JTEKT

JTEKT Koyo TOYODA

第二回 DEOS協会　ｵｰﾌﾟﾝｼｽﾃﾑ･ﾃﾞｨﾍﾟﾝﾀﾞﾋﾞﾘﾃｨ ｼﾝﾎﾟｼﾞｳﾑ
～　自動車・航空宇宙分野における総合信頼性の実現に向けて　～

自動車業界における論証フレームワーク

ｼﾞｪｲﾃｸﾄ 株式会社
ｽﾃｱﾘﾝｸﾞ ｼｽﾃﾑ事業部
米木 真哉

Value & Technology
技に夢を求めて 価値ある技術をあなたのもとへ

Safety Caseに関する豆知識

- 豆知識 1
  - 証拠(evidence)のない論証(argument)は根拠がない
  - 議論(argument)のない証拠(evidence)は説明できない

- 豆知識 2
  - Safety case = **"the case of safety (安全の具体的な事例)"**
    - 文書の存在には依存しない安全の事例もある
    - ｾｰﾌﾃｨｹｰｽ報告書はｾｰﾌﾃｨｹｰｽを纏めるための一手段に過ぎない

- 豆知識 3
  - 論証では、主張の組合せによって、その上位の主張が満たされていることを演繹的に証明することはほとんどできない。
    - 保証が不足する部分が存在する。
    - 論証を文書化することの目的は、そのような不足を理解させ、許容、または受け入れられないかを判断できるようにすることである。

ISO/FDIS 26262でのSafety Case(その1)

- ISO 26262-1:2011
  - argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development
    NOTE Safety case can be extended to cover safety issues beyond the scope of ISO 26262.
- ISO/FDIS 26262-1
  - argument that functional safety is achieved for safety-related products, such as items, systems, elements, and satisfied by evidence compiled from work products of the safety activities during development.
    NOTE Safety case can be extended to cover safety issues beyond the scope of the ISO 26262 series of standards.

主張(claim):
1st edition → ｱｲﾃﾑの安全要求が完全で満足されていること
2nd edition → 機能安全が達成されてること

2nd editionでは主張が機能安全の達成に明確化される見込み。

ISO/FDIS 26262でのSafety Case(その2)

- ISO 26262-2:2011

  6.4.6 Safety case

  6.4.6.1 This requirement shall be complied with for items that have at least 1 safety goal with an ASIL (A), B, C, or D: a safety case shall be developed in accordance with the safety plan.

