A06 超小型衛星の構造設計に対する安全要求のゴール指向要求分析

南部 陽介 (大阪府立大学)
Yohsuke Nambu (Osaka Prefecture University)

概要

スマート構造による航空機翼のモーフィングや宇宙望遠鏡の形状制御の実用に際しては，システム全体の安全に対する影響を評価すると共に，明示的な議論によってシステム全体の安全を保証することが求められる．本研究では，近年，自動車業界をはじめ多くの産業において規格化が進んでいるアシュアランスケースに着目し，実際に宇宙へ打ち上げられた超小型衛星 OPUSAT を事例として，その安全性に関わる議論をゴール指向分析により構造化・可視化すると共に，要求仕様との関連性を明らかにすることを目的とする．特に，構造サブシステムに関するハザードについて分析を行い，モデリングに際しての推奨記述法を提案し，それにより安全に関する議論とシステム要求との整合性の確保が格段に容易になることを示した．

1. 序論

近年，自動車をはじめ，多くのシステムにおいて，その制御にコンピュータが導入されている．それに伴い，ハードウェアだけでなくソフトウェアをも含めたシステム全体としての安全性を考える必要が出てきている．2011 年には，自動車の車載電子システムの安全規格として ISO26262[1] が発行され，機能安全への注目が高まっている．機能安全とは，監視装置や防護装置などの付加機能によるリスク低減策のことであり，事故の原因そのものを取り除く本質安全と異なる考え方である．電車と自動車の衝突事故を防ぐために，踏切に警報機や遮断機を設置するのが機能安全，立体交差にするのが本質安全の考え方である．その他の安全規格としては，列車システムに関する Railway Yellowbook[2]，航空管制システムに関する EUROCONTROL[3]，防衛に関する Defence Standard 00-56[4] などがあり，いずれも機能安全の完全性を保証するために，アシュアランスケースの作成が義務付けられている．

アシュアランスケースとは，与えられた運用環境におけるシステムの適用に関して，安全であることを，強制的かつ理解可能，妥当な事例として提供する，根拠資料の集まりによって支援された構造化された議論を意味する．1988 年 7 月に起きた北海油田 Piper Alpha 事故 [5]（229 名中 167 名死亡，270 億円の被害）を契機に，安全を確保する手順だけでなく，明示的な議論と根拠文書により安全を保証するために，アシュアランスケースの作成が求められるようになった．ソフトウェア工学におけるアシュアランスケースの標準である ISO/IEC 15026-2:2011[6] では，アシュアランスケースの内容として以下を含むことが要求されている．

1. システムの性質に対する主張
2. 主張に対する系統的な議論
3. 議論を裏付ける証拠
4. 明示的な前提

アシュアランスケースは，通常，自然言語によって記述されるが，GSN(Gaol Structural Notation)[7] を用いたグラフィカルな記法が採用されることもある．さらに，アシュアランスケースの概念をシステムのディペンダビリティの保証に応用したディペンダビリティケース [8] に関する研究も，ソフトウェアの分野では進んでいる．システムのディペンダビリティとは，一般的な信頼性を越えて，例え一部が壊れても残りの部分でうまく働くといった自立的自己修復的な動作を指す概念である．

近年，スマート構造による航空機翼のモーフィングや宇宙望遠鏡の形状制御が注目されている．アクティブな可変形状構造物は，システム全体に少なからぬ影響を及ぼすため，実用に際しては，システム全体の安全に対する影響を評価すると共に，明示的な議論によってシステム全体の安全を保証することが求められる．形状制御や振動制御に関する研究は数多あるが，スマート構造の安全性やディペンダビリティを扱った研究は，著者の知る限り存在しない．そこで，本研究では，将来のスマー

ト構造実用化を見越し，宇宙構造物に関する安全性に関わる議論の構造化と可視化を試みる．事例として H-IIA ロケット 23 号機により打ち上げられた超小型衛星 OPUSAT を取り上げ，その安全性に関わる議論を GSN により構造化・可視化すると共に，要求仕様との関連性を明らかにすることを目的とする．

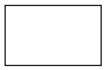
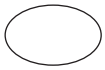
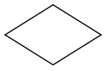
2. GSN と SysML

