2017年度第2回ITリスク学研究会

セーフティとセキュリティの統合に関する課題と方法論

Security First

CAV Technologies

田口研治

（株）シーエーブイテクノロジーズ

2017年08月02日

自己紹介

【経歴】

- (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)～
- 産業技術総合研究所　招聘研究員　(併任) 2010年4月～
- 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20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(12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】

十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)
十形式手法、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 '17, ICECCS '17, HASE '16, SASSUER '17, SAFECOMP '18)

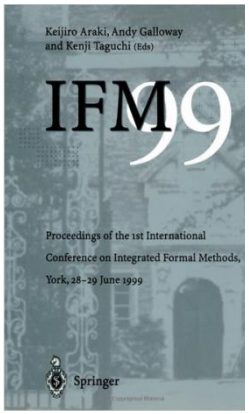
【規格、国際会議関連】

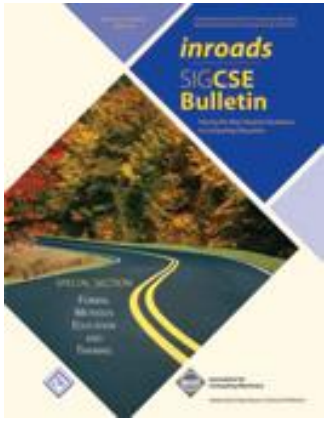
- International Conference on Formal Engineering Methods 2012 のプログラム委員長
- OMG System Assurance Platform Task Force の co-chair
- SICE 認証工学 WG 主査
- IEC TC65/WG 20 (Framework to bridge the requirements for safety and security) Expert

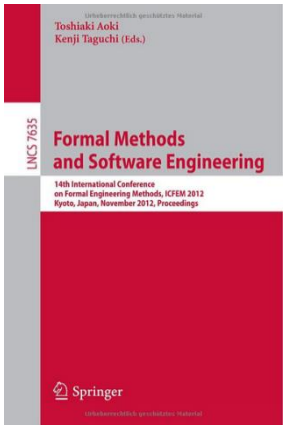
【弊社の活動】

- SIP V2X セキュリティにおける「脅威分析共通プラットフォーム」の研究開発
- 車載系の機能安全開発プロセスとセキュア開発プロセスの統合支援
- 脅威分析ツール Seculia 共同開発

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

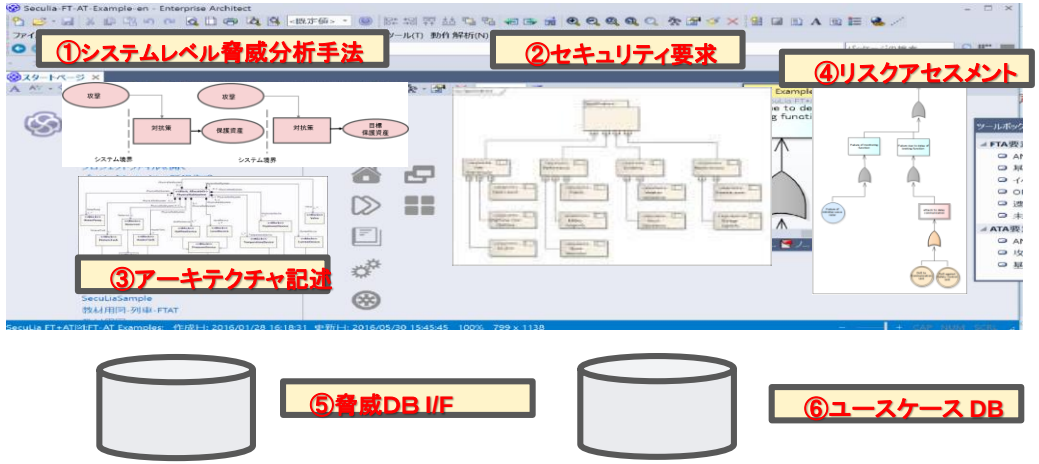
ACM SIGCSE, inRoads Bulletin, 2009年。共同編者
(Special Issue on Formal Methods Education and Training)

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

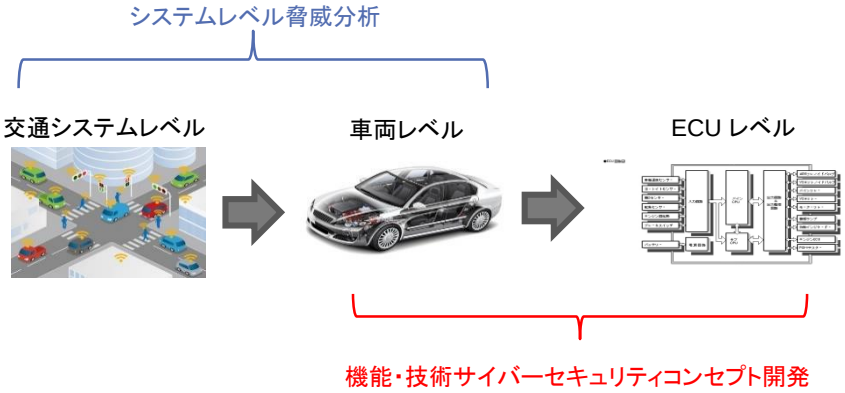
International Conference on Formal Engineering Methods (ICFEM) 国際会議 2012年。共同編者

SIPプロジェクト(2016年度):脅威分析共通プラットフォームの開発

- 以下の SIP プロジェクトのために、車載システム開発のための統合的な、脅威分析共通プラットフォームの開発を支援しております。
- 戦略的イノベーション創造プログラム(SIP)
  - http://www8.cao.go.jp/cstp/gaiyo/sip/
  - 内閣府の総合科学技術・イノベーション会議による、科学技術イノベーションを実現するために創設するプログラム。
  - 11分野(次世代パワーエレクトロニクス、自動走行システム、重要インフラ等におけるサイバーセキュリティの確保、他)にわたる課題に注力
- 自動走行システム
  - 情報セキュリティ
    (1)自動走行システムの安全性・信頼性の確保
    (2)共通モデル構築・脅威分析、セキュリティ要件・対策
    (3)攻撃への対策の評価・認証
    (4)通信システムのセキュリティ機能

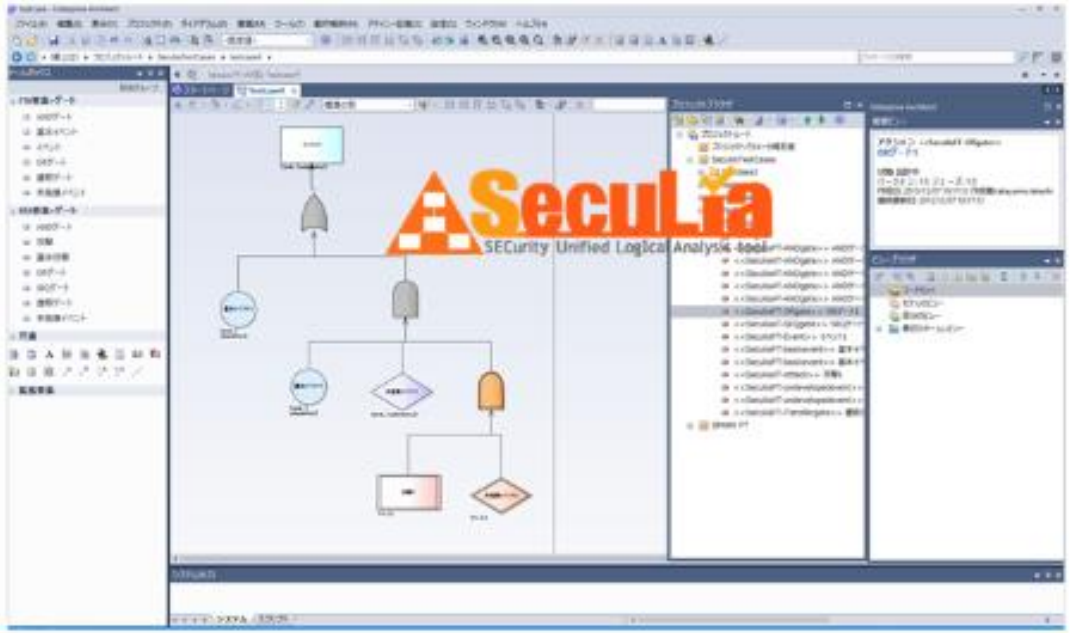


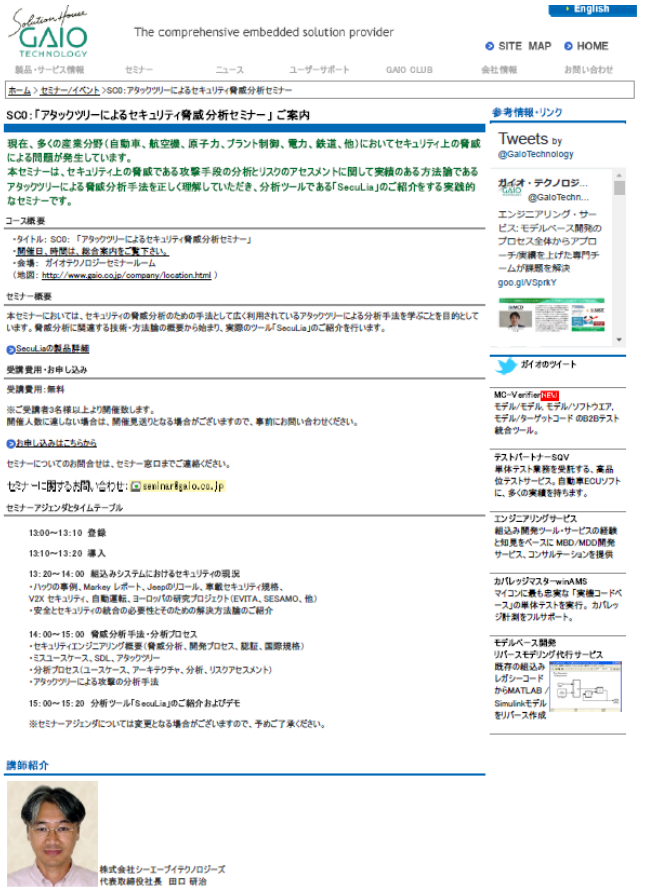
実現予想図(開発中)



支援開発フェーズ

SECULIA と（無償）脅威分析セミナー





- **SecuLia は弊社とガイオ･テクノロジー社との共同で開発された脅威分析ツール**
  - https://www.gaio.co.jp/product/dev_tools/pdt_seculia.html
  - Enterprise Architect（Sparx Systems 社）のプラグインとして提供
- **機能**
  - Fault Tree 分析
  - Attack Tree 分析
    - ✓ CC-CEM と EVITA に基づいたアセスメント計算
    - ✓ アタックシナリオ（最少カット集合）とそのアセスメント計算
- **FT-AT 分析**
  - FT分析とAT分析を統合した新手法
  - セキュリティによる安全への侵害の分析が可能

- **SC0:「アタックツリーによるセキュリティ脅威分析セミナー」**
  - https://www.gaio.co.jp/event/regular/sem_sc0.html
- **セキュリティ上の脅威分析についての概要説明**
  - セキュア開発プロセス
  - Attack Tree 分析
  - FT-AT 分析

1. 安全とセキュリティの課題

1-1. 迅速な対応（インシデントに対する分析・対応）

- 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？

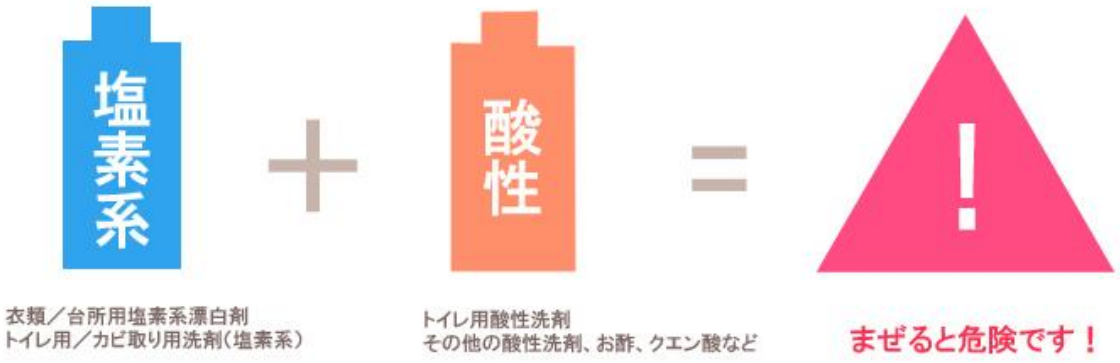
従来は、安全性・信頼性を考えていれば良かったが、事故の原因としてセキュリティ上の脅威が加わったことでその対応が必要になった。

機械故障？

もしかしてハッキング？

1-2. セーフティとセキュリティの統合って簡単？

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？

1-3. オーストラリアの下水処理場（Maroochy）でのインシデント

- **対象システム**
  - オーストラリア、マルーチーにおける下水処理場
  - SCADA システムは、汚水処理の管理のための 300ノード（142のポンプステーション）から構成
  - 無線による制御
- **インシデント**
  - 2000年に、3カ月間に46の異なるインシデント
  - 150 のポンプステーションの制御が乗っ取られる
- **利用された装置**
  - ラップトップPCと無線送信機
  - 盗んだ SCADA制御ソフトを利用

Chapter 6

LESSONS LEARNED FROM THE MAROOCHY WATER BREACH

Jill Slay and Michael Miller

Abstract Supervisory control and data acquisition (SCADA) systems are widely used to monitor and control operations in electrical power distribution facilities, oil and gas pipelines, water distribution systems and sewage treatment plants. Technological advances over the past decade have seen these traditionally closed systems become open and Internet-connected, which puts the service infrastructures at risk. This paper examines the response to the 2000 SCADA security incident at Maroochy Water Services in Queensland, Australia. The lessons learned from this incident are useful for establishing academic and industry-based research agendas in SCADA security as well as for safeguarding critical infrastructure components.

