Safety Concept Notation Open Conference 名古屋（SCN-OC 名古屋）

セーフティーとセキュリティの統合に関する課題、現在の動向、今後の展望

2016年10月19日

国立研究開発法人　産業技術総合研究所
情報技術研究部門
ソフトウェアアナリティックス研究グループ

田口研治

自己紹介

【経歴】

- 産業技術総合研究所　招聘研究員　（併任）2010年4月～
- （株）シーエーブイテクノロジーズ 代表取締役社長 2011年4月（設立）～
- 産業界における11年間の経験
  - ソフトウェア業界における研究開発・コンサルティング
- 大学・研究機関での17 年間の経験
  - 日本の大学 教員（3年間）　九州大、他
  - 海外の大学 教員（5年間）　Uppsala 大 (Sweden), Bradford 大 (UK)
  - 研究機関（11年間）　国立情報学研究所　特任教授、産業技術総合研究所　招聘研究員

【専門分野】

＋高信頼システム開発方法論（形式検証、国際規格認証、システム保証、安全・セキュリティ分析方法論）
＋形式手法、ソフトウェア工学、システムアシュアランスに関する、多くの主要な国際会議の PC等 を歴任
（ ASSURE ‘16, FM’16, ICFEM ’16, HASE ’16, RISK ’16, ICECCS’16, SASSUER ’16 ）

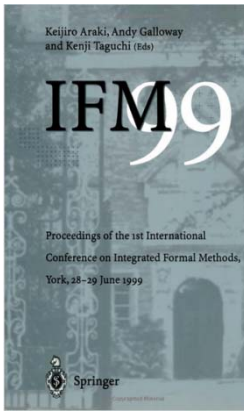
【規格、国際会議関連】

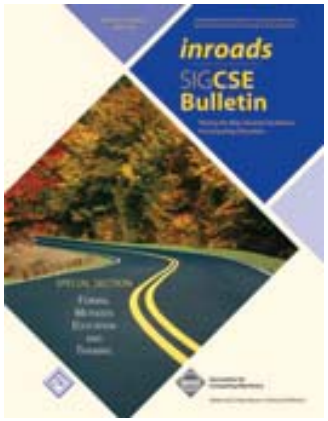
- International Conference on Formal Engineering Methods 2012 のプログラム委員長
- OMG System Assurance Platform Task Force の co-chair
- SICE 認証工学 WG 主査
- IEC TC65/WG 20 (Framework to bridge the requirements for safety and security) Expert

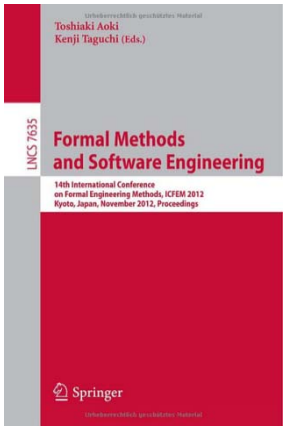
【共同研究】

＋ 無線式列車制御システムの安全・セキュリティ評価・規格適合性支援（西日本旅客鉄道（株）様との共同研究）
＋戦略的イノベーション創造プログラム（SIP）：（b）社会実装に向けた共通プラットフォームの実現とセキュリティ人材育成

著書（編者、著者）







Integrated Formal Methods (iFM) 国際会議設立(1999年）。共同編者

ソフトウェア科学基礎、近代科学社 2008年。共同著者

ACM SIGCSE, inRoads Bulletin, 2009年。共同編者
(Special Issue on Formal Methods Education and Training)

セキュリティ要求工学の実効性、情報処理学会学会誌 2009年。共同編者

International Conference on Formal Engineering Methods (ICFEM) 国際会議 2012年。共同編者

研究グループの研究紹介

1. システムの保証（System assurance）に関する方法論の研究

高度な安全、信頼性、セキュリティが必要なシステムは、社会インフラなどを中心に幅広く広がっており、どのようにそれらの特性を保証するかが大きな課題となっております。様々な安全規格ガイドラインでは、安全性の保証を審査するための根拠資料として**セーフティケース**の提出が義務付けられています（例：鉄道、原子力、防衛、医療機器、航空機）。**セーフティケース**による安全性保証を支援するために、**GSN (Goal Structuring Notation)** を用いた、支援方法論の研究を中心に、**安全**・**セキュリティ**分析の手法や、成果物間の**トレーサビリティ**確保のための手法など、様々な研究を実施しています。

2. 様々な国際規格・ガイドラインに関する適合性確認支援手法の研究

多くの産業分野において、その安全性等の保証のための規格、ガイドラインが発行され、それらへの準拠が必要になっています。しかし、安全性を担保しつつ、認証のためのコストを削減するのは容易ではなく、工学的な手法の必要性が認識されつつあります。私共は、**「認証工学」**という工学分野を確立するために、認証からみたシステムライフサイクル全体を統括、管理する「統合的認証管理システム」の構築をめざしています。さらに、**安全性**と**セキュリティ**を同時に担保するための手法や、それらの規格に対する同時認証手法の開発を目指しています。

セーフティケース研究

セーフティケース作成支援

- GSN を用いたセーフティケースの（半）自動生成方法の提案

□ 「**RAMS の認証とセーフティケース**」 WOCS 2014 一般講演（http://www.ipa.go.jp/files/000036237.pdf）相馬、**田口**、西原、大岩（AIST）、矢田部、森（JR西）

□ **Supporting Certification of Railway Standard IEC 62278/EN 50126 (RAMS) Using GSN**, SICE Annual Conference 2014, Souma, **Taguchi**, Nishihara (AIST), Yatabe, Mori (JR-W)

GSN (Goal Structuring Notation) の拡張

- 変数表現の導入とその意味の厳密化
- トレーサビリティとの連携
- セキュリティとセーフティの統合ケース

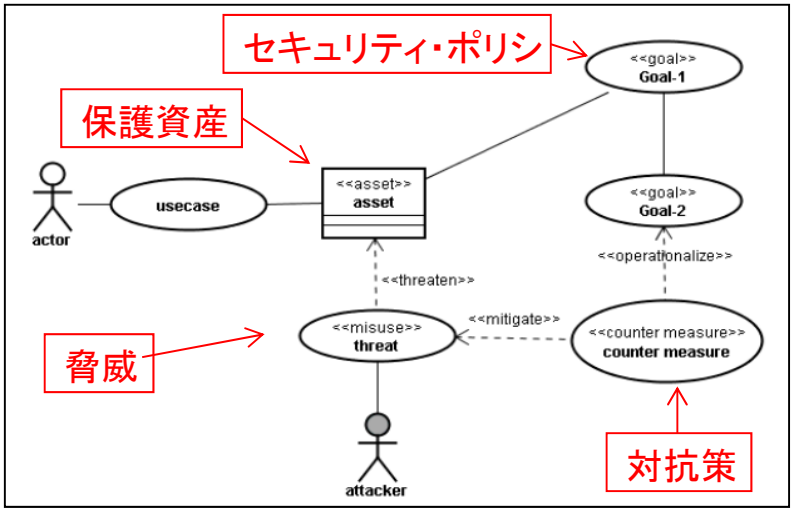
□ Y. Matsuno, **K. Taguchi**: **Parameterised Argument Structure for GSN Patterns**. QSIC 2011: 96-101

□ **K. Taguchi**, D. Souma, H. Nishihara, T. Takai: **Linking Traceability with GSN**, ASSURE 2014

□ **K. Taguchi**, D. Souma, H. Nishihara: **Safe & Sec Case Patterns**, ASSURE 2015

- **セーフティーケース紹介（動画）**
  - **https://www.youtube.com/watch?v=VedmkvMcBEg**
- **国際標準規格策定関連**
  - OMG SACM (Structured Assurance Case Metamodel) RTF (Revision Task Force) メンバー
- **セーフティケースに関連する国際会議関連での学会活動**
  - ASSURE (International Workshop on Assurance Case for Software-intensive Systems) 2013, 2014, 2015 PC
  - AAA (International Workshop on Argument for Agreement and Assurance) 2013, 2015 Program co-chair
- **その他**
  - External Examiner, ヨーク大学、Linling Sun, “Establishing Confidence in Safety Assessment Evidence” (2012) (指導教官: Tim Kelly)

セキュリティ脅威分析手法



脅威分析のための独自にミスユースケース記法を拡張

1) 通常のユースケース図を作成
2) 保護資産の同定
3) セキュリティ・ポリシの策定
4) 脅威の同定
5) 対抗策を作成

【利点】

- 広く利用されているユースケース図をセキュリティに拡張したものなので、様々なステークホルダ（顧客、マネージメント層、システム開発者）にとり、共通理解が容易。
- 脅威分析に必要な十分な分析要素を網羅。
- UML の拡張機能を利用して、様々な分析要素を容易に追加が可能（例：脆弱性、パッチ、他）

[1] **K. Taguchi**, Y. Tahara: Curriculum Design and Methodology for Security Requirements Analysis, Special Issue: Future of Software Engineering for security and privacy, Progress in Informatics, No. 5, pp19-34 (2008)
[2] 吉岡、**田口（共同編者）**: セキュリティ要求工学の実効性、情報処理学会学会誌、2009年
[3] **田口**、H. Mouratidis、セキュアトロポス（Secure Tropos）概論、情報処理学会学会誌、2009年
[4] **K. Taguchi**, N. Yoshioka, T. Tobita, H. Kaneko: Aligning Security Requirements and Security Assurance Using the Common Criteria. SSIRI 2010: 69-77
[5] T. Okubo, **K. Taguchi**, N. Yoshioka: Misuse Cases + Assets + Security Goals. CSE (3) 2009: 424-429
[6] T. Okubo, **K. Taguchi**, H. Kaiya, N. Yoshioka: MASG: Misuse case with Assets and Security Goals, J. Information Processing (2014)

セキュリティとセーフティの統合研究

セーフティとセキュリティの同時認証方法論

機能安全規格とセキュリティ規格を適切かつ効率的に認証するための手法

- **「ハイブリッド認証に向けての工学的アプローチ~機能安全とセキュリティの同時認証のための方法論~」 WOCS 2014** 招待講演
  - 講演資料（www.ipa.go.jp/files/000036521.pdf）
  - 講演動画（http://www.youtube.com/watch?v=60l12Zk1REo）
- **「セーフティー＆セキュリティ」 ET 2014** パネルセッション
- **「セーフティとセキュリティ規格の同時認証方法論について」 WOCS 2015** 専門セミナー
- **「IoTシステムにおけるセーフティとセキュリティ（規格と認証）」 STARCアドバンストセミナー 2015年3月**

セーフティとセキュリティの統合方法論

プロセスの統合や分析手法、アセスメントの統合手法

- **「システムの安全性、セキュリティ保証の枠組み」** ZIPC ユーザカンファレンス 2015
- **「セーフティとセキュリティの統合のための課題とその解決方法論」** IPA シンポジウム 2015

講演のフォーマット

- 仮定
  - 参加者は、様々な意見を持っており、意見を交換できる機会があれば、発言したい。
  - 講師より自分の方が良く講演内容が分かっている。
    - 故に、間違えがあれば正したい。
  - 議論によってこそ、新たな知を得ることが出来る