  6.4.6.2 The safety case should progressively compile the work products that are generated during the safety lifecycle.

- ISO/FDIS 26262-2

  6.4.8 Safety case

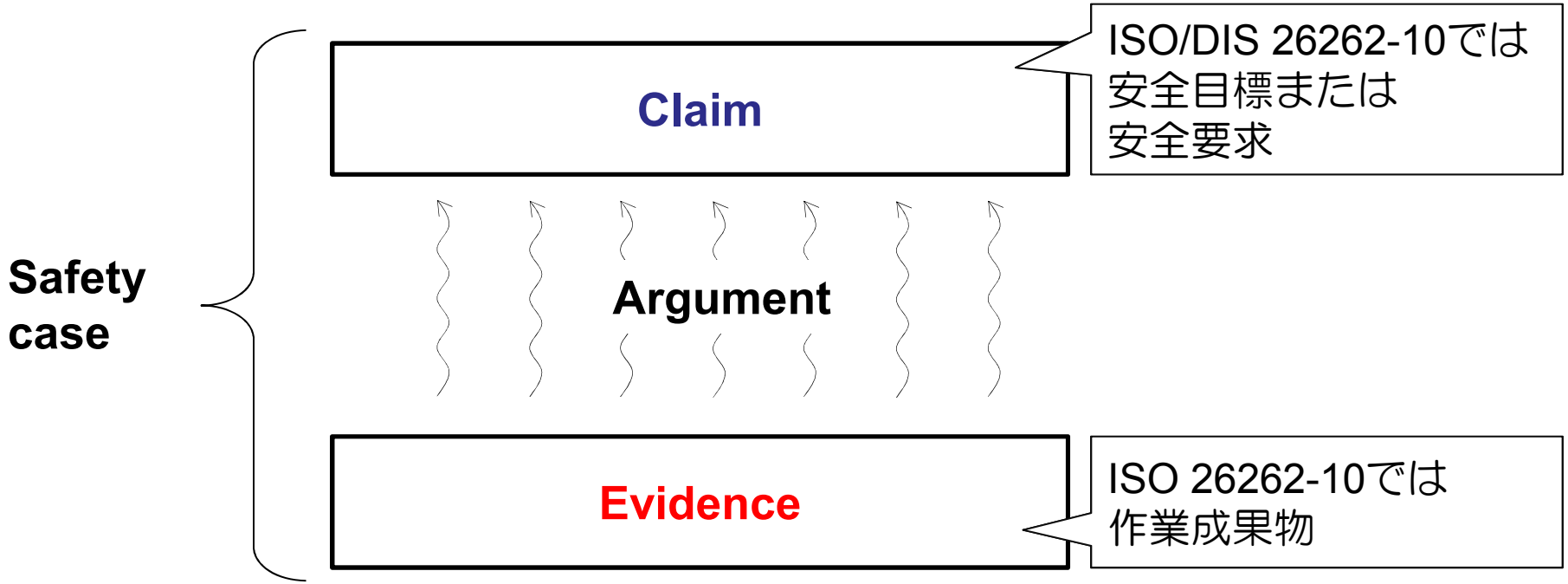
  6.4.8.1 A safety case shall be developed, in accordance with the safety plan, **in order to provide the argument for the achievement of functional safety.**.
  ⇒ 目的は機能安全の達成の論証を提供するため

