SCN-OC 2019

セキュリティ分野へのSCDL適用事例

Security First

CAV Technologies

（株）シーエーブイテクノロジーズ

2019年10月30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)
- 非常勤講師　京都大学、慶応大学、名古屋工業大学(ICSCoE)
- **招聘研究員**　**中国科学院合肥物質科学研究所**

【最近の講演】

- Autosec China: Mission Possible: Advanced Threat Analysis Tool for All", Shanghai, China, 2019
- WESPr: Safety and Security Co-engineering – A new emerging discipline for safe and secure system development –, International Workshop on Evidence-based Security and Privacy in the Wild, 2018

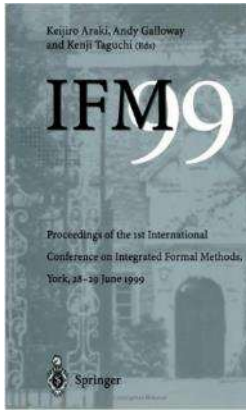
【専門分野】

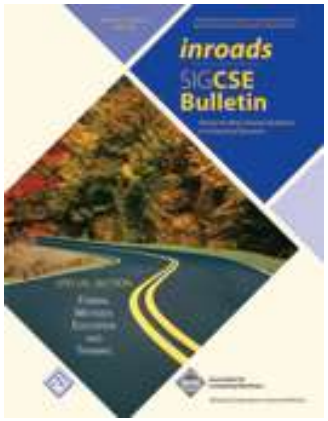
- 高信頼システム開発方法論(形式検証、国際規格認証、システム保証、安全・セキュリティ分析方法論)
- 安全工学、システムアシュアランス、形式手法、ソフトウェア工学に関する、多くの主要な国際会議の PC等 を歴任(RSSRail '19, SAFECOMP '19, '20、FMTea'19)

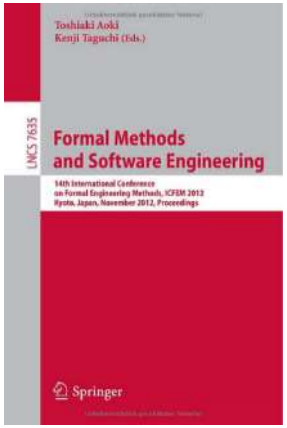
【規格、国際会議関連】

- International Conference on Formal Engineering Methods 2012 program co-chair(終了)
- SICE 認証工学 WG 主査 (終了)
- FP7 OPENCOSS プロジェクトの External Advisory Board Member (終了)
- JASPAR 機能安全ワーキング　安全論証開発グループ (2016年度) (終了)
- IEC TC65/WG 20 (Framework to bridge the requirements for safety and security) Expert (終了)
- International Workshop on Assurance Cases for Software-intensive Systems (2017) Program co-chair (終了)
- OMG System Assurance Platform Task Force co-chair(終了)
- **QA4AI (AI プロダクト品質保証コンソーシアム)メンバー**
- **Formal Methods Europe Education sub-committee member**

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

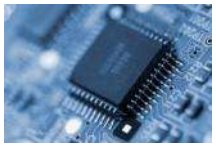
ACM SIGCSE, inRoads Bulletin, 2009年。共同編者
(Special Issue on Formal Methods Education and Training)

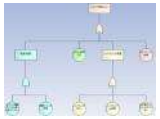
セキュリティ要求工学の実効性、情報処理学会学会誌 2009年。共同編者

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

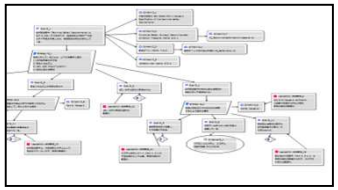
弊社のご提供する主要技術

- C(認証)
  - 様々な産業分野（電子機器、車載組み込み、鉄道、航空、医療機器）における機能安全やセキュリティに関する認証支援
    - ✓IEC 61508
    - ✓ISO 26262/J3061
    - ✓EN 50128
    - ✓DO-178C, DO-326A
- A(保証)
  - システム（AIシステムを含む）の安全性、セキュリティなどのシステム保証（論証）、第三者検証に関する技術支援
    - ✓安全分析・セキュリティ脅威分析
    - ✓セーフティー／サイバーセキュリティケースの作成、保守
    - ✓高信頼性システム開発技術
    - ✓第三者検証（IV&V）
- V(検証)
  - 形式手法（モデル検査、形式仕様記述）を用いた、システム検証技術支援
    - ✓形式手法技術導入支援
    - ✓形式手法を用いた開発、システム検証
    - ✓システム認証に必要な検証技術の導入支援





Attack Tree



GSN

モデル検査（SPIN, PAT）

形式仕様（VDM, Z）

SCDL セキュリティSWG

- SCDL（Safety Concept Description Language）のセキュリティ応用を目指して発足した SWG。
- 産業界、学界など様々なメンバーにより構成されている。

所属名	氏名
(株)アドヴィックス	河野　文昭
(株)アトリエ	水口　大知
おがたコンサルティング	緒方　健
オムロン(株)	廣部　直樹
ガイオ・テクノロジー(株)	小野　嘉翔
ガイオ・テクノロジー(株)	田中　伸明
ガイオ・テクノロジー(株)	光山　栄太
カルソニックカンセイ(株)	佐々木　喜好
(株)構造計画研究所	太田　洋二郎
(株)構造計画研究所	市村　健太朗
産業技術総合研究所	寶木　和夫
産業技術総合研究所	三科　雄介
シーエーブイテクノロジーズ(株)	田口　研治
スズキ(株)	村松　稔久
仙台高等専門学校	岡本　圭史
(株)チェンジビジョン	岩永　寿来
DNV GLビジネス・アシュアランス・ジャパン(株)	平野　薫
DNV GLビジネス・アシュアランス・ジャパン(株)	松並　勝
DNV GLビジネス・アシュアランス・ジャパン(株)	山下　修平
(株)デンソー	東道　徹也
日本自動車研究所(JARI)	伊藤　寛
日本自動車研究所(JARI)	福田　和良
日本大学	松野　裕
ベクター・ジャパン(株)	中村　伸彦
三菱電機(株)	友永　一生

本発表は、本SWGでの検討結果を基にしていますが、発表内容については発表者の独自見解が含まれていることをここに明記します。

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？

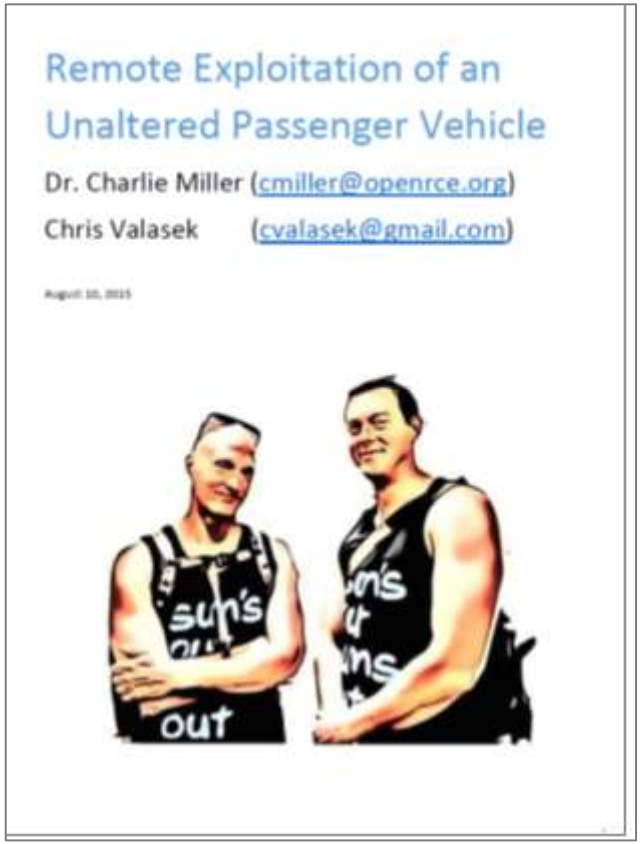
もしかしてハッキング？

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。

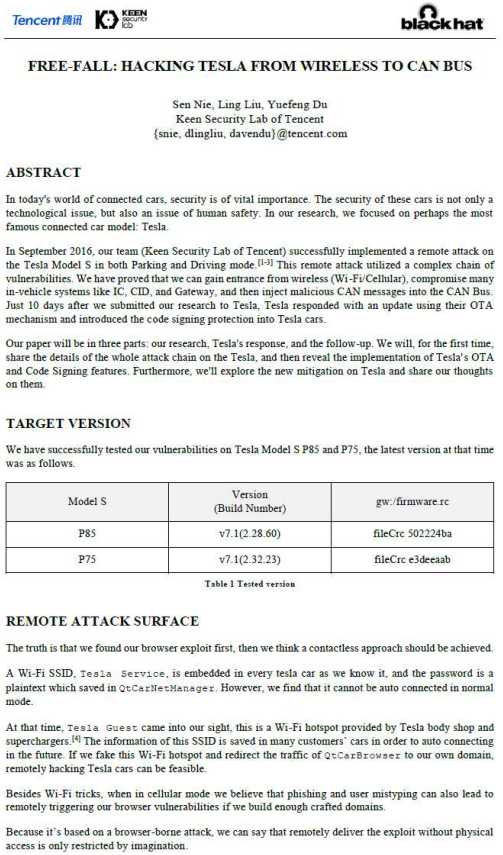
- **セキュリティ上の脅威 vs 安全のためのメカニズム**
  - Diagnostic session に遷移するのは低速時だけ、という安全機構である程度、防御されていた。



（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

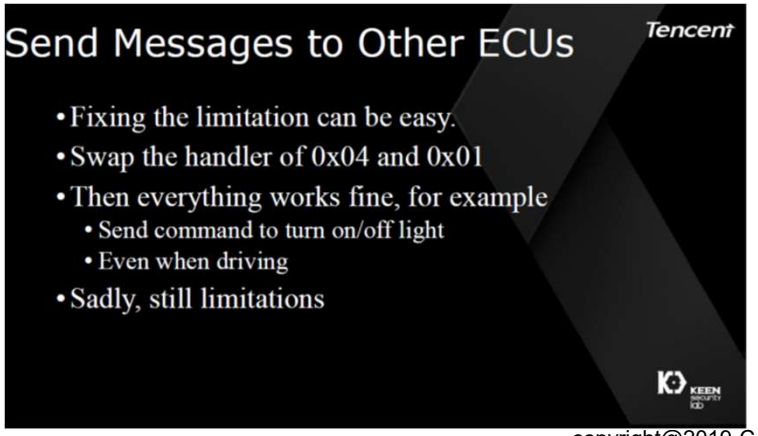
The truth is that we found our browser exploit first, then we think a contactless approach should be achieved.

