信頼性技術叢書

機能安全の基礎と応用

自動車・鉄道分野を通して学ぶ

信頼性技術叢書編集委員会【監修】
伊藤　誠・金川信康【編著】
石郷岡祐・金子貴信・川野　卓・
平尾裕司・福田和良【著】

日科技連

信頼性技術叢書の刊行にあたって

信頼性技術の体系的図書は 1983 年から 1985 年にかけて刊行された全 15 巻の「信頼性工学シリーズ」以降久しく途絶えていました．その間，信頼性の技術は着実に産業界に浸透していきました．現在，家電や自動車のような耐久消費財はほとんど故障しなくなっています．例えば部品を買い集めて自作したパソコンでも，めったに故障しません．これは部品の信頼性が飛躍的に向上した賜物と考えられます．このように，21 世紀の消費者は製品の故障についてあまり考えることなく，製品の快適性や利便性を享受できるようになっています．

しかしながら，一方では社会的に影響を与える大規模システムの事故や，製品のリコール事例は後を絶たず，むしろ増加する傾向にあって，市民生活の安全や安心を脅かしている側面もあります．そこで，事故の根源を断ち，再発防止や未然防止につなげる技術的かつ管理的な手立てを検討する活動が必要になり，そのために 21 世紀の視点で信頼性技術を再評価し，再構築し，何が必要で，何が重要かを明確に示すことが望まれています．

本叢書はこのような背景を考慮して，信頼性に関心を持つ企業人，業務を通じて信頼性に関わりのある技術者や研究者，これから学んでいこうとする学生などへの啓蒙と技術知識の提供を企図して刊行することにしました．

本叢書では 2 つの系列を計画しました．1 つは信頼性を専門としない企業人や技術者，あるいは学生の方々が信頼性を平易に理解できるような教育啓蒙の図書です．もう 1 つは業務のうえで信頼性に関わりを持つ技術者や研究者を対象に，信頼性の技術や管理の概念や方法を深く掘り下げた専門書です．

いずれの系列でも，座右の書として置いてもらえるよう，業務に役立つ考え方，理論，技術手法，技術ノウハウなどを第一線の専門家に開示していただき，また最新の有効な研究成果も平易な記述で紹介することを特徴にしています．

また，従来の信頼性の対象範囲に捉われず，信頼性のフロンティアにある事項を紹介することも本叢書の特徴の 1 つです．安全性はもちろん，環境保全性との関連や，ハードウェア，ソフトウェアおよびサービスの信頼性など，幅広く取り上げていく所存です．

本叢書は 21 世紀の要求にマッチした，実務に役立つテーマを掲げて，逐次刊行していきます．

今後とも本叢書を温かい目でご覧いただき，ご利用いただくよう切にお願いします．

信頼性技術叢書編集委員会

益　田　昭　彦
鈴　木　和　幸
二　川　　清

まえがき

情報技術の著しい進展によって，さまざまな領域において自動化が進むようになってきた．複雑なロジックで動作し，人間とも密接に関わり合うシステムにおいて安全を確保しようとするとき，そのシステムを人間から隔離するといったやり方は意味をなさない．安全を確保できても，そのシステムは使い物にならないだろう．むしろ，状況を監視し，状況に応じて必要な制御を行う，すなわち「機能で安全を確保」することが重要である．こうした意味での「機能による安全」としての，「機能安全」について，読者諸兄とともに学ぼうというのが，本書執筆の(少なくとも筆者にとっての)動機の一つである．

今日では，「安全のことは安全の専門家に任せておけばよい」という時代ではなくなっている．この意味で，本書は，さまざまな分野，職種の技術者が知っておくべき機能安全についての基礎的な知識について，具体的な事例とともに学ぶことができるように配慮した．安全設計を専門的に行う技術者のみならず，要素技術の開発に取り組んでいる方々にも読んでいただければ幸いである．自分が開発している技術が安全にどう関わりうるかを知り，いかにして安全を確保しうるかを知ることによって，よりよい設計につなげていただければ，筆者らにとってこれ以上の喜びはない．