  6.4.8.2 The safety case should progressively compile the work products that are generated during the safety lifecycle **to support the safety argument.**
  ⇒ 安全論証をｻﾎﾟｰﾄするために、作業成果物を段階的に編纂

2nd editionではargument(論証)が協調された書き方になる見込み。

Clam, Argument, Evidence

■ ISO 26262-10の図6のように表すと下のようになる。



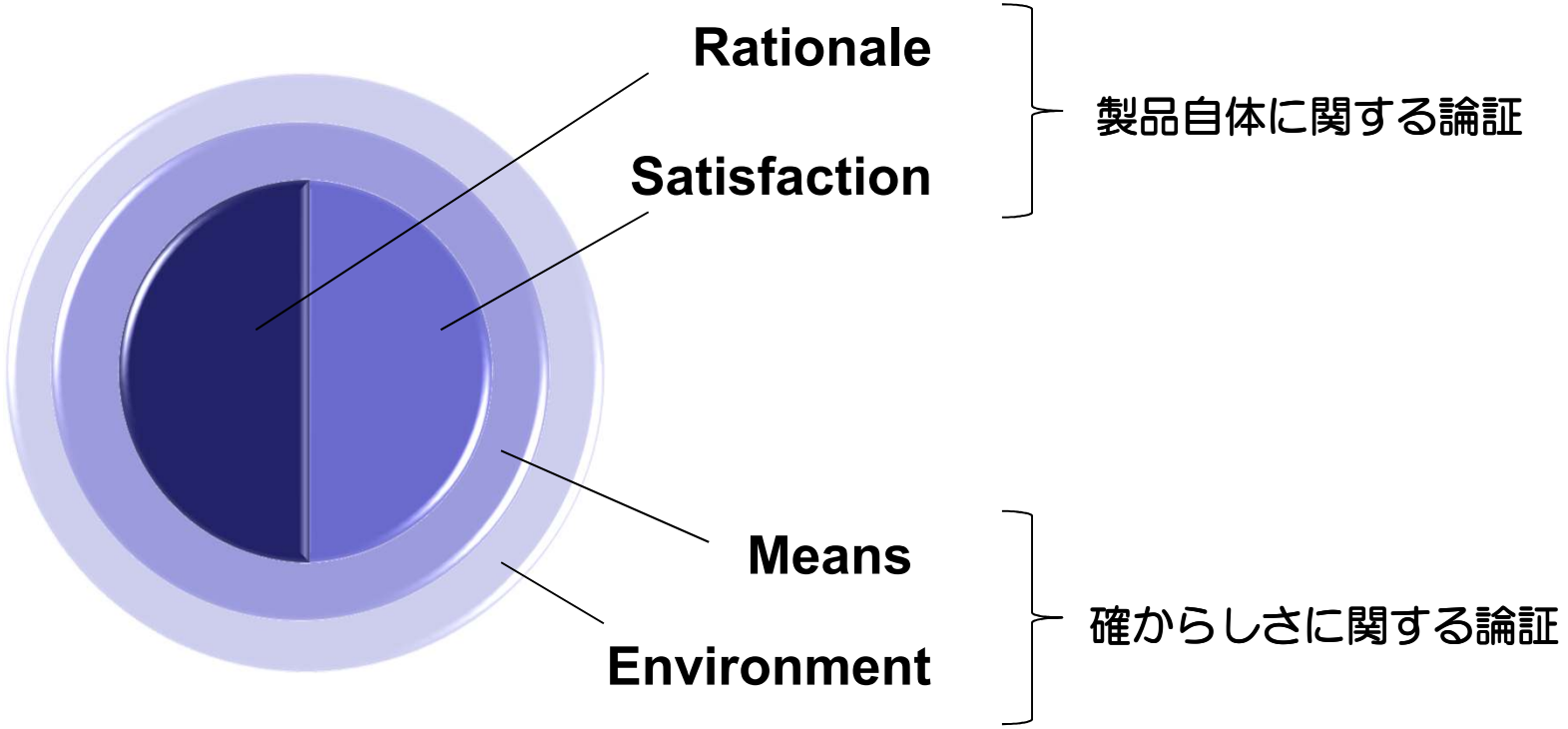
注)
ISO/FDIS 26262-1の定義の見直し、およびISO/FDIS 26262-2のsafety caseに対する要求事項の変化に完全には追従していない。