1. なぜ、セーフティとセキュリティが問題となるのか？

1-1. なぜセーフティとセキュリティの統合に対して配慮が必要か？

- 現在、多くの安全が重要視されている産業（鉄道、自動車、プラント制御、原子力発電、他）において、セキュリティの脅威が顕在化している。

事故の原因は？

機械故障？

従来は、安全性・信頼性だけを考えていれば良かったが原因としてセキュリティ上の脅威が加わった。

もしかしてハック？

混ぜるな危険、その組み合わせ！

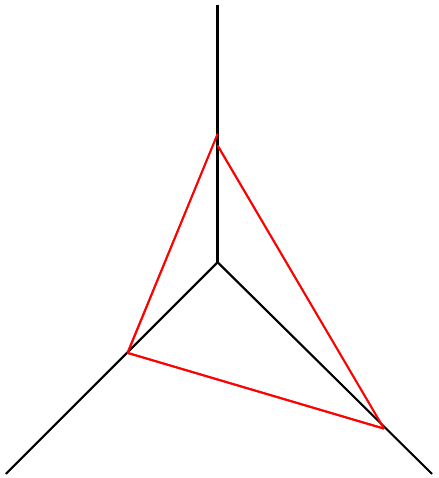
セーフティ ＋ セキュリティ ＝ ？

危険でない混ぜ方はあるのか？

1-2. 相互のバランス？

- うまくバランスを取ることが大事（最適な設計解を求めて）
- 問題は、相互の影響と、それを考慮したトレードオフ？

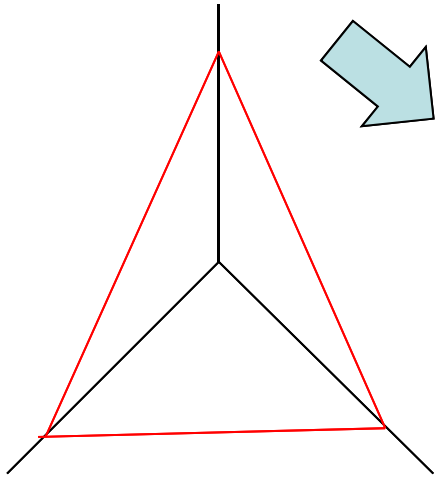
全体の最適化？



セーフティ　　セキュリティ

セキュリティの人は大体
このような考え方になる

全体の最適化？



セーフティ　　セキュリティ

最適なものを作ることが、より安全でセキュアなシステムの開発につながり、コスト削減につながることが期待される

1.3. セーフティとセキュリティは対称、非対称？

- 比較をすると対称形（もしくは準同型？）である箇所が多い。
- しかし、両方を混ぜようとすると（統合？）、全てが対称形にはならない。

【概念レベルでの対称性】

ハザード vs 脅威

対抗策 vs 軽減策

共通の概念（リスク）

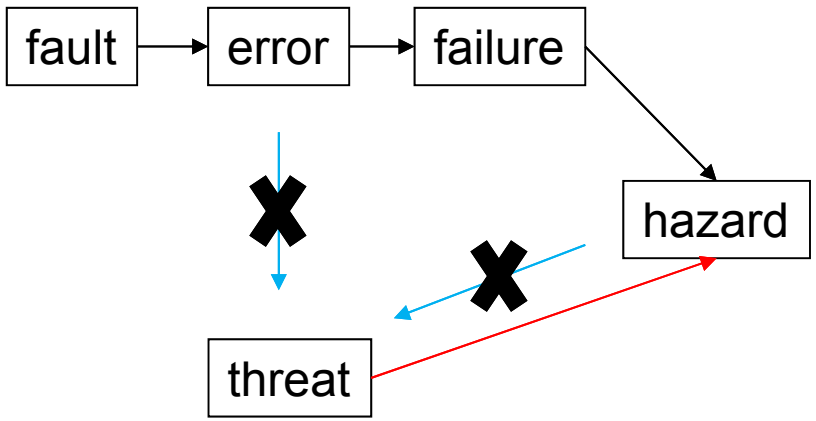
【プロセスレベルでの対称性】

HARA vs TARA

対抗策同定 vs 軽減策同定

Safety Coding vs Secure Coding

【セーフティから見た場合の概念図】



脅威とハザードの関係を見るとセキュリティから安全への影響はあるが、逆はない？

1.3. セーフティとセキュリティは対称、非対称？

- 比較をすると対称形（もしくは準同型？）である箇所が多い。
- しかし、両方を混ぜようとすると（統合？）、全てが対称形にはならない。

【概念レベルでの対称性】

ハザード vs 脅威

対抗策 vs 軽減策

共通の概念（リスク）

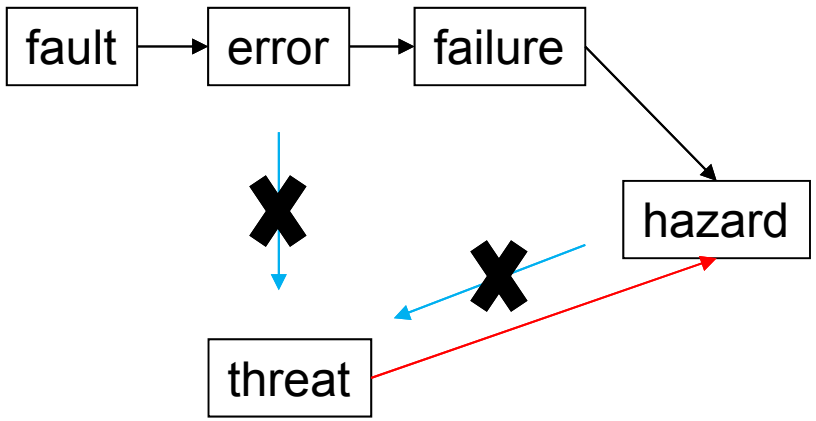
【プロセスレベルでの対称性】

HARA vs TARA

対抗策同定 vs 軽減策同定

Safety Coding vs Secure Coding

【セーフティから見た場合の概念図】



脅威とハザードの関係を見るとセキュリティから安全への影響はあるが、逆はない？

議論したい内容（1）

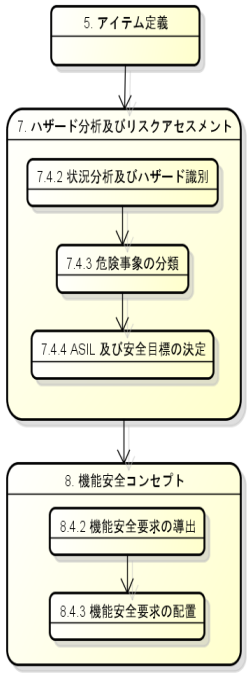
- 問題の本質的な理解
  - セーフティとセキュリティの関係はどのようになっているのか？
  - 対称形、非対称形？包含関係？
- 課題の理解
  - 本当にセーフティとセキュリティの統合が本当に必要なのか？
    - 実際に問題が生じた例があるのか？
- 解決策への期待
  - もし課題があるとすれば、その解決策や方法論は必要か？
  - 解決することで、品質が向上し、開発コストが削減できるのか？

2. プロセス

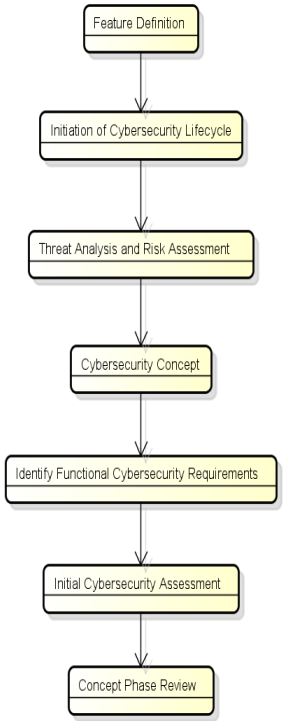
2-1. 悪い混ぜ方の例（ライフサイクルの統合例）?

- 機能安全規格とセキュリティ規格におけるプロセス統合のまずい例

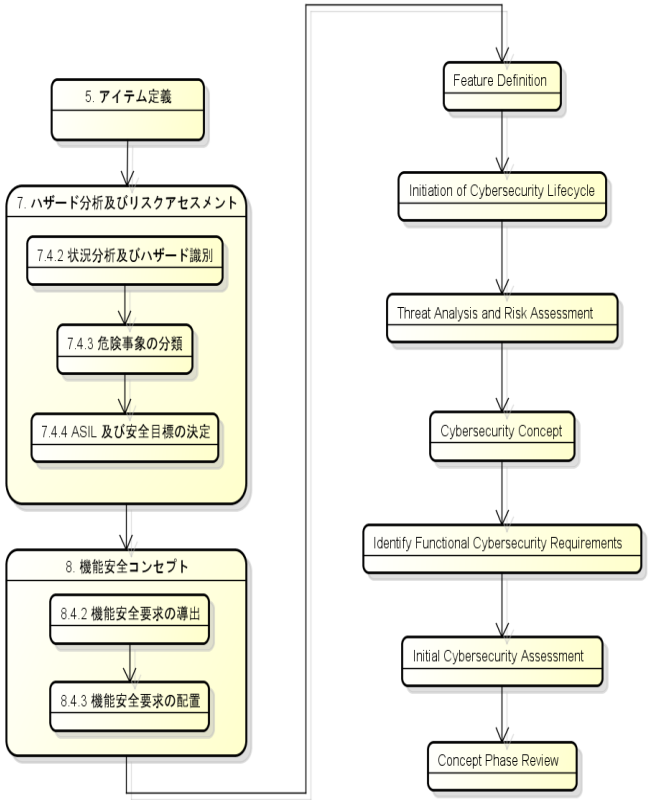
安全側のプロセス（ISO 26262-3）



セキュリティ側のプロセス（J3061 ）



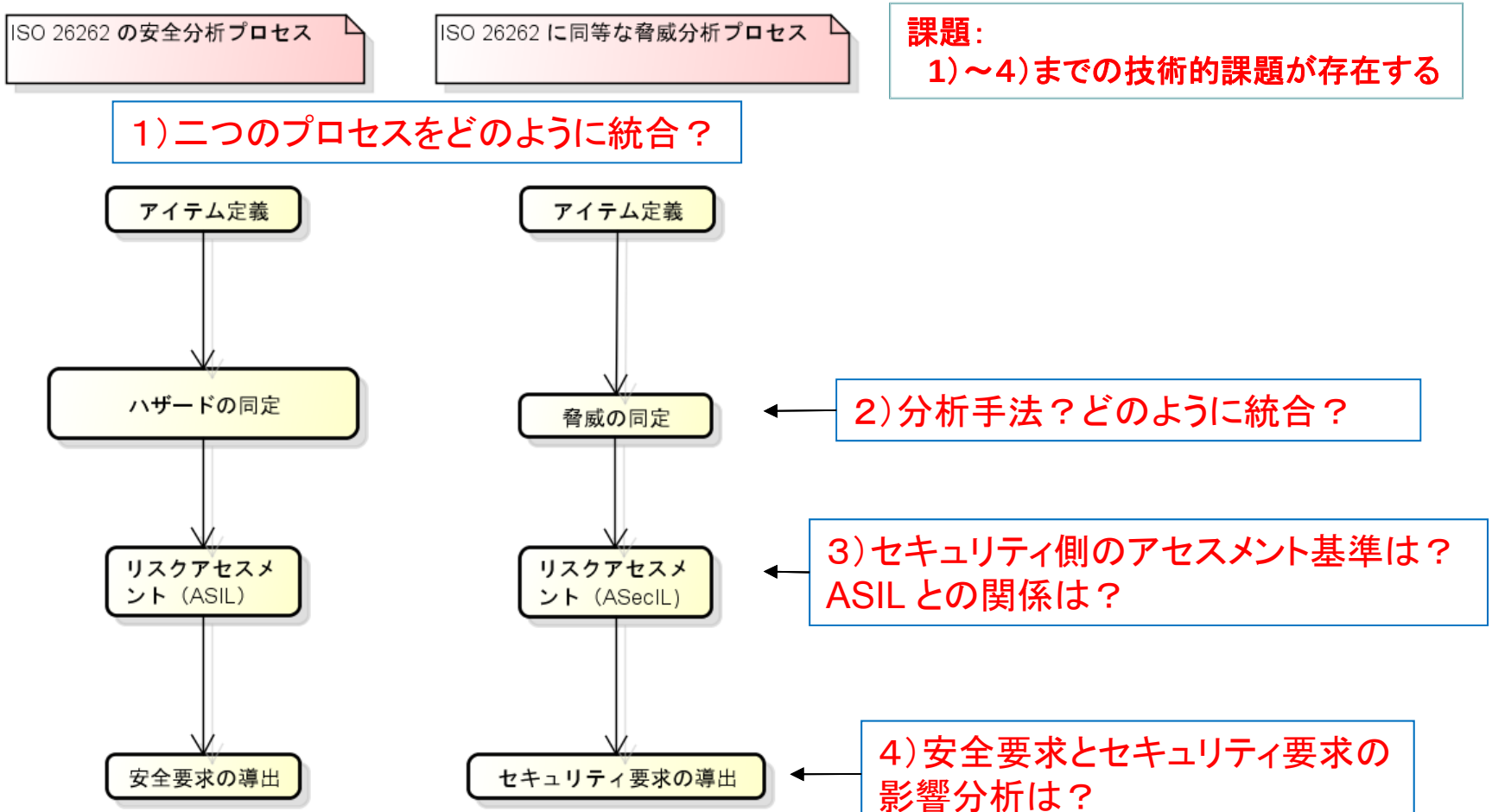
安全の後にセキュリティをやれば良い（？）



ISO 26262, Road vehicles – Functional safety (2011)
J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)