Keywords: SCADA security, Maroochy Water Services breach

1. Introduction

Great concern has been expressed regarding the security of supervisory control and data acquisition (SCADA) systems in the light of the breach that occurred in 2000 at Maroochy Water Services in Queensland, Australia [6, 13]. This paper discusses the Maroochy Water incident and the response to the incident. Lessons learned from the incident, which have not been widely reported, are discussed in this paper. These lessons are useful for establishing academic and industry-based research agendas in SCADA security as well as for safeguarding critical infrastructure components.

2. SCADA Systems

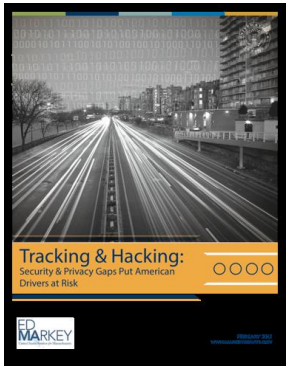
SCADA systems are used for gathering real-time data, monitoring equipment and controlling processes in industrial facilities and public utilities, including chemical plants and refineries, electrical power generation and transmission systems, oil and gas pipelines, and water and sewage treatment plants [9]. Servers,

Slay, J. and Miller, M., 2008, in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 73–82.

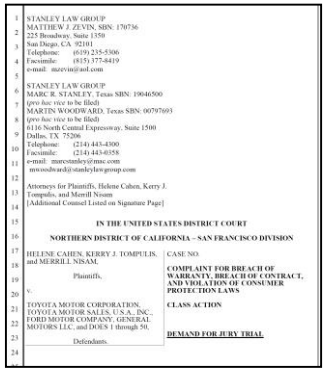
1-4. 自動車業界におけるセキュリティの課題

- 2014年　米国上院議員 E. Markey 氏が自動車のセキュリティに関する報告書を出しました。
- 2015年3月　Markey 議員によるレポートの指摘から、Ford, GM, Toyota が、車載ネットワークの脆弱性に対して対抗策を実施していなかった、ということで集団告訴が起こりました。
- 2015年 Chrysler 社の Jeep Chelokee のハッキング問題でリコールが発生しました。
- 2015年 通称 Spy Car Act Bill が提出され、今後、車のセキュリティ対策が法制化される可能性があります。
- 2016年2月 日産 LEAF のアプリ（Nissan Connect EV）から VIN によるアクセスでエアコン等が制御可能であることが発見されました。
- それ以降も、Tesla 社の Model S へのハッキングなど、様々な事例が報告されています。

Markey レポート



告訴状


STANLEY LAW GROUP
MATTHEW J. ZEVIN, SBN: 170736
225 Broadway, Suite 1350
San Diego, CA 92101
Telephone: (619) 235-5306
Facsimile: (815) 377-8419
e-mail: mzevin@stanleylaw.com

STANLEY LAW GROUP
MARC R. STANLEY, Texas SBN: 19046500
(*pro hac vice* to be filed)
MARTIN WOODWARD, Texas SBN: 00797693
(*pro hac vice* to be filed)
6116 North Central Expressway, Suite 1500
Dallas, TX 75206
Telephone: (214) 443-4300
Facsimile: (214) 443-0358
e-mail: marcstanley@msc.com
mwoodward@stanleylawgroup.com

Attorneys for Plaintiffs, Helene Cahen, Kerry J. Tompulis, and Merrill Nissm
[Additional Counsel Listed on Signature Page]

IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN FRANCISCO DIVISION

HELENE CAHEN, KERRY J. TOMPULIS, and MERRILL NISAM,

Plaintiffs,

v.

TOYOTA MOTOR CORPORATION, TOYOTA MOTOR SALES, U.S.A., INC., FORD MOTOR COMPANY, GENERAL MOTORS LLC, and DOES 1 through 50,

Defendants.

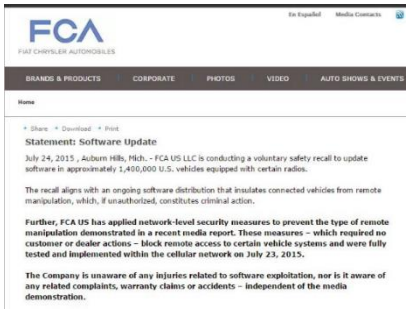
CASE NO.

COMPLAINT FOR BREACH OF WARRANTY, BREACH OF CONTRACT, AND VIOLATION OF CONSUMER PROTECTION LAWS

CLASS ACTION

DEMAND FOR JURY TRIAL

リコール


FCA
FIAT CHRYSLER AUTOMOBILES

En Español Media Contacts

BRANDS & PRODUCTS CORPORATE PHOTOS VIDEO AUTO SHOWS & EVENTS

Home

Share Download Print

Statement: Software Update

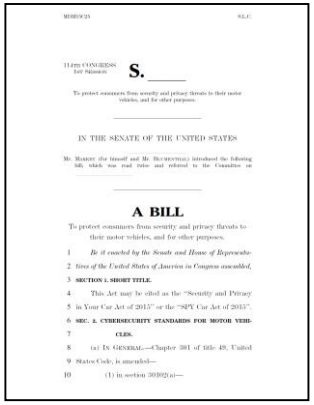
July 24, 2015 , Auburn Hills, Mich. - FCA US LLC is conducting a voluntary safety recall to update software in approximately 1,400,000 U.S. vehicles equipped with certain radios.

The recall aligns with an ongoing software distribution that insulates connected vehicles from remote manipulation, which, if unauthorized, constitutes criminal action.

Further, FCA US has applied network-level security measures to prevent the type of remote manipulation demonstrated in a recent media report. These measures – which required no customer or dealer actions – block remote access to certain vehicle systems and were fully tested and implemented within the cellular network on July 23, 2015.

The Company is unaware of any injuries related to software exploitation, nor is it aware of any related complaints, warranty claims or accidents – independent of the media demonstration.

Spy Car Act Bill


S. _____

IN THE SENATE OF THE UNITED STATES

A BILL

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

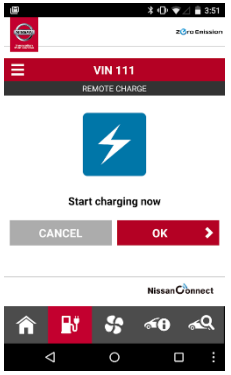
This Act may be cited as the "Security and Privacy in Your Car Act of 2015" or the "SPY Car Act of 2015".

SEC. 2. CYBERSECURITY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—Chapter 301 of title 49, United States Code, is amended—

(1) in section 30102(a)—

Connect EV

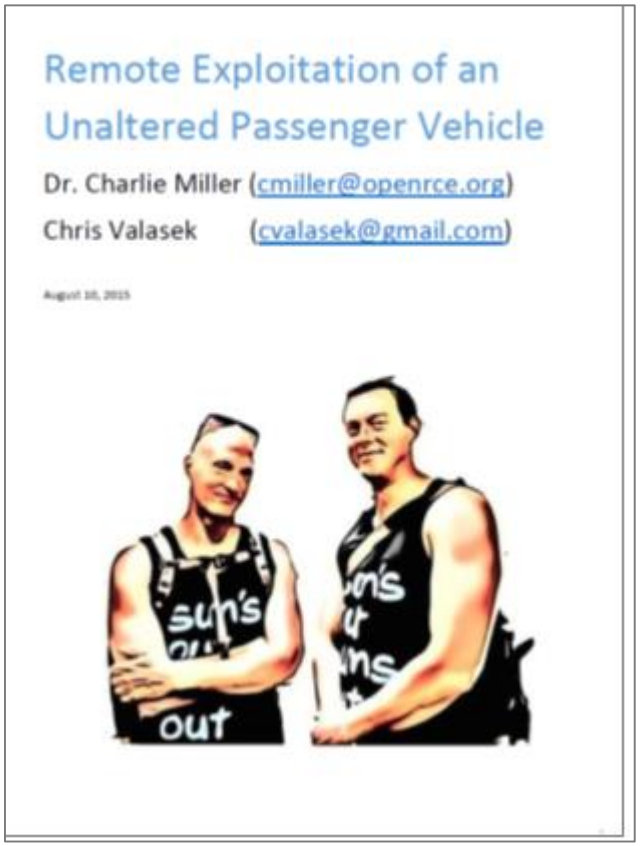


1-5. 自動車業界におけるハックの例

- **Jeep Chelokee への遠隔からのハッキングが、C. Miller と Chris Valasek により行われました。**
  - Black Hat 2015, Remote Exploitation of an Unaltered Passenger Vehicle, 2015
  - レポートは以下から入手可能
    - ✓ http://illmatics.com/Remote%20Car%20Hacking.pdf

- **攻撃の特徴**
  - 外部からの遠隔操作
    - ✓ CANバスに直接、接続して侵入したのではなく、外部から Infotainment 系を経由して、遠隔操作に成功。
  - 制御の乗っ取り。
    - ✓ 複数の ECU による制御に対して、一つのECU を diagnostic session に遷移させ、ECU への制御用メッセージのなりすましに成功。

- **セキュリティ上の脅威 vs 安全のためのメカニズム**
  - Diagnostic session に遷移するのは低速時だけ、というセーフティ機構である程度、防御されていた。



（リコールの際に配布されたメモリースティック）

自動車業界におけるハックの例（2）

- **2016 年の Tesla Model S に対するハッキングは Jeep の例と同様に、セキュリティ上の攻撃と安全機構との関連が明らかに示されている。**
  - Black Hat 2016, Free-Fall: Hacking Tesla From Wireless to CAN Bus
- **攻撃の特徴**
  - 外部からの遠隔操作
    - ✓ Infotainment 系を経由して、遠隔操作に成功。
  - 制御の乗っ取り。
    - ✓ ECU への制御用メッセージのなりすましに成功。
- **セキュリティ上の脅威 vs 安全のためのメカニズム**
  - Jeep と同様に、高速で運転している場合、なりすましメッセージを送付しても無視された。

Tencent 腾讯 KEEN SECURITY LAB　black hat

FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

Sen Nie, Ling Liu, Yuefeng Du
Keen Security Lab of Tencent
{snie, dlingliu, davendu}@tencent.com

ABSTRACT

In today's world of connected cars, security is of vital importance. The security of these cars is not only a technological issue, but also an issue of human safety. In our research, we focused on perhaps the most famous connected car model: Tesla.

In September 2016, our team (Keen Security Lab of Tencent) successfully implemented a remote attack on the Tesla Model S in both Parking and Driving mode.[1-3] This remote attack utilized a complex chain of vulnerabilities. We have proved that we can gain entrance from wireless (Wi-Fi/Cellular), compromise many in-vehicle systems like IC, CID, and Gateway, and then inject malicious CAN messages into the CAN Bus. Just 10 days after we submitted our research to Tesla, Tesla responded with an update using their OTA mechanism and introduced the code signing protection into Tesla cars.

Our paper will be in three parts: our research, Tesla's response, and the follow-up. We will, for the first time, share the details of the whole attack chain on the Tesla, and then reveal the implementation of Tesla's OTA and Code Signing features. Furthermore, we'll explore the new mitigation on Tesla and share our thoughts on them.

TARGET VERSION

We have successfully tested our vulnerabilities on Tesla Model S P85 and P75, the latest version at that time was as follows.

Model S	Version (Build Number)	gw://firmware.rc
P85	v7.1(2.28.60)	fileCrc 502224ba
P75	v7.1(2.32.23)	fileCrc e3deeaab

Table 1 Tested version

REMOTE ATTACK SURFACE

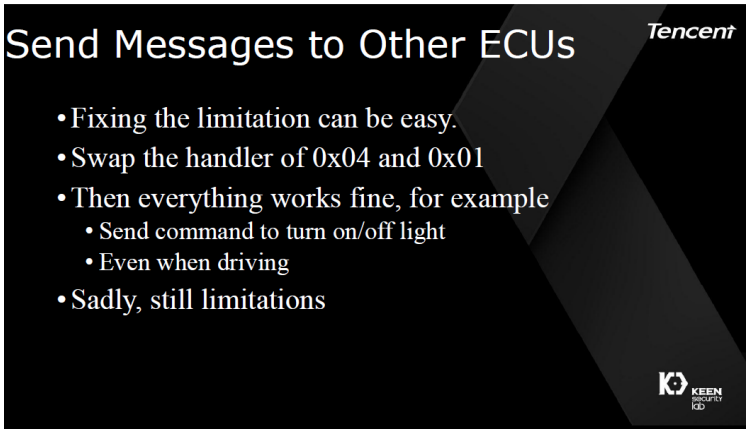
The truth is that we found our browser exploit first, then we think a contactless approach should be achieved.

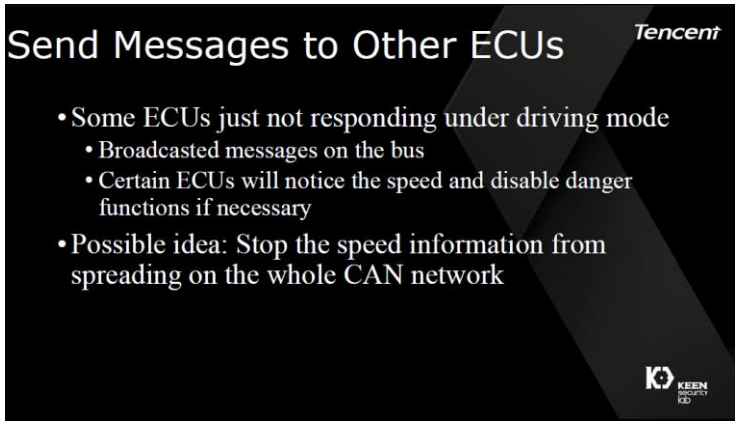
A Wi-Fi SSID, `Tesla Service`, is embedded in every tesla car as we know it, and the password is a plaintext which saved in `QtCarNetManager`. However, we find that it cannot be auto connected in normal mode.

