N-026

機能安全設計におけるリスク分析のための事故事例の分類と活用方法

Failure Case Grouping and Utilization for Risk Analysis Process in Functional Safety Design

小原 俊逸 † 余宮 尚志 † 大場 聡司 †
Shunitsu Kohara Hisashi Yomiya Satoshi Oba

† 株式会社 東芝 Toshiba Corporation

1. はじめに

半導体の微細化技術の進歩により，さまざまな製品に半導体システムが組込まれるようになった．こうした製品に組込まれるシステムの大規模化・複雑化に伴い，製品の安全性を確保するための設計コストも増大している．IEC 61508 は半導体システムを含む製品の機能安全を対象とした国際安全規格である．同規格が提示するとおり，製品の安全性を確保するには潜在するリスクを設計時に分析する必要がある．リスク分析では過去の事例を参考にすることが望ましいとされている．しかしながら，機能安全設計の観点でどのような事例をどう参考にすべきかといった議論はあまりされていない．本稿では機能安全設計におけるリスク分析を効率よく実施するための，事故事例の分類と活用方法を提案する．提案手法により，製品の安全性を損なわずに安全機能の設計コストを低減することが期待できる．

2. 機能安全設計におけるリスク分析

機能安全は，本質安全と対置される概念である．危害は潜在的な危険源（ハザード）との接触で発生するが，本質安全が危険源の除去や低減を手段として確保する安全である一方，機能安全は機能を追加することで確保する安全である．

IEC 61508 は半導体システムを含む製品の機能安全を対象とした国際安全規格である．IEC 61508 では機能安全を実現する製品の設計・開発・運用のプロセスを「安全ライフサイクル」として提示している（図 1）．

「安全ライフサイクル」のボックス 3 では製品に潜在するリスクを分析することを求めている．ここで見逃したリスクは認知されないまま製品の開発および運用に至ってしまうため，重要なフェーズと言える．リスク分析の手法として，IEC 61508 では Failure Mode and Effect Analysis（FMEA）や，A Hazard and Operability Study（HAZOP）などを提示している．前者は IEC 60812，後者は IEC 61882 にその手順が提示されている．

3. リスク分析の過程を考慮した事例の分類と活用方法

リスク分析手法に FMEA や HAZOP を用いる場合，製品の機能ブロック図を作成し，想定しうるリスクを網羅的に見積る．網羅性を確保するための方策の一つとして，過去の事例を参考にする方策がある．IEC 60812 に対応する JIS C 5750–4–3 では，「新たに行う FMEA は，それを構成する既存のサブアセンブリに関する情報をできる限り使用することが望ましい」[2] と記載されている．

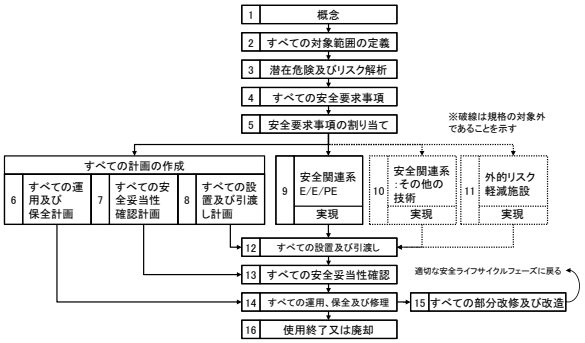

図 1 安全ライフサイクル（[1] を基に作成）

ここで参考にする事例は，リスクの網羅性の観点から，製品分野に固有の事例だけでなく，半導体システムを含む製品に共通する事例も含めるのが望ましい．しかしながら，該当する事例を単純に参照すると事例の数が膨大になり，設計コストが上がるばかりか，むしろ作業量の増大によって本来発見されるべきリスクを見逃す恐れがある．そこで，事前に事例を分類しておき，FMEA や HAZOP の過程に応じて必要な事例のみを参照することを検討する．

3.1 事例の分類方法

事故事例の分類方法に関する研究には [3–5] 等があるが，いずれも機能安全設計に関するものではない．

半導体システムを含む製品の機能ブロック図において，その要素は，（1）ハードウェア，（2）ソフトウェア，（3）人間のいずれかである．各要素の故障を想定する際はそのいずれかであるかは明確なので，まずは事例を故障の発生箇所で 3 つに分類できる．

IEC 61508 では故障をシステマティック故障（決定論的原因故障）とランダム故障の 2 つに分類している．ハードウェアの故障は経年劣化に伴う故障か否かでこの 2 つに明確に分類できる．

ソフトウェアの不具合をシステマティック故障と捉えるか，ランダム故障と捉えるかは，議論の余地がある [6]．しかしながら，リスク分析の目的を考えれば「設計以前に混入された不具合」と「実装以降に混入された不具合」の 2 つに分類するべきと考えられる．前者はたとえばソフトウェアは仕様どおりに作られたにも関わらず危険な事象が発生した場合，いわゆる仕様の不備であり，これはリスク分析の際にリスクとして想定されなくてはならないリスクと言える．後者はたとえば開発者が設計と異なる実装をしてしまう，いわゆるバグを混入してし

Copyright © 2011 by Information Processing Society of Japan and
The Instiute of Electronics, Information and Communication Engineers
All rights reserved.