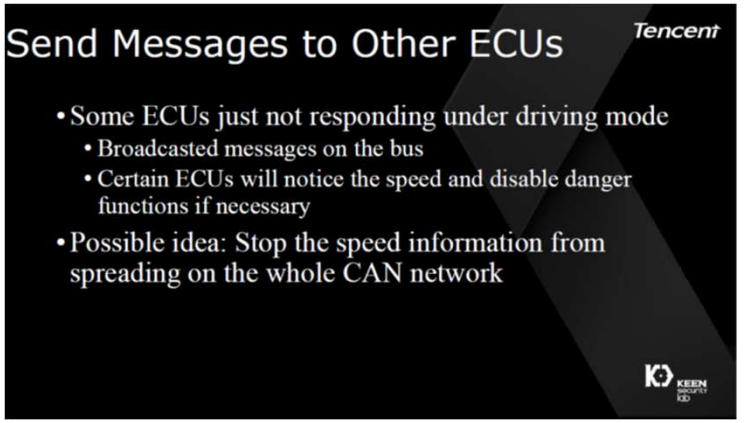
A Wi-Fi SSID, `Tesla Service`, is embedded in every tesla car as we know it, and the password is a plaintext which saved in `QtCarNetManager`. However, we find that it cannot be auto connected in normal mode.

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.





質問（1）

- **C. Miller と Chris Valasek による Jeep Chelokee に対するハッキングと、tencent による Tesla Model S へのハッキングにおいて、セキュリティ上の攻撃が安全機構により防御されていました。その点については、合意頂けますでしょうか？**

- **同様な例をご存知でしょうか？**

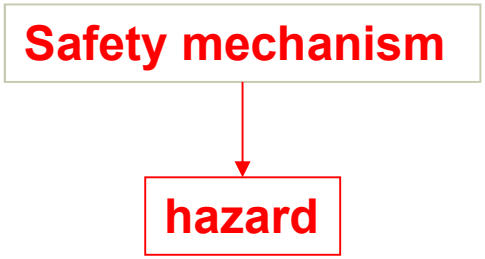
BASIC CONCEPTS RELATED TO SAFETY

- **Safety related concepts such as hazard, accident, risk, failure have different definitions and understanding in industries and countries.**

- **Definitions (from ISO 26262)**
  - Hazard
    - ✓ potential source of harm caused by malfunctioning behaviour of the item
  - Safety mechanism
    - ✓ technical solution implemented by E/E functions or elements, or by other technologies, to detect faults or control failures in order to achieve or maintain a safe state.
    - ✓ Remark: Safety mechanism includes simple monitor-arbitration logic to more complex fault tolerant/redundancy mechanisms

Examples of hazard:
1) Overheat of battery charging device causes its explosion and/or make burns.
2) ECU produces unintended assist torque.

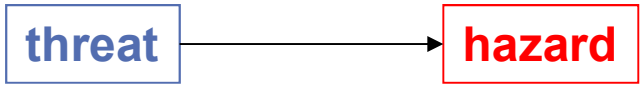
The following simplified figure is used to represent safety mechanism against hazard.



THREAT AND HAZARD: HOW DO THEY INTERACT EACH OTHER?

- **There is no clear and definitive definition on how threat and hazard are related each other.**
- **Definitions (from J3061)**
  - Threat
    - ✓ A circumstance or event with the potential to cause harm, where harm may be with respect to financial, reputation, privacy, safety, or operational.
- **We take that a hazard may be caused by threat as a working assumption.**

That a threat causes a hazard relationship



Hazard: Overheat of battery charging device causes its explosion and/or makes burns.

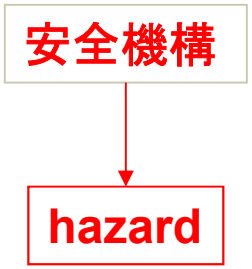
Threat (action): Malware causes malfunction of battery charging device.

Hazard: ECU produces unintended assist torque.

Threat (action): Control message is spoofed.

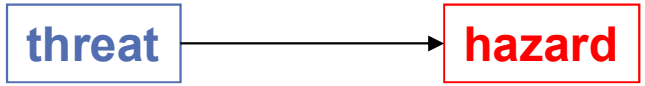
安全機構 VS セキュリティ機構

【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



【今後の可能性】

SCDLによる統合設計/
分析フレームワーク？

【安全機構とセキュリティ機構による防御】

質問(2)

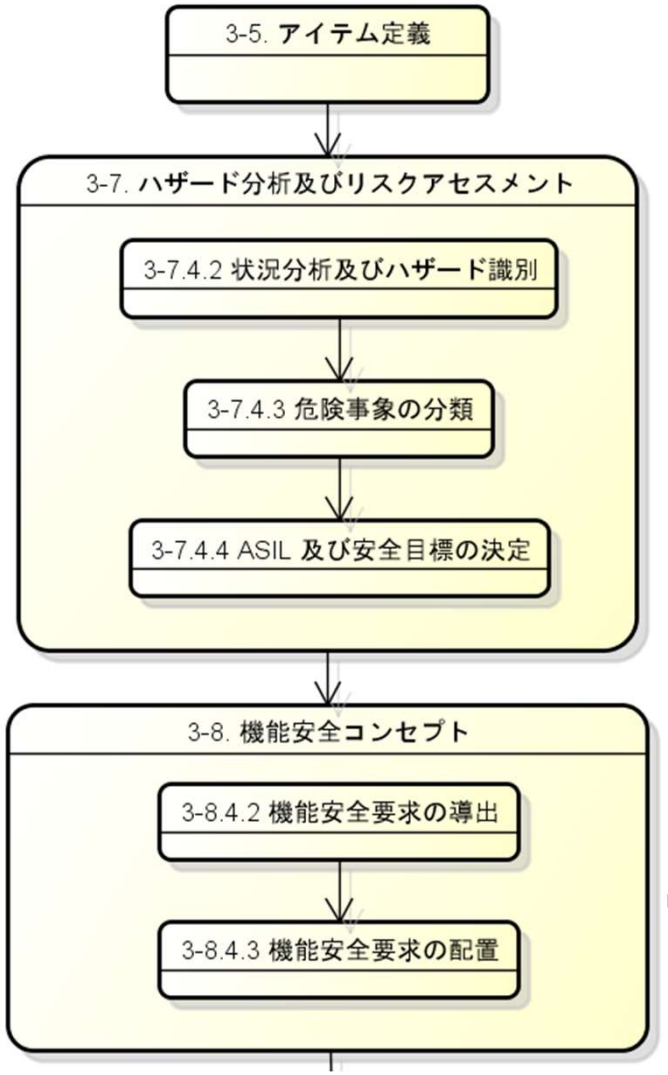
- **Hazard と Threat の関係、安全機構とセキュリティ機構との関係を示しました。この定義は(正しい)間違っているでしょうか？**

- **より良い定義はありますでしょうか？**

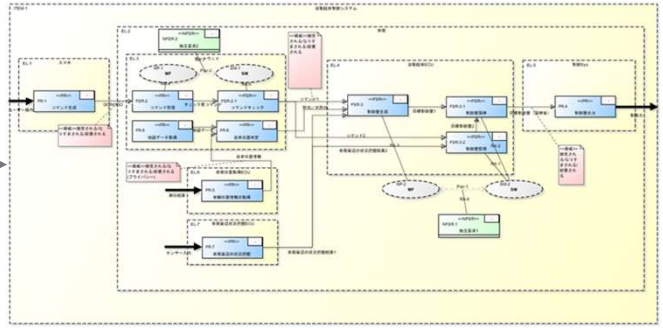
- **三択の質問**
  - 正しい
  - 間違っている
  - 何かしっくりこない。現時点では不明。

【ISO 26262】

想定シナリオ



【SCDLで記述された機能安全コンセプト】



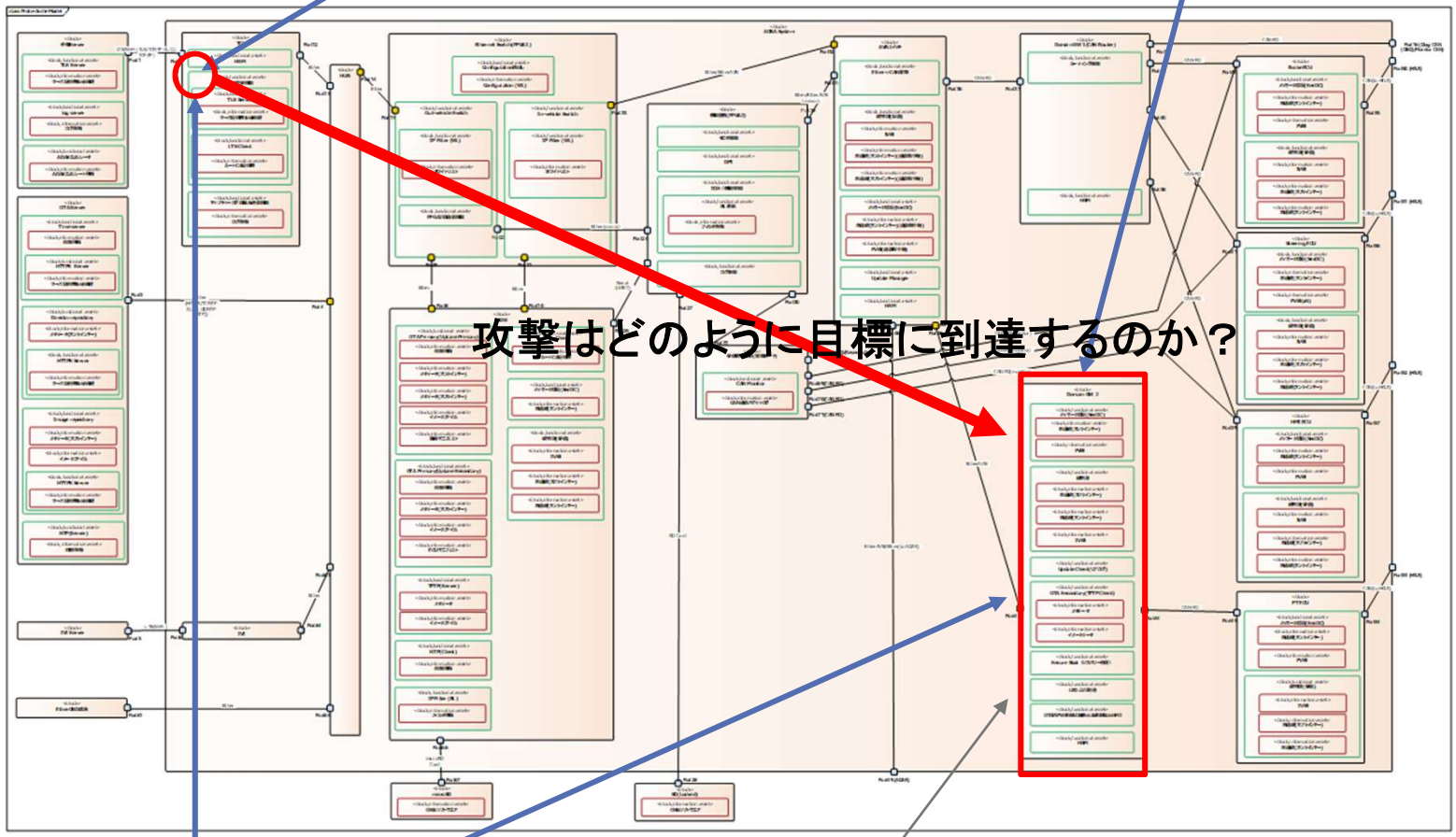
SCDLで記述された機能安全コンセプトに対して脅威分析が可能かを試行

- 従来の分析方法論の枠組みと SCDL の比較
- 従来の分析手法の試行（適用可能性の評価）

脅威を分析する際の必要な要素（アーキテクチャ要素から）

どこから攻撃がくるのか？

何を攻撃から守るのか？



どのような攻撃が可能か？

どこまでが守る範囲なのか？

5W法

そのほかの要素：
＋誰が攻撃をするのか？
＋どのフェーズで行われるのか？

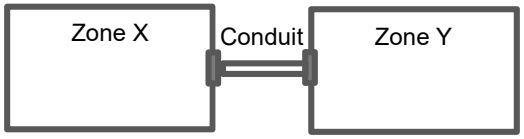
国際規格やガイドラインにおいて規定されている脅威分析に関連する概念

- 様々な国際規格において、脅威や脆弱性分析に関連する概念が規定されている。以下にその一部を紹介する。

Asset (ISO 27005)