2.1. GSN

GSN は，アシュランスケースの内容として要求される主張，議論，証拠，前提をグラフィカルに表現する記法である．表 1 に示した 5 種類のノードと 2 種類の矢印によって，アシュアランスケースを表現する．ゴールノードには,「システムは安全である」など，対象システムに関して議論すべき命題を記述する．戦略ノードには,「ハザード原因ごとに場合分け」など，ゴールをサブゴールに分割し，詳細化を行う際の議論の仕方を記述する．分割の理由を戦略ノードに明記することが，GSN の大きな特徴である．前提ノードには，運用環境やハザードリストなど，ゴールや戦略を議論する際に前提となる情報を記述する．証拠ノードには，試験報告書など，詳細化されたゴールが達成されていることを最終的に保障する証拠を記述する．前提ノードや証拠ノードには，通常，文書は書かれず，前提情報や証拠を与える文書名が記述される．未達成ノードは，ゴールを保証する証拠がない場合に使用される．ゴールノードから戦略ノード，戦略ノードからゴールノード，ゴールノードから証拠ノードへのリンクは，支援リンク（Supported by）が用いられる．ゴールノードや戦略ノードから前提ノードへのリンクは，前提リンク（In context of）が用いられる．

各ノードの文書は，自然言語で記述するため，文体が揃っていることが推奨されている．ゴールノードは，命題の形をしている必要があり,「『システム』が『状態』である」や「『システム』は『条件』を満たす」などの表現が用いられる．戦略ノードは，ゴールとそのサブゴール郡の関係が理解しやすくなるように記述する必要があり,「『観点』に分けて説明 (議論，確認) する」などの表現が用いられる．

表 1. GSN で用いるノード

名称	記号	概要
ゴール		議論すべき命題を記述する
戦略		ゴールを分割する際の議論の仕方を記述する
前提		ゴールや戦略を議論する際の前提情報を記述する
証拠		ゴールを保障する証拠を記述する
未達成		証拠がないことを表す

2.2. SysML

ハードウェア設計に CAD 等のコンピュータ支援が導入されて久しいが，近年では，より綜合的な支援を目的とした MBSE（Model-based Systems Engineering）に注目が集まっている．システムズエンジニアリング（SE）とは，大規模かつ分野横断的なシステムの設計開発において，適切なマネジメントプロセスと技術プロセスを提供する手法群一般を指す [10]．MBSE では，システムの要求や構造，振る舞いを図によって一元的に管理する．MBSE には，一貫性・整合性とトレーサビリティの確保，既存モデルの再使用性，MILS (Model-In-the-Loop)，SILS (Software-In-the-Loop) などのシミュレーションベースの開発との親和性に優れているという特徴がある．MBSE を実践するためには開発者間で共有するルールに則ってシステムモデルを構築しなければならないが，そのための標準的な言語として SysML[11] がある．

本研究では，安全に関する議論とシステム要求を一元的に管理することを目指し，GSN と SysML の要求図を融合させることを試みる．GSN と SysML の要求図の融合に関しては，過去に山本ら [12] の研究があるが，超小型衛星のような複雑かつ実運用レベルのシステムを対象としたものはない．

2.3. BALUS

GSN や SysML の要求図を描くには，ツールが不可欠である．本研究では，著者らが独自に開発し

ている Web アプリケーション BALUS (Browser-based Assisted Library Universal System design application)[14] を利用する．BALUS は，複雑なシステムの設計開発を効率的に遂行するフレームワークとして著者らが提案する Open MBC （Model-based Collaboration）を実現するアプリケーションである [1]．

複雑なシステムの設計開発に取り組む際，エンジニアは 3 つの問題に直面する．第一に，複雑なシステムでは，全体を理解すること自体が困難である．全体を理解できないようなシステムの設計開発では，要求の見落とし，安易な仕様変更，統合時の不整合などが起こり，手戻りが何度も発生する．第 2 に，組織をまたがる作業や遠く離れた拠点間での作業では，情報共有，コミュニケーション，ワークフローなどにおいて，さまざまな齟齬が発生する．システムの設計開発では，分散的かつ同時的な作業を，円滑に進めることのできる仕組みが求められる．第 3 に，経験の乏しいシステム開発においては，適切に工程を分割できず，工数の見積もりができないなどの問題が生じる．エンジニアは，試行錯誤を重ねて開発を進めていくしかなく，このような遠回りによって，開発スケジュールの遅延，コストの超過が生じる．