At that time, `Tesla Guest` came into our sight, this is a Wi-Fi hotspot provided by Tesla body shop and superchargers.[4] The information of this SSID is saved in many customers' cars in order to auto connecting in the future. If we fake this Wi-Fi hotspot and redirect the traffic of `QtCarBrowser` to our own domain, remotely hacking Tesla cars can be feasible.

Besides Wi-Fi tricks, when in cellular mode we believe that phishing and user mistyping can also lead to remotely triggering our browser vulnerabilities if we build enough crafted domains.

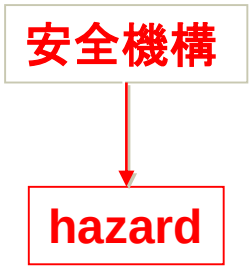
Because it's based on a browser-borne attack, we can say that remotely deliver the exploit without physical access is only restricted by imagination.





1-6. 安全機構 VS セキュリティ機構

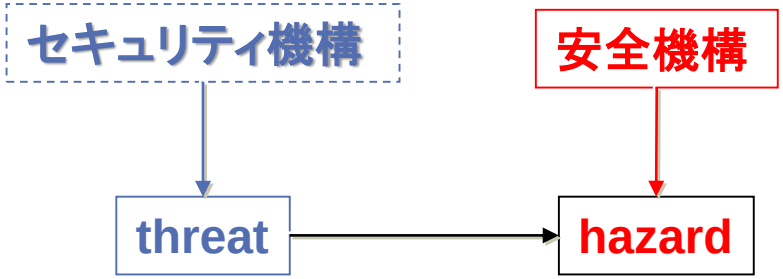
【安全だけの場合】



【セキュリティが加わった場合（基本図式）】

注：ここでは、ハザードの原因となる
脅威について考察

【安全機構とセキュリティ機構による防御】

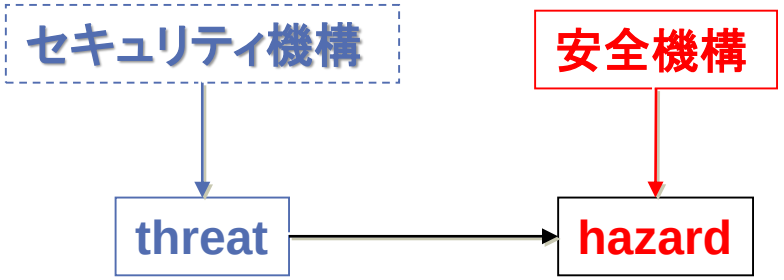


【今後の可能性】

？

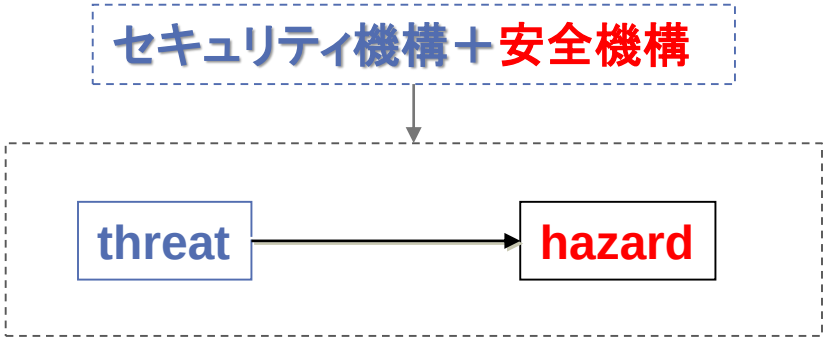
1-7. 安全機構とセキュリティ機構の関係

【安全機構とセキュリティ機構による防御】

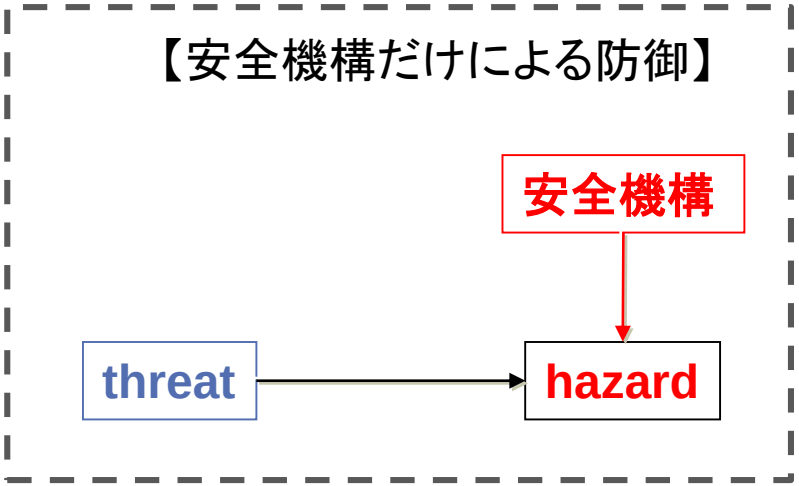


（ジープの例）

【安全機構とセキュリティ機構の合成】

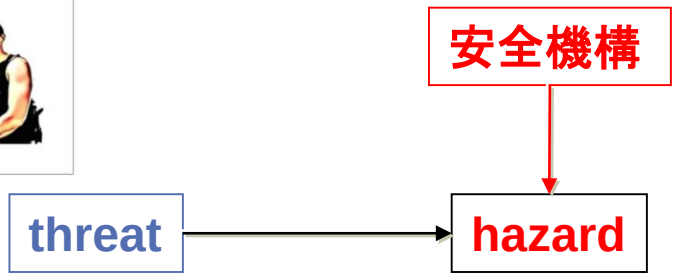


【安全機構だけによる防御】



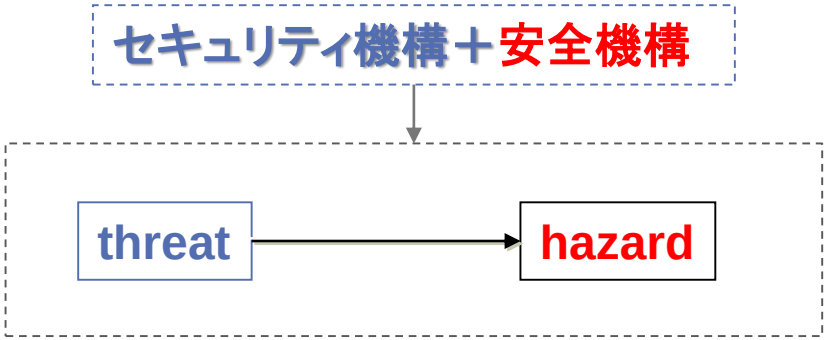
1-8. 安全機構とセキュリティ機構の補完関係

【安全機構だけによる防御】



- セキュリティ上の脅威が発生しても、安全機構により、安全状態に遷移させる。
- 縮退機能により、機能が低下しても動作を保証。

【安全機構とセキュリティ機構の合成】



- 安全機能、例えば、冗長系を用いて、セキュリティ機能を補完する。
- セキュリティ機能（侵入検知）と安全機能で類似した機能（例えば、イベントログの解析）を統合することで、効率的に対策する。

1-9. SESAMO

- **SESAMO (Security and Safety Modeling)**
  - 安全要求とセキュリティ要求の合成とトレードオフについて研究。
  - D2.1 – Specification of Safety and Security Mechanisms, ver. 01, 2013

- **暗号化・復号化、署名生成と検証、ノード認証、アクセス制御・トラフィックフィルタリング、といった 18 の代表的なセキュリティ機能に対して、分析を行っている。**

- **以下に、暗号化・復号化に対する分析例を示す。**
  - トレードオフ
    - ✓ 安全性を保証するためのリアルタイム制約に対して、セキュリティからの影響としては、遅延が存在する。
    - ✓ リアルタイム特性を満たした場合、セキュリティに対しては、セキュリティのレベルの低下という影響考えられる。
  - 合成
    - ✓ セキュリティ機能としての暗号学的チェックサムは、符号誤りの検知にも利用できるので、双方にとり役に立つと言える。

	安全性	セキュリティ
トレードオフ	遅延 暗号・復号化のための計算量は暗号鍵の長さに依存。	セキュリティのレベル セキュリティのレベルは、暗号鍵の長さに依存。
合成	暗号学的チェックサムはフォルトの発見に役立つ。	

2. 安全とセキュリティに関する国際規格

2-1. 様々な業界におけるセキュリティの規格

- **多くの産業分野において、セキュリティの規格が策定されつつあります。これらの規格への対応は必須になります。**
  - 自動車業界 J3061
  - 航空機業界 DO-326A/ED-202A、DO-356、DO-355/ED-204
  - 鉄道業界 IEC 62280
  - 産業制御システム IEC 62443

- **情報セキュリティマネジメント**
  - ISO 27000 シリーズ

- **NIST**
  - SP-800 シリーズ

- **ISO/IEC 15408 (Common Criteria)**

2-2. 航空機のセキュリティ規格

規格	題	内容	発行日
DO-326A/ED-202A	Airworthiness Security Process Specification	セキュリティリスクのアセスメント方式、セキュリティの防御の設計、これらの防御が有効であることの保証について記述。	2014年8月
DO-356　注1）	Airworthiness Security Methods and Considerations	DO-326A において記述されているプロセスと活動を支援する考察と方法を記述。	2014年9月
DO-355/ED-204	Information Security Guidance for Continuing Airworthiness	航空機の運用、保守、これらのタスクを実施する要員、組織に対するガイダンス。	2014年6月

注意：
1）DO-356 の EUROCAE 版は現時点では、策定されていない。主な理由としては、ヨーロッパ勢が北米勢の提案について合意がされなかったと言われている。

2-3. 様々な産業界における安全とセキュリティの規格

- 既にある様々な安全規格とセキュリティ規格との統合・調和（ハーモナイゼーション）が問題となってきています。

Safety	Security	RAMS	Security	Safety	Security
ARP 4754A /ED-79A	DO-326A	IEC 62278	IEC 62280	ISO 26262	?

注：RAMS (Reliability Availability Maintainability Safety)

2-4. 自動車業界における安全規格とセキュリティ規格の関係

対応は大別して二通り考えられる

Safety

ISO 26262

Security の要素を導入

もしくは

Safety

ISO 26262

Security

?

どのレベルで導入するかは色々な考え方が可能

ISO 化

IEC 62443

ISO/IEC 15408

SAE J-3061 Cybersecurity Guidebook

VDA (German Association of the Automotive industry)

2-5. 計測制御関連の安全とセキュリティの規格

- **関連する機能安全規格とセキュリティ規格としては以下を上げることが出来ます。**

Safety

IEC 61508　IEC 61511

Security

IEC 62443

IEC TC65 において新しいワーキンググループが立ち上がり
セーフティとセキュリティの統合について検討が始まった。

2-6. TC65 WG 20

- **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 は日本が担当、日本からの expert は 4名
  - ✓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**

2-7. IEC における他のセーフティとセキュリティ関連の規格

- 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。

2-8. セーフティとセキュリティの認証に対する課題

【セキュリティ側】

- IEC 62443 に関連する認証制度
  - EDSA 認証
    - ソフトウェア開発の各フェーズにおけるセキュリティ評価(SDSA：Software Development Security Assessment)
    - セキュリティ機能の実装評価(FSA：Functional Security Assessment)
    - 通信の堅牢性テスト(CRT：Communication Robustness Testing)
  - CSMS（Cyber Security Management System）認証
    - セキュリティマネジメントに関する認証

【セーフティ側】

- IEC 61508 や IEC 61511 に関する認証
  - 従来の機能安全関連の認証

双方を認証する場合の課題

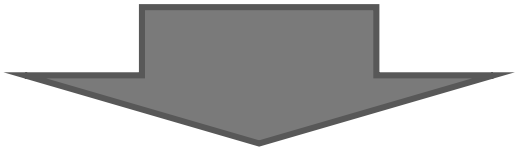
認証コストの増大

製品情報（安全、セキュリティ双方の開示）

開発・運用プロセスの新たな構築

2-9. 同時認証の課題

- 認証コストの増大
  - 二つの異なる規格による認証によりコストは2倍以上に上がる可能性がある
- 製品情報（安全、セキュリティ双方の開示）
  - 片方（セーフティもしくはセキュリティ）側での認証を受ける場合、他方からの影響を見るために他方の製品情報の開示も必要になる？
- 開発・運用プロセスの新な構築
  - 片方の開発・運用プロセスが既に完成している場合、他方の開発・運用プロセスとの相互影響等について分析し、何らかのインタフェイスを提供する必要がある？