さらに個人的には，自動化に係るヒューマンファクターの技術者にも本書を手に取ってもらいたいと考えている．機械・システムの側でできることには限りがある．だからこそ，多くの場合人間がシステムを監視するのである．ヒューマンファクターの専門家と機能安全の専門家とのコラボレーションが進むことが，より安全で，より便利なシステムの実現につながると信じている．

本書では，具体的な事例として，自動車と鉄道の分野を取り上げた．自動車分野では，まさに運転支援や自動運転の開発が進む中，機能安全に関する膨大な取組みが行われている．一般消費財としての自動車の中で機能安全をどう取り扱っていくのかを知ることができる点で，自動車分野以外の方々にも多くの

気づきが得られるであろう．

また鉄道分野は，大勢の乗客の安全を確保するという責任を負っており，求められる安全のレベルが文字どおり「桁が違う」．その中で，安全を確保しつつも，より高い利便性の提供に向けた取組みが続けられている．鉄道分野からも，また新たな気づきが得られると確信している．

実際，執筆者同士の議論の中でも機能安全に関する多くの気づきがあった．機能安全という概念の奥深さ，それぞれの分野固有の事情による異なる発展の歴史など，まさにともに学ぶことができた次第である．本書を手に取っていただいた皆様とも，このワクワク感を共有したい．

本書は，機能安全に関する規格を解説するものではなく，基本的な考え方を知っていただくためのものである．事例として自動車および鉄道分野を取り上げているが，生活支援ロボット，ドローンなど，一般の人々の生活に深く関わる機械・システムは今後多様さを増していくと考えられる．本書のターゲットは，むしろこうした分野なのである．

信頼性技術叢書編集委員会の益田昭彦先生，鈴木和幸先生，二川清先生には，本書を企画する機会を与えていただいたばかりではなく，企画立案から原稿の細部にわたる検討において多くの貴重な意見を賜りました．お礼の言葉が最後になってしまいましたが，この場をお借りして厚く御礼を申し上げます．ありがとうございました．

おわりに、本書の執筆において，さまざまな示唆・助言をいただいた日科技連出版社の鈴木兄宏氏，石田新氏に心からの御礼を申し上げます．

2022 年 7 月

著者を代表して

伊　藤　　誠

目　　次

コラム

第1章

機能安全を学ぶにあたって

安全に関する研究・開発を行っている人にとっても，機能安全は難しく，近寄りがたい印象をもたれることがある．固有技術の技術者であれば，なおさらであろう．

この印象を払拭するために，第 1 章では，本書で機能安全について学ぶための準備として，まず安全に関わる事項についておおよそのイメージをつかむことをねらう．各用語の厳密な定義や説明については，第 2 章以降で与える．

1.6

機能安全の位置づけ

そもそも，本書のように「機能安全」をことさらに取り上げ，議論しなければいけないのはなぜだろうか．その理由は，機能安全は安全確保のための一つの考え方に過ぎないということにある．機能安全は有用な考え方であるのは間違いないが，それだけで安全確保のために十分だというわけではない．

安全を実現するための考え方としてよく行われる分類に，本質安全と機能安全の区別がある．本節では，これらを対比させて説明してみよう．

1.6.1　本質安全とは？

製品・サービスに不安全さが内包されているとすると，そこで安全を確保するためには当事者たる人間が対応することが重要な役割を担う．しかし，「誤るは人の常」(To err is human.)といわれるように，人の手で安全を確保するのは限界がある．そこで，安全の確保は人の行動に頼るのではなく，本質的，原理的に安全が確保されるような仕組み，設計にしておくべきであると考えられるようになった．そのための考え方が，本質安全である．

道路交通を例にとり，交差点の出会い頭事故を考えてみよう．縦・横に交わる 2 つの道路を立体交差にすれば，そもそも出会い頭に 2 台の車両が衝突するという可能性を除去できる．こうすれば，本質的に，安全が確保できるであろうということである(**第 2 章**参照)．

このように，可能な限り本質安全を図ることが基本的に重要と考えられている．

1.6.2　本質安全と機能安全

本質安全は，安全確保のためには有用であるが，現実には，本質安全ですべての問題が解決するわけではない．交差点の例でいえば，立体交差で本質安全化できるとはいっても，すべての交差点でそれを実施できるわけでもない．

