Vol.2017-ARC-225 No.13
Vol.2017-SLDM-179 No.13
Vol.2017-EMB-44 No.13
2017/3/9

車載システムを想定した セーフティ＆セキュリティ制御システム開発プロセスの検討

左近　透[†1]　中本　幸一[†2]

概要：セキュリティ機能と安全機能の関係について ISO26262 をベースとした車両開発を想定した場合のセキュリティ機能の要件定義を検討する．機能安全とセキュリティの要件定義/設計を統合し，安全機能とセキュリティ機能の相互関係を明確にするために，安全/セキュリティ機能の動作をモデル化，それにしたがい，安全/セキュリティ機能の界面を明確化，相互の関連を確認可能にした．また，セキュリティ脅威分析リスク評価を，機能安全設計での各段階での利用情報に応じた脅威分析粒度を定義して段階的に実施すること，並びに ASIL 相当のレベル分けに関しては，リスク評価を，具体的な脅威の導出が可能になる時点での CRSS 値の指定と置き換えた．このことで，要件定義の上流での，脅威の具体化に必用とおもわれる詳細技術情報を不要とし，分散開発に適応した要件定義/設計手法とした．

キーワード：自動車電子制御システム，機能安全，セキュリティ，ハザード分析，脅威分析，リスク評価，

Safety & Security Control System Development Process For In-Vehicle System

Toru Sakon[†1]　Yukikazu Nakamoto[†1]

1. はじめに

自動車や製造機械，発電所，鉄道や医療用器械に代表される制御機器の設計に際しては，故障や動作異常の発生により生命や設備を危険にさらすことを阻止することが優先度の高い目標である．安全には，危険そのものを発生させない発生しない本質安全と，危険につながる事象が発生した場合に，それに対処する機能により危険回避をおこなう機能安全がある．機能安全設計のための規格として，IEC61508（電気・電子・プログラマブル電子(E/E/PE)機能安全に関する国際規格）がある．この規格は，産業別に派生規格が存在し，たとえば，自動車に関しては，ISO26262(Road Vehicles －Functional Safety)[1]が存在する．

しかし, 近年, 制御機器の安全動作に対する脅威として，機器の故障などに加えて，サイバー攻撃の懸念が高まりつつある．また，研究者による自動車のセキュリティホールを利用した攻撃の発表や，プラントに対する攻撃の報道などサイバー攻撃の実施例も発生した．米国 ICS-CERT によると 2009 年以降，インシデント報告は増え続け，2013 年では 250 件を越えたインシデントが報告されている．

このような制御機器に対するサイバー攻撃に対する対応として，E/E/PE 機能安全システムに対するセキュリティ規格である IEC62443 が規格制定されている．この規格は組み込みシステムに対するセキュリティ認証(EDSA 認証)として一部の企業や政府関係では納入要件となっている．また，自動車産業においても，米国 SAE が開発した J3061-Cybersecurity Guidebook for Cyber-Physical Vehicle Systems などサイバー攻撃に対するガイドラインや規格が提案されている[2].

しかし，開発プロセスにおいて機能安全とセキュリティの開発の進め方や，機能安全機構とセキュリティ機構の関係などは議論が継続されている．たとえば J3061 などの既存の規格やガイドラインでは，セキュリティ機能の実現を中心に規定，記述されている．しかし安全機能との関係性は，相互の情報を交換が必用とし，幾つかの例示として記載されているのみである. また, 産業構造上も, 車メーカ，Tier-1,Tier2，部品メーカで構成される産業構造と，そこでおこなわれる分散開発体勢に適合しなければならない．

本論文では，セキュリティ機能と安全機能の関係について ISO26262 をベースとした車両開発を想定した場合のセキュリティ機能の要件定義を検討する．初めにセキュリティ機能の開発手法と機能安全開発手法の共通点，相違点について概要を纏める．さらに，適用対象となる自動車製造業界の構造からくる要求を述べる．次に，機能安全の機能要求仕様設計，技術要求仕様設計に相当したレベルでのセキュリティ要求仕様の導出に抽象度の高い，Modification/Destruction/Disclosure の 3 種類の脅威による分析をおこない，さらに，STRIDE からの脅威分析により具体的な脅威を定める．機能安全における故障モード対策が脅威との対応を確認，対処出来ない部分についてセキュリティ機能要件定義および上流設計をおこなう手法を検討する．