これらの問題に対し，著者らは，システムモデル，コラボレーティブワークフロー，オープンエンジニアリングプラットフォームの融合というソリューションを提案している．システムモデルは要素同士の関係性をグラフィカルに表現し，コラボレーティブワークフローは GitHub[13] のような効率的な共同作業を提供し，さらに知見の再発見と再利用を促進するプラットフォームとして機能する．これらを有機的にまとめた Open MBC は，ものづくりの高速道路となり得るコンセプトであると考えている．

BALUS の主な機能 は，

1. ノードとリンクで構成されるリレーショングラフの作成機能
2. プルリクエスト駆動のバージョン管理機能
3. 知見の再発見と再利用を促進するプラットフォーム機能

である．本研究では，BALUS を用いて GSN と SysML の要求図を描き，超小型衛星の知見をシステムモデルという形で集約する．

[1] 詳細は `http://balus.me` に記載．BALUS は，現在，β 版のみ使用可能である．

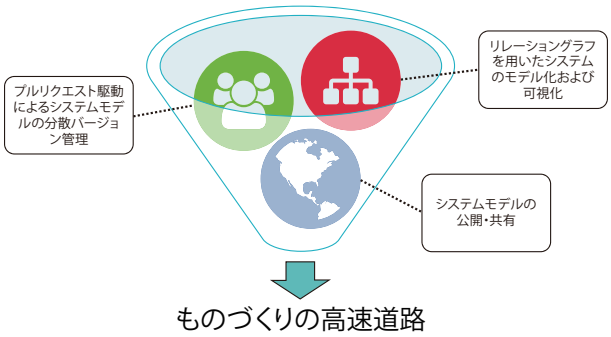


図 1. Open MBC のコンセプト

3. 超小型衛星 OPUSAT の概要

大阪府立大学の学生が中心となって開発した超小型衛星 OPUSAT（図 2）は，全球降水観測計画（GPM）主衛星のピギーバック衛星として，平成 26 年 2 月 28 日に，H-IIA ロケット 23 号機によって打ち上げられた [15]．軌道投入後，一般公募により集められた 113 件の案のなかから，「こすもず（CosMoz）」という愛称が付けられた．

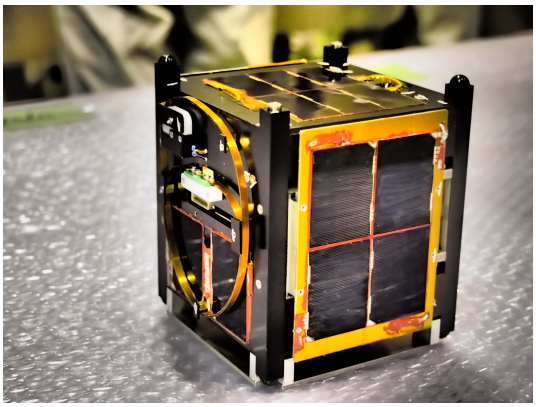


図 2. 超小型衛星 OPUSAT“CosMoz”

OPUSAT のサクセスクライテリアを表 2 に示す．ミニマムサクセスは，衛星からの OOK（on-off-keying）通信によるモールス信号受信と AFSK（Audio frequency shift keying）によるデータ受信である．要するに，ミニマムサクセスは，地上衛星間通信の確保である．

フルサクセスは，リチウムイオンキャパシタ（LIC）の充放電実験の実施と太陽指向制御実験および太陽電池パドル展開実験の実施である．

OPUSAT では，衛星バス電源の一部として，リチウムイオンバッテリ（LIB）と組み合わせて LIC を利用している．これは世界初の試みである．また，磁気トルカによってスピン安定方式による太陽指向制御を行うと共に，軌道上で太陽電池パドルを展開する．

エクストラサクセスには，パドル展開後の太陽指向制御に加え，GFSK（Gaussian filtered frequency shift keying）を用いた通信系ミッションがある．AFSK によるダウンリンクが 1200 bps に対し，GFSK によるダウンリンクは 9600 bps と高速である．OPUSAT では，ふたつの変調モデムを搭載しており，切り替えて使用することができる．

表 2. OPUSAT のサクセスクライテリア

ミニマム	モールス信号によるデータ受信
	AFSK によるデータ受信
フル	リチイウムイオンキャパシタの軌道上での充放電確認
	太陽指向制御
	太陽電池パドルの展開
	LIB − LIC 複合電源による運用
エクストラ	パドル展開後の太陽指向制御
	GFSK によるデータ受信

