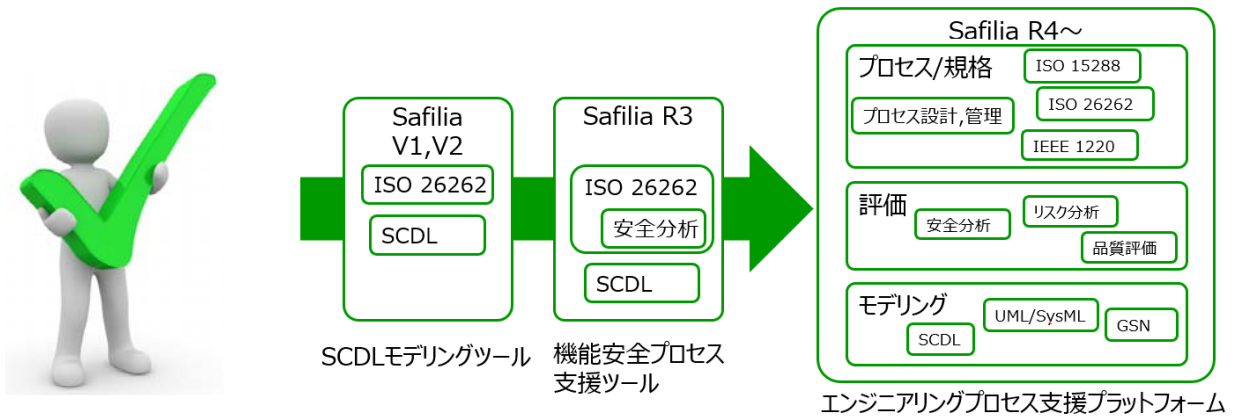


# Safilia R5 (セイフィリア)

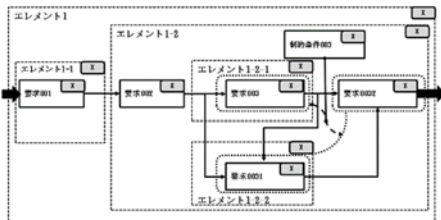
## システムズエンジニアリングをサポートするツール

- ①SCDLをベースとした安全コンセプト設計の支援
- ②安全開発に加え機能開発と連携し両者で一貫した設計を支援
- ③安全コンセプトに加え要求や分析と連携した安全開発の支援



### ①SCDLをベースとした安全コンセプト設計の支援

安全コンセプト記述言語：SCDL

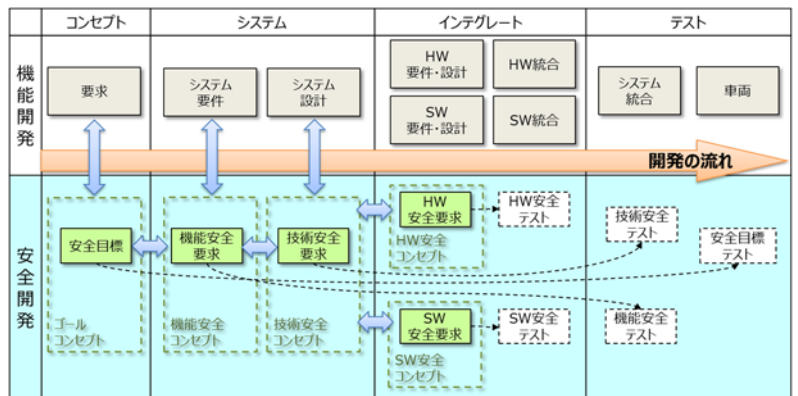


安全アーキテクチャをビジュアルに表記

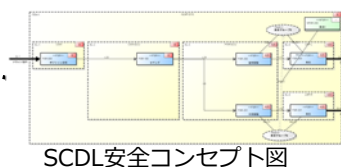
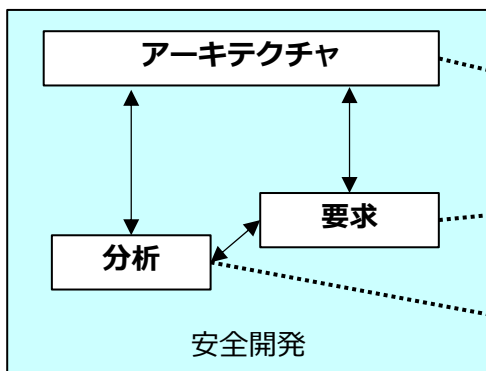
SCDL (Safety Concept Description Language)