なお，本論文では利用する用語は ISO26262 を元に利用する．そのため，情報システム側の用語との相違がある部分が存在するが，初出時に注意記載する

†1 兵庫県立大学
University of Hyogo

Vol.2017-ARC-225 No.13
Vol.2017-SLDM-179 No.13
Vol.2017-EMB-44 No.13
2017/3/9

2. ISO26262 と TP15002

ここでは，以降の議論に必用なため，自動車制御システムの機能安全規格である ISO26262 と，併せて，自動車開発目的として開発されたセキュリティ分析手法として自動車技術会の技術レポート TP15002[3]の概要を説明する．

2.1 ISO26262

ISO26262 は IEC61508 をベースとした安全規格であり，3,500Kg 以下の自動車の制御システム開発に特化したものである．全体の開発プロセスは，要件定義から設計，製造，検証に至るウオーターフォール型のプロセス（V 字プロセス）が定義されている．ここでは，本論文の検討対象である要件定義から設計に至る手順を見る．

(1) アイテム定義（開発対象定義）

アイテムとは，車全体観点でみた機能を提供するサブ機能の集合体として定義される開発対象である．アイテムは，形式的には，センサーなどの外部入力，入力，演算などの内部処理，アクチュエータへの出力からなる構成および機能および非機能要求，制約条件からなる．内部処理には，車全体としての機能要求，および機能を提供するためにエレメントと呼ぶサブ機能ブロックが定義されている．

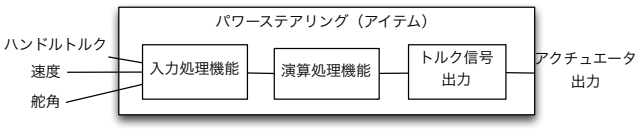

図 1 （パワーステアリング）アイテム構成図例

(2) ハザード分析とリスクアセスメント

ISO26262 ではリスクを「危害発生確率とその危害の過酷度との組み合わせ」で定義している． 安全は，リスクの低減が目標である．ISO26262 では目標の指標を 4 段階のレベルで示している．

まず，ハザード(危機事象)とハザードが発生する状況の特定を実施する．一般には，HAZOP(Hazard and Operability Study)手法で抽出，さらに FMEA(Fault Mode and Effect Analysis)/FTA(Fault Tree Analysis)で実際発生可能性の分析を行う．次に特定されたハザードと状況に対してリスク評価をおこなう．ISO26262 では到達すべきリスク軽減度の指標として ASIL(Automotive Safety Integrity Level)を定める．

ASIL は，不具合発生時にその状況や操作者の回避可能性を考慮してさだめる到達すべき安全度の指標としてのリスク低減目標である．ハザードの特定の結果，得られるハザードの過酷度，発生頻度，回避可能性から ASIL を定める．

S：過酷度（Severity）は操作者または他の交通関係者が受ける傷害の重さの見積もりである．

E:発生頻度（probability of Exposure）これは，想定される運転状況の期間，もしくは，ある状況の発生頻度のどちらかの指標により見積もられる．

C:回避可能性（Controllability）危害を回避するために危険事象に対し十分に抑制することができる確率の見積もり．

これらの各クラスから，定められた分類表に従って 4 段階の ASIL および一般品質保証レベルでの対処（QM）の分類を決定する．開発に際しては，ASIL のレベルに応じた開発手法や検証，システム構成をとることが要求される．

ハザード分析とリスクアセスメントの最後に，ハザードに対する安全に対する要求をセーフティゴール(安全目標)として定める．

表 1 パワーステアリングの場合のセーフティゴール例

ハザード	高速走行中ハンドルが軽い状態となる．ASIL-B
安全目標	高速走行中にハンドルが軽くならないようにする
安全状態	走行中はパワーステアリングをオフにする