2-2. 安全とセキュリティ開発プロセスの課題

ISO 26262 Part 3 相当の安全、セキュリティプロセス（想定図）

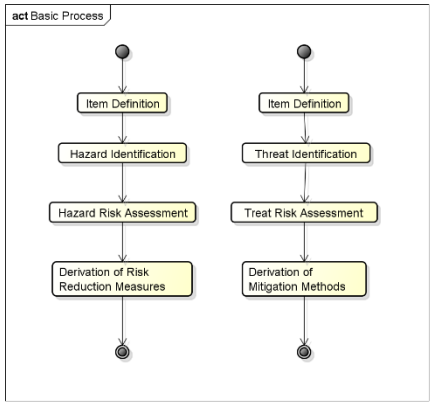


注：ASecIL (Automotive Security Integrity Level)

2-3. 安全とセキュリティのプロセス統合（分類）

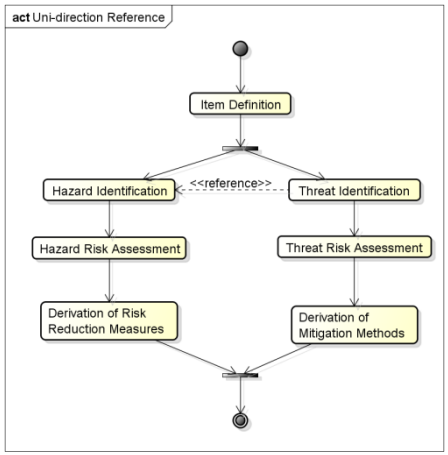
- セキュリティと安全の開発プロセスをどのように統合するかは、まだ解決されていない、大きな課題である。
- 様々な提案がされているが、どれもが決定的では無い。
- 研究プロジェクト、セキュリティ規格等の調査の結果、以下の基本形に分類可能。
- これらを基に、様々な組み合わせが、詳細レベルで可能。

K. Taguchi, D. Souma, H. Nishihara: Safe & Sec Case Patterns, ASSURE 2015



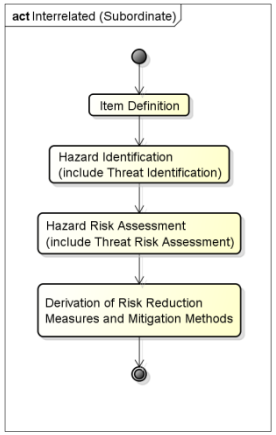
個々に独立
（基本型）

安全側分析結果
をセキュリティが参照
（一方向参照型）



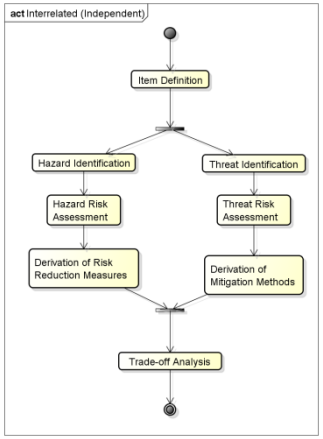
航空機セキュリティ規格（DO-326A）
を抽象化した形

安全側がセキュリティ
を包括（従属型）



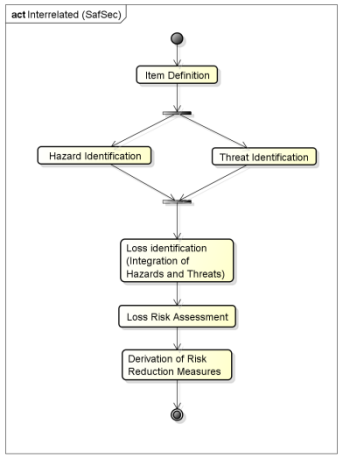
FTA が ATA
を含む分析方法

ある時点で、トレードオフ
を実施（相互関連型）



SESAMO（FP7）
安全要求とセキュリティ要求
のトレードオフ分析

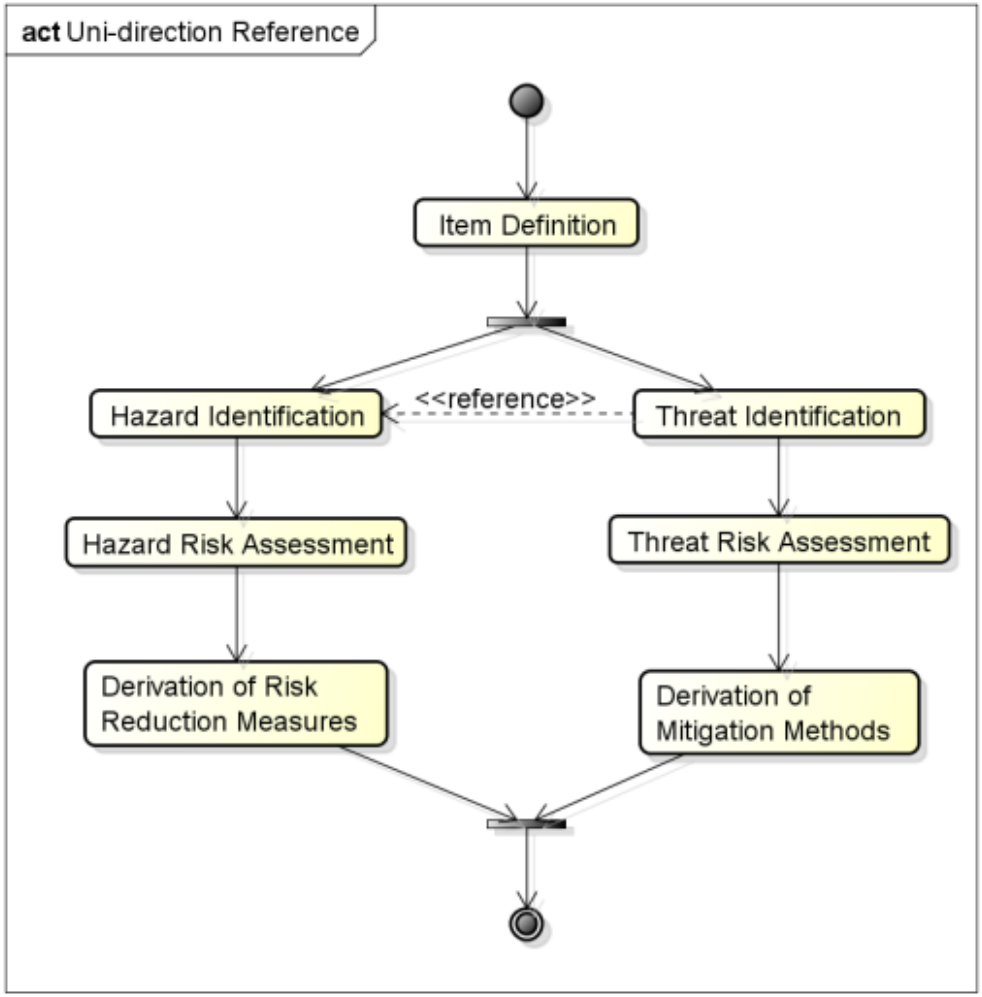
ロスとして統合
（SafSec型）



同時認証方法論 SafSec
におけるプロセスを抽象化
した形

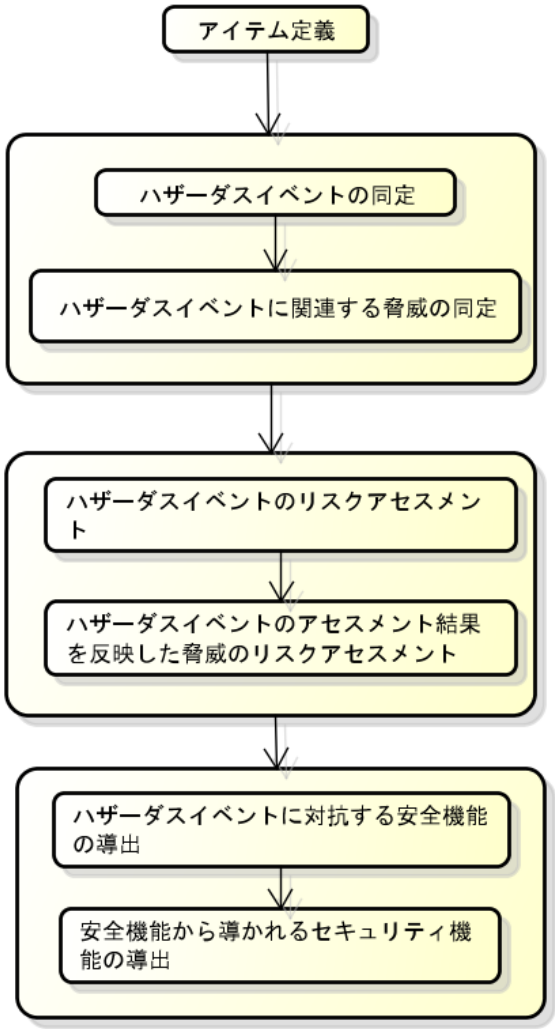
2-4. 一方向参照型

- 本統合プロセスは、航空機のセキュリティ規格DO-326A におけるプロセスを簡略化した示したものである。
- ここでは、セキュリティ側のデータは、安全側では利用されない。



2-5. 従属型のプロセス(ISO 26262 Part3):詳細版

- ISO 26262 の Part 3 (安全コンセプト)のプロセスで、セキュリティの従属型のプロセスは右の図のようになる。
  - ただし、ここでは ASIL 分解については取り扱っていない。
- 各フェーズの活動は、セキュリティ側の活動を含む形になっている。
- **そのためには、安全側の成果物をセキュリティ側で利用するための手法が必要になる。**



2)安全、脅威分析の統合

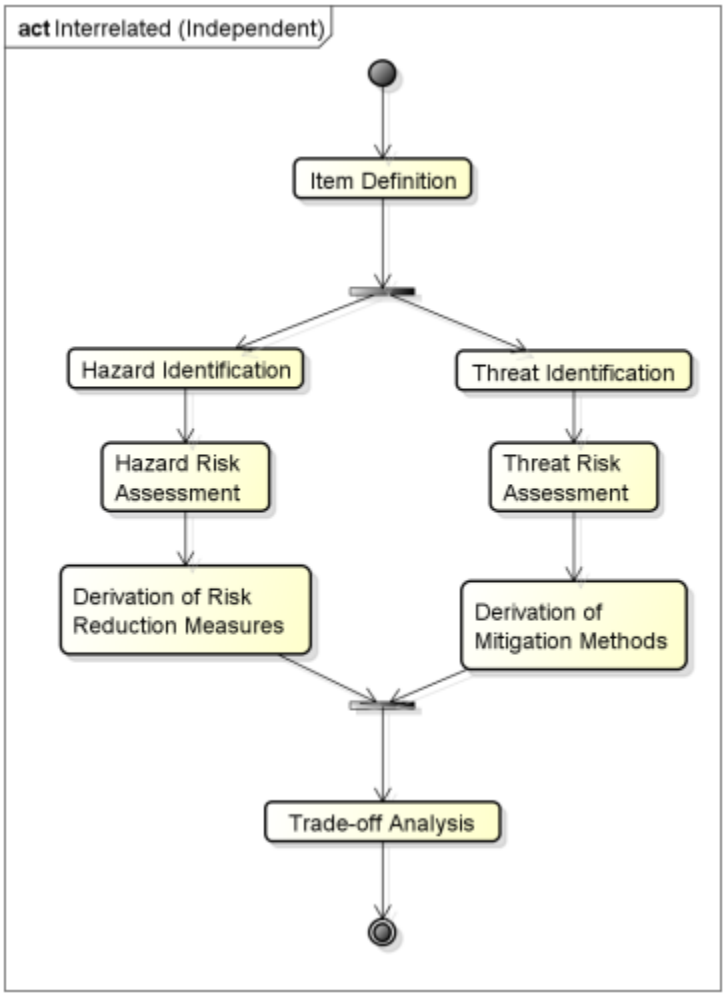
3)安全、セキュリティアセスメントの統合

4)安全機能、セキュリティ機能導出の統合

もしくは、安全側に必要に応じてセキュリティ側の要素を織り込むプロセス

2-6. トレードオフを入れたプロセス

- 導出された安全要求とセキュリティ要求のトレードオフ分析を実施する。
- トレードオフ分析は、様々なレベルで実施する必要があるが（例：アーキテクチャレベル）、ここでは、要求レベルで実施することを想定している。
- FP7 SESAMO プロジェクトにおいて、トレードオフに関する研究が実施されている。



