ISO/SAE 21434：自動車サイバーセキュリティのソフトウェア認証

EDN edn.com/iso-sae-21434-software-certification-for-automotive-cybersecurity/

Mark Pitchford

2022 年 8 月 8 日

Mark Pitchford has over 30 years' experience in software development for engineering applications. He has worked on many significant industrial and commercial projects in development and management, both in the UK and internationally. Since 2001, he has worked with development teams looking to achieve compliant software development in safety- and security-critical environments, working with standards such as DO-178, IEC 61508, ISO 26262, IIRA, and RAMI 4.0. Mark earned his Bachelor of Science degree at Trent University, Nottingham, and he has been a Chartered Engineer for over 20 years. He now works as Technical Specialist with LDRA Software Technology.

車載組込みアプリケーションは、従来、他から分離したもので、静的、固定の機能、かつデバイスに固有の実装であり、開発手法やプロセスもその状況に依存してきました。しかし現在、コネクティビティの需要が爆発的に増加したことで、エンターテイメントシステムなどクリティカルでないシステムが、ステアリングやブレーキ、制御システムと同じ通信インフラを共有するようになりました。こういった変化は、サイバー攻撃に起因する安全性や経済的リスクの可能性をもたらしていますが、自動車業界の開発者向けの標準ガイダンスはそれに追いつくのに苦労しています。

ISO 26262「路上走行車－機能安全」規格は、自動車メーカーが開発ライフサイクル全体を通じて機能安全のベストプラクティスを採用する方法を提供するため、2012 年に発行されました。ISO 26262 では、機能安全に対するあらゆる脅威に適切に対処することが求められています。そこにはセキュリティ上の脅威に関するものも暗黙に含まれていますが、サイバーセキュリティに関する明確なガイダンスは示されていません。ISO 26262 の発行時点でそのことは、おそらく予期されていました。

しかし、業界の変化は速く、4 年後の発行時までに SAE J3061 Cybersecurity Guidebook For Cyber-Physical Vehicle Systems が大いに期待されることになりました。しかし、SAE J3061 はこの問題に広く対処するためのより公式の規格を開発するまでの時間かせぎとなる一時的なものでしたので、SAE J3061 は 2021 年に ISO/SAE 21434:2021 に取って代わられたのです。

ISO/SAE 21434 は ISO 26262 を補完するものと考えられ、ISO 26262 が機能安全に対応するためのプラクティスに関するガイダンスを提供するように、サイバーセキュリティの観点から開発のベストプラクティスに関するガイダンスを提供します。同じ時期に、国連欧州経済委員会（UNECE）の自動車規準調和世界フォーラム（WP.29）で、サイバーセキュリティ管理システム（CSMS）の新しい UNECE WP.29 規則 R155 が採択され、2022 年 6 月から自動車の型式認承への準拠が義務づけられることになりました。R155 では、サイバーセキュリティスキルに適合した参考文献として ISO/SAE 21434 が引用されています。

では、ISO/SAE 21434 は自動車開発チームにとってどのような意味を持つのでしょうか。この記事シリーズの第一部（本記事）で、自動車開発者のための進化する規格の詳細と影響について説明します。第二部では、従来の開発での V モデルのステップを順に見て、規格で概説されている原則が各段階でどのように適用されるか説明します。

機会を逸したのか、柔軟性が向上したのか?

ISO/SAE 21434 は J3061 に取って代わるものですが、この 2 つの文書はスタイルが異なっています。SAE J3061 ではセキュリティと安全性のプロセスを互いに関連づけるのに対し、ISO/SAE 21434 ではそれらを分離します。この違いにもかかわらず、ISO 26262 は ISO/SAE 21434 と密接な関係を保っており、繰り返し ISO/SAE 21434 で参照されています。

しかし、多くの人が ISO/SAE 21434 は機会を逸したと見ています。

ページ数を比較するだけでその理由がわかります。ISO 26262 は 12 のパートから成り、その多くが、準拠するアプリケーションソフトウェアの開発方法に直接影響を与えるものです。「ソフトウェアレベルでの製品開発」と題されたパート 6 だけでも 66 ページにも及びます。一方、ISO/SAE 21434 は全体が 81 ページで、そのスコープはサプライチェーン全体を通じて、路上走行車の電気・電子システムのあらゆる側面に及んでいます。

開発者は、機能安全の観点からは ISO 26262 で、サイバーセキュリティの観点からは ISO/SAE 21434 で、達成すべきことの詳細を発見すると期待できます。ただし、ISO 26262 では、その目的を達成するための具体的な方法の詳細も示されているのに対して、ISO/SAE 21434 ではそのようにはなっていません。