(No picture)

Zone and conduit (IEC 62443)



Trust boundary (MS Threat Modeling Tool)
Security perimeter (DO-356)

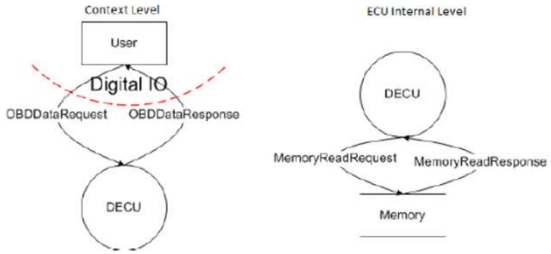
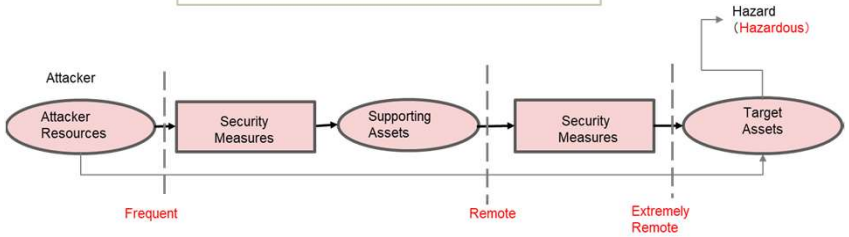


Figure 5-2: Data flow diagram of on-board diagnostics (OBD) use case.

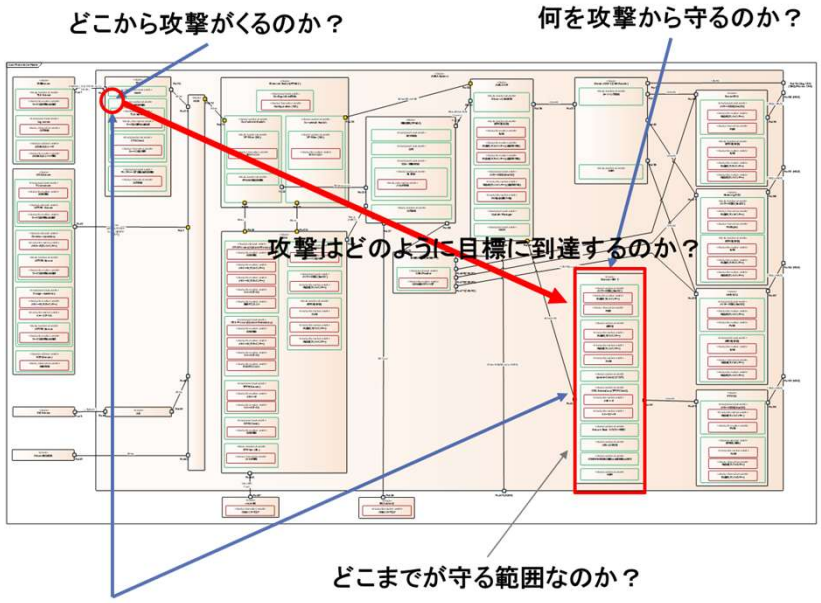
(HEAVENS, Security models D2, ver. 2.0, March 18, 2016)

Threat scenario (DO-356)



(RTCA DO-356: Airworthiness Security Methods and Considerations, 2014)

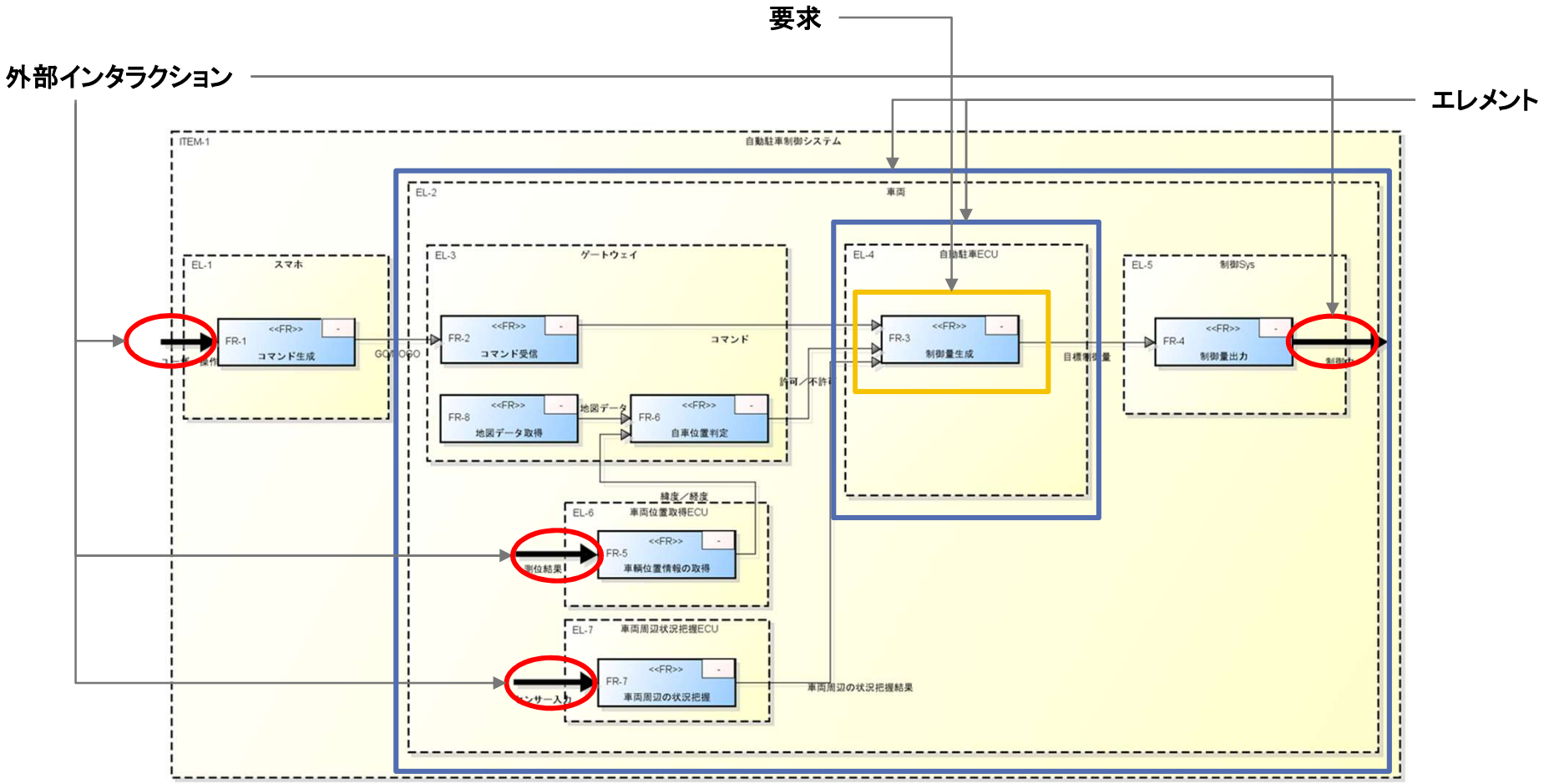
脅威を分析する際の必要な要素（アーキテクチャ要素から）：詳細説明



- どこから攻撃がくるのか？
  - アタックサーフェイス（Attack Surface）
- 何を攻撃から守るのか？
  - 保護資産（Asset）
- どのような攻撃が可能か？
  - 攻撃の分類
  - 攻撃の詳細分析
- 攻撃はどのように目標（保護資産）に到達するのか？
  - 攻撃パス、攻撃シナリオ
- どこまでが守る範囲なのか？
  - 保護するシステムと外部の界面

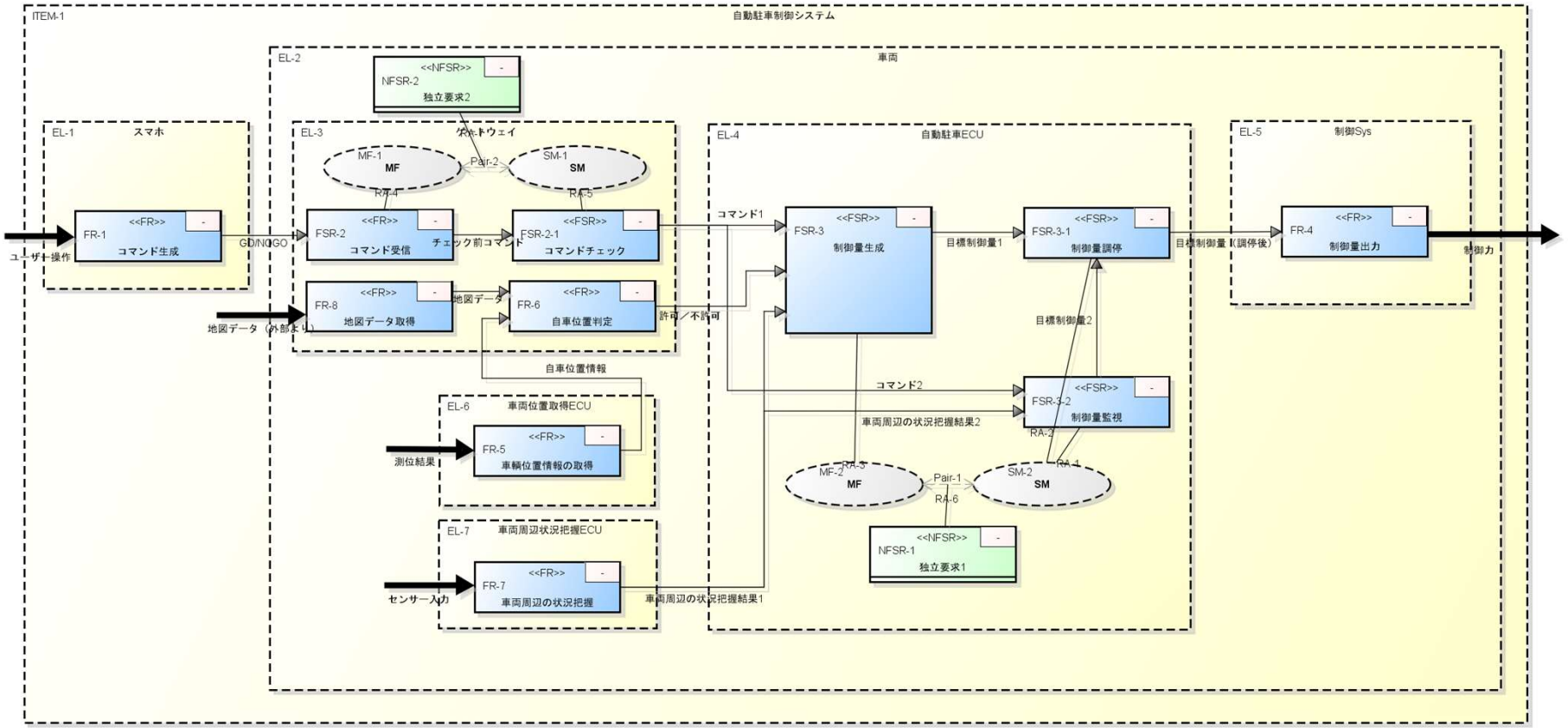
SCDLの説明

- **SCDL（Safety Concept Description Language) とは？**
  - システムの安全設計をアーキテクチャ視点から整理し、論じるための表記法。
- **SCDLの構成要素**
  - 要求
  - エレメント
  - インタラクション/システムバウンダリインタラクション