MISRAの取り組み

- MISRAでは自動車向けの safety case 開発のためのｶﾞｲﾄﾞﾗｲﾝ "Guidelines for Automotive Safety Case Arguments" を2017年の発行を目指して作成中。
  - 2016年11年にpublic comment募集実施
  - 現在はｺﾒﾝﾄを踏まえて内容をﾌﾞﾗｯｼｭｱｯﾌﾟ中(?)

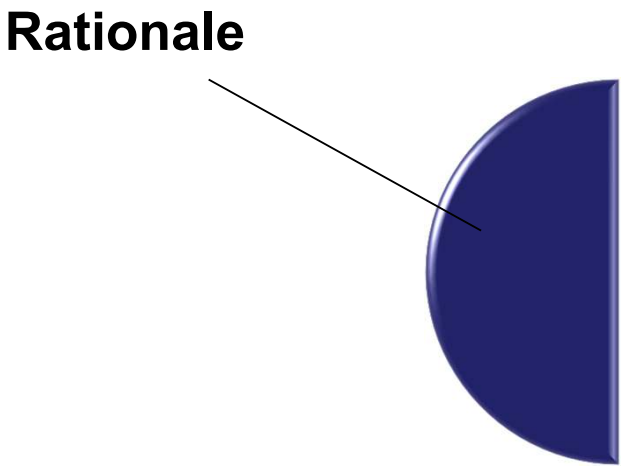
MISRAのArgument Model

■ 4つの論証で安全である事を主張する。



4つのargument- Rationale

