levii

第12回D-Case研究会

システムモデリングツールを用いた超小型衛星のシステム安全に関する知見の整理と共有

大阪府立大学 工学研究科

南部 陽介

出典：トヨタ自動車（株）

プリウス
（約1700 kg）

出典：三菱電機（株）

ひまわり8号
（約3500 kg）

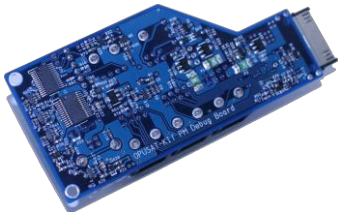
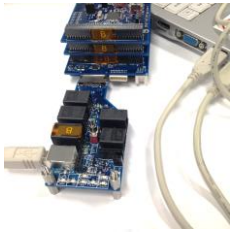
小型バス
（約7000 kg）

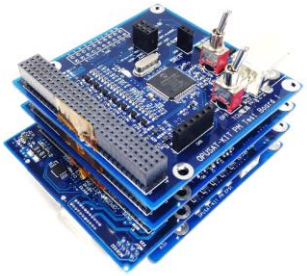
通常の衛星のサイズ感

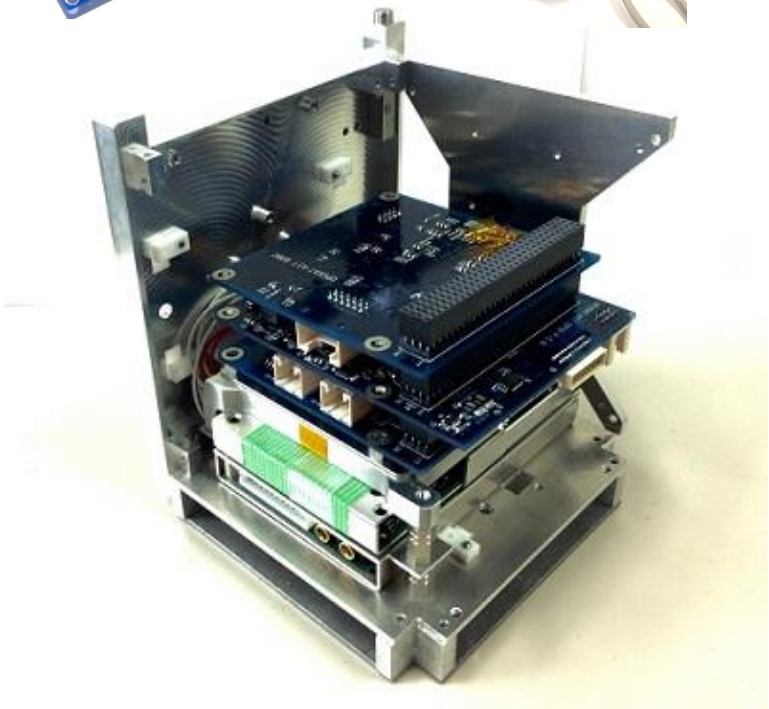
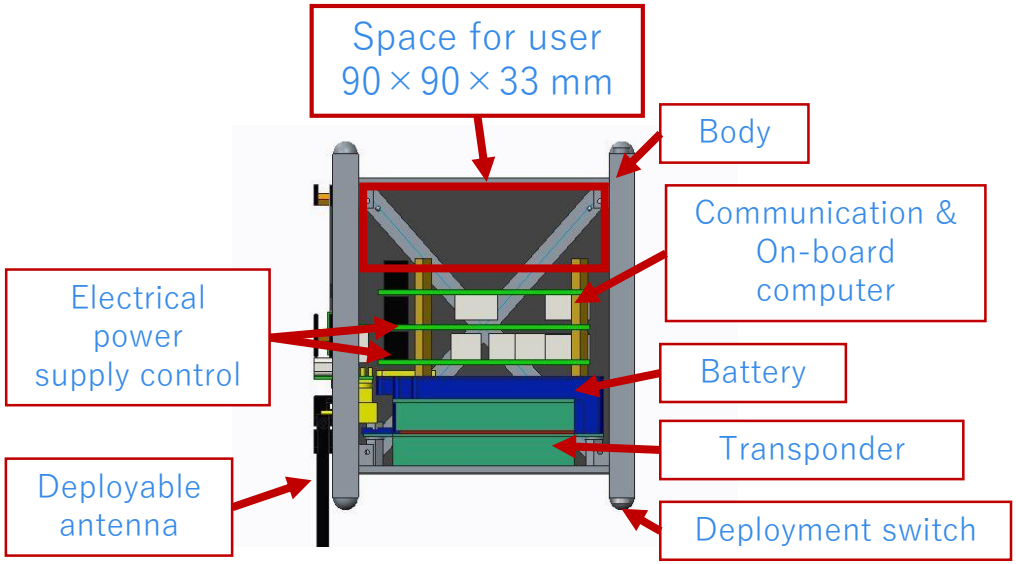
超小型衛星OPUSAT「CosMoz」

世界中の大学生が人工衛星を作る時代

OPUSATは、２０１４年２月にH-IIAロケット23号機で打ち上げられた。このサイズで世界で初めてとなる太陽指向制御を実現。リチウムイオンキャパシタを用いた衛星電源サブシステムも世界で初めての試み。

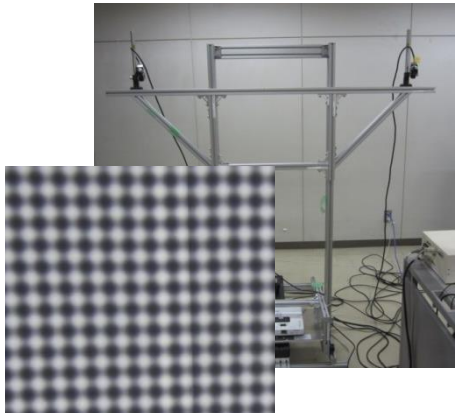





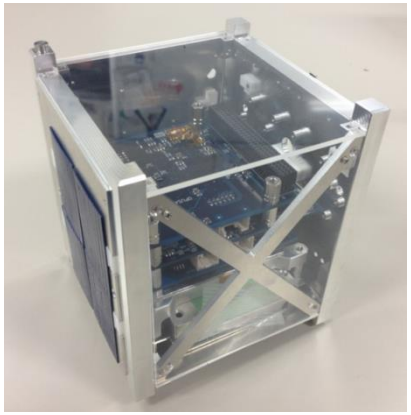



CubeSat用標準バスOPUSAT-KIT

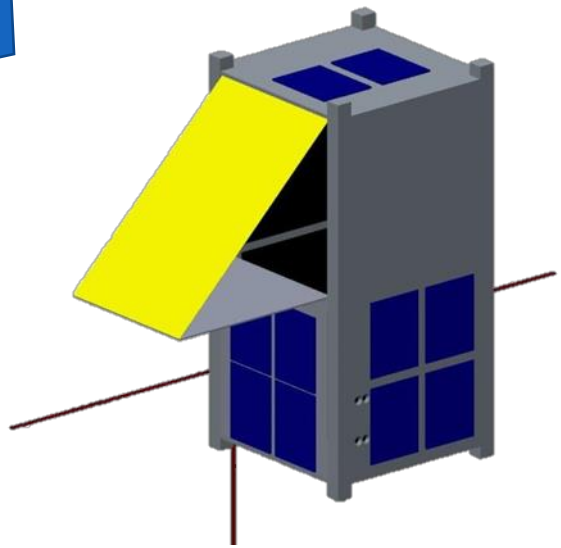
はじめてCubeSatを作る人がミッション部開発に集中できるように…
株式会社ニッシンとの共同開発



高精度計測システム

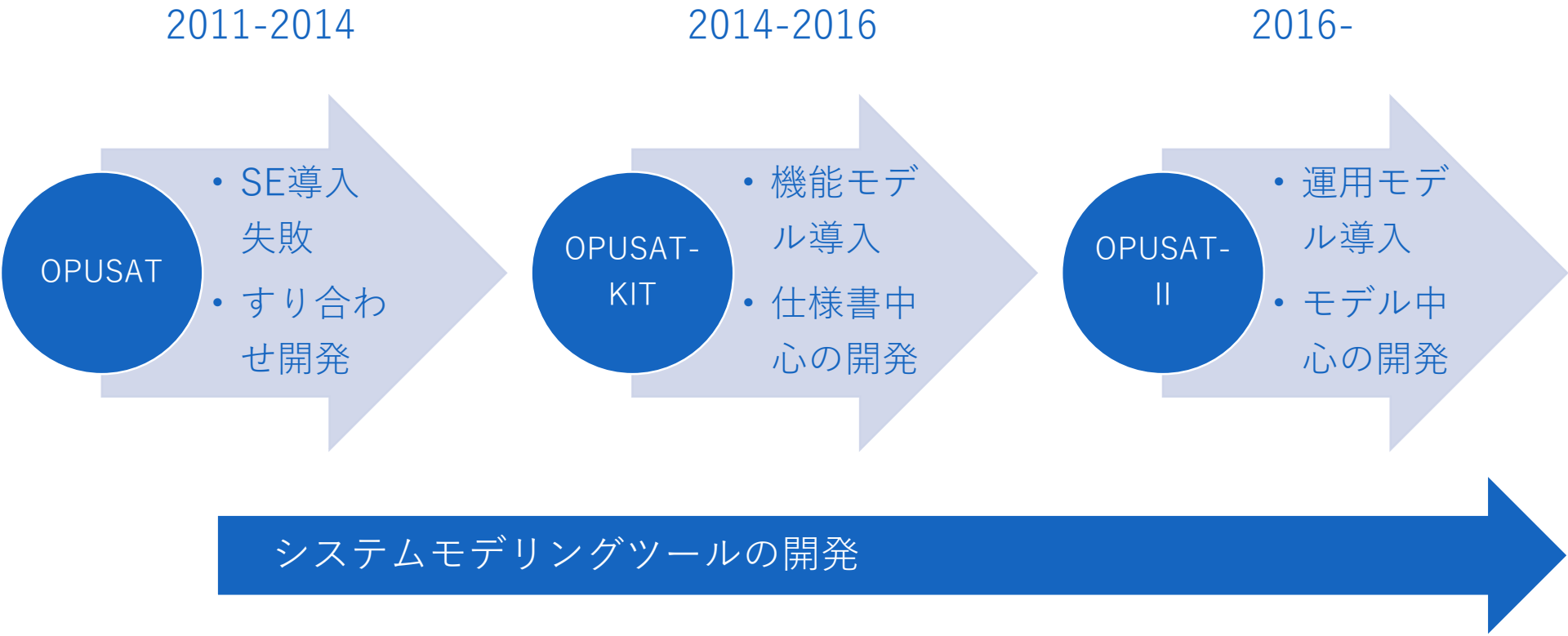


標準バスシステム



超小型衛星OPUSAT-II

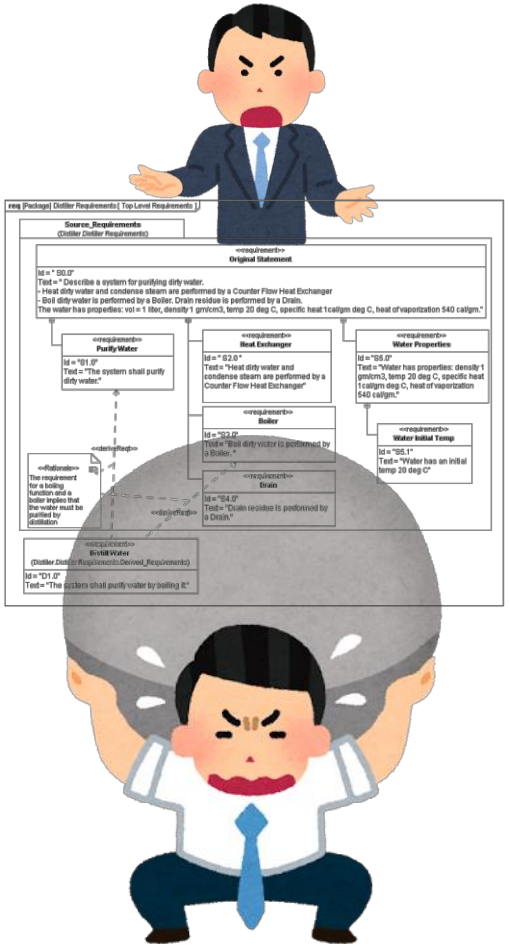
軌道上で構造物の形状を計測する．摂南大 岸本准教授，室蘭工大 樋口教授・勝又助教，鳥取大 岩佐准教授，福井大 藤垣教授，千葉工大 秋田准教授のご協力の元，「板ミウラ折り展開構造×平面度の測定」を軸にコンセプト検討中．



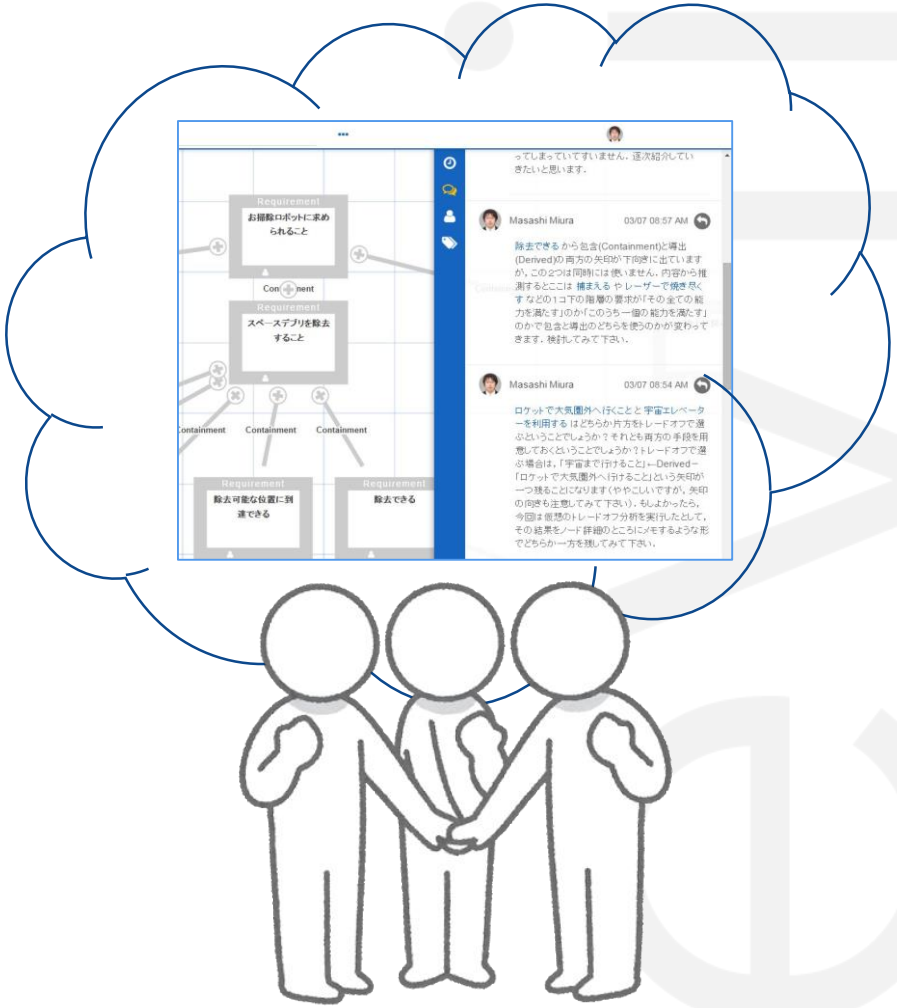
MBSE導入とモデリングツール開発の遍歴

最初の人工衛星OPUSATでは、文書ベースのSEのトレーニングを受けて導入を試みたが敢えなく失敗。OPUSAT-KITでは、技術継承の必要性から機能モデル・仕様書中心の開発に移行。効率化のため最近ではシステムモデル中心に変わってきている。なお、現在のメンバーは、学部1回生の頃からモデリングツールでシステム思考を学んできている。

トップダウンではなくコラボレーション



従来のモデリングツール



私達のモデリングツール

コラボレーティブ モデリング

OPUSAT-IIにおける MBSE導入の目的は何か

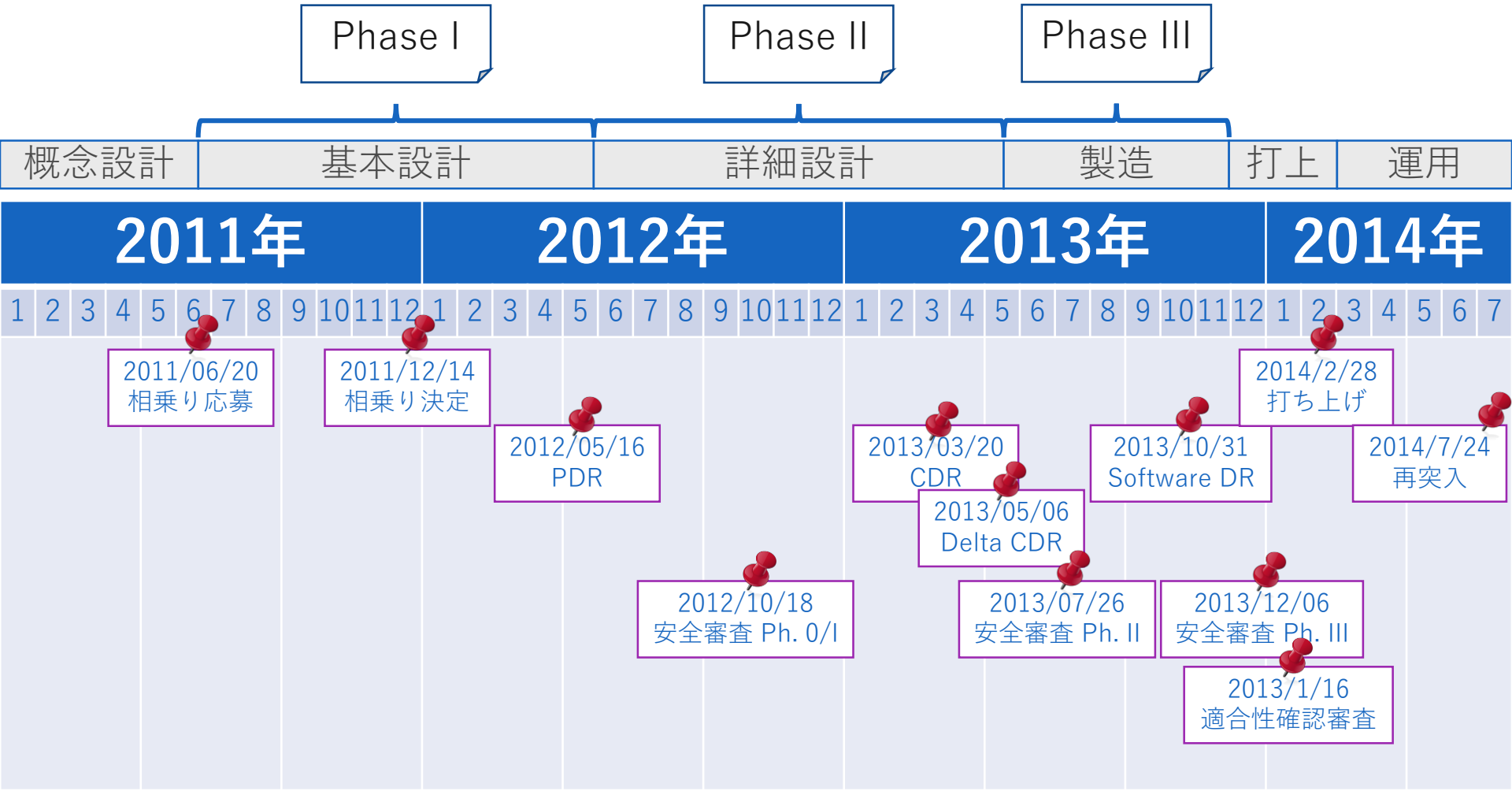
目的

- 開発スケジュールの遅延を防ぐ
  - ２０１８年度打ち上げという目標を達成するため
- 品質の向上
  - ふたつにひとつの大学衛星は宇宙で動かない.
  - 統合試験が肝であることはわかっている.
  - 統合試験の質と速度を高めたい.
- コスト削減
  - 安全審査を優位に進めることが，コスト削減に直結する.
  - 衛星が安全であることを系統的に説明できないと，NASAやJAXAから次々と過保護な機能を追加される.
  - 結果としてコストとスケジュールを圧迫し，本当に宇宙でやりたいことができなくなってしまう.

課題の深掘り

- スケジュールの遅延は，次の２点が主な原因
  - 経験のないものを新規開発する際には，作りながら仕様が変化する．初期段階では十分に仕様を詳細化できずに，あとになって仕様を詳細化すると，この仕様では実現不可能だったことに気がつく．
  - 衛星が実現するべきことに漏れがあり，全体に影響をおよぼすような機能追加が行われる．（OPUSAT-KITは，当初OPUSATそのもののはずだったが，スポンサーからの要望で，その後ユーザーが使いやすいようにソフトウェアを一新したり，開発支援などの機能が加わり，プロジェクトの期間が１年から２年に伸びた．）
- OPUSATの統合試験で苦労したのは，仕様がきちんと明文化されていなかったので，いま目の前にある衛星の仕様がどうなっているのかを試験担当者が把握するところ．
- OPUSATの安全審査では，NASAやJAXAのプロジェクトの進め方，「故障許容設計」や「リスク最小化設計」などNASAやJAXAの設計思想，「安全を保証する」ためのロジックを理解するのが大変だった．形式的に勧めているにもかかわらず，「全体像が見えない」と感じた．

超小型衛星の
安全審査について



超小型衛星OPUSATのライフサイクル

PDRやCDRはディシジョンゲートとしてではなく，経験者からのアドバイスを頂く場となっていた．安全審査がゲートとしての機能を持っていた．

衛星システムの「安全」とは

ハザードが事故等に至らないように，除去，最小化又は制御されている状態．即ち，リスクが許容できるレベルまで低い状態．

ハザード：事故をもたらす要因が顕在又は潜在する状態をいう

リスク：被害の期待値．即ち，ハザードで識別した安全の度合いを，予想される「被害の度合い」と「発生の可能性」で表したもの

（出典：宇宙航空研究開発機構，JMR-001B システム安全標準）

衛星の「システム安全」とは

プロジェクト等の事業遂行に関する計画立案から整備，運用・実施，撤収に至るシステムのライフサイクルの前段階を通じて，運用効果，スケジュール，及びコストへの配慮の下に安全を最適化し，事故等のリスクを合理的に可能な限り小さくするため，工学及び管理の原理，基準及び手法を用いること.

（出典：宇宙航空研究開発機構，JMR-001B システム安全標準）

システム安全のアプローチ

これまでの知見・経験を基づいた安全設計要求に従って衛星を設計する.

可能性のある故障を想定して，システム全体での評価を行い衛星を設計する.

ハザード解析

ハザードとその原因を識別する

ハザードの除去・制御方法を決定する

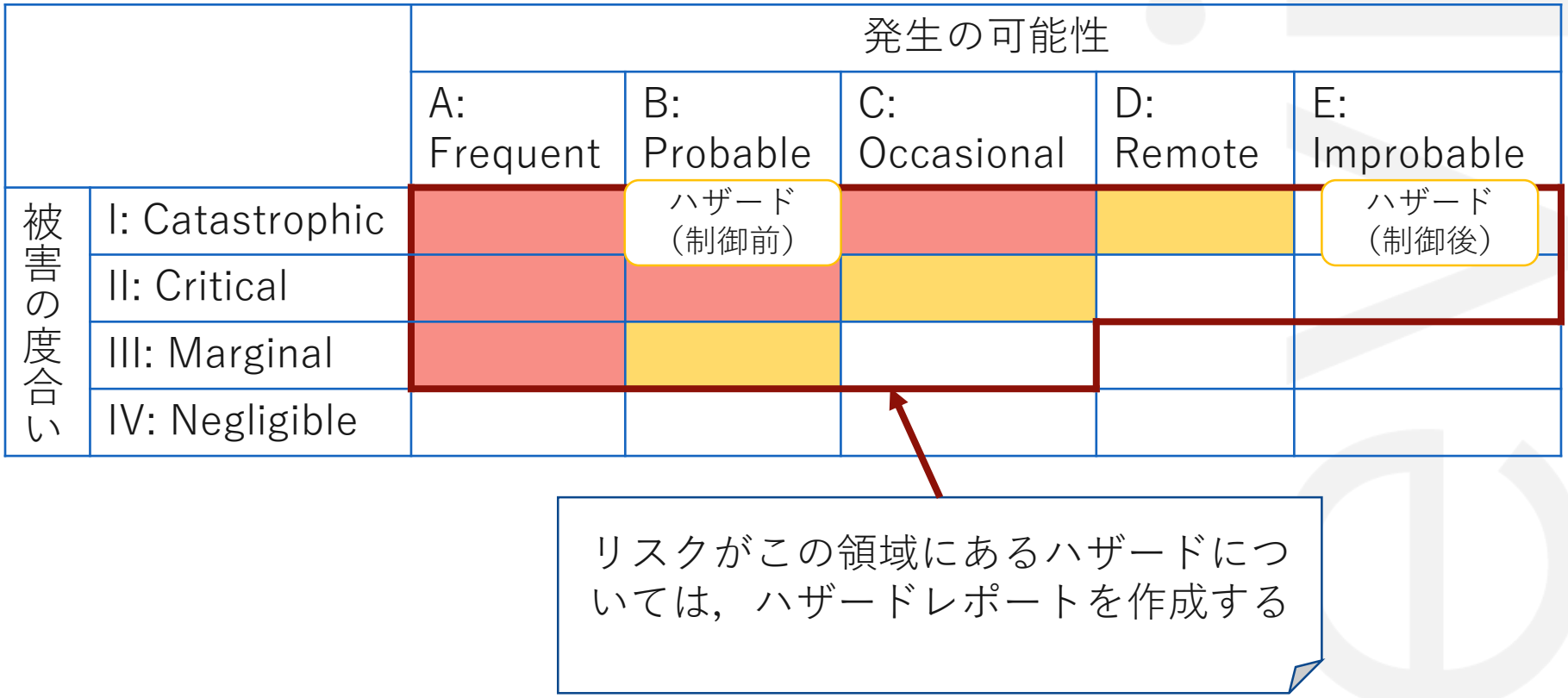
ハザードを除去・制御する

ハザード制御の有効性を検証する

ハザードの識別

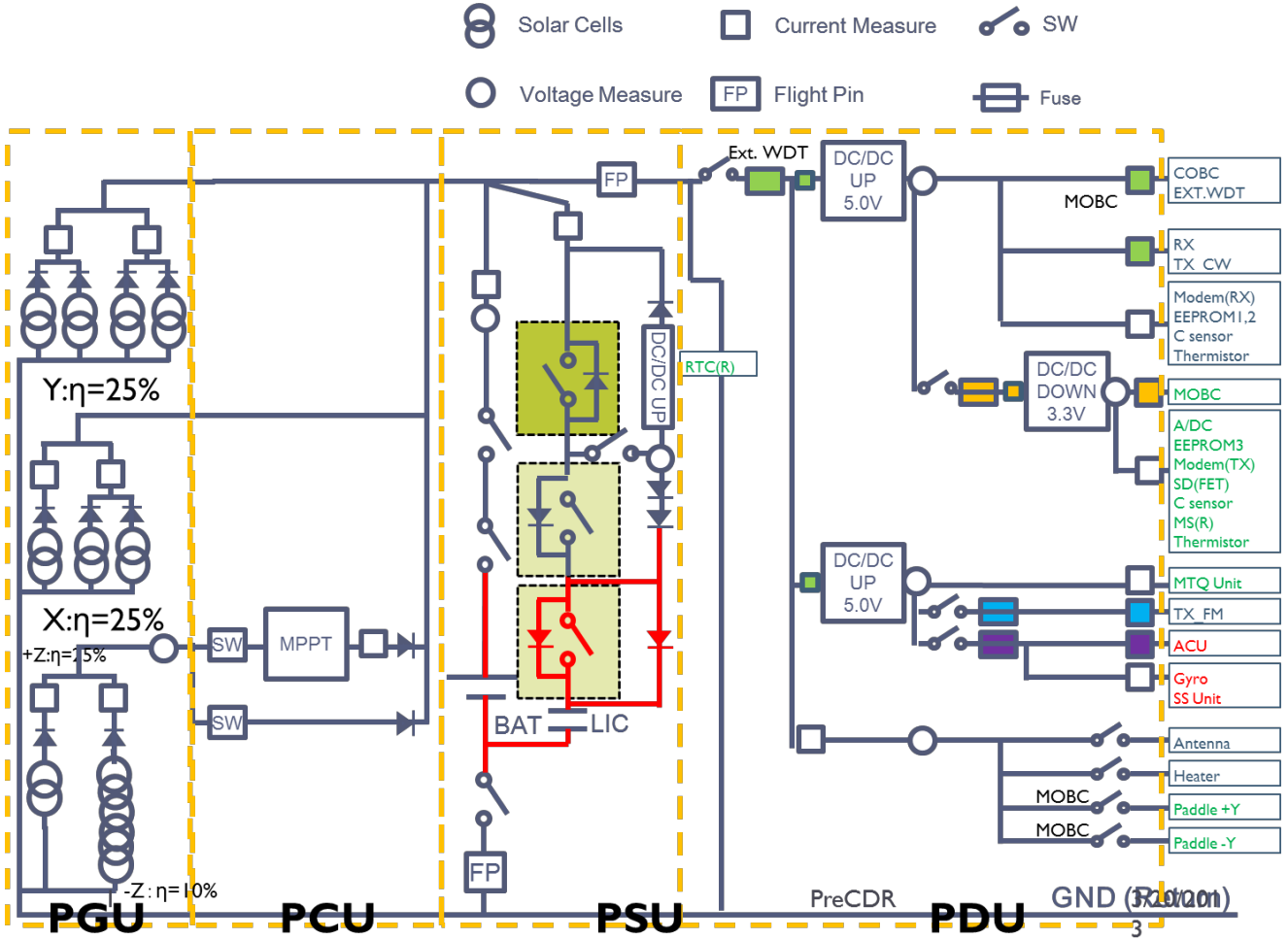
- ハザードを起こすエネルギー源に着目し，想定外のエネルギーの流れが起きた場合に，起こりうる事象を最悪ケースで想定する
- 識別対象のハザード
  - 作業員を怪我や死亡に至らせるもの
  - ロケット，相乗り衛星，地上装置，射場設備へのダメージ
- ハザードの深刻さによって，カタストロフィックハザード，クリティカルハザード，マージナルハザード

発生の可能性を下げて白の領域に入るようにハザードを制御する



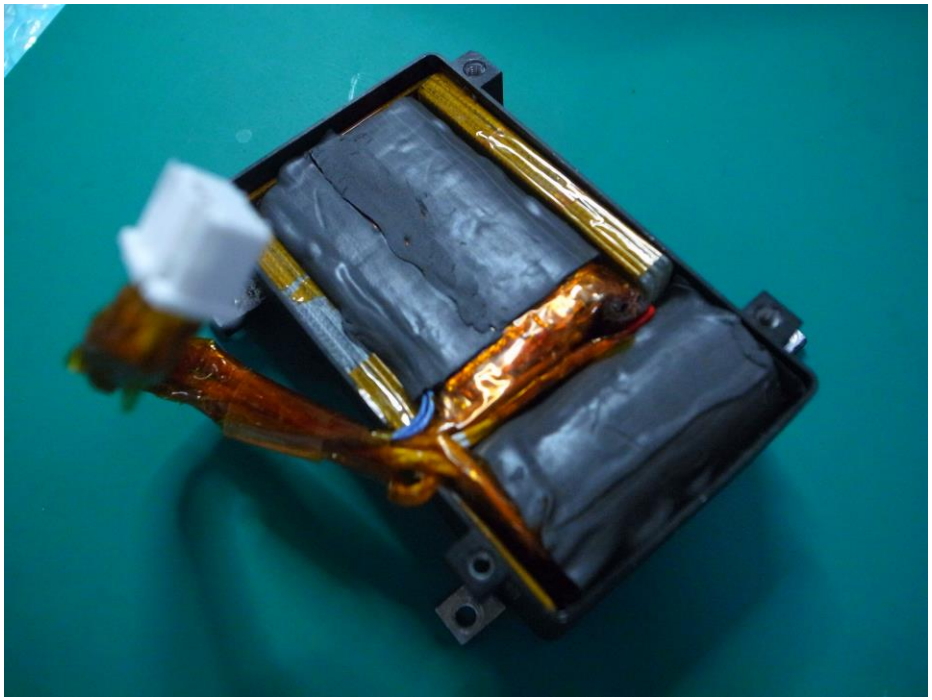
ハザード制御方法

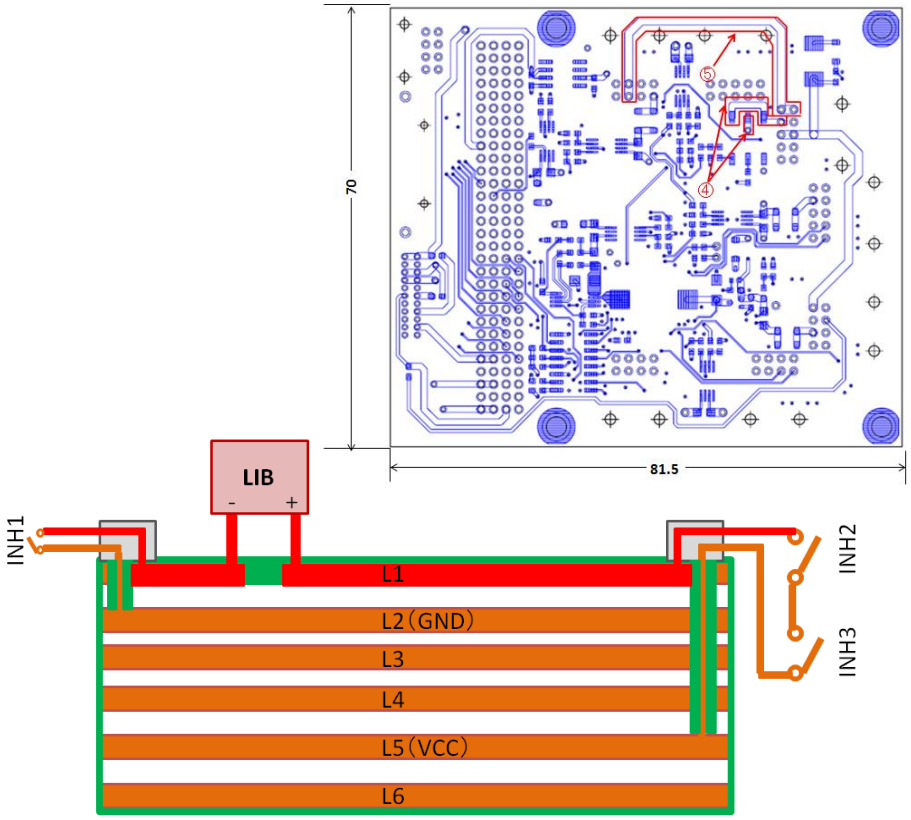
- 基本は故障許容設計により制御
- それが非現実的でない場合はリスク最小化設計



故障許容設計の例

キルスイッチが2つ故障しても衛星の電源がはいることはない





バッテリと機械スイッチの間は
すべて二重に絶縁とする

リスク最小化設計の例

これだけやっておけば，まぁ大丈夫だという落とし所

二重に絶縁しておけば，ショートは想定できない

安全審査のフェーズ

- Phase 0/I : 小型衛星とGSEの基本設計が安全要求を満足すると共に、射場のシナリオが安全要求を満足し、ハザード解析結果が問題ない（ハザードの除去、最小化、又は制御の手段が適切に設定されている）ことが要求される
- Phase II:フェーズ I の安全審査で示されなかった小型衛星／GSE インタフェース、射場作業、手順及びその実施時期についてのハザードの評価が追加され、審査される
- Phase III:ペイロード等の最終的な設計、製造結果及び射場作業が本標準の安全要求を満足し最終的なハザード解析結果が問題なく、安全検証が完了していることを審査すること。

実際にやること

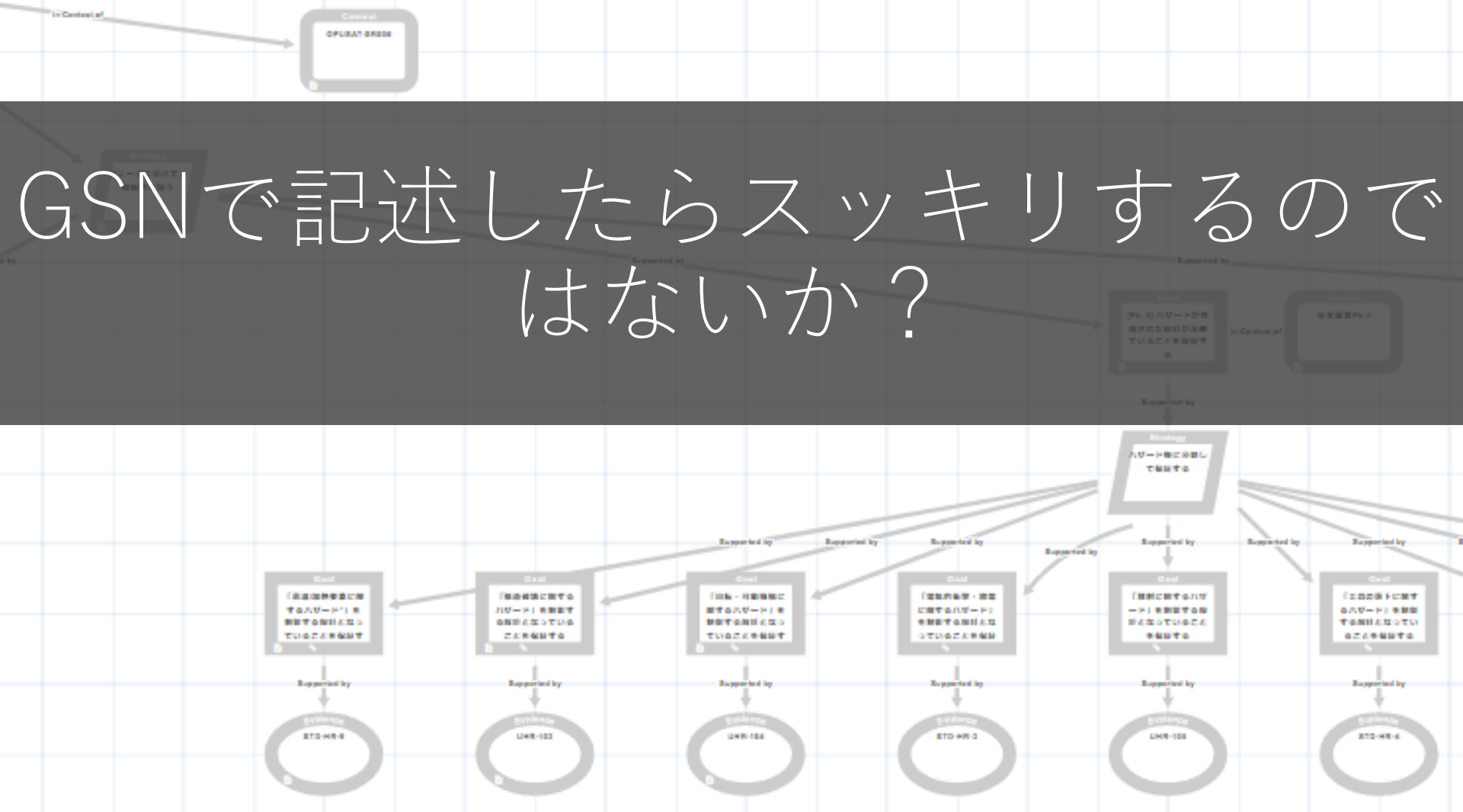
1. ハザートを見つける
2. ハザードの原因を洗い出す
3. ハザードの制御方法を決める
4. ハザード制御の検証方法を決める
5. 上記をハザードレポートに記述する
6. 検証する
7. 検証結果と共にハザードレポート最終版を提出する

安全審査 Ph.0/Iで機能設計レベルの合意を取る．安全審査 Ph.IIで物理設計レベルの合意を取る．

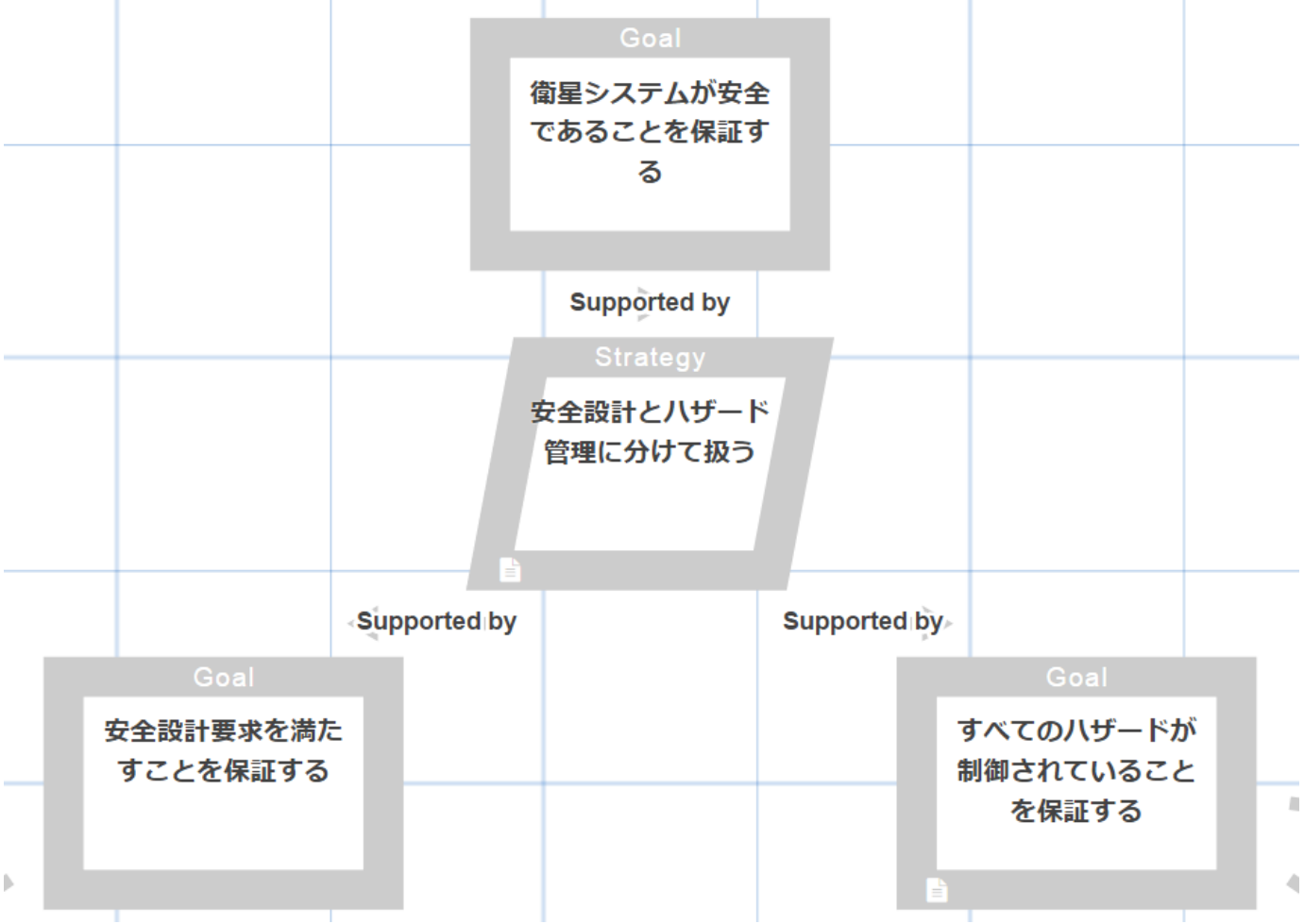
安全審査 Ph.IIIで検証結果に対する評価（当該ハザードが制御されていること）の合意を取る．

アプローチが2つあったり，
聞き慣れない言葉や概念が出
てきて当初は混乱しました

GSNで記述したらスッキリするのではないか？

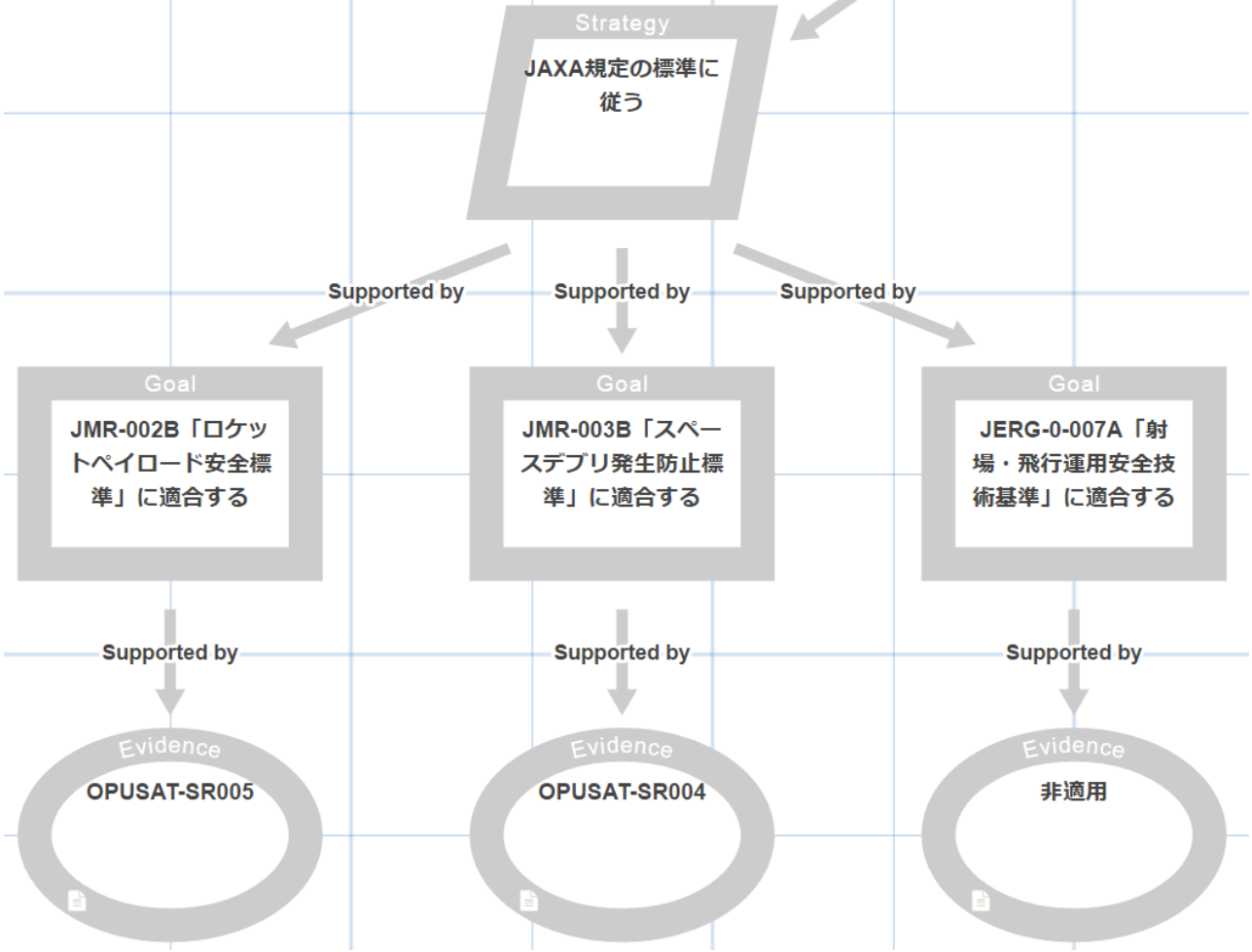


自作のシステムモデリング
ツールを利用してGSNを描い
てみることにしました



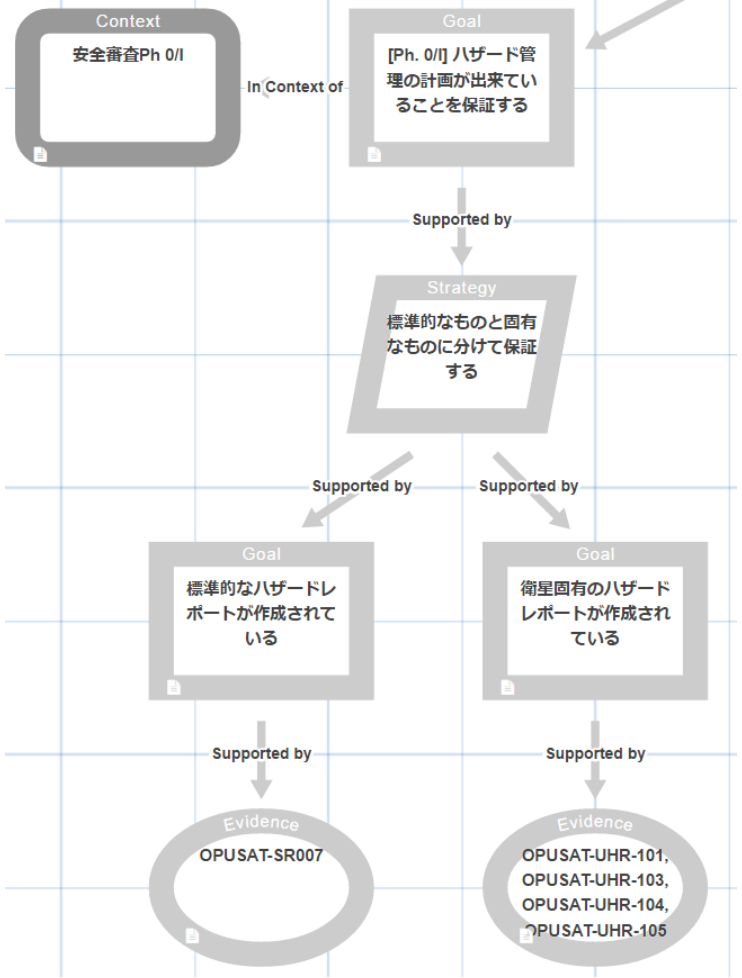
一番上位のゴールとサブゴール

はじめて超小型衛星を作る人達は，この分割が「重要である」という認識がない

