リスクシナリオに繋がるコンテキスト情報を抽出する レビューメタモデルの提案

Review Meta Model to Identify Contexts Leading to Risk Scenarios

国立研究開発法人　宇宙航空研究開発機構　研究開発部門　第三研究ユニット
Japan Aerospace Exploration Agency, Research and Development Directorate, Research Unit III
○梅田　浩貴　　波平　晃佑[1)]　　植田　泰士[1)]　片平　真史[1)]　　森崎　修司[2)]
○Hiroki Umeda　Kohsuke Namihira[1)]　Yasushi Ueda[1)]　Masafumi Katahira[1)]　Shuji Morisaki[2)]

Abstract To ensure the software, it is important to consider the assumption (context) for use of system and software at the design phase. To prevent unexpected circumstances, software engineers need not only develop software to the exact specifications but also continue to identify risk scenarios in the context at the design phase as well. However, in the cyber physical systems such as spacecraft systems, there are difficulties in identifying the context: high uniqueness for each system and the chain of many assumptions and constraints. We proposed an analysis and a review method for identifying risk scenarios using three views focused on the context.

1. はじめに

ソフトウェア（以下、SW という）をシステムの目的に対して保証するためには、システム稼働後の利用や運用状況などの前提（以下、コンテキストという）を設計やレビュー時に考慮することが重要となる。特に、ソフトウェアの振る舞いがシステムの利用や運用へ致命的な影響を与える、クリティカルソフトウェアでは、コンテキストの考慮漏れは、リスクシナリオの検討漏れとなり、損失が大きい事故につながり得る。一方、従来の宇宙機システムのプロダクトや開発プロセス等の特性から、コンテキストの抽出や伝達において、以下の難しさが存在する。

プロダクト上の特性として、プロダクト毎のミッションの固有性が高いことからシステム毎にコンテキストの差異が大きい。加えて、同一のプロダクトを製造する機会が限られているため、機能を固定してアップデートを図りながら、利用運用中にコンテキスト情報を収集し反映する難易度が高い。

開発プロセス上の特性として、大規模且つ多組織であるため、システムエンジニアリングプロセス[1]に基づき、システム、サブシステム、コンポーネントと階層毎に多重の V 字モデル開発を行っている。そのため、組織間や工程を超えたコンテキスト情報の伝達難易度は高くなっている。

設計手法の特性として、解析及びモデリング中心で設計される。ソフトウェアの要求や設計は、シミュレーション等の解析の実施や、UML 等の静的モデルで設計結果を表現している。コンテキストに該当する、シミュレーションの解析条件およびその前提の全てを伝達可能な状態で残すことは困難であり、解析者自身がコンテキスト情報を保有している。また、UML 等の既存のソフトウェア設計手法では、複数の異なる要素のコンテキストを分析する方法（例：システムのシナリオ、コンポーネントの制約、SW の振る舞いを同時に分析する方法等）がサポートされていない。

本論文では、上記の特性を有する状況下において、コンテキストの抽出と組み合わせによってリスクシナリオを作成する方法とそのレビュー手法を提案する。

国立研究開発法人　宇宙航空研究開発機構　研究開発部門　第三研究ユニット
Research Unit III, Research and Development Directorate, Japan Aerospace Exploration Agency
茨城県つくば市千現 2-1-1 Tel: 050-3362-2805　e-mail:umeda.hiroki@jaxa.jp
2-1-1 Sengen, Tsukuba, Ibaraki, Japan
1) 国立研究開発法人　宇宙航空研究開発機構　研究開発部門　第三研究ユニット
Research Unit III, Research and Development Directorate, Japan Aerospace Exploration Agency
2) 名古屋大学 大学院情報学研究科
Graduate School of Informatics, Nagoya University
【キーワード】リスクシナリオ、コンテキスト、利用時品質、サイバーフィジカルシステム

2. 手法の前提概念

2.1 コンテキストとは

コンテキストとは、一般的に文脈、前後関係、背景、状況などの意味である。システム及びソフトウェア開発では、利用者の意図や状況、環境などの総体や、同じ処理や記述でも状況に応じて動作などが異なる場合に、その選択基準となる判断材料や条件などを指している[2]。ソフトウェア開発上でコンテキストは、ソフトウェアの目的とその使用環境を合わせる重要な役割を担っている[3]。コンテキストを分析する方法は、領域分析、シナリオベース（ユースケース分析等）、ゴール指向分析、ブレーンストーミング等がある。

本論文では、システム、利用運用者やハードウェア等のコンポーネント、SW モジュール等の要素（以下、構成要素という）とした場合、該当構成要素の入力前提をコンテキストと定義する。例えば、外部環境、構成要素 A、B の順序で入出力関係があった場合、構成要素 A のコンテキストは構成要素 A の制約とその制約に関係のある外部環境である。同様に構成要素 B のコンテキストは、構成要素 B の制約とその制約に関係のある外部環境や要素 A からの出力である。（図 1）

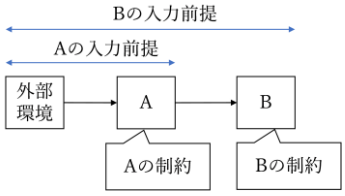

図 1　コンテキストの定義

2.2 サイバーフィジカルシステムとしてのコンテキスト

サイバーフィジカルシステム（以下、CPS という）は、「異なる性質の物理プロセスと密接に結合した計算機，通信，制御コンポーネントによって構成されるシステム」と定義されている[4]（図 2）。CPS におけるコンテキストは、運用、HW、物理法則、法規制等があるが、最も重要な点は CPS を構成するコンポーネントやソフトとウェア等の構成要素がそのコンテキストを共有していることである[5][6]。CPS のコンテキストを分析する方法として UML を拡張した手法[7]やオントロジーに着目した分析方法[7]が提案されている。CPS は全ての物理プロセスを取り込むことは不可能であることから、特定の視点からモデル化することや、物理空間から測定されるデータには誤差や時間的な揺らぎがあるため、CPS としてのロバストネスを分析することが重要となっている。加えて、CPS は物理プロセス自体を制御する、つまりコンテキスト自体が動的に変化するといった不確実な状況を扱う必要がある。そのため、静的構造視点、機能的視点、振る舞い視点から複合的なモデリング技法でコンテキストを分析する方法[8]が提案されている。

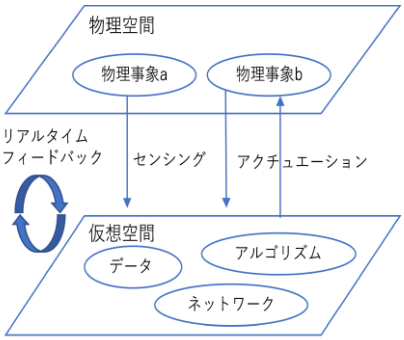

図 2　CPS イメージ

宇宙機搭載ソフトウェアは、機能冗長を達成するため複数の物理事象を元に自律的に制御しており、且つ、地上と軌道上のシステムが総合システムとして通信を行い制御することでミッションを達成するシステムであるため、サイバーフィジカルシステムの特性を有している[9]。

2.3 利用時品質（SQuaRE）

システム及びソフトウェアの多岐にわたるステークホルダーがもつ多様な品質要求の定義とその実装を評価する基準として国際規格 SQuaRE[10]がある。SQuaRE の品質モデルは、製品品質、データ品質、利用時の品質と 3 つのモデルがあり、システムの利用運用中にコンテキストが動的に変化していく CPS では、利用時品質の品質特性であるリスク回避性が重要となってくる。リスク回避性を計測する指標として、仕様外のリスクシナリオを考慮している件数[11]（以下、仕様外シナリオ想定度という）がある。CPS のロバストネスや、不確実な状況に対しても事故とならないよう対策が求められるクリティカルソフトウェア[12]では、利用時品質の指標である「仕様外シナリオ想定度」の計測も重要となってくる。

3. 提案手法

3.1 概要

複数の物理プロセスと計算プロセスが密に融合した CPS では、物理的な時間の推移と仮想空間上の情報伝達を同時に分析する必要があるため、提案手法は同じコンテキストを共有する構成要素を時間の推移で確認する時系列ビューを導入した。CPS 稼働後の将来にわたり全ての物理プロセスを想定することは困難であるため、提案手法は CPS 構成要素が保有する「制約」（例：センシングの限界、アルゴリズム動作時の条件等）を抽出する構造ビューを導入した。また、多数ある CPS 構成要素のうちリスクのある箇所に焦点を当てるため、提案手法は構成要素の抽象化によって同一コンテキストを集約し、構成要素の具体化によって「違い」があるコンテキストの抽出するツリービューを導入した。（図 3）

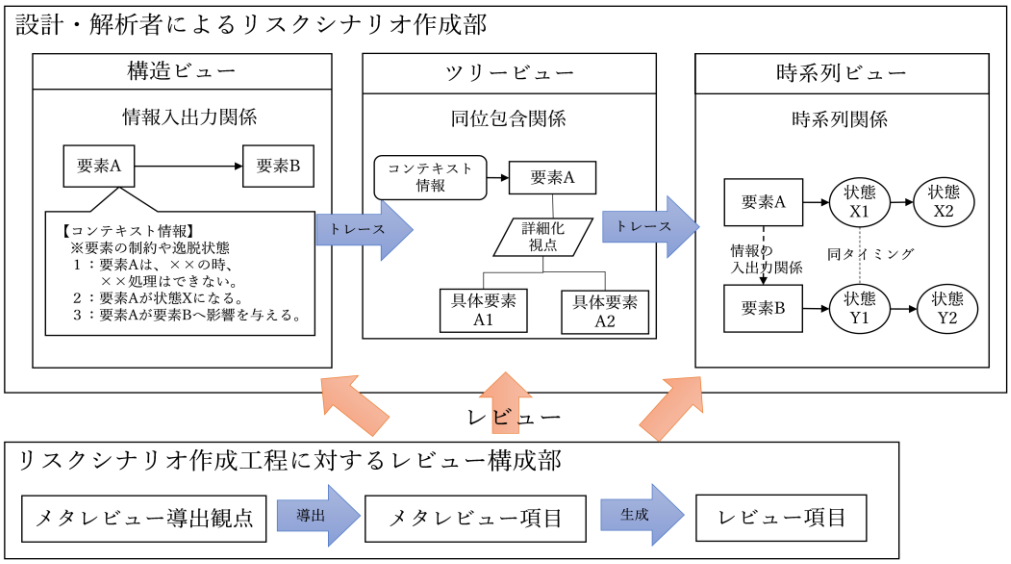

図 3：提案手法の概要

3.2 コンテキストを活かした 3 つのビューによるリスクシナリオ作成の提案

提案手法の分析工程を図 4 に定式表現を表 1 に示す。なお、定式表現上の添え字「i」はコンポーネント、「j」は SW モジュール上の識別子としている。

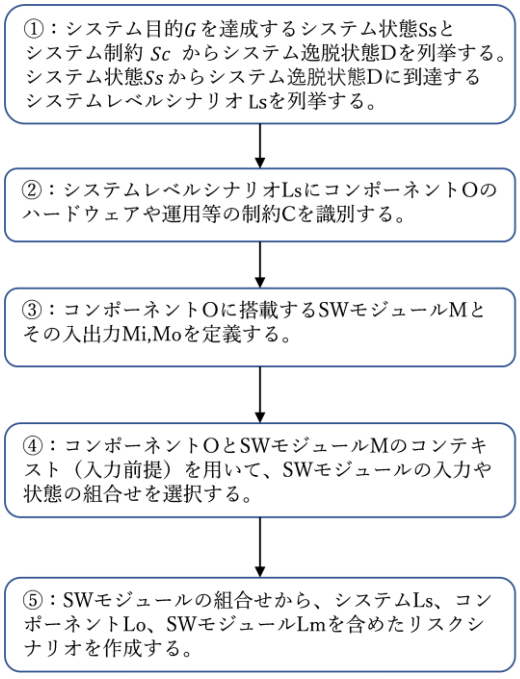

図 4　分析工程

表 1：定式表現

内容	定式
システムの目的	$G := \{g_1, g_2, \dots g_a\}$
システムの目的を達成する状態	$Ss := \{s_1, s_2 \dots s_b\}$
システムの制約	$Sc := \{c_1, c_2, \dots c_b\}$
システムの逸脱状態	$D := \{d_1, d_2 \dots d_c\}$
システムの外部環境	$E := \{e_1, e_2, \dots e_d\}$
システムレベルシナリオ	$Ls := \{ls_1, ls_2, \dots ls_e\}$
コンポーネントレベルシナリオ	$Lo := \{ls_{1.1}, ls_{1.2}, \dots ls_{1.f}\}$
SWモジュールレベルシナリオ	$Lm := \{ls_{1.1.1}, ls_{1.1.2}, \dots ls_{1.1.g}\}$
コンポーネント	$O := \{o_1, o_2, \dots o_l\}$
コンポーネントO_iの制約	$Oc := \{oc_{i1}, oc_{i2}, \dots oc_{im}\}$
コンポーネントO_iの入力	$Oi := \{oi_{i1}, oi_{i2}, \dots oi_{in}\}$
コンポーネントO_iの出力	$Oo := \{oo_{i1}, oo_{i2}, \dots oo_{io}\}$
SWモジュール	$M_i := \{m_{i1}, m_{i2}, \dots m_{ip}\}$
SWモジュールm_{ij}の制約	$Mc := \{mc_{ij1}, mc_{ij2}, \dots, mc_{ijq}\}$
SWモジュールm_{ij}の入力	$Mi := \{mi_{ij1}, mi_{ij2}, \dots mi_{ijr}\}$
SWモジュールm_{ij}の出力	$Mo := \{mo_{ij1}, mo_{ij2}, \dots mo_{ijs}\}$
SWモジュールm_{ij}の状態	$Ms := \{ms_{ij1}, ms_{ij2}, \dots ms_{ijt}\}$

3.2.1　構造ビューによるコンテキストの抽出と範囲設定

構造ビュー(図 5)は、同時に分析するコンテキストの範囲を決めるため、システムの外部環境とその状態、逸脱状態等から、情報の入出力があるコンポーネント（工程①）や SW モジュール（工程③）とその制約を記述する。なお、システムの制約 C や逸脱状態 D の分析は、既存のハザード解析等を用いる。コンポーネントの制約 Oc や SW モジュール制約 Mc は、不具合分析や仕様変更点の分析を用いる。

表 2　分析前提

定式表現	事例
システム状態 s1	姿勢変更状態
システム制約 c1	回転速度が一定以下であること
システム制約 c2	通信が不可となる期間がある
システム逸脱状態 d1	姿勢不安定状態
外部環境 e1	放射線がある宇宙空間

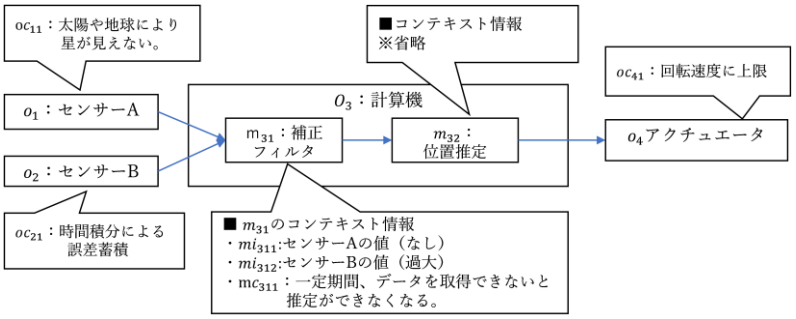

図 5　構造ビュー（事例）

3.2.2　ツリービューによるコンテキスト詳細化と組合せ

構造ビューで抽出されたコンテキスト情報の一部に対して、ガイドワードや構成要素に対する網羅性を与えることで、新たなコンテキストの抽出やコンテキストを共有する構成要素を決める。コンポーネントレベルの展開（工程②）と SW モジュールレベルの展開（工程④）となる。なお、HAZOP 等の異常パターンの発想を支援するガイドワード[13]は、別表で分析しその結果をツリービュー上のコンテキスト情報として記述するか、ツリービュー上の「詳細化視点」として分析する。SW モジュールとして「実装可能な条件」まで展開ができた場合、ツリービューの特性である上位と下位要素の包含関係から、最上位のから最下層までの 1 つのルート上にある構成要素がコンテキストを共有している。

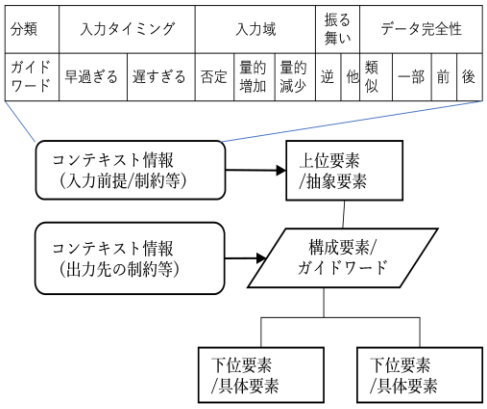

図 6 ツリービューとガイドワード

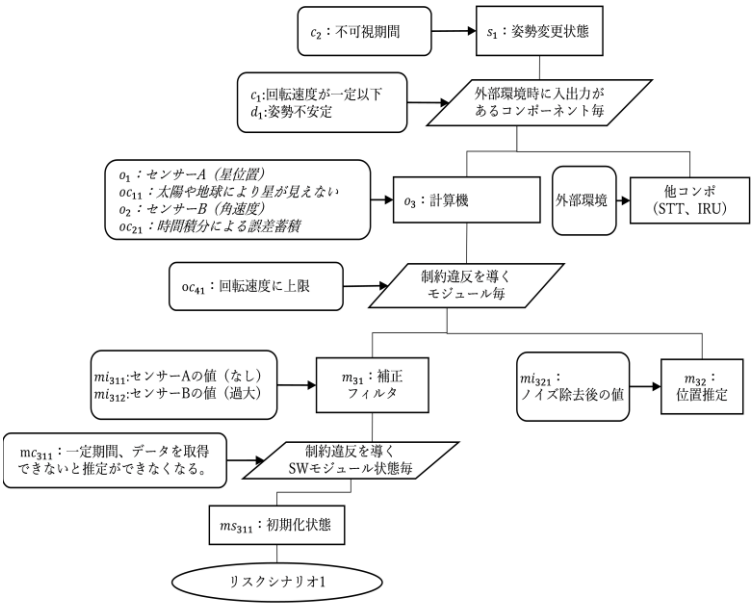

図 7　ツリービュー（事例）

3.2.3　時系列ビューによる組合せコンテキスト情報からリスクシナリオの作成

ツリービューの最上位から最下層まで 1 つのルート上のコンテキスト情報を参照して、システムシナリオ、コンポーネントシナリオ、SW モジュールシナリオを 1 つの時系列ビューで表現し、コンテキストが共有されているか確認する。(工程⑤)。その際、時系列ビュー上で物理事象の時間推移や情報

の入出力を補完して CPS としてのシナリオを作成する。(図 8) その補完時に「コンテキスト」の抜けがあった場合は、ツリービューに戻って新たなシナリオを追加することで網羅性を上げていく。

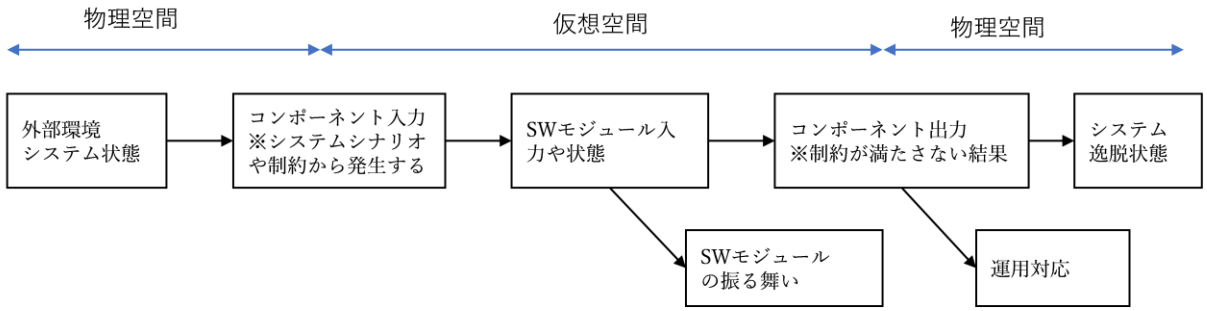

図 7：時系列ビューによる分析イメージ

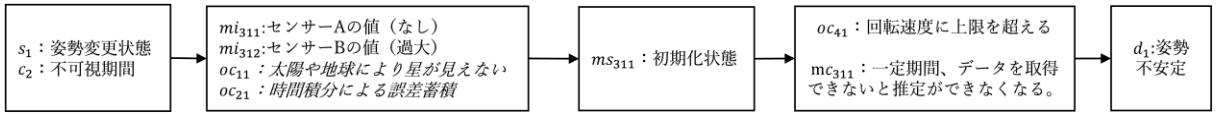

図 8：時系列ビューによる分析事例（未補完版）

3.3　3 つのビューに対するレビュー項目の提案

提案手法は、特性が異なる 3 つのビューを用いてリスクシナリオを作成するため、そのビュー毎にレビュー観点が異なりレビューの難易度が高くなる。そのため、各ビューの特性を考慮したメタレビュー項目からレビュー項目を作成することを提案する。

3.3.1　3 つのビューに対するメタレビュー項目の導出観点

3 つのビューのモデリングルールの特性を抽出するため、メタレビューの導出観点として、要素、要素間関係、ビュー間トレース、ビュー間逆トレースの 4 つとした（図 9)。要素の種類は、システム（逸脱状態がある要素)、コンポーネント O（HW や運用利用者等の制約がある要素)、SW モジュール M（機能、処理等の条件がある要素）であり、要素間関係は、構造ビューでは「情報の入出力関係と制約」、ツリービューでは「同位包含関係」、時系列ビューでは「順序関係とタイミング関係」である。

また、仕様外となるリスクシナリオを抽出するため、コンテキスト情報が「特徴（他の類似要素と違い)」や、「懸念（他の要素へ与える影響)」をメタレビュー項目に導入した。(図 10)。

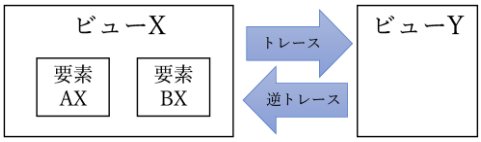

図 9　メタレビュー項目導出観点 1

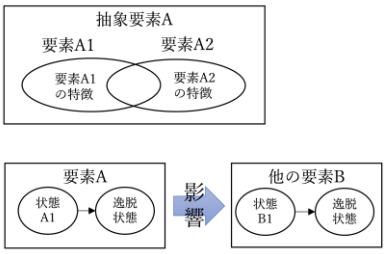

図 10　メタレビュー項目導出観点 2

3.3.2　3 つのビューに対するメタレビュー項目とその適用例

3.3.1 項によって導出したメタレビュー項目とその適用例を表 3 と表 4 に示す。

表 3　要素関係のメタレビュー項目と事例（抜粋）

種別	導出観点	メタレビュー項目	レビュー項目事例
構造	入出力 要素	懸念（要素自体の状態変化や他の要素への影響）と関係がある要素となっているか。	・システムの逸脱状態は、含まれているか。 ・コンポーネントの故障状態は、含まれているか。
構造	コンテキスト 情報	要素の特徴（従来や類似要素との違い、複雑性を含む要素）となっているか。	・過去の不具合や設計不採用となった等の失敗経験に基づく特徴は考慮されているか。 ・状況によって動作が変わる特徴はあるか。

種別	導出観点	メタレビュー項目	レビュー項目事例
ツリー	上位要素	上位要素は、解析目的と合致しているか。	・システム逸脱状態が明示されているか。
ツリー	中間要素	中間要素は、類似要素や抜けている要素はないか。	・特定状況下の動作を考慮しているか。
ツリー	下位要素	下位の要素は、より具体的になっているか	・SW としての処理条件が明確であるか。
時系列	状態・イベント	状態やイベントが抜けていないか。	・SW の入出力やモード遷移が抜けていないか。 ・同時に考えるシナリオは他にないか。
ツリー	包含関係	上位下位要素は、包含関係であるか。	・上位よりも下位の要素が抽象的な要素はないか。
ツリー	同位関係	要素の同位関係となっているか。	・2 項対立や MECE となる視点であるか。 ・視点と要素名が同じになっていないか。
ツリー	継承関係	最上位から最下層の要素にあるコンテキスト情報を組み合わせて、1 つのシナリオを作成できるか。	コンテキスト情報の組合せは、 ・SW の入力前提が明確になっているか。 ・SW からの出力結果の影響が明確になっているか。
時系列	同タイミング関係	要素間で共有するイベントが抜けていないか。	・同じタイミングで入力される情報は考慮されているか。
時系列	分岐関係	シナリオの分岐が不足していないか。	・SW の処理条件の分岐が不足していないか。

表 4　トレース・逆トレースのメタレビュー項目（抜粋）

トレース元	トレース先	メタレビュー項目
構造ビュー	ツリービュー	全てのコンテキスト情報は、ツリービューに反映されているか。
ツリービュー	構造ビュー	ツリービューで追加されたコンテキスト情報は、入出力関係のある要素の追加があるか。

4.　提案手法の有効性確認

4.1　有効性確認の方法

提案手法の有効性確認として、実際の SW 開発と並行して設計者及びレビューアによるリスクシナリオ数と仕様外シナリオ想定度の計測を行う。なお、リスクシナリオは、SW の条件が明確である

RQ1：設計者が 3 つのビューを用いて、リスクシナリオ数および仕様外シナリオ想定度が増加するか。

＜実験条件＞

・設計者は、設計文書作成後に、本手法を用いてリスクシナリオを作成する。

・表形式のフォーマットに入力することで 3 つのビューが生成される支援ツールを用いる。

RQ2：レビューアがメタレビュー項目を用いて、リスクシナリオ数および仕様外シナリオ想定度が増加するか。

＜実験条件＞

・レビューアは最初に通常の方法でレビュー(レビュー工程 1)を行う。

・レビュー工程 1 の完了後、提案手法を用いてレビュー(レビュー工程 2)を実施する。

・レビュー工程 1 と 2 は、同一のレビューアである。

表 5：実験条件の一覧

No	企業種別	SW 種別	機能	設計者	レビューア
1-1	企業 A	組み込み	機能 A1	1 名	1 名
1-2	企業 A	組み込み	機能 A2	1 名	1 名
1-3	企業 A	組み込み	機能 A3	1 名	1 名
1-4	企業 A	組み込み	機能 A4	1 名	1 名
2-1	企業 B	エンタープライズ	機能 B1	1 名	1 名
2-2	企業 B	エンタープライズ	機能 B2	1 名	1 名
3-1	企業 C	エンタープライズ	機能 C	1 名	2 名

4.2　有効性の確認結果

RQ1 対する実験結果を表 6 と図 11、RQ2 に対する実験結果を表 7 と図 12 に示す。

表 6　設計者が作成したリスクシナリオ数(RQ1)

No	リスク シナリオ数	仕様外 シナリオ数	仕様外シナリオ の作成割合
1-1	18	6	0.33
1-2	60	24	0.40
1-3	10	10	1.00
1-4	22	16	0.73
2-1	12	10	0.83
2-2	17	11	0.65
3-1	103	86	0.83

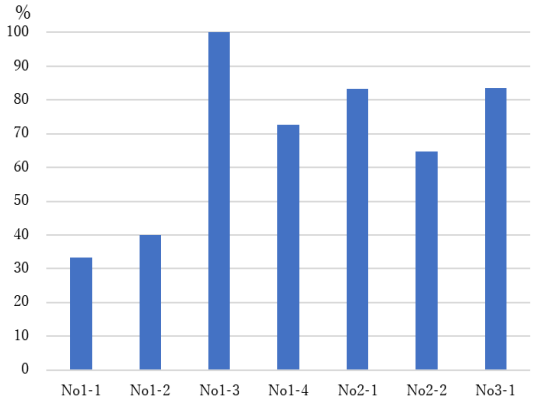

図 11　仕様外シナリオの作成割合

表 7 レビュー後のシナリオ数(RQ2)

	リスクシナリオ数			仕様外シナリオ想定度		
No	レビュー前	手法なし	手法あり	レビュー前	手法なし	手法あり
1-1	18	38	54	6	11	15
1-2	60	68	109	24	32	69
1-3	10	10	20	10	10	20
1-4	22	25	31	16	19	19
2-1	12	15	20	10	10	15
2-2	17	18	23	11	11	14
3-1-1	103	107	122	86	90	90
3-1-2	103	116	120	86	94	97

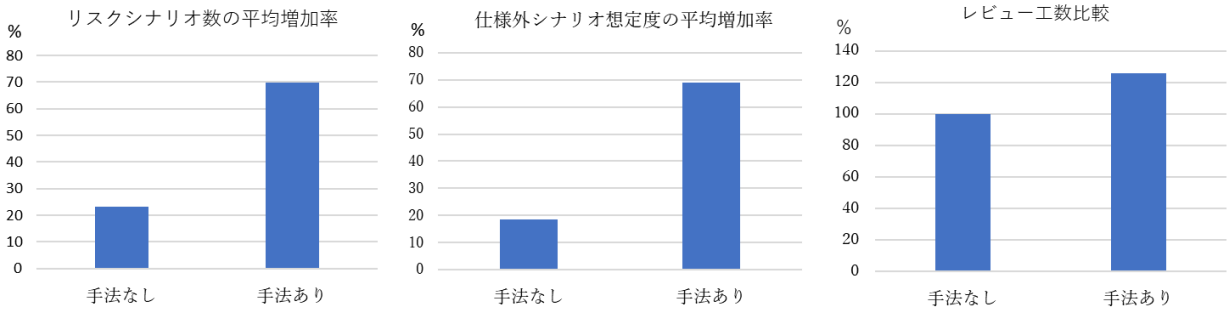

図 12：メタレビュー項目を用いた結果

4.3 考察

3 つのビューによって CPS の複数の構成要素が共有すべきコンテキストからリスクシナリオが作成されている。仕様外のシナリオも導出されており、その作成割合は平均 68%である。ケース 1-1 と 1-2 は仕様外シナリオ作成割合が低いが、いずれのケースも既存機能の改良となっており、仕様としての成熟度が高くなっているためと考えられる。他のケースは、新規性が高い機能や大規模な機能である。3 つのビューに対するレビューは、一旦レビュー後でも、提案手法を用いるとリスクシナリオ数がさらに平均 46%増加することを示している。一方、レビュー時間は 25%増加しているため、さらなる作業対効果を上げる工夫が必要である。具体的には、レビュー項目に合わせた情報を自動収集する仕掛けを入れることで、レビューアが各ビューにある情報を探す工数は削減できる。

本手法のメリットは、システム状態 S から逸脱状態 D に至るリスクシナリオを識別できること、各構成要素の制約によってシナリオ数を押さえられること、リスクシナリオを構成する SW の入力や状態も同時に分析するためその原因も同時に突き止められること、各コンテキストから分析対象の漏れや影響判定もできる点である。一方、本手法の限界は、システムやコンポーネントの制約 C が明確でないと現実的に分析可能なシナリオ数にならない点である。

5. まとめ

構造ビューで制約を起点に分析するコンテキストの範囲を決め、ツリービューでコンテキストの組合せを行い、時系列ビューで物理時間の経過と情報の入出力を同時に確認することで、CPS 搭載 SW のリスクシナリオを作成できる。また、メタレビュー項目によって、リスクシナリオや仕様外シナリオを増加させることができる。従来、経験がありコンテキスト情報を多数保有している技術者は、本手法でリスクシナリオを作成し、仕様外シナリオ想定度を向上させることができるが、コンテキスト情報を保有していない技術者への利用方法、及び、コンテキスト情報の効率的な抽出から利用までの組織的な活用は、今後検討が必要である。

6. 参考文献

[1] JAXA、システムズエンジニアリングの基本的な考え方(BDB-06007B)、2007
[2] IT 用語辞典 e-Words
[3] SWEBOK v3.0
[4] CyPhERS、Cyber-Physical European Roadmap and Strategy, Research Agenda and Recommendations for Action CyPhERS、2015
[5] T. Sanislav at el.、A dependability analysis model in the context of cyber-physical systems、18th International Carpathian Control Conference (ICCC)、pp.146-150、2017
[6] M.Daun at el.、Fostering concurrent engineering of cyber-physical systems、3rd International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC)、2016
[7] J. Al-Jaroodi at el., Software Engineering Issues for Cyber-Physical Systems、IEEE International Conference on Smart Computing (SMARTCOMP)、2016
[8] T.Bandyszak at el.,Model-based Documentation of Context Uncertainty for Cyber-Physical Systems,IEEE 14th International Conference on Automation Science and Engineering(CASE)、2018
[9] A. T. Klesh at el.、Cyber-Physical Challenges for Space Systems、IEEE/ACM Third International Conference on Cyber-Physical Systems、2012
[10] IEEE Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality model、ISO/IEC 25000
[11] 独立行政法人情報処理推進機構、つながる世界のソフトウェア品質ガイド
[12] Oxford University Press、A Dictionary of Computing、2004
[13] IEC 61882: Hazard and operability studies (HAZOP studies)