講演９．陸上交通のシステム開発における ライフサイクルとセキュリティ

鉄道認証室　　※森 崇　　吉永 純

１．はじめに

近年陸上交通においても、安全性を中心にしたライフサイクル管理の標準だけではなく、セキュリティに関する標準も整備されつつある。サイバーセキュリティに関する標準としては、産業用オートメーション及び制御システム(IACS：Industrial Automation and Control System)全般を対象としたセキュリティ標準 IEC 62443 (Industrial communication networks – Network and system security)が着目され、鉄道においてもシステムとこの標準との整合性が問われつつある現状となってきている。

しかしながら、IEC 62443 は、項目が多岐にわたり、分冊も多く、標準を今後活用していこうとするユーザーにとっては決してわかりやすいとは言えず、その複雑さが障壁となっている。このため、鉄道においては、IEC 62443 を鉄道に活用した場合、開発・設計の特定のタイミングで具体的に何をすべきかをある程度具体化した CLC/TS 50701 が発行され、活用が見込まれている。

また自動車においても、ISO/SAE 21434 が発行されている。

本稿では、鉄道及び自動車で使用されているライフサイクルモデルを元に、機能安全についてある程度知識がある方が、サイバーセキュリティについて検討する際に、特徴的な点や、注意した方がよい点を記述する。

２．ライフサイクルモデル

鉄道において、機能安全や、システム全体の安全性と経済性のバランスを考える際に参照するライフサイクルは、一般的に RAMS (Reliability, Availability, Maintainability and Safety)ライフサイクルといわれるいくつかの段階が定義されている。RAMS ライフサイクルモデルには IEC 62278 と、EN 50126 に定義されているものがあり、このライフサイクルモデルに沿った設計・製作・試験・運用がシステム発注者によって求められる場合が増加している。この 2 つのライフサイクルモデルの違いは、Operation and Maintenance 以降の段階の区分にあり、開発・製作段階において大きな差異はない。

自動車においても、ISO/SAE 21434 は、E/E(Electric and Electronics)における安全ライフサイクルの行為を規定した機能安全標準である ISO 26262 のライフサイクルに沿った要求を定義している[1]。これらから分かるように、鉄道においても、自動車においても、既存のライフサイクルモデルに、サイバーセキュリティの観点を加え、既存のモデルを活用できるように工夫されているものである。

図 1 に CLC/TS 50701 の参照モデルとなっている EN 50126 [2]のライフサイクルモデル、及び図 2 に ISO/SAE 21434 の参照モデルである ISO 26262[3]のモデルを示す。