システムに，安全を確保するための機能を加え，この機能によって安全を実現するのが機能安全(functional safety)の基本的な考え方である．交差点の例でいえば，立体交差を作り込む代わりに，信号という車両の流れをコントロールする機能をシステムの中に加え、この機能により安全を図ることが，機能による安全といえる．

なお，「本質安全でカバーしきれないものを仕方なく機能安全で補う」というわけではない点に留意をされたい．情報技術に立脚することによって，従来では思いもよらないほどの高度なシステムの運用ができるようになるという意味で，機能安全は積極的な価値を有するのである．

例えば，自動車の運転でいえば，単に事故を起こさないようにすることだけを考えるならば，歩車分離を徹底し，交通参加者同士が接触の機会をもたないようにすればよい．しかし，このような考え方の下で作られた交通社会は，街を分断し，人の流れを阻害する，不便さを伴うものである．こうしたことへのアンチテーゼとして，歩行者と自動車とが対等な立場で移動する場としてshared space という考え方も生まれている[9]．今のところ，shared space は，そこにいる交通参加者(歩行者，ドライバ)がそれぞれに注意をすることによって結果的に不安全になる可能性が高まらないことをねらっている．しかし，これでは結果的にたまたま事故が増えないということが起きるとしても，安全であることを「保証」するものとはならない．これに対し，shared space に参加する自動車が状況を監視し，制御することによって事故を回避する仕組み，すなわち機能安全を取り入れ，この機能によりリスクが十分低いと判断できれば，今までにない新しい道路交通が実現することになる．

なお，安全を確保するための考え方としては，本質安全・機能安全の区別にとどまらず，より詳細な分類もありうる．詳しくは，佐藤[10]などを参照されたい．

第2章

機能安全と背景

機能安全とは，監視装置や防護装置などの付加機能により許容可能なまでにリスクを低減する方策であり，安全を実現，確保する安全方策の一つである．ここで「機能」とは「動作上，性能上」という意味で，「機能安全」とは，「動作，性能上で実現された安全」を意味し，システムを構成する個々のサブシステムのみの安全性にはこだわらず，対象とするシステム全体としての安全を対象とするアプローチである．機能安全規格 IEC 61508 は電気，電子，コンピュータ制御で構成されているものを対象にしているため，従来の機械安全の範囲にとどまらず，さらに高機能，高性能でインテリジェントな制御システムを実現できる可能性を秘めている．

本章では，まず機能安全そのものについて述べた後に，機能安全を取り巻く考え方として，用語の説明，標準化団体，規格体系，機能安全規格の概要，そして将来展望について述べる．

第3章

自動車の機能安全

自動車は，運転手の操作に基づいて「走る」，「曲がる」，「止まる」を実現する制御システムである．自動車は利用者の移動時間を短縮できる利便性を提供する一方で，車両同士や障害物，歩行者への衝突事故などの安全性の懸念がある．そのため，利便性と安全性とコストのバランスを重視する製品特性を要しており，低コストで機能安全を達成するための技術が重要視される．

本章では自動車の機能安全を紹介する．3.1 節ではこの製品特性に基づいて発展した自動車の機能安全の特徴と，IEC 61508[1] の分野規格として自動車向けに策定された機能安全規格 ISO 26262 “Functional Safety” [2] を中心に解説する．3.2 節では，自動車分野向けのリスク水準である Automotive Safety Integrity Level(ASIL) によるリスクの評価手法について事例を用いて解説する．

第4章

鉄道の機能安全

列車運転の安全を保証する鉄道信号システムにおいては，列車を停止させることが多くの場合に安全であることから，装置の故障を含め異常が生じたときには列車を停止させることを原則として，フェールセーフ設計による安全性技術を確立してきた．

高度な機能を有する鉄道信号システムの実現のためにマイクロコンピュータ適用の研究開発が行われたが，特定の故障モードを有しないマイクロコンピュータ，各種電子デバイスで構成されるシステムにおいてフェールセーフ性をどのように実現し SIL 4 相当の安全性を確保するかが最大の課題であった．

本章では，鉄道の機能安全として，4.1 節でこのような鉄道信号システムの安全性技術の特徴と IEC 61508 における機能安全との違いを中心に述べ，4.2 節で機能安全によって実現された高機能な鉄道信号システムの事例を紹介する．

