



Erprobung einer modellbasierten integrierten Werkzeuflösung für funktionale Sicherheit bei General Motors

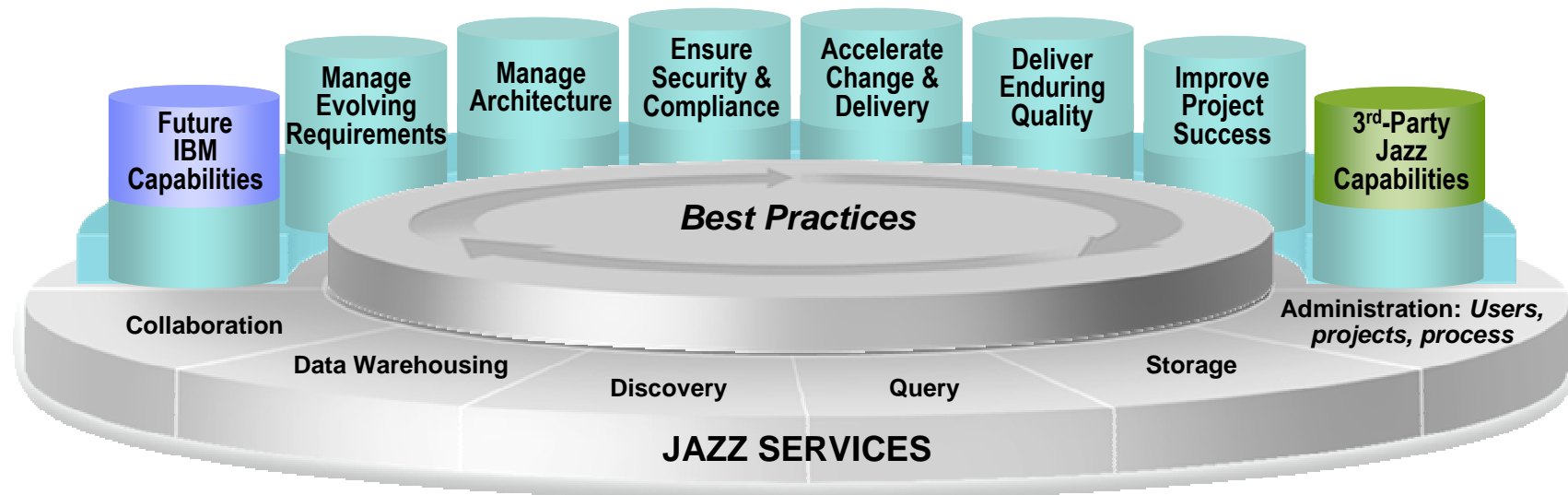
Dr.-Ing. Manfred Schölzke, Adam Opel AG
Michael Soden, ikv++ technologies ag



ikv

Motivation – Situation bei GM / Opel (1/2)

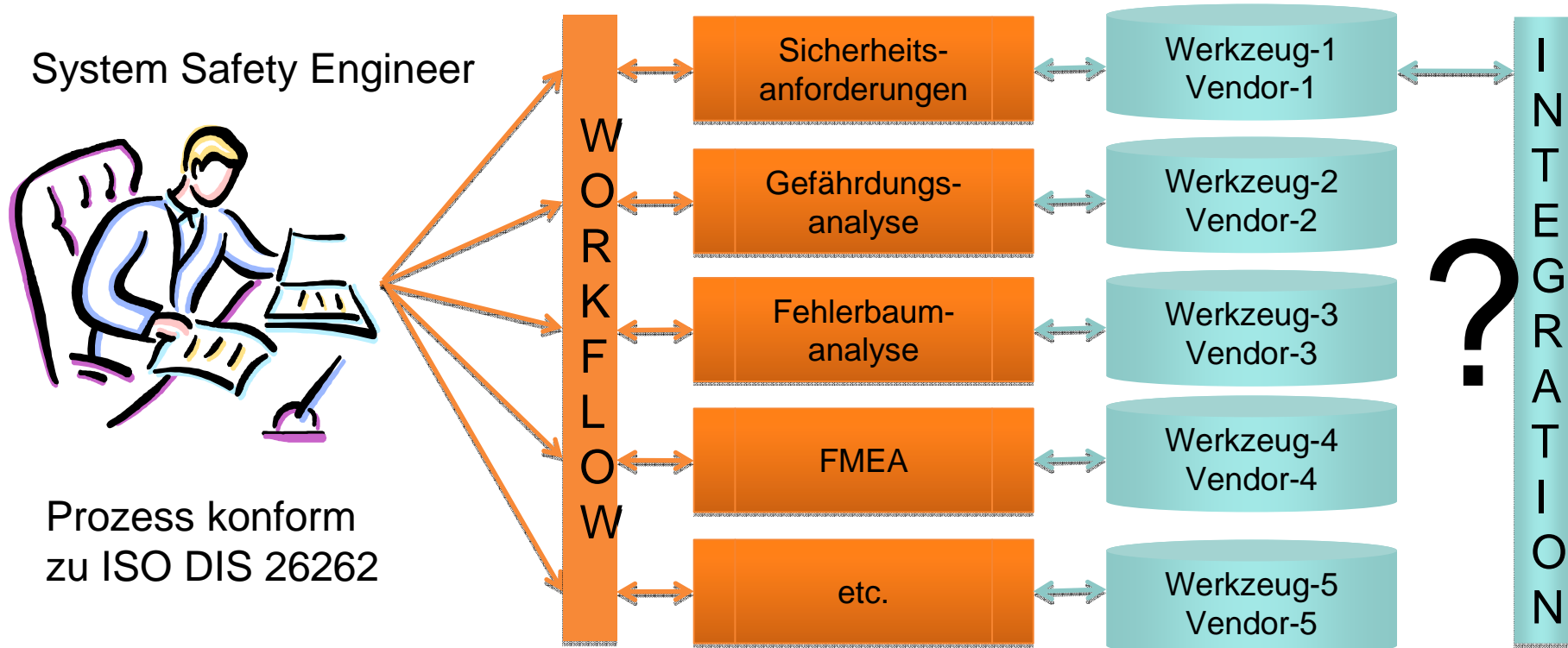
„Software und Systems Engineering“ Werkzeugkette



