機能安全とその保証に関する理論的枠組

田口　研治

(独)産業技術総合研究所
組込みシステム技術連携研究体
招聘研究員

2010年4月～
(独)産業技術総合研究所　招聘研究員 (主にシステム検証、信頼性保証の研究に従事)

2005年4月～2010年3月まで
国立情報学研究所　特任教授(ソフトウェア工学教育、形式手法研究に従事)

1997年～2005年
Bradford 大、Uppsala大講師、九州大学助手

1985年~1997年
ソフトウェア開発、研究コンサルに従事

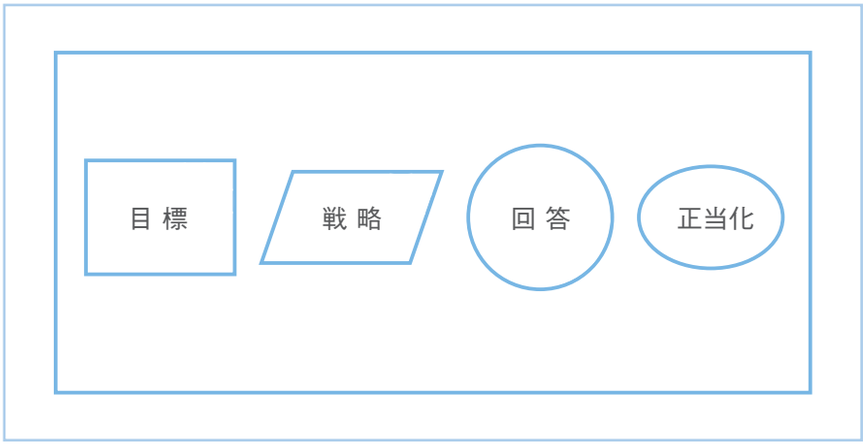
■はじめに

「安全性」は21世紀における全ての産業に関連する、大きなキーワードになっており、それはソフトウェア製品開発にも言える。現在、車載組込みシステムにおいては、安全なシステムを開発するための開発プロセス、開発方法論、開発ツール、安全性分析、安全性保証とその認証といった多岐に渡る、多くの技術課題が存在する。本稿は、「安全性」に関わる車載組込みシステムの「機能安全」に関する「安全性の保証」技術の動向について概観することを目的とするものである。

1. 安全性保証の理論的枠組み

安全性を保証するために、開発プロセス、開発方法論などの多くの方法論が提案されているが、ここでは、システムの安全性を保証するための根拠を示すためにはどのような技術があるかを俯瞰する。安全性の保証が必要なのは、計算機システムに限ったことではなく、軍事、原子力、鉄道、航空、化学プラントなど多くの産業分野が存在する。そのような分野において利用されているのが、セーフティケース(safety case)と呼ばれる理論的枠組みである。安全性の保証は、様々な産業分野において義務化されており、Railway Yellow Book (英国の鉄道) [1]、EUROCONTROL(航空機)[2] などが知られている。

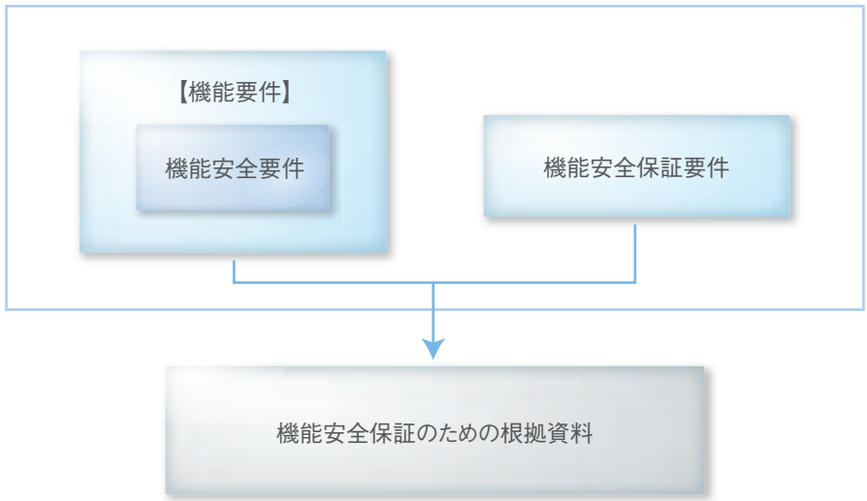
セーフティケースは安全性がいかに保証されるかを、構造化された議論(structured argumentation)により示すものであり、代表的なものに T. Kelly [3] によるGSN (Goal Structuring Notation)、Adelard 社 [4] による CAE (Claims Arguments and Evidence) がある。ここでは、GSNを例として示す。GSN にも多くの変種が存在するが、ここではオリジナルから、基本的な記号のみを解説の都合上示す。