(3) 機能安全コンセプトの導出

次に，安全目標を実現するために必用な，安全機能（機能安全要件）の抽出を行う．ここで定義される，機能安全要件とは，安全目標に基づくアイテムの安全な振る舞いの仕様および実装に依存しない安全方策である．

まず，安全目標を達成するのに必用な機能を導出する．アイテムの構成図などから，機能安全目標を詳細化して安全機能を導出する．

これらの機能安全要件を，作業時点で判明しているアイテムの具体的な構成に基づいて各エレメントもしくはアイテム外部での対策に割り当てる．この割り当ておよび機能安全要求のすべてを機能安全コンセプトと呼ぶ．

表 2 機能安全コンセプトの例

安全目標	高速走行中にハンドルが軽くならないようにする	
機能安全要求	速度とハンドル操作を補助しているトルクを監視し，速度に比べて補助トルクが異常に大きければ，補助トルクを出すアクチュエータを停止する．	
理由	高速走行中に大きなハンドルを切ると事故につながりやすい．低速走行時にハンドルが重くなった場合でも，事故は起こりにくい．また運転手の気づきにより修理工場へ行くことが促される．	
速度信号の検出	速度を直接監視機能に入力する	監視機能,
トルクの検出	トルクを直接監視機能に入力する	監視機能,
異常の検出	速度とトルクを比較して異常を検出する	監視機能
アクチュエータオーバライド	監視機能からアクチュエータ出力をオーバライドする	監視機能, アクチュエータ

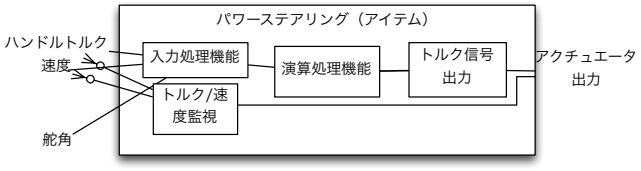

図 2 パワーステアリングアイテム構成図

なお，一般にはコンセプトから機能が導出されるが，ISO26262 では順序が逆になっている．

Vol.2017-ARC-225 No.13
Vol.2017-SLDM-179 No.13
Vol.2017-EMB-44 No.13
2017/3/9

(4) 技術安全要件の導出とシステム設計

機能安全コンセプトを，本段階で利用出来るシステム基本設計に当てはめて，実装に関する要件をだしたものが技術安全要件である．

表 3 技術安全要求の例

機能安全要求	速度とハンドル操作を補助しているトルクを監視し，速度に比べて補助トルクが異常に大きければ，補助トルクを出すアクチュエータを停止する．		
技術安全要求 1	速度信号と補助トルク信号を直接計測し，両者の値を比較することで異常を検知し，検知した場合にトルク信号出力をオーバーライドしアクチュエータを停止する		
速度信号直接計測	信号線追加	速度信号を直接監視機能に入力する信号線を追加する	監視機能，信号線
トルク直接計測	信号線追加	トルク信号を直接監視機能に入力する信号線を追加する	監視機能，信号線
異常検出	速度信号数値化	速度信号を数値に変換	信号変換
	トルク信号数値化	トルク信号を数値に変換	信号変換
アクチュエータオーバライド	信号線追加	監視機能からアクチュエータ出力をオーバライドできる信号線を追加する	監視機能，信号線 アクチュエータ

システム設計では，実装に関する要件である技術安全要求を受けて，本段階で利用できるシステム基本設計に安全機能を追加して，ハードウェアまたはソフトウェアの基本設計を完了する．

2.2 TP15002 セキュリティ分析

TP15002 は公益社団法人自動車技術会により取りまとめられた自動車システム向けのセキュリティ分析ガイドである．このガイドにおけるセキュリティ分析は，評価対象の定義，脅威分析，リスク評価，対策方針決定，セキュリティ要件の選択という５つのフェイズからなる．

