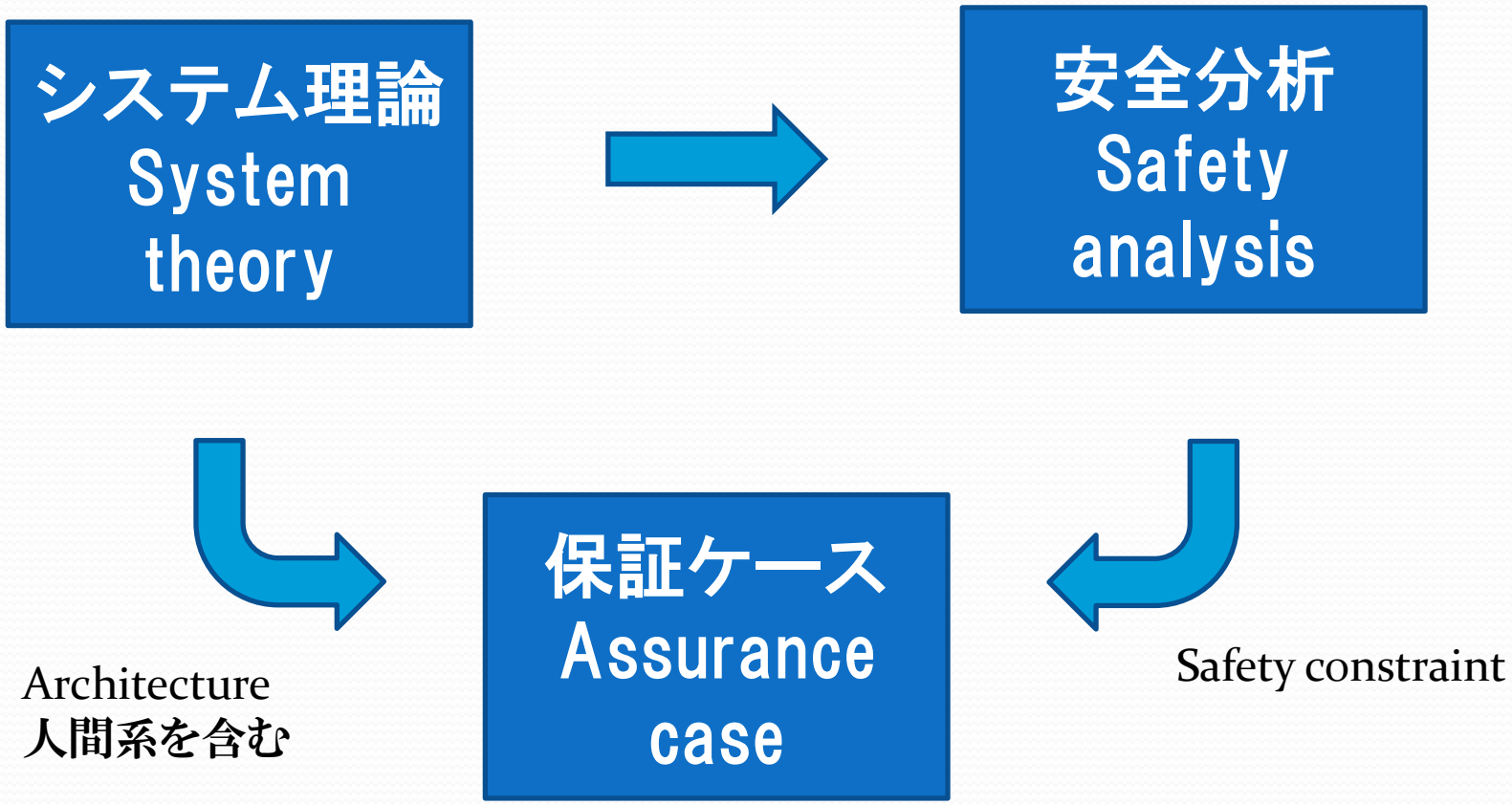
システム理論と保証ケース手法の融合に向けた研究課題

Research Issues for integrating System Theory and Assurance Case

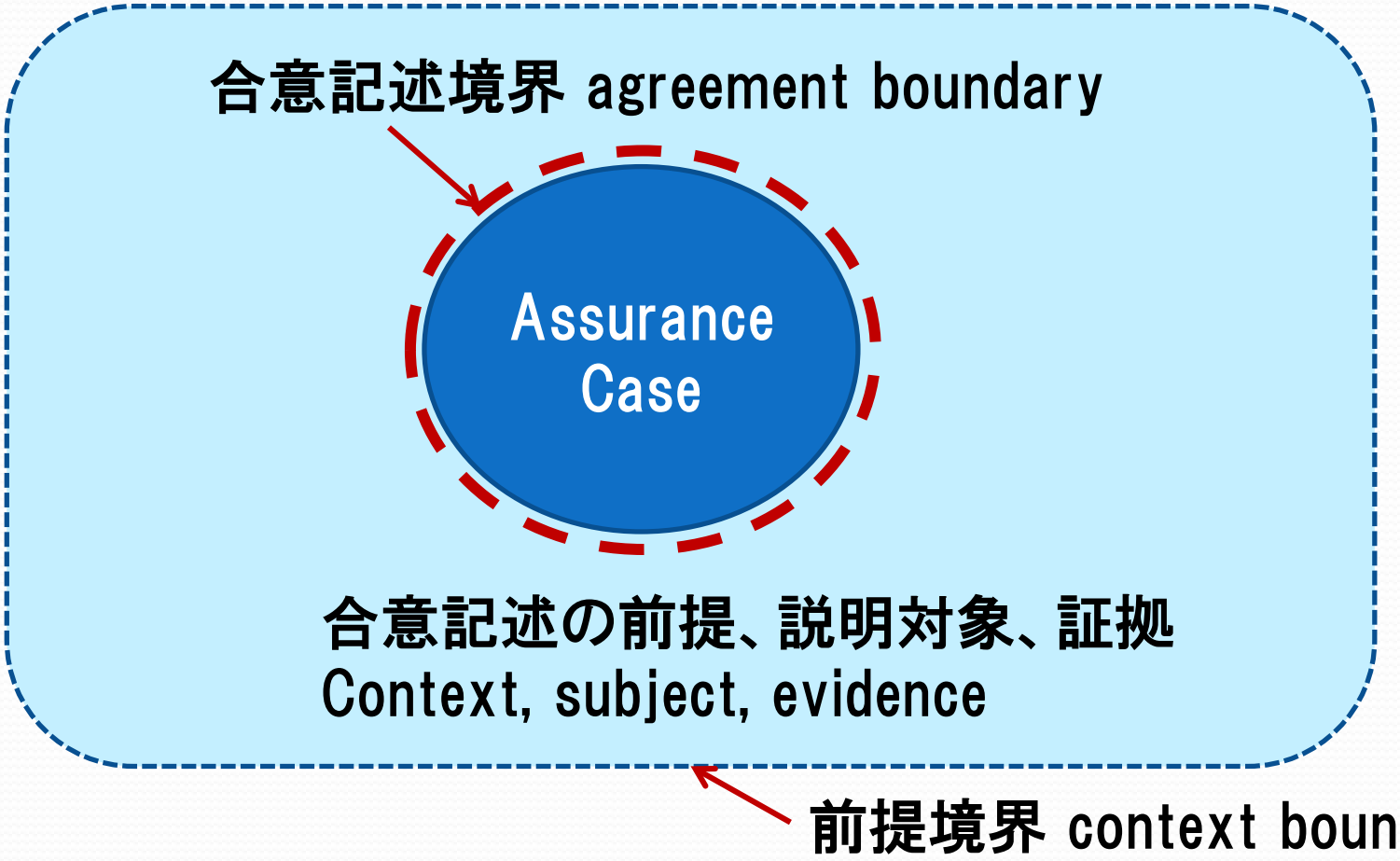
- システム理論 -- System Theory
- STAMP
- 保証ケース　-- Assurance case
- アーキテクチャ指向保証ケース開発法　ABACE
  Architecture Based Assurance Case Engineering
- O-DA -- Open Dependability through Assuredness

