プラント・機械設備のリスク分析・安全度水準（SIL）評価サービス

Risk Analysis and Safety Integrity Level Analysis Services for Plants, Machinery, and Equipment

佐久間　晃　　米木　真哉　　櫛引　豪
■SAKUMA Akira　■YONEKI Shinya　■KUSHIBIKI Takeshi

機能安全規格IEC 61508（国際電気標準会議規格61508）の制定により，プラントや機械設備の設計においてリスクベースの考え方が浸透し，リスク分析の実施が必須になり始めている。

東芝は，原子力プラントで実績のある確率論的安全評価技術を活用して，プラントや機械設備のリスク分析業務並びに機能安全規格への適合支援業務を実施しており，危険事象の発生頻度の評価や，機能安全規格で要求される安全度水準（SIL：Safety Integrity Level）の適合評価を行っている。

Following the establishment of the IEC 61508 international functional safety standard by the International Electrotechnical Commission, risk analysis has become obligatory and risk-based management has been expanding in the design of plants, machinery, and equipment.

Toshiba provides risk analysis and support services for plants, machinery, and equipment to ensure conformity with the functional safety standard, applying probabilistic safety assessment techniques developed for nuclear power plants. We also provide estimations of the frequency of hazardous events and the safety integrity level (SIL) in accordance with the requirements of the functional safety standard.

1　まえがき

国際標準化機構（ISO）及び国際電気標準会議（IEC）の共通の安全規格のガイドラインとして，1990年にISO/IEC Guide 51[1]（第1版）が制定された。ISO/IEC Guide 51はリスクの概念を用いて安全を定義しており，安全に対するリスクベースの考え方が広く用いられるようになっている。

2000年にIECで制定された機能安全国際規格IEC 61508[2]（日本ではJIS C 0508[3]）は，ISO/IEC Guide 51に準拠した電気，電子，プログラマブル電子安全関連系（Electrical/Electronic/ Programmable Electronic（E/E/PE）Safety Related System）の安全規格であり，近年になって大幅な技術進歩を成し遂げているコンピュータ技術を利用した安全確保の手法や技法を体系化したものである。この規格の対象分野は広く,様々な産業界に分野規格や指針として波及し，海外，特に欧州の影響が強い地域では化学プラントなど，機能安全規格に適合した設計が求められるようになり，リスク分析の実施が必須になっている。

一方，国内においても，2016年までにポリ塩化ビフェニール（PCB）廃棄物の処理完了を目指すPCB処理施設では，事業基本事項の中で，“リスクマネジメントに基づく安全対策”を取り入れ，設計段階でのリスク評価を実施している。

東芝は，原子力分野で広く用いられる確率論的安全評価（PSA：Probabilistic Safety Assessment）手法をベースに，化学分野で広く用いられるHAZOP（HAZard and OPerability study）などを適用した機械設備やプラント向けのリスク分析・評価サービスを提供している。そこでは，火災や人身事故などのハザード（潜在的危険事象）が発生する頻度の確率論的リスク評価を行っており，更にIEC 61508への適合が要求された場合には，E/E/PE安全関連系が安全度水準（SIL：Safety Integrity Level）の要求を満足しているかの評価を行う。その適用手順並びに適用手法について以下に述べる。

2　リスク分析・評価手順

火災や有害物質の放出など，人身や環境に影響を及ぼす危険事象の発生による安全上のリスクと，事故による設備損傷や操業停止などの事業リスクの評価を目的として，プラントや設備のリスク（危険事象の発生頻度と被害の大きさで表現される指標）の分析及び評価を行う。**図1**は，リスク分析手順を示したもので，概要は次のとおりである。

2.1　評価対象範囲の選定

評価の対象とするシステムの範囲の選定，ハザードの特定，及び安全目標の設定を行う。

2.2　設備特性の把握

施設の主機能ブロックと，それをサポートする共用ブロック,施設全体に関連する電源系や制御系のブロックに分類し，その相互関連を模式化した機能相関図を作成し，設備特性を明確化する。