事例

- **自動駐車制御システム**
  - スマホから入力されたコマンド（GO/NOGO）に従って、地図データ、現在地（測位情報）、環境データ（車両周辺の情報）により、駐車を行う。

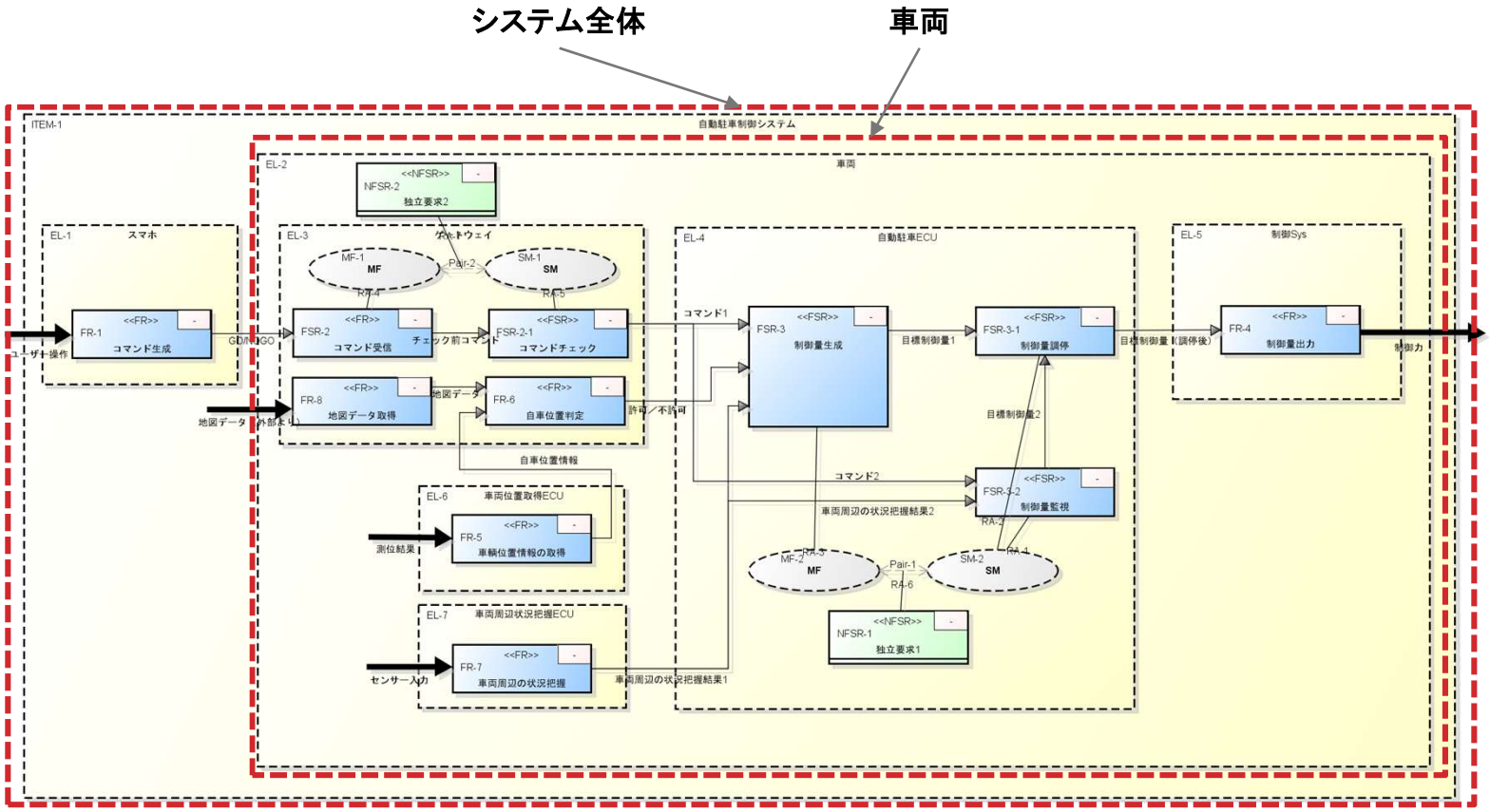


スマホ

車両

どこまでが守る範囲なのか？

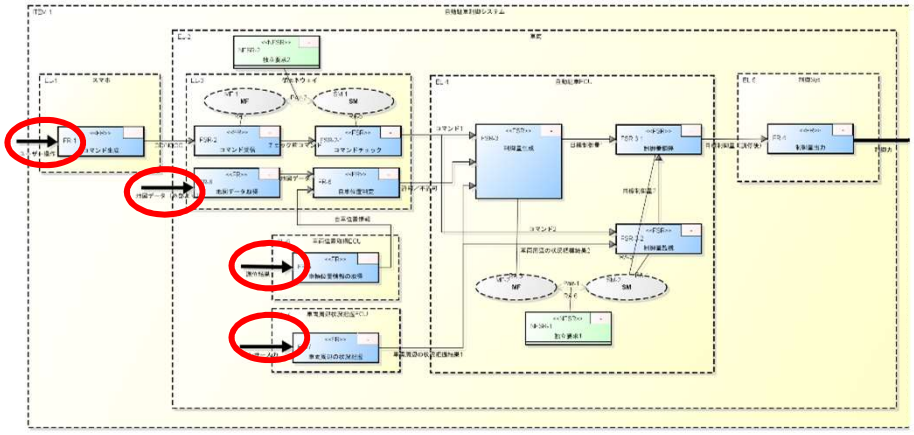
- 守る範囲（システムの境界）は、SCDLの任意のエレメントとすれば良いと考えられる。
  - 範囲のネスティングも自然に解釈できる
    - ✓ 注：DO-326A では、Security Perimeter のネスティングが可能



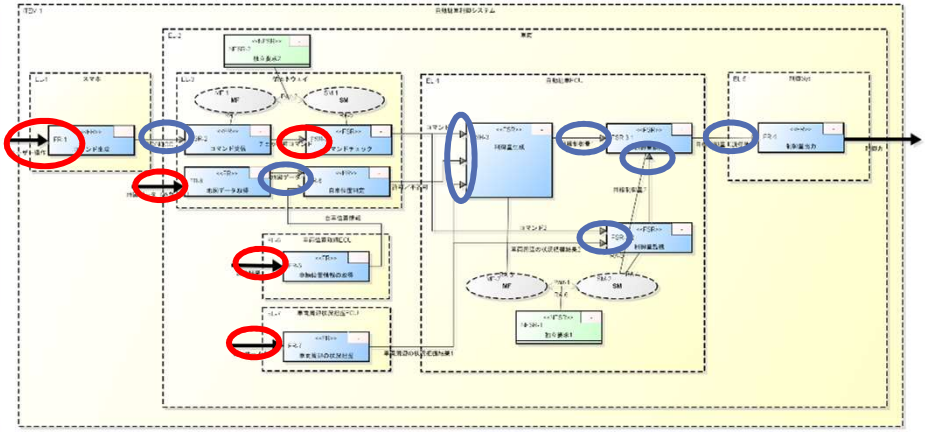
アタックサーフェイスの解釈

- **攻撃の侵入口と解釈して利用。**
  - 前提： SCDLのモデル要素では、攻撃の侵入口として見なされるモデル要素はあるのか？あるならばそれは何か？　＝＞インタラクション
  - 解釈＃１： あるエレメントから見た、外部からのインタラクション（外部インタラクション）？
  - 解釈＃２： 全てのエレメントから見た、外部からのインタラクション？

