自動車向け機能安全国際規格 ISO 26262に対応した東芝の取組み

Construction of Software Development Process for Automotive Applications to Enhance Functional Safety in Compliance with ISO 26262 Standard

山内　信之　■YAMAUCHI Nobuyuki
青峰　亮子　■AOMINE Ryoko
余宮　尚志　■YOMIYA Hisashi

2011年11月に発行された自動車向け機能安全に関する国際規格ISO 26262（国際標準化機構規格26262）への対応は，車載事業において必須となっている。この規格では，ハードウェア故障以外にソフトウェア起因によるシステム障害に関しても十分な注意を払うことが求められており，ソフトウェア開発プロセスの確立がキーとなっている。

東芝はこれに対応するため，ISO 26262ソフトウェア開発プロセスに関して第三者認証を2012年3月に取得した。その際，現場へ容易に浸透させるためプロセス策定は既存のプロセスをベースにするなどの工夫を行った。現在，プロセスを実製品へ適用する取組みを推進している。また海外拠点を含む東芝グループ車載関連部門の機能安全対応力強化のため，全社的な教育と支援の体制を構築中である。

The ISO (International Organization for Standardization) 26262 standard, which is a functional safety standard introduced in November 2011, is applicable to software development processes for in-vehicle electrical and electronic systems. This standard is indispensable in the automobile industry to minimize risk resulting from vehicle system failures due to software as well as random hardware failures.

With this as a background, Toshiba received ISO 26262 certification for its software development process from TÜV SÜD, a German-based international certification organization, in March 2012. To disseminate the process certification throughout our software design sites, we adopted realistic and constructive approaches based on reusing and enhancing our existing processes. Some projects applying the ISO 26262 standard to actual products are now in progress. We are also constructing a corporate-level education and support system in order to reinforce the functional safety capabilities of our automotive-related departments including overseas bases.

1　まえがき

自動車向け機能安全に関する国際規格ISO 26262が2011年11月に正式発行されたことで，車載事業に変化が見え始めた。顧客からの要求事項に機能安全が入ることは当然のこととなり，開発現場でもその対応を加速させる必要が出ている。これには電動車両の開発が本格化しつつある背景があり，組込みソフトウェアによる電子制御の割合が増加の傾向にあることが要因の一つと言える。

ここでは，東芝が推進しているISO 26262に対応したプロセスの導入とその実践に関する取組みについて述べる。

2　ソフトウェア開発プロセス認証の取得

当社は，ISO 26262に関わるソフトウェア開発プロセス認証を2012年3月に取得した。この認証は，当社のソフトウェア開発プロセスがISO 26262規格の要求に従っており，かつ当社が，規定されたプロセスに従ってソフトウェア開発を確実に実施できる企業であることを証明するものである。

ここでは，ソフトウェア開発プロセス認証を取得することの意義と開発プロセス策定のステップ，更にプロセス認証取得によって可能な機能安全ソリューションについて述べる。

2.1　ソフトウェア開発プロセス認証の意義

ISO 26262において，故障は2種類に分類される。製品の開発及び製造過程で設計ミスやプロセスの不備などによって発生する障害が原因となるシステマティック故障と，製品運用中に発生するハードウェアエレメントの障害が原因となるランダムハードウェア故障である。機能安全を考慮したシステムでは，安全関連機能に関するこれら二つの故障への対策を施すことが求められる。

ただし，ソフトウェアの故障は，システマティック故障だけであるとされる。なぜなら，ソフトウェアはハードウェアのように運用中に突然壊れることはなく，全てのソフトウェア障害は開発段階から潜在的に存在している，いわゆるソフトウェアの不具合によるからである。このため，ISO 26262のソフトウェアへの要求は，システマティック故障を防ぐためのものであり，ある認証機関によれば，開発プロセスに対するものが全要求の85％となっている。

したがって，ISO 26262要求を満たすソフトウェアを開発するためには，ISO 26262要求に準拠したソフトウェア開発プロセスを策定し，これに従った開発を行うことが大変重要であると言える。