名古屋大学大学院情報科学研究科
Nagoya University
山本修一郎 Shuichiro Yamamoto

システム理論、安全分析、保証ケース

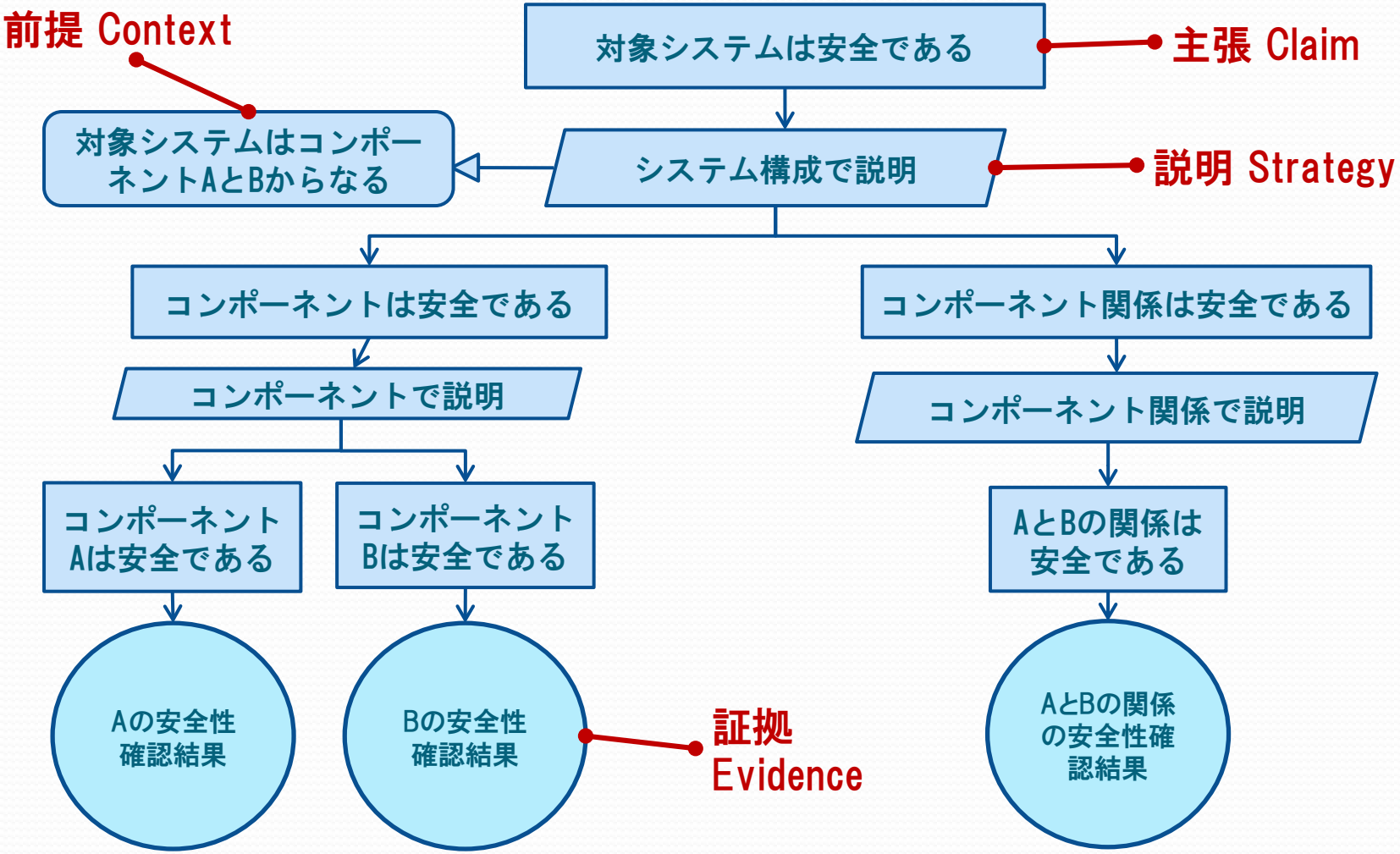


合意記述の前提、記述境界、前提境界



保証ケース - Assurance case

- 証拠によって主張が正しいことを説明する手法

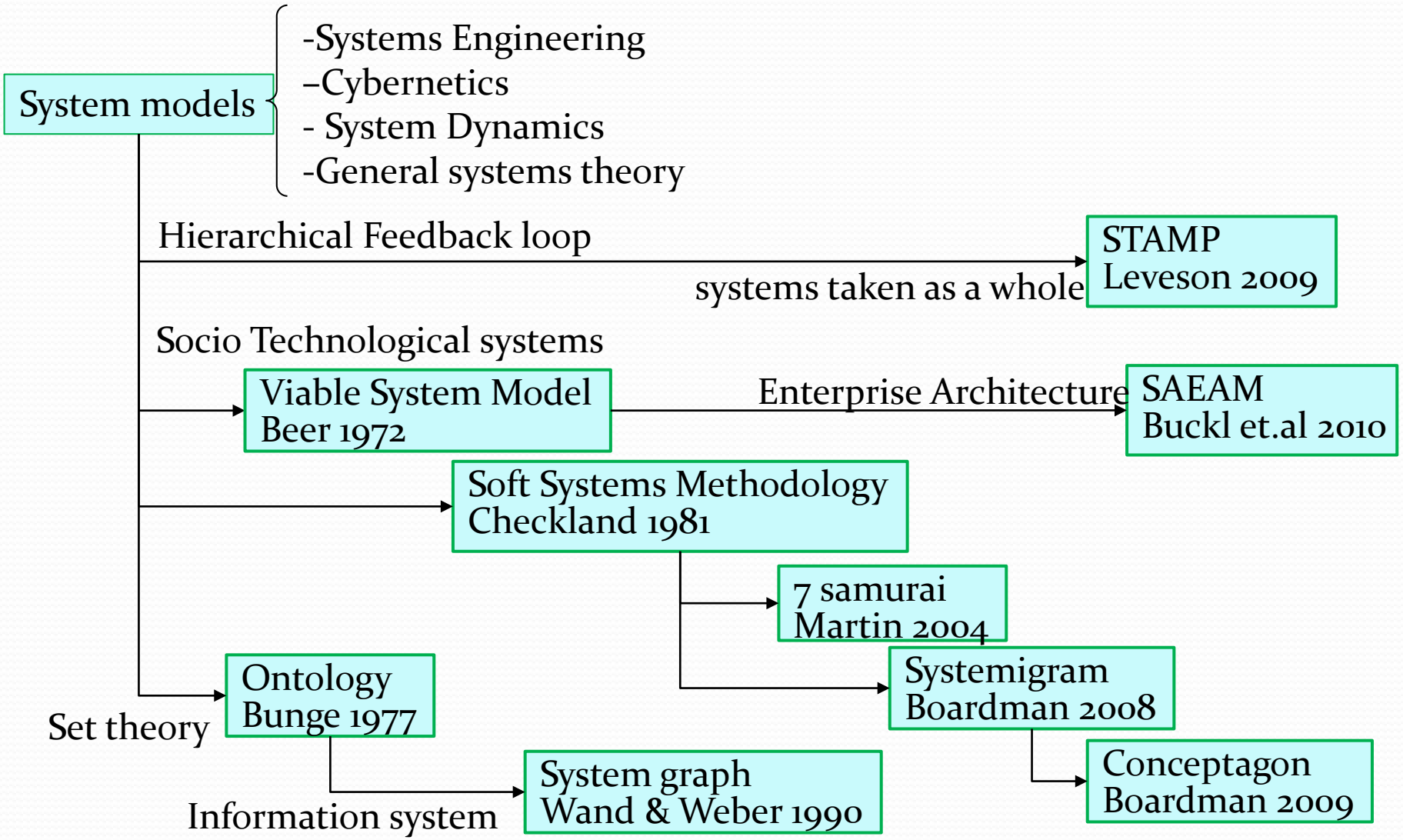


名古屋大学

システム論

System theory

システム論の展開 Evolution of System Theory

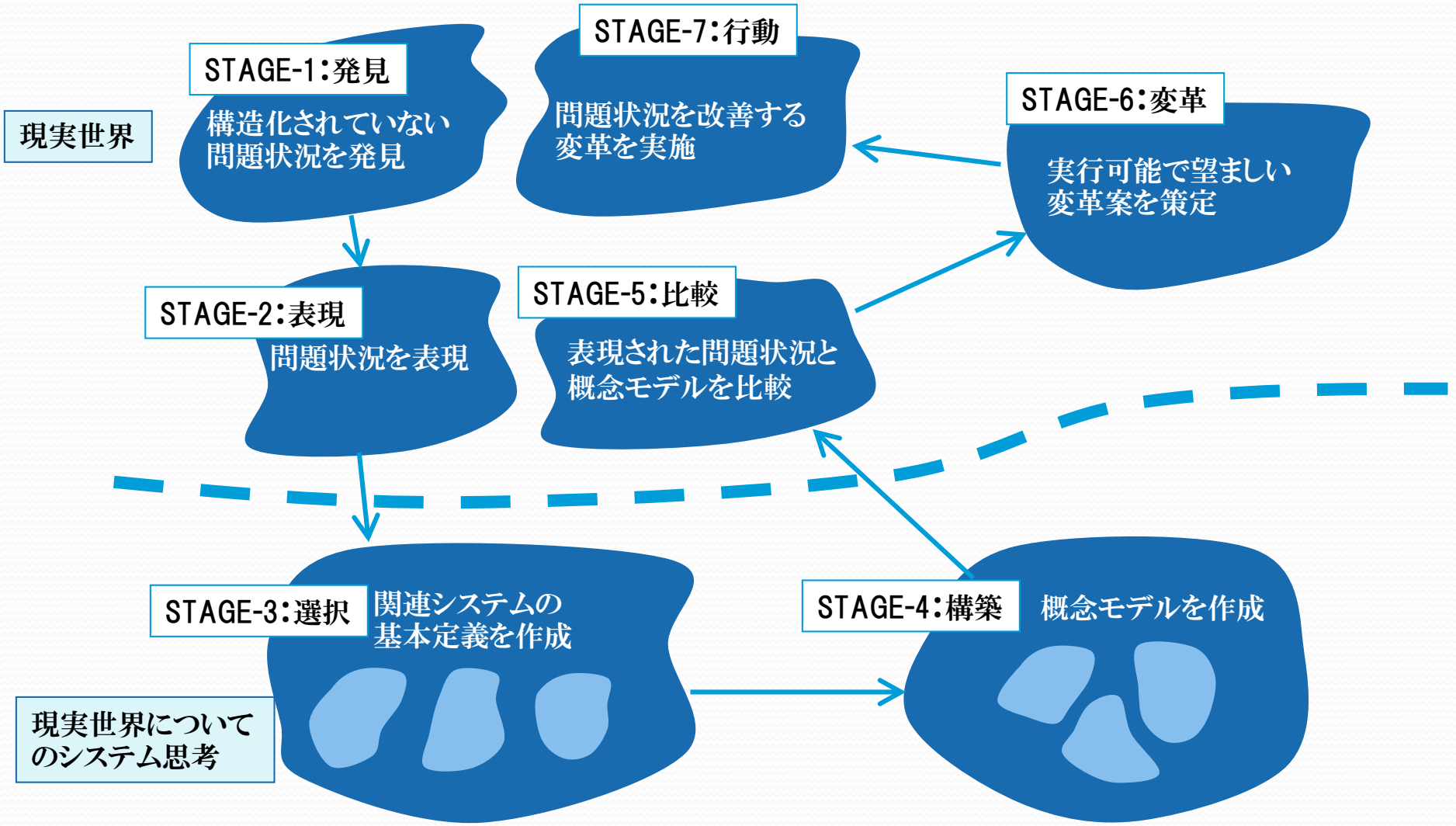


システムとは

- A system S = (T, R) where
  T is a set of things and
  R is a relation defined on T