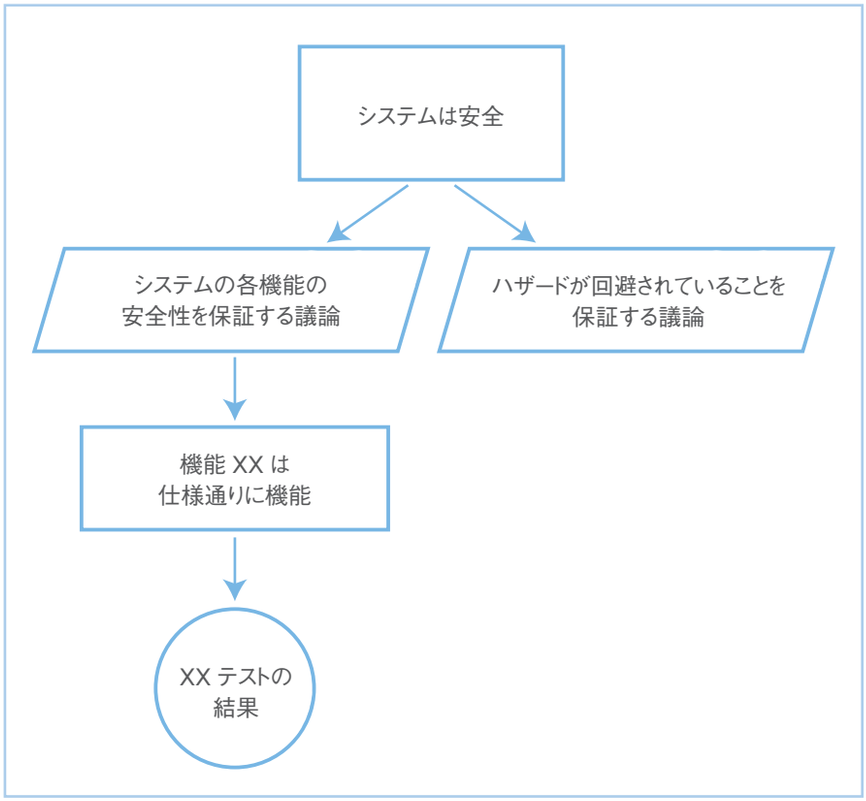
[図1] GSN のモデル要素

目標(Goal)とはシステムにより満足されるべき要件、制約である。目標は、さらに詳細な目標(部分目標)に分解される。戦略(Strategy)とは、目標から部分目標を導く際の規則や方針である。回答(Solution)は目標が成立するための根拠である。回答は、目標を成立させるための、証拠、分析結果、認証者の報告書などである。正当化(Justification)は用いられている戦略の妥当性の根拠を示すものである。

機能安全を例に考えると、機能安全要件（Functional Safety Requirements）と、機能安全を保証する要件（Functional Safety Assurance Requirements）があり、開発システムが機能安全保証要件を満たすことを示す議論を行うのがセーフティケースである（図2）。