その目的を達成するための詳細なガイダンスが与えられていないので、ソフトウェアの観点からは ISO/SAE 21434 は、この規格が置き換えるドキュメントを承認する以上のものではありません。しかし、ISO/SAE 21434（とそれ以前の SAE J3061）は、ソフトウェア開発者が達成すべき価値ある一連の目標を提示しています。楽観的な見方をすれば、詳細が不明であることは、その達成方法について柔軟性があると言えます。

機能安全を超えて

ISO/SAE 21434 と ISO 26262 の間には明らかな相乗効果がありますが、ISO/SAE 21434 は機能安全要件にセキュリティの考慮事項を含める必要性を公式にするだけではないことに気づくことが重要です。これらの要件の定義において、悪意が重要であることを過小評価してはなりません。

それほど明らかではありませんが、ISO 26262 のような公式の開発プロセスにサイバーセキュリティを導入することは、セーフティクリティカルではないアプリケーションでも、そしておそらくこれまではそれを適用する義務のなかった組織でも、同様の厳密な技術を使用することを意味しています。ISO/SAE 21434 は、プライバシー全般、そして特に個人を特定できる情報（PII）について説明し、両者に対するリスクが安全システムの潜在的な危険に劣らず重要であると強調しています。

実際の問題として、個人の連絡先やブラウザや位置情報の履歴、クレジットカード他の金融情報など、コネクテッドカーを経由してアクセスできる個人情報の保護には、今や ISO 26262 並みの厳密さが求められています。

ISO 26262、HARA、ASIL

ISO 26262:3 で要求されるハザード分析およびリスクアセスメント（HARA）は、ハザードにつながる可能性のある誤動作の特定、ハザードに関連するリスクの評価、そして安全目標の策定に使用されます。その結果導き出される自動車安全水準 ASIL（Automotive Safety Integrity Level）は、ISO 26262 で定義された開発プロセスにおける重要な概念です。ASIL は開発者が危険事象を防ぐために相応するレベルの努力を払えるように設計されています。

危険事象には、重大度による分類（S0～S3）、曝露確率による分類（E0～E4）、制御可能性による分類（C0～C3）が設定されています。数値が高いほど、それぞれのケースで最も望ましくない特性を表します。危害の可能性は、これら要因の組み合わせであり、それが割当てられた ASIL に反映されます。

ISO 26262 では、重大度だけでなく ASIL にも取り組みのレベルを比例させることが求められています。たとえ生命を脅かすような危険事象であっても、それが起こる可能性が極めて低い場合には、その予防に多額の投資を行う必要はありません。

Methods		ASIL			
		A	B	C	D
1a	Requirement-based test	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test	+	+	++	++
1d	Resource usage test	++	++	++	++
1e	Back-to-back test between code and model, if applicable	+	+	++	++
1f	Verification of the control flow and data flow	+	+	++	++
1g	Static code analysis	+	++	++	++
1h	Static code analysis based on abstract interpretation	++	++	++	++

"++" The method is highly recommended for this ASIL.

"+" The method is recommended for this ASIL.

"o" The method has no recommendation for or against its usage for this ASIL.

表 1 「ソフトウェア統合の検証方法」は、このように ISO 26262-6:2018 の表 10 に規定されています
出典：LDRA

ISO/SAE 21434、TARA、そして?

ISO/IEC 21434 で提案された脅威エージェントリスク評価 TARA（Threat Agent Risk Assessment）は、ISO 26262 の HARA に似ています。TARA は、サイバーセキュリティリスクの特定・評価・優先順位付け・管理を支援する脅威ベースの方法論です。これは、緩和制御と許容されるリスクレベルを考慮して、最も重要な曝露を決定する実用的な方法です。

「リスク値」の計算は、以下のような要因に依存して、重大度と攻撃が成功する可能性を考慮するという点で、ASIL の計算と似ています。

- 脅威シナリオの特定

- インパクト
- 攻撃経路
- その経路に対する攻撃の実現可能性

安全上の損傷に関する「インパクト水準」は ISO 26262 の定義を引用しています。ISO 26262 の ASIL 水準を確認するために使用されるものと同じインパクト尺度が使用されます。この原則は、財務上の損害や運用上の損害、プライバシーの損害を引き起こす可能性のある脅威に対処できるよう ISO/SAE 21434 で拡張されました。

