Experiences with safety assessments and safety cases

What can go wrong and hints to do it right

ZF DIQS11 Frank König

2021-08-23

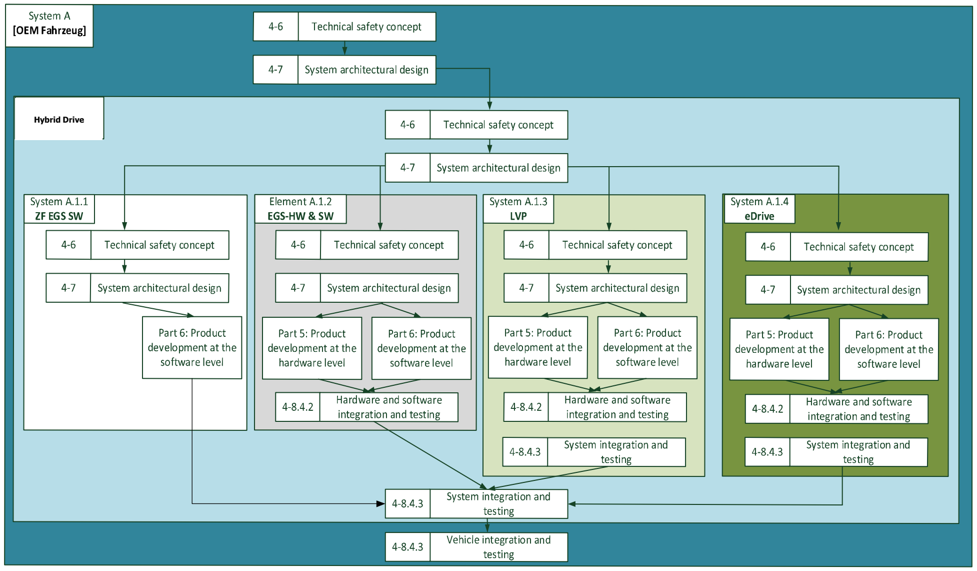
Motivation

Safetycases get more complex due to:

- complex systems,
  esp. AD Systems

- complex supply chains

- Additional processes related to functional safety have to be considered
  (SOTIF, Cybersecurity, High voltage, ….)



System A
[OEM Fahrzeug]
4-6 Technical safety concept
4-7 System architectural design
Hybrid Drive
4-6 Technical safety concept
4-7 System architectural design
System A.1.1
ZF EGS SW
4-6 Technical safety concept
4-7 System architectural design
Part 6: Product development at the software level
Element A.1.2
EGS-HW & SW
4-6 Technical safety concept
4-7 System architectural design
Part 5: Product development at the hardware level
Part 6: Product development at the software level
4-8.4.2 Hardware and software integration and testing
System A.1.3
LVP
4-6 Technical safety concept
4-7 System architectural design
Part 5: Product development at the hardware level
Part 6: Product development at the software level
4-8.4.2 Hardware and software integration and testing
4-8.4.3 System integration and testing
System A.1.4
eDrive
4-6 Technical safety concept
4-7 System architectural design
Part 5: Product development at the hardware level
Part 6: Product development at the software level
4-8.4.2 Hardware and software integration and testing
4-8.4.3 System integration and testing
4-8.4.3 System integration and testing
4-8.4.3 Vehicle integration and testing

Glances to key points of ZF approach will follow on the next slides …

„Definition of safe"

Relation to agile „definition of done"

Our project context definition

100 % of defined safety work products available and released

100 % safety requirements coverage

100 % safety test coverage

100 % safety tests passed or justified

100 % of reported anomalies / deviations closed or justified

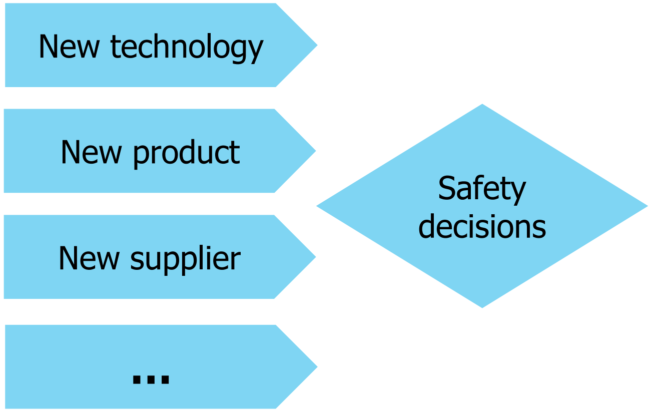
Mainly a requirements management topic:
- Traceability
- Safety attribute

