

ICT を用いたシステムの安全性に関する最近の動向

小林 洋^{*1}

Recent Trends in System Safety Using ICT

by

Hiromi KOBAYASHI^{*1}

(received on Aug.28, 2019 & accepted on Nov.15, 2019)

あらまし

本稿では、情報通信技術 (Information Communication Technology: ICT) を用いたシステムの安全性に関する規格と解析／評価手法についての最近の動向を述べる。

Abstract

This paper presents the recent trends of standards and analysis/assessment methods in system safety using ICT.

キーワード: 安全性, 自動運転, STAMP/STPA, SafetyII, レジリエンス

Keywords: Safety, Automated Driving, STAMP/STPA, SafetyII, Resilience

1. はじめに

近年, ICT はあらゆる産業分野で用いられているが, ICT を用いた製品やシステムは, 技術の進歩が著しい上に次第に大規模複雑化すると共にネットワークで結ばれる傾向にあるために, それらに適合した安全性 (safety) に関わる規格や解析／評価手法が求められている. 本稿では, まず, 安全性の概念にも関わる用語の定義について示した後で, 機能安全 (functional safety) と自動車関連の規格の最近の動向について述べる. 次に, 最近, 産業界で注目されるようになってきた解析手法である STAMP/STPA (systems theoretic accident model and processes/ system-theoretic process analysis) および安全性の新しい概念である SafetyII やレジリエンスとその解析／評価手法について述べる.

2. 安全性の規格について

ICT 関連の製品やシステムの安全性の用語の定義や機能の規格については, 国際的には ISO や IEC (International Electrotechnical Commission: 国際電気標準会議) により制定されており, WTO (World Trade Organization) の TBT (Technical Barriers to Trade) 協定に基づき, 製品やシステムの輸出入における技術的障壁を取り除く必要性から, 国際規格と整合性のある国内規格が JIS で制定されている. ICT の進歩は著しいため, 次々と新しい規格が作られると共に, 数年から 10 年程度で改定が行われる. 以下に, 安全の概念, 機能安全, および自動運転技術にも関わりのある自動車関連の規格についての最近の動向を

述べる.

2.1 安全の概念

ICT 関連の安全⁺¹に関する用語の定義としては, まず, ガイドラインとして国際規格 ISO/IEC Guide51(国内対応規格 JIS Z 8051) が作られている¹⁾. この規格において安全の概念はリスク (risk) を用いて定義されており, ISO/IEC Guide51:2014 での Safety の定義は「freedom from risk which is not tolerable.」, 対応する JIS Z8051:2015 での安全の定義は, 「許容不可能なリスクがないこと」となっており⁺², リスクがゼロの絶対安全は理想だが現実的に不可能であるという考え方である. リスクは「危害の発生確率及びその危害の度合いの組合せ」と定義され, 許容可能なリスクは社会の価値観等によって決定される旨も記されるようになった. 一方, 信頼性に関する用語の国際規格としては IEC60050 (192) があり, この 2015 年の第 1 版と 2016 年の追補 (Amendment) 1 を基にした JIS Z8115:2019 には, 日本工業規格として安全という用語が追加されているのだが, その定義は「許容できないリスクから免れている状態」と, 前述のガイドラインとの整合性が図られている. なお, この規格で広義の信頼性, 即ち, ディペンダビリティについては, 用語として「総合信頼性」がディペンダビリティに併記されるようになり, 定義については「アイテム⁺³が, 要求されたときに, その要求どおりに遂行するための能力」となっている²⁾.

+1 安全性と信頼性は見方が異なる. 例えば, 事故の可能性が僅かでもあれば停車する列車は, 安全性は高いが, 要求機能遂行の信頼性は低いということになる.

+2 以前の規格では unacceptable (受容出来ない) だったのが, not tolerable (許容できない) に変更された.

+3 アイテムとは対象となるもの. 個別の部品, 構成品, システム等で, ハードウェア, ソフトウェア, 人間から構成され, サービスを対象とする場合もある.