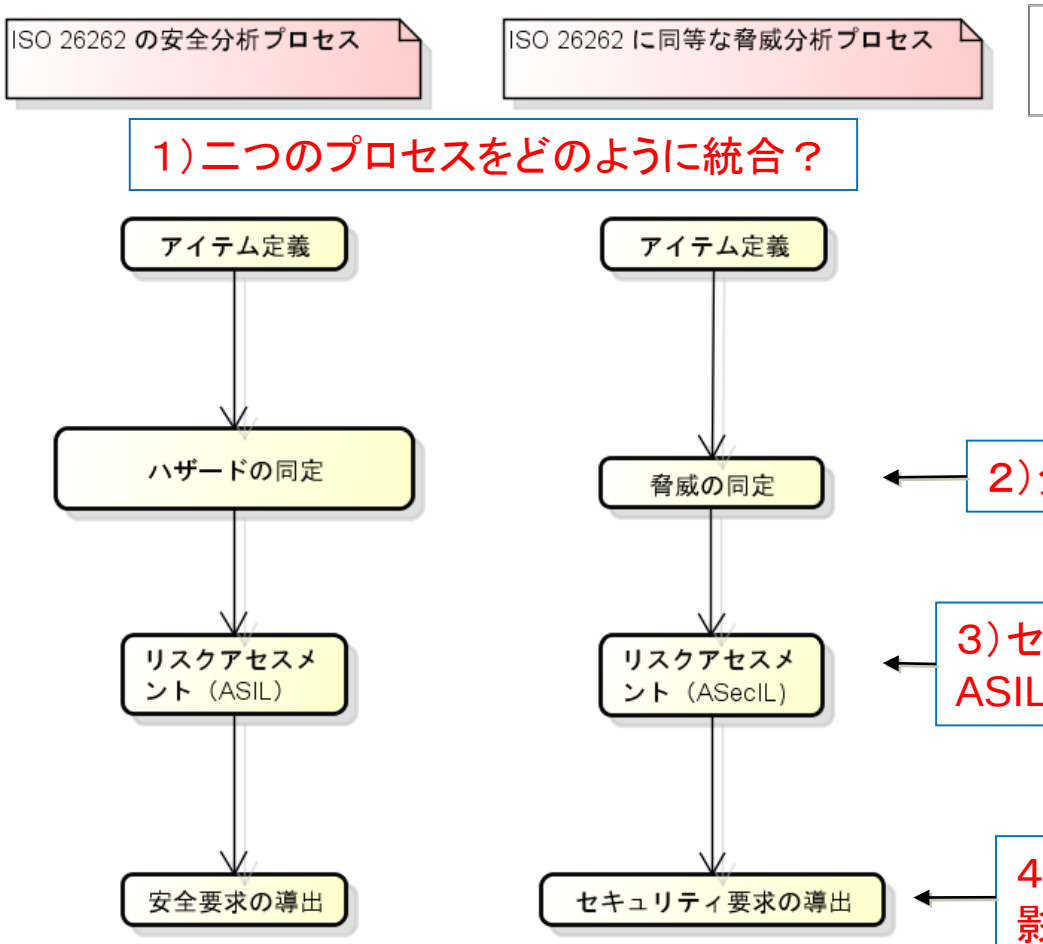


認証のための新たな枠組みが必要？

3. ライフサイクルの統合

3-1. 安全とセキュリティ開発プロセスから見た4つの課題

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



課題：
1）～4）までの技術的課題が存在する

1）二つのプロセスをどのように統合？

2）分析手法？どのように統合？

3）セキュリティ側のアセスメント基準は？
ASIL との関係は？

4）安全要求とセキュリティ要求の影響分析は？

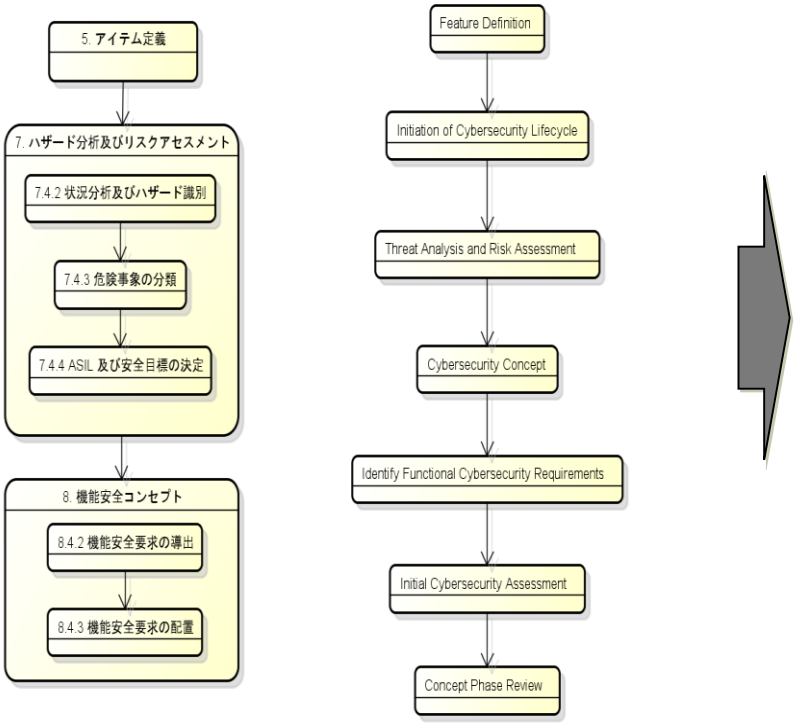
注：ASecIL (Automotive Security Integrity Level)

3-2. 悪い混ぜ方の例（ライフサイクルの統合例）?

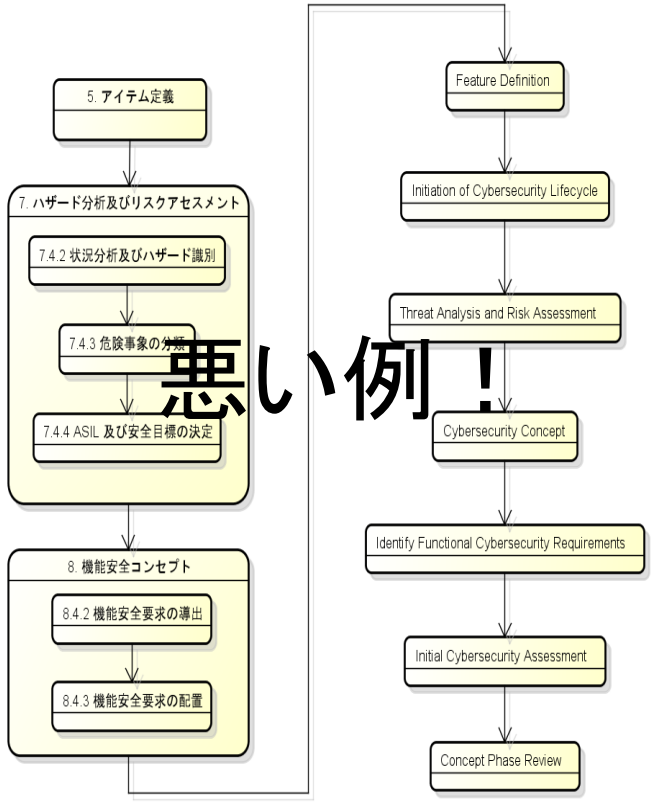
- 機能安全規格とセキュリティ規格におけるプロセス統合のまずい例（車載の例）

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（？）

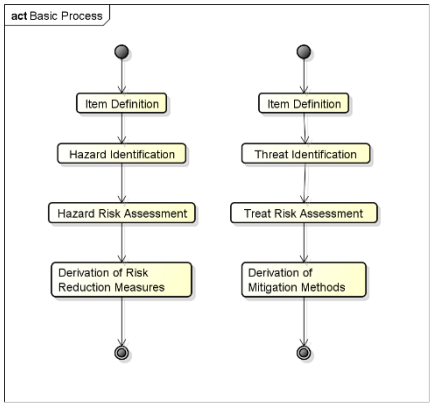


悪い例！

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

3-3. 安全とセキュリティのプロセス統合（分類）

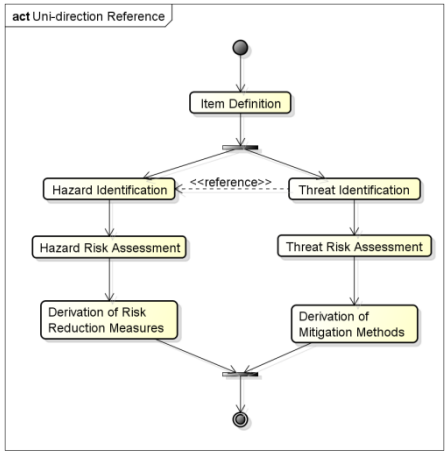
- セキュリティと安全の開発プロセスをどのように統合するかは、まだ解決されていない、大きな課題である。
- 様々な提案がされているが、どれもが決定的では無い。
- 研究プロジェクト、セキュリティ規格等の調査の結果、以下の基本形に分類可能。
- これらを基に、様々な組み合わせが、詳細レベルで可能。



個々に独立
（基本型）

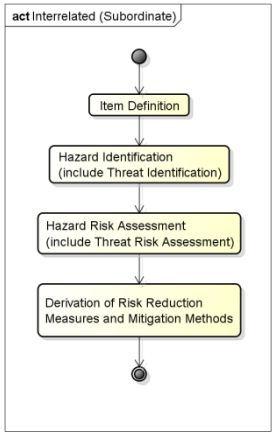
K. Taguchi, D. Souma, H. Nishihara: Safe & Sec Case Patterns, ASSURE 2015

