解 説

ロボットの安全と System Assurance

Robot Safety and System Assurance

中 坊 嘉 宏^{*1} 松 野 裕^{*2} ^{*1}(独) 産業技術総合研究所 ^{*2}東京大学情報基盤センター

Yoshihiro Nakabo^{*1} and Yutaka Matsuno^{*2}

^{*1}National Institute of Advanced Industrial Science and Technology (AIST) ^{*2}Information Technology Center, The University of Tokyo

1. は じ め に

サービスロボットをはじめ、ロボットの安全に対するニーズはますます高まっている。筆者らは国際標準化団体 Object Management Group (OMG) の System Assurance Platform Task Force (SysA PTF) において、システムの安全や信頼にかかわる標準化活動を行っている。ただし安全規格や信頼性規格を作っているわけではない。本稿では OMG でどのような安全の規格を作ろうとしているのか、また System Assurance とは何かについて解説する。

2. OMG における安全の規格

2.1 国際安全規格と OMG

産業用ロボットの安全については、機械安全の ISO/IEC ガイド 51 [1] のもと、階層的な規格体系がすでに構築されている。また次世代サービスロボット、あるいは生活支援ロボットについても ISO 13482 として規格の発行が間近である [2]。そのなかでも、特に制御システムやソフトウェアによる安全機能については機能安全規格 IEC 61508 が重要である。これらの ISO/IEC 規格の基本的な考え方は、まずリスクアセスメントによりシステムのリスクを洗い出し、次に設計から開発、運用に至る安全ライフサイクルを通して十分にリスクを低減することと言える。

その際、安全のアセスメント、設計開発、そして安全の保証をするにあたって、ソフトウェアツールを用いることが有効であると考えられる。すなわち、モデルベース開発、あるいはそれを実現するツールチェーンの構築である。これを実現するには、ツールが扱うデータや開発プロセスが標準化されていなければならない。すなわち、ツールで安全を扱うための標準が必要となる。筆者らはこれを OMG で行っている。

2.2 System Risk Assessment Metamodel (SRAM)

筆者は 2009 年 3 月の OMG 会議において、最初の SRAM の提案を行った。SRAM の目的は ISO 12100:2010 (ISO 14121:2007) で示されるリスクの概念、およびリスクアセスメントについて、UML で抽象モデル化し、ソフトウェアツールの支援とシームレスな設計開発を実現することである [3]。当初はロボットの安全を目指すものとして OMG Robotics DTF にて提案したが、安全の議論は時期尚早として見送られ、代わりに急遽プレゼンを行った SysA PTF において、彼らの主たる活動である System (の安全性) を Assure (保証) する実例の提案として歓迎された。

SysA PTF では、ロボットを含む機械の安全は他の様々な分野 (ドメイン)、例えばセキュリティ、内部統制、ソフトウェア信頼性などにおけるリスク低減の一例題にすぎない。すなわち提案したリスクアセスメントの UML モデルは、抽象化した Metamodel として規格化を進めている。またリスクアセスメントにおいては、考え得る限りのすべてのリスクを網羅することが最も重要であり、これは人の想像力に依存せざるを得ない部分である。すなわち、アセスメントの手順やプロセスが重要となることから、単なるリスクのモデルではなく、リスクアセスメントのモデルを目指すこととした。規格化検討の詳細は OMG SysA PTF の WEB ページ [4] などをご参照いただきたい。

3. Assurance Case

3.1 Assurance Case とは

Assurance Case とはシステムの安全性などを議論するための文書一式のことで、Case とは法廷用語の「根拠」を意味する。イギリスなど欧米では Safety critical なシステムを開発運用する際に、認証機関に提出することが義務付けられるほどに普及している。システムの安全性を議論する場合は Safety Case、信頼性などを議論する場合は Dependability Case などと呼ばれる。SysA PTF ではシステムを保証 (Assure) するための基礎として、この Assurance Case を考えている。

Assurance Case の基本構造は木構造であり (図 1 参照)、

原稿受付 2011 年 3 月 31 日

キーワード: Service Robot, Personal Care Robot, System Assurance, Safety Case, Risk Assessment

^{*1}〒 305-8568 つくば市梅園 1-1-1

^{*2}〒 113-8658 文京区弥生 2-11-16

^{*1}Tsukuba-shi, Ibaraki

^{*2}Bunkyo-ku, Tokyo

図 1 Assurance Case の基本構造 [5]

図 2 GSN で書かれた Assurance Case の例

議論すべきゴール（システムの安全性など）をトップに置き、それをサブゴールに分割することにより詳細化する。詳細化されたサブゴールは、最終的にエビデンスによって保証される。

木構造を明示的に示し、議論しやすくするために、Assurance Case はしばしばグラフィカルな記法で書かれる。主要な記法はイギリスの York 大学で開発された Goal Structuring Notation (GSN) [6] と、イギリス Adelard 社で開発された Claim, Argument, Evidence (CAE) [7] である。GSN を用いた簡単な Assurance Case を図 2 に示す。