G. Klir, Facets of System Science, New York: Kluwer, 2001.

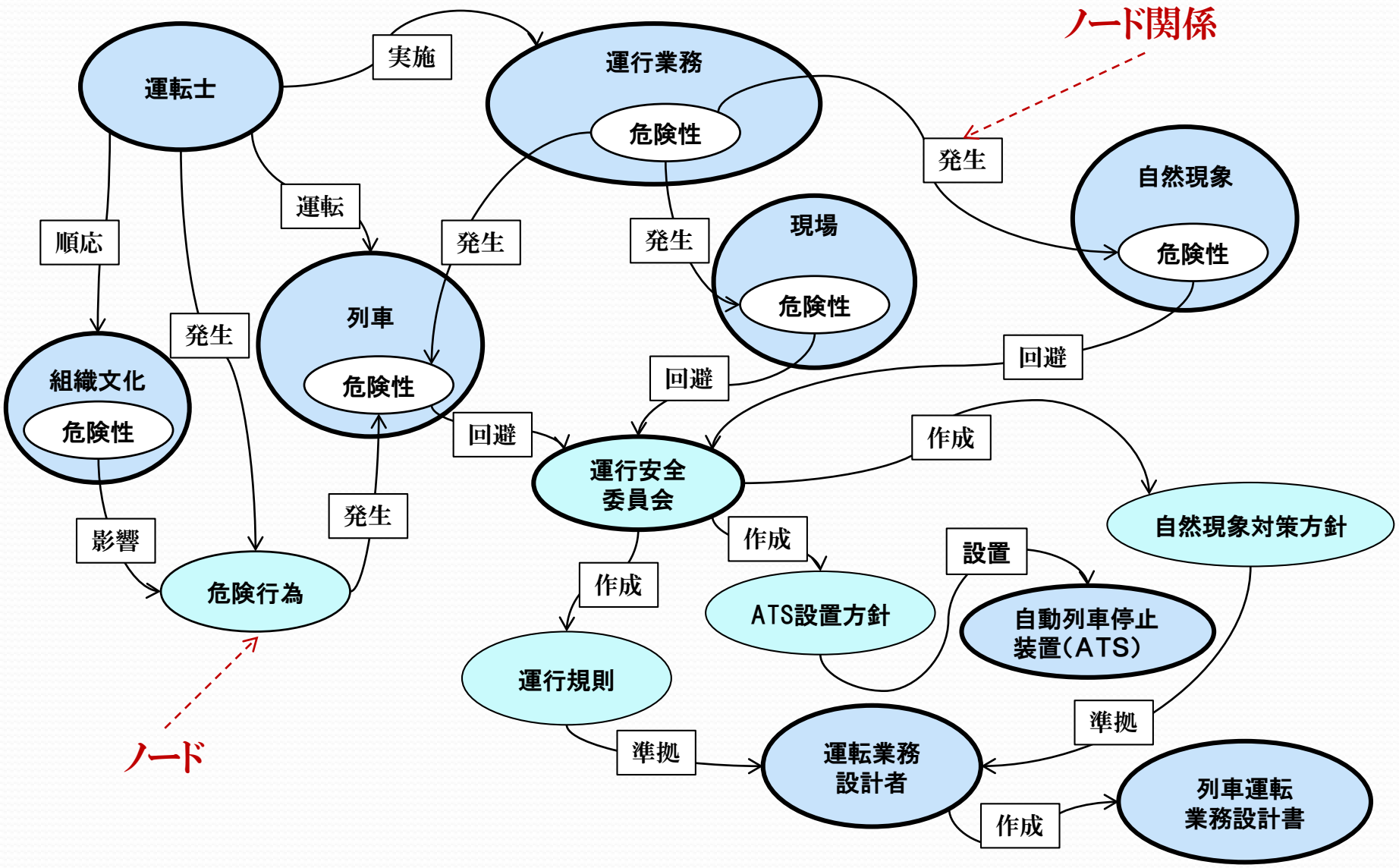
SSM:Soft Systems Methodology



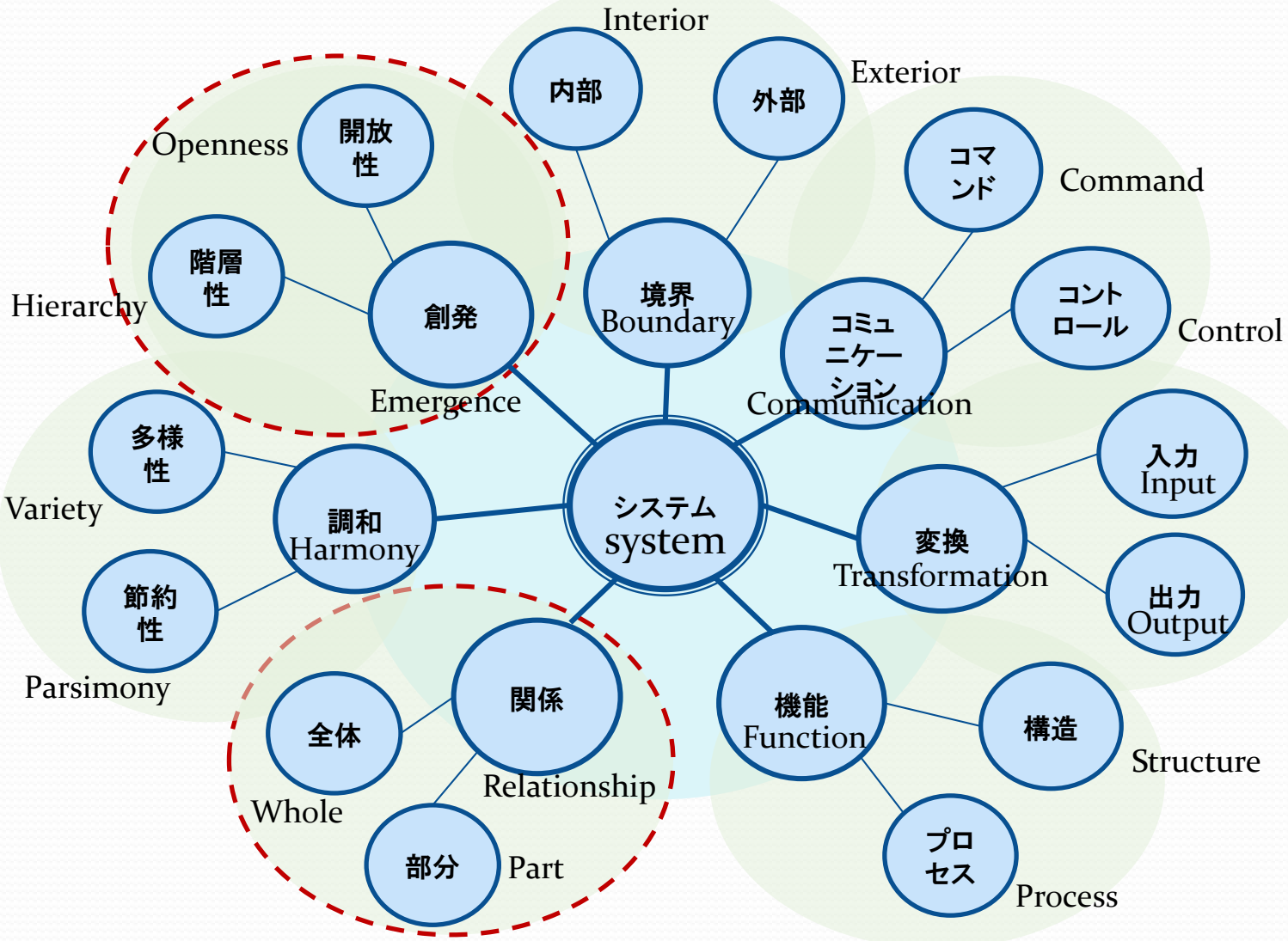
BSSMとSSM

段階	視点	SSM	BSSM
1	状況の抽出	問題状況を分析	同左
2	状況の表現	■適切な選択を可能とするように状況を表現 ■構造とプロセスの相互関係「状況の風潮」	同左
3	基本定義	■特定の視点「世界観」によるシステムの命名 ■問題状況を改善する仮説群	構造化文章により システム要素を定義
4	概念モデル	■入力ー変換ー出力 ■構成要素＝動詞 ■形式化できるシステムとそれを取り巻く環境 ■階層化 ■終了条件	システムミグラム Systemigram によって入力を出力に変換するシステムの行為を記述する
5	比較	■概念モデルによる問題状況の評価 ■反復的な評価	系統的な質問 概念モデルと現実を比較
6	改革案	■構造改革■プロセス改革■行動改革	同左
7	改革の実行	改革による問題状況が解消されることを監視 新たな問題が発生する場合，段階1に戻る	同左