SeSaMo: http://sesamo-project.eu
Born, M.: An Approach to Safety and Security Analysis for Automotive Systems: SAE 2014 World Congress and Exhibition (2014)

2-7. プロセス統合についての今後の動向

- プロセスの統合については、様々な考え方があり、当面は、様々な関連から試行が行われることが予想される。
- 統合のレベル
  - 産業分野
  - 製品
  - 開発コストに依存
    - 航空機と、制御機械（例：PLC）では、開発コストが大幅に異なる。よりライトウェイトなプロセスや、詳細なプロセスなど、その産業分野、製造品により、様々なレベルのプロセスが開発されることが予想される

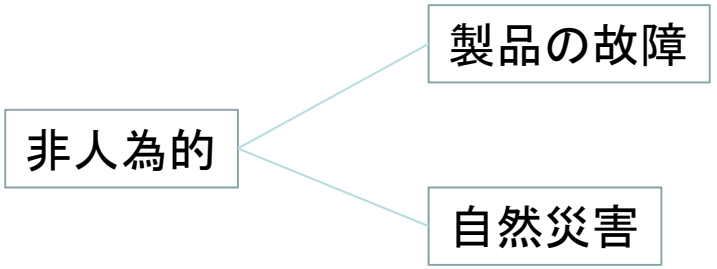
議論したい内容(2)

- セーフティとセキュリティのライフサイクルの統合は必要か？
- 統合って何？どのレベルで行うのか？単なるインタフェイスではダメなのか？じゃあ、インタフェイスって何？
- 何がライフサイクルの統合で問題になるのか？

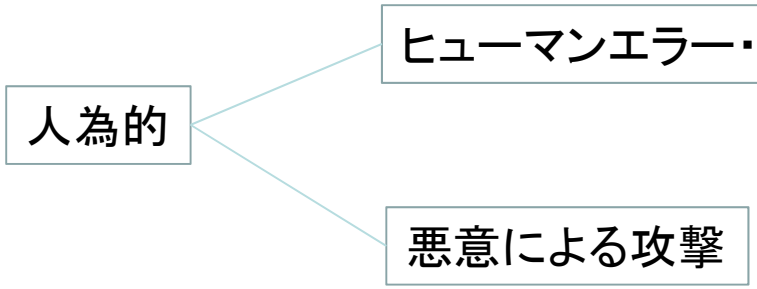
3. 分析技術

3-1. 安全分析手法の統合

まず、故障などの原因の分析から考えてみる。

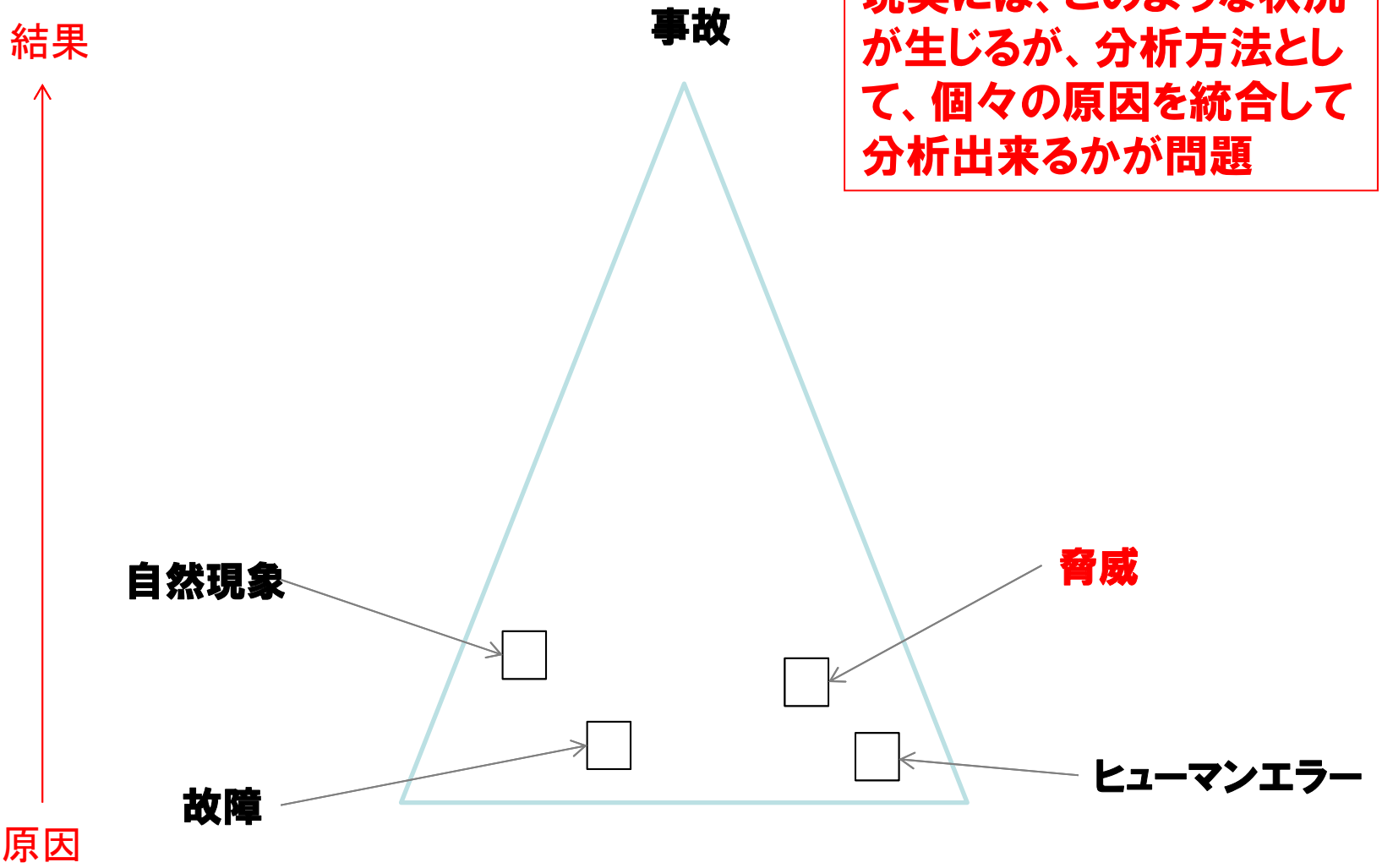


＋「製品の故障」は、製品の故障率に関係する信頼性であるが、安全性との関係において重要である。
＋「自然災害」は、発生確率を考慮することが出来るが、自然災害の原因をどこまで分析するかは、利用可能なデータ源までと考えられる（例：地震、洪水）。



「誤用」と「悪意による攻撃」は混同しやすいが、現在、巧妙な攻撃が増えてきており、明確に区別可能。また、そのアセスメントは明確に異なる基準で行うことが可能。

3-2. 事故原因の分析


結果
事故
現実には、このような状況が生じるが、分析方法として、個々の原因を統合して分析出来るかが問題
自然現象
脅威
故障
ヒューマンエラー
原因

3-3. これまでの分析手法（安全とセキュリティ）

【安全分析】

- 実効性が経験的に実証されている、様々な安全分析手法を利用して行われている。
  - Preliminary Hazard Analysis
  - FMEA
  - FTA
  - HAZOP

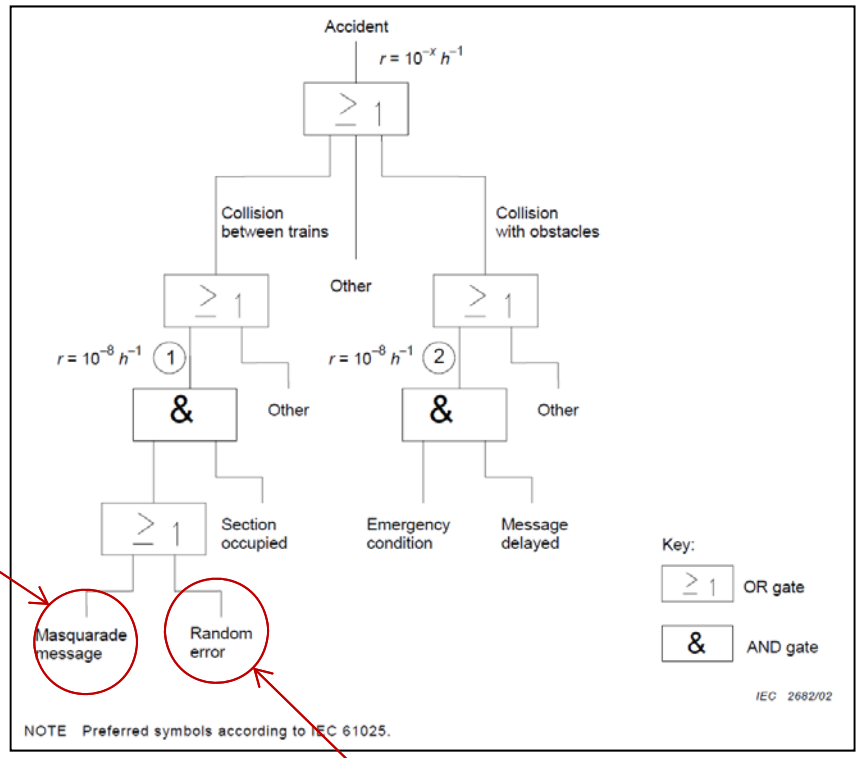
【脅威分析】

- どこまで実効性があるかが不明。
- 安全分析と同様に、様々な手法が提案されている。
  - Misuse cases
  - Attack Trees
  - SDL
  - …