図 2 において、議論すべきトップゴールは「システム X では欠陥が生じない」である。もちろん、すべての欠陥が生じないことは保証できないので、ここではリスク分析の結果から得られた二つの欠陥 A, B について議論している。トップゴールにつけられた、丸みがついた長方形のノードはコンテキストノードと呼ばれ、ゴールを議論する際の環境情報が記述される。ゴールの下につく平行四辺形のノードはストラテジと呼ばれ、そのゴールを分割する際の理由が記述される。この例では、欠陥 A, B に分けて議論することが記述されている。ストラテジの下にゴールは、欠陥 A,

B についてであり、それぞれ運用時のモニタリング, FTA 解析の結果などによるエビデンス（楕円形のノード）によって保証されている。

3.2 Assurance Case の目的とその利用

Assurance Case が普及した背景には、1988 年におきた、死者 167 名を出した北海油田事故など近年イギリスで発生した深刻な障害がある。単にシステムの開発や運用を手順通りにするだけでなく、その開発や運用で、なぜシステムが安全になるのか、エビデンスをもとに議論する必要性がイギリスで広く認識された [5]。以後原子力発電所など Safety critical なシステムの開発運用において、Safety Case の記述が義務付けられるようになった。研究に関しては、特にイギリス York 大学の Tim Kelly らのグループ（文献 [6] など多数）が有名で、GSN を用いて、どのようにすれば安全性をより確かにできるような Safety Case が記述できるか、リスク分析手法などとの組み合わせや、複雑なシステムにおける記述の検討などが活発に研究されている。

Assurance Case ツールの数は現在それほど多くなく、Adelard 社で開発されている ASCE ツール [7] が最も広く使われている。ただし Assurance Case の重要性が高まるにつれて、いくつかのツールが開発されはじめており、我が国でも、筆者らが JST CREST、実用化を目指した組み込みシステム用ディペンダブルオペレーティングシステム研究領域 [8] において、D-Case Editor と呼ばれるツールを開発中で、近々フリーウェアとして公開予定である。

3.3 Assurance Case に関する標準化活動

Assurance Case に関する国際規格としては、改訂中の ISO/IEC 15026 Systems and software engineering—Systems and software assurance の Part 2 において、Assurance Case の基本構造と用語が定義されている。OMG では York 大学や Adelard 社が中心となり、Argumentation Metamodel (ARM) [4] が 2010 年に策定された。ARM では GSN と CAE の共通部分を UML メタモデルとして定義している。ASCE では ARM への準拠をすでに行っており、今後開発されるツールは ARM への準拠が必要になると思われる。また他に、Software Assurance Evidence Metamodel (SAEM) [4] という、ソフトウェアに関する Assurance Case を記述する際のエビデンスの形式についても OMG で規格化されている。

4. お わ り に

以上、ロボットの安全と OMG 標準, Assurance Case について述べた。Assurance Case は自動車の機能安全規格である ISO/IEC 26262 でも記述が要求されるなど、世界的に注目を集めている。システムの安全性やディペンダビリティの保証は今後ますます重要になると思われる。我が国としても国際規格の策定に積極的にかかわる必要があ

り，産業技術総合研究所や東京大学が，ISO や OMG など
で Assurance に関する標準化活動を行っている。

参 考 文 献

- [1] ISO/IEC Guide 51:1999, Safety aspects—Guidelines for their inclusion in standards.
- [2] 尾暮拓也，山田陽滋：“生活支援ロボットの安全性に関する国際標準化活動”，第 28 回日本ロボット学会学術講演会予稿集 DVD-ROM, AC1B2-2, 2010.
- [3] 中坊嘉宏，山田陽滋：“人と共存するロボットののためのオブジェクト指

向によるリスクアセスメントのモデリング”，日本機械学会ロボティクス・メカトロニクス講演会'08 講演論文集，2A1-A19, 2008.

- [4] <http://sysa.omg.org/>
- [5] P.G. Bishop and R.E. Bloomfield: “A Methodology for Safety Case Development,” Safety-critical Systems Symposium, 1998.
- [6] T.P. Kelly and R.A. Weaver: “The Goal Structuring Notation—A Safety Argument Notation,” Workshop on Assurance Cases (in DSN2004), 2004.
- [7] <http://www.adelard.com/web/index.html>
- [8] <http://www.crest-os.jst.go.jp/>

中坊嘉宏 (Yoshihiro Nakabo)

2000 年東京大学大学院工学系研究科計数工学専攻博士課程修了，同大学リサーチ・アソシエート，理化学研究所バイオ・ミメティックコントロール研究センター，産業技術総合研究所知能システム研究部門安全知能研究グループを経て，2010 年よりディペンダブルシステム研究グループ主任研究員。人と共存するロボットの安全，機能安全の研究に従事。
(日本ロボット学会正会員)

松野 裕 (Yutaka Matsuno)

2006 年東京大学大学院新領域創成科学研究科博士課程修了，東北大学電気通信研究所，同大学情報科学研究科，産業技術総合研究所システム検証研究センターを経て，2010 年より東京大学情報基盤センター特任講師。プログラミング言語，システムのディペンダビリティ保証に興味を持つ，日本ソフトウェア科学会所属。