2.3　事故シナリオの抽出（ハザードの特定）

HAZOPやFMEA（Failure Mode and Effect Analysis）

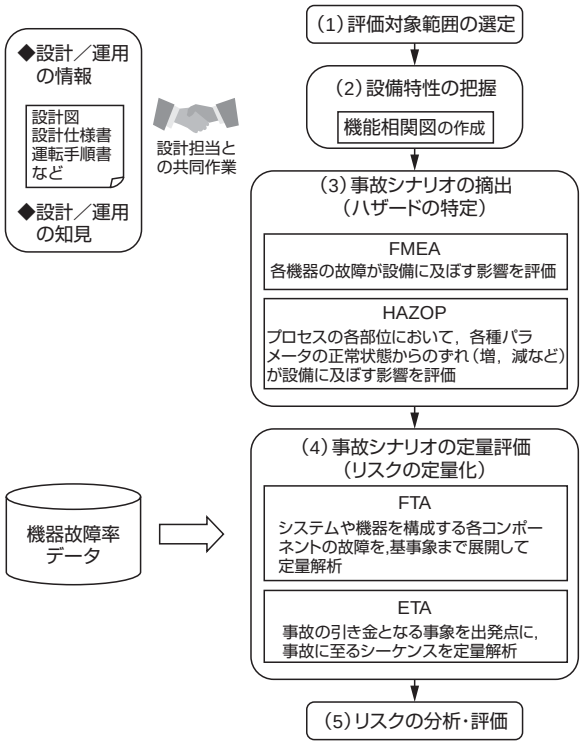

図1．リスク分析手順 ― ハザードに至る事故シナリオを抽出し，事故シナリオの発生頻度を定量的に評価する。

Steps in risk assessment

などの定性的リスク評価手法を用いて，設備に内在するハザードを特定し，危険事象に至るシナリオを摘出する。HAZOP及びFMEAの例を**図2**に示す。

HAZOPは，プロセスの各部位について，各種パラメータの正常状態からの“ずれ”（増，減など）を想定し，その原因と影響，現状の安全対策の有効性を検討する手法である。

FMEAは，機器レベルの故障を想定して，設備への影響を分析する帰納的な解析手法である。対象とする機器の様々な故障モードを想定し，これが結果として設備全体に及ぼすであろう影響を分析する。

また，作業従事者が介在する作業工程については，What-If手法を用いることもある。What-If手法は,「もし･･･ならば」という質問を繰り返すことにより設備や運転面でのハザードを抽出し，それに対する安全対策を講じることでシステムの安全化を図る手法である。

特定すべきハザードは対象設備により異なるが，廃棄物処理施設の評価の例では，次に示すハザードを対象とした。

⑴　火災
⑵　爆発
⑶　有害物質の漏えい，放出
　⒜　ガス：ダイオキシン，硫黄酸化物（SO_X）など
　⒝　固体：炭化物，不燃物に含まれる有害物質
　⒞　液体：排水中に含まれる有害物質
⑷　臭気，騒音，振動

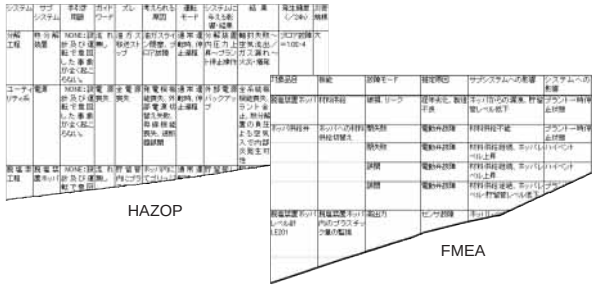

図2．HAZOP及びFMEAの例 ― 設備に内在するハザードを特定し，危険事象に至るシナリオを摘出する。

Examples of hazard and operability study (HAZOP) and failure mode and effect analysis (FMEA)

2.4　事故シナリオの定量評価（リスクの定量化）

抽出された事故シナリオについて，イベントツリー解析（ETA：Event Tree Analysis）を実施し，その発生頻度を算定する。また，イベントツリーの分岐確率を求めるにあたり，必要に応じてフォールトツリー解析（FTA; Fault Tree Analysis）を実施する。ETA及びFTAの例を**図3**に示す。