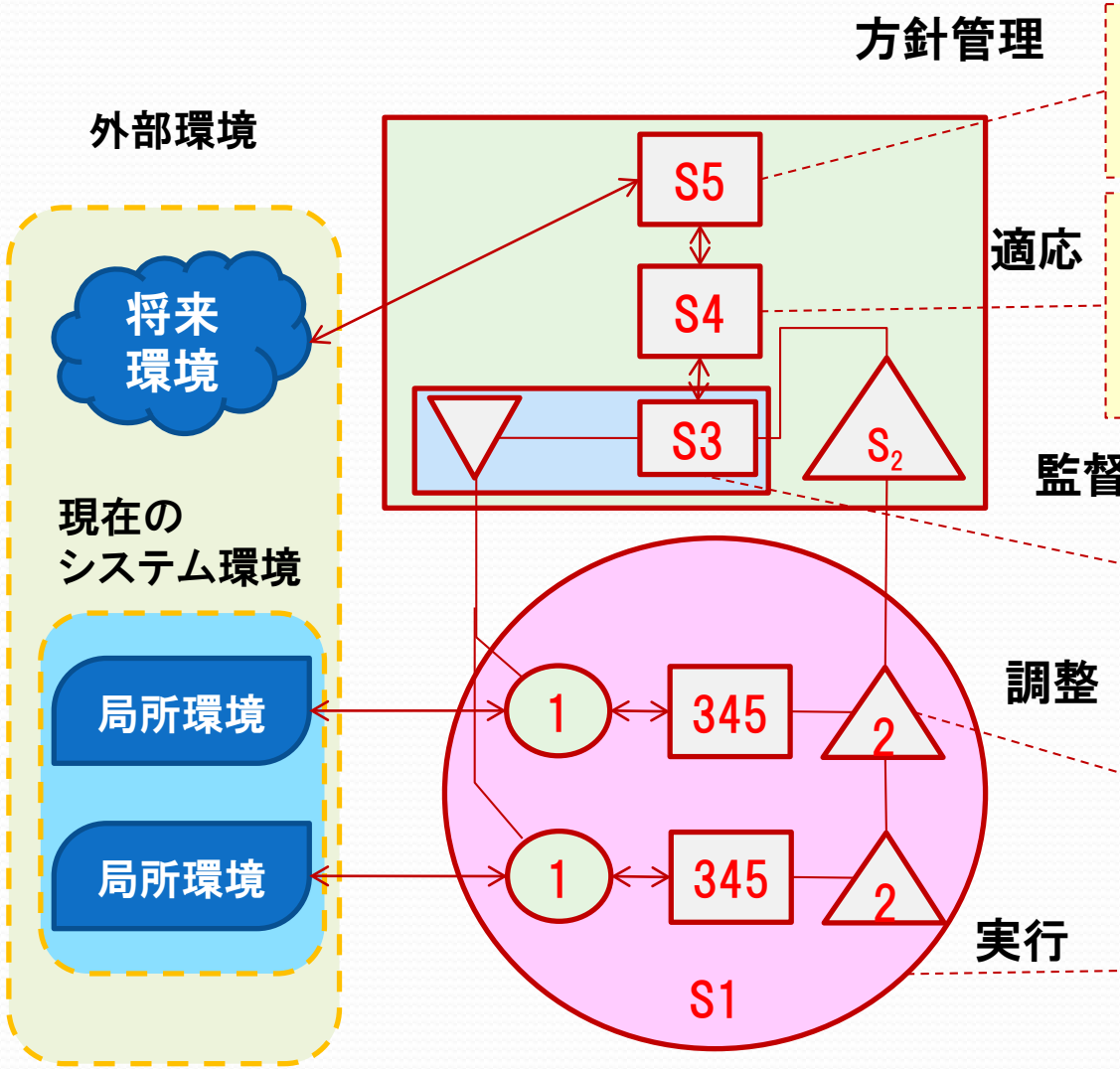
列車運行システムのシステミグラム
systemigram for train operation



コンセプタゴン Conceptagon



VSM -- Viable System Model



ポリシー(S5)
組織全体方針の決定により，現在と未来ならびに，部分全体を均衡

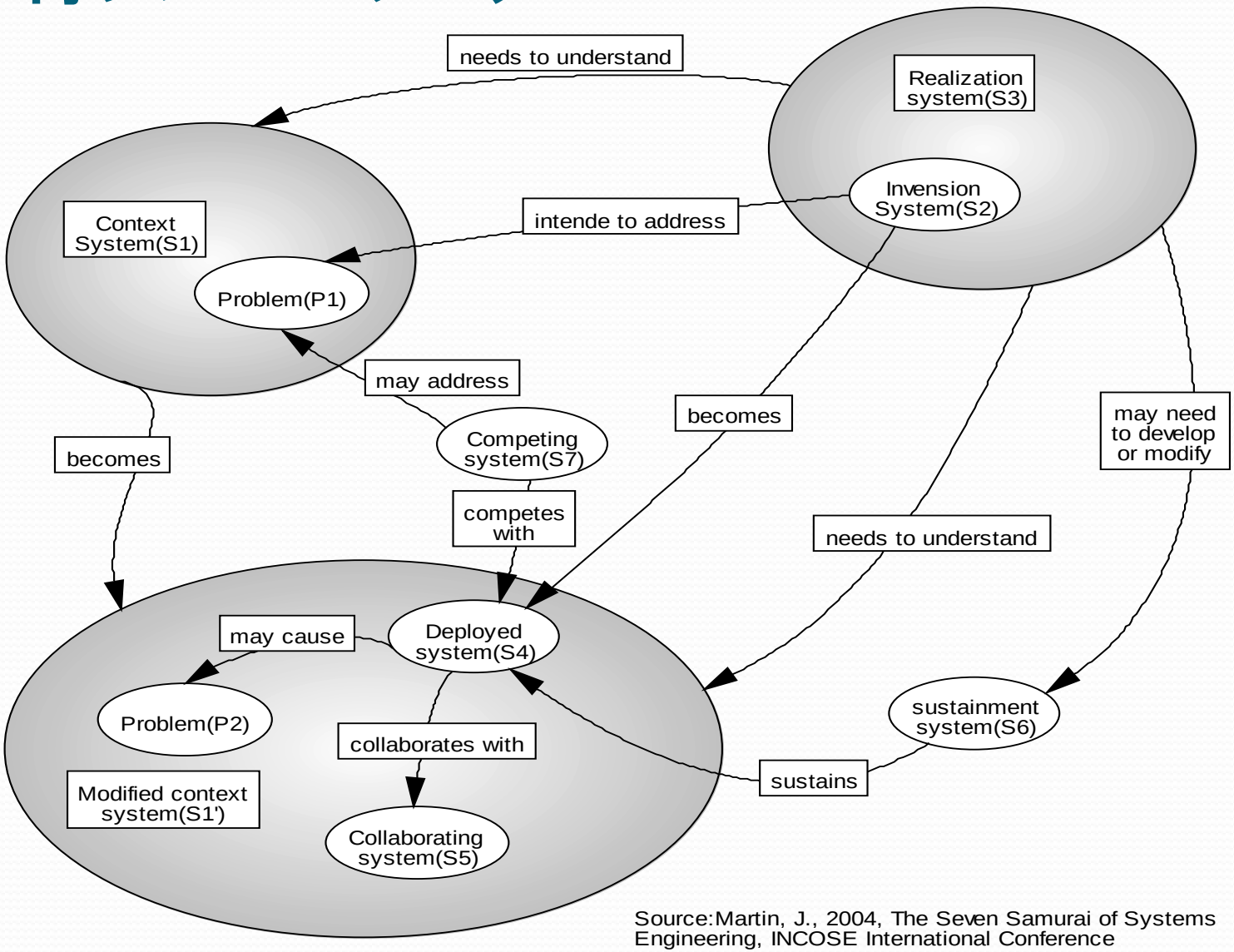
インテリジェンス(S4)
外部環境の変化に対しS3との相互作用により適応
戦略的意思決定と危機管理