Impact rating / **Damage category**	Severe	Major	Moderate	Negligible
Safety Criteria used by ISO/SAE 21434 are taken from ISO 26262-3:2018	S3: Life-threatening injuries, fatal injuries	S2: Severe and life-threatening injuries (survival probable)	S1: Light and moderate injuries	S0: No injuries
Financial impact	Catastrophic consequences which might not be overcome	Substantial consequences which can be overcome.	Inconvenient consequences, overcome with limited resources	No effect, negligible consequences or is irrelevant
Operational	Loss or impairment of a core vehicle function	Loss or impairment of an important vehicle function.	Partial degradation of a vehicle function.	No perceivable impairment of a vehicle function
Privacy	Significant or even irreversible impact to the road user	Serious impact to the road user	Inconvenient consequences to the road user	Negligible consequences to the road user

表 2　インパクト水準の概略説明は、ISO/SAE 21434 の表 F.1～F.4 を引用したものです
出典：LDRA

ISO/SAE 21434 は、セーフティクリティカルでない分野にも公式の開発をもたらすだけでなく、その開発範囲を従来のプロジェクト開発ライフサイクルをはるかに超えて拡張しています。たとえば、現場で明らかになった脆弱性に対処するためのインシデント対応プロセスの確立、無線（OTA）更新の考慮、車両所有者の変更時のサイバーセキュリティへの考慮などがあります。

ASIL 等価を求める

ISO/SAE 21434 は ISO 26262 HARA と比較して、取るべき TARA アプローチについて、より規範的ではありません。さらに重要なことに、ASIL と等価なものを定義するには至っていません。ISO 26262 とは異なり、ISO/SAE 21434 では確認と検証の労力のレベルを開発中のソフトウェアの重要度に対応させてはいません。

しかし、これらの評価は、ISO 26262 で示される ASIL の分類に対応させるのに役立ちます。

表 3 は、表 1 にリスク値（計算法に依存する数値）を重ね合わせたものです。これが、安全性クリティカルな場合のベストプラクティスを表しているのであれば、他の特性でクリティカルなアプリケーションであっても、同じアプローチが同等に適切であるとするのが論理的です。

Methods		ASIL			
		A	B	C	D
		ISO/SAE 21434 risk value			
		Low	Moderate	High	Very high
1a	Requirement-based test	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test	+	+	++	++
1d	Resource usage test	++	++	++	++
1e	Back-to-back test between code and model, if applicable	+	+	++	++
1f	Verification of the control flow and data flow	+	+	++	++
1g	Static code analysis	+	++	++	++
1h	Static code analysis based on abstract interpretation	++	++	++	++
"++" The method is highly recommended for this ASIL. "+" The method is recommended for this ASIL. "o" The method has no recommendation for or against its usage for this ASIL.					

表 3　ISO/SAE 21434 の重大度によるグループ分けを ISO 26262-6:2018 の表 10 で規定される「ソフトウェア統合の検証方法」に重ね合わせたもの　出典：LDRA

ISO/SAE 21434 サイバーセキュリティと ISO 26262 の連動

SAE J3061 は、その開発プロセスを明示的に ISO 26262 の開発プロセスに結びつけました。ISO/SAE 21434 は、それほど緊密な結びつきではありませんが ISO 26262 を繰り返し参照しており、両方の規格が適用されるケースが多いでしょう。実際、これらの規格は、製品ライフサイクルの各段階で両者を統合するのに適しており、同じテストチームを配備して両方の役割を果たすようにできる程です。

たとえば、ハザード分析、安全リスク評価、脅威分析、そしてセキュリティリスク評価を一つの統合されたテンプレートと手法で同時に実施できます。

安全性が考慮されない場合でも、ISO/SAE 21434 の高レベルな要求に対応するために実績のある ISO 26262 のベストプラクティスを採用することは、開発チームがすでに利用しているであろう既知のツールや技法を適用できる実用的なアプローチです。

編集者注：自動車のサイバーセキュリティに関するこの記事シリーズの第二部では、修正 V モデルのアプローチでソフトウェア開発に最も影響を与える ISO/SAE 21434 のセクション間の関係を示し、規格で概説された原則がどのように適用できるかをより詳細に説明しています。

Mark Pitchford は LDRA Software Technology のテクニカルスペシャリストで、DO-178、IEC 61508、ISO 26262、IIRA、RAMI 4.0 などの規格に取り組みながら、安全性とセキュリティクリティカル環境においてコンプライアンスに則ったソフトウェア開発を目指す開発チームと協力してきました。