LDRAcoverage
LDRA news from the world of testing
Issue 24 Winter 2019

LDRAツールスイートで改善し続ける Critical Software 社

クライアント

1998 年に設立された Critical Software 社は、セーフティ・ミッション・ビジネスクリティカルなアプリケーション向けにシステム/ソフトウェアサービスを提供しており、ソフトウェアの安全性や性能、信頼性において最も要求の厳しい品質基準を共有する、さまざまな業界のクライアントと共に活動しています。Critical Software 社の High Integrity System 部門(HIS)は、20 年以上にわたりセーフティクリティカルなシステムに取り組んでいます。

プロジェクト

ビジネスジェットの電源制御ユニット(PCU)は、電源(外部 AC、外部 DC、エンジンを含む)を割り当て、それらをスムーズに切り替えるために、数百ものアナログ信号とデジタル信号を管理します。

このプロジェクトは、証明機関が商用ソフトウェアベースの航空宇宙システムを承認するためのリファレンスとなる第一の標準 DO-178C の対象でした。PCU システムの障害は航空機に対する致命的な障害状態を意味するので、このプロジェクトには設計保証レベル A (DAL A) が割り当てられました。

利点

Critical Software 社の首席技師 Vitor Conceição 氏は、20 年以上のプロジェクト経験があります。彼の見るところでは「変更要求は、ほぼすべてのプロジェクトで共通していて、頻繁に発生し、予期しないもので、かつ非常に短い時間で応答することが要求されます」

LDRA ツールスイートは、このプロジェクトのクライアントが選択したツールでしたが、Critical Software は、その選択に非常に満足しています。

LDRA ツールスイートは、レビュー対象のコードをコーディング規約と比較することで、ソースコードの「検査」を自動化します。不適合は、DO-178C で要求されるように、複雑性が高いなど他の望ましくない特性とともに強調表示されます。

しかし、Conceição 氏が特に感銘を受けたのは単体テスト機能でした。「オンターゲットのテスト機能が特に重要です」と Conceição 氏。「テストケースファイルには、テストデータや環境/ターゲットのセットアップなど、テストの再実行に必要なすべての設定が保存されます。これにより、特にプロジェクトが変更管理に入った後、変更に対応したリグレッションテストをずっと効率化できます」

この回帰テスト機能だけで、以前に変更に対処するのに費やされた時間の約 15%を節約できたと Conceição 氏は試算しています。

将来

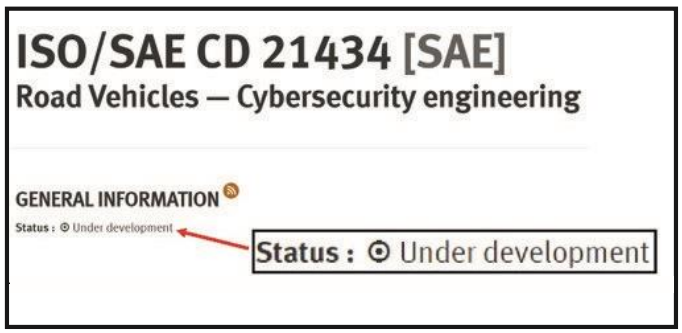
「ツールチェーンは、このプロジェクトのためにお客様から指定されたものですが、我々の将来の仕事でも間違いなく利用すると考えています」と Conceição 氏。「我々が関与するアプリケーションはますます複雑になると予想します。その複雑さに対処する上で LDRA ツールスイートが、私たちをさらに効率的にして、継続的なサポートコストを削減し、これまで以上に競争力を与えてくれると期待しています」

この号の内容

姿を変える自動車規格：♪ We can work it out ♫

SAE J3061? ISO/SAE 21434?

2016 年 1 月、SAE は J3061「Cybersecurity Guidebook for Cyber-Physical Vehicle Systems」を発行しました。ISO 26262 初版を補完するよう作成されたこの文書は、開発ライフサイクル全体を通じてサイバーフィジカルの車両システムのベストプラクティスを形式化する試みを表しています。



SAE J3061 の理論的根拠には「さらなる規格開発のための基盤」を形成するということもあり、近刊の ISO/SAE 21434 規格「Road vehicles - Cybersecurity engineering」に反映される可能性が高いものです。それが開発の基礎として実用的に使用することができるようになるには数ヶ月かかることでしょう。

しかし、SAE J3061 が昨日のニュースであって、ISO/SAE 21434 が明日のニュースなら、今日のニュースは何でしょうか?

