解説/Review:

機能安全から見た横幹的係わりと意義

川島 興*

Meaning and Relation of Various Fields Across Boundaries in Functional Safety

Ko KAWASHIMA*

Abstract– The functional safety focuses on the hardware, software, and human which construct the safety-related control system, and specifies the requirements corresponding to the severity of the damage foreseen when the safety-related control system becomes malfunction. In order to achieve the functional safety, practical use of the basic researches accumulated in the past in fields, such as dependability, reliability, electricity, machinery, software, and management of an organization, is essential. This paper describes the relation of the technology of dependability and risk management fields across boundaries in functional safety.

Keywords– functional safety, dependability, IEC 61508, risk

1. はじめに

現代社会には，自動車，交通システム，化学プラント，医療機器，産業用ロボットなど，電子制御で機能し，故障や機能不全が危険な状態を引き起こす恐れのあるものが溢れている．電子制御は大変便利で使いやすい反面，多数の電子部品からなる電子回路とソフトウェアによって動作するため，どの部品がどう故障したときに何が起こるかを完璧に特定し，また，人に起因するソフトウェアや維持・管理などの運用上の不具合をゼロにすることは困難である．

日常生活において，まれに遭遇する交通機関，金融機関などのシステムダウンも同様である．後日の報道で，「バックアップのためにシステムを 2 重化していたが全く同じ部品を使用していたため，2 系統同時に故障した.」というような調査結果を耳にし，アセスメントが適切に実施されていなかったのではないかと思うことがある．

機能安全は，安全を確保するための電子制御のシステムに，故障時に予見される危険や被害への適切なレベルの安全要求事項を達成させ，必要なときに安全機能が合理的な確実さで働くようにするための技法である．

本稿では，複数の分野にまたがって分野横断的に技術を活用する事例として，電子回路とソフトウェアによる制御システムで安全を確保する技術“機能安全”と，ディペンダビリティ及びリスクマネジメントとの関係及び意義について国際規格の側面から紹介する．

2. 機能安全とは

2.1 横幹的係わりが支える安全技術

機能安全は，安全機能を制御するシステムを構成するハードウェア，ソフトウェア及び人間に着目し，それぞれにその制御システムが機能しなくなった場合に予見される被害の程度に応じた要求事項を規定する．この要求事項を満たすことで，予見される被害の大きさに見合った安全性を確保したと見なすことができる．この要求事項は，アーキテクチャと部品の信頼性で決まるハードウェアの故障確率にとどまらず，設計技法，解析技法，検証技法，開発から廃却までのライフサイクル全体にわたるマネジメントシステムの運用，要員の資質にまで及ぶ．そのため，機能安全を運用するには，信頼性，電気，機械，ソフトウェア，電磁両立性（electromagnetic compatibility），材料，組織のマネジメント，人間信頼性などの幅広い分野において過去に積み上げられた基礎研究の活用が不可欠である．機能安全によって安全を確保する技術は，まさに横幹連合が提唱する横断型基幹科学技術である．

*オリエンタルモーター株式会社　技術本部 技術管理統括部 安全規格課　千葉県柏市篠籠田 1400
*ORIENTAL MOTOR CO., LTD., 1400 Shikoda, Kashiwa-shi, Chiba
Received: 13 July 2011, 7 August 2011

2.2 機能安全の活用

電子回路やコンピュータが発達する以前，工場でものづくりに使われる機械で，安全確保のための制御回路といえば，多くの場合スイッチ，リレー，ヒューズなどの電気機械部品で物理的に電気回路を遮断して動作を停止させるものであった．

安全確保以外の目的においてはコンピュータによる制御が急速に普及したが，安全確保には電子回路より比較的単純，かつ，長い年月にわたって実績と信頼性を積み上げてきた電気機械部品による制御回路が用いられてきた．多数の電子部品を組合せた電子回路は，安全機能として使うのに十分なレベルまで故障確率を減らすことや，回路設計の誤り，ソフトウェアの不具合を少なくすることが難しいためである．