3-4. IEC 62280-2 におけるリスクアセスメント方式例

見本として示された、FT (Fault Tree) はこれで良いのか？

C.4.2 Hazard analysis

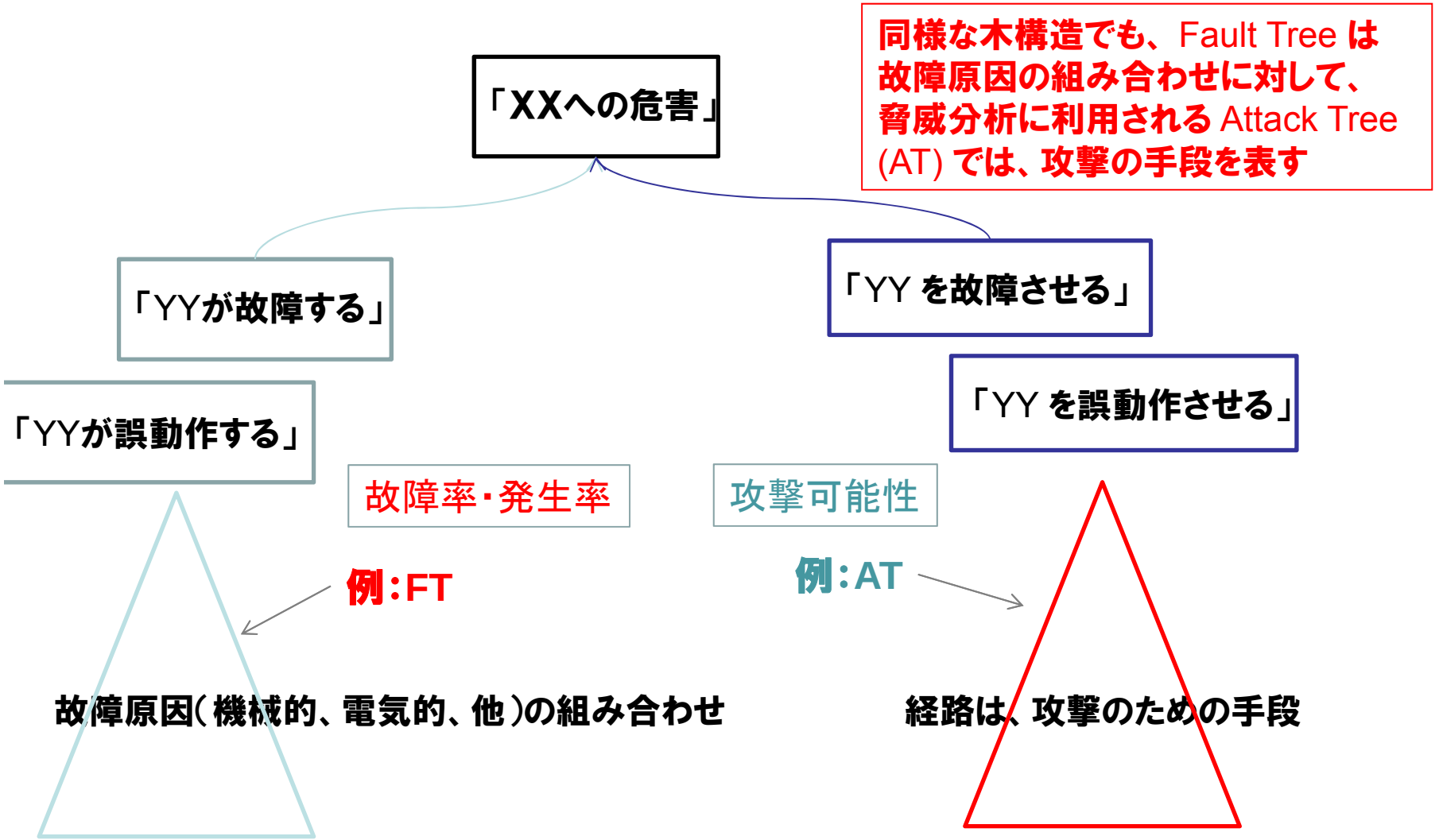


脅威

H/W 故障

(IEC 62280-2: 2002, Railway applications - Communication, signalling and processing systems - Part 2: Safety-related communication in open transmission systems

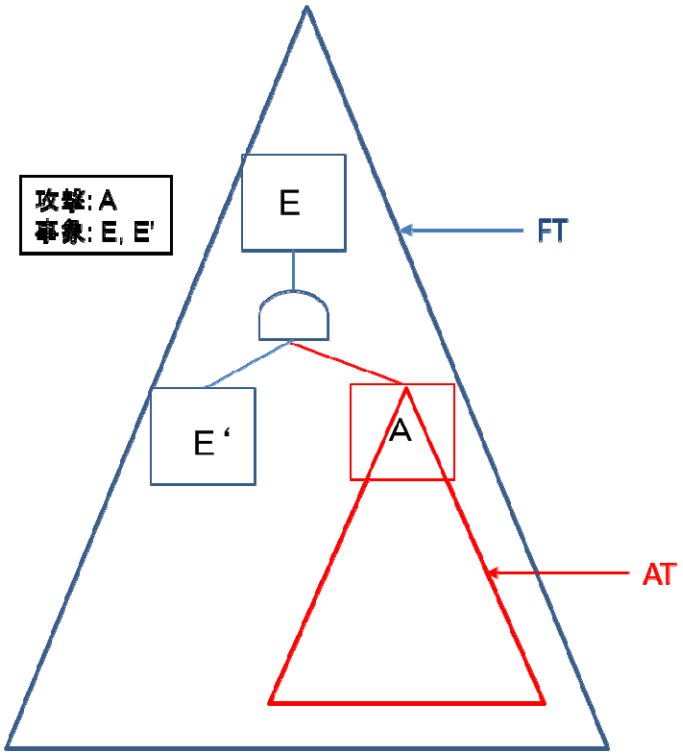
3-5. 安全性とセキュリティの分析の特徴



+ B. Schneier: Attack Trees, Dr. Dobbs Journal 1996
+ EVITA: Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios, 2008.

3-6. 安全分析とセキュリティ分析の統合

- 安全分析とセキュリティ分析の統合は、安全プロセスとセキュリティプロセスを統合する際の第一の課題である。
- 特に、セキュリティ側から安全側への影響を考える場合には、下記のような故障木（FT）と攻撃木（AT）の統合手法を利用する必要がある。
  - ただし、統合した場合のリスクのアセスメントの仕方には、まだ未解決の問題がある。



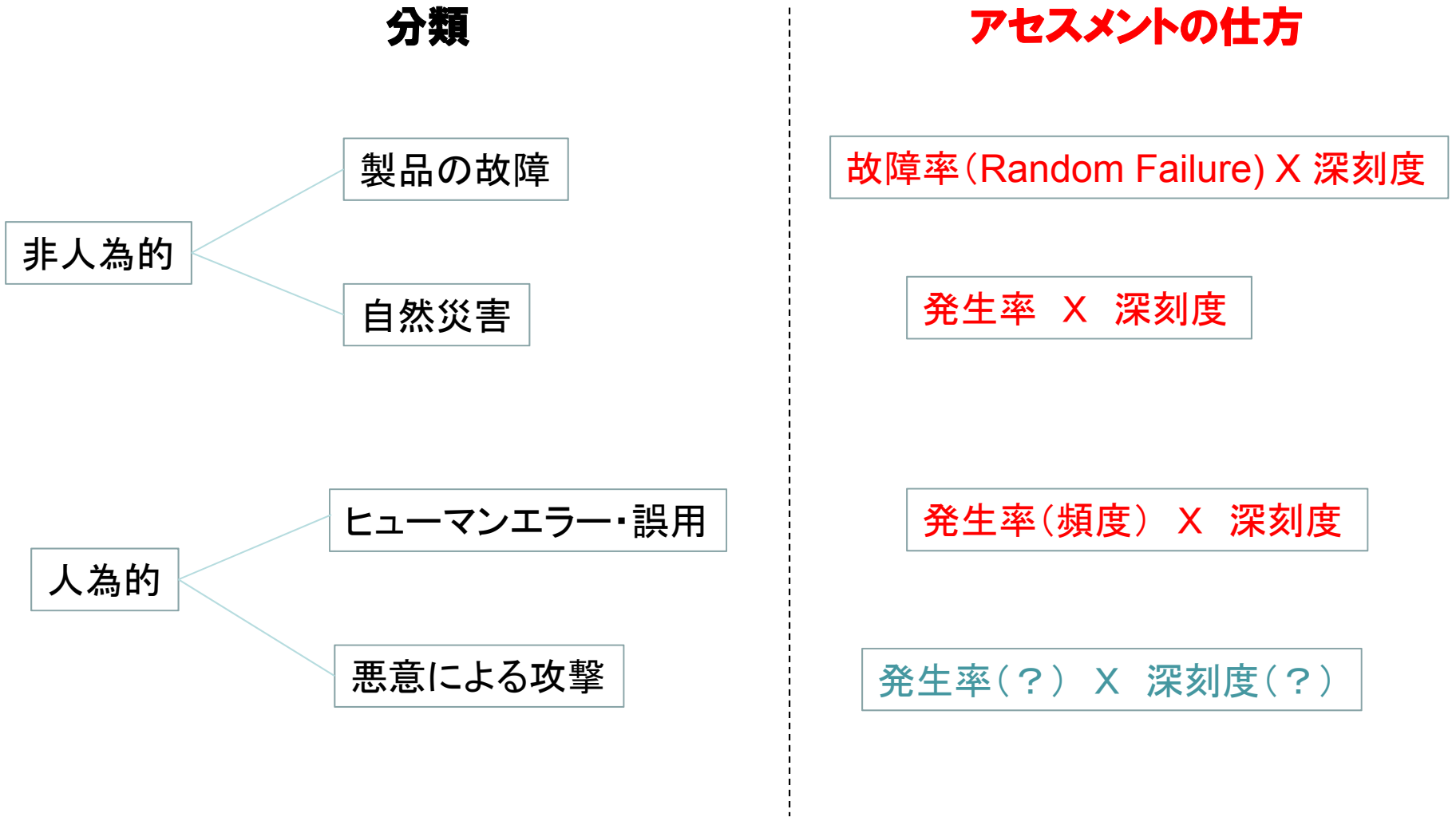
+ A. Roy, D. S. Kim, K. S. Trivedi: ACT: Towards unifying the constructs of attack and defense trees, Security and Communication Networks, 5(8), pp929-943 (2012)
+ M. Steiner and Peter Liggesmeyer: Combination of Safety and Security Analysis – Finding Security Problems that Threaten the Safety of a System, Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) 2013
+ K. Taguchi, et. al.,: Integration of Safety and Security Analyses for Automotive Systems (Draft)

議論したい内容(3)

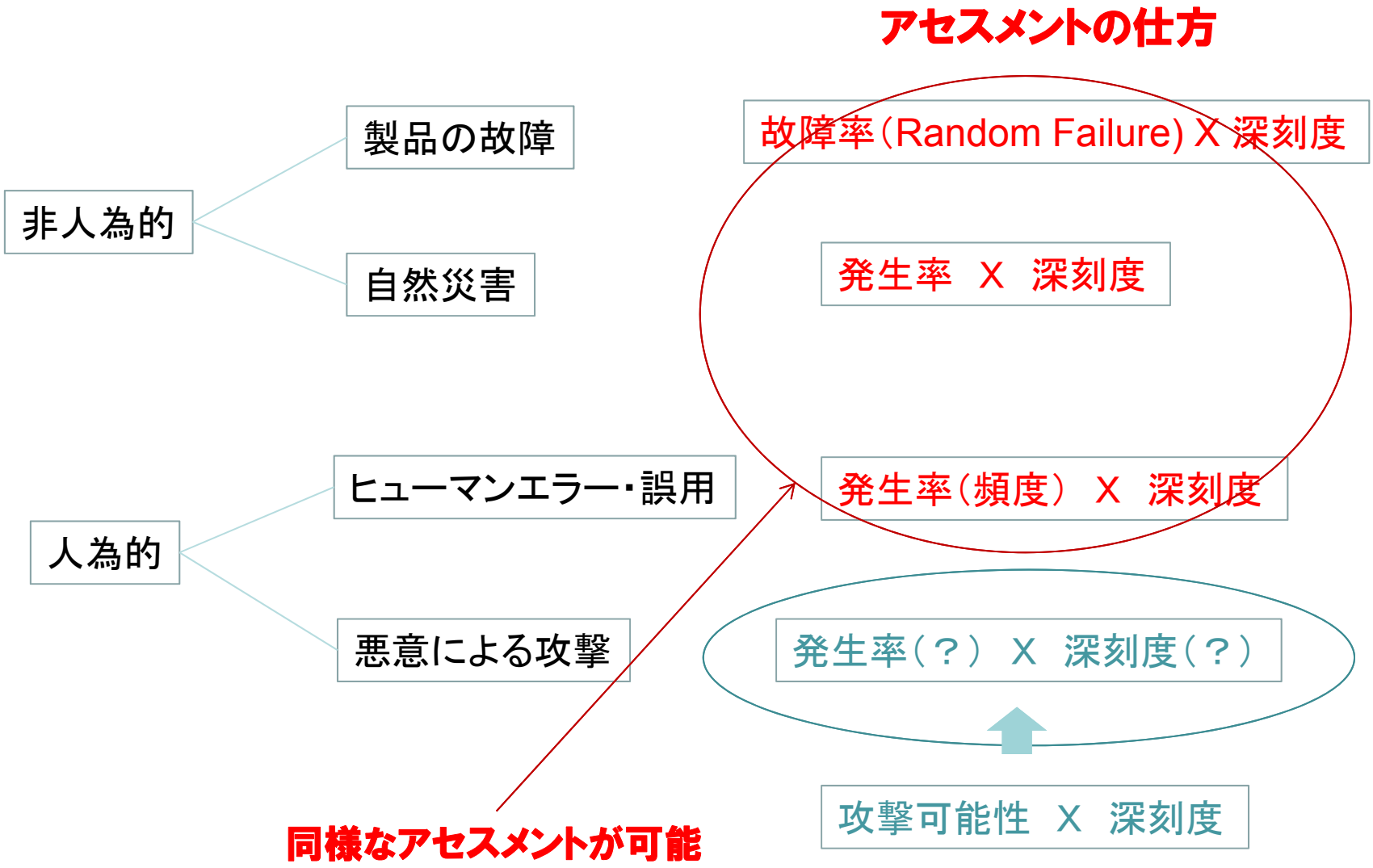
- セーフティとセキュリティの分析についての統合は必要か？
  - 別々にすれば？今でも何とかなっているでしょ！
  - 影響(セキュリティからセーフティ方向)があるようだが、無視できるものなのか？
- 統合できるとしたら、双方を結び付ける何か原理的な法則が必要か？それは何か？

4. リスクアセスメント

4-1. 原因の分類（人為的 vs 非人為的）とアセスメント（1）



4-2. 原因の分類（人為的 vs 非人為的）とアセスメント（2）



4-3. セキュリティのアセスメント例（CC-CEM [1] ）

- 非常に複雑なアセスメントのためのメトリックスを利用
  - 時間（攻撃にかかる時間）
  - 専門知識（攻撃に関連する知識）
  - 機会（攻撃可能な機会）
  - 装置（攻撃に利用される装置）
- 車載関係では FP7 EVITA ([3]）で、若干の修正の上利用
- 同様に、ETSI/TVRA (Threat Vulnerability Risk Analysis) ([2]）でも CC-CEM ベースのものを利用。

[1] ISO/IEC 15408, Common Criteria, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Sep 2012, Ver. 3.1, Rev. 4.