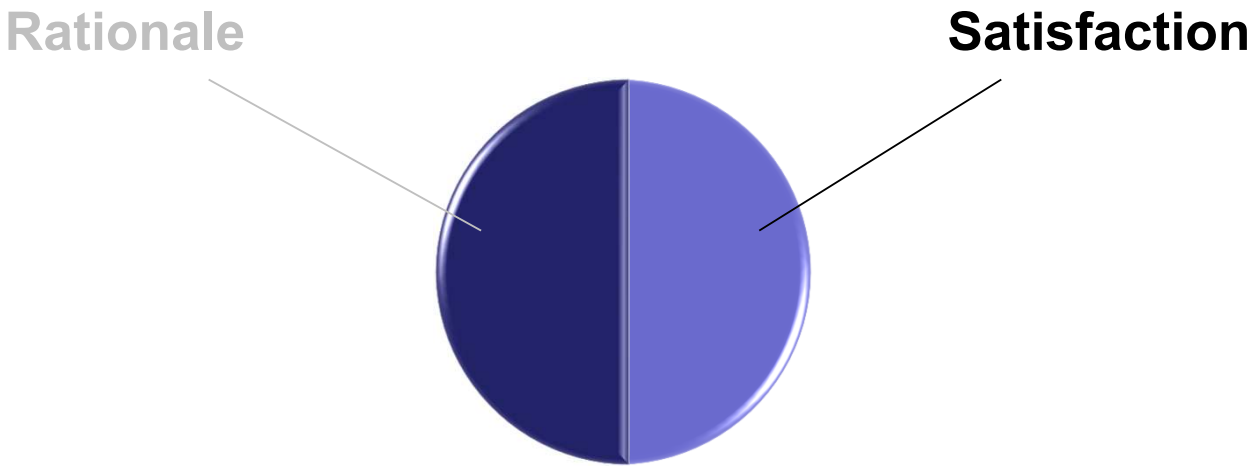
■ Rationale=根拠



- 安全要求が適切であることの技術的な根拠
- 代表的なｴﾋﾞﾃﾞﾝｽは安全分析や論理的な理由
- ｴﾝｼﾞﾆｱが頭の中で考えているようなこと

4つのargument- Satisfaction

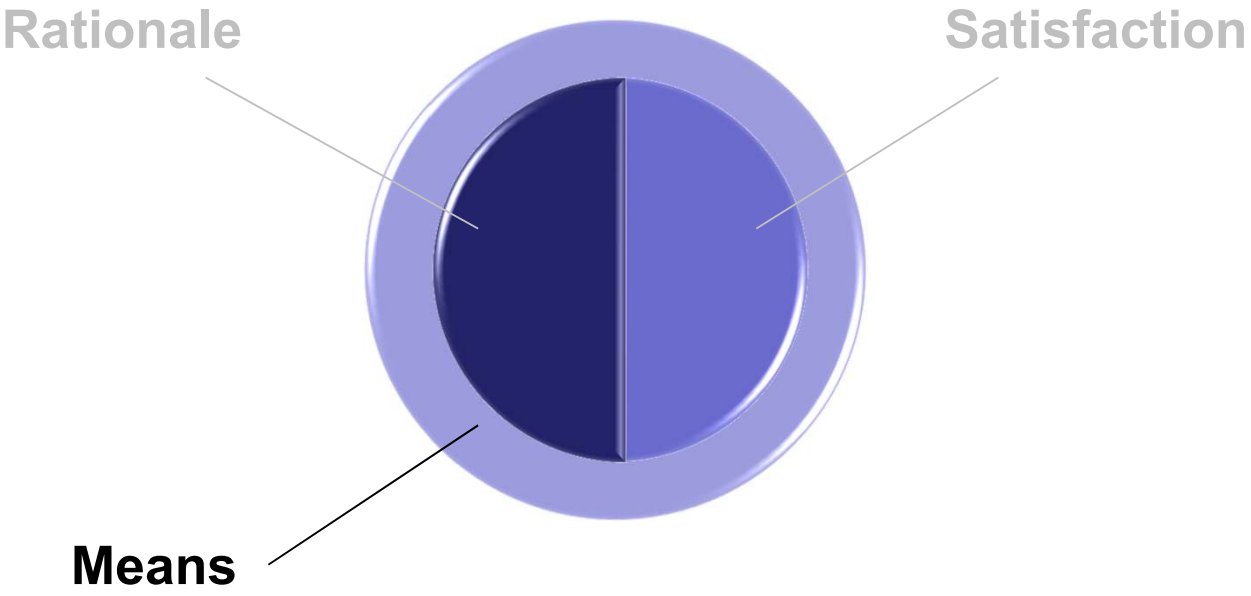
■ Satisfaction=満足



● 車両、ｼｽﾃﾑ、ｴﾚﾒﾝﾄの振る舞いが割り付けられた安全要求を満足することを主張

4つのargument- Means

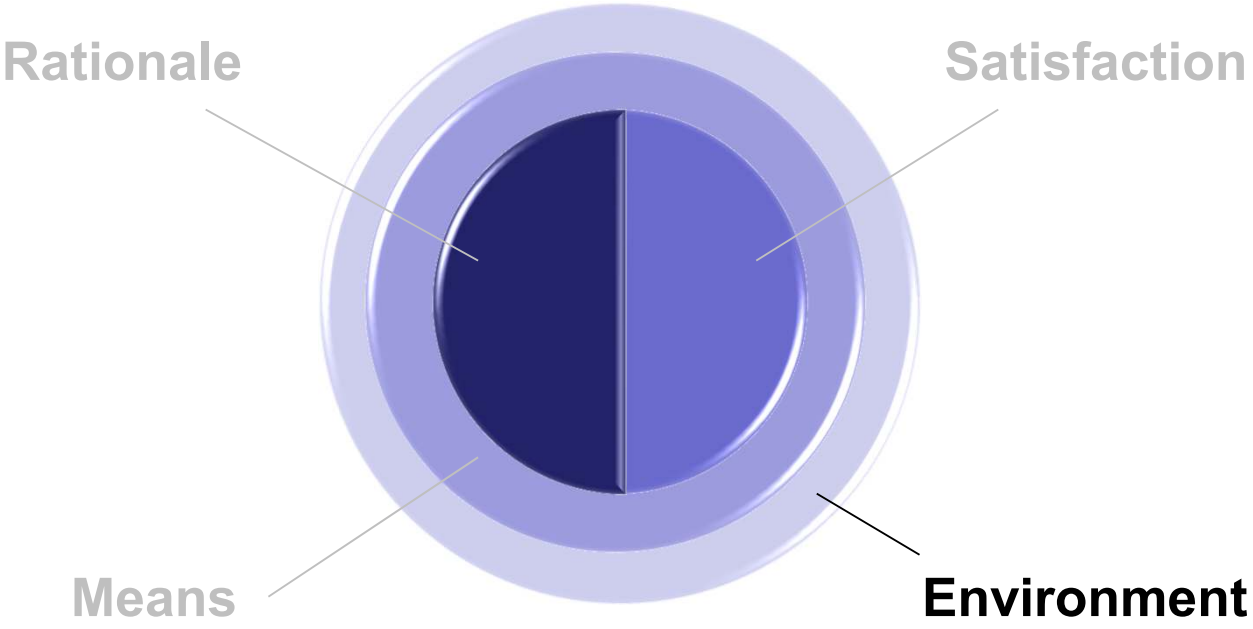
