Vol.2013-SE-181 No.12
2013/7/18

ASSURE2013 参加報告

松野裕[†1]

2013 年 5 月に IEEE ICSE と併催された国際ワークショップ ASSURE2013 (International Workshop on Assurance Cases for Software-intensive Systems)の報告を行う.

A Report of ASSURE2012 Workshop

YUTAKA MATSUNO[†1]

We report ASSURE 2013(International Workshop on Assurance Cases for Software-intensive Systems), held with IEEE ICSE in May 2013.

1. はじめに

2013 年に 5 月 19 日に開催された，ASSURE2013 (International Workshop on Assurance Cases for Software-intensive Systems)の報告を行う。ASSURE2013 は、ソフトウエア工学の歴史ある国際会議 ICSE2013(International Conference on Software Engineering) と併催して行われた。ASSURE2013 は、近年欧米で高安全なシステムの開発運用の際に提出が義務付けられるまでに普及している assurance case（保証ケース）の、特にソフトウエアを志向したワークショップであり、今回が第 1 回目であった。Organizing committee, program committee は以下であった。図 1 に会議の様子を示す。

図 1．会議の様子

Organizing Committee
Ewen Denney, SGT / NASA Ames, USA
Ibrahim Habli, University of York, UK
Tim Kelly, University of York, UK
John Knight, University of Virginia, USA
Ganesh Pai, SGT / NASA Ames, USA

Program Committee
Robin Bloomfield, City University, UK
Luke Emmet, Adelard, UK
Richard Hawkins, University of York, UK
Kelly Hayhurst, NASA Langley, USA
Michael Holloway, NASA Langley, USA
Daniel Jackson, MIT, USA
Insup Lee, University of Pennsylvania, USA
Peter Lindsay, University of Queensland, Australia
Tom Maibaum, McMaster University, Canada
Nikolai Mansourov, KDM Analytics, USA
Robert Martin, MITRE Corporation, USA

Yutaka Matsuno, Nagoya University, Japan
Roger Rivett, Jaguar Land Rover, UK
Christel Seguin, ONERA, France
Kenji Taguchi, AIST, Japan
Fredrik Torner, Volvo Car/ Chalmers, Sweden
Alan Wassyng, McMaster University, Canada
Robert Weaver, Airservices Australia, Australia
Charles Weinstock, SEI

筆者は Program Committee としても参加した（2012 年度の所属は名古屋大学である)。システム検証、システム保証などの分野から多くの専門家が集まった。特に Assurance case は、概念自体は以前より知られていたが、普及しはじめたのはここ 20 年程度の、若い分野である。この分野に対して先駆的な研究を行なっている研究者および実践している企業関係者が多く集まった。参加者は２０名を超え、活発な

†1 電気通信大学
The University of Electro-Communications.

議論が行われた。今後につながると思われる。

日本においてはAssurance caseについて耳にした人は多くないと思われる。筆者らは、JST CREST Dependable Embedded Operating System (DEOS)プロジェクトにおいて、assurance caseに関する研究開発を行なっている。詳しくはhttp://www.dcase.jpをご覧頂きたい。

本稿の構成は以下の通りである。2節において、assurance caseの概要を説明する。3節において、発表内容を幾つか紹介する。4節においてまとめを行う。

2. Assurance Caseについて

Assurance Caseとはシステムの安全性やディペンダビリティを証拠(Evidence)に基づいて議論するためのドキュメントである。その基本構造は木構造などで表される。

図2に参考文献[1]にある図をもとにしたassurance caseの基本構造を示す。Assurance caseは、「システムは安全である」など、システムが満たすべき命題をトップゴールとして、それを詳細化し、最終的に証拠によって詳細化された部分が成り立つことを保証する。詳細化のためのゴール分割の形を議論の構造と呼ぶ。

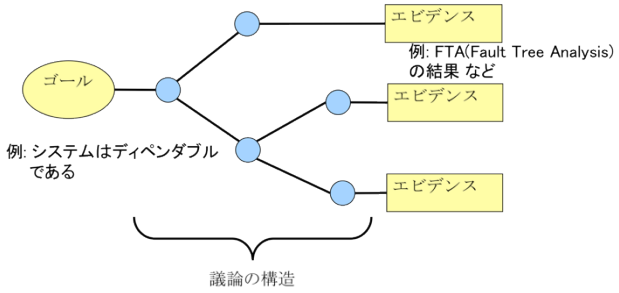

図2 Assurance caseの基本構造

Assurance caseの定義は色々あるが、ここでは[1]の定義を示す。

“A documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment.”