[2] Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN): Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis, ETSI TS 102 165-1, v4.2.3 (2011-3).

[3] Deliverable D2.1: Security requirements for automotive on-board networks based on dark-side scenarios, ver. 1.1, Dec 2009.

4-4. リスクの概念からインテグリティレベルへ

古典的定義

リスクの定義 ： Risk = Severity * Likelihood/Probability

現代的定義

安全規格等における定性的・定量的リスクの定義： Safety Integrity Levels

TABLE I. Severity categories

SEVERITY CATEGORIES		
Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	2	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

MIL-STD-882

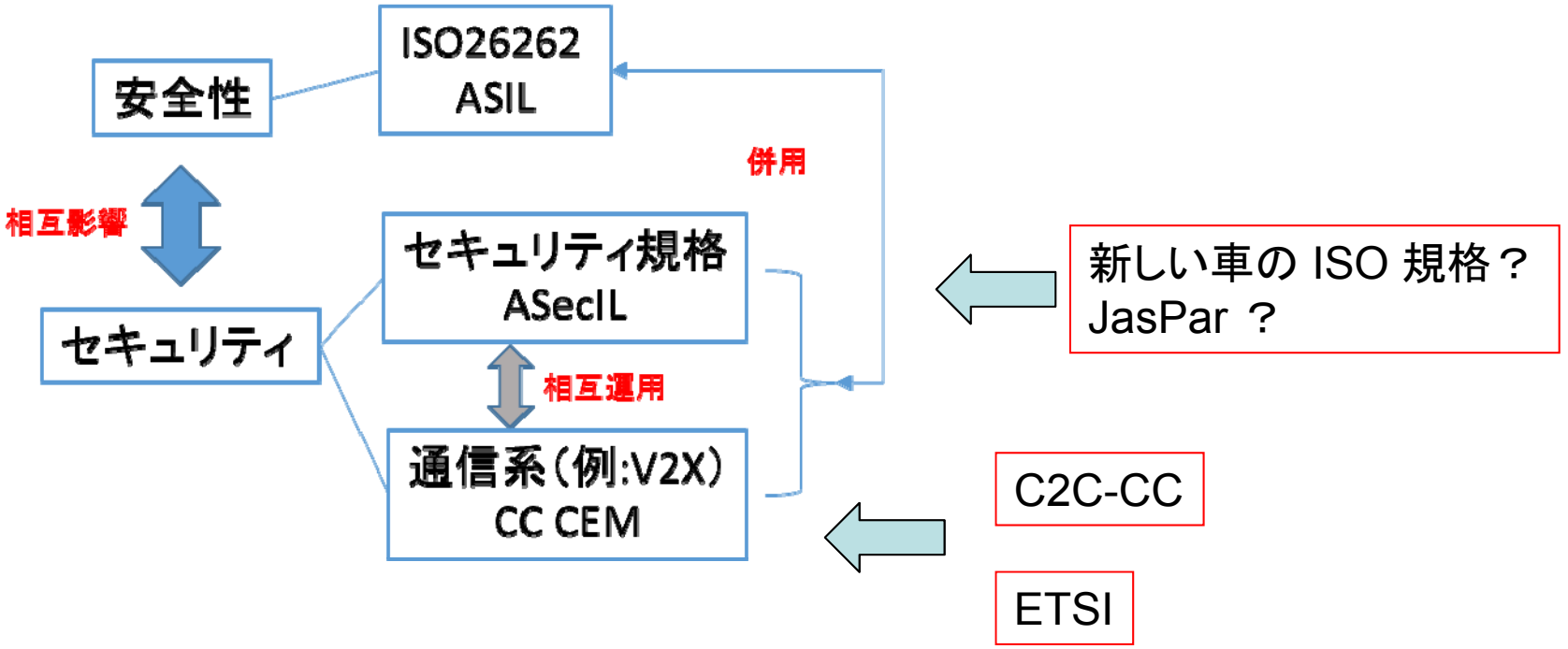
なぜ、このようなレベル分けに根拠があるのか科学的な根拠は不明

様々な規格における Integrity Level

- **安全側**
  - **SIL (Safety Integrity Level) , ISO/IEC 61508**
  - **ASIL (Automotive Safety Integrity Level) , ISO 26262**
  - **DAL (Design Assurance Level), DO-178C**
- **セキュリティ側**
  - **CC-CEM**
  - **SL (Security Level), IEC 62443**

4-5. アセスメント方式の混在

- 今後は、安全性のメトリックス（ASIL）とセキュリティのメトリックス（ASecIL）と、他の規格におけるメトリックス（CC-CEM）が混在した状況になると予想される。



4-6. アセスメントの根本的な課題

- セキュリティメトリックスの最も根本的は課題は、まだ、何をメトリックスの要素とするかの確立した定説が無いこと。
- 現在のセキュリティメトリックスは、攻撃の容易さ（Attack potential/probability）など、攻撃に対する特性を用いている。
- リスクの低減についての計算が出来ない
  - （機能）安全と同様に、受容可能や許容可能なリスクに低減されているかどうかのアセスメントの計算が出来ない。

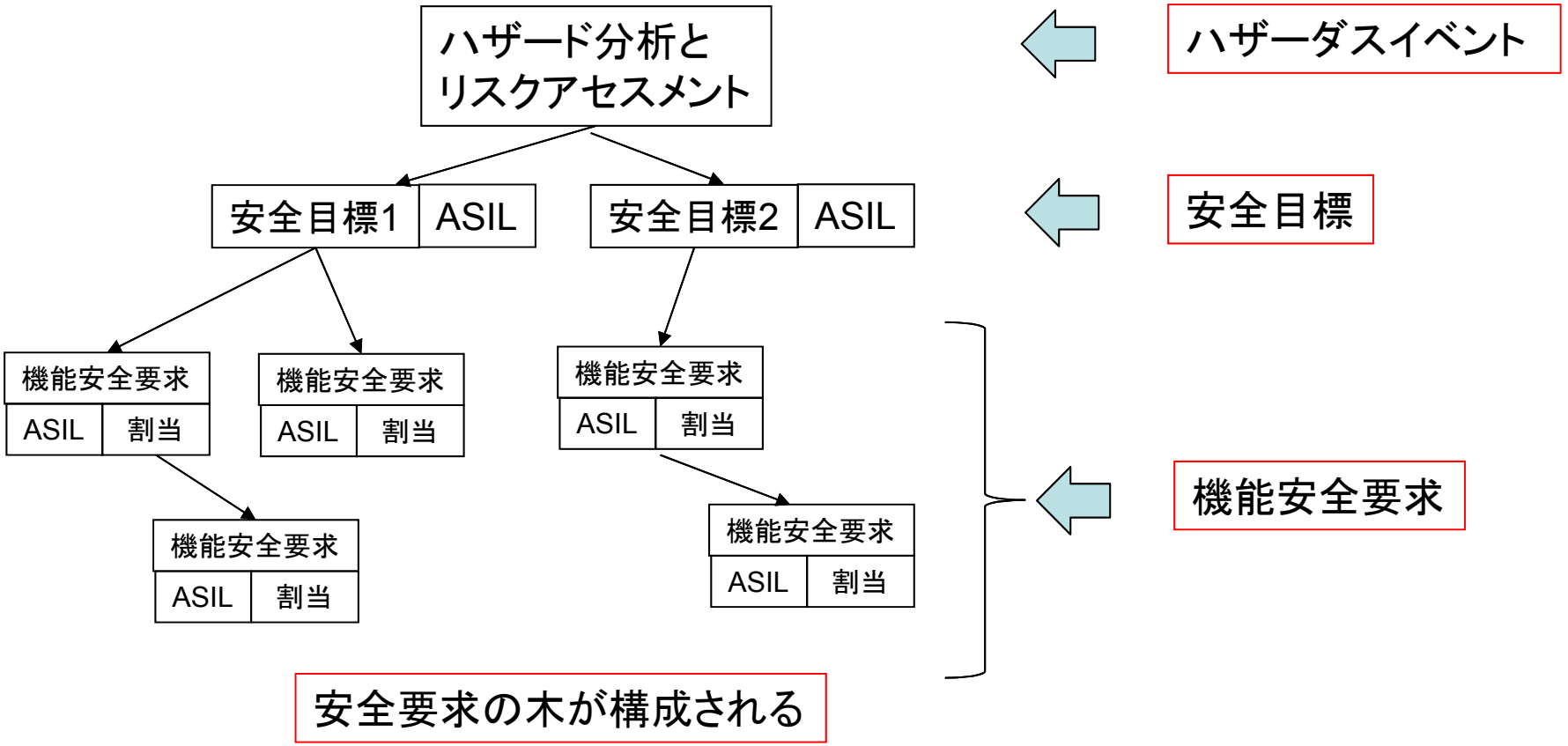
議論したい内容(4)

- セーフティとセキュリティにおいてリスクという概念は同一と考えてよいのか？
  - 許容可能なリスク、受容可能なリスク、残存リスク、ALARP (As Low As Reasonably Practicable)といった概念は共通して利用できるのでは？
- リスクをアセスメントする評価原理(要素)を明確にすることが重要だが、それは統一できるのか？
- セキュリティのリスクアセスメントとセーフティのリスクアセスメントは影響しないのか？もし影響がある場合は、どのようにすれば良いのか？

5. 要求

5-1. 機能安全要求の導出方法

- ISO 26262 Part 3（安全コンセプト）の機能安全要求の導出方法
  - 要求工学におけるゴール指向要求分析（Goal-Oriented Requirements Engineering とほぼ同等

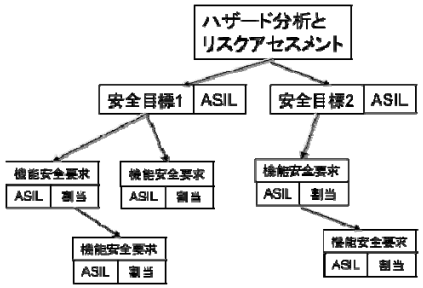


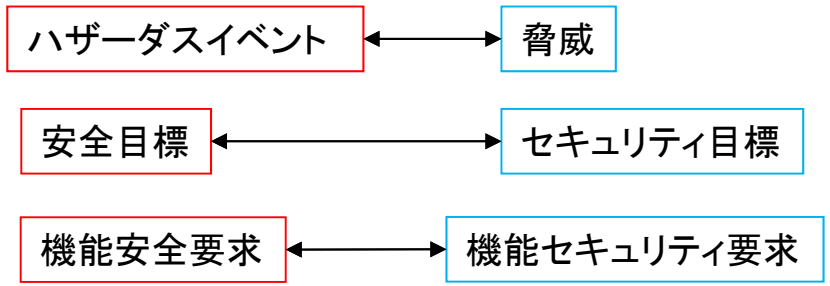
A. van Lamsweerde: Requirements Engineering: From System Goals to UML Models to Software Specifications, Wiley (2009)

5-2. 安全とセキュリティの平行理論/準同型写像(要求レベル)