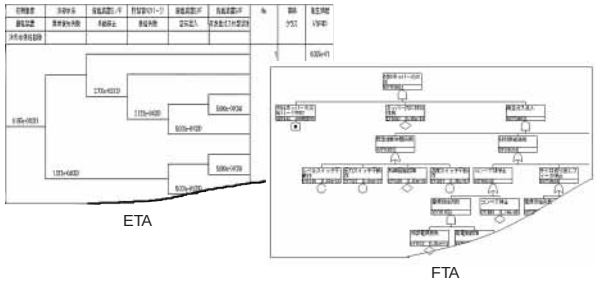

図3．ETA及びFTAの例 ― 摘出された事故シーケンスについて，危険事象の発生頻度を定量評価する。FTAを実施し，その結果をETAの各イベントの分岐確率に使ってETAを実施する。

Examples of event tree analysis (ETA) and fault tree analysis (FTA)

ETAは，危険事象の引き金となる事象（起因事象）を基点に，安全機能の成否やプラントの状態変化を考慮し，危険事象の発生頻度を評価する手法である。すなわち，起因事象を基点に，安全関連系の作動／不作動，アラームに基づくオペレータ操作による危険事象回避の成功／失敗などを分岐として組み合わせることで，事象進展のメカニズムをツリー状に展開する。また，各分岐の確率を計算することで，危険事象の発生頻度を算定する。

FTAは，起こってほしくない事象を頂上事象に設定し，その事象が起こるメカニズムを，安全装置を構成する個々の部品の故障など，基本的な事象（基事象）にまで，ANDやOR

一般論文

の論理ゲートを用いて展開して解析する手法である。機器の故障率などを用いることで，頂上事象の発生確率を算定することができる。リスクの定量化では，イベントツリーの分岐確率あるいは起因事象の発生頻度を算定するために，この結果を用いる。

2.5　リスクの分析・評価

事故シナリオの定量評価のアウトプットは，個々の事故シナリオの発生頻度と，それらをトータルした各危険事象（火災，有害物質の放出など）の発生頻度であり，これらの値が安全上の目標値を満足するか否かを評価する。このとき，目標値を満足しなければ，追加対策を検討し，再度定量評価を行うことになる。

3　機能安全規格に基づくSIL評価

プラントや機械設備の設計及び施工において，IEC 61508やIEC 61511[4]，ISA 84.00.01[5]（ISA：The Instrumentation, Systems, and Automation Society）への適合が要求されたときには，設備のリスクを評価し，安全目標を満足するように安全関連系を設置することになる。**図4**は，SILの評価手順である。用いられる手法は前項のリスク評価手法と重複するが，E/E/PE安全関連系へのSILの割当てとSIL実現の評価の手順が異なる。以下に，E/E/PE安全関連系へのSILの割当てとSIL実現の評価手順について述べる。

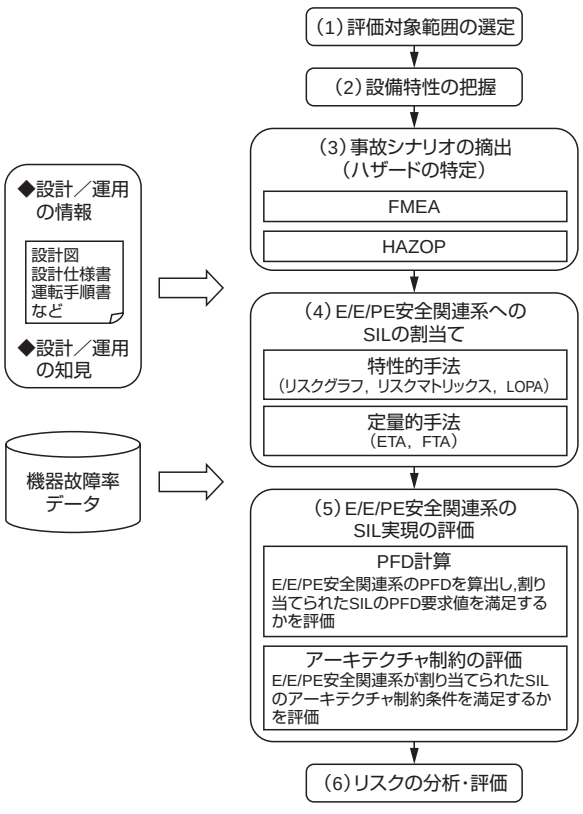

図4．安全度水準（SIL）の評価手順 ― E/E/PE 安全関連系へのSILの割当てを行い，割り当てられたSILの要件を満足するかを評価するため，E/E/PE 安全関連系の構成機器のPFDavgを算出し評価する。

