❹ 社会インフラストラクチャを支える制御システムにおけるセーフティとセキュリティ

金川信康　山田　勉（(株) 日立製作所）

制御システムの特徴

制御システムは，工場の自動化や機器の制御に用いられ，電力・鉄鋼・交通・上下水などの社会インフラ構築のための中核の役目を果たしている．これらの分野は特に，リアルタイム性，信頼性，拡張性が要求される分野で，自律分散，FTC（Fault-Tolerant Computer）などの特徴ある技術を生み出してきた．

一方，ネットワークに目を向けると，旧来はリアルタイム制約へ対処するため独自構成の計算機やネットワークが用いられてきた．しかしながら，近年では生産性・付加価値向上に向けて，オープン技術の導入が制御システムにおいても活発化している．OS やネットワークプロトコル等のオープン技術導入が進むのと並行して，IT 分野におけるセキュリティ脅威も制御システムにおいて現実のものとなった．さらに制御システムの影響力に着目した悪意ある組織・個人により，制御システムに対して脆弱性をつく攻撃が顕在化した．イランの核燃料プラントに対するマルウェア Stuxnet の攻撃によるプラント破壊や，ウクライナの電力系統システムに対するマルウェア BlackEnergy による大規模停電の発生などが例である．

以下，制御システムにおけるセーフティ，セキュリティについて述べ，最後に近年の規格化動向を踏まえてセーフティとセキュリティの両立について述べて本稿を閉じる．

制御システムにおけるセーフティ

インターロック，フェールセーフ

システムを異常時には緊急停止させ，起動条件が満たさないと起動させない「インターロック」が安全性を担保する手段として制御分野では古くから用いられている．近年になり，「インターロック」の電子化が進み，2000 年に機能安全規格 IEC 61508 が制定されている．なお同規格中，「安全関連系（safety related system）」とはこの「インターロック」のことである．

機能安全規格制定を受けてこれに準拠する（基本構成で SIL（Safety Integrity Level）2 まで対応可能な）機能安全コントローラ HISEC R800FS，さらには可用性・保守性と性能を向上させた R800FS バージョン 2 が開発されている．

鉄道保安システムでは自動列車制御装置（ATC：Automatic Train Controller）（図 -1）などが実用化されている．地上の保安システムは，それぞれの列車の位置関係に基づいて制限速度指令を車上の ATC に供給する．当初の ATC の機能自体は指定された制限速度を超えればブレーキ指令を出力させる単純なものであった．ATC は安全運行の決め手になるために高い安全性が要求され，特に装置が故障した際に確実にブレーキ指令を出すフェールセーフ性が重要で，鉄道の分野では長年にわたってこのための技術が蓄積されてきた．ATC の機能は早い時期から ATC-LSI（Large-Scale Integrated Circuit）として集積化され，小型化と信頼性向上（故障率削減）を実現している．