ISO 26262 topics

Safety assessment passed

Safety audit passed

Risk based approach widely used



safety assessment strategy
- use an external technical service for new systems,
- Internal assessors for follow up projects

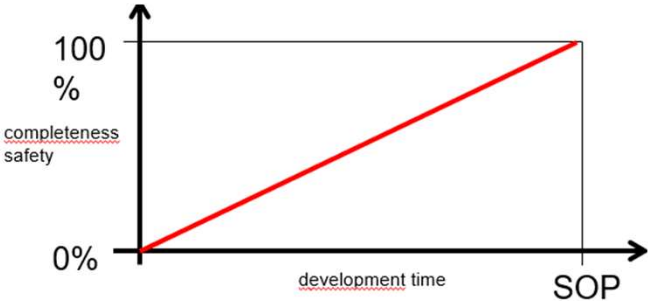
Tailor the safety life cycle

But you can also **add additional topics** like:
- External safety assessment for suppliers
- Additional reviews

Release types with different criteria and usages

Distribute the realization of the safety functions over the project time

Analyses:
Start early with the analyses, see them as support for design

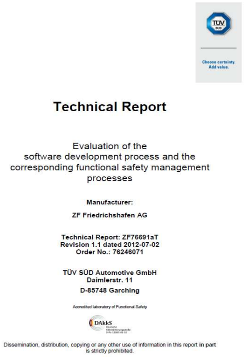


L1	L2	L3a	L3b	L4
test rig	test area	public restricted	public no restrictions	series release

Compliance & acceptance

External safety reviews:

- standard processes
- new products



Choose certainty.
Add value.

Technical Report

Evaluation of the
software development process and the
corresponding functional safety management
processes

Manufacturer:

ZF Friedrichshafen AG

Technical Report: ZF76691aT
Revision 1.1 dated 2012-07-02
Order No.: 76246071

TÜV SÜD Automotive GmbH
Daimlerstr. 11
D-85748 Garching

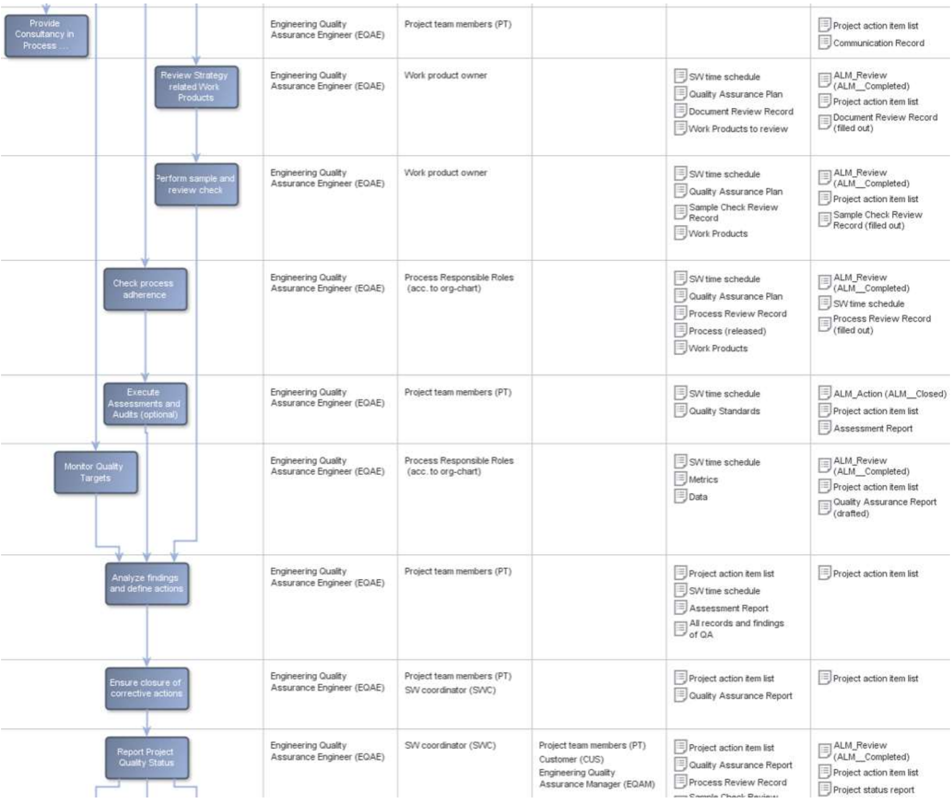
Accredited laboratory of Functional Safety