和訳すると以下のようになる。
「与えられた適用先と、環境において、システムがディペンダブルであることの 確かで、正しい議論を提供する、エビデンスを元にしたドキュメント」

また、ISO/IEC 15026-2:2011 Systems and software engineering – Systems and software assurance – Part 2: Assurance case において、

・ケースの構造と内容に対する最低限の要求を規定

・Assurance caseの内容
システムや製品の性質に対する主張(claim)、主張に対する系統的な議論、(argumentation) 議論を裏付ける証拠(evidence) 明示的な前提(explicit assumption)

・ 議論の仮定で、補助的な主張を用いることにより、最上位の主張に対して証拠や前提を階層的に構成

などが規定されている。 Assurance caseは、従来は安全性を議論するドキュメントとして、safety caseと呼ばれてきた。議論すべきシステムの性質に応じて、~caseと呼ばれる。例えばセキュリティを議論する場合はセキュリティケース(Security Case)と呼ばれる。これらを総称した言葉が、assurance caseである。ISO/IEC 15026 においてassurance caseと呼ばれているように、今後assurance caseという言葉が一般的になると思われる。

Safety caseは、現在自動車の機能安全規格であるISO 26262などでも要求項目になっているなど、特に欧米では高い安全性が要求されるシステムを開発運用する際には提出が義務付けられるほどに普及している。普及した背景には、近年におきた、欧米での深刻な障害事例がある。1988年におきた北海油田における爆発事故では、167名が死亡した。従来、システムの安全性確認は安全性に関するチェックリストの項目を満たしているかとどうか、認証者 などが判定することにより主に行われていた。しかしながら、なぜチェックリスト の項目を満たすと、システムが安全であるのか、明示的な議論が行われることが少なかった。北海油田における事故などの反省から、チェックリストの項目にある手順やテストのみではなく、なぜそれらの手順やテストで、対象システムの安全性が保たれるのか、明示された議論で、証拠(エビデンス)をもとに議論する重要性が認識された。Safety caseという言葉は、北海油田事故の調査報告書である[2]が主な初出である。以来セーフティケースはイギリスを中心として欧米でシステム安全性認証(Safety Certification)で義務付けられるほど普及している。 アメリカでは、2007年に National Academy of Scienceから、近年の深刻な障害事例の調査報告書[3]を出版され、その中でassurance caseの必要性が言われたことが一つの契機になって、assurance caseがアメリカにおいても認識されはじめた。例えばUS. Food and Drug Administration (FDA)では、点滴ポンプなどの医療器具を病院に導入する際にそのsafety caseを提出することを義務付けている[4]。

Assurance caseは普及しているが、まだ若い分野であり、様々な課題がある。 基本的な課題としては、assurance caseの記述法や評価法が未だ確立されていないことがある。そのため、ときとしてずさんなsafety caseがあることが報告されている。有名な例としては、Nimrod 軍用機の例がある。2006 年 9 月 2 日、アフガニスタンで作戦飛行中のMR.2 XV230 が、空中給油を受けた直後に火災が発生 して墜落する事故が発生した。2007 年 12 月 4 日、イギリス国防省は調査報告を発 表し、墜落した機体は、給油後タンクから燃料漏れが生じており、高温空気パイプの熱によって発火、拡大して墜落に至った、と分析した[5]。Nimrod軍用機のsafety caseはあったのだが、上記の障害が起こりうることを、十分に議論していなかった、またsafety caseの記述の十分性のチェックが行えるような管理体制が機能していなかったなどの問題点が報告された。Safety caseが適切に管理されていれば、障害に至る欠陥を解析するための有効な材料になり得たはずであると報告された。

きちんとした議論で、適切な証拠をもとにシステムの安全性やディペンダビリティや安全性を保証することの重要性が世界的に認識されつつあると考える。これからの分野であることから、課題も多い。ASSURE2013はこれらの課題を解決するための端緒を見つけるためのワークショップであるといえる。

3. 発表内容について

プログラムは以下の通りであった。発表資料はhttp://www.cs.york.ac.uk/assure2013/Program.html より取得可能である。以下いくつかの発表についてコメントを加える

8.30 - 9.00

Welcome and Introduction to Assurance Cases

Ibrahim Habli (University of York)

Assurance case の初心者のためのチュートリアルが行われた。発表者の Habli 氏は York 大学の Tim Kelly 教授の元で assurance case の研究を行なっている。特に assurance case のグラフィカルな表記法の一つである GSN(Goal Structuring Notation)[6]の説明が行われた。GSN は Tim Kelly 教授が主に開発し、最もよく用いられている assurance case の表記法の一つである。GSN の例を図 3 に示す。