コントロール(S3)
S1を制御、S2を監督
システムの資源配置を維持
責任体制の構築と制御

コーディネーション(S2)
S1及びシステム間を調整するための情報チャネル

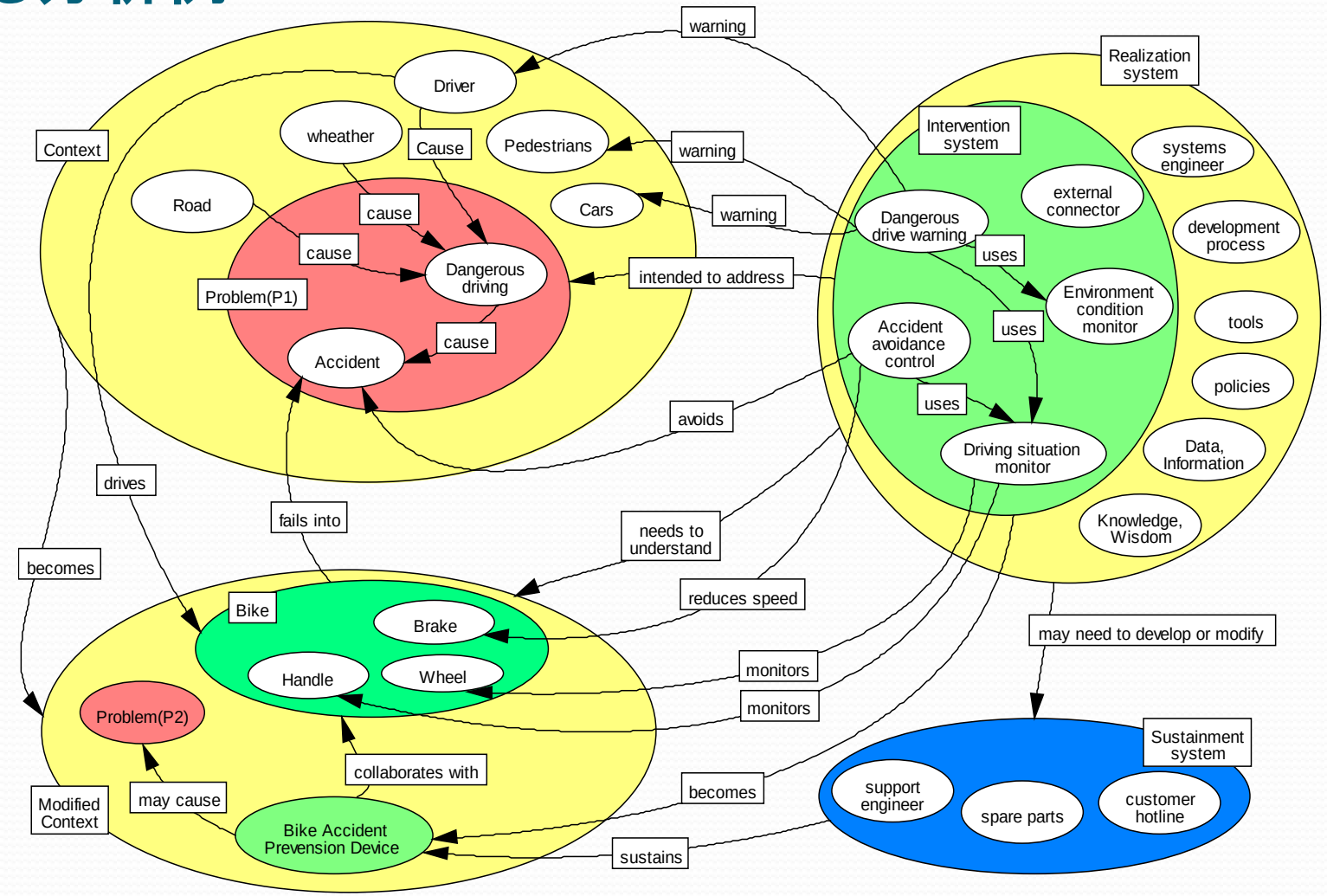
インプリメンテーション(S1)
対象システムの基本活動
環境とのインタフェースを持つ

7人の侍フレームワーク -7 samurai framework

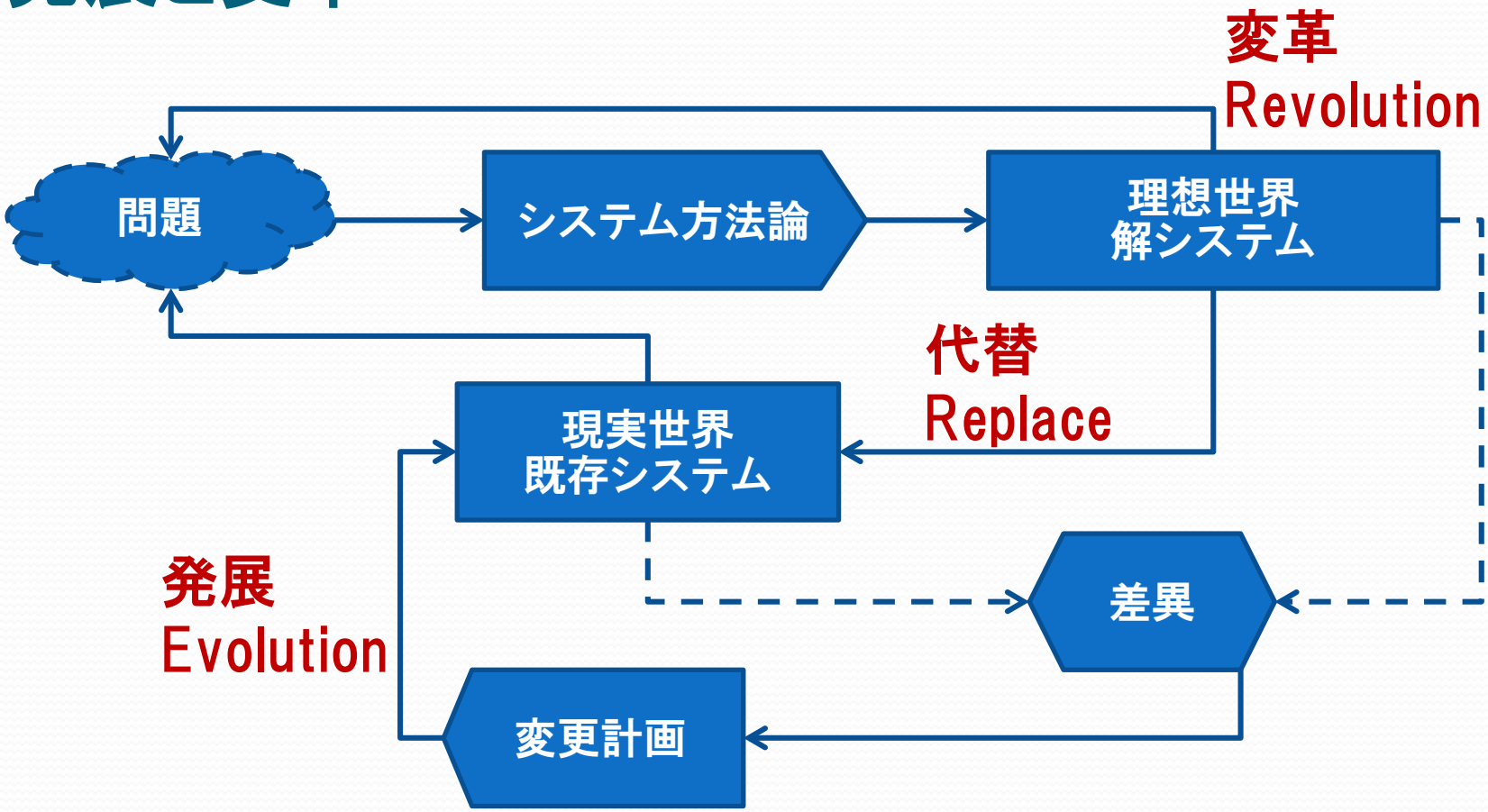


Source:Martin, J., 2004, The Seven Samurai of Systems Engineering, INCOSE International Conference

自転車事故防止システムの7人の侍フレームワークによる分析例



発展と変革



参考) Hitchins, Derek, K., Systems Engineering- A 21st Century Systems Methodology, John Wiley & Sons, Ltd., 2007.

社会技術的システム
socio-technological system

- 技術環境を用いて人々がワークフロープロセスを遂行するシステム

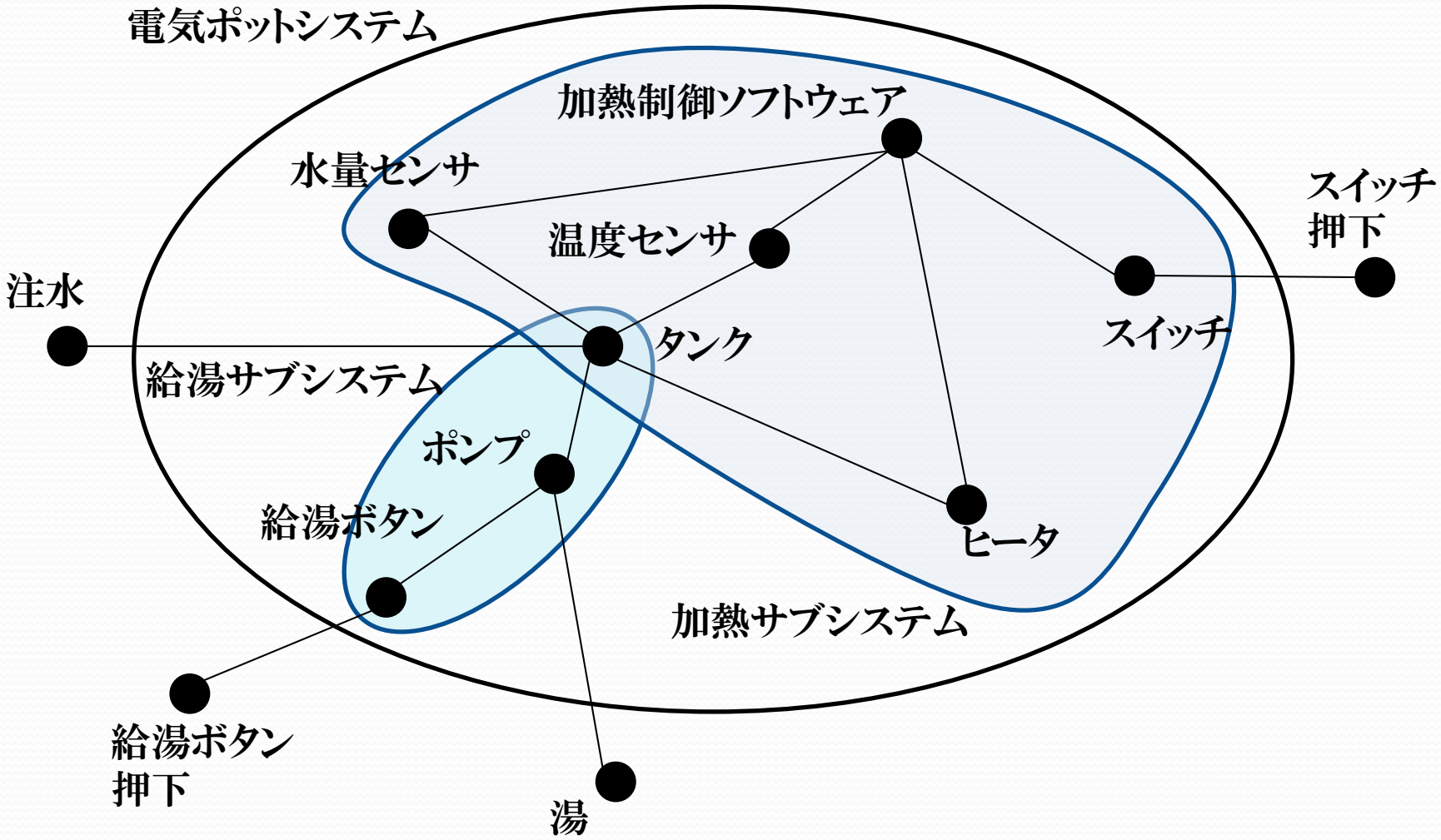
人 People

プロセス Process

技術環境 Technology environment

参考) Rebovich, G., and Brian, W., Enterprise Systems Engineering – Advances in Theory and Practice, CRC Press, 2011.