【解釈＃1】

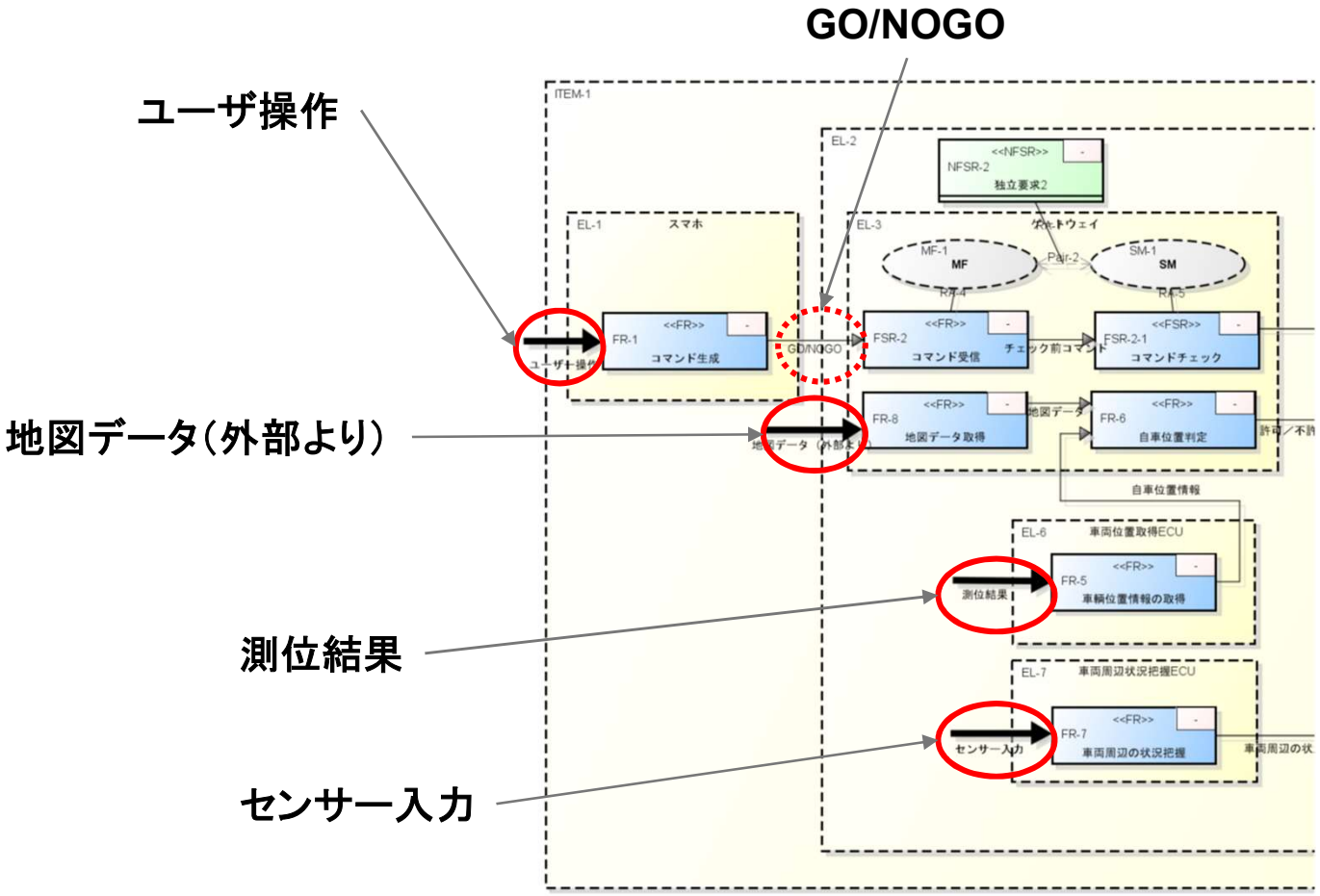


【解釈＃2】



アタックサーフェイスの解釈：解釈＃１

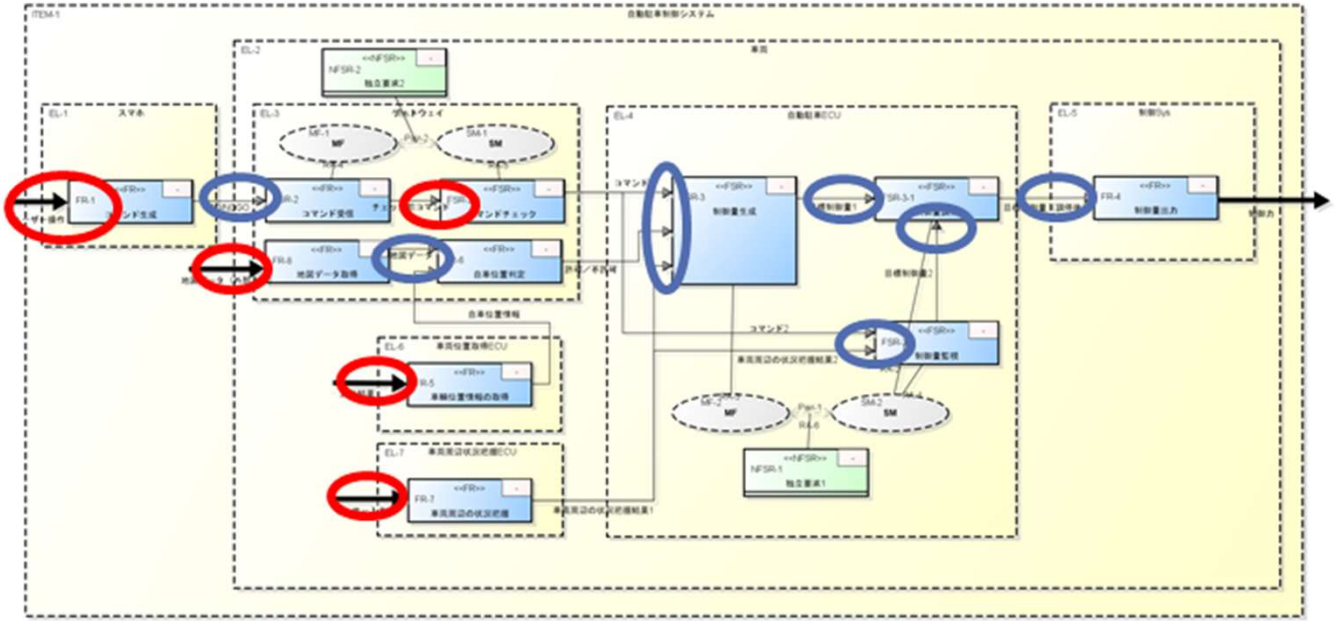
- **解釈＃１：　あるエレメントから見た、外部からのインタラクション（外部インタラクション）？**
  - ここでは、車両エレメントとから見た、外部インタラクションを見ているが、実は、スマホからの入力については、外部インタラクションでは無いので、その分は補完する必要がある。



アタックサーフェイスの解釈：解釈＃2

- **解釈＃2：　全てのエレメントから見た、外部からのインタラクション？**
  - 特定のエレメントを攻撃対象と考えると、どこをアタックサーフェイスと考えるかは非常に相対的。
  - どこを守るのかの設定により、変わるという考えて良いと思われる。

【解釈#2】



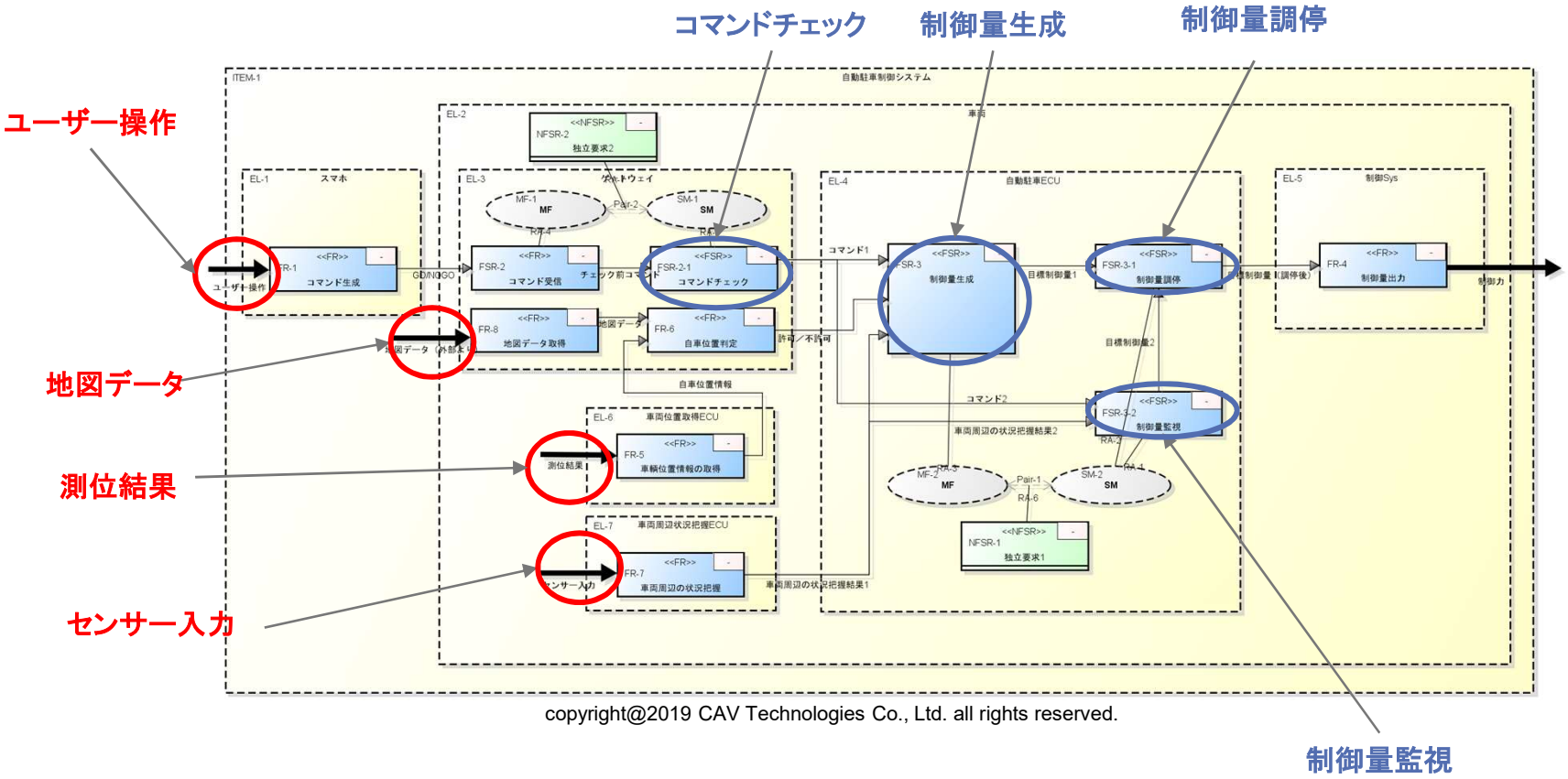
質問(3)

- エレメントとインタラクションの間がアタックサーフェイスとして考えることは妥当であるように見えます。他の意見、コメント、質問はありますでしょうか？

保護資産の解釈

保護資産の入れ子構造もエレメント構造で記述が出来る。

- **攻撃から守るべき対象。**
  - 前提： SCDLのモデル要素では、何が保護資産として考えられるか？
    - ✓ データを保管する場所という概念は SCDL には存在しない。
  - 解釈＃1： （安全、システム）機能？ => 機能資産（FRとFSR 両方）？
  - 解釈＃2： インタラクションの要素名？ => 情報（データ）資産？
  - 解釈＃3： 上記の両者？



抽出された保護資産

機能資産	機能区分
コマンド生成	FR
コマンド受理	FR
コマンドチェック	FSR
地図データ取得	FR
自動位置判定	FR
車両位置情報の取得	FR
車両周辺の状況把握	FR
制御量生成	FSR
制御量監視	FSR
制御量調停	FSR
制御量出力	FR

情報資産	情報区分
ユーザ操作	外部
GO/NOGO	
地図データ	外部
チェック前コマンド	
コマンド1、2	
緯度／軽度	
測位結果	外部
センサー入力	外部
許可／不許可	
車両周辺の状況把握結果1，2	
目標制御量1，2	
目標制御量（調停後）	
制御力	

これはアタックサーフェイスと同じ？

SCDLでは、I/Fの名前が無いようなので、情報資産とアタックサーフェイスが同じものとして解釈される

質問(4)

