

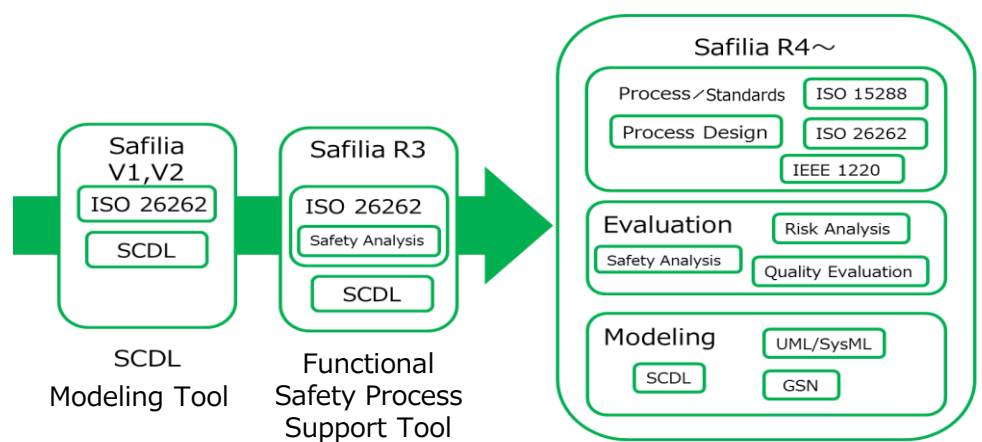
Safilia R5

Safilia Designer

Safilia Integrator

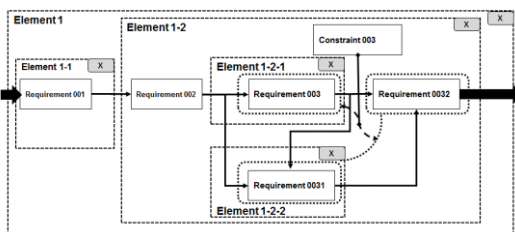
System Engineering Support Tool

- ① Safety Concept Design support based on SCDL
- ② Supports Integrated Design of Functional Development as well as Safety Development
- ③ Supports Safety Design incorporating Requirements and Analysis along with Safety Concepts



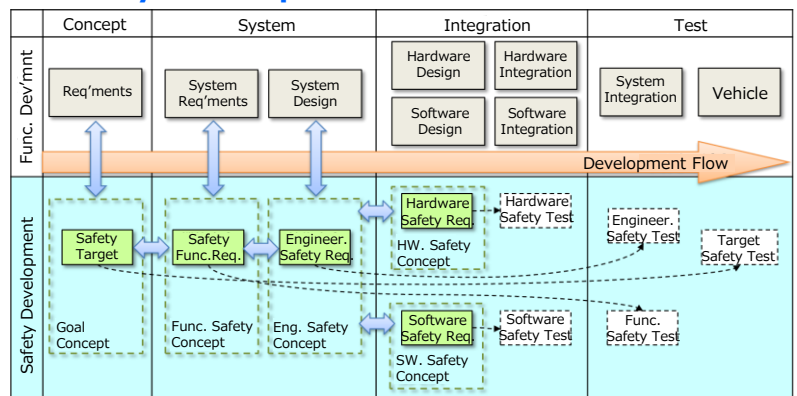
Engineering Process Support Platform

① Safety Concept Design support based on SCDL

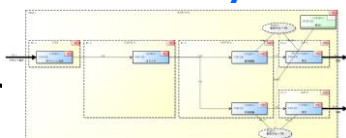
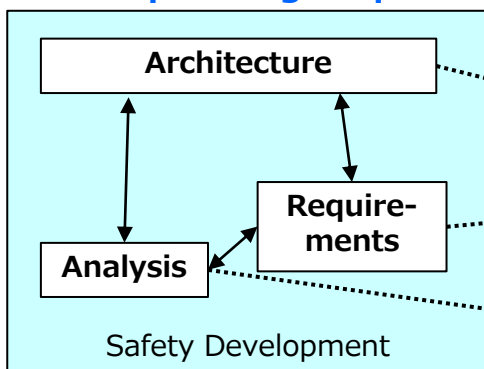


Visualization of Safety Architecture
SCDL (Safety Concept Description Language)
SCN-SG URL : <https://ssl.scn-sg.com>