^{*1} 情報通信学部情報メディア学科 教授
School of Information and Telecommunication
Engineering, Department of Information Media
Technology, Professor

2.2 機能安全

ICT 関連の製品やシステムでは、機能安全 (functional safety) についての規格が定められている³⁾。まず、電気・電子・プログラマブル電子安全関連系の機能安全についての IEC61508:2010 (対応規格 JIS C0508:2012) があり、これは製品やシステムによらない共通の基本安全規格となっている。この規格では、ソフトウェアを含むシステムの安全性を扱うために、故障をランダムハードウェア故障と系統的故障 (systematic failure) (JIS C0508 の用語では、決定論的原因故障) に分類している。前者は、ハードウェア部品の劣化による故障について故障確率を基に、後者は、全安全ライフサイクルのプロセスに関する要求事項を基に対処するものとしている。この基本安全規格を基に、分野別にプロセス産業関連の IEC61511、原子力関連の IEC61513、機械類関連の IEC62061、鉄道関連の IEC62278、自動車関連の ISO26262 等が制定されている。なお、機能安全規格は、現在、人の安全機能に対する具体的な要求事項も考慮できるように改定が試みられている³⁾。

2.3 自動車関連の規格

近年、車載電気電子システムや自動運転関連の技術の発達に伴い、自動車関連の安全性の規格の制定が急速に進んでいる⁴⁻⁵⁾。前述の自動車関連の機能安全規格 ISO26262:2018 は、車載電気電子システムを対象とした規格で、2012 年の第 1 版制定の際にはセーフティケース (safety case) と呼ばれるシステムが安全に作られていることを示す証拠 (論拠) の作成が義務付けられていることが、産業界で話題となった。

ところで、ISO26262 では、機能安全の考え方を基にしているため、システム故障がなければ安全という考え方で、ランダムハードウェア故障と系統的故障のみを扱っている。しかし、自動運転技術への対応の必要性もあり、システム故障以外の、他のドライバの運転や天候、更には性能限界や誤使用等により引き起こされる安全上のリスクについても、早急に規格として制定する必要が生じたため ISO/PAS 21448: 2019 SOTIF (Safety of the Intended Functionality) が制定された。また、自動運転技術では、ネットワークへ常時接続したコネクティッドカー (connected car) での運用のために、ISO と SAE (Society of Automotive Engineers: 米国自動車技術者協会) と合同でサイバーセキュリティ対策のための ISO/SAE 21434 の制定が進められている。ネットワークで接続されたシステムでは、セキュリティの脆弱性への攻撃により安全性が損なわれる事があるために、安全性とセキュリティは統合して扱う必要が生じているためと考えられる。

3. 解析／評価手法

安全性や信頼性の解析手法として、現在産業界で普及しているものとしては、FMEA (Failure Modes and Effects Analysis: 故障モード・影響解析)、FTA (Fault Tree Analysis: 故障の木解析)、ETA (Event Tree

Analysis: 事象の木解析)、および HAZOP (Hazard and Operability Study) 等が上げられ、評価手法としては PRA (Probabilistic Risk Assessment: 確率的リスク評価) 等が上げられる⁶⁻⁷⁾。これらの手法は、1950～60 年代に開発されたものであるが、未だに産業界では良く使われている。しかし、近年、システムが大規模複雑化しネットワークで結ばれ、また、ソフトウェア化が進み、構成品や部品等のシステムの構成要素間の相互作用が複雑になってきたことから、これらに対応するための新しい手法の必要性が高まっている。

以下に、まず、最近産業界で注目されるようになってきた解析手法である STAMP/STPA について述べ、次に、安全性の新しい考え方である SafetyII とレジリエンスおよびその解析と評価に用いられる FRAM (Functional Resonance Analysis Method: 機能共鳴分析) と RAG (Resilience Assessment Grid: レジリエンス分析評価グリッド) について述べる。

3.1 STAMP/STPA

STAMP/STPA⁷⁻¹⁴⁾ は、航空機産業等で安全性の研究を行ってきた N. G. Leveson により開発されたモデルと解析手法である。STAMP は、システムを安全のための制御を行う要素のコントローラと制御される要素の被コントロールプロセスによってモデル化したもので、システムをコントローラから被コントロールプロセスへのコントロールアクションと逆方法のフィードバックデータの相互作用によるリアクティブシステム (reactive system) として捉えている。