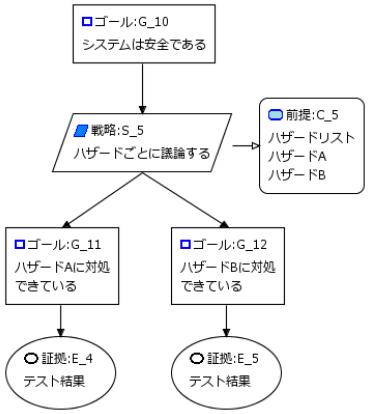

図 3 GSN の例

GSN は図のように、ゴール指向の表記法の一種である。トップゴールにシステムが満たすべき命題を置き、それが満たされていることをサブゴールに展開することにより示す。ここではシステムの安全性を、想定されるハザードごとに議論することにより示している。長方形のノードはゴール(goal)と呼ばれ、命題が置かれる。平行四辺形のノードは戦略(strategy)ノードと呼ばれ、ゴール分割における説明が置かれる。丸みを帯びた長方形のノードは前提(context)と呼ばれ、ゴールノードや戦略ノードを議論するときの前提を示す。楕円のノードは証拠(evidence)ノードと呼ばれ、分割されたゴールを最終的にサポートするためのテスト結果などが置かれる。

Principles

9.00 - 9.30

Safety Cases: A Review of Challenges

Zarrin Langari, Tom Maibaum (McMaster University)

現状の assurance case/safety case の課題が報告された。Assurance case は欧米、とくにイギリスにおいて広く使われるようになったが、いまだ多くの課題がある。本発表ではそれらをリストアップすることにより、話題提供を行った。課題を以下にリストアップしている。

Report and Presentation
- Size and complexity
- Readability
- Graphical Notation

Content and Structure
- Variety of evidence
- Challenges with context and assumptions
- Challenges with arguments

General
- Confirmation Bias
- Challenges of process- and product-based approaches
- Challenges with safety cases for product lines
- Safety Cases in the SDLC
- Assessment of safety cases by regulators

9.30 - 10.00
Measuring Assurance Case Confidence Using Baconian Probabilities
Charles Weinstock, John Goodenough, Ari Klein (Software Engineering Institute)
Assurance case を記述しても、それによってどの程度システムの安全性などに確信を得られるのかを評価することは難しい。本発表では、Baconian Probabilities を用いて、assurance case の確信度(confidence)を評価するための基礎的な考察を述べていた。基本的に Defeater と呼ばれる、(GSN における)ゴールの内容、戦略の妥当性、証拠の妥当性を攻撃する要因を列挙し、それらにどの程度 assurance case の記述内容が耐えうるかにより確信度を計測する。筆者の感想としては極めてシンプルな考え方であり、面白いと思ったが、実際に適用するためには未だ多くの課題があると思えた。

Tool Demonstrations 1
10.00 - 10.15
AdvoCATE: An Assurance Case Automation Toolset (Tool Demonstration)
Ewen Denney, Ganesh Pai, Atef Suleiman (SGT., Inc. NASA Ames Research Center)
NASA の AMES 研究所で開発中の、AdvoCATE ツールのデモが行われた。従来の GSN のモジュールでは、モジュール間のネットワークは任意に作ることができたが、AdvoCATE はモジュールが階層的(hieratical)に管理できる仕組みをとりいれている。そのほか、形式手法を応用したデモが行われた。

10.15 - 10.30
Model-Based Safety Cases in AutoFOCUS3 (Tool Demonstration)
Tim Kelly (University of York), Carmen Carlan, Sebastian Voss (fortiss GmbH)

10.30 - 11.00
Coffee Break

Notations and Techniques
11.00 - 11.30
An Evaluation of Argument Patterns to Reduce Pitfalls of Applying Assurance Case
Shuichiro Yamamoto, Yutaka Matsuno (Nagoya University)
筆者と、昨年まで筆者が在籍していた山本修一郎教授との共著である。日本ではまだ assurance case は殆ど使われていない。本研究では、assurance case を実際に日本企業の方に行なってもらった実験結果および実験に用いた assurance case pattern の妥当性などについて論じている。

11.30 - 12.00
Nuanced Term-matching to Assist in Compositional Safety Assurance
Philippa Conmy, Katrina Attwood (University of York)

12.00 - 12.30
An Implementation of GSN Community Standard
Yutaka Matsuno, Shuichiro Yamamoto (Nagoya University)
筆者と山本教授の共著である。GSN は GSN Community Standard[6]において GSN の定義が行われているが、実際に定義されている構文、特にモジュールなどを実装しているツールはこれまでほとんどなかった。本発表では、DEOS プロジェクトで開発中の D-Case Editor[7]において GSN モジュールを実装した経験を述べている。GSN Community Standard にはいくつか曖昧なところがあり、実装において問題になった点などを報告した。
12.30 - 14.00
Lunch Break