監修者紹介

益田昭彦(ますだ　あきひこ)

1940年川崎市生まれ．電気通信大学大学院博士課程 修了．工学博士．

日本電気㈱にて通信装置の生産技術，品質管理，信頼性技術に従事(本社主席技師長)．帝京科学大学教授，同大学大学院主任教授，日本信頼性学会副会長，IEC TC 56信頼性国内専門委員会委員長などを歴任．

現在，信頼性七つ道具(R7)実践工房 代表，技術コンサルタント．

主な著書に，『品質保証のための信頼性入門』(共著，日科技連出版社，2002年)，『新FMEA技法』(共著，日科技連出版社，2012年)がある．

工業標準化経済産業大臣表彰，日本品質管理学会品質技術賞，日本信頼性学会奨励賞，IEEE Reliability Japan Chapter Award(2007年信頼性技術功績賞)．

鈴木和幸(すずき　かずゆき)

1950年渋谷区生まれ．東京工業大学大学院博士課程 修了．工学博士．

電気通信大学 名誉教授，同大学大学院情報理工学研究科 特任教授．

主な著書に，『信頼性・安全性の確保と未然防止』(日本規格協会，2013年)，『未然防止の原理とそのシステム』(日科技連出版社，2004年)，『品質保証のための信頼性入門』(共著，日科技連出版社，2002年)がある．

Wilcoxon Award(米国品質学会，米国統計学会,1999年)，デミング賞本賞(2014年)．

二川　清(にかわ　きよし)

1949年大阪市生まれ．大阪大学基礎工学部物性物理工学科卒業，同大学院修士課程修了．工学博士．

NEC，NECエレクトロニクス，大阪大学などで信頼性の実務と研究開発に従事．

現在，デバイス評価技術研究所 代表．

主な著書に『半導体デバイスの不良・故障解析技術』(編著，日科技連出版社，2019年)，『はじめてのデバイス評価技術 第2版』(森北出版，2012年)，『新版 LSI故障解析技術』(日科技連出版社，2011年)がある．

信頼性技術功労賞(IEEE信頼性部門日本支部)，論文賞(レーザ学会)などを受賞．

編著者紹介

伊 藤　誠(いとう　まこと)　全体編集，第 1 章執筆担当

1970 年生まれ．筑波大学第三学群情報学類卒業．博士(工学)．

現在，筑波大学システム情報系教授．

主な著書に，『安全・品質問題と信頼』(日科技連出版社，2016 年)，『交通事故低減のための自動車の追突防止支援技術』(共編著，コロナ社，2015 年)がある．

IEEE SMC Society A. P. Sage Best Transaction Paper Award，日経品質管理文献賞，計測自動制御学会論文賞(友田賞)，ヒューマンインタフェース学会論文賞などを受賞．

金 川 信 康(かねかわ　のぶやす)　全体編集，第 2 章執筆担当

1962 年生まれ．東京工業大学大学院理工学研究科修士課程(制御工学専攻)修了．博士(工学)．

1987 年，㈱日立製作所　日立研究所入所．現在，研究開発グループ　制御・ロボティクスイノベーションセンタ　シニア社員．1991 ～ 1992 年 UCLA Computer Science 学科 Visiting Scholar．主として宇宙用，産業用各種フォールトトレラントシステムの研究開発に従事．

電子情報通信学会ディペンダブルコンピューティング(DC)研究専門委員長(2014 ～ 2016 年)，同フェロー(2018 年)，日本信頼性学会会長(2016 ～ 2018 年)．IFIP(情報処理国際連合) TC.10(Computer Systems Technology)，WG.10.4(Dependable Computing and Fault Tolerance)各メンバー．情報処理学会 IFIP 日本代表委員．IEC TC 65 SC 65A/MT 61508(機能安全規格)，SC 65A/WG 17(ヒューマンファクターと機能安全)，WG 20(Framework to bridge the requirements for safety and security)，各国際エキスパート．IEEE Senior Member．

主な著書に，『信頼性ハンドブック』(共著，日科技連出版社)，『新版 信頼性ハンドブック』(共著，日科技連出版社)，*Dependability in Electronic Systems*(共著，Springer，2014)などがある．

