記述者視点に基づく GSN のパターン分類による セーフティケース記述の容易化に関する研究

令和 3 年 7 月

日本大学大学院理工学研究科博士後期課程
情報科学専攻

越山 勉

目次

第 1 章 序論

1.1. 背景

近年、宇宙、航空機などの分野において、高度な技術が求められるシステムは電子化が進みそれらは増大傾向を続けている。我々の身近な分野としての自動車業界においてもその傾向は同様であり、自動車の構成要素は、機械部品に加え、電子部品、さらにはマイコンを搭載した ECU の搭載数も増加をし続けている。1970 年代後半で初めて搭載された ECU は、現在は、1 車両あたりに 30 個を超えるものも登場してきている。一方で電子化が進んだ車両システムにおいては、安全性が問われる事例も増加し、近年では、自動車のスロットル制御システムリコール訴訟に対して 940 億円といった巨額の和解金が生じた事例もある [1]。そのような背景において、安全性が求められるシステムを開発する企業においては、達成されている安全性を証拠及び根拠と共に論理的に説明する、又は常に説明できるようにしておく必要がある。そして、それらの説明を遂行するためにセーフティケース（Safety Case）が注目されてきている。

セーフティケースとは、システムの安全性を示すための文書であるが、自動車の機能安全基準 ISO26262 [2] [3]においてもその必要性が提言されている。近年では、自動運転技術の開発及び導入が進み、それらの自動化の技術はより身近なものになりつつある。そこで、自動運転に求められる安全性においては、SOTIF（Safety of the intended functionality） [4]において ISO/DIS21448 として標準化が進められている。また、それらの規格 [2] [3] [4]に対し、安全性の議論、及びセーフティケースにおける補完的なガイドラインとして UL4600 [5]がある。

一方で、セーフティケースを叙述形式の文書としてではなく、より視覚的かつ構造的に論証する方法の一つとして GSN（Goal Structuring Notation）がある。GSN は、これらの規格やガイドライン [2] [3] [4] [5]においてセーフティケースを視覚的に表すことができる方法の一つとして推奨、又はそれら基準書の中で実際に使用されている。このように、セーフティケースが必要とされることに加え、それらを視覚的、かつ構造的に論証する方法が求められるようになってきており、GSN が着目されている。

1.2. 本研究の目的

抽象度の高い主張（安全性など）の達成について論証を行う場合には、具体的、かつ判断可能なものとして、証拠や根拠によって、判断、確信が得られるようにする必要がある。そのためには、抽象的な内容について、段階的かつ、階層的に説明を行うことが有効である。そして、論証を木構造として、段階的かつ構造的に構成する手法の一つに GSN があり、本研究は、GSN における主張同士の構造的解釈に関するものである。

GSN は、文法構造がシンプルであるが、それが故に GSN の木構造として配置された親ゴールと、単一、又は複数の子ゴール同士の関係性において、見かけ上の構成は同じであっても（子ゴール同士の成立の AND の関係で親ゴールが成立するといった構造上の前提においても）それらの関係性は、同じになるとは限らない。そして、GSN の記述者がそれらの違いがあることを、意識せずに作成している場合や、仮にそれらの違いを意図して作成されている場合であっても、GSN の読み手がそれらの違いを記述者の意図する通りに読み取ることは難しい。これらのことが GSN の作成、及び読み取りを難しくしていると考える。

そこで、本研究では、GSN におけるそれら構造上に存在する関係性の違いを、調査及び分類し GSN 上での記述の容易化を図ることを目的とし、以下の項目について検討を行った。

⑴ GSN で表現されているセーフティケースサンプルを調査し、GSN の構造上のバリエーションについて調査する。

⑵ 調査したサンプルに従って記述の容易化が図れるための構造上の分類を行う。

⑶ 分類における妥当性、有効性の検証を行う。

1.3. 本論文の構成

本論文は、第 1 章から、第 8 章によって構成されており、各章の内容は以下のようである。

第 1 章　序論

本論文の背景、目的について述べる。

第 2 章　GSN の基本構造について

本論文で扱う GSN の基本構造について説明する。GSN の文法についての説明、及び GSN 上の部品（ノード）で構成される木構造において、主張のノード上への配置のされ方と、ストラテジノードによる変換と分割についての説明を行う。

第 3 章　GSN のパターン分類

GSN を 6 個のパターンに分類する上での全体についての説明を行う。それぞれのパターンの特徴についての説明を行う。

第 4 章　GSN のパターンマッチング

既存の GSN サンプルに対して、6 パターンを当てはめることを行う。インターネット上で入手した GSN サンプルへのパターンマッチングを行う。

第 5 章　ワークショップによる検証

第 3 者による、6 パターンを用いた GSN の読み取り、及び作成についての試行をワークショップ形式で行う。

第 6 章　既存研究における分類と考察

産業界における GSN 使用事例についてと 6 パターンを比較する。GSN を含む木構造手法における議論パターン全般に関する研究と、6 パターンとの比較と検証を行う。

第 7 章　冗長機構への適用の検証

安全機構における安全性について、機能構造を表すブロック図と GSN とを組み合わせることによる安全性についての説明を行う。

第 8 章　結論

本論文の成果をまとめる。

第 2 章　GSN の基本構造について

2.1. GSN の文法

GSN におけるノードと呼ばれる図形部品は、それぞれ 図 1 左に示す種類と働きがあり、図 1 右のように木構造で構成される。これらのノードの構成及び、詳細な記法については [6]を参照とされたい。なお、特に断りがない限り、それぞれのノードを示す場合には、以下省略した表記とする。

・ゴールノード ⇒ ゴール
・ストラテジーノード ⇒ ストラテジ
・コンテキストノード ⇒ コンテキスト
・エビデンスノード ⇒ エビデンス
・アサンプションノード ⇒ アサンプション
・ジャスティフィケーションノード ⇒ ジャスティフィケーション

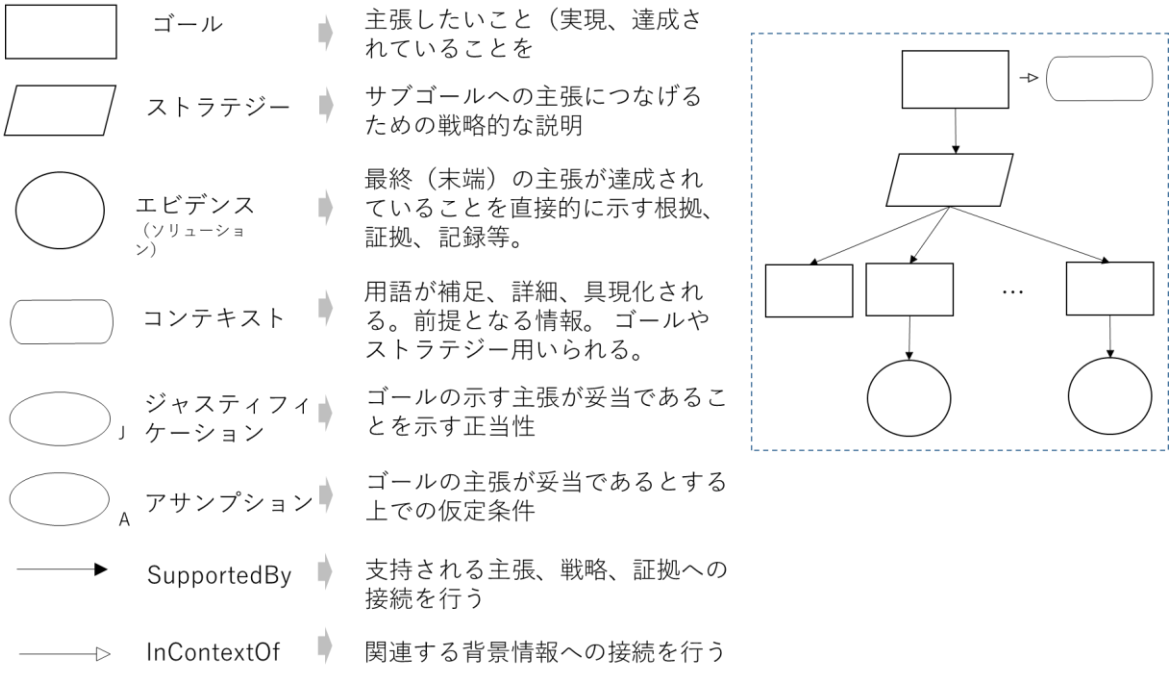


図 1 GSN におけるノードと木構造

以下に、GSN のサンプルを示す。
図 2 において、親ゴール G1 は、ストラテジ S を介して、子のゴール G2、G3、G4 へと分割される。一番上層の根に位置するもの（この木構造では G1）は、記述者が、この GSN 上で最終的に達成していることを示したい主張である。記述者が、G2、G3 及び G4

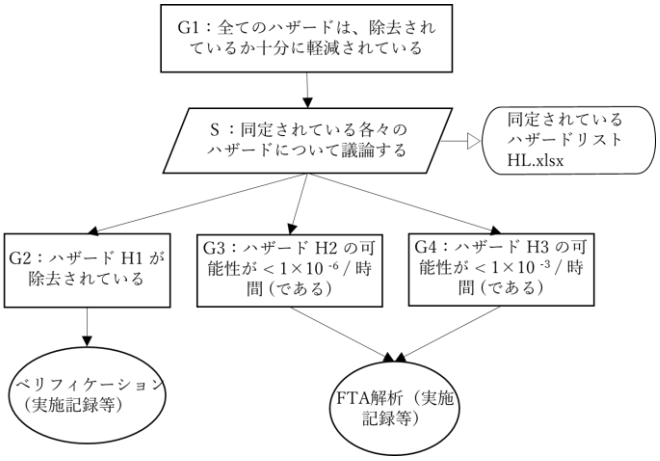


図 2 GSN の例

における主張の全てが達成されることで、G1 の主張が達成されると考えていることが、読み手にとっても、同じ解釈によって納得されることがこの GSN の役割である。

なお子同士の達成条件を OR 条件として記載する方法もオプションとして用意されているが、この例のように、単に矢印で接続されている場合は、AND 条件の関係になる。達成を示す順序は、より末端におけるゴールの主張が達成されることであり（この例では、2 階層目の G2、G3 及び G4 が最末端にあるゴールである）、さらにそれらに接続された、エビデンスが提示されることによって、それらゴールの達成が直接的に示される。そして、G2、G3 と G4 の達成は、間接的に、G1 の達成を示すことになる。

なお、S から白抜きの矢印で接続されているノードは、コンテキストと呼ばれ、ゴールやストラテジに接続される。ゴールやストラテジに記載された内容について具現化を行うことが可能であり、図 2 では、同定されているハザードがリスト（HL.xlsx）に定義されているものとして、それらハザードについての所在そのものの具現化がなされている。なお、ここでの”ハザード”とは、”潜在的な危険源”を示すものとする。もし、このハザードについての存在や詳細が曖昧であった場合、GSN モデル全体の主張の達成が不確定なものになってしまう。このように、コンテキストはゴールやストラテジにおける抽象的な情報をより具体的なものにするために使われる。

2.2. 主張と木構造

GSN の構造上におけるゴール及びストラテジの組み合わせは、4.4 章において表 6 のようなバリエーションが存在することが GSN サンプル調査よりわかった。ここでは、GSN モデルの木構造においては、子における主張が達成されることで、親における主張の達成が示される。主張とは“達成されていること”、又は“達成しようとする”ことについての記述を指す。

図 3 は、GSN における主張の達成どうしの関係を示したものである。木構造における子同士の関係は複雑ではない。それらは、子の達成を AND 関係で結びつけることで親の達成が成立するものとして示されるといったシンプルな構造であると言える。なお、通常は、図 3 の左に示される AND 関係であるが、右に示す OR 関係として表すことも可能ではある。詳しくは、GSN Community Standard [6]を参照されたい。

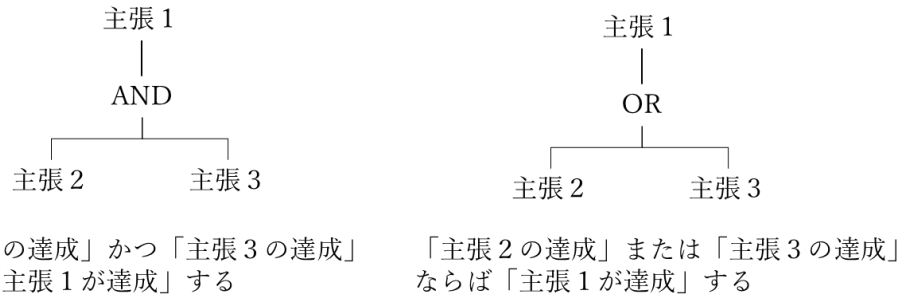


図 3 GSN における AND と OR 木構造

これら木構造において子同士、又は親と子 がどのような関係性になっているべきかの決まりはない。主張 2 と主張 3 の AND としての成立が、主張 1 に対して論理的に等価であるとは限らない。主張 2 と主張 3 のそれぞれが成立し、それらが論理的に AND（又は OR）の関係にある場合に主張 1 の成立が示されることは、記述者の想定において設計された構成であることに他ならない。

2.3. ストラテジの 2 つの働き

主張同士の関係を捉えるにあたり、主張が定義されるノードについて考える。ストラテジには通常、戦略が定義される。戦略とは、そのストラテジの下層に配置される子ゴールによって、どのように主張がなされるかの説明をすることが可能なノードである。

しかし、ストラテジについては、記載上、省略される場合や、戦略であると同時に（隠れた）主張を含む場合もある。そこで、本研究ではゴールだけでなく、ストラテジに含まれる主張も含めそれらの関係を捉えることとしている。そして、GSN 上のそれら主張同士の関係を捉えることで、効率的に GSN を読み取ることが可能になると考える。以下に、ストラテジの持つ 2 つの働きについて考える。

- **分割としての働き**

1 つ目は分割としての働きである。ここで分割とは親の主張が、複数の子における主張に分けられる操作を指すものとする。

なお分割がなされる目的は、対象となる物、事について、特性や特徴が成立していること（又は成立する見込み）を示す場合、対象となる主張を部分に分けて考えることにより、達成の説明を効率的、又は容易に行うことができると考える。
図 4 にストラテジよって分割されている例を示す。
この GSN において、ストラテジは、ゴール G1 を、ゴール G2 と G3 の主張に分割している。

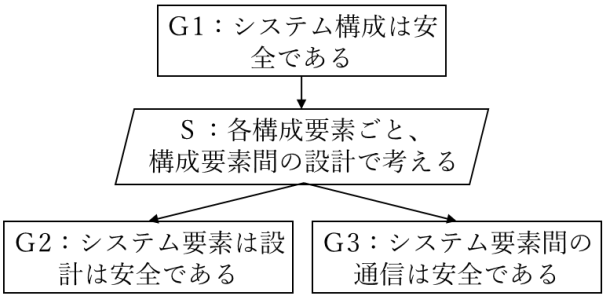


図 4 ストラテジの分割の働き

このように、ストラテジの分割の働きは、下層の子への分割に先立っての指針を示すことができることである。(但し、分割としてのストラテジが用いられる場合、分割される子ゴールにおける説明とほぼ同じ内容の記載になることを避けるために、ストラテジが省略され、直接子ゴールが接続される場合がある。)
この GSN におけるゴールとストラテジの関係は、図 5 の左図のように表され、主張の分割の構造は、図 5 の右図のように表すことができる。

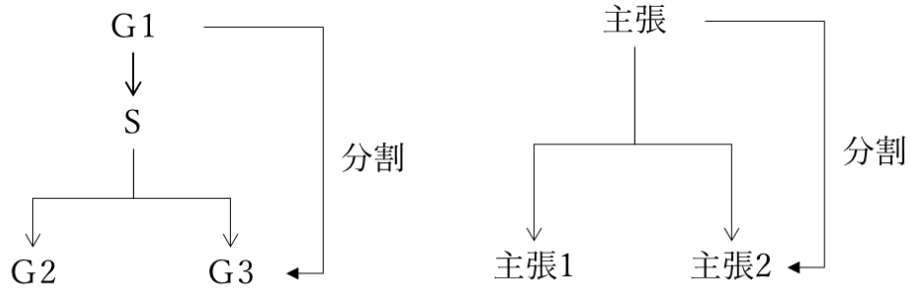


図 5 分割としてのストラテジ

- **変換としての働き**

2 つ目は主張の変換として用いる場合である。
ストラテジによって、単一の子ゴールに変換される GSN の例を図 6 に示す。

このGSNにおいては、ストラテジにより、下層に接続されている子ゴールG’に、どのように説明がなされるかの戦略としての説明がなされているが、G’における内容について、主張の変換がなされている例である。

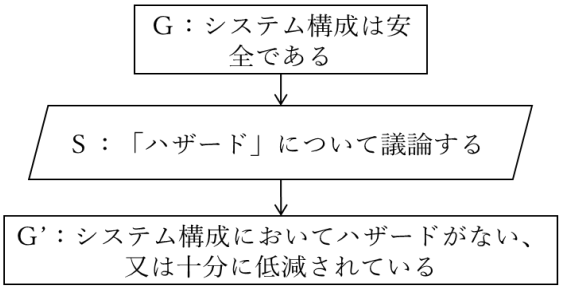


図6 ストラテジによる変換

なお、この例において、主張が置き換えられた理由としては、まず一般的には安全であるという性質を説明、証明すること一般的には難しいといったことがある。そこで、“ハザードがないこと、又は十分に低減されている”を説明することで、代わりに“安全である“が達成されていることを示すことを試みている。
このGSNにおけるゴールとストラテジの関係は、図7の左のように表され、主張の変換の構造は、図7の右のように表すことができる。

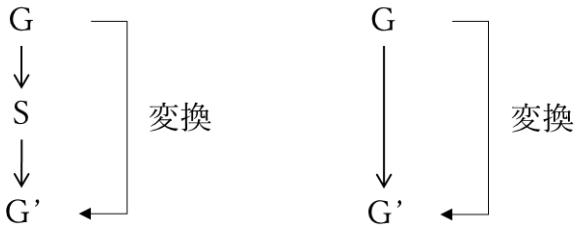


図7 変換としてのストラテジ

次に、図8のGSNについて考える。
最初のゴールGにおける主張をストラテジS1により主張の内容にとしてゴールG’に変換している。次に、ゴールG’は、ストラテジS 2によって、子ゴールG1、G2に分割されている。

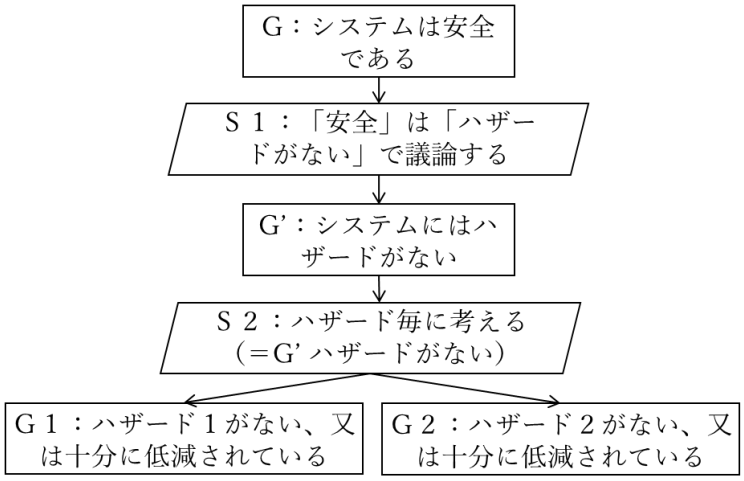


図 8 変換されたゴールを表記した場合

この GSN は、途中のストラテジ S1 と、ゴール G'が省略された形として、図 9 のようにも表すことが可能である。

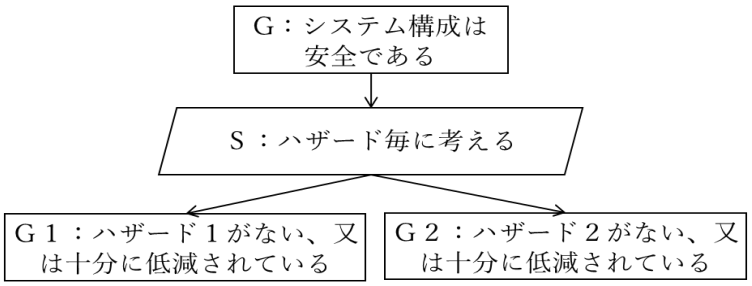


図 9 変換されたゴールが省略された場合

さらに、図 9 の GSN における、ゴール、ストラテジの関係は、図 10 の左図のように表され、主張の変換と分割の様子は、図 10 の右図のように表すことができる。

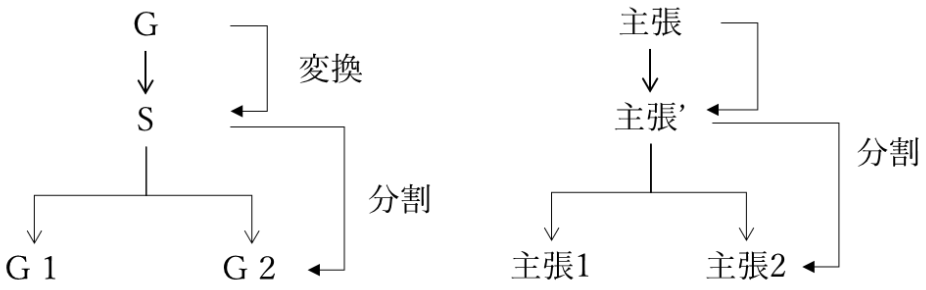


図 10 変換と分割の複合例

この 2 つの GSN 図 8 と図 9 の内容は、どちらも登場する主張の内容は同じであり、どちらの GSN としての表現も間違いではない。また、図 8 の GSN における主張の関係は、図 9 の GSN の場合と同じく、図 10 の右図のようになる。このようにストラテジが変換の働きを伴うばあいは、変換された主張がゴールとして表現されていない場合があり、変換された主張があるかどうかを考慮して GSN 上の主張同士の関係を読み取る必要がある。

このようにストラテジは、ゴールにおける主張の構成を分割、変換する働きがある。しかし、ストラテジがそのどちらの働きとして用いられているかは、見かけ上からは区別がつかず前後の主張の内容、関係性から判断する必要がある。ストラテジは（分割としてのストラテジの場合）省略される場合も多く、また変換が行われている場合には、変換された主張が隠れている場合が多い。

このように、ゴール、及びストラテジのノードの存在だけで、主張の関係性を識別することは難しい。そこで、主張が存在する部分を見極めて、それらの関係性についての分類を行っている。

2.4. まとめ

GSN での 6 パターン分類を行うにあたり、GSN 上における主張同士の関係に着目することを説明した。また、ストラテジでゴールの主張が変換されている場合があることを示し、ゴールの他に、ストラテジについても着目する必要があることについて確認を行った。

第 3 章　GSN のパターン分類

3.1. パターン分類の視点と過程

図 11 は、最終的に 6 種類のパターン(a)から(f)に分類に至った全体を示している。以下この図に従って説明を行う。

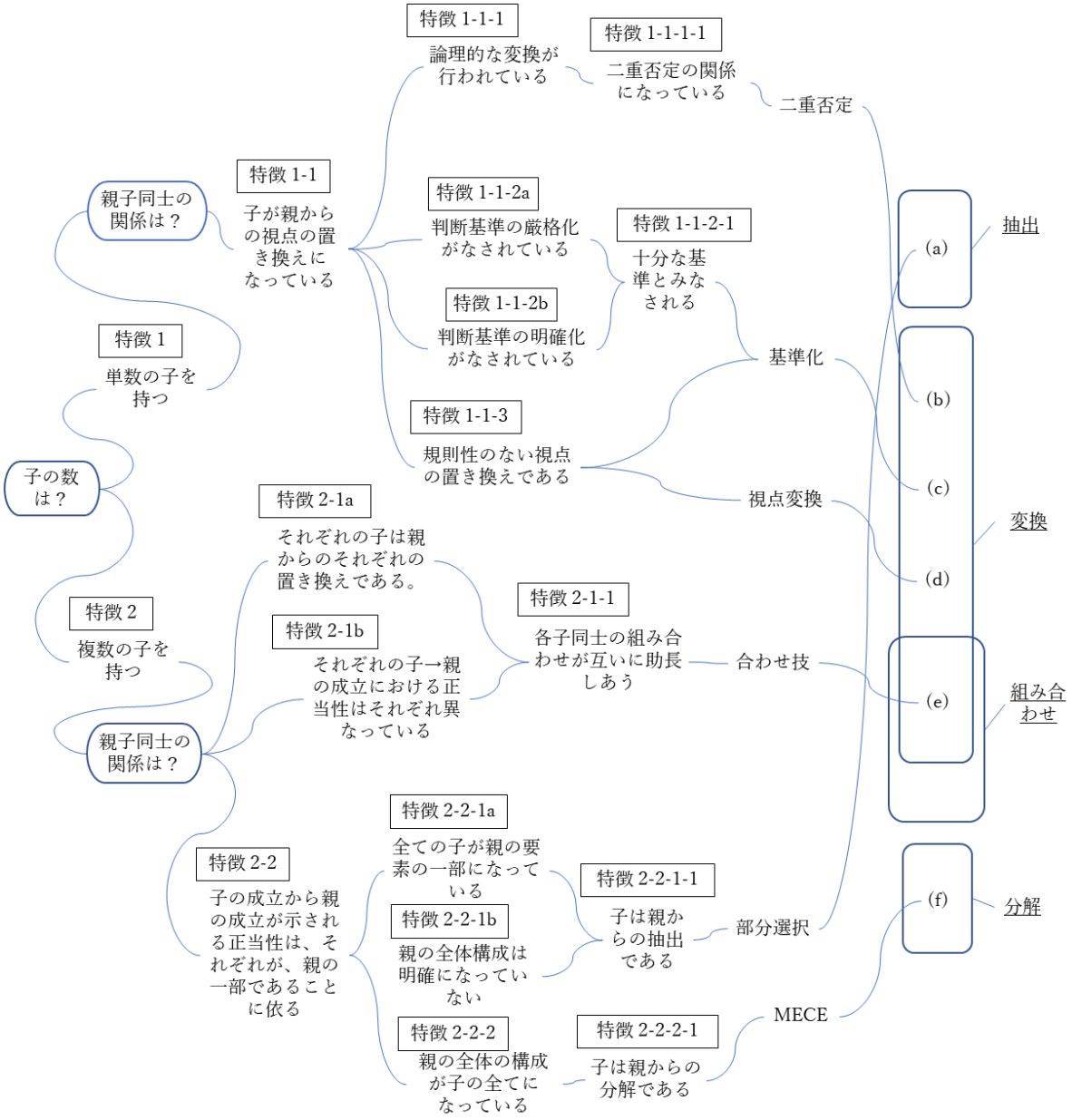


図 11 パターン分類の全体

最初に階層間の関係で、“単数の子を持つ（特徴 1）”と、“複数の子を持つ（特徴 2）”とで分けて考える。

● 単数の子を持つ分類

子が単数である構造は“子が親からの視点の置き換えなっている（特徴 1-1）”の特徴を持つと考え、更なる分類を行っている。

図 12 の GSN の特徴について考える。

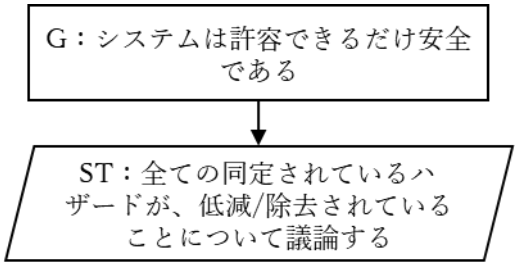


図 12 二重否定 （[18] Figure39）

これは“安全である”を“危険でないこと”（ここでは“ハザードが低減、除去されている”を同義としている）への置き換えと見なし、この置き換えの関係を“二重否定の関係になっている（特徴 1-1-1-1）”の特徴とし、パターン“二重否定”と分類した。これは“論理的な変換が行われている（特徴 1-1-1）”の一つであると見なされるが、本研究の分類では、二重否定以外の論理的関係のものは、GSN のパターンとしては存在していないものと見なしている。

なお、この GSN の例では、子に相当するノードが、ゴールではなくストラテジとなっているが、このストラテジには主張としての内容も含まれているためこのストラテジにおける主張との関係を捉えている。このストラテジにおける“全ての同定されているハザードが、低減/除去されていることについて議論する”は“ハザードが、低減/除去されている”といった（親の主張から置き換えられた）主張を含むストラテジであると見なしている。

次に、図 13 の GSN に示す視点の変換について考える。

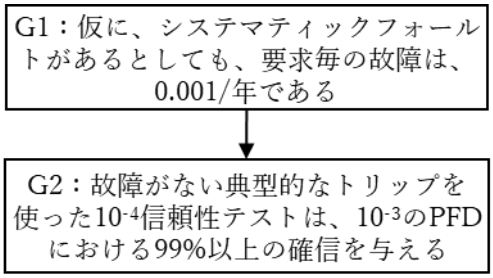


図 13 判断基準の厳格化 （[18] Figure129）

ここで、故障が起きる頻度の基準値を G1 において“ 要求毎の故障は、0.001/年”の成立を、G2 において別の基準値として“10^{-4} 信頼性テストは、10^{-3} の PFD における 99%以上

の確信”に置き換えられている。ここで置き換えられている基準値が、置き換えられる前の基準値に対して十分な程度を以て置き換えが行われているといった特徴により“判断基準の厳格化がみなされている（特徴 1-1-2a）”とみなしている。なお、この GSN 上では、G2 において置き換えられた基準値が、理論的、専門的な観点から十分な程度を以ているか否かについての説明がなされていないが、記述者に判断においてこの置き換えが十分な程度を以て行われている想定であるものと見なしている。

さらに、図 14 の GSN について考える。

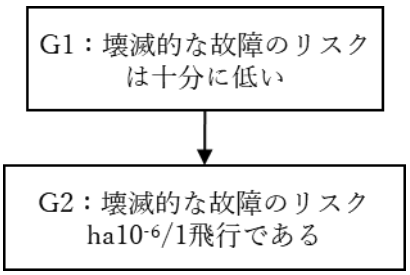


図 14 判断基準の明確化 （ [21] Figure14）

ここでは“故障のリスク”の程度について置き換えが行われている。しかし、その程度については“十分に低い”といった抽象的な表現が“10^{-6}/1 飛行である”といった具体的な数値によっての表現に置き換えられている。この変換は“判断基準の明確化がなされている（特徴 1-1-2b）”の特徴として分類した。

ここで“判断基準の厳格化がなされている（特徴 1-1-2a）”と“判断基準の明確化がなされている（特徴 1-1-2b）”の両方について比較した場合、この 2 つに共通して作者にとって十分な程度による表現、基準に置き換えが行われているといった共通の特徴があると考えた。特徴 1-1-2b に於いては、抽象的な程度が明確な基準に置き換えられているものであるが、これは変換後の基準が、記述者にとって十分な程度を持った基準であると見なされているものと考えた。そこで、この特徴 1-1-2a と特徴 1-1-2b の双方に共通する特徴として“十分な基準への置き換えとみなされる（特徴 1-1-2-1）”として分類するものとした。この 2 つの特徴のものをパターン“基準化”とした。

同じく置き換えの GSN の例として、図 15 について考える。

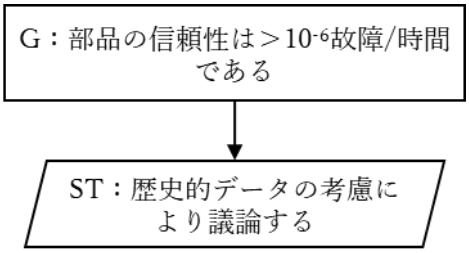


図 15 規則性のない置き換え（ [21] Figure15）

この GSN においては、図 12 と同様に、変換後は、ゴールではなくストラテジになって

いるが“歴史的なデータで考慮されている”といった置き換えられた主張がこのストラテジには含まれているとみなすことができる。

この置き換えは、二重否定や、数値化の厳格化や明確化でもない。それは“信頼性＞10^{-6}故障/時間”であることを説明するために選定された方針とみなすことができる。ここで“歴史的データの考慮”については、他の方針を変換後の主張に置く可能性があることを想像することは難しくはない。例えば“構造設計上の値による説明”や“実験データによる説明”といった視点での説明により主張に置き換えられる可能性もある。これは記述者が説明する場合において都合の良い視点が選択されていると考える。その視点は、“二重否定”のような論理的な変換や“基準化”といった特定の変換の法則性はない。記述者視点にとって説明をし易くするために選択された視点の変換とみなされ“規則性のない視点の置き換えである（特徴 1-1-3）”として分類した。これをパターン“視点変換”とした。

“二重否定”又は“基準化”以外の視点の置き換えについては“視点変換”に含めるものとしている。視点の種類は、様々なものがあると考えるが、それらは“規則性がない視点の置き換えである（特徴 1-1-3）”に集約して該当されるものと見なしている。なお、視点の変換は記述者の視点毎によって異なるため、敢えてそれら視点毎の違いを分類することはせず、視点の置き換えが行われていること自体を識別することを重視した分類としている。

● 複数の子を持つ分類

図 16 の GSN について考える。

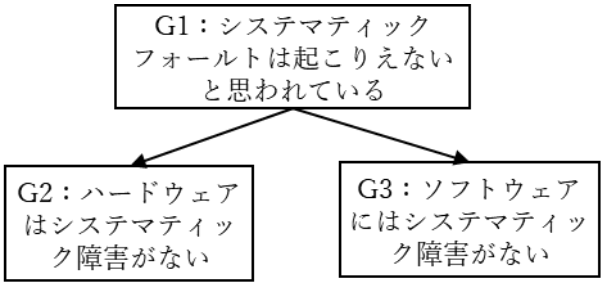


図 16 親からの分解（[18] Figure127）

図 16 において、G2 と G3 の主張は、共通し、システマティック障害についての主張になっている。そして、ハードウェアとソフトウェアという網羅的な 2 つの要素の組み合わせで関するシステマティック障害についての説明として成立させようとしている。この子の主張同士は、親の主張から分解されている特徴に着目し“親の全体の構成が子の全てになっている（特徴 2-2-2）”といった特徴と、さらに“子は親からの分解である（特徴 2-2-2-1）”といった特徴があると考える。これをパターン“MECE”として分類した。

パターン“MECE”において、子の成立で親が成立する関係性は、“子の成立から親の成

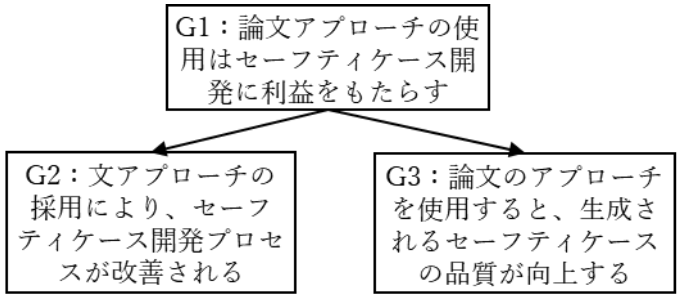


図 17 親からの抽出 （[18] Figure107）

立が示される正当性は、それぞれが親の一部であることに依る（特徴 2-2）”といった特徴があることに着目した。

次に図 17 の GSN について考える。G2 の“開発プロセスが改善される”と G3 の“セーフティケースの品質が向上する”は、G1 の“セーフティケース開発への利益”の一部であると考えられる。しかし、ここで、G1 における“セーフティケース開発への利益”の全てを G2 と G3 で表していると見なすことは難しい。これは、G2 と G3 が G1 の全てであることは、一概には判断できないからである。そこで、G1 の要素の一部分だけを G2、G3 で挙げていると見なし“全ての子が親の要素の一部になっている（特徴 2-2-1a）”でありと同時に、“子は親からの抽出である（特徴 2-2-1-1）”といった特徴があると考える。

なお、“子は親からの抽出である（特徴 2-2-1-1）”といった特徴は、“全ての子が親の要素の一部になっている（特徴 2-2-1a）”としての特徴に紐づいているのと同時に“親の全

体構成は明確になっていない（特徴 2-2-1b）” といった特徴に起因する場合もあると考えた。これは、親の主張の要素の全体が明確にすることが困難な場合（安全性や利便性などの抽象的な特徴について、要素の全体を挙げるのが難しい場合）が挙げられる。これら 2 つの特徴について共通して “子は親からの抽出である（特徴 2-2-1-1）” といった特徴に基づき、これらをパターン “部分選択” として分類した。なお、パターン “部分選択”、とパターン “MECE” に共通する特徴として “子の成立から親の成立が示される正当性は、それぞれが、親の一部であることに依る（特徴 2-2）” があると考える。

次にこの特徴と対称的な “それぞれの子の成立から親の成立における正当性は、それぞれが異なっている（特徴 2-1b）” といった特徴を持つ分類について考える。

図 18 の GSN について考える。図 18 において、G1 における “許容されるだけ安全である” について、G2 における “操作上のハザードに対処している” と G3 における “安全基準と放棄に準拠していること” とで成立を示そうとしている。ここで “ハザードへの対処”

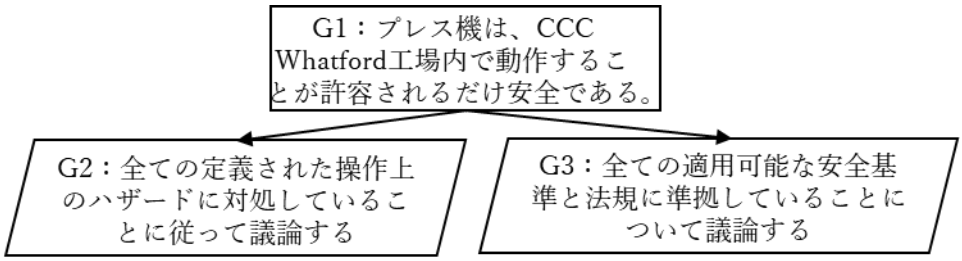


図 18 子同士が互いに助長しあう（[6] Figure41）

と “安全基準と法規に準拠” は、それぞれ、G1 における “許容されるだけ安全である” を示すにあたっての正当性は、それぞれ異なった視点に依るものと考えられる。また、同時に、それぞれが異種的なアプローチの視点であるが故に、それぞれを組み合わせることによって、相乗効果が得られることが期待され、G1 の主張の達成の程度を助長しているとも感じることができる。それは “各子同士の組み合わせが互いに助長しあう（特徴 2-1-1）” の特徴を持つものとして、パターン “合わせ技” と分類するものとした。

なお、このパターンは “それぞれの子は親からのそれぞれの置き換えである（特徴 2-1a）である” といった特徴もあり、これは、パターン “視点変換” の持つ特徴としての “規則性のない視点の置き換えである（特徴 1-1-3）” が複数の子に対して適用されている場合と見なすことができる。

なお “各子同士の組み合わせが互いに助長しあう（特徴 2-1-1）” に該当しないものは、“全ての子が親の要素の一部になっている（特徴 2-2-1a）” 又は “親の全体の構成が子の全てになっている（特徴 2-2-2）” のいずれかに該当するものとみなし、“複数の子を持つ（特徴 2）” 以下におけるパターンの網羅性は確保できていると見なしている。

以上の考察により、“二重否定”、“基準化”、“視点変換”、“MECE”、“部分選択”、“合わせ技”の 6 種類のパターンとした分類について、これらを図 11 の右にように抽出、変換、

組み合わせ、分解といった区分の順番との対比として、それぞれを以下(a)から(f)の順番のパターン記号とすることとした。

(a) 部分選択

(b) 二重否定

(c) 基準化

(d) 視点変換

(e) 合わせ技

(f) MECE

3.2. 主張の関数表現

GSN 上における主張について関数で表現することを考える。

対象をサブジェクトとし、また、対象についての特徴や性質をプロパティとする。さらに、プロパティを関数 P とし、サブジェクトを変数 X とする場合、主張についての関数 P(X)のように表すものとする。

例えば、“システムは安全である”とする主張を表した場合、以下のように表すことができるものとする。

X：システム

P：安全である

P(X)：システムは安全である

3.3. 6 パターンの説明

以下にそれぞれのパターンについての説明を行う。

(a) 部分選択

図 19 の GSN について、2 つの子ゴール G1 、 G2 同士の関係を考える。

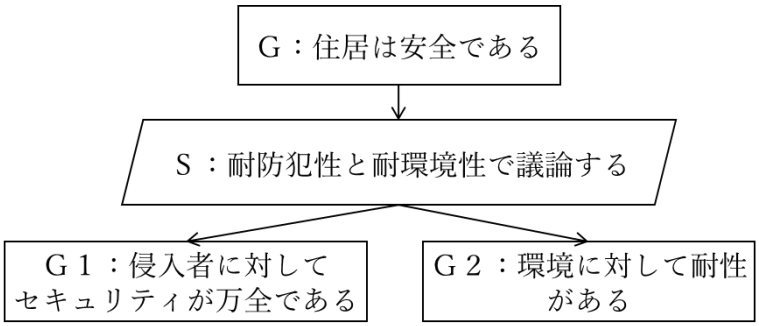


図 19（a) 部分選択

“住居が安全である”といった親における主張を“侵入者に対してセキュリティが万全である”と“環境に耐性がある”とした子の主張の達成で導こうとしている。しかし、ここで、この二つの子で達成を説明しようとしていることには、一種の不完全さを感じるかもしれない。それは、このどちらの子の主張も、親の主張の達成を支えていることには否定できないが、住居の安全については、これら二つの主張だけでは十分であると考えることは難しいからである。これら 2 つの主張における視点だけを用いて“住居が安全である”を説明することは、記述者にとって妥当性があるものと判断されていると考えられる。
（なお、この GSN においてストラテジ S は、子ゴールへの分割における指針を示しているが、内容はゴール G1 と G2 の内容と同じ内容であるために、表記上では省略される場合がある。）

以下のいずれの特徴を全て持つものを、このタイプに分類した。

- 複数の子ゴールは、親ゴールに対しては、全体に対して、部分を表している。
- 子ゴールが親ゴールの主張の部分的要素として選択された視点又は特徴となっている。
- 子ゴールどうしの構成は、親ゴール全体の構成になっているとは考えられない。

本タイプの主張どうしの関係は、以下のような式で表すことができる。
図 19 の GSN において G について

P：安全である
X：住居

とするとき、関数 P、及び変数 X を用いて以下のような式で表すことができる。

P(X)：住居は安全である

と表すことができる。同様に、 G1、G2 については、それぞれ

X：住居
Q1：侵入者に対してセキュリティが万全である
Q2：環境に対して耐性がある

とするとき、関数 Q1、Q2、及び変数 X を用いて以下のような式で表すことができる。

Q1(X)：住居は侵入者に対してセキュリティが万全である
Q2(X)：環境に対して耐性がある

ここで、G1 は G にとって、また G2 は G にとっての必要条件の関係であると言える。また、G2 と G の関係はそれぞれ以下の関係として表すことができる。(“→”は“ならば”をあらわす。)

P(X)→Q1(X)
P(X)→Q2(X)

さらに、n 個の子であるとき以下のように表すことができる。

P(X)→Q1(X)
P(X)→Q2(X)
：
P(X)→Qn(X)

(b) 二重否定

図 20 の GSN について考える。

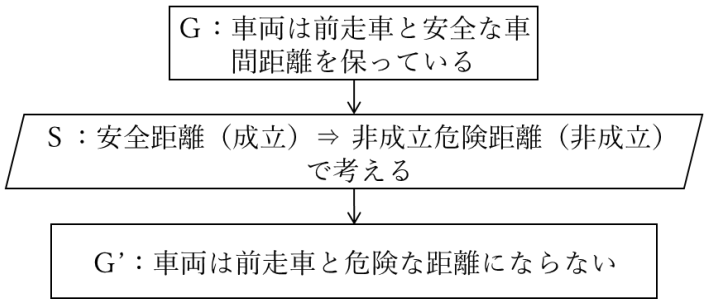


図 20 (b) 二重否定

ストラテジ S により、主張 G は G'に置き換えられていて、置き換え前後の関係は、お互いに二重否定の関係になっている。

この例における置き換えが行われている目的を考えた場合、物体が一定以上であること（つまり安全な車間距離）を検出する仕組みに比べ、一定距離の範囲にあること（つまり危険な距離）を検知する仕組みは、センサ等を用いることで物理的に優位な場合が多い。このように、説明においてより優位な関係の主張に置き換えが行われていると考えられる。

以下の全ての特徴を全て持つものを、このタイプに分類した。

- 変換後の主張が、変換前の主張の代用としての置き換えになっている。
- 置き換え後の主張が、置き換え前のものに対して二重否定の関係になっている。
- 変換前後の主張どうしは、等価としてみなすことができる。

本タイプの主張どうしの関係は、以下のような式で表すことができる。
図 20 の GSN における G について

変数 X：車両
関数 P：前走車と安全な車間距離を保っている

とするとき、関数 P、及び変数 X を用いて以下のような式で表すことができる。

P(X)：車両は前走車と安全な車間距離を保っている

一方で、G' について

変数 X：車両
関数 Q：前走車と危険な距離にならない

とするとき、関数 Q、及び変数 X を用いて以下のような式で表すことができる。

Q(X)：車両は前走車と危険な距離にならない

と表すことができる。
さらに、本タイプでは、二重否定であることから以下の関係が成立する

$Q(X) = \neg \neg P(X)$

(c) 基準化

図 21 の GSN について考える。

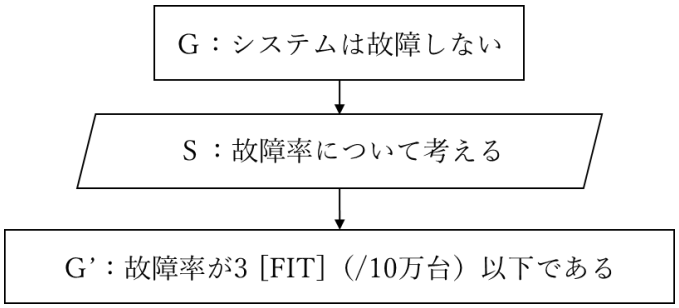


図 21（c) 基準化

ストラテジ S は、主張 G をより明確な基準を伴う 主張 G’ に置き換えている。
以下の全ての特徴を全て持つものを、このタイプに分類した。

- 変換後の主張が、変換前の主張の代用としての置き換えになっている。
- 置き換え後の主張が、置き換え前のものと比較し、より厳しい基準、又は明確な基準となっている。
- 基準が厳しく、又は明確になることで、達成されることの判断基準が十分な程度であると見なされている。

本タイプの主張どうしの関係は、以下のような式で表すことができる。
図 21 の GSN において G について

変数 X：システム
関数 P：故障しない

とするとき、関数 P、及び変数 X を用いて以下のような式で表すことができる。

P(X)：システムは故障しない

G’ について

変数 X：システム
関数 Q：故障率が 3 FIT（/10 万台）以下である

とするとき、関数 Q、及び変数 X を用いて以下のような式で表すことができる。

Q(X)：(システムは)故障率が 3 [FIT]（/10 万台）以下である。

と表すことができる。

本タイプでは、より厳しい基準や明確な基準に置き換えられているとき、Q(X)は、P（X）にとっての十分条件であるとみなされ、以下の関係が成立する。但し、明らかに、数字や程度が十分な程度を持っている場合の他に、変換後においてより明確化がなされる場合は、それが十分であるかの判断は記述者の主観による。

Q(X)→P(X)

(d) 視点変換

図 22 の GSN について考える。

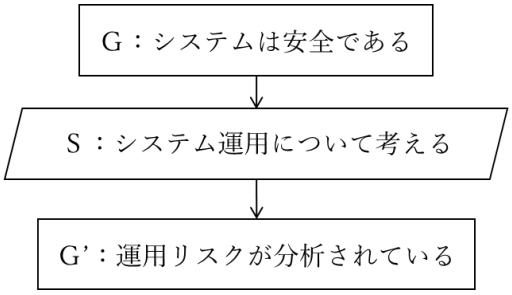


図 22 (d) 視点変換

最初のゴール G における主張をより、説明しやすい主張の内容としてのゴール G‘ に変換がなされている。この例において、主張が置き換えられた理由を考える。まず、安全であるという性質を説明、証明すること一般的には難しい。そこで、運用時におけるリスクの分析がなされていることを説明することで、安全であることを達成されていることを試みている。

以下の全ての特徴を持つものを、このタイプに分類した。

- 変換後の主張が、変換前の主張の代用としての置き換えになっている。
- 置き換えに際して、必然である法則性は見られない
- 説明しやすい（又は理解されやすい）主張に置き換えが行われている。

本タイプの主張どうしの関係は、以下のような式で表すことができる。

図 22 の GSN における G について

変数 X：システム
関数 P：安全である

とするとき、関数 P、及び変数 X を用いて以下のような式で表すことができる。

P(X)：システムは安全である

G’ について

変数 X：システム
関数 Q：運用時リスクが分析されている

とするとき、関数 Q、及び変数 X を用いて以下のような式で表すことができる。

Q(X)：(システムは)運用時リスクが分析されている。

さらに、本タイプでは G の視点は、G’ に置き換えられて関係であるが、その置き換え後の主張の形態は唯一無二であるものではなく、記述者の都合や利点に依存したものに沿ったものになると考えられる。

(e) 合わせ技

図 23 の GSN について、2 つの子ゴール G1、G2 どうしの関係を考える。
“システムが安全である”という親における主張を“機構上の安全性”と“製造過程の品質の

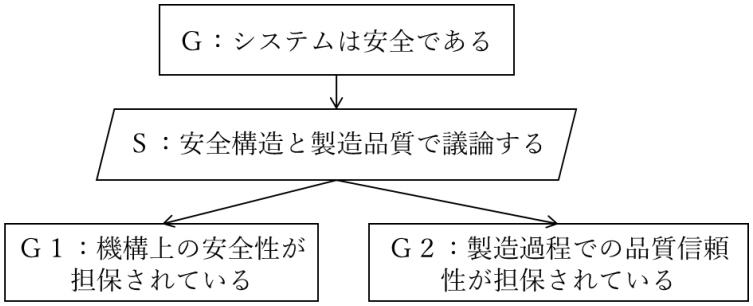


図 23 (e) 合わせ技

信頼性”といった二つの視点の達成で導こうとしている。ここで、これら二つの子の主張同士の関係性を考えた場合、これら 2 つの主張が、“システムが安全である”といった主張の何かしらの要素の分解によって得られた要素であるとは考えにくい。
この類のものは分解の分類（後述のパターン(f)）とは異なるタイプとであり、さらに、子における二つの主張が共に達成されることで、親の主張の達成を示そうとするものと

して“合わせ技”とする。（なお、この GSN においてストラテジ S は、分割における指針を示しているが、内容はゴール G1 と G2 の内容と同じ内容であるために、表記上省略される場合がある。）

以下の全ての特徴を全て持つものを、このタイプに該当する。

- それぞれの子ゴールが、親ゴールからの分解ではない。
- 各子ゴールには、それぞれ異なる特徴、又は視点に従って親ゴールから置き換えられた主張が定義されている。
- それぞれの子の主張が、単体として、親の主張の達成を示すことについて、一定の妥当性がある。
- 各子のゴール同士の達成を併せて示すことでそれぞれの達成として示す場合に比べ、相乗的な効果として親の主張の達成がなされていると感じられ、それぞれが個別に示されるよりも、より納得の合理性が増したものとして受け入れられる特徴がある。

本タイプの主張どうしの関係は、以下のような式で表すことができる。

図 23 の GSN における、G について

変数 X：システム
関数 Q：安全である

とするとき、関数 P、変数 X を用いて以下のような式で表すことができる。

P(X)：システムは安全である

と表すことができる。同様に G1 、G2 について、

変数 X：システム
関数 Q1：機構上の安全性が担保されている
関数 Q2：製造過程の品質信頼性が担保されている

とするとき、関数 Q1、Q2 及び変数 X を用いて

Q1(X)：システムは機構上の安全性が担保されている
Q2(X)：システムは製造過程の品質信頼性が担保されている

と表すことができる。

なお、Q1(X) と Q2(X) とはそれぞれ“機構上の安全性”と“製造過程の品質信頼性”といった異種の特徴としてアプローチであり、それぞれが個々に達成した場合に比べ、より相乗的に納得の合理性を得られるものと考えられる。

(f) MECE

（MECE は、“Mutually Exclusive and Collectively Exhaustive”の略であり、“互いに重複せず、全体として漏れがない”の意味を指すものとする。）

図 24 の GSN について考える。

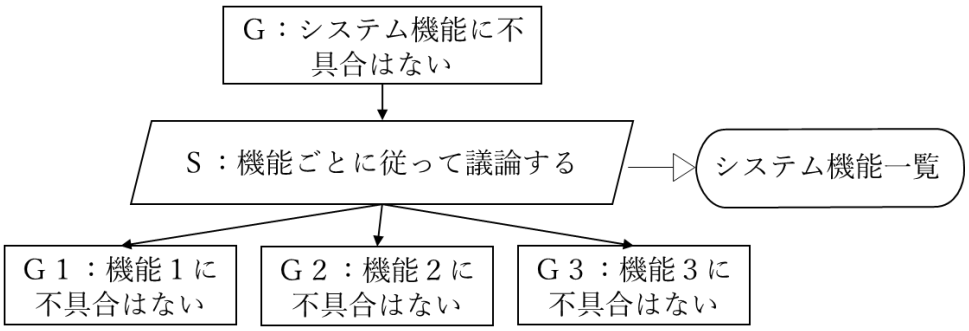


図 24（f) MECE（サブジェクト）

この GSN において、親における主張“システム機能に不具合はない”に対して、各子のゴールの主張においてそれぞれの機能に不具合がないことが説明しようとしている。されあにストラテジ S に対して接続されたコンテキストにおいて“システム機能一覧”としてシステムの機能構成の全体（の存在）が定義されている。つまり、このシステムにおける機能は、機能 1、機能 2、および機能 3 で全体が構成されているとする前提が与えられていると想定できる。それらより、各子ゴールにおける主張がそれぞれ全て達成された場合（全て機能において確認された場合）に、親ゴールの“システム機能に不具合はない”の達成がなされるものとしている。

本タイプの主張どうしの関係は、以下のような式で表すことができる。

図 24 の GSN における G について

変数 X：システム機能
関数 P：不具合がない

とするとき、関数 P、変数 X を用いて以下のような式で表すことができる。

P(X)：システム機能は不具合がない

と表すことができる。
同様に、G1、G2 、G3 については

X_1：システム機能 1
X_2：システム機能 2
X_3：システム機能 3
関数 P：不具合がない

とするとき、関数 P 、及び変数 X_1、X_2、X_3 を用いて

$P(X_1)$：（システム）機能 1 に不具合はない
$P(X_2)$：（システム）機能 2 に不具合はない
$P(X_3)$：（システム）機能 3 に不具合はない

と表すことができる。
本タイプでは、サブジェクトとしての変数 X が、X_1、X_2、X_3 は、分解されている。

別の例を考える。
図 25 の GSN における、G について

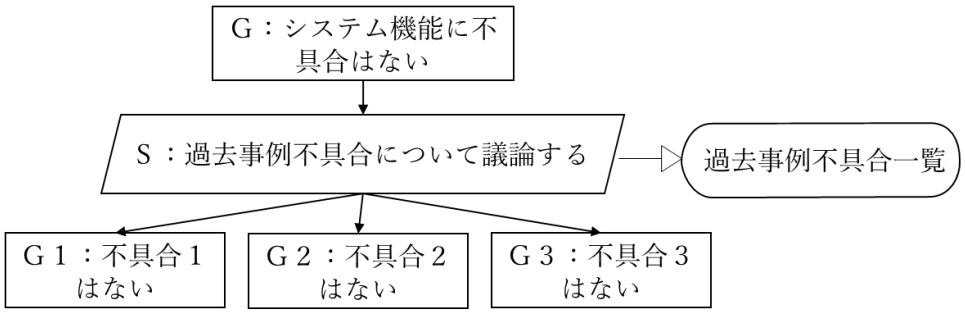


図 25（f) MECE（プロパティ）

変数 X：システム機能
関数 P：不具合がない

とするとき、関数 P、変数 X を用いて以下のような式で表すことができる。

P(X)：システム機能は不具合がない

と表すことができる。
同様に、G1、G2 、G3 について

関数 P_1：不具合 1 がない
関数 P_2：不具合 2 がない
関数 P_3：不具合 3 がない

とするとき、関数 P_1、P_1、P_3、及び変数 X を用いて以下のような式で表すことができる。

$P_1(X)$：システムに不具合 1 がない
$P_2(X)$：システムに不具合 2 がない
$P_3(X)$：システムに不具合 3 がない

と表すことができる。
本タイプでは、プロパティとしての関数 P が、P_1、P_2、P_3 は、分解されている。
（図 25 においては、図 24 と同様に、コンテキスト（“過去事例不具合一覧”）によって、不具合 1、不具合 2、不具合 3 が、不具合の全体であるものと見なす。）

以下のいずれの特徴を全て持つものを、このタイプに分類する。

- それぞれの子ゴールが、親ゴールからの分解となっている。
- 分解の対象は、サブジェクトに対して行われている場合と、プロパティについて行われている場合がある。
- それぞれの子ゴールの全てが漏れなく達成することで、親ゴールの達成が得られる妥当性がある。

3.4. 特徴の分析

6 パターンそれぞれについて、以下特徴の視点で分類を行い、それらを表 1、表 2 にまとめる。以下、それぞれの特徴の視点(1)から(9)について説明する。

(1) 子主張の数

- パターン(e)、(f)は複数の子構造を持つ。子主張の数は“複数”となる。
- パターン(b)、(c)、(d)は単一の子構造を持つ。子主張の数は“単数”となる。
- パターン(a)は、特徴(2)の“子階層への変化の形態”において、“抽出”の形態であることから、“複数”の他に“単数”の形態をとる可能性もあると見なされる。

(2) 子階層への変化の形態

- パターン(a)は、親に対して子は部分的な関係であるため”抽出”とみなす。
- パターン(b)、(c)、(d)は、単一の子を持つ構造における“変換”と見なされる。パターン(d)は複数の子を持つ構造であるが、それぞれの子は、それぞれ親からの変換でみなされるため同様に“変換”と見なされる。
- パターン(e)は、複数の子に対して、それぞれ“変換”がなされていると見なされる。
- パターン(f)における子は、親に対して網羅的でかつ全体からの”分解”であると見なされる。

(3) 変化の対象

主張が分割又は変換される場合、理論的には、その対象はサブジェクト、プロパティのどちらでも可能である。しかし、今回パターンマッチングの結果としては、4.3 章の表 5 に示すように、パターン(f) を除いては、対象は、全てプロパティであった。そのため、この結果を優先し、パターン(f) はサブジェクト、プロパティ（のどちらか一方ずつ）とし、パターン(f) 以外は全ての対象はプロパティのみであるとする特徴とした。

(4) 帰納的、又は演繹的

変換または分割された主張どうしが、元の主張の達成に対する関係を考える。

- パターン(a)：抽出後の部分から全体の達成を示そうとする性質は帰納的な関係であると言える。
- パターン(b)：二重否定は、論理的に等価な変換であり演繹的な関係と言える。
- パターン(c)：変換された基準は、親の主張の基準に対して、より高度なもの、又はより明確さが増すものとして、より高い納得の合理性を持ったものに変換される。子は親に対して演繹的な関係であると言える。
- パターン(d)：視点の置き換えは、元の主張の達成を示すにあたっての、記述者にとっての固有の戦略的な置き換えと言える。固有な置き換えであるため帰納的、演繹的のどちらでもないと言える。
- パターン(e)：複数の子の主張は、親の主張の達成を示すにあたっての、相乗的に示すための、複数の主張であると言える。それぞれの子の主張については(d)と同様に、固有な置き換えであるため帰納的、演繹的のどちらでもないと言える。
- パターン(f)：親の主張に対して網羅性を以て説明がなされる妥当性は演繹的であると言える。

(5) 必要、十分条件

- パターン(c)については、変換後の子の主張が、変換前の親の主張に対して基準化がなされることで、明確さが増す、または、より高度又は厳格な基準へ変換され、それは親の主張に対して“十分条件”であると言える。
- パターン(b)、(f)は親子の関係は“等価”であると言える。
- パターン(a)は子が親の部分であることを持って、“必要条件”であると言える。
- パターン(d)、(e)は、主張の視点が変換されていることにより、同様に判断ができないと考え、“どちらでもない”と言える。

(6) 記述者/読み手の解釈

パターン（b)、(f）は親と子の等価な関係からも記述者（又は読み手）の解釈に“依存しない”とされる。また、パターン(c)は、基準化により、明確さ、厳格さが増すことから、それらが普遍的である前提のもとに、同様に“依存しない”とされる。
一方、パターン(d)、(e)については、親から子への主張の変換がなされていることから、その変換の合理性は記述者（又は読み手）の解釈に“依存する”と考えられる。
パターン(a)については親に対して子が部分とされることの妥当性は同様に記述者（又は読み手）の解釈に“依存する”と考えられる。

(7) 議論の強弱

それぞれのパターンにおいて、子ゴールの達成から得られる親ゴールの関係はそれらの特徴の違いにより、子の主張の達成により、親の主張が達成されることは、議論としての強弱が存在するものと考えられる。子の主張で達成していることが、親の主張での達成を上回っていると記述者（又は、読み手）が感じる場合、“強まる“とみなす。一方で、その逆は、“弱まる”ものと識別するものとする。

- パターン(c)においては、親に対する子の関係は、十分条件であることから“強める”関係であるといえる。これは、基準化における明確化や厳格化が一般的に同意されるものであることが前提とした場合、その変換は、子の主張が、親の主張に対して“強まる”とみなされる。
- また、パターン(e)においては、単一の子の主張と他の子の主張が相乗的に高める性質があると考える。そのため、その効果は結果的に“強める”ことにつながると考える。但し、この場合の“強まる”度合は、記述者（または読み手）の解釈によって異なるため、“不変、又は強める”とした。

- 一方でパターン(a)においては、子が親の部分的なものであることから、“弱まる”と考える。但し、これも部分が全体に対して、部分的なものであっても説明するのに十分であると記述者（又は読み手）が解釈する場合を考慮し“不変、又は弱まる”とした。
- パターン(b)、(d)、(f)については“不変”としている。但し、パターン(b)と(f)は、親子の関係は等価であることで、記述者（又は読み手）の解釈に依存せず、“不変”となる。一方でパターン(d)は、親から子へ視点の変換が置き換えられているため、その強弱は“不変”としたが、その度合いは、記述者（又は読み手）の解釈に依存する。

(8) 特徴を表す式

それぞれのパターンにおける分割、変換における特徴を表す式は、3.3 章においてパターン毎に示しているものをまとめたものである。

(9) 関連する既存研究での分類

関連する既存研究における分類である。
既存研究と関連性があるものについて表 1 の(9)に挙げている。なお、それぞれとの関連性についての考察は、6 章にて行う。

表 1 特徴によるまとめ（1/2）

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
パターン名	子主張の数	子階層への変化の形態	変化の対象	帰納的/演繹的/どちらでもない	必要条件/十分条件/等価	記述者/読み手の解釈	議論の強弱
(a)部分選択	単数/複数	抽出	プロパティ	帰納的	必要条件	依存する	不変、又は弱まる
(b)二重否定	単数	変換	プロパティ	演繹的	等価	依存しない	不変
(c)基準化	単数	変換	プロパティ	演繹的	十分条件	依存しない	強める
(d)視点変換	単数	変換	プロパティ	どちらでもない	どちらでもない	依存する	不変
(e)合わせ技	複数	変換	プロパティ	どちらでもない	どちらでもない	依存する	不変、又は強める
(f)MECE	複数	分解	プロパティ/サブジェクト	演繹的	等価	依存しない	不変

表 2 特徴によるまとめ (2/2)

	(8)	(9)
パターン名	変換式	関連する既存研究での分類
(a)部分選択	親：P(X)に対して、子：Q1(X)、Q2(X)、Qi(X)と表され、以下の関係がある。 P(X)→Q1(X)、P(X)→Q2(X)、...、P(X)→Qi(X)	Concretion block [17]
(b)二重否定	親：P(X)に対して、子：Q(X)と表され、以下の関係がある。 Q(X) = ¬¬ P(X)	Substitution block [17]
(c)基準化	親：P(X)に対して、子：Q(X)と表され、以下の関係がある。 Q(X)→P(X)	Substitution block [17] Safety margin [18]
(d)視点変換	親：P(X)が、子：Q(X)に置き換えられている。	Substitution block [1 7]
(e)合わせ技	親：P(X)が、子：Q1(X)、Q2(X)として置き換えられている。 Q1、Q2のそれぞれが単独で達成することで得られる確信より、両方が同時に達成される場合に得られる確信の程度の方が大きい。	Multi-legged argument [13][14] Diveese Argument [18]
(f)MECE	親：P(X)が子：P(X1)、P(X2)、P(Xi)（P=P1+P2+…+Pi）に置き換えられる。 又は、親：P(X)が子：P1(X)、P2(X)、....、Pi(X)（X=X1+X2+…+Xi）に置き換えられる。	アーキテクチャ分解、他[12] Decomposition block [17]

3.5. まとめ

数十個のサンプル調査による初期調査から、パターン分類の視点を検討した。6 パターンに分類できることを示し、さらに、6 パターンについて、最終的に 7 つの特徴の視点により、比較し、また、特徴を表す式により表現をした。これらより、6 個のパターンは、特徴として重複するところはなく、それぞれが、それぞれ異なった特徴を持ち得ていることが確認された。既存研究における分類と比較については、6 章で行う。

第 4 章 GSN のパターンマッチング

4.1. パターンマッチングによる検証

前章の 6 パターンの特徴に基づき、サンプル調査を続け、サンプル数を増やすことを行った。本研究の 6 パターンの分類は、幾つかの既存の GSN のモデルの調査を行い、分類を行ってきている。そのため、それら分類の妥当性を検証するために、さらに、GSN モデルについてのそれらのパターンが当てはまることを確認するための調査を行った。
サンプルの調査範囲は、以下の通りである。

調査方法：インターネット Google、及び Google scholar を用いた検索

対象：公開されている論文に GSN サンプルについてダウンロード可能なもの

キーワード：“GSN” 及び ”Safety Case”を含むもの（各条件共通）

なお、ダウンロード可能が可能なもの論文の数は、全部で 1025 であったのに対して、89 の論文について、以下の 3 種類の条件において調査を行い表 3 のようになった。
なお”関連性で並び替え”は、Google Scholar で設定可能な指定値である。

条件 1 ：Google：無作為

条件 2 ：Google Scholar：関連性で並び替え、期間指定：なし

条件 3 ：Google Scholar：関連性で並び替え、期間指定：2021 年の全部と 2020 年の一部

階層の制限：ゴール、又はストラテジの階層は 1 つの GSN 上で 5 階層までとしている。これは、公開されている GSN の中のほとんどは 5 階層以下に収まっているが、一部それを超えた階層のものについては、限度を 5 階層までとしている。

表 3　GSN サンプル調査数

検索条件	論文数	GSN数	パターン数
条件 1	10	76	137
条件 2	56	156	436
条件 3	23	41	145
合計	89	273	718

4.2. 各パターンのマッチングの例

以下に GSN 上でのパターンマッチングの例を示す。

1 つ目の例を図 26 に示す。

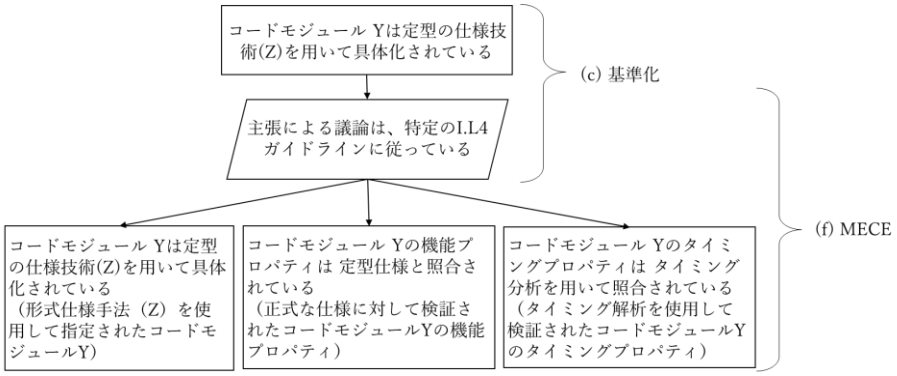


図 26 パターンマッチング例（ [18] Figure 19）

ゴールが、ストラテジを介して 3 つのゴールに分割されている。ストラテジは、下層の 3 つのゴールに分割する役割を担っていて、その関係は、(f)MECE であるものと判断している。なお、ストラテジのガイドラインは、親のゴールにおける“具体化されている”に対して、その具体化されている判断基準を与えていると考えられる。つまりストラテジは“具体化されている”を“I.L4 ガイドラインに従っている”に置き換えている主張を含んでいるとみなされる。従って、この GSN には、パターン“(c)基準化”とパターン“(f) MECE”の 2 つのパターンを含んでいると見なされる。

2 つ目の例を図 27 に示す。

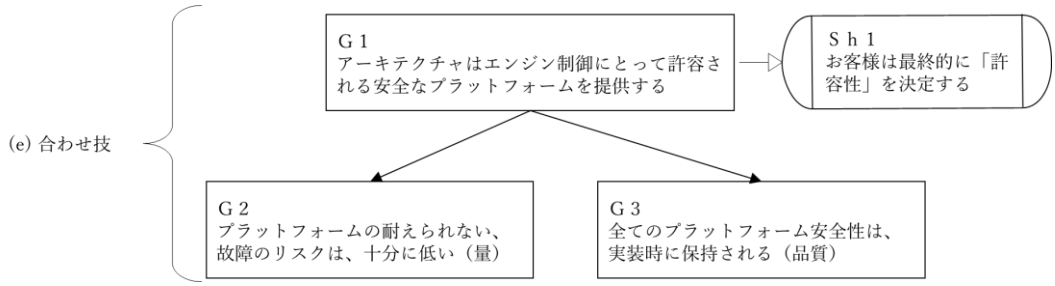


図 27 パターンマッチング例（ [18] Figure 43）

親ゴール G1 がストラテジを介さずに 2 つの子ゴール G2 と G3 とでその達成を支持されている。G2 における“量”としてと、G3 における“品質”としての 2 つの視点でのアプローチの掛け合わせとして、G1 の主張の達成を示そうとしているためパターン“(e) 合わせ技”として合致させることができる。なお Sh1 のノードは、ステークホルダについての明確化をするためのコンテキストの拡張である（ [6]-ANNEX B2 ）。

4.3. 各パターン一致数

パターンごとの一致数は表 4 のとおりであった。

表 4　各パターンに対して一致した数

パターン名		一致数
(a)	部分選択	16
(b)	二重否定	9
(c)	基準化	105
(d)	視点変換	183
(e)	合わせ技	199
(f)	MECE	206
該当なし		0
合計		718

なお、調査した全 GSN と、それぞれのマッチングの様子は、付録の章に記載をしている。

各パターンにおいて分割、変換が行われている対象についてプロパティ、サブジェクトのどちらに対して行われているかの集計し、表 5 のようになった。

表 5　ノード木構造ごとの一致数

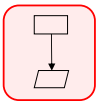
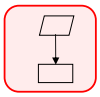
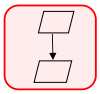
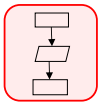
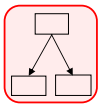
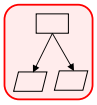
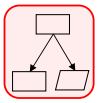
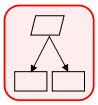
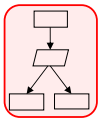
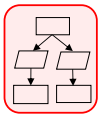
パターン名		サブジェクト	プロパティ	計
(a)	部分選択	0	16	16
(b)	二重否定	0	9	9
(c)	基準化	0	105	105
(d)	視点変換	0	183	183
(e)	合わせ技	0	199	199
(f)	MECE	21	185	206
合計		21	697	718

4.4. 木構造としてのマッチング

マッチングにおける木構造上と 6 パターンとのマッチングの結果は表 6 のとおりであった。部品が 3 階層になっているものは、2 階層目のストラテジで表現されている内容が、2 階層目のゴールと同じ内容の説明になっているものであり、それらは、1 階層目と 3 階層目の主張の関係性で捉えることができるものとして分類している。

なお、ストラテジが子として配置されている例も多くあり、これらはストラテジに隠れた主張があるものとして読み取ることで、これらを主張の親子関係の構造として捉えることが可能となっている。また、表 6 の No.8 のように、子が、ゴールとストラテジの混在のものも見つかっており、これらも同様にストラテジに含まれる主張を読み取ることで、GSN の主張同士の関係として捉えることができている。

表 6　分割及び変換の対象

No.	木構造	(a)	(b)	(c)	(d)	(e)	(f)	Total
1	 G→G	1	1	33	30	0	0	65
2	 G→S	1	5	17	133	0	0	156
3	 S→G	0	0	51	13	0	0	64
4	 S→S	0	0	1	0	0	0	1
5	 G-S-G	0	3	3	6	0	0	12
6	 G→Gs	5	0	0	1	92	47	145
7	 G→Ss	2	0	0	0	28	8	38
8	 G→G,S	1	0	0	0	10	1	12
9	 S→Gs	9	0	0	0	44	104	157
10	 G→S→Gs	0	0	0	0	24	42	66
11	 G→Ss→Gs	0	0	0	0	2	0	2
Total		19	9	105	183	200	202	718

4.5. まとめ

6 パターンの適用妥当性を確認するために、パターンマッチングを行った。
718 のパターンについて調査を行い、それらを 6 パターンいずれかに当てはめることができ、6 パターンの可用性が確認された。

なお、パターン(b)及びパターン(f)は、等価な関係として、子の主張への展開を形成するが、それらは、全体の 1/3 以下に留まっている。それ以外のパターンは、何かしらの置き換えが行われていると考えられるが、そのことはセーフティケースを GSN 上で論証を展開する上で、多くの場合、階層間で何かしらの置き換えがなされることが必然的であるものと見なすことができる。

同時に、調査したパターンについて、変換や分割の対象となる対象（プロパティ、サブジェクトのどちらか）についての数の集計、及び、ゴール、ストラテジの木構造の分類数も集計を行った。それらより、それぞれのパターンの使用頻度とそれが用いられている GSN 上でのノード部品の構成についての傾向が分かった。なお親子、及び、子同士の関係としての、ゴールとストラテジの組み合わせは、多くのバリエーションが見つかったことより、ゴールだけでなく、本パターン分類において、主張同士の関係として捉えることが有効であったことも確認された。

第５章　ワークショップによる検証

分類した６パターンについて、それぞれの特徴としての妥当性、及び分類のされ方について検証を行う目的として、ワークショップを開催した。

5.1. オンライン方式による実施

本ワークショップ実施時期は、新型コロナウィルスの影響により、対面方式での実施が困難な状況にあった。そのためオンライン方式での実施を検討し、同時に、オンライン方式でもワークショップを効率的に行うための実施方法の検討、及びツール選定を行った。

また、演習実施を考慮した場合、５～６人程度であれば、一つのグループで行うことが可能であるが、それ以上の場合は、グループ分けが望ましい。なお、従来の対面方式の場合、各グループに分かれ、それぞれのグループにおいて、ホワイトボード、模造紙等上に付箋紙等で、互いが意見交換をしながら、作図することが可能であった。

そこで、グループ内での会話と、作図を行う場所を、それぞれ Zoom の Breakout room 機能と、D-case Communicator [7]での共同作業画面を用いて実現することで、従来の対面方式と同等の環境を目指すものとしている。

- **D-Case について**

D-Case とは、Dependability Case の略で、セーフティケースをはじめとするアシュアランスケースを表現する手法として使われている。また、D-Case は、変化に対応するサイクルとして定義されており、それらは、DEOS プロセスとして定義されている [8]。
なお、D-Case における図法は、GSN モデルにおける図法をベースに拡張している [9]。
また、D-Case Communicator は、GSN モデルの図法をサポートしている。

- **D-Case Communicator について**

D-case Communicator [7] は、サーバ上で稼働し、クライアントからログインしたサーバ上に GSN を作成することができる。サーバ上に作成した GSN は、指定したユーザと共有することが可能であり、ユーザ同士で同一画面上において同じ GSN に対して同時に編集することが可能である。図 28 は、作成した GSN について共有しているユーザとの関係を示している画面である。（本ツール上で GSN は D-Case と表現されている。）

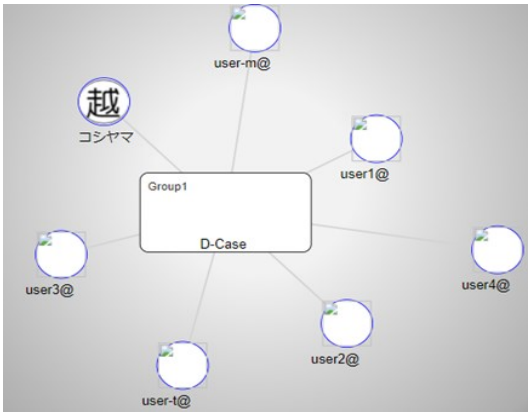


図 28 D-Case（GSN）図の共有関係画面

図 29 に示す作図エリアは 4 人のユーザによる同時作成を行っている例であり、各ユーザは自分の作図している領域をウィンドウ内で好みの位置、及び縮尺に調整することが可能である。図の編集状態は共通の作図エリア上で即時更新されるため、同一グループ内で、他のユーザの作図状態を参考にしながら進めることが可能である。

なお、D-case Communicator 作図操作は共有できるが、音声は共有できないため、音声は、Zoom を介して共有される。

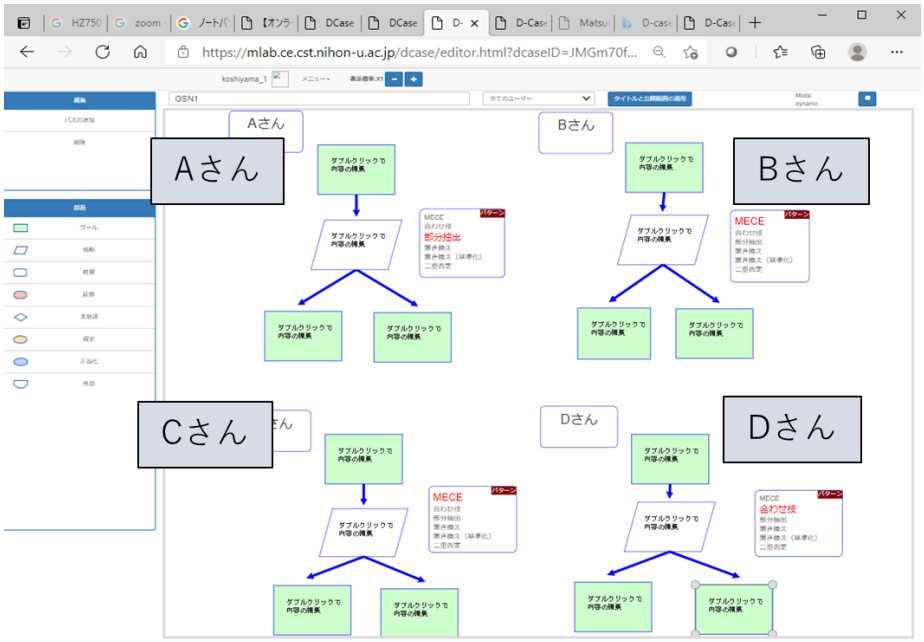


図 29 D-Case communicator 編集画面

5.2. 全体概要

ワークショップは 2 回実施した。それぞれの実施について表 7 に示す。ワークショップ＃1 は、ワークショップ#２に先行して行われ、ワークショップ#1 は、限定的な対象者（株式会社チェンジビジョンのエンジニア）に対し、ワークショップ#２は一般募集により参加者を募集している。

GSN 編は、ワークショップを行うことで、6 パターンの妥当性検証を行うことを目的としている。6 個のパターンの考え方は、既存の GSN モデルサンプルに対して、パターンマッチングを行うことでその可用性を検証しているが、一方で、これから GSN モデルを作成しようとする技術者にとっての可用性を検証する目的で行っている。

なお、ワークショップ#１では、GSN 編に加えて、SCDL 編の実施を行っている。

これは、GSN モデルの作成を、システムの安全機構設計と併せて作成することの効果を狙ったものであり詳細については 7 章で説明をする。

表 7 各ワークショップの実施形態

	ワークショップ ＃１	ワークショップ＃２
講師人数	2名	3名
参加人数	11名	11名
時間	4時間	3時間
実施環境	リモート	リモート
使用ツール	Zoom Astah SystemSafety	Zoom D-Case communicator
構成	GSN編 ＋SCDL編	GSN編
全体演習	参加者全員に対して例題を示し、各自が該当すると思われるパターンをZoomの挙手機能で意思表示を行う	参加者全員に対して例題を示し、各自が該当すると思われるパターンをZoomの挙手機能で意思表示を行う
個別演習作業	各自のPCで個別で作成する	Zoom ブレークアウトルームで音声を、D-Case Communicatorので作図エリアを各グループ毎に共有する
個別演習の発表	任意で指名し、参加者全員への画面共有で発表を行う	Zoom 上でD-Case Communicatorの各グループ画面を参加者全員で共有

GSN 編では、内容と演習については、2 回の開催において同一である。前半は、主にはパターンについての考え方の説明を行っている。また説明後に幾つかの GSN モデルサンプルを示し、当てはまると思うパターンに手を挙げてもらい（Zoom での挙手機能）、パターンマッチングに対する考え方の理解度を確認し、個別演習に向けての理解度の確認を行うことで、その後の個別演習への準備としている。説明時及び全体演習時には、参加者は、適宜 Zoom のチャット機能を用いて随時質問をすることができる。なお、全体演習（数サンプル）と個別演習時間は、それぞれ 30 分間程度として行った。

個別演習では、課題は 2 回のワークショップにおいて同一の内容であり、各自が共通で与えられた課題について GSN モデルを作成し、さらにそれぞれが作成した GSN モデル

の木構造（主張同士の関係）に対して、当てはまる箇所にそのパターンを示すことを行う。

なお、個別演習は、2 回のワークショップで、それぞれ実施の形態が異なっている。ワークショップ＃ 1 は、各自が自分の PC 環境で作業し、発表時には、Zoom での全員に対して、個々の画面を共有する方式に行っているのに対し、ワークショップ＃ 2 では、Zoom の Breakout room 機能を使用することでグループ分けでの作業を可能になるようにしている。一方、作図作業は、D-Case Communicator 上で、グループ毎の共有画面上での複数人同時作業を行うことを可能としている。D-Case Communicator の共有画面上では、各自の作図における操作は時間の遅れに対しても違和感なく編集が可能であり、また編集した内容はグループ内のメンバーに即時共有することが可能である。しかし音声は共有できないため、Zoom を介しての音声共有と併用することで対面方式のグループワークと近しい環境を提供している。

演習時は、講師も各グループの Zoom と、D-case communicator 画面にログインし、適宜アドバイスを行うことで、演習時の疑問点を早い段階で解決させ演習作業の滞りを防止することが可能である。

また、この 2 つのツールを併用した共有化は、作図時にはグループ内の他の人の作図状況を互いに参考にすることを可能とし、また演習結果の発表時には各グループ単位での作図結果画面を効率よく共有することが可能となり、作図と発表の作業を効率的に進行させることを可能としている。

5.3. 演習の実施

参加者が 6 パターンについての説明を受けた後に、以下の課題について演習を行った。これは、各パターンの特徴について参加者に伝わり理解されているかの確認に加え、実際に 6 パターンの考え方が、第三者にとって GSN 作成時に使うことができるかの有用性の確認を行うためである。以下が行った課題である。（SCDL 編の演習については、7 章で説明を行う。）

課題：（2 回の各ワークショップ実施において、課題の内容は同一である。）

- トップ事象のゴールの主張に対して、下層に向けて、各自 GSN を作成する
- 階層は、2～3 階層を目安とする。
- 作成した GSN 上のゴール間又は、ストラテジ間で該当箇所と思われる箇所に、本 6 パターンのいずれかとのマッチングを示す。

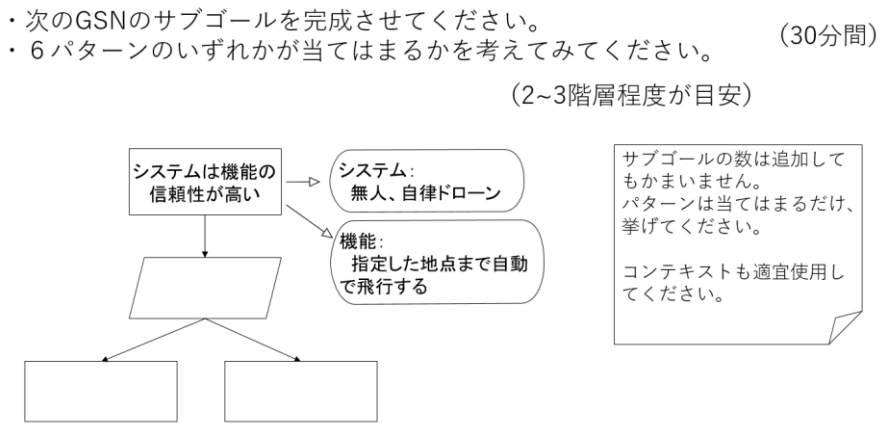


図 30 演習問題

5.4. 演習の成果物

● 演習結果及び作成された成果物

２回の開催において参加者が作成し（回収ができたものの）サンプルを以下に示す。ワークショップ＃１（サンプル１－１～サンプル１－５）とワークショップ＃２（サンプル２－１～２－８）を以下に示す。

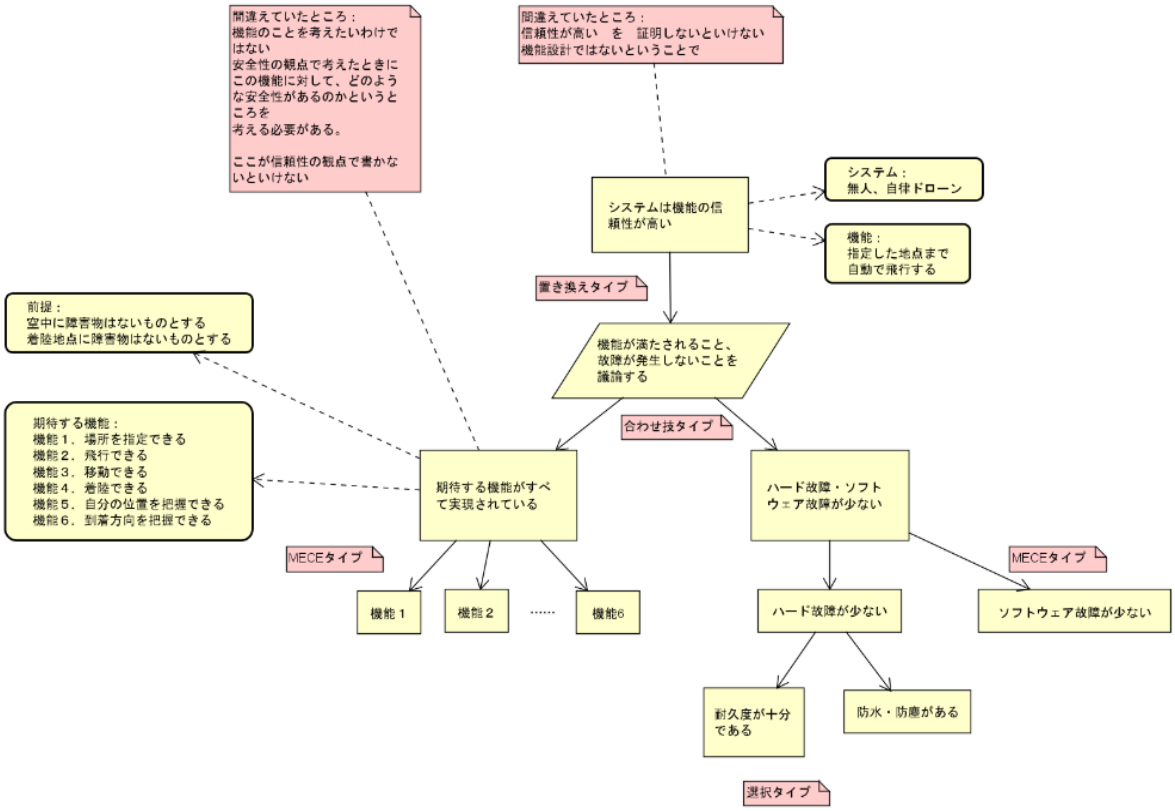


図 31 作成された GSN（サンプル 1 - 1）

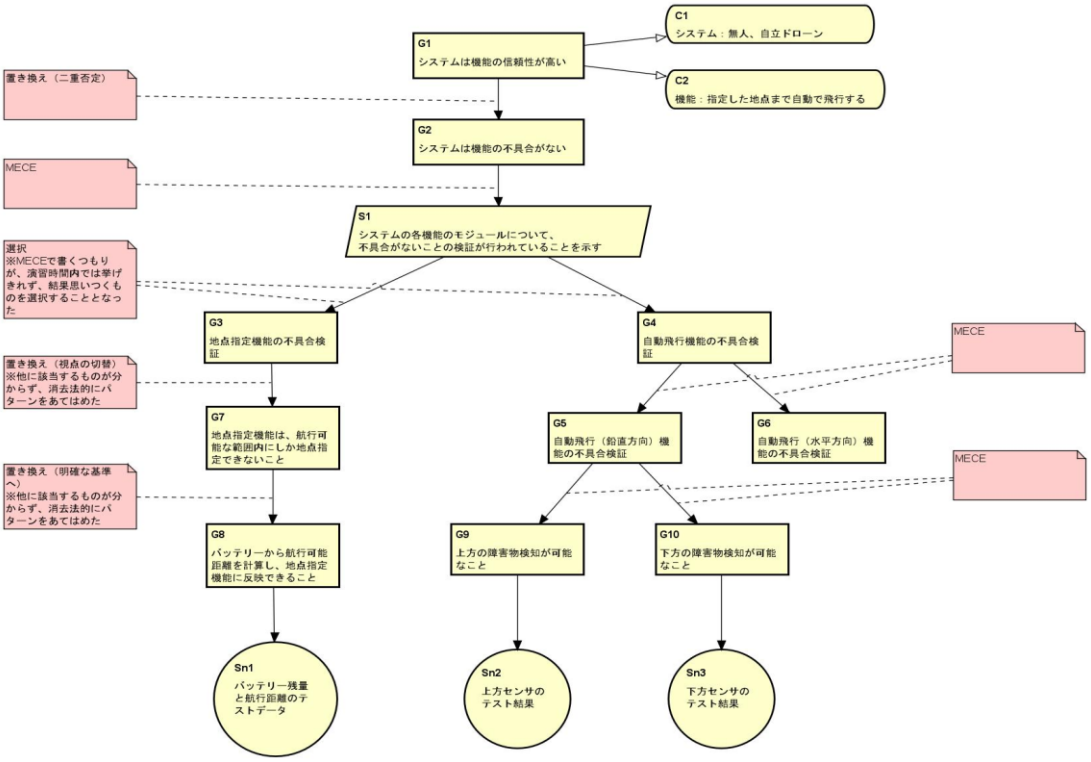


図 32 作成された GSN（サンプル 1 - 2）

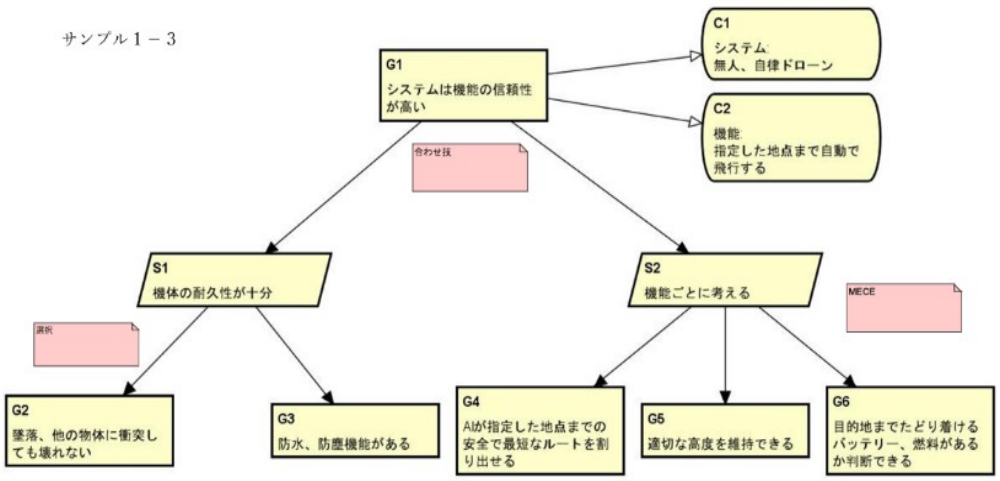


図 33 作成された GSN（サンプル 1 - 3）

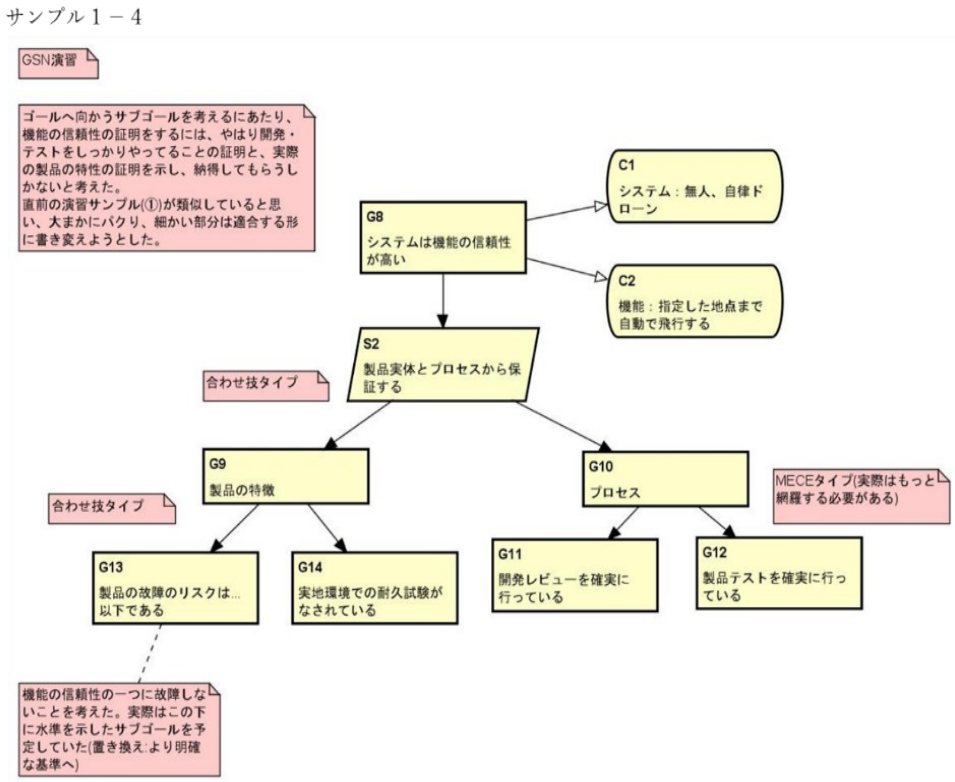


図 34 作成された GSN（サンプル 1 - 4）

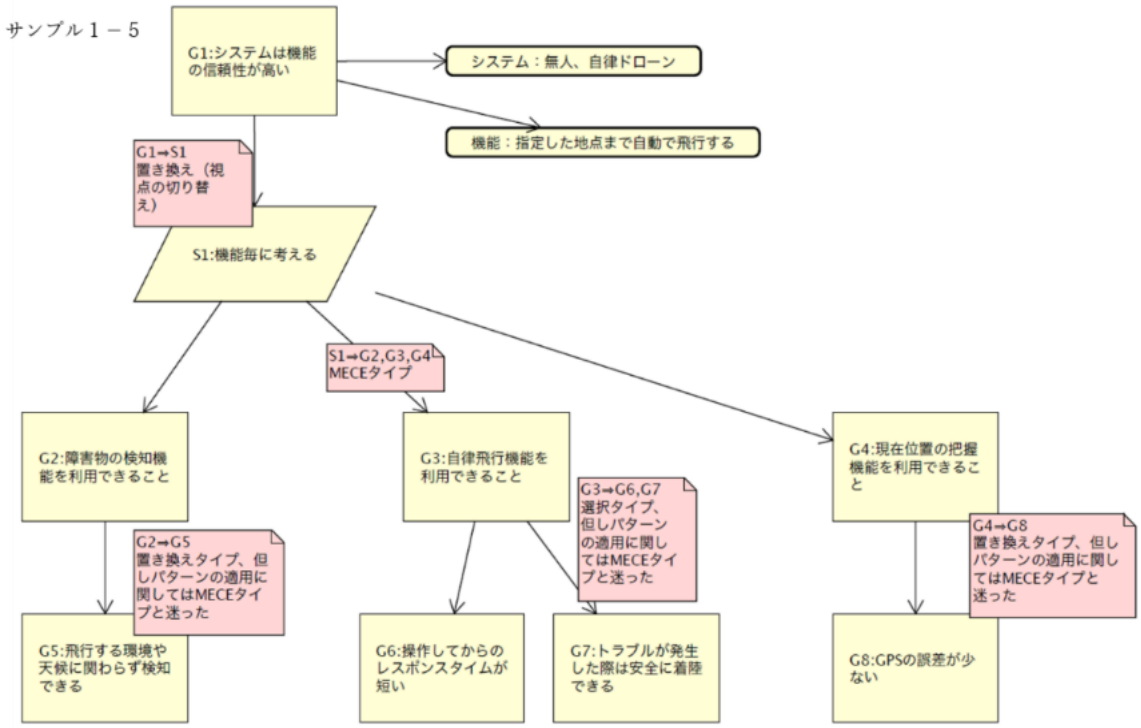


図 35 作成された GSN（サンプル 1 - 5）

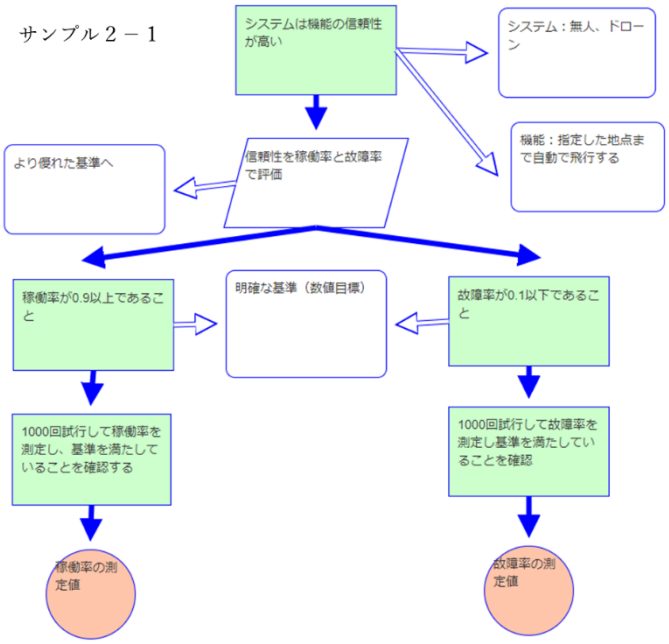


図 36 作成された GSN（サンプル ２-１）

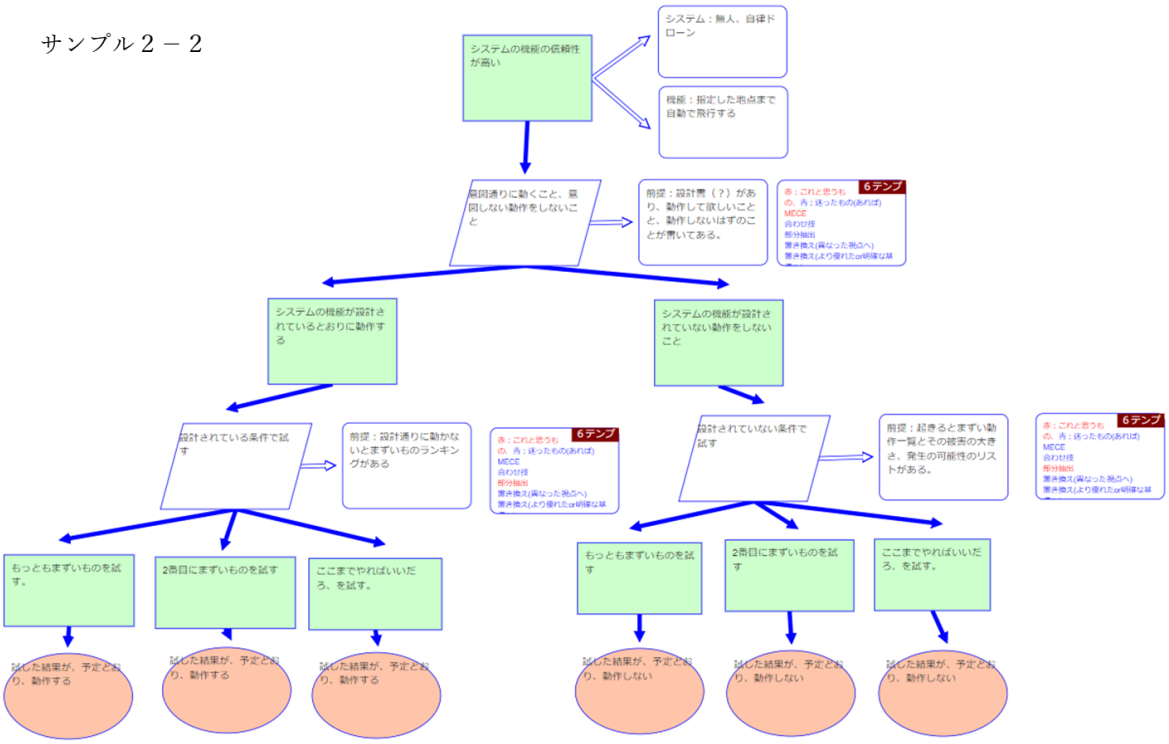


図 37 作成されたＧＳＮサンプル（サンプル２－２）

サンプル２－３

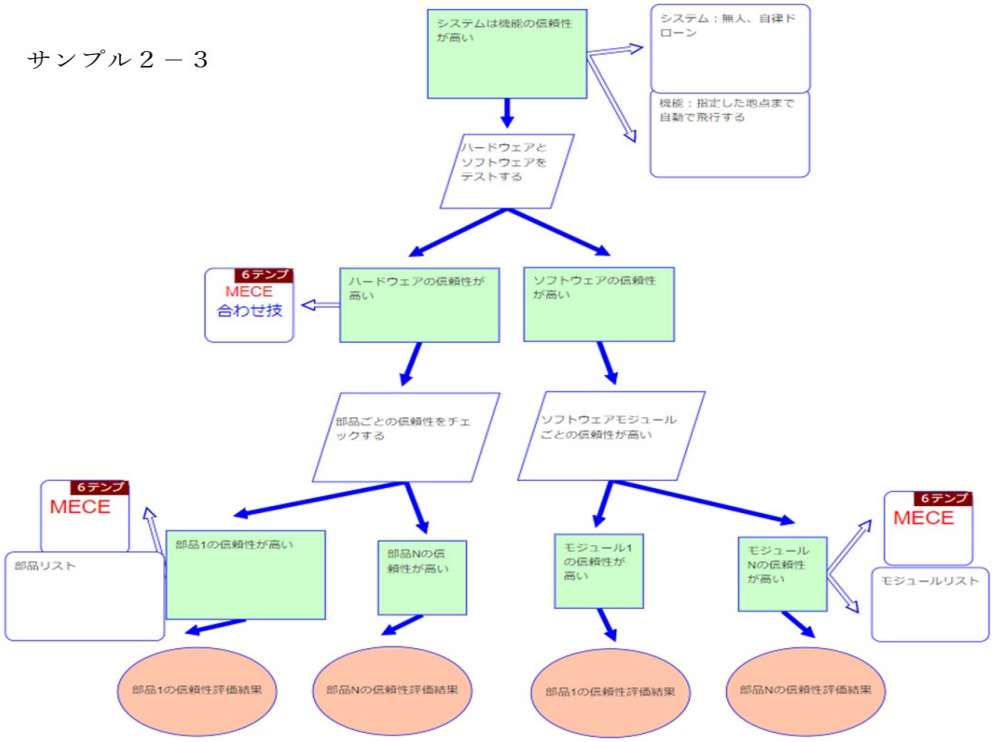


図 38 作成された GSN（サンプル２－３）

サンプル２－４

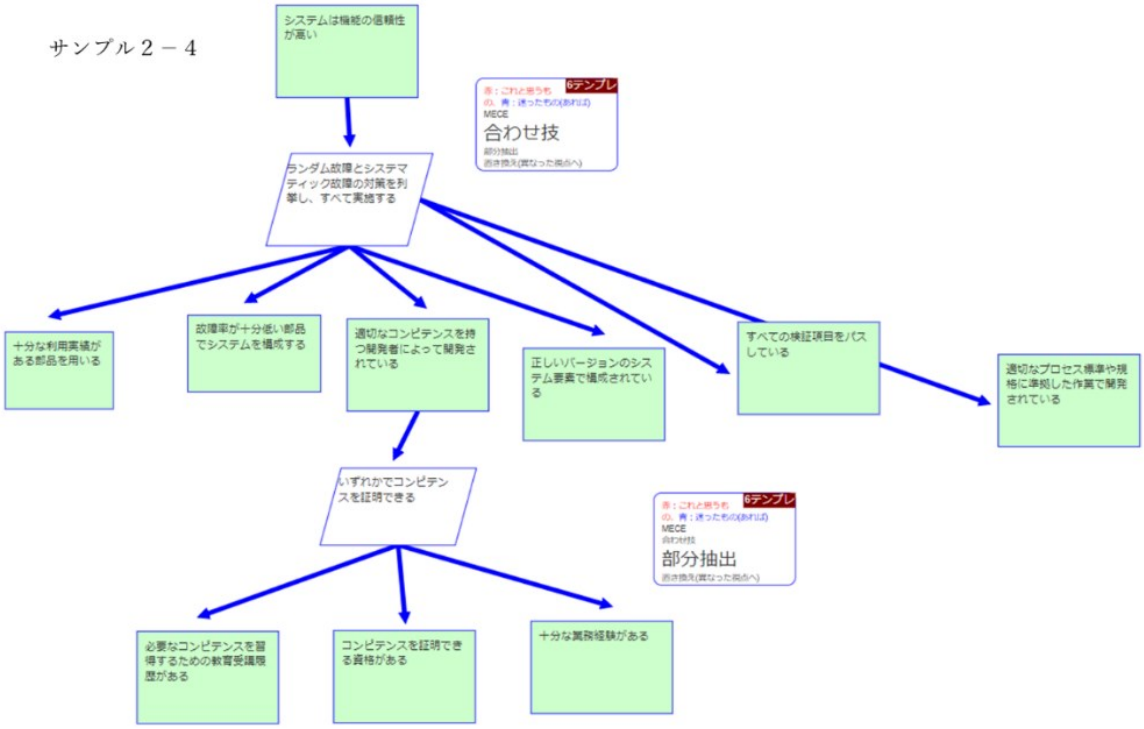


図 39 作成された GSN（サンプル２－４）

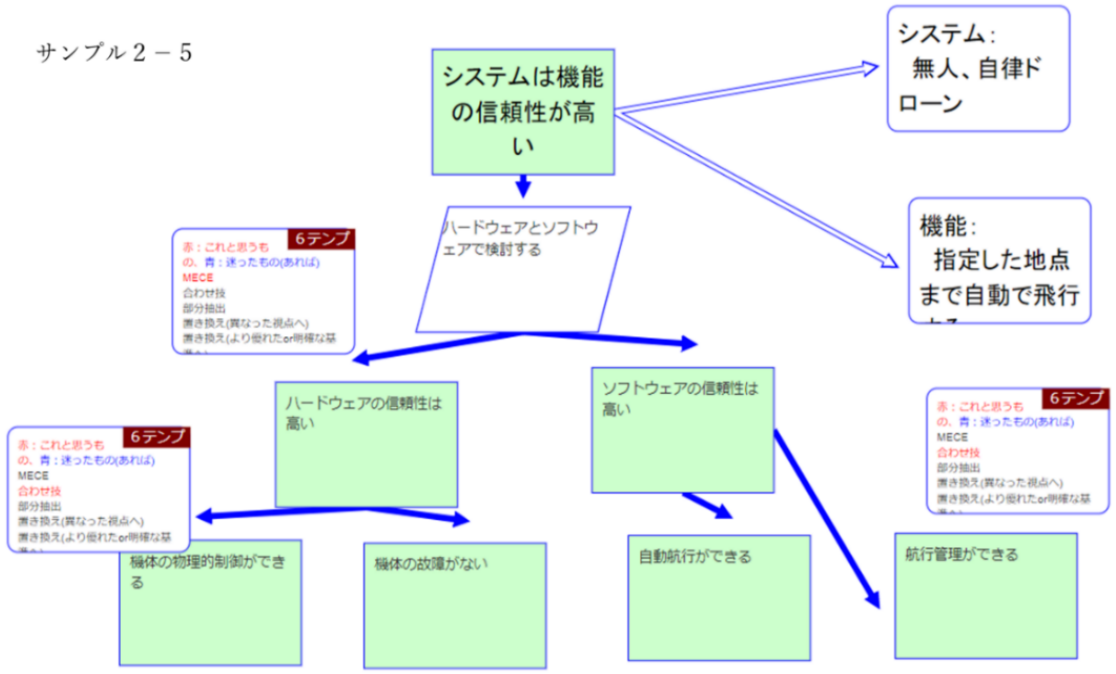


図 40 作成された GSN（サンプル２－５）

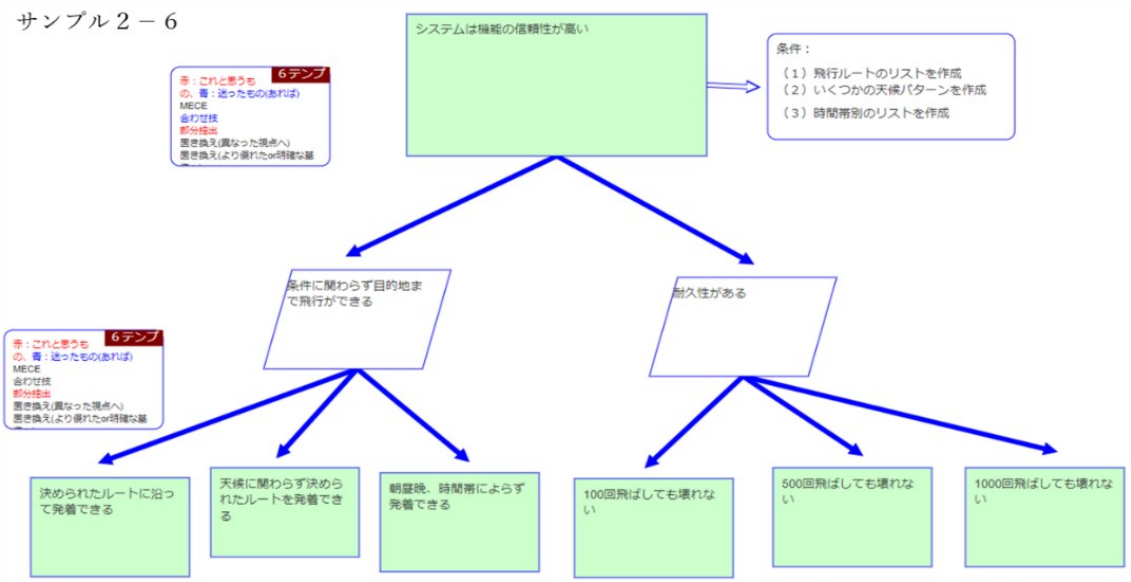


図 41 作成された GSN（サンプル２－６）

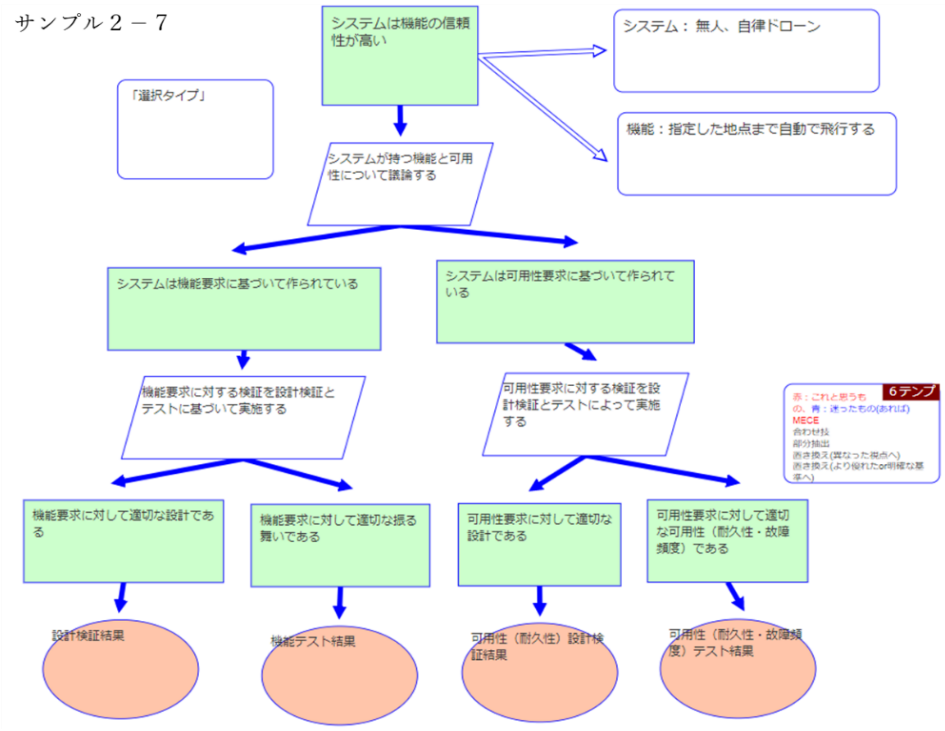


図 42 作成された GSN（サンプル２－７）

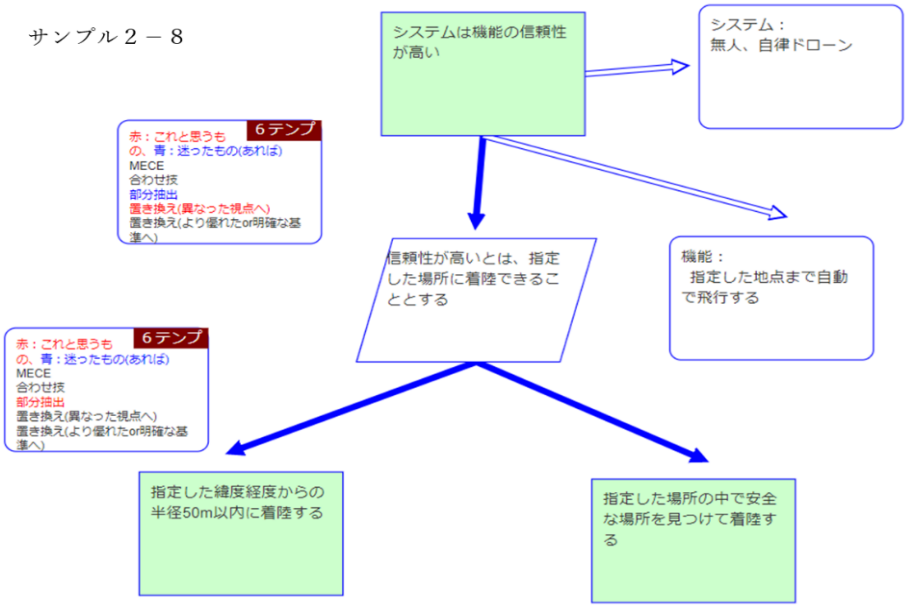


図 43 作成された GSN（サンプル２－８）

● **演習で作成されたパターン**

各ワークショック実施回での、参加者が作成した GSN に登場してきたパターンについてそれぞれ、表 9、表 8 のようになった。

表 8 作成された各パターンの数（ワークショップ#１）

WS#1 サンプル		1-1	1-2	1-3	1-4	1- 5	計
(a)	部分選択	1	1	1	0	1	4
(b)	二重否定	0	1	0	0	0	1
(c)	基準化	0	1	0	0	0	1
(d)	視点変換	1	1	0	0	3	5
(e)	合わせ技	1	0	1	2	0	4
(f)	MECE	2	2	1	1	1	7

表 9 作成された各パターンの数（ワークショップ#２）

WS#2 サンプルNo.		2-1	2-2	2-3	2-4	2-5	2-6	2-7	2-8	計
(a)	部分選択	0	0	0	1	0	2	1	1	5
(b)	二重否定	0	0	0	0	0	0	0	0	0
(c)	基準化	3	0	0	0	0	0	0	0	3
(d)	視点変換	0	0	0	0	0	0	0	1	1
(e)	合わせ技	0	0	0	1	2	0	0	0	3
(f)	MECE	0	1	3	0	1	0	2	0	7

5.5. アンケート結果

各ワークショップ実施後にアンケートを行っている。以下、それぞれのアンケートの設問と得られた回答を示す。(SCDL 編の演習の内容については、7 章で説明を行う。)

● **ワークショップ＃１アンケート結果**

参加者 11 人中 11 人より回答を得た。
以下質問事項とし、アンケートの作成、及び改修は、Google Forms を用いて行った。

設問：

GSN 編

①GSN 編について伺います [説明は分かりやすかったですか？]
②GSN 編について伺います [演習の難易度はいかがでしたか？]
③GSN 編について伺います [説明の時間はいかがでしたか？]
④GSN 編について伺います [演習の時間はいかがでしたか？]
⑤GSN 編について、説明又は演習について分かり易かった（又はわかりづらかった）点を具体的に教えてください。
⑤GSN 編について、説明又は演習について分かり易かった（又はわかりづらかった）点を具体的に教えてください。
⑥特徴は理解できましたか？
⑦パターンとして適切だと思いますか？
⑧役に立つと思いますか？（他人の GSN を読むとき）
⑨役に立つと思いますか？（自分で GSN を書くとき）
※⑥から⑨の設問において、回答フォーム上にパターン(c)箇所の回答欄が設けられていなかったため回答を回収できていない。

SCDL 編

①SCDL の説明について伺います。[説明は分かり易かったですか？]
②SCDL 編について伺います [演習の難易度はいかがでしたか？]
③SCDL 編について伺います [説明の時間はいかがでしたか？]
④SCDL 編について伺います [演習の時間はいかがでしたか？]
⑤説明又は演習について具体的に分かり易かった（又はわかりづらかった）点を具体的に教えてください。
⑥GSN と SCDL の組み合わせについて伺います。[組み合わせの事例は応用できそうでしょうか？]
⑦GSN と SCDL の組み合わせについて伺います。[組み合わせの事例は応用できそうでしょうか？]
⑧（GSN と SCDL 編を通して）説明又は演習について具体的に分かり易かった（又はわかりづらかった）点を具体的に教えてください。

①GSN編について伺います［説明は分かりやすかったですか？］

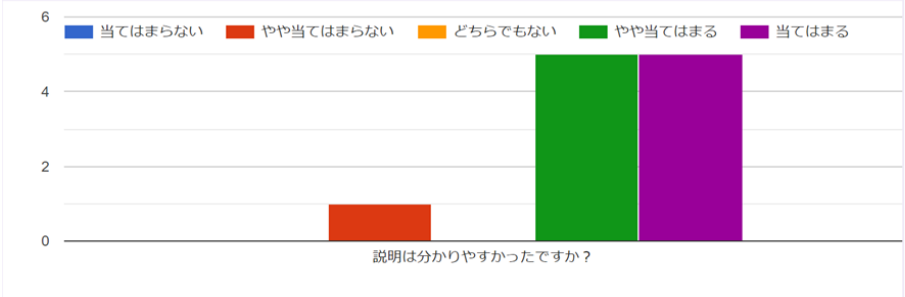


図 44 アンケート回答（ワークショップ＃1 GSN 編 ①）

②GSN編について伺います［演習の難易度はいかがでしたか？］

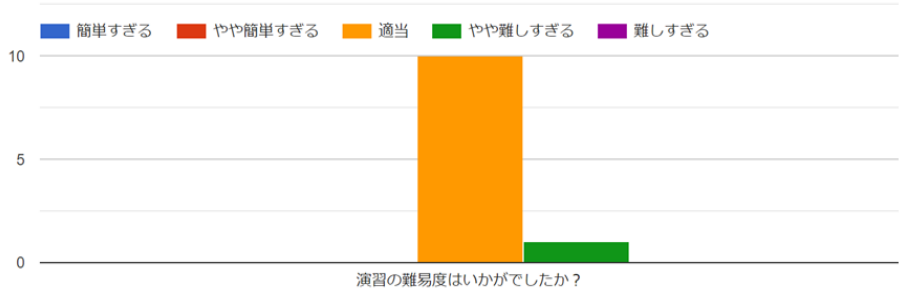


図 45 アンケート回答（ワークショップ＃1 GSN 編 ②）

③GSN編について伺います［説明の時間はいかがでしたか？］

④GSN編について伺います［演習の時間はいかがでしたか？］

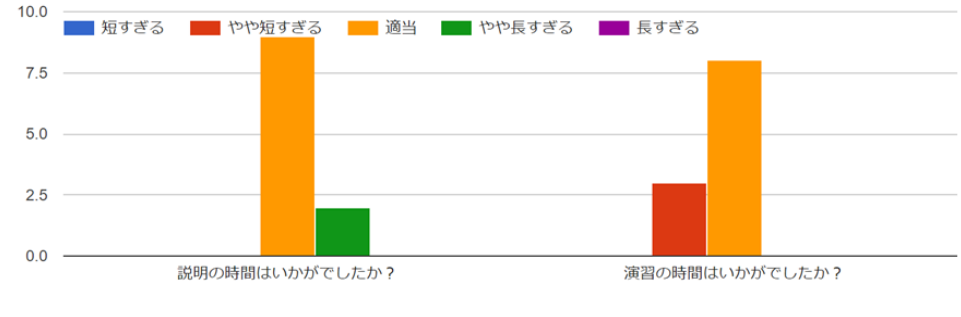


図 46 アンケート回答（ワークショップ＃1 GSN 編 ③④）

⑤説明又は演習について分かり易かった（又はわかりづらかった）点を具体的に教えてください。

具体的な例と、パターンわけがあって、わかりやすかった

質問も含めて、パターン分類の解釈の疑問点がだいぶ解消できました。

タイプの分類が曖昧で、あまり理解できませんでした。

私が聞き逃してしまったのかもしれませんが、説明の後に「ご提案です」と説明された事に戸惑ってしまいました。
説明前にGSNの普遍的な仕様や書き方なのか、それとも提案なのかを強調して頂けると嬉しいです。"

"事例に基づいてパターンを説明して頂いたので、わかりやすかったです。
今までは、自分でGSNを書こうと思ってもどう書いていいかイメージがわかないことが多かったですが、このパターンで書いてみようというように書き方の指針にもなるなと思いました。"

説明はわかりやすかったですが、ちょっと長かったです。受講者に定期的に質問をすると長さを感じないかもしれません。

6つのパターンタイプで分類しながら読み解いていく観点がとても勉強になりました。今後ありがたく使わせて頂きます。Goal、Strategy、Solution、Contextは実例が豊富だったのでどのような時に使うか分かった反面、JustificationとAssumption、及びUndevelopedなGoalはまだ今一つ使い方が分かってないので今後軽くでもいいので説明頂けるようなセミナーに発展されるとうれしいです。

GSNの6パターンを理解できてよかった。演習は、ヒントがあったので、自分で考えられてよかった。

6タイプ間の違いがどこにあり、どの程度まで曖昧かなどの感覚がわかりやすかった。

図 47 アンケート回答（ワークショップ＃1 GSN 編 ⑤）

⑥特徴は理解できましたか？

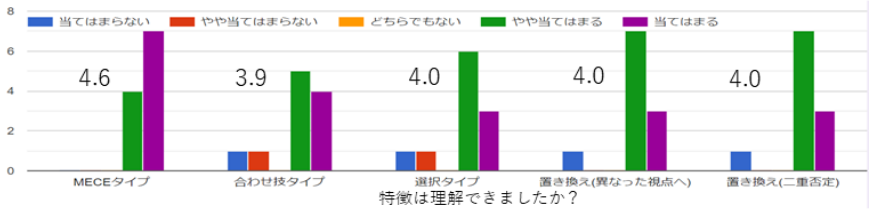


図 48 アンケート回答（ワークショップ＃1 GSN 編 ⑥）

⑦パターンとして適切だと思いますか？

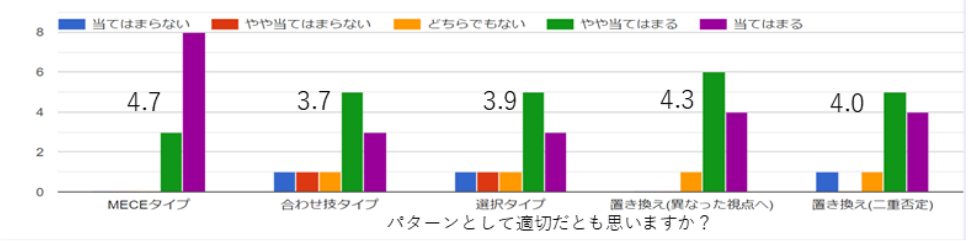


図 49 アンケート回答（ワークショップ＃1 GSN 編 ⑦）

⑧役に立つと思いますか？（他人のGSNを読むとき）

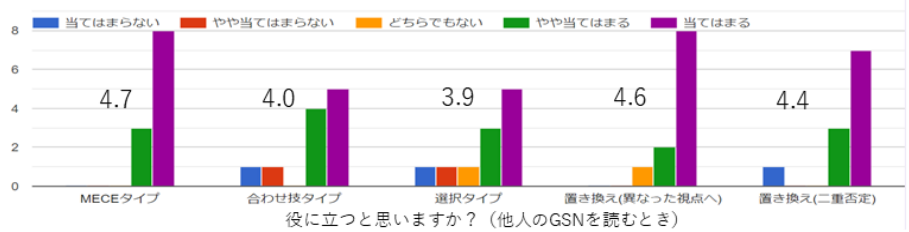


図 50 アンケート回答（ワークショップ＃1 GSN 編 ⑧）

⑨役に立つと思いますか？（自分でGSNを書くとき）

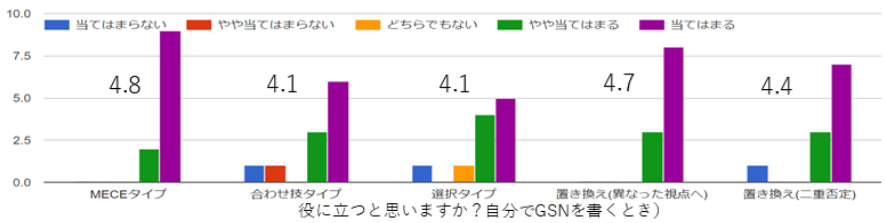


図 51 アンケート回答（ワークショップ＃1 GSN 編 ⑨）

SCDL 編

①SCDLの説明について伺います。［説明は分かり易かったですか？］

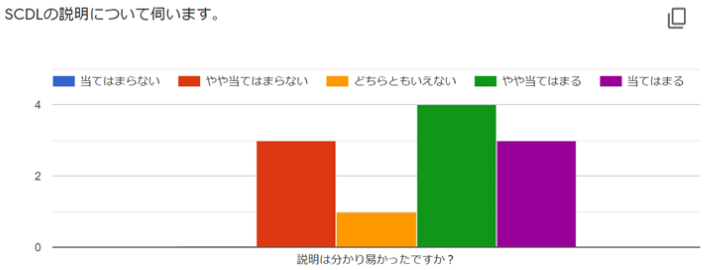


図 52 アンケート回答（ワークショップ＃1 SCDL 編①）

②SCDL編について伺います［演習の難易度はいかがでしたか？］

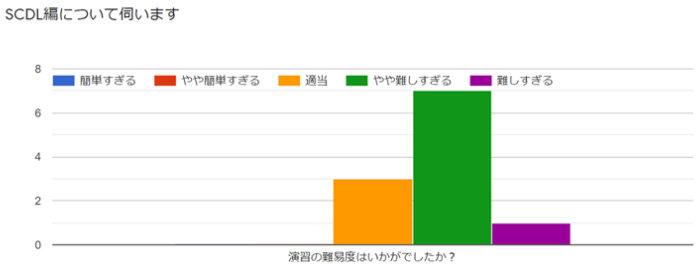


図 53 アンケート回答（ワークショップ＃1 SCDL 編②）

③SCDL編について伺います［説明の時間はいかがでしたか？］

④SCDL編について伺います［演習の時間はいかがでしたか？］

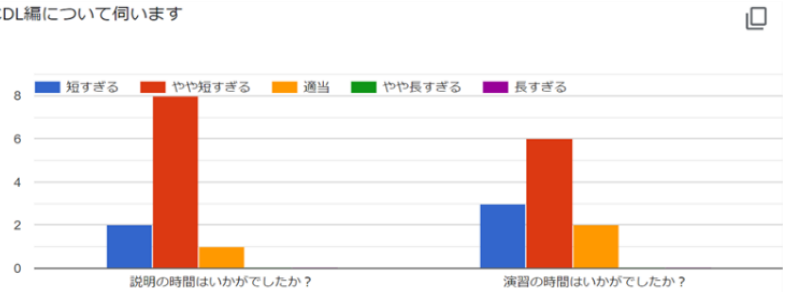


図 54 アンケート回答（ワークショップ＃1 SCDL 編③④）

SCDL編

⑤説明又は演習について具体的に分かり易かった（又はわかりづらかった）点を具体的に教えてください。

具体的な例でわかりやすかったです。問題としてはちょっとあれもこれもで欲張りだったかと思います。やってもらうことを絞るといいと思います。

SCDLで表現される機能要求間の関連が、GSNとどう関連していくのが良いのかが分かりづらかった
SCDLは自分で書くとなかなか思うように描けないのですが、徐々に冗長化が進む過程を見れて参考になりました。

説明はわかりやすく、どういうふうに書いていくのかがなんとなくわかったが、演習が難しかったので、途端にハードルがあがってしまったように感じました。もう少し細かく(機能ごとに分割するなど)区切って演習を進めるとわかりやすいのではないかと思いました。

時間が押していて短かったため、GSNに比べあっさりした説明に感じました。

今回、SCDL編は時間が押していたこともあって説明や演習時間が短かったのは仕方ないと思います。要求やエレメントの目的・使用方法についてはよく分かりました。
グループペアリングについてまだ理解していない気がしますが、グループ１＝機能要件（主機能）、グループ２＝非機能要件（冗長構成やチェック機能）で分けるという理解で合っていますでしょうか？

SCDLの使い方の例を知ることができてよかった。もう少し詳しい説明や例、簡単な演習があるとよかったと思う。

SCDLは未経験だったので、そもそも何であるかを飲み込むのに戸惑った。
冗長性についても、どの程度まで考えればいいか基準がわからず、演習に着手できなかった。

図 55 アンケート回答（ワークショップ＃1 SCDL 編⑤）

⑥GSNとSCDLの組み合わせについて伺います。［組み合わせの事例は応用できそうでしょうか？］

⑦GSNとSCDLの組み合わせについて伺います。［組み合わせの事例は応用できそうでしょうか？］

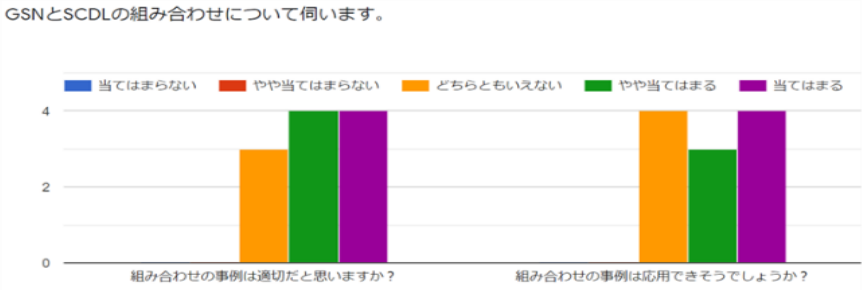


図 56 アンケート回答（ワークショップ＃1 SCDL 編⑥⑦）

GSN編とSCDL編を通して
⑧説明又は演習について具体的に分かり易かった（又はわかりづらかった）点を具体的に教えてください。

全体的に丁寧でわかいやすかったです。ありがとうございました。

できればもっと具体的な連携機能の強化を行って行きたいところですが、Astah System Safetyで言うと、ハイパーリンク機能による緩い設計要素との関連付けも思っていたより有効そうだと感じることができて良かったです。

主観になりますが、GSNよりもSCDLの方が直感的に理解が難しかったため、SCDLの時間を長めにして頂けると嬉しいです。

"GSNの方はパターン化するという切り口がわかりやすかったですが、SCDLの方が演習が難しく一気にハードルが上がってしまった気がしました。受講する人のスキルが一定ではないので、誰に合わせるかは難しいなと思いますが、どれくらいのレベル感の方を対象にしているのかなどを明確にしてもよさそうに思いました。初級、中級、上級のようにレベル分けするとかもいいかもしれないと思いました。
今回受講させて頂いて、特にGSNは自分で書く時に指針にできそうなことがいっぱいありました。ありがとうございました。"

GSNとSCDLの違いや関係性について知ることができて良かったです。

配布頂いた今日の教材を熟読したいと思います。まさかGSNとSCDLをリンクさせることができるとは思わなかったのでとても勉強になりました。

GSNとSCDLの説明を聞いてから、GSNとSCDLの組み合わせを聞いたので分かりやすかった。

GSNとSCDLの要素に対応付けができ、互いに参照づけて説明できることはわかった。

図 57 アンケート回答（ワークショップ＃1 SCDL 編⑧）

- **ワークショップ＃2 アンケート結果**

以下質問事項とし、アンケートの作成、及び改修は、Google Forms を用いて行った。参加者 11 人中 7 人より回答を得た。

設問：

質問 1 業種は？

質問 2 職種は？

質問 3 説明はわかりやすかったか？

質問 4 説明について分かり易かった(又は分かりづらかった)点を具体的に

質問 5 演習の難易度は？

質問 6 演習の量は？

質問 7 時間配分について

質問 8 演習について分かり易かった(又は分かりづらかった)点は？

質問 9 それぞれのパターンは理解できたか？

質問 10 パターンとして適切だと思うか？

質問 11 役に立つと思うか？(他人の GSN を読むとき)

質問 12 役に立つと思うか？(自分で GSN を書くとき)

質問 13 全体を通じてご意見ご感想がありましたらお願いします。

設問1）

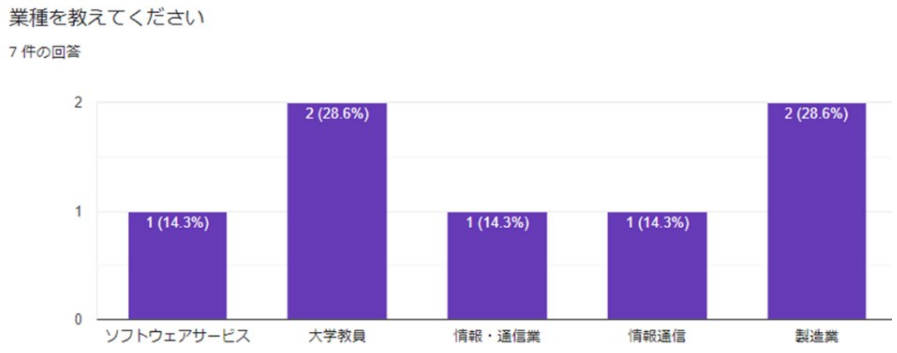


図 58 アンケート回答（ワークショップ＃2 設問 1）

設問2）

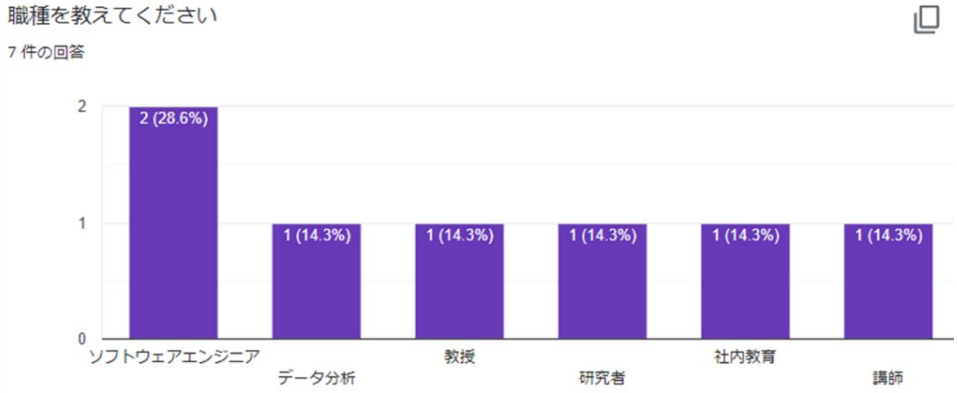


図 59 アンケート回答（ワークショップ＃2 設問 2）

設問3）

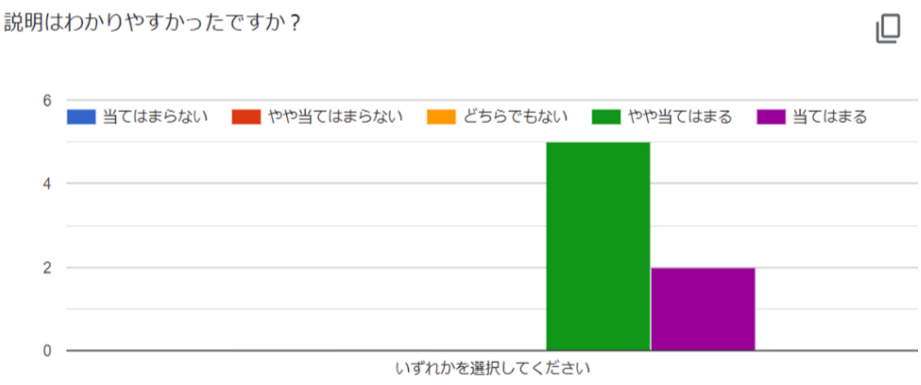


図 60 アンケート回答（ワークショップ＃2 設問 3）

設問4）

説明について分かり易かった（又は分かりづらかった）点を具体的に教えてください。

3 件の回答

PPTは最初にいただけると有難いです

最初は漠然としていましたが、実際に全体演習、その後個別演習になったことで、具体的なイメージがつきやすくなりました。

最初、パターンを理解するのに時間がかかった

図 61 アンケート回答（ワークショップ＃2 設問 4）

設問5）

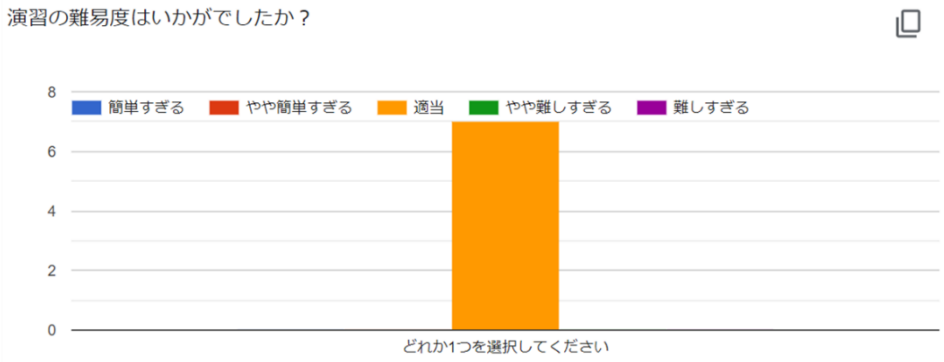


図 62 アンケート回答（ワークショップ＃2 設問 5）

設問6）

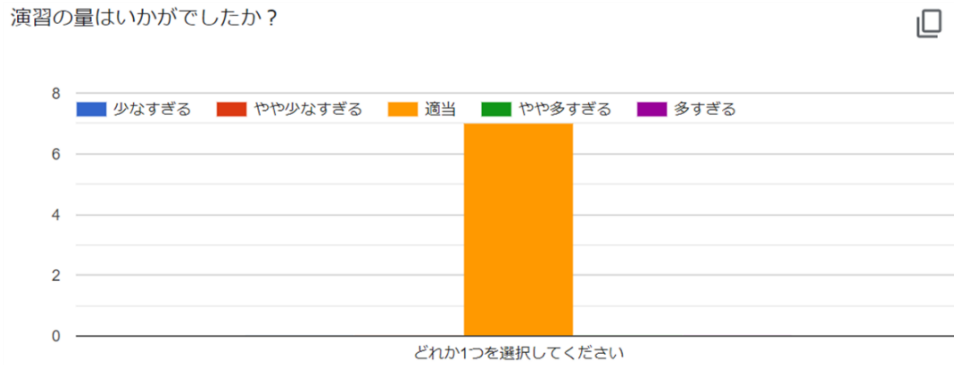


図 63 アンケート回答（ワークショップ＃2 設問 6）

設問7）

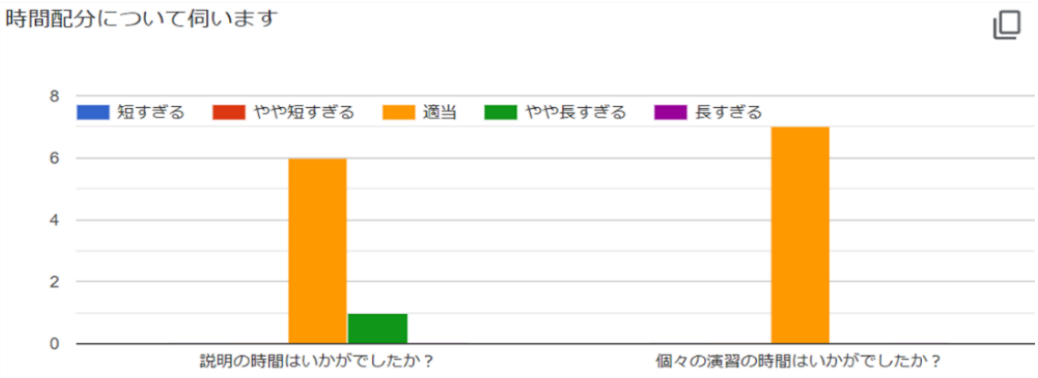


図 64 アンケート回答（ワークショップ＃2 設問 7）

設問8）

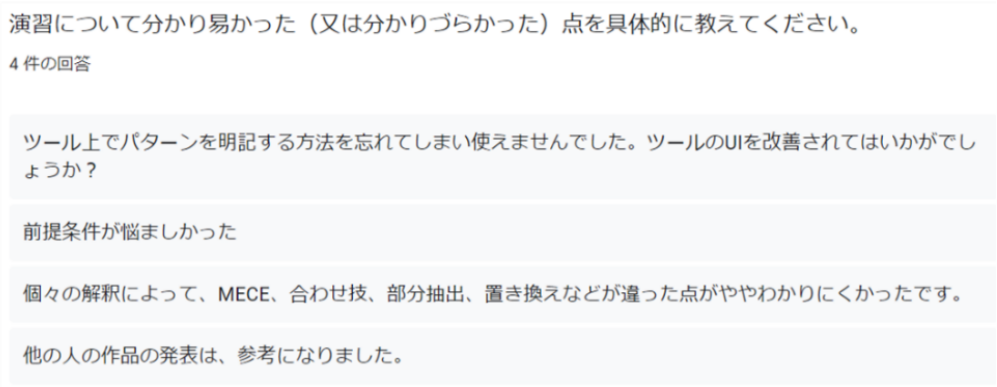


図 65 アンケート回答（ワークショップ＃2 設問 8）

以降の設問においてパターン名称はそれぞれ以下のように対応される。

- 置き換え（異なった視点へ）⇒ 視点変換
- 置き換え（より優れた or 明確な基準へ）⇒ 基準化

設問9）

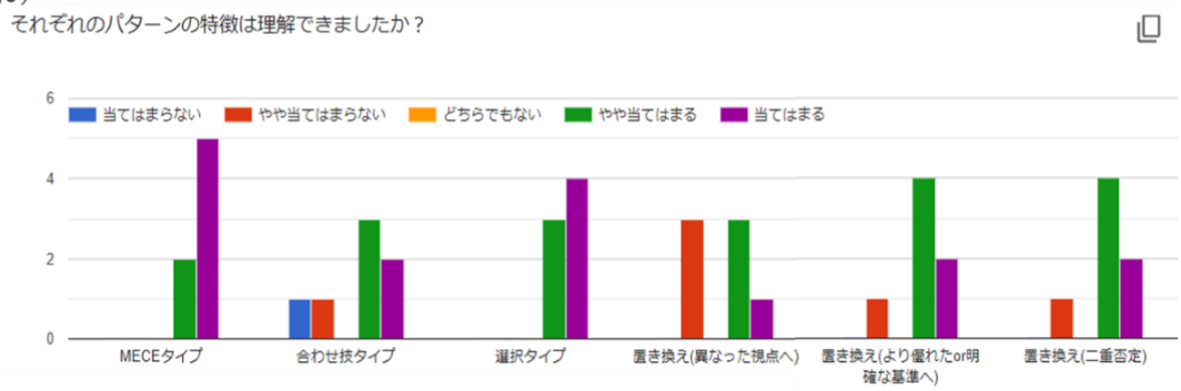


図 66 アンケート回答（ワークショップ＃2 設問 9）

設問10）

パターンとして適切だと思いますか？

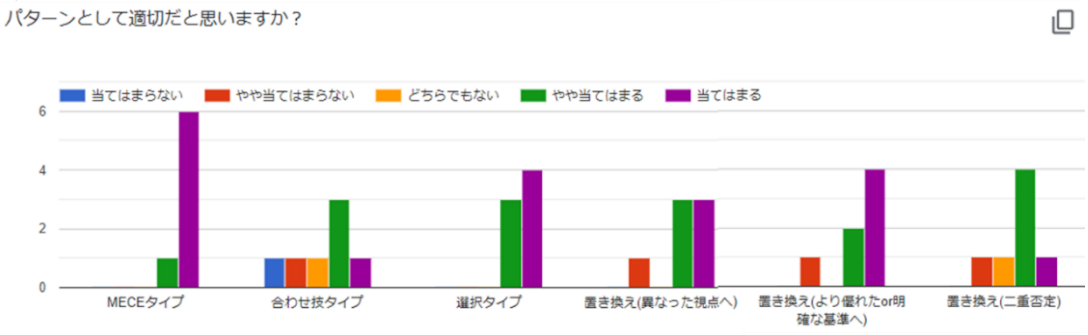


図 67 アンケート回答（ワークショップ＃2 設問 10）

設問11）

役に立つと思いますか？（他人のGSNを読むとき）

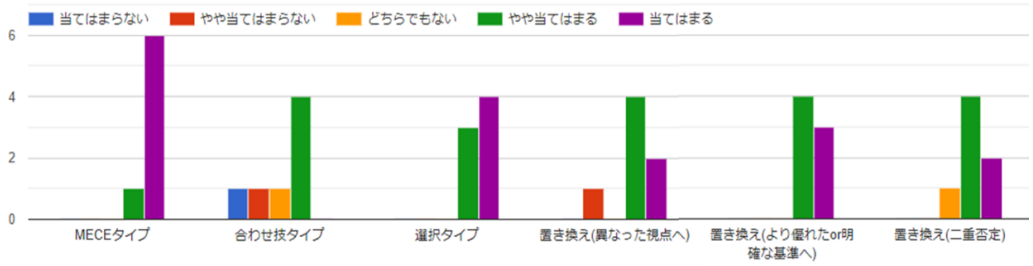


図 68 アンケート回答（ワークショップ＃2 設問 11）

設問12）

役に立つと思いますか？（自分でGSNを書くとき）

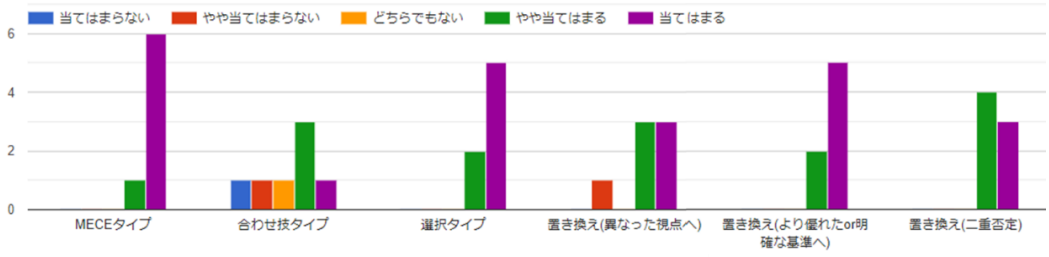


図 69 アンケート回答（ワークショップ＃2 設問 12）

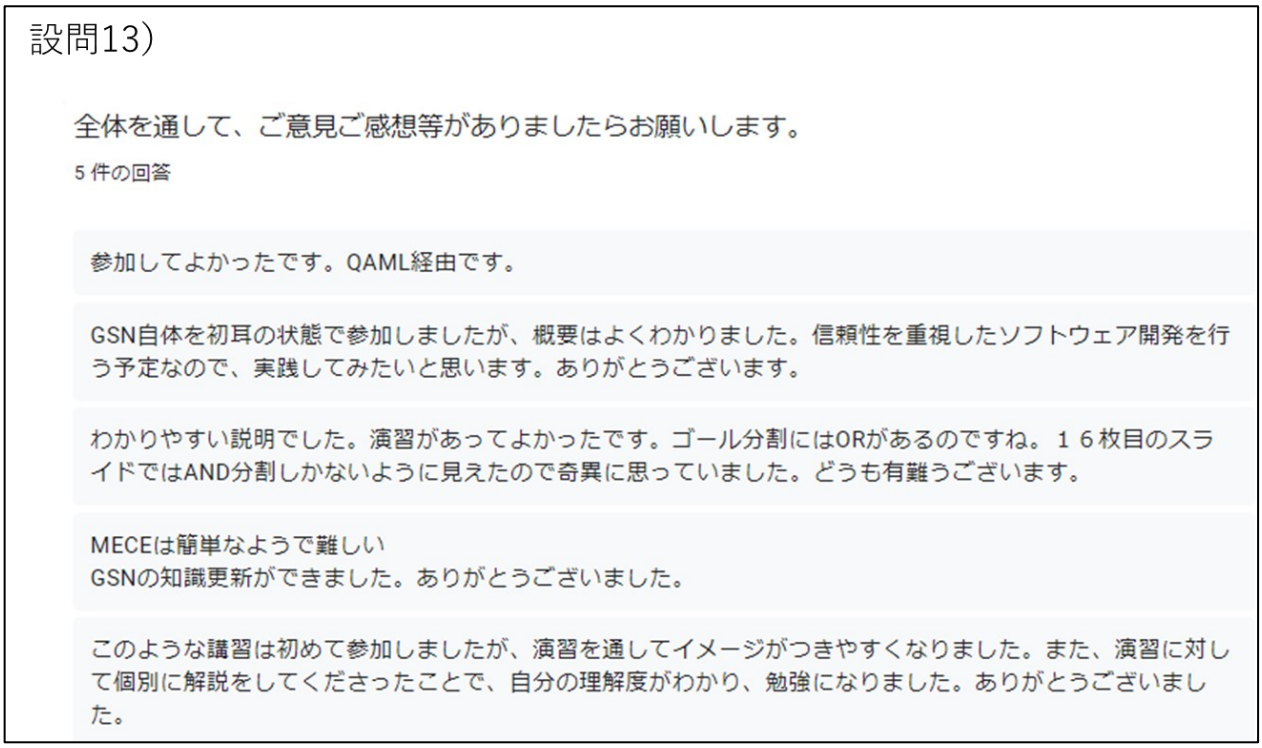


図 70 アンケート回答（ワークショップ＃2 設問 13）

5.6. ワークショップついての考察

ワークショップにおける演習及びアンケートの結果より以下のことが得られた。

- **分割パターンの理解度**

  演習で作成された GSN 成果物には、パターン(a)(e)(f)のいずれかとしてあてはめられたものが成果物に存在していることから、それぞれの可用性が示されていると考える。なお、パターン(f)以外にも、パターン(a)及び(e)が作成されたことは、分割された主張どうしの関係性において分解であるものと分解でないものとの違いがあることについて理解を得られたと考える。同時にパターン(a)(e)(f)のそれぞれの違いと特徴について理解が得られたものと考える。

- **変換パターン理解度**

  パターン(b)(c)(d)のそれぞれが演習で作成された GSN 成果物に登場してきていることから、これらの有効性を確認することができたと考える。一方でパターン(b)についてはワークショップ#2 における成果物には、登場してこなかったが、アンケートにおいて、GSN を読むとき、又は書くときに役立つか、の設問では、高い評価が得られていることから、パターンの特徴としては、一定の理解を得られたと考える。

- **変換パターンの必要性**

  主張について、説明しやすい視点の置き換えを行っていることが意識されたと同時に、意図的に用いられることが行われていることが、演習で作成された GSN 成果物より示された。

- **パターンのバリエーション**

  同じ親ゴールの主張についてであっても、子ゴールの主張への展開方法は一通りにならない。今回、演習で作成された GSN 成果物においても子ゴールへの展開は、各参加者において同じにはならず、それぞれのパターンとしての構成のものが作成された。そのことは、記述者の視点によってその違いを使いわけることができることが確認されたものと考える。GSN 上の構造上での変換、及び分割の関係性を構造的解釈として使い分ける場合において、本パターンの有用性が確認されたと考える。

5.7. まとめ

6パターンの有用性を検証する目的で、ワークショップを行った。実施は、2回行い、1回目は、企業向けに実施、11名のSEの参加者に参加に対して、2回目は、一般公募による参加者に対して実施し11名の不特定の業種の参加者に対して実施した。両実施を通じて、共に、6パターンの特徴について理解がなされたことが、アンケート結果より測定できた。また、演習による参加者が作成したGSNに、6パターンのいずれかが適用され、さらに、6つのパターンのそれぞれが登場してきたことより、各パターンのそれぞれの有用性が確認された。

第 6 章　既存研究における分類と考察

6.1. 産業界における GSN 使用事例

以下、産業界で、GSN モデルが使われている事例と共に 6 パターンとの比較を行った。

● DEOS（Dependability Engineering for Open Systems）

産業界の 1 つ目の事例として DEOS について取り上げる。
DEOS においては、様々な変化に対応するシステムとして、合意形成と説明責任を全うするプロセスを提案している [8]。そのプロセスは大きくは、以下 3 つのサイクルの組み合わせで構成され、それぞれを子の主張として、D-Case を用いて定義されることが推奨されている。

・通常運用サイクル

・変化対応サイクル

・障害対応サイクル

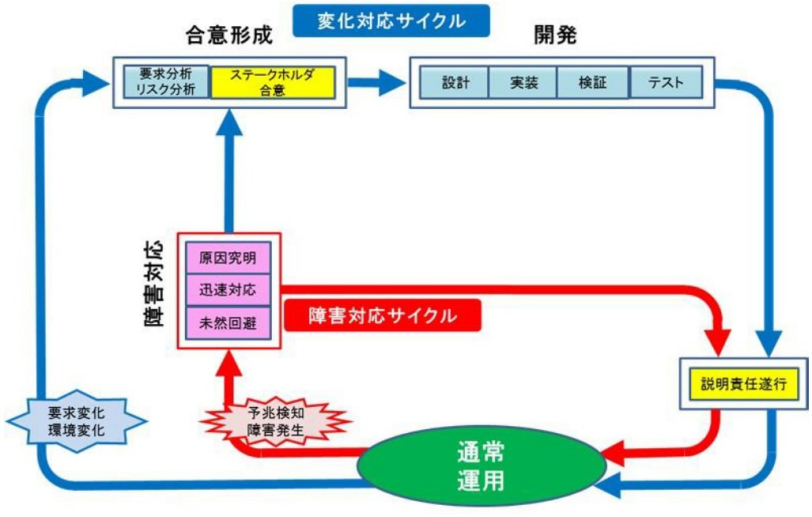


図 71 DEOS ライフサイクルモデル （[8] 図 2.8 より）

なお、D-Case 構文 [9]としては、変化に対応すべくモニタ及びアクションを定義するためのノードが、GSN 構文に対しての拡張として用意されている。

そこで、上記の 3 つのサイクルが全てとして考えられ、これらサイクルを各子とする GSN を作成した場合、パターン“(f)MECE”とみなすことができると考える。

● Guidelines for Automotive Safety Arguments

産業界の事例の 2 つ目の事例として、以下ガイドラインについて取り上げる。
自動車開発における機能安全 ISO26262 の論証アプローチとしての検討 [10]に続き、MISRA（自動車メーカ、部品メーカ、エンジニアリング・コンサルタントで活動を行っている組織団体）により、本ガイドラインとして発行された [11]。本ガイドラインにおいては、GSN を用いた、ISO26262 における安全論証の表現が行われている。さらにそれらは、GSN の子の主張に以下の 4 つで構成することを推奨している。

・Rationale（論理的根拠）

・Satisfaction（満足）

・Means（手段）

・Organisational Environment （組織、環境）

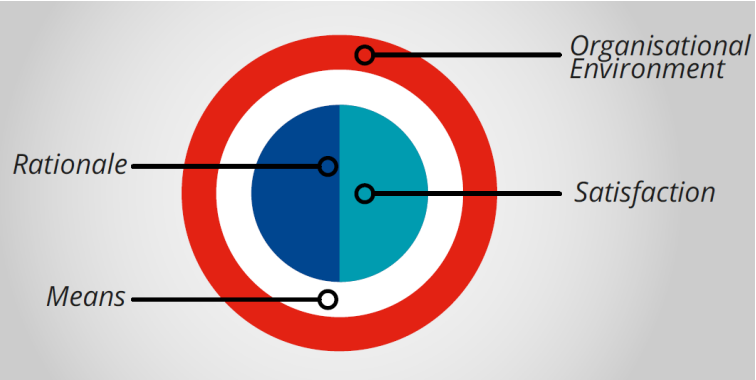


図 72 Layered Argument Model（ [11] Figure.1 より）

これらの組み合わせは、以下のように、2 組の組み合わせとして考えることもできる。この場合、前者の 2 つは、説得性や充足さを求めるものであり、一方で後者の 2 つは手法、及び、それらを行う組織についての確認がなされることになる。

- “Rationale”と Satisfaction”
- “Means”と“Organisational Environment”

この 2 組は異なる視点のものの組み合わせとして“人が判断する妥当性や充足”と“実際の物や手法や組織”といったものどうしの組み合わせである。この組み合わせは、言い換えれば“非物質的な論拠”と“物質が基本となるものとしての根拠”としての特徴の組み合わせであるとみなすことができ、その場合この 2 組の組み合わせはパターン“(e)合わせ技”とみなすこともできる。しかし、一方で、これら 4 つの構成が定型化された組み合わせとして提案がなされていると見なした場合、パターン“(f)MECE”に該当すると考える。

6.2. 既存パターン分類に対する考察

GSN のパターンと同様に木構造を持つ以下関連研究のそれぞれについて考察を行う。

(1) 分解型の分類

(2) 多足議論（Multi-legged arguments）

(3) CAE を用いた主張同士の関係性のパターン

(4) セーフティケースパターンカタログ

(1) 分解型の分類

GSN の子ゴールの構成は、記述者の視点に従って、子ゴールに分解することが可能である。それらゴール同士の分類を行った研究として“保証ケース議論分解パターン” [12]がある。[12]においては、以下の種類の視点による分解パターンが定義されている。

1　アーキテクチャ分解

2　機能分解

3　属性分解

4　帰納分解

5　完全分解

6　単調分解

7　修正分解

これらは、本研究におけるパターン(f)に相当するものと考える。また、上記 1～7 の一連の分類は、パターン(f)のサブ分類に相当すると考える。

(2) 多足議論（Multi-legged arguments）

木構造におけるゴール思考の研究のうち、複数の足（子ゴール）における多重議論の従来研究として Multi-legged arguments [13] [14]がある。Multi-legged arguments においては、2 足の議論構成により、2 足の上位の主張を達成させるものであり、以下 1～4 の 2 足構成が存在する。これらにおいて共通する特徴として、親と子の関係は、子の階層の主張の達成が親のそれを支持する場合、子における主張同士が、相乗的に、又は補足的に支持することができるといった特徴がある。

1. 論理的と統計的な主張

2. 間接的と直接的な証拠や主張

3. 主となるものと弱点を補う主張

4. 複数チームによる主張

上記の 1〜4 についての特徴については [13]において、それぞれ以下のような特徴を持つものとされている。

1. 論理的と統計的な主張

論理的証拠に基づく足（子）と運用テストからの統計的証拠に基づく足（子）である関係。例： ソフトウェアの信頼性についての議論の場合、1 番目は障害（のクラス）からの完全な脱却の主張、2 番目は要求に応じた特定の失敗確率の主張を含む。

2. 間接的と直接的な証拠や主張

設計プロセスの品質などの間接的な証拠に基づく足と、構築されたシステムの直接評価に基づく足。各足は専門家の判断による評価を含む。例：ソフトウェアの場合、1 番目の足（子）は CMM（Capability Maturity Model）レベルや使用する手順の種類などの証拠を含み、2 番目の足（子）は静的分析と運用テストの証拠を含む。

3. 主となるものと弱点を補う主張

広範囲な証拠を含む主要な議論の足（子)、およびその目的が主要の議論の足の潜在的に深刻な弱点を補うための 2 番目の足（子)。

4. 複数チームによる主張

まったく同じ証拠に基づいているが、専門家アナリストのコミュニケーションの取れていない異なるチームに基づく足。

多足議論（Multi-legged arguments）において、相互の足の主張が、それらが単体で、示されるより、複数で示されることによって相乗的な効果がある特徴があることについては、本研究におけるパターン(e)と共通している。そこで、上記の 1 から 4 のそれぞれの特徴に対して、どのように一致しているかの確認を調査した GSN サンプルに対して確認を行った。

- **1 との一致**

調査したサンプルにおいてこの特徴に合致するものがあり、その GSN を図 73 に示す。

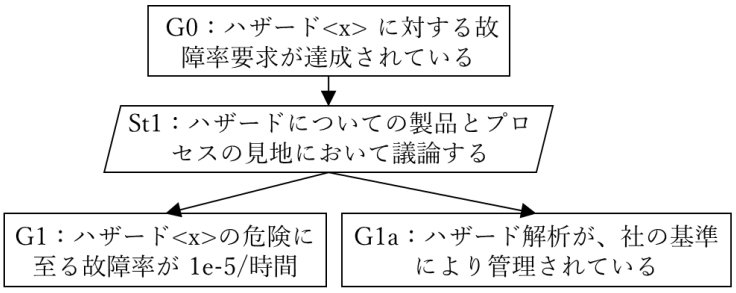


図 73 論理的と統計的な主張 （ [6] Fugure50）

● **2 との一致**

調査したサンプルにおいてこの特徴に合致するものがあり、その GSN を図 74 に示す。なお、S1、S2 はゴールと同様に主張を持つ子（足）としてのストラテジと見なしている。

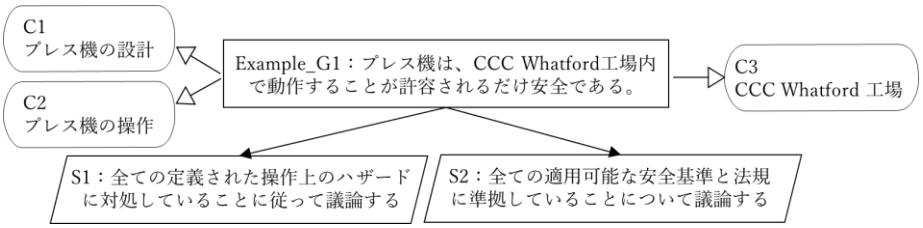


図 74 間接的と直接的な証拠や主張（ [6] Figure41）

● **3 との一致**

今回調査した GSN サンプルの中に、この特徴を持つ GSN は見つからなかった。一方で、この特徴は、1-out-of-2 の考え方に類似している。そして調査した GSN サンプルには同類の見つかっていないものの、この特徴を持つ GSN を作成することは可能であると考える。

なお、1-out-of-2 は機能安全の分野において取り入れられている考え方であり、例として安全機構を持つシステムの機能設計構造において、この構造的な関係性が見られる。それは、機能安全の安全機構の設計において意図する機能が不全に至った場合、それを検知し、安全機能が働く機構の関係に類似する。これらについての検証の詳細については、7 章にて示す。

● **4 との一致**

この特徴に該当する GSN はサンプル調査において見つけることはできなかった。しかし、この 4 における想定において“アナリストによる解析”を“同じ開発品について、複数のチームが開発”といった具合に置き換えて考えることもできる。また“複数のチームが開発する行為”については、“複数のチームによって開発されたシステムが振る舞う動作”といった表現に置き換えて考えることも可能である。

つまり、何かしらのシステム上の機能について、“同一の機能を実現する独立かつ並列した機能が、冗長的に達成しようとする”又は、“複数同一処理が、多数決論に基づいた出力を決定する”といったフォールトトレランスとしてのアプローチに当てはめて考えることができる。

前者の例は、航空機の複数のエンジンのうち 1 つが故障した場合でも、残りのエンジンで飛行を継続できるようにする、といった場合が該当する。

後者の例は、例えば、演算や判断を司る機構において、マイコン等が暴走し、誤った演算結果を出力した場合に、並列される機構において正しい結果に補正が可能なものが該当する。(ただし一般的には、間違った出力であることを互いに判断できないために、3 個以上の冗長系システムを保有する場合が多い。)

故障には、ランダムハードウェア故障とシステマティックフォールトがある。寿命や耐久性に依存し、電気部品の確率論的に発生するものはランダムハードウェア故障とされ、一方で、設計、実装、製造上におけるミス、ヒューマンエラーによって作り込まれた要因が故障に至らしめるものは、システマティックフォールトとして分類される。

これらフォールトトレランスのアプローチは、どちらの要因によって作り込まれた故障についても対策としては有効である。また、ソフトウェアのバグはシステマティックフォールトに該当する。そこで、同一の機能性を実現するための機能をそれぞれ別のソフトエンジニアによってプログラム開発を行った、ソフトウェアをそれぞれ搭載させ、互いに、動さに差異があった際は、異常と判断するといった方法が考えられる。ソフトウェアでは、N バージョンプログラミング [15]と呼ばれている。(ただし、上記のマイコンの並列処理と同様に、2 つの並列処理では、片方が異常値を出力した場合、正常である側との区別がつかないために、3 つ以上の並列処理が使われる。)
これらに関する検証の詳細は 7 章にて示す。

(3) CAE を用いた主張同士の関係性のパターン

GSN と同様に、階層化された木構造として論証を行う方法に CAE [16]がある。 [17]においては、親子関係の主張同士の関係についての議論構造を CAE を用いて表現している。[17]においては、主張同士の関係性としての以下分類としての定義を行っている。

- Decomposition block

- Substitution block
- Evidence incorporation block
- Concretion
- Calculation block

- **Decomposition block**

Decomposition block においては、オブジェクト X に対するプロパティ P（X）が、それから構成されるサブオブジェクト X1、X2、…、Xn の プロパティ P1（X1）∧P2（X2）∧…∧Pi（Xn）を参照することによって示されることを示す。（なお”X”に相当するものは [17]においてはオブジェクトと呼んでいるが、本研究ではサブジェクトと呼んでいる。）オブジェクト X のプロパティ P（X）とするとき、本ブロックでの関係は [17] より、図 75 ようにあらわされる。[17]において、プロパティ、サブジェクトのどちらか一方を分割された形態を Single decomposition と定義している。

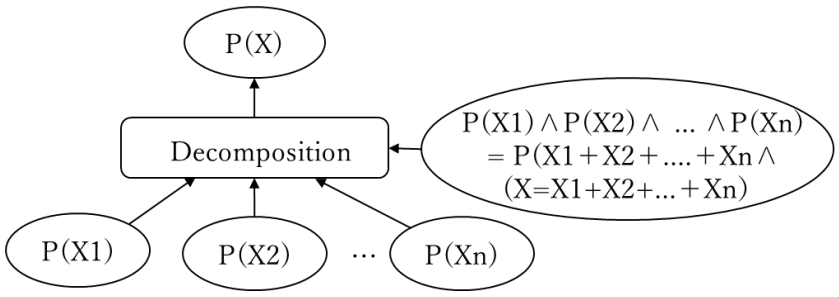


図 75 Decomposition block （[17] Figure5）

オブジェクト X が、X1、....、Xn として分割される形態は、パターン(f)と類似する。一方で、本研究での GSN サンプル調査で見つけられた範囲において、プロパティ、又はサブジェクトはどちらか一方について分割されている GSN サンプルのみが検出されており、その両方が同時に分解されている形態のものは見つかっていない。従って、現時点でのサンプル調査の範囲において、プロパティ、サブジェクトのどちらか一方だけが分割されているものとして、Single decomposition に相当するものがパターン(f)の特徴と類似したものとして考える。

- **Substitution block**

Substitution block においては、オブジェクト X のプロパティ P（X）が、別のプロパティ、オブジェクト Q(Y)に置き換えられている形態を示している。オブジェクト X のプロ

パティ P（X)、オブジェクト Y のプロパティ Q（Y）とするとき、本ブロックでの関係は[17]より図 76 のように表される。

この分類は、本研究のパターン(b)、(c)、(d)に類似している。なお、パターン(b)、(c)、(d)は、単一の子を持つ構造を持つものであり、複数の子を持つ構造をもつパターン(e)についても、置き換えが行われていると考えられるので、パターン(e)についてもこの分類と特徴が一致していると考えられる。

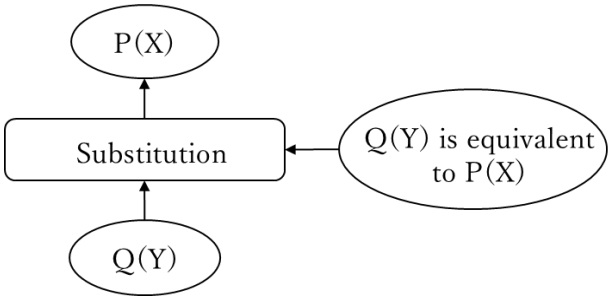


図 76 Substitution block （[17] Figure6）

ただし、Decomposition block と同様に、[17]においては、プロパティ、オブジェクトが同時に置き換えられているが、本研究の GSN サンプル調査においては、プロパティに対しての置き換えがなされている GSN のみが見つかっている。

- Concretion block

Concretion block においては、オブジェクト X のプロパティ P（X）が、具体化された P1、X1 によって P1(X1)として具現化されている形態を表している。本ブロックでの関係は[17]より図 77 のように表される。

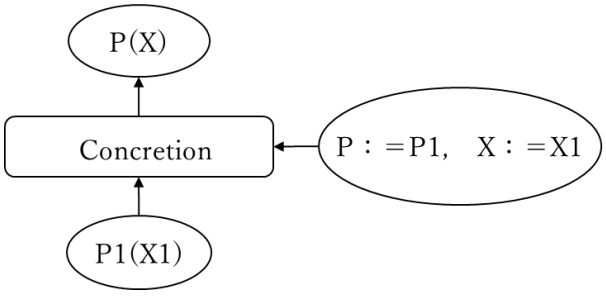


図 77 Concretion block （[17] Figure8）

ここで、本研究において、パターン(a)の持つ特徴が、元の主張に対して、選択、抽出された一部分を以て、元の主張（全体）についての達成を示そうとしているが、このConcretion block に類似していると考える。

- Calculation block

Calculation block おいては、オブジェクト X が証拠と共に計算として示される特徴としている。計算によって示される特徴として該当するパターンは、6 パターンにはないが、親ゴールの全要素が、子ゴールの各要素から成り立っている特徴としては、パターン(f)MECE に類似する。

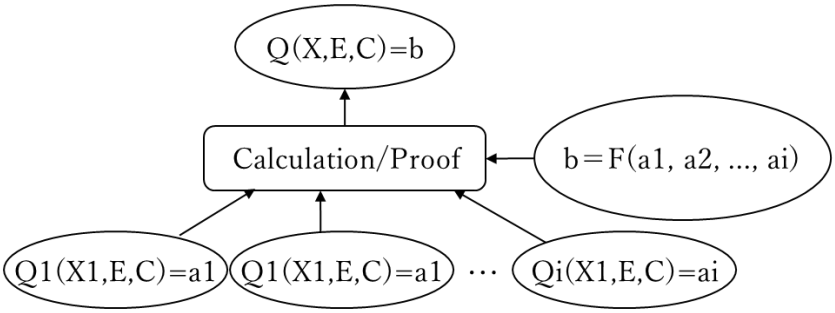


図 78 Calculation block

(4) セーフティケースパターンカタログ

セーフティケースを表すための、GSN カタログとして、 [18]において以下が 3 つの視点について沿って挙げられている。

1.トップダウンパターン

- ALARP（As Low As Reasonably Practicable）

  主張に対して、合理的にかつ実行可能な限りにおいて低いことを目指すといった指針であり、主張同士の構造上の関係を表す特徴ではないため本研究の 6 パターンの分類とは関係性はないと考える。

- Hazard Directed Integrity Level Argument

  システムに及ぶ危険性に適した完全性のレベルにまで開発がなされていることを目的とした主張による構成について指しており、主張同士の構造上の関係を表す特徴ではないため本研究の 6 パターンの分類とは関係性はないと考える。

- Control System Architecture Breakdown

  システム等の構造に着目した展開である。これは、保証ケース議論分解パターン [12]における、“1.アーキテクチャ分解”に相当し、本 6 パターンにおいては、パターン(f)MECE の部類の一部に属ずるとみなすことができる。

2.一般的構造パターン

- Diverse Argument [18]

  達成を支持する主張に対して、もし、その主張の妥当性や根拠が失われた場合に、補足的に別の主張を多足的に持つ考えである。本 6 パターンにおいては、パターン(e)が類似するが、足同士（子ゴール同士）の主となる議論の破綻に備えての副となる主張といった関係性は想定していない。パターン(e)は、それぞれ異なる視点同士の主張の組み合わせにより、相互的に、相乗的に親の主張の達成を示す場合のものとして想定している点において、特徴が異なる。また、この分類は、“(2)多足議論（Multi-legged arguments）“の“3. 主となるものと弱点を補う主張”に類似する特徴と考える。

- Safety Margins

  [18] に 挙げられている“Safety Margin”としての考え方としての GSN モデルを示す。

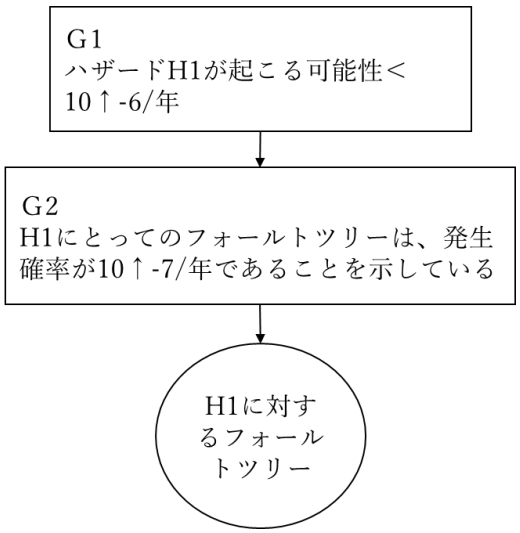


図 79 Safety Margin（ [18] Figure 76）

この分類は、ゴール G1 における基準値が、より安全方向へのマージンを持つ範囲としてG2置き換えられていることが分かる。この考え方は、パターン(c)における、より厳しいものへの置き換えている考え方と一致している。

ただし、パターン(c)では、このような基準値を上げたものへの置き換えに加え、不明確な基準（又は、主張自体に基準がない）ものに対して、何かしらの基準値を設けて、より明確なものへの変換についても含まれ、これら双方を併せて一つのパターン(c)として分類している。

これは安全性や信頼性を主張する際には、何かしらの基準を設けて説明しようとしているとケースは見られ、曖昧さがなくなり明確になるようにする過程であるが、明確な基準を付与することと、より厳しい基準に置き換えることの双方において、記述者にとっては、基準に対して十分であるレベルを設定しようとするものであることから、双方は同じパターン区分として分類としている。

3.ボトムアップパターン

- Fault Tree Evidence

FTA(Fault Tree Evidence)の分析を根拠とする論証の分類である。

FTA の結果を基準化として採用する場合は、パターン(c)との類似性も考えられるが、基準化や、証拠に用いる手法や種類についての特定は、本 6 パターンでの分類では区別していない。

これら(1)から(4)について表 10 から表 12 にまとめた。

表 10　関連研究との比較（1）

関連研究における分類		比較結果
(1)分解型の分類	1.アーキテクチャ分解	分解に相当しパターン(f)に属するとみなされる。全ての子を合わせたものは親における全範囲にとって網羅性があるといった特徴において、パターン(f)と類似する。これらはパターン(f)について、さらに細分化された分類であるとみなすことができる。
	2.機能分解	
	3.属性分解	
	4.帰納分解	
	5.完全分解	
	6.単調分解	
	7.修正分解	
(2)多足議論（Multi-legged arguments）	1.論理的と統計的な主張	主張同士が相乗的、又は補完的な関係である特徴において、パターン(e)と共通の特徴を持つ。
	2.間接的と直接的な証拠や主張	主張同士が相乗的、又は補完的な関係である特徴において、パターン(e)と共通の特徴を持つ。
	3.主となるものと弱点を補う主張	副となる側が、主となる側の主張に対してその脆弱性を補うことが想定されるといった点については、相乗効果としての性質としてパターン(e)の特徴と一致する。しかし、実際にこのような関係性を持つ子ゴール同士を持つものは、本研究で行ったGSNサンプルには見つかっていないため、パターン(e)とは異なる特徴とみなすことが妥当と考える。一方で、この分類に該当するものは、1-out-2といった機構としての構造上の冗長性を表す場合に有効であると考える。
	4.複数チームによる主張	同様の主張を複数のチームや、機構で達成しようとする構成がこの分類に該当すると考える。片方の主張の達成が破綻した場合に、もう片方が補うことができるといった関係は、相乗的な関係性としては、パターン(e)の特徴と類似する。しかし、実際のGSNのサンプルにおいては、このような構成に該当するものは見つからず、パターン(e)と同類とはみなされないと考える。また、これも「3」と同様に、機構としての構造上の冗長性（2重冗長、3重冗長、等）との類似性があるとみなされる。

表 11　関連研究との比較（2）

関連研究における分類		比較結果
(3)CAEを用いた主張同士の関係性のパターン	Decomposition block	パターン(f)に類似する。一方で、サンプル調査においては、サブジェクトと、プロパティが同時に分割されている（Double decomposition）ものはなく、どちらか一方が分割されているもの（Single decomposition）に相当するものとしてのみ存在する。
	Substitution block	単一の主張への置き換えがなされている特徴としては、パターン(b)(c)(d)の特徴と共通する。複数の主張への置き換えとしを含めた場合、パターン(e)についても共通性がある。また、Substitutionにおける変換に際しては、置き換え前後が等しいものとして想定されているが、パターン(b)以外のパターン(c)(d)(e)の置き換えにおいては、強弱の変化や、読み手の解釈の違いが影響するものとし、必ずしも等しい置き換えを想定していない。また、Substitionは、サブジェクトとプロパティの両方が変換されていることを示しているが、サンプル調査において見つかったものに基づきパターン(b)(c)(d)(e)は、プロパティだけが変換されるものとしている。
	Evidence incorporation block	GSNの構成においては、ゴールに対して、エビデンスの関係に相当する。本研究の6パターンは主張同士の関係に着目しているため、該当、及び類似性はない。
	Concretion	具体的な主張で全体の主張を示す方法は、パターン(a)の考え方に類似している。Concretionでは、サブジェクト、プロパティの両方が同時にその変換をする想定であるが、パターン(a)では、どちらか一方だけの変換だけが想定されており、さらにサンプル調査においては、プロパティの変換だけが検出されている。
	Calculation block	子ゴールの計算によって、親ゴールの妥当性が示される分類である。子ゴールの計算結果が、親ゴールの結果を満たすといった想定の場合、パターン(f)と類似するが、計算といった方法で示すという、視点に特価した分類としては異なっている。

表 12　関連研究との比較（3）

関連研究における分類			比較結果
(4)セーフティケースパターンカタログ	1.トップダウンパターン	ALARP（As Low As Reasonably Practicable）	リスクを下げるための視点にそった達成を目指すものであり、主張同士の構造の特徴ではなく、本6パターンの特徴とは共通点はない。
		Hazard Directed Integrity Level Argument	ハザードレベルに沿った議論アプローチを指している。主張間の関係性を表す本6パターンとは関係性はない。
		Control System Architecture Breakdown	対象とするサブジェクトに対して、アーキテクチャの視点に沿って子ゴールへの展開がなされる。アーキテクチャ分解[12]に類似し、パターン(f)の一つであるとみなすことができる。
	2.一般的構造パターン	Diverse Argument	子ゴール同士が、多様性のある、子ゴールを持つことで、その多様性が大きいほど、親ゴールの達成の各示度が増すといった考え方である。異なる視点の主張同士を組み合わせる方法であり、これは、パターン(e)の特徴と類似している。しかし、Diverse Argumentにおいて、より多くの多様性を子ゴールとして追及しようとする目的は、どれかの子ゴールの主張の達成に意義が唱えられた時に、他の子ゴールが補完的に、親ゴールの達成の支持を行うといった意図が強い。一方で、パターン(e)については、親ゴールの主張に対して、ある子ゴールの主張に対して、相乗効果を生み出すための、最良な組み合わせを見出すことにある。
		Safety Margins	基準値として、より安全な主張によって達成しようとしているパターンである。パターン(c)と類似している。一方で、パターン(c)は安全性のような不明確な主張に対して明確な基準（公認されている安全性レベル等）を与える場合についても含まれる。
	3.ボトムアップパターン	Fault Tree Evidence	FTA(Fault Tree Analysis)から導出できる主張の性質のことを表している。本6パターンにおける主張同士の関係性の視点とは異なる。

6.3. まとめ

- 産業界における GSN 事例について挙げた。また、それら GSN が 6 パターンにおいて、パターン(f) に該当することを確認した。6 パターンのうちの一つに合致したことで、6 パターンの有効性が確認された。ただし、今回産業界における GSN サンプル調査は十分ではないため、今後サンプルを増やすことが課題である。
- 6 パターンの特徴について過去の関連研究との関係性について比較を実施した。既存のパターンの考え方が、6 パターンのいずれかに含めて考えることが可能なものもあったが、6 パターンと完全に一致するものではなかった。また、関連研究におけるパターンの中で、理論上はあり得るとされる特徴を持つ特徴であっても、6 パターンには含まれない場合があり、それらは GSN サンプル調査で見つかっていないものに基づいているため、6 パターンに欠落しているものについては、網羅性としては、問題ないと考えられる。
- 既存のパターンのうち、2 足（2 つの子ゴール）における主張の関係が、構造上の冗長性を表すものについては、GSN のとして表現することができないことについて説明をした。なお、それら構造上の冗長性と GSN の関係については 7 章で説明する。

第 7 章　冗長機構への適用の検証

以下に、実際に安全機構については、例えば、以下のような機能ブロック図を用いて表現することができる。これは 6.2 章における“(2)多足議論”の“3. 主となるものと弱点を補う主張”に対して、機構上の冗長性設計と比較した場合の検証である。

自動車などのアクセル制御を持つシステムにおいて、アクセル操作量に応じて、アクセル開度出力を生成する機能ブロックを考える。

ワークショップ#1 において、行った演習については、7.3 章で説明する。

ここでは、あくまで、1-out-of―2 の考え方についての冗長構成を表す手法として、SCDL の図法 [19]を使用するものとする。

以下の事例を示す。

外部入力をアクセル操作量とし、外部への出力をアクセル開度出力とするシステムを考えるとする。その機能ブロック図は、例えば図 80 のように表現することができる。

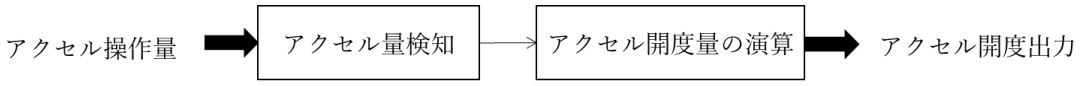


図 80 アクセル制御の機能ブロック図（安全機構なし）

この機能ブロック図において、一連の、アクセル操作量 →アクセル量検知 →アクセル制御量の計算 →アクセル開度出力 は、本来のアクセル制御を行うといった機能を担う。

次に、アクセル量検知機能において何かしらの機能障害が発生した場合を想定した安全機構としての安全機能を付与した場合の表現について考える。

安全機構としては、例えば、異常を検知し、安全側に操作する機能としてアクセル量をゼロにする機構を考えた場合、安全機構を付与した状態の機能ブロック図は図 81 のように表すことができる。

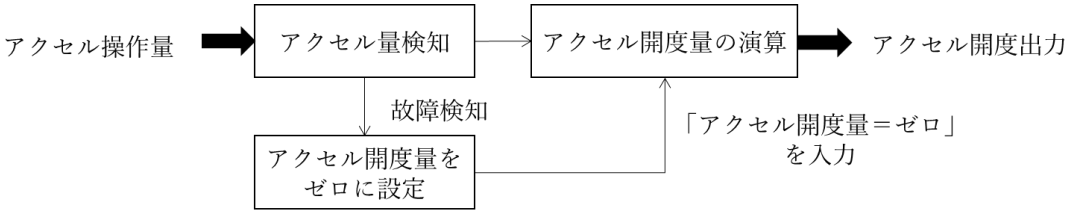


図 81 アクセル制御の機能ブロック図

次に、この安全機能を付与したシステムについての安全論証を GSN 上で表現した場合の例としては、図 82 のように表すことができると考える。

アクセル操作についての安全性を示すにあたり、主となる足（子）としての G1 に対し、G1 の潜在的に深刻な弱点を補うためのもう片方の足として G2 が構成されている。（これは、6.2 章における“(2)多足議論（Multi-legged arguments）”の“3.主となるものと弱点を補う主張”の特徴を持つ GSN の作成事例と考える。）

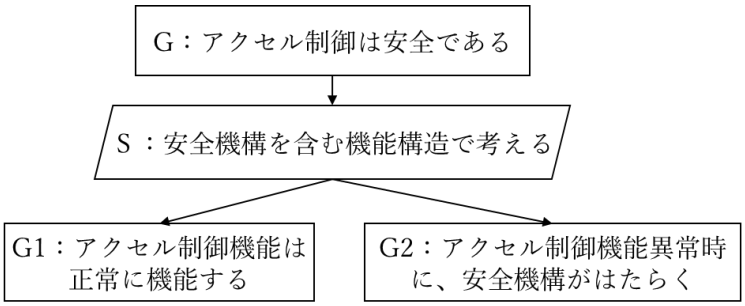


図 82 アクセル制御の GSN

次に、図 83 の機能ブロック図に示す冗長機構について考える。これは、自動車のステアバイワイヤの操舵量演算機能の並列処理機能の冗長機構としての例である。

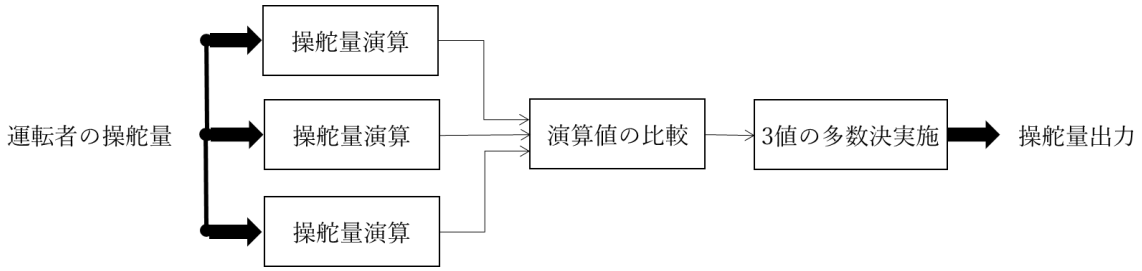


図 83 ステアバイワイヤの機能ブロック図

この機能フロー図においては、並列される操舵量演算が相互に同じ機能を持つ冗長接続の関係になっている。（これは、6.2 章における“(2)多足議論（Multi-legged arguments）”の“4. 複数チームによる主張”の特徴に相当する冗長性について検討する上で、機能ブロック構造として表したものである。）

この機能ブロック図における演算は並列な構造関係として成立している。なお、機能ブロック図の個々のブロック図における内容は、機能についての説明であり、主張ではないと言える。つまりシステムの冗長的な機能について並列に設けられている、冗長機構そのものを GSN の足として表現することは適当ではない。（“4. 複数チームによる主張”に該当するものは、見当たらなかった結果からも、同様にことが言える。）

一方で図 84 のように、機能構造としての冗長機構が、なぜ、安全を担保できているかを説明する GSN モデルを作成することは可能であると考える。この GSN における足（子）

同士の関係は、“4. 複数チームによる主張”について、拡張した考え方としての”冗長性を持った機構"に対する複数の足の構造とは異なった関係になっている。

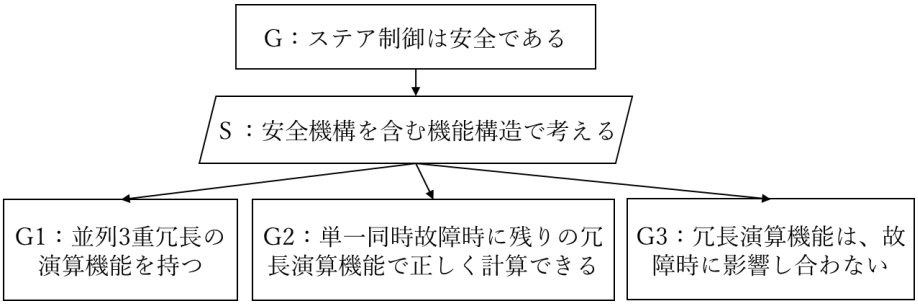


図 84 ステアバイワイヤの GSN

このように、冗長としての機構そのものを、GSN での木構造の足（子）に対応させて表現することは、適当ではないが、その冗長性を説明するための主張としての GSN を作成することは可能であると考える。

そこで、ワークショップ#１の SCDL 編において、機能ブロック図と、GSN とを組み合わせた安全性の説明についてのその事例を示すことを行った。この実施については、7.1 章にて説明する。

7.1. 検証の流れ

ワークショップ#１の SCDL 編においては、以下について実施し、本章においては、これらについての説明を行う。

- SCDL を使った機能モデルの作成についての説明
- SCDL を使った安全機構設計の演習
- SCDL と GSN を組み合わせた使用例（説明のみ）

7.2. SCDL について

SCDL の文法はについて詳しくは [19]に説明があるが、図 85 に簡単な例を示す。SCDL を使った図法では、図 85 の右に示す部品を用いて、要求（機能要求）の関係、フローを描くことができる。なお SCDL によるモデルは、構造を表す機能ブロック図が該当するが、機能フローを表現することも兼ねている。また、エレメントと呼ばれる部品は、機能構成を設計した後で、物理的なサブシステムや部品等への割り付けを行うことも想定されており、機能要求の表現を物理的な要求（構造要求）への割り付けの表現も可能としている。本ワークショップでは、エレメントは使わず、機能レベルでそれぞれの機能の関係性を表現することに注力するものとしている。

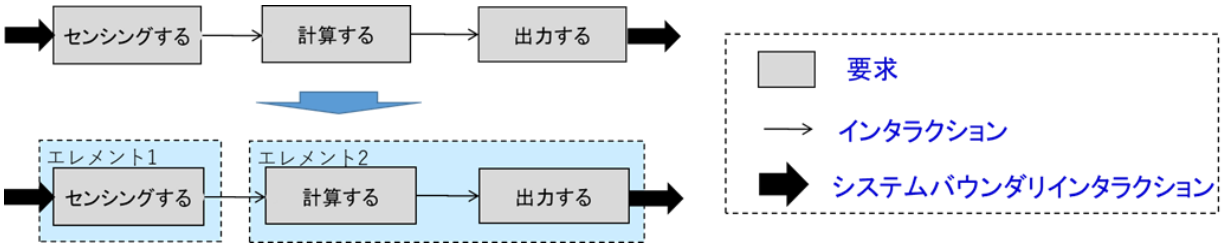


図 85 SCDL を用いた表現

次に、機能どうしが描かれる場合に、機能不全を起こした場合の振る舞いを考える。図 86 において、加速機能を持つシステム（自動車等）において上段の加速度を出力する機能構成に対して、下段の図は、加速度を制御する機能が機能不全に至った場合を考慮し、安全に振る舞う機構を加えた構成を表している。

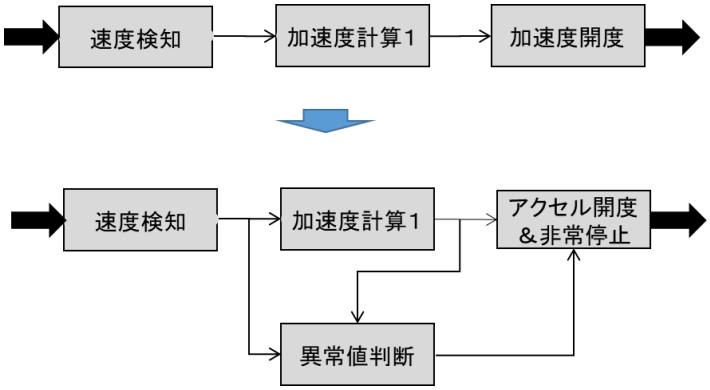


図 86 SCDL を用いた表現（安全機構）

7.3. 演習結果

7.2 章のような機能ブロック図（フロー図）に表すことで、このアクセル制御機能に、安全機構が付与されていることが分かる。なお、図 86 において、加速度計算 1 が機能不全に至った場合、異常値判断が連動して同時に機能不全に至らないことは安全設計上において必要であり、そのような観点の気づきを与えてくれる図法でもある。(“同時に機能不全に至らない”を SCDL 図上に記載することも可能である。)

参加者に対して、図 87 の演習課題を行った。

演習）

A1) システム故障時として、各機能（要求）エレメントごとが機能不全に至った場合の冗長機構を追加してください。

A2) 意図する機能(主機能と言ったりもします）と冗長機能についてそれぞれのペアを作ってください。

B1) 以下の操作を行った場合、自動操舵機能はキャンセルされ、以後、ユーザの操作に委ねられます。
・ユーザがステア操作力を与えた場合
・ウィンカー操作を行った場合
これらのユーザ動作から始まる操作も(ユーザの代行操作と捉え）①での冗長機能と同様に追加してください。

B2）「A2」と同様にペアを作ってください。

※ここでの、自動操舵機能は、車線に沿って走行する機能を対象とし、交差点右左折や車線変更は含まれません。

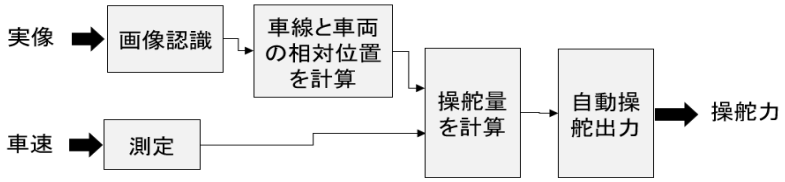


図 87 SCDL 演習

なお、参加者が作図する際は Astah System Safety を事前にインストールしてもらい各自の PC で演習時間内で作図を行っている。

図 88 に参加者から演習で得られた結果のサンプルを示す。

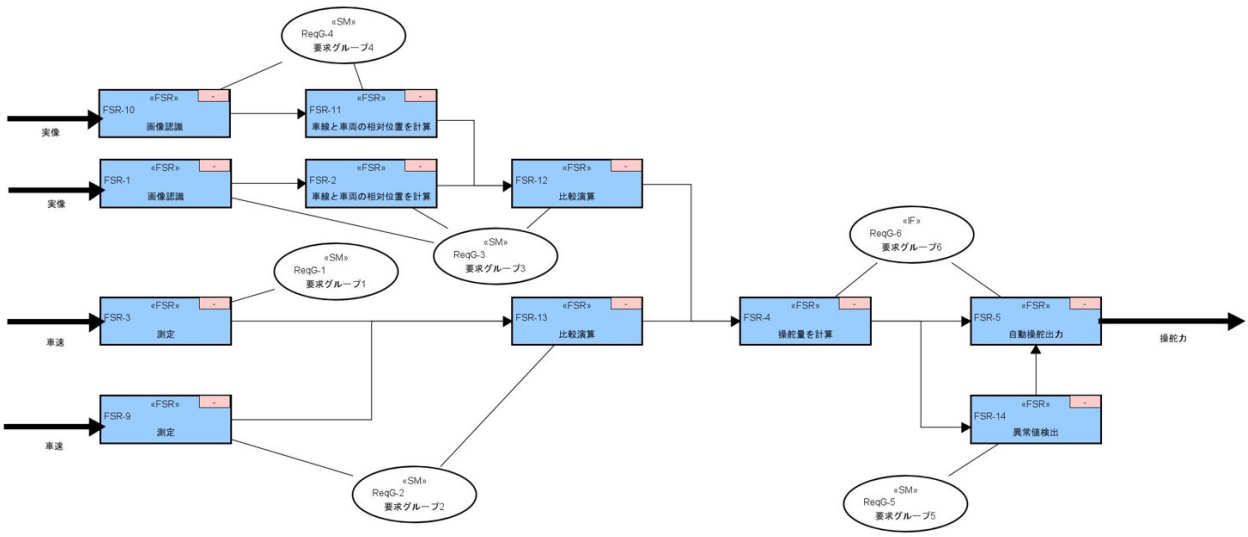


図 88 参加者により作成された SCDL モデルサンプル

7.4. SCDL と GSN の共用

続いて、本ワークショップにおいて、SCDL で描かれた安全機構について GSN モデルを用いて安全である根拠についての表現することについての説明を行った。SCDL モデルを作成した図の安全機構の働きが、どのように、GSN モデル上で説明することができるかを説明し、理解してもらうことを試みている。

但し、本ワークショップへの参加者は、SCDL モデルを使った機能ブロック図を作図するといった作業を経験することに終始し、相互を組み合わせて表現する方法を紹介することに留まっている。(今後のワークショップでは、さらに、実習を通じての理解を得てもらうことを目指したいと考えている。)

図 89 に今回の SCDL の演習の回答例を示す。なお、この SCDL を用いてに設計された安全機構を GSN で説明するために、安全機構 SM1～SM6 を明記してある。

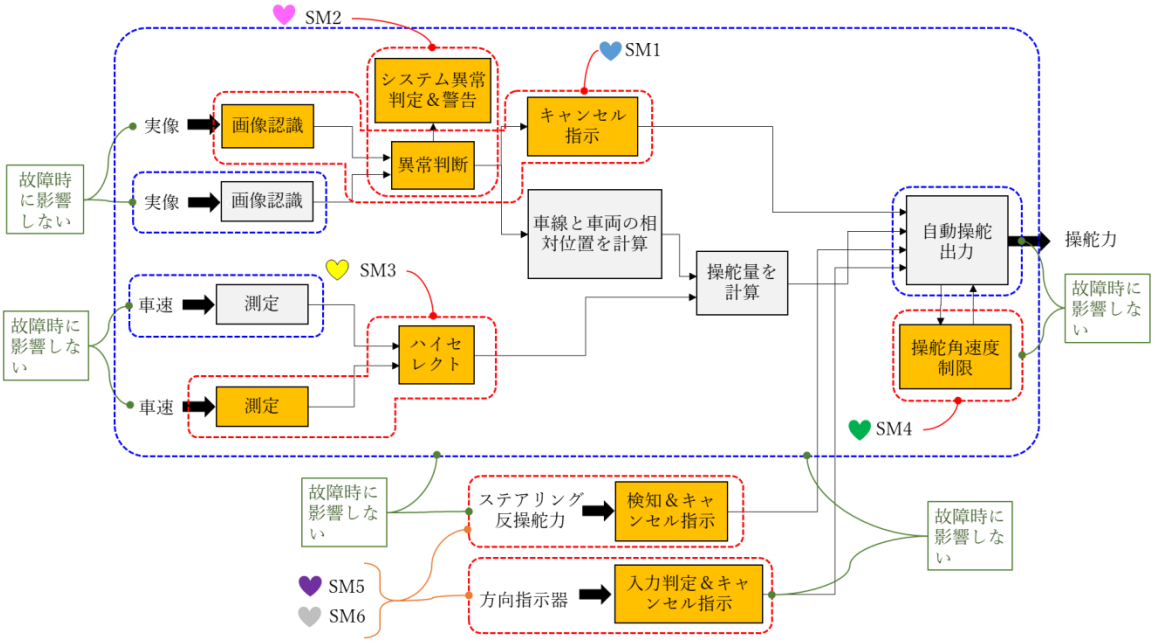


図 89 SCDL の作成（回答例）

次に、図 89 における SCDL において、達成されている安全性を説明するための GSN サンプルを図 90 として用意した。(用意した GSN は、今回のワークショップでは、説明用として予め用意したものであり、演習として参加者が作成することは行っていない。)

この GSN は、機能構成を表している SCDL について、その機構上で、達成されている安全性について説明しようとするものである。以下、それぞれの安全機構 S1～S6 に対応したものとして、GSN 上のゴールの主張として説明がなされている。(安全機構 S1～S6 は SCDL 上の機構上の関係性から読み取ることが可能である)

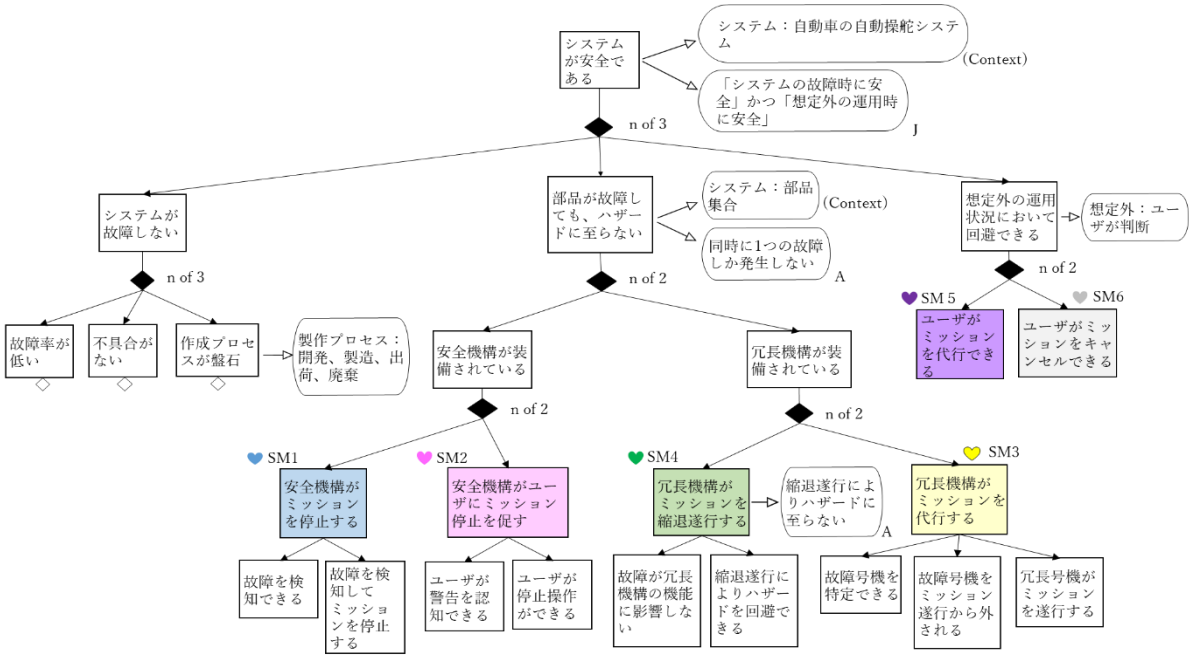


図 90 SCDL 図に対応する GSN モデルの例

SM1：“安全機構がミッションを停止する”

故障時にミッションを停止する。これは、ミッションを安全に停止することが可能でかつ停止が完了した後も安全性が確保されることが求められる

SM2：“安全機構がユーザにミッション停止を促す“

故障時にミッションを停止するために、ユーザの判断と操作が介入する。これは、システム単独では、安全に停止を行うことが難しい場合が相当する。

SM3：“冗長機構がミッションを代行する“

システムに付帯されている安全機構が意図する機能の機能不全（故障）に対して代行し、ミッションを遂行することを意味する。

SM4：“冗長機構がミッションを縮退遂行する”

SM3 と同じくシステム自体によってミッションを遂行しようとするが、機能不全（故障）による影響を除外又は最小限にし、ミッションを遂行することを意味している。

SM5：“ユーザがミッションを代行できる“

ユーザがミッションを代行することを想定している、安全機構である。警告灯表示、音声警告等がこれに該当する。

SM6：“ユーザがミッションをキャンセルできる”

このように、本ワークショップにおいては、冗長性を持つ安全機構について、SCDL を用いて機能の機構を表現することを行い、それらの安全機構の考え方についての説明を行うための GSN を用意することを行った。

これらは、6.2 章の Multi-legged argument における“3. 主となるものと弱点を補う主張”及び、“4. 複数チームによる主張”における足（子）同士の考え方との関連があると考えるが、冗長構造自体を GSN 上の足（子）の関係として表現することは適当でないと考えた。そこで、機能の安全機構を題材とし、まずは SCDL モデルを用いてそれらの構造上の表現を行い、その構造の仕組みについて安全性が保たれる説明を用意するための GSN とを組み合わせることで、安全機構に関係する安全性の論証において効果的な GSN の使い方ができるものと考えた。

7.5. まとめ

安全機構の冗長性について GSN をどのように記述できるかの検討を行った。パターン(e)においては、Multi-legged argument と共通する特徴があることが挙げられるが、そのうち、1-out-of-2 とする安全機構設計に対し、GSN を併用し、それらの安全性を表記する試行を行った。

第 8 章　結論

本論文では、主な成果は以下のとおりである。

1. GSN を使った記述の容易化を行うため、構造上の特徴を捉えるための検討、分類を行い、6 個のパターンへの分類を行った。

2. 6パターン分類を行うにあたって、GSN 上での以下の特徴について検討を行い、パターン分類を行う上での着眼点とした。
   これらより、パターン分類を行うにあたり、ゴール以外に、ストラテジにも着目し、主張が含まれるノード間の関係として捉えることが適当であることを見出した。
   - GSN の子ゴール同士の、親ゴールに対する関係は分解以外の構成も存在することを見出した。
   - 親から子の階層のゴール展開で、主張の変換がなされていることを見出した。
   - 主張の変換が行われる場合、ストラテジの使われ方において、隠れた主張があることに注意が必要であることを見出した。

3. 数十個のサンプル調査を経て、(a)から(f)の 6 個のパターンに分類できることを導き出した。

4. 6 個のパターンについて、特徴を整理し、子の数の構成といった構造上の違いの他、議論上の強弱関係があるといった違いがあることを見出した。

5. 既存の公開されている 273 個の GSN 図に対してサンプル調査を行い、718 箇所に対して、6 パターンへのパターンマッチング（いずれかに一致ができるかどうかの確認）をおこなった。
   パターンマッチングの結果、調査した全ての GSN について 6 パターンのいずれかに合致させることが確認された。

6. パターンが一致したものとしては、合計 11 種類のゴール、ストラテジの構成バリエーションのとして見つけることができた。

7. パターンについては、取得できる全論文の 8%程度の調査にとどまっている。全てのパターンが登場してきているため、傾向を掴む目的としてのサンプルとしては要件を満たしているが、今後、調査対象数を広げることで、それらの精度を上げることができると考える。

8. ワークショップを行い、6 パターンが第三者にとって理解され、かつ有効なものになるかの確認を行った。結果は、参加者が作成した GSN 上において 6 パターンを意識した GSN を作成することができたこと、及び、各パターンの特徴の理解度、有用性について参加後のアンケートより、高評価を得ることで、6 パターンの有用性が確認された。

9. ワークショップの実施は、2 回行った。更に回数を増やすことで、第三者の評価の精度が向上すると考える。またパターンの特徴についてより分かりやすい説明や、より理解されやすい GSN サンプルの選定といったことが、改良されていくものと考える。

10. ワークショップは、新型コロナの影響で、2 回共に、リモート形式で行った。実施に向けては、説明や、演習をリモート方式においても効率的に行うために、ツール選定や参加者との相互コミュニケーションをとるための工夫を行った。今後も、ワークショップの回数を重ねることで、それらは、更に改良がされていくと考える。

11. 既存の多足議論（Multi-legged argument）の考え方や、GSN のパターンのカタログ的に挙げられているサンプルについて比較考察をおこなった。結果、個々のパターン単体として特徴として、類似しているものが幾つかあることを確認された。しかし GSN 上で、親子、または子同士の関係性を特徴として捉え、理論的な解釈を付加しながら、階層間を読み進めるのに適当なパターン群のパッケージとしては、類似するものはないことが確認された。

12. 関連研究の考察において、GSN では表現され得ない（少なくともサンプル調査では見つかっていない）ものがあった。それは、機構上の冗長性を多足議論の考えとして表すものに相当する部類であると考察した。

13. 機構上の冗長性における、安全性を示すための、用いることができる GSN について検討をした。結果、機構上の冗長性そのもの GSN で表すのではなく、別途機構を表す表現と GSN を併せて用いることの可能性の提案をおこなった。自動運転の自動操舵における安全機構を題材に、機能ブロック図と GSN を併用し表したものとしてサンプルを作成した。

14. 6 パターンにおけるサンプル調査した結果については、元の GSN 図から、主張の部分だけを抽出した形式、かつ日本語に翻訳した形式として、マッチングに使用した全ての主張と、それぞれに一致させたマッチングの結果について表形式にまとめた。

謝辞

本研究をまとめるにあたり、種々のご指導、ご鞭撻、ご支援を賜りました、日本大学理工学部 松野裕准教授、高橋聖教授、細野裕行教授、泉隆特任教授に心から感謝の意を表します。また、貴重なご助言をいただきました、名古屋国際工科専門職大学 情報工学科 教授（名古屋大学 名誉教授）山本修一郎博士に感謝を申し上げます。ワークショップ開催におけるサポートをいただきました、株式会社チェンジジョン 高井利憲博士に深く感謝いたします。社会人として博士課程に臨むにあたり、貴重なご助言をいただきました日産自動車株式会社 大村一世氏に心より感謝いたします。

参考文献

[1] 日本経済新聞社, “トヨタ、940 億円で和解　米大規模リコール訴訟,” *日本経済新聞,* 27 12 2012.

[2] ISO, ISO 26262: Road vehicles - Functional safety, 2011.

[3] ISO, ISO 26262: Road vehicles - Functional safety, 2018.

[4] ISO, “ISO/DIS21448,” 2021.

[5] Underwriters Laboratories Inc., “UL4600 October 2, 2019,” 2 10 2019.

[6] The Assurance Case Working Group [ACWG], Goal Structuring Notation Community Standard, 2018.

[7] Y. Matsuno, D-case communicator: A web based GSN editor for multiple stakeholders, Computer Safety, Reliability, and Security - SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017.

[8] DEOS 協会 技術部会・標準化部会, はじめてみる IEC62853 の実装, 2018.

[9] DEOS 協会 D-Case 部会, D-Case 構文定義書, DEOS 協会 D-Case 部会, 2015.

[10] Birch, Safety Argument Framework for Vehicle Autonomy, HORIBA MIRA Ltd, 2017.

[11] MISRA, Guidelines for Automotive Safety Arguments, 2019.

[12] 山本修一郎, 保証ケース議論分解パターン：要求工学, 株式会社ビジネスコミュニケーション社, 2013.

[13] Bloomfield , Littlewood, Multi-legged arguments: the impact of diversity upon confidence in dependability arguments, : pp 35－34, International Conference on Dependable Systems and Networks, 2003.

[14] B. Littlewood , D. Wright, “The Use of Multilegged Arguments to Increase Confidence in Safety Claims for Software-Based Systems, ” IEEE Transactions on Software Engineering, 2007.

[15] Knight , Leveson, AN EXPERIMENTAL EVALUATION OF THE ASSUMPTION OF INDEPENDENCE IN MULTI-VERSION PROGRAMMING, 第 %1 巻（全 %2 巻)Volume: SE-12, IEEE Transactions on Software Engineering (Volume: SE-12, Issue: 1, Jan. 1986), , Jan. 1986, p. 96–109.

[16] ADELARD, “Claims, Arguments and Evidence (CAE)”.

[17] Bloomfield, Building Blocks for Assurance Cases, : IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2014, p. 186–191.

[18] Kelly, Arguing Safety - A Systematic Approach to Managing Safety Cases, PhD Thesis. Department of Computer Science, The University of York, 1998, p. Sec. 4.8.1.

[19] Safety Concept Notation Study Group, SCDL 仕様書 Ver1.5, : Safety Concept Notation Study Group, 2018.

[20] Hawkins, Habli, Kelly , Mcdermid, Assurance cases and prescriptive software safety certification: A comparative study, Safety Science 59 (2013), 2012.

[21] Kelly, A Six-Step Method for the Development of Goal Structure, York Software Engineering, Flixborough, 1997.

[22] Wagner, Schatz, Puchner , Kock, A Case Study on Safety Cases in the Automotive Domain: Modules, Patterns, and Models, IEEE 21st International Symposium on Software Reliability Engineering, 2010, p. 269–278.

[23] Wang, Guiochet, Motet , Schön, Modelling Confidence in Railway Safety Case, Safety Science, Safety Science (110 part B), 2018, pp. 286-299.

[24] 松野裕, 越山勉 , 他, はじめての D-Case, 一般社団法人 ディペンダビリティ技術推進協会 D-Case 部会, 2018.

[25] Rushby, “The Interpretation and Evaluation of Assurance Cases,” Technical Report SRI-CSL-15-01, 2015.

[26] Hawkins, Kelly, Knight , Graydon, “A new approach to creating clear safety arguments,” Springer, London, 2011.

[27] Fenn, Hawkins, Williams , Kelly, “Safety case composition using contracts-refinements based on feedback from an industrial case study,” Springer, 2007.

[28] Kelly, “A systematic approach to safety case management,” JSTOR, 2004.

[29] Habli , Kelly , “A safety case approach to assuring configurable architectures of safety-critical product lines,” Springer, 2010.

[30] Björnander, Land , Graydon, “A method to formally evaluate safety case evidences against a system architecture model,” 2012.

[31] Habli , Kelly, “Safety case depictions vs. safety cases-would the real safety case please stand up?,” 2007.

[32] R. Lewis , “Safety case development as an information modelling problem,” 2009.

[33] Z. Li , “A systematic approach and tool support for assessing GSN-based safety case,” 2016.

[34] D. Bush , A. Finkelstein, “Reuse of safety case claims-an initial investigation,” 2001.

[35] C. Hirata, S. Nadjm , Tehrani, “Combining GSN and STPA for Safety Arguments,” 2010.

[36] J. Guiochet, Q. D. Hoang , M. Kaaniche, “A model for safety case confidence assessment,” Springer, 2014.

[37] T. Kelly , J. McDermid, “Safety case construction and reuse using patterns,” 1997.

[38] T. Kelly, “Concepts and principles of compositional safety case construction,” 2001.

[39] C. Holloway, “Safety case notations: Alternatives for the non-graphically inclined?,” 2008.

[40] K. Taguchi, D. S , H. Nishihara, “Linking traceability with GSN,” IEEE International, 2014.

[41] P. Chinneck, D. Pumfrey , T. Kelly, “Turning up the HEAT on safety case construction”.

[42] T. Kelly , J. McDermid, “Safety case patterns-reusing successful arguments,” 1998.

[43] A. Ayoub, B. Kim, I. Lee , O. Sokolsky, “A safety case pattern for model-based development approach,” Springer, 2012.

[44] P. Chinneck, D. Pumfrey , J. McDermid, “The HEAT/ACT preliminary safety case: a case study in the use of goal structuring notation,” Citeseer, 2004.

[45] R. Dardar, B. Gallina , A. Johnsen, “Industrial experiences of building a safety case in compliance with iso 26262,” 2012.

[46] R. Palin , I. Habli, “Assurance of automotive safety–a safety case approach,” Springer, 2010.

[47] W. Greenwell, E. Strunk , J. Knight, “Failure analysis and the safety-case lifecycle,” Springer, 2004.

[48] Y. Luo, Z. Li, M. van , d. Brand, “A categorization of GSN-based safety cases and patterns,” 2016.

[49] E. Denney, G. Pai , I. Habli, “Perspectives on software safety case development for unmanned aircraft,” 2012.

[50] E. Denney , G. Pai, “A lightweight methodology for safety case assembly,” Springer, 2012.

[51] G. Jolliffe , M. Nicholson, “Exploring the possibilities towards a preliminary safety case for IMA blueprints,” Springer, 2005.

[52] A. Rudolph, S. Voget , J. Mottok, “A consistent safety case argumentation for artificial intelligence in safety related automotive systems,” 2018.

[53] A. Eardley, O. Shelest , S. Fararooy, “Electronic Data Interchange System for Safety Case Management,” 2006.

[54] S. Guarro, M. Yau, U. Ozguner , T. Aldemir, “Risk Informed Safety Case Framework for Unmanned Aircraft System Flight Software Certification,” 2017.

[55] M. Mumtaz, S. Anwar , N. Mumtaz, “ENGINEERING SAFETY CASE ARGUMENTS USING GSN STANDARDS,” 2019.

[56] Q. D. Hoang, J. Guiochet, D. Powell , M. Kaâniche, “Human-robot interactions: Model-based risk analysis and safety case construction,” 2012.

[57] E. Heikkilä, R. Tuominen, R. Tiusanen , J. Montew, “Safety Qualification Process for an Autonomous Ship Prototype – a Goal-based Safety Case Approach,” 2017.

[58] R. Weaver, J. Fenn , T. Kelly, “A pragmatic approach to reasoning about the assurance of safety arguments,” 2003.

[59] I. Habli, I. Ibarra, R. Rivett , T. Kelly, “Model-based assurance for justifying automotive functional safety,” 2010.

[60] I. Habli , T. Kelly, “Process and product certification arguments: getting the balance right,” 2006.

[61] A. . D. Oliveira, R. Braga, P. Masiero , Y. Papadopou, “Supporting the automated generation of modular product line safety cases”.

[62] T. Kelly, “Using software architecture techniques to support the modular certification of safety-critical systems,” 2007.

[63] C. Liu, X. Sha, F. Yan , T. Tang, “A scenario-based safety argumentation for CBTC safety case architecture,” 2010.

[64] I. Šljivo, B. Gallina, J. Carlson , H. Hansson, “A method to generate reusable safety case argument-fragments from compositional safety analysis,” 2017.

[65] E. Denney, G. Pai , I. Whiteside, “Formal foundations for hierarchical safety cases,” 2015.

[66] R. Clothier, E. Denney , G. Pai, “Making a risk informed safety case for small unmanned aircraft system operations,” 2017.

[67] I. Habli, S. White, M. Sujan, S. Harrison , M. Ugarte, “What is the safety case for health IT? A study of assurance practices in England,” 2018.

[68] E. Denney, G. Pai , I. Whiteside, “Hierarchical safety cases,” Springer, 2013.

[69] D. Nešić, M. Nyberg , B. Gallina, “Constructing product-line safety cases from contract-based specifications,” 2019.

[70] B. Gallina, “A model-driven safety certification method for process compliance,” 2014.

[71] Y. Jia, T. Lawton, S. White , I. Habli, “Developing a Safety Case for Electronic Prescribing,” 2019.

[72] T. Kelly, I. Bate, J. McDermid , A. Burns, “Building a preliminary safety case: An example from aerospace,” 1998.

[73] X. Larrucea, S. Mergen , A. Walker, “A GSN approach to SEooC for an automotive hall sensor,” Springer, 2016.

[74] R. Wang, J. Guiochet, G. Motet , W. Schön , “D-S theory for argument confidence assessment,” Springer, 2016.

[75] P. Koopman , B. Osyk, “Safety argument considerations for public road testing of autonomous vehicles,” 2019.

[76] O. Jaradat, I. Bate , S. Punnekkat, “Facilitating the maintenance of safety cases,” 2016.

[77] S. Wagner , B. Schätz, S. Puchner , P. Kock, “A case study on safety cases in the automotive domain: Modules, patterns, and models,” 2010.

[78] Y. Matsuno, “Design and implementation of GSN patterns: A step toward assurance case language,” 2014.

[79] A. Bayzat, “GSN Models of Safety Assurance for the Automotive Industry,” 2019.

[80] D. Tola, P. Larsen, J. Fitzgerald , T. Oda, “A Co-Simulation Based Approach for Developing Safety-Critical Systems,” 2021.

[81] M. Javed, F. Muram, H. Hansson, S. Punnekkat , H. Than, “Towards dynamic safety assurance for Industry 4.0,” 2021.

[82] K. Attwood, T. Kelly , J. McDermid, “The Use of Satisfaction Arguments for Traceability in Requirements Reuse for System Families: Position Paper,” 2004.

[83] R. Hawkins, C. Paterson, C. Picardi, Y. Jia , R. Calines, “Guidance on the assurance of machine learning in autonomous systems (AMLAS),” 2021.

[84] A. Mjeda , G. Botterweck , “Uncertainty Entangled; Modelling Safety Assurance Cases for Autonomous Systems,” 2021.

[85] Y. Jia, T. Lawton, J. McDermid, E. Rojas , I. Habl, “A Framework for Assurance of Medication Safety using Machine Learning,” 2021.

[86] H. Bourbouh, M. Farrell, A. Mavridou, I. Sljivo, G. Brat, L. A. Dennis , M. Fisher, “Integrating Formal Verification and Assurance: An Inspection Rover Case Study,” Springer.

[87] M. Graydon , J. Cronin, “Retrospectively documenting satisfaction of the Overarching Properties: An exploratory prototype,” 2021.

[88] S. Foster, Y. Nemouchi, M. Gleirscher, R. Wei , T. Kelly, “Integration of formal proof into unified assurance cases with Isabelle/SACM,” Springer, 2021.

[89] R. Calinescu, D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli , T. Kelly, “Engineering Trustworthy Self-Adaptive So ware with Dynamic Assurance Cases,” 2018.

[90] X. Zhao, A. Banks, J. Sharp, V. Robu, D. Flynn, M. Fisher , X. Huang, “A safety framework for critical systems utilising deep neural networks,” Springer, 2020.

[91] S. Ramakrishna, C. Hartsell, A. Dubey, P. Pal , G. Karsa, “A Methodology for Automating Assurance Case Generation,” 2020.

[92] I. Habli, R. Alexander, R. Hawkins, M. Sujan , J. McDerm, “Enhancing Covid-19 Decision-Making by Creating an Assurance Case for Simulation Models,” 2020.

[93] Y. Yamagata , Y. Matsuno, “Algebraic Approach for Confidence Evaluation of Assurance Cases,” Springer, 2020.

[94] F. Ward , I. Habli, “An Assurance Case Pattern for the Interpretability of Machine Learning in Safety-Critical Systems,” Springer, 2020.

[95] J. Birch, D. Blackburn, J. Botham, I. Habli , D. Higham, “A Structured Argument for Assuring Safety of the Intended Functionality (SOTIF),” Springer, 2020.

[96] R. Kaur, R. Ivanov, M. Cleaveland, O. Sokolsky , I. Lee, “Assurance Case Patterns for Cyber-Physical Systems with Deep Neural Networks,” Springer, 2020.

[97] R. Salay, S. Kokaly, A. D. Sandro, N. Fung , M. Chechik, “Heterogeneous megamodel management using collection operators,” Springer, 2020.

[98] O. Jaradat, I. Sljivo, R. Hawkins , I. Habli, “Modular Safety Cases for the Assurance of Industry 4.0,” 2020.

[99] J. Reich, D. Schneider , I. Sorokos, “Engineering of Runtime Safety Monitors for Cyber-Physical Systems with Digital Dependability Identities,” Springer, 2020.

[100] G. Whitman, P. Amoroso , G. Black, “IV&V Assurance Case Design for Artemis II,” 2020.

[101] B. Smith, M. Feather , T. Huntsberger, “Software Assurance of Autonomous Spacecraft Control,” 2020.

[102] N. KOBAYASHI , S. SHIRASAKA, “Proposal on how to use assurance cases for learning the mindset to respect diversity,” 2020.

著者発表論文

【論文】

104. Tsutomu Koshiyama and Sei Takahashi: Six-Assurance Case Patterns by Strengthening/Weakening Argument, International Journal of Systems and Software Security and Protection (IJSSSP) 12(1), 2021（査読付き）

【国際ワークショップ】

105. Yuto Onuma, Toshinori Takai, Tsutomu Koshiyama, Yutaka Matsuno : D-Case Steps: New Steps for Writing Assurance Cases, SAFECOMP 2018 Workshops（査読付き）

【研究会】

106. 越山 勉：GSN における Goal 設定最適化についての考察、第 12 回 D-Case 研究会＆第 2 回 D-Case ワークショップ 2017 年 3 月

107. 越山　勉、高井利憲、松野 裕、高橋 聖：アシュアランスケースの主張の変換を含めた議論パターンの提案、信学技報, vol. 118, no. 267, R2018-36, pp. 13-18

108. 越山 勉： GSN ゴール間における 6 パターン分類の試み、D-Case 研究会 名古屋 2019 年 10 月

【著書】

109. 松野裕、越山勉、他：はじめての D-Case, 一般社団法人 ディペンダビリティ技術推進協会 D-Case 部会, 2018

付録

調査した GSN サンプル

パターンマッチングの調査を行った、全 GSN モデルについて、木構造を表形式にまとめたものを次ページ以降で示す。なお、今回の 6 パターン対象とする主張を含むことができるゴール、又はストラテジ（それぞれ、G、ST と表記）のみを抽出したものとして挙げている。（コンテキスト、エビデンス、等のノードは省略されている。）

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	1	自動運転は便利だ	G	乗る人全ての視点毎のメリットについて考える	ST	(a)部分選択	Property	運転者のメリットがある	G	(f)MECE	Property									[24]	図4-9
								同乗者のメリットがある	G												
1	2	ハザード<x> に対する故障率要求が達成されている	G	ハザードについての製品と（ハザードの）プロセスの見地において議論する	ST			ハザード<x>の危険に至る故障率が 1e-5/時間	G	(e)合わせ技	Property									[6]	Figure 50
								ハザード解析が、社の基準により管理されている	G												
1	3	S18 WBSの危険にBSCUソフトウェアの貢献が受容できる	G	WBSの危険に対するソフトウェアのそれぞれの貢献について議論する	ST			必要なときにブレーキを掛けるソフトウェアの故障は、許容されるように管理されている	G	(f)MECE	Subject									[20]	Fig. 6
								必要でないときに制動を指令するソフトウェアは、許容されるように管理されている	G												
								誤った制動を指令するソフトウェアによる制動力は許容されるように管理されている	G												
1	4	必要なときにブレーキを掛けるソフトウェアの故障は、許容されるように管理されている	G	BSCUアーキテクチャにために定義されたSSRについて議論する	ST	(d)視点変換	Property	SSRはコマンドチャンネルソフトウェアの実現によって対処される	G	(f)MECE	Property									[20]	Fig. 8
								SSRはモニタチャンネルソフトウェアの実現によって対処される	G												
1	5	ブレーキモジュールのソースコードは、可能性のあるハザードに至るエラーを含まない	G	静的コード解析（情報のフロー）はランタイムエラーがないことを証明している	G	(e)合わせ技	Property													[20]	Fig. 14
				ブレーキモジュールコードはエラーを確認するためにレビューされている	G																
1	6	SSRは、コマンドチャンネルソフトウェアの実現によって対処されている	G	SSR 01は、アーキテクチャ設計の実現を通じて対処されている	G	(f)MECE	Subject	SSR 01はアーキテクチャに与えられる証拠により明らかに満足されている	G	(e)合わせ技	Property	システムインテグレーションテストにSSR 01が合致する	G	(c)基準化	Property					[20]	Fig. 9
								SSR 01は下位層設計のコマンドチャンネルの実現を通じて対処されている	G												
				SSR 02は、コマンドチャンネル設計の実現を通じて実現されている	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	7	SSRはコマンドチャンネル下位層設計により対処されている	G	下位層での設計コマンドチャンネル設計にとって定義されたSSRについて議論する	ST	(d)視点変換	Property	SSRはコマンドチャンネルブレーキモジュールの実現により対処されている	G	(f)MECE	Property									[20]	Fig. 10
								SSRはコマンドチャンネルABSモジュールの実現により対処されている	G												
								SSRはコマンドチャンネル変更モジュールの実現により対処されている	G												
								SSRはコマンドチャンネル入力モジュールの実現により対処されている	G												
								SSRはコマンドチャンネル出力モジュールの実現により対処されている	G												
1	8	BSCUソフトウェアがWBSハザードに寄与する可能性のある方法が完全かつ正確に特定されている	G	WBSシステムレベルFTAの基本イベントは、WBSハザードに対するすべての潜在的なソフトウェアの寄与とそれらの相対的な重要度を識別します。	G	(d)視点変換	Property													[20]	Fig. 7
1	9	コマンドチャネル設計における潜在的な危険な障害は、許容範囲内で管理されます。	G	コマンドチャネルの設計に危険なエラーは含まれていません	G	(e)合わせ技	Property	コマンドチャネル設計の手動レビューは、危険なエラーが設計に存在しないことを示しています	G	(d)視点変換	Property									[20]	Fig. 11
				コマンドチャネル設計のSSRは、特定された潜在的に危険な動作に対処します。	G			ソフトウェアの潜在的に危険な障害モードは、コマンドチャネル設計から正しく識別されます	G	(e)合わせ技	Property										
								ソフトウェアの特定された危険な障害モードに対処するのに十分なSSRが、コマンドチャネル設計用に定義されています	G												
1	10	コマンドチャネルブレーキモジュールの実現を通じて対処されたSSR。	G	コマンドチャネルブレーキモジュール設計の実現を通じて対処されたSSR1.1	G	(f)MECE	Subject	SSR1.1は、低レベルの設計で提供された証拠を通じて明らかに満足しています。	G	(e)合わせ技	Property	ユニットテストは、SSR1.1が満たされていることを示しています	G	(c)基準化	Property					[20]	Fig. 12
								SSR1.1は、ブレーキモジュールのソースコードの実現を通じて対処されます。	G												
				コマンドチャネルブレーキモジュール設計の実現を通じて対処されたSSR1.2	G																
				コマンドチャネルブレーキモジュール設計の実現を通じて対処されたSSR1.3	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	11	コマンドチャネルブレーキモジュール設計の実現を通じて対処されたSSR1.1	G	ブレーキモジュールのソースコードのSSRに関する議論	ST	(d)視点変換	Property	SSR1.1は、ソースコードに提供された証拠を通じて明らかに満足しています	G	(e)合わせ技	Property	セマンティックコード分析は、SSR1.1が満たされていることを示しています	G	(c)基準化	Property					[20]	Fig. 13
								SSR1.1は、ブレーキモジュールのコンパイル済みオブジェクトコードで対処されています	G			ブレーキモジュールのオブジェクトコードは、ソースコードと同等です	G	(d)視点変換	Property	使用されるコンパイラの整合性に関する議論	ST	(d)視点変換	Property		
1	12	違反（ギャップ＞安全距離）にならないようにする	G	解決（違反）	ST			状況の回避（ギャップ＜安全な距離）	G	(b)二重否定	Property									[22]	Figure 23
1	13	壊滅的な故障のリスクは十分に低い	G	壊滅的な故障のリスクha10↑-6/1飛行である	G	(c)基準化	Property													[21]	Figure 14
1	14	部品の信頼性は＞10↑-6故障/時間である	G	歴史的データの考慮により議論する	ST	(d)視点変換	Property													[21]	Figure 15
1	15	コントロールシステムは操作にとって十分に安全である	G	全てのハザードは、除去されているか十分に軽減されている	G	(e)合わせ技	Property	定義されている各々のハザードについて議論する	ST			ハザードH1は低減されている	G	(f)MECE	Subject					[25]	Figure 4.4
												ハザードH2の起こる可能性は、<1×10↑-6/年	G								
												ハザードH3の起こる可能性は、<1×10↑-3/年	G								
				コントロールシステムのソフトウェアはハザードに適したSIL用に開発されている	G			第一構成要素、第二構成要素について議論する	ST			SIL4用に開発された主としての保護システム	G	(f)MECE	Subject						
												SIL2用に開発された副としての保護システム	G								
1	16	プレス機は、CCC Whatford工場内で動作することが許容されるだけ安全である。	G	全ての定義された操作上のハザードに対処していることに従って議論する	ST	(e)合わせ技	Property													[6]	Figure 41
				全ての適用可能な安全基準と法規に準拠していることについて議論する	ST																
1	17	モジュールの故障率は、1×10↑-6/年より少ない	G	モジュールZのテスト結果によって論じる	ST	(d)視点変換	Property													[18]	Figure 21
1	18	コードモジュール Yは定型の仕様技術(Z)を用いて具体化されている	G	主張による議論は、特定のI.L4ガイドラインに従っている	ST	(c)基準化	Property	形式仕様手法（Z）を使用して指定されたコードモジュールY	G	(f)MECE	Property									[18]	Figure 19
								正式な仕様に対して検証されたコードモジュールYの機能プロパティ	G												
								タイミング解析を使用して検証されたコードモジュールYのタイミングプロパティ	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	19	Control Systemの故障がない	G	全てのControl Systemの安全要求について議論する	ST	(e)合わせ技	Property	G17 プレスコントロールが「詰まっている」と、プレスが停止する	G	(f)MECE	property	G17→G18 G18 PLCステートマシンの「失敗」遷移には、BUTTON_INがTRUEのままであることが含まれます	G	(e)合わせ技	Property					[18]	Figure 24
												G17→G41/G20→G41 G41 C / Sステートマシンは、実装動作の正確な表現である	G								
								G20 プレスが物理的なPoNRを通過する前にコントロールを解放すると、プレス操作が中止される	G			G17→G41/G20→G41 G41 C / Sステートマシンは、実装動作の正確な表現である	G	(e)合わせ技	Property						
												G20→G21 G21 PLCステートマシンの「中止」遷移には、BUTTON_INがFALSEになることが含まれる	G								
								G18 C / Sは、すべての単一コンポーネントの障害をフェイルセーフ（停止）し、（クラクションを鳴らして）通知する	G												
				全ての定義されたソフトウェアにおけるハザードの除去毎に議論する	ST			（PoNR後の）意図しないプレスの開放は、コンポーネントの故障の結果としてのみ発生する可能性がある	G	(f)MECE	property										
								プレスの意図しない閉鎖は、コンポーネントの故障の結果としてのみ発生する可能性があります	G												
1	20,21	プレスは、CCCワットフォードプラント内で操作するのに許容できるほど安全です	G	すべての特定された操作上の危険に対処することによる議論	ST	(e)合わせ技	Property	「プレスのピストンに操作者の手を挟まれる」についてのハザードが十分に低減されている	G	(f)MECE	Subject									[18]	Figure 32 Figure 33
								「プレスの駆動に操作者の手が挟まれる」についてのハザードが十分に低減されている	G												
								「プレスのピストンに上半身を挟まれる」についてのハザードが十分に低減されている	G												
				適用されるすべての安全基準および規制への準拠による議論	ST			英国のHSE規定および作業装置規則の使用に準拠したプレス機	G	(f)MECE	Subject										
								EU機械指令の英国制定に準拠したプレス機	G												
								EC1508に準拠したプレス設計のPES要素	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	22	操作者の手がプレスの可動部分に挟まれることについてのハザード は十分に低減されている	G	モータ/クラッチ/ドライブベルトが安全柵で囲まれている	G	(d)視点変換	Property	もし、安全柵が不当に改造されたプレス機の運転は（安全に）停止される	G	(d)視点変換	Property									[18]	Figure 34
1	23	システムは許容できるだけ安全である	G	全てのハザードが除かれている	ST			ハザードH1が除かれている	G	(b)二重否定	property									[18]	Figure 37
1	24	システムは許容できるだけ安全である	G	全ての同定されているハザードが、低減/除去されていることについて議論する	ST	(b)二重否定	Property													[18]	Figure 39
1	25	ハザードH1が起こる可能性は許容できるほど低い	G	設計上の機械的インターロックの効果で訴える	ST			機械的インターロックの適用は許容されるほど信頼できる	G	(d)視点変換	property									[18]	Figure 36
1	26	システムはいかなる単一故障にも耐性がある	G	システムに実装されているトリックモジュラーの冗長性について議論する	ST	(d)視点変換	Property	単一フォールトは制限時間内で検出される	G	(e)合わせ技	Property									[18]	Figure 38
								単一フォールトは利用可能な冗長性を通じて耐性がある	G												
1	27	システムは「SAFE手法」によって開発されている	G	ハザードの定義と評価を通じて達成される	G	(d)視点変換	Property	事前のハザードの定義は遂行されている（過去の経験とチェックリストに基いて）	G	(e)合わせ技	Property									[18]	Figure 40
								事前のハザードの定義の結果は、全てのシステム機能についての完全な機能ハザード分析の遂行を通じて、洗練され、議論されている。	G												
1	28	アーキテクチャはエンジン制御にとって許容される安全なプラットフォームを提供する	G	プラットフォームの耐えられない、故障のリスクは、十分に低い（量）	G	(e)合わせ技	Property													[18]	Figure 43
				全てのプラットフォーム安全性は、実装時に保持される（品質）	G																
1	29	耐えられないプラットフォームの故障のリスクは、十分に低い（量）	G	ランダム故障率は耐えられないプラットフォーム故障への貢献は十分に低い	G	(f)MECE	Property	コンポーネントFEMAテーブルによって満たされることが示されたコンポーネント信頼性目標	G	(d)視点変換	Property									[18]	Figure 44
				システマティック故障の耐えられないプラットフォーム故障への貢献は十分に低い	G			特定された障害の重大度に応じて適切なツール、技法、および方法が使用されている	G	(d)視点変換	Property	開発保証レベルAに準拠したシステムプロセスガイドライン	G	(c)基準化	Property						
1	30	全てのプラットフォーム安全性は実装時に保持される	G	全ての非機能プラットフォームの安全性は実装時に保持される	G	(f)MECE	Property	提示されたタイミングの提示は正しい	G	(e)合わせ技	Property									[18]	Figure 45
								リソース利用は常にアプリケーションにとって十分である	G			増大するリソース要求をサポートするために、計測可能なアーキテクチャが定義されている	G	(e)合わせ技	Property						
												リソース利用の最悪ケースは、定義された限界内である	G								
				全ての機能プラットフォームは実装時に保持される	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	31	提示するタイミングの振る舞いは正しい	G	タイミングの要求は正しい	G	(f)MECE	Property	エンジンの振る舞いが、タイミング要求が正しいことを示すことについて議論する	ST	(e)合わせ技	Property	エンジンテスト中に正しいエンジンの振る舞いが見られる	G	(f)MECE	Property					[18]	Figure 46
												エンジンシミュレーションにおいて正しいエンジンの振る舞いが見られる	G								
								タイミング要件は、同様のエンジンで10e +7時間以上安全に動作するために使用されてきた共通の要件セットから導き出されます。	G												
				タイミングの要求がみたされる	G			スケジューリングポリシーが決定的である場合、タイミング要件を保証できる	ST			スケジューリングの方針は決定論的である	G	(e)合わせ技	property						
												タイミング要求は、静的なタイミングの解析を保証する	G								
1	32	全ての機能プラットフォーム安全性は実装時に保持される	G	プラットフォーム故障の挙動について考慮すべきこと毎について議論する	ST			信ぴょう性のある障害の存在下で決定的なプラットフォームの挙動	G	(d)視点変換	Property	故障は検出される（有界時間内に）	G	(f)MECE	Property	投票メカニズムを通じて検出されたプロセッサ間の値の不一致	G	(f)MECE	Property	[18]	Figure 47
																ウォッチドッグタイマーによって検出されるタイミング不一致	G				
												故障が回復する（有界時間内に）又は、安全に許容される	G			プラットフォームはシャットダウンと再起動を通じて検出されプロセッサのフォールトから復帰を試みる	G	(f)MECE	Property		
																プロセッサ再起動がフォールトを取り除けない状況において、故障源は、可能な構成から除去される	G				
1	33	システムは、容認できるほど安全である	G	特定された全てのハザード毎に議論する	ST	(b)二重否定	Property	ハザードH1は対応されている	G	(f)MECE	Subject									[18]	Figure 70
								ハザードH2は対応されている	G												
								ハザードH3は対応されている	G												
								ハザードH4は対応されている	G												
1	34	最悪値周期時間は、2.7に決定された	G	経路の最悪ケースを決定するために使われる静的解析	G	(e)合わせ技	Property													[18]	Figure 71
				入出力 潜在故障が決定されている	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	35	トリップシステムは、いかなるガスダクトの温度が上昇し過ぎた場合に正しく動作する	G	デザインの単一性は、トリップ機能のテストと検証を補助する	G	(e)合わせ技	Property													[18]	Figure 73
				ソフトウェアは規定されたトリップ機能を遂行することを公式に証明されてきている	G																
				プログラムとトリップパラメータが別々のPROMで維持されるため、トリップ機能に障害が発生するリスクが最小限に抑えられる	G																
				成熟したハードウェアとソフトウェアツールが、トリップ機能におけるシステマティックフォールトのリスクを最小限にするために使われてきている	G																
1	36	ハザードH1が起こる可能性が十分に低い	G	ハザードに至る単一故障はない	G	(e)合わせ技	Property													[18]	Figure 74
				ハザードの故障ツリーは、確率が1.4×↑10-6であることを示している	G																
1	37	ハザードH1が起こる可能性＜10↑-6/年	G	H1にとってのフォールトツリーは、発生確率が10↑-7/年であることを示している	G	(c)基準化	Property													[18]	Figure 76
1	38	ハザードH1は起こらない	G	多様な形式の証拠において議論する	ST	(d)視点変換	Property	H1に関連するコンディションがないことを定型化された形式の解析で示す	G	(e)合わせ技	Property									[18]	Figure 77
								拡張されたリグにH1が起こらないことを示す	G												
1	39	システムXは安全である	G	システムに実装されている全ての安全関係の機能についての安全を主張することで議論する	ST	(d)視点変換	Property	機能Yが安全である（×n個）	G	(e)合わせ技	Property									[18]	Figure 88
								システム機能間の関係にハザードがない	G												
								全ての機能は独立している（相関がない）	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	40	IMAシステムは安全である	G	十分なパーティショニングと分離がモジュール間で提供されている	G	(e)合わせ技	Property													[18]	Figure 98
				時間管理手段は、少なくとも、サイクル実行と同様に安全である	G																
				IMAは、さまざまな整合性のモジュールを安全にサポートする	G																
				モジュールの再構成は安全である	G																
				モジュールの交換は、正しく行われる	G																
				モジュール間の共通原因故障は十分に起こり得ない	G																
				各々のモジュールは独立して安全である	G																
				モジュールは安全に接続されている	G																
1	41	XXXX 及び XXXXに先立つXXXXXの廃炉は安全である	G	全体的なSAPの目標への準拠による議論	ST	(c)基準化	Property	最終的なプラントの状態が標準の核安全目標に準拠する	G	(f)MECE	Property									[18]	Figure 99
								最終的なプラントの状態が放射線防御目標に準拠する	G												
								最終的なプラントの状態が技術安全目標に準拠する	G			プラントの変更と最終状態は、適用するSAPsの資料からの原則を順守する	G	(e)合わせ技	Property						
												停泊の変更と管理は安全正当評価リスクXXXXを持つ、核安全分類 XXシステムである	G								
												最終的なプラントの状態は、定義された全てのプラントの能力について確実にする	G								
												最終的なプラントの状態は、起こり得るとみなされる全ての内部的、外部的な環境ハザードについて耐性がある	G								
												原子炉の安全要件が満たされていることを確認し（最終的なプラント状態が維持されている）、早期に提供するために提供される原子炉プラントの監視	G								
												最終的なプラントの状態は、最終デフエルの間、妥協しない	G								

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	42	XXXが安全であることを保証するために実装された準拠安全管理プロセス	G	安全に関するprEN50126に定義されているプロジェクトフェーズ1から6にとっての安全に関するタスク XXXについて議論する	ST	(d)視点変換	Property	フェーズ1 の安全タスクが十分に完了した	G	(f)MECE	Subject									[18]	Figure 100
								フェーズ2 の安全タスクが十分に完了した	G												
								フェーズ3 の安全タスクが十分に完了した	G												
								フェーズ4 の安全タスクが十分に完了した	G												
								フェーズ5 の安全タスクが十分に完了した	G												
								フェーズ6 の安全タスクが十分に完了した	G												
								安全監査は問題なく完了している（分解未定）	G												
								独立した安全評価が問題なく完了している	G												
1	43	G0 xxxの操作が安全である	G	G1 YYY機能は、XXXXの安全操作を支持する	G	(e)合わせ技	Property	G9 プラントのリセットに対する特定されたすべてのYYYハザードは十分に軽減されています	G	(e)合わせ技	Property									[18]	Figure 101
								G5 YYYは、すべての機能要件と整合性要件を満たしています	G			G11 YYYは、ZZZ ZZZ、ZZ、およびZZZを適切にサポートします	G	(e)合わせ技	Property						
												G12 YYYは十分な構造的完全性を持っています	G								
								G6 YYYは、該当するすべての安全性評価原則を満たしています	G												
				G2 YYY機能は安全である	G			G4 特定されたすべてのYYYハザードは十分に軽減されています	G	(e)合わせ技	Property	G9 プラントのリセットに対する特定されたすべてのYYYハザードは十分に軽減されています	G	(f)MECE	Subject						
												G10 提供されたすべての内部YYYハザードは十分に軽減されています	G								
								G6 YYYは、該当するすべての安全性評価原則を満たしています	G												
				G3 YYYの操作を支持するシステムは安全である	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	44	基本の条件と操作はMod SPSCsに従う	G	Mod SPSCsを原則と基準に分割する	ST			基本の条件と操作は原則に従う	G	(f)MECE	Property	原則は全ての状態と操作のレベルにおいて処理される	G	(e)合わせ技	Property					[18]	Figure 102
												全ての核設備と関連する操作は、原則を満たす	G								
								基本の条件と操作は基準に従う	G												
1	45	論文アプローチの使用はセーフティケース開発に利益をもたらします	G	論文アプローチの採用により、セーフティケース開発プロセスが改善されます。	G	(a)部分選択	Property													[18]	Figure 107
				論文のアプローチを使用すると、生成されるセーフティケースの品質が向上します	G																
1	46	論文アプローチの採用は、セーフティケースプロセスを改良する	G	アプローチの3要素について議論する	G	(d)視点変換	Property	論文アプローチの採用は初期の開発プロセスを改良する	G	(f)MECE	Subject									[18]	Figure 108
								論文アプローチの採用は、管理プロセスを改良する	G												
								論文アプローチの採用は、プロセスの再利王を改良する	G												
1	47	論文アプローチの採用は、初期の開発プロセスを改良する	G	論文アプローチの採用は、安全議論の早期定義される結果を得る	G	(a)部分選択	Property													[18]	Figure 109
				論文アプローチの採用は、認定問題について遅れて発見されることに起因する設計の再作業における努力が費やされることを減らす	G																
				論文アプローチの採用は、議論のアプローチの合意に至ることについての過度の反復の努力が費やされることを削減する	G																
1	48	メンテナンスプロセス 論文アプローチの採用は、メンテナンスプロセスを改善します	G	迅速なメンテナンス 論文アプローチを採用することで、安全ケースの整備作業にかかる時間を短縮できます。	G	(e)合わせ技	Property	再発見を減らす 論文アプローチの採用により、過去の安全事例における安全論を「再発見」するために必要な時間が短縮されます。	G	(f)MECE	Property									[18]	Figure 110
								影響の特定を減らす 論文アプローチの採用により、安全ケースの変更による影響を特定するために必要な時間が短縮されます。	G										
				体系的なメンテナンス 論文アプローチの採用により、安全事例影響評価の有効性が向上します。	G																

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	49	プロセスの再利用を改善する	G	安全議論の定義づけを早めることができる	G	(e)合わせ技	Property	セーフティケースの臨時の性質を減らす	G	(f)MECE	Property									[18]	Figure 111
								不可欠なセーフティケース開発を損なうリスクを減らす	G												
				非公式のセーフティケースの再利用のプロセス問題の潜在性を減らす	G																
1	50	セーフティケース生成物の品質を改善する	G	アプローチの3つの要素について議論する	ST	(d)視点変換	Property	初期のサーフティケースの質を改善する	G	(f)MECE	Subject									[18]	Figure 112
								持続されるセーフティケースの質を改善する	G												
								将来のセーフティケースの質を改善する	G												
1	51	論文アプローチを採用することで、初期の安全ケースの質が向上する質を改善する	G	論文アプローチの採用は、より明確に伝達された安全性の議論をもたらします。	G	(d)視点変換	Property													[18]	Figure 113
1	52	論文アプローチの採用は、維持された安全ケースの品質を向上させます	G	論文アプローチの採用により、安全ケースは変更に照らしてより正確かつ完全に更新されます	G	(d)視点変換	Property													[18]	Figure 114
1	53	論文アプローチの採用は、将来の安全ケースの質を向上させます	G	論文アプローチの採用は、非公式の安全ケースの再利用の（製品）問題の可能性を減らします	G	(d)視点変換	Property	適当でないセーフティケースの再利用を減らす	G	(a)部分選択	Property									[18]	Figure 115
								セーフティケース間の矛盾を減らす	G												
								セーフティケース論証の再利用のトレーサビリティを改善する	G												
1	54	トリップシステムが操作上、受容されるだけ安全である	G	機能要求について議論する	ST	(e)合わせ技	Property													[18]	Figure 116
				性能要求について議論する	ST																
				使用及びメンテナンス要求について議論する	ST																
				生涯にわたる完全性について議論する	ST																
				安全基準について議論する	ST																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	55	需要における故障の可能性は0.001/年未満 である	G	4チャンネルと二重の熱電対は要求上の故障のリスクを削減する	G	(e)合わせ技	Property													[18]	Figure 125
				継続的なオンラインチェックにより、明らかにされていない障害によるオンデマンドの障害のリスクが軽減されます	G																
				特定されたトリップ機能を遂行すべく、ソフトウェアは形式的に証明される	G																
				需要上のトリップ機能の故障のリスクを最小限にするために、どちらの熱電対かが高温側の読み取りは、リアクターをトリップさせる	G															
				プログラムとトリップのパラメータは別々のPROMで維持され、オンデマンドでのトリップの失敗につながる障害が発生するリスクを最小限に抑えます	G															
				ハードウェア、ソフトウェアのツールは需要上の故障につながるシステマティック障害のリスクを最小限にする	G																
				需要毎のランダム故障に起因する故障は0.001/年より小さい	G																
				需要毎の故障は、たとえ、システマティックフォールトがあっても0.001/年より小さい	G																
				フェースセーフ設計はシステマティックフォールトに起因する故障について少なくとも90%がフェールセーフされることを確実にする	G															
1	56	ランダム故障に起因する需要上の故障は、0.001/年より少ない	G	システマティック障害はあり得ないと思われる	G	(e)合わせ技	Property													[18]	Figure 126
				ハードウェア信頼信頼性解析は、FT推定を支持する	G																
				FTAは、PFDが、0.13×10↑-3/年になるようことを見積もってる	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	57	システマティックフォールトは起こり得ないと思われている	G	ハードウェアはシステマティック障害がない	G	(f)MECE	Property	「ハードウェアはシステマティック障害がない」ことを確立した設計は意味している	G	(e)合わせ技	Property									[18]	Figure 127
								テストは、システマティックハードウェアの欠陥を明らかにしていない	G												
				ソフトウェアにはシステマティック障害がない	G			システムは、コンパイラに起因する障害を明らかにするためのテストをクリアしている	G	(e)合わせ技	Property										
								コードは正式に証明されている	G												
1	58	仮に、システマティックフォールトがあるとしても、要求毎の故障は、0.001/年である	G	故障がない典型的なトリップを使った10↑-4信頼性テストは、10↑-3のPFDにおける99%以上の確信を与える	G	(c)基準化	Property													[18]	Figure 128
1	59	フェールセーフ設計は、「システマティックフォールトによる故障の少なくとも90%は、フェールセーフである」といったことを確実にする	G	二重の熱電対の断線又は、使用禁止はトリップを起こす	G	(e)合わせ技	Property													[18]	Figure 129
				コンパイラ、ローダ、及びプロセッサの欠点は、リバースコンピューティング技術に対して守られている。	G																
				ADCにおける欠点、ソフトウェアの適用、構成、トリップ限界とトリップロジックは、動的オンラインテストによって明らかにされる	G																
1	60	最大応答時間は、5sc未満である	G	過度の、又は無限ループは、リバーシブルコンピューティングの実装によって検出される	G	(e)合わせ技	Property													[18]	Figure 130
				設計の単純化は、最悪応答時間が設定され、タイミングテストやコード解析から用意された、かつ確固としたものとなる	G																
				最大応答時間は、2.7とされている	G																
				測定された応答時間は最大で、2.7である。	G																
1	61	最大応答時間は、2.7とされている	G	コードの経路の最悪ケースを確定するために、静的解析が使われる	G	(e)合わせ技	Property													[18]	Figure 131
				入力/出力の待ち時間は、分かっている	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	62	MTTR時間（情報の識別を含む）は、≦10時間である	G	もし、システマティック又はランダムフォールトに遭遇した場合、障害検出は、"フェーリングセーフ"によって、処置される	G	(e)合わせ技	Property													[18]	Figure 133
				"分離監視コンピュータ"は、チャンネル故障のオンラインと熱電対の故障の診断を可能とする	G																
				2oo2 低レベルロジックセンサによる比較は、センサの故障を検出において補助する	G																
				ハードウェア部品の交換は、修復時間を短縮する	G																
1	63	疑似トリップレートは、＜0.1/年である	G	冗長チャンネルにおける2oo4採択は、トリップレートを減らす	G	(e)合わせ技	Property													[18]	Figure 134
				必要な時だけ、トリップされることをソフトウェアは形式的に証明されてきている	G																
				2oo2 lowトリップロジックは、一つのセンサの一時的な消失（例、修理）又は、拒否権を使用しない、low読み込みを行うセンサーの消失に耐えうる	G																
				プログラムとトリップパラメータは、見せかけのトリップを引き起こす分離されたFROMの最小限化されたリスクに保持される	G																
				成熟したハードウェアとソフトウェアによるツールは、疑似トリップにつながるシステマティックフォールトのリスクを最小限にするのに使われる	G																
1	64	トリップシステムは、オンラインでテストできなければならない	G	冗長のチャンネルは、トリップが引き起こすことなくてテストを続けることができる	G	(e)合わせ技	Property													[18]	Figure 135
				分離されたモニタコンピュータは、チャンネルと熱電対のオンライン故障診断を可能にする	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	65	トリップシステムは保守のの間違いと悪意ある攻撃に耐えうる	G	リバーシブルコンピューティング技術は、悪意あるプログラム改ざんを明らかにする	G	(e)合わせ技	Property													[18]	Figure 136
				分離されたモニタコンピュータは、4つのチャンネルにおけるソフトウェアの堅牢性の始動前チェックを行う	G																
				トリップパラメータとロジックは、PROM書き込み装置と物理的な装置へのアクセスなしには成し得ない	G																
				装置は、ロックされ、適切なキー（チャンネル毎に異なった）の使用によってのみアクセス可能である	G																
				予想されるすべてのメンテナンスおよび運用エラーに対してセーフガードが実施されています	G																
1	66	安全装置は予期される全ての保守と操作エラーに対して用意される	G	安全装置は、耐久試験におけるエラーに対して守るために用意される	G	(f)MECE	Property													[18]	Figure 137
				安全装置は、故障診断のエラーから守るために用意される	G																
				安全装置は、保守活動におけるエラーから守るために用意される	G																
				安全装置は、操作禁止のエラーから守るために、用意される	G																
				安全装置は、燃料投入におけるエラーから守るために用意される	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	67	トリップシステムは、引き起こされる保守フォールトの最小限のリスクで、予期される変化に応じることができるように、変更されることができる	G	チャンネルと熱電対のの冗長は、保守時の誘発故障を減らす	G	(e)合わせ技	Property													[18]	Figure 138
				設計の簡易は、システムの改変が容易にできることを意味する	G																
				シンプルな入出力インターフェースは、新しいセンサ種類に適用するために、容易にアップグレードすることができる	G																
				PROMにおいて、分離されたプログラム領域とトリップ変数は、保守における変更を独立したものにする	G																
				危険なフォールトを引き起こすデータの更新を防止するために、十分な防止が設置される	G																
				危険なフォールトを引き起こすプログラムの更新を防止するために、十分な防止が設置される	G																
1	68	全ての予期される変更は、設計とセーフティケースによって供給される	G	入力数の変更は、設計とセーフティケースによって供給される	G	(f)MECE	Subject													[18]	Figure 139
				コンピュータH/W又は、S/Wツールの変更は、設計とセーフティケースによって供給される	G																
				予期される機能要求の変更は、設計とセーフティケースによって供給される	G																
				センサの変更は、設計とセーフティケースによって供給される	G																
				予期される規制の変更は、設計とセーフティケースによって供給される	G																
1	69(1)	危険なフォールトを引き起こすデータの更新を防止するために、十分な防止が設置される	G	予期される変更を安全に供給するために、十分なインフラが設置される（例：セーフティケースレビュー）	G	(e)合わせ技	Property													[18]	Figure 140
				データとプログラムの更新をテストするために、手順は設置される	G																
				ADCにおける欠陥、アプリケーションソフト、設定、トリップ限界、トリップロジックは動的オンラインテストによって明らかにされる	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	69(2)	危険なフォールトを引き起こすプログラムの更新を防止するために、十分な防止が設置される	G	予期される変更を安全に供給するために、十分なインフラが設置される（例：セーフティケースレビュー）	G	(e)合わせ技	Property													[18]	Figure 140
				データとプとグラムの更新をテストするために、手順は設置される	G																
				ADCにおける欠陥、アプリケーションソフト、設定、トリップ限界、トリップロジックは動的オンラインテストによって明らかにされる	G																
1	70	セーフティケースの妥当性は、システムの運用を一貫して保持される	G	十分なインフラの支持は予測される変更を安全に供給できるように設置される	G	(e)合わせ技	Property													[18]	Figure 141
				操作上の記録は、保持され、セーフティケースにおいての想定や見通しを確実にするために、解析される	G																
1	71	有効なシングルフォールトはない	G	安全機能は、2つのチャンネルフォールトが故障でトリップしない場合でも維持される	G	(d)視点変換	Property													[18]	Figure 142
1	72	安全に影響する二つの独立したフォールトはない	G	安全機能は、2つのチャンネルが故障でトリップしない場合でも維持される	G	(e)合わせ技	Property													[18]	Figure 143
				システムは、ハードウェアやコンパイラーによって作り出された異常におけるシステマティック故障とランダム故障の存在においてフェールセーフする	G																
1	73	システムは操業に許容できるだけ安全である	G	すべてのハザードについて議論する	ST	(b)二重否定	Property	ハザード１は低減されている	G	(f)MECE	Subject	多様な証拠により議論する	ST	(d)視点変換	Property	証拠クレーム1	G	(f)MECE	Subject	[26]	Fig. 2
								ハザード2は低減されている	G							証拠クレーム2	G				
1	74	システムXが意図する適用にとって受容できるだけ安全である	G	EN50129で要求される安全許容条件への適合による議論	ST	(c)基準化	Property	効果的な品質管理（QMR）	G	(e)合わせ技	Property									[23]	Figure 3
								効果的な安全管理（SMR）	G												
								システムが十分に安全であることを設計についての技術的な方法で担保する（TSR）	G												
								一部のサブシステムまたはコンポーネントの認定されたセーフティケースが入手可能	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
1	75	設計についての技術的手法は、システムが十分に安全であることを担保する [技術安全レポート（TSR）]	G	安全性確証のための信頼できる技術的な証拠により議論する	ST	(d)視点変換	Property	正しい機能操作は、担保される（TSR： Section 2）	G	(f)MECE	Property	システムおよび安全要件に従った正しい操作による議論	ST	(d)視点変換	Property	システム要件仕様が満たされている	G	(f)MECE	Property	[23]	Figure 4
																安全件仕様が満たされている	G				
																正しいハードウェア機能仕様が担保されている	G				
																正しいソフトウェア機能が担保されている	G				
								故障の効果は、安全目標を満足する（TSR: Section 3）	G												
								システムは外部の影響下で正しく安全に動作する（TSR：セクション4）	G												
								システムに関連するアプリケーションのルール、条件、および制約が明確に定義されている（TSR：セクション5）	G												
								運転条件下での安全認定試験が無事に完了してる（TSR：セクション6）	G												
1	76	「アクセルが下限値以上になる」ことに違反することを回避する	G	解決（違反）	ST			「アクセルが下限値未満になる」を回避する	G	(b)二重否定	Property									[22]	Figure 6

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	1	システムXは許容できるだけ安全である。	G	同定された{システムX}の安全性に関係する機能について議論する	ST	(d)視点変換	property	機能Aの操作は許容できるだけ安全である	G	(f)MECE	property									[27]	Figure 1
								機能Bの操作は許容できるだけ安全である	G												
								機能Cの操作は許容できるだけ安全である	G												
2	2	アーキテクチャはアプリケーション間の不要な通信を防止する	G	パーティション機構の利用について理論する	ST	(d)視点変換	property	満足のいくパーティショニングが提供される	G	(c)基準化	property									[27]	Figure 7
2	3	満足のいくパーティショニングが提供されている	G	パーティショニングのタイプについて議論する	ST	(d)視点変換	property	メモリパーティショニングが十分である	G	(e)合わせ技	property									[27]	Figure 8
								一時的なパーティショニングが十分にサポートされている。	G												
								信頼できる関数呼び出しメカニズムは仕様どおりに動作する	G												
2	4	C/S ロジックは故障がない	G	すべてのC / S安全要件を満たすことによる議論	ST	(e)合わせ技	property	プレスコントロールが「詰まっている」と、プレスが停止する	G	(f)MECE	property	PLCステートマシンの「障害1」遷移には、BUTTON_INがtrueのままであることが含まれます	G	(c)基準化	property					[28]	Figure 5
								通過する物理PoNRを押すためのコントロールをリリースすると、プレス操作が中止される	G			PLCステートマシンの「中止」遷移には、BUTTON_INがFALSEになることが含まれます。	G	(c)基準化	property						
								C / Sは安全にフェイルセーフ（停止）し、（クラクションを鳴らすことによって）すべての単一コンポーネントの障害を通知する	G												
				定義されている全てのソフトウェアハザードの除去による議論	ST			（PoNRの後の）意図しないプレスの開放コンポーネント故障の結果としてのみ発生し得る可能性がある	G	(f)MECE	property										
								（PoNR後の）意図しないプレスの閉鎖は、コンポーネントの故障の結果としてのみ発生する可能性がある	G												
2	5	ブレーキシステムは通常の操作において許容できるだけ安全である	G	全てのブレーキシステムのハザードが十分に対処されている	G	(e)合わせ技	property	存在する新たなブレーキシステムに関するハザードについて理論する	ST			存在するブレーキシステムハザードが十分に対処されている	G	(f)MECE	property					[28]	Figure 8
												ブレーキシステムにより導入された新たなハザードが十分に対処されている	G								
				ブレーキシステムは関連する安全要求に合致する。	G			法的要求、基準とベストプラクティスについて議論する	ST			ブレーキシステムが法的要求を対処する	G	(e)合わせ技	property						
												ブレーキシステムが、認定され（適用可能な）安全基準に適合している	G								
				ブレーキシステムは存在するシステムに改良された安全性を提供する	G			それぞれの安全機能について議論する	ST	(d)視点変換	property	ベストプラクティスに従って開発されたブレーキシステム	G	(c)基準化	property						

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	6	車両速度が15km/hを超える間アクチュエータの始動は回避されている	G	AND リファインメントによる分解	ST	(d)視点変換	property	VS ECUは AC ECUに対して正確な車速情報を送信する	G	(f)MECE	property									[29]	Fig. 7
								車速が15km/hより大きい場合に、AC ECUはアクチュエータを起動しない	G												
								VS ECUは 冗長スイッチに正確な車速を送信する	G												
								車速が15km/hを超えた場合、冗長スイッチはオープン状態にある	G												
								AC ECUによって起動されていて、冗長スイッチがCloseの場合に限って、アクチュエータが有効化される	G												
2	7	ハザード「衝突後、エアバッグが長時間膨張しないままである」は十分に管理されている。	G	全ての関連するソフトウェアはMISRA C 2004に合致する	G	(e)合わせ技	property													[30]	Figure 2
				エアバッグの50ms以内に膨張する	G																
2	8	システムXは環境Yにおいて使用するために、許容されるだけ安全である。	G	特定された安全要件の有効性と満足度、およびプロセスの信頼性に関する議論	ST			同定された安全要求は有効である	G	(e)合わせ技	property									[31]	Figure 3
								同定された安全要求は満たされている	G												
								ライフサイクルプロセスは、信頼に値する	G												
2	9	G1: 操作上の安全は、{システム}においてベリファイされている	G	S1: {システム}についてのすべての仕様の満足について議論する	ST	(e)合わせ技	property														Figure 2
				G2: 全ての操作上のハザードが低減されている。	G			S3: 全ての操作上のハザードについて議論する	ST			G3: {操作上のハザード}が低減されている	G	(f)MECE	property	S4: 適用された {操作上のハザード}のシナリオについて議論する	ST	(d)視点変換	property		
				S2: {システム}のすべての適切なレベルでの信頼性に関する議論	ST																
2	10	G1: 操作上の安全は"GPCA"システム"において検証されている	G	S1: "GPSAシステム"についての仕様の満足について議論する	ST	(e)合わせ技	property														Figure 9
				G2: 全ての操作上のハザードが低減されている	G			S3: 全ての操作上のハザードについて議論する	ST	(d)視点変換	property	G3: "過剰注入" は低減されている	G	(f)MECE	property						
												G3: "注入不足" は低減されている	G			A4: 適用された"注入不足"のシナリオについて議論する	ST	(d)視点変換	property		
				S2: "GPSAシステムの全ての適切なレベルの信頼性について議論する	ST																
2	11	{システム}は許容できるだけ安全である	G	特定されたすべてのもっともらしいハザードに対処したと主張することによる議論	ST	(b)二重否定	property	{ハザードH1}が対処されている	G	(f)MECE	property									[23]	Figure 1
								{ハザードH2}が対処されている	G												
								{ハザードHn}が対処されている	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	12	{システム}は意図する適用にとって許容できるだけ安全である	G	EN50129によって要求される安全合意条件への一致について議論する	ST	(d)視点変換	property	効果的な品質管理は、{品質管理レポート(QMR)} を実装する	G	(f)MECE	property									[23]	Figure 3
								効果的な安全性管理は、{品質管理レポート(SMR)} を実装する	G												
								設計の技術的方法により、システムが十分に安全であることが保証される{技術的安全性レポート(TSR)}	G												
								コンポーネントの一部のサブシステムの認定された安全ケースが利用可能である{関連する安全ケース(RSC)	G												
2	13	デザインの技術手法は、システムが十分に安全であることを確実にする。{技術安全レポート(TSR)}	G	技術安全保証のための信頼できる技術証拠について議論する	ST	(d)視点変換	property	正しい機能操作が確実にされている(TSR: セクション2)	G	(f)MECE	property	システムおよび安全要件に従った正しい操作による議論	ST	(d)視点変換	property	システム要件仕様が満たされている（TSR：セクション2.3）	G	(f)MECE	property	[23]	Figure 4
																安全要件仕様が満たされている（TSR：セクション2.4）	G				
																正しいハードウェア機能が保証されます（TSR：セクション2.5）	G				
																正しいソフトウェア機能が保証されます（TSR：セクション2.6）	G				
								故障の影響は安全目標を満たしている（TSR：セクション3）	G												
								システムは外部の影響下で正しく安全に動作する（TSR：セクション4）	G												
								システムの安全性に関連するアプリケーションのルール、条件、および制約が明確に定義されている（TSR：セクション5）	G												
								運転条件下での安全認定試験が無事に完了する（TSR：セクション6）	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	14	G12 安全要件仕様は設計によって満たされます（TSR：セクション2.4）	G	S12.1 すべての安全要件のトレーサビリティと満足度による議論	ST	(e)合わせ技	property	G12.1 すべての安全要件は、各ライフサイクルフェーズで追跡されます	G	(e)合わせ技	property	S12.3 十分な安全性のレビューと文書化および設計の分析による議論	ST			G12.4 さまざまな要件仕様、テストケースなどの間のトレーサビリティが保証されます	G	(e)合わせ技	property	[23]	Figure 6
																G12.5 設計の前提条件は、製造、設置、および保守プロセスで保証されます	G				
								G12.2 すべての安全要件の満足度は、テストとシミュレーションによって検証されます	G			G12.6 シミュレーションは、安全要件の満足度を検証します	G	(e)合わせ技	property						
												G12.7 機能テストは、安全要件の充足を示しています	G			G12.9 システムの機能テストは、安全要件の充足を検証します	G	(e)合わせ技	property		
																G12.10 指定された環境条件下での機能テストは、安全要件の充足を検証します	G				
												G12.8 サージイミュニティ（堅牢性）テストに合格	G								
				S12.2 実際の使用で実証された高い信頼性による議論	ST			G12.3 安全な操作と経験の必要な期間が満たされています。	G	(d)視点変換	property										
2	15	WSP-G1 安全要件SR1は、WSPシステムのECUに組み込まれたソフトウェアの設計によって満たされます。	G	WSP-S1 2つの異なるV＆V技術からの検証と妥当性確認の結果による議論	ST	(d)視点変換	property	WSP-G2 正式な証明は、ソフトウェア設計に問題がないことを示しています	G	(e)合わせ技	property									[23]	Figurre 13
								WSP-G3 機能テストは、安全要件の満足度を検証します	G			WSP-G4 テストプロセスは正しい	G	(e)合わせ技	property						
												WSP-G5 テスト結果は正しい	G								
2	16	SysSafe システムは、特定の環境で動作するのに許容できるほど安全です	G	ArgSysHz 特定されたシステムハザードのリスクに関する議論	ST	(b)二重否定	property	HzRisk2 危険H2のリスクは許容可能です	G	(f)MECE	property									[29]	Fig. 2
								HzRisk4 ハザードH4が許容できる場合のリスク	G												
								HzRisk リスクとハザードH1は許容可能です	G			ArgRiskMitig リスク軽減策に訴えることによる議論	ST	(d)視点変換	property	CompSafe コンポーネントC1は意図したとおりに機能します（検出）	G	(f)MECE	Subject		
																CompSafe2 コンポーネントC2は意図したとおりに機能します（回復）	G				
																CompSafe3 意図したとおりのコンポーネントC3の機能（バックアップ）	G				
																ComInter コンポーネント間の相互作用は意図したとおりです	G				
								HzRisk3 危険H3のリスクは許容可能です	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	17	R1 飛行中の逆推力装置の不注意な展開は十分にありそうにないものでなければならない	G	S1 逆推力装置の展開を推進するための小切手への訴えによる議論	ST	(d)視点変換	property	R2 EECは遮断弁を「閉じた」ように命令します	G	(f)MECE	property									[29]	Fig. 6
								R3 EECと機体は方向制御弁「前進」を指揮します	G												
								R4 航空機は「オン」の第3ロックをコマンドします	G												
								R5 スロットルインターロックが提供されなければならない	G												
2	18	RiskHzdOvSpped 危険な速度超過のリスクは許容されます	G	ArgRiskAssManag 危険な速度超過の原因となる障害の軽減に関する議論	ST	(c)基準化	property	T1 / P1_Module-T1 / P1 危険な過速度へのT1 / P1測定の寄与は許容されます	G	(f)MECE	property									[29]	Fig. 10
								FuelFlow_MOdule 0 FuelFlow 危険な過速度への燃料フロープロセス制御の寄与は許容されます	G												
								FMV_Module-FMV 危険な過速度へのFMV位置制御の寄与は許容されます	G												
								SpeedMeasure_Module-速度測定 危険な超過速度への速度測定の寄与は許容されます	G												
								OverspeedProtect_Module-過速度保護 危険な過速度への過速度保護の寄与は許容されます	G												
								FuelMetering_Module-燃料計量 危険な過速度への燃料計量の寄与は許容されます	G												
2	19	T1 / P1 危険な過速度へのT1 / P1測定の寄与は許容されます	G	ArgRiskT1 / P1 T1 / P1の読み取り、条件付け、送信に関する議論	ST			T1 / P1REading T1 / P1センサーの読み取り値は正確です	G	(f)MECE	property	T1 / P1Reading Contract 読み取り	G	(c)基準化	property					[29]	Fig. 11
								T1 / P1Conditioning T1 / Paセンサーの読み取り値の調整は正確です	G			T1 / P1Cond Contract コンディショニン	G	(c)基準化	property						
								T1 / P1TransEEC T1 / P1値のEECへの送信は許容できるほど安全です	G			T1 / P1-EEC Contract EECトランスミッション	G	(c)基準化	property						

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	20	Argument 10.0 ヒューマンファクターハザード分析は、すべての運用コンテキストに適用されています。	G	Strategy 10.0 すべてのATC運用コンテキストがヒューマンファクターハザード分析の対象になっていることを示す	ST	(d)視点変換	property	Arg 10.1 ハザード分析の対象となるATC運用コンテキスト「セクター調整」	G	(f)MECE	property									[32]	Fig. 1
								Arg 10.2 ハザード分析の対象となるATC運用コンテキスト「フライトクリアランス」。	G												
								Arg 10.3 ハザード分析の対象となるATC運用コンテキスト「フライトホールディング」。	G												
2	21	G_1 スマートハウスのリスクが許容レベルまで低下	G	S_1 危険に応じて話し合う	ST	(d)視点変換	property	G_2 危険リストには、考えられるすべての危険が含まれています	G	(e)合わせ技	property	S_2 「抽象レベル」、「アーキテクチャレベル」、「実装レベル」についてハザードについて話し合う	ST			G_3 「抽象レベル」の危険有害性リストは包括的です	G	(f)MECE	property	[33]	Figure 5.4
																G_4 「アーキテクチャレベル」の危険性は包括的です	G				
								G_5 ハザードごとに、ハザードのリスクが許容レベルまで低下します	G			S_3 「リスク低減構造」、「アーキテクチャ設計」、「実装」について話し合います。	ST			G_6 リスク低減構造はすべての危険状況に対処します	G	(e)合わせ技	property		
																G_7 すべての建築設計はリスク削減を実装します	G				
																G_8 実装はシステム仕様を満たしています	G				
2	22	G-O0 検出されない破損を引き起こすデータ準備の確率はさらに悪い[XXXXXX]		G-O1 PageMillが破損を引き起こす確率は[XXXXXX]です	G	(f)MECE	Subject	（G-01→）（G-04→）S-O1 アプリケーションの性質からの議論。	ST	(c)基準化	property									[34]	Figure 1
				G-O4 ユーザーが破損を引き起こす可能性は[XXXXXX]です	G			S-O2 アプリケーションのユーザーのメソッドからの引数。	ST	(c)基準化	property										
				G-O5 破損が検出されなくなる確率は[XXXXXX]です	G			S-O5 処理されたページングが手動でチェックされるという引数。	ST	(c)基準化	property										
				G-O6 サーバー側の処理が破損を引き起こす可能性は[XXXXX]です。	G			（G-05→）（G-06→）S-O3 サーバーがフィールドチェックを実行するという引数。	ST	(e)合わせ技	property										
								S-O4 サーバーコードが正しく実装されているという引数。	ST												
2	23	G1：列車のドアコントローラーには、特定された事故につながる許容できないリスクがありません	G	S1：STPAを使用した事故と危険が軽減されます。	ST	(d)視点変換	property	G3：H1（出入り口の人のドアが閉まる）が軽減されます	G	(f)MECE	property									[35]	Fig. 2
								G4：H2（列車が移動しているときまたは駅にいないときにドアが開く）が軽減されます	G												
								G5：H3（緊急時に乗客が退出できない）が軽減されます	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	24	G12：UCA1（人または障害物が出入り口にあるときに列車のドアコントローラーがドアを開けるコマンドを提供しない）が軽減されます	G	S5：安全でない制御アクションの緩和を特定するためのシナリオと因果要因に関する議論	ST	(d)視点変換	property	G16：CF1（プロセスモデルに一貫性がない：プロセスモデルは、人または障害物が出入り口にあるときにコントローラーがドアを開ける必要があるとは見なしません）に対処します	G	(a)部分選択	property									[35]	Fig. 4
								G17：CF2（動作が不十分なセンサー：センサーが確実に動作していない。人や障害物が出入り口にあることを感知しない）に対処します。	G												
2	25	G16：CF1（プロセスモデルに一貫性がない：プロセスモデルは、人または障害物が出入り口にあるときにコントローラーがドアを開ける必要があるとは見なしません）に対処します	G	S6：因果要因に対処することを達成するための要件に関する議論	ST	(d)視点変換	property	G20：要件1（ドアの状態が「出入り口にいる人」でドアの位置が「部分的に開いている」場合は「ドアを開ける」制御アクションが発行されます）が正しく完全に実装および検証されている	G	(c)基準化	property									[35]	Fig. 5
2	26	G1 {システムX}には、特定された事故につながる許容できないリスクがありません。	G	S1 事故や危険が軽減されることについての議論	ST	(d)視点変換	property	G3 {ハザードY}が軽減されます	G	(c)基準化	property	S2 安全制御構造{SCS}を使用して、安全でない制御アクションを特定し、特定された危険を軽減する理由	ST	(c)基準化	property	S3 特定された安全でない管理措置と軽減すべき危険性に関する理由	ST	(c)基準化	property	[35]	Fig. 6
2	27	G1：{システムX}は安全です	G	S1：特定されたすべてのもっともらしいハザードに対処したと主張することによる議論	ST	(d)視点変換	property	G2：{ハザードH1}が解決されました	G	(f)MECE	property									[36]	Fig. 1
								G3：{ハザードH2}が解決されました	G												
								Gn：{ハザードHn}が解決されました	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	28	G19 C / Sロジックに障害はありません	G	S04 すべてのC / S安全要件を満たすことによる議論	ST	(e)合わせ技	property	G17 プレスコントロールが「詰まっている」と、プレスが停止します	G	(f)MECE	property	G18 PLCステートマシンの「Failure1」遷移には、TRUEのままのBUTTON_INが含まれます	G	(d)視点変換	property					[37]	Figure 1
								G20 物理的なPoNRを押す前にコントロールを解放すると、プレス操作が中止されます	G			(G17→)(G20→) G41 C / Sステートマシンは、実装動作の正確な表現です	G	(d)視点変換	property						
								G38 C / Sは、すべての単一コンポーネントの障害をフェイルセーフ（停止）し、（クラクションを鳴らして）通知します	G			G21 PLCステートマシンの「中止」遷移には、BUTTON_INがFALSEになることが含まれます	G	(d)視点変換	property						
				S03 特定されたすべてのソフトウェアハザードの省略による議論	ST			G42 （PoNR後の）意図しないプレスの開放は、コンポーネントの故障の結果としてのみ発生する可能性があります	G	(f)MECE	property										
								G43 意図しないプレスの閉鎖は、コンポーネントの故障の結果としてのみ発生する可能性があります	G												
2	29	G1：{システムX}は安全です	G	S1：特定されたすべてのもっともらしいハザードに対処したと主張することによる議論	ST	(d)視点変換	property	●n→ G2：{ハザードX}が解決されました	G	(f)MECE	property									[37]	Figure 3
2	30	G1：システムのソフトウェア要素は「障害なし」です	G	S1：すべてのソフトウェアの安全性/要件を満たすことによる議論	ST	(e)合わせ技	property	●m→ G2：ソフトウェアによって強制される<プロパティx>	G	(f)MECE	property									[37]	Figure 4
				S2：ソフトウェアを示すことによる議論は、特定された危険なソフトウェア状態を引き起こすことはできません	ST			●n→ G3：<条件y>は、物理コンポーネントの障害によってのみ発生する可能性があります	G	(f)MECE	property										
2	31	SysAccSafe {システムX}は許容できるほど安全です	G	ArgOverFunctions {システムX}の特定されたすべての安全関連機能に関する議論	ST	(d)視点変換	property	FnASafe 機能操作は許容できるほど安全です	G	(f)MECE	property									[38]	Figure 7
								FnBSafe 機能Bの操作は許容範囲内で安全です	G												
								FnCSafe 機能Cの操作は許容範囲内で安全です	G												

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	32	<全体的な安全目標> システム「許容可能」	G	<安定した（障害）状態> （物理的な）障害のない/障害が安定した条件下で許容されるシステム	G	(e)合わせ技	property	<個人の正しさ> 各アプリケーションの個々の動作は許容されます	G	(e)合わせ技	property									[38]	Figure A..1
								<障害の安定性> 識別された障害のあるリソースは、システムの他の部分に影響を与えることはできません	G												
								<望ましくない緊急行動はありません> すべての飛行体制で許容できるアプリケーションの複合効果	G			<スタートアップ> 起動時に許容できない緊急動作はありません	G	(f)MECE	property						
												<モード変更> モード/ブループリントの変更時に許容できない緊急動作はありません	G								
												＜通常動作＞ 通常の状態では許容できない緊急の動作はありません	G								
												<シャットダウン> シャットダウン中に許容できない緊急動作はありません	G								
				<物理的な故障状態> システムは、物理的な障害が存在する場合/発生した場合でも許容されます	G																
				<構成管理> 航空機内のシステムは、システム定義で許可されているシステムです。	G																
2	33	<個々の正しさ> 各アプリケーションの個々の動作は許容されます	G	<安全要件を特定する> 特定されたこのアプリケーションの安全要件	G	(f)MECE	property	＜連続制御＞ アプリケーションが正しいI/P-> O / P動作を維持する必要がある場所を特定する	G	(e)合わせ技	property									[38]	Figure A.2
								＜安全性＞ アプリケーションが維持しなければならない安全特性を特定します。 つまり、「常に...」、または「...決して起こり得ない」	G										
				＜仕様＞ 仕様は安全要件、および他のアプリケーションの期待を満たしています	G			<安全な行動を確立する> このアプリケーションには、他のアプリケーションの想定される動作に基づいて、安全性が必要です。	G	(e)合わせ技	property										
								<期待に応える> このアプリケーションに関して他のアプリケーションによって行われた仮定が満たされている	G										
				<実装と実行> 安全特性に関して正しく実装および実行された仕様	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	34	<実装と実行> 安全特性に関して正しく実装および実行された仕様	G	<実装> 安全特性の正しい実装	G	(e)合わせ技	property													[38]	Figure A.3
				<ハードウェアの正しい実行> ターゲットハードウェアは、実装されたコードを正しく実行します	G																
				<実行時> このアプリケーションで利用可能なリソース	G			<リソース割り当て> 必要に応じて利用可能なリソース	G	(e)合わせ技	property	<時間の割り当て> 各アプリケーションは、実行に必要な時間を取得します	G	(f)MECE	property						
												<メモリの割り当て> 各アプリケーションは、実行に必要なメモリを取得します	G								
												<コミュニケーションの配分> 各アプリケーションは必要に応じて通信できます	G								
								<利用可能なリソース> 十分なシステムリソースが利用可能	G												
				<非干渉> このアプリケーションは、別のアクティビティ/障害によって破損することはありません	G																
				<例外のない操作> アプリケーションの実行は、正当な入力を伴う実行時例外を生成できません	G																
2	35	SystemSafe 制御システムは許容できるほど安全です	G	HazardHandled 特定されたすべての危険が排除または十分に軽減されている	G	(e)合わせ技	property	ArgOverHaz 特定されたすべてのハザード（H1、H2、H3）に関する議論	ST	(d)視点変換	property	H1Elim H1が削除されました	G	(f)MECE	property					[39]	Figure 2
												H2OK H2が発生する確率<1x10-6 / 年	G								
												H3OK H3が発生する確率<1x10-3 / 年	G								
				許容可能なプロセス ソフトウェアは、関連する危険に適した完全性レベルに開発されています	G			PrimIL4 完全性レベル4に開発された一次保護システム	G	(f)MECE	property										
								SecIL2 完全性レベル2に開発された二次保護システム	G												

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	36	RAMS-P03-G01 リスク分析フェーズは十分に実行されます	G	RAMS-P03-S01 インプットの目的と適切性の達成について議論する	ST	(d)視点変換	property	RAMS-P03-G02 リスク分析フェーズの目標は十分に達成されています	G	(e)合わせ技	property	RAMS-P03-S02 それぞれの目的について議論する	ST	(d)視点変換	property	RAMS-P03-G04 システムに十分な危険が特定されている	G	(f)MECE	property	[40]	Fig. 8
																RAMS-P03-G05 ハザードにつながるイベントが十分に特定されている	G				
																RAMS-P03-G06 ハザードに関連するリスクは適切に決定されています	G				
																RAMS-P03-G07 継続的なリスク管理のプロセスが確立されます。	G				
								RAMS-P03-G03 文書はリスク分析フェーズの入力に適しています	G												
2	37	RAMS-P03-004 システムに十分な危険が特定されている	G	RAMS-P03-S03 ハザードの特定方法、ハザードの原因の完全性、およびハザードを特定する担当者について議論する	ST	(d)視点変換	property	RAMS-P03-G08 ハザードは体系的な方法で特定されます	G	(e)合わせ技	property									[40]	Fig. 9
								RAMS-P03-G09 危険の十分な原因が考慮されます	G												
								RAMS-P03-G10 危険を特定する人員とその能力は適切です	G												
2	38	G 1.1.4.7 ハザードログ要件が満たされている	G	G 1.1.4.7.1 ハザードログが開始されました	G	(f)MECE	property													[41]	Figure 2
				G 1.1.4.7.2 ハザードログが正しく維持されている	G																
				G 1.1.4.7.3 プロジェクト全体のリスクレベルを評価するために使用されるハザードログ	G																
2	39	G 1.1.4.7 ハザードログ要件が満たされている	G	G 1.1.4.7.1 ハザードログが開始されました	G	(f)MECE	property													[41]	Figure 3
				G 1.1.4.7.2 ハザードログが正しく維持されている	G			G 1.1.4.7.2.1 ハザードログへのアクセス権は正しく管理されています	G	(f)MECE	property										
								G 1.1.4.7.2.2 サインオフ手順とハザードログの権利が正しく管理されている	G										
								G 1.1.4.7.2.3 一貫して使用されるハザードログ	G										
								G 1.1.4.7.2.4 ハザードログの更新手順が理解され、正しく実行された	G										
				G 1.1.4.7.3 プロジェクト全体のリスクレベルを評価するために使用されるハザードログ	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	40	G 3.2 サブシステムXは許容できるほど安全です	G	G3.2.1 サブシステムXには、単一障害後の安全性を確保する冗長性が組み込まれています	G	(e)合わせ技	property													[41]	Figure 4
				G3.2.2 サブシステムXは、障害のない状態でも許容範囲内で安全です	G																
				G3.2.3 サブシステムXは、他の機能の安全性に悪影響を与えません	G																
2	41	G 4.3.3 ユニットYは許容できるほど安全です	G	S 4.3.3 直接証拠の質を示す間接証拠によって裏付けられた直接（分析、試験、製造および設置）証拠への訴えによる議論	ST	(d)視点変換	property	G4.3.3.1 分析とテストは、ユニットYの設計が安全であることを示しています	G	(e)合わせ技	property									[41]	Figure 5
								G4.3.3.2 ユニットYは、適切な基準に従って製造および設置されています	G												
								G 4.3.3.3 分析は有能なスタッフによって準備され、レビューされます	G												
								G 4.3.3.4 テストプログラムは適切に開発され、監査されています	G												
2	42	G 1 SystemZは許容できるほど安全です	G	G 1.1 システムZに関連するすべての危険からのリスクが許容レベルに低減されました	G	(e)合わせ技	property													[41]	Figure 6
				G 1.2 指定されたプロセスに従って設計および実装されたSystemZ	G			G1.2.1 Zのハザード関連の証拠の存在は、プロセスの完了を意味します	G	(d)視点変換	property										
2	43	G 1.1 システムZに関連するすべての危険からのリスクが許容レベルに低減されました	G	S 1.1 特定されたすべてのハザードに関する議論	ST	(d)視点変換	property	G 1.1.1 ハザード1に関連するリスクは許容可能です	G	(f)MECE	property									[41]	Figure 7
								G1.1.2 ハザード2に関連するリスクは許容可能です	G												
								G 1.1.n ハザードnに関連するリスクは許容可能です	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	44	G 1.2 指定されたプロセスに従って設計および実装されたSystemZ	G	G1.2.1 PHIが完了し、ハザードログに記録されました	G	(f)MECE	property													[41]	Figure 8
				G1.2.2 初期リスク評価が完了し、ハザードログが更新されました	G																
				G1.2.3 機能障害分析が完了し、新しいハザードがハザードログに記録されました	G																
				G 1.2.n 安全性の証拠が統合され、一貫性がチェックされています	G																	
2	45	G 1.2 指定されたプロセスに従って設計および実装されたSystemZ	G	G1.2.1 コンプライアンスマトリックスの手段は、プロセスステップの証拠が提示される場所を示します	G	(f)MECE	property													[41]	Figure 9
				G1.2.2 プロセスは、十分な証拠がない場合にコンプライアンスマトリックスが完成しないことを保証します	G																
2	46	G 1.1.4 Def Stan00-56に従って開発された安全管理システム	G	S 1.1.4 第5章内のすべての条項に対処することによる議論	ST	(f)MECE	property	G1.1.4.1 安全プログラム計画の要件が満たされている	G	(f)MECE	property									[41]	Fiture 10
								G1.1.4.2 主要なスタッフの要件が満たされている	G												
								G 1.1.4.3 安全性レビュー要件が満たされました	G												
								G 1.1.4.4 品質保証要件が満たされている	G												
								G 1.1.4.5 構成管理要件が満たされている	G												
								G 1.1.4.6 下請け業者の要件の監視と制御が満たされている	G												
								G 1.1.4.7 ハザードログ要件が満たされている	G												
								G 1.1.4.8 設計文書の要件が満たされている	G												
				G 1.1.4.9 安全ケースを維持するための適切な手順	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	47	制御システムは安全です	G	特定されたすべての危険が排除/十分に軽減	G	(e)合わせ技	property	H1が削除されました	G	(f)MECE	property									[42]	Figure 2
								H2が発生する確率<1x10-6 / 年	G												
								H3が発生する確率<1x10-3 / 年	G												
				I.L.に開発されたソフトウェア関係する危険に適切	G			I.L.に開発された一次保護システム 4	G	(f)MECE	property										
								I.L.に開発された二次保護システム 2	G												
2	48	G1 {to}は、{意図された環境}の{特定のプロパティ}を満たします	G	S1.1 {from}と開発メカニズムに関する議論	ST	(e)合わせ技	property	G2 {from}は{特定のプロパティの一部}を満たします	G	(e)合わせ技	property									[43]	Fig. 1
								G3 使用される開発メカニズムは、{from}部分と{to}部分の間の一貫性を保証します	G												
				S1.2 検証による議論	ST			G4 {to}は{特定のプロパティ}に対して検証されます	G	(d)視点変換	property												
2	49	G1 PCA実装ソフトウェアはGPCAの安全要件を満たしています	G	S1.1 GPCA時限オートマトンモデルと開発メカニズムに関する議論	ST	(e)合わせ技	property	G2 GPCA時限オートマトンモデルは、モデルレベルで形式化および検証できるGPCA安全要件を満たしています	G	(e)合わせ技	property									[43]	Fig. 2
								G3 使用される開発メカニズムは、GPCAの安全要件の満足度をGPCA時限オートマトンモデルからPCA実装ソフトウェアに伝播します。	G												
				S1.2 GPCAの安全要件に対してPCA実装ソフトウェアを検証することによる議論	ST			G4 PCA実装ソフトウェアは、GPCAの安全要件に対して検証されています	G	(d)視点変換	property												
2	50	G1.1.2.1.1 関連するすべての耐空性要件が完全かつ正確に特定されています	G	AwComplete 関連する要件を見落とす可能性が非常に低いことを示すことによる議論	ST	(e)合わせ技	property	G1.1.2.1.1.1 指定された耐空性要件	G	(e)合わせ技	property									[44]	Figure 4
								G1.1.2.1.1.2 関連する耐空性要件は、該当する場合、義務付けられた基準を満たします	G												
								G1.1.2.1.1.3 有能なスタッフによって評価されたHEAT / ACTに対する耐空性要件の関連性	G												
				AwCorrect 要件を導き出すために使用された仮定を示すことによる議論は正しかった	ST			G1.1.2.1.1.4 仮定は飛行試験によって正しいことが証明されています	G	(c)基準化	property												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	51	G1 ハザードが特定され、分析されました	G	G2 必要なプロセスアクティビティが実行されました	G	(e)合わせ技	property													[45]	Figure 3
				G6 製品の動作が分析されました	G																
2	52	G2 必要なプロセスアクティビティが実行されました	G	S1 役割をめぐる議論	ST	(e)合わせ技	property	G3 役割は資格があります	G	(c)基準化	property									[45]	Figure 4
				S2 活動のステップに関する議論	ST			G4 ハザードの特定と分類	G	(e)合わせ技	property										
								G5 前方および後方ハザード分析	G												
2	53	G6 製品の動作が分析されました	G	G7 識別および分類された危険	G	(e)合わせ技	property													[45]	Figure 5
				G8 危険なイベントの影響と原因	G																
2	54	車両の安全性 車両は許容できるほど安全です	G	製品開発 製品開発中の安全要件の実施に関する議論	ST	(f)MECE	property	事前定義された安全要件 車両は、事前定義された安全要件を満たしています	G	(e)合わせ技	property									[46]	Fig. 3
								(●m→) システムの安全性 {system}は、指定された環境で操作しても問題ありません。	G												
				ポストプロデュース開発 製品開発後の安全要件の実施に関する議論	ST			生産エラー 車両は製造時に故障がありません	G	(f)MECE	property											
								生命の安全を通して 車両は、使用中の監視、サービスの更新、および規定された使用中のメンテナンスの対象となります。	G											
2	55	事前定義された安全要件 車両は事前定義された安全要件を満たしています	G	属性とクラッシュシーケンスパフォーマンスベースの車両属性とクラッシュイベントの3つの特定されたフェーズに関する議論	ST			プリクラッシュ 車両の衝突前の属性が満たされている	G	(f)MECE	property									[46]	Fig. 4
								クラッシュワージネス 車両の耐衝撃性属性が満たされている	G												
								クラッシュ後 車両の衝突後の属性が満たされている	G												
2	56	制限 車両の機能が制限されています	G	エンジン実行中 エンジンの実行中にシステム障害が検出されると、システムが非アクティブ化され、実行されたままになります	G	(f)MECE	property													[46]	Fig. 9
				エンジンオフ エンジンがオフのときにシステム障害が検出されると、システムが動作を停止し、キースタートが必要になります	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	57	G1 高度違反を認識しているコントローラー	G	G2 ARTSは、追跡対象の航空機に関するタイムリーで正確な情報を提供します。	G	(d)視点変換	property													[47]	Figure 3
2	58	G1 高度違反を認識しているコントローラー	G	G2 MSAWは、高度違反が発生するとアラートを発します	G	(c)基準化	property	G3 MSAWが高度違反を検出	G	(f)MECE	property									[47]	Figure 4
								G4 高度違反が検出されると、MSAWはアラームを発します	G												
2	59	G1 高度違反を認識しているコントローラー	G	G2 MSAWは、高度違反が発生するとアラートを発します	G	(c)基準化	property	G3 MSAWが高度違反を検出	G	(f)MECE	property	G5 ソフトウェアは正しい	G	(f)MECE	property					[47]	Figure 5
												G6 テレインDB正しい	G								
												G7 レーダーは正確に戻ります	G								
												G8 有効な構成	G								
								G4 高度違反が検出されると、MSAWはアラームを発します	G												
2	60	SWContribAccept システムレベルのハザードへのソフトウェアの貢献は許容されます	G	SWContribIdent システムレベルの危険に対するすべてのソフトウェアの寄与が特定されました	G	(a)部分選択	property													[48]	Figure 4
				ArgOverSWContrib システムレベルのハザードに対する特定されたすべてのソフトウェアの寄与に関する議論	ST			HSFMAccept 危険なソフトウェア障害モード{HSFM}のすべての原因は許容されます	G	(c)基準化	property										
				SWSRTraceability ソフトウェアの安全要件と安全性の証拠のトレーサビリティが示されています	G																

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	61	G1 オートパイロットモジュールは正しい迎え角を正確に計算します	G	S1 入力が信頼できるという議論	ST	(e)合わせ技	property	G1.1 ピトープローブは、オートパイロットに信頼できるセンサー値を提供します	G	(d)視点変換	property	S1.1 オンデマンドでセンサーが故障する可能性が低いという議論	ST			G1.1.1 ピトープローブは、オンデマンドで故障する可能性が許容範囲内に低い	G	(d)視点変換	property	[49]	Figure 2
				S2 計算が正しいという議論	ST			G2.1 迎え角を計算するための仕様は正しいです	G	(e)合わせ技	property	S2.1 仕様で正しい式が使用されているという議論	ST	(f)MECE	property	G2.1.1 仕様では、迎え角を計算するための正しい式を使用しています	G	(c)基準化	property		
												S2.2 仕様で正しい校正定数が使用されているという議論	ST			G2.1.2 仕様で使用されている校正定数は正確です	G	(c)基準化	property		
								G2.2 迎え角の計算が正しく実装されている	G			S2.3 実装の正当性の証明による議論	ST	(d)視点変換	property	G2.2.1 AutoCert検証ツールを使用して生成された正しい実装の証明	G	(c)基準化	property		
				（G2.1.1→）S2.1.1 レビューによる議論（ドメインの専門知識に訴える）	G			G2.1.1 迎え角を計算するための仕様は、航空機設計チームによって正しいとレビューされています	G	(c)基準化	property										
				（G2.1.2→）S2.1.2 正しい実験的キャリブレーションの議論	G			G1.1.1 ピトープローブの校正は正確です	G	(c)基準化	property										
2	62	G0 [推進システムの危険性]が軽減されます	G	S0 特定されたハザードに関するの議論	ST	(d)視点変換	property	G1 [モーターの過熱]が軽減されます	G	(f)MECE	property	S1 特定された原因に関する議論	ST	(d)視点変換	property	G1.1 【風量不足】を管理	G	(f)MECE	property	[50]	FIg. 3
																G1.2 【運転中の故障】を管理	G				
								G2 [KDモーターコントローラーの誤ったプログラミング]が軽減されます	G			S2.1 特定された原因に関する議論	ST	(d)視点変換	property	G2.1.1 [戦闘前にプログラミングをチェックするための不適切な手順]が管理されている	G	(c)基準化	property		
2	63	G2 [KDモーターコントローラーの誤ったプログラミング]が軽減されます	G	S2.1 特定された原因に関する議論	ST	(a)部分選択	property	G2.1.1 [戦闘前にプログラミングをチェックするための不適切な手順]が管理されている	G	(c)基準化	property									[50]	Fig. 4
				StrStatCheck [静的チェック]による議論	ST			GStatCheck [ソフトウェアはプログラムされたパラメータ値が有効であることを確認します]	G	(c)基準化	property										
				SRunVerf [実行時検証]による議論	ST			GRunVerf [ソフトウェアはプログラムされたパラメータ値に対してランタイムチェックを実行します]ホールド	G	(c)基準化	property										

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	64	G1 IMAシステムは許容できるほど安全です	G	S1 安全な青写真と安全なマッピングルールの正しい組み合わせが、安全なIMA構成への安全な移行を提供すると主張する	ST			G2 IMAシステムの静的ブループリントは許容範囲内で安全です	G	(e)合わせ技	property	G5 IMAシステムハードウェアブループリントは許容範囲内で安全です	G	(f)MECE	property					[51]	Figure 4
												G6 IMAシステムソフトウェアブループリントは許容範囲内で安全です	G								
												G7 IMAシステム構成ブループリントは許容範囲内で安全です	G								
								G3 IMAシステムランタイムブループリントは許容範囲内で安全です	G			G4 IMAシステムマッピングルールは許容範囲内で安全です	G	(f)MECE	property						
												G8 構成間のIMAシステムの移行は許容範囲内で安全です	G								
												G9 IMAシステムのランタイムブループリント構成は許容範囲内で安全です	G								
2	65	G1 ニューラルネットワークは安全に操作できます	G	G2 ニューラルネットワークソフトウェアは、関連する危険に適切なASIL用に開発されました	G	(e)合わせ技	property	S1 要素（プライマリ、セカンダリ、..）に割り当てられたASILに関する引数	G	(c)基準化	property	G4 （多様な）冗長性および/または専用ASILへの監視	G	(d)視点変換	property					[52]	Figure 4
			G	G3 すべての危険が排除されているか、十分に軽減されています	G			S2 特定された各ハザードに関する議論	G	(d)視点変換	property	G5 決定された危険の確率	G	(e)合わせ技	property						
												G6 ニューラルネットワークの危険性が排除されました	G								
2	66	G4 （多様）専用ASILへの冗長性および/または監視	G	G4.2 モニタリング	G	(e)合わせ技	property													[52]	Figire 5
				G4.1 冗長性と障害処理	G																
2	67	G6 ニューラルネットワークの危険性が排除されました	G	S3 安定性基準	ST	(e)合わせ技	property	G7 堅牢なニューラルネットワークトポロジ	G	(c)基準化	property									[52]	Figire 6
				S4 自制心	ST			G8 ニューラルネットワークは危険な出力を作成しません。	G	(e)合わせ技	property										
								G9 運用パフォーマンス	G												
2	68	G8 ニューラルネットワークは危険な出力を作成しません	G	G10 結果空間の制限	G	(e)合わせ技	property													[52]	Figire 7
				G11 形式手法	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	69	G PFD、SYST.2 フェイルセーフ設計により、系統的な障害による障害の少なくとも90％が確実に失敗します。	G	G.HTL.TRIP 二重熱電対の切断または拒否はトリップを引き起こします	G	(e)合わせ技	property													[53]	Fig. 4
				G.FS-RC コンパイラー、ローダー、プロセッサーの欠陥は、可逆計算によって保護されています	G																
				G.チェック ADC、アプリケーションソフトウェア、構成トリップ制限、およびトリップロジックの欠陥は、次のように明らかになります。	G																
2	70	Gi 2-D UAS制御システムに関連するリスクシナリオが軽減されます	G	Giy1 「離陸」フェーズ中のリスクシナリオが軽減されます	G	(f)MECE	property													[54]	Figure 9
				Giy2 「ウェイポイントフォロー」フェーズ中のリスクシナリオが軽減されます	G			Giy21 「パーマネントラジオ」のリスクシナリオが緩和されました	G	(f)MECE	property										
								Giy22 「一時的なGPS-INS障害」のリスクシナリオが緩和されました	G												
								Giy23 「永続的なGPSINS障害」のリスクシナリオが軽減されました	G												
				Giy3 「着陸」段階でのリスクシナリオが軽減されます	G																
2	71	G1：システムは安全です	G	G2：要件は競合しています	G	(e)合わせ技	property													[55]	Fig: 2
				G3：すべての要件が満たされている	G																
2	72	G1 制御システムは許容できるほど安全に操作できます	G	G2 特定されたすべての危険が排除または十分に軽減されている	G	(e)合わせ技	property	S1 特定された各ハザードに関する議論	ST	(d)視点変換	property	G4 ハザードH1が排除されました	G	(f)MECE	property					[56]	Fig. 10
												G5 ハザードH2が発生する確率<1x10-6 /年	G								
												G6 ハザードH3が発生する確率<1x10-3 /年	G								
				G3 制御システムのソフトウェアは、関連する危険に適切なSIL用に開発されています	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	73	G1 MIRASロボットは、少なくとも従来の歩行器と同じくらい安全です。	G	S1 ロボット歩行器によって引き起こされる新しいリスクは正しく軽減されます	ST	(f)MECE	property													[56]	Fig. 11
				S2 従来の歩行器の使用によって誘発されるリスクは、正しく軽減されるか、増加しないかのいずれかです。	ST																
2	74	G9 HN12のリスクは、許容できる信頼性の高い報酬システムによって管理されています	G	S3 補償制度の受容性をめぐる議論	ST	(d)視点変換	property	G9.1 設計上の欠陥は適切に管理されています	G	(e)合わせ技	property									[56]	Fig. 15
								G9.2 補償システムの未検出の故障率（物理的な障害による）は許容範囲内です（$\lambda < \lambda_{max}$）	G												
								G9.3 患者の不均衡に続く補償システムの適用範囲は許容範囲内です（C> C_min）	G												
2	75	G1.1 船舶は周囲の物体を確実に検出して分類します	G	St1.1 SAシステム	ST	(d)視点変換	property	G1.1.1 周囲の景色が作成されます	G	(f)MECE	property	St1.1.1 SA センサーシステム	ST	(c)基準化	property					[57]	Figure 4
								G1.1.2 システムは関連するサイズのオブジェクトを検出します	G			（G1.1.2→）（G1.1.3→） St1.1.2.SA センサーフュージョン	ST	(c)基準化	property						
								G1.1.3 システムはオブジェクトを分類し、オブジェクトリストを維持します	G												
2	76	St1.1.1 SA センサーシステム	G	G1.1.1.1 センサーシステムの機能は、すべての条件で人間の監視機能と同等またはそれを上回ります	G	(e)合わせ技	property													[57]	Figure 5
				G1.1.1.2 リアルタイムのセンサーステータスデータが利用可能です	G																
				G1.1.1.3 センサーシステムは、個々のセンサーを失うために冗長です	G																
2	77	G1 システムは許容できるほど安全です	G	G2 システムの安全要件が完了している	G	(e)合わせ技	property													[58]	Fig. 1
				G3 システムの安全要件が満たされている	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	78	G1 特定されたすべての危険が排除/十分に緩和された	G	S1 特定されたすべてのハザードに関する議論	ST			G2 ハザードH1は排除されました	G	(f)MECE	property									[58]	Fig. 3
								G3 H2が発生する確率<1x10-3	G												
								G4 H3が発生する確率<1x10-6	G												
2	79	G1 システムは許容できるほど安全です	G	G2 システムの安全要件は有効です	G	(e)合わせ技	property													[58]	Fig. 5
				G3 システムの安全要件が満たされている	G																
				G4 システムの安全要件は追跡可能です	G																
2	80	G1 制御システムは、乗務員に適切な酸素を供給します	G	S1 メインシステムが不十分な場合のバックアップシステムによる酸素供給の提供による議論	ST	(d)視点変換	property	G2 メイン酸素供給サブシステムは適切な供給を提供します	G	(f)MECE	property									[58]	Fig. 6
								G3 モニターが主酸素供給の障害を検出し、バックアップシステムが適切な供給を提供します	G												
2	81	G1 制御システムは、乗務員に適切な酸素を供給します	G	S1 メインシステムが不十分な場合のバックシステムによる酸素供給の提供による議論	ST	(d)視点変換	property	G2 メイン酸素供給サブシステムは適切な供給を提供します	G	(f)MECE	property									[58]	Fig. 8
								G5 モニターが主酸素供給の障害を検出し、バックアップシステムが適切な供給を提供します	G			G3 モニターが主酸素供給の障害を検出	G	(f)MECE	property						
												G4 バックアップ酸素供給サブシステムは適切な供給を提供します	G								
2	82	G1 100～200の範囲のXの値エラーは発生しません	G	G2 100～120の範囲のXの値エラーは発生しません	G	(c)基準化	property													[58]	Fig. 10

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	83	G1-SAL4 システム出力のアクティブ化は許容範囲内で安全です	G	S1 すべてのコンポーネントの正しい動作に関する議論	ST	(d)視点変換	property	G2-SAL 4 システムのアクティブ化に関して正しい制御システム機能	G	(f)MECE	property	S2 制御システムの機能に関する議論	ST	(d)視点変換	property	G5-SAL 4 制御システムは正しい表示データを提供します	G	(f)MECE	property	[58]	Fig. 12
																G6-SAL 4 制御システムは、オペレーターがアクションを開始したときにのみ出力をアクティブにします	G				
								G4-SAL4 オペレーターは表示された情報と環境を正しく解釈し、安全な場合にのみシステムをアクティブにします	G											
								G3-SAL4 表示システムは、制御システムによって出力されたデータを正しく表示します	G			S3 ディスプレイシステムの機能に関する議論	ST	(d)視点変換	property	G8-SAL 4 ディスプレイ出力ステージは、画面にデータを正しく表示します	G	(f)MECE	property		
																G9-SAL 4 グラフィックジェネレーターとディスプレイ出力機能は独立しており、一般的な原因による障害の影響を受けません。	G				
																G7-SAL 4 GraphicsGeneratorは表示データを正しく解釈します	G				
2	84	G7-SAL4 グラフィックジェネレータは誤検知出力を引き起こすことはできません		S4 コンパレータとグラフィックジェネレータに関する議論	ST	(e)合わせ技	property	G11-SAL3 表示システムは、制御システムによって出力されたデータを正しく表示します	G	(f)MECE	property									[58]	Fig. 15
								G12-SAL 3 制御システムは、表示と表示の戻りデータを比較し、不整合がある場合は拒否権を生成します	G											
				G10-SAL 4 グラフィックジェネレータとコンパレータは独立しており、一般的な原因による障害の影響を受けません	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	85	AirSusClaim すべてのデューデリジェンスは、指定された環境で動作するAirSusに関して実行されました	G	Stra_AirSus 特定されたハザードのリスクに関する議論	ST			Hz_Oversteer 「予想されるオーバーステアとは異なる」のリスクは許容可能です	G	(f)MECE	property									[59]	Fig. 4
								Hz_Understeer 「予想されるアンダーステアとは異なる」のリスクは許容可能です	G												
								Hz_LeanResp_Module-リーンレスポンドハザード引数 「予期しない無駄のない反応」のリスクは許容できる	G												
								Hz_DHandling 「差動処理」のリスクは許容されます	G												
								Hz_Red_Traction 「トラクションの低下」のリスクは許容されます	G												
								Hz_LHeadloghts_Module-Headloghts低ハザード引数 「ヘッドライトが低い」というリスクは許容範囲内です	G												
								Hz_Towing 「けん引安定性の低下」のリスクは許容範囲内です	G												
								Hz_Headilights 「ヘッドライトが高い」のリスクは許容可能です	G												
								Hz_Trap 「トラップ」のリスクは許容可能です	G												
								Hz_Plip 「Plipによる高さの変更」のリスクは許容されます	G												
2	86	inbability_Height_Corner' 「各コーナーの高さを測定できない」という障害の影響は適切に管理されています（P / 6.5.6）	G	dHeight_Module-デフォルトの高さ引数' AirSusは車高をデフォルトに下げます	G	(f)MECE	property													[59]	Fig. 12
				dHeight_Module-高さ変更を無効にする' 高さ変更の要求は無効になっています	G																
				faultWarning3_Module-ドライバー警告3' ドライバーが故障を警告	G																	

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	87	IdentHazards ハザード分析とリスク評価は、信頼できる方法で関連するハザードを特定して分析します	G	Stra_Process プロセスコンプライアンスとプロセスの弱点の管理に関する議論	ST	(e)合わせ技	property	Process_Compliance ハザード分析とリスク評価はISO26262ガイダンスに準拠しています	G	(c)基準化	property	Stra_Activity ハザード分析とリスク評価活動に関する議論	ST	(d)視点変換	property	HazIdent 状況分析とハザードの特定が適切に実施された 危険なイベントにつながる可能性のあるシステムの潜在的な意図しない動作を特定し、特定しました	G	(f)MECE	property	[59]	Fig. 13
																HazClass ハザード分類が適切に実行され、アイテムの考慮されたハザードに関連する重大度（S）、暴露の確率（E）、および可制御性（C）が決定されました。	G				
																HazASIL 自動車の安全性完全性レベル（ASIL）がそれぞれについて決定されました 特定された危険	G				
																HzTeam ハザード分析とリスク評価を実施するチームには、システムの動作、および車両とそのドライバーの動作方法に関する十分な知識とドメイン経験を持つ人が含まれていました。	G				
				Process_Weaknesses ハザード分析とリスク評価プロセスの弱点は適切に管理されています	G			Stra_Process_Weaknesses 特定されたプロセスの弱点に関する議論	ST	(c)基準化	property	Underclass 以前に調査されていない新しい行動の過小分類は、追加の車両テストによって軽減されました	G	(c)基準化	property						
2	88	BXTestingTrustworty ブラックボックステストは信頼できます	G	ArgBXTestProcess ブラックボックステストプロセスを考慮した議論	ST	(d)視点変換	property	BXTestTeam テストチームは有能です	G	(f)MECE	property									[60]	Figure 5
								BXTestRqSys 試験方法は、安全要件に体系的に対処します	G			ArgBXTestCaseGen テストケースの生成と実行を考慮した議論	ST	(d)視点変換	property	BXTestRqGen テストケースの生成は徹底的でした	G	(f)MECE	property		
																BXTestCaseExec テストケースは、安定したプラットフォームとオブジェクトコードバージョンで実行されました	G				
																BXTestAnalysis ブラックボックステストの結果を分析しました。	G				
								BXTesTraceability テストプロセスは追跡可能です	G			ConfigMang 構成管理プロセスは信頼できる	G	(d)視点変換	property						

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	89	ArgSMachineProcess ステートマシン分析プロセスを考慮した議論	G	SMachineRepresentation ステートマシン分析の正確なシステム表現	ST	(d)視点変換	property	SmachineTeam 分析チームは有能です	G	(f)MECE	property									[60]	Figure 6
								SmachineTeam 分析チームは有能です	G												
								SMachineTraceability ステートマシン分析は追跡可能です	G			ConfigMang 構成管理プロセスは信頼できる	G	(d)視点変換	property						
								SMachineToolDependability ステートマシンツールは信頼できます	G												
2	90	Goal：Brake_Unit1 Brake_Unit1は安全です	G	Strategy：St1 特定されたハザードによって分解された議論	ST	(d)視点変換	property	Module：No_Brake_4W 4輪すべてのブレーキが完全に失われる危険性に対処しました	G	(f)MECE	property									[61]	Fig. 5 a
								Module：Val_Braking 誤ったブレーキ値の危険性に対処しました	G												
2	91	Goal：Val_Braking 誤ったブレーキ値の危険性に対処しました	G	Strategy：S_1 コンポーネント障害の軽減に関する議論	ST	(d)視点変換	property	Module：WNC ホイールノードコントローラーの障害は十分に管理されています	G	(f)MECE	property									[61]	Fig. 5 b
								Module; IWB ホイールブレーキでは、故障は十分に管理されています	G												
2	92	SysAccSafe {システムX}は許容できるほど安全です	G	ArgOverFunctions {システムX}の特定されたすべての安全関連機能に関する議論	ST	(d)視点変換	property	FnASafe 機能操作は許容できるほど安全です	G	(f)MECE	property									[62]	Figure 3
								FnBSafe 機能Bの操作は許容範囲内で安全です	G												
								FnCSafe 機能Cの操作は許容範囲内で安全です	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	93	G1 列車は安全にデポを離れます	G	S1 すべての危険が処理されました	ST	(d)視点変換	property	G2 VOBCセルフチェック	G	(f)MECE	property	G9 入力エコーチェック	G	(e)合わせ技	property					[63]	Figure 5
												G10 VOBCはセーフティリレーを採用	G								
								G3 通信回路を確認できます	G												
								G4 RAMS要件を超える高信頼性MMI_Argumentモジュール	G												
								G5 WOBCとZC間の信頼性の高い通信	G												
								G6 VOBCとMMT間の信頼性の高い通信	G												
								G7 VOBC間の信頼性の高い通信	G												
								G8 2本のケーブル間の信頼性の高い伝送	G												
								G11 VOBCは、電源投入時のセルフチェックで処理されます。そうしないと、正常に実行できません。	G												
2	94	AbsHSFMValue 寄与ソフトウェア機能（CSF）に値がないタイプの危険なソフトウェア障害モード{HSFM}	G	ArgFailureMech 失敗のメカニズムに関する議論	ST	(d)視点変換	property	AbsValSecondary 他のコンポーネントの二次障害の既知の原因は許容範囲内で処理されます	G	(f)MECE	property									[64]	Figure 6
								AbsValPrimary コンポーネント（CSF）は、主要な障害を正常に処理します	G												
								AbsValControl CSFは正しくスケジュールされています（クレームはCSFを管理する項目に対応しています）	G												
2	95	AbsHSFMValue 寄与ソフトウェア機能（CSF）に値がないタイプの危険なソフトウェア障害モード{HSFM}	G	ArgFailureMech 失敗のメカニズムに関する議論	ST	(d)視点変換	property	AbsValControl CSFは正しくスケジュールされています（クレーム CSFを制御する項目に対処します）	G	(f)MECE	property									[64]	Figure 15
								AbsValPrimary コンポーネント（CSF）は、主要な障害を正常に処理します	G			ArgAbsValPrimary 一次障害に関連する特定された各契約に関する議論	ST	(c)基準化	property	Goal：<A、G> LACU-2_sat 契約<A、G> LACU-2は十分な自信を持って満足しています	G	(f)MECE	property		
																Goal：<A、G> LACU-1_sat 契約<A、G> LACU-1は十分な自信を持って満足しています	G				
								AbsValSecondary 他のコンポーネントの二次障害の既知の原因は許容範囲内で処理されます	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	96	G7 GBDAA機能の回避機能は、輸送回廊への侵入者の航空機を許容範囲内で回避します。	G	S1 回避機能の配分をめぐる議論	ST	(d)視点変換	property	G9 GBDAA機能の回避機能の技術的実装は、輸送回廊での侵入者の航空機を回避するために許容されます。	G	(f)MECE	property	S7 耐空性保証による議論	ST	(e)合わせ技	property					[65]	Figure 1
												S8 装備の議論	ST			G16 UAに搭載された装備は、高度情報を送信することにより、通過回廊への侵入者の航空機の回避に貢献します。	G	(d)視点変換	property		
								G8 GBDAA機能の回避機能の手続き型実装は、輸送回廊での侵入者の航空機を回避するために受け入れられます	G			S2 オペレーター主導の回避手順に関する議論	ST	(e)合わせ技	property	G10 UAS操作のためのオペレーター主導の回避手順は、侵入者の航空機を容認できるように回避することに貢献します。	G	(c)基準化	property		
												S5 矛盾解消手順を適用することの議論	ST			G17 UAS運用のための解体手順は、侵入者の航空機を容認できるほど回避することに貢献します	G	(c)基準化	property		
2	97	G1 Lipoバッテリーシステムの故障は許容範囲内です	G	S1 識別されたすべての障害モードの許容範囲を表示	ST	(e)合わせ技	property	G2 バッテリーシステムの短絡が解消されます	G	(f)MECE	property									[66]	Figure 4 (b)
								G3 バッテリーパックの熱暴走が軽減されます	G												
				S2 冗長性の使用	ST																
2	98	G1 意図されたUAS操作は操作範囲（OR）内で安全に実行できます	G	S1 システムライフサイクルの各フェーズで安全にリスク管理を示す	ST			G5 該当するシステムの設計は、許容できない安全上のリスクを引き起こしません	G	(f)MECE	property									[66]	Figure 5
								G6 システムとそのコンセプトの実装は、許容できない安全上のリスクを引き起こしません	G												
								G3 該当するすべての運用上の安全リスクが完全かつ正確に特定されている	G												
								G2 特定され適用可能なすべての安全リスクは、運用において適切に管理されています	G			S2 それぞれの危険の結果に個別に対処する	ST	(d)視点変換	property	G7 OR内の地面衝突イベントのリスクは許容レベルまで減少します	G	(c)基準化	property		

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	99	G1 OR内の空中衝突（MAC）イベントのリスクが許容レベルまで低下し]ます	G	S1 MACリスクの要素を減らす	ST	(d)視点変換	property	G2 重大度はMACイベントが許容レベルに維持されていることです	G	(e)合わせ技	property									[66]	Figure 6
								G3 OR内のMACイベントの残りの可能性は許容可能です	G			S2 OR内のMACにつながるすべてのシナリオを緩和します	ST	(d)視点変換	property	G5 OR内でMAVにつながる、信頼できる特定されたすべてのシナリオが発生する可能性は許容範囲内です。	G	(f)MECE	property		
																G4 OR内のMACにつながるすべての信頼できるシナリオが完全かつ正しく識別されています	G				
2	100	G5 OR内のMACにつながるすべての信頼できる識別されたシナリオが発生する可能性は許容範囲内です	G	S1 識別されたMACシナリオの確率的モデリングを通して表示	ST	(e)合わせ技	property	G6 MACにつながる各個人の特定されたシナリオの可能性の確率的な組み合わせは許容されます	G	(c)基準化	property									[66]	Figure 7
				S2 各シナリオの緩和策を個別に表示する	ST			G7 MACにつながる空中紛争のシナリオは容認できるほど軽減されます	G	(c)基準化	property	S4 回復能力を示す	ST	(e)合わせ技	property	G9 空中紛争/安全な分離の喪失の場合、UAは視覚的に取得して確認および回避することができます	G	(c)基準化	property		
												S3 シナリオの開始イベントが発生する可能性が低いことを示す	ST			G8 空中紛争イベントの可能性は許容できるほど低い	G	(c)基準化	property		
2	101	G14 ORへの空中侵入者は十分に管理されています	G	S1 安全戦略の階層の適用を示す	ST	(d)視点変換	property	G27 多層防御を提供する複数の安全対策が実装されています	G	(a)部分選択	property									[66]	Figure 8
								G26 複数の安全対策を実施し、それぞれがリスク低減に貢献します	G			S2 各安全対策のリスク低減への貢献を個別に示す	ST			G15 空中侵入が発生した場合、十分に早期の警告が提供されます	G	(f)MECE	property		
																G17 緊急手順は、ORへの空中侵入者に対応するために定義されています	G				
																G20 UAを空中侵入者から分離するための規定が展開されています	G				
								G19 ORへの空中侵入を軽減するために効果的に組み合わせる複数の安全対策が実装されています	G												

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	102	G1 MACイベントのリスクを軽減するために使用される監視と回避の障壁は独立しています		S1 その一般的な原因の故障モードを示します。エスカレーションは管理されています	ST	(e)合わせ技	property	G4 監視および回避の障壁の失敗の一般的な原因が軽減されます	G	(d)視点変換	property	S5 それぞれの一般的な原因に個別に対処する	G			G8 監視システムの電源は、UAへの制御リンクに使用される電源とは異なります。	G	(f)MECE	property	[66]	Figure 9
																G6 監視システムの動作周波数と、回避操作を命令/実行するために使用される制御リンクの干渉は、許容範囲内で管理されます	G				
				S2 実装の多様性を示す	ST			G2 監視と回避の障壁は、別々の物理システムに実装されています	G	(d)視点変換	property										
				S3 データの多様性を示す	ST			G3 監視と回避の障壁の間のデータ依存の程度は許容できるほど低い	G	(d)視点変換	property										
				S4 少なくとも1つの独立した機能の可用性を示す	ST			G7 回避バリアには、監視バリアが失敗した/利用できないときに呼び出すことができる複数の操作が含まれています	G	(d)視点変換	property										
2	103	G2 地上監視は、UAの運用に対する信頼できる脅威である空中の標的を十分に早期に検出して追跡します	G	S6 構成要素に割り当てられた要件が満たされていることを示す	ST	(d)視点変換	property	G3 レーダーシステムは、信頼できる脅威をもたらす可能性のある非協力的/協力的な侵入機を適切に検出して追跡します	G	(f)MECE	property									[66]	Figure 10
								G32 統合監視ディスプレイ（ISD）は、現実と一致する、作戦の空域とその周辺の状況図を提供します	G			S11 ISDが状況認識に必要な情報を提供することを示す	ST	(d)視点変換	property	G28 ISDは、OR、拡張TV、およびSVを表示できます。	G	(f)MECE	property		
																G29 ISDは、位置、高度、速度などのターゲットトラックを表示します	G				
																G33 ISDは、現実と一致するORの簡単に理解できるビューを提供するように調整され、中央に配置されます。	G				
								G16 AD-B地上受信機は、OR内でBVLOSを操作しているUAを検出して追跡します	G			S10 オンボード機器の使用	ST	(d)視点変換	property	G8 UAに搭載された機器は、地上のADS-B受信機による検出を可能にします	G	(a)部分選択	property		
																G34 ADS-BOutトランスポンダーによってブロードキャストされたGPS位置レポートは信頼できます	G				
								G18 信頼できる脅威をもたらすレーダーコーンオブサイレンス内の空中ターゲットが検出され、追跡されます	G			S9 視覚的監視の使用	ST	(d)視点変換	property	G23 地上の視覚観測（VO）は、レーダーの場所に配置されます	G	(a)部分選択	property		
																G24 沈黙のレーダーコーン内の空中の脅威は視線内にあります	G				

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	104	G1 監視システム（バリア）の性能と有効性は検証可能です	G	S1 パフォーマンスと有効性が監視されていることを示す	ST			G11 パフォーマンスと効果的な対策が定義されています	G	(f)MECE	property									[66]	Figure 11
								G12 パフォーマンスと有効性のデータが収集され、要件に対して裏付けられます	G			S6 各監視サブシステムの監視を個別に表示	ST			G2 レーダーのパフォーマンスと機能が監視および検証されます	G	(f)MECE	property		
																G13 ADS-Bのパフォーマンスと機能は監視および検証されます。	G				
2	105	HITの安全性 健康ITは、定義されたケア環境で安全に使用できます	G	リスク戦略 HITの臨床リスクに基づく議論	ST	(d)視点変換	property	残存リスク 特定されたすべてのハザードからの残留臨床リスクが受け入れられ、管理されます	G	(c)基準化	property	管理されたリスク 定義されたコントロールが与えられると、関連する臨床的残存リスク ハザードインスタンスが許容基準を満たしている	G	(e)合わせ技	property					[67]	Figure 2
												臨床的利点 臨床的利益を無効にすることは、残存する臨床的リスクを上回り、それ以上の管理は実行不可能です。	G								
2	106	組織 組織はHITリスク管理に十分なサポートを提供します	G	組織的 さまざまなタイプの組織的サポートに基づく戦略の議論	ST	(d)視点変換	property	リソース 組織は十分なリソースを利用できるようにします	G	(f)MECE	property									[67]	Figure 5
								人員 組織には、HITリスク管理を実行するための知識、経験、および能力を備えた担当者がいます。	G												
								CSO 組織には資格のあるCSOがあります	G												
								文化 組織はオープンで公正な安全文化を維持しています	G												
2	107	SwiftUASは安全です	G	すべてのUASサブシステムとサブシステム間の相互作用に関する議論	ST			SwiftUAS通信インフラストラクチャは安全です	G	(f)MECE	property									[68]	Figure 1
								空中システム（Swift UAV）は安全です	G			SwiftUAVのすべてのハザードカテゴリーに対する緩和の議論	ST	(d)視点変換	property	動作環境またはSwiftUAVからの危険が軽減されます	G	(f)MECE	property		
																SwiftUAVの相互作用の危険性が軽減されます	G				
																SwiftUAVの故障の危険性が軽減されます	G				
																SwiftUAVの{ハザードカテゴリーX}が軽減されます	G				
								スイフト地上局は安全です	G												
								SwiftUASサブシステムの相互作用は安全です	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	108	降下中のソフトウェア障害が軽減されます	G	ソフトウェアシステムの正しさの議論	ST	(d)視点変換	property	ソフトウェアシステムに障害がない	G	(c)基準化	property	アーキテクチャの内訳に関する議論{すべてのソフトウェア実行レイヤーとコンポーネント}	ST			共通グラフィックライブラリは正しい	G	(f)MECE	property	[68]	Figure 6
																リフレクション仮想マシンは正しい	G				
																WindowsXP組み込みOSは正しく動作します	G				
																SwiftUAVソフトウェアのスクリプトは正しい	G				
2	109	オートパイロットの設計は正しい	G	自動操縦機能の内訳に関する議論	ST	(d)視点変換	property	オートパイロットモジュールは正しい迎え角を正確に計算します	G	(c)基準化	property	計算が正しく指定されているという引数	ST	(c)基準化	property	迎え角を計算するための仕様は正しいです	G	(c)基準化	property	[68]	Figure 7
2	110	G9 {推進システムの危険性}が軽減されます	G	S10 特定されたハザードに関する議論	ST	(d)視点変換	property	G13 {KDモーターコントローラーの誤ったプログラミング}が軽減されます	G	(f)MECE	property	S9 識別された原因をめぐる議論	ST			G14 [飛行前にプログラミングをチェックするための不適切な手順]が管理されている	G	(d)視点変換	property	[68]	Figure 12
								G10 [モーターの過熱]が軽減されます	G			S7 特定された原因に関する議論	ST	(d)視点変換	property	G11 【運転中の故障】を管理	G	(f)MECE	property		
																G12 【風量不足】を管理	G				
2	111	PLは安全です	G	システム1は安全です	G	(f)MECE	property	システム1は安全です（w.r.t.ハザードH1）	G	(f)MECE	property	G 'はH1を軽減します	G	(e)合わせ技	property					[69]	Figure 4
												システム1は、各yで（A '、G'）を満たします	G			前提（ｉ）と（ii）について議論する	ST	(f)MECE	property		
																「遂行」のセマンティクスについて議論する	ST				
																原子成分の検証によって議論する	ST				
								システム1は安全です（w.r.t.ハザードH2）	G												
2	112	CFLDは、各yで（A '、G'）を満たします	G	系1の前提が成り立つと主張する	ST	(f)MECE	property	前提（ｉ）が成り立つ	G	(f)MECE	property									[69]	Figure 5
								前提（vi）が成り立つ	G												
				各「遂行」のセマンティクスが成り立つと主張する（当然の前提（iii））	ST			A 'はA1を伴う	G	(f)MECE	property										
								A1はA2を伴います	G												
								G11はG 'を伴う	G												
				原子成分の契約が満たされていることを検証して議論する（当然の前提（iv））	ST			Ca-SENSは（A4、G4）を満たします	G	(f)MECE	property										
								Cd-SENSは（A3、G3）を満たします	G												
								Cb-ESTは（A10、G9）を満たします	G												
2	113	G1 タスクta1が実行されました	G	S1 役割Rをめぐる議論	ST	(a)部分選択	property	G1.ro1 ro.1が認定されています	G	(c)基準化	property									[70]	Fig. 8
				S2 作業成果物をめぐる議論W	ST			G1.wp1 wp1が利用可能です	G	(c)基準化	property										
				S3 ツールTをめぐる議論	ST			G1.to1 to1は修飾されています	G	(c)基準化	property										
				S4 ガイダンスGをめぐる議論	ST			G1.gu1 fu1がフォローされました	G	(c)基準化	property										

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	114	EPSの安全性 EPSは、定義されたケア環境で安全に使用できます	G	リスク戦略 特定されたハザードに関する議論	ST	(d)視点変換	property	残存リスク 特定されたすべての危険からの残留リスクは許容されます	G	(c)基準化	property	許容できるリスク 定義された管理が与えられると、各ハザードの残留臨床リスクは許容基準を満たします	G	(f)MECE	property					[71]	Figure 4
												許容できるリスク 臨床的利益は各ハザードの残存臨床リスクを上回り、それ以上の管理は実行不可能であるため、リスクは許容範囲内です。	G								
2	115	SysAccSafe {システムX}は許容できるほど安全です	G	ArgOverFunctions {システムX}の特定されたすべての安全関連機能に関する議論	ST	(d)視点変換	property	FnASafe 機能操作は許容できるほど安全です	G	(f)MECE	property									[72]	Figure 3
								FnBSafe 機能Bの操作は許容範囲内で安全です	G												
								FnCSafe 機能Cの操作は許容範囲内で安全です	G												
2	116	ホールセンサーはASILDの要件を満たしています	G	特定された各ハザードに関する議論	ST	(d)視点変換	property	ホールセンサー用のHARAコンプリート	G	(c)基準化	property	機能安全コンセプトの完成	G	(d)視点変換	property	アイテムの統合とテスト計画	G	(f)MECE	property	[73]	Figure 3
																システム設計仕様	G				
																技術的安全コンセプト	G				
2	117	目標を達成するために設計されたハードウェア	G	ハードウェアの安全要件]	G	(d)視点変換	property	各ハードウェアメトリックに関する議論	ST	(e)合わせ技	property	ハードウェアアーキテクチャメトリック	G	(f)MECE	property					[73]	Figure 4
												ハードウェアランダムメトリック	G								
								想定される動作限界を超える議論	ST			ドリフトと直線性の限界	G	(f)MECE	property						
												オーバーレンジハンドリング	G								
2	118	目標を達成するために設計されたソフトウェア	G	ソフトウェアの安全要件	G	(d)視点変換	property	各ソフトウェアメトリクスに関する議論	ST			ソフトウェアアーキテクチャ	G	(f)MECE	property					[73]	Figure 5
												ソフトウェアユニット	G								
2	119	アーキテクチャは依存障害を適切に削減します	G	ASILDの分解	G	(d)視点変換	property	ハードウェア依存の障害に関する議論	ST	(f)MECE	property	干渉を最小限に抑えるための多様なハードウェア	G	(e)合わせ技	property					[73]	Figure 6
												分解されたハードウェア用の個別のリソース	G								
								ソフトウェア依存の失敗に関する議論	ST			ソフトウェア依存の失敗に関する議論	G	(e)合わせ技	property						
												干渉を最小限に抑えるための多様なソフトウェア	G								
2	120	ホールセンサーはAsil-Dの要件を満たしています	G	特定された各ハザードに関する議論	ST			ホールセンサー用のHARAコンプリート	G	(d)視点変換	property	機能安全コンセプトの完成	G			アイテムの統合とテスト計画	G	(f)MECE	property	[73]	Figure 7
																システム設計仕様	G				
																技術的安全コンセプト	G				
2	121	G1 {システムX}は許容できるほど安全です	G	S1 特定されたすべてのもっともらしいハザードに対処したと主張することによる議論	ST	(d)視点変換	property	G2 {ハザードH1}に対処しました	G	(f)MECE	property									[74]	Fig, 1
								G3 {ハザードH2}が解決されました	G												
								Gn {ハザードHn}が解決されました	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	122	G1：路上テストは十分に安全です	G	S1：次の同時確率に基づく議論：自律性の失敗、タイムリーな監督者の対応、適切な監督者の緩和	ST			G2：タイムリーな監督者の対応	G	(e)合わせ技	property	S2：監督者の応答時間の要素に関する議論	ST			G21：覚醒	G	(f)MECE	property	[75]	Figure 1
																G22：自律障害の検出	G				
																G23：メンタルモデルの精度	G				
																G24：ODD違反の検出	G				
																G25：フィールドデータの確認	G				
								G3：適切な監督者の緩和	G			S3：監督者の対応の有効性の要素に関する議論	ST			G31：状況認識	G	(f)MECE	property		
																G32：正しい対応を計画する	G				
																G33：応答を適切に実行する	G				
																G34：車両が監督者の命令に応答する	G				
																G35：フィールドデータの確認	G				
								G4：適切な自律障害プロファイル	G			S4：検証方法に関する議論：設計、クローズドコーステスト、シミュレーション、..。	ST			G41：シミュレーションベースの検証	G	(f)MECE	property		
																G42：クローズドコースの検証	G				
																G43：フォールトインジェクション	G				
																G4x：…その他の検証と妥当性確認..。	G				
																G44：フィールドデータの確認	G				
2	123	MainSafe FLESは、意図した操作コンテキストで操作するのに十分安全です	G	AllHazardMitigated システムの危険性は適切に軽減されます	G	(b)二重否定	property	AllHazardidentified すべての危険が特定されました	G	(e)合わせ技	property	HazardAnalysis ハザード分析は適切です	G	(d)視点変換	property	HzrAnaProcAdeq ハザードを特定するために使用されるハザード分析プロセスは適切です	G	(c)基準化	property	[76]	Fig. 8
								MitigateStrat ハザード軽減に関する議論	ST			MitigationHazard1 ハザード1「予告なしの燃料不足」の緩和策が指定され、実施されている	G	(c)基準化	property	SG1Trace 安全目標1.0は、ハザード1を軽減するために導き出されます。	G	(f)MECE	property		
																SG2Trace 安全目標2.0は、ハザード1を軽減するために導き出されたものです。	G				
																SG1.0ImplAssur 安全目標1.0が実装され、保証されています	G				
																SG2.0ImplAssur Safety Gaol 2.0が実装され、保証されています	G				
																SafetyGoalAdeq 安全目標1.0および2.0は、ハザード1を適切に軽減します	G				

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	124	SafetyGoalsImpAssu 導出されたすべての安全目標が実装され、保証されています	G	SGsImpAndAssur 導き出された安全目標に関する議論	ST			SG1.0ImplAssur 安全目標1.0が実装され、保証されています	G	(f)MECE	Subject	DecSG 1.0 SG1.0をFSRに分解します	ST			FSR1.0.2.0 分解されたFSR1.0.2.0が実装され、保証されています	G	(f)MECE	property	[76]	Fig. 9
																FSR1.0.3.0 分解されたFSR1.0.3.0が実装され、保証されています	G				
																FSR1.0.1.0 分解されたFSR1.0.1.0が実装され、保証されています	G				
																ValidFSR1-2Deco 一緒に、FSR1.0.1.0とFSR1.0.2.0はSG1.0を満足させ保証します	G				
								SG2.0ImplAssur 安全目標2.0が実装され、保証されています	G			DecSG 2.0 SG2.0をFSRに分解します	ST			ValidFSR2.0.1.0Deco FSR2.0.1.0はSG2.0を満たし、保証します	G	(f)MECE	property		
																FSR2.0.1.0 分解されたFSR2.0.1.0が実装され、保証されています	G				
2	125	FuelLevelWarningBK.G1 FuelLevelWarningBKは、totalFuelLevel値を提供することを保証します	G	NotPrevented FuelLevelWarningBKに干渉する不要な相互作用はありません	G	(e)合わせ技	property													[76]	Fig. 10
				SArgDepnd 関連する依存関係に関する議論	ST																
				FuelEstimationBK.G5 FuelEstimationBKは、totalFuelLevel値を提供することを保証します	G																
2	126	EstimatorImplCorr Estimatorシステムの設計は、機能的および技術的な安全要件に準拠しています。	G	EstimatorImpUnDSpec Estimatorはソフトウェアユニットの設計仕様を満たしています	G	(c)基準化	property	EstimatorImpFunTech 機能安全および技術安全要件の実装は正しい	G	(e)合わせ技	property									[76]	Fig. 11
								EstimatorImoCon Estimatorのインターフェースの実装は一貫していて正しい	G			EstmaInnInter Estimatorの内部インターフェースの実装は一貫していて正しい	G	(f)MECE	property	SInterfaces 指定されたすべてのインターフェイスでの引数	ST	(c)基準化	property		
												EstimatorExtInter Estimatorの外部インターフェースの実装は一貫していて正しい	G								
								EstimatorImpRobust 機能安全および技術安全要件の実装	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	127	G1 システムは安全です	G	S1 障害仮説に対してフェイルセーフが保証されます	ST	(e)合わせ技	property	G2 考慮されるすべての関連する障害	G	(e)合わせ技	property									[77]	Figure 1
								G3 障害が障害につながることはありません	G												
				S2 フェイルセーフのために保証されたハザードセーフティ	ST			G4 常に故障によって引き起こされる危険	G	(e)合わせ技	property										
								G5 考慮されるすべての関連する危険	G												
2	128	G1 信号が無効であるが有効としてマークされていることを避けてください	G	S1 どの状況が安全要件を満たしているかを議論する	ST	(d)視点変換	property	G1.1 （SCからグランドへ）信号が無効であるが有効としてマークされていることを避けてください	G	(f)MECE	property									[77]	Figure 5
								G1.2 （信号の中断）信号が無効であるが有効としてマークされていることを避けてください	G												
								G1.3 （過負荷）信号が無効であるが有効としてマークされていることを回避する	G												
2	129	G1 クルーズコントロール機能にはエンジントルク<= 0が必要です	G	S1 <CC機能の分割信号フローと計算の責任にはエンジントルクが必要です<= 0>	ST	(c)基準化	property	G1.1 reqSpdControlは、目標速度信号の変化に応じてreqVehSpdを計算しています	G	(f)MECE	property									[77]	Figure 7
								G1.2 目標速度の変更は、reqSpdControlに直接送信されます	G												
								G.1.3 reqSpdControlはreqVehSpdをcruiseControlに直接転送します	G												
2	130	G_1 C / Sロジックには考えられる障害がありません	G	S_1 考えられるそれぞれの障害について議論する	ST			G_2 C / Sロジックに障害Aがない	G	(f)MECE	property									[78]	Fig. 2
								G_3 C / Sロジックに障害Bがない	G												
2	131	G_1 システムは信頼できます	G	S_1 関数に関する議論	ST	(d)視点変換	property	G_2 (関数)[┴]は信頼できる	G	(c)基準化	property									[78]	Fig. 10
2	132	G_1 システムは信頼できます	G	S_1 関数に関する議論	ST	(d)視点変換	property	G_2 [Function1]は信頼できる	G	(f)MECE	property									[78]	Fig. 11
								G_3 [Function2]は信頼できる	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	133	G_1 システム[┴]は安全です	G	S_1 システムのすべての安全関連機能に関する議論	ST	(d)視点変換	property	G_2 各機能は安全です	G	(f)MECE	property	S_3 各関数に関する議論	ST	(d)視点変換	property	G_4 機能[┴]は安全です	G	(c)基準化	property	[78]	Fig. 14
								G_3 システム機能間のすべての相互作用は危険ではないか、すべてのシステム機能は独立しています	G			S_2 ORの引数	ST	(d)視点変換	property	G_5 システム機能間の相互作用は無害です	G	(e)合わせ技	property		
																G_6 すべてのシステム機能は独立しています（相互作用なし）	G				
2	134	G_6 システム[自動車]は安全です	G	S_4 システムのすべての安全関連機能に関する議論	ST			G_7 各機能は安全です	G	(f)MECE	property	S_6 各関数に関する議論	ST	(d)視点変換	property	G_9 機能[実行中]は安全です	G	(f)MECE	property	[78]	Fig. 15
																G_11 機能【ブレーキ】は安全です	G				
								G_8 システム機能間のすべての相互作用は無害であるか、システム機能は独立しています	G			S_5 ORの引数	ST	(d)視点変換	property	G_10 システム機能間の相互作用は無害です	G	(c)基準化	property		
2	135	G_4 ユースケースは適切です	G	S_2 ユースケースコンポーネントに関する議論	ST	(d)視点変換	property	G_5 ユースケース図は適切です	G	(f)MECE	property									[78]	Fig. 16
								G_6 ユースケースの説明は適切です	G												
								G_7 ユースケースシナリオは適切です	G												
2	136	G_50 [ユースケース]は適切です	G	S_23 [ユースケース]コンポーネントに関する議論	ST	(d)視点変換	property	G_51 [ユースケース図]で十分です	G	(f)MECE	property									[78]	Fig. 18
								G_52 [ユースケースの説明]で十分です	G												
								G_53 [シナリオリスト]で十分です	G												
2	137	ゴール1 すべての意図しないシステム動作システムが特定され、適切なASILが割り当てられています	G	戦略1 ハザード分析は準備段階から開始され、事故の可能性を通じてシステムの動作を分析し、安全リスクを評価しながら、潜在的なシステムのハザードを体系的に特定します。	ST	(d)視点変換	property	ゴール1.1 ハザード分析の準備作業は十分に完了しています。	G	(e)合わせ技	property									[79]	Figure 3.1
								ゴール1.2 意図しないシステム動作がすべて特定されました	G												
								ゴール1.3 ASILは、リスク評価の計算を通じて正しく決定されています	G												

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	138	ゴール1.1 ハザード分析の準備作業は十分に完了しています	G	戦略1.1 ハザード分析の予備作業リストに従います	ST	(d)視点変換	property	目標1.1.1 標準的な慣行に準拠した安全作業部会が設立されました	G	(f)MECE	property									[79]	Figure 3.2
								目標1.1.2 システムの入力、出力、機能など、システムの概念が適切に定義されている	G												
								目標1.1.3 システム機能は完全に分析されました	G												
								目標1.1.4 意図されたすべてのシステム動作条件が分析されました	G												
								目標1.1.5 意図されたすべての動作条件での意図されたシステム動作が分析されました	G												
2	139	目標1.1.2 システムの入力、出力、機能など、システムの概念が適切に定義されている	G	戦略1.1.2 システムの境界とスコープが定義され、説明されている	ST			目標1.1.2.1 車両プラットフォームを含むシステムコンセプトの潜在的なアプリケーションは適切に定義されています。	G	(e)合わせ技	property									[79]	Figure 3.4
								目標1.1.2.2 システムの特徴と機能に関する仮定は適切に概説されています。	G												
2	140	目標1.1.2 システムの入力、出力、機能など、システムの概念は適切に定義されています。	G	戦略1.1.2 システムの境界とスコープが定義され、説明されています。	ST	(e)合わせ技	property	目標1.1.2.1 車両プラットフォームを含むシステムコンセプトの潜在的なアプリケーションは適切に定義されています	G	(c)基準化	property	戦略1.1.2.1 スコープが定義され、適切かどうかが確認されます	ST			目標1.1.2.1.1 システム安全コンセプトの範囲は適切に定義されています。	G	(e)合わせ技	property	[79]	Figure 3.5
																目標1.1.2.1.2 システムの安全範囲は、レビューに従って適切であると判断されました	G				
				目標1.1.2.2 システムの特徴と機能に関する仮定は適切に概説されています	G			戦略1.1.2.2 システムの機能とその前提条件は、妥当性を判断するために完了したレビューで定義されます	ST			目標1.1.2.2.1 システムの特徴と機能は完全に定義されています	G	(e)合わせ技	property							
												目標1.1.2.2.2 システムの安全概念の仮定は完全に定義されています	G								
												目標1,1,2,2,3 レビューによると、システムの安全性は適切であると判断されています	G								

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	141	目標1.1.3 システム機能は完全に分析されました	G	戦略1.1.3 システムの理解は分析を通じて伝えられます	ST	(d)視点変換	property	目標1.1.3.1 システムインテントが定義されました	G	(f)MECE	property									[79]	Figure 3.6
								目標1.1.3.2 システム出力が変更する車両のパラメータが定義されています	G			戦略1.1.3.2 車両パラメータの相互作用を表示するための図が作成されます	ST	(d)視点変換	property	目標1.1.3.2.1 目的の車両ステートマシンの論理ビューが開発されました	G	(d)視点変換	property		
								目標1.1.3.3 システムがその機能を達成するマナーが定義されています	G												
								目標1.1.3.4 システムがアクチュエータを直接制御するかどうかが決定されました	G			戦略1.1.3.4 センサー入力とアクチュエータ出力の関係は、情報処理リンクで定義されます	ST	(d)視点変換	property	目標1.1.3.4.1 システムの機能アーキテクチャは、システムおよび車両レベルで定義されています	G	(d)視点変換	property		
								目標1.1.3.5 システムが他のアクチュエータに対して持っている権限が述べられています	G			戦略1.1.3.5 システムとアクチュエータの関係の概要	ST			目標1.1.3.5.1 ASILが最も高いシステムは、安全コンセプトでシステムアクチュエータの完全性を詳しく説明しています	G	(d)視点変換	property		
2	142	目標1.1.4 意図されたすべてのシステム動作条件が分析されました	G	戦略1.1.4 すべてのシステム動作条件が考慮されます	ST	(e)合わせ技	property	目標1.1.4.1 運転段階でのシステムの運転条件が考慮されている	G	(c)基準化	property	戦略1.1.4.1 すべてのシステム相互作用条件が考慮されます	ST			目標1.1.4.1.1 意図された動作条件下で車両内で動作するシステムが考慮されています	G	(f)MECE	property	[79]	Figure 3.7
																目標1.1.4.1.2 車両内の他のシステムとの潜在的なシステムの相互作用が考慮されています	G				
																目標1.1.4.1.3 オペレーター（ドライバー、乗客、サービスクルーなど）との潜在的なシステムの相互作用が考慮されています	G				
				目標1.1.4.2 サービスフェーズ中のシステムの動作条件が考慮されています	G																
				目標1.1.4.3 メンテナンス段階でのシステムの動作条件が考慮されています	G																
				目標1.1.4.4 廃棄段階でのシステムの動作条件が考慮されています	G																

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	143	目標1.1.5 意図されたすべての動作条件での意図されたシステム動作が分析されました	G	戦略1.1.5 意図された動作状態での意図されたシステム動作を識別するために、要素のリストが識別されます	G	(c)基準化	property	目標1.1.5.1 システム内のエネルギーの種類が特定されています	G	(f)MECE	property									[79]	Figure 3.8
								目標1.1.5.2 エネルギーの流れの経路が特定されました	G												
								目標1.1.5.3 システム内のエネルギー放出のメカニズムが特定されています	G			戦略1.1.5.3 すべてのエネルギー出口源が考慮されます	ST	(d)視点変換	property	目標1.1.5.3.1 エネルギーの流れの潜在的な指揮源が特定されました	G	(e)合わせ技	property		
																目標1.1.5.3.2 機能-必ずしもコントローラーが特定されているとは限りません	G				
								目標1.1.5.4 相互作用するシステムエネルギーが特定されました	G												
2	144	ゴール1.2 意図しないシステム動作がすべて特定されました	G	戦略1.2 HAZOP手法が適用され、ガイドワードを利用して、設計意図からの逸脱が機器、アクション、または材料でどのように発生する可能性があるか、および逸脱の結果が危険につながる可能性があるかどうかを発見します	ST	(d)視点変換	property	目標1.2.1 車両レベルでのすべてのシステム機能のすべてのシステム機能の意図しないシステム動作が考慮されています	G	(e)合わせ技	property									[79]	Figure 3.9
								目標1.2.1 ハザード特定ステップは適切に完了しています	G												
2	145	目標1.2.1 車両レベルでのすべてのシステム機能の意図しないシステム動作が考慮されています	G	戦略1.2.1 すべての車両レベルの意図しない動作を考慮してください	ST	(d)視点変換	property	目標1.2.1.1 車両レベルでのすべてのシステム機能の意図しないシステム動作が考慮されています	G	(f)MECE	property	戦略1.2.1.1 システム内のすべての意図しない行動と影響力を考慮してください	ST			目標1.2.1.1 システムが制御または影響を与えるさまざまなアクチュエータが考慮されています	G	(e)合わせ技	property	[79]	Figure 3.10
																目標1.2.1.1.2 すべての潜在的な相互作用行動が考慮されています	G				
								目標1.2.1.2 車両レベルでのすべてのメンテナンスフェーズでの意図しないシステム動作が考慮されています	G												
								目標1.2.1.3 車両レベルでのすべてのサービスフェーズでの意図しないシステム動作が考慮されています	G												
								目標1.2.1.4 車両レベルでのすべての廃棄フェーズでの意図しないシステム動作が考慮されています	G												

		第 1 階層		第 2 階層				第 3 階層				第 4 階層				第 5 階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	146	目標1.2.2 ハザード特定手順は適切に完了しています	G	戦略1.2.2 FTA、FMEA、一般的な原因分析などの詳細なハザード分析を実施する際に、ハザードの原因が特定および分析されます。	ST	(d)視点変換	property	目標1.2.2.1 HAZOP分析結果からの意図しないシステム動作が特定され、システム動作に変換されました。	G	(e)合わせ技	property									[79]	Figure 3.11
								目標1.2.2.2 システムの動作は車両の動作に変換され、ハザードは特定の機能に対して同じ/同様の車両の影響と組み合わされています。	G										
								目標1.2.2.3 すべてのシステムレベルおよび車両レベルの危険が特定され、記録されています	G										
								目標1.2.2.4 ベストプラクティスのガイドラインが見直され、ハザードリストが更新されました	G										
								目標1.2.2.5 安全ワーキンググループは、関連するすべてのレビューを無事に完了しました	G										
2	147	目標1.2.2.5 安全ワーキンググループは、関連するすべてのレビューを無事に完了しました	G	戦略1.2.2.5 安全ワーキンググループは、ハザード分析文書をレビューし、矛盾を特定しました	ST	(c)基準化	property	目標1.2.2.5.1 すべてのハザード分析の不一致が特定および解決され、改訂コメントが文書化されています	G	(e)合わせ技	property									[79]	Figure 3.16
								目標1.2.2.5.2 システムハザード分析は、正式なシステム安全性レビュー中に技術レビュー委員会によって承認されました。	G										
2	148	ゴール1.3 ASILは、リスク評価の計算を通じて正しく決定されています	G	戦略1.3 リスク評価の計算は、ISO 26262 /ドラフト国際規格（DIS）と一致しており、それに基づいています。	ST	(c)基準化	property	目標1.3.1 各ハザードの最悪の事故の可能性が特定されました	G	(f)MECE	property									[79]	Figure 3.17
								目標1.3.2 最悪の場合のASIL分類の安全リスクが評価されました	G										
								目標1.3.3 システムの安全状態は、安全な状態のガイドラインを考慮して決定およびレビューされています	G										
								目標1.3.4 ベストプラクティスガイドラインの一貫性が確認され、ハザード分析レポートに必要な更新が行われました。	G										
								目標1.3.5 安全ワーキンググループは、関連するすべてのリスク評価レビューを無事に完了しました	G										

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	149	目標1.3.1 各ハザードの最悪の事故の可能性が特定されました	G	戦略1.3.1 各ハザードには、最悪の場合の事故の可能性が1つある必要があり、操作シナリオによっては複数の可能性がある場合もあります。	ST			目標1.3.1.1 潜在的な事故シナリオと考えられるドライバーの対応が特定されました	G	(c)基準化	property									[79]	Figure 3.18
2	150	目標1.3.2 最悪の場合のASIL分類の安全性リスクが評価されました	G	戦略1.3.2 ISO 26262DISに基づくリスク評価基準が決定	ST			目標1.3.2.1 安全対策なしの最悪の場合のリスクアセスメントが割り当てられました	G	(c)基準化	property									[79]	Figure 3.19
2	151	目標1.3.3 システムの安全な状態は、安全な状態のガイドラインを考慮して決定およびレビューされています	G	戦略1.3.3 リスクが許容可能であるために安全状態として分類されたものを含め、特定されたすべての危険が考慮されます	ST			目標1.3.3.1 システムセージの状態は完全に定義されています	G	(d)視点変換	property									[79]	Figure 3.20
2	152	目標1.3.5 安全ワーキンググループは、関連するすべてのリスク評価レビューを無事に完了しました	G	戦略1.3.5 安全ワーキンググループはハザード分析をレビューし、矛盾を特定しました	ST			目標1.3.5.1 すべての不整合が特定され、文書化された改訂コメントで解決されました	G	(e)合わせ技	property									[79]	Figure 3.22
								目標1.3.5.2 フォーマットシステムの安全性レビュー中に、ハザード分析の承認が技術レビュー委員会から取得されました	G												
2	153	目標1 システムの安全要件は、適切に定義、分析、分解され、サブシステムまたはコンポーネントに割り当てられています。	G	戦略1 このプロセスでは、システムの安全要件を特定し、それらを分析して分解し、サブシステムと潜在的なコンポーネントに割り当てます。	ST			ゴール1.1 システムの安全要件が特定され、分析され、分解され、サブシステムと潜在的なコンポーネントに割り当てられました。	G	(e)合わせ技	property									[79]	Figure 3.23
								ゴール1.2 要件の分解とASILの割り当てが完了しました	G												
2	154	目標1,1 システムの安全要件が特定され、分析され、分解され、サブシステムと潜在的なコンポーネントに割り当てられました	G	戦略1.1 要件の引き出し、技術的なレビューによる一般的な間違いの分析、分解、割り当てが完了しました	ST			目標1.1.1 システムの安全要件は、それぞれの要件ソースを通じて導き出され、定義されます	G	(e)合わせ技	property									[79]	Figure 3.24
								目標1.1.2 システムの安全要件は、技術専門家およびプロジェクトの利害関係者との非公式のレビューを通じて分析されます	G												
								目標1.1.3 システムの安全要件は分解され、ソフトウェアとハードウェアの機能要素に割り当てられます	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
2	155	目標1.1.2 システムの安全要件は、技術専門家およびプロジェクトの利害関係者との非公式のレビューを通じて分析されます	G	目標1.1.2.1 一連の要件は正しい	G	(e)合わせ技	property													[79]	Figure 3.26
				目標1.1.2.2 安全要件のセットが完了しました	G																
				目標1.1.2.3 安全要件のセットは一貫しており、競合しません	G																
				目標1.1.2.4 要件のセットは追跡可能です	G																
				目標1.1.2.5 一連の要件は明確で明確です	G																
2	156	目標1,2 要件 分解とASILの割り当てが完了しました	G	戦略1.2 ASIL分解は、安全要件のASILを、同じ安全要件への準拠に寄与するいくつかの要素に分散し、同じ安全目標に対応します。	ST			目標1.2.1 すべての安全目標には、関連する危険のリスク分類に基づく対応するASILがあります。	G	(f)MECE	property									[79]	Figure 3.28
								目標1.2.2 システム要素のASIL削減は、ASIL分解によって達成されました。	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	1	G1 システムは、通常の動作条件下で障害物との衝突を回避します	G	G2 システムは大雨での動作に耐えることができます	G	(a)部分選択	property													[80]	Figure 10
				G3 システムは濃霧での動作に耐えることができます	G																
				G4 システムは、不正確なセンサー測定に耐えること	G																
3	2	目標：SR1_SF 「AGVは、SIL2に適合した進行方向の経路に現れる障害物と衝突してはならない」	G	ストラト：SRsat 要素契約に関する議論	ST	(d)視点変換	Property	目標：elementCont 識別された要素の契約は、SIL2に対する「AGVは静的および動的な障害物を検出して回避する」を満たします。	G	(e)合わせ技	Property	ストラト：SRsatThing 物事契約に関する議論	ST	(e)合わせ技	Property	目標：AGVProp AGVは、静的および動的な障害物との衝突を処理するために必要なプロパティを提供します	G	(c)基準化	property	[81]	Figure 4
												ストラト：SRsatInfra インフラ契約をめぐる議論	ST			目標：CloudProps クラウドサーバーは必要なプロパティを提供します	G	(e)合わせ技	Property		
																目標：FogProps フォグコントローラーは必要なプロパティを提供します	G				
																目標：TransProps フォグコントローラーとAGV間のデータ送信には最大50msかかります	G				
								目標：elementContIdent 要素が「AGVが他のAGV、作業装置、および人間の労働者からの安全な距離を維持していない」という危険に寄与する可能性のある方法が完全かつ正確に特定されている	G										
3	3	飛行中のトラストリバーサーの不注意な展開は十分にありそうにないものとします。	G	S1 逆推力装置の展開を確認するためのアピールによる議論	ST	(d)視点変換	Property	R2 EECは、遮断弁を「閉じる」ように命令するものとします。	G	(f)MECE	Property									[82]	Fig. 2
								R3 EECと機体は、方向制御弁を「前方」に指令するものとします。	G												
								R4 航空機は、第3ロックを「オン」に命令するものとします。	G												
								R5 スロットルインターロックが提供されなければならない	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	4	Cl1 逆推力装置の展開をチェックするための要件の分解が完了し、飛行中の逆推力装置の不注意な展開が十分に起こりそうにないことを読者に保証するのに十分です。	G	S1 十分性の議論	ST			Cl2 逆推力装置の展開を推進するためのチェックをまとめると、不注意による展開が十分に起こりそうにないことが保証されます。	G	(e)合わせ技	Property	S3 チェックの失敗率への訴えによる議論	S	(d)視点変換	Property	Cl4 遮断弁、方向制御弁、三次ロック、およびスロットルインターロックの合計故障率は、飛行時間あたり1x19＾-9以下です。	G	(c)基準化	Property	[82]	Fig.3
				S2 完全性の議論	ST			Cl3 不注意による逆推力装置の展開の考えられるすべての原因が考慮されており、それらが発生するリスクは許容範囲内です。	G												
3	5	G2.1 MLモデルの開発では、割り当てられたシステムの安全要件が満たされます	G	S2.1 指定されたML安全要件に関する議論	ST	(d)視点変換	Property	G2.2 MLモデルはMLの安全要件を満たしています	G	(e)合わせ技	Property	S2.2 さまざまなタイプのML安全要件の満足に関する議論	ST	(d)視点変換	Property	G2.4 MLの性能安全要件が満たされている	G	(e)合わせ技	Property	[83]	Figure 7
								G2.3 ML安全要件は、割り当てられたシステム安全要件の有効な開発です。	G							G2.5 MLの堅牢性の安全要件が満たされている	G				
3	6	G3.1 MLMの開発と検証に使用されるデータは十分です	G	S3.1 データの十分性の要件に関する議論	ST	(d)視点変換	Property	G3.2 MLデータ要件は、ML安全要件を満たすMLMを開発できるようにするのに十分です。	G	(e)合わせ技	Property									[83]	Figure 9
								G3.3 生成されたMLデータはMLデータ要件を満たします	G			S3.2 さまざまなタイプのMLデータ要件に関する議論	ST	(d)視点変換	Property						
3	7	G4.1 学習したモデルの開発で十分です	G	S4.1 ターゲット展開の制約内でのモデル開発の十分性に関する議論	ST	(d)視点変換	Property	G4.2 選択したモデルは、内部テストデータを使用するときにMLの安全要件を満たしています	G	(e)合わせ技	Property									[83]	Figure 12
								G4.3 モデルを作成するために採用された開発アプローチで十分です	G			G4.5 選択したモデルのタイプは、定義されたML安全要件を満たすのに適しています	G	(f)MECE	Property						
												G4.6 モデルパラメータは、定義されたML安全要件を満たすのに適しています	G								
												G4.7 モデル開発プロセスは、定義されたML安全要件を満たすのに適しています	G								

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	8	G6.1 割り当てられたシステムの安全要件は、ML コンポーネントをシステムに導入することで満たされます。	G	S6.1 MLコンポーネントの統合と操作に関する議論	ST			G6.2 MLコンポーネントがに統合されている場合、割り当てられたシステムの安全要件は、定義されたすべての操作シナリオで満たされます。	G	(e)合わせ技	Property	S6.2 定義された運用シナリオに関する議論	ST	(d)視点変換	Property					[83]	Figure 16
								G6.3 割り当てられたシステムの安全要件は、システムの運用全体を通じて満たされます	G			S6.3 システムの設計と運用中の動作に関する議論	ST			G6.6 MLコンポーネントが統合されているシステムの設計により、割り当てられたシステムの安全要件が運用全体で確実に満たされます。	G	(e)合わせ技	Property		
																G6.7 展開されたコンポーネントの運用上の成果は、安全要件を満たしています	G				
3	9	G1 ビジョンベースのラインフォロー動作は常に正しい	G	S1 レーンフォロー障害を引き起こす理由について議論する	G	(d)視点変換	Property	G2 トラック照明の変動は正しく補正されます	G	(a)部分選択	Property	S2 トラックの照明条件に対する事前の信念の不確実性について議論する	ST	(d)視点変換	Property	G3 照明補正が必要です。 不確実性が軽減されます	G	(e)合わせ技	Property	[84]	Figure 1
																G4 照明補正設計の不確実性が軽減されます	G				
								G5 道路標示が正しく検出される	G			S3 正しい想起の不確実性について議論する	ST	(e)合わせ技	Property	G6 正しいリコールの不確実性が軽減されます	G	(c)基準化	Property		
												S4 誤検知の不確実性について議論する	ST			G7 誤検知の不確実性が軽減されます	G	(c)基準化	Property		
								G8 レーン相対推定は常に正しい	G												
3	10	G1 ダッキーボットはどのタイプのダッキーにもヒットしません	G	G2 promptType：必須 ダッキーボットは、検出されたダッキーとの衝突を停止または回避します	G	(e)合わせ技	Property													[84]	Figure 2
				G3_Meta タイプ：重ね合わせ promptType：必須 ダッキーの検出が困難なために発生するリスクを特定して軽減する	G			G4_Meta タイプ：entangledGoal 信念：0.9 すべての緩和策が特定され、十分です	G	(e)合わせ技	Property										
								G5_Meta タイプ：entangledGoal 信念：0.1 障害対応と違反戦略には、事故ログへのフィードバックが含まれます	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	11	心房細動の予防 心房細動のリスクは、ベータ遮断薬の投与によって制御されます	G	AF制御戦略 投薬管理の段階を考慮した議論	ST	(d)視点変換	Property	処方 栄養チューブの利用可能性を考慮して処方された適切なベータ遮断薬	G	(f)MECE	Property									[85]	Fig. 7
								調剤 処方されたベータ遮断薬または適切な代替薬が調剤された	G												
								管理 適切な経路で適切な用量で投与された調剤されたベータ遮断薬	G			ハザード対策戦略 ハザードタイプ別の議論{不正解、手数料、省略}	ST	(d)視点変換	Property	間違った薬 制御された管理でBBを管理する際の誤ったBBの原因	G	(f)MECE	Property		
																BBの不適切な投与量 制御された投与におけるBBの過剰または過少投与の原因	G				
																BBの委託 管理された管理におけるBBの委託の原因	G				
																BBの省略 制御された投与におけるBBの脱落の原因	G				
								モニタリング 投与されたベータ遮断薬の効果が監視されます	G												
3	12	G5-2 危険EI1--バッテリーの消耗は十分に軽減されます	G	S5-2 ハザードEI1の原因と局所的な影響が十分に管理されていることを示す	ST			G6-2 ハザードの原因として特定されたすべてのEI1は、十分に管理されています	G	(e)合わせ技	Property	S6-2 特定されたすべての原因の分解	ST	(d)視点変換	Property	G13-2 識別された原因は、個別に、または組み合わせて、危険を引き起こします、EI1	G	(f)MECE	Property	[86]	Fig. 5
																G7-4 ハザードEI1の原因である充電ステーションの場所が間違っていることが管理されています	G				
																G7-3 原因、目的地への到達は計画よりも多くのバッテリーを消費し、危険、EI1は管理されています	G				
																G7-5 ハザードEI1の原因、充電ステーションが想定どおりに選択されていないことが管理されている	G				
				S4 ハザードEI1が、その原因に適用された緩和策によって十分に管理されていることを示す	ST			G13 適用された緩和策は、ハザードEI1の十分なリスク低減につながります	G			S5 ハザードRI1に対処する緩和要件に関する議論	ST			G14 R1が保持する緩和要件	G	(c)基準化	Property		
3	13	GIntent：SAFEGUARDの定義された意図された動作は、目的の動作に関して正しく完全です	G	StDVnV： 開発とV＆Vの両方に関する議論	ST			GGenerated：SAFEGUARDの要件は、目的の動作に対処するために生成されました	G	(e)合わせ技	Property									[87]	Figure B2
								GRsNecessaryContent：SAFEGUARDの要件は、対処しなければならないことに対処します	G												
								GVerifiedAndValidated：SAFEGUARDの要件は検証および妥当性確認されています	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	14	GGenerated： SAFEGUARDの要件は、望ましい動作に対処するために生成されました	G	GRsDerived：SAFEGUARDの要件はフローダウンされ、システム要件（SWE-051）から（部分的に）導出されました。	G	(e)合わせ技	Property													[87]	Figure B3
				GNPR7150.2BC： SAFEGUARDとその開発はNPR7150.2Bに準拠しています	G																
				GSafetyReqs： SAFEGUARDの要件は、（部分的に）安全性分析から導き出されました	G																
3	15	GRsNecessaryContent： SAFEGUARDの要件は、対処しなければならないことに対処します	G	StAoKindsOfThings：対処すべき事柄の種類に関する議論	ST	(d)視点変換	Property	GRsAddrsHazards： SAFEGUARDの要件には、ソフトウェアの介入を必要とするハザード、状態、またはイベントの制御が含まれます	G	(a)部分選択	property	GRsAddrsFlyaway： SAFEGUARDの要件は、滞在地域外または滞在地域内（フライアウェイ）での飛行の危険性に対応しています。	G	(c)基準化	property					[87]	Figure B4
								GRsAddrsFOC： SAFEGUARDの要件は、予測可能な動作条件に対応しています	G			GMinSCFeatures： SAFEGUARDの要件には、セーフティクリティカルソフトウェア（SWE-134）の最小機能が含まれます。	G	(c)基準化	property						
3	16	GRsAddrsFOCs： SAFEGUARDの要件は、予測可能な動作条件に対応しています	G	StAoEnlFOC： 外部FOCと内部FOCの両方に関する議論	ST			GRsAEFOC： SAFEGUARDの要件は、外部FOCに対応しています	G	(f)MECE	property									[87]	Figure B5
								GRsAIFOC：SAFEGUARDの低レベル要件は内部FOCに対応します	G												
3	17	GRsAEFOC：SAFEGUARDの要件は外部FOCに対応しています	G	GRsAOFOC：SAFEGUARDの要件は、不特定のUASでの運用の予測可能な条件に対応しています	G	(c)基準化	property	StAoGnSCases：一般的なケースと特定のケースの両方に関する議論	ST			GRsAEFOCsG： SAFEGUARDの要件は、一般的に外部FOCに対応しています	G	(e)合わせ技	property					[87]	Figure B6
												GRsAEFOCsS：SAFEGUARDの要件は、外部FOCの注目すべき側面に対応しています	G								
3	18	SFR_Assurance すべてのSFRは、抽象モデルTIS_modelによって満たされます	G	FSR_Argument すべてのSFRに関する議論	ST			SFR1_C1 SFR1はTIS_modelLによって満たされます	G	(f)MECE	Subject	SFR1_Formalization TISは、TISとSFR1の形式化と形式的検証により、SFR1を満たします。	G	(c)基準化	property					[88]	Fig. 12
								SFR2_C1 SFR2はTIS_modelLによって満たされます	G												
								SFR3_C1 SFR3はTIS_modelLによって満たされます	G			SFR3_Formalization TISは、TISとSFR3の形式化と形式的検証により、SFR3を満たします。	G	(c)基準化	property						
3	19	SFR1_Formalisation TISは、TISとSFR1の形式化、および形式的検証によってSFR1を満たします。	G	SFR1_S1 形式化による議論	ST	(d)視点変換	property	FSFR1_Verified FSFR1は、TIS_Invを満たす任意の状態で検証できます。	G	(c)基準化	property									[88]	Fig. 13

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	20	目標：ReqsSatisfied形式化された{システム要件}が満たされている	G	目標：ReqsConfiguration {現在の構成}で達成された{システム要件}	G	(e)合わせ技	Property	戦略：ConfigReqs {現在の構成}の正式な要件に関する議論	ST	(d)視点変換	Property	目標：RxAchieved {現在の構成}を使用して達成される要件{Rx} 目標：RxVerified {現在の構成}について検証された要件{Rx}	G	(e)合わせ技	Property	目標：RxVerified {現在の構成}について検証された要件{Rx}	G	(e)合わせ技	Property	[89]	Fig 11
																アウェーゴール： {現在の構成}に対して検証されたReqsPreservedByPlatform要件{Rx}は、制御されたソフトウェアシステムによって実装されます	G				
												アウェーゴール： NoErroneousBehaviour誤った行動は容認できるように管理されています	G								
				目標：再構成 {システム要件}は再構成によって達成されます	G																
3	21	アウェーゴール： NoErroneousBehaviour 誤った行動は容認できるように管理されています	G	目標：EngErrorsAbsent エンジニアリングエラーは自己適応システム（SAS）では導入されません	G	(e)合わせ技	property	目標：NoProcessError ENTRUSTエンジニアリングプロセスはエラーを引き起こしません	G	(e)合わせ技	property	アウェーゴール：SuitableSoftEngProcess標準ソフトウェアエンジニアリングプロセスを採用	G	(e)合わせ技	property					[89]	Fig 12
												目標：NoMethodologicalErrorENTRUST方法論はエラーを導入しません	G								
								目標：NoController＆SystemError ENTRUSTコントローラーとシステムにエラーが含まれていません	G			ゴール：NoControllerError ENTRUSTコントローラーにエラーが含まれていません	G	(e)合わせ技	property						
												アウェーゴール： ControlledSystem制御されたシステムはエラーを引き起こしません	G								
				目標：FMsManaged システム要件は、SASの関連する障害モード（FM）に対応します	G			目標：FMsIdentified SAS用に正しく識別された関連FM	G	(e)合わせ技	property										
								目標：ReqsDerived 要件は、特定されたFMに対応できます	G												

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	22	目標：ReqsSatisfied 正式なUUV要件が満たされている	G	目標：ReqsConfiguration {現在の構成}で達成されたUUV要件	G	(f)MECE	Subject	戦略：ConfigReqs {現在の構成}の正式な要件に関する議論	ST			目標：R1達成 {現在の構成}を使用して達成された要件R1	G	(f)MECE	property	目標：R1検証済み {現在の構成}について検証された要件R1	G	(e)合わせ技	property	[89]	Fig 13
																アウェーゴール： ReqsPreservedByPlatform {現在の構成}について検証された要件R1は、制御されたソフトウェアシステムによって実装されます	G				
												目標：R2達成 {現在の構成}を使用して達成された要件R2	G								
												目標：R3達成 {現在の構成}を使用して達成された要件R3	G								
												目標：R4達成 任意の構成で達成された要件R4	G			アウェーゴール： ReqsPreservedByPlatform 構成について検証された要件R4は、制御されたソフトウェアシステムによって実装されます	G	(e)合わせ技	property		
				目標：再構成 再構成によって達成されたUUV要件	G											目標：R4Verified 要件R4はすべての構成で検証済み	G				
3	23	目標：ReqsSatisfied 正式なFX要件が満たされている	G	目標：ReqsConfiguration {現在の構成}で達成されたFX要件	G	(f)MECE	Subject	戦略：ConfigReqs {現在の構成}の正式な要件に関する議論	ST			目標：R1達成 {現在の構成}を使用して達成された要件R1	G	(f)MECE	property	目標：R1検証済み {現在の構成}について検証された要件R1	G	(e)合わせ技	property	[89]	Fig. 18
																アウェーゴール： ReqsPreservedByPlatform {現在の構成}について検証された要件R1は、制御されたソフトウェアシステムによって実装されます	G				
												目標：R2達成 {現在の構成}を使用して達成された要件R2	G								
												目標：R3達成 {現在の構成を使用して達成された要件R3	G								
												目標：R4達成 任意の構成で達成された要件R4	G			アウェーゴール： ReqsPreservedByPlatform 構成について検証された要件R4は、制御されたソフトウェアシステムによって実装されます	G	(e)合わせ技	property		
				目標：再構成 再構成によって達成されるFX要件	G											目標：R4Verified 要件R4はすべての構成で検証済み	G				

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	24	目標：ReqsSatisfied形式化されたFX要件が満たされている	G	目標：ReqsConfiguration 構成で達成されたFX要件（MW0、TA0、FA0、AI1、Or0、No1）	G	(e)合わせ技	Property	戦略：ConfigReqs 構成の形式化された要件に関する議論-（MW0、TA0、FA0、AI1、Or0、No1）	ST	(d)視点変換	Property	目標：R1達成 構成（MW0、TA0、FA0、AI1、Or0、No1）を使用して達成される要件R1	G	(f)MECE	property	目標：R1検証済み 要件R1の構成が検証されました（MW0、TA0、FA0、AI1、Or0、No1）	G	(e)合わせ技	Property	[89]	Fig. 20
																アウェーゴール：ReqsPreservedByPlatform 構成（MW0、TA0、FA0、AI1、Or0、No1）について検証された要件R1は、制御されたソフトウェアシステムによって実装されます。	G				
												目標：R2達成 構成（MW0、TA0、FA0、AI1、Or0、No1）を使用して達成される要件R2	G								
												目標：R3達成 構成（MW0、TA0、FA0、AI1、Or0、No1）を使用して達成される要件R3	G								
												目標：R4達成 構成（MW0、TA0、FA0、AI1、Or0、No1）を使用して達成される要件R4	G			アウェーゴール：ReqsPreservedByPlatform 構成（MW0、TA0、FA0、AI1、Or0、No1）について検証された要件R4は、制御されたソフトウェアシステムによって実装されます。	G	(e)合わせ技	Property		
																目標：R4Verified 要件R4の構成が検証されました（MW0、TA0、FA0、AI1、Or0、No1）	G				
				目標：再構成 再構成によって達成されるFX要件	G																
3	25	G1 DNNは十分に安全です	G	S1 全ての安全関連プロパティに関する議論	ST			G2-信頼性 pfd <Preqwothα信頼水準	G	(f)MECE	property									[90]	Fig.2
								G3-その他のプロパティ 他のプロパティに関連するすべてのリスクが軽減されました	G												
3	26	G2-信頼性 pdf＜α信頼水準の前提条件	G	S2 CBIに関する議論とライフスタイル活動からCBIへのインプット	ST			G4 正確な運用データが収集されました	G	(f)MECE	property									[90]	Fig.4
								G5 CBIモデルの仮定が評価されます	G												
								G6-部分的な事前 部分的な事前情報は、CBIへの入力として受け入れられます	G												

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	27	G6-部分的な事前 部分的な事前情報は、CBIへの入力として受け入れられます	G	S3 事前知識{Y}には十分な自信があると主張する：Pr（pfd≦ε）＝θ	ST	(d)視点変換	property	G8 事前の知識を得るという仮定の疑いが捕らえられる	G	(e)合わせ技	property									[90]	Fig.6
								G9 アクティビティ{Y}の仮定はオンラインで監視されます	G												
3	28	先行車が後続車と衝突しない	G	車の運転状態に基づいて安全クレームを分解します	ST	(d)視点変換	property	リーダーカー静止フォロワーカー移動	G	(f)MECE	property									[91]	Fig.3
								リーダーカー移動フォロワーカー移動	G												
3	29	G 後続車が先頭車と衝突しない	G	S 車の動作状態（移動中、静止中）に基づいて安全性の主張を分解します。 特に関心のある2つのケースが検討されます	ST			SG1 リーダーカー静止フォロワーカー移動		(f)MECE	property	S1 LIDAR、オブジェクト検出、ブレーキマネージャーのコンポーネントが安全要件を満たしていることを示すことで安全要件を主張する	ST			G12 ブレーキマネージャーモジュールは逆極性RPWM>VPWMを提供します				[91]	Fig.6
																G5 障害物距離モジュールは、範囲（0,12）mの障害物の距離を提供します		(e)合わせ技	property		
																G8 障害物検出モジュールは、範囲（0.1、1）mの車の画像を検出します					
								SG2 リーダーカー移動フォロワーカー移動				S2 LIDAR、オブジェクト検出、ブレーキマネージャーのコンポーネントが安全要件を満たしていることを示すことで安全要件を主張する	ST			G5 障害物距離モジュールは、範囲（0,12）mの障害物の距離を提供します		(e)合わせ技	property		
																G8 障害物検出モジュールは、範囲（0.1、1）mの車の画像を検出します					
																G12 ブレーキマネージャーモジュールは逆極性RPWM>VPWMを提供します					
3	30	主張 緩和介入はプラスとマイナスの効果をもたらします	G	議論戦略 プラスの効果をめぐる議論	ST	(f)MECE	property	主張 緩和介入により、救命救急のピーク需要が2/3減少します	G	(a)部分選択	property									[92]	Figure 2
								主張 緩和介入は死者の数を半分にします	G												
				議論戦略 悪影響をめぐる議論	ST			主張 緩和介入により、救命救急ベッドのピーク需要は、利用可能なサージ容量の8倍になります。	G	(a)部分選択	property												
								主張 緩和介入により、すべての患者が治療できたとしても、英国では250000人が死亡します。	G												
								主張 緩和介入は、集団の集団免疫をほとんどもたらさず、介入が終了すると、セカンドウェアの可能性をもたらします	G												

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	31	クレーム1.1.4 シミュレーションは、72時間での細胞凝集の緊急行動をキャプチャします	G	戦略1.1.4.1 代表的な数のPPが72時間の終わりに形成されると主張する	ST			クレーム1.1.4.1 シミュレーションは、代表的な数のPPを生成するように調整されています	G	(e)合わせ技	property									[93]	Fig.3
				戦略1.1.4.2 以前に公開された実験結果を再現するシミュレーションの能力について議論する	ST			クレーム1.1.4.2.1 シミュレーションは、[31,39,41,42]のさまざまな条件下でのバッチ形成を示す実験結果を再現します。	G												
				戦略1.1.4.3 シミュレーションはPPの空間特性をキャプチャすると主張します	ST			クレーム1.1.4.3.1 インシリコで生成されたPPとインビボで生成されたPPを比較することができます	G												
3	32	解釈可能性の主張 MLシステムは、意図したコンテキストで十分に解釈可能です	G	解釈可能性の本質的な側面に基づく議論	ST			正しい方法 システム構造とセグメンテーションマップは、システムロジックの透明性を提供し、臨床医が決定を理解できるようにします	G	(f)MECE	property	解釈可能性の方法に関する議論	ST			解釈可能性の方法は正しいタイプです（正しいことは説明されています）	G	(f)MECE	property	[94]	Fig.3
																解釈可能性の方法は、システムプロセスに適切に忠実です	G				
								適切なコンテキスト 網膜診断経路で作成されたセグメンテーションマップ	G			適切なタイミング セグメンテーションマップは、診断予測と一緒に作成されます	G	(f)MECE	property	臨床医は、すべての診断予測と一緒に説明が必要です	G	(c)基準化	property		
												正しい設定 説明は臨床現場で利用可能です	G			明らかに、臨床医は臨床現場でこれらの説明にアクセスできる必要があります	G	(c)基準化	property		
												正しい聴衆 網膜臨床医のために作成された説明	G			臨床医は、システムの予測を理解して信頼するための説明が必要です	G	(c)基準化	property		
								正しいフォーマット 解釈の形式は、セグメンテーションマップを含む透過的なシステムロジックです。	G			セグメンテーションマップの作成を含むシステム構造は、通常の臨床的意思決定プロセスに非常に似ており、システムロジックに対する包括的な洞察を提供します。	G	(c)基準化	property						

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	33	SOTIFの達成 {Item}の意図された機能（IF）またはその合理的に予見可能な誤用に関連する危険なイベントによる不当なリスクの欠如が達成されます	G	リリース前とリリース後 IFの開発と現場での運用について議論する	ST			プレリリース IFは、最初に現場に導入されたとき、不当なリスクがありません。	G	(f)MECE	property	ODD-アクティベーション状態 ODD-アクティベーション状態とそれらの間の遷移によって構造化された引数	ST	(d)視点変換	property	状態1の危険なイベント 状態1内のIFによって引き起こされる、または状態1からの移行時に、不当なリスクをもたらす危険なイベントはありません。	G	(f)MECE	property	[95]	Fig. 2
																状態2の危険なイベント 状態2内のIFによって引き起こされる、または状態2からの移行時に、不当なリスクをもたらす危険なイベントはありません。	G				
																状態3の危険なイベント 状態3から移行するときにIFによって引き起こされる危険なイベントは、不当なリスクを示しません	G				
																状態4の危険なイベント 状態4から移行するときにIFによって引き起こされる危険なイベントは、不当なリスクを示しません	G				
								リリース後 リリース後のSOTIFの問題に関連するリスクに対処するために十分な考慮が払われています	G											
3	34	G1：∀i∈I、∀t∈Ti、S1の廊下の壁からの車の距離は常にゼロより大きい	G	モデルベースのアプローチ	ST	(d)視点変換	property	G2：∀i∈I、∀t∈Ti、S1のNNコントローラーで構成されたS1のCPSNNのモデルの廊下の壁からの車の距離は常にゼロより大きい	G	(e)合わせ技	property	全体的アプローチ	ST	(d)視点変換	property					[96]	Fig. 8
								G3：CPSNN / NNの選択されたノードは、S1のCPSNN / NNを正確に表します。	G			S1のCPSNN / NNのモデルにおける観測とダイナミクスモデルの選択に関する議論	ST			選択した観測モデルは、S1の廊下での取引LiDAR操作を表しています。	G	(e)合わせ技	property		
																キネマティック自転車モデルはF1 / F10車を正確に表現しています	G				
3	35	G1：S2のdist（t0）未満の制動距離の場合、自我車両は、静止車両から前方にある場合、常にゼロより大きい距離を維持します。	G	モデルベースのアプローチ	ST	(d)視点変換	property	G2：知覚ベースのNNで構成されるS2のCPSNN / NNのモデルでdist（t0）未満の制動距離の場合、自我車両は常にその前の静止車両からゼロより大きい距離を維持します	G	(c)基準化	property	仮定/保証アプローチ	ST	(d)視点変換	property					[96]	Fig. 10

		第1階層		第2階層				第3階層				第4階層				第5階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	36	G1：車速が15km / hを超えているときにアクチュエータを作動させることは避けてください	G	S1：ANDリファインメントによる分解	ST			G1.1：VSECUは正確な車速情報をACECUに送信します	G	(f)MECE	property	S1.1：ソリューションは目標G1.1をテストするのに十分なカバレッジを持っていることが示されています	ST	(d)視点変換	property					[97]	Fig. 33
								G1.2：VSECUは正確な車速情報を冗長スイッチに送信します	G			S1.3：ソリューションは目標G1.2をテストするのに十分なカバレッジを持っていることが示されています	ST	(d)視点変換	property						
								G1.3：車速が15km / hを超える場合、アクチュエーターに電力が供給されません。	G			S2 ASIL分解戦略（CからBおよびA）	ST	(d)視点変換	property	G2.3：ACECUと冗長スイッチの十分な独立性が示されています		(f)MECE	property		
																G2.1：車速が15km / hを超える場合、ACECUはアクチュエータに電力を供給しません					
																G2.2：車速が15km / hを超える場合、冗長スイッチは開いた状態です。					
								G1.4：アクチュエータは、ACECUから電力が供給され、冗長スイッチが閉じている場合にのみ作動します。	G			S1.4：ソリューションは目標G14をテストするのに十分なカバレッジを持っていることが示されています	ST	(d)視点変換	property						
3	37	Goal; SR1sat 「警告ログの信号は、許可されていないAGVが制限区域に入ってから0.5秒以内に発生するものとします」必要なレベルの保証に満足している	G	Strat：SRsat IoT要素をめぐる議論	ST	(d)視点変換	property	Goal：elementSat 識別されたIoT要素は、必要なレベルの保証で安全要件を満たします	G	(e)合わせ技	property	Goal：thingsSat 物事は必要なレベルの保証で安全要件を満たします	G	(e)合わせ技	property	Goal：lightProp 警告ランプの契約が満たされている	G	(e)合わせ技	property	[98]	Fig. 6
																Goal：LidarProp Lidarの契約が満たされている	G				
																Goal：lightSat 物事によって保証される特性は、安全要件を満たすのに十分です	G				
												Goal：infraSat インフラストラクチャ要素は、必要なレベルの保証で安全要件を満たします	G								
								Goal：elementIdent 安全要件の実装に関係するIoT要素が正しく識別されている	G												
3	38	安全目標：プラトゥーニング中に安全トラックの距離に違反しない（ASIL D）	G	戦略：影響パラメータの障害モードの制約に関する議論は、最悪の場合、または整合性を持って測定します	ST	(d)視点変換	property	Req0：関連するすべての障害モードが特定されました。		(f)MECE	property									[99]	Fig.3
								Req1：フォロワーの反応距離が短すぎることは避けなければなりません（ASILD）。													
								Req2：フォロワー加速距離12が低すぎることは避けなければなりません（ASILD）。													
								Req3：フォロワーの制動距離が短すぎることは避けなければなりません（ASILD）。													
								Req4：リーダーの制動距離が長すぎることは避けなければなりません（ASILD）。													
								Req5：実現されたトラック距離が短すぎることは避けなければなりません（ASIL D）													

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	39	G1 EGSは、起動前にコマンドによる中止を開始します	G	S1 コマンド生成の保証による議論	ST	(f)MECE	property	G2 EGSソフトウェアは、abortコマンドを生成してパッケージ化します	G	(c)基準化	property									[100]	Figure 2
				S2 SLSコマンド経路のSLSコマンドの保証による議論	ST			G3 SLSソフトウェアはEGSからアボートコマンドを受信します	G	(f)MECE	property										
								G4 SLSソフトウェアは、打ち上げ前に打ち切りコマンドを受信すると、打ち上げロケットを保護します	G			S4 ソフトウェア成果物の正確性と完全性による議論	ST	(e)合わせ技	property	G8 アボートコマンドに対するSLS応答を定義するソフトウェア要件は正しく、完全です	G	(f)MECE	property		
																G9 中止コマンドに対するSLS応答のソフトウェア実装は正しく、完全です	G				
												S5 独立したテスト実行による引数	ST			G10 SLSソフトウェアシミュレーションはコマンドの中止に正しく応答します	G	(c)基準化	property		
				S3 オリオンコマンド経路の保証による議論	ST			G6 OrionソフトウェアはEGSから中止コマンドを受け取ります	G	(f)MECE	property										
								G7 Orionソフトウェアは、起動前に中止コマンドを受信すると中止を開始します	G												
3	40	MEXEC on ASTERIAは、安全性と進歩の目標を達成しています	G	Tasknetの実行は安全です（安全上の制約に違反しません）	G	(e)合わせ技	property	MEXECソフトウェアの実行は、宇宙船のソフトウェアまたはデータを破壊しません	G	(f)MECE	property	標準ソフトウェアV＆V	G	(d)視点変換	property					[101]	Figure 1
								MEXECとASTERIAオペレーションおよびFSWとの相互作用は安全です	G			EXECとASTERIAオペレーションおよびFSWとの相互作用のすべてのもっともらしいハザードに関する議論	ST			MEXECとASTERIAオペレーションまたはFSWとの相互作用のすべてのもっともらしい危険性が特定されました	G	(e)合わせ技	property		
																MEXECとASTERIAOperationsまたはFSWとの相互作用は、特定されたすべてのもっともらしい相互作用の危険から安全です。	G				
								MEXECで再計画されたtastnetは安全に実行できます	G			ASTERIA実験でMEXEC再計画が無効になっている	G	(d)視点変換	property						
				MEXECは、セマンティクスごとにタスクネットを実行します	G			初期実験で使用されたタスクネットセマンティックコンストラクトに関する議論	ST	(f)MECE	property	MEXECは、セマンティクスに従ってシーケンスを実行します	G	(f)MECE	property	ASTERIAテストベッドでのテスト	G	(c)基準化	property		
												MEXECは、セマンティクスに従って開始/終了時刻でタスクネットを実行します	G			ASTERIAテストベッドでのテスト	G	(c)基準化	property		
								他のタスクネットセマンティック構造（連続性、制約、並列タスクなど）に対する議論	ST			ASTERIAの初期実験ではこれらのコンストラクトを使用しません	G	(c)基準化	property	実験のタスクネットの検査	G	(c)基準化	property		

		第１階層		第２階層				第３階層				第４階層				第５階層				引用元	
検索	番号	内容	ノード	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象	内容	ノード	パターン	対象		
3	41	G1 自律走行中の滑走路横方向のオーバーアンのリスクは許容レベルです	G	S1 リスクの構成要素に関する分解	ST	(e)合わせ技	property	G3 横方向の滑走路の逸脱の可能性は許容できるほど低い	G	(c)基準化	property	S6 精製	ST			G12 緊急ブレーキの信頼性は許容範囲内です		(f)MECE	property	[102]	Figure 1
																G11 緊急ブレーキがいつでもオンデマンドで利用できない可能性は許容範囲内です					
																G10 真のクロストラックエラー（CTE）≧任意のギベン時間で許容される横方向オフセットの確率は許容できるほど低い					
				S2 ハザード軽減へのアピール	ST			G2 「滑走路の中心線からの航空機の逸脱が許容される横方向のオフセットを超える」という危険は十分に軽減されます	G	(c)基準化	property	S3 ハザードの原因による分解	ST	(e)合わせ技	property	G9 「コントローラーが不要なときに航空機を操縦する」という条件は十分に緩和されています	G	(d)視点変換	property		
												S4 中心線のずれの予防緩和に訴える	ST			G5 航空機が中心線からの許容される横方向のオフセットを超えないようにするための緩和策があります	G	(e)合わせ技	property		
																G8 中心線からの最大横方向オフセットの違反を防ぐための緩和策は、個別におよび集合的に効果的で信頼性があります	G				
				S5 滑走路オーバーランの防止緩和に訴える	ST			G4 航空機が滑走路のサイドストライプや舗装を横切るのを防ぐための緩和策があります	G	(e)合わせ技	property										
								G6 航空機の横方向の滑走路のオーバーランを防ぐための緩和策は、個別におよび集合的に効果的です	G												
								G7 横方向の滑走路のオーバーランを防ぐための緩和策は、オンデマンドで利用できます	G												

以上