Steps in SIL assessment

3.1　E/E/PE安全関連系へのSILの割当て

IEC 61508では，E/E/PE安全関連系が担うべきリスク軽減の度合をSILで表現する。SILのレベルは1から4まであり，各レベルに対して，**表1**に示す機能失敗尺度が割り当てられている。なお，プラントのE/E/PE安全関連系（すなわち，安全計装系）は大半の場合，表1の低頻度作動要求モードが対応する。

表1．E/E/PE安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

SIL definitions

SIL	低頻度作動要求モード運用(＊1)	高頻度作動要求又は連続モード運用(＊2)
4	10^{-5}以上10^{-4}未満	10^{-9}以上10^{-8}未満
3	10^{-4}以上10^{-3}未満	10^{-8}以上10^{-7}未満
2	10^{-3}以上10^{-2}未満	10^{-7}以上10^{-6}未満
1	10^{-2}以上10^{-1}未満	10^{-6}以上10^{-5}未満

＊1：作動要求当たりの機能失敗平均確率
＊2：単位時間当たりの機能失敗平均確率（1/h）

ここで，個人死亡リスクの安全目標が1×10^{-6}回/年として，安全関連系がない場合の危険事象の発生によるリスクが1×10^{-2}回/年のとき，安全関連系の設置により，リスクを1万分の1以下に軽減することが必要になる。このリスク軽減は複数のE/E/PE安全関連系やそのほかの技術，方策を用いて達成してもよいが，最終的にE/E/PE安全関連系が担うべきリスク軽減の機能失敗尺度のレベルが割り当てられるSILとなる。

E/E/PE安全関連系へのSILの割当てでは，リスクグラフなどの定性的手法と，ETAなどを用いた定量的手法による方法がある。リスクグラフの例を**図5**に示す。あらかじめ設定した分岐条件により，対象とするE/E/PE安全関連系がないと仮定した場合の状態を区分し，E/E/PE安全関連系に割り当てるSILを決定する。ETAを用いる場合には，対象安全関連系を除く各防護手段の失敗確率を分岐条件として，危険事象の発生頻度を算出する。その値と安全目標の値を比較し，リスクを安全目標値以下とするため，軽減率からE/E/PE安全関連系のSILを決定する。

3.2　E/E/PE安全関連系のSIL実現の評価

E/E/PE安全関連系にSILが割り当てられたとき，使用されるE/E/PE安全関連系が割り当てられたSILの要件を満足しているかどうかを評価する。IEC 61508では，各SILに

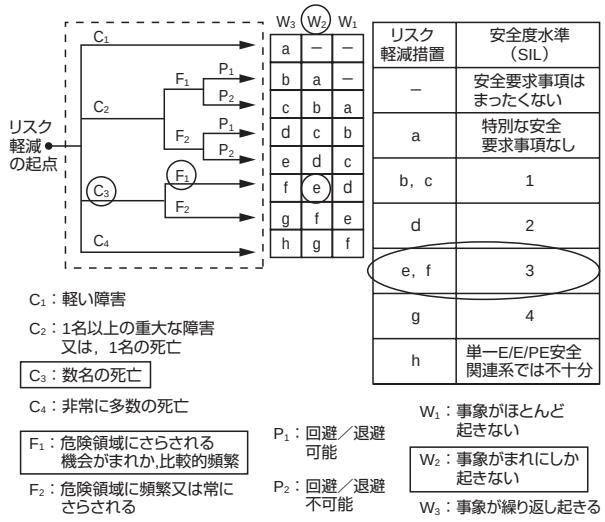

図5．リスクグラフの例（IEC61508-5 付属書D） ― 事象の発生頻度，被害の大きさ，暴露時間，回避の可能性により，危険事象を分類し，E/E/PE 安全関連系に割り当てるSILを選別する。