"I'm taking the time for a number of things
That weren't important yesterday"
Lennon-McCartney

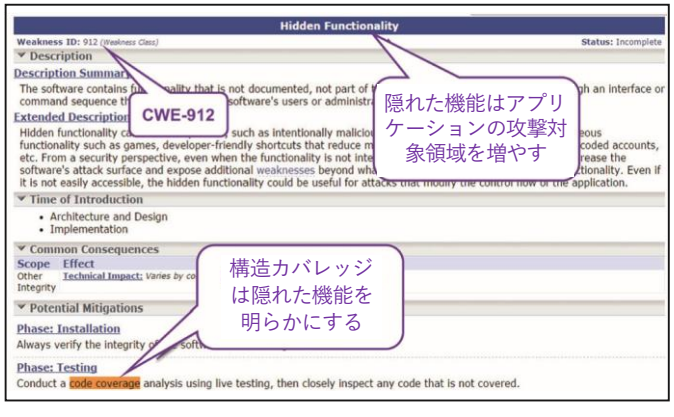
この過渡的な問題は、今日のシステム開発者にとって、セキュアなコードを時間とともに、どのように開発するのが最善かという、より大きな問題にスポットを当てています。共通の特徴が多くあり、サイバー攻撃によって安全性が脅かされる恐れがあるにもかかわらず、サイバーセキュリティのための設計と開発には、一般に、機能安全とは異なる焦点を当てることが必要です。例えば、サイバーセキュリティは、はるかに速く変化する環境であり、活動している侵略者が潜在しているということは、従来の機能安全の世界とは異質なものです。需要に対して適切な規格の開発が遅れているということは驚くことではありません!

根本的な事実は、どのような手順を踏んでも、接続されたシステムは孤立したシステムと同じほどセキュアではありえないということです。セキュアアーキテクチャ、最小特権原則、ドメイン分離技術、セキュアコーディングとテスト技術などを組み合わせた「多層防御」を適用することで、テクノロジーが許す限りシステムを安全にすることができます。そして、セキュアなアプリケーションコードは、他の防御メカニズムと同じくらい大きな役割を果たします。

「正しい」ことをなす

SAE J3061 と ISO/SAE 21434 の基本原則が根本的に違っているという可能性は低いでしょう。もちろん進歩はあるでしょうが、共通の原則は良いエンジニアリング原則を遵守することであり、ルールを書く人が誰であれ、それは同じです。例えば以下のルールです。

1. **セキュリティ要件を確立し、それらにトレーサビリティを示す。**自動車ソフトウェア開発者は、安全要件に対する双方向トレーサビリティへの ISO 26262 の要求を熟知しています。セキュリティに対してもまったく同じ原則が適用されます。
2. **セキュアコーディング規約への準拠を保証する。**ISO 26262 は、元々コーディング規約への準拠を要求しています。MISRA が実証しているように、機能的に安全なコードを作成する優れたコーディング手法のほとんどに対していくつか追加を行うことで、セキュアなコードが作成できるでしょう。
3. **単体テストとシステムテスト。**これらの動的テスト手法は、セキュリティ要件が正しく実装されているという証拠を提供することと、リスクベースのテストをサポートすることの両方の面で役に立ちます。
4. **構造カバレッジ。**構造カバレッジは、テスト対象コードにおいて通過するパスが十分に実行されていて、アプリケーションの攻撃対象領域を増やして弱点を露呈させる隠れた機能がないということを示します。



隠れた機能を防ぐために CWE では構造カバレッジ解析を推進

AUTOSAR++? MISRA C++?

同様の難問が AUTOSAR Adaptive アプリケーション開発の世界にも存在します。今年の初め、MISRA と AUTOSAR は、それぞれの C++言語サブセットを統合するパートナーシップを発表しました。このガイドラインは、当初は ISO/IEC 14882 C++17 までのバージョンに適用され、C++言語の新バージョンのリリースサイクル 3 年を反映するよう継続的に進化します。

AUTOSAR から導入されたガイドラインは MISRA の規則と用語に合わせます。MISRA C++:2008 のガイドラインが新しいドキュメントの基礎として使用され、その理論的根拠と例題を改善しています。

背景

AUTOSAR(AUTomotive Open System ARchitecture) パートナーシップは、車両 ECU ソフトウェアのリファレンスアーキテクチャを継続して開発することに焦点を当てている自動車 OEM とサプライヤーのシナジー効果をもったグループです。

Adaptive Platform は、ハードリアルタイム性と安全制約を受ける組込みシステムに向け長年にわたって確立された Classic Platform を補完するもので、高度に自動化された運転や自律運転などのユースケースに対応する安全関連システムを構築するための AUTOSAR 高性能コンピューティング ECU 向けのソリューションです。Classic Platform のアプリケーションは C で開発され、Adaptive Platform のアプリケーションは C++で開発されます。