SCN-SG URL : <https://ssl.scn-sg.com>

### ②安全開発に加え機能開発と連携し両者で一貫した設計を支援



### ③安全コンセプトに加え要求や分析と連携した安全開発の支援



要求ID	ID	名前	種別	ASIL	デコンポ理由	配置UI	要求グループID	要求グループID	要求の自然言語記述 (テキスト)	入力	出力
FSR-000	ボジション送信	FSR	B		EL-1					SI-1	I-25
FSR-100	コマンド	FSR	B		EL-2					I-26	I-26
FSR-200	左側駆動	FSR	A(B)		EL-3	ReqG-3				I-26	I-17
FSR-201	右側駆動	FSR	A(B)		EL-3	ReqG-4				I-8	I-19
FSR-300	発光	FSR	A(B)		EL-4	ReqG-3				I-17	SI-2
FSR-301	発光	FSR	A(B)		EL-6	ReqG-4				I-19	SI-4
NFSR-200	要求6	NFSR	-								

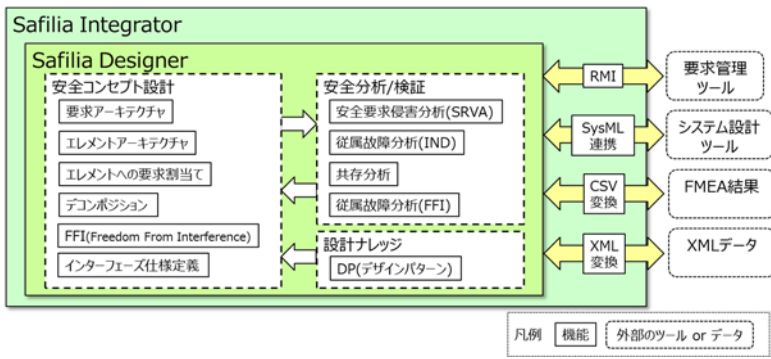
安全要求

安全要求グループ種別	安全要求グループID	ID	安全要求 (SR)	ASIL	上位 SR 侵害の可能性のある機能不全	安全方策	安全方策 ID
	FSR-000	ボジション送信	B		誤ってボジション信号を送信する	設計中	
	FSR-100	コマンド	B		誤ってコマンド信号を送信する		
ReqG-3	FSR-200	左側駆動	A(B)		誤って左側駆動信号を送信する	右側ランプを点灯する。	ReqG-4
	FSR-300	発光	A(B)		誤って左側ランプを点灯する		
ReqG-4	FSR-201	右側駆動	A(B)		誤って右側駆動信号を送信する	左側ランプを点灯する。	ReqG-3
	FSR-301	発光	A(B)		誤って右側ランプを点灯する		

安全要求侵害分析(SRVA)