しかし，ここ数年，機能安全が広がり始めるとともに，安全機能の電子制御化も目に見えて進み始めてきた．その理由は様々だが，多くはコンピュータによる制御の利便性を安全機能にも展開するためである．

例えば，複数の機器をケーブル 1 本でリンクできる通信ネットワークで接続し，制御の省配線化が実現できたとする．ここに従来の方式で安全機能を追加するためには，リレーやスイッチなどの電気機械式部品とそれらを接続するための何本もの配線を追加しなければならない．しかし，機能安全を適用すれば，安全機能の制御信号はネットワークでやりとりでき，電気機械式のリレーではなく半導体回路での電源遮断も可能である．ネットワークによる省配線のメリットをできる限り活かした安全機能の制御システムが構築できる．

また，例えば，機械の動作中に作業者が巻き込まれるのを防ぐための安全シャッターで，閉まる速度が速すぎると，シャッターに挟まれてけがをする恐れがあるとする．このような場合，シャッターの速度を制御する機能は，安全機能として扱う必要がある．シャッターをサーボモーターで開閉しているならば，サーボモーターの駆動回路を機能安全規格の一つである IEC 61800-5-2（**Table 1** 参照）の所定の要求事項に適合させることで，想定外の速度変化に対する安全確保がなされていると見なされる．

工場の機械を事例に機能安全の活用について説明したが，機能安全は，プロセス産業の安全計装システム，自動車の制御などの様々な分野で活用され，また，さらに展開が進んでいる．これは，機能安全の要求事項を採り入れた国際規格が年々増加していることからも明らかである．

2.3 機能安全に関する国際規格

(1) 基本安全規格 IEC 61508

電子回路とソフトウェアを使った複雑な制御システムの安全性をどう評価するのか，その方法や基準を統一することは大変重要である．工場の機械の安全関連制御システムやプロセス産業の安全計装システムは，多数の部品やサブシステムから構成されている．すべての部品，サブシステムの安全性が統一された基準で評価されていない場合，これらを統合したシステムの最終的な安全性の推定は困難になる．

Table 1: Representative sector standards

Standards	Title
IEC 61511 series	Functional safety – Safety instrumented systems for the process industry sector
IEC 61784-3 series	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses
IEC 61513	Nuclear power plants – Instrumentation and control for systems important to safety
IEC 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional
IEC 61326-3-1 IEC 61326-3-2	Electrical equipment for measurement, control and laboratory use – EMC requirements – Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)
IEC 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC/TS 61000-1-2	Electromagnetic compatibility (EMC) - Part 1-2: General Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena
ISO 26262 series	Road vehicles – Functional safety

このようなことから，IEC（International Electrotechnical Commission：国際電気標準会議）は，機能安全に関する国際規格を制定している．中でも，基本安全規格として位置付けられる IEC 61508（Functional safety of electrical/electronic/programmable electronic safety-related systems）シリーズ [1] は，機能安全の土台となる要求事項を規定している．この IEC 61508 シリーズは，**Table 2** のように技術報告書（Technical Report）1 部と規格書 7 部から構成されている．

(2) 各産業分野の規格

基本安全規格である IEC 61508 シリーズは，特定の産業分野に特化した規格ではない．そのため，各分野それぞれの差異を考慮した個別の要求事項を規定する分野規格が必要となる．現在制定されている分野規格に

Table 2: Contents of IEC 61508 series

Standards	Contents
IEC/TR 61508-0	Functional safety and IEC 61508
IEC 61508-1	General requirements
IEC 61508-2	Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3	Software requirements
IEC 61508-4	Definitions and abbreviations
IEC 61508-5	Examples of methods for the determination of safety integrity levels
IEC 61508-6	Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC 61508-7	Overview of techniques and measures

は，モーターの可変速駆動システム，産業用の機械類，フィールドバス，プロセス産業の安全計装システムなどがある．また，近年電子化が進んでいる自動車に対しても，自動車専用の機能安全規格 ISO 26262 シリーズの開発がほぼ完了している．ISO 26262 シリーズは，本稿を執筆している 2011 年 6 月末時点ですでに内容が確定し発行作業段階に入っており，もうまもなく発行されるだろう．

