N-025

国際安全規格 IEC 61508 に対応した教育教材の開発及び教育の実施
Development of Training Material and Its Implementation for International Safety Standard – IEC 61508

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

1．はじめに

多くの製品ではシステムが大規模化し、またその構造が複雑になってきており、安全性を重視したシステム設計の重要性がより高まっている。

これまでも、高い安全性を実現するための設計は行われてきた。そして、設計者向けの教育にもさまざまなものがある (企業の提供するものでは、例えば[1]など)。

他方、国際安全規格 IEC 61508 が 2000 年に、その改訂版となる IEC 61508 Ed.2.0 が 2010 年に制定された[2]。また、その下位規格となる ISO 26262 が 2011 年度内にも制定される見通しである[3]。

このような背景のもと、国際安全規格の認証を取得した製品、またはそれに準じた安全性を確保した製品を望む声が高まっている。しかし、そのためには、設計者や管理者が当該製品の国際安全規格についての知識を得る必要があり、国際安全規格に関する教育を用意する必要が生じていた[4]。

そこで本稿では、より高い製品の安全性を確保するため、IEC 61508 をはじめとする国際安全規格の知識獲得のための教育教材を開発し、教育を実施した結果について報告する。

2．国際安全規格の知識獲得に対する課題

製品の安全性を高める観点としては、従来は信頼性やセキュリティなどが主流であり、システムの安全性に関わる教育もこれらに主眼を置いたものがほとんどであった。しかし、信頼性やセキュリティでは、国際安全規格の要求事項を満たすことはできない[5]。また、医用機器、自動車、エレベータなどの製品では、安全性を確保するために古くからその製品に特化した安全のための技術を保持しており、当該組織の中で技術を伝播している。しかしながら、そのノウハウをほかの製品へ展開する仕組みはほとんど見られない。つまり、これまでは多くの設計者にとって、IEC 61508 などの国際安全規格や、それに準じた高い安全性を実現するための技術を習得する機会が限られていた。

IEC 61508 では、機能安全と言う観点から製品の安全性を確保する。そして、設計は安全ライフサイクルと言うプロセスに沿って行われる[6]。安全ライフサイクルでは、ハザードの特定やリスクアセスメントを Failure Mode and Effect Analysis (FMEA) や、A Hazard and Operability Study (HAZOP) などの手法を用いながら進める。これらは、従来の設計で必ず行われているとは限らない手法である。しかも、国際安全の規格書は、概念的な記述に留まっており、これらの手法をどのように使えばよいのかまでは記されていない。

そして、国際安全規格は製品分野ごとに制定される場合があり、改定も行われる。設計者にとっては、常に最新の規格に関する情報を取り入れることが重要であるにも関わらず、その情報をいち早く入手することが大きな負担となっている。国際安全規格の知識を得るための公開講座や教育を受けるには、それらが開発・提供されるまで待たなければならないが、規格の制定から時間を要することが多い。

以上の課題を整理すると、以下の 3 つとなる。

(1) これまでの教育では、IEC 61508 などの国際安全規格の理解に必要な情報が十分に含まれていない
(2) 国際安全の規格書は概念的な記述に留まっており、手法の具体的な使い方や手順が記されていない
(3) 多くの設計者にとって、新しい国際安全規格の情報を迅速に入手することが容易ではない

3. 教育教材の開発

教育教材開発の目的と、開発した教育教材について報告する。

3.1 教育教材開発の目的

2. で述べた 3 つの課題に対応するため、教育教材の開発では以下の 3 つを目的とした。教育教材をもとに実施する教育は、国際安全規格についての知識を必要とする全ての設計者を想定した。

(1) 国際安全規格に対する基礎的な知識が得られること
(2) 国際安全規格の中で推奨されている手法や手順が具体的に習得できること
(3) 新しい国際安全規格の情報が迅速に得られること

IEC 61508 では、新しい用語の定義や考え方などの知識が数多く必要となる。特に、安全ライフサイクルに沿った設計プロセスは、これまでのシステム設計プロセスと必ずしも同じとは言えない[7－9]。これらについて、前提知識を求めず、製品に特化しない内容の教育教材として広く設計者に提供することとした。

次に、国際安全の規格書には具体的な手段や手順が記されていないことに対応するため、それらの習得ができるものにし、教育で得た知識を設計現場で展開しやすくすることを目指した。

そして、国際安全規格の改訂や下位規格への情報の入手のしやすさを重視した。自動車向け国際安全規格である ISO 26262 など、現時点で未制定の新しい規格に関する知識にも、教育内容を拡充することで、迅速に対応できることを目指した。

† 株式会社東芝 Toshiba Corporation

3.2 開発した教育教材

教育教材開発の目的を満たすため、教育教材は以下のような 3 部構成をとった。

第 1 部: 国際安全規格に対する基礎的な知識
第 2 部: リスクアセスメントを中心とした演習
第 3 部: 新しい国際安全規格の情報

第 1 部では、安全意識の高まりやその重要性について触れ、続いて安全についての基本的な概念を理解できるようにした。そして、リスク、ハザード、危害、本質安全、機能安全など、IEC 61508 をはじめとした国際安全規格を理解する上で必要不可欠な用語を解説した。また、製品安全に関わる国際規格の体系、そして安全ライフサイクルや安全度水準とその考え方が習得できるようにした。