電気ポットのシステムグラフ – system graph of electric pot



STAMP

Systems-Theoretic Accident Modeling and Processes

名古屋大学

アーキテクチャ指向保証ケース開発法

ABACE, Architecture Based Assurance Case Engineering

アーキテクチャとは

- An Architecture A = (C, R, P) where
  C is a set of components
  R is a relation defined on C and
  P is a property that C and R satisfy

ABACEの手順

【手順1】まず、アーキテクチャを構成する3要素である対象システムの構成要素Cと関係Rならびに、対象システムが満たすべき品質特性Pを定義する。

【手順2】次いで、アーキテクチャに基づいて、最上位主張「システムが品質特性を満たす」を作成する。

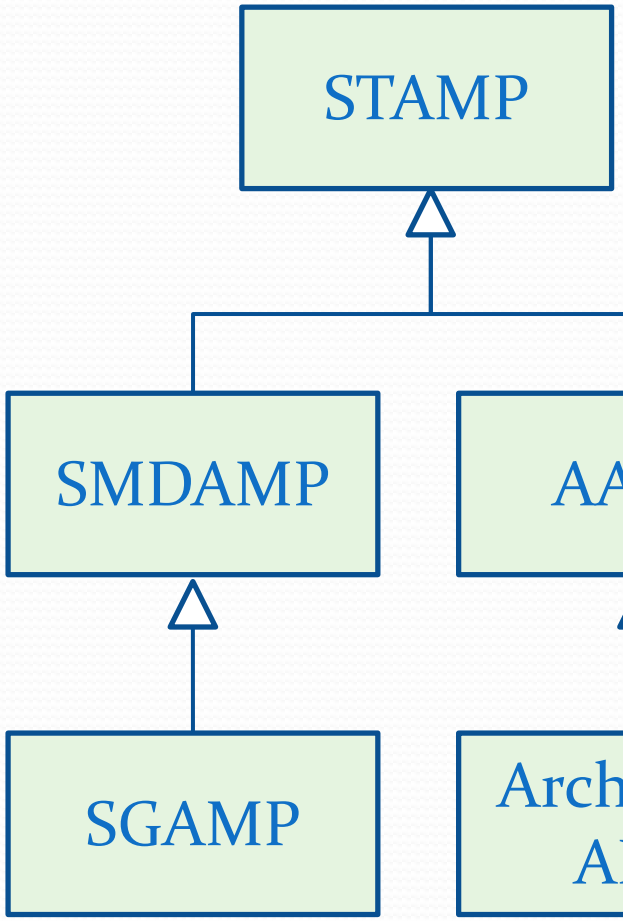
【手順3】さらに、最上位の主張を、構成要素とその関係に基づいて、2つの下位の主張「構成要素は品質特性を満たす」と「構成要素関係は品質特性を満たす」に分解する。

【手順4】この2つの主張を、それぞれ、構成要素と構成要素関係の実体ごとに下位の主張に分解していく。

【手順5】最終的に、すべての構成要素と構成要素関係の実体が品質特性を満たすという主張に分解されたら、これらの主張が成立する上でのリスクに対策できているという主張に分解する。

【手順6】リスクに対応できているという主張ごとに、それを説明する証拠を作成する。

STAMPの具体化



System Theoretic Accident Modeling and Process

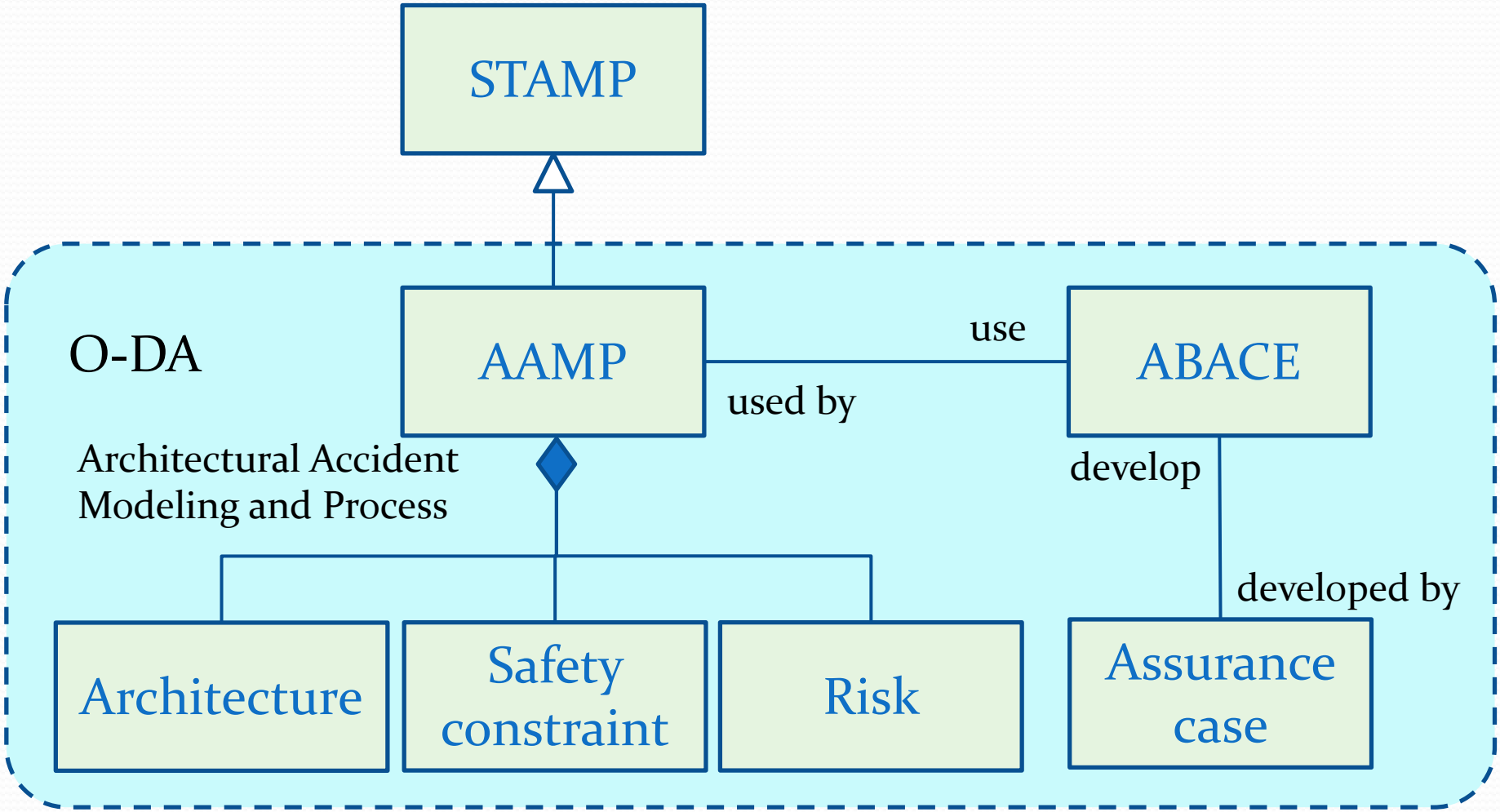
System Model Driven Accident Modeling and Process