② Supports Integrated Design of Functional Development as well as Safety Development



③ Supports Safety Design incorporating Requirements and Analysis along with Safety Concepts



SCDL Safety Concept Diagram

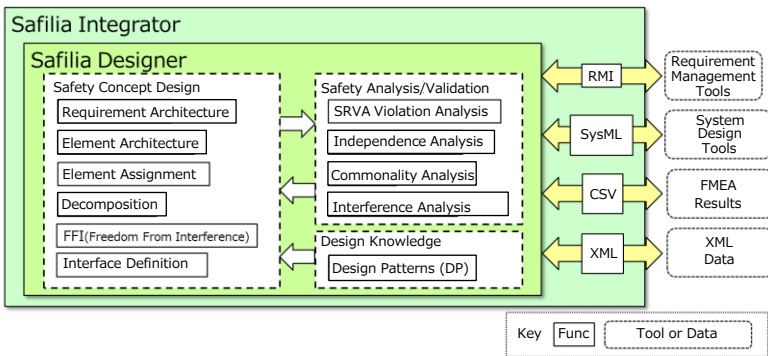
Requirement ID	ID	Name	Type	ASIL	Reason for decomposition	Allocated element	Requirement Group ID	Requirement's natural language description (text)	Input	Output
SS-2	Requirement1	Calculate target speed of vehicle	FSR	B(D)	Excessive brake when target vehicle speed is too slow	EL-3	MF	MF-2	F-8	F-10
FSR-7	Defect obstacle	Defect obstacle	FSR	B(D)	Excessive brake when target vehicle speed is too slow	EL-3	MF	MF-1	SS-11	F-13
FSR-8	Cc	Cc	FSR	B(D)	Excessive brake when target vehicle speed is too slow	EL-3	MF	F-1	SS-12	F-14
FSR-10	Judge crash possibility	Judge crash possibility	FSR	B(D)	Excessive brake when target vehicle speed is too slow	EL-3	MF	MF-1	F-15	F-8
FSR-11	Calculate target deceleration	Calculate target deceleration	FSR	B(D)	Excessive brake when target deceleration is too slow	EL-4	MF	MF-2	F-16	F-12
FSR-12	Guard upper/lower limit of target deceleration	Guard upper/lower limit of target deceleration	FSR	B(D)	Excessive brake when guard value of upper limit speed is excessive	EL-4	SM	SM-2	F-17	SS-13
FSR-13	Guard upper/lower limit of vehicle speed	Guard upper/lower limit of vehicle speed	FSR	B(D)	Excessive brake when guard value of upper limit speed is excessive	EL-4	SM	SM-1	F-18	F-15

Requirement Group Type	Requirement Group ID	ID	Safety Requirement (SR)	ASIL	Potential malfunctions which violate upper SR	Safety Measure	Safety Measure ID
MF	MF-1	FSR-7	Detect obstacle	Q(M/D)	detect obstacle by mistake	stop automatic brake control when sensor obstacle detection has occurred	SM-1
		FSR-10	Judge crash possibility	Q(M/D)	Misjudge crash possibility	Stop automatic brake control when misjudgment has occurred	SM-2
	MF-2	FSR-11	Calculate target speed of vehicle	B(D)	Excessive brake when target vehicle speed is too slow	Set upper limit to target deceleration	
		FSR-12	Calculate target deceleration	B(D)	Excessive brake when target deceleration is too slow		
		FSR-13	Guard upper/lower limit of vehicle speed	D(D)	Excessive brake when guard value of upper limit speed is excessive	Consider in system level (Part-4)	
SM	SM-1	FSR-14	Judge valid/invalid of	D(D)	Misjudging valid/invalid of obstacle		

Safety Requirement Violation Analysis (SRVA)

