機能安全規格の動向と普及の課題*

Current Situations for Functional Safety Standards and Tasks for Practical Use

佐藤吉信**

Yoshinobu SATO

Key words functional safety, risk assessment, IEC, ISO, JIS, risk-based safety standard

1. はじめに

20 世紀後半に著しく発展したコンピュータ技術は、各種産業設備や交通システム等に適用され、プロセスの自動化などに貢献してきた。当初、適用は安全に関連しない機能の履行に限られていたが、前世紀の終盤では次第に安全機能の遂行にも及んできた。安全機能とは、アイテムを安全な状態に維持し、または安全な状態に移行させる機能である。そこで、コンピュータ技術を含んだ電気・電子・プログラマブル電子システムを用いて安全機能を遂行するシステム（以下、安全関連系）により安全を確保するために、その設計、製造、設置、運用等全般に対する指針が必要になった。こうして発行された規格が IEC 61508¹⁾であり、いち早く 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」²⁾として翻訳 JIS 化された。

安全関連系は、典型的に、センサーなど入力装置、プログラマブル電子装置、アクチュエータなど出力装置などから構成され、所与の安全機能を所定の確率論的な性能基準すなわち安全度水準（SIL）で遂行するシステムである。

本稿では、IEC 61508 に関連する機能安全規格の現況、それら規格の普及における課題などについて述べる。

2. 機能安全規格の現況

2.1 機能安全規格群

IEC 61508 は、第 1 部「一般要求事項」、第 2 部「電気・電子・プログラマブル電子安全関連系に対する要求事項」、第 3 部「ソフトウェア要求事項」、第 4 部「用語の定義及び略語」、第 5 部「安全度水準決定方法の事例」、第 6 部

「第 2 部及び第 3 部の適用指針」そして第 7 部「技術及び手法の概観」から構成されている。このうち、第 1 部、第 3 部および第 4 部は基本安全規格に指定されている。

IEC 61508 に基づいて、プロセス分野における安全計装システムの機能安全規格 IEC 61511³⁾（これを翻訳した JIS C 0511⁴⁾）、機械類における安全関連電気・電子・プログラマブル電子制御システムの機能安全規格 IEC62061⁵⁾などが発行され、さらに 2011 年には自動車電子システムに係る機能安全規格 ISO 26262 が発行される予定である⁶⁾。

2.2 規格の背景

プログラマブル電子技術を含む安全関連系は、その技術の進歩の速さ、その複雑度などの理由から従来のような設計仕様や構造仕様による方法では十分な安全基準を策定することが困難である。また、設計仕様や構造仕様による基準化は、非関税障壁化しやすく、国際標準としては避けるべきものである。加えて、近年、後述のように「可能な限り安全にする（ALARP）」という考え方が欧米先進国で主流となった。この考え方を実現するためには、アイテムの相対的または絶対的な安全水準を評価する必要がある。このため、安全はできるだけ客観性をもった定量的尺度により評価されなければならないという状況に至り、定量的尺度としてリスクという概念が導入された。

2.3 規格の方法論

機能安全規格の特徴として次があげられる。1) 安全関連系がその安全機能の遂行に失敗する原因を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する、2) ランダムハードウェア故障に係る安全関連系の安全性能をリスクに基づく定量的性能基準で規定する、3) 決定論的原因故障の抑制に係る要求事項を全安全ライフサイクルの枠組みを用いて系統的に規定する、4) ソフトウェアに係る要求事項を規定する。

異なる部品ごとに異なる率で生ずる多くの縮退のメカニズムが存在し、製造・保管・運送・据え付け・使用条件上の許容誤差が相まって、運転中の部品の故障を異なる時刻において引き起こす。したがって、多くの部品から構成される装置の故障は、その率においては予測可能でも、予測

*原稿受付 平成 21 年 6 月 22 日

**東京海洋大学海洋工学部（東京都江東区越中島 2-1-6）

佐藤吉信

早稲田大学大学院修士機械工学専攻修了。工博（京大）。人間-ロボット系の安全性評価、機能安全のための安全度評価、確率論的安全評価・管理、リスクアセスメントに係る研究。著書は「安全の科学」（リアライズ社）、「機械安全/機能安全実用マニュアル」（日刊工業新聞社）など。

能安全実用マニュアル」（日刊工業新聞社）など。

不能なランダムな時刻において発生する。このように、ハードウェアの多様な劣化のメカニズムのもとで生ずる時間的に無秩序な故障がランダムハードウェア故障である。スキルベースあるいはルールベースのヒューマンエラーも、しばしば、定量化可能なランダムエラーに分類される。