Architectural Accident Modeling and Process

System Graph Accident Modeling and Process

ArchitMate Accident Modeling and Process

STAMPと保証ケース

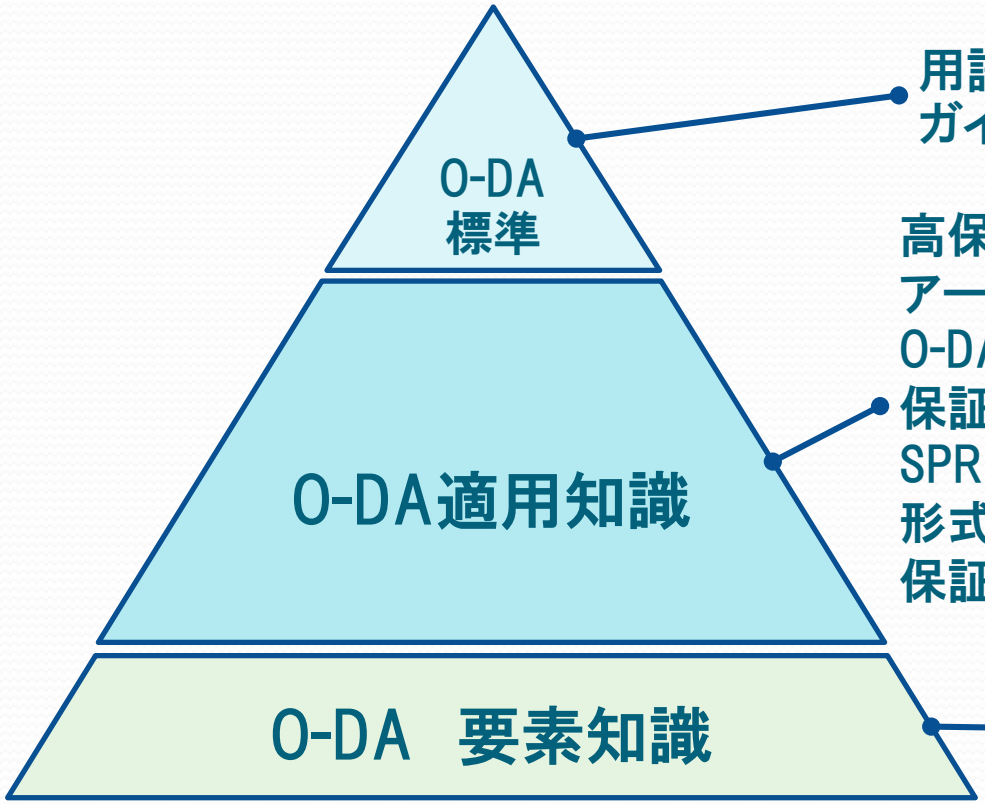


O-DA: Open Dependability through Assuredness

O-DAとは

Dependability through Assuredness™ (O-DA) Framework
Open Group Standard, 2013

O-DA標準の知識体系



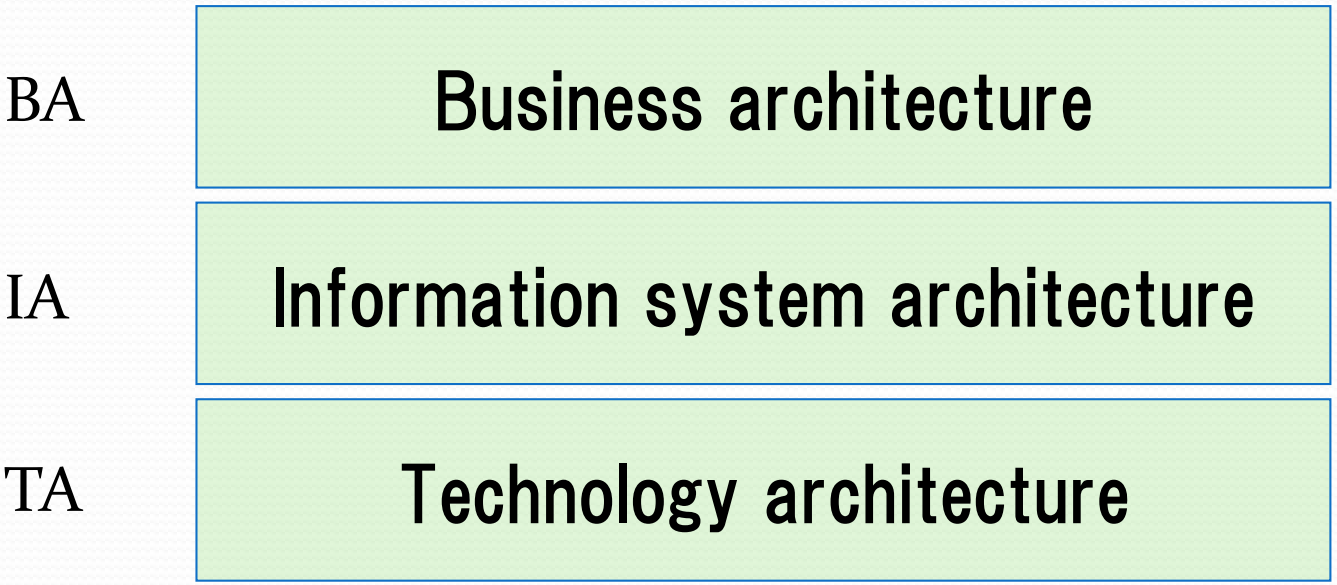
用語定義、フレームワーク、
ガイドライン、形式手法の位置づけ

高保証ADM(Assured ADM)
アーキテクチャ指向保証ケース開発法(ABACE)
O-DAテンプレート、O-DA適用事例
保証ケースレビュ手法
SPRME(対象、品質特性、リスク、対策、証拠)
形式的ABACE(FABACE)
保証ケース導入準備能力評価指標

TOGAF、ADM(Architecture
Development Method)、ArchiMate、
保証ケース、形式手法

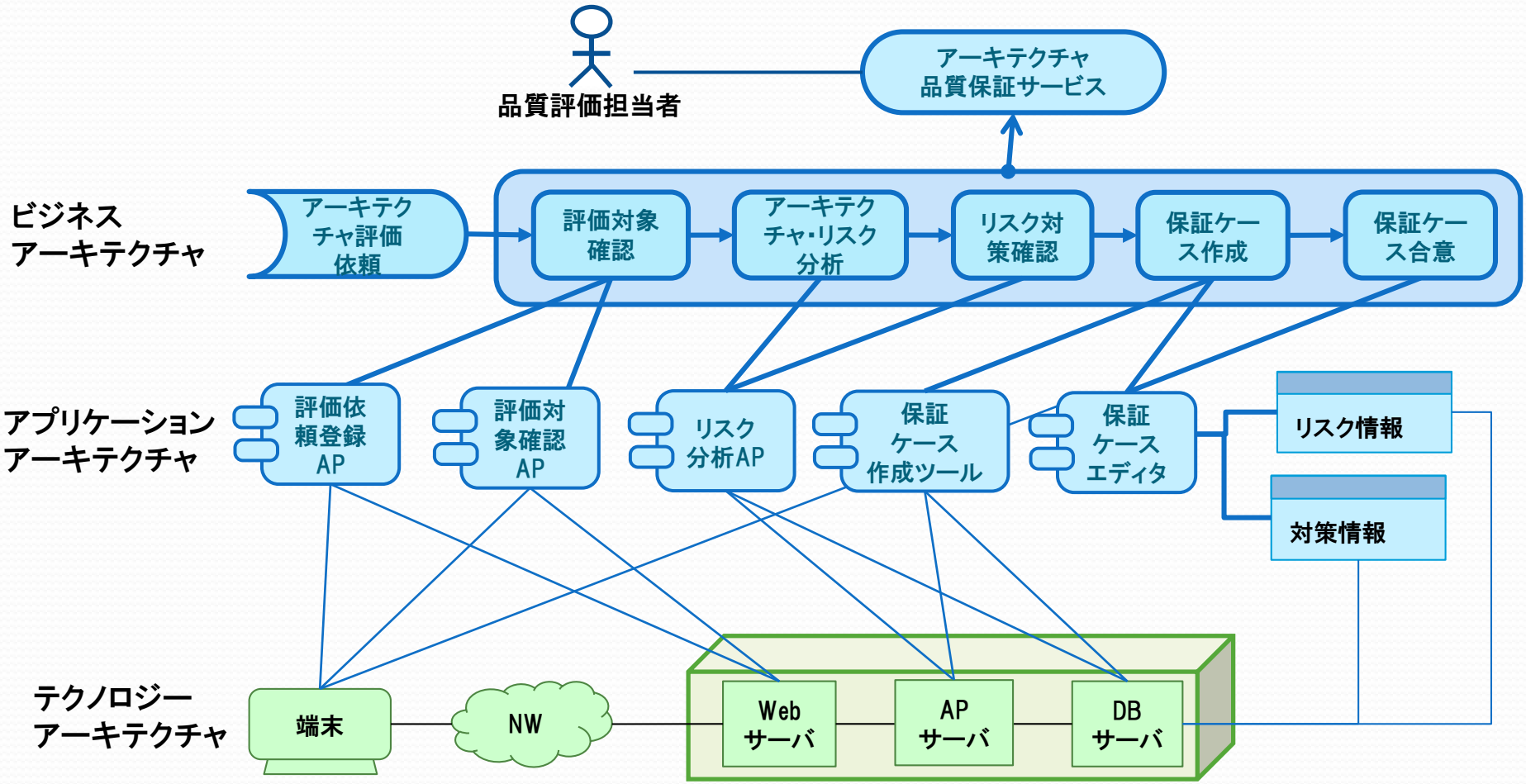
Enterprise Architecture

- 技術環境を用いて人々がビジネスプロセスを遂行するシステム



参考) TOGAF®, an Open Group Standard; www.opengroup.org/togaf.

ArchiMateによるアーキテクチャ品質保証サービス



高保証アーキテクチャ Assured Architecture

- 指定された保証すべき性質が実現されているアーキテクチャを高保証アーキテクチャ(Assured Architecture)という.