■ Means=手段



- 特定の活動を実施するために適切な手法が用いられていることを主張
- 人、ﾌﾟﾛｾｽ、ﾂｰﾙに関する"手段"に基づいた主張を検討する際に活用

4つのargument- Environment

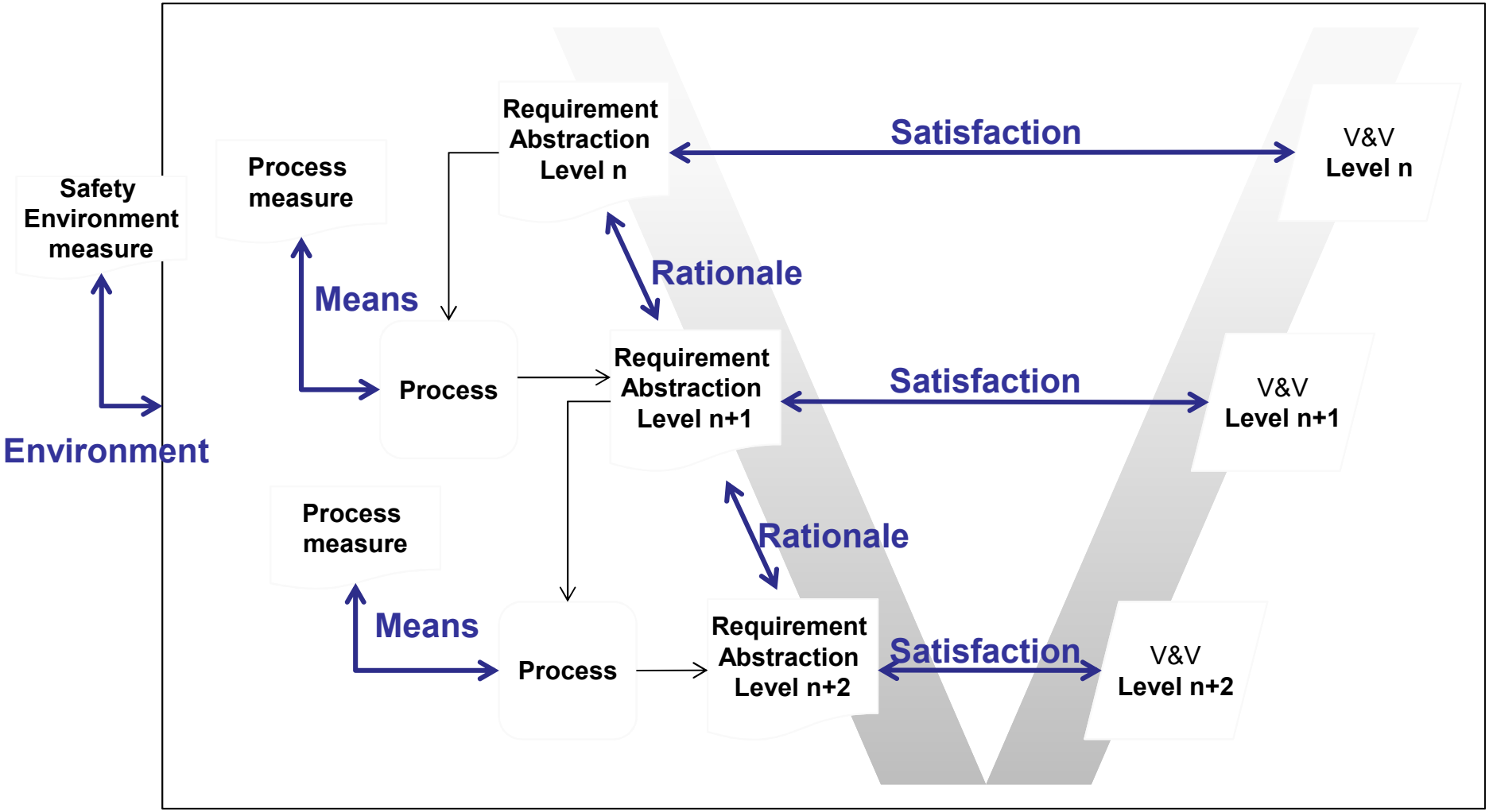
■ Environment=環境



- 活動が行われる開発環境に関する主張
- ある活動に特定したものではなく、異なるｱｲﾃﾑの論証での再利用が可能
- 部門や組織全体に関する主張のこともある

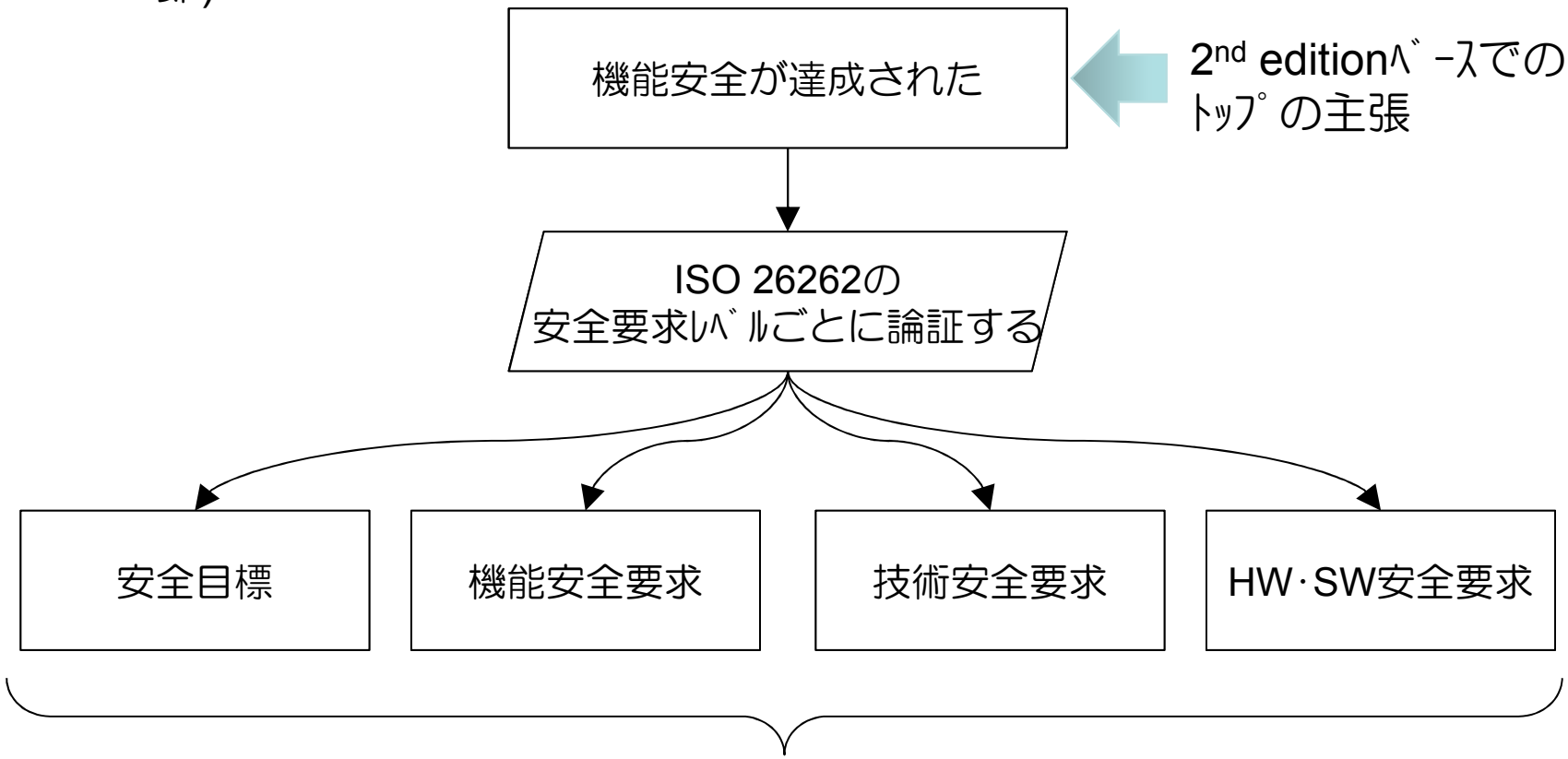
Vモデルへのマッピング

■ Vモデルに各主張のタイプを配置する。