2.2　ソフトウェア開発プロセス策定のステップ

2.2.1　プロセス策定方針　ソフトウェア開発プロセスの策定方針として，まったく新しいプロセスを一から作るのではなく，既に開発者が運用している当社既存のソフトウェア開発プロセスをベースに，ISO 26262要求を補完することとした。これは，ISO 26262要求がもともとAutomotive SPICE®(注1)やCMMI®(注2)などの一般的なソフトウェア開発プロセスと親和性があることから，当社の既存プロセスと大きな差異はないことが推測できたからである。また，何よりも，策定したプロセスを実際の開発に適用しなければ意味がない。現場の開発者が抵抗なく開発できるよう，できる限り既存プロセスの形を残す方針をとった。

また，ISO 26262を詳細に理解していない開発者であっても，プロセス文書に記載した指示の順守と成果物チェックリスト及び成果物テンプレートの使用によって，ISO 26262要求に必然的に従うことになるような仕組みを策定した。

2.2.2　ギャップ分析　ISO 26262要求と既存のソフトウェア開発プロセスのギャップ分析を行った。ギャップ分析の対象は，ISO 26262のソフトウェア要求に関連する部分であり，具体的には，ISO 26262 Part2 管理のソフトウェア開発に関連する部分，ISO 26262 Part6 製品開発：ソフトウェアレベルの全て，及びISO 26262 Part8 支援プロセスのソフトウェア開発に関連する部分である。

この範囲の規格に記載されている全ての要求事項に当社の既存プロセスが適応しているか，適応している場合は既存プロセスの適応箇所（ドキュメント名，具体的な記載箇所）を記録し，適応していない場合は不足項目として記録し，分析結果としてまとめた。

2.2.3　ギャップ分析結果による施策　ギャップ分析の結果，当社の既存プロセスの主な不足部分は三つに大別されることがわかった。これらのギャップについて，以下に述べるように対策を検討し既存プロセスに追加した。

一つ目は，機能安全特有の開発管理に関する要求である。ISO 26262は，機能安全に関連した活動の計画と管理を行う安全管理者を任命することを要求している。また，安全計画や安全分析のレビュアーと，安全監査の実施者には，プロジェクトや組織からの独立性が求められ，その独立性レベルへの要求は求められるASIL（Automotive Safety Integrity Level）によって異なる。このような開発管理に関する要求は機能安全特有であり，既存プロセスにはなかったものである。そこで，新たに安全管理者の役割とスキルを規定し，プロジェクトに必ず安全管理者を任命することを規程文書に記載した。これらについて，プロジェクト計画書のチェックリストにチェック項目を設け，計画工程のレビューで確認できるようにした。

二つ目は，エンジニアリングに関する項目である。設計や実装の原則は，既存プロセスで規格要求をほぼ満たしていたが，要求仕様及び設計仕様の表記手法や，テスト手法，各成果物のレビュー手法などASILごとに推奨される手法は対策が必要であった。これらの手法の選択基準を規程文書に記載し，各成果物レビュー時に使用するチェックリストにチェック項目を設けた。また，アーキテクチャレベルでの安全分析や異なるASILレベルのエレメント間の独立性確保など，機能安全設計のための要求についてもチェック項目を設けた。

三つ目は，ソフトウェアツール認定や，ソフトウェアコンポーネント認定，キャリブレーションの扱いなどISO 26262特有の要求群である。これらについて，まずISO 26262規格の要求内容を理解し，当社としてどのように取り組むかを検討した。その上で，ソフトウェア開発に適用するソフトウェアツール認定とソフトウェアコンポーネント認定のガイドラインを作成し規程文書に追加した。

2.2.4　パイロットプロジェクトによるプロセスの試行

策定したプロセスを実際に実施可能であることを示すために，このプロセスに従った機能安全対応のソフトウェアプロジェクトを試行した。最高レベルASIL Dの技術安全要求を仮定して，安全計画に従って要求分析，設計，実装，及びテストを実施し，ISO 26262が要求する活動の成果物を作成した。