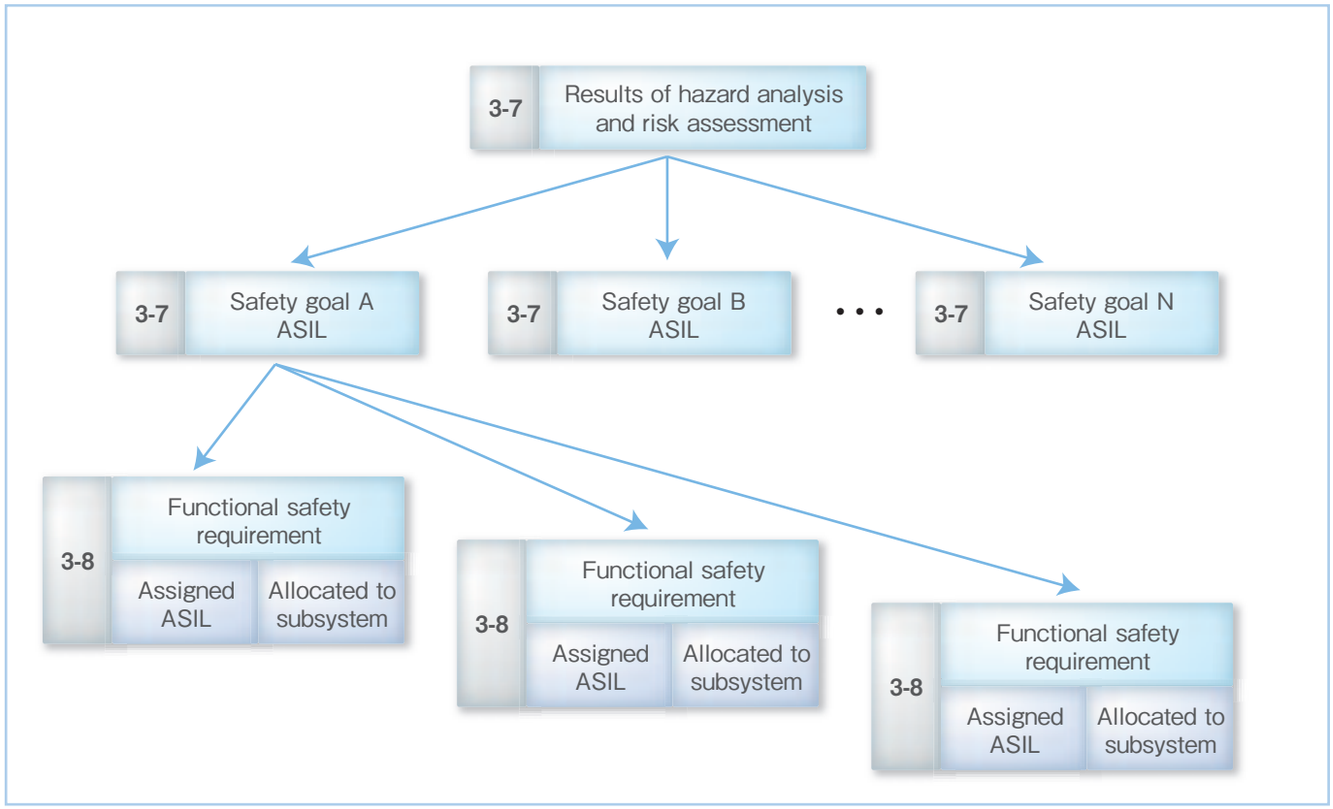
［図2］機能安全保証のための根拠資料



［図3］GSN による記述例

GSN における機能の安全を保証する議論の形式を図3に示す。ここでは、トップの安全目標を設定し、それに対して、より詳細な部分目標を導き出す方策を戦略として示す。そしてその戦略に基づいて部分目標を導き出し、その部分ゴールがそれ以上詳細化出来ない場合、その部分目標が成立するための根拠を回答として示す。ここでは、テスト方式による機能の検証によりその部分ゴールの保証が満足されること示している。

車載組込みシステムの機能安全規格 ISO/DIS 26262 [5]のPart3 では、概念フェーズについて述べられており、「ステップ1: Item の同定」、「ステップ2: ハザードの同定とリスクアセスメント」、「ステップ3: 安全目標と安全機能要件の定義」といったプロセスが示されている。ステップ3が実は、セーフティケースを構築するステップであり、形は違うが、安全ゴールから、機能安全要件を導き出し、ASIL (Automotive Safety Integrity Level)の割り当てにより、どのような保証のための根拠（テスト、形式手法による検証など）を実行しなければならないかが示される。



［図4］安全目標と機能安全要件の階層（ISO/DIS 26262 part3 より）

ISO26262/DIS においては、GSN における戦略について記述をすることは指示されていない。しかし、いかに安全目標から機能安全要件を導き出したかという情報は非常に重要であり、明示的に記述する方が、作成された機能安全要件に関する資料の共有、再利用などを考えると有効であると考えられる。

2. セーフティケースの国際標準化と開発支援ツール

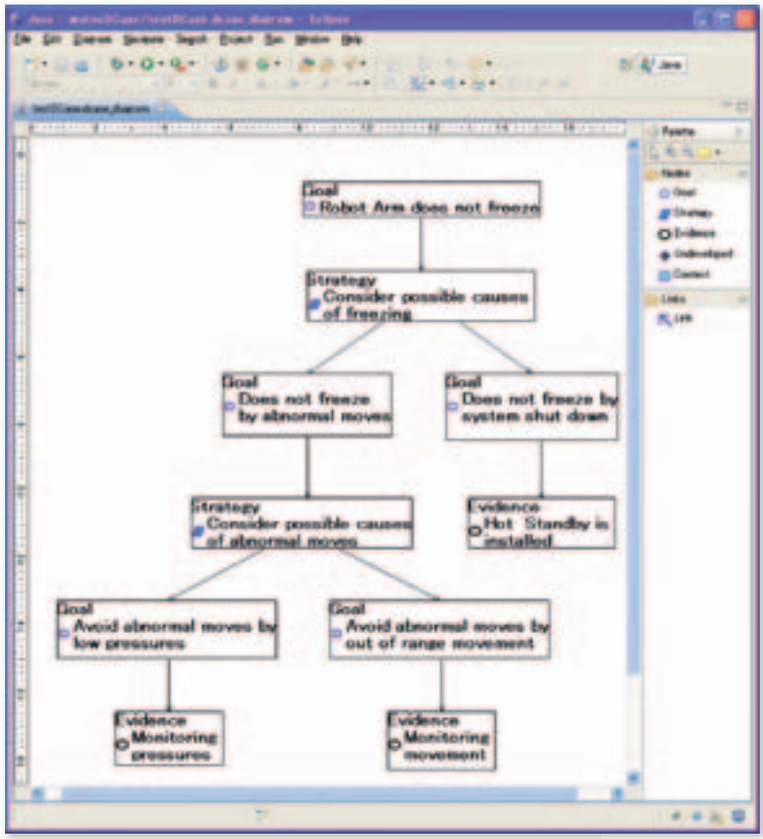
国際標準化としてはOMG(Object Management Group)における、System Assurance Task Forceにおいて、上記の CAE と GSN を統合するメタモデル ARM (Argument Metamodel) と安全性・信頼性の保証の議論の際の根拠資料に関する標準化案であるSAEM (Software Assurance Evidend Metamodel)として標準化が進行中である。現在、ARM と SAEM を統合するSACM (Structured Assurance Case Metamodel) の標準化が始まっており、来年度には標準化されることが予定されている。