Dissemination, distribution, copying or any other use of information in this report **in part** is strictly prohibited.

Internal reviews in cooperation with EQAs:

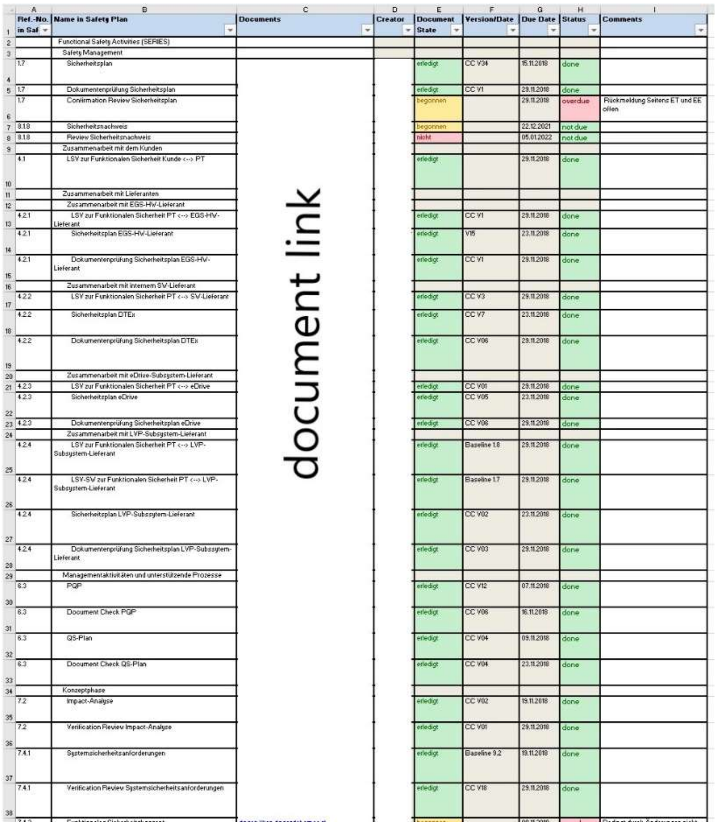
- Process compliance
- Work products
- Gate Reviews
- Safety Release Levels