OPUSAT の諸元を表 3 に示す．寸法，質量は典型的な CubeSat であるが，磁気トルカを用いたスピン安定制御を行うため，Z 軸の慣性モーメントが最大となっている．また，残留磁気が極力小さくなるように材料選定や消磁を施しているため，極めて小さな残留磁気に抑えることができている．パドル未展開時には，太陽電池はボディマウントとなっており，無制御状態において平均発電量が 1.2 W となるように設計されている．

図 3 に OPUSAT のシステム構成図を示す．OPUSAT のシステムは，5 つのサブシステム（電源系，通信系，データ処理系，姿勢制御系，構造系）から構成される．通信系，データ処理系，姿勢制御系は，それぞれ独自の OBC（On Board Computer）を有している．

なお，OPUSAT は，パドル展開以外のミッションを成功裏に終え，平成 26 年 7 月 24 日に南太平洋上空にて大気圏に再突入し，運用を終了した．

表 3. OPUSAT の諸元

寸法	$10 \times 10 \times 12$ cm
質量	1.52 kg
慣性モーメント 括弧内：展開時	X : 0.00260(0.00321) kg m^2 Y : 0.00271(0.00267) kg m^2 Z : 0.00283(0.00335) kg m^2
平均発電量	1.2 W (無制御時予測値)
残留磁気	0.0062 A m^2
通信周波数	430 MHz (Uplink) 144 MHz (Downlink)
打上	2014 年 2 月 28 日
軌道	高度：400 km 軌道傾斜角：65 deg

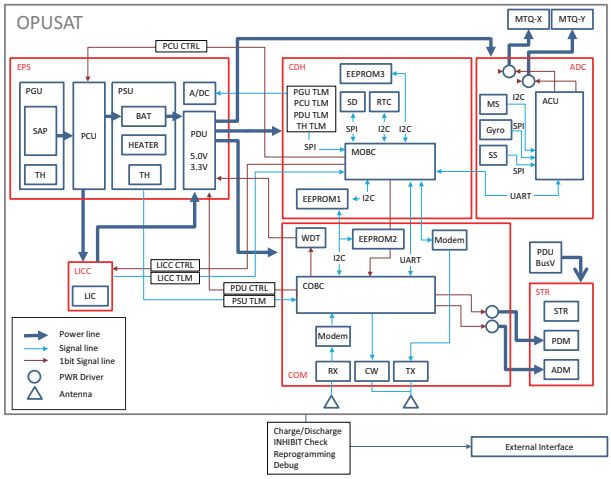


図 3. OPUSAT のシステム構成図

4. OPUSAT の安全要求

H-IIA ロケットを利用して超小型衛星を打ち上げる場合，主衛星やロケット，その他設備や人員に対して，当該衛星が安全であることが求められる．安全確保のアプローチは，過去の経験からの安全設計アプローチと未来予測からのハザード管理アプローチに分けて考えることができる．GSN で表現[2]すると，図 4 のように，「衛星システムが安全であることを保証する」というゴールに対し，「安全設計とハザード管理に分けて扱う」という戦略によって，「安全設計要求を満たすことを保証する」と「すべてのハザードが制御されていることを保

[2]ダイアグラム全体は https://app.balus.me/diagrams/5631725669449728 より閲覧可能である．

証する」というサブゴールに分割する形となる．

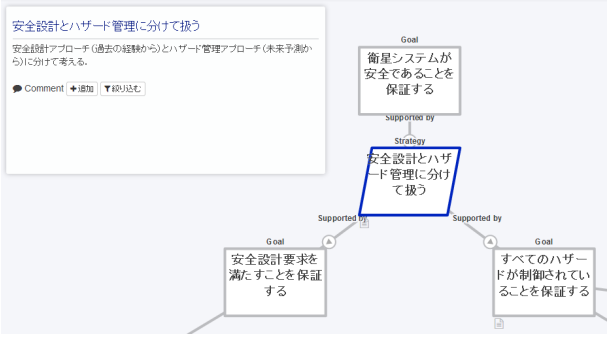


図 4. 安全確保のアプローチ

安全設計アプローチは，JMR-002B「ロケットペイロード安全標準」などの JAXA が規定する標準に適合するというゴールに分割されていき，最終的には，安全要求コンプライアンスマトリックスという適合性をチェックした一覧表が証拠として提示される．安全設計アプローチからの要求は明確であり，議論の余地も少ないため，以降は，ハザード管理アプローチについて，詳細を見ていく．