機能安全の代表的な分野規格を **Table 1** に示す．

3. 機能安全とリスク定量化

3.1 リスクを把握する

機能安全を達成するためには，安全機能の制御システムが機能しなかった場合の被害の程度に応じた所定の要求事項を満足しなければならない．そのために，制御システムに存在するリスクを特定し，発生確率や発現した場合の被害の程度などを分析し，その結果から対策の必要性の有無や優先順位を決定する．この作業は，リスクアセスメントと呼ばれ，後に想定外の事故が起こることを防ぐ重要な鍵となる．リスクアセスメントについても国際的規格に基づいて，適切に実施することが大切である．

3.2 リスクアセスメントに関する国際規格

ここで，リスクアセスメントに関する国際規格の動向に触れておく．リスクアセスメントは，1970 年代に商用の原子力施設の安全性を評価するために用いられ，これが産業分野の安全性評価に展開された．やがて，社会システムが複雑化，高度化するとともに，安全性以外の，例えば経済，環境分野なども含めた様々な領域でリスクマネジメントが注目されるようになり，同時にリスクアセスメントも広がり始めた [2]．安全分野では，それまで機械安全分野のリスクアセスメントの原則を規定した規格として欧州の EN 1050 や ISO 14121-1 などが知られていたが，機能安全分野においては，個々の規格中でリスクアセスメントの概要や事例が示される程度であった．

Table 3: Representative risk assessment techniques which are useful for the functional safety described in IEC/ISO 31010

Analysis techniques	Reference
Hazard and operability studies (HAZOP)	IEC 61882
Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)	IEC 60812
Fault tree analysis (FTA)	IEC 61025
Application of Markov techniques	IEC 61165
Analysis techniques for dependability – Event tree analysis (ETA)	IEC 62502

2009 年，ISO（International Organization for Standardization：国際標準化機構）は，リスクマネジメントの方法を国際的に統一するために，リスクマネジメント用語を規定した ISO Guide 73, Risk management – Vocabulary[3]，及びリスクマネジメントの原則と指針を示した ISO 31000，Risk management – Principles and guidelines[4] を制定した．また，リスクマネジメントのプロセスに不可欠なリスクアセスメントについても，同年に IEC/ISO 31010，Risk management – Risk assessment techniques[5] として制定された．IEC/ISO 31010 には，リスクアセスメントの概念，プロセス及び利用できる解析技法とその選択方法が示されている．

なお，日本では，これらを JIS Q 0073，JIS Q 31000，JIS Q 31010 として，日本工業規格への取り込みを進めている．

IEC/ISO 31010 に採り上げられている，機能安全に役立つ代表的な技法を **Table 3** に示す．

3.3 リスクアセスメントとディペンダビリティ解析技法

IEC/ISO 31010 で採り上げている解析技法の大部分は，ディペンダビリティ分野の解析技法として知られている．ディペンダビリティ (dependability) とは，要求されるときにその要求を遂行できる能力である．つまり，狭義の信頼性 (reliability) だけでなく，保全性，保全支援性能まで考慮した総合的な信頼性である．安全機能を制御するシステムにおいて，システムのディペンダビリティが高ければ安全性も高まる傾向にある．ディペンダビリティとリスクは常に密接な関係にあることから，ディペンダビリティの解析とリスクの解析に共通の技法が用いられていることは至って自然である．