2.2.5　認証機関による監査　策定したソフトウェア開発プロセスは，ドイツの認証機関であるTUV SUD Automotiveに監査を依頼した。全ての規程文書，成果物テンプレート，チェックリスト，及びガイドラインと，パイロットプロジェクトの全ての成果物について監査を受けた。認証機関は主に，ASILごとに推奨される技術の選択基準が明確になっているか，またそれらの技術や手法を開発者が確実に実行できるかを重要視した。これらに対して，技術選択基準を明確に規定し，技術教育カリキュラムや関連資料の整備によって現場のエンジニアが必要に応じて技術を学び実践できる体制を整えていることを示した。この監査によって，当社が開発現場でISO 26262に対応した開発を確実に実行できることが認められた。

2.3　プロセス認証によって実現する機能安全ソリューション

ISO 26262認証を取得したソフトウェア開発プロセスに準拠して当社製の機能安全を考慮したマイコン用のライブラリを開発中である。このライブラリ製品は，ISO 26262準拠を示すエビデンスとともにユーザーに提供する予定である。また，機能安全を考慮したマイコンはハードウェア故障を自己診断する回路を備えており，この技術は，IEC 61508（国際電気標準会議規格61508）のSIL 3（Safety Integrity Level 3）を実現可能であるとして，2009年にTUV SUD Automotiveから高い評価（テクニカルレポート受領）を受けている（**図1**）。

故障診断機能を備えたマイコンと認証プロセスに準拠して

（注1）　Automotive SPICEは，Verband der Automobilindustrie e.V.（VDA）の登録商標。
（注2）　CMMIは，米国カーネギーメロン大学の登録商標。

開発したマイコン用ライブラリを提供することで，ユーザーはマイコンの故障診断機能を容易に開発できる。更に，ユーザーシステム全体でのISO 26262準拠を示すエビデンス（セーフティケース）整備の一端を担うことが可能になる（**図2**）。

機能安全は，マイコンなどの部品だけで実現できるものではなく，システム全体の安全分析に基づいて設定された最上位の安全目標を達成することによって実現されるものである。システムレベルで設計された安全メカニズムは，システムを構成するハードウェア及びソフトウェアレベルへの要求として詳細化される。マイコンやソフトウェアに機能安全をサポートする機能やエビデンスがそろっていれば，システム全体の設計を容易にし開発工数を削減できる。

このように，ハードウェアとソフトウェアの連携による機能安全実現のソリューションは，ユーザーにとって高度な機能安全対応システムを実現すると同時に，開発工数の削減に貢献している。

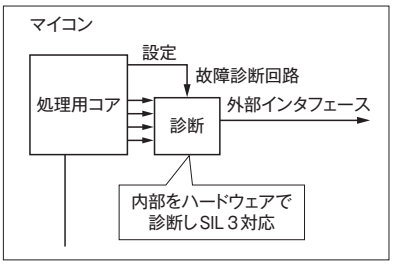

図1．東芝製機能安全対応マイコンの故障診断 ― 処理用コアと内部信号を参照する診断回路を組み合わせ，比較と自己診断を自動実行させる。
Fault diagnosis of Toshiba microcontroller units (MCUs) corresponding to functional safety