4.1. OPUSAT のシステムのハザード

ISO26262 では，ハザードを「アイテムの機能不全の振る舞いにより引き起こされる危害になりうる原因」と定義している．例えば,「工具の落下」は，落下して運動エネルギを持った工具が人体に衝突することで人体に危害を引き起こすため，ハザードとして識別される．ハザード識別には FMEA（Failure Mode and Effect Analysis）や HAZOP（HAZards and OPerability study）といった手法が使われるが，ここでは詳しくは説明しない．

OPUSAT では，図 5 のように，各サブシステム毎にハザードになりうるコンポーネントを洗い出し，ハザードを整理している．本稿では，特に構造系に関するハザードである「構造的欠陥」と「回転体・可動機構」について詳しく述べる．

4.2. ハザード制御に関する GSN

4.2.1. ハザードタイプ「構造破壊」

「構造破壊に関するハザードを制御する設計となっていることを保証する」というゴールを,「ハザード原因毎に保証する」という戦略の下，サブ

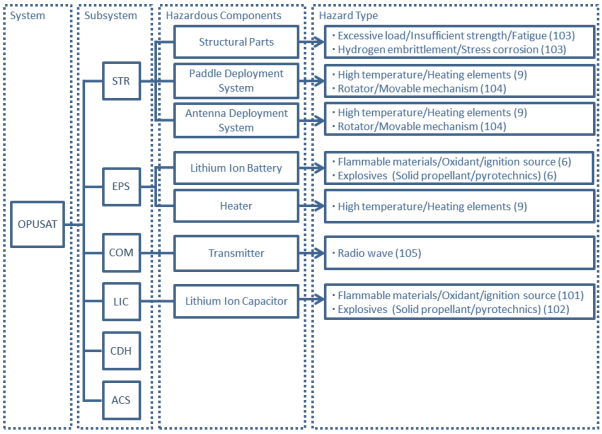


図 5. OPUSAT のハザード分析

ゴールに分割する．考えうるハザード原因として「不適切な構造材料の選定」,「設計欠陥による構造強度の不足」,「不十分な締め付けトルクによるボルトの緩み」などがあるため，図 6 のように，6 個のサブゴールに分割することができる．

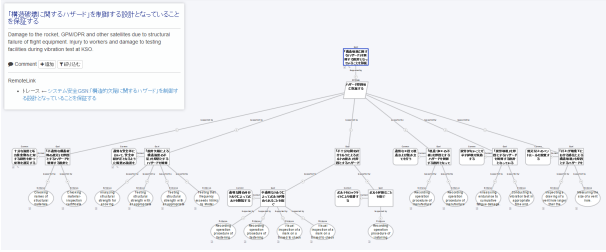


図 6. ハザードタイプ「構造破壊」を扱った GSN

「『設計欠陥による構造強度の不足』を原因とするハザードを制御する設計となっている」というゴールについては，十分に詳細化されたと判断し，図 7 のように，そのゴールが達成されている証拠と結びつける．通常のアシュアランスケースでは，証拠には，文章を書くことはせず，試験報告書などの参照する文書名のみを記載するが，本研究では検証方法をノードタイトルに記載するようにしている．例えば，図 8 のように「Analyzing structural strength for allowing positive margin of safety.」がタイトルに記載され，さらに (OPUSAT-SR033) “ structural_analysis ” なる文書へのリンクが，文書のステータス（OPEN/CLOSE）と共に参照されている．