STPA は、STAMP モデルを用いた安全性解析手法で、コントロールアクションとフィードバックの不適切なタイミングに起因するアクシデント (accident)

(または、損失 (loss)) を、次のような手続きで解析する⁷⁻¹³⁾。

(準備) アクシデント (または、損失) を識別し、そのハザード (hazard: 危害の潜在的な源) と安全制約を導き出す。次に、安全制約の実現に関係するコンポーネント及びその相互作用からなる制御構造図を構築する。

(1) 非安全なコントロールアクション (unsafe control action: UCA) 識別を、制御構造図でのコントロールアクション毎に、次の 4 種類に分類したハザードを適用して行う。

① コントロールアクションが与えられないことによる (not providing) ハザード、② 与えられるとハザード (providing causes hazard)、③ 早すぎる／遅すぎる／誤順序でハザード (too early/too late/wrong order causes hazard)、④ 早すぎる停止／長すぎる適用によるハザード (stop too soon/applying too long causes hazard)。

(2) ハザード要因 (hazard causal factor: HCF) とそのシナリオの特定を、UCA 毎に制御構造図上に想定される不適切な動作をマッピングすることにより行う。

STAMP/STPA の実システムへの導入事例は、文献 7-8) 等に示されている。

3.2 SafetyII と解析／評価手法

SafetyII¹⁵⁻²³⁾ は認知システムや人間工学の分野等から安全性の研究を行ってきた E.Hollnagel により提唱された安全の考え方であり、2. で示した従来の安全 (SafetyI と彼らは呼ぶ) が、リスクが排除された状態として定義され、物事がうまくいかないことを防ぐことによって達成しようとするのに対して、SafetyII では物事がうまくいくことを確実にすることによって達成しようとしている。定量的には、SafetyI は受け入れられないアウトカムの数ができるだけ少ない状況、他方、SafetyII は受け入れられるアウトカムの数ができるだけ多い状況との説明がされている²⁰⁾。この考え方の背景としては、システムは多くの場合、人間の臨機応変性や協調性により安全の許容範囲内でうまく運用されているので、その状態が維持できるようにしようということであり、ヒューマンファクタを重視したアプローチである。SafetyII のもう一つの背景にあるのは、大規模システムでは、構成要素相互間の影響が複雑で事前に把握し難く、設計段階でシミュレーションに時間をかけても大きなトラブルは稀にしか起きないため異常時のデータは取得し難いということが挙げられる。稀にしか起きないようなトラブルの少量のデータを基にして安全対策を考えるという従来のアプローチよりも、正常なオペレーション、つまり安全の許容範囲内でのオペレーションでの大量の取得データを基に安全な状態を維持した方が良いのではないかという考え方である。

SafetyII とレジリエンス (resilience) の関係については、SafetyII は、システムのレジリエンス (resilience)、つまり弾力性、復元力、回復力に基づいた安全性の概念であると位置づけられており、レジリエンスを、システムが想定内および想定外のいずれの条件でも、要求通りの働きをするための調整を行う能力 (potential: ポテンシャル) という意味で用いている¹⁶⁻²³⁾。システムのレジリエンスのポテンシャルが高ければ、オペレーションでの変動が大きくても安全にオペレーションは遂行されることになる。レジリエンスの解析と評価の手法として提唱されているものに、FRAM と RAG がある。

FRAM は、システムを複数の機能 (活動) から構成されるものとして捉え、各機能は 6 種類の要素 (入力 (I)、出力 (O)、前提条件 (P)、資源 (R)、時間 (T)、制御 (C)) で外部と相互作用するコンポーネントとしてモデル化し、六角形に各要素のポートをつけた記号で表す。そして、関連する機能の要素間を線で結んだ図を用いて、機能共鳴 (functional resonance) と呼ばれる、人や組織の機能のパフォーマンスの調整作用により生まれる相互作用の解析を行う。