Applications

14.00 - 14.30
Architecting and Generalizing a Safety Case for Critical Condition Detection Software - An Experience Report
Martin S. Feather (JPL, California Institute of Technology), Lawrence Markosian (SGT., Inc. NASA Ames Research Center)

14.30 - 15.00
Creating Safety Assurance Cases for Rebreather Systems
Alma Juarez Dominguez (University of Waterloo), Bruce Partridge (Shearwater Researchlivepage.apple.com Inc.), Jeffrey Joyce (Critical Systems Labs Inc.)
Rebreather system とは、潜水に使うための酸素循環器である。酸素循環器の安全性を示すために、GSN を用いて、安全であること、国際規格に準拠していることを assurance case によって示すことを試みた。Assurance case を記述することによって、リスクおよび残余リスクへの認識が高まり、専門家・開発者との議論の促進を得ることができ、時間と資金に相応のメリットが得られたとしている。しかしながら定量的な評価はなされておらず、若干主張が弱いと感じられた。Assurance case 自体の良さを定量的に評価することは研究課題の一つであり、評価基準の確立が求められる。

15.00 - 15.30
Constructing Safety Assurance Cases For Medical Devices
Arnab Ray (Fraunhofer CESE), Rance Cleaveland (University Of Maryland)

Tool Demonstrations 2

15.30 - 15.45
D-Case Editor and D-Case/Agda (Tool Demonstration)
Yutaka Matsuno (Nagoya University), Makoto Takeyama (AIST)
D-Case Editor のデモを行った。GSN のモジュールなどの実際のデモは興味深く受け入れられた。

Assurance Case Standards
15.45 - 16.00
Overview of Standardization Efforts
神奈川大学の武山誠氏より DEOS で行われている assurance case に関する国際標準化活動について報告が行われた。特に武山氏が力をいれている、MACL(Machine-checkable Assurance Case Language)の OMG(Object Management Group)での標準化活動が紹介された。従来 assurance case は自然言語で記述されてきたが、整合性検査などに困難が生じる。MACL では整合検査が可能であるような assurance case の記述言語の仕様の標準化を目指している。

16.00 - 16.30
Coffee Break

16.30 - 17.45
Panel Discussion
Chair: Ewen Denney (SGT., Inc. NASA Ames Research Center)
John Goodenough (Software Engineering Institute), Tim Kelly (University of York), Makoto Takeyama (AIST), Alan Wassyng (McMaster University)

17.45 - 18.00
Wrap-up
Ganesh Pai (SGT., Inc. NASA Ames Research Center)

4. まとめ

本稿では、ICSE2013 と併催して行われた ASSURE2013 の報告を行った。Assurance case は若い分野であり、課題も多い。欧米で広く用いられているとしても、実際の適用現場では FTA(Fault Tree Analysis, 故障木解析)など従来の手法と混用するなど、多くの誤用があると思われる。しかしながら ASSURE2013 での活発な議論、また筆者らの日本での企業の方々との議論から、複雑化、ネットワーク化するこれからのシステムの安全性、ディペンダビリティのためには、assurance case は重要になってくると思われる。今後も ASSURE などの国際会議、ワークショップなどに関わり、研究を進めて行きたい。

謝辞 本研究会論文は JST CREST「実用化を目指した組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(DEOS)」プロジェクトよりの支援を受けて行われた。

参考文献

1) Bishop, P. & Bloomfield, R. (1998). A Methodology for Safety Case Development, in Proc. of the 6th Safety-critical Systems Symposium, Birmingham, UK. Feb 1998
2) Cullen, The Hon. Lord. (1990). The Public Inquiry into the Piper Alpha Disaster, Vols. 1 and 2 (Report to Parliament by the Secretary of State for Energy by Command of Her Majesty).
3) Daniel Jackson, Martyn Thomas, and Lynette I. Millett, Software for Dependable Systems – Sufficient Evidence?, The National Academies Press, Washington D.C., 2007
4) Richard Chapman, Assurance Cases for External Infusion Pumps http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsCon ferences/UCM217456.pdf, 2010
5) The Nimrod Review, http://www.official-documents.gov.uk/document/hc0809/hc10/1025/1025.pdf
6) GSN Community Standard version 1.0. http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf
7) D-Case Editor, http://www.dependable-os.net/tech/D-CaseEditor/D-Case_Editor_J.html