- basierend auf IBM Rational Tool-chain und Jazz Framework
- siehe YouTube-Video „The Chevrolet Volt: IBM Rational Software helps GM deliver smarter products“ unter <https://www.youtube.com/watch?v=CjjASGV36mw>

Motivation – Situation bei GM / Opel (2/2)

„System Safety Engineering“ Prozess



System Safety Engineer



Prozess konform
zu ISO DIS 26262

Status quo:

- keine durchgängige Integration der verschiedenen Werkzeuge
- Traceability und Konsistenzhaltung aufwändig und fehleranfällig



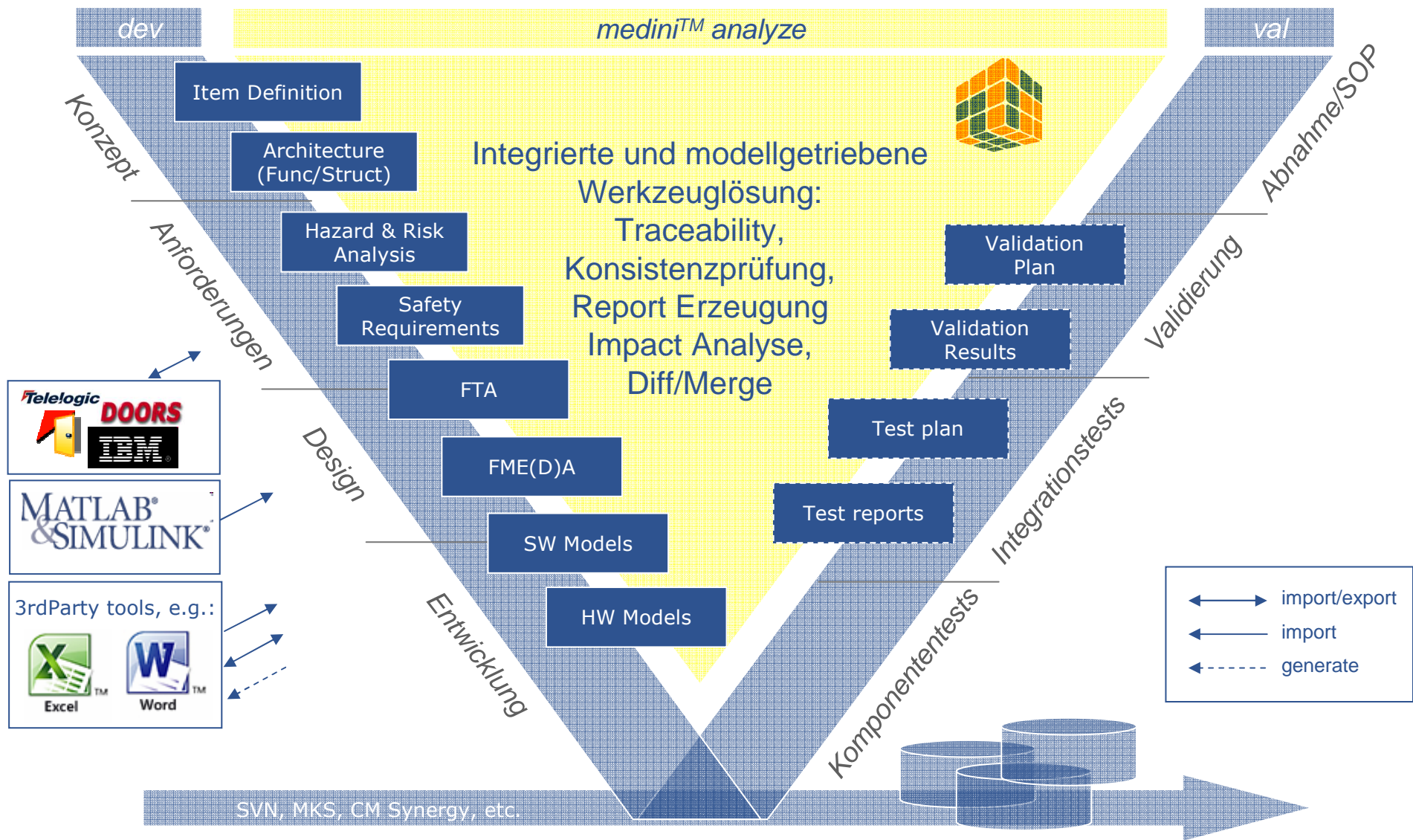
Motivation – Ziele der Pilotierung für GM / Opel

Pilotprