Integrating STPA into an Automotive Digital Engineering Process

MBSE Strategy, ISO/IEC/IEEE 15288, ISO 26262, ISO/SAE 21434

David Hetherington

Mark Vernacchia (STPA Task Force)

Ikue Warren (STPA Task Force – Japanese Language Advice)

 |

T1 - Welcome

Agenda for the session.

Today's Lecture

T1 - Welcome

Id	Name	Text
T1	Welcome	Agenda for the session
T2	Introductions - Instructor	Personal introduction by the instructor
T3	Digital Thread	Brief discussion of the digital thread in a realistic development organization
T3	MBSE Strategy	How do we adapt different kinds of MBSE tools for STPA?
T4	ISO/IEC/IEEE 15288	The overall systems engineering workflow
T5	ISO 26262	Integrating STPA into the ISO 26262 functional safety flow
T6	ISO/SAE 21434	Integrating STPA into the ISO/SAE 21434 cybersecurity flow
T7	SAE STPA Task Force	Update on the SAE STPA Task Force standards and recommended practices
T8	Questions	Question and answer session

 |

T2 - Introductions - Instructor

Personal introduction by the instructor.

自己紹介

Leaving Pearl Harbor, May 2018

T2 - Introductions - Instructor

May 1, 2018. David Hetherington with US Navy nuclear officer Ryan Hetherington on the deck of the USS Theodore Roosevelt (CVN-71) pulling out of Pearl Harbor during a “Tiger Cruise” to San Diego.

2018年5月1日。デイビッド・ヘザリントンと米海軍の原子力将校ライアン・ヘザリントンが、真珠湾からサンディエゴへの「タイガークルーズ」で出航中のUSSセオドア・ルーズベルト（CVN-71）の甲板に座っている。

Multiple Roles

T2 - Introductions - Instructor

ヘサリントン友子

David Hetherington

Until Year End 2025

System Strategy, Inc
dhetherington@systemxi.com
Boutique MBSE Consultancy
~20 people
Defense/Commercial

Asatte Press, Inc
David.Hetherington@asattepress.com
Publishing
2 people / 5 authors

Industry Groups
David_Hetherington@ieee.org
Standards, Industry Working Groups

 |

STPA Task Force

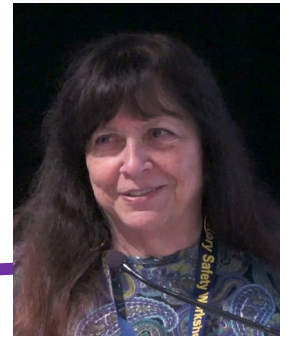
T2 - Introductions - Instructor

INCOSE Automotive Working Group

SAE STPA Task Force

Mark Vernacchia
GM (Retired)
Chair of SAE
STPA Task Force

John Thomas, MIT
Author of STPA Handbook



Nancy Leveson
Professor MIT
Author of STPA

Ikue Warren
UL Solutions

David Hetherington
System Strategy, Inc

Security Subgroup

William “Dollar” Young
Author of STPA-Sec

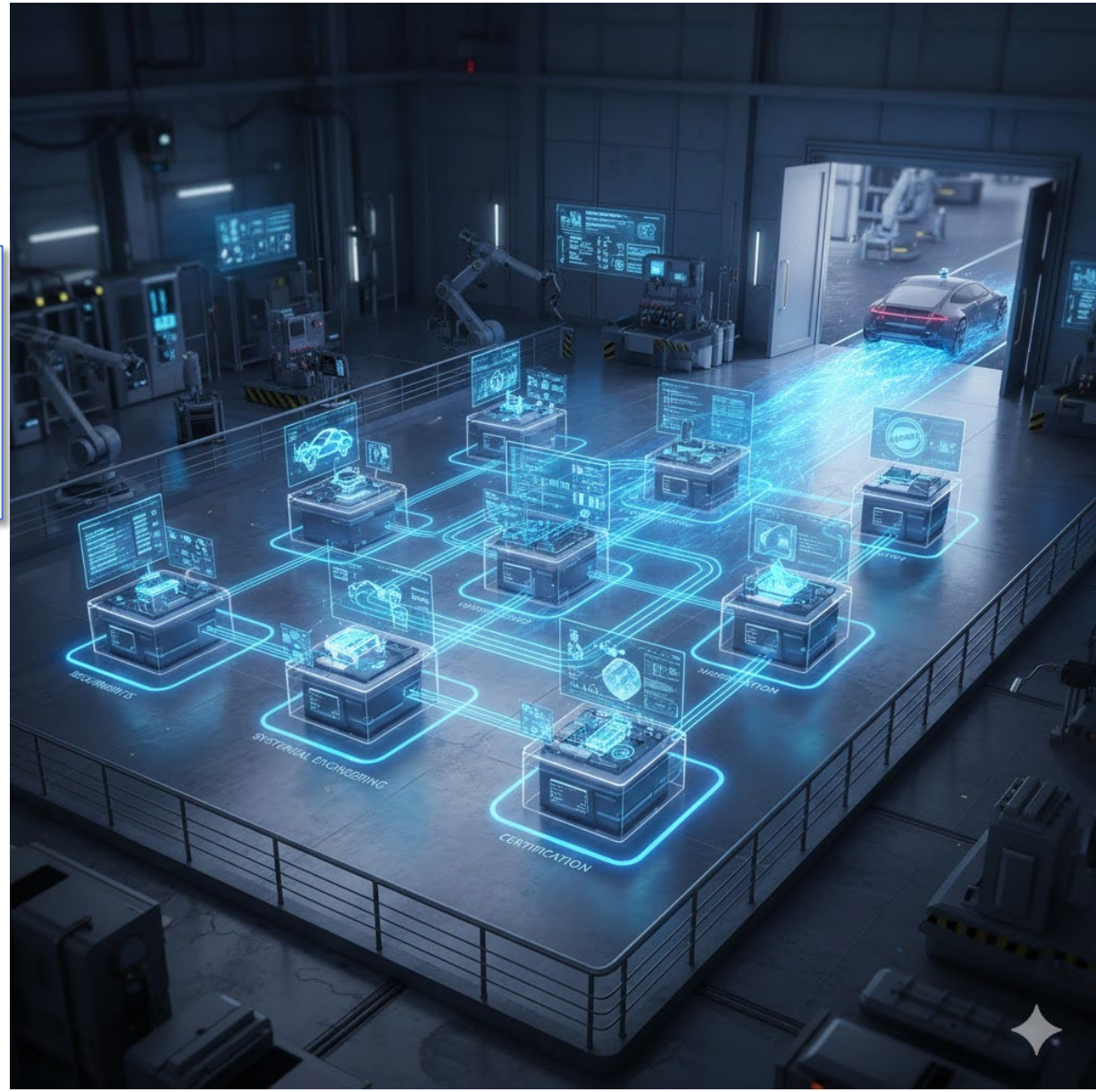
The STPA Task Force publishes SAE J3187 STPA Best Practices and the SAE J3307 STPA Standard. There is a significant overlap with INCOSE AWG.

STPA タスクフォースは、SAE J3187 STPA ベスト プラクティスと、SAE J3307 STPA 標準を公開します。INCOSE AWG と大幅に重複しています。

T3 - Digital Thread

Brief discussion of the digital thread in a realistic development organization.

現実的な開発組織におけるデジタル スレッドについて簡単に説明します。



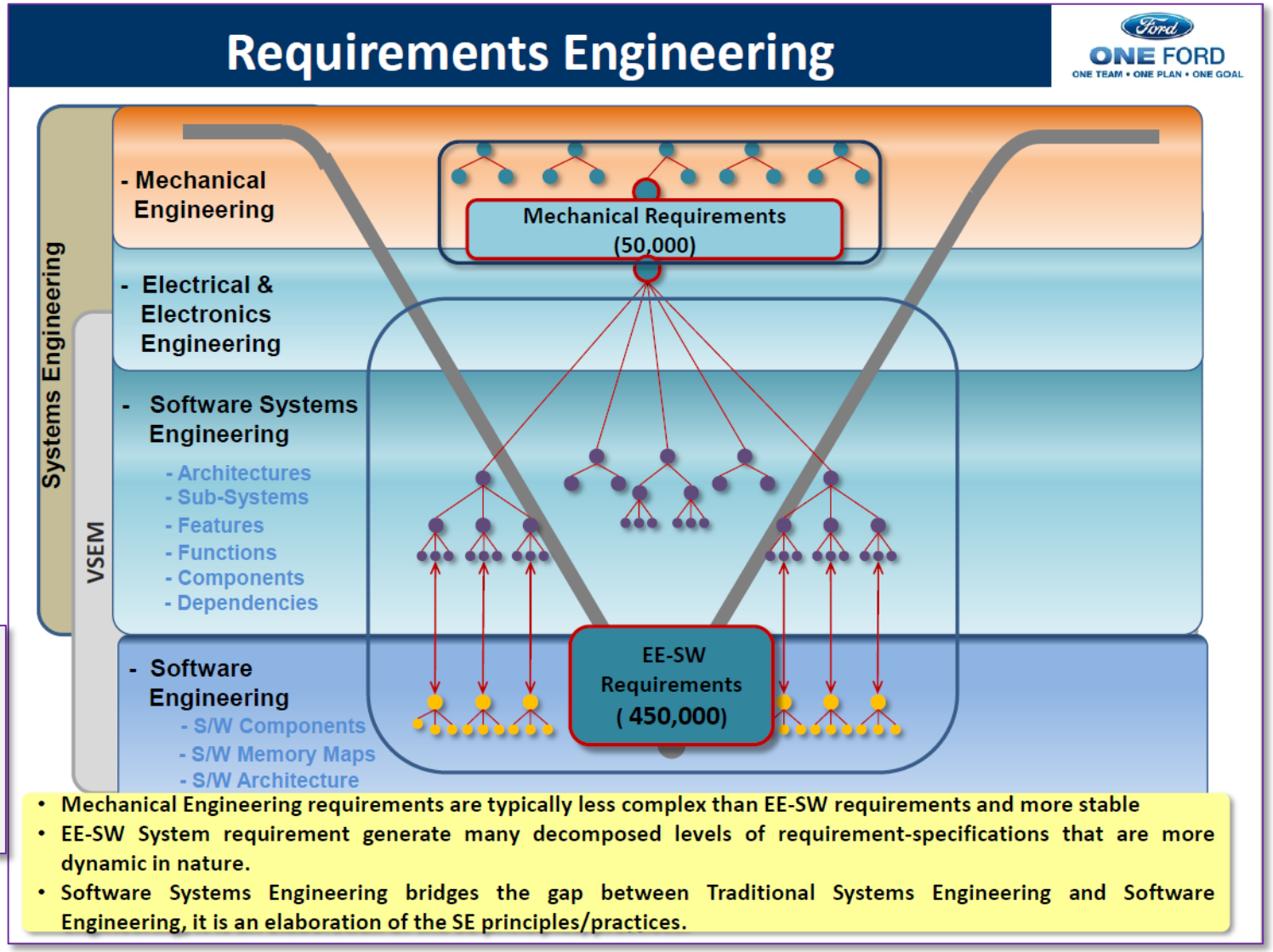
First – The Requirements

T3 - Digital Thread

The aggregate total of the number of requirements needed to fully design a car is far too large to handle effectively only with spreadsheets and clipboards.

自動車を完全に設計するために必要な要件の総数は、スプレッドシートとクリップボードだけで効率的に処理するには大きすぎます。

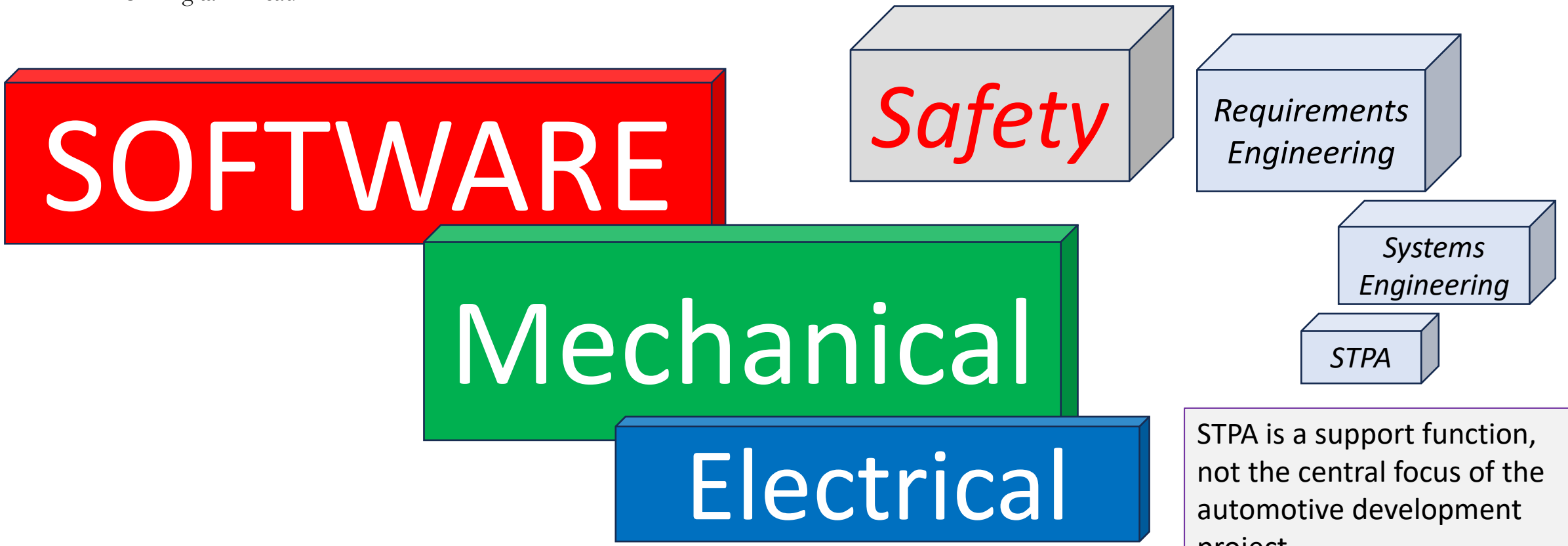
Automotive Software Systems Complexity: Challenges and Opportunities
Christopher Davey
Senior Technical Leader
Software & Control Systems Engineering
Global EE Systems Engineering Group
Ford Motor Company
INCOSE International Workshop MBSE Workshop January 26th-28th, 2013



 |

Relative Weight of Different Automotive Teams

T3 - Digital Thread



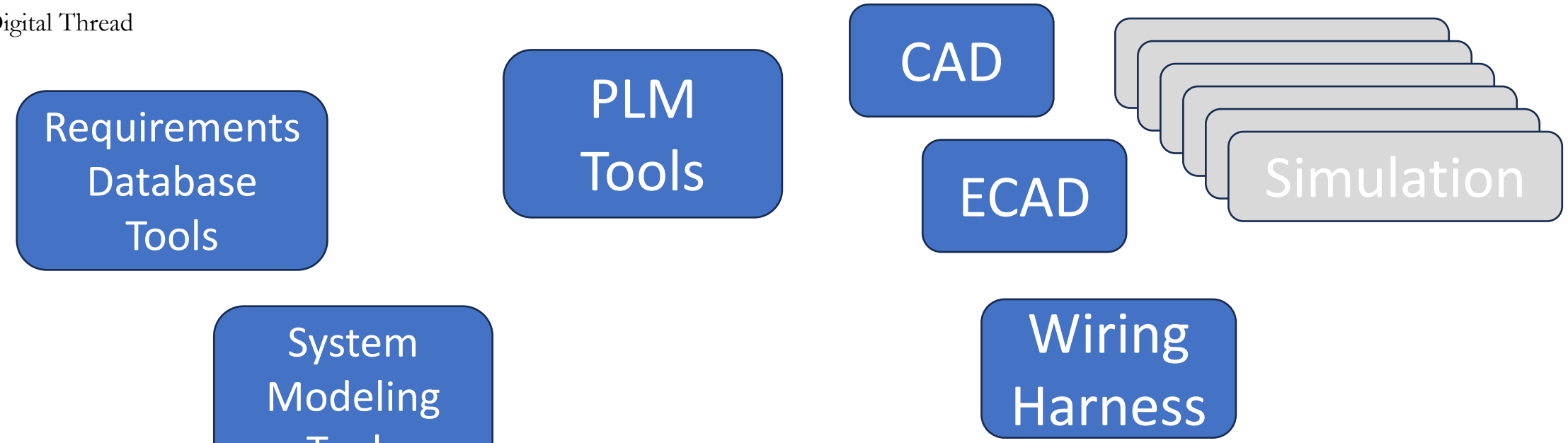
STPA is a support function, not the central focus of the automotive development project.

STPAは自動車開発プロジェクトの中心ではなく、サポート機能です。

 |

Coarse View of Digital Thread

T3 - Digital Thread



Ideally, these should all be integrated by OSLC or by proprietary digital thread tools (Intercax, ReUse Company)

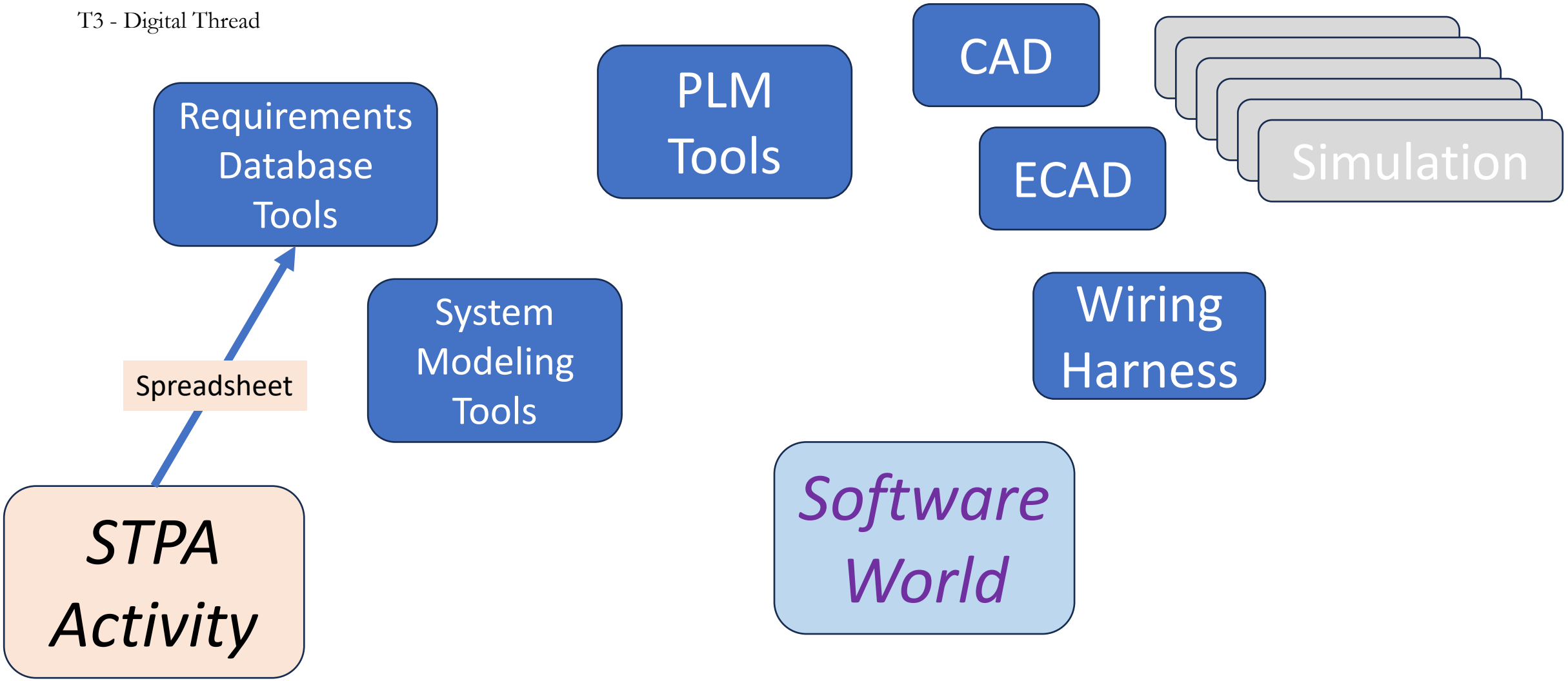
In reality there is a blizzard of spreadsheets flying around.

理想的には、これらはすべて OSLC または独自のデジタル スレッド ツール (Intercax、ReUse Company) によって統合される必要があります。

現実には、スプレッドシートが大量に飛び交っています。

STPA – Probably Current Approach

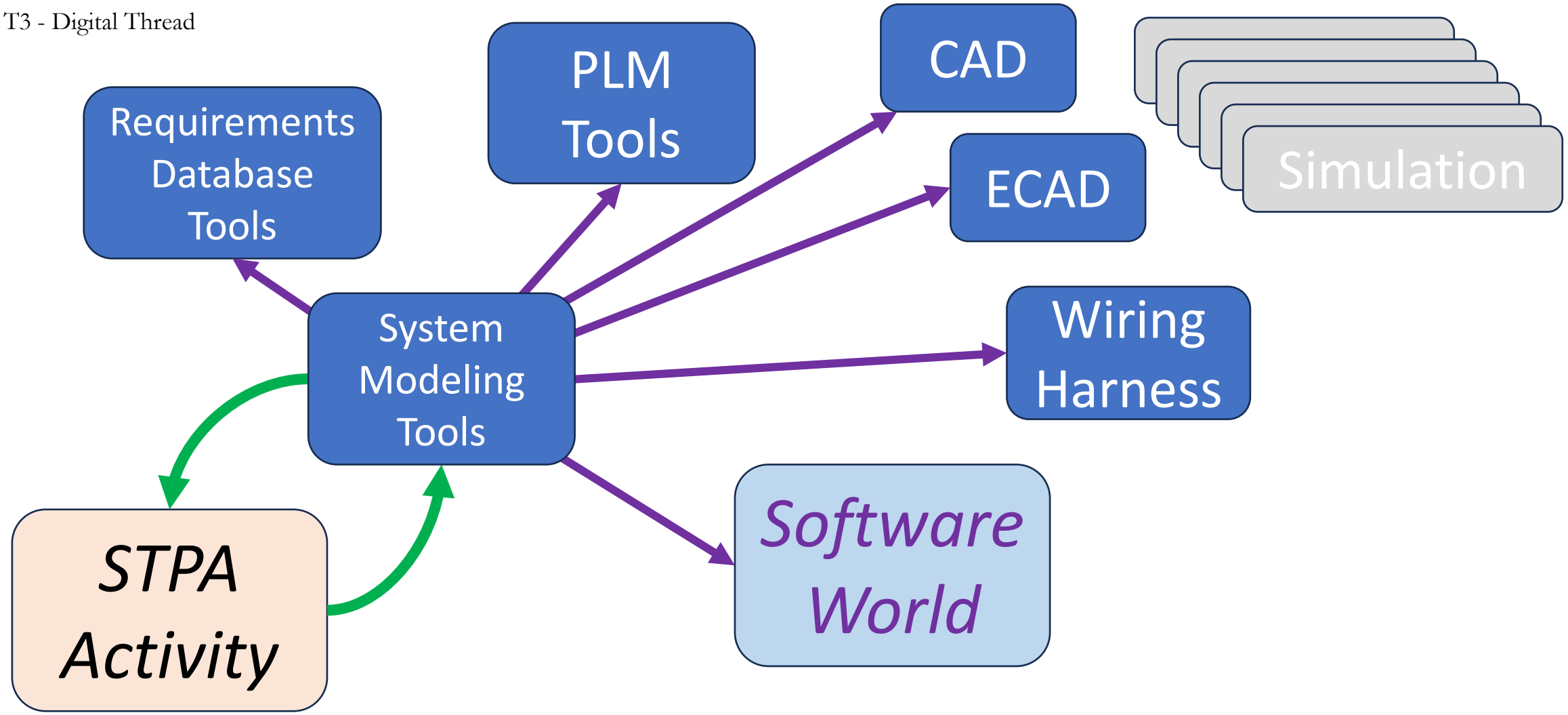
T3 - Digital Thread



 |

STPA – Better Approach

T3 - Digital Thread



 |

T3 - MBSE Strategy

How do we adapt different kinds of MBSE tools for STPA?

さまざまな種類の MBSE ツールを STPA にどのように適応させるのでしょうか?

MBSE Tools and Languages?

SysML V1.x

We will look at this in more detail in this presentation.

SysML V2

At least two efforts are underway here.

Arcadia/Capella

Contact me for my presentation from ERTS2022.

The general approach for these will be similar although the underlying details will be different.

これらに対する一般的なアプローチは似ているが、根本的な詳細は異なる。.

Purpose-Built Tools

At least VWAY and Change Vision have commercial tools available.

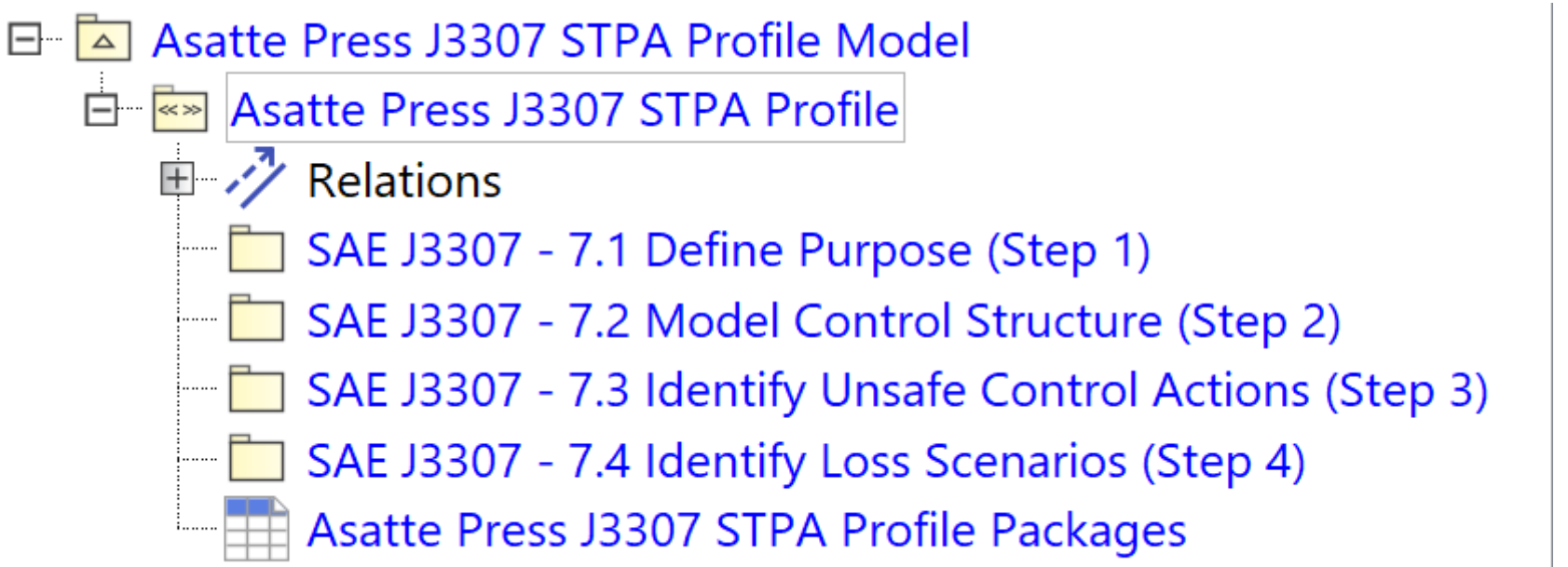
 |

SysML V1 – Create a Profile

For SysML V1, we will want to create a model containing a UML profile.

The UML profile is itself a special kind of package and can contain other packages.

In order to keep the profile neat and understandable, I recommend creating a package (and profile diagram) for each STPA step.



SysML V1 の場合、UML プロファイルを含むモデルを作成する必要があります。

UML プロファイル自体は特別な種類のパッケージであり、他のパッケージを含めることができます。

プロファイルを整理してわかりやすくするために、STPA ステップごとにパッケージ (およびプロファイル図) を作成することをお勧めします。

 |

A Simple Example System

T3 - MBSE Strategy

In order to demonstrate the look of an actual SysML model using the profile, we will introduce a simple example system.

Our example system is the “Asatte Press AI Coffee Vending Machine”.

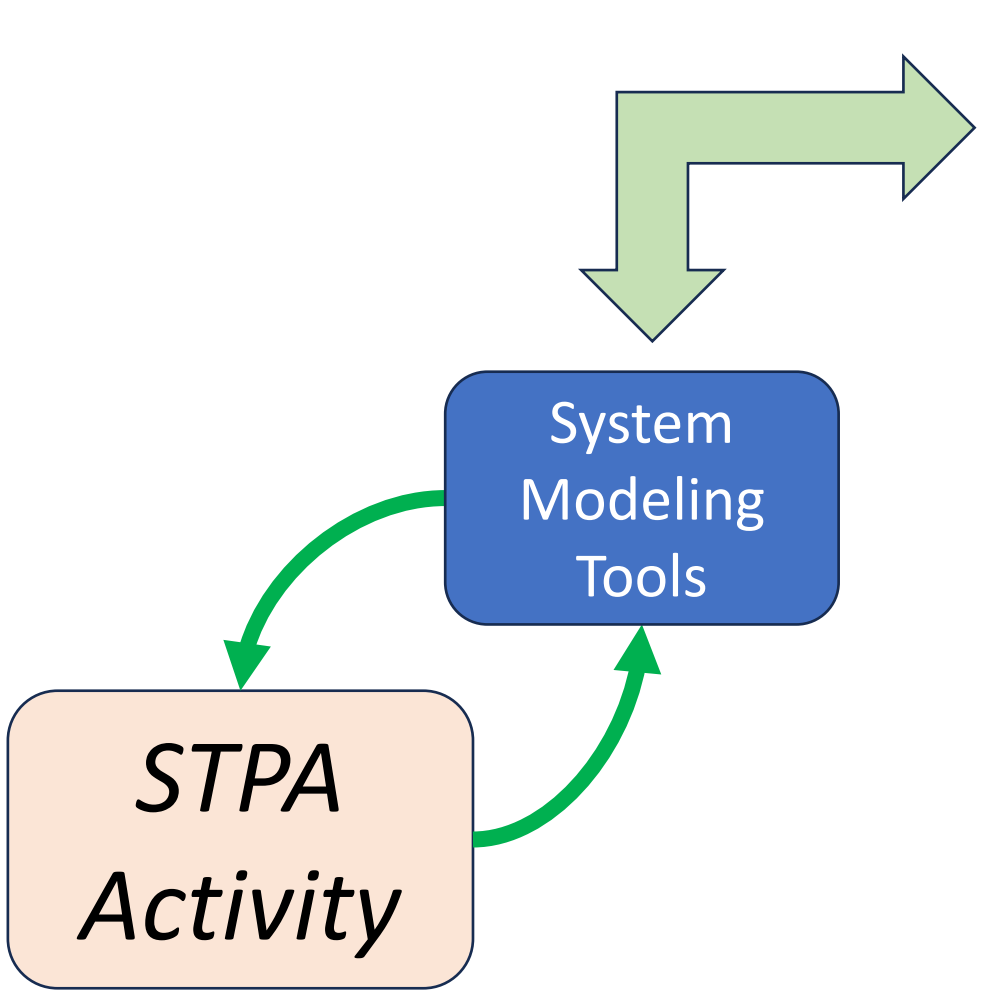
This vending machine does not have any buttons or menus to click. Instead, it converses naturally with approaching customers and prepares their favorite coffee beverage according to the customer's wishes.

Note: This presentation will NOT include a full STPA workup of this system. Instead, the system model will simply show some example views of how the UML profile would be applied in the modeling tool.

「アサッテプレスAIコーヒー自動販売機」には、クリックするボタンやメニューはありません。代わりに、近づいてきたお客様と自然な会話をしながら、お客様の好みに合わせて好みのコーヒードリンクを淹れてくれます。

 |

The Goal is to get to the Requirements Tools



Most MBSE tools (Not just SysML) have a requirement construct.

Most MBSE tools already have gateways to integrate with DOORS, Jama, Visure, etc…

ほとんどの MBSE ツール (SysML だけでなく) には要件構造があります。

ほとんどの MBSE ツールには、DOORS、Jama、Visure などと統合するためのゲートウェイがすでに備わっています。

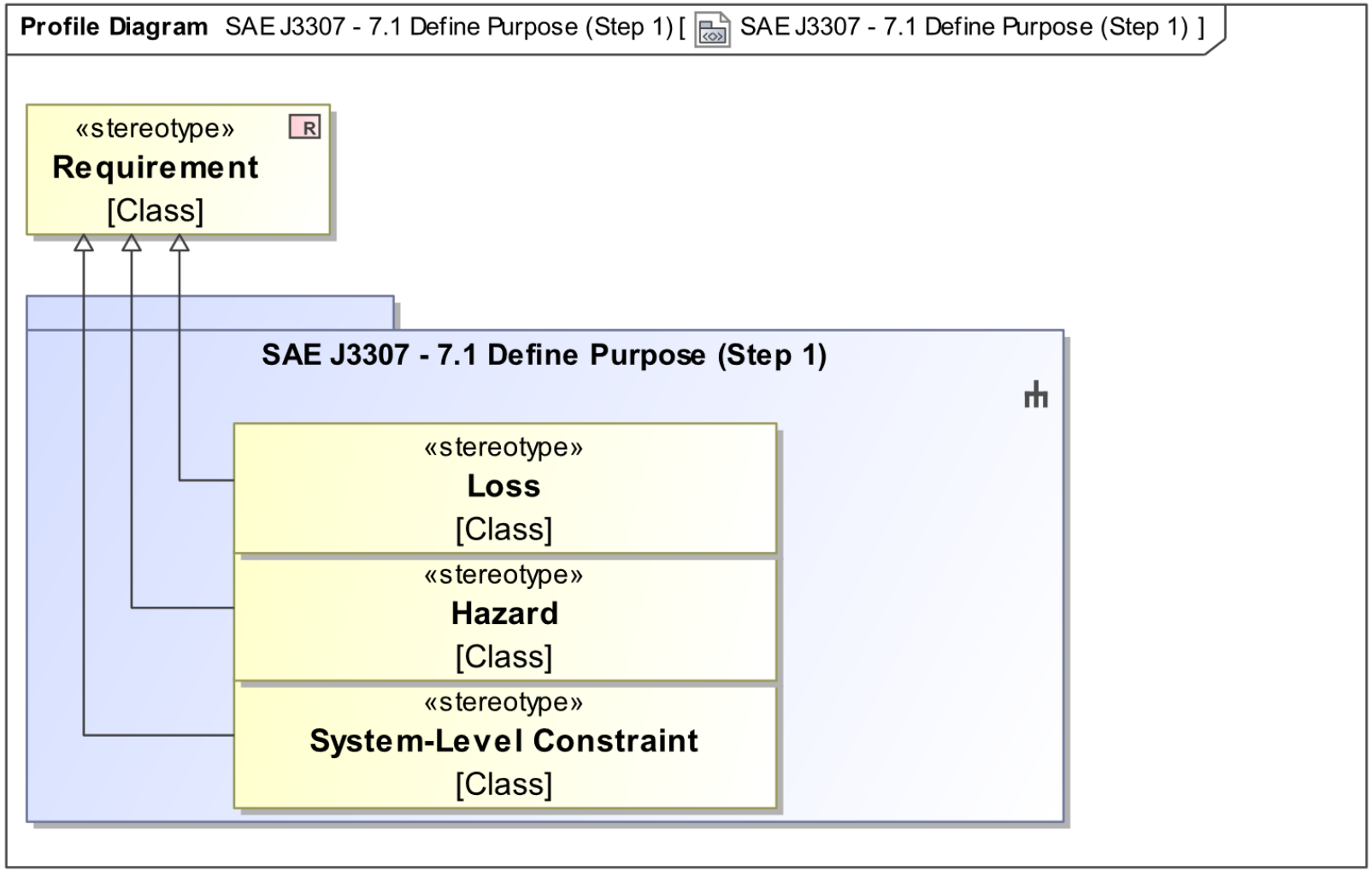
 |

Step 1- Leverage the SysML V1 Requirement

T3 - MBSE Strategy

By identifying losses, hazards, and SysML V1 requirements we automatically benefit from the already existing gateways between the SysML V1 tools and the Requirements Management tools.

損失、危険、SysML V1 要件を特定することで、SysML V1 ツールと要件管理ツール間の既存のゲートウェイのメリットを自動的に享受できます。



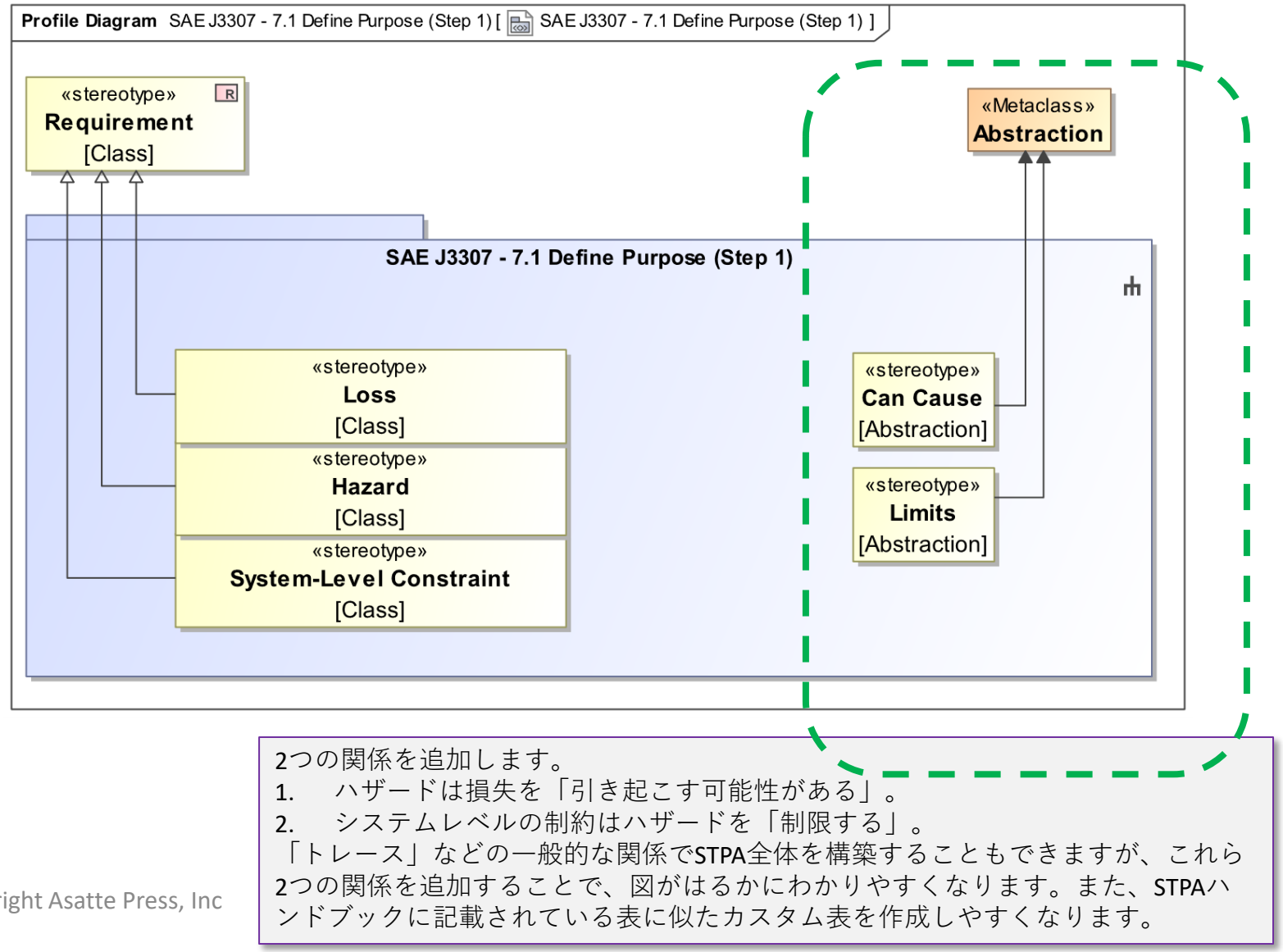
 |

Step 1- Add Two Relationships

T3 - MBSE Strategy

Add two relationships:
1. A hazard “Can Cause” a loss.
2. A system-level constraint “Limits” a hazard.

While one could attempt to construct the entire STPA with generic relationships such as “trace”, these two will make diagrams much more understandable. They will also make it easier to construct custom tables similar to the tables in the STPA handbook.



2つの関係を追加します。
1. ハザードは損失を「引き起こす可能性がある」。
2. システムレベルの制約はハザードを「制限する」。

「トレース」などの一般的な関係でSTPA全体を構築することもできますが、これら2つの関係を追加することで、図がはるかにわかりやすくなります。また、STPAハンドブックに記載されている表に似たカスタム表を作成しやすくなります。

 |

Benefit of Using Requirements

T3 - MBSE Strategy

#	Name	Text
1	H1 Human Exposed to Danger	Any exposure of a human to danger caused by the system.
2	H1.1 Exposure to Scalding Water	Human exposed to scalding water.
3	H1.1.1 Customer exposed to scalding water.	Customer exposed to scalding water.
4	H1.1.2 Service Personnel Exposure to Scalding Water	Service personnel exposed to scalding water.
5	H1.2 Exposure to High Voltage	Human exposed to high voltage.
6	H1.2.1 Customer Exposure to High Voltage	Customer exposed to high voltage.
7	H1.2.2 Service Personnel Exposure to High Voltage	Service personnel exposed to high voltage.

Most SysML tools have convenient features for handling requirements such as automatic hierarchical numbering of nested requirements. These fit the STPA application perfectly.

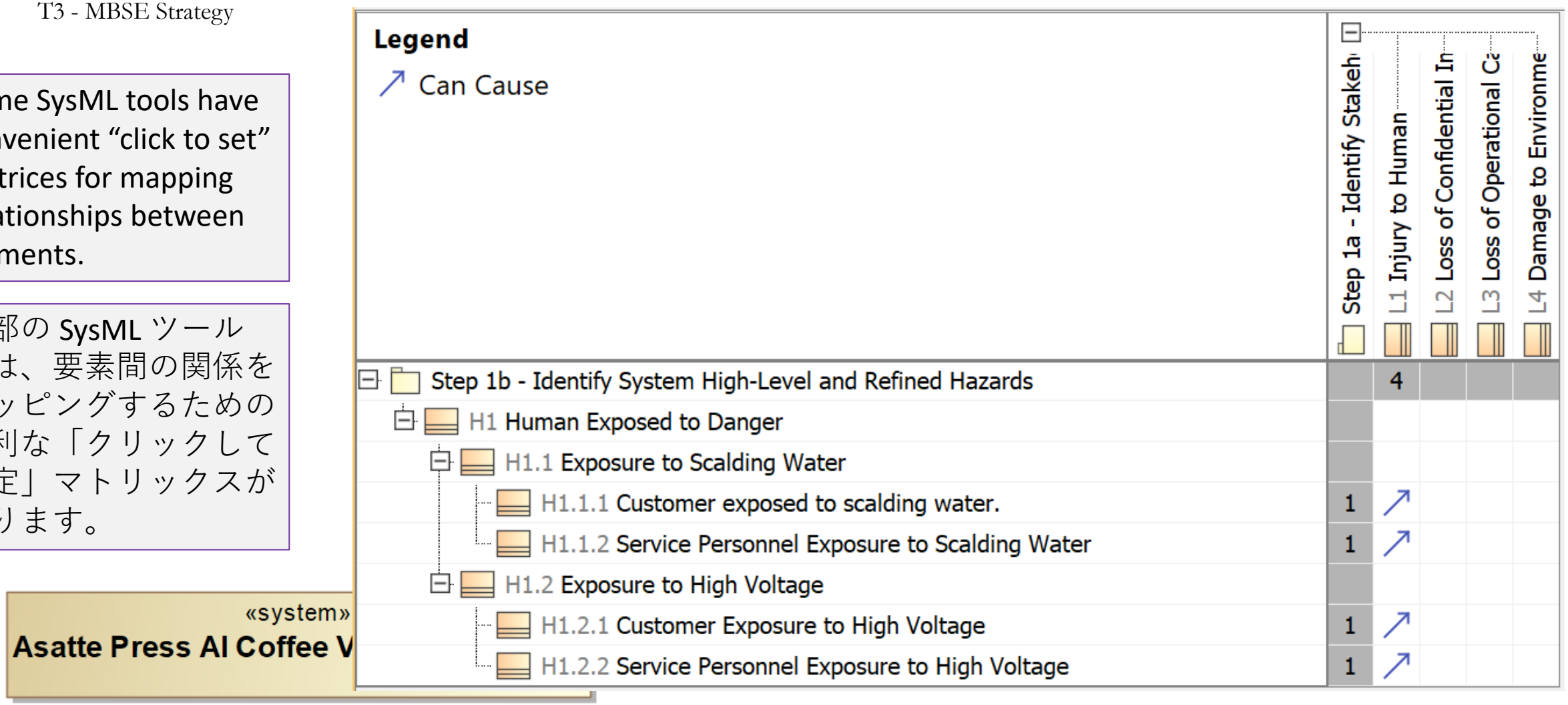
«system»
Asatte Press AI Coffee Vending Machine

ほとんどのSysMLツールには、ネストされた要件の階層的な自動番号付けなど、要件処理に便利な機能が備わっています。これらはSTPAアプリケーションに最適です。

Benefit of Using Requirements

Some SysML tools have convenient “click to set” matrices for mapping relationships between elements.

一部の SysML ツールには、要素間の関係をマッピングするための便利な「クリックして設定」マトリックスがあります。

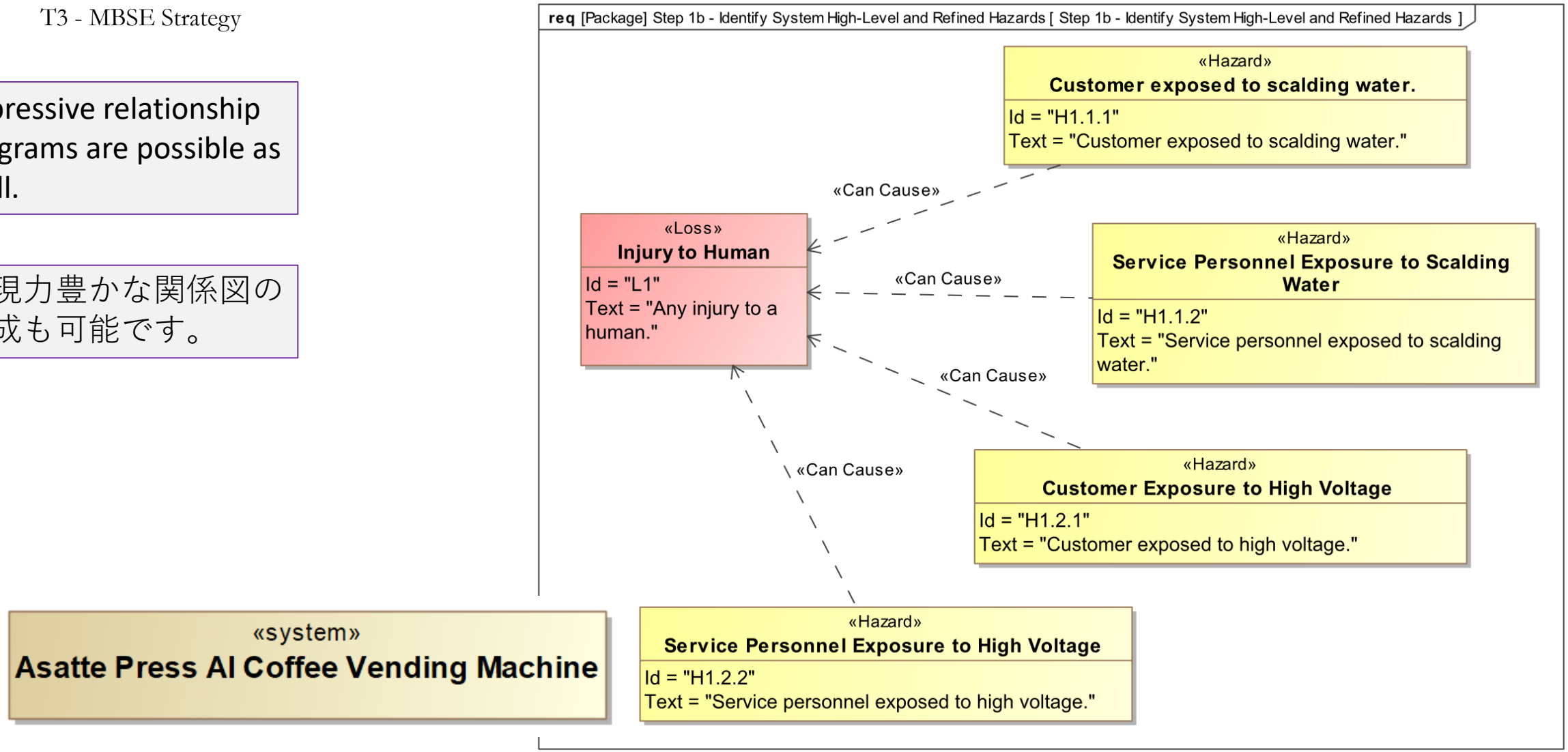


 |

Benefit of Using Requirements

Expressive relationship diagrams are possible as well.

表現力豊かな関係図の作成も可能です。



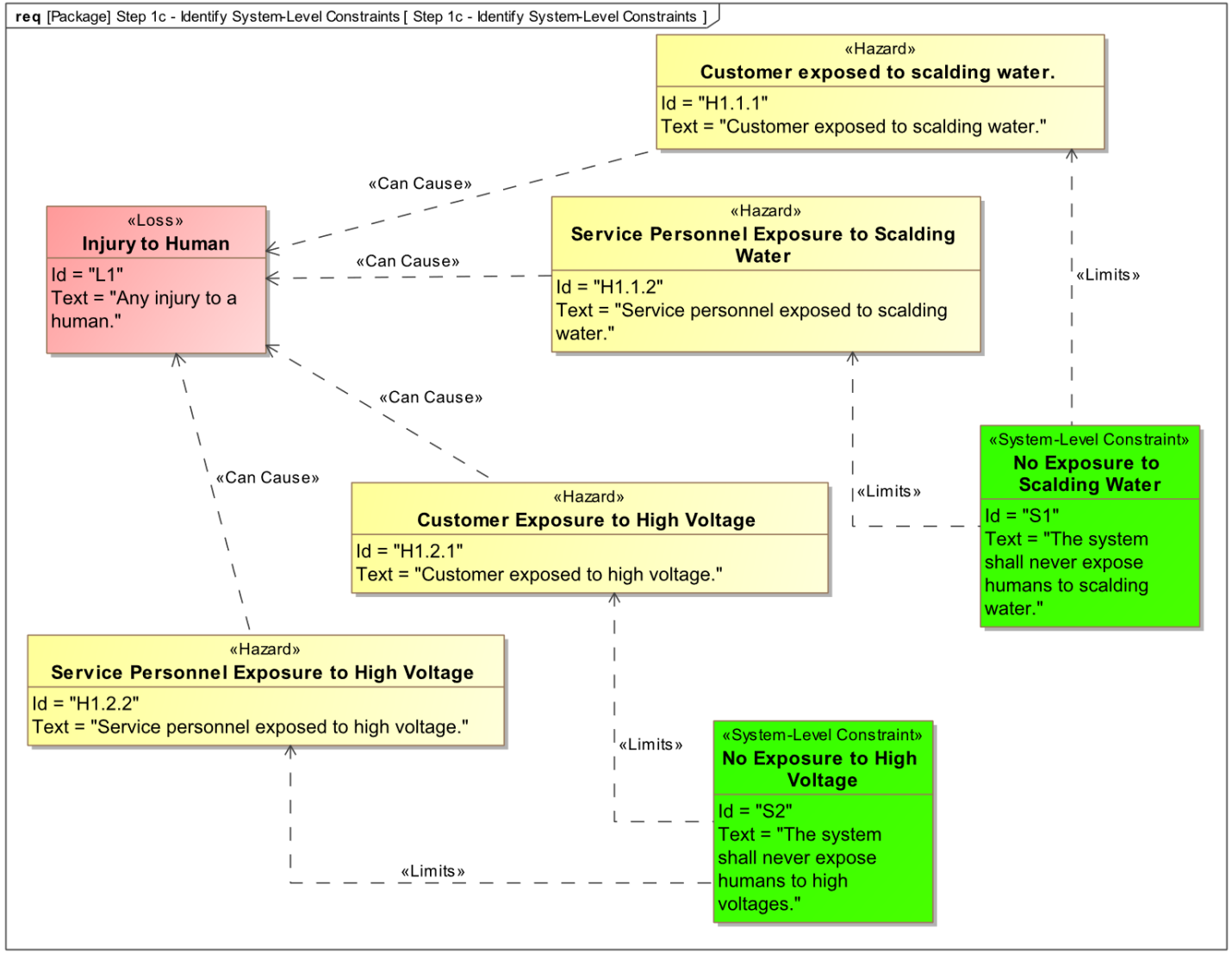
 |

Rounding Out Step 1

T3 - MBSE Strategy

In Step 1c we can create system-level constraints to limit the hazards that could cause losses.

ステップ 1c では、損失を引き起こす可能性のある危険を制限するためにシステム レベルの制約を作成できます。



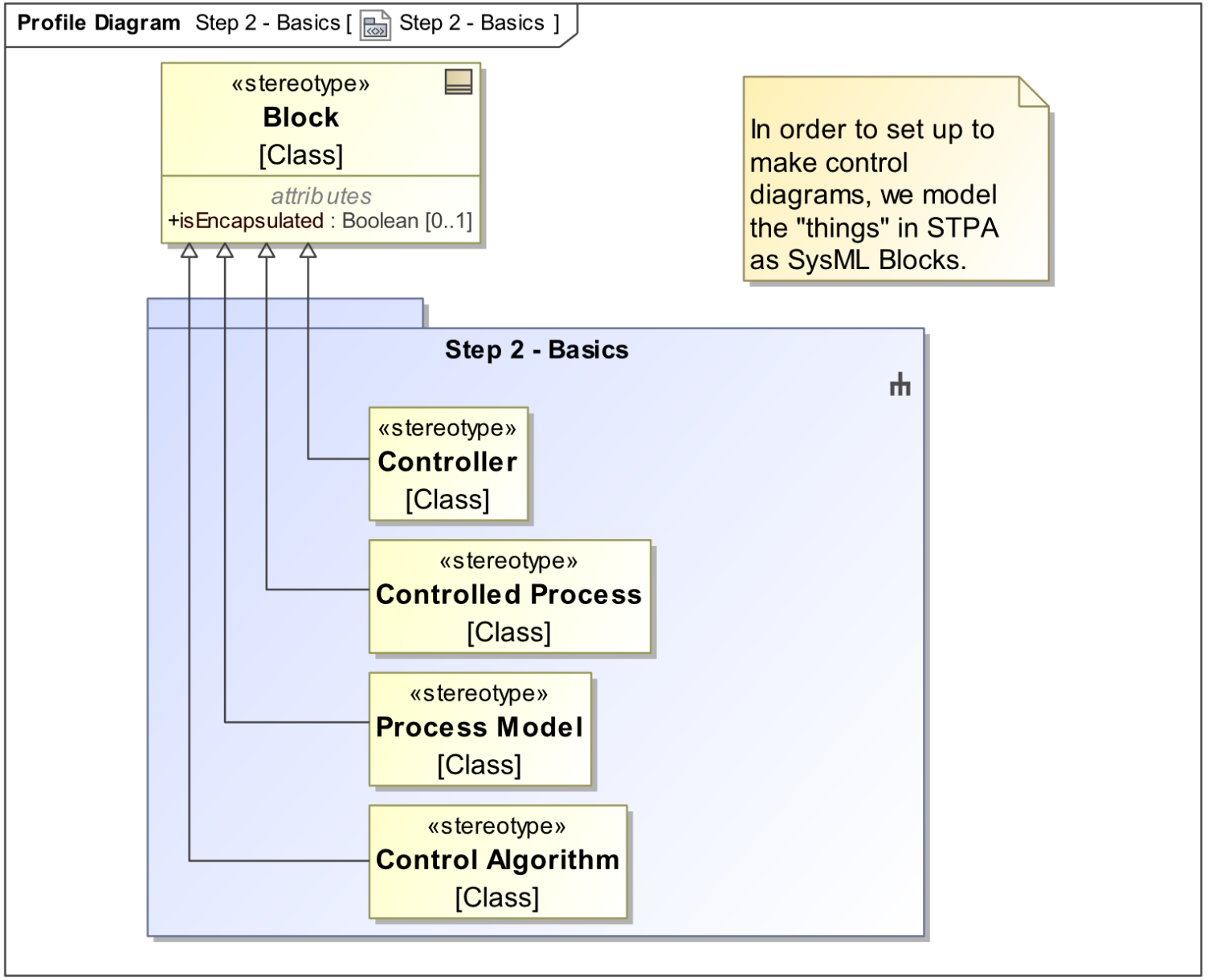
 |

Step 2 - Basics

T3 - MBSE Strategy

STPA Step 2 contains many concepts that need to be modeled. In order to keep the profile readable, we will use multiple profile diagrams to assemble this portion of the profile.

STPAステップ2には、モデル化が必要な概念が多数含まれています。プロファイルを読みやすくするために、この部分は複数のプロファイル図を使用して組み立てます。

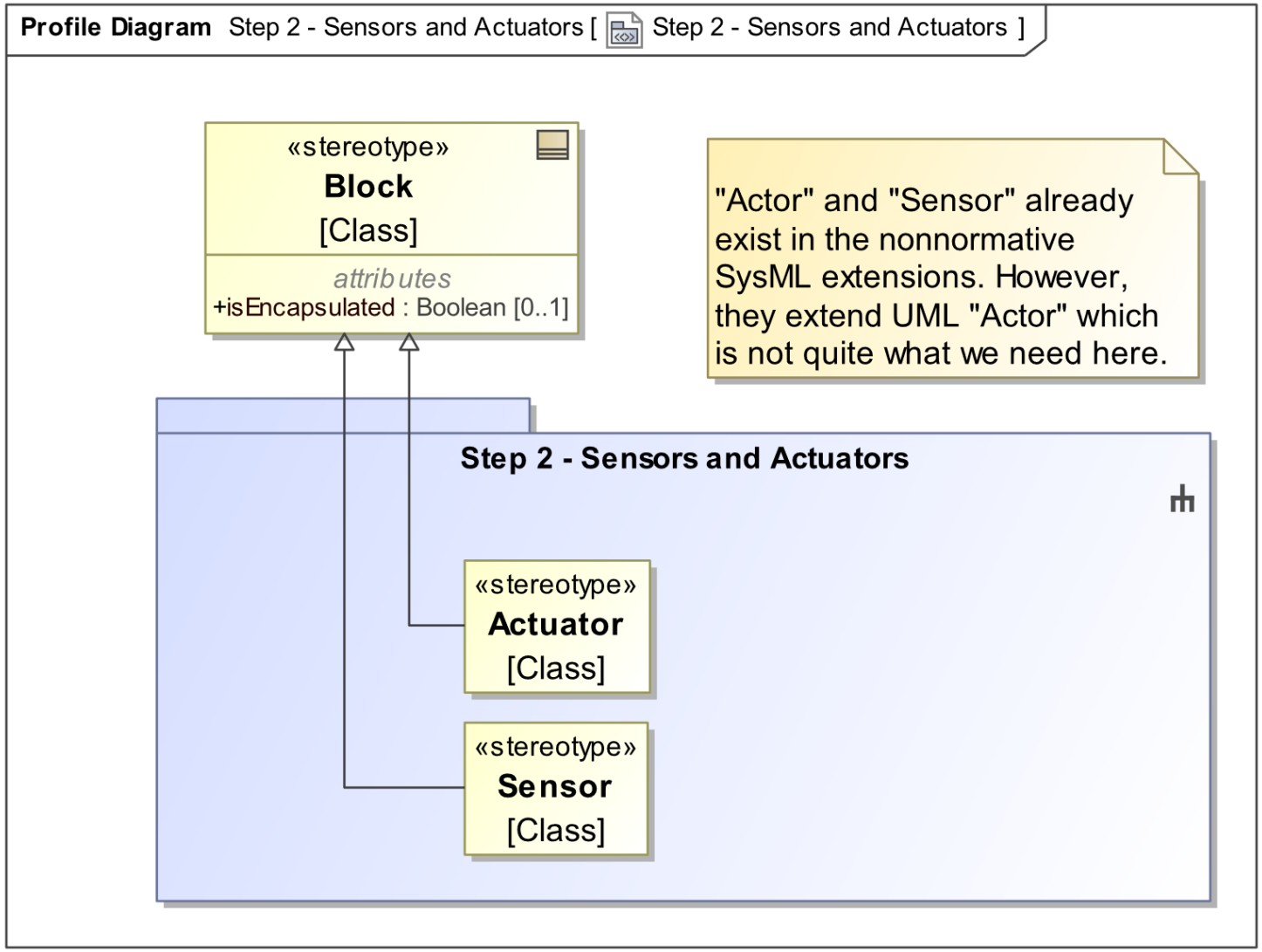


 |

Step 2 – Sensors and Actuators

Sensors and actuators are not sufficiently described (yet) in SAE J3307. In the STPA Handbook they are introduced in Step 2 in footnote 7 on page 25.

センサーとアクチュエータについては、SAE J3307では（まだ）十分に説明されていません。STPAハンドブックでは、25ページの脚注7のステップ2で紹介されています。

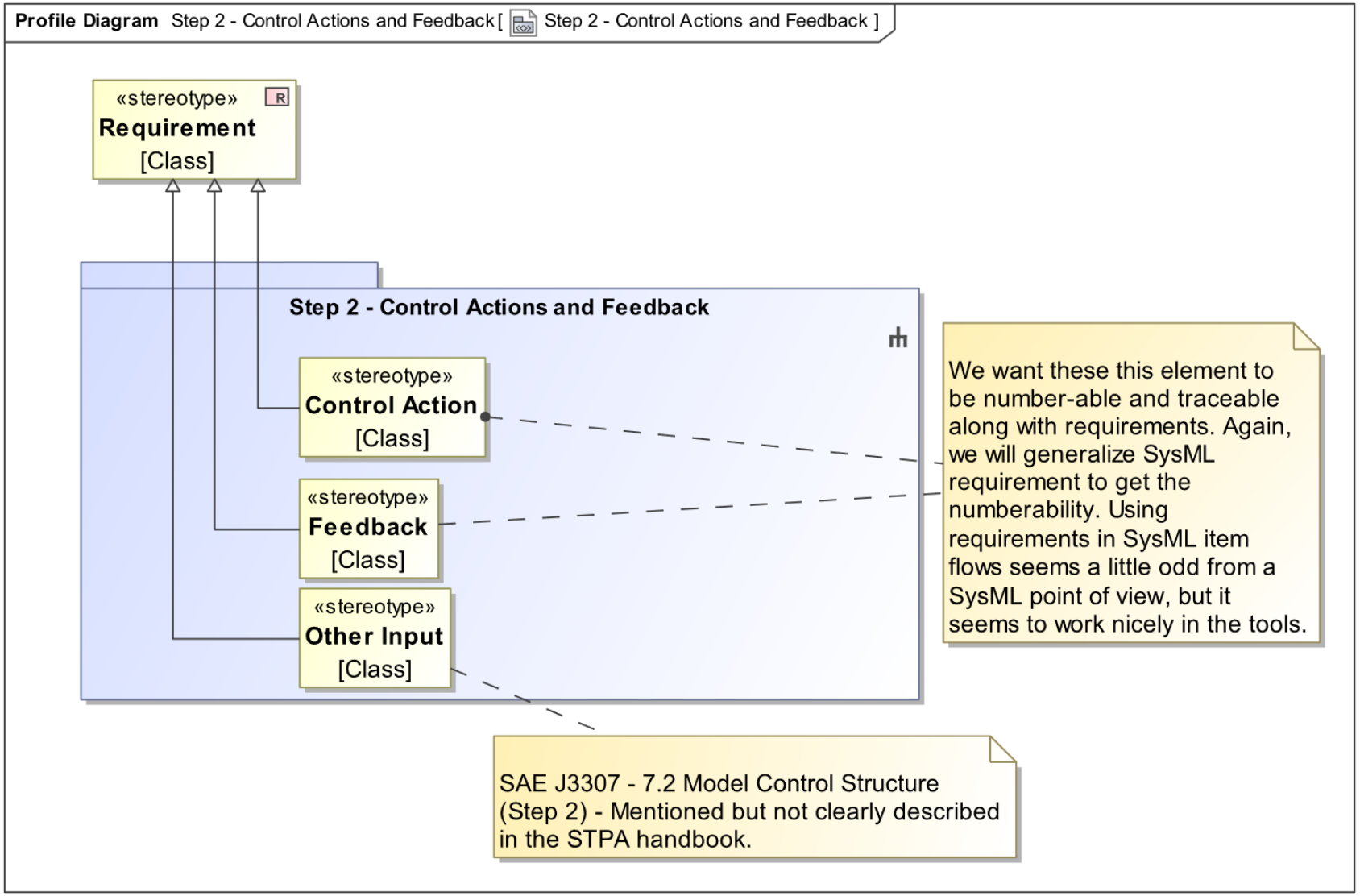


 |

Step 2 – Control Actions and Feedback

Even though we are going to want to use these elements in item flows, we also want the requirements numbering and management. As such we will use “Requirement” rather than “Block”.

これらの要素をアイテムフローで使用する予定ですが、要件の番号付けと管理も必要です。そのため、「ブロック」ではなく「要件」を使用します。



 |

Step 2 – Responsibilities

Finally, we close out Step 2 by modeling the controller responsibilities.

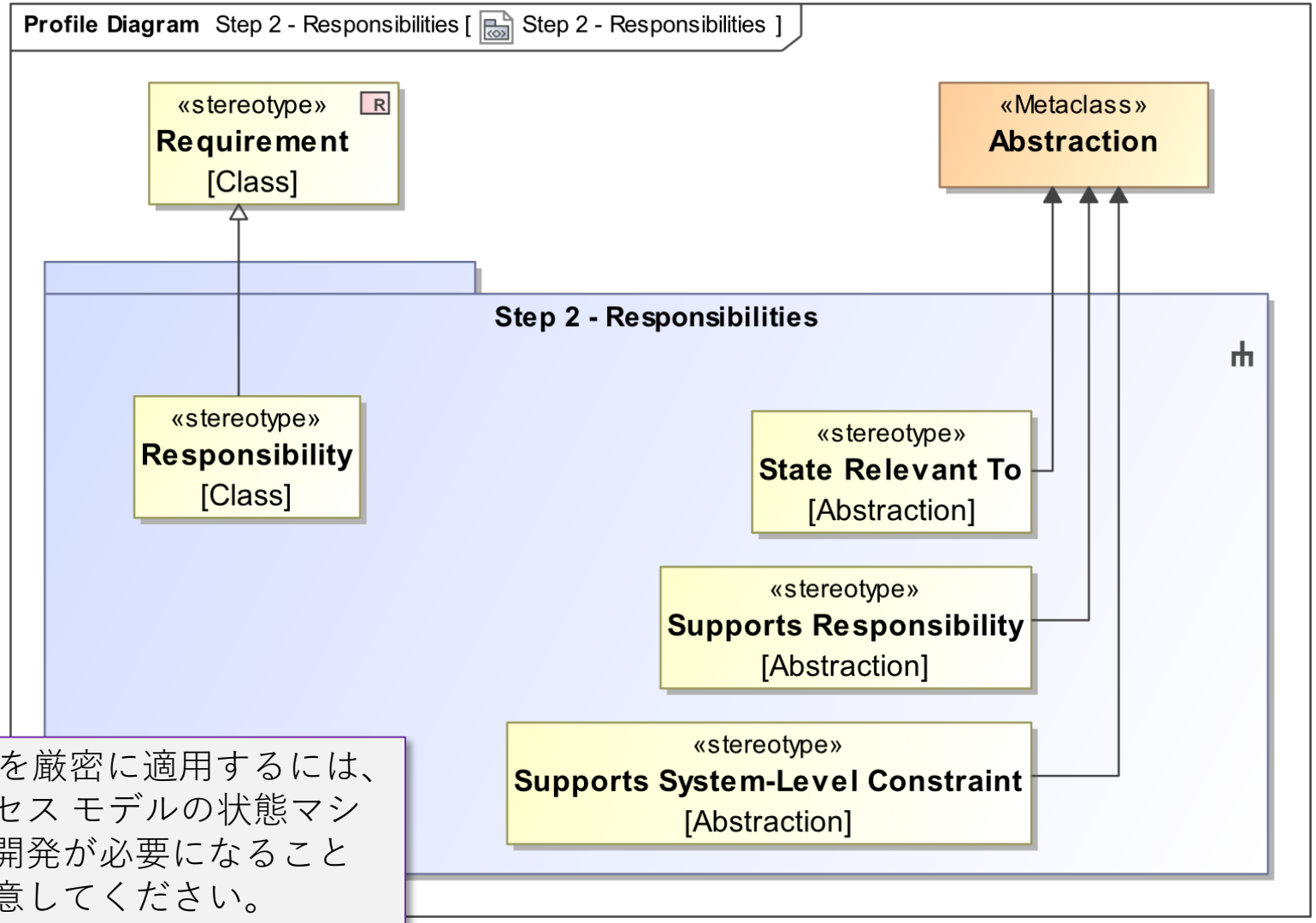
Here we add a few special relationships to support the creation of Table 2-2 on page 30 of the STPA handbook.

Note that a rigorous application of STPA will involve developing state machines for the process models.

最後に、コントローラーの責任をモデル化してステップ 2 を終了します。

ここでは、STPA ハンドブックの 30 ページの表 2-2 の作成をサポートするために、いくつかの特別な関係を追加します。

STPA を厳密に適用するには、プロセス モデルの状態マシンの開発が必要になることに注意してください。



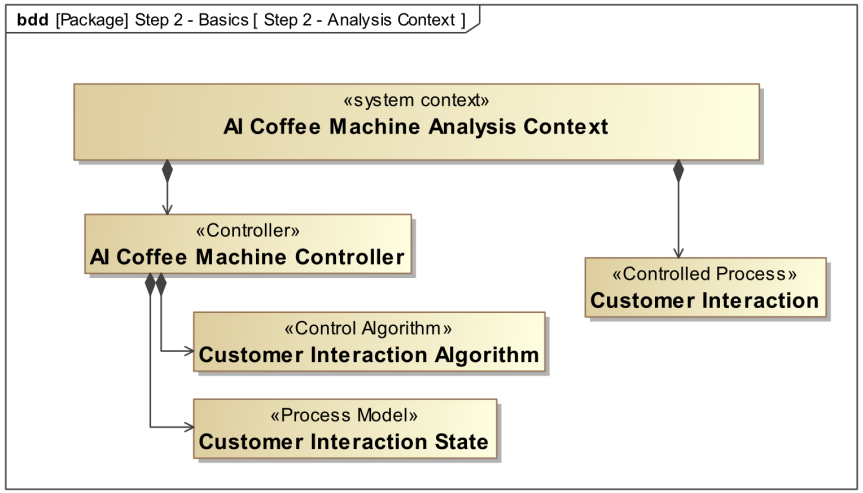
 |

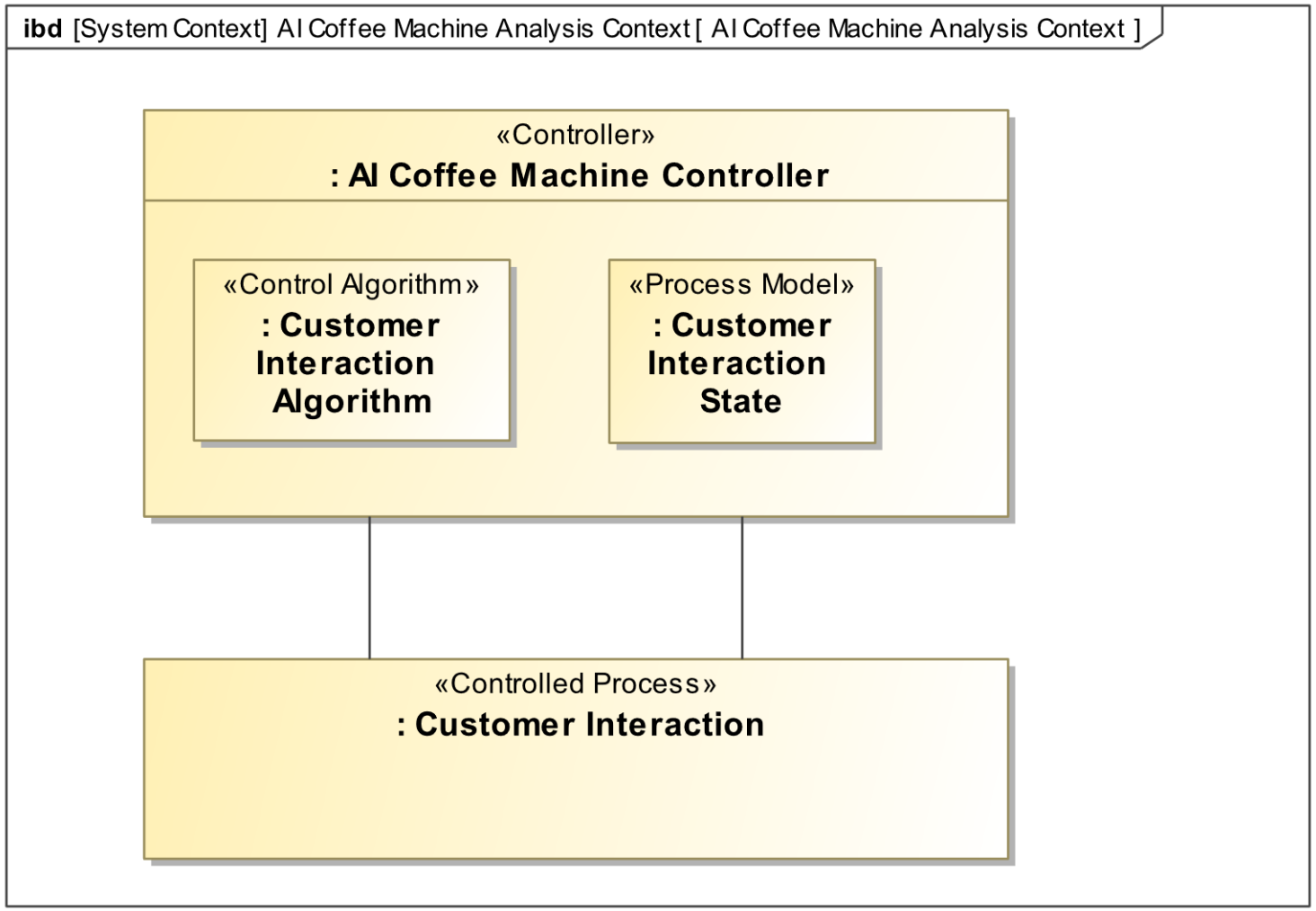
Step 2 – Modeling the Control

T3 - MBSE Strategy

First, we can set up the basic control diagram.

まず、基本的な制御図を設定します。



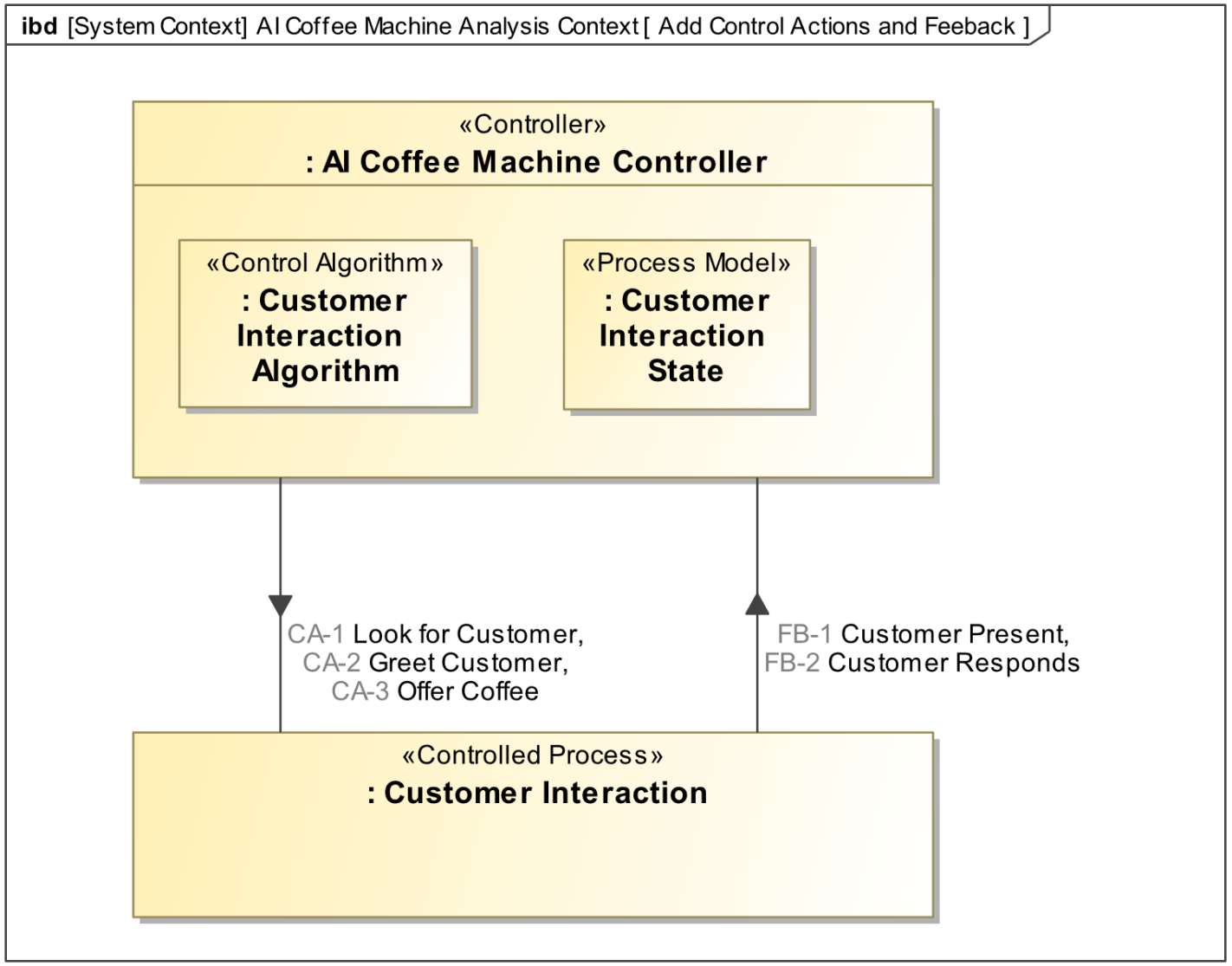


 |

Step 2 – Control Actions and Feedback

Control actions and feedback items can be added and look quite natural.

コントロールアクションとフィードバック項目を追加することができ、見た目も非常に自然です。



 |

Step 2 – Responsibilities

T3 - MBSE Strategy

#	Id	Name	System-Level Constraint	Context (State)	Feedback
1	R-1	Protect from Scalding Water	SC-1 No Exposure to Scalding Water	Handing Product to Customer	FB-10 Liquid Temperature
2	R-2	Protect from High Voltage	SC-2 No Exposure to High Voltage	Handing Product to Customer	FB-15 Ambient Voltage

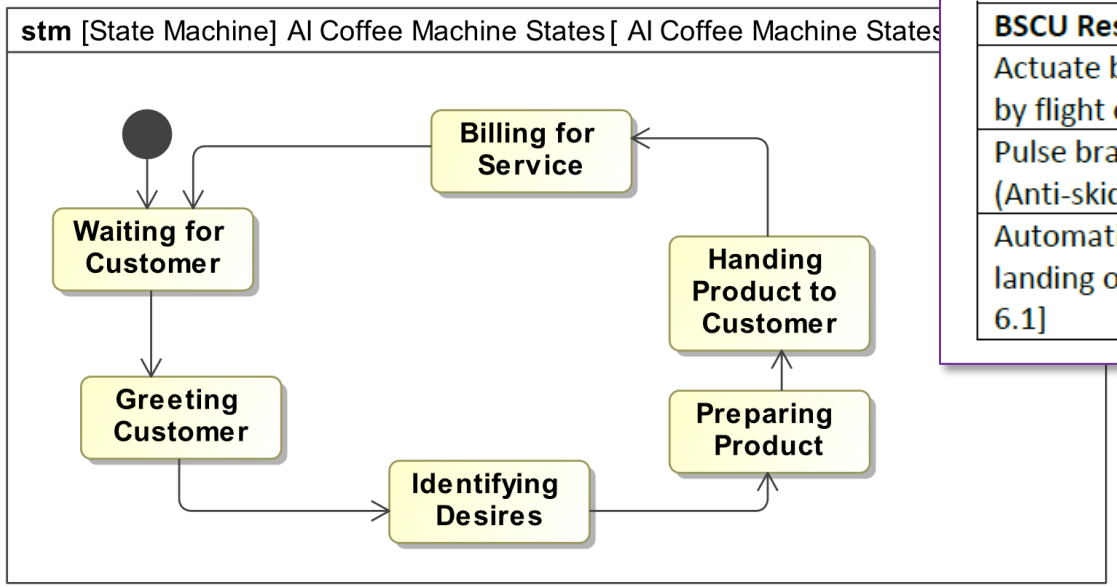


Table 2.2: Examples showing how feedback can be derived from responsibilities

BSCU Responsibility	Process Model	Feedback
Actuate brakes when requested by flight crew [SC-6.1]	Braking is requested by flight crew	Brake pedal applied
Pulse brakes in case of a skid (Anti-skid) [SC-6.2]	Aircraft is skidding	Wheel speeds Inertial reference unit
Automatically engage brakes on landing or RTO (Autobrake) [SC-6.1]	Aircraft landed Takeoff is rejected	Weight on wheels Throttle lever angle

The tool can be used to automatically generate a table similar to Table 2.2 on page 30 of the STPA handbook.

このツールを使用すると、STPA ハンドブックの 30 ページの表 2.2 に類似した表を自動的に生成できます。

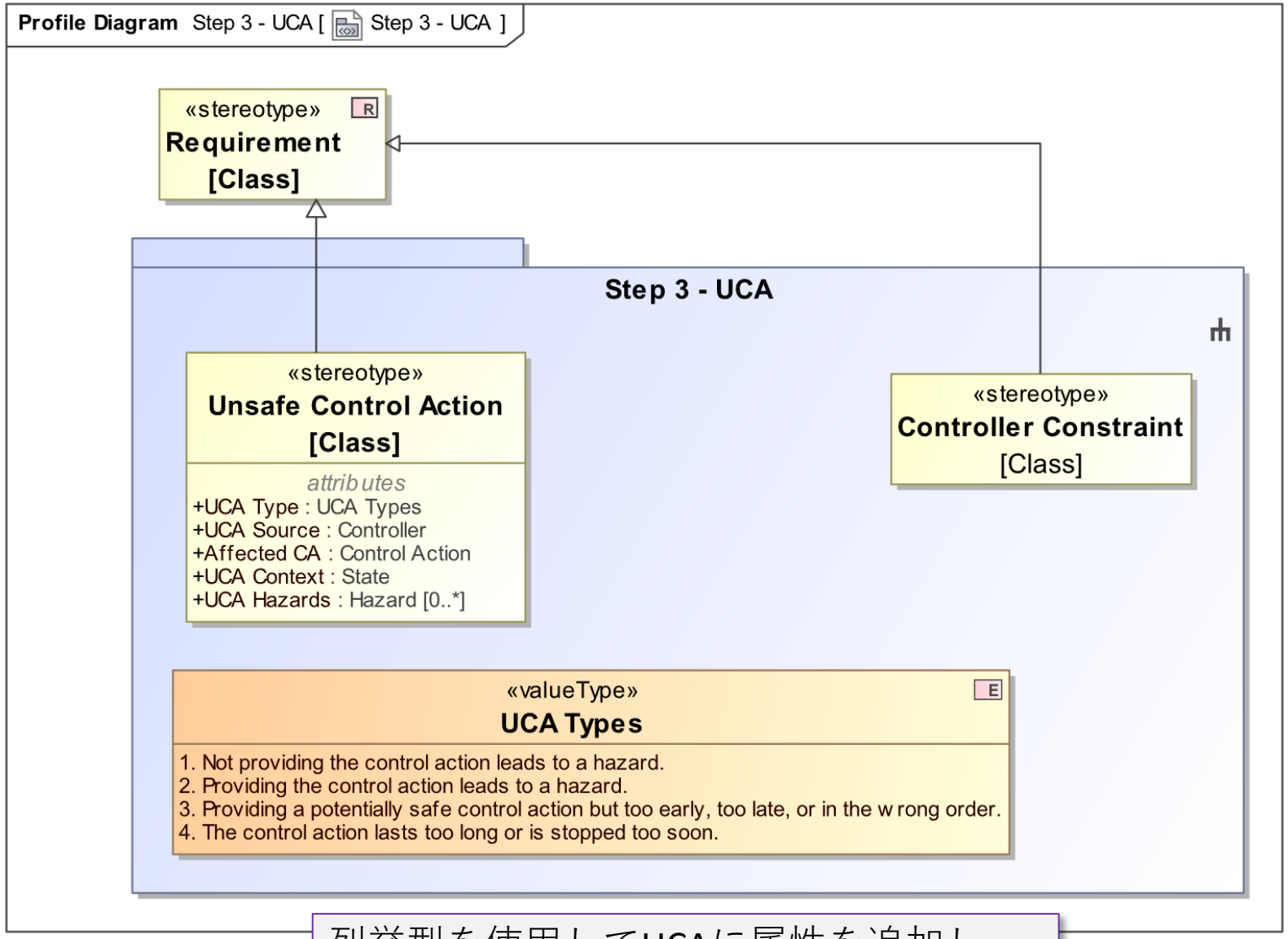
Step 3 – UCA

T3 - MBSE Strategy

We can use an enumeration to add an attribute to the UCA to identify which kind of UCA it is.

Since we need a property to represent the UCA type anyway, we can represent the other relationships by stereotype properties as well.

This approach makes it easy to set attributes directly in a table, but does not support showing relationships in a requirement diagram.



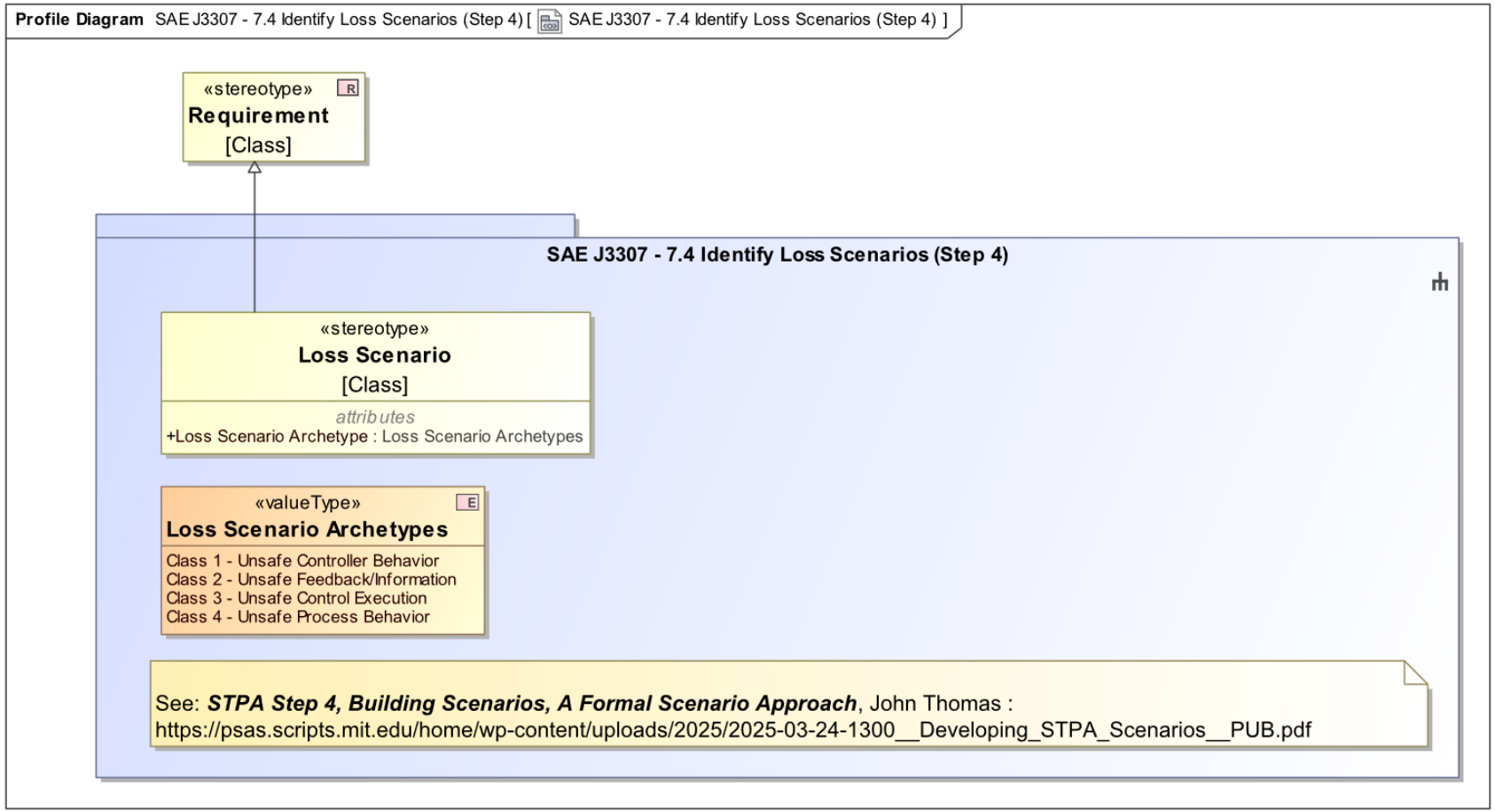
列挙型を使用してUCAに属性を追加し、それがどの種類のUCAであるかを識別することができます。

 |

Step 4 – Loss Scenarios

T3 - MBSE Strategy

今年発表されたジョン・トーマスの改良された損失シナリオ・アプローチを活用しています。



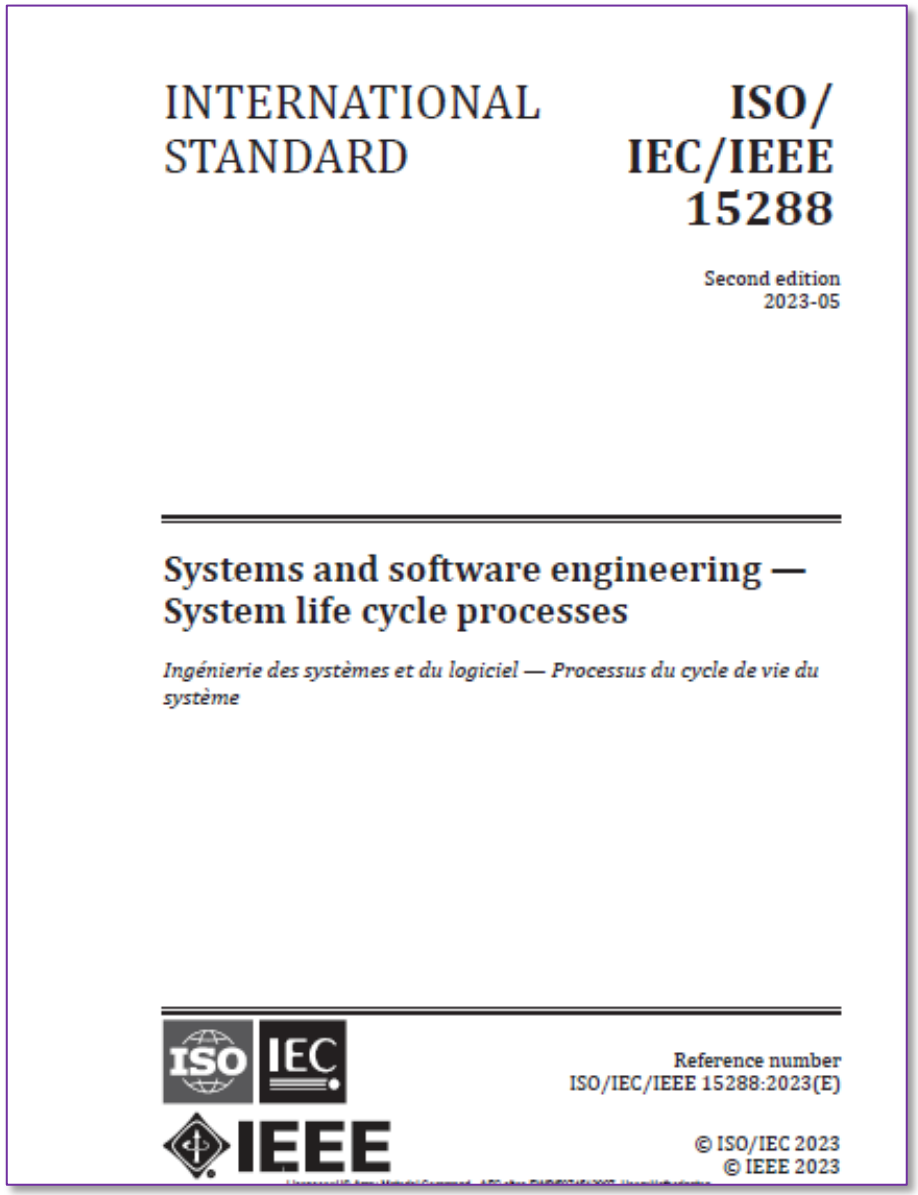
Note that we leverage the improved loss scenario approach:
STPA Step 4, Building Scenarios, A Formal Scenario Approach, John Thomas :
https://psas.scripts.mit.edu/home/wp-content/uploads/2025/2025-03-24-1300__Developing_STPA_Scenarios__PUB.pdf

 |

T4 - ISO/IEC/IEEE 15288

The overall systems engineering workflow

システム エンジニアリングの全体的なワークフロー



 |

ISO/IEC/IEEE 15288

T4 - ISO/IEC/IEEE 15288

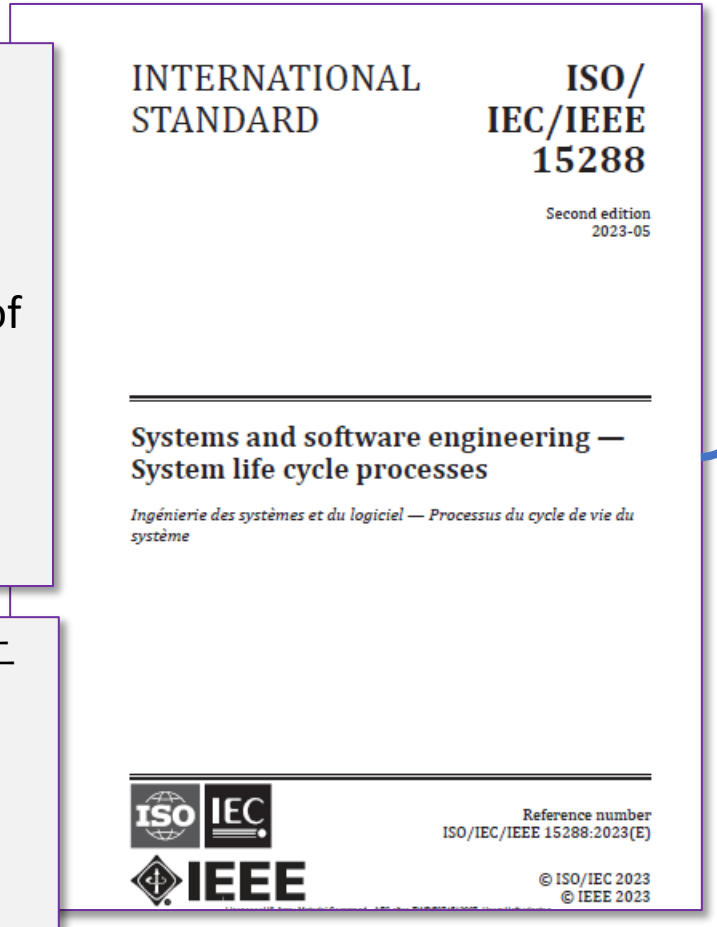
ISO/IEC/IEEE 15288 is the central international standard for systems engineering.

For STPA, we are interested in two sections of the standard:

- **5.5.2 System life cycle stages**
- **5.7.5 Technical processes**

ISO/IEC/IEEE 15288 は、システム エンジニアリングの中心的な国際標準です。
STPA については、規格の 2 つのセクションに注目します。

- 5.5.2 システムのライフサイクル段階
- 5.7.5 技術的プロセス


INTERNATIONAL STANDARD

ISO/IEC/IEEE 15288

Second edition
2023-05

Systems and software engineering — System life cycle processes

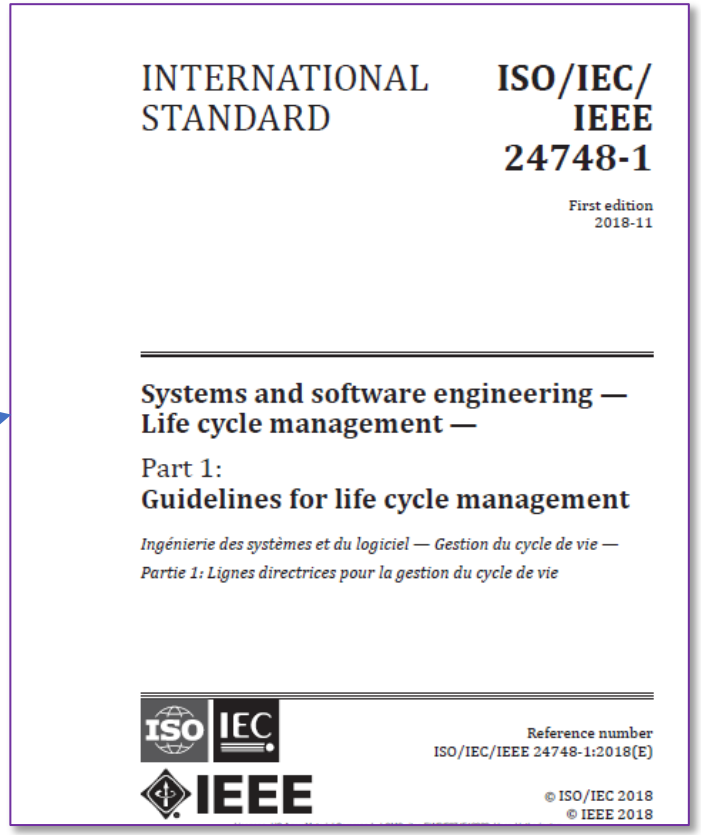
Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système

ISO IEC

IEEE

Reference number
ISO/IEC/IEEE 15288:2023(E)

© ISO/IEC 2023
© IEEE 2023


INTERNATIONAL STANDARD

ISO/IEC/IEEE 24748-1

First edition
2018-11

Systems and software engineering — Life cycle management —

Part 1:
Guidelines for life cycle management

Ingénierie des systèmes et du logiciel — Gestion du cycle de vie —
Partie 1: Lignes directrices pour la gestion du cycle de vie

ISO IEC

IEEE

Reference number
ISO/IEC/IEEE 24748-1:2018(E)

© ISO/IEC 2018
© IEEE 2018

 |

5.5.2 System life cycle stages

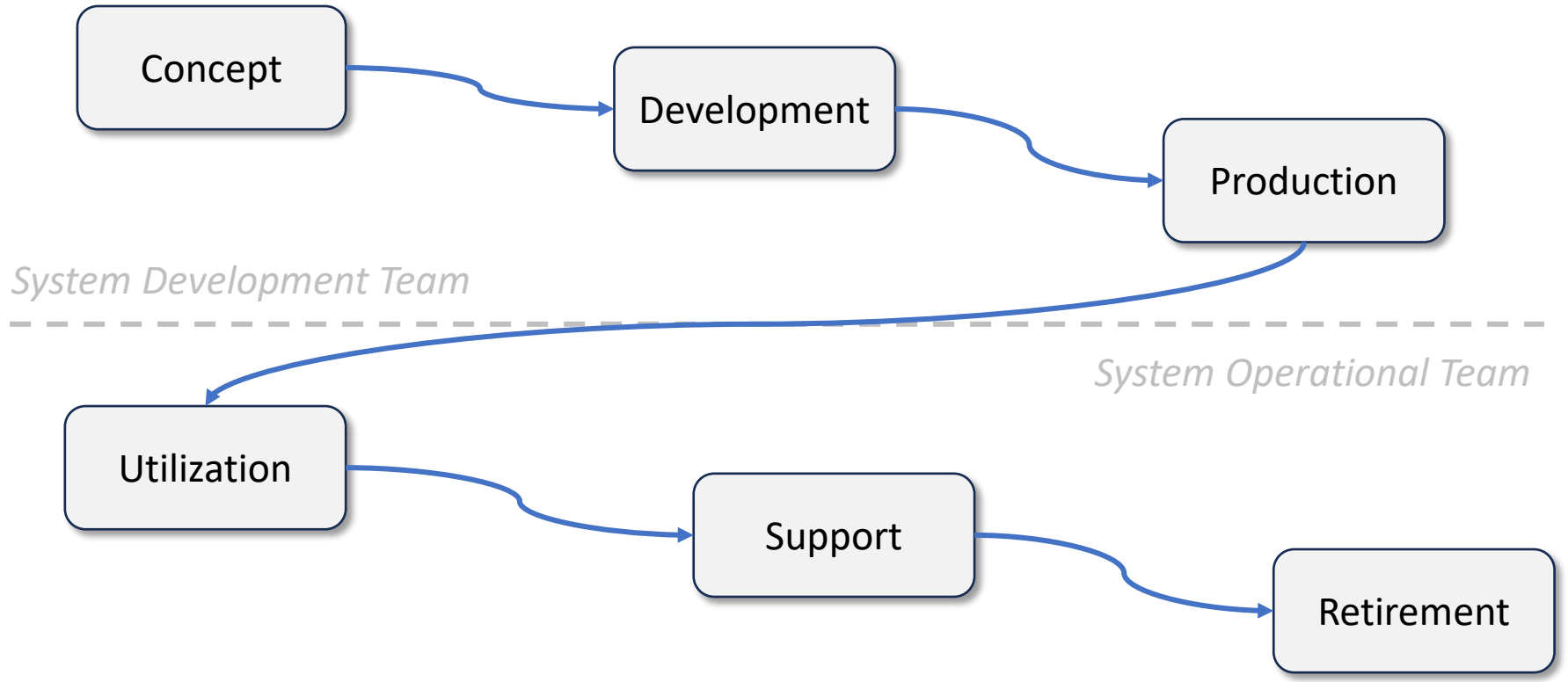
T4 - ISO/IEC/IEEE 15288

定義によれば、これらのライフサイクルは、沖合石油掘削プラットフォームなどのプロジェクトには最適です。しかし残念ながら、自動車のような最終消費者向け製品には適していません。

ISO/IEC/IEEE 15288 lists six key systems life cycle stages. However, the list is actually a reference to ISO/IEC/IEEE 2478-1.

As defined, these are perfect for a project such as an offshore oil drilling platform.

They do not fit the automotive business very well.



From ISO/IEC/IEEE 24748-1 section 4.3.2 is referenced by ISO/IEC/IEEE 15288:2023 section 5.5.2

 |

5.5.2 System life cycle stages (Adjusted)

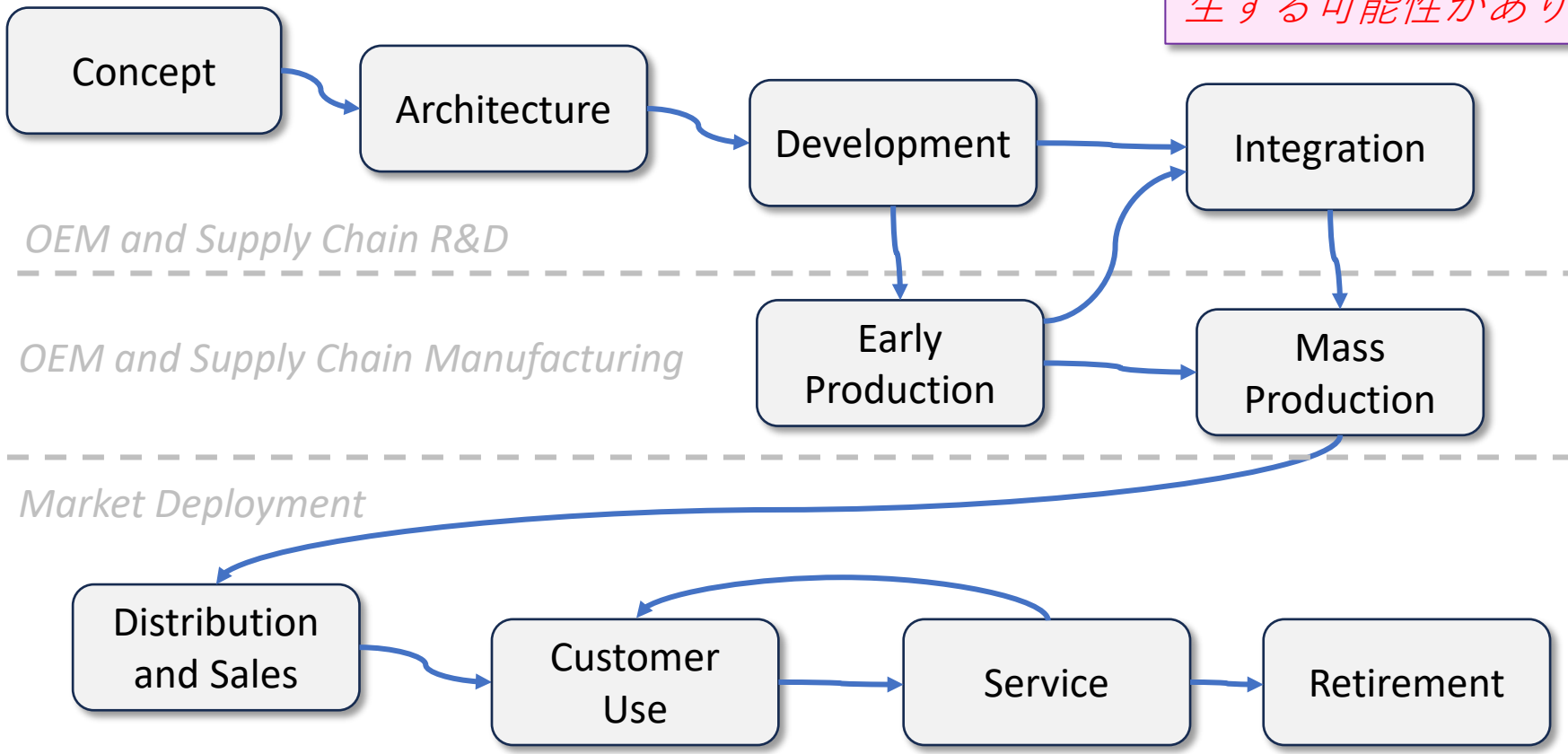
T4 - ISO/IEC/IEEE 15288

サイバー攻撃はライフサイクルのどのフェーズでも発生する可能性があります。

This is an adjusted view of the life cycle of an automobile.

Cyber attacks can occur during any life cycle phase!

Considering only "Customer Use" may be adequate for safety, but it is NOT adequate for cyber security.



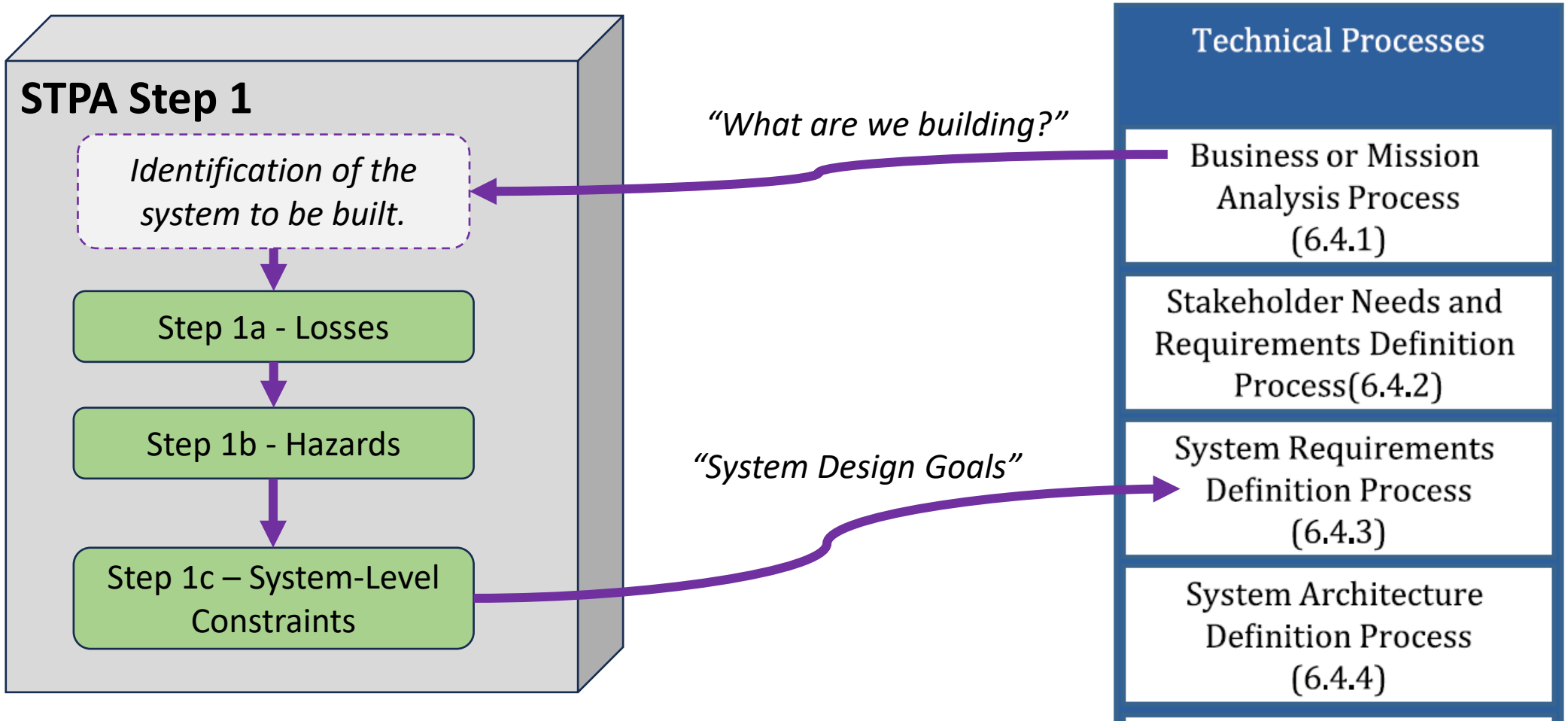
Ideally, a separate STPA workup should be performed for each lifecycle stage.

理想的には、ライフサイクルの各ステージごとに個別の STPA ワークアップを実行する必要があります。

 |

5.7.5 Technical processes – STPA Step 1

T4 - ISO/IEC/IEEE 15288



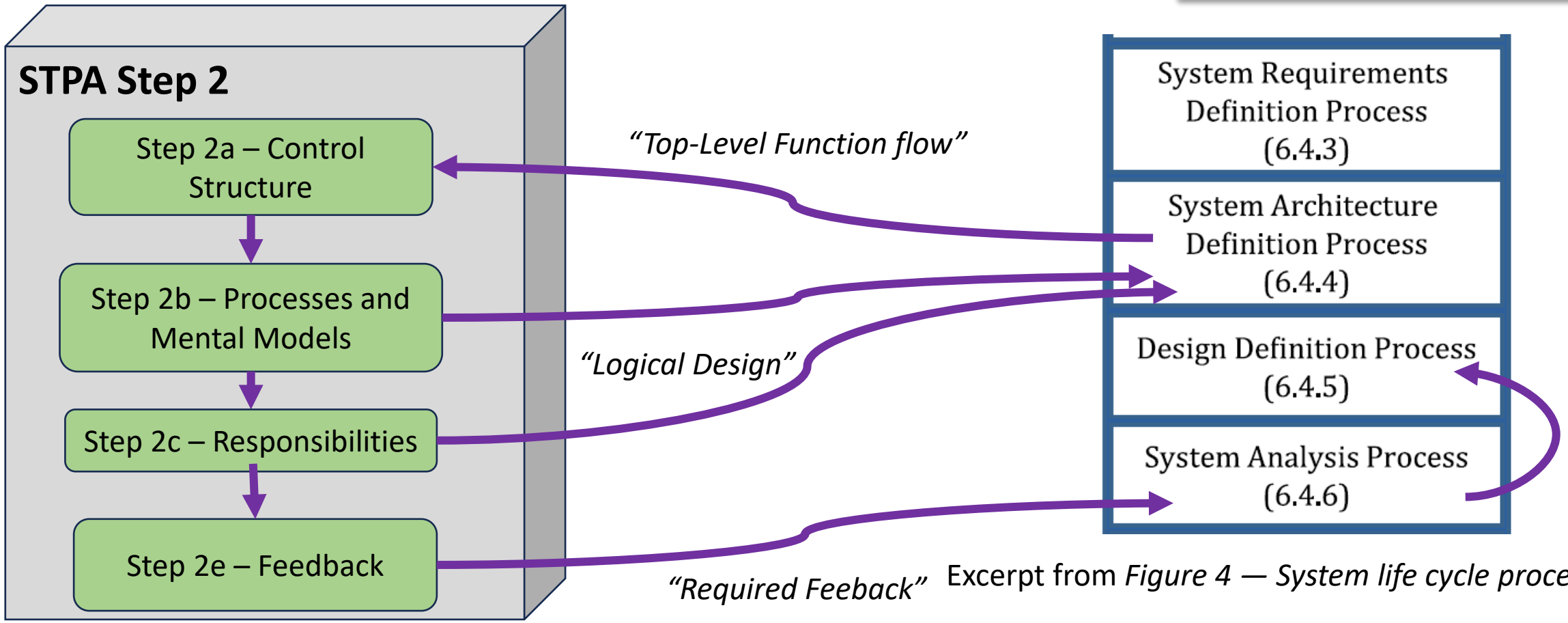
Excerpt from *Figure 4 — System life cycle processes*

 |

5.7.5 Technical processes – STPA Step 2

T4 - ISO/IEC/IEEE 15288

必要なフィードバックを確実に識別できることは、STPA の大きな強みの 1 つです。



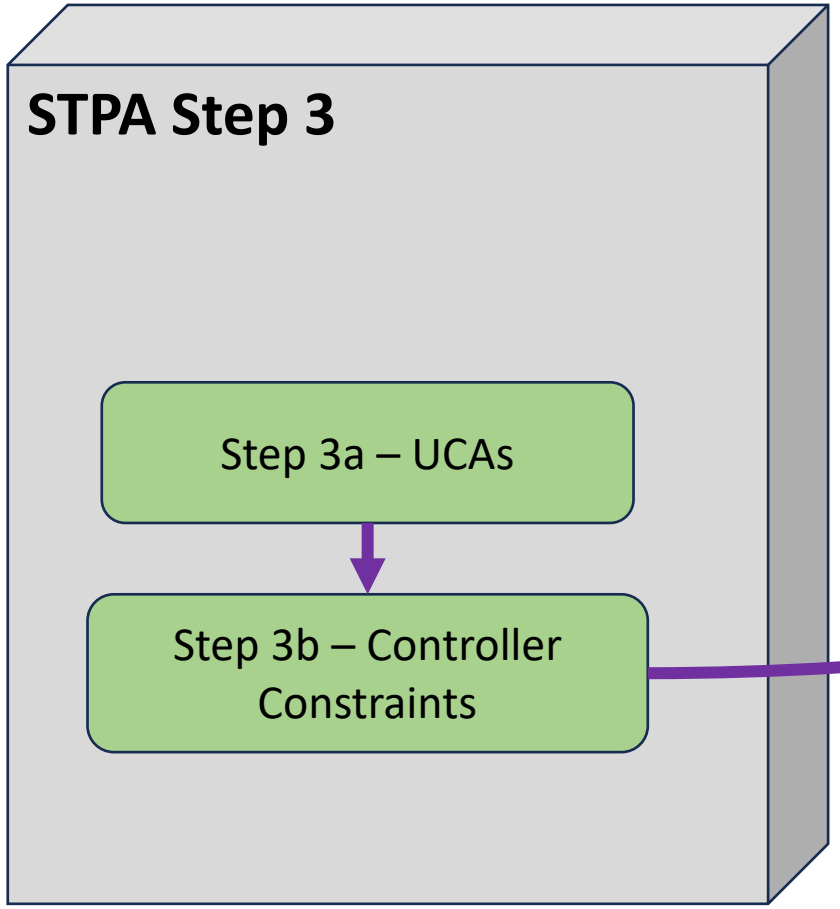
Excerpt from *Figure 4 — System life cycle processes*

The airtight identification of required feedback is one of the major strengths of STPA.

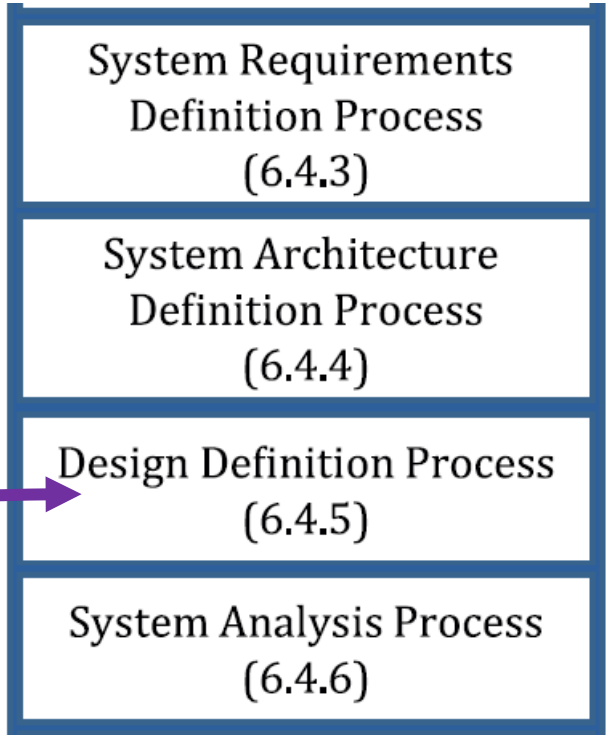
 |

5.7.5 Technical processes – STPA Step 3

T4 - ISO/IEC/IEEE 15288



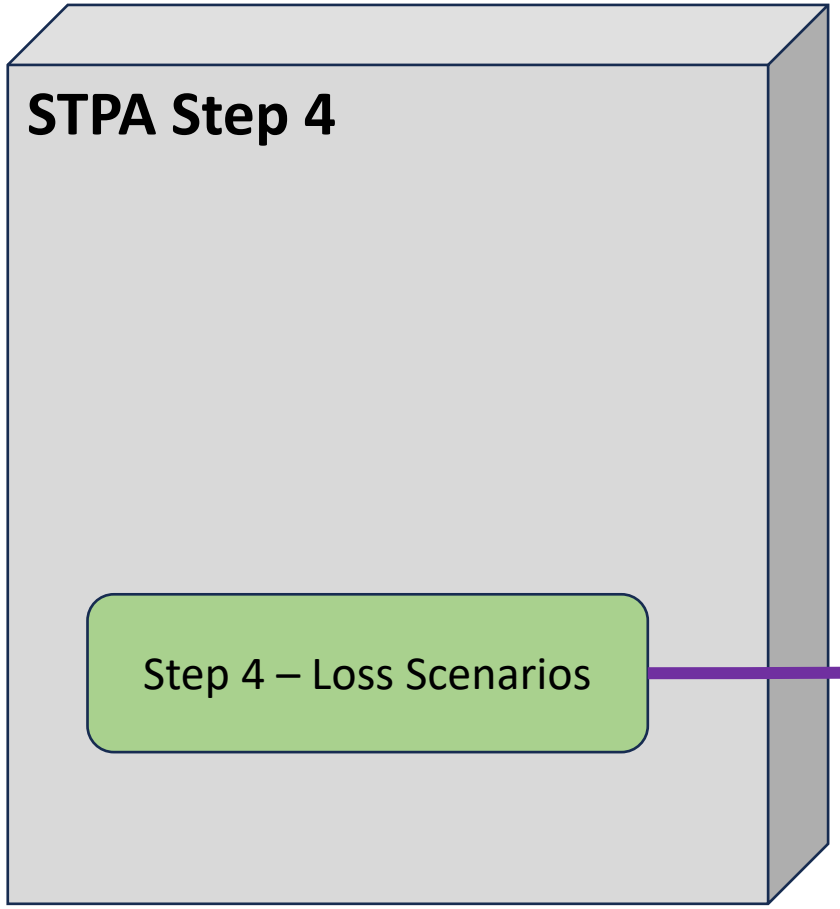
"Design Goals for Controllers"



Excerpt from *Figure 4 — System life cycle processes*

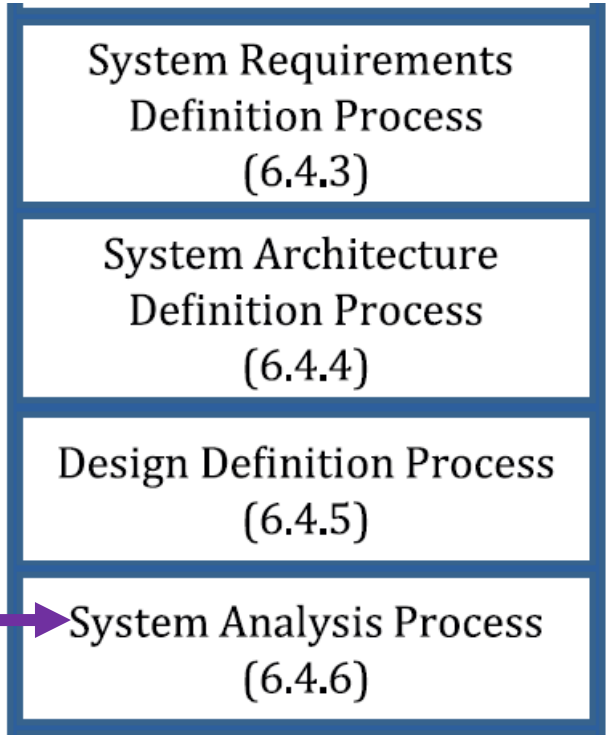
5.7.5 Technical processes – STPA Step 4

T4 - ISO/IEC/IEEE 15288



In fact, STPA Step 4 is where the STPA process comes together with the ISO 26262 process. STPA Step 4 essentially sets up the mental framework to dramatically increase the effectiveness of the ISO 26262 HARA step.

"Design vulnerabilities"



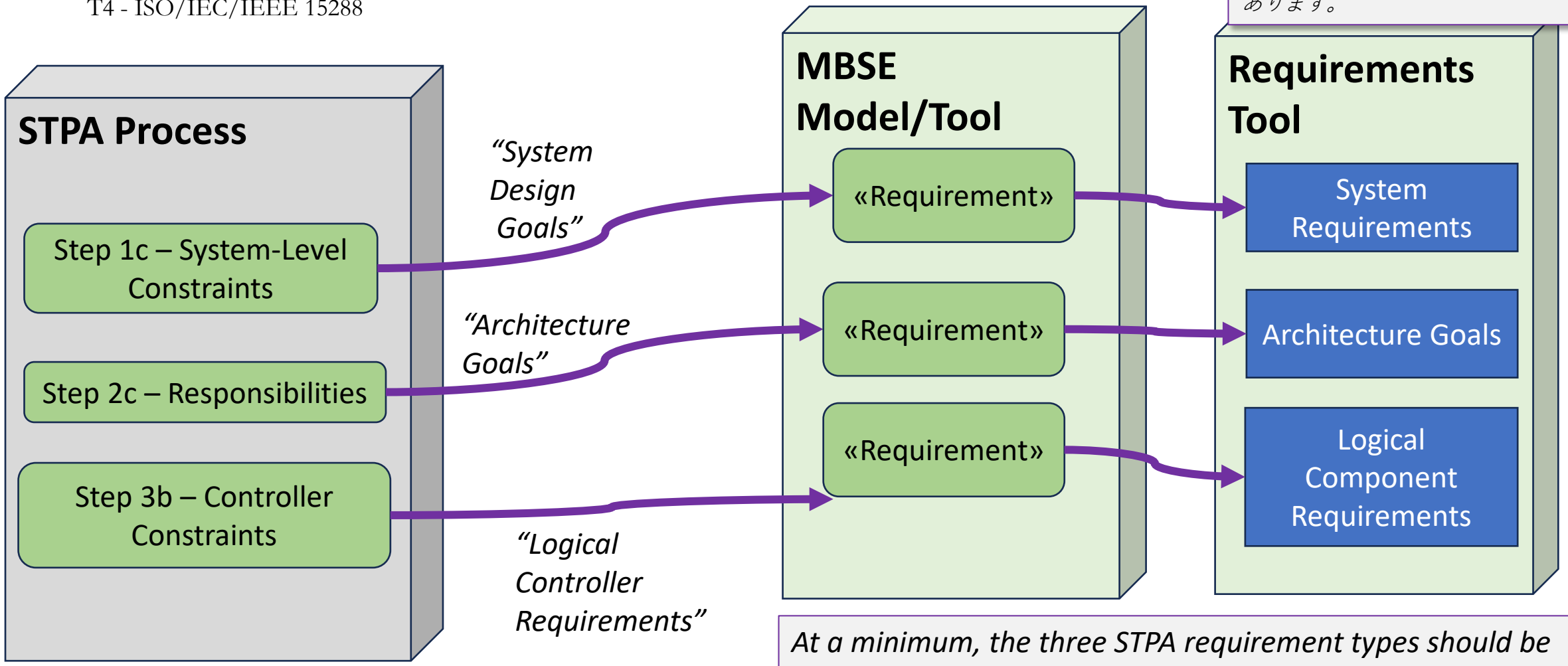
Excerpt from *Figure 4 — System life cycle processes*

STPAステップ4は、STPAプロセスとISO 26262プロセスを統合するステップです。STPAステップ4は、本質的にはISO 26262のHARAステップの有効性を飛躍的に高めるための精神的な枠組みを構築します

 |

5.7.5 Technical processes – Digital Thread

T4 - ISO/IEC/IEEE 15288



少なくとも、STPAの3つの要件タイプを要件定義ツールにプッシュする必要があります。ただし、実際には、すべてのSTPA要素を要件定義ツールにプッシュすることが有用な場合もあります。

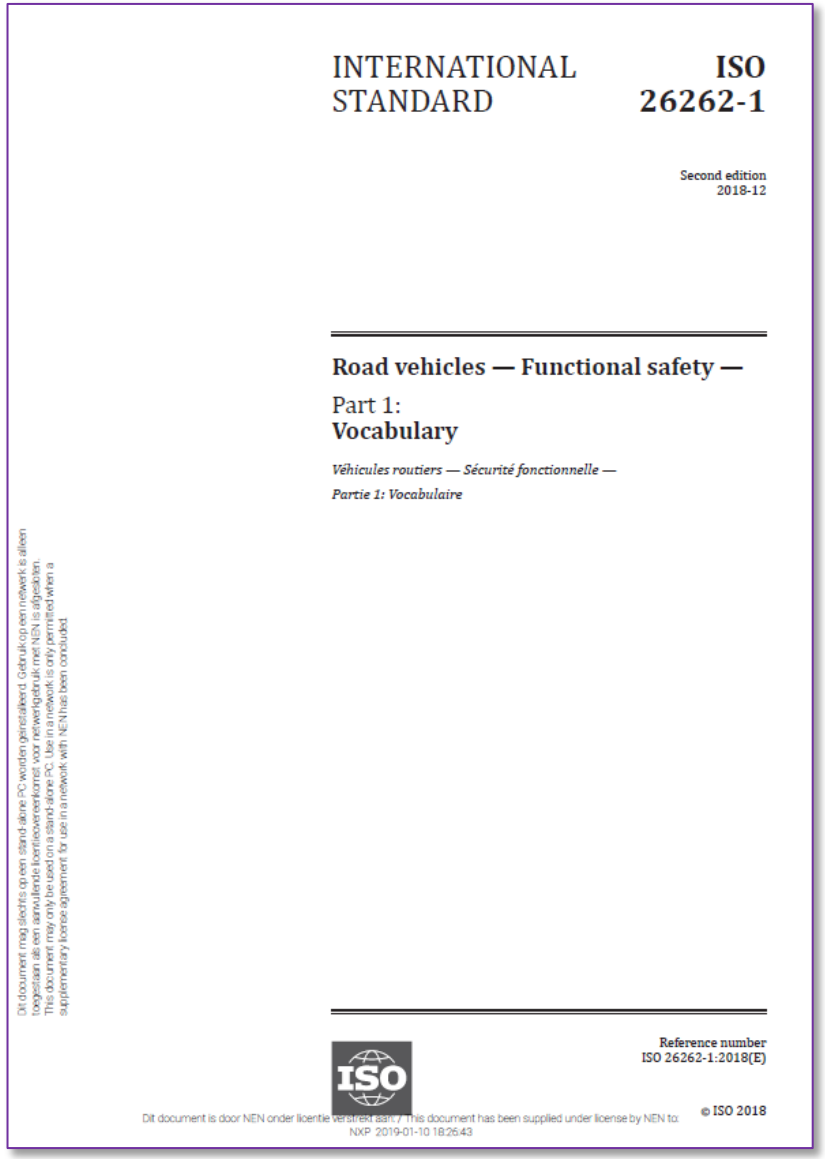
At a minimum, the three STPA requirement types should be pushed through to the requirements tool. Actually, however, it may be useful to push all of the STPA elements into the requirements tool.

 |

T5 - ISO 26262

Integrating STPA into the ISO 26262 functional safety flow.

STPA を ISO 26262 機能安全フローに統合します。



INTERNATIONAL STANDARD

ISO 26262-1

Second edition
2018-12

Road vehicles — Functional safety —

Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

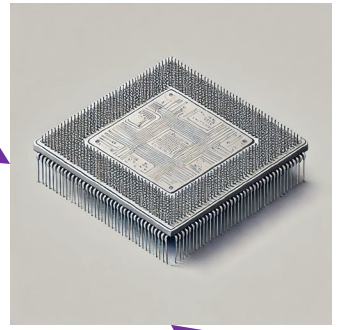
Reference number
ISO 26262-1:2018(E)

SAE/ISO 21434 and ISO 26262 Scope Issue

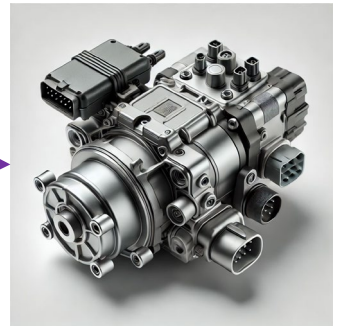
T5 - ISO 26262

Sensor
センサー

Controller
コントローラ



Actuator
アクチュエータ



Typical "Item" for ISO 26262
ISO 26262の典型的なアイテム

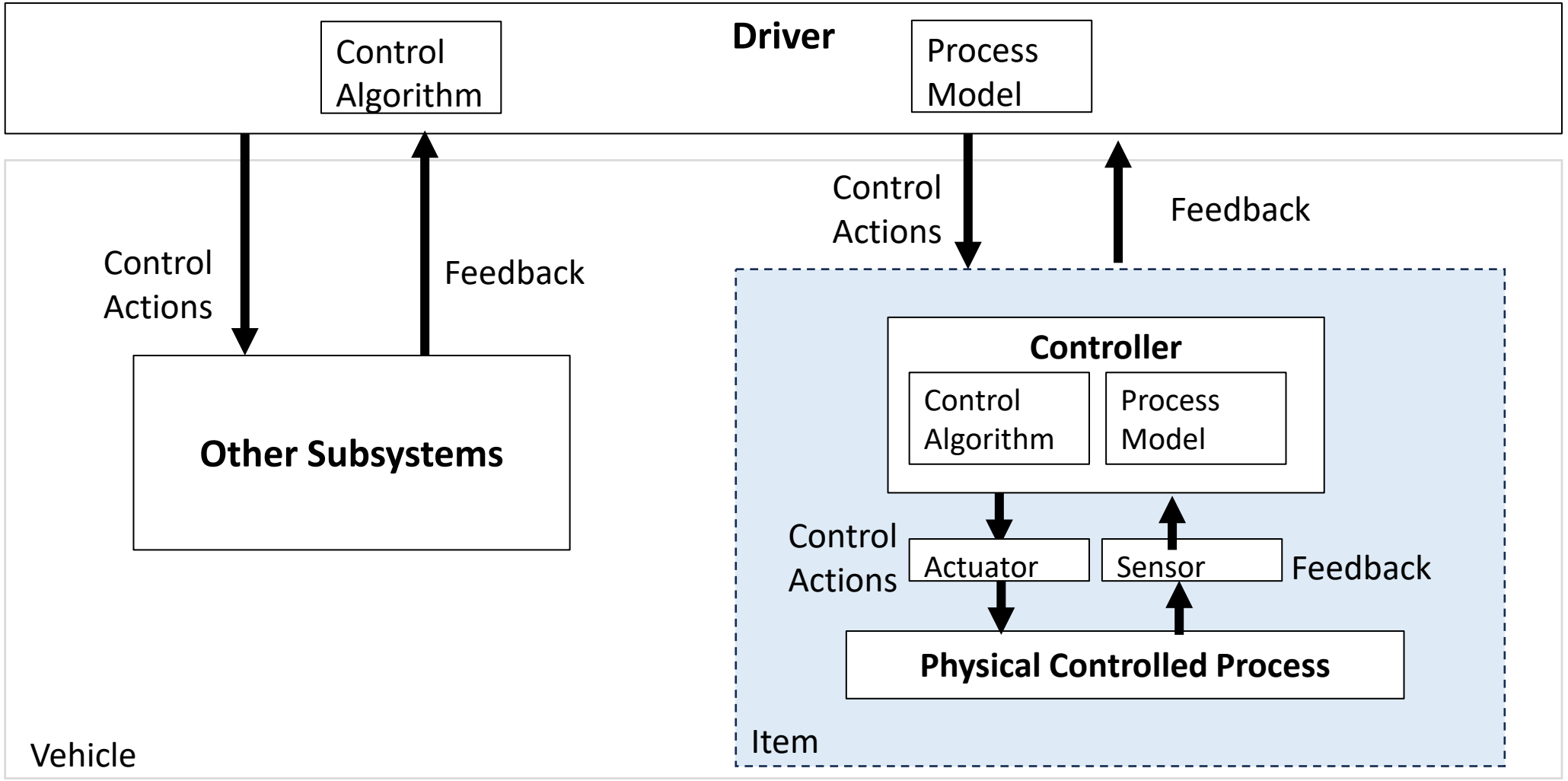
- Both ISO 26262 and ISO/SAE 21434 are scope-limited to "electronics and software".
- Both are written around the concept of an "item", often a sensor + a controller + an actuator.
- No humans.
- For cybersecurity, the humans are important.
- For STPA, we have to model the bigger picture and include the "item" as a subsystem.

- ISO 26262 と ISO/SAE 21434 はどちらも、範囲が「電子機器とソフトウェア」に限定されています。
- どちらも「アイテム」の概念、通常はセンサー + コントローラー + アクチュエーターを中心に書かれています。
- 人間の役割は考えられていない。
- サイバーセキュリティでは、人間が重要です。
- STPA では、全体像をモデル化し、「アイテム」をサブシステムとして含める必要があります。

 |

STPA View of the Item

T5 - ISO 26262



 |

Start with Systems Engineering – RFLP Overview

T5 - ISO 26262

ステークホルダー - Stakeholders

R = Requirements (要件)

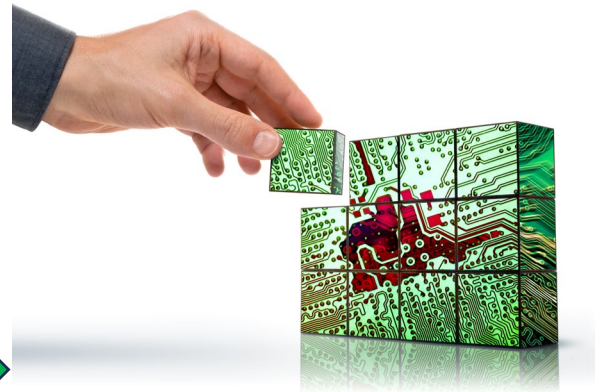
F = Functional (機能的)

L = Logical (論理的)

P = Physical (物理的)

Notice that "RFLP" is similar to, but not identical to the ISO 15288 technical process breakdown.

「RFLP」は ISO 15288 の技術プロセス内訳に似ていますが、同一ではないことに注意してください。



素敵なシステム - Nice System

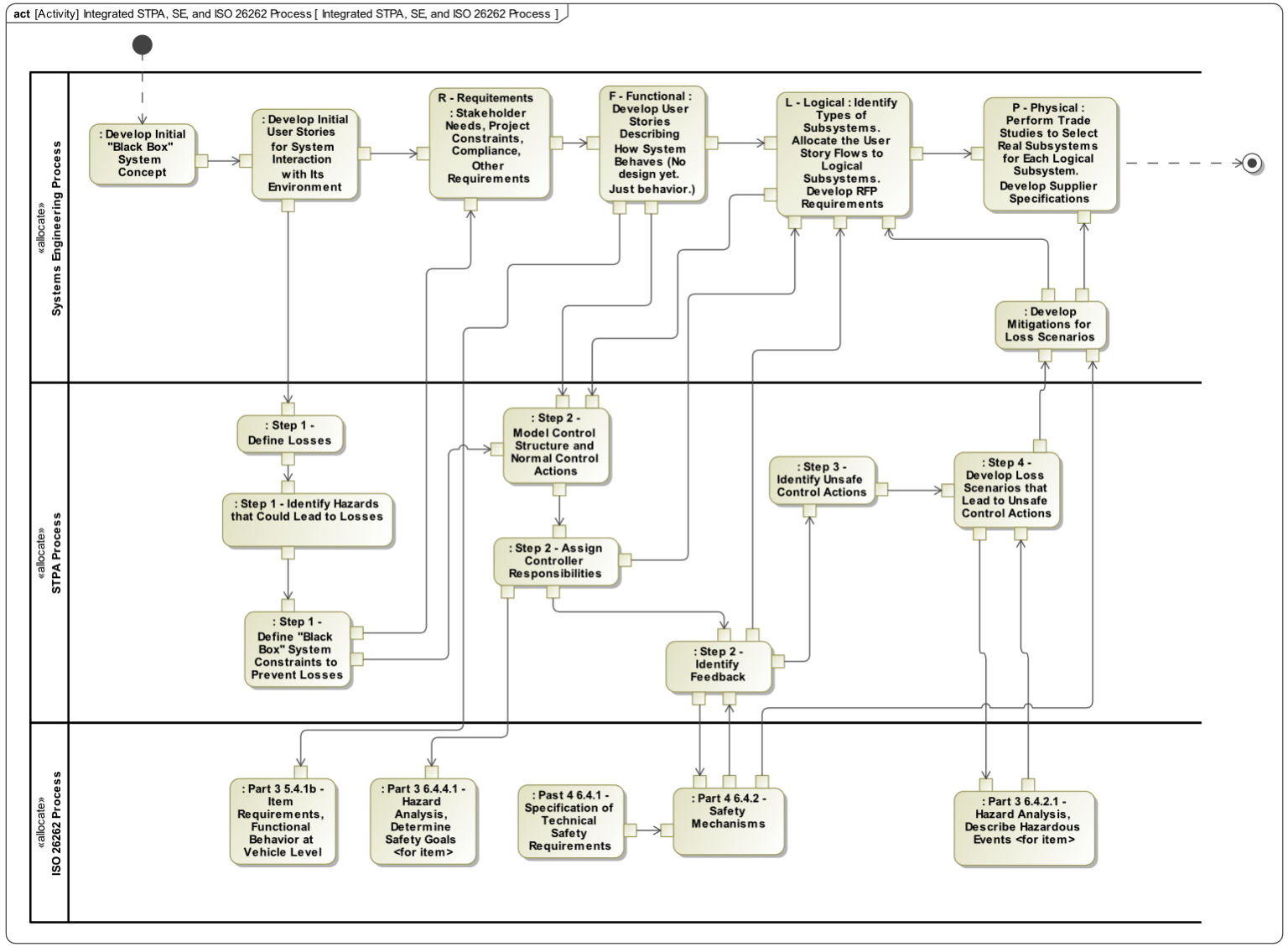
英語でも日本語でも、「R」を表す単語はたくさんあります。「R = 要件」が提示されましたが、他の言葉も可能です。「R=要求」も良いです。ただし、「ニーズ」と「望み」も可能です。西村先生にご相談してください。

Integrate SE, STPA, ISO 26262 Workflow

T5 - ISO 26262

- Most of the integration with STPA will be in parts 3 and 4 of ISO 26262.
- STPA process and the ISO 26262 process will iterate back-and-forth.
- One key difference: HARA comes at the end, not at the beginning.

- STPAとの統合の大部分は、ISO 26262のパート3とパート4で行われます。
- STPAプロセスとISO 26262プロセスは、相互に繰り返し実行されます。
- 重要な違いは、HARAが最初ではなく最後に来ることです。



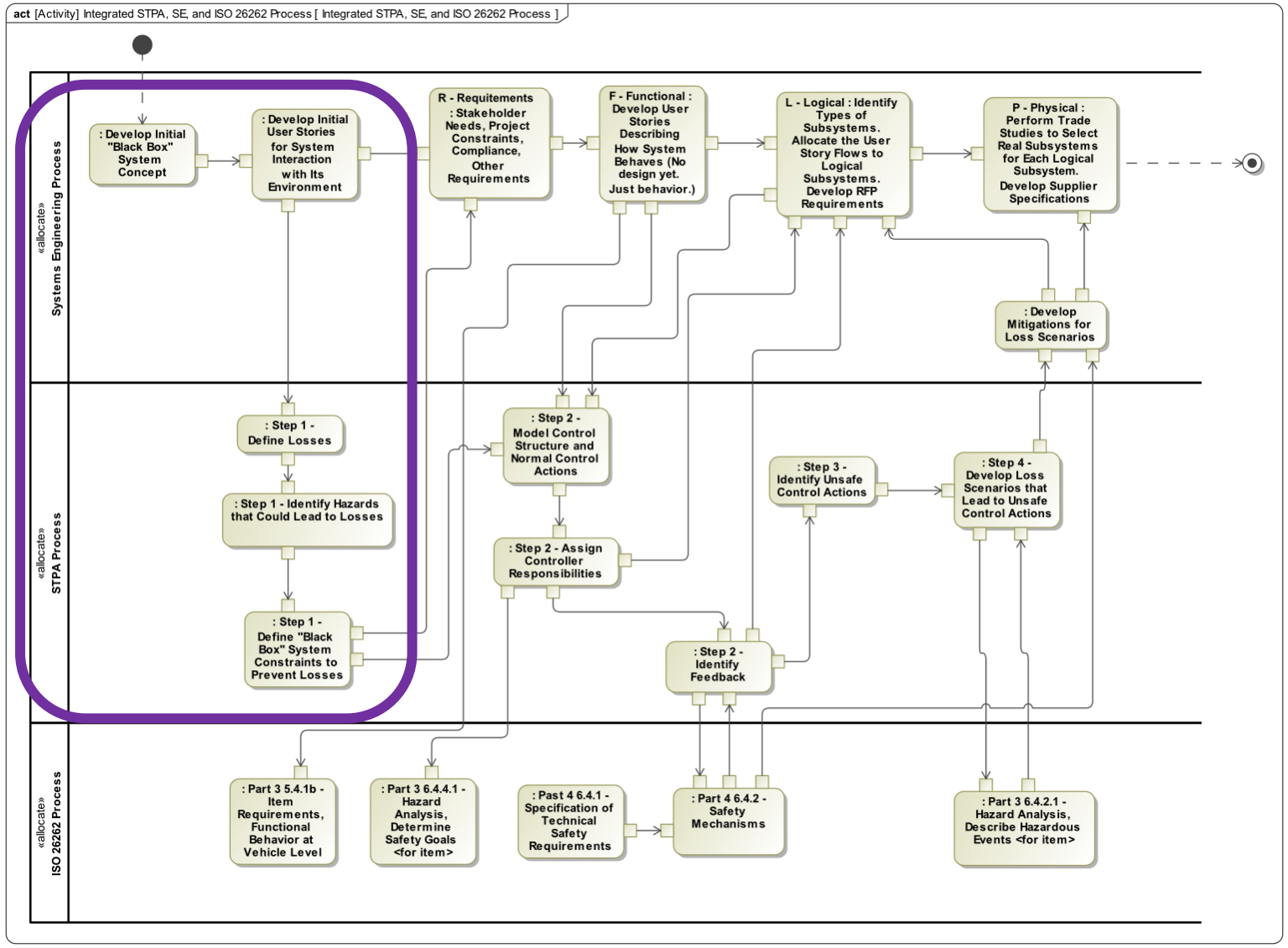
 |

The Concept Has to Come First for STPA

T5 - ISO 26262

- Neither STPA nor ISO 26262 can be done from a blank sheet of paper.
- Are we developing an automobile? A microwave oven? A swimming pool? A motorcycle? A passenger bus?
- Once the top-level product concept is nailed down, STPA Step 1 can proceed:
  - Losses
  - Hazards
  - System-Level Constraints

- STPAもISO 26262も、白紙の状態から始めることはできません。
- 開発しているのは自動車でしょうか？電子レンジでしょうか？スイミングプールでしょうか？オートバイでしょうか？それとも旅客バスでしょうか？
- トップレベルの製品コンセプトが固まったら、STPAステップ1に進みます。損失ハザードシステムレベルの制約



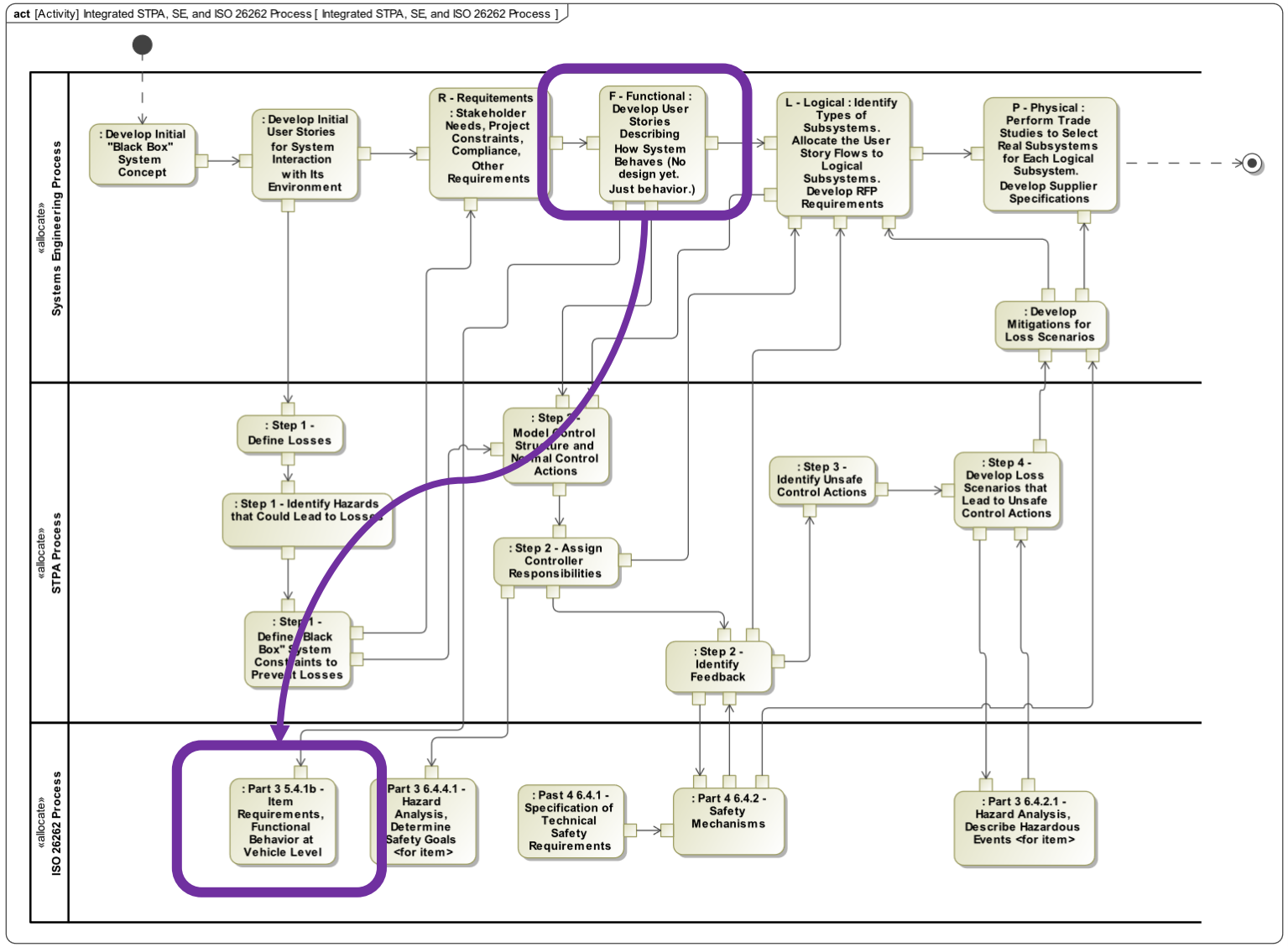
 |

Vehicle Level Functional Behavior Comes Next

T5 - ISO 26262

- Although it is easy to miss in casual reading, in Part 3 5.4.1b ISO 26262 requires the functional behavior at the vehicle level as an input.
- STPA likewise requires this level of definition as an input to Step 2. No behavior concept? You can't do STPA.
- This information comes from the "F" step of "RFLP".

- ざっと読むだけでは見落としがちですが、ISO 26262のパート3 5.4.1bでは、車両レベルの機能的動作を入力として必要としています。
- STPAも同様に、ステップ2への入力としてこのレベルの定義を必要とします。動作の概念がなければ、STPAは実行できません。
- この情報は「RFLP」の「F」ステップから得られます。



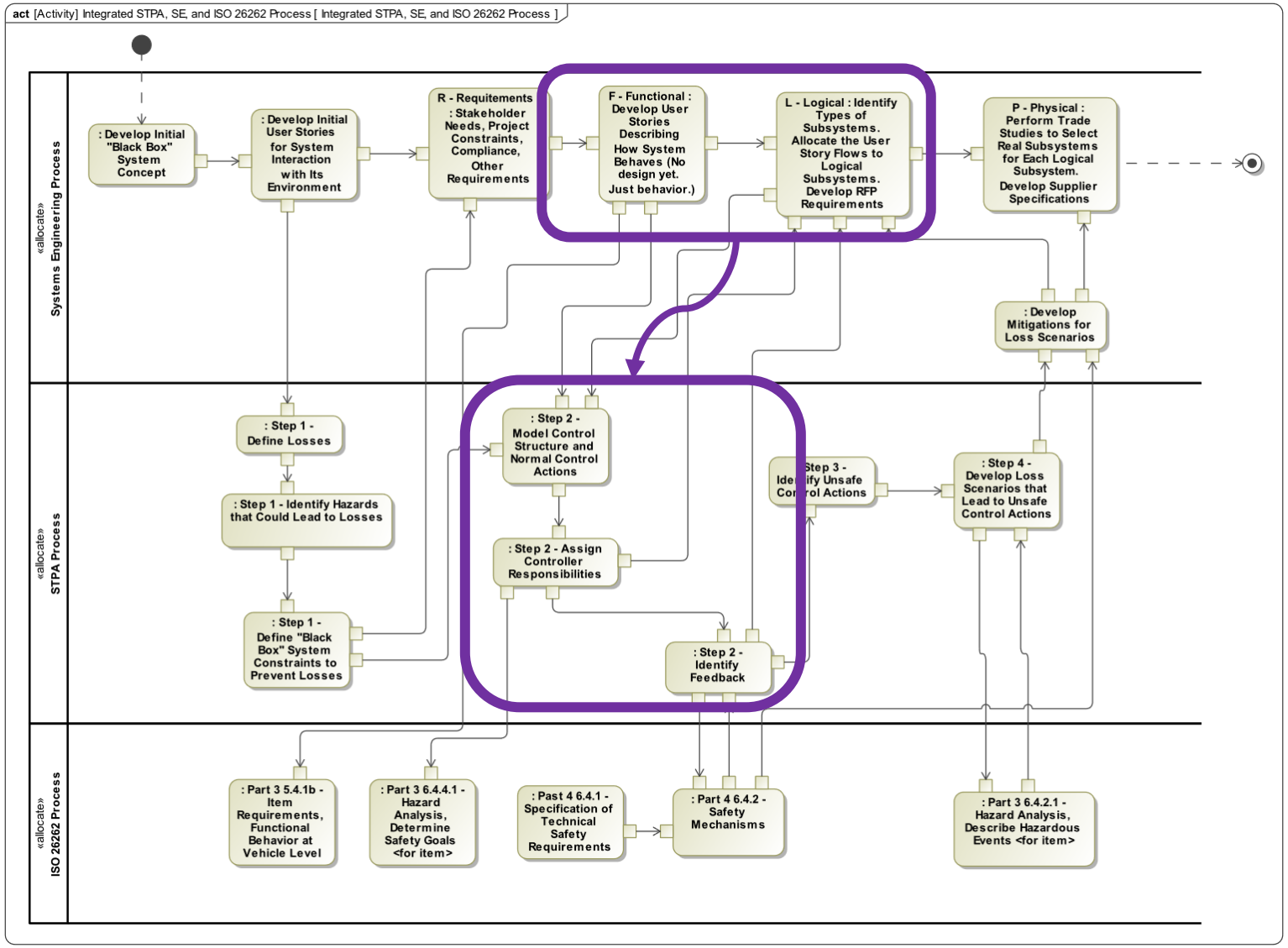
 |

Functional and Logical Needed for STPA Step 2

T5 - ISO 26262

- Although it is easy to miss in casual reading, in Part 3 5.4.1b ISO 26262 requires the functional behavior at the vehicle level as an input.
- STPA likewise requires this level of definition as an input to Step 2. No behavior concept? You can't do STPA.
- This information comes from the "F" step of "RFLP".

- ざっと読むだけでは見落としがちですが、ISO 26262のパート3 5.4.1bでは、車両レベルの機能的動作を入力として必要としています。
- STPAも同様に、ステップ2への入力としてこのレベルの定義を必要とします。動作の概念がなければ、STPAは実行できません。
- この情報は「RFLP」の「F」ステップから得られます。



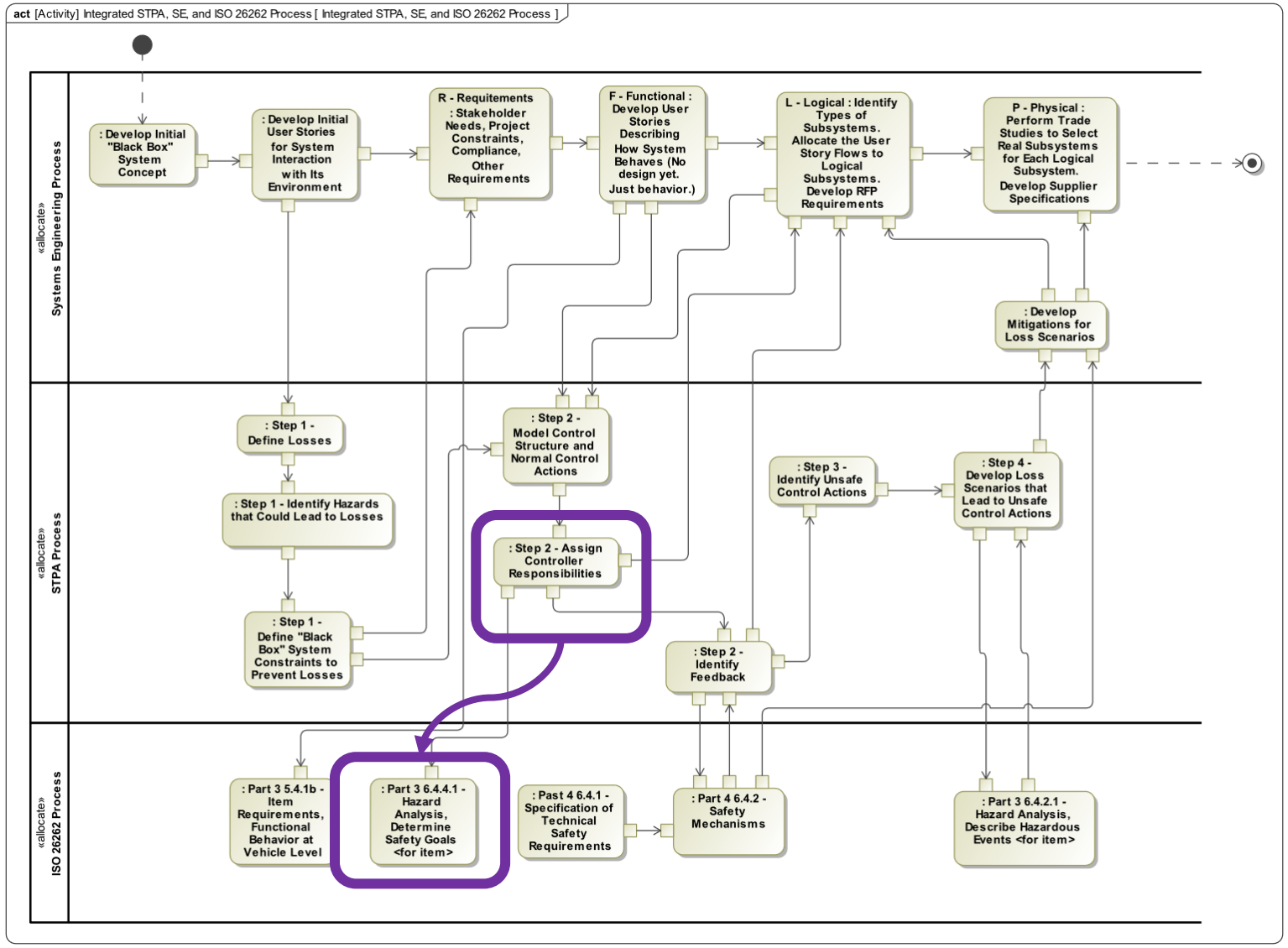
 |

STPA Step 2 Sets Safety Goals for the Item

T5 - ISO 26262

- STPA Step 2 “Controller Responsibilities” become the ISO 26262 “Safety Goals” for the Item.

- STPA ステップ 2「コントローラの責任」は、アイテムの ISO 26262「安全目標」になります。



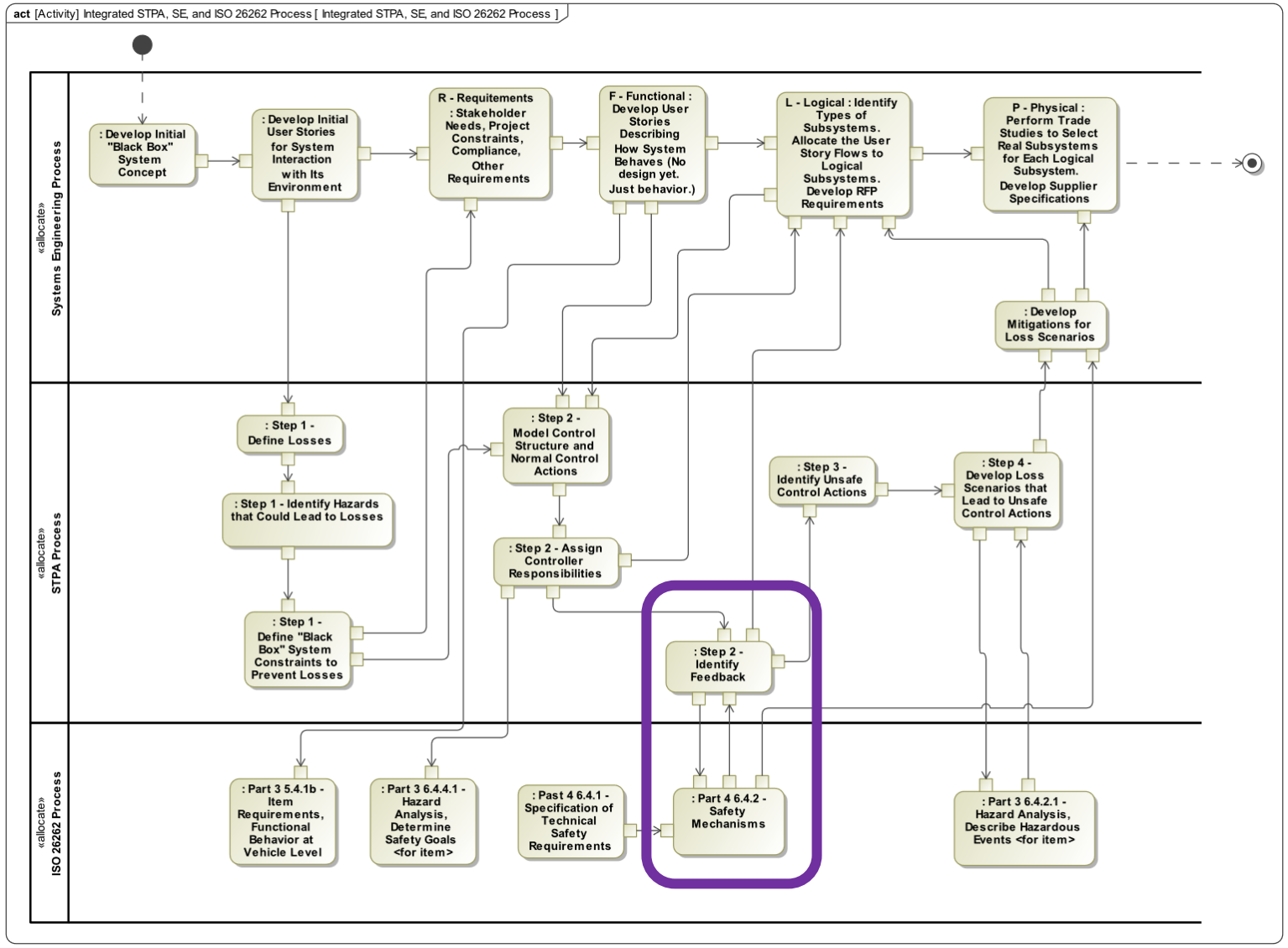
 |

STPA Feedback Related to Safety Mechanisms

T5 - ISO 26262

- STPA Step 2 “Identify Feedback” is closely related to the ISO 26262 “Safety Mechanisms” for the Item.

- STPA ステップ 2「フィードバックの識別」は、アイテムの ISO 26262「安全メカニズム」と密接に関連しています。



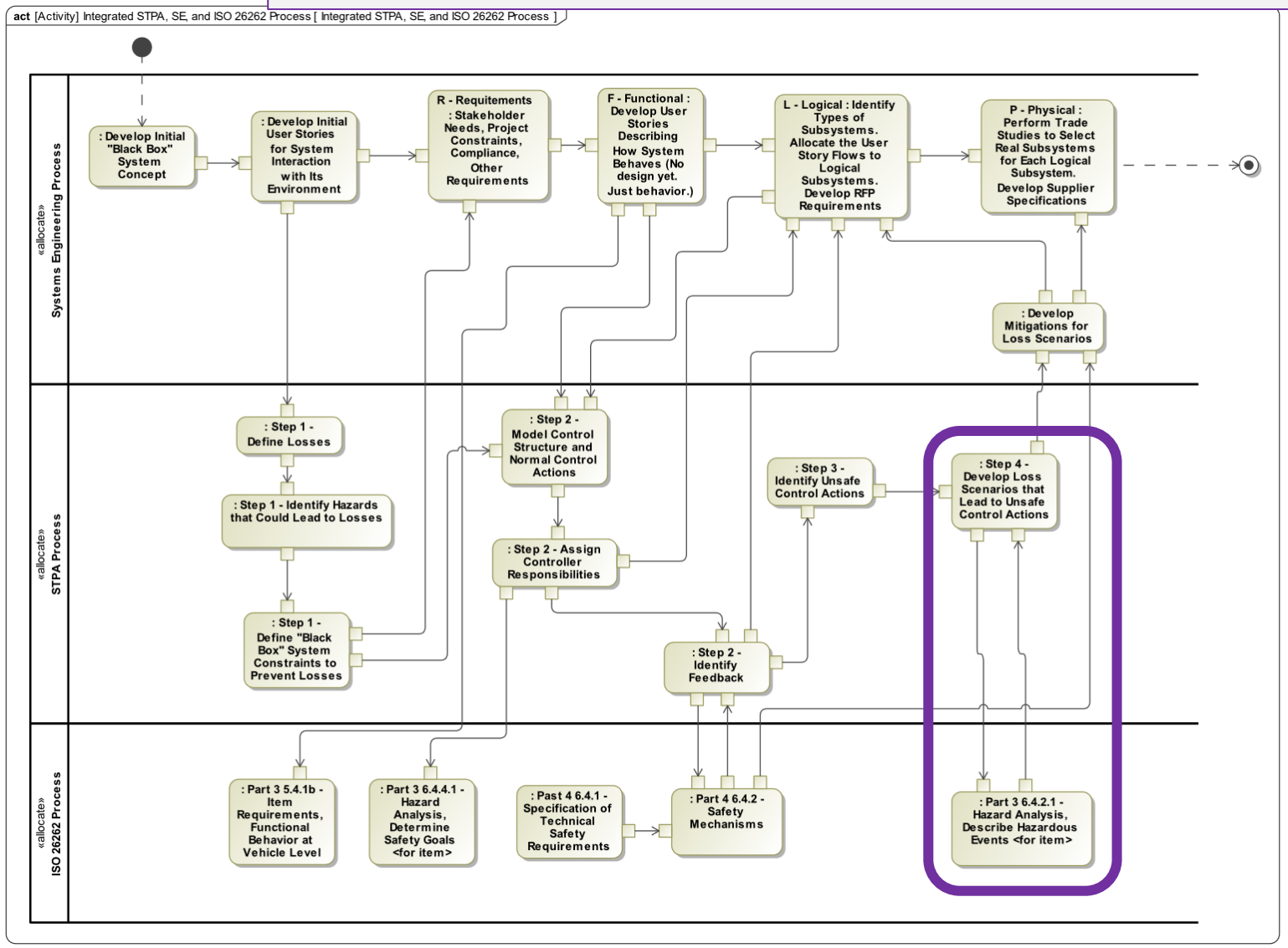
 |

HARA Comes Last!

HARAは最後にあり、STPAステップ4の一部です。これは、従来の安全対策の専門家にとっては直感に反するように思えるかもしれません。

T5 - ISO 26262

- HARA comes last and is part of STPA Step 4.
- This will seem counter intuitive to traditional safety practitioners!
- However, there is a reason that this comes last in STPA!
- Attempts to do HARA at the beginning can easily become unfocused and drown in complexity or lack coherent completeness.
- STPA provides the cognitive framework to perform an efficient HARA.
- Findings from HARA / Loss Scenarios are used to iteratively refine the rest of the analysis.



 |

T6 - ISO/SAE 21434

Integrating STPA into the ISO/SAE 21434 cybersecurity flow

STPA を ISO/SAE 21434 サイバーセキュリティ フローに統合します。

SAE INTERNATIONAL

SURFACE VEHICLE STANDARD

ISO/SAE 21434

Issued 2021-09

Road Vehicles - Cybersecurity Engineering

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

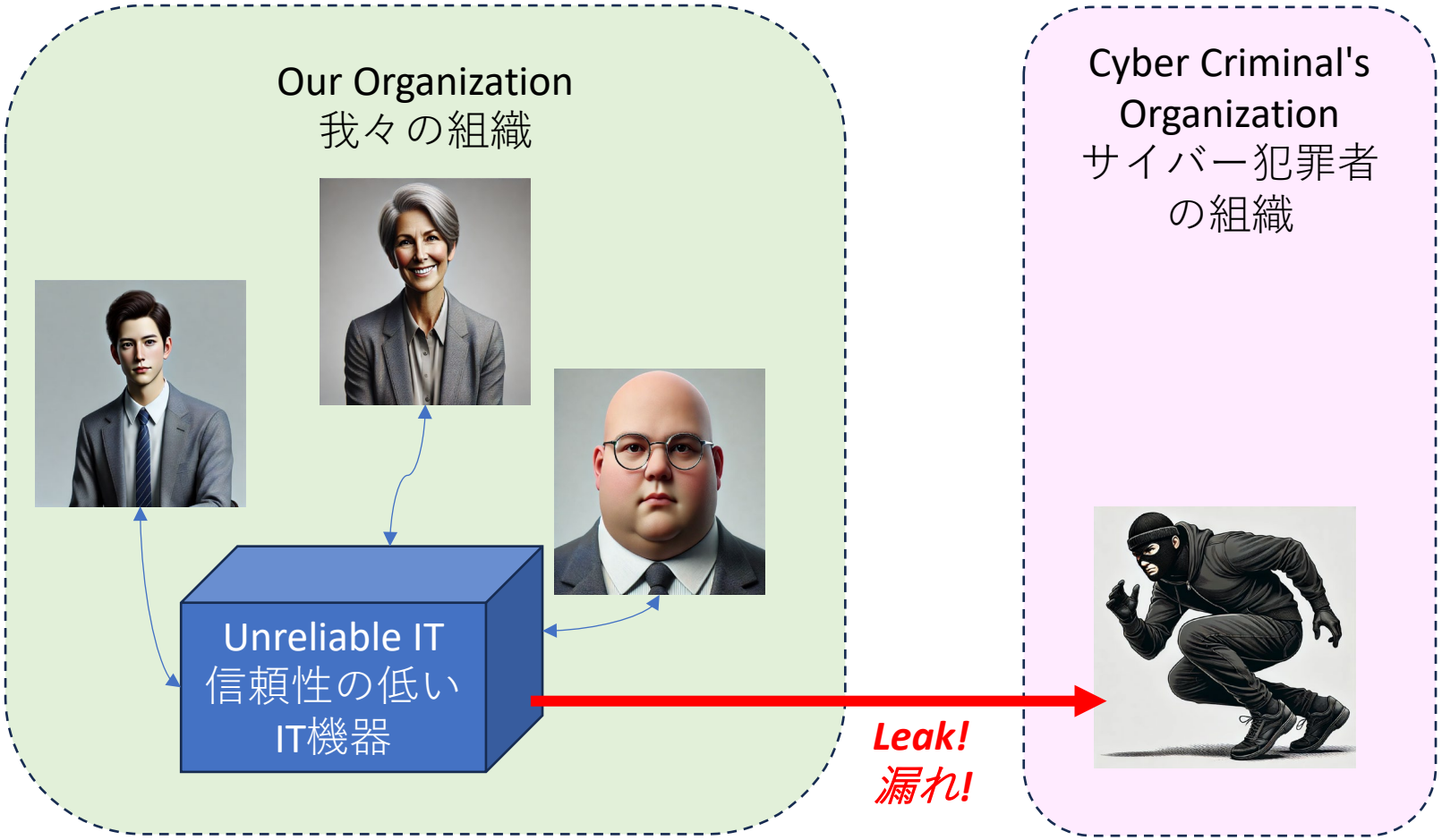
ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

SAE International
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

Published in Switzerland and USA

Confidentiality Losses are Challenging

T6 - ISO/SAE 21434



- Information leaks (loss of 'C') are difficult to architect against.
- There is no feedback path.
- Usually, it is difficult to install a feedback sensor in the cyber criminal's organization.

- 情報漏洩（「C」の損失）に対するアーキテクチャーは難しい。
- フィードバック経路がない。
- 通常、サイバー犯罪者の組織にフィードバックセンサーを設置することは難しい。

 |

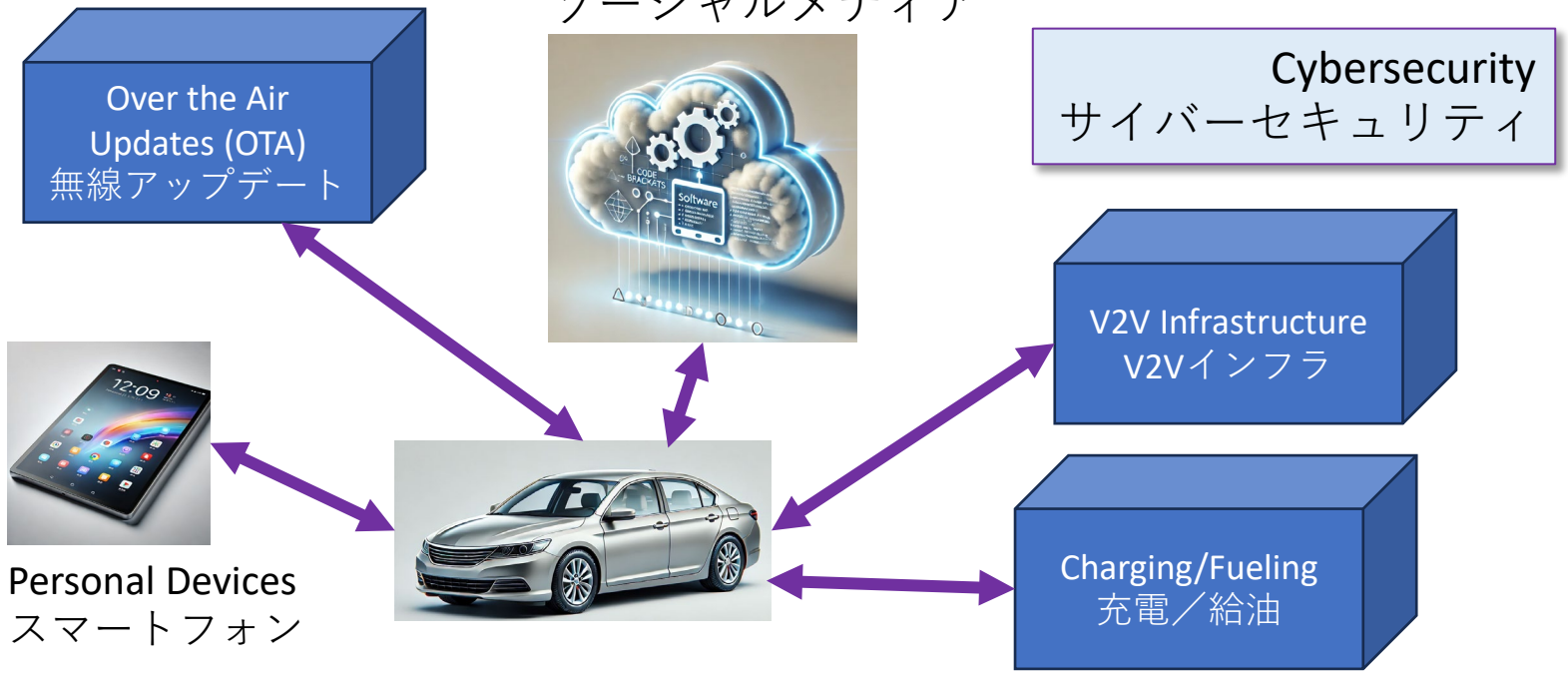
Determining the System Boundary Can be Challenging

T6 - ISO/SAE 21434

Functional Safety
機能安全

- Our system is only the car.
- When the car is off, it is “safe”.
- Everything else is some other department’s problem.

- 私たちのシステムはあくまで車である。
- 車が止まっているときは 「安全」だ。
- それ以外はすべて他の部門の問題だ。



- Once we start analyzing cybersecurity, the system scope gets very large.
- “Just the car” will not satisfy anyone.
- We also need to consider all the system states for the car.

- サイバーセキュリティを分析し始めると、システムの範囲は非常に大きくなる。
- 「車だけ」では誰も満足しない。
- 車のすべてのシステム状態についても考える必要がある。

 |

Cybersecurity Basics - C, I, and A

T6 - ISO/SAE 21434

C = Confidentiality

I = Integrity

A = Availability

C = 機密性

I = 完全

A = 可用性

When using STPA for cybersecurity, these become the main losses we are concerned about.

STPAをサイバーセキュリティに使用する場合、これらの損失が懸念される。

Model Loss of Safety, Loss of CIA, and Loss of Mission Capability

T6 - ISO/SAE 21434

L-1 : Loss of Human Life/Health
人命・健康の損失

L-2 : Loss of C-I-A
C-I-Aの損失

L-3 : Loss of System Capability
システム機能の損失

- Doing STPA for functional safety and cybersecurity together is highly recommended.
- You may want to add a third loss to represent excessive sacrifices of system capability to block the other two losses.

- 機能安全とサイバーセキュリティの STPA を一緒に行うことを強くお勧めします。
- この二つの損失をブロックするために、システム機能の過度の犠牲を表す 3 番目の損失を追加することもできます。

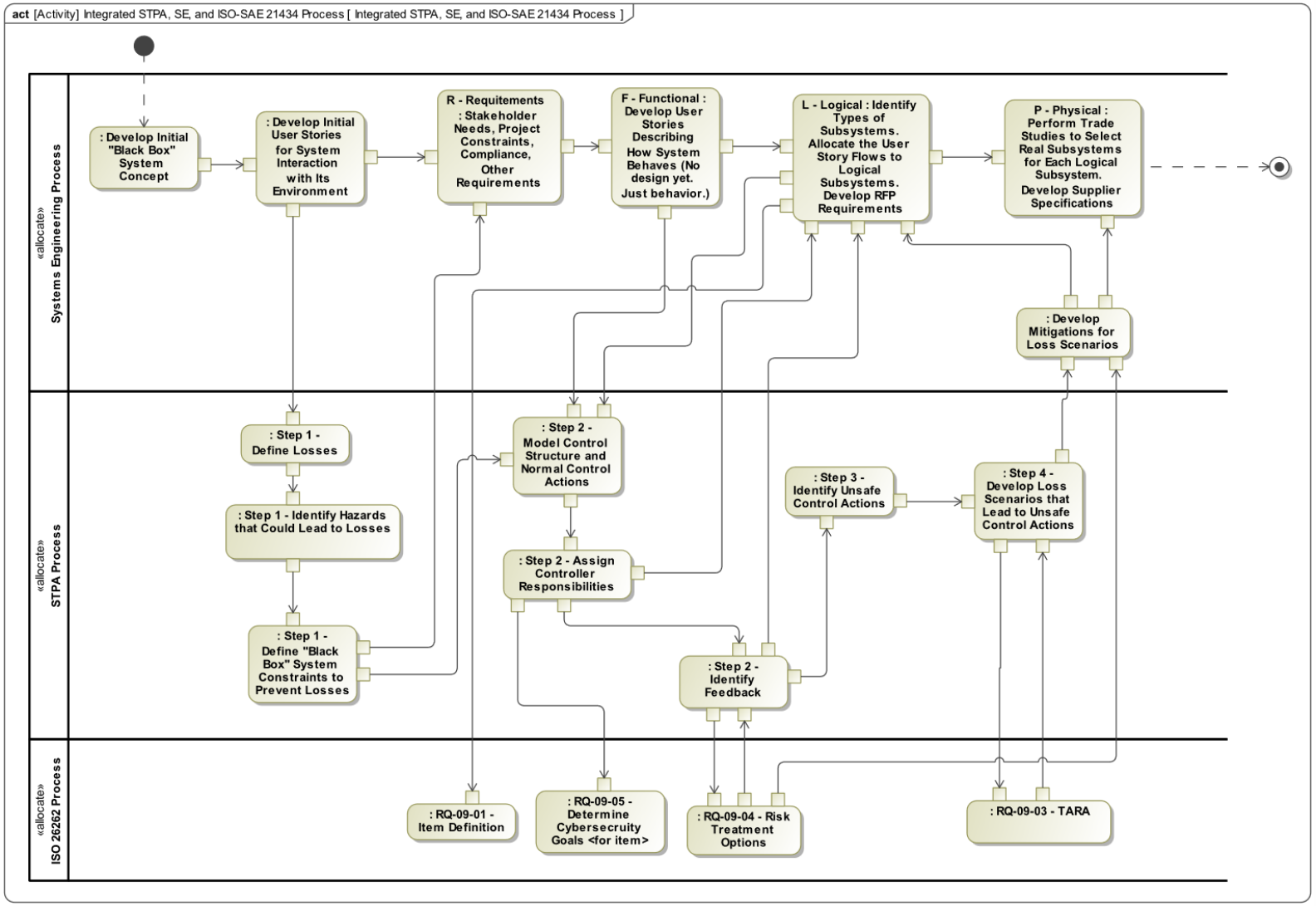
 |

Integrate SE, STPA, ISO/SAE 21434 Workflow

T6 - ISO/SAE 21434

- ISO/SAE 21434 is about 1/8th the size of ISO 26262.
- The integration is correspondingly simpler.

- ISO/SAE 21434 は ISO 26262 の約 8 分の 1 のサイズです。
- そのため、統合もよりシンプルになります。



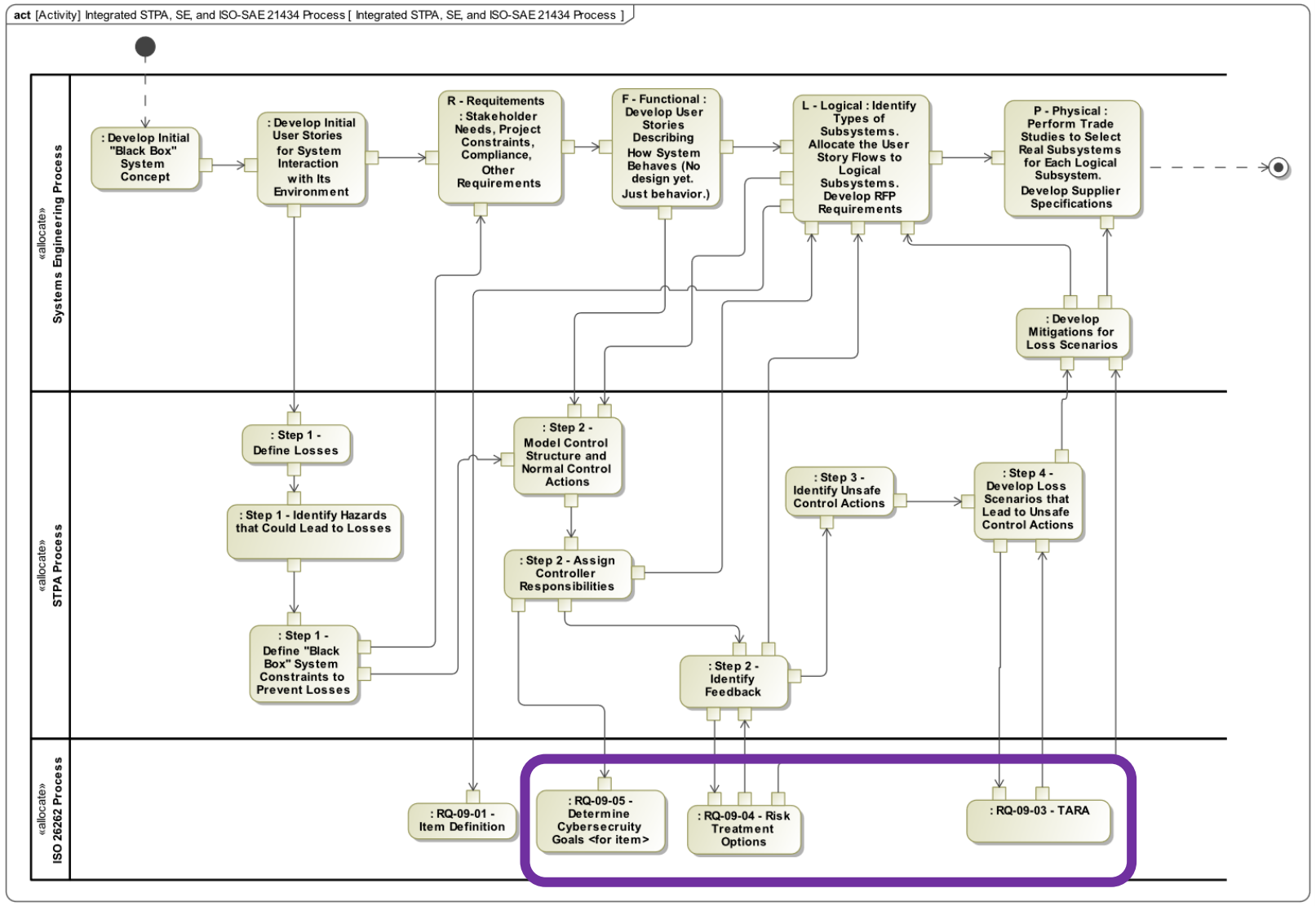
 |

Order of TARA, Treatment, Goals is Rearranged

T6 - ISO/SAE 21434

- The ISO/SAE 21434 order of “TARA”, “Treatment”, “Goals” is illogical.
- (Decide what your goals were after you do the work)
- STPA will rearrange the order.

- ISO/SAE 21434 の「TARA」、「処理」、「目標」という順序は非論理的です。
- （作業完了後に目標を決定してください。）
- STPA が順序を並べ替えます。



 |

T7 - SAE STPA Task Force

Update on the SAE STPA Task Force Standards and Recommended Practices

SAE STPAタスクフォースの標準と推奨プラクティスの最新情報

SAE STPA Task Force

STPA Task Force Objectives:

- To develop a simple straightforward STPA Standard that defines the steps, tasks, and flow necessary to execute a System Theoretic Process Analysis (STPA) system safety evaluation process and outlines the expected deliverables To align STPA best practices across industries regarding the implementation and use of STPA to support hazard evaluations of safety critical applications and to explore areas suited for STPA use and/or for supplementing other safety tools.

J3307_202503 - System Theoretic Process Analysis (STPA) Standard for All Industries

Quality, Testing and Safety, Vehicle Systems and Performance

CURRENT This is a Current Standard 2025-03-24

CURRENT REVISED 2023-05-22

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry J3187_202305

This document provides recommended practices regarding how System Theoretic Process Analysis (STPA) may be applied to safety-critical systems in any industry.

Existing STPA Recommended Practices

CURRENT REVISED 2023-05-22

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry J3187_202305

CURRENT ISSUED 2023-09-06

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Human Machine Interactions (HMIs) J3187-1_202309

CURRENT ISSUED 2023-09-06

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Safety of the Intended Functionality J3187-2_202309

CURRENT ISSUED 2023-09-06

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Model-Based Systems Engineering (MBSE) J3187-3_202309

 |

SAE STPA Task Force

T7 - SAE STPA Task Force

STPA Task Force 2026 – 2027 Objectives:

- Publish new J3187 Recommended Practices appendices – J3187-4 STPA and Security Engineering & J3187-5 STPA and Medical Devices/Processes (Q1 – 2026)
- Update J3187 Recommended Practices base document to coordinate with new J3307 STPA Standard (Q4 – 2026)
- Update J3187-3 STPA and Model Based Systems Engineering appendix based on new info since 2023 (Q2- 2027)
- Consider update to J3307 Standard based on These Recommended Practices updates (Q4 2027)

STPAタスクフォース 2026～2027 目標：

- J3187 推奨プラクティスの付録（J3187-4 STPAとセキュリティエンジニアリング、J3187-5 STPAと医療機器／プロセス）を公開（2026年第1四半期）
- 新しいJ3307 STPA規格と整合させるため、J3187 推奨プラクティスの基本文書を更新（2026年第4四半期）
- 2023年以降の新しい情報に基づき、J3187-3 STPAとモデルベースシステムエンジニアリングの付録を更新（2027年第2四半期）
- これらの推奨プラクティスの更新に基づき、J3307規格の更新を検討（2027年第4四半期）

 |

T8 - Questions

Question and answer session

質疑応答セッション

 |

Thank You!

T8 - Questions

David Hetherington
Austin, Texas

+1 (512) 695-1365
David.Hetherington@asattepress.com
David_Hetherington@ieee.org

 |