評価対象の定義では，評価対象の構成要素および構成要素間の情報フローを明確したモデルを作成する．

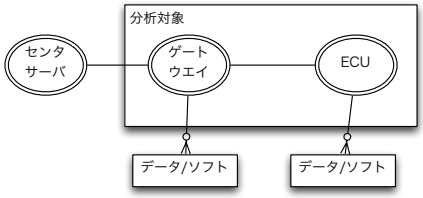

図 3 評価対象モデル例

さらに構成要素毎に，提供機能と構成要素が含む保護資産を明確にする．保護資産には保護すべき機能とデータがある．例として，車外と車内の通信システムの中間に介在するゲートウエイ ECU の機能・保護資産を示す．

表 4 ゲートウエイ ECU の機能・保護資産

	機能	保護資産	C	I	A
ゲートウエイ ECU	認証機能	認証機能		○	○
		認証鍵	○	○	
	情報転送機能	情報転送機能		○	○

最後に対象システムのライフサイクルを明確にする．

脅威分析では，まず評価対象システムの置かれた環境や条件を定義する．次に当該条件における脅威を，どのインターフェイス(Where)から，誰が(Who)，いつ(When)，どのような動機(Why)で，どのように引き起こされる脅威（What）かを樹上に整理して洗い出す．

表 5 脅威の例

Where	ゲートウエイとサーバのインターフェイスから
Who	第三者が
When	走行中に
Why	通信データ(認証データ)を
What	盗聴して漏えいさせる，なりすます．

リスク評価では，抽出された脅威について CRSS(CVSS based Risk Scoring System)や RSMA(Risk Scoring System for Automotive systems)を用いてリスクスコアリングをおこなう．ある基準以上の脅威については FTA などにより原因を抽出し、すべての事象に対して対策方針を決定する．

表 6 対策方針の例

脅威	原因	対策目標	対策方針		
			#	種別	方針内容
走行中（運用時）	ゲートウエイとセンターサーバ間の認証データを盗聴して成りすます	ゲートウエイとセンターサーバ間の認証データの盗聴を防止する		IT	盗聴によって入手した認証情報を利用不可にする

最後にセキュリティ機能要件とセキュリティ保証要件を定義する．機能要件は，Common Criteria Part2 で定義されるセキュリティ機能コンポーネントを要件として書き換えたものである．また保証要件は，Evaluation Assurance Level で指定する．

3. 機能安全＆セキュリティ開発の問題点

安全機能開発におけるセキュリティへの取り組みで，本論文で解決すべき問題点を列挙する．

(1) 安全機能とセキュリティ機能の相互作用

攻撃者による悪意在る攻撃が実施された場合，一部の攻撃は安全機能で対処可能な場合がある．例として，車載ネットワークにおける Flooding によるサービス拒否攻撃を想定する．この攻撃の結果，車載ネットワークに接続された ECU 間の通信が途絶する．しかし，安全機能上，断線による通信途絶が想定されていた場合，機能安全機能により安全状態へ移行する．しかし，全車載ネットワークが Flooding によるサービス拒否攻撃を受けた場合には，機能安全の想

Vol.2017-ARC-225 No.13
Vol.2017-SLDM-179 No.13
Vol.2017-EMB-44 No.13
2017/3/9

定する故障モードではない可能性がある．

したがって，機能安全開発とセキュリティ開発では，相互の想定している故障モードの内容および脅威内容を対比し，さらに対処を決定した場合，その作用を相互に検討する手続きを定義することが必用と考える．

(2) 安全とセキュリティの脅威分析とリスク評価

先に述べたように，機能安全では，全体レベルの機能が損なわれた場合の障害をハザードとして抽出する．FTA/FMEA により，抽出されていないハザードが無いことを確認した後に，ハザードとその発生状況における過酷度，発生頻度，回復可能性からリスク軽減度の目標である ASIL を定める．つまり開発対象の機能をサブ機能ブロックが定義された段階で脅威分析とリスク評価が完了する．