第 2 部では、解説を交えながら、演習を通して受講者が実習できる構成とした。具体的に演習の対象としたのは、安全ライフサイクルにおける「リスク分析の実施」、「安全要求事項の定義」、「安全要求事項の割り当て」、「安全系の実現」、「安全関連系の妥当性確認」などに関するフェーズである。演習の題材には、寒冷地における空調管理システム[4]を用い、FMEA や HAZOP を用いたリスクアセスメントの演習に重点を置いた。このほかにもリスクグラフによる安全度要求水準を決定する演習を用意し、実際に手法や手順を習得できるような教育教材とした。

また、本教育教材は既に IEC 61508 Ed.2.0 の内容を含むものとなっているが、現在開発中の第 3 部で、後に行われる改定やさまざまな下位規格にも対応できるようにした。具体的には、ISO 26262 では新しい用語や概念が登場し、IEC 61508 とは異なる要求事項が存在する。これらについて、IEC 61508 との差異を示すことで、ISO 26262 の情報を迅速に得られるようにする予定である。将来は、設計者・管理者のニーズに応じて ISO 26262 以外の IEC 61508 関連規格へも対応する。

4. 教育の実施と評価

開発した教育教材の第 1 部と第 2 部について、年 4 回の教育を開催しており、国際安全規格に関する知識獲得の機会を多く提供している。これまでの全受講者数は、約 90 名に上っている。

また、教育教材開発の目的に対する達成度を測るため、「教育の理解度」や「設計業務への有用度」などについてアンケートを行ない、教育評価を実施している。

これまでのアンケートで、全受講者の中で安全性を必要とする製品の設計経験のある約 87%に、

(1) 国際安全規格に対する基礎的な知識の獲得
(2) リスクアセスメントの手法や手順の習得

の 2 つについて問うた結果、(1) 90%以上が国際安全規格についての新しい有益な知識が得られたと回答し、(2) 70%以上が具体的な手法や手順の習得に効果があったと回答するなど、目標に対する成果が確認できた。

このようなアンケートを通じて、教育教材開発の目的の達成度合いを評価し、教育教材と教育の実施形態についての改善に役立てている。

さらに、開発中の第 3 部では、ISO 26262 の情報を含めている。自動車向け製品の設計者へ、ISO 26262 の情報が得られる機会をこれまでの教育の枠組みの中で提供する。この教育は、ISO 26262 制定前の年内にも、ドラフト版の情報をもとに教育を実施する計画であり、教育教材開発の 3 つめの目的についても達成できる見通しである。

5. おわりに

本稿では、IEC 61508 をはじめとする国際安全規格についての教育教材を開発し、教育を実施した結果について報告した。開発した教育教材は、国際安全規格の基礎的な知識を得ること、国際安全規格で推奨されている手法や手順を具体的に習得すること、新しい国際安全規格の情報を迅速に得ること、と言う 3 つを満たすものである。

今後は、国際安全規格の改定や新しい規格への対応を引き続き行い、アンケートに基づいた設計者・管理者のニーズに対応する。また、教育を受講した前後で、設計者の安全性に関する設計力の向上度合いを定量的に図り、それに基づいた改修も行う予定である。

そして、将来は機能安全に関する中級・上級レベルの設計者・管理者向けの教育教材も開発し、安全性に関する知識獲得の場を広げていく。

参考文献

[1] NEC ラーニング株式会社: 研修サービス, NEC ラーニング (オンライン), 入手先 < http://www.neclearning.jp/training/index.html > (参照 2011－06－28).
[2] S+IEC 61508 Ed.2.0: Functional safety of electrical/ electronic/ programmable electronic safety-related systems- ALL PARTS together with a commented Redline version.
[3] 山内信之, 深谷哲司, 古森誠司: 自動車の電子化・電動化を支えるソフトウェア技術と課題, 東芝レビュー, Vol.66, No.2, pp.17－20 (2011).
[4] 余宮尚志, 大場聡司, 田中里奈: ソフトウェアを中心とした安全設計技術, 東芝レビュー, Vol.65, No.7, pp.37－40 (2010).
[5] 社団法人組込みシステム技術協会 安全性向上委員会 製品安全ワーキンググループ(編著): 組込み系技術者のための安全設計入門, 電波新聞社 (2010).
[6] JISC0508－1:1999,電気・電子・プログラマブル電子安全関連系の機能安全.
[7] 向殿政男(監修): 安全設計の基本概念, 日本規格協会 (2007).
[8] 向殿政男(監修): 井上洋一, 平尾裕司, 蓬原弘一ほか: 制御システムの安全, 日本規格協会 (2007).
[9] 独立行政法人情報処理推進機構 ソフトウェア・エンジニアリング・センター(編): 組込みシステムの安全性向上の勧め (機能安全編) , オーム社 (2006).