RAG は、組織のレジリエンス評価方法であり、診断的質問を用いて評価を行う。質問群には標準的なもの

が提案されており、それを分野に合わせて修正して用いる。質問群は、対処 (respond)、予見 (anticipate)、学習 (learn)、監視 (monitor) の 4 つのポテンシャル評価用に分かれており、各々 8~10 項目程度の質問項目を設定し、各項目について優秀 (excellent)、満足 (satisfactory)、受容可 (acceptable)、受容不可 (unacceptable)、欠落 (deficient)、考慮無し (missing) の 6 段階で評価を行い、スターチャート (別名、レーダーチャート) にまとめる。

FRAM や RAG の適用方法については、文献 16, 20) 等に示されている。

4. 議論

(1) 安全性のガイドラインにも書かれているように、許容可能なリスクの決定は社会の価値観にもよる。安全対策のためには、危害を評価しなければならない。そのためにはまず危害に対する価値判断をしなければならない。価値というのは、組織での立場によって異なる場合がある他、主観的で人によって異なる場合がある。特に、複数の人や資産が対象になる場合、価値判断に関する合意の形成をしなければならないことが、安全対策を考える上で難しい点である²⁴⁻²⁵⁾。このことから、自動運転の場合には、SAE レベル 4 の特定条件下における高度自動運転については空港や港湾の産業用等で実用化が進んでいるが、一番上のレベル 5 の完全自動運転は、安全対策で複数の人や資産の危害についてのトレードオフが必要となり、トレードオフの方針まで完全に規格化するのは極めて困難なことから、現実的ではないように思われる。

(2) STAMP/STPA を従来の FMEA や FTA と比較すると、従来手法では抽出できなかったハザード要因が STAMP/STPA で抽出できたというケースがある一方で、逆のケースもあるようで、両方を組み合わせて使うのが良いかもしれないとの提案もなされている¹²⁾。解析手法については、システムの形態によって適した手法があるように思われる。また、一種類の手法ではどうしても漏れが出てしまうので、一般的にはいくつかの手法を組み合わせて用いるのが良いということになるのであろう。

(3) SafetyII の評価手法として、レジリエンスの評価手法である RAG を用いる理由については、RAG においてレジリエンスのパフォーマンスに対するポテンシャルを評価することが、SafetyII での見方と一致しているためと述べられている。また、SafetyII の説明で示されている受け入れられるアウトカムを数えるよりも、RAG における 4 つのポテンシャルを評価する方が簡単であるとも記されている²⁰⁾。しかしながら、これらの説明は直観的で厳密性に欠けているように思われる。

(4) レジリエンスという言葉は様々な分野で使われるようになってきているが、ISO の社会セキュリティ関係 (危機管理等も含む) の専門委員会 (TC) ではレジリエンスに関する規格化が進められており、

ISO22300:2018 Security and Resilience-Vocabulary 等の一連の規格が次々と制定されている。レジリエンス関連の規格は、当面、社会セキュリティの分野が中心となり作成されていくのかもしれない。

5. おわりに

本稿では、まず、安全性に関する規格の最近の動向について述べた。技術の進歩の著しい ICT 関連の安全性に関する規格は、数年から 10 年程度で改定されると共に次々と新しい規格が作られていく。用語の定義、つまり概念も技術の進歩とともに変更が加えられたり、新しい規格で定義されたりする。機能安全規格についても、技術の進歩と適用領域の拡大に追従するように、遅滞なく改定や新規作成を行う努力がされている。次に、本稿では、最近注目され始めている安全性の解析／評価手法について示した。STAMP/STPA は、システムを制御系としてモデル化し、コントロールアクションとフィードバックデータの組み合わせを解析するところに特徴がある。解析手法はシステムの形態によって適した手法があるように思われ、一般的には、いくつかの手法を組み合わせで用いるのが良いのであろうが、導入には費用対効果を考慮する必要がある。SafetyII については、概念自体が新しいもので、本稿執筆の 2019 年 8 月末時点では、ICT 関連の安全規格に直接の影響は与えていないようなので、解析／評価手法として FRAM と RAG を紹介し、その基となる概念を示すという位置づけで記した。FRAM や RAG は、人間の臨機応変性や協調性による組織のレジリエンス性を解析／評価するものであり、今後、社会技術システムの安全性の解析や評価にどのように影響を与えていくかについて注目していきたい。