一方，一般にセキュリティにおける脅威分析は，発生頻度に相当する情報を持たない．TP15002 で利用している CRSS や RSMA では攻撃可能地点(エントリーポイント)，攻撃界面（アタックサーフェス）との隣接度，攻撃の難易度や攻撃者の熟練度を利用する．また，TP15002 は資産としてデータなどの情報資産も含む．しかし，これらの情報が，要件定義の ASIL 導出段階で存在していることは保証されない．また，ある機能の実装は，アルゴリズムだけで実装するか，データとアルゴリズムで実装するかは要件定義段階では決められない．従って，要件定義の手順としてリスク評価も機能安全開発と同等の情報で実施出来なければならない．

(3) 安全機能仕様の詳細化とセキュリティの抽象化

先に示した様に，機能安全では，アイテム定義→ハザード・リスク評価→機能安全コンセプト導出→技術安全要求導出→システム設計と段階が進むにつれて，対象機能が詳細化され，それぞれの必用に対して安全機能が割り振られる．一方，セキュリティでは，データフローダイヤグラムによる抽象モデルの作成後，エントリーポイント，アタックサーフェスの決定，Where,Who,When,Why,What による網羅的な脅威の抽出と，対応すべき脅威の特定がおこなわれる．この手法の相違により，安全要件や安全機能と，セキュリティ要件，セキュリティ機能との対応を取る事が複雑になる．

4. 提案手法

本論文では，機能安全とセキュリティの関係を統合するモデルを設定する．機能安全とセキュリティ機能の関係は，要件定義/設計の各段階にモデルを当てはめて定義する．次に，各段階で利用可能な情報を元に導出されるべき要件や脅威の粒度を定義する．この粒度は相互参照が可能なものに規定する．

(1) 機能安全・セキュリティ統合モデル

機能安全機構は図　のようにモデル化できる．制御機能(controller)は車両本体のセンサー類や他の ECU，運転車などからと情報を交換して通常動作している．しかし，故障モードに陥った場合には，機能安全機構に制御を行い，安全状態に移行する．もし機能安全機構で対処出来ない場合には，他の手段，たとえばエンジンが停止しない場合，Kill スイッチでエンジンを強制停止させるなどの手段をとる．

機能安全機能とセキュリティ機能を両立させるため，機能安全＆セキュリティ機能の関係をモデル化する．

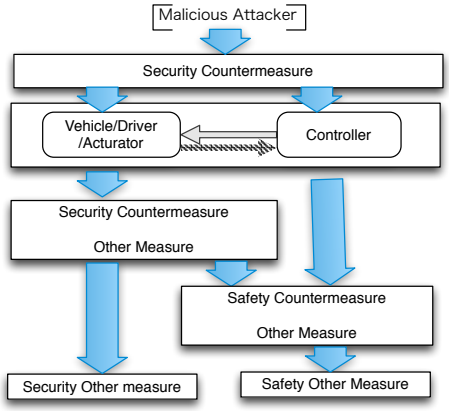

図 4　機能安全&セキュリティ機能動作モデル

このモデルでは，攻撃者の攻撃は，まず本来機能を保護するセキュリティ機能が対応する．このセキュリティ対応機能は，発生した攻撃の種類に応じて機能安全機能の処理もしくは，内部のセキュリティ機能の処理を起動する．さらに内部のセキュリティ機能は，処理の内容に応じて，機能安全機能もしくは他のセキュリティ機能の処理を起動する．安全機能とセキュリティ機能は分離され，機能安全のインターフェイスを通じて関係する．

このモデルは次の利点がある．

- 安全機能とセキュリティ機能の関係を単純化(第 4 節，問題(1))．表などの形式で，機能対応が確認出来る．
- 安全機能とセキュリティ機能の粒度の対応を取る必用から，脅威やリスクの粒度が統一される(第 4 節，問題(2)(3))．