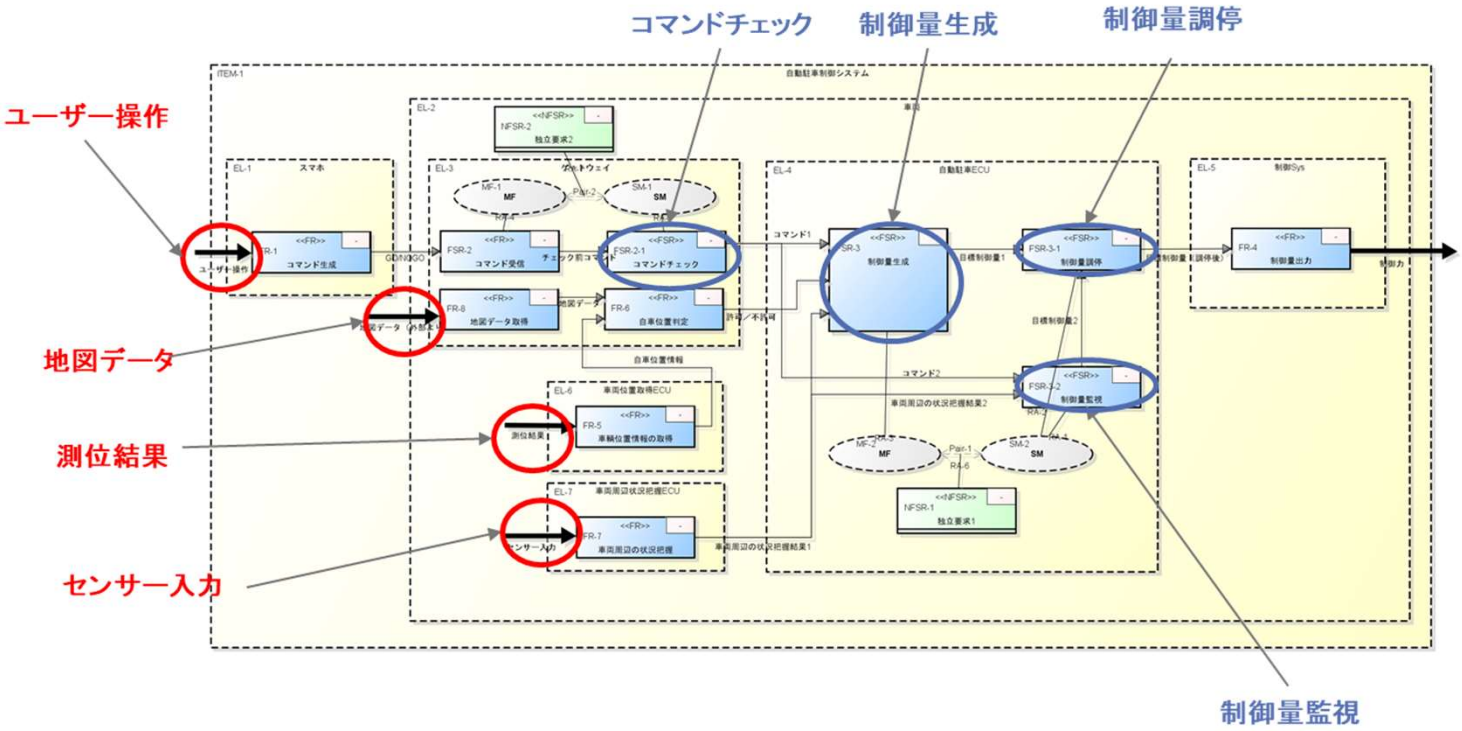
- 保護資産として、インタラクションに指示されたデータ(情報)と要求を対象とすることは良さそうです。
  - 特にデータ(情報)と機能を分ける必要は無い、という意見もありそうです。
- 他の意見、コメント、質問はありますでしょうか？

どのような攻撃が可能かの解釈

- **攻撃が可能なアタックサーフェイスと保護資産に対して、特徴的な攻撃を示すガイドワードである STRIDE を適用。**
  - STRIDEが最も広く利用されているので採用しただけであり、他のガイドワードが可能ならば利用することは可能。

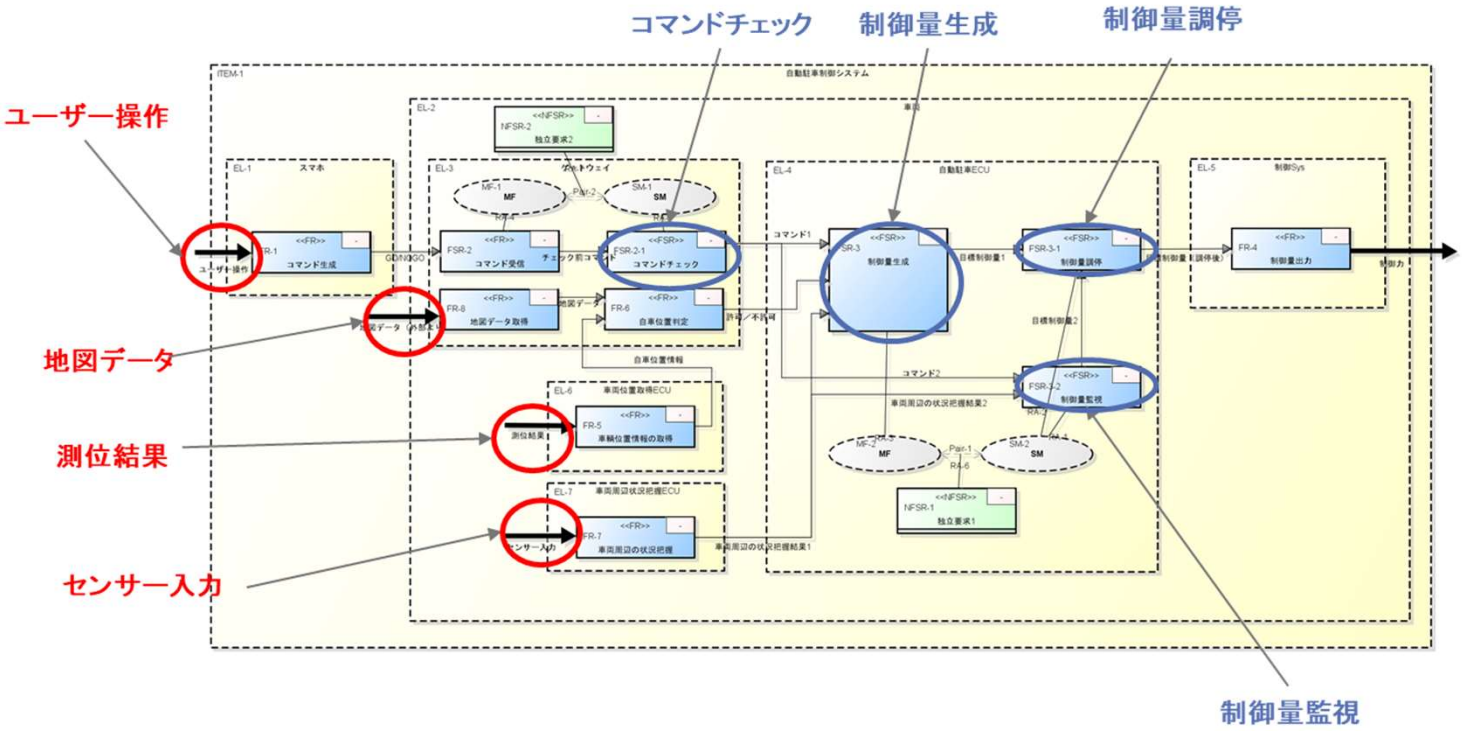
脅威	必要とされる性質
Spoofing（なりすまし）	Authentication（認証）
Tampering（タンパリング）	Integrity（完全性）
Repudiation（否認）	Non-Repudiation（否認不可）
Information Disclosure（情報漏えい）	Confidentiality（機密性）
Denial of services（サービスの拒否）	Availability（可用性）
Elevation of privilege（特権昇格）	Authorization（認可）

どのような攻撃が可能かの解釈：アタックサーフェイス



	S	T	R	I	D	E
ユーザ操作	✔	✔		✔	✔	
地図データ	✔	✔		✔	✔	
測位結果	✔	✔		✔	✔	
センサー入力	✔	✔		✔	✔	

どのような攻撃が可能かの解釈：保護資産

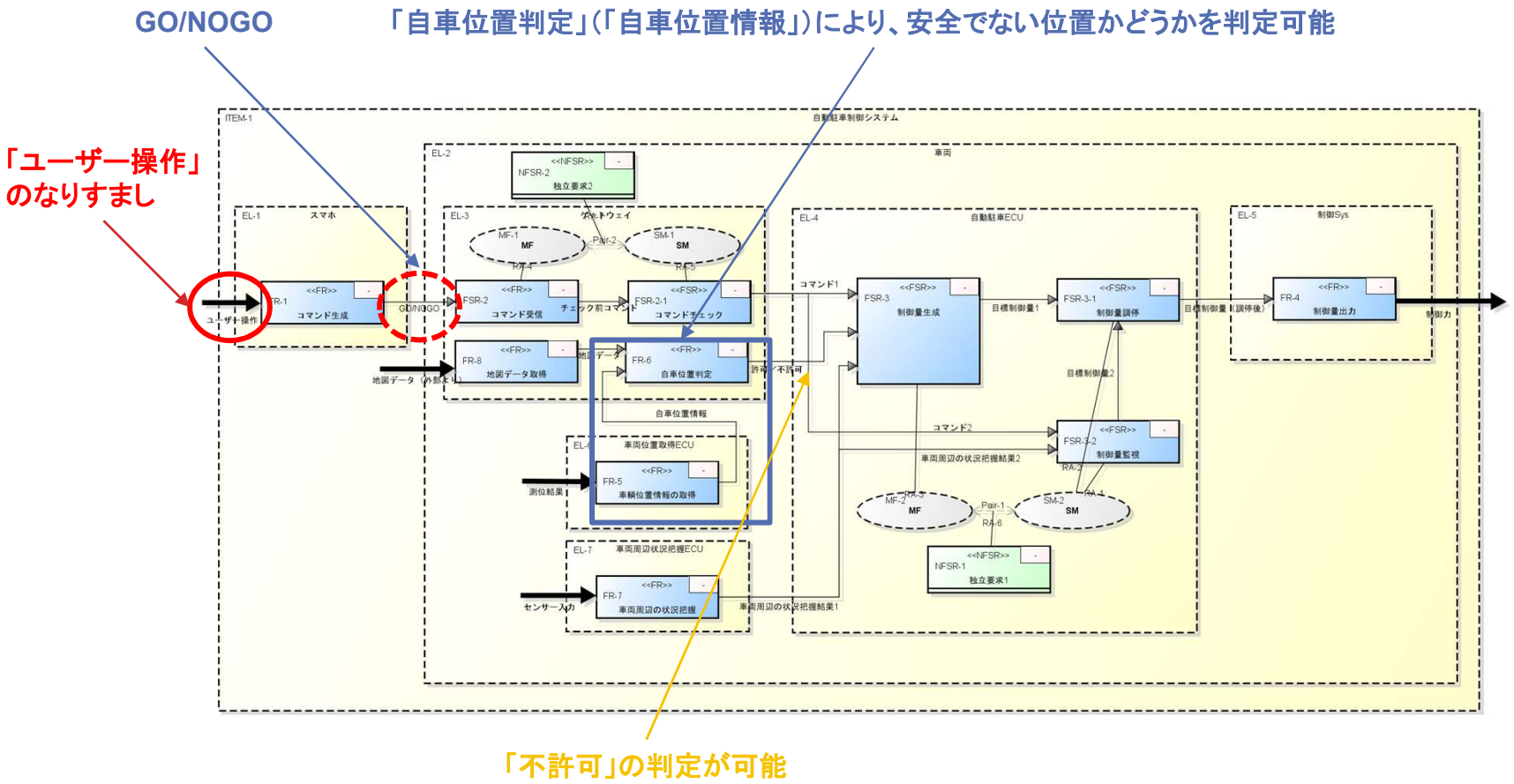


	S	T	R	I	D	E
コマンドチェック	✔	✔			✔	✔
制御量生成	✔	✔			✔	✔
制御量調停	✔	✔			✔	✔
制御量監視	✔	✔			✔	✔

質問(5)

