ソフトウェアを中心とした安全設計技術

Safety Design Technologies for Software

余宮　尚志　　大場　聡司　　田中　里奈
■ YOMIYA Hisashi　■ OBA Satoshi　■ TANAKA Rina

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，安全性を考慮したソフトウェア設計技術の重要性がより高まっている。

東芝は，安全性の高い製品開発を実現するため，安全設計ガイド，安全設計教育，及び安全設計技術の開発に取り組んでいる。安全設計ガイドは，過去の事例から安全設計についての知識をまとめた文書であり，安全設計についての技術を東芝グループ内で共有することを目的としている。安全設計教育は，実習を通して安全設計ガイドの内容を習得できる教育プログラムである。安全設計技術は，事業部門での汎用的な適用を目指した，安全設計を効果的に実現するための技術である。東芝グループは，これら三つを活用して，製品の安全性を更に高めている。

In order to realize highly safe products, Toshiba has been making continuous efforts to develop the following safety design technologies for software: (1) safety design guides that summarize various safety-related knowledge acquired during the development of past products, (2) safety design education programs for software engineers to enable them to acquire mastery of the safety design guides through practical training, and (3) safety design technologies that enable business units to effectively implement safety design into their products.　We are applying these approaches to the development of products with higher safety for a broad range of markets.

1　まえがき

機能安全規格IEC 61508（国際電気標準会議規格61508）[1]が制定され，高い安全性を実現する製品の開発を望む声が，以前にも増して高まっている。また，多くの製品でシステムの大規模化，構造の複雑化が進んでおり，それに比例して，安全性を考慮したソフトウェア設計技術の重要性も高まっている。

東芝グループでは，ソフトウェアを中心とした安全設計の知識を共有し，製品の安全性を確実かつ効率的に実現するため，次の三つの取組みを進めている。

(1)　安全設計ガイドの開発
(2)　安全設計教育教材の開発と教育実施
(3)　安全設計技術の開発

ここでは，当社が取り組んでいるこれらのソフトウェア安全設計について述べる。

2　安全設計とは

安全を実現するための考え方には，“本質安全”と“機能安全”とがある。

(1)　本質安全[2]　　機械の設計又は運用方法を変更することによって，人や機器に危害を及ぼす原因を除去することで，又は危害の要因の数や影響の程度を低減することで達成される安全

(2)　機能安全[2]　　危害を及ぼす原因を除去するのではなく，システムに新しい機能として安全機能を導入して，発生する危害を許容できる水準にとどめることで達成される安全

従来は，このうち本質安全が重要視されてきた。しかし，特に大規模なソフトウェアを持つシステムでは，本質安全を達成するために，システムの基本機能や運用方法の大幅な変更が必要になる場合が増えている。そのため，近年では機能安全が注目されるようになっている。

安全設計とは，製品を設計する段階で，安全機能を組み込むことである。具体的には，機能安全を達成するためのリスクアセスメント[2]と，リスクを低減することを意味する。

また，安全設計のうち，ソフトウェアで機能安全を実現することを，ソフトウェア安全設計と呼ぶ。

3　安全設計ガイド

安全設計ガイドは，機能安全で実績のある製品の成功事例と技術ノウハウを文書としてまとめたものである。この安全設計ガイドは，安全設計の技術を東芝グループ内で共有することを目的としている。

従来，機能安全は，ソフトウェアではなくハードウェアで実現してきた。しかし，システム上の制約によって，ハードウェアだけで機能安全を達成するのは困難になってきている。安全

設計ガイドでは，システム全体としての機能安全について述べている。特にソフトウェアに関する機能安全は，過去の事例を参照しつつ，IEC 61508に基づいた解説になっている。

安全設計ガイドは，次の3分冊構成になっている。

(1) システム事例編
(2) ソフトウェア設計編
(3) 実践編

システム事例編では，ハードウェア，ソフトウェア個別の視点ではなく，システムとして，障害の検出や，誤制御対策，機能分担，テストなどについて，実事例を用いながら述べている。

ソフトウェア設計編では，ソフトウェアに焦点を当て，排他制御やプロセス・スレッド(注1)管理，リソース管理，通信方式，CPU管理など，製品の安全性実現のための実事例を取り入れたものになっている。

実践編は，システム事例編やソフトウェア設計編の理解促進を目的としたものである。車両運行制御システムなど，具体的なシステムを想定し，実際に安全設計の実践ができるものになっている。

三つのガイドは，事例に基づいてはいるものの，特定の事業領域によらない汎用的な内容としてまとめている。今後，ISO/DIS 26262（国際標準化機構／国際規格案26262）など，新しい機能安全規格にも対応していく。