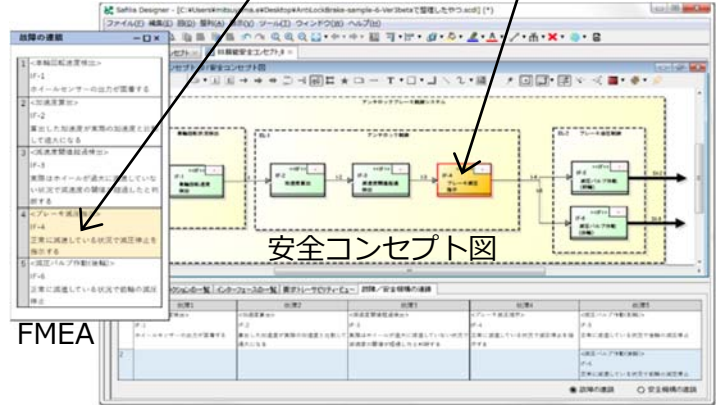
ツール連携

安全設計に関連する多種多様なツール/成果物と連携可能



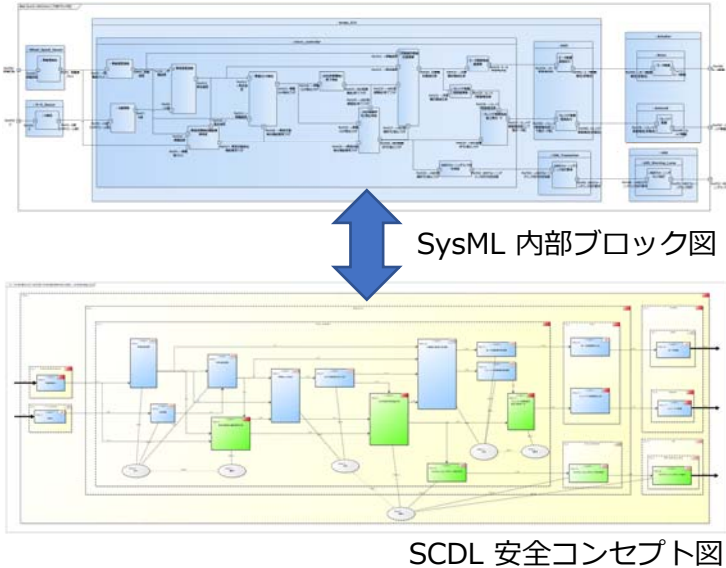
故障の連鎖の可視化

FMEAより故障をクリックすると故障が発生する安全コンセプト図上の機能をハイライト表示可能



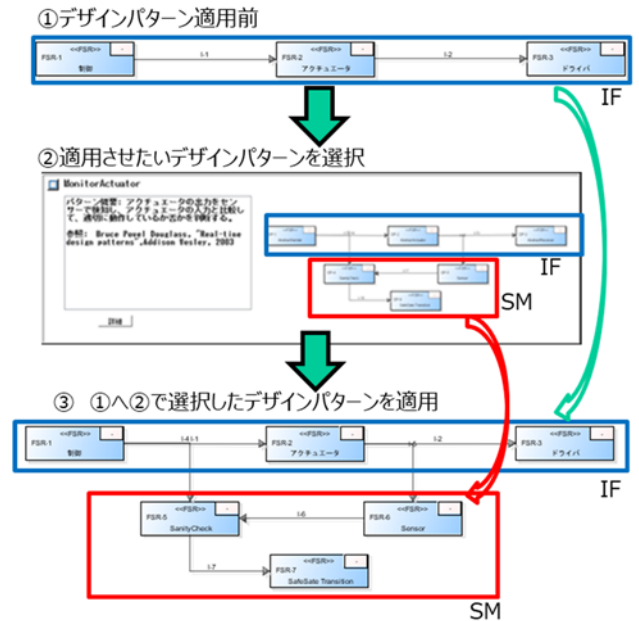
ツール連携の一例(SCDL⇔SysML変換)

SysMLで設計したアーキテクチャを安全観点(SCDL)で表示、両者の一貫性の確保が可能



デザインパターン

実績ある安全機構を再利用可能とし安全設計を効率化



Safilia R5 新機能/機能強化

Safilia Designer V5.0

モデル要素として、故障モデルと連鎖矢印を追加

Safilia Analysis V3.0

安全要求侵害分析(SRVA)  
- ガイドワード機能を追加

Safilia Binder V2.0

- SysML連携機能強化
  - SysMLとSCDL変換のユーザー操作手順を改善し、変換時間を短縮
- 故障連鎖表示機能
  - 故障が安全コンセプト図上のどの要求に対して波及するか確認が可能
  - ハイライト機能で、安全機構の効果の確認が可能

【新機能】ガイドワード機能

上位SR侵害の可能性のある機能不全・安全方策の決定とハイライト表示によりガイドワードの網羅性が確認可能

SRVA サンプル - 安全要求侵害分析 (SRVA)	安全要求侵害分析 (SRVA)	SRVA サンプル	ホーム	ハイライト表示	設定	更新 (F5)		
要求グループ別	要求グループID	ID	安全要求 (SR)	ASIL	ガイドワード	上位 SR 侵害の可能性のある機能不全	安全方策	安全方策ID
MF	SR-1	SRP-7	非意図的故障	機能(D)	閉(ring)	非意図的無しと判定される。	誤って意図的無しと判定する時は、自動ブレーキ制御禁止とする。	
					逆(reverse)			
					他(other than)			
					次(more)			
					少(less)			
					等(as well as)			
					部(part of)			
					準(nearly)			
					遅(late)			
					前(before)			
					後(after)			