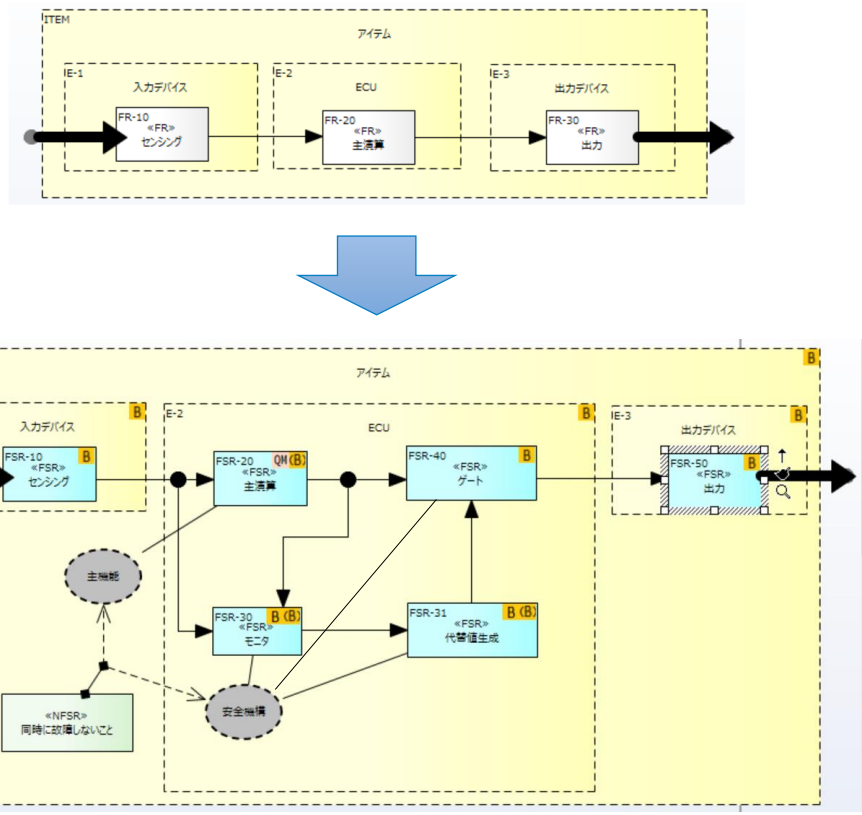
機能安全における安全分析の効率効果的な実装に向けて

SCN-SG SCDL-SA Draft Team
株式会社構造計画研究所
宮本 秀徳

はじめに

SCDL-SAでは、機能安全コンセプトを適切に正しく導出するモデルSRVA(準形式化)の定義を目指しています。



SRVAを使用して、
安全コンセプトを導出しました。

＜目標＞
正しい分析アプローチで、適切に検討し導出されたものとみなされること

安全分析を取り巻く現状課題

このようなお話をよく伺います・・・

- 各社および取引先によって、分析方法やフォーマットが異なり、安全分析手順が標準化できない。
- FMEAやFTAといった手法はいわれるが、この手法で安全要求をどのように導出したらいいかわからない。
  - FMEAといわれると、AIAG4版やAIAG-VDA統合FMEA形式をイメージするが、これらのフォーマットで機能安全を分析する方法がわからない。
  - FTAは安全目標侵害がトップ事象となることはわかるが、記載方法の自由度が高いため、どうツリー展開していけばいいか、正しい書き方がわからない。
- FMEA-MSRも登場したが、安全目標の記載がなくどうしていいか？
- フォーマットがバラバラのため、Excelでの作業となる。Excelは罫線を引くだけの支援しかしてくれず、確からしさは「人」次第。