Example of risk graph: Attachment D to IEC 61508-5

対して作動要求当たりの機能失敗平均確率（PFD_{avg}：average Probability of Failure on Demand）のほかに，アーキテクチャ制約や使用する技法の要件が記載されるが，ここではPFD_{avg}の要件についてのみ述べる。

E/E/PE安全関連系が，センサ＋ロジックソルバ（ESD：Emergency ShutDown system）＋アクチュエータで構成される場合，E/E/PE安全関連系のPFDは各要素のPFDを足し合わせた値になる。

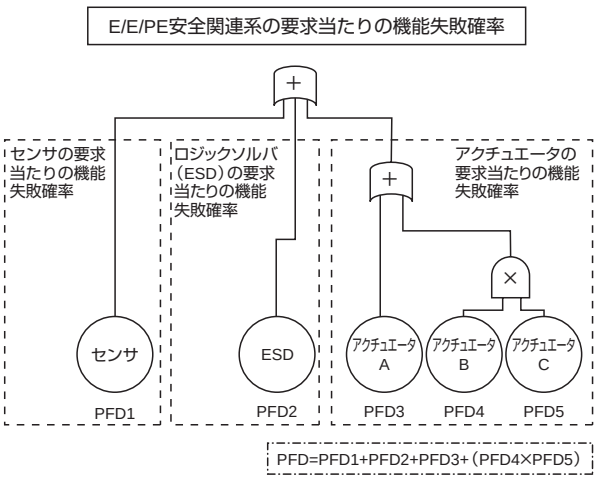

図6．フォールトツリーによるE/E/PE 安全関連系のPFD計算例 ― E/E/PE安全関連系へのSILの割当てを行い，SISが割り当てられたSILの要件を満足するかを評価するため，SIS構成機器のPFDavgを算出し評価する。

Example of probability of failure on demand (PFD) calculation with fault tree (FT) method

PFDは一般的に，機器の故障率と試験間隔に基づいて計算することができる。E/E/PE安全関連系全体のPFDは，構成する機器のPFDを基に，例えば**図6**に示すように，E/E/PE安全関連系の構成を示すフォールトツリーを用いて計算することができる。

4　あとがき

PSA手法をベースに，リスクの分析・評価や，E/E/PE安全関連系のIEC 61508への適合のためのSILの評価手順について述べた。プラントや機械設備のリスク分析の要求は，これまでは海外プラントが主対象であったが，IEC 61508のJIS化に続き，現在プロセス産業の分野規格であるIEC 61511のJIS化も進められており，国内においても安全確保に，機能安全規格に基づいたリスクベースの考え方が広がりつつある。

今回は，ハードウェアのリスク分析を中心にリスク評価の手順を述べたが，IEC 61508ではソフトウェアの安全性についても詳細な要求事項などがあり，今後はソフトウェアの安全性確保のための支援も進めていく。

文　献

(1) ISO/IEC GUIDE51, “Safety aspects - Guidelines for their inclusion in standards”. 1999.
(2) IEC 61508, “Functional Safety of Electrical/ Electronic/Programmable Electronic Safety Related Systems”. 1998.
(3) 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”. 日本規格協会. 2000.
(4) IEC 61511, “Functional safety - Safety instrumented systems for the process industry sector”. 2003.
(5) ANSI/ISA-84.00.01, “Functional Safety： Safety Instrumented Systems for the Process Industry Sector”. 2004.

佐久間　晃　SAKUMA Akira

電力システム社 情報制御事業推進室参事。リスク評価及び安全規格適合支援業務に従事。

Information & Control Solution Dept.

米木　真哉　YONEKI Shinya

東芝プラントシステム（株）原子力機械システム設計部 評価・解析技術グループ担当。リスク評価及び安全規格適合支援業務に従事。

Toshiba Plant Systems & Services Co.

櫛引　豪　KUSHIBIKI Takeshi

東芝ソリューション（株）ソリューション第四事業部 社会情報システムソリューション部。一般産業のリスク評価業務に従事。

Toshiba Solutions Corp.