安全側分析結果
をセキュリティが参照
（一方向参照型）



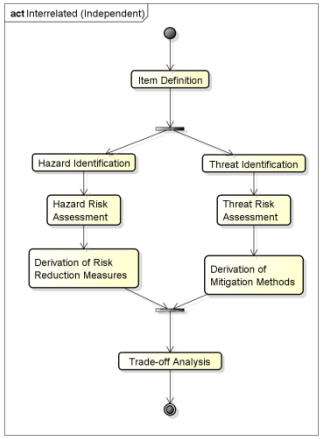
航空機セキュリティ規格（DO-326A）
を抽象化した形

安全側がセキュリティ
を包括（従属型）



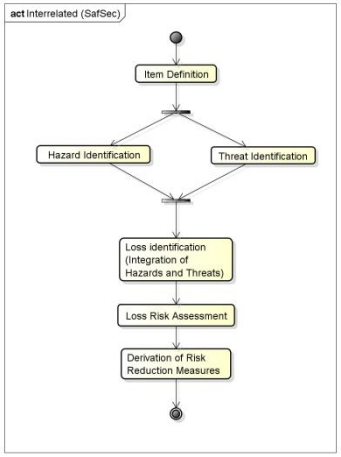
FTA が ATA
を含む分析方法

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

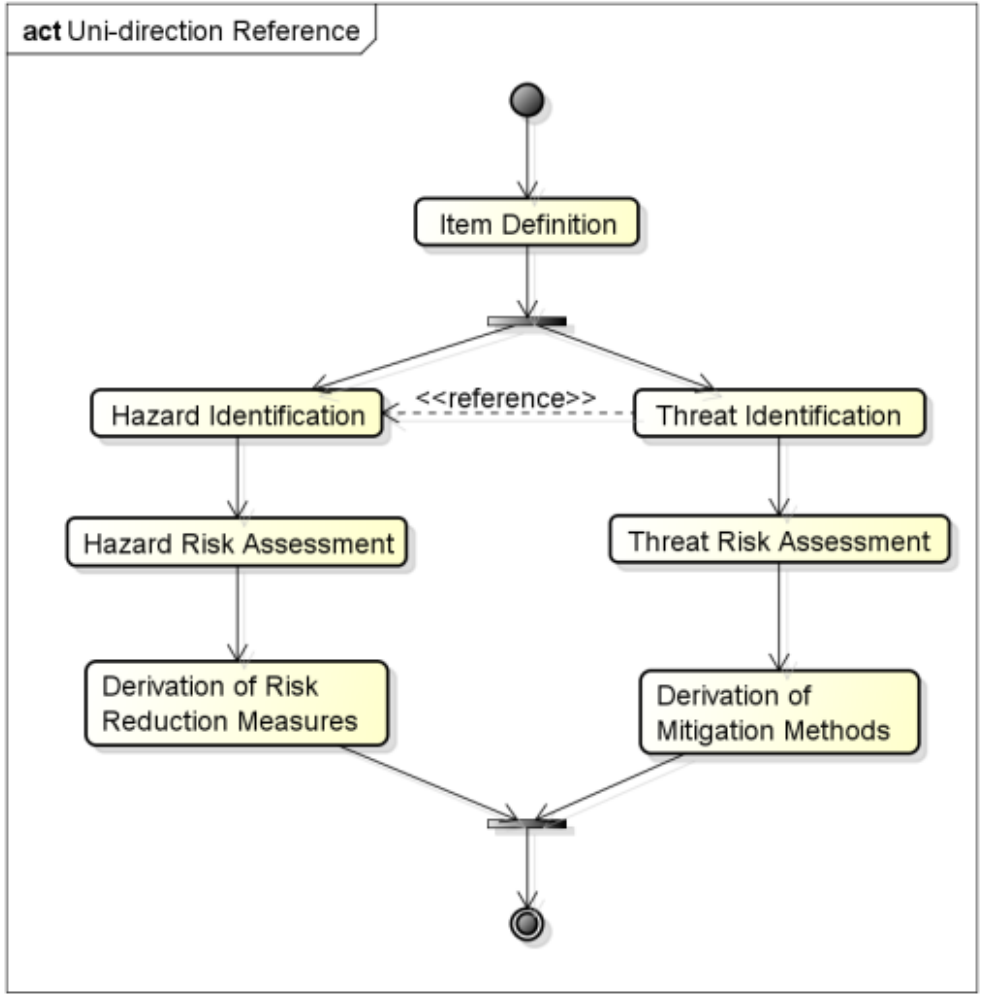
ロスとして統合
（SafSec型）



同時認証方法論 SafSec
におけるプロセスを抽象化
した形

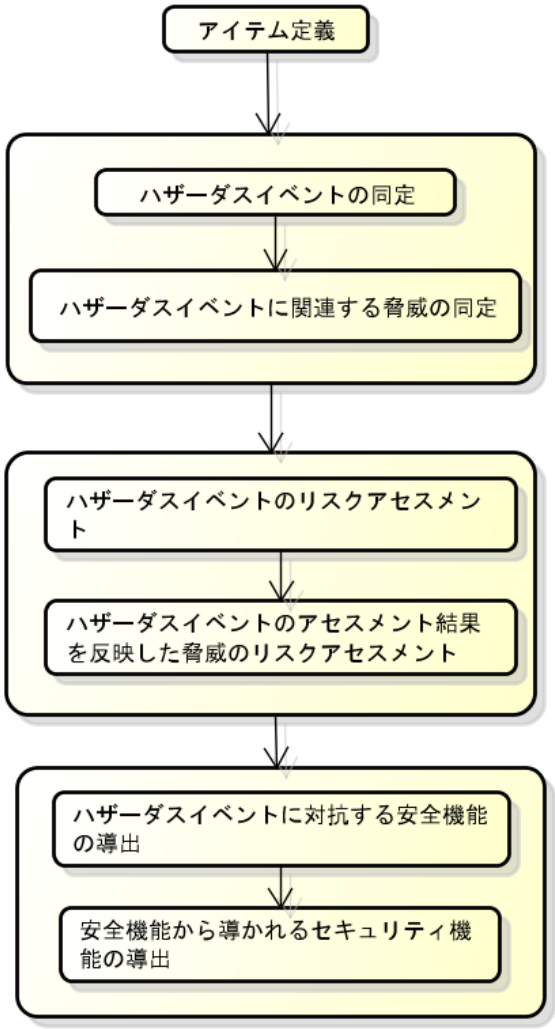
3-4. 一方向参照型

- 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。



3-5. 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

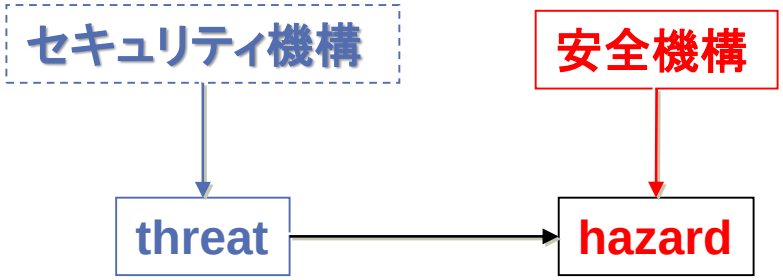
4）安全機能、セキュリティ機能導出の統合

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

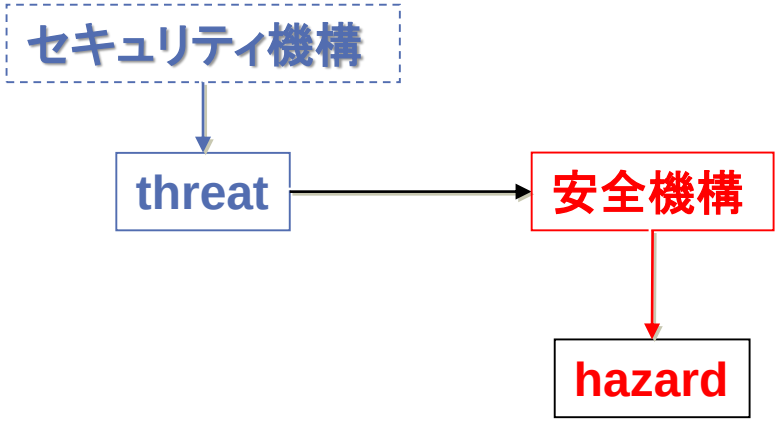
3-6. 様々な観点からの統合方法

- 安全側から見ると、セキュリティは安全機構を守るためのものと考えられる。

【基本形】



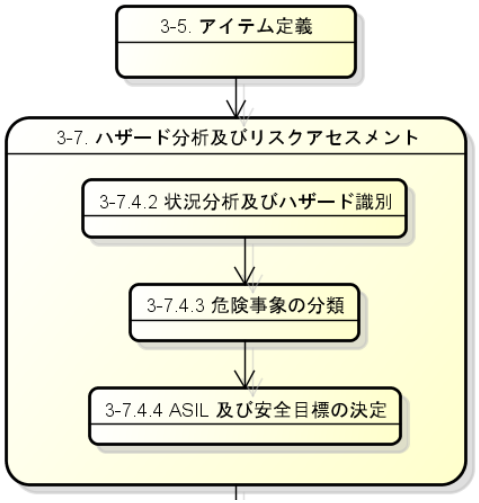
【安全機能に対する脅威に対してセキュリティ機構を設計する】



3-7. 基本形のプロセス

- **安全分析の後に同定されたハザードの起因となるセキュリティ上の脅威を分析する。**
  - 全てのハザードに対して、脅威が要因になる訳ではない。

機能安全側のプロセス

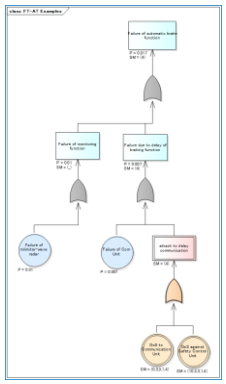


安全分析で同定されたハザード

ハザードリスト

セキュリティ側のプロセス

個々のハザードに対して脅威を分析



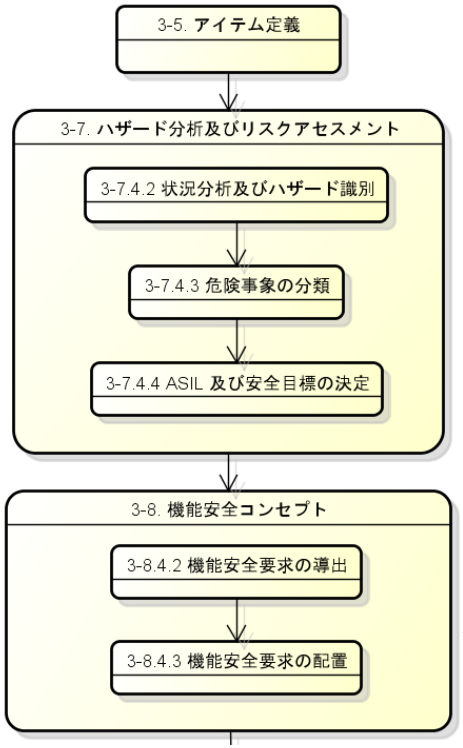
例：FT-AT図

同定された脅威に対してセキュリティ機構を導出

3-8. 安全機構のセキュリティ機構による保護

- **安全分析の後に同定されたハザードの起因となるセキュリティ上の脅威を分析する。**
  - 全てのハザードに対して、脅威が要因になる訳ではない。

機能安全側のプロセス

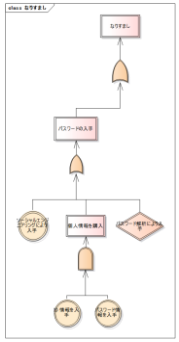


安全分析を基に導出された安全要求

安全要求

セキュリティ側のプロセス

安全要求に対する脅威を分析

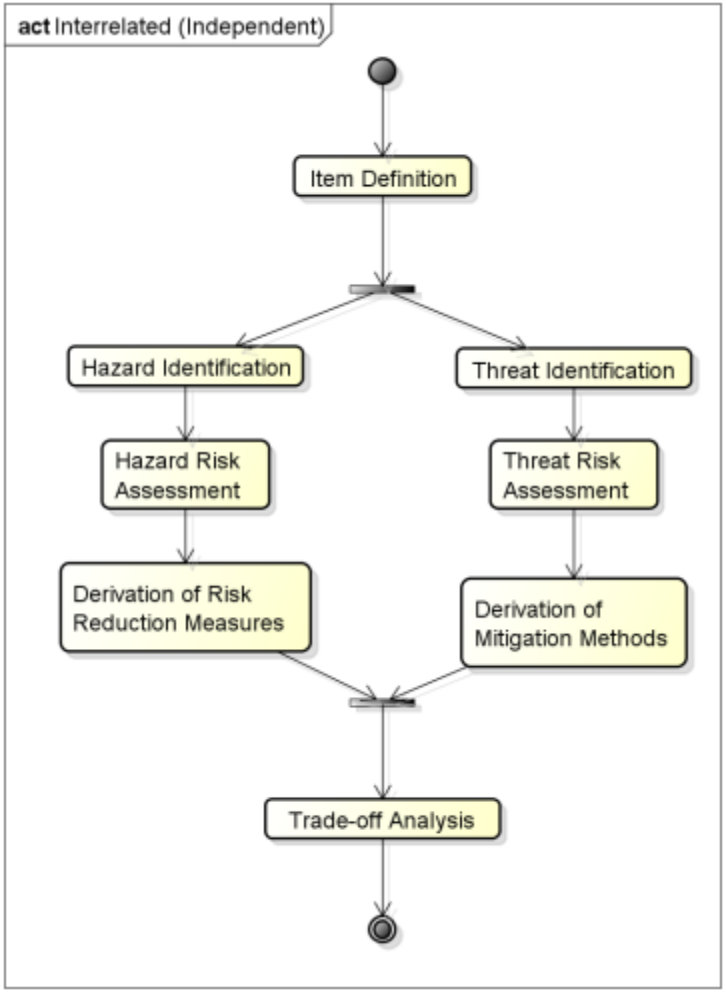


例：AT図

同定された脅威に対してセキュリティ機構を導出

3-9. 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。
- SESAMO プロジェクトにおけるトレードオフの考え方を導入。



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

3-10. プロセス統合についての今後の動向

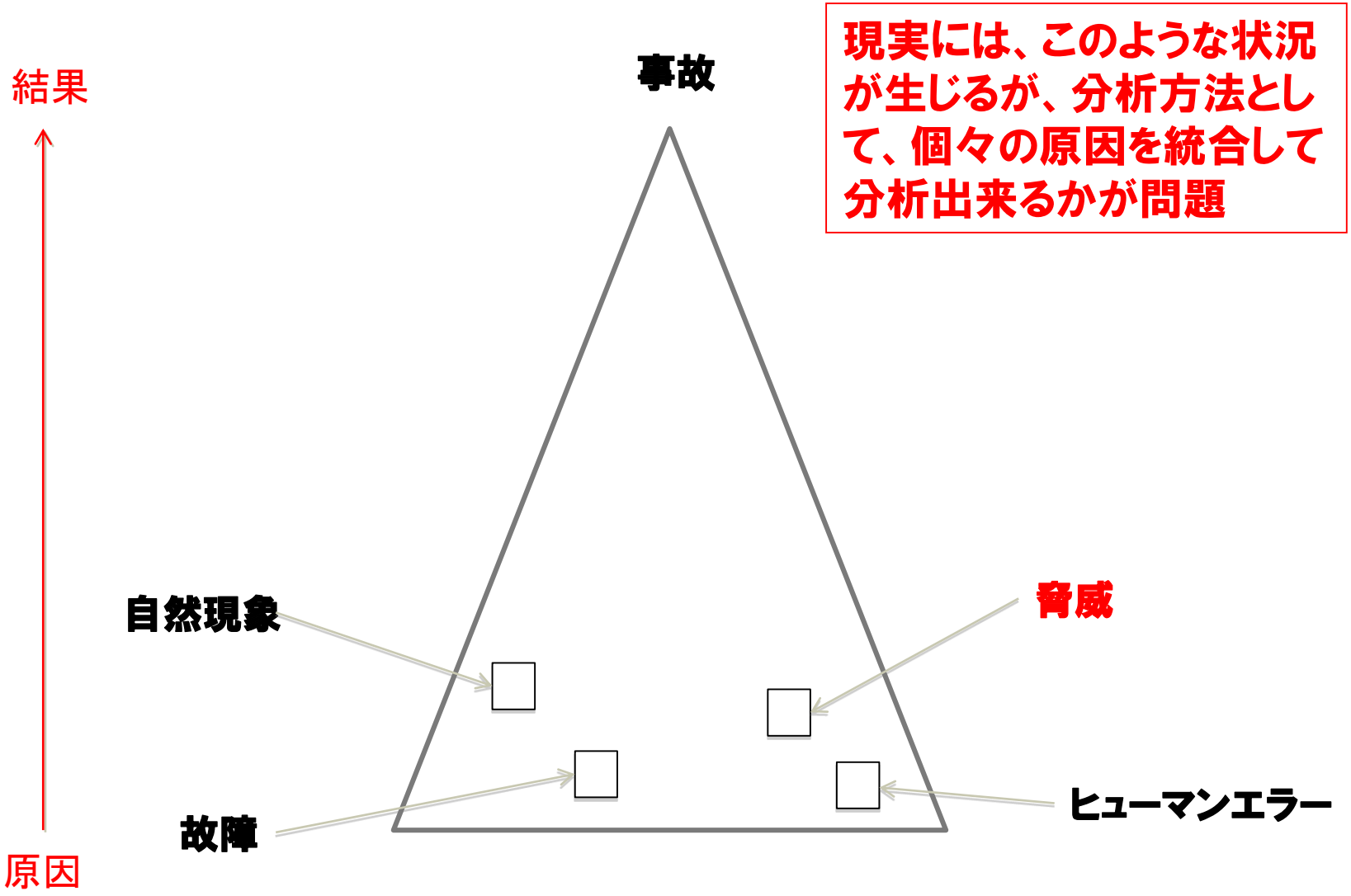
- **プロセスの統合については、様々な考え方があり、当面は、様々な観点から試行が行われることが予想される。**