- Safety audits
- Safety assessments for follow up projects



Provide Consultancy in Process …	Engineering Quality Assurance Engineer (EQAE)	Project team members (PT)			Project action item list Communication Record
Review Strategy related Work Products	Engineering Quality Assurance Engineer (EQAE)	Work product owner		SW time schedule Quality Assurance Plan Document Review Record Work Products to review	ALM_Review (ALM__Completed) Project action item list Document Review Record (filled out)
Perform sample and review check	Engineering Quality Assurance Engineer (EQAE)	Work product owner		SW time schedule Quality Assurance Plan Sample Check Review Record Work Products	ALM_Review (ALM__Completed) Project action item list Sample Check Review Record (filled out)
Check process adherence	Engineering Quality Assurance Engineer (EQAE)	Process Responsible Roles (acc. to org-chart)		SW time schedule Quality Assurance Plan Process Review Record Process (released) Work Products	ALM_Review (ALM__Completed) SW time schedule Process Review Record (filled out)
Execute Assessments and Audits (optional)	Engineering Quality Assurance Engineer (EQAE)	Project team members (PT)		SW time schedule Quality Standards	ALM_Action (ALM__Closed) Project action item list Assessment Report
Monitor Quality Targets	Engineering Quality Assurance Engineer (EQAE)	Process Responsible Roles (acc. to org-chart)		SW time schedule Metrics Data	ALM_Review (ALM__Completed) Project action item list Quality Assurance Report (drafted)
Analyze findings and define actions	Engineering Quality Assurance Engineer (EQAE)	Project team members (PT)		Project action item list SW time schedule Assessment Report All records and findings of QA	Project action item list
Ensure closure of corrective actions	Engineering Quality Assurance Engineer (EQAE)	Project team members (PT) SW coordinator (SWC)		Project action item list Quality Assurance Report	Project action item list
Report Project Quality Status	Engineering Quality Assurance Engineer (EQAE)	SW coordinator (SWC)	Project team members (PT) Customer (CUS) Engineering Quality Assurance Manager (EQAM)	Project action item list Quality Assurance Report Process Review Record Sample Check Review	ALM_Review (ALM__Completed) Project action item list Project status report

XLS Cemetery vs. argued Safety Case



	A	B	C	D	E	F	G	H	I
1	Ref.-No. in Saf	Name in Safety Plan	Documents	Creator	Document State	Version/Date	Due Date	Status	Comments
2		Functional Safety Activities (SERIES)							
3		Safety Management							
4	1.7	Sicherheitsplan			erledigt	CC V34	15.11.2018	done	
5	1.7	Dokumentenprüfung Sicherheitsplan			erledigt	CC V1	29.11.2018	done	
6	1.7	Confirmation Review Sicherheitsplan			begonnen		29.11.2018	overdue	Rückmeldung Seitens ET und EE offen
7	8.1.8	Sicherheitsnachweis			begonnen		22.12.2021	not due	
8	8.1.8	Review Sicherheitsnachweis			nicht		05.01.2022	not due	
9		Zusammenarbeit mit dem Kunden							
10	4.1	LSV zur Funktionalen Sicherheit Kunde <--> PT			erledigt		29.11.2018	done	
11		Zusammenarbeit mit Lieferanten							
12		Zusammenarbeit mit EGS-HV-Lieferant							
13	4.2.1	LSV zur Funktionalen Sicherheit PT <--> EGS-HV-Lieferant			erledigt	CC V1	29.11.2018	done	
14	4.2.1	Sicherheitsplan EGS-HV-Lieferant			erledigt	V15	23.11.2018	done	
15	4.2.1	Dokumentenprüfung Sicherheitsplan EGS-HV-Lieferant			erledigt	CC V1	29.11.2018	done	
16		Zusammenarbeit mit internem SV-Lieferant							
17	4.2.2	LSV zur Funktionalen Sicherheit PT <--> SV-Lieferant			erledigt	CC V3	29.11.2018	done	
18	4.2.2	Sicherheitsplan DTEx			erledigt	CC V7	23.11.2018	done	
19	4.2.2	Dokumentenprüfung Sicherheitsplan DTEx			erledigt	CC V06	29.11.2018	done	
20		Zusammenarbeit mit eDrive-Subsystem-Lieferant							
21	4.2.3	LSV zur Funktionalen Sicherheit PT <--> eDrive			erledigt	CC V01	29.11.2018	done	
22	4.2.3	Sicherheitsplan eDrive			erledigt	CC V05	23.11.2018	done	
23	4.2.3	Dokumentenprüfung Sicherheitsplan eDrive			erledigt	CC V06	29.11.2018	done	
24		Zusammenarbeit mit LVP-Subsystem-Lieferant							
25	4.2.4	LSV zur Funktionalen Sicherheit PT <--> LVP-Subsystem-Lieferant			erledigt	Baseline 1.8	29.11.2018	done	
26	4.2.4	LSV-SV zur Funktionalen Sicherheit PT <--> LVP-Subsystem-Lieferant			erledigt	Baseline 1.7	29.11.2018	done	
27	4.2.4	Sicherheitsplan LVP-Subssytem-Lieferant			erledigt	CC V02	23.11.2018	done	
28	4.2.4	Dokumentenprüfung Sicherheitsplan LVP-Subssytem-Lieferant			erledigt	CC V03	29.11.2018	done	
29		Managementaktivitäten und unterstützende Prozesse							
30	6.3	PQP			erledigt	CC V12	07.11.2018	done	
31	6.3	Document Check PQP			erledigt	CC V06	16.11.2018	done	
32	6.3	QS-Plan			erledigt	CC V04	09.11.2018	done	
33	6.3	Document Check QS-Plan			erledigt	CC V04	23.11.2018	done	
34		Konzeptphase							
35	7.2	Impact-Analyse			erledigt	CC V02	19.11.2018	done	
36	7.2	Verification Review Impact-Analyse			erledigt	CC V01	29.11.2018	done	
37	7.4.1	Systemsicherheitsanforderungen			erledigt	Baseline 9.2	19.11.2018	done	
38	7.4.1	Verification Review Systemsicherheitsanforderungen			erledigt	CC V18	29.11.2018	done	

document link

ISO P2: Ch 6.4.8.1:

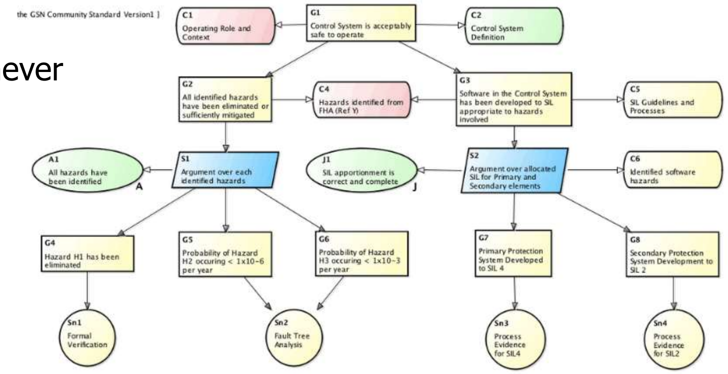
A safety case shall be developed, in accordance with the safety plan, in order to provide the argument for the achievement of functional safety.

In stable organizations /processes we can live with the XLS list.

Text documents may add:

Arguments for processes and techniques used.

Formal GSN like in the picture I have never seen in automotive.


the GSN Community Standard Version1]
C1 Operating Role and Context
G1 Control System is acceptably safe to operate
C2 Control System Definition
G2 All identified hazards have been eliminated or sufficiently mitigated
C4 Hazards identified from FHA (Ref Y)
G3 Software in the Control System has been developed to SIL appropriate to hazards involved
C5 SIL Guidelines and Processes
A1 All hazards have been identified
A
S1 Argument over each identified hazards
J1 SIL apportionment is correct and complete
J
S2 Argument over allocated SIL for Primary and Secondary elements
C6 Identified software hazards
G4 Hazard H1 has been eliminated
G5 Probability of Hazard H2 occuring < 1x10-6 per year
G6 Probability of Hazard H3 occuring < 1x10-3 per year
G7 Primary Protection System Developed to SIL 4
G8 Secondary Protection System Development to SIL 2
Sn1 Formal Verification
Sn2 Fault Tree Analysis
Sn3 Process Evidence for SIL4
Sn4 Process Evidence for SIL2

Picture from: Visualizing Safety Cases – Tim Kelly on GSN (Goal Structuring Notation) – Are you modeling? – The most essential concepts in modeling today

What’s next?

Safety Audit
- actual we use XLS checklists
- SOQRATES approach in CAPADV is used for combined assessments
- in future Safety Extension of ASPICE 4.0 will be the goal, we contribute …

Safety Tooling
Beside the analyses tools, we plan a new cloud based workflow and reporting.

Agile Safety
Establish safety as stakeholder
Safety documentation adds value

Questions?

Don‘t forget your life assurance

Include safety regression tests for every release you deliver on the road …

Thank you very much for your attention!