機能的には ATC-LSI では，現在速度が制限速度

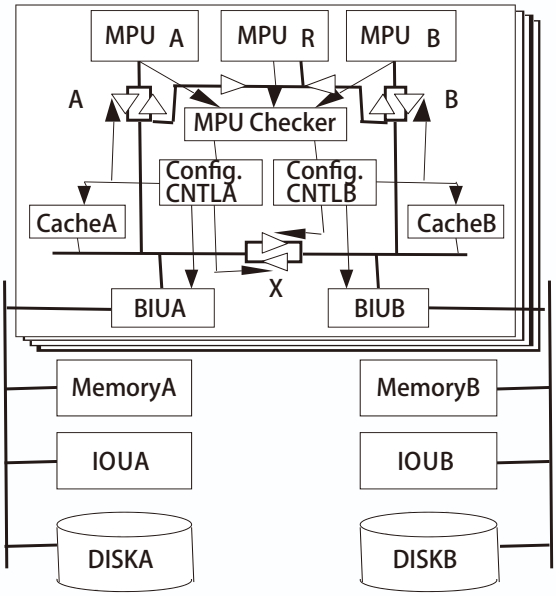


図 -1　TPR（Triple Processor check Redundancy）アーキテクチャ

を超えた場合にブレーキ指令を出力すれば良いが，フェールセーフのために次のような工夫がされている．現在速度と制限速度を周波数に比例した信号で表現して，両者の周波数を比較し，車速が制限速度を超え「ていない」場合に「ブレーキをかけなくともよい」ことを意味する交番信号（Brake）を出力する．交番信号（一種のシグナチャ信号）に「ブレーキをかけなくともよい」という意味を持たせてるのは，故障時には交番信号を生成できなくなる確率が高いという性質（非対称故障特性）を考慮して，故障時に即ブレーキを動作させてフェールセーフ性を実現するためである．周波数を比較する論理はフェールセーフな周波数論理により実現しており，さらに 2 重化している．

近年では，ATC-LSI で培った技術を元にチップ内冗長化によるセルフチェッキングプロセッサ[1]に進化し，ATC の安全性を保ったまま柔軟性を高めた進化形であるディジタル ATC にも用いられている．

高信頼（高可用性）システム

制御システムでは高可用性（High Availability，故障による機能停止の確率が低いこと）のために，独立した複数のコンピュータから構成されるマルチコンピュータアーキテクチャが広く採用されている．

一瞬たりともサービス停止が許されない電力・鉄道などの分野を中心に，システムの 24 時間無停止連続運転やオンライン拡張が求められるようになってきた．無停止連続運転やオンライン拡張をサポートするフォールトトレラント機は日立では 3 つのプロセッサと比較器を組み合わせた TPR（Triple Processor check Redundancy）アーキテクチャ[2]に始まる．本アーキテクチャでは図 -1 に示すようにバス，主記憶装置，周辺回路をすべて 2 重化して，いかなる単一故障が発生しても動作を継続可能としている．

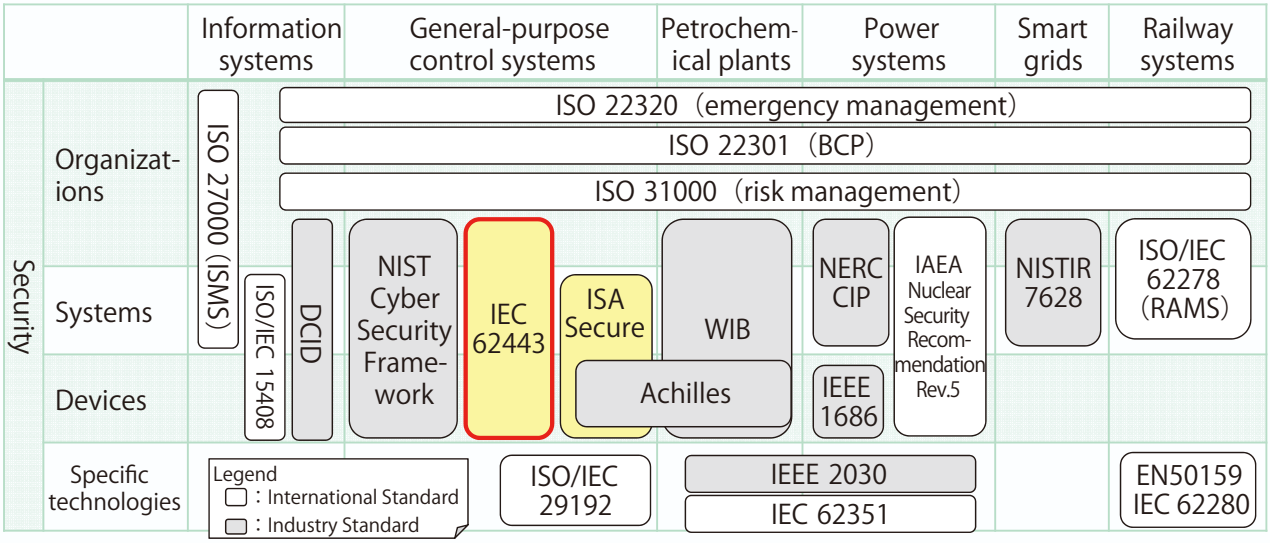
本技術は鉄道の電力管理や運行管理，高速道路の遠隔制御システムに適用され運用実績において高い信頼性を示した．その後，保守時のモジュール交換の容易性から密結合（クロックレベルで同期）四重化方式を経て，現在，高速クロック動作に適した疎結合（タスクレベルで同期）四重化方式の CF-1000/FT に至っている．