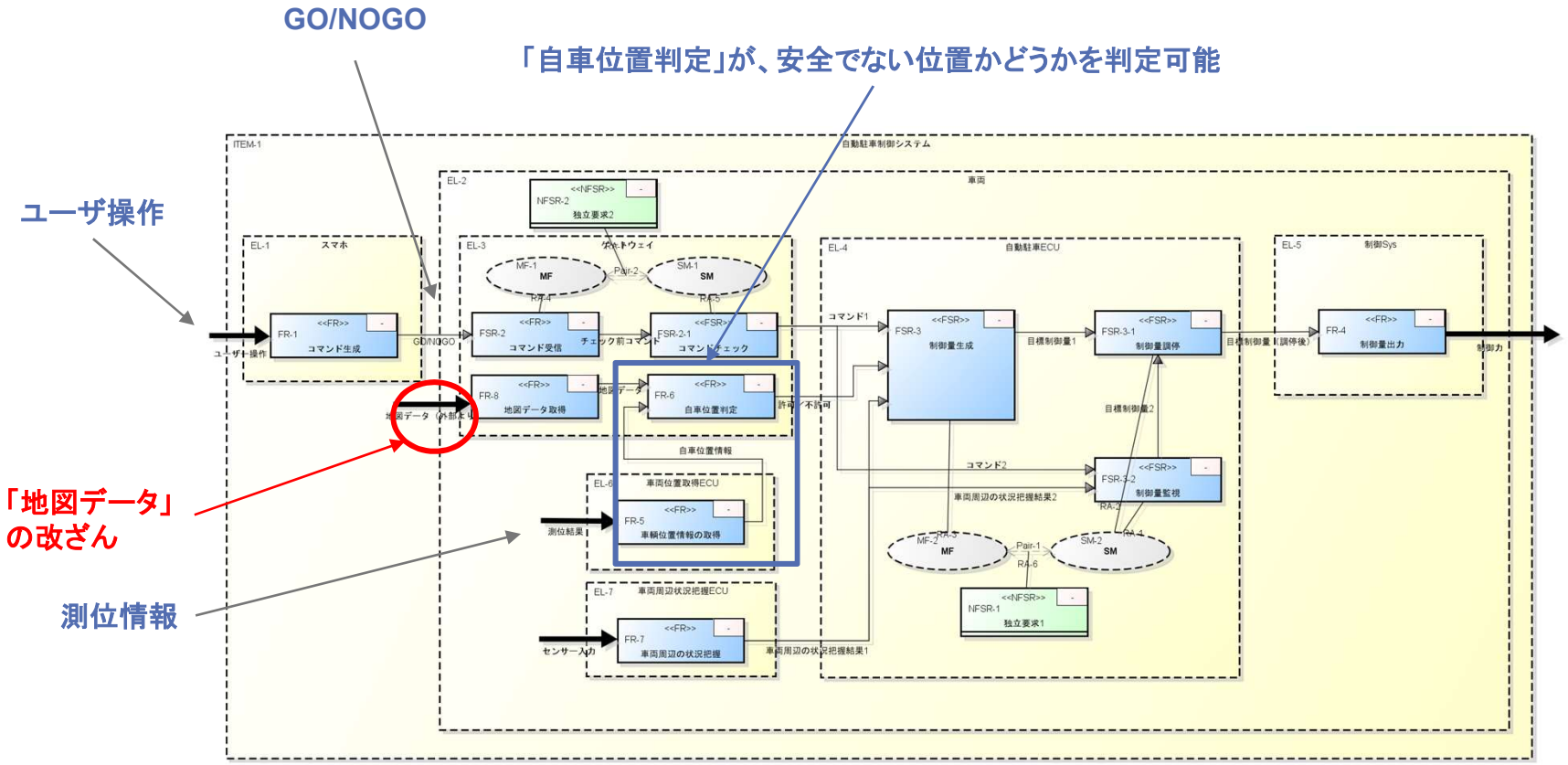
- 攻撃の同定には **STRIDE** を用いました。
- **STRIDE**による分析についてはどのようなご意見をお持ちでしょうか？
- 攻撃には対象によりパターンがあるようです。このようなパターンは一般的であると考えられますが、正しいと思われますでしょうか？

実際の攻撃の分析例（1）



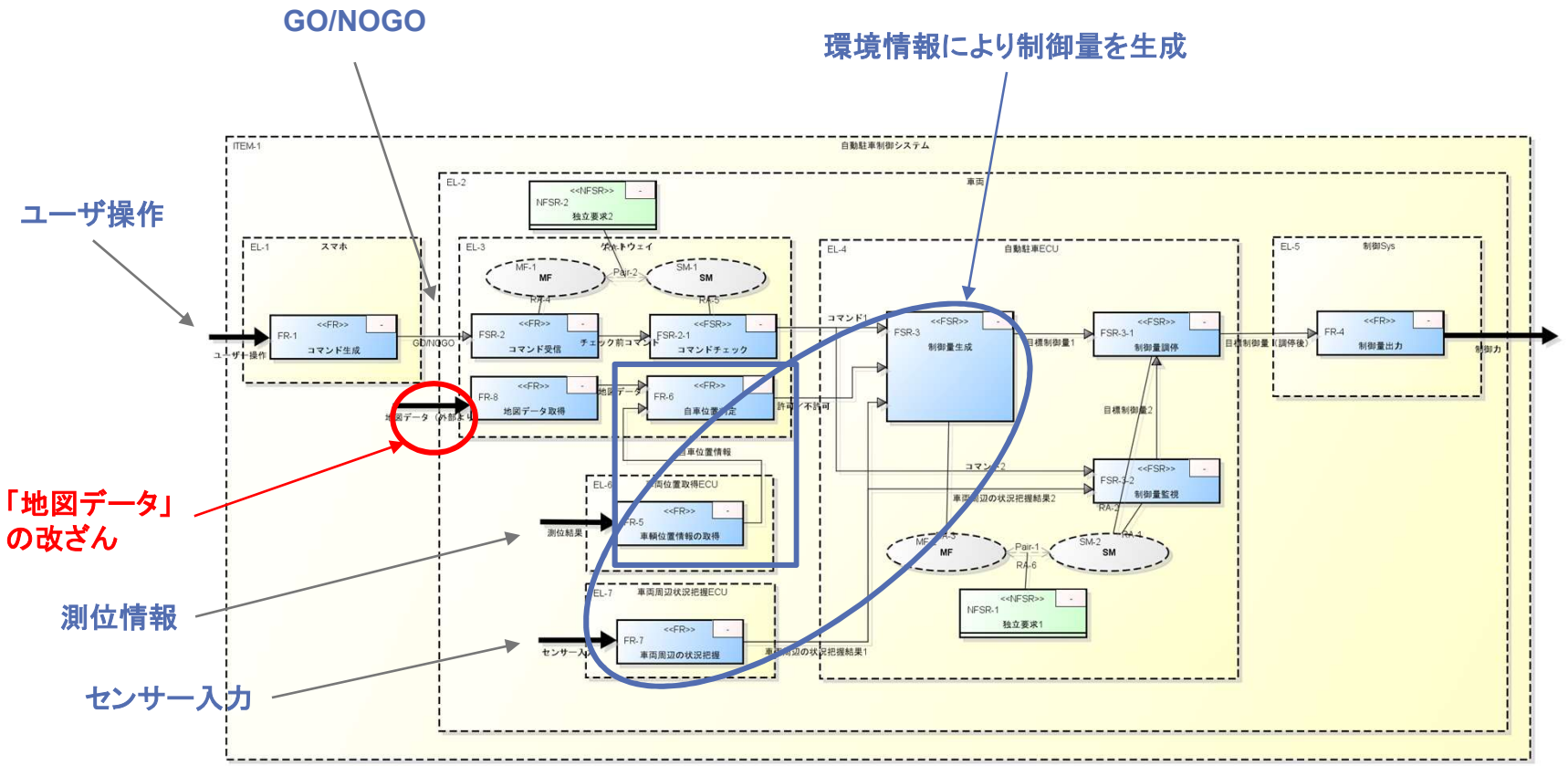
- 「意図されていない駐車位置への駐車（をすることで車両の破損）」を目的とした攻撃を想定
  - 「ユーザ操作」がなりすまされた場合。
- 「自車位置判定」（「自車位置情報」）により、安全でない位置かどうかを判定可能

実際の攻撃の分析例(2-1)



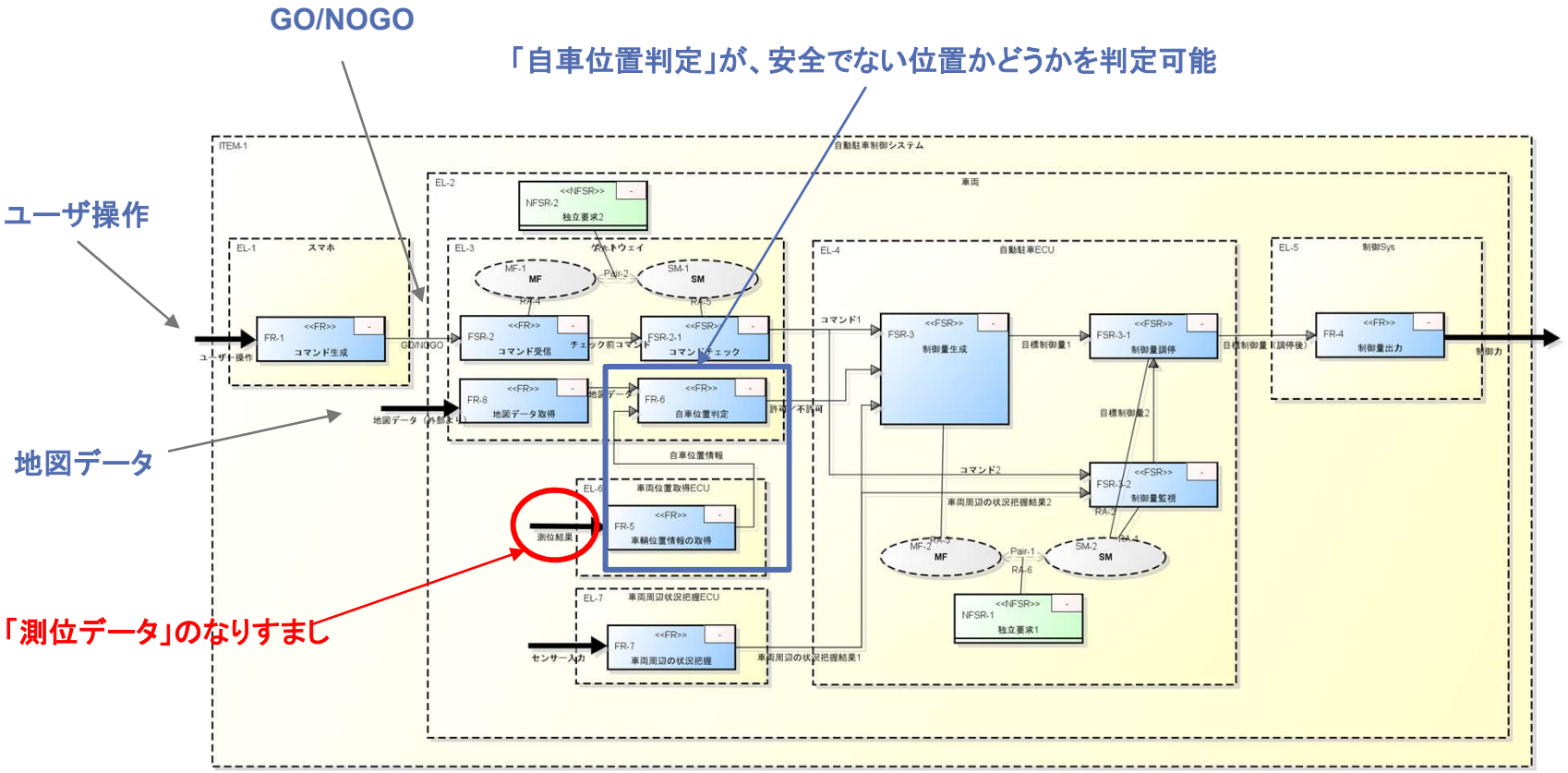
- 「地図データ」の改ざん(駐車場所には実際には何等かの障害物(例:家))
- 「測位情報」があるので、攻撃が防げる?