また，特殊な使用方法として，前提ノードにハザード制御方法を記載している．例えば,「適切な安全率において，安全余裕が正となるように衛星

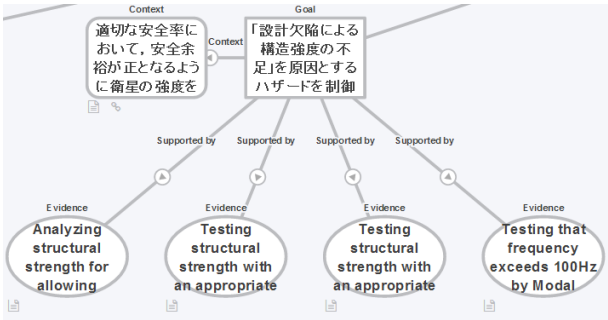


図 7. ハザード原因「設計欠陥による構造強度の不足」を扱った GSN

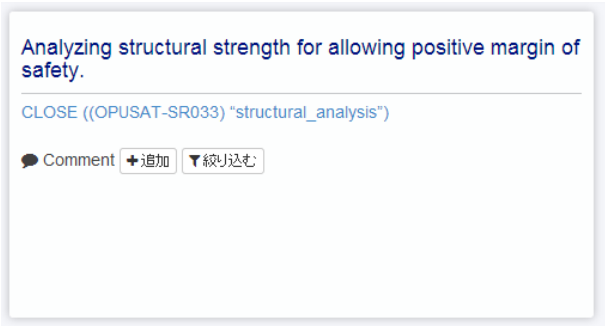


図 8. 証拠ノード「Analyzing...safety.」の詳細

の強度を設計する」なる文章が記載されている．まとめると，図 9 のような構造となっている．この構造は，超小型衛星のハザードレポートの文書構造をグラフィカルに表現したものである．アシュランスケースでは，ハザードレポートは文書で作成し，その構造を GSN で表現することはしない．しかし，後述の通り，本研究では GSN のノードと要求ノードと紐付け，トレーサビリティを向上させることを図るために，従来であればハザードレポートとして記述するものに関しても GSN で記述することとした．超小型人工衛星の電源サブシステムに対してアシュアランスケースを適用した Tanaka ら [16] の研究においても，図 9 に近い構造が見受けられる．

4.2.2. ハザードタイプ「回転体・可動機構」

前節と同様に，「『回転・可動機構に関するハザード』を制御する設計となっていることを保証する」というゴールを，「ハザード原因毎に保証する」という戦略の下，サブゴールに分割する．GSN の展開は前節と同様であるため詳しくは扱わず，本節では，要求図との関係について述べる．

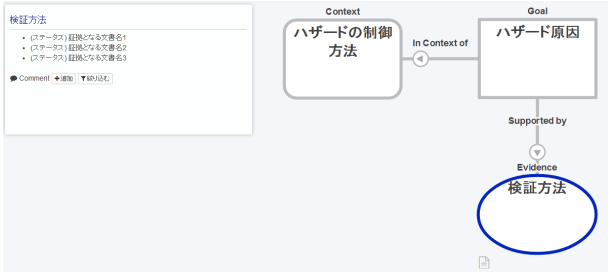


図 9. ハザードレポートの文書構造と GSN

「回転・可動機構に関するハザード」とは，より具体的には，「アンテナおよびパドルの意図せぬ展開に関するハザード」である．ハザード原因はいくつか存在するが，ここでは，「ニクロム線に誤って電力共有がされること」のみを扱う．このハザード原因を制御するために，OPUSAT では，「衛星の電源共有を遮断するインヒビットを直列に 3 つ設ける」という方法を採用した．ハザードレポートの構造は，図 10 のようになる．

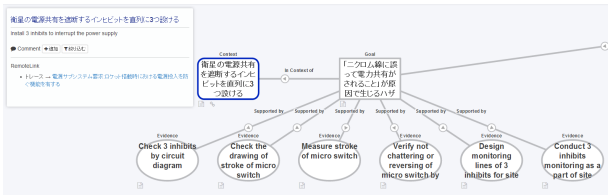


図 10. 意図せぬ電力供給の制御に関する GSN

前提ノードの詳細には，「電源サブシステム要求: ロケット搭載時における電源投入を防ぐ機能を有する」なる記述がある．これは，電源サブシステム要求を表す要求図のノードへ関連付けがされていることを表現している．リンク先を辿ると，図 11 に示した要求図へ移動する．図 11 は，電源サブシステムの要求を表した図 12 の一部である．一連の流れは，「アンテナおよびパドルの意図せぬ展開」というハザードを制御するために，「ロケット搭載時における電源投入を防ぐ機能を有する」なる機能要求が存在していることを表している．この機能要求から「ロケット搭載時に太陽光を遮断する」や「キルスイッチを有する」などの要求が導出され，最終的にはシステムを構成するブロックへと紐付く．すなわち，GSN と SysML の要求図を併用することにより，ハザード識別からシステム構成に至るまでのトレーサビリティを確保することができる．