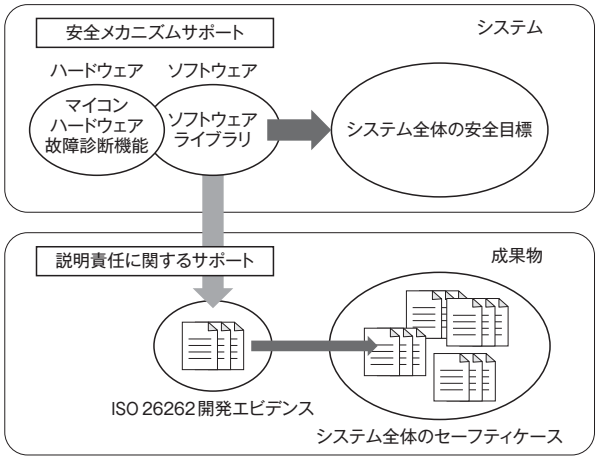

図2．ハードウェアとソフトウェアの連携による機能安全サポート ― 故障診断機能を備えたマイコンと認証プロセスに準拠して開発したマイコン用ライブラリを提供することで，ユーザーはマイコンの故障診断機能を容易に開発できる。
Functional safety supported by collaboration of hardware and software

3　東芝グループ全社の開発プロセス構築への取組み

東芝グループでは，複数の事業部門がグループ会社とともに車載向け製品を開発しており，製品分野に応じた開発プロセスを持っている。ISO 26262に準拠した製品開発を進めるためには，これらの事業部門やグループ会社の開発プロセスがISO 26262に準拠している必要がある。しかし，開発プロセスの修正や確認のための時間やコストが問題となっていた。

2章で述べた，ISO 26262に対応したソフトウェア開発プロセスをそのまま適用すると，製品分野の違いや各事業部門とグループ会社が持っている開発プロセスに関するノウハウを継承することができない。

そこで当社では，機能安全を専門とする全社的な組織が，事業部門やグループ会社それぞれの開発プロセスをISO 26262に対応させるための支援を行っている。これにより，開発プロセスの修正や確認のための時間やコストの問題を解決している。

開発プロセスの構築は，次の手順で行う。

(1)　既存の開発プロセスを分析し，ISO 26262に対応した新しいプロセスの枠組みを決定する
(2)　既存の開発プロセスで満たしていないISO 26262の要求事項を抽出する
(3)　(1)で決定した新しいプロセスに(2)で抽出した満たしていない要求事項を追加し修正する
(4)　(3)で得られた新しいプロセスが，ISO 26262の要求事項を満たしているかを確認する
(5)　パイロットプロジェクトで新しいプロセスを試行する

(1)の新しいプロセスの枠組みとは，既存の開発プロセスとISO 26262で定められている用語との対応を定義すること，安全管理者などISO 26262で求められる役割を追加すること，及び安全ライフサイクルを満たすためのフェーズを追加することの三つである。

(1)は事業部門やグループ会社と共同で進め，(2)と(4)は全社的組織が中心に進めている。(3)については，事業部門ごとの製品分野の違いやノウハウを吸収しながら事業部門が開発していく。必要に応じて，全社的組織が実践で活用することを想定したガイドやテンプレートの開発を支援している。ガイドは，例えばFMEA（Failure Mode and Effects Analysis）やHAZOP（Hazard and Operability Study）などのリスク分析手法の実践手順を記した文書である。テンプレートは，ISO 26262に準拠するために記載しなければならない内容に抜け漏れがないようにフォーマットを定めたものである。

このようにして構築した，事業部門やグループ会社それぞれに特化したISO 26262ソフトウェア開発プロセスが実際に運用できることを，パイロットプロジェクトによって確認している。

このほか全社的組織では，ISO 26262のプロセス構築の際に，同時にAutomotive SPICE®やCMMI®について専門家

による支援が可能な体制を整備している。

このメリットは，開発プロセス構築までの時間やコスト以外に，次の2点にまとめることができる。

(1) 事業部門は要求事項の追加（前記(3)）に注力できる

(2) Automotive SPICE®やCMMI®にも準拠した開発プロセスの構築ができる

この取組みにより，ISO 26262に対応したプロセスの構築を，事業部門やグループ会社だけで開発プロセスを構築する場合に比べて，約1/2の期間で実現している。

4 コンピテンスの構築

ISO 26262に準拠した製品開発では，安全管理者や開発者の育成と，適性の管理が重要である。しかし，これらを東芝グループの各事業部門で行う場合，開発者育成のための教育を独自に用意するには時間が掛かり過ぎる。第三者認証機関などの外部に委託するには教育の実施時期に制約があったり，コストが掛かり過ぎるという問題があった。