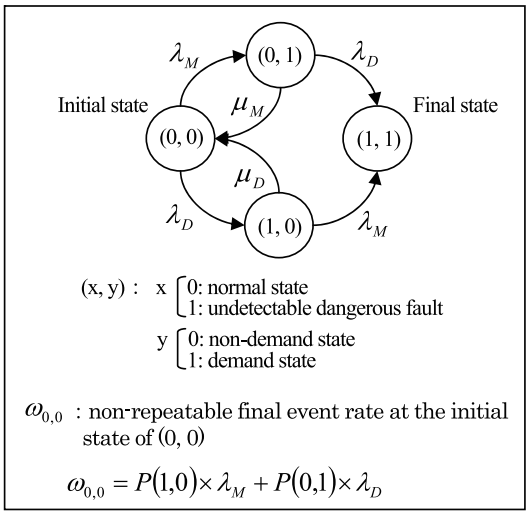

Fig. 1: Calculation of final event rate at the initial state

3.4 ハードウェアの偶発故障に伴うリスクの定量化

絶対に故障しない部品やシステムは存在しない．ハードウェアの偶発故障によって生じるリスクは，機能安全を達成するために考慮すべきパラメータの一つである．個々の部品が故障したときに，どのくらいの確率で事故が起こるかを定量化することは，リスクアセスメントのプロセスの一部として重要である．

安全機能の制御システムのリスクを定量的に算出する場合，安全機能の作動要求が連続して発生している状態以外では部品が故障したからといって必ず事故が起こるとは限らない．事故が起こるのは，故障が発生して制御システムがフォールト（機能しない状態）にある間に安全機能の作動要求が発生したときである．例えば，機械の非常停止システムの部品が故障し，非常停止システムが機能しない状態にあるとき，機械に挟まれそうになって非常停止スイッチを押した（作動要求した）が止まらない，という状況である．

また，故障が発生しても安全機能の作動要求が発生する前に，フォールトを検出して機械を自動停止したり，フォールトを修復したりできれば事故は発生しない．

このことからわかる通り，事故の発生確率は，安全機能を制御するシステムの故障確率やフォールトにある確率だけで決まるものではない．リスクを定量化するためには，複数の事象及び状態の複雑な関係を整理し解析する必要があり，それにはディペンダビリティ分野の技法が有用である．

ディペンダビリティ分野の解析技法をリスクの定量化に適用した例として，事故の発生率 $\omega_{0,0}$ の算出例を **Fig. 1** に示す．この例では，マルコフ技法を用いることで，作動要求及び発生したことを検出できない危険側故障の状態及び遷移を視覚的に示すことができる．

4. おわりに

機能安全から見て．ディペンダビリティの解析技法とリスクアセスメントは欠かすことの出来ない存在である．

本稿では機能安全の要求事項のうち，ハードウェアの偶発故障に関するものにしか触れていないが，機能安全の達成には，例えば，マネジメントシステムや要員の資質，人間信頼性などについても取り組まなければならない．複雑な電子回路，ソフトウェアで構成された制御システムを安全で確かなものにしていくには，様々な分野の知見を必要とする．

機能安全が安全確保のための技法としてさらに発展，深化していくために，分野をまたぐ横断型科学基盤技術，すなわち横幹的つながりを活かした総合的な取り組みを継続していくことが必要であろう．

謝辞: これまで機能安全，ディペンダビリティ及びリスク定量化についてご指導いただいた諸先輩及び日本信頼性学会要素技術安全研究会各位，並びに今回の執筆の機会を提供下さった関係者各位に感謝いたします．

参考文献

[1] IEC 61508-1～7 (Ed.) 2.0: “Functional safety of electrical/electronic/programmable electronic safety-related systems,” 2010.

[2] 川島興，下平庸晴，佐藤吉信: IEC/TC56-Dependability 2010 Limerick 会議報告及び規格動向，電子情報通信学会技術研究報告 SSS2011-3，2011.

[3] ISO Guide 73:2009: “Risk management – Vocabulary,” 2009.

[4] ISO 31000:2009: “Risk management – Principles and guidelines,” 2009.

[5] IEC/ISO 31010 (Ed.) 1.0: “Risk management – Risk assessment techniques,” 2009.

[6] IEC 61165 (Ed.) 2.0: “Application of Markov techniques,” 2006.

川島 興

1990 年千葉工業大学工学部精密機械工学科卒業．1991 年オリエンタルモーター株式会社入社．生産設備設計，電動アクチュエータ設計，製品の安全性管理業務に従事．日本信頼性学会　要素技術安全研究会主査，電子情報通信学会　安全性専門委員会委員，産業用ロボット安全性 ISO 10218 国内対策 WG 委員，IEC/TC56 Dependability エキスパート．