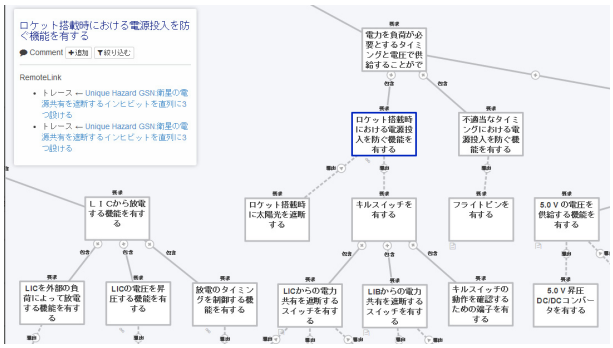


図 11. OPUSAT の電源サブシステム要求（一部）

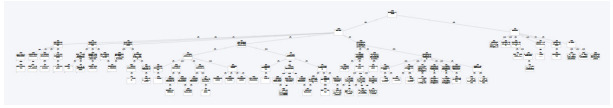


図 12. OPUSAT の電源サブシステム要求（全体）

システム安全を担当するエンジニアと個々のサブシステムを担当するエンジニアは異なることが多く，安全に関する議論と複雑に絡み合ったシステム要求の間で整合性を維持するのは，大変な労力を必要とするものであった．OPUSAT においても，例外ではなく，多くの労力と時間を費やした．本研究で提案する手法では，WEB アプリケーションが管理する単一のリポジトリに，安全に関する議論とシステム要求を記述することができることに加え，個々のノードをリンクによって紐付けることができる．これにより，トレーサビリティが格段に向上し，整合性の確保が容易になる．

5. 結言

超小型衛星の安全要求について，アシュアランスケースで用いられるゴール指向分析により議論を可視化・構造化する手法を述べた．GSN と要求図をトレーサブルにすることで，開発項目の漏れと無駄を防ぐことができる可能性を示した．今後は，安全審査の体系を可視化することで，問題点を洗い出し，超小型衛星に適したものへ改善できるよう働きかけていきたいと考えている．また，スマート構造の実利用化を鑑み，スマート構造を有するシステムのディペンダビリティに関する研究への発展を目指す．

謝辞

本研究遂行に当たって多大な御協力を頂いた OPUSAT 開発チームおよび BALUS 開発チームに感謝の意を表する．

参考文献

1) ISO 26262, Road Vehicles Functional Safety, 2011.
2) Railtrack, Engineering Safety Management Issue 3, Yellow Book 3, Volume 1 and 3, Fundamentals and Guidance, 2000.
3) European Air Traffic Management, Safety Case Development Manual, European Organisation For the Safety of Air Navigation, Ed. 2.2, Nov 2006.
4) Ministry of Defence, Defence Standard 00-56, Issue 4 Publication Date 01, June 2007.
5) Cullen, The Hon. Lord., 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, 1990.
6) ISO/IEC 15026-2:2011, Systems and Software Engineering Systems and Software Assurance - Part 2: Assurance case, 2011
7) T. Kelly, Arguing Safety-A Systematic Approach to Managing Safety Cases, Ph.D Thesis, University of York, 1998.
8) D. Jackson, M. Thomas, L.I. Millett, Software for Dependable Systems - Sufficient Evidence, The National Academies Press, Washington D.C., 2007.
9) 松野 裕, 山本 修一郎, 高井 利憲, D-Case 入門 ～ディペンダビリティ・ケースを書いてみよう！～, ダイテックホールディング, 2012
10) SE Handbook Working Group. Systems engineering handbook - a guide for system life cycle processes and activities, International Council on Systems Engineering, INCOSE-TP-2003-002-03.2.1, 2011.
11) S. Friedenthal, A. Moore, R. Steiner, システムズモデリング言語 SysML, 東京電機大学出版局, 2012.
12) 山本 修一郎, SysML 要求図を GSN と比較する, ビジネスコミュニケーション, Vol. 49, No. 7, pp. 100-104, 2012.
13) 大塚 弘記, GitHub 実践入門 Pull Request による開発の変革, 技術評論社, 2014.
14) 南部 陽介, 三浦 政司, 吉澤 良典, 萩原 利士成, 弓山 彬, 五十嵐 智, 超小型衛星の技術共有と分散型共同開発のためのコラボレーションツールの研究開発, 宇宙科学技術連合講演会講演集 58, 2A01, 2014.
15) 南部 陽介, 超小型衛星 OPUSAT「こすもず」の概要と初期運用結果, 信学技報, Vol. 114, No. 87, pp. 5-10, 2014.
16) K. Tanaka, Y. Matsuno, Y. Nakabo, S. Shirasaka, S. Nakasuka, Toward strategic development of hodoyoshi microsatellite using assurance cases, In Proc. of International Astronautical Federation (IAC2012), 2012.