以下，本論文では，この動作モデルに基づき，機能安全とセキュリティ機能の要件定義/設計を次の手順で進める．

4.1 アイテム定義

機能の対応を取る必要上，アイテムの定義は，機能安全とセキュリティの要件定義/設計で同じものを利用する．ただし，エントリーポイント，アタックサーフェスが必ずしもアイテムに上記のものが含まれていない．そのため，データフロー作成の際に，通信路を明示的に示す記法を取る．

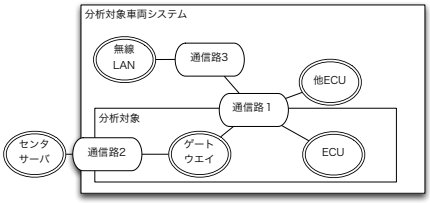

図 5　セキュリティ用 DFD 改

Vol.2017-ARC-225 No.13
Vol.2017-SLDM-179 No.13
Vol.2017-EMB-44 No.13
2017/3/9

4.2 機能安全共存セキュリティ脅威分析とリスク評価

機能安全では，アイテム定義の後，ハザードを導出し，それと発生状況に対応する過酷度，発生頻度，回避可能性を定め ASIL を導出した．セキュリティの脅威分析，リスク評価は多段階でおこなう．初めに，抽象度の高い脅威，改ざん，破壊，盗聴の 3 つによる機能安全ハザードとの対応付けを確認する．

次に，機能安全コンセプトに対応する要件（機能セキュリティ要件）の導出にさいして，先の抽象度の高い 3 つの脅威にたいして具体性の増した脅威，たとえば STRIDE 手法[4][5]の(1)Spoofing(なりすまし)，(2)Tampering(改ざん)，(3)Repudiation(否認), (4)Information Disclosure(情報漏えい), (5)Denial of Service(サービス拒否)，(6)Elevation of Privilege(特権の昇格)に対応づける．さらに技術安全要件またはシステム設計に対応する要件/設計（技術セキュリティ要件またはセキュリティシステム設計）では，脅威分析の手法を用いて STRIDE の要因となる脅威を抽出し，エントリーポイント/アタックサーフェスを考慮して CRSS や RSMA を用いてリスク評価を実施する．

この CRSS や RSMA を実施した後にリスク対応をきめる閾値や，これらで利用されるパラメータ値は過酷度と回避可能性が判明している機能安全の ASIL 決定時におこなう．

最後に，セキュリティシステム設計を，攻撃からの直接防御，内部の安全機能，セキュリティ機能の通知と処理の観点から実施する．

4.3 機能安全機能とセキュリティ機能の関連づけ

機能安全機能とセキュリティ機能の関連づけ方法を示す．まず，アイテム定義段階では，機能安全で定義したアイテムに通信路情報を追加する．すなわち，通信路情報のみが追加情報として扱われ，その他は共通である．

ハザード分析およびリスク評価では，ハザードを引き起こす要因としてエレメント毎に割り当てられた原因事象が，それぞれエレメントまたは通信路上の改ざん，破壊，盗聴に対応づける．

機能安全コンセプトレベルでは，3 つのセキュリティ脅威が STRIDE に分割/詳細される一方，ハザード原因に対する機能安全要求が導出される．この段階では，機能安全要求（コンセプト）と STRIDE で表記された脅威が対応づけられる．

機能安全要件/システム設計レベルでは，具体化されたシステム設計を元に脅威分析およびリスクアセスメントを実施する．このときには，各セキュリティ脅威と機能安全機能および技術セキュリティ要件/機能が対応する

5. 仮想的な開発ターゲットへの適用

4 章で提案した要件定義/設計手法を検証するために，ここでは仮想的な開発ターゲットを定義し，提案手法の検証をおこなう．ハンドルと操舵装置の間を車載 LAN で接続した Fly-by-Wire 方式の操舵装置を例として検討する．