ツールとしては、英国Adelard 社における ASCE (Adelard's Assurance and Safety Case Environment) や、DEOS (Dependable Operating Systems for Embedded Systems) プロジェクトで現在開発中の D-case エディタがある [6], [7]。図5に D-case エディタによるロボットアームに関する安全性分析の例を示す。D-case エディタはシステムの dependability の保証をする際の構造化議論の支援ツールである。従来のセーフティケース支援ツールにおいては明確に取り上げられていなかった、ステークホルダ間の合意形成の支援に重点を置くものである。

3. アーキテクチャ記述言語

アーキテクチャ記述言語(Architecture Description Language) は D. Garan らによる研究から始まり、それ以降、Darwin、Acme など様々な言語が提案されている。車載組み込みシステムに関連した言語としては、EAST-ADL2 [8] とAADL [9] が開発されている。AADL はSAE(Society of Automotive Engineers)により開発された、実時間、組込み機器用アーキテクチャ記述言語であり、航空機、自動車、宇宙、ロボットなど広い分野をターゲットとしている。ツールとしては CMU の SEI において開発された OSATE がある。

EAST-ADL2 はヨーロッパのATTEST (Advancing Traffic Efficiency and Safety Through Software Technology) プロジェクトにより開発された、車載組み込みシステム開発のためのアーキテクチャ記述言語であり、様々な新しい機能を支援しているが、プロダクトライン工学におけるバライアビリティ、セーフティケースの支援といった特徴を持っている。EAST-ADL2 のメタモデルは UML profile として公開されている。ツールとしてはPapyrusがある。EAST-ALD2 は Autosar、ISO26262 対応を表明している。EAST-ADL における信頼性保証の枠組みは忠実に GSN を利用しており、主張(Claim)(本稿における目標)における属性として、証拠(evidence)、
目標分割戦略(goalDecompositionStrategy)、正当化(justification)が定義されている [10]。



[図5] D-case エディタ

4. おわりに

本稿では、安全性の保証に関する理論的枠組みとしてセーフティケースについて国際標準化の動きなどを含めて概観した。そして、特に車載組込みシステムにおける機能安全との関連を、開発支援ツール、アーキテクチャ言語を取り上げることで明確化を行った。車載組込みシステムの開発に取り組む技術者に対して機能安全を理解する一助になれば幸いである。

参考文献

[1] Engineering Safety Management, Issue3, Yellow Book3, volume 1 and 2, Fundamentals and Guidance, RailTrack, 2000.
[2] European Air Traffic Management, Safety Case Development Manual, 2006.
[3] T. Kelly, Arguing Safety – A Systematic Approach to Managing Safety Cases, PhD thesis, U. York, 1998.
[4] Adelard, http://www.adelard.com/web/index.html
[5] International Organization for Standardization, Road vehicle – Functional safety -, ISO/DIS 26262 1~9, ISO Committee, 2009.
[6] Y. Matsuno, H. Takamura, Y. Ishikawa, “Dependability Case Editor with Pattern Library”, to appear in the 12th IEEE International Assurance Systems Engineering Symposium, 2010
[7] 松野, D-case: ステークホルダとシステムをつなぐドキュメント, Bulletin JASA 2010 JUN. Vol. 34 pp10-12
[8] DJ. Chen, R. Johansson, et. al., Modelling Support for Design of Safety-Critical Automotive Embedded Systems, SAFECOMP 2008, LNCS 5219, pp. 72-85, Springer, 2008.
[9] P. H. Feiler, D. P. Gluch, J. J. Hudak, The Architecture Analysis Design Language (AADL) : An Introduction, CMU/SEI-2006-TN-011, 2006.
[10] ATESST, EAST-ADL Profile Specification, 2.1 RC3, 2010.