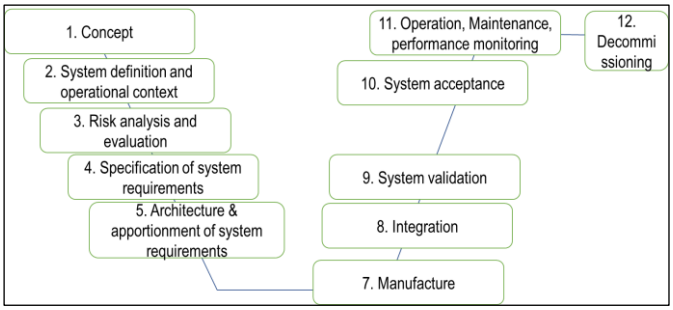

図 1 EN 50126 のライフサイクルモデル

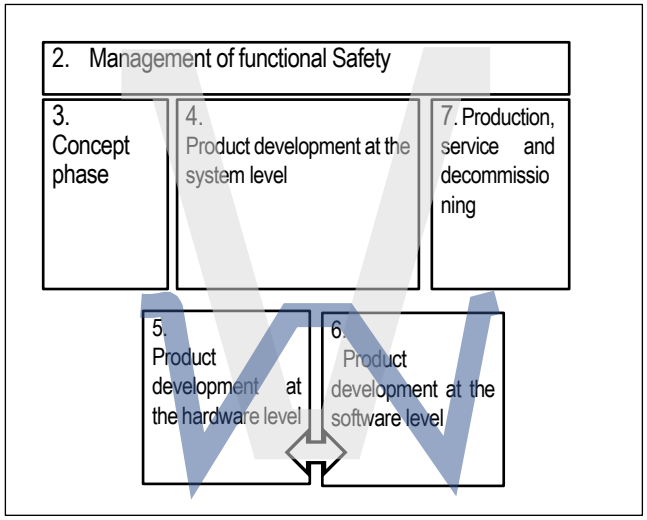

図 2 ISO 26262 ライフサイクルモデル

これらのライフサイクルモデルは、コンセプトをブレークダウンし、システムの設計・製作を行うとともに、そのブレークダウンの粒度と相当する試験を確実に実施する管理体制を構築し、機能安全の構築や安全と経済性のバランスをとることを目的としている。これは機能安全を「サイバーセキュリティ」に置き換えても成り立つ。このライフサイクルモデルを活用し、サイバーセキュリティの対処をどうするかを考えるのは前述のように今までの思想の延長線上にあると言える。

3．機能安全とサイバーセキュリティの対処の差異

機能安全もサイバーセキュリティも人命を毀損する恐れがあるという点では同じであるが、機能安全はシステムの不具合から人を守り、サイバーセキュリティ対策は、外部からの攻撃に対してシステムを守る相互補完的な関係にあると CLC/TS 50701 は述べている。

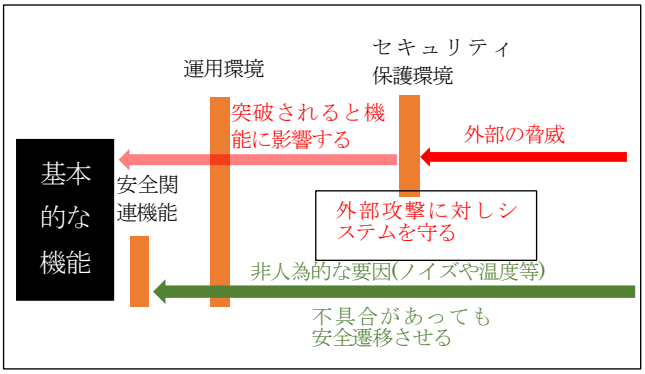

図 3　機能安全とサイバーセキュリティ防護の基本的な考え方

図 3 に基本的な機能安全対処とサイバーセキュリティの対処を示す。

サイバーセキュリティの外部脅威に対しては、まずセキュリティ保護環境(Security-protected Environment)を設け、この層で外部攻撃を無効化する。外部攻撃に対し、リスクの低減がセキュリティ保護環境において十分ではない場合、脆弱性(Vulnerability)となる[4]。脆弱性があってもそれは直ちにシステムの機能に影響を与えるかどうかは一概には言えず、運用環境(ネットワークがどの程度脅威にさらされているかなど)にも大きく依存する。

一方、機能安全については、偶発故障(Random fault)によるものは、サイバーセキュリティの運用環境とは観点が大きく異なるが、ノイズ、温度、湿度など運用環境に依存し、偶発故障が起こったとしても、安全に状態が遷移するように、安全要求機能を設定し、故障時安全側遷移をするフェールセーフ性を確保することにより対処を行っている。

以下に、各段階における対処の差異を述べる。図 4 に EN 50126 のライフサイクルモデルと、そのライフサイクル段階で CLC/TS 50701 に要求されているサイバーセキュリティにおいての項目を示している。

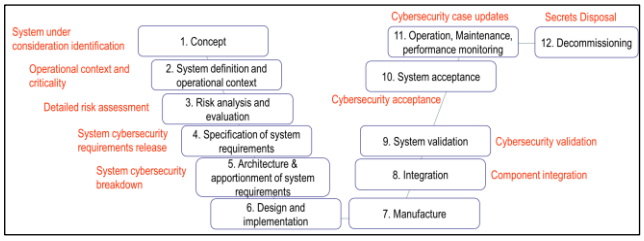

図 4 EN 50126 RAMS ライフサイクルとサイバーセキュリティ要求項目

3．1．コンセプト

システムのコンセプトを確立する際、システムの範囲、目的、ユーザーのシステムにおける考え方を明らかにしていく。この際に安全に関する基本的な考え方を明確にしていく。安全に対する基本的な考え方において、機能安全の場合、ライフサイクル全体で装置の故障が発生しても、許容範囲を超えない頻度で安全側に遷移するフェールセーフ思想でシステムを構築する[5]。しかしながら、サイバーセキュリティへの対処