5.1 アイテム定義

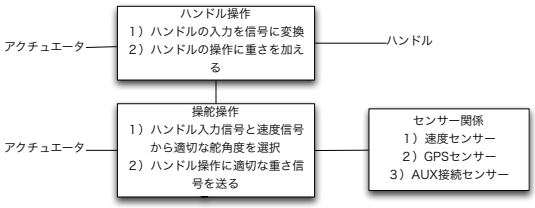

図 1　対象システムアイテム図(左二つ)

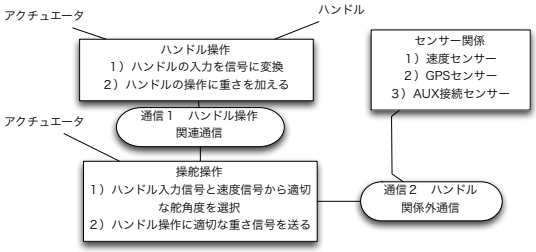

図 6　セキュリティ対応対象システム DFD 改

ここでは，ハンドル操作機能と操舵機能は通信 1 の専用線通信で結ばれているが，速度は通信 2 のハンドル関係外通信から得られる．また，通信 2 には，エントリポイントとなる速度以外のセンサーもあることが情報として記載されている．

また，物理的な制約条件として，操舵機能とハンドルは離れた場所に設置されるため，通信 1 をおこなう通信路は数メートルの長さで，物理攻撃の対象となる．また操舵部分は物理的に隔離された位置にあり交換は操舵システム全体で，エレメントへの直接接触は困難である．同様に，ハンドル操作部もハンドルと一体形成されており，エレメントへの直接接触は困難であるとする．

5.2 アイテム定義段階での脅威分析

次に，機能安全側のハザード分析，リスク評価に対応するセキュリティ側での作業をおこなう．上のシステムで想定されるハザードは，1)ハンドル操作に重みを加えすぎた結果のハンドル固着，2)操舵側で操舵トルクが 0 もしくは最大で動かなくなる操舵固着，3)ハンドルと操舵が連動しなくなる．4)速度に対応するハンドル重さにならない，の 4 つが導出されたと想定する．この場合の FTA の結果によるエレメントへの原因割り付け，およびセキュリティ脅威の割り付けを，４)に限定して，脅威要因の FMEA 実施後に対応を表 11 に示す(通信路切断などのハード要因は除く).

表 7 ハザード/ハザード要因と脅威対応

	ハザード要因	ハンドル操作	通信路	操舵
速度に対応するハンドル重さにならない	通信２が異常/エラー多発		改ざん 破壊	
	送出された信号が不正．異常動作			改ざん

なお，この段階で，ハンドル重さと速度と連動しない場

Vol.2017-ARC-225 No.13
Vol.2017-SLDM-179 No.13
Vol.2017-EMB-44 No.13
2017/3/9

合の過酷度と回避可能性は機能安全側で定められている．連動しなくなった場合の回避可能はあるため，重大事故が発生する可能性はさほど高くないと仮定すると，セキュリティ攻撃の阻止はある程度の実現可能性に対しても実施すればよい．たとえば CRSS 分析を実施した場合，低い CRSS スコアの脅威は対応が不必要となるよう閾値を指定できる．

5.3 機能安全コンセプト相当段階セキュリティ作業

機能安全コンセプト相当段階では，ハザード要因に対して適切な機能安全コンセプトが導出されている．それに対応して脅威を割り付ける．

表 8　機能安全コンセプトと脅威

安全目標	ハンドル重さと速度を連動させる	セキュリティ脅威
機能安全要求 1	通信 2 のエラーが多い場合には，操舵操作から出す重さ信号を最大に設定する．	通信路（改ざん・破壊）
理由	高速走行中に大きなハンドルを切ると事故につながりやすい．低速走行時にハンドルが重くなった場合でも，事故は起こりにくい．また運転手の気づきにより修理工場へ行くことが促される．	
エラーの検出	通信 2 の状態を直接監視機能に入力する	
異常の検出	通信路の異常を検出する	
重さ信号オーバライド	監視機能から重さ信号出力をオーバライドする	