表 1　分類結果

分類	発生箇所	故障の分類	事例 ID
1-(a)	ハードウェア	システマティック故障	CA0000077, CA0000081, CA0000180, CA0000431, CA0000506, CA0000519, CC0000184
1-(b)		ランダム故障	CA0000178, CA0000624, CB0011012
2-(a)	ソフトウェア	設計以前に混入された不具合	CA0000284, CA0000298, CA0000430, CA0000486, CA0000505, CB0012018, CC0200016
2-(b)		実装以降に混入された不具合	CA0000425, CA0000429, CA0000443, CA0000496, CA0000502, CA0000623, CZ0200702
3	人間	ヒューマンエラー	CA0000293, CA0000294, CA0000621, CC0000020, CC0000039, CZ0200713, CZ0200714, CZ0200723

まったために危険な事象が発生した場合で，リスク分析の目的を鑑みれば，これはリスク分析の際に要素に起こりうる故障として想定しなくてはならないリスクと言える．

人間が発生させる故障，すなわちヒューマンエラーは IEC 61508 が提示するとおり，すべてランダム故障に分類される．

以上の考察により，細かく分けて下記の 5 分類になった．

1. 故障の原因がハードウェア
   （a）システマティック故障
   （b）ランダム故障
2. 故障の原因がソフトウェア
   （a）設計以前に混入された不具合
   （b）実装以降に混入された不具合
3. ヒューマンエラー

3.2　分類した事例の活用方法

リスク分析の過程で，各要素の故障を想定する際は，発生箇所に応じて，1–(b), 2–(b), 3 に分類された事例を参考にするだけで良いと考えられる．一方，リスク分析の結果，許容できないリスクが見つかった場合，安全機能の追加を検討する前に，もともとの仕様に問題がないかを検討するべきだが，その際は，1–(a) と 2–(a) を参考にするだけで良いと考えられる．

4.　「失敗知識データベース」からの事例抽出と分類結果

提案した分類方法を用いて，「失敗知識データベース」[7] の事例を抽出・分類した．同データベースは科学技術振興機構の事業によって構築された事故事例のデータベースである．

「失敗知識データベース」に登録されている全 1175 事例について，「事例名称」「事例概要」「事象」「原因」の 4 項目を調査し，失敗の原因が半導体システムに関係していることを条件に事例を抽出した．なお，機能安全設計においては，事故の原因が半導体システムに関係しないリスクも対象ではあるが，そういったリスクは半導体システムを組込んだ製品に共通するリスクとは言えないため，抽出条件からは外した．

抽出した事例を提案する観点で分類した．その結果を表 1 に示す．

5.　有効性の検討

事例「CA0000284」と事例「CA0000496」を例として考える．前者は有名なアリアン 5 型ロケットの爆発事故だが，これは 64 ビット浮動小数を 16 ビット符号付整数へ変換する際に，オーバーフローしたことが原因とされている．この不具合は，本来リスク分析の結果として明らかにされ，対処されるべき不具合だったと言える．後者はアメリカで起きた放射線治療機の事故で，原因の一つはソフトウェアの不具合により誤った表示がされていることだった．この不具合は，リスク分析の際にソフトウェア要素に起こりうる故障として想定しなければならない不具合と言える．この 2 つの事例が 2–(a) と 2–(b) に分類されているとき，リスク分析の過程に応じてそれぞれの事例を参照することで設計コストの削減が期待できる．

6.　おわりに

本稿では機能安全設計におけるリスク分析を効率よく実施するための，事故事例の分類と活用方法を提案した．今後の課題は，事例の網羅性を確保しつつ，事例の細分化と活用手順の詳細化を進めることである．

参考文献

[1] JIS C 0508–1:1999, 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 部: 一般要求事項.

[2] JIS C 5750–4–3:2011, ディペンダビリティ マネジメント — 第 4–3 部：システム信頼性のための解析技法 — 故障モード・影響解析（FMEA）の手順.

[3] 太刀掛俊之, 山本仁, 臼井伸之介: 大学における事故事例の収集に関する研究: 人的要因の分析に向けて, 信学技報 SSS, Vol.105, No.238, pp.1–4（2005）.

[4] 森下壮一郎, 三島健稔: 内的セキュリティ問題の観点に基づくインシデント事例の分類に関する考察, 信学技報 SITE, Vol.109, No.74, pp.63–66（2009）.

[5] 米重宏美, 木村昌臣, 鍋田啓太ほか: 医薬品・医療機器等の回収に関するクラス分類の提案, 信学技報 SSS, Vol.109, No.177, pp.17–20（2009）.

[6] 情報処理推進機構ソフトウェア・エンジニアリング・センター編：組込みシステム安全性向上の勧め（機能安全編）, p.60, オーム社 （2006）.

[7] 畑村洋太郎ほか: 失敗知識データベース, 畑村創造工学研究所（オンライン）, 入手先〈http://www.sozogaku.com/fkd/〉（参照 2011–04–04）.

Copyright © 2011 by Information Processing Society of Japan and
The Instiute of Electronics, Information and Communication Engineers
All rights reserved.