- **統合の観点**
  - セーフティ中心
  - セーフティとセキュリティの調和指向

- **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

4. 分析手法

4-1. 事故原因の分析

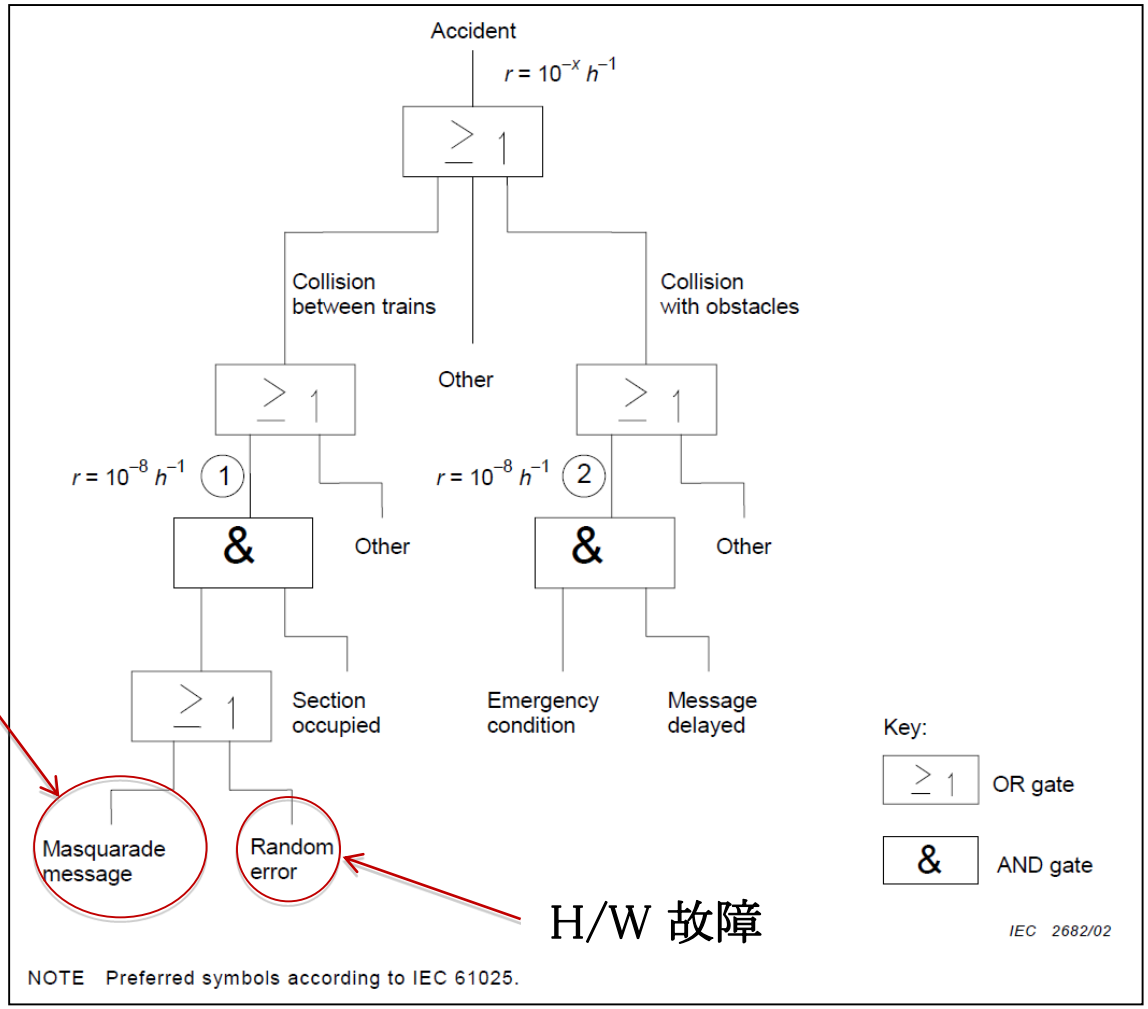


現実には、このような状況が生じるが、分析方法として、個々の原因を統合して分析出来るかが問題

4-2. 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



4-3. 攻撃木分析（ATTACK TREE ANALYSIS）

- **ATA（Attack Tree Analysis）は、B. Schneier [1] が発案されたと言われている。**
- **安全分析における分析手法である FTA (Fault Tree Analysis) をセキュリティの脅威分析に応用（ほぼ同一の構文規則）。**
- **攻撃の手段を抽象度の高い方から、より詳細な手段へと分解し、そのリスクの度合いを分析する手法（トップダウンの解析方法）。攻撃の組み合わせに何があるかを分析することが出来る。**
- **FTA と異なり、ATA の場合、どのようにリスクのアセスメントをするかは多くの提案があり、一般的に確立したものは無い。**
  - どのような評価要素を含めるかに所説あり（攻撃は確率事象では無いのは重要な点）。
- **AT図の様々なバリエーション。**
  - セキュリティ要求との組み合わせ（Attack Defense Trees や Attack Countermeasure Trees ）。
  - 新しいゲート（順序、並列、など）や木以外の表現形式（グラフ表現）。
- **FTA（[2]）と異なり、国際規格は存在しない。**
- **安全分析と脅威分析の統合のための FT と AT を統合した手法の提案がある。**

[1] B. Schneier: Attack trees: modeling security threats, Dr. Dobb's J 24 (1999) pp21-9.
[2] IEC 61025: 2006: Fault Tree Analysis

4-4. AT の種類

- **構造的拡張（木 vs グラフ）**
- **防御（対抗策もしくはセキュリティ要求）**
  - Attack Defense Trees [1]
  - Defense Trees [2]
  - Attack Countermeasure Trees [3]
- **安全との統合**
  - Fault Trees と Attack Trees との統合 [4, 5]

[1] B. Kordy, S. Mauw, S. Radomirovic, P. Schweitzer: Foundation of Attack-Defense Trees, FAST 2010, LNCS 6561, pp. 80-95, 2011, Springer.

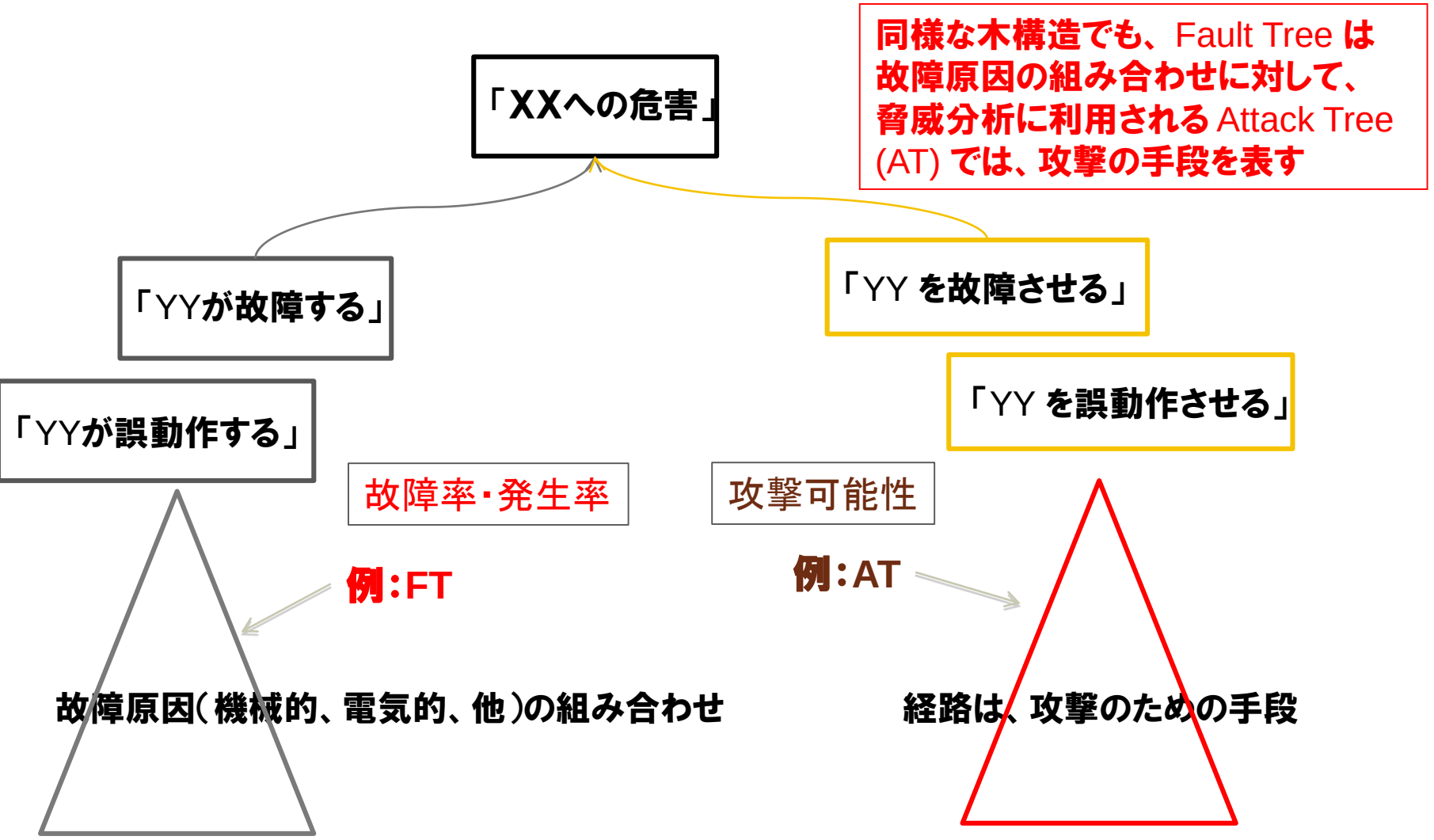
[2] K. Edge, U. Major: A Framework for Analyzing and Mitigating the Vulnerabilities of Complex Systems via Attack and Protection Trees, PhD thesis, 2007

[3] A. Roy, D. S. Kim, K. S. Trivedi: ACT: Towards unifying the constructs of attack and defense trees, Security and Communication Networks, 2011:3:1-15

[4] Steiner, M., Liggesmeyer, P.: Combination of Safety and Security Analysis – Finding Security Problems That Threaten The Safety of a System. In: Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) (2013)

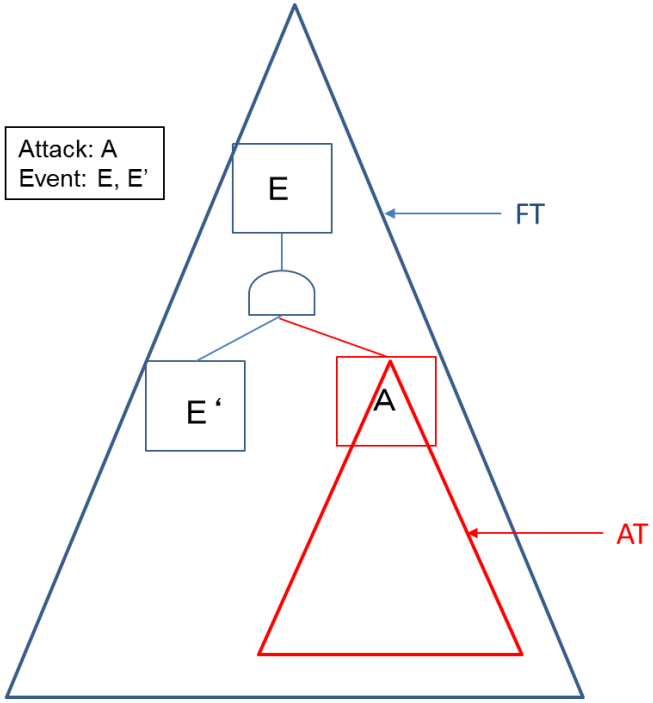
[5] I. N. Fovino, M. Masera, A. D. Cian: Integrating cyber attacks within fault trees, J. Reliability Engineering and System Safety, 94 (2009) 1394-1402

4-5. 安全性とセキュリティの分析の特徴

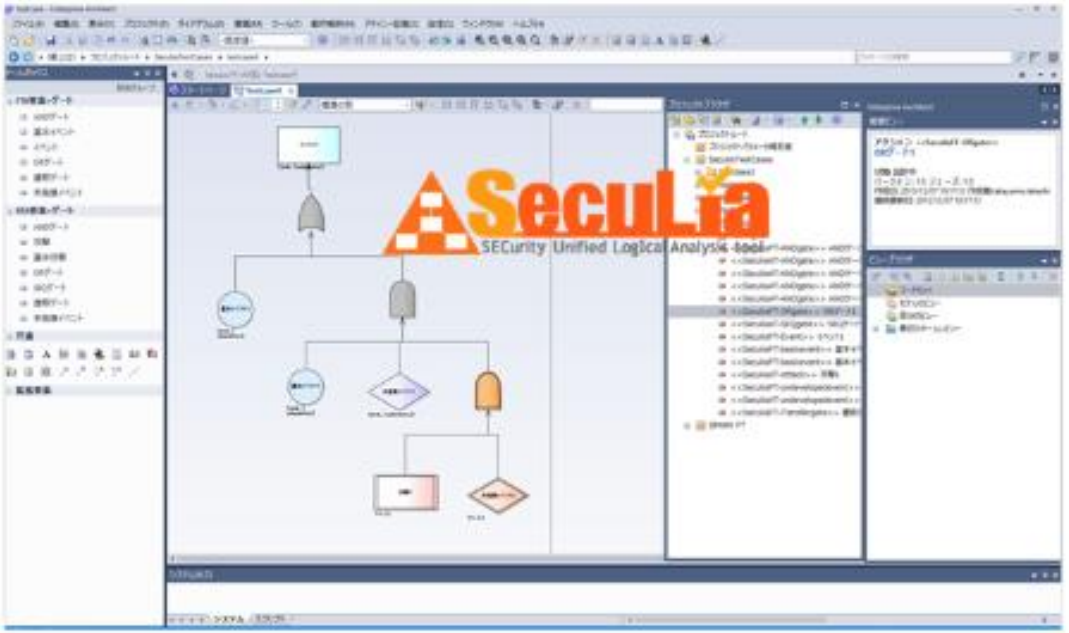


4-6. 安全とセキュリティの統合分析手法：FT-AT図

- 安全性を脅かすセキュリティ上の脅威を分析する手法として、FTA と ATA を統合する方法が提案されている。
- 基本的には、故障の原因として、セキュリティ上の脅威を含んだ分析が可能となる。
- FT の一部として AT が現れるとは、ゲート記号の下に、AT が現れる形を意味する。
  - ただし、AT の中に FT は決して現れない。
  - FT の中に AT が複数現れることは許される。
- これは、意味論的には、攻撃の手段、原因がハードウェア故障やソフトウェアのバグが原因であることは定義上あり得ないことに由来する
  - 人為的な手段によるもののみを攻撃と呼ぶことに起因する。
- 本図表現を FT-AT図を呼ぶことにする。