MISRA は、メーカー、部品サプライヤー、エンジニアリングコンサルタント間のコラボレーションでもありますが、言語サブセットとして最もよく知られています。MISRA は自動車分野から生まれましたが、最近では、医療機器、産業、航空宇宙、鉄道輸送など、多くの安全・セキュリティ分野において、そのガイドラインが一般的に使用されています。

Adaptive Platform の環境を定義する過程で、AUTOSAR では C++14 とそれに続く言語の進化をサポートする言語サブセットが必要になりました。MISRA C++ は優れたものと考えられていましたが、C++03 をサポートするため 2008 年に公開されたものであり、十分に新しいものではありませんでした。

"Life is very short and there's no time for fussing and fighting my friend."
Lennon-McCartney

AUTOSAR は、MISRA が MISRA C++:2008 のアップデートを約束していることを知らずに、MISRA C++:2008 を独自ルールで補完して AUTOSAR C++14 ガイドラインを作成したので、ほぼ同じものが二つ並行して開発されることになってしまいました。1 月の発表は、AUTOSAR と MISRA それぞれのパートナーシップでの最新の取り組みを融合させることによって、その状況を解決するものです。

AUTOSAR アプリケーション開発への影響

一般に、組込み開発の世界では、デファクトの C++言語サブセットと、それを言語の進化にともなって継続的に保守することを求めてきました。この共同発表は、そのためだけでも歓迎されるものです。

AUTOSAR アプリケーション開発者にとっては、規則や規制の簡素化と合理化が特に歓迎されています。ISO 26262 機能安全規格、SAE J3061 サイバーセキュリティガイドライン、そして AUTOSAR 規格自体で定義されているプロトコルの要求など対処するべきことはすでに十分にあるなかで、言語サブセットの選択が不必要に複雑になることはありません。

AUTOSAR の Adaptive Platform と Classic Platform で共通するものは AUTOSAR Foundation 規格に反映されており、両者に適用可能な要件と技術仕様が含まれています。Adaptive アプリケーションで使用する統合された C++言語サブセットにおいて MISRA の規約と用語を採用することは、Classic 開発で既に使用されている MISRA C ガイドラインに一致するものであり、両方のプラットフォームに関わるすべてのユーザーの作業を簡素化するのに役立って、使用する「正しい」コーディング規約が明確になります。

LDRA ツールが自動車のセキュリティやコーディング規約にどのように役立つかについて詳しくは、お問い合わせください。

LDRA: Getting so much better all the time

ツール統合ニュース

LDRA は、主要な ALM、PLM プロバイダと提携し、組込みソフトウェア市場向けに、コードまでのトレーサビリティとターゲットハードウェアでのテストの検証と妥当性確認を備えた全アプリケーションライフサイクル管理のソリューションを提供しています。LDRA ツールスイートを Jama Connect や Polarion ALM、PTC Windchill RV&S と組み合わせることで、双方向でデータを交換し、業界固有の開発プロセスをサポートしてテストコストを削減し、コードの品質・安全性・セキュリティを向上させます。

LDRA ニュースルーム

LDRA 自動車リソースセンター

この度、自動車リソースセンターがオープンしました。

LDRA には世界中のセーフティ・セキュリティクリティカルな組込みシステムの世界で 40 年以上の経験があり、当社のお客様は、製品やサービスを使用するたびにその経験の恩恵を受けることができます。今回のリソースセンターは、お客様や他の人々が当社の豊富なリソースから一層の恩恵を受けることを支援します。

https://resources.ldra.com にアクセスして、当社独自のビデオやガイドをご覧ください。

ソーシャルネットワーク

Twitter、Facebook、LinkedIn のプロフィールに参加して、LDRA のニュース、製品の更新情報、イベント、Webinar などの最新情報を入手してく

@ldra_technology
LDRA Software Technology
LDRA Limited

LDRA
Software Technology

ご存知でしたか?

LDRA は Michael Hennell 教授によって、リバプール大学で彼の原子核物理学研究で使用していた数学ライブラリの品質評価を行うために作成したソフトウェアテストベッドを商品化するため、1975 年に設立されました。

An experimental testbed for numerical software

M. A. Hennell

Computational Science Department, University of Liverpool

https://academic.oup.com/comjnl/article/21/4/333/356861

LDRA

電話 EMEA : +44 (0)151 649 9300
電話 USA : +1 (855) 855 5372
電話 India : +91 80 4080 8707
メール : info@ldra.com
Web : www.ldra.com

ニュースレターへの寄稿

読者からの寄稿を歓迎します。ソフトウェアテストの世界に関連すると思われるコメントやストーリーをお持ちの方は、ご連絡ください。