については、相手のレベルアップや予期しない脆弱性の発見などの対処が出来るようにシステムの準備をしておくことが求められる[6]。言い換えると、機能安全については事前対処、サイバーセキュリティについては機能安全の事前対処に加え、将来対応できるような準備をコンセプトとして考えておく必要がある。

この対処について、鉄道においては、サイバーセキュリティに対する対処と、安全関連系の防御は切り離して考えることが一般的である。

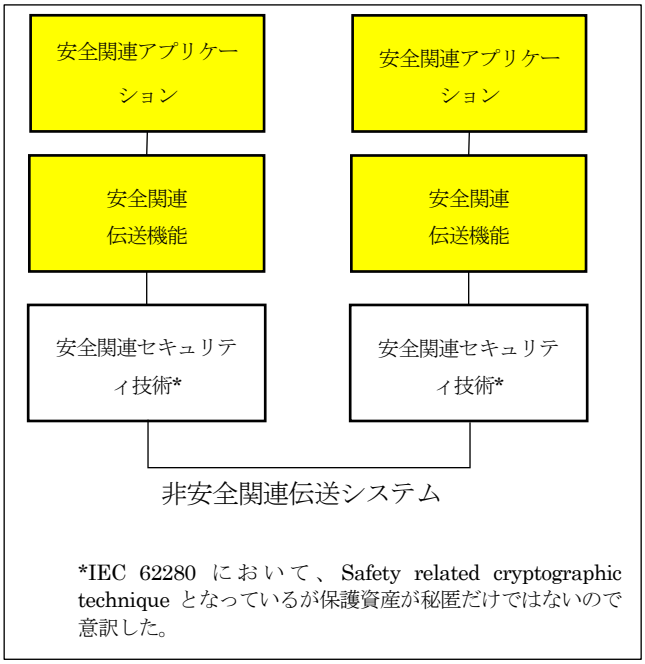

図 5 IEC 62280 における伝送参照モデル
（黄色の部分を安全関連系として管理することが要求されている）

図 5 に IEC 62280:2014 (Railway applications – Communication, signalling and processing systems –Safety related communication in transmission systems)に示されている伝送参照モデルを示した。そのモデルの中で、黄色で示されている部分は、安全関連系として(機能安全として)扱うこととして示されている。人為的ではない機能安全を阻害する伝送エラーについては、安全関連伝送機能により、機能安全の実現として対処を行うこととなっている。これは、ノイズによって引き起こされる、ランダムエラーやバーストエラーの対処であり、システムの改修や環境条件の変化がない限り、ライフサイクル全体によってそれほど変化するものではない。また、前提とするエラーの特性に十分な対応能力を持つ、CRC 検定をはじめとするメッセージダイジェスト符号で誤りの検出を行うことが一般的であり、その符号の符号化と復号化は、安全関連系のハードウェア、ソフトウェアとそれに適した技術と管理手法で行う。

一方、サイバーセキュリティへの対応は、「安全関連セキュリティ技術」で行い、これは機能安全による対応は必ずしも求められていない。

自動車においても、ISO/SAE 21434 によると、機能安全の人的な役割・責任のプロセスをサイバーセキュリティの力量などに含むことができ、機能安全とサイバーセキュリティの要求の矛盾を解消することが求められているが、セキュリティ技術の実装に機能安全は求められていない。

これは、セキュリティ技術については、世の中の技術をそのまま導入することのメリットが、自ら製作者が作ることよりも大きいことや、対応の迅速性が求められることなどから、現実的な解法としてこのような規定になっていると考えられる。

また、鉄道においては、サイバーセキュリティのアイテムの設計・製作自体が定義されておらず、自らサイバーセキュリティに関連するアイテムを製作することが、標準上想定されていないことにも留意する必要がある。

３．２．リスク解析

機能安全について、一般的に考えられるのは、許容される THR(Tolerable Hazard Rate)を設定し、機能分析し、機能ごとに TFFR(Tolerable Functional Failure Rate)を決定し、受容できるリスクを機能ごとに設定する方法である。また、この受容可能リスクの厳しさに整合するよう SIL(Safety Integrity Level)を設定し、採用する品質管理及び技術的手段を決定する。この際、部品の故障など、確率論的なアプローチで対処できるものにおいては、どのような対策を行えば受容できるレベルまでリスクを低減できるかの解析方法の一つとして、FTA(Fault Tree Analysis)を採用することが一般的である。