5.4 技術安全要求/システム設計相当段階

技術安全要求仕様相当段階では，機能安全コンセプトにたいしてその実装要求(技術安全要求)が導出されている．ここで，セキュリティ脅威を詳細化する．

表 9　技術安全コンセプトと脅威

安全目標	ハンドルと速度を連動させる		セキュリティ脅威
機能安全要求 1	通信 2 のエラーが多い場合には，操舵操作から出す重さ信号を最大に設定する．		通信路(改ざん・破壊) → 上記に該当する STRIDE 事象 DoS 攻撃 成りすまし 改ざん
技術安全要求	単位時間当たりの通信 2 のエラー通信数を取得することで通信エラーを判定し，閾値を超えたときにハンドル重さを最大とする．		
エラーの検出	通信エラー率を取得する I/F を設置する	通信機能	
異常の検出	不正エラー率を定める．それを越えるエラーでオーバライド処理を起動	監視機能	
重さ信号オーバライド	正規の出力の停止 I/F	通常機能	
	重さ信号送出機能	監視機能	

次に，STRIDE で相当する脅威の内容を検討する．

表 10　STRIDE の脅威内容

STRIDE	脅威要因
成りすまし	偽の速度情報通信を通信路 2 に接続されているエレメントから送出する⇒正規信号と偽信号の混在
改ざん	通信路 2 に接続されているデバイスで速度情報通信をエラー化する⇒エラーの増大
DoS	通信路 2 を Flooding により麻痺させる．⇒エラーは発生しにくいため正規情報が入ってこない

この 3 つの要因のうち，改ざんに関しては，技術安全コンセプトの要求で対応可能である．しかし，成りすましと DoS 攻撃に対しては，対処出来ていない． この 2 つの事象に対して，さらにシステム設計以降の詳細な情報がえられた段階で，さらに詳細な脅威の分析をおこなう．たとえば，CRSS などによるリスクスコアリングと，6.2 で指定される，リスクスコアの閾値を用いてリスク対応必用な脅威を選択し，対処を定める．

6. 関連研究・標準

自動車におけるセキュリティ機能開発に関連する標準の提案は幾つか提案されている．この中で，明示的に機能安全開発とセキュリティ開発の関連性について述べているのは，J3061 である．しかし，概念的な説明にとどまり，方式や統合モデルの提案には至っていない．

また，研究レベルでは，セキュリティ脅威を一種の機能故障モードと見なし，ASIL を調整する方式も提案されている[5]．しかし，セキュリティ脅威が必ずしも故障モードに該当する保証はなく，また，例え，低レベルの ASIL で合っても，暗号関連機能を利用する場合，鍵の漏えいなどに対して強固なセキュリティが必用とされる場合が想定される．そのため，セキュリティリスクが増大，もしくはそれを見直した場合，低 ASIL のエレメントに対して過大な開発コストを科す結果をもたらす可能性がある．

また，リスク評価に関して，機能安全でのハザードの過酷度と回避可能性のみを使い，技術要件もしくはシステム設計段階以降での，システムに対する脅威にたいする CRSS 等のリスク評価値で対処を定める．そのため，上流の要件定義者は下流の技術詳細を知ることなく対応レベルの指示が可能となる．

7. まとめ

本論文では，安全機能とセキュリティ機能の要件定義・設計の手法を検討，提案した． 今後，より詳細な仮想開発ターゲット上での検討を実施し，実用性の検討や方式の改良を実施したい．

参考文献

[1] ISO 26262：2011. Road vehicles － Functional Safety －
[2] SAE J3061：2016. Surface Vehicle Recommended Practice
[3] 公益社団法人自動車技術会:JASO テクニカルペーパ 自動車-情報セキュリティ分析 ガイド, JASO TP15002, 2015.
[4] Shostack,A. threat modeling. Wiley, 2014
[5] G. Macher, H. Sporer, R. Berlach, E. Armengaud and C. Kreiner, “SAHARA: a Security-Aware Hazard and Risk Analysis Method,” in DATE, 2015.