性機器とは明確に異なる。

(2) システマティック故障への対応

システマティック故障対応のうち，ソフトウエア設計への対策は重要である。IEC61508 の Part3 では，ソフトウエア設計に関して，誤解のない仕様記述を行い，それと対応付けられた設計を十分に管理された設計ツールを用いて行い，設計前段階で計画されるモジュールレベルやシステムレベルの検証を的確に行い，設計変更時には影響解析を含め厳しい管理を行うことを規定し，システマティック故障を防止できる仕組みを示している。これらの規定通りに実際の開発・設計プロセスが実行されていることを，第 3 者が確認することも規定されている。

今回開発した安全システム ProSafe-RS は，ここで示したランダムハードウエア故障とシステマティック故障への対応の両者が規格に合致していることを，第 3 者機関 TÜV によって認証されている。

4. おわりに

安全は全ての産業において最優先事項である。これまで危険ゼロ，すなわち絶対安全を目指してきた考え方に対し，ここで紹介したリスクベースの安全管理は，“ 許容リスク ” という言葉が何らかの妥協をもたらしているように受けとめられるかもしれない。しかし，厳密なリスク解析を実施してプラントの潜在的な危険を把握し，それに対して具体的なリスク低減手段を求めていることは，より厳しい要求であることを理解していただきたい。階層的防護の考え方は，最後の砦があれば，その内側では多少の緩和を許すというものでなく，制御装置の信頼性が高いことを理由に安全計装システムの安全度水準を下げる根拠を与えるものでもない。規格に適合した安全計装システムは，通常機器と違った卓越した自己診断機能を備えることでその認証を得ている。従来のリレーによる安全機能の実現と比して，遥かに安全性の向上に貢献できる安全計装システムが，今後更に普及することが予測される。

参考文献

(1) IEC61508 First edition : Functional Safety of electrical/electronic/programmable electronic safety-related systems

(2) 清水久ニ，福田隆文，機会安全工学ー基礎理論と国際規格，養賢堂，2000，188p.

(3) 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，2001，p. 220-243