実際の攻撃の分析例(2-2)



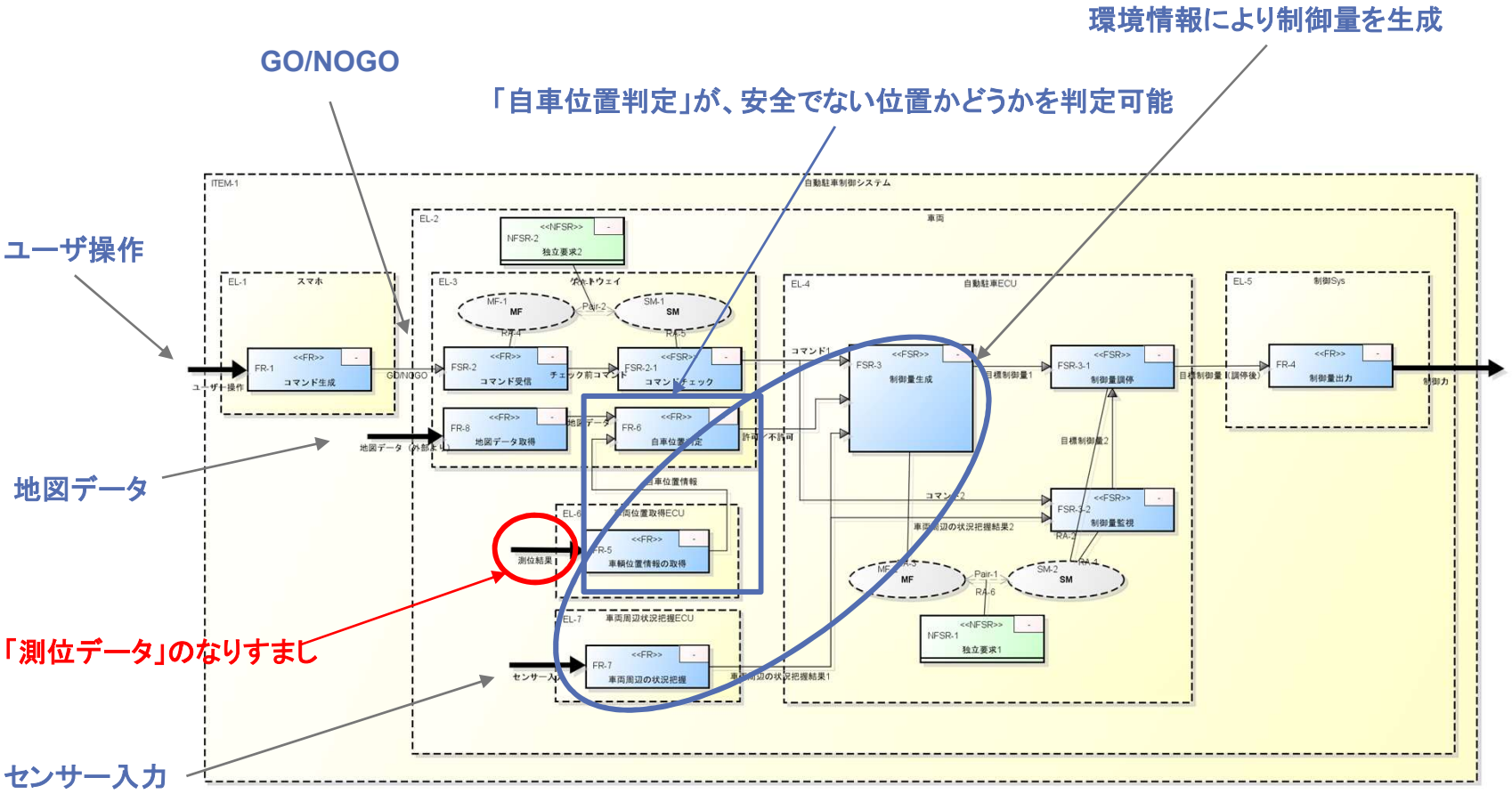
- 「測位情報」だけだと、地図情報における位置情報が改ざんされている場合、攻撃を防ぐことが出来ない。
- 車両の周辺情報は「センサー情報」で取得し、「制御量生成」が行われる。この場合、位置情報が改ざんされていても、障害物がある場合には、制御量の生成が行われず、ここで防御が行われる。

実際の攻撃の分析例(3-1)



- 「測位データ」がなりすまされた場合、「自車位置判定」が侵害される。

実際の攻撃の分析例(3-2)



- 「測位データ」がなりすまされた場合、「自車位置判定」が侵害されるが、車両の周辺情報は「センサー情報」で取得し、「制御量生成」が行われる。
- この場合、測位データがなりすまされていても、障害物がある場合には、制御量の生成が行われず、ここで防御が行われる。

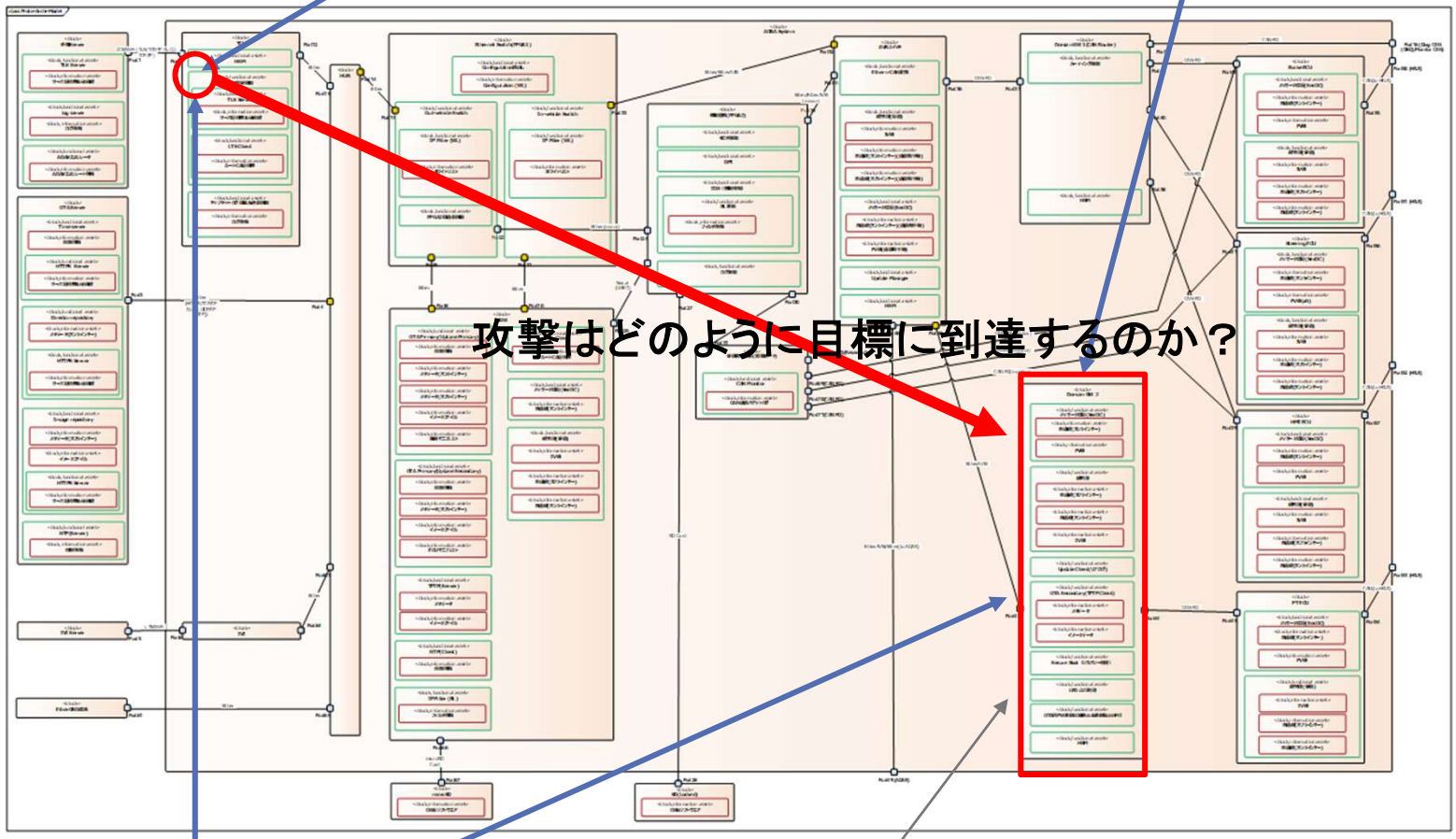
どのような経路の攻撃が可能かの解釈

- アタックサーフェイスから侵入し、あるコンポーネント（エレメント、要求）を踏み台にし、攻撃するといった連続攻撃の形の分析は難しい。

SCDLで実現可能な脅威を分析する際の必要な要素

どこから攻撃がくるのか？ OK

何を攻撃から守るのか？ OK



どのような攻撃が可能か？ OK

どこまでが守る範囲なのか？ OK

5W法

そのほかの要素：
＋誰が攻撃をするのか？
＋どのフェーズで行われるのか？

だからといって有効なのか？

- **SCDL で記述した安全コンセプトに対して脅威分析はある程度可能であることが判明した。**
  - 攻撃分析に必要な要素を、SCDLのモデル要素で解釈することがある程度可能
- **攻撃に対して、（安全）機能要求が対抗可能かどうかの判定はある程度出来ることが判明した。**
- **これらの攻撃の分析からセキュリティ要求の抽出も可能であり、またセキュアなアーキテクチャの分析も可能であると考えられる。**

最良のシナリオ ⇒ **サイバーセキュリティコンセプト記述に利用**

可能なシナリオ ⇒ **安全コンセプトからの脅威分析をセキュリティ設計の補助として利用**

これらの課題については、規格、開発プロセスなどにより大きく変わる可能性がある。

おわりに

- **セキュリティSWGの現在の活動**
  - SCDLのセキュリティ適用に関する報告書を作成中
    - ✓国際会議への論文投稿
    - ✓SCDLの仕様書へのアネックスとして発表
- **今後の希望的観測**
  - サイバーセキュリティコンセプト（？）の分析・記述言語として拡張

まだ、やるべきことは多くありますので、是非、ご参加を下さい！