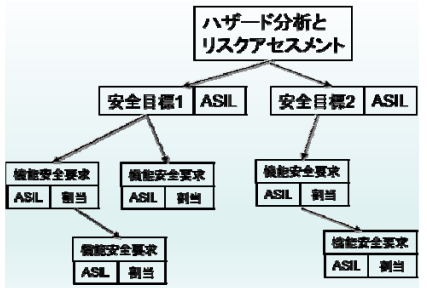
- 安全要求の導出方法はそのままセキュリティ要求の導出方法の方法として利用することは、原理的に可能。
- 安全側とセキュリティ側の概念の類似性から、以下のような対応関係を定義し、(機能)セキュリティ要求を導出する、というプロセスの構築は可能。

安全側(ISO 26262 Part3)



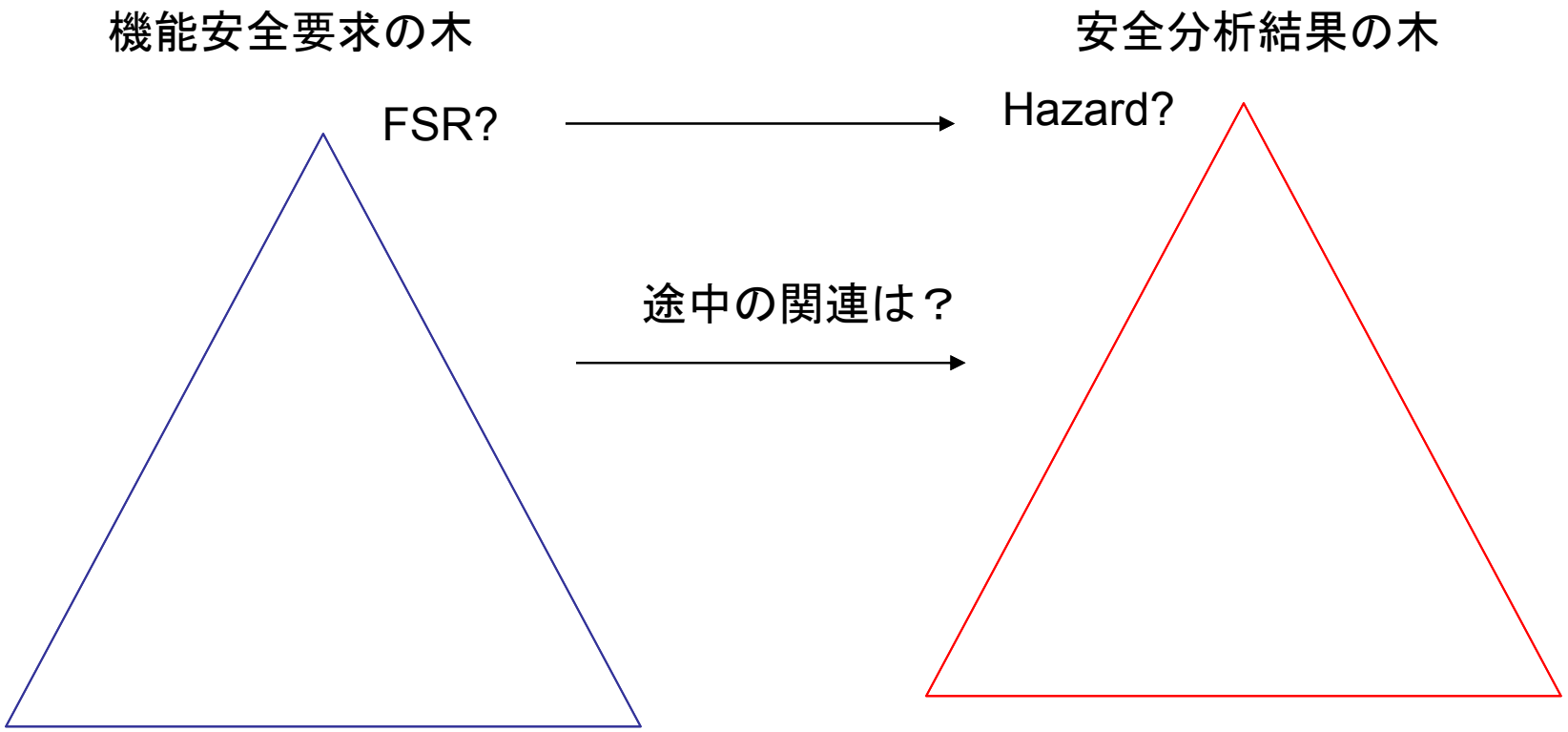


セキュリティ側(?)



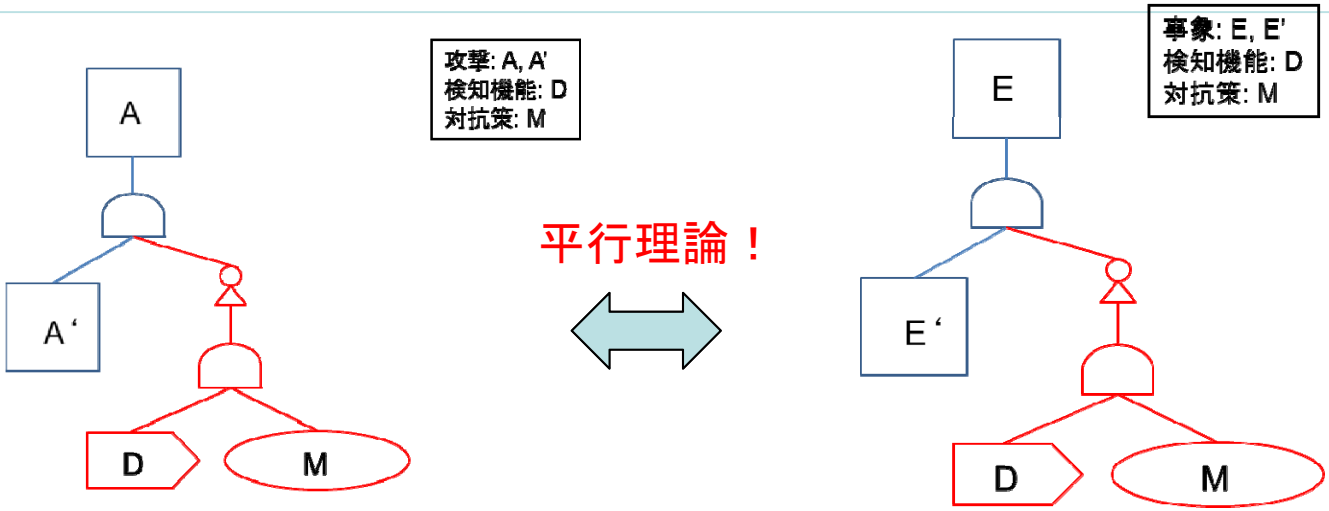
5-3. 安全要求の故障との関連

- 安全要求の導出の結果、得られる要求木と故障の原因の分析との関連は？
- 要求の木に対して、故障の木（例えば、FT）との関係は明確になっているか？
- 両者は対応が可能か？



5-4. 安全要求とセキュリティ要求（FT と AT)

- 機能安全要求とセキュリティ要求の分析と統合には、攻撃木の拡張である Attack Countermeasure 木と、その故障木版である Fault Mitigation 木を利用することが可能である。
- このような手法を利用することで、故障診断と機能安全要求、攻撃手段と対抗策を同時に分析することが出来る。



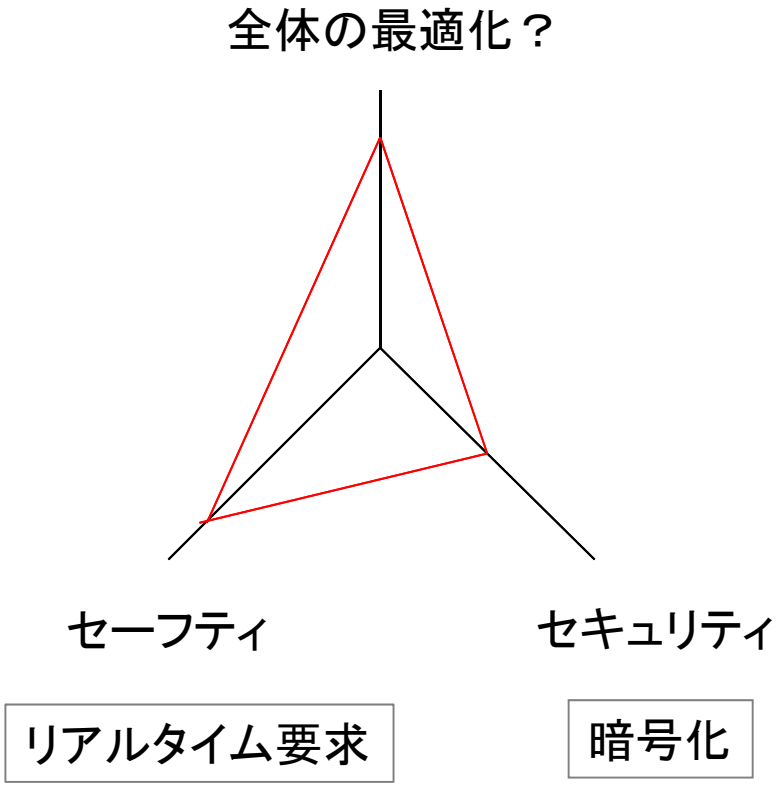
Attack countermeasure 木

Fault Mitigation 木（田口考案）

+ A. Roy, D. S. Kim, K S. Trivedi: ACT: Attack Countermeasure Trees for Information Assurance Analysis, INFOCOM IEEE Conference on Computer Communications Workshops, p1-2 (2010)
+ A. Roy, D. S. Kim, K. S. Trivedi: ACT: Towards unifying the constructs of attack and defense trees, Security and Communication Networks, 5(8), pp929-943 (2012)

5-5. セーフティ要求とセキュリティ要求のトレードオフ

- セーフティ側からの要求とセキュリティ側からの要求を同時に満足できない場合がある
  - これは特にセーフティとセキュリティに限られた話ではない
- 簡単な例としては、以下のような要求の場合、
  - セーフティ—要求：何らかのハードなリアルタイム性
  - セキュリティ要求： 暗号・復号化



安全側からは、このようにしたい！

議論したい内容(5)

- セーフティとセキュリティのトレードオフは必要か？
- 必要な場合、何か方法論があるのか(評価、改変、導出等)？
- セーフティ側とセキュリティ側ではアセスメントの基準が違うようだが、何が最適であるかについて公平に判断することは可能か？

6.セーフティとセキュリティの規格の状況

6-1. 国際規格おけるセーフティとセキュリティの統合（新たな動向）

- IEC TC65
  - Industrial-process measurement, control and automation（工業用プロセス計測制御）
    - 以下の機能安全規格とセキュリティ規格策定の母体
    - IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems -
    - IEC 62443, Industrial communication networks – Network and system security –

- WG 20（Framework to bridge the requirements for safety and security）
  - 今年 5月に立ち上がった新ワーキングで、Convener は出町氏（横河）、日本からの expert は 4名（田口（AIST）、金川氏（日立）、神余氏（三菱）、櫛引氏（JQA））
  - 現在、expert は全体で 30名。国別ではドイツが8名で最大。ドイツは本WG設立には反対票を出していたが、現在は最大の参加となっている
  - 国内委員会は28名（第一回委員会での参加者）
  - 何をするかはまだ議論が完全に収束していないが、以下のような議論がある
    - **IEC 61508 と IEC 62443 に対して、recommendation を出す**
    - **IEC 61508 と IEC 62443 をブリッジする（これは CD の主内容として入っている）**
    - **安全とセキュリティのオントロジーの整理**
    - **プロセスのマッピング**

6-2. 他のセーフティとセキュリティ関連規格

- IEC 全体での調和は？
  - TC 44 (Safety of machinery –Electrotechnical aspects) が同様の規格を策定しようとしているので、そこで競争がある。ただし、両方に参加している委員もあり、今後、反発、融合、独自路線の選択等がありうる。
  - **ただし、TC65 は basic standard である 61508 と horizontal standard である 62443 を担当しているので、こちらの方が取扱い規格の範囲が大きく、影響力が強いという特徴がある。**
- 他の規格団体とどのように調和するか？
  - 特に、IEC 62443 は ISA 99 が策定した規格を採用しているので、外部組織との調整が必要
- 何がスコープかが明確でなく、様々な利害を抱えているメンバー間での調整が必要。

6-3. 様々な産業界における安全とセキュリティの規格

- 多くの産業分野において、安全性とセキュリティの保証が必要になっています。
- それらの産業分野において（機能）安全とセキュリティの規格が策定されつつあります。

Safety DO-178C　Security DO-326A

RAMS IEC 62278　Security IEC 62280

Safety ISO 26262　Security J-3061

注：RAMS (Reliability Availability Maintainability Safety)

6-4. 自動車業界における安全規格とセキュリティ規格

対応は大別して二通り考えられる

Safety

ISO 26262

Security

?