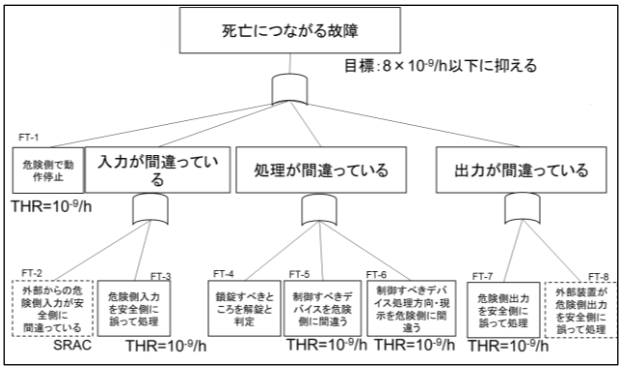

図 6 FTA 解析のイメージ

対してサイバーセキュリティにおいては、「どの程度脅威にさらされているのか(誰でもアクセスできるか、システムが専用機器室に収容されているか、インターネット接続か、専用線かなど)」「脆弱性のレベルとアタッカーの実力」など、環境条件が大きなファクターとなり、確率的なアプローチでは解析できないと考えられる。このため、攻撃の容易さを指標として解析を行う、「アタックツリー解析」が ISO/SAE 21434 で定められており、有効であると考えられる。

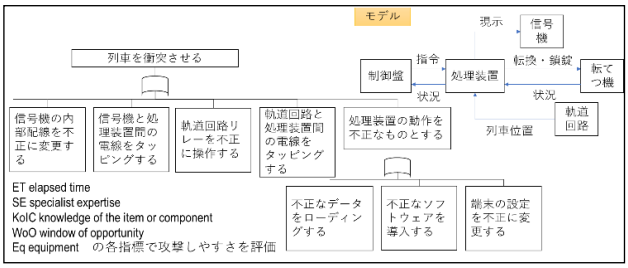

図 7 アタックツリーのイメージ

アタックツリーなどの解析をもとに、SL(Security Level)という概念を導入することが IEC 62443 に規定されている。各機能において、サイバーセキュリティ上求めるレベルである SL-T(Target)を設定し、技術的対応とその能力である SL-C(Capability)を選択し、SL-C の選択後、どのレベルまで到達したかを評価する SL-A(Achieved)を同定し、SL-T の求めるレベルまで到達したかを評価する。

自動車においても、cybersecurity assurance level (CAL)というレベルにおいて評価する方法が述べられている[7]。しかしながら、基本的にはライフサイクル全体を継続的に評価することについては、攻撃者の能力が向上することや、脆弱性の発見など変化があることに留意する必要がある。

３．３．運用とメンテナンス

鉄道における機能安全については、運用とメンテナンスについては FRACAS(Failure Reporting Analysis and Corrective Action System)を用い、情報分析を行い、PDCA を回すことになっているが、それほど重視されているわけではない。しかしながら、自動車においては、不特定多数が占有される動産として扱われることから、制御システムを解析することが、鉄道に比べて容易であり、鉄道のサイバーセキュリティ対策と比べても、情報収集とトリアージに重点が置かれていることが特徴的である。

４．おわりに

本報告では、鉄道と自動車の標準を双方参照し、ライフサイクル管理における機能安全とサイバーセキュリティにおける取り組みの差異のうち、注意すべき点を示した。今後とも陸上交通に関する機能安全及びサイバーセキュリティ標準に着目し、皆様から信頼される鉄道認証業務を遂行して参りたい。

参考文献

1) INTERNATIONAL STANDARD ISO/SAE 21434:2021, Figure 1 - Overview of this document”
2) EUROPEAN STANDARD EN 50126:2017, 6.2 Life cycle for the system under consideration
3) INTERNATIONAL STANDARD ISO 26262-2:2018-“5.2.1 Overview of the safety lifecycle”
4) TECHNICAL SPESIFICATION CLC/TS 50701:2021, Annex D Safety and Security
5) INTERNATIONAL STANDARD IEC 62278:2002, 4.8 Fail-safe concept
6) TECHNICAL SPESIFICATION CLC/TS 50701:2021, 5.3 Activities, synchronization and deliverables
7) INTERNATIONAL STANDARD ISO/SAE 21434:2021, Annex E Cybersecurity assurance levels