SECULIA



- **SecuLia は弊社とガイオ・テクノロジー社との共同で開発された脅威分析ツール**
  - Enterprise Architect（Sparx Systems 社）のプラグインとして提供
- **機能**
  - FT 分析
  - AT 分析
    - ✓ CC-CEM と EVITA に基づいたアセスメント計算
    - ✓ アタックシナリオ（最少カット集合）とそのアセスメント計算
- **FT-AT 分析**
  - FT分析とAT分析を統合

5. リスク分析

5-1. セキュリティにおけるリスクアセスメント方式

- **様々なシステム特性に応じて、リスクアセスメントのためのメトリックスが開発されている**
  - ソフトウェアの脆弱性に関するリスクアセスメント方式
    - ✓CVSS (Common Vulnerability Scoring System)
  - CC認証において利用
    - ✓CC/CEM
- **特定のドメインに特化するために、変更（主に簡略化）して利用される場合もある**
  - 自動車（J-SAE, JASO TP15002: 自動車 – 情報セキュリティ分析ガイド)
    - ✓CVSS -> CRSS（CVSS based Risk Scoring System)
    - ✓ISO/IEC 27000 と CC/CEM -> RSMA (Risk Scoring Methodology for Automotive Systems)

5-2. CC/CEM

- 以下の評価要素が用いられている。
- 所要時間
  - Elapsed Time (ET)
- 専門知識
  - Expertise (Ex)
- TOE の知識
  - Knowledge of system (K)
- 機会
  - Window of opportunity (W)
- 機器
  - Equipment (Eq)

要因(Factor)		評価値(Value)
経過時間	≦1日	0
	≦1週	1
	≦2週	2
	≦1月	4
	≦2月	7
	≦3月	10
	≦4月	13
	≦5月	15
	≦6月	17
	＞6月	19
経験的知識	一般人(Layman)	0
	熟練者(Proficient)	3 *(1)
	専門家(Expert)	6
	複数の専門家(Multiple exerts)	8
システムへの知識	公知(Public)	0
	制限(Restricted)	3
	要注意(Sensitive)	7
	機密(Critical)	11
機会の時間枠	不必要/制限無きアクセス (Unnecessary/unlimited access)	0
	容易(Easy)	1
	適度(Moderate)	4
	困難(Difficult)	12
	無し(None)	** (2)
装置	標準(Standard)	0
	特殊化(Specialized)	4 (3)
	特注品(Bespoke)	7
	複数の特注品(Multiple bespoke)	9

5-3. 攻撃確率（ATTACK PROBABILITY)

- 各攻撃イベントは、5つのパラメータを持つ。これを（ET, Ex, K, W, Eq) と表す、これらの値を加算したものが、下記の表の値になる。
- Values（総和）= ET + Ex + K + W + Eq
- EVITA では、これらの総和（Values）により、攻撃確率を 1 から 5 までの段階で分割している。

総和（Values）	潜在的攻撃力（Attack Potential）	攻撃確率（Attack Probability） AP
0－9	基本（Basic）	5
10－13	拡張基本（Enhanced Basic）	4
14－19	中間（Moderate）	3
20－24	高い（High）	2
≧ 25	高を超える（Beyond High）	1

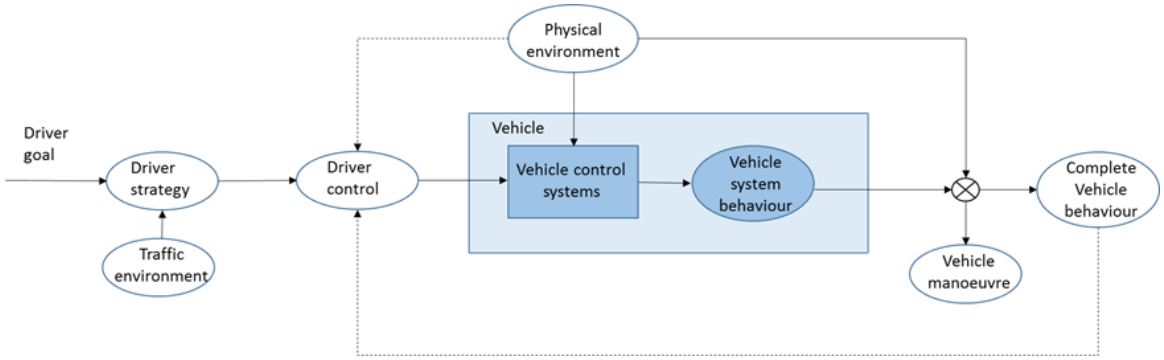
5-4. ASIL

- **ISO 26262 においては、ASIL (Automotive Safety Integrity Level) と呼ばれるインテグリティ・レベルが規定されており、以下の3つの因子によりリスクのアセスメントを行う。**
  - 深刻度（Severity）
    - ✓ estimate of the extent of harm (1.56) to one or more individuals that can occur in a potentially hazardous(1.57) situation
  - 発生頻度（Provability of Exposure）
    - ✓ state of being in an operational situation (1.83) that can be hazardous (1.57) if coincident with the failure mode (1.40) under analysis
  - 回避可能性（Controllability）
    - ✓ ability to avoid a specified harm (1.56) or damage through the timely reactions of the persons involved, possibly with support from external measures (1.38)

5-5. リスクアセスメント：セキュリティから安全への影響

- **回避可能性（Controllability）は MISRA の安全ガイドラインにより規定されたものであり、Driver in the loop という制御モデルに基づいている。**

（[2] p41, Figure 4.5: “Driver in the loop” model of vehicle control systems 引用）



攻撃

- **例えば、操舵、ブレーキ、アクセル等、ドライバーが自動車の操作に利用可能な機能に対して、攻撃された場合、当然、リスクの評価値が変わることになる。**

5-6. ATA におけるリスクアセスメント方式

- **アセスメント方式において重要な点（一般論）**
  - どのようなリスクを評価するかにより、メトリックス（表現としてのマトリックス）は異なる。
- **アセスメント計算のための二つの重要な要素**
  - 各攻撃ノード（基本的には、基本攻撃イベント）への評価値
  - ゲートの計算
  - AT木の階層構造（異なる意味付けをする場合：例 EVITA）
- **ここでは、EVITA [1] の方式を紹介する。**

[1] Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios, 2008

5-7. EVITA プロジェクトとは？

- **EVITA (E-safety Vehicle Intrusion proTected Application) [1] はヨーロッパのFP7 により支援された、自動車の車内ネットワークに関連するコンポーネントと機密データが、セキュリティ上の脅威から保護される、プロトタイプアーキテクチャの設計、検証のための研究プロジェクト。**

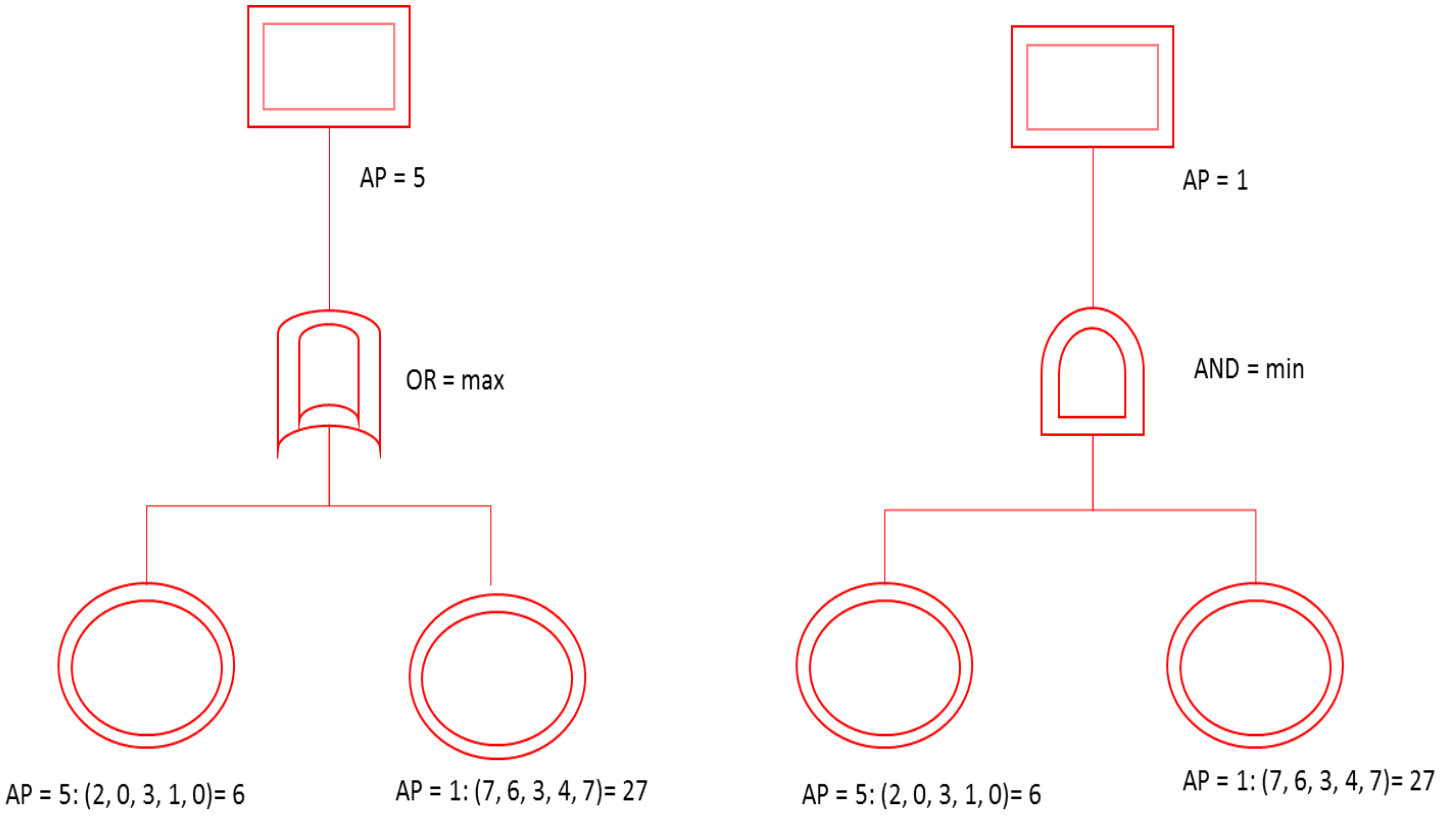
- **EVITA の結果の一つは、AT を用いて、非常に詳細なセキュリティ分析を実施し、それに基づいてセキュリティ機能の導出を行った。**

- **AT のセキュリティメトリックスは Common Criteria (CC)（ISO 15408）の CEM の若干の修正版が用いられている。**
  - CC-CEM は、CC における脆弱性評価のための基準 [2]。

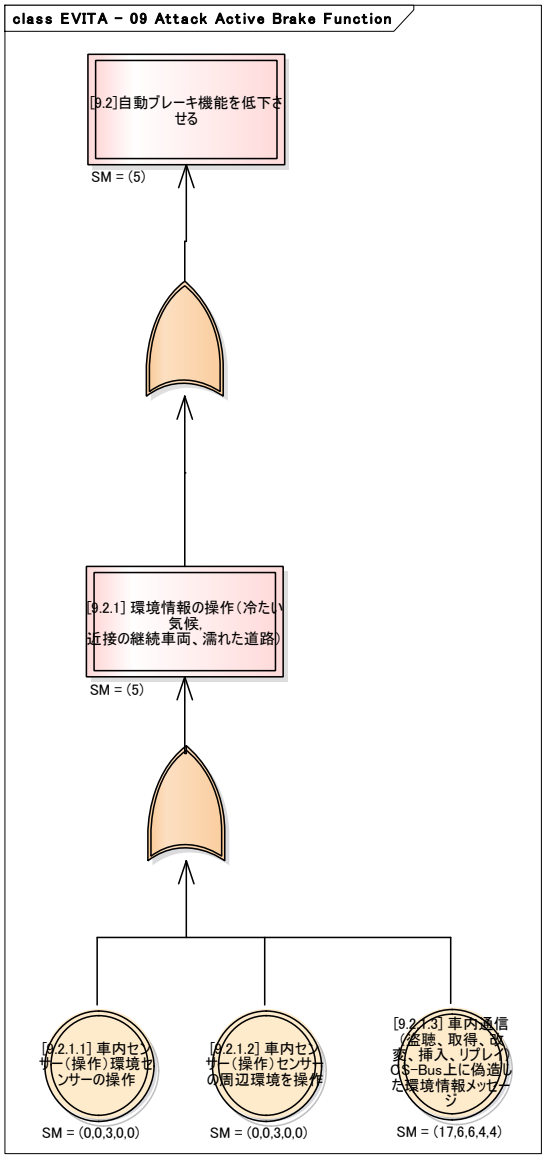
[1] http://evita-project.org/
[2] 情報技術セキュリティ評価のための共通方法　評価方式 2012年9月 バージョン3.1 改訂第4版、CCMB-2012-09-004（Common Methodology for Information Technology Security Evaluation の日本語版）

5-8. EVITA 流 AT アセスメント例

- **ゲートの計算**
  - ORゲートは max
  - ANDゲートは min
- **下図における基本アタックイベントの書式の意味**
  - AP = 攻撃確率 : (ET, Ex, K, W, Eq) = 総和



5-9. アクティブブレーキ機能への攻撃(2)



- **「自動ブレーキ機能を低下させる」攻撃**
  - 環境に関する情報を操作する場合
    - ✓環境に関するセンサーを操作
    - ✓車内通信において盗聴、取得、改変、挿入、リプレイにより、環境に関する偽造した情報を流す