SAE J-3061 Cybersecurity Guidebook

IEC 62443

ISO/IEC 15408

VDA (German Association of the Automotive industry)

もしくは

Safety

ISO 26262

Security の要素 (I/F)を導入

どのレベルで導入するかは色々な考え方が可能

6-5. 航空機の場合

現状

Safety　　Security

DO-178C ⟷ DO-326A

- プロセスとしての関連付け
- 認証としての関連付け

航空機業界においては、2014年に以下のセキュリティの規格が発行された。

+ DO-326A/ED-202A
+ DO-356
+ DO-355/ED-204

理想的な状況に見えるが、いくつかの問題点がある。

- 安全側とセキュリティ側のプロセスが同等でない。
- 北米の規格団体（RTCA）とヨーロッパの規格団体（EUROCAE）の間で合意がなされてないガイドラインが存在する（DO-356)

- セキュリティと安全の関連は付いている。

議論したい内容(6)

- 規格レベルでの統合を早くやってほしい？必要ない？
  - 勝手に決めるな？
- 規格レベルで統合したら、本当に問題は解決するのか？
  - 無駄な仕事を増やすな？
- 規格レベルで決められるほど、双方を統合するやり方が解明されているのか？

7. セーフティーケース

7-1. セーフティーケース（制度）とは？

・1988年7月における、北海油田における Piper Alpha 事故167名死亡（229名中）、270億円の被害を生じた。

・Cullen 卿による事故調査レポートにより安全ケースの重要性が強調された。

“Compliance with detailed prescriptive regulations was not sufficient to ensure safety”

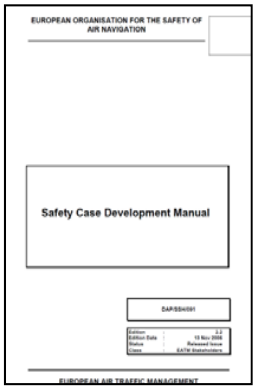
The Offshore Installations (Safety Case) Regulations 1992 に導入。
(最新版 2005)

法規、規格に書かれた通りにすれば安全であるという考え方への反省から、セーフティケースの提出、アセスメント方式の厳格化などについて社会的基盤の形成、研究が進んだ。

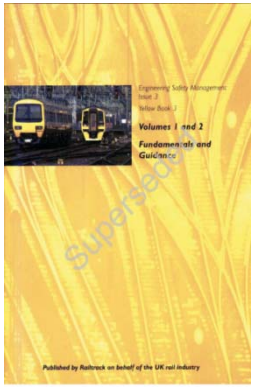
セーフティーケース制度（Safety Case Regime）の導入！

7-2. セーフティーケースの提出が必要な規格

- EUROCONTROL
  - 航空管制システムにおける安全性の保証



- Rail Yellow Book
  - 英国における鉄道信号システムの安全性の保証
- Railway Safety Case Regulations
  - 英国における鉄道安全法規
- IEC 62425/EN 50129
  - 鉄道システムのセーフティーケース規格



- ISO 26262
  - 車載組込みシステムの機能安全規格

- その他（防衛、原子力、海上設備、医療機器）

7-3. 車載の安全とセキュリティ（保証のフレームワーク）

SafSec 方法論

Safety

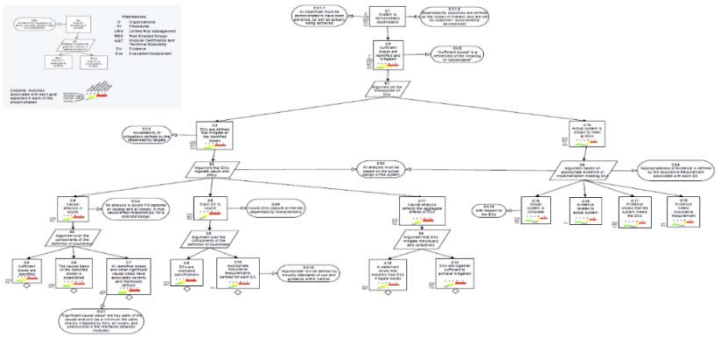
Def-Stan 00-56

Security

ISO/IEC 15408

Dependability の保証

Dependability Case による統合



Safety Case & Security Case

Safety

ISO 26262

Security

J-3061
Cybersecurity
Guidebook (SAE)

Safety Case　Cybersecurity Case

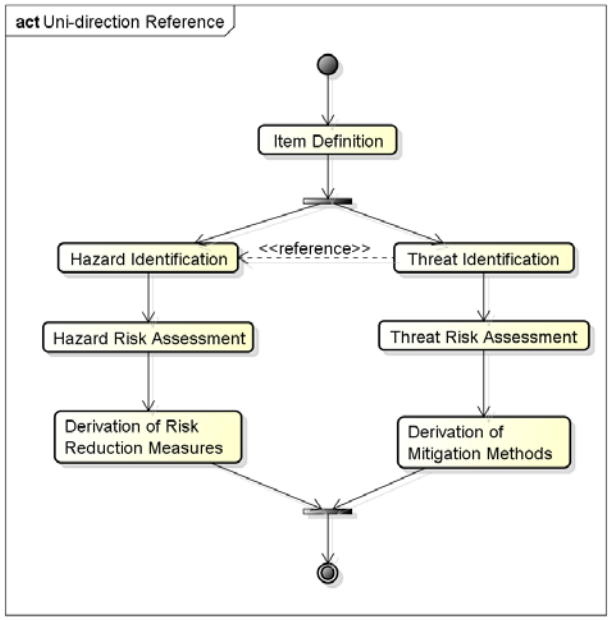
可能な未来像の一つ

Praxis: SafSec: Integration of Safety & Security Certification, SafSec Methodology: Guidance Material, 2006.
Praxis: SafSec: Integration of Safety & Security Certification, SafSec Methodology: Standard, 2006.

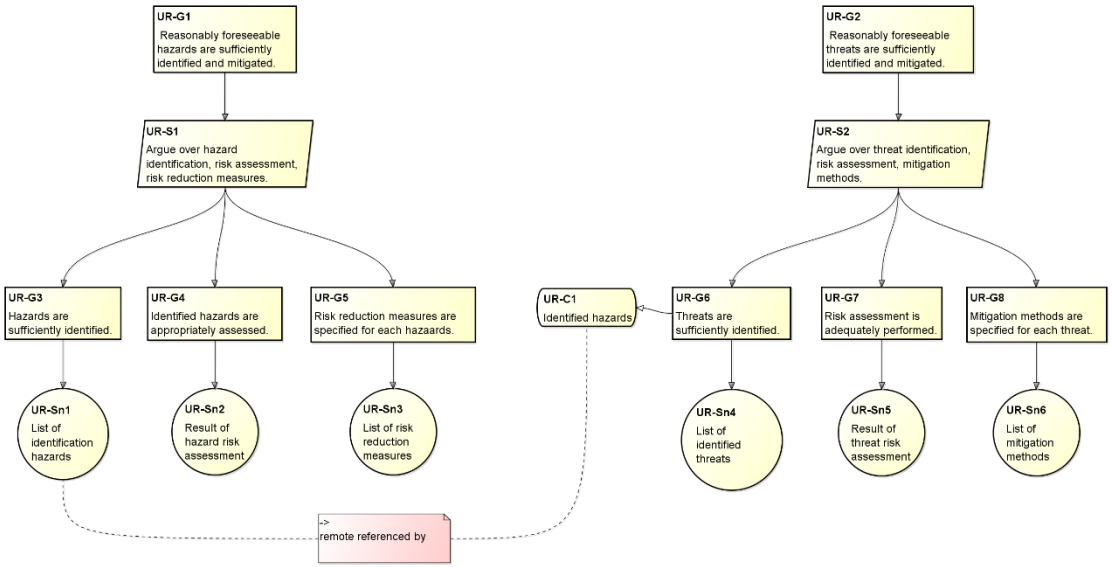
7-4. Safe & Sec Case Patterns

- 今後、安全性とセキュリティの両方を保証する枠組みとして、セーフティーケースとセキュリティケースの整合的な統合が必要になる。
- 安全とセキュリティの統合プロセスパターンに従って、セーフティーケースとセキュリティケースの構造をパターン化可能である。

プロセスとして独立、単方向参照型プロセス



左のプロセスに基づいた Safe&Sec Case の GSN での表現



+ K. Taguchi, D. Souma, H. Nishihara: Safe & Sec Case Patterns, ASSURE 2015

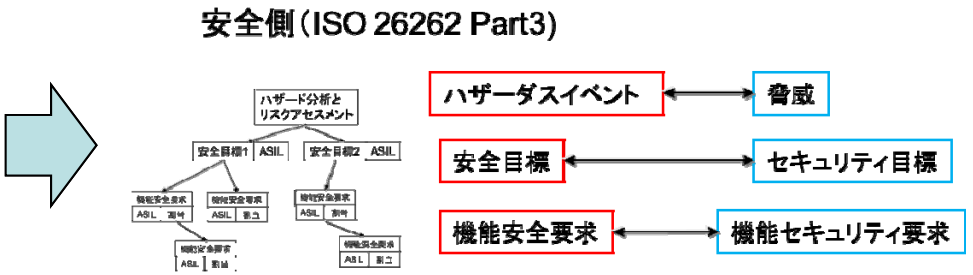
8. SCDL

- SCDL がセキュリティ側の開発で利用することはできるのか？

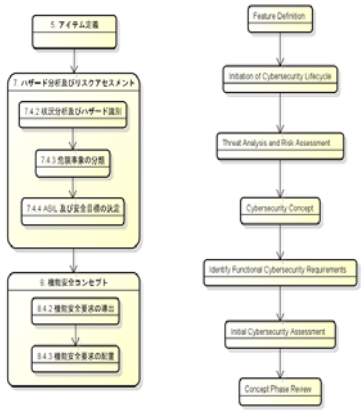
- 可能ならば、安全側の機能安全コンセプト開発支援とセキュリティ側の機能セキュリティコンセプト開発支援が統合した形で実施可能になり、開発コストの削減や品質の向上につながる可能性があるのか？

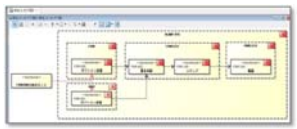
8-1. SCDL と セキュリティ

- 安全要求 vs セキュリティ要求
  - 「要求を割り当てる」というのは、様々な機能安全において標準的に規定されていないが、有効な開発手段
  - セキュリティ機能の開発支援
- 機能安全コンセプト vs サイバーセキュリティコンセプト
  - J3061 においては、cybersecurity concept の開発が示されている。
  - SCDL を用いて、cybersecurity concept の開発を支援
- 機能安全コンセプトの作成結果をセキュリティ分析において利用
  - 安全要求とセキュリティ要求の調和的開発支援言語として利用



ISO 26262 Part 3　J3061





脅威の同定、等を実施

SCDL 図

8-2. SCDL に対するセキュリティからの要求

- 支援が要求されるタスク
  - 脅威分析
    - アタックサーフェイスの同定（通信経路、通信路）
    - 脅威の同定
    - 保護資産の同定
  - セキュリティ要求
    - 導出
    - 安全要求とセキュリティ要求の影響分析
  - リスクアセスメント

9. 最後に

9-1. 今後の展望

- 今後、3~10年の間に、セキュリティとセーフティの関連が明確になり、統合プロセスや統合的な分析手法が明確になり、ガイドライン、規格としても整理されることが予想される。

- これをビジネスチャンスとして捉えるか（品質向上、新機能の開発）、従来のプロセスや開発手法に対する影響を考え、ネガティブに捉えるかにより、ビジネスに影響がある可能性がある課題だと思われる。