一方、設計変更、製造過程、運転手順、文書化などに直接かわり、この類の要因の修正によってのみ除去できる故障が決定論的原因故障である。これには、安全要求仕様の策定、ハードウェアの設計・製造・設置・運転、あるいはソフトウェアの設計・履行の際に混入するヒューマンエラーなどが含まれる。

ランダム故障と決定論的原因故障とを区別する主な特徴は、ランダム故障から生ずるシステムの機能失敗（喪失）の程度が、確率などの適切な統計的尺度を用いることで合理的に予見可能であるのに対し、決定論的原因故障に基づくそれは、そもそも発生してはじめてその存在がわかるので、統計量としての把握ができない点にある。

3. リスクと安全

3.1 リスクの安全への導入

リスクは、今日では日常的にも広く使用されるようになったが、1960年代以前では、宇宙開発や軍需産業など非常に限られた分野でのみ用いられていたにすぎなかった⁷⁾。しかし、1970年代、米国において商用原子力施設の安全性を評価するためにリスクアセスメントが適用され⁸⁾、当該施設の安全性に対して非常に高い社会的関心がもたれていたこともあり、リスクの概念および技法は一般の産業分野にも急速に浸透してゆくことになった。信頼性とリスクの評価技術には共通する部分が多々あり、その後、両技術は両輪として発展し、今日に至っている。現在、欧米では製品安全の観点からもリスク評価を実施しなければならない⁹⁾。また、わが国においても、職場の安全のためにリスク評価は必須となりつつある¹⁰⁾。

3.2 リスクの原義

リスクという概念を史上最初に使用したのは、古代ギリシャの都市国家アテネの市民ともいわれている。都市国家アテネの政治家かつ哲学者であり、アテネの民主主義政治を確立したペリクレス（Pericles, BC495～429 ごろ）は、アテネの政治システムが優れている理由の一つとして、彼らが政治的決定を行う際に発揮するリスク（Risk）を推定し、査定する能力をあげている。リスクとは、将来の事態ないし状況がこのようになるであろう、あるいはこのようにならないと心に描いたものの、実際は必ずしもそのようにならないという将来の状況の不確かさと不確かさから生ずる結果とを意味していた。

強制されない自主的なリスク評価において、リスクを理性的かつ合理的に評価し、これを何らかの意思決定や行動様式に反映させ、有意な結果を得るためには、1) 当事者がある程度善良で正直である、2) ある程度の言論および表現の自由が存在し、3) 社会的に議論好きの傾向が存在

図1 事象の生起確率に対するリスクと危険性

する、ことが最低限必要である。すなわち、リスクを推定すると必ずしも当事者に都合のよい結果がでるとは限らず、そのような場合でも正直に報告することが必要である。大多数の人々にとって都合の悪いリスク分析結果でも、それを発表させる寛容さがなければならない。リスクを発見し報告するとき、それに係る議論に進んで参加する傾向が衆人に存在しないとリスク評価の意欲は衰退する。多分に都市国家アテネの市民および社会は、以上の資質を満たしていたと思われ、これをリスクマネジメントにおけるアテネの3条件ということにする。

3.3 リスクと安全安心

リスクの安全分野への導入が広く社会的に知られるようになった契機が米国における商用原子力施設のリスクアセスメントであることはすでに述べた。リスクの概念は古くより存在し、安全の問題から派生したものではないことは前節に述べた。ここでは、安全に適用したリスクの意味について考える。

図1は、横軸がリスク（不確かさをもった）事象生起のその確からしさを示す。この場合、確からしさは0から1の確率で表される。例えば、12時までに約束した場所に到着するべきところ遅刻するという事象の確からしさである。0は絶対に遅刻しないことを、1は必ず遅刻することを意味する。縦軸はリスクの相対的な大小関係を示している。ここでのリスクは、期待するものからのズレ（deviation）を意味している。

時間に間に合う、あるいは遅刻することは心に描くことができるが、半分遅刻するなどは描けないであろう。もしも：(イ) 間に合う（遅刻しない）ことを心に描いたとき、リスク事象生起の確からしさが0から増加するにつれて、リスクも相対的に増大する；(ロ) 遅刻する（間に合わない）ことを描いたとき、リスク事象生起の確からしさが1から減少するに従い、リスクは相対的に増大する。(イ)の結果はネガティブで、(ロ)の結果はポジティブといえるかもしれない。図中、凸形の曲線がこれを概念的に表している。

一方、安全の分野では、リスク事象は典型的に危害の発

図2 規制による安全と安全リスク領域

生である。危険性は危害の発生確率が大きくなるほど増大する。図中、直線はこれを概念的に表している。注目すべきは、危害発生確率が0の近傍では、一般的な意味のリスクと危険性とがほぼ重なることである。しかし、危険性は危害発生確率が大きくなるとリスクと一致しない。

