慶應義塾大学学術情報リポジトリ
Keio Associated Repository of Academic resouces

Title	システムズエンジニアリングに基づくアシュアランスケース記述方法の提案 : トレーサビリティの見える化と階層性を利用した段階的品質確認の実現
Sub Title	Proposal of description rules for assurance cases based on systems engineering : realization of visualizing traceability and progressive confirmation of quality by utilizing system hierarchy
Author	田中, 康平(Tanaka, Kohei) 白坂, 成功(Shirasaka, Seiko)
Publisher	慶應義塾大学大学院システムデザイン・マネジメント研究科
Publication year	2012
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2012年度システムエンジニアリング学 第109号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40002001-00002012-0040

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

修士論文　　2012 年度

システムズエンジニアリングに基づくアシュアランスケース記述方法の提案

―トレーサビリティの見える化と階層性を利用した段階的品質確認の実現―

田中　康平

(学籍番号：81133395)

指導教員　白坂 成功

2013 年 3 月

慶應義塾大学大学院システムデザイン･マネジメント研究科
システムデザイン・マネジメント専攻

Master's Dissertation 2012

Proposal of Description Rules for Assurance Cases Based on Systems Engineering - Realization of Visualizing Traceability and Progressive Confirmation of Quality by Utilizing System Hierarchy -

Kohei TANAKA

（Student ID Number：81133395）

Supervisor Seiko SHIRASAKA

March 2013

Graduate School of System Design and Management,
Keio University
Major in System Design and Management

論　　文　　要　　旨

学籍番号	81133395	氏　名	田中康平

論 文 題 目：

システムズエンジニアリングに基づくアシュアランスケース記述方法の提案
―トレーサビリティの見える化と階層性を利用した段階的品質確認の実現―

（内容の要旨）

設計情報のトレーサビリティの見える化と開発フェーズに沿って段階的に品質を確認し合うための方法をアシュアランスケースという考え方を利用して提案する．

近年，システムの巨大化・複雑化が進んでいる．このことによって 1 つのシステムに関わるステークホルダは増えている．そのため，システムの整合性を示すことや技術リスクへの対処ができているかどうかを判断することが難しくなってきている．

このことから，欧州を中心に，第三者へとシステムの安全性を説明する仕組みとして，セーフティケースという概念が提唱された．これは，1988 年に 167 名の死傷者を出した北海油田における事故の調査を機に提唱された．従来，システムの安全性はチェックリストの項目を満たしているかどうかを認証者や作業従事者がチェックすることにより確認されてきた．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は，明示的な議論が行われていることが少ない．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．

今では，システムの安全性のみではなく，その信頼性・運用性・可用性もシステムを利用する上では重要であると認識されており，総じて品質を確認し合うための方法としてアシュアランスケースという概念が提唱されている．

アシュアランスケースは，イギリスを中心に，欧州全体で第三者にシステムの品質を提示するための方法として近年注目されている．このアシュアランスケースを記述するための方法として，Tim Kelly が提唱している Goal Structuring Notation がある．2011 年に GSN を記述するためのマニュアル（GSN Community Standard）が発行されたが，GSN を利用した記述対象はソフトウェア分野が中心であり，システムのトレーサビリティを保証する方法や，システムのライフサイクルを通して品質を保証するための方法はまだ十分に検討されていない．

本研究では，従来の記述方法の課題を指摘し，その課題を解決するための記述方法を提案した．具体的には，システムの開発には欠かすことができない，トレーサビリティの見える化と段階的に品質を確認することを実現する方法を提案する．そして，その記述方法を下に現在開発中の人工衛星のサブシステム及び CanSat と呼ばれるロボットを対象にアシュアランスケースを記述し，開発メンバと議論した結果について報告する．

キーワード（5 語）

超小型衛星｜品質保証｜アシュアランスケース｜ゴール指向分析｜D-Case

SUMMARY OF MASTER'S DISSERTATION

Student Identification Number	81133395	Name	Kohei TANAKA

Title

Proposal of Description Rules for Assurance Cases Based on Systems Engineering

- Realization of Visualizing Traceability and Progressive Confirmation of Quality by Utilizing System Hierarchy -

Abstract

This paper introduces the way to describe the assurance case about satellite and the results of adopting assurance cases to the development of Hodoyoshi satellite.

As the technology of satellite has been highly advanced, it has become difficult to assure dependability of a satellite system. Currently, dependability of satellite system is mainly supported by various risk analysis and verification results. However, due to time and cost constraints, management of risk analysis and verification has been done in an ad-hoc manner. Therefore, it is difficult to assure why such analysis and verification result are required for the dependability in some cases.

An assurance case is 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. Assurance cases are written in a top-down manner to argue the top goal about dependability of the system. In Europe, assurance cases are widely used as regulation in safety-critical areas. Assurance cases are often written in a graphical notation to ease the difficulty of writing and certifying them. GSN (Goal Structuring Notation) is one of such notations. A characteristic of GSN is that when decomposing a goal, it is required to explicitly write the rationale for the decomposition. There are still some issues to solve.

There are three benefits. First, an assurance case helps to ensure a minimum number of criteria to develop a reliable satellite by using strategies of the assurance case from the other reliable satellites. Secondly, all project members can argue logically about the system reliability. From this, designers can recognize whether the system is enough or not. At last, the project member can understand the critical points of design and the impact of design changes.

Key Word(5 words)

Microsatellite, System assurance, Assurance case, GSN, Dependability-Case