著者紹介

石 郷 岡 祐(いしごうおか　たすく)　3.1 節執筆担当

1983 年生まれ．武蔵工業大学大学院修士課程修了．名古屋大学大学院博士後期課程修了．博士(情報学)．

2008 年，㈱日立製作所 日立研究所入社．2013 年日立ヨーロッパ出向，2015 年帰任．現在，日立 Astemo ㈱(出向)．

エンジン，ブレーキ，インバータ，車載ゲートウェイ，AD/ADAS ECU に関する機能安全，AUTOSAR，マルチコア対応ソフトウェア開発技術の研究開発に従事．ダルムシュタット工科大学，ブラウンシュヴァイク工科大学，フラウンホーファー，東京大学ほか，多くの共同研究経験をもつ．自動車機能安全カンファレンス 2021 基調講演を担当．IEEE，情報処理学会会員．情報処理学会組込みシステム研究会運営委員．

金 子 貴 信(かねこ　たかのぶ)　3.2 節執筆担当

1958 年生まれ．慶應義塾大学工学部計測工学科卒業．

自動車メーカ，サプライヤなどで，車両のセンシング技術，シャシー制御，通信を用いたプローブカーや ITS 標準化などの研究に従事．

2008 年 2 月，(一財)日本自動車研究所入所，ISO 26262 機能安全規格の解釈や ASIL 評価のための判断材料に関わる研究に従事．現在，機能安全グループシニアエキスパート．

川 野　　卓(かわの　たかし)　4.2 節執筆担当

1968 年生まれ．東京理科大学理工学部卒業．長岡技術科学大学大学院工学研究科博士課程修了．博士(工学)．

1991 年 4 月，東日本旅客鉄道㈱入社，㈶鉄道総合研究所(出向)にてデジタル方式の ATC(自動列車制御装置)の研究，その後同社にて山手線・京浜東北線 D-ATC (Digital-ATC)システム開発・導入に従事．現在，国際事業本部 標準化戦略・推進部門長．

主な著書に『信号システムの進歩と発展』(共著，日本鉄道電気技術協会，2009 年)，『新版 信頼性ハンドブック』(共著，日科技連出版社，2014 年)，『はじめての STAMP/STPA』(共著，情報処理推進機構，2016 年)がある．

信頼性学会理事，電気学会会員，英国IRSE(Institution of Railway Signal Engineers) フェロー．

平 尾 裕 司(ひらお　ゆうじ)　4.1 節執筆担当

1953 年生まれ．函館工業高等専門学校電気工学科卒業．博士(工学)東京大学．

鉄道総合技術研究所で列車制御システムの研究開発に従事，長岡技術科学大学技術経営研究科長，システム安全専攻長・教授．

現在，長岡技術科学大学名誉教授，IRSE(Institution of Railway Signal Engineers) Vice President．

福 田 和 良(ふくだ　かずよし)　3.2 節執筆担当

1967 年生まれ．東京電機大学工学部応用理化学科卒業．

電機メーカ，半導体メーカで，液晶ディスプレイ向 IC，携帯電話向 LSI，自動車向 LSI などの開発や ISO 26262 機能安全規格対応組織構築に従事．

2013 年 11 月(一財)日本自動車研究所入所，ISO 26262 共同研究で機能安全規格の解釈や実運用課題の研究に従事．現在，機能安全グループ主席研究員．

■信頼性技術叢書
機能安全の基礎と応用
―自動車・鉄道分野を通して学ぶ―

2022 年 8 月 30 日　第 1 刷発行

監修者　信頼性技術叢書編集委員会
編著者　伊藤　誠　金川信康
著　者　石郷岡祐　金子貴信　川野　卓
　　平尾裕司　福田和良
発行人　戸羽節文
発行所　株式会社日科技連出版社
　〒 151-0051 東京都渋谷区千駄ヶ谷 5-15-5
　DS ビル
　電話　出版 03-5379-1244
　　営業 03-5379-1238
　URL　https://www.juse-p.co.jp/

印刷・製本　河北印刷株式会社

ISBN978-4-8171-9764-1