参考文献

規格自体については省略する。

- 1) 向殿政男監修, 安全の国際規格 1, 安全設計の基本概念, 2:機械安全, 3:制御システムの安全, 日本規格協会, 2007.
- 2) 益田昭彦, JIS Z 8115ディペンダビリティ (信頼性) 用語の現状と将来, IEICE Fundamentals Review, Vol. 9, No. 4, pp. 318-329, 2016.
- 3) 佐藤吉信, 機能安全の基礎, 日本規格協会, 2014.
- 4) ビジネスキューブ・アンド・パートナーズ, ISO26262 実践ガイドブック, 日経BP, 2013.
- 5) ビジネスキューブ・アンド・パートナーズ, ISO26262 について, https://biz3.co.jp/lp_category/iso26262
- 6) N.G. Leveson: Safeware-System Safety and Computers, Addison Wesley, 1995.
- 7) N.G. Leveson: Engineering a Safer World, MIT, 2011.
- 8) N.G. Leveson, J.P. Thomas, STPA HANDBOOK, 2018. <http://psas.scripts.mit.edu/home/materials/>
- 9) はじめてのSTAMP/STPA, IPA, 2016 <https://www.ipa.go.jp/ikc/reports/20190329.html>
- 10) はじめてのSTAMP/STPA (実践編), IPA, 2017 URL 同上
- 11) はじめてのSTAMP/STPA (活用編), IPA, 2018 URL 同上
- 12) 川野卓, 鉄道信号システムの安全性解析における STAMP/STPA の適用について, 日本信頼性学会誌, Vol. 41, No. 2, pp. 96-102, 2019.
- 13) 高田哲也, 浅野晃, 鉄道信号の安全性と安全性評価の動向, 日本信頼性学会誌, Vol. 41, No. 3, pp. 198-205, 2019.
- 14) 宮崎義弘, 橋本岳雄, 岡田学, 自動車運転システムへの STPA 試行事例, JASPER, www.ipa.go.jp/files/000070993.pdf, 2018.
- 15) E. Hollnagel, D.D. Woods, N. Leveson 編著, 北村正晴監訳, レジリエンスエンジニアリング: 概念と指針, 日科技連, 2012.
- 16) E. Hollnagel, J. Paries, D.D. Woods, J. Wreathall 編著, 実践レジリエンスエンジニアリング, 日科技連, 2014.
- 17) C.P. Nemeth, E. Hollnagel, レジリエンスエンジニアリング応用への指針, 日科技連, 2017.
- 18) エリック・ホルナゲル著, 小松原明哲監訳, 社会技術システムの安全分析: FRAMガイドブック, 海文堂, 2013.
- 19) エリック・ホルナゲル著, 北村正晴, 小松原明哲監訳, Safety-I & Safety-II: 安全マネジメントの過去と未来, 海文堂, 2015.
- 20) エリック・ホルナゲル著, 北村正晴, 小松原明哲監訳, Safety-IIの実践: レジリエンスポテンシャルを強化する, 海文堂, 2019.
- 21) 北村正晴, レジリエンスエンジニアリングが目指す安全Safety-IIとその実現法, IEICE Fundamentals Review, Vol. 8, No. 2, pp. 84-95, 2016.
- 22) エリック・ホルナゲル, 松本隆明, IoT時代に求められるレジリエンスエンジニアリングの考え方, SEC journal, Vol. 13, No. 1, pp. 2-7, 2017.
- 23) 野本秀樹, 道浦康貴, 石濱直樹, 片平真史, FRAM (機能共鳴分析手法) による成功学に基づく安全工学, SEC journal, Vol. 14, No. 1, pp. 42-49, 2018.
- 24) 小林洋, システムの安全性とは何に対する安全性なのか?, ソフトウェアシンポジウム2012(SS2012), ソフトウェア技術者協会, pp. 3.1-3.7, 2012.
- 25) 小林洋, 安全性についての課題一価値判断とAIの使用について, 東海大学紀要情報通信学部, Vol. 10, No. 1, pp. 114-116, 2017.