

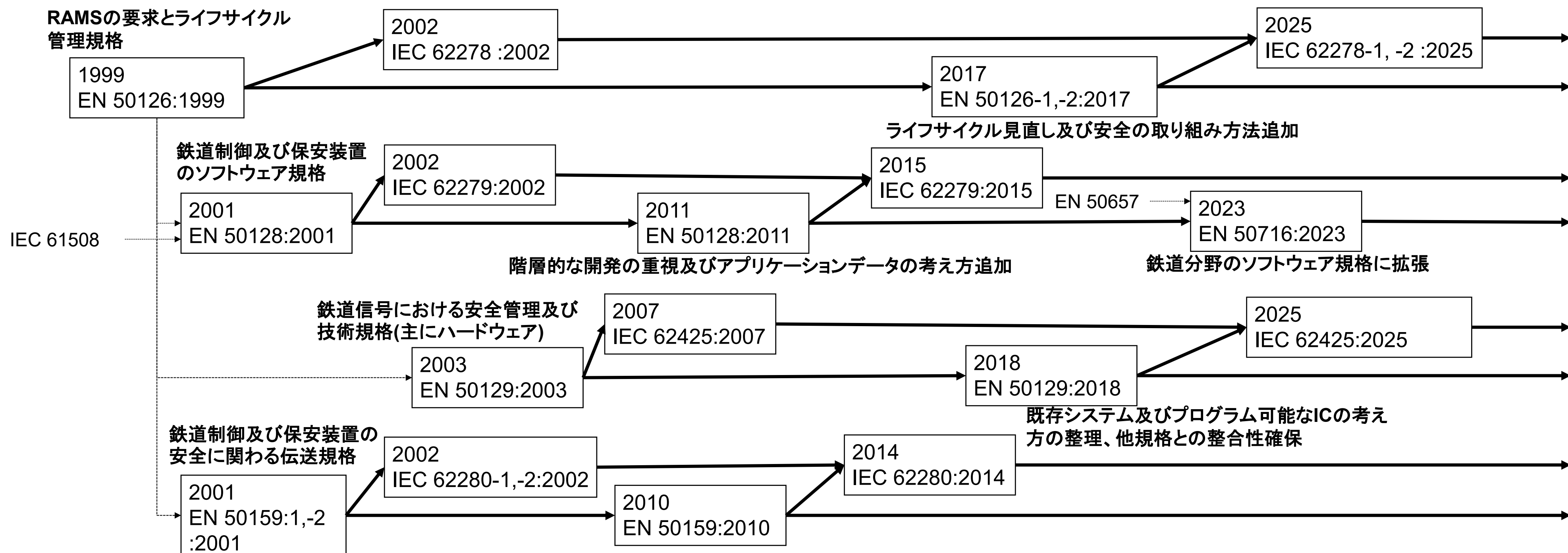
改定されたRAMS関係規格の注意点について

-鉄道における国際規格IEC 62425規格の変更とそのポイント-

鉄道認証室 ※森 崇 吉永 純

はじめに: 鉄道製品のマネジメント規格(RAMS*規格)の概要と変遷

*RAMS: Reliability, Availability, Maintainability and Safety



IEC 62425と機能安全

機能安全とは

入力に対して、物理的ユニットと機能が正常に働くことにより安全を確保することをいう。

安全を阻害する入力

処理BOX

やれやれ、またアブないデータが来たよ。ルールに基づいて、このデータは捨ててしまおう。

健全な精神は健全な肉体に宿る！システムが健全に作りこまれ、また「危険な場合の動作定義」をする必要がありますよね

でもそれなら機能安全を実現するヒントと受け入れられるレベル感が欲しいですね

対象製品に対してどのような安全のマネジメント、技術手法の選択をするかをSafety Planにまとめて、開発で行う事項を違う目で確認(verification)をしてもらうことを計画する。

対象製品に対して、リスクアセスメントで必要なレベルの安全関連機能の失敗頻度とその安全レベルを決め、できた製品が計画通りか否か、また安全に関するすべての証拠をまとめたSafety Caseを作成する。また、確認結果をverification reportに、最終的に試験も含め計画通りの出来栄えかをvalidation reportにまとめる。

オレ流の安全ではカバ鉄道さんは突破できないかな。。

アセスメント計画の例

①システムイメージを準備し、物理的な接続や機能的な接続をイメージする。

②発生する事象と頻度を勘案したリスクマトリックスを準備する。

③システムの接続されている相手（ハザード源）から、どんなハザードがありそうかを抽出し、ハザードリストを作る。

④ハザードの重大性とリスクマトリックスから、Tolerable Hazard Rateを決める。また、想定される頻度と重大性から、対処すべきハザードであるかを定める。

⑤ハザードの対処機能を安全関連機能として位置付ける。安全を守るための機能は「安全関連機能」となり、その機能の安全レベルであるTFFRとそれに対応するSILを決める。SRACとなる要求は、その旨整理する。これらをハザードログに整理する。

IEC 62425の変更点

SRACsについて

安全を担保するのはなんや？安全のための機能か？

使う時の制約や前提を守ってもらうためのSRACs(Safety Related Application Conditions)もいるで。

● いままで、SRACsについては、その管理に関してそれほど規定があったわけではありませんが、使い方を誤ると、せっかくの装置も台無しなので、規格上も重視されるようになりました。SRACsについては、"できないことを前提にするな"など「べからず」が明記されるとともに、事故を引き起こす要因である「ハザード」と必ず対応させることが求められます。「なんとなく危なそうだから制約をつけておこう!」というのは、避けなければなりません。

既存装置の活用と規格適合性について

ウチの今までの開発資産どうなる？

今までは、「対象外」とされていたが、これからは要求を守れば「規格適合対象」にできるんや。

● 会社は過去の資産を抜きに開発を行うことは少ないでしょう。これらの資産を抜きにして開発を進めると大変非効率ですので、過去は「IEC 62425適合性対象外」としてきましたが、対象システムの中で対象の部分と対象外の部分が混載してしまいます。これを避けるため、一定の条件を付けて「規格適合」とすることができるようになりました。機能やインターフェースの明確化、故障モードとその故障の起きる頻度、試験とそのverificationがなされていることが大まかな条件となります。(他に条件あり)

ユーザがプログラムできるLSIについて

なんか焼き込んで動作定義できるLSIこの頃よく使うらしいな。

FPGAとかPLDとかいうやつやな。ロジックゲートを記述言語でプログラムできる。ハードとロジックの設計双方の技術が必要や。

● システムの高密度化を進めるため、FPGA,PLDなどのLSIにロジック回路をプログラムする手法が安全関連システムにも導入されるようになってきました。これは、ロジック回路設計をSystem VerilogなどのHDL(Hardware Description Language)を用い記述します。このため、LSIのハードウェアのランダム故障だけではなく、システムティック故障も考えなければなりません。また、ソフトウェアの規格 IEC 62279では手薄な、ロジック回路が同時並行的に動くことによる、タイミングの問題(Clock domain crossingやMeta stability)などが発生する可能性があるため、こういったことも注意する必要があります。

最後に

RAMSの要求とライフサイクル管理規格IEC 62278も改定され、今後新しい規格の規格適合性認証も増加してくると思われます。また、今後鉄道分野のソフトウェアの国際規格の統合策定、また鉄道サイバーセキュリティ規格の制定などがスケジュールに入ってきています。鉄道認証室も、皆様のご期待に沿えるよう、新しい規格の審査を円滑に進められるように十分な準備を行い、着実に認証業務を進めてまいります。