次に、図2では、当初、領域Aにあったアイテムの危険性がアイテムの国や諸団体の設計仕様や構造仕様など決定論的規制あるいは基準への適合により、斜線の領域Bへと低減したことを表す。通常、決定論的規制や基準はわずかに不確か性を含む危険性を残す。これが、米国における商用原子力施設のリスクアセスメントのポイントである。元来、商用原子力施設の設計、建設にあたっては、十分な規制や基準が整備され、これを遵守して建造された施設は安全なはずである。安全であっても、さらに安心が求められる場合がある。安全といっても真に安全なのか、残る危険性はないのか、あるとすればどの程度の危険性なのかという疑問が生じ、疑問が解決されなければ安心は得られない。当該リスクアセスメントは安心を得るためのものであろう。

今日では、図2の斜線領域Bは製品や職場の安全として最低限すなわち根柢の領域を表す。図中、斜線部右側の領域Aは、アイテムが規制や基準を満足しない確定的に危険な領域であることを表している。この領域は、リスクとは乖離し、リスクで表現するのは不適切である。図中、斜線領域Bの左側の領域Cは、安全リスク領域ともいえるべき領域で、リスクの概念を適用すべき領域である。すなわち、安全性においては、不確かさを含む危険性がリスクであり、このリスクは可能な限り低減されなければならない。

4. リスクによる安全性能基準

自動車は40年程以前までは機械製品の代表的アイテムであった。これには電子技術はほとんど適用されていなかった。電子技術そのものが未熟であったという事情もある。その後、電子技術の飛躍的発展は、燃費や環境問題に対応するため、自動車の駆動、制動システムの電子制御を

実現させた。さらに、危害リスクの軽減すなわち安全機能に関係する部分も徐々に電子化が進んだ。今日では、組み込む電子部品およびソフトウェアが年々増加しているという。

近年の各種工業製品は、機械、電子などさまざまな技術の集大成によるものである。したがって、これにISO、IECおよびその他のさまざまな規格類を適用しなければならない状況となっている。このような事態に至っては、規格類相互間に矛盾がないことがアイテムの製造と使用において極めて重要である。ISOおよびIECから毎年のように安全に関連する規格類が発行されるが、これら相互に整合性をもたせるため、ISO/IEC Guide 51（以下、G51）¹¹⁾が制定された。すなわち、ISOおよびIECにおける安全に関連する規格類を策定する場合、基本的考え方、用語等はこのG51に準拠しなければならない。その後、その改定版が発行され、ISOおよびIECから発行する安全に係わる規格は、基本安全規格、グループ安全規格、製品の安全規格に分類されることになった。例えば、IEC 61508（その翻訳JIS C 0508）はG-51に準拠した最初の本格的な基本安全規格である。

G51では、安全は「受容できない（危害）リスクから免れていること」と定義されている。安全性の評価尺度を危害リスクとすることにより、アイテムの安全性能を当該リスクに基づいて規定することが可能になった。IEC 61508やISO 13849-1¹²⁾は、安全度水準やパフォーマンスレベル（PL）といったリスクに基づく確率論的基準によりアイテムの安全性能を規定している。

図2において、横軸は0から1までの確率で表されているが、リスク事象の確からしさの尺度はさまざまに工夫しなければならない。リスク事象が時間に関してランダムに発生する場合、例えば、安全関連系の故障が時間に関してランダムに発生し、安全関連系への作動要求もランダムに起きれば、リスク事象すなわち危害も時間に関してランダムに起きよう。すると、危害の発生頻度あるいは発生率が候補に挙がる。実際、わが国では頻度が多用されている。

暦の時間には、危害が起き得る時間と起き得ない時間とが含まれる。例えば、人が交通事故に遭う機会は、交通事故の結果として入院している時間以外である。頻度は暦の単位時間すなわち入院している時間も含む単位時間当りの危害リスク事象の発生確率である。他方、危害リスク事象の発生率は入院している時間すなわち危害が起き得ない時間を除いた単位時間当りの発生確率である。したがって、発生率は頻度よりも危害リスク事象の確からしさの尺度として妥当である。安全度水準はリスク事象の発生率から決定される。

5. 規格の有効性と普及

リスクに基づく安全規格の有効性について考察する。まず、このような新しいタイプの規格のプラントなど産業システムへの導入は、従来の規格や規制が完備している社会

環境では、新旧の規格間の摩擦のため容易ではない。

一方、歴史的な事情により旧来の安全規格や規制があまり整備されていない社会環境、例えばアジアの新興大国 Z 国は、最先端に行く規格 IEC 61508 をその発行と同時に国家強制規格として導入することに成功したという。しかし、最近 Z 国において数年間にわたって当該規格を施行してみたものの、事故が一向に減らないという事実が当局を慌てさせているということである。