- 保証(Assurance)
  - アーキテクチャが高保証性を持つことを確認すること

- 保証ケース(Assurance case)
  - 保証するための議論構造を記録する成果物

TOGAF ADMフェーズ

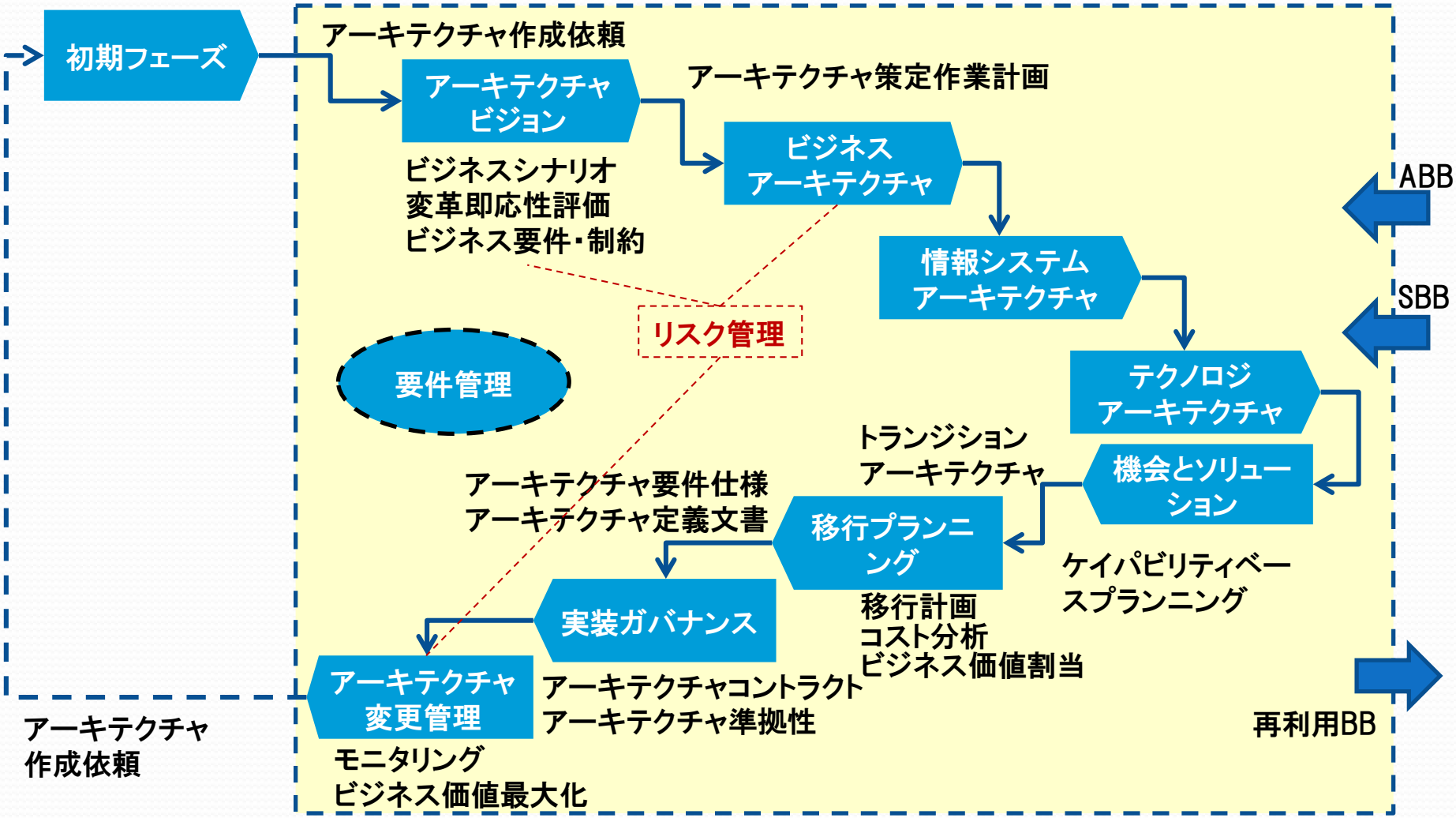


ABB: Architecture Building Block
SBB: Solution Building Block

高信頼ADMの概要

工程	AADM
P.準備	①アーキテクチャリポジトリでの証拠文書と保証ケースの格納 ②ディペンダビリティ委員会での主張間の優先順位の合意
A.アーキテクチャビジョン	①ディペンダビリティスコープ定義 ②主張の定量評価尺度定義 ③保証ケース能力評価 ④ディペンダビリティパラメタ定義
B.ビジネスアーキテクチャ	①ディペンダビリティ原則定義 ②BA保証ケース作成 ③BA保証ケースレビュ
C.情報システムアーキテクチャ	①IA保証ケース作成 ②IA保証ケースレビュ
D.技術アーキテクチャ	①TA保証ケース作成 ②TA保証ケースレビュ
E.機会とソリューション	①BA, IA, TA保証ケースを統合 ②一貫性を確認
F.移行計画	①運用管理の保証ケース作成 ②ディペンダビリティパラメタ価値分析
G.実装ガバナンス	①保証ケースの証拠を作成 ②プロセス保証ケースの証拠を作成 ③網羅的に主張と証拠の関係を確認 ④運用に対する保証ケースをレビュ
H.アーキテクチャ変更管理	①運用保証ケースの証拠を管理 ②主張の不成立への対応策の確認③保証ケースによるリスク管理 ④保証ケースによる障害分析
R.要求管理	保証ケースの主張と要求の追跡管理

Ref. *Open Group Standard,* **Real-Time and Embedded Systems:, Dependability through Assuredness™ (O-DA) Framework, 2013**

AADM に対するO-DA適用法

凡例：■提案済み　■提案予定

O-DA適用法	AADMの活動
■システム論的事故分析保証手法	①システムグラフを用いた障害分析と保証ケース作成
■証拠作成法	①保証ケースの証拠を形式手法で作成（FABACE） ②プロセス保証ケースの証拠を作成
■アーキテクチャ・リポジトリ	①アーキテクチャリポジトリでの証拠文書と保証ケースの格納②保証ケースの主張と要求の追跡管理③保証ケースの証拠を管理
■リポジトリ活用法	①網羅的に主張と証拠の関係を確認 ②主張の不成立への対応策の確認 ③保証ケースによるリスク管理
■主張間の優先順位	①ディペンダビリティ委員会での主張間の優先順位の合意 ②主張の定量評価尺度定義　③ディペンダビリティパラメタ定義 ④ディペンダビリティパラメタ価値分析
■スコープ定義	①ディペンダビリティスコープ定義②ディペンダビリティ原則定義
■アーキテクチャ指向保証ケース作成法 ABACE	①BA保証ケース作成②IA保証ケース作成　③TA保証ケース作成　④BA, IA, TA保証ケースを統合⑤運用管理の保証ケース作成 ⑥一貫性を確認
■保証ケースレビュ手法	①BA保証ケースレビュ ②IA保証ケースレビュ ③TA保証ケースレビュ ④運用に対する保証ケースをレビュ
■保証ケース導入能力評価指標	①保証ケース能力評価

FABACE = Formal Evidence + ABACE

- 検証すべき形式的証拠(TBV, To Be Verified)の分類

分類	検証内容
TBV1	コンポーネントの入出力の関係
TBV2	コンポーネントの事前条件と事後条件の関係
TBV 3	コンポーネント間の相互作用の正当性
TBV 4	コンポーネント間の一貫性

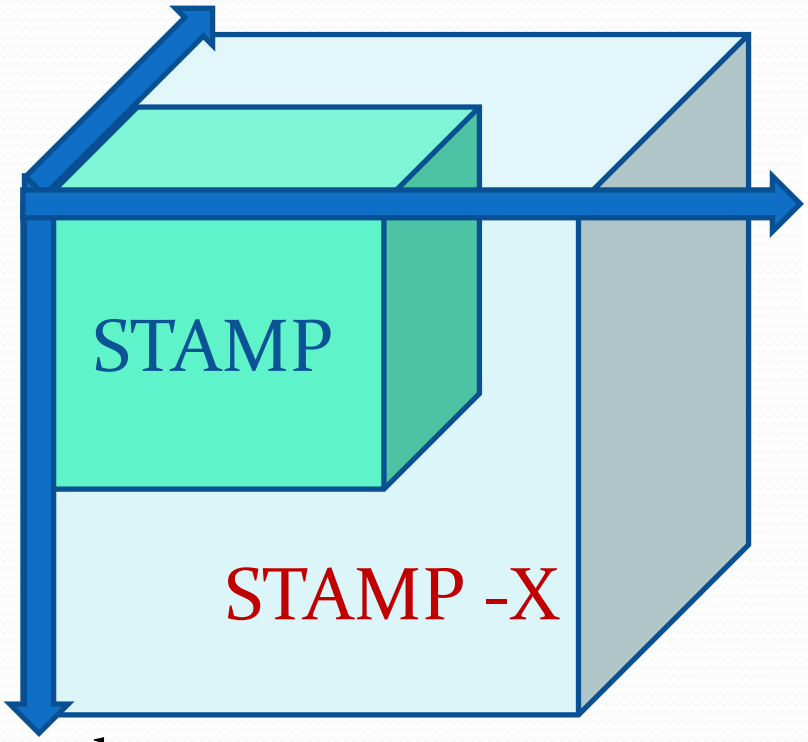
形式手法の例： B, Event-B, VDM, SPIN, UPAAL

まとめ

- システム理論
- STAMP
- 保証ケース
- アーキテクチャ指向保証ケース開発法
- O-DA

STAMPの境界　Boundary of STAMP

Process boundary　プロセスの品質保証



AM boundary
事故モデルの構造

ST boundary
多様なシステム理論への展開

現代エンタープライズ・アーキテクチャ概論 - ArchiMate入門

本書では,エンタープライズ・アーキテクチャのモデリングと,その高信頼性を保証するための基本的な知識を踏まえて、日本から提案したO-DA(Open Dependability Through Assuredness)標準とその具体的な適用事例についても解説している.

現代エンタープライズ・アーキテクチャ概論 - ArchiMate入門
(MyISBN - デザインエッグ社)
2016/7/20
山本 修一郎

保証ケース作成支援方式の研究成果

http://de-science.icts.nagoya-u.ac.jp/download.html

- 保証ケース統合作成支援ツール
- 教材[保証ケースレビュ手法]
- 教材[統一的保証ケース]
- 保証ケース導入能力評価指標

本研究は，独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター（SEC: Software Reliability Enhancement Center）が実施した「2015 年度ソフトウェア工学分野の先導的研究支援事業」の支援を受けたものです．