手法の名前は上がるが、適したものがない・・・
効率効果的な業務へ改善の余地がある

安全分析を取り巻く現状課題

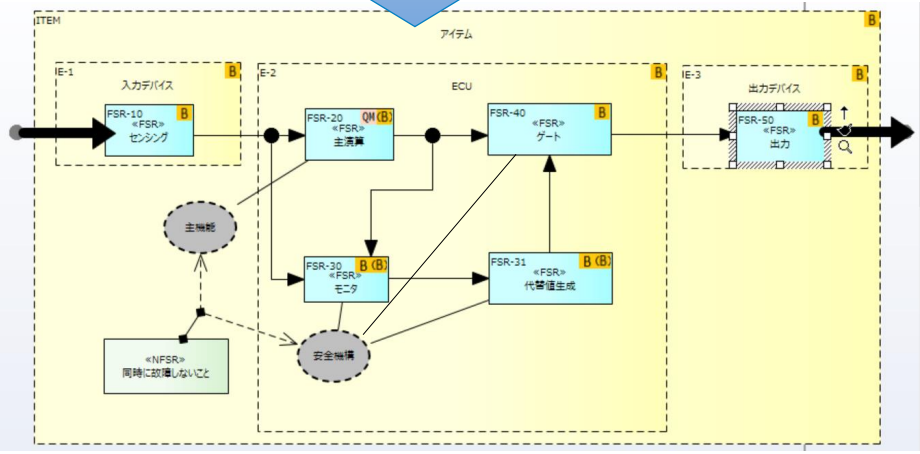
ツールベンダ（弊社）のなやみ

機能安全要求の詳細と安全分析

機能安全要求事項						安全分析					
						安全目標侵害に至る機能不全（故障モード）	侵害する安全目標		安全方策	処理時間合計	安全状態へ移行する安全要求
名称	ID(FR)	ID	種別	要求事項	処理時間		安全目標	FHTI			
センシング	FR-10	FSR-10	IF								
主演算	FR-20	FSR-20	IF	【FSR-10】からセンシング量正しく受信し、制御量を演算する。 制御量を【FSR-30】に出力する。		誤演算で過大な出力	100度を超えた場合に冷却水バルブが20 ms 以上クローズ状態にならないこと	200ms	モニタしてゲートする	140ms	モニタ 代替値生成 ゲート
モニタ		FSR-30	SM	センサからの入力と比較し異常を検知	100ms						
代替値生成		FSR-40	SM	異常を受け取り代替値を生成	20ms						
ゲート		FSR-50	SM	代替値が入力された場合は代替値を出力	20ms						
出力	FR-30	FSR-60	IF	制御値をアクチュエータを制御							
同時に故障しないこと			NF								

＜弊社ツールの安全分析(SRVA相当)画面＞
SCDLと連携し、主機能の故障による安全目標侵害の特定、安全状態移行に必要な安全要求の導出、FHTIのチェックなどを実施

連携



- 故障モードの影響を解析しており、FMEAとも呼べなくないが、AIAG4版やAIAG-VDA統合FMEAのフォーマットとは大きく異なるため、「FMEA 」とすると誤解を招く。
- そのため「安全分析」としているが、抽象的な表現でどのような手法なのか、妥当性がどうなのか、ユーザに伝わりにくい。