この教訓は、図 2 における危険な領域 A から、決定論的な規制や基準への適合領域 B を飛び越えて、安全リスク領域 C へと二段階の飛び級を行うことがいかに難しいかを示している。「急がば回れ」の格言があるが、領域 A から領域 B へ、そして安全リスク領域 C への進級が着実なプロセスと考えられる。

リスク規範の新しいタイプの規格では、自主的なリスク評価に基づいて対策を実施することが前提となる。自主的なリスク評価には、3.2 節で述べた都市国家アテネのリスクマネジメント 3 条件に加えて、古代に比較して遥かに複雑となったシステムのリスク評価を行うための知識と技術、そして対策を実施するための知識と技術が必要とされる。このような知識と技術そして故障率のデータベースは、信頼性工学の技術とともに少なくとも 60 年間は蓄積されてきた。したがって、高々 10 年程度では咀嚼が困難である。今後、これは規格の普及において最大の課題となるかもしれない。

一般的な安全の分野では、リスクを導入してからあまり時間が経過していない。したがって、リスクの定量的な取扱いにさほど経験を積んだとはいえないのが事実である。特に、安全の分野で定量的にリスクを取り扱うために必要な素養として、信頼性工学の知識に基づくリスク分析の経験と知識が必要とされよう。しかし、先進諸国においても、リスク分析に精通している安全の専門家は稀である。機能安全規格における要求事項についても従来の決定論的な様式が多々混在しており、その結果、要求事項間相互に矛盾が存在すると考えられる場合も散見される¹³⁾。また、安全度等安全性能の確率論的指標の規定方法も未熟である¹⁴⁾¹⁵⁾。これらの問題の解決は今後の課題である。

6. ま と め

本稿では、まず、機能安全規格の特徴と現況および制定の背景について解説した。次に、機能安全規格はリスクア

セスメントに基づいて実施されるもので、リスクと安全、すなわちリスクの原義、リスクの安全への導入、リスクと安全安心について解説した。また、リスクに基づく安全性能規準である安全度水準およびパフォーマンスレベルについて言及した。さらに、規格普及の課題として、規格実施に必要な条件を考察した。特に、従来の決定論的な規制や基準が整備されていない環境において、リスク規範の安全規格を実施することには過大な困難が伴うであろうことに言及した。最後に、規格自体にも未成熟な点があり、これらの改善も今後の課題であることを述べた。

参 考 文 献

- 1) IEC 61508: Functional Safety of Electrical/electronic/programmable Electronic Safety-related Systems, Part 1~7, IEC, (1998~2000) 1.
- 2) 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, 第 1~7 部, 日本規格協会, (1999~2000) 1.
- 3) IEC 61511: Functional Safety—Safety-instrumented Systems for the Process Industry Sector, Part 1~3, IEC, (2003) 1.
- 4) JIS C 0511: 機能安全—プロセス産業分野の安全計装システム—第 1 部~3 部, 日本規格協会, (2008) 1.
- 5) IEC 62061: Safety of Machinery—Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems, IEC, (2005) 1.
- 6) 山下修平, 自動車用電子機能安全規格 ISO/CD26262 の紹介, 自動車技術, **62**, 10 (2008) 67.
- 7) E.J. Henley and H. Kumamoto: Probabilistic Risk Assessment, IEEE PRESS, (1992) 1.
- 8) USNRC: Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, (1975) 1.
- 9) 松本俊次: 安全とリスクに関連した訴訟に対する日本と欧米との違い, 標準化と品質管理, **61**, 12 (2008) 30.
- 10) 厚生労働省: 危険性又は有害性等の調査等に関する指針公示第 1 号, (2006) 1.
- 11) ISO/IEC Guide 51: Guidelines for the Inclusion of Safety Aspects in Standards, ISO/IEC, (1990) 1.
- 12) ISO 13849-1: Safety of machinery—Safety-related Parts of Control Systems—Part 1—General Principles for Design, ISO (2006) 1.
- 13) I. Yoshimura and Y. Sato: Safety Achieved by the Safe Failure Fraction (SFF) in IEC 61508, IEEE Trans. on Reliability, **57**, 4 (2008) 662.
- 14) 川原卓也, 市塚昭弘, 佐藤吉信: 自己診断を有する安全関連系の状態遷移モデルと機能安全評価, 電子情報通信学論文誌 (A), **J86-A**, 3 (2003) 241.
- 15) 下平庸晴, 佐藤吉信, 陶山貢市: 定常作動要求状態での平均危険事象率の推定と SIL 決定法, 日本機械学会論文集 (C 編), **72**, 715 (2006) 953.