5-10. FT-AT図におけるリスクアセスメント

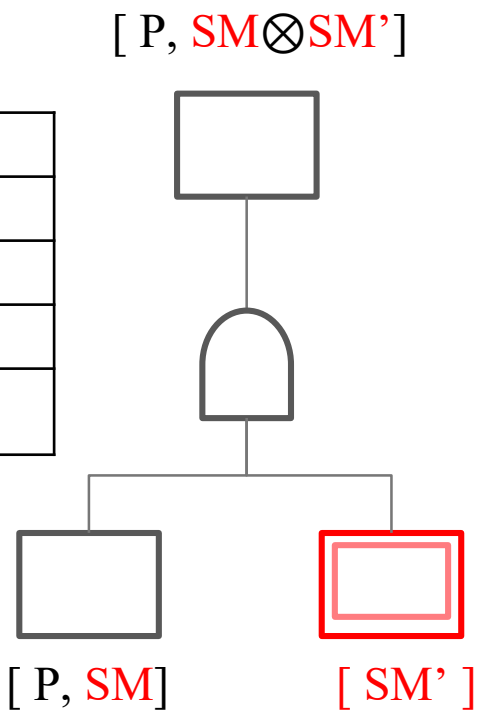
- **安全側（FTA）とセキュリティ側（ATA）では、リスクのアセスメントメトリックスが異なる。**
  - FTA（故障確率）
  - ATA（攻撃確率）
- **原理上は安全性とセキュリティは相互に影響があるが、まだメトリックス上でそれをどのように表現し、影響を計算するかについては明確では無い。**
- **このような理由から、FT-AT図においては以下のように、故障イベントにおいて、安全側とセキュリティ側の両方を値を取れるように工夫がされている。**

ノードと値	説明
Event [P, _]	故障イベント E において故障率 P のみを保持する場合
Attack (AP)	攻撃イベントAttack の攻撃確率
Event [P, AP]	故障イベント Event が故障率 P と攻撃確率 AP を保持する場合

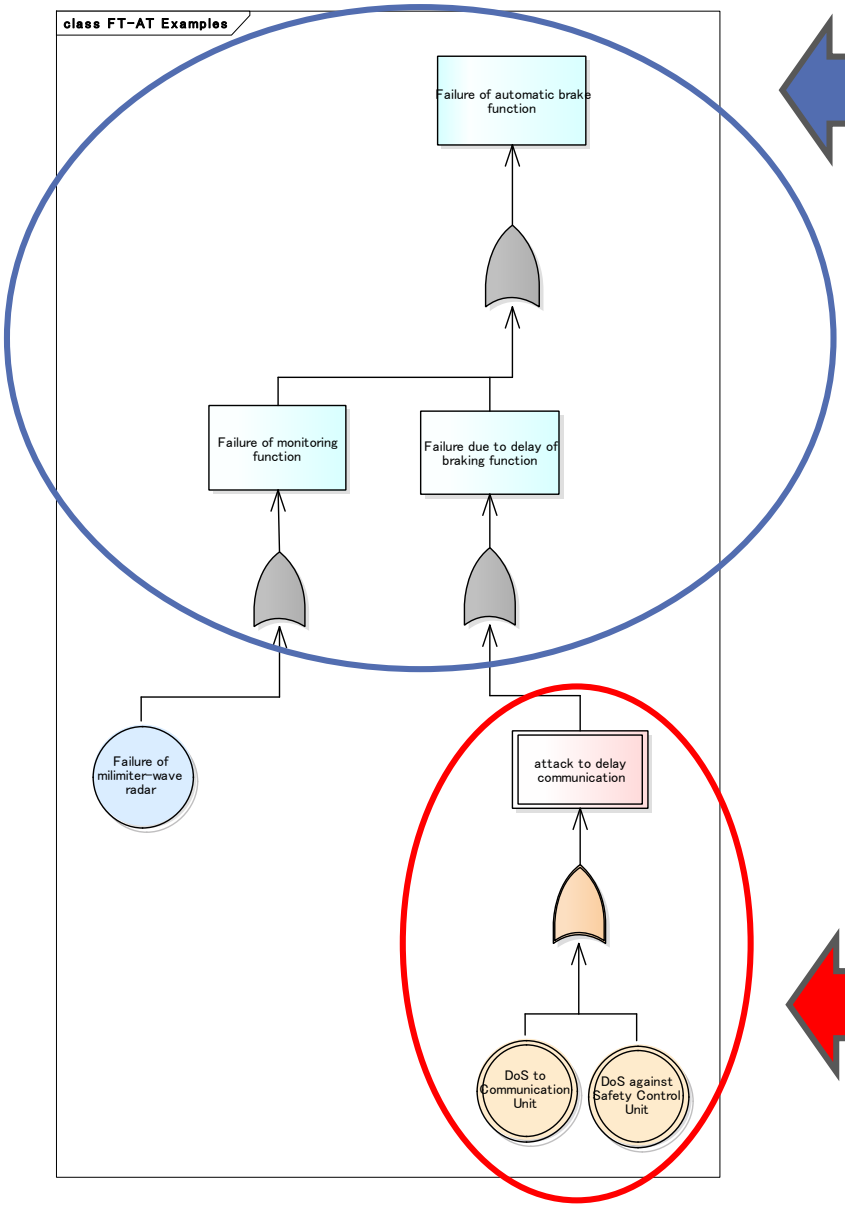
5-11. FT-AT図におけるアセスメント計算

- FT図において、AT図が連結された場合のアセスメント計算の方式
- ここで F-AND は FT図における AND ゲートを表している（ここでは AND ゲートの計算のみを説明）。
- AT 側の演算子 ⊗ は、AT側の AND-ゲートの演算子を表している（例えば、EVITA 流では min）

イベント　ゲート	計算方式
[P, _] F-AND [P’, _]	[P * P’, _]
[P, _] F-AND [_, SM]	[P, SM]
[P, SM] F-AND [_, SM’]	[P , SM ⊗ SM’]
[P, SM] F-AND [P’, SM’]	[P * P’, SM ⊗ SM’]



5-12. 事例（1）



この部分が FT

- **FT-AT 図は FT の機能と AT の機能を統合した機能を提供。**
- **FT-AT は FT と AT の統合をある限定した構文規則の中で実施。**
  - AT は FT の部分木として表れる。
  - AT は FT の任意の場所に部分木として表れることが出来る。
  - ただし、故障事象は、AT に含まれてはならない。
  - FT は AT の部分木として含まれてはならない。

この部分が AT

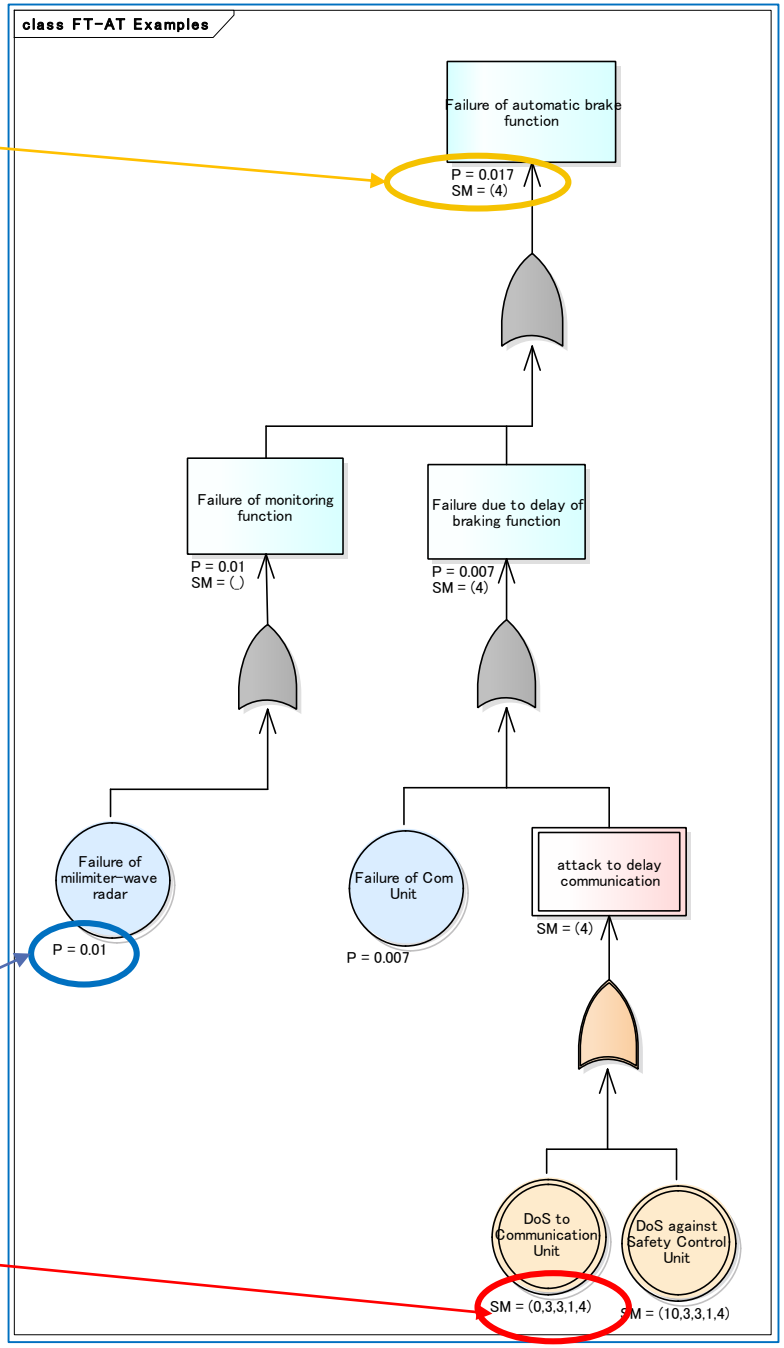
5-13. 事例(2)

- この FT-AT 図で示されているのは、FTA における確率計算と ATA における攻撃確率計算が同時に行われている点である。
- この例で示されているのは、“Failure of automatic braking function” は 0.017 の故障の確率を持ち、攻撃確率は 4 であることである。

(確率,攻撃確率)

確率

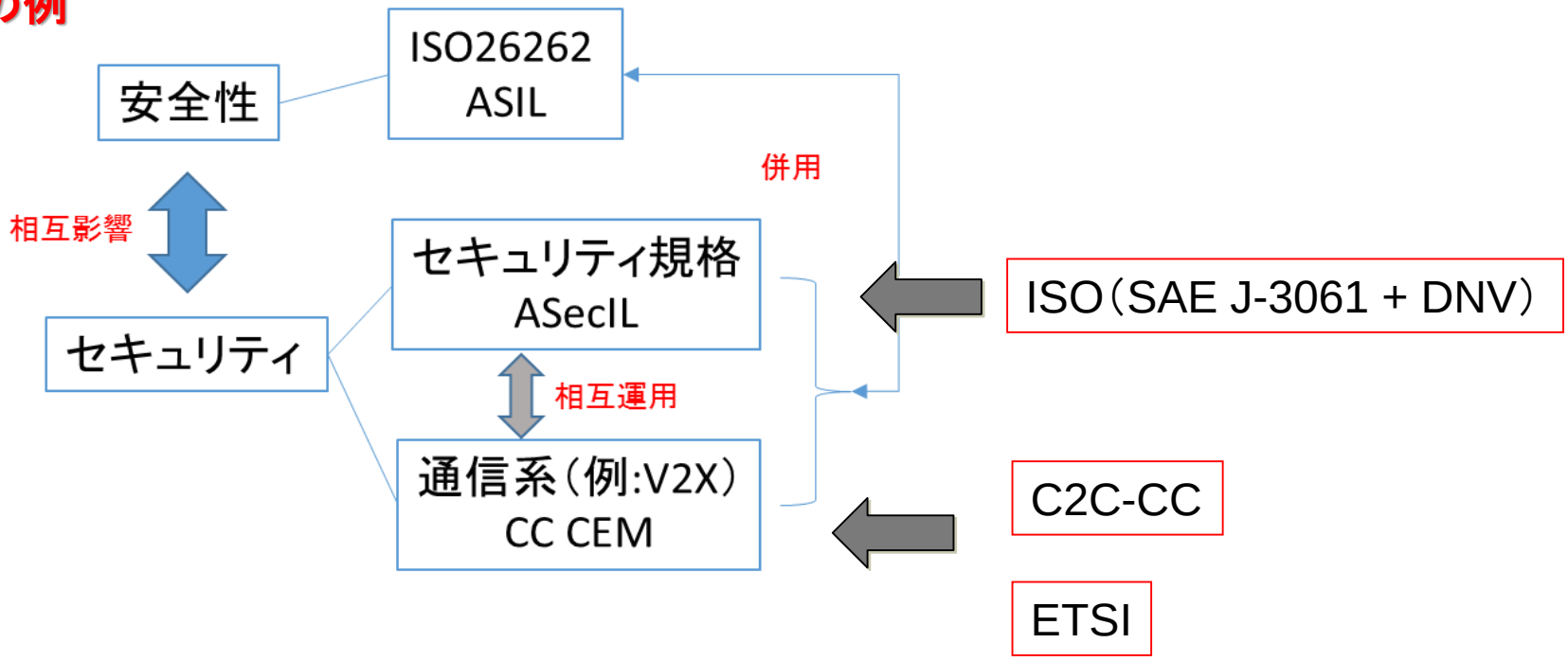
攻撃確率



5-14. アセスメント方式の混在（車載の場合）

- 自動車産業においては、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（Security Integrity Level）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。
- そのような場合に、どのように、相互を利用して行くかは今後の課題である。

車載の例



ASecIL (Automotive Security Integrity Level)

おわりに

- 現在、safety and security co-engineering という名称で、様々な研究成果が出始めている。今後、安全とセキュリティの相関関係の解明や、新しい分析手法、設計方式などが出てくる可能性が高い。

- 今後、3~10年
  - セキュリティとセーフティの相互関連の理解の深まり
  - 統合プロセス（様々な形で実施）の確立
  - 統合的な分析手法の開発
  - ガイドライン、規格の整理
  - 実際に双方を考慮した製品の開発

- ビジネスチャンス？
  - ポジティブな見方
    - 品質向上、新機能の開発の好機
  - ネガティブな見方
    - 従来のプロセスや開発手法に対する悪影響
    - コスト拡大要因