**SRVAという手法名が認知され、
ツールへの信頼感につながることを期待！**

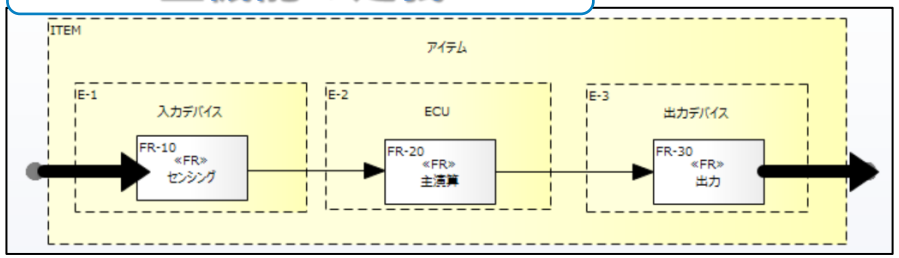
ありたい分析モデルの姿

＜SRVAで実現したいこと（して欲しいこと）＞

- 正しく、必要な安全要求や独立要求などが導きだされること
- 安全分析、提出エビデンス作成、レビュー対応など、関係業務すべてにおいて、効率/効果的になること
- このモデルを利用されていることが、正しい安全要求であると認知されること
- ツールベンダが採用し、各社のシステム利用による業務の正確性や効率の改善が図れること(Excelからの脱却)
- SysMLなど他のモデルに対し、互換性を有すること(が望ましい)

SRVAを使用した安全分析イメージ例(デモンストレーション)

主機能の定義

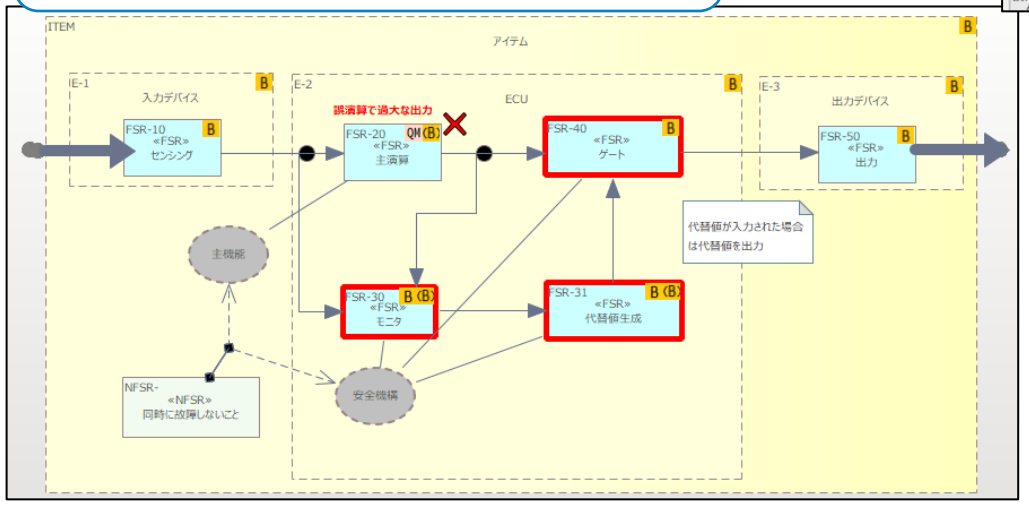


主機能に対するSRVAの実施 必要な安全要求(FSR)の特定

機能安全要求の詳細と安全分析

名称	ID(FR)	ID	要求事項	安全分析			適用ASIL		配置先エレメント
				安全目標侵害に至る機能不全	安全方策	追加要求	ASIL	コメント	
センシング		FSR-10					ASIL B		1.3. 入力デバイス
主演算		FSR-20	センシング量を演算する。 演算結果を出力する。	演算誤りで過大な制御量を出力	出力をモニタしてゲートする	モニタ 代替値生成 ゲート	QM (B)	デコンポジション	1.2. ECU
モニタ		FSR-30					ASIL B(B)	デコンポジション	1.2. ECU
代替値生成		FSR-31					ASIL B(B)	デコンポジション	1.2. ECU
ゲート		FSR-40					ASIL B		1.2. ECU
出力		FSR-50					ASIL B		1.1. 出力デバイス

ダイナミックドキュメント による検証レビュー



（将来的に） SRVAによる成果物データ 帳票の自動生成

今後の活動について

- みなさまにSRVAを使っていただき、正しく、効率/効果的な開発の実現を目指しています。
- SRVAに対するご意見、ご要望をぜひお寄せいただくとともに、ツールベンダの方々にもモデルの利用をご検討いただければ助かります。

どうぞよろしくお願いいたします。
ご清聴、ありがとうございました。