4 安全設計教育

安全設計の効果的な実現には，安全設計ガイドの内容を技術者に正確かつ適切に伝えていく必要がある。そのため，安全設計ガイドの開発と並行して，安全設計教育教材の開発と，教育の実施を進めている。

安全設計教育は，安全設計にかかわる初級から中級の技術者を対象としており，東芝グループ全体の安全設計技術力の向上を第一の目標としている（**図1**）。

安全設計教育の基礎編は，広く開発手順を理解するための教育で，次の2点を目的としている。

(1) 製品の“安全”と“機能安全”の基礎を理解
(2) 安全な製品を開発するうえでの知識と手法を習得

安全設計教育では，IEC 61508で定義されている，次の主要な設計手順を学ぶことができる。

(1) リスク分析
(2) 安全要求事項の定義
(3) 安全要求事項の割当て
(4) 安全関連系の実現と妥当性確認

安全設計教育の基礎編で，特に重点を置いているのはリスクアセスメントにかかわる演習である。具体的なシステムを想定して次のような演習を行い，安全設計に関する知識だけでなく，実例を通して設計手法を実践する能力を養う。

(1) FTA（Fault Tree Analysis），FMEA（Failure Mode and Effect Analysis），HAZOP（Hazard and Operability Studies）によるリスク分析(注2)
(2) リスクグラフを用いたリスク評価
(3) リスク低減策の検討
(4) 安全要求事項の作成