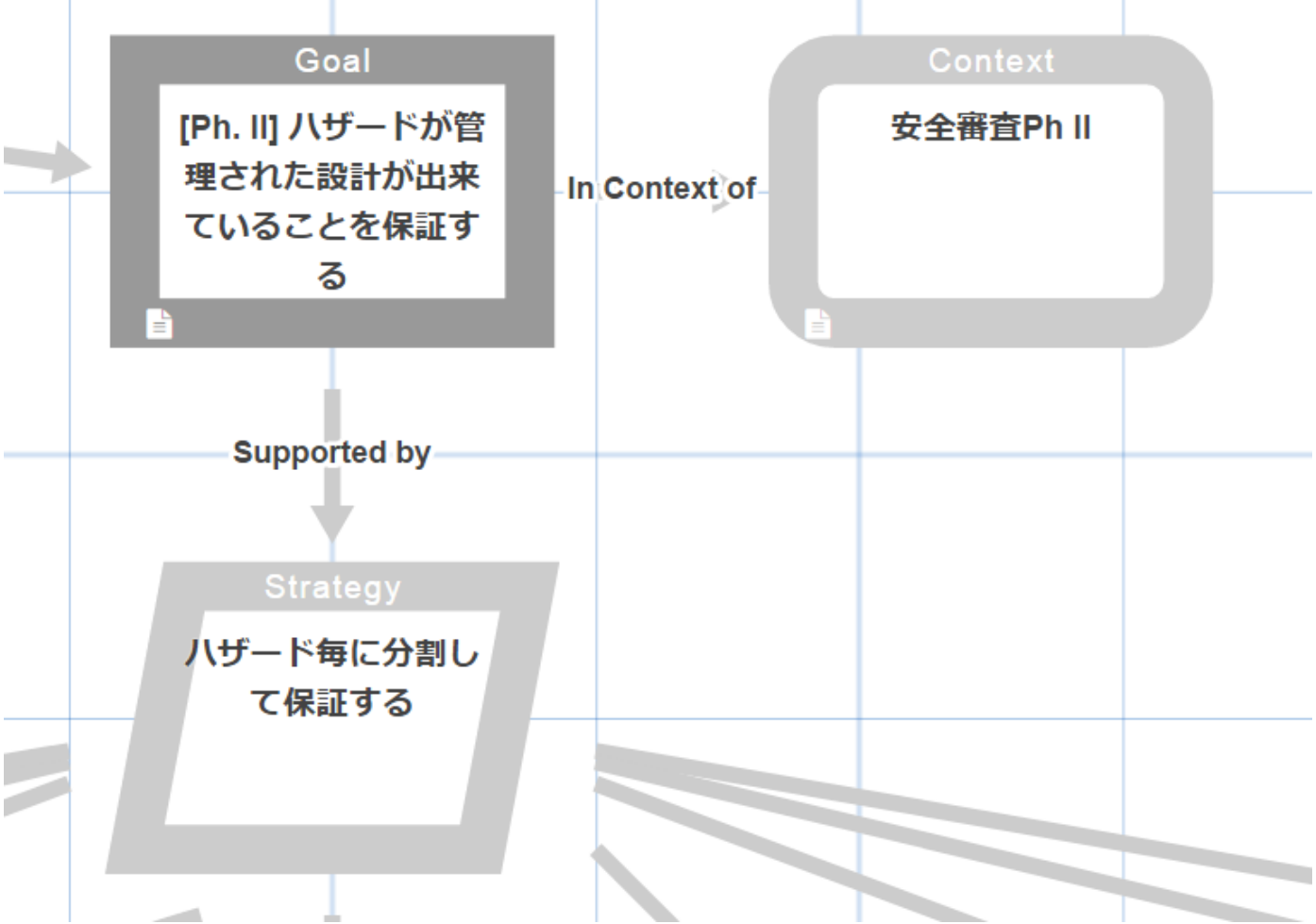


安全設計要求を満たすことを保証するために

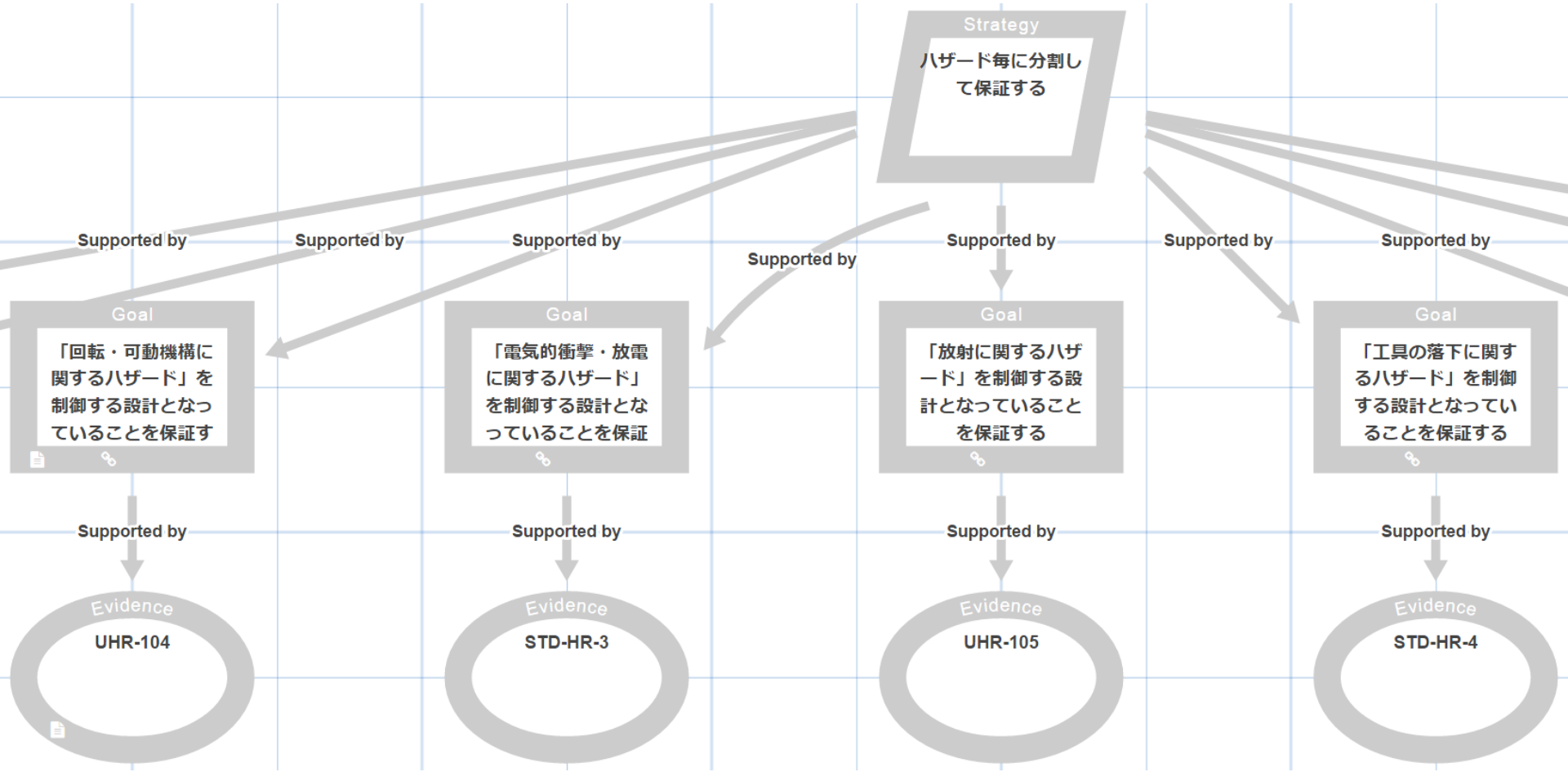
親切なJAXAさんが標準への適合マトリクスを用意してくれている



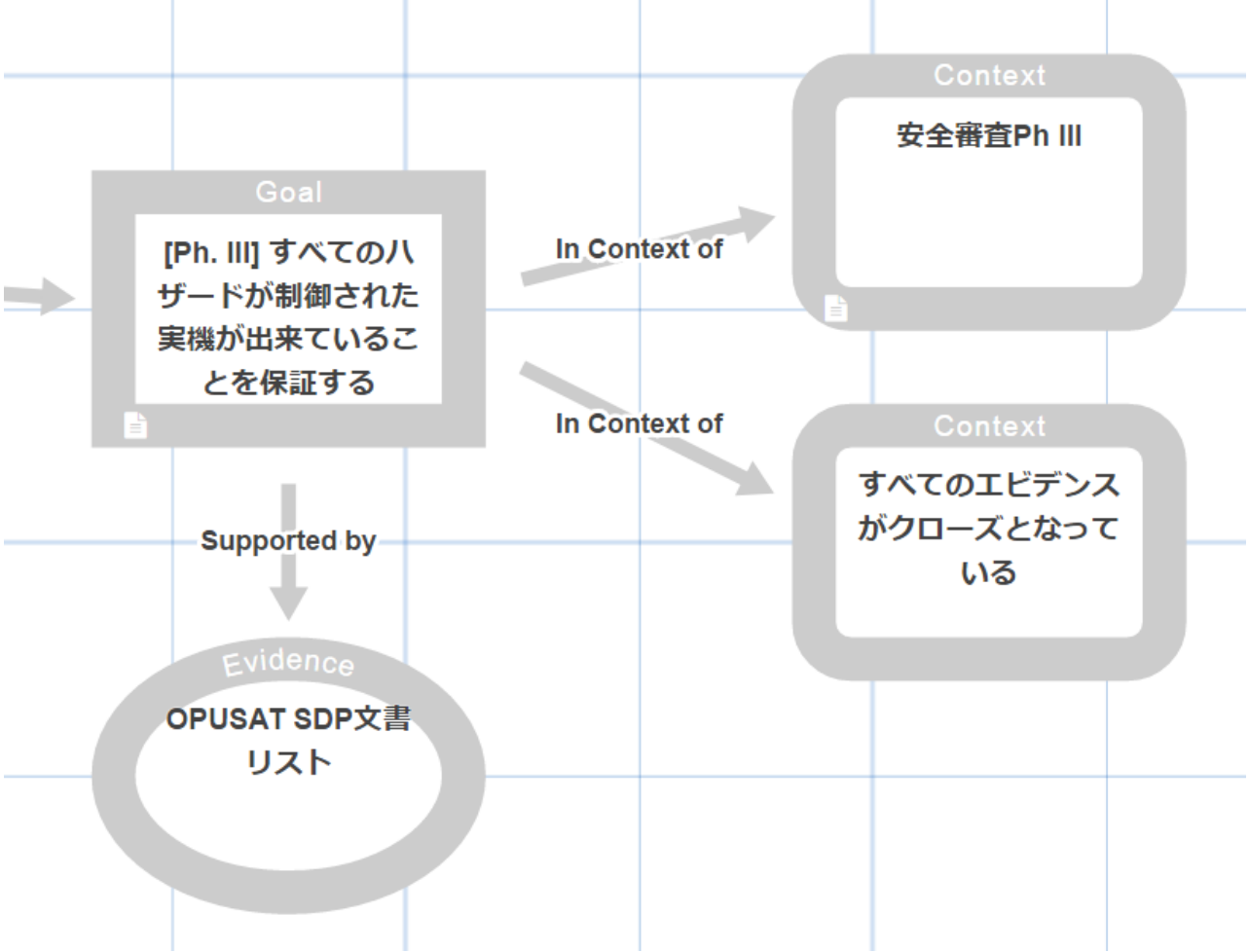
すべてのハザードが制御されていることを保証するために，ハザード管理計画を審査する



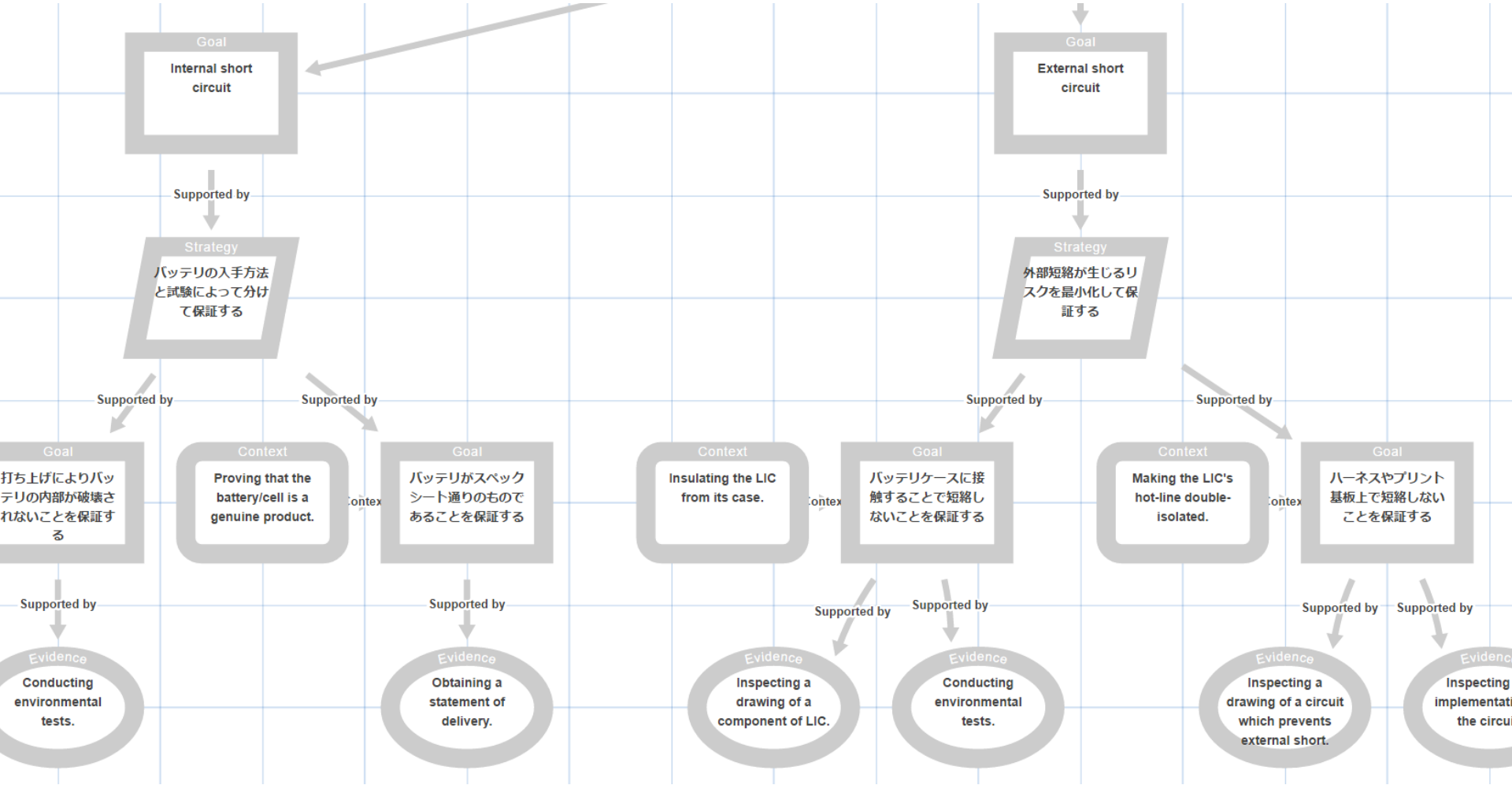
すべてのハザードが制御されていることを保証するために，適切な設計かを審査する



設計はハザード毎に審査する



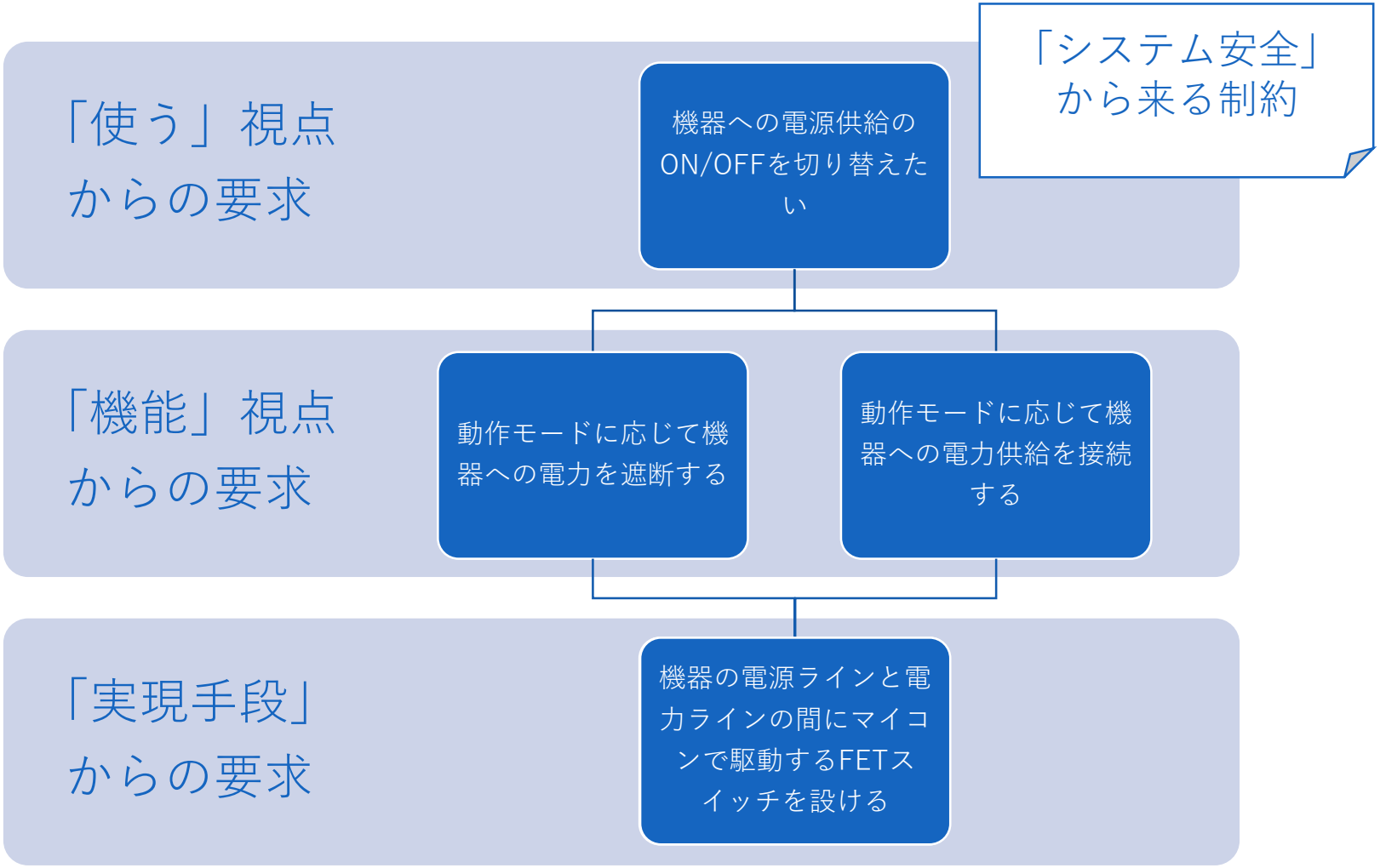
すべてのハザードが制御されていることを保証するために，実機を審査する



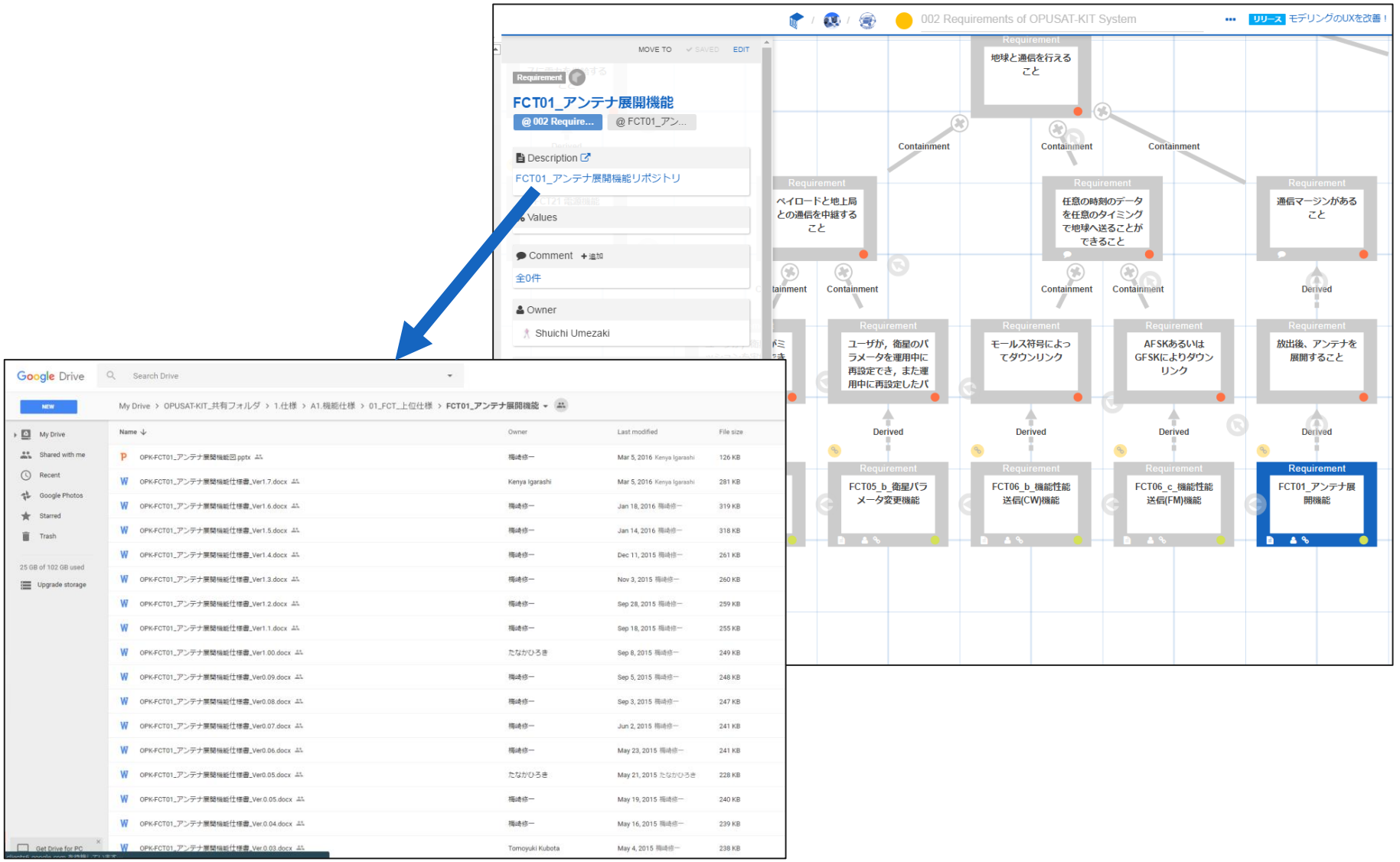
試しにハザードレポートをGSN化しましたが やりすぎた感があります

システムモデリングツールで GSNを描く利点は何か？

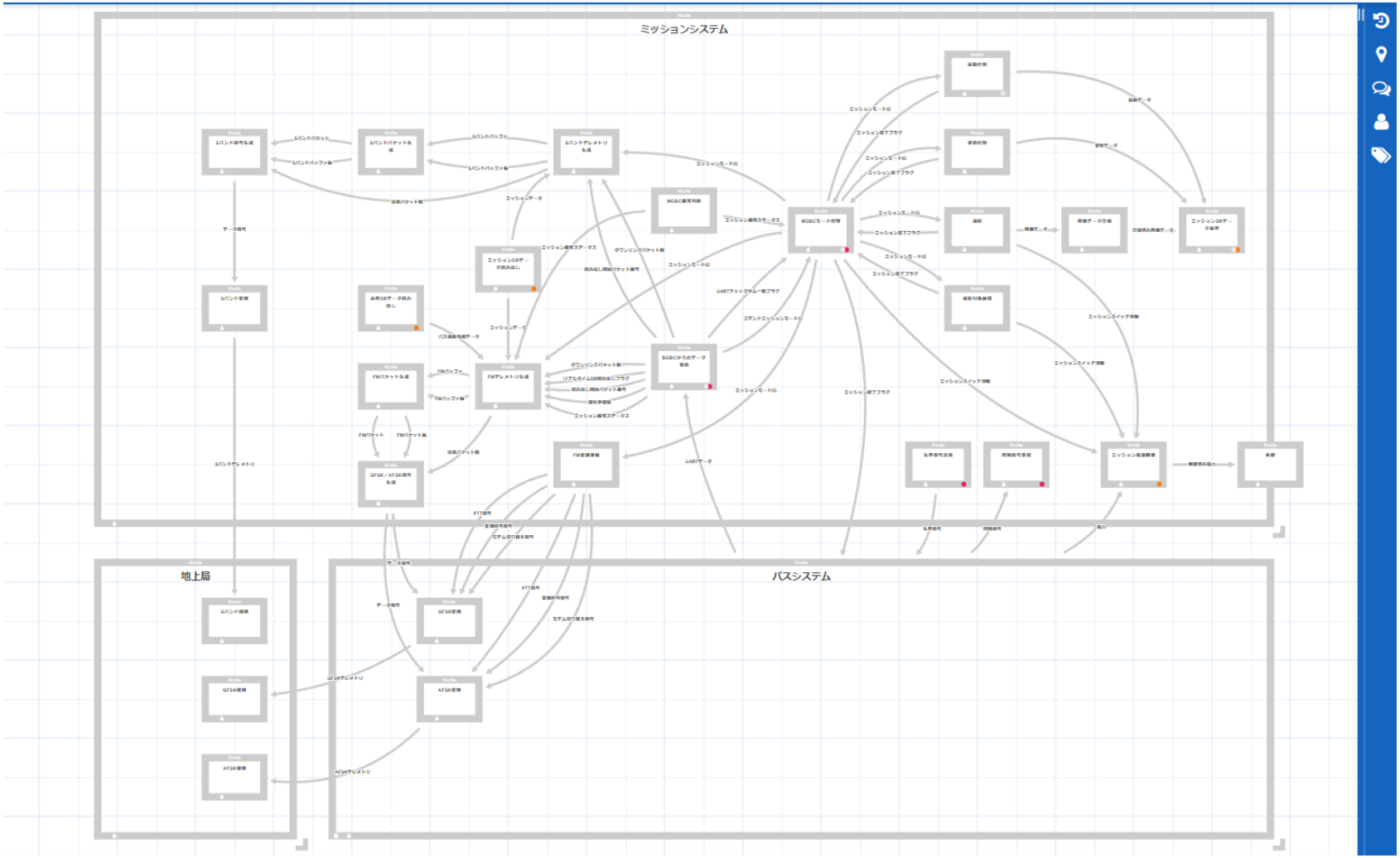
機能モデルとシステム安全からの要求を紐付けることができる



衛星の機能モデルをモデリングツールで作成している．各機能が満たすべき仕様や要求の中に，ハザード制御も含まれてくる．



機能ノードと仕様書リポジトリがリンク



インターフェイスの管理をモデルで行う

システム安全 GSN
＋
機能モデル
＋
ロジカルアーキテクチャ

責任範囲と根拠が明確になり
現場が動きやすくなる

モデリングの価値

- IPO図や仕様をきちんと作成・管理しているため，下級生を開発に割り当てやすくなった．能力の高い上回生が難易度の高い開発にリソースを避けるようになるため，全体としての開発力が向上した．
- GSNで全体像を把握した上で，システム担当者と電子回路設計者が共通の言葉（論理モデル・物理モデルなど回路図手前）で議論することによって，相互の理解が深まり，質の高い電子回路を設計できた．（企業と大学のやり取りも運用モデルを通じて行うことで円滑にすすめることができた）
- 統合試験前のドタバタが明らかに減った．
- メンバーの関係がギクシャクしないままプロジェクトを終了することができ，次につなげることができた．

まとめ

- 超小型衛星を作っていく上で，システム安全の全体像が把握しづらいという課題に直面した
- GSNを用いて，システム安全を可視化した
  - 達成したい目標が明確化された
  - 個々の文書の位置付けが明確化された
- 機能モデルやロジカルモデルと紐付けて，現場への責任移譲や認識共有を円滑に行えるようにした

ご清聴ありがとうございました