ISO 26262への適応

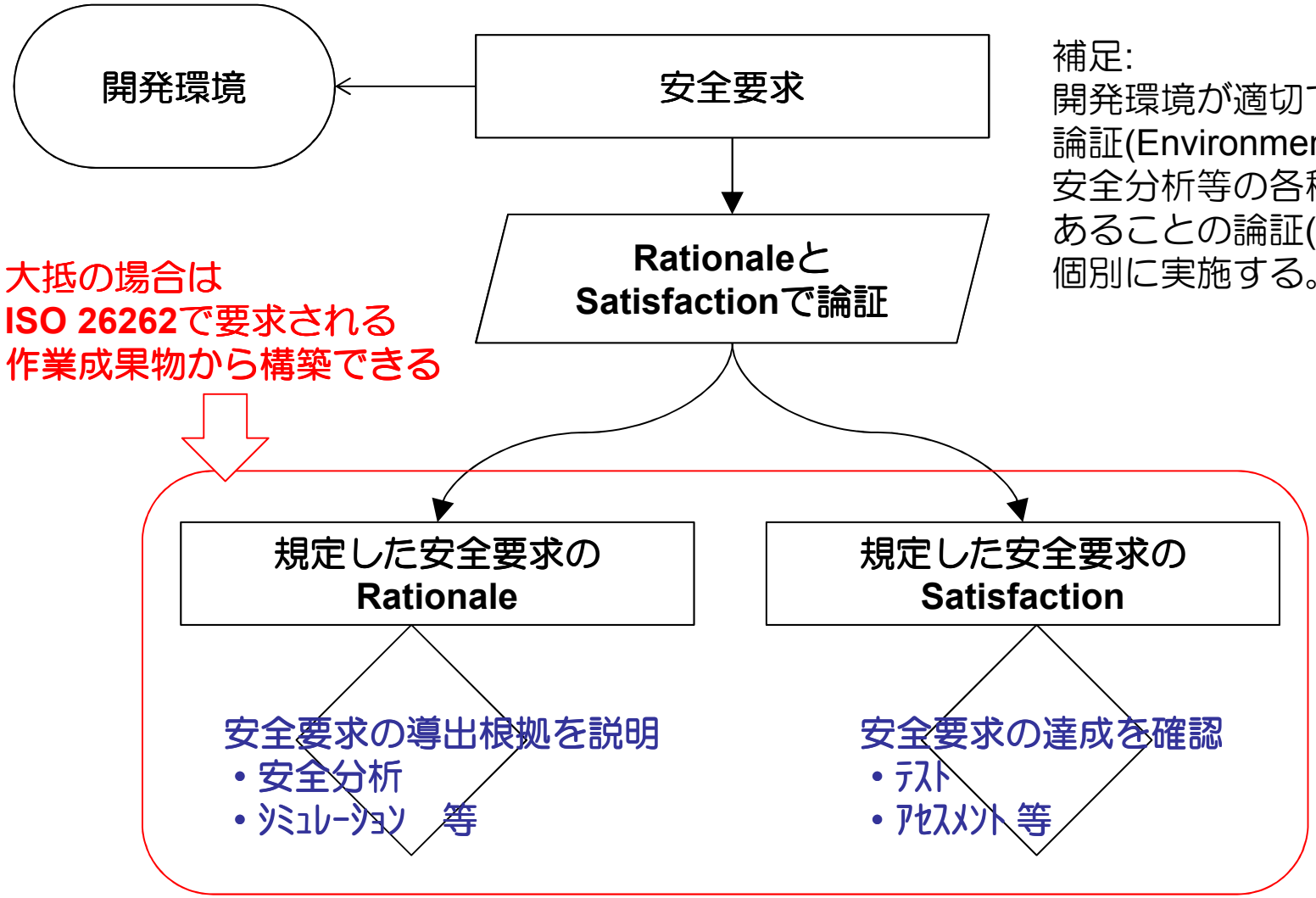
- A safety case shall be developed, in accordance with the safety plan, in order to provide an argument for the achievement of functional safety (ISO/DIS 26262-2, 6.4.6.1節)



製品開発ﾌｪｰｽﾞでの**safety case**としては、**Part 3-6**がすべて
適切に実施されていること示せれば良い。

安全要求の論証

■ 基本的には次のように論証する



補足:
開発環境が適切であることの論証(Environment)、および安全分析等の各種手法が適切であることの論証(Means)は個別に実施する。

まとめ

- ISO 26262の改訂後には、safety caseが従来の個別の要求事項に対する論証から、機能安全が達成できていることの論証に位置づけが変わる。
- このため、単に作業成果物をﾘｽﾄｱｯﾌﾟしただけではsafety caseとは呼べなくなる可能性もある。
- MISRAの提唱するsafety caseは構造がわかりやすく、現場ﾚﾍﾞﾙ(機能安全管理者)でも扱えるものであり、上記変化に対応するための手段のひとつと考えられる。