このほか，中級編として，IEC 61508で定義されている設計手順の詳細化など，機能安全を実現するための技術ノウハウを深く伝えるための教育を開発している。

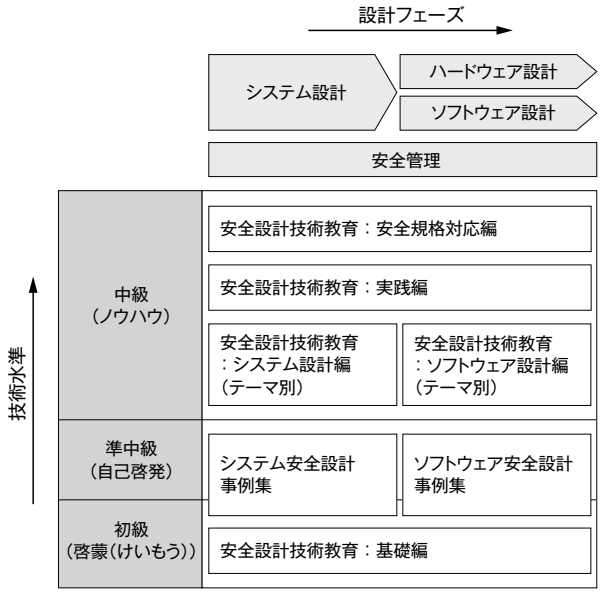

図1. 安全設計教育の教材体系 — 安全設計にかかわる初級から中級の技術者を対象としており，東芝グループ全体の安全設計技術力の向上を第一の目標としている。

Course materials for safety design education program

5 安全設計技術

当社では，多くの事業部門で共通して利用できる，安全設計技術の開発を進めている。安全設計ガイドや，安全設計教育に加え，安全設計をより効率的に実現するためである。

ここでは，次の二つの技術について述べる。

(1) 安全QCP（Quality Control Process）(注3)
(2) 安全なシステム構造の設計技術

5.1 安全QCP

安全QCPとは，標準的なシステム・ソフトウェア開発プロセ

(注1) ソフトウェア又はCPUの実行単位。

(注2) FTA，FMEA，HAZOPは，それぞれリスクアセスメント技法。
(注3) 安全QCPは，安全設計に関する品質管理プロセス。

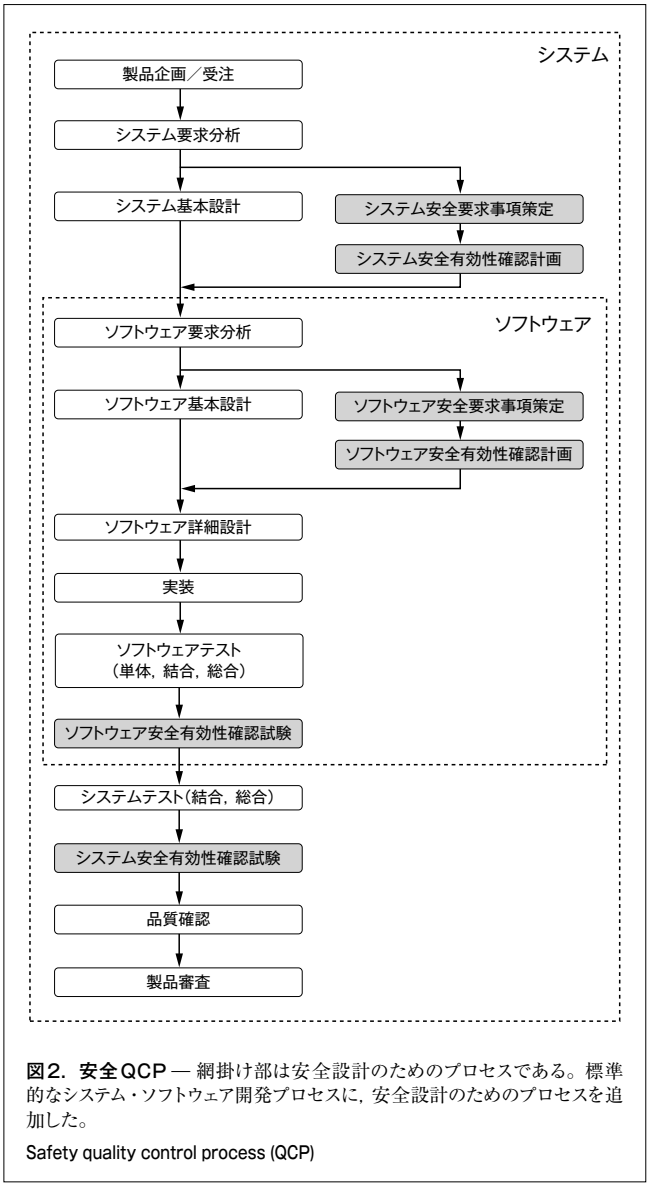

図2．安全QCP — 網掛け部は安全設計のためのプロセスである。標準的なシステム・ソフトウェア開発プロセスに，安全設計のためのプロセスを追加した。

Safety quality control process (QCP)

スに，IEC 61508で規定されているプロセスを融合させたものである（**図2**）。

従来の開発プロセスでは，システムやソフトウェアの要求分析の中で，安全設計が行われていた。安全QCPでは，社内の過去の成功事例を基に，設計の過程で機能安全を明確に意識し，確実に実施するプロセスを定義した。安全QCPによって，設計工程での安全設計が効率的に確保できる。

安全QCPの従来プロセスからの変更点や，各プロセスでの具体的な作業は，安全設計ガイドや安全設計教育教材へ反映して，安全QCPの普及を進めている。

5.2　安全なシステム構造の設計技術

システムの機能安全を実現するためには，安全にかかわるリスクをすべて抽出し，各リスクを低減させる安全機能を効果的に設計へ反映させなければならない。

そこで，システムを構成するEUC（Equipment Under Control）(注4) 及びEUC制御系(注5) から，安全関連系を分離し，安全関連系以外のシステムの干渉を最小限にとどめる安全防御機能を設計し実装する技術を開発した（**図3**）。

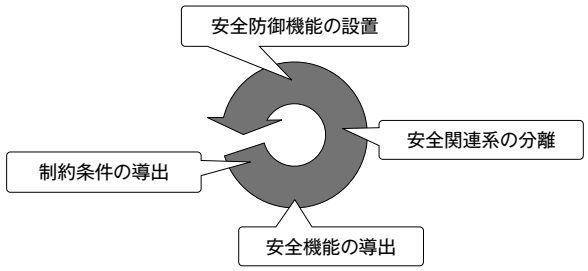

図3．安全なシステム設計のプロセス — 安全関連系を分離し，EUC制御系など安全関連系以外のシステムからの干渉を最小限にとどめた。

System design process for safety

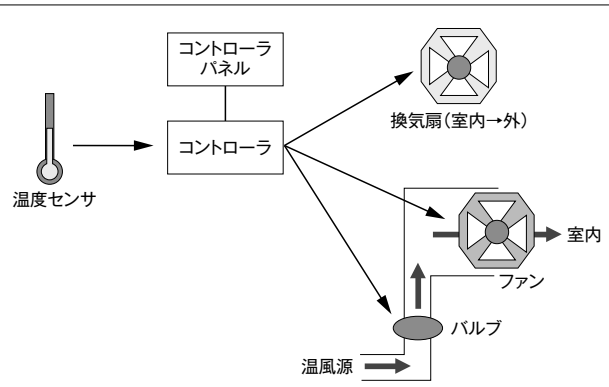

図4．例題とした，寒冷地における空調管理システムの仕様 — 温度センサ，コントローラパネル，コントローラ，換気扇，ファン，及びバルブは，ハードウェアやソフトウェアとの協調で動作する。

Specification of air-conditioner system for cold regions

図3に示す四つの手順について，寒冷地における空調システムを例題に，試行を行った。空調システムの仕様を**図4**に示す。それぞれの手順について次に述べる。

5.2.1　制約条件の導出　応答性能や開発期間，開発コストなど，開発の際に考慮しなければならない制約を，チェックリストを用いて抽出する。

空調システムでは，ハードウェアの変更や追加をしないことを制約条件とした。

5.2.2　安全機能の導出　FTAやFMEA，リスクグラフなどを用いてリスクアセスメントを行い，安全にかかわるリスクを抽出し評価する。そして，その結果に基づき安全機能を導出する。

（注4）　製造，プロセス，運輸，医療などで使用され，制御される設備，機械類，機器，又はプラント。

（注5）　プロセスやオペレーターからの入力信号に応じてEUC運転の出力信号を生成するシステム。

空調システムでFTAを実施した結果，室温が一定値以下になるときに，リスクが顕在化することが判明した。この結果を受けて，更にFMEAを用いて分析を行い，室温センサの故障を起因とするリスクを抽出した。そこで安全機能として，温度センサを監視する機能と，その機能を診断する機能の二つを導入した。

5.2.3　安全関連系の分離　安全機能を持つ安全関連系を，EUC制御系から干渉を受けずに設計どおりに動作させるために，これらから分離する。

空調システムでは，5.2.1で抽出した制約条件から，安全関連系を分離させる方法として，ハードウェアの変更や追加を行わずに，ソフトウェアの構造を分離させた（**図5**）。

5.2.4　安全防御機能の設置　制約条件を考慮したうえで，“安全関連系の動作への干渉”，及び“安全関連系のリソース（メモリ領域など）への干渉”の二つの観点に注目して，安全防御機能を導入する。

空調システムで，EUC制御系が安全関連系に与える干渉を分析したところ，EUC制御系が実行権を占有し，安全関連系が，動作できない場合があることが判明した。そこで安全関連系が一定間隔で確実に動作していることを保証するために，ウォッチドッグ機能(注6)を導入した。更に，安全関連系のメモリ空間をEUC制御系と独立させ，EUC制御系からのアクセスによるメモリの破壊を防止するメモリ保護機能を基本ソフトウェア（OS：Operating System）に追加した（図5）。

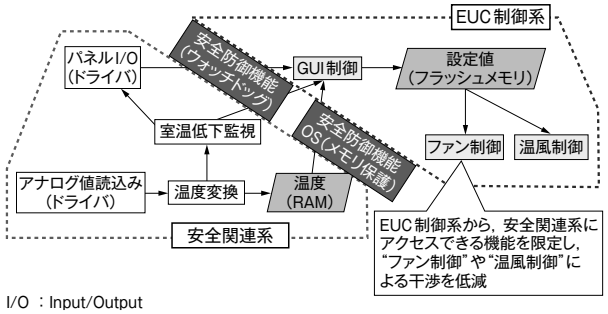

図5．安全関連系の分離 ― 室温低下を監視する安全関連系と，EUC制御系との間に安全防御機能を設置し，干渉を防止する。
Partitioning of safety-related systems

(注6)　システムが正常に動作しているかどうかを監視する機能。

6　あとがき

ソフトウェアを中心とした安全設計の取組みとして，安全設計ガイドの開発，安全設計教育教材の開発と教育実施，及び安全設計技術の開発について述べた。

東芝グループでは，このほかにもIEC 61508規格適合性を評価するツール“安診太郎”TM(3)の開発及び販売なども手がけており，安全設計の取組みへの一助としている。

今後とも，ソフトウェア安全設計技術の開発を進め，いっそうの安全性確保を推進していく。

文　献

(1) S+IEC 61508 Ed.2.0 : 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems-ALL PARTS together with a commented Redline version.
(2) 向殿政男，ほか．安全の国際規格 第3巻 制御システムの安全．日本規格協会，2007，287p.
(3) 東芝システムテクノロジー．“安診太郎”．東芝システムテクノロジー ホームページ．<http://www3.toshiba.co.jp/tst/product/anshintaro.htm>，(参照 2010-05-09)．


余宮　尚志　YOMIYA Hisashi
ソフトウェア技術センター　ソフトウェア設計技術開発担当主務。ソフトウェア設計技術の研究・開発，及びソフトウェア開発プロジェクトの管理業務に従事。情報処理学会会員。
Software Design Technology Group


大場　聡司　OBA Satoshi
ソフトウェア技術センター　ソフトウェア設計技術開発担当。ソフトウェア設計技術の研究・開発に従事。
Software Design Technology Group


田中　里奈　TANAKA Rina
ソフトウェア技術センター　プロダクツ開発部。
ソフトウェア開発プロジェクトの支援業務に従事。情報処理学会会員。
Products Development Dept.