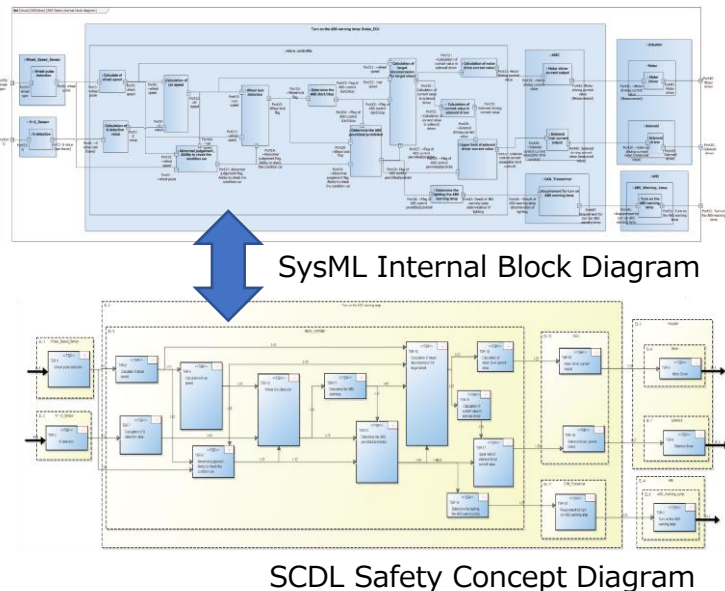
Tool Combinations

Can combine with many tools and resources relating to Safety Design



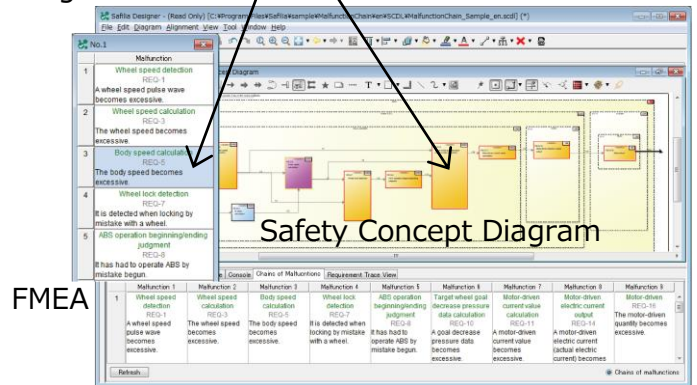
Example of Tool Collaboration (SCDL<->SysML)

Architecture designed in SysML can be displayed in SCDL – Equivalence can be confirmed



Visualizing Fault Linkage

Clicking on a Fault in the FMEA highlights the functions affected by that fault in the concept diagram



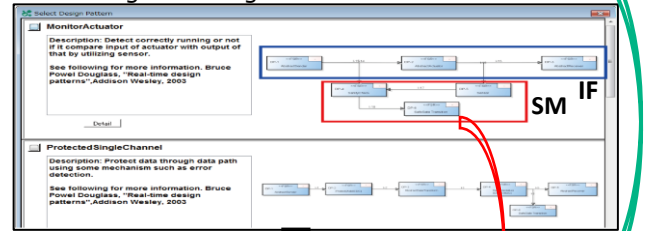
Design Patterns

Proven Safety Structures can be reused giving more efficient Safety Design

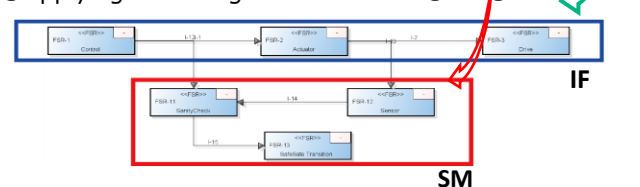
① Before applying Design Pattern



② Selecting the Design Pattern



③ Applying the Design Pattern from ② to ①



[NEW!] Guide Word Function

Possible to confirm Guide Word coverage from selection and highlighting of Safety Measures and Function Weaknesses which have possible High-Level Safety Requirement Violations

03.PAA (TSC Level) 3 - Safety Requirement Violation Analysis (SRVA)							
Safety Requirement Violation Analysis (SRVA)				03.PAA (TSC Level) 3			
Requirement Group Type	Requirement ID	ID	Safety Requirement (SR)	ASIL	Guide words	Potential failures which violate upper SR	Safety Measure
	TR-1		Switch sensor		no reverse other than more less as well as part of early late before after		SM-1

Safilia R5 New/Improved Functions

Safilia Designer R5.0

Addition of Linkage Arrows and Fault Models as Design Elements

Safilia Analysis V3.0

Safety Requirement Violation Analysis (SRVA)
- Guide Word Function added

Safilia Binder V2.0

SysML related functions improved
- SysML to SCDL conversion process improved, leading to reduction in conversion time
Fault Linkage Display Function
- Possible to confirm effects of Faults on Requirements in Safety Concept Diagram
- Highlight Function allows confirmation of effectiveness of Safety Structures