当社では，ISO 26262に関わるコンピテンスを，開発プロジェクトでの役割に応じて必要な職務経験（種類と年数）及び受講すべき教育科目を定めて育成し管理している。

教育に関しては，ISO 26262の教育を自社で開発している。その教育体系を**図3**に示す。ここでは，職務経験に関する要件は省略している。

“機能安全設計教育 基礎編”は，安全についての用語や概念などを広く理解するための教育で，IEC 61508を主とした教育内容である。機能安全についての基礎知識だけではなく，FMEAやHAZOPなどのリスク分析手法について，演習を通じて習得できることも特長である。

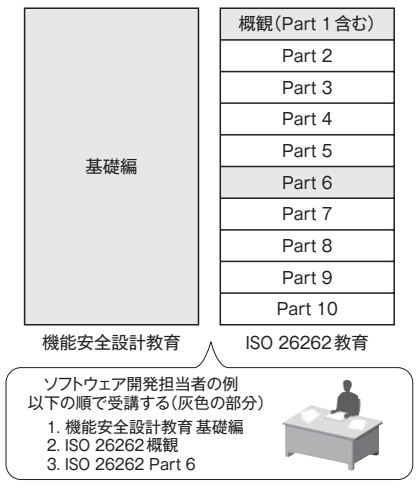

図3．東芝グループにおけるISO 26262の教育体系 — ISO 26262の教育体系を定めて独自に教育を開発している。
Structure of ISO 26262 education in Toshiba Group

“ISO 26262概観”は，ISO 26262について規格の構成や内容を短期間で習得できる。その他に，ISO 26262の各Partに対応した教育を用意している。

これらの教育は，開発プロジェクトでの役割に応じて，開発プロジェクトの開始前までに適切なタイミングで受講できるように運用している。

これらの教育体系のメリットは，次のとおりである。

(1) 安全一般や機能安全に関する基礎的な教育を用意することで，全開発者の安全に対する知識を深めることができる

(2) 開発プロジェクトの開始時期に合わせた教育を事業部門内で速やかに実施できる

(3) 開発プロジェクトでの役割に応じた人材を効率的に育成できる

この教育は，車載向け製品を開発する事業部門やグループ会社に対して，国内だけでなくインドなど海外でも実施しており，安全管理者や開発者を適切に育成し，適性を管理している。

5 あとがき

当社は機能安全への取組みの一環として，ISO 26262に対応したソフトウェア開発プロセスについて第三者認証を取得した。更に，コンピテンスを満たした安全管理者や開発者を育成する体制も構築中である。これらを生かして，また半導体とソフトウェア及びそれらの教育の相乗効果を背景に，今後も自動車の安全性向上に貢献していきたい。

文 献

(1) 山内信之 他．自動車の電子化・電動化を支えるソフトウェア技術と課題．東芝レビュー．66，2，2011，p.17-20.

(2) 余宮尚志 他．ソフトウェアを中心とした安全設計技術．東芝レビュー．65，7，2010，p.37-40.

山内 信之 YAMAUCHI Nobuyuki
社会インフラシステム社 鉄道・自動車システム事業部 自動車システム統括部参事。自動車向け基盤ソフトウェア技術の開発に従事。
Railway & Automotive Systems Div.

青峰 亮子 AOMINE Ryoko
セミコンダクター＆ストレージ社 システム・ソフトウェア推進センター ソフトウェア開発技術担当主務。組込み用ソフトウェア開発技術及び開発プロセスの管理業務に従事。
System & Software Solution Center

余宮 尚志 YOMIYA Hisashi
ソフトウェア技術センター ソフトウェア設計技術開発担当主務。ソフトウェア設計技術の研究・開発とソフトウェア開発プロジェクトの管理業務に従事。情報処理学会会員。
Corporate Software Engineering Center