なお近年では信頼性だけでなく，可用性，ロバスト性などを含むディペンダビリティというより広い概念が提案され[3]広く用いられている．

制御システムにおけるセキュリティ

制御システムセキュリティの状況

制御システムにおけるセキュリティ対策は不可避である．一方，制御システムは IT システムとは異なり，計算機資源をリアルタイム制御へ最優先に割り当てるため，セキュリティ機能へ割り当てる余地が少ない．また業務上停止させることが困難なため，稼働中にパッチを当ててリブートができないケースが多い．すなわち，IT システムにおけるセキュリティ対策とは違う観点で，制御システムに適したセキュリティ対策が必要である．これまで，制御システムの特性に応じたガイドラインや標準規格が多数開発されている（図 -2）[4]．



CIP : Critical Infrastructure Protection, DCID : Director of Central Intelligence Directive,
RAMS : Reliability, Availability, Maintainability and Safety, WIB : International Instrument Users'Association,
NISTIR : National Institute of Standards and Technology Interagency Report, NERC : North American Electric Reliability Corporation
※AchillesはGEの登録商標，ISASecureはASCIの登録商標である．

図 -2　国際規格の関連

セキュリティ対応の手順

制御システムで優先して保護する対象は事業であり，事業継続をするためには HSE（Health, Safety and Environment）の維持，すなわち事業が健康・安全・環境へ悪影響を及ぼさないことが重要である．

セキュリティ実装の手順は，産業制御システムのセキュリティ規格である IEC 62443 に基づけば，制御システムを所有する事業者（アセットオーナ）の経営者のコミットメントから始まり，体制，対応すべき事業リスクの優先度を抽出する．リスク対策が必要な脅威に対して，詳細なリスク分析と対応策を設計する．また，セキュリティ対応は単発的な対応ではなくプロセスである．そこで，継続的な対応をするための体制を整備する．以上を繰り返すことにより，新たな脅威への対応が可能となる．

セキュリティ対応の参考文書

セキュリティ対策の手順として，IEC 62443 シリーズが参考になる．IEC 62443 シリーズは 13 分冊からなり，2017 年 7 月現在 6 分冊が発行済みである．たとえば，前節の手順は IEC 62443-2-1 と IEC 62443-3-2（ドラフト）による．

また，IEC 62443 以外に，特に重要インフラ向けに政府機関が整備するガイドラインや，規制が各国において存在する．日本におけるガイドラインとして，電力制御システムセキュリティや，サイバーセキュリティ経営に関するものが存在する．他に有力なガイドラインとして，米国 NIST が定めるサイバーセキュリティフレームワークが多くの事業分野で利活用可能であり有用である．また，北米電力事業者が従うべき規格として NERC CIP がある．これは違反すると罰則を伴う強制規則である．

ビジネス分野では，独政府が推進する Industrie 4.0 に関する活動が活発化している．Industrie 4.0 に適するセキュリティのコンセプトはすでに公表されており，今後の製造システムの動向に影響することが予想される．また，制御システムのリリースから保守，廃棄までを管理する Industrial Internet Consortium（IIC）の活動も活発化している．IIC は陽に規格化を進めてはいないが，推奨するセキュリティ対策をユースケースに即してガイドラインで示している．

今後の展開

制御システムにおける動向として，IoT 技術を活用したシステムが注目されている．IoT システムは

制御システムと比較して迅速な導入と成果の導出が求められるが，一方でセキュリティ対策の不備による事故事例も報告されてきている[5]．制御システムの現場とデータの入出力をするIoT装置は，制御システムの装置と類似しており，セキュリティ対策も類似の対策が必要である．すなわち，制御システムにおけるセキュリティ対策をIoTまで拡張する観点が必要になると考える．

セーフティとセキュリティの両立

本特集のほかの記事ですでに述べられているように，セーフティとセキュリティの両立のための規格化が進められている．筆者も規格委員会に参加して，両方の分野の専門家の間ではアプローチどころか用語もまったく異なり，まるでバベルの塔を建設するかのようなチャレンジングなプロジェクトであると実感している．創世記の中では果たせなかったバベルの塔実現に向けて，セーフティ専門家の立場から，本稿で触れたセーフティとセキュリティの両立のために有望なアプローチについて以下に記す．

デザインダイバーシティ

元来，高信頼化のためにデザインダイバーシティ（設計の多様化）という概念が提案されてきていた．機器を冗長化しても共通のデザインフォールト（設計上の誤り）があるとすべての機器が影響を受けてしまうので，デザインに多様性を持たせることにより，デザインフォールトの影響を回避しようとする概念である．デザインに多様性を持たせることにより同様に冗長化した機器間に共通の脆弱性を防止して，サイバー攻撃に対する脆弱性の影響を回避できる可能性がある．この概念の代表的なものとしてN-バージョンプログラミングという手法が広く知られている．

Intrusion Tolerance Project

以上述べたような背景のもと，欧州を中心にIntrusion Tolerance Projectが進められている[6]．Intrusion-toleranceとは，フォルトトレランスをIntrusionすなわちサイバー攻撃による侵入に広げた概念で，サイバー攻撃による侵入を完全にシャットアウトしようとするのではなく，あらかじめ機能のダイバーシティを持ったレプリカを用意しておいてその影響を防止するアプローチである．このアプローチはセーフティとセキュリティの両立を実現できる可能性を秘めている．

参考文献

1) Kanekawa, N., et al. : Self-checking and Fail-safe LSIs by Intra-chip Redundancy FTCS-26, pp.426-430 (1996).
2) 金川信康 他：基板内フォールトマスキング方式によるフォールトトレラントコンピュータの高速化と透過性，電気学会論文誌，114-D, 9, pp.903-909 (1994).
3) Laprie, J. C. : Dependable Computing and Fault Tolerance : Concepts and Terminology, FTCS-15, pp.2-11 (1985).
4) 山田 他：安心な社会インフラシステムに向けたセキュリティ標準規格の動向と展開，日立評論，Vol.96, No.3, pp.219-222 (2014).
5) Trend Micro :「IoT」でも「セキュリティ」：明確にIoT機器を狙い始めたLinuxマルウェア，https://www.trendmicro.com/jp/iot-security/special/10063
6) Neves, N., Sousa, P. : Information Assurance, Security and Privacy Services (Handbooks in Information Systems, volume 4), Emerald Group Publishing Limited, pp.805 615-678 (2009), ISBN:9781848551947 - pdf, http://www.navigators.di.fc.ul.pt/wiki/Publication:Verissimo09his

(2017年7月26日受付)

金川信康（正会員） ■ Nobuyasu.kanekawa.ef@hitachi.com

1987年東京工業大学大学院理工学研究科修了．同年（株）日立製作所に入社．以来高信頼システムの研究開発に従事．博士（工学）．IEEE，電子情報通信学会，電気学会会員．日本信頼性学会会長．IFIP TC 10, WG 10.4メンバ．

山田　勉 ■ tsutomu.yamada.bs@hitachi.com

1994年京都大学大学院工学研究科修了．同年（株）日立製作所に入社．以来制御システムのアーキテクチャ，セキュリティの研究開発に従事．技術士（総合技術監理部門，情報工学部門）．IEEE，計測自動制御学会会員．