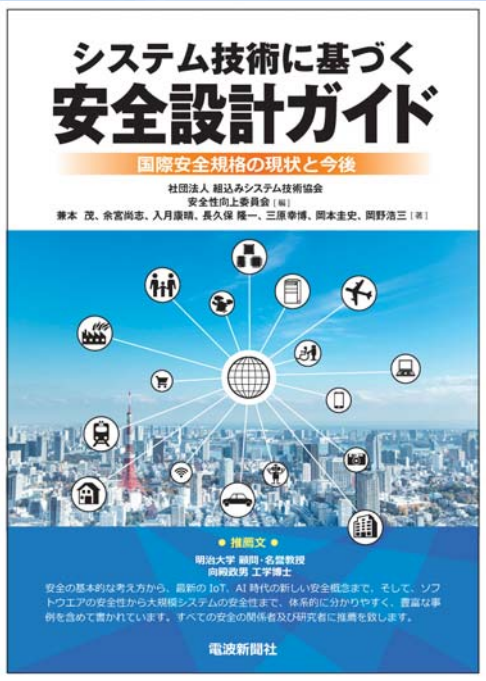
「システム技術に基づく安全設計ガイド」の出版について

余宮 尚志

安全性向上委員会 安全仕様化WG副主査



「システム技術に基づく安全設計ガイド」(電波新聞社殿より2019年秋出版予定)

出版の背景

2019年秋に「システム技術に基づく安全設計ガイド」が、本協会の会員でもある電波新聞社殿から出版される。

AIとIoT時代の到来で、セキュリティとあわせて、安全にかかわる重要性がより増している。ISOやIECなどの国際安全規格に対応したスキルが大前提として求められる時代になっているが、エンジニアが十分に育成できているとは言いがたい現状がある。

そこで、JASA安全性向上委員会では、既存知識の体系化を進め、企業で働く安全技術者の入門用テキストを出版することにした。

本書の特徴

国際安全規格や安全設計に対する予備知識のない方も対象に、安全設計の基本原理や安全論証の考え方などの基礎から解説しており、以下のような内容を含んでいるのが特徴である。

- 現状の規格の裏にある本質的な考え方まで解説している
- 従来の安全分析手法に加え、IoTとAI時代を見据えた新しい安全分析の概念を解説している
- ソフトウェア技術の重要性を意識し、豊富なソフトウェア安全設計の技術を解説している
- 最新版の規格に対応し、自動車や生活支援ロボットの規格も解説している

本書の内容

本書は以下で紹介する第1章から第9章までで構成されており、21個の豊富なコラムをあわせて掲載している。

・第1章「安全の基本」

安全の基本、安全設計の原理、安全論証の考え方、安全設計の基本戦略を解説。

・第2章「安全規格体系と概要」

安全規格と標準化、基本規格であるISO/IEC Guide 51やISO 12100を解説。規格の適用範囲や規格の限界にも言及。

・第3章「リスクアセスメント」

リスクアセスメントの原理原則、手順を解説。FMEA, FTA, HAZOPなど既存の安全分析手法の紹介と豊富な事例を紹介。

・第4章「機械系安全規格から見た安全設計の基本」

機械系安全規格ISO 13849に基づいたリスク低減方策として、3ステップメソッドを中心に解説(旧版のみに対応)。

・第5章「機能安全設計の基本/IEC 61508」

電気・電子・プログラマブル電子の機能安全規格IEC 61508の要求事項に基づいて、安全関連系の設計・開発方法について解説。IEC 61508:2010に対応。

・第6章「自動車の機能安全/ISO 26262」

自動車の機能安全規格ISO 26262について、規格の概略や全体構成、安全ライフサイクル、規格の主要なパートにおける考え方を中心に解説。ISO 26262:2018に対応。

・第7章「生活支援ロボットの安全規格/ISO 13482」

生活支援ロボットの安全規格であるISO 13482について、規格の構成や安全設計の流れについて、簡単な事例を用いながら、概略を解説。ISO 13482:2014に対応。

・第8章「システム思考で考えるこれからの安全」

システム理論に基づく安全分析手法(STAMP/STPA)について、背景にあるシステム思考の考え方、分析手順をいくつかの具体例を通して解説。

・第9章「ソフトウェアエンジニアのための安全設計」

安全設計で重要度を増すソフトウェアについて、(1)ウォータフォールとアジャイル開発プロセス、(2)モデルベース開発、(3)モデル検査、(4)コーディングガイド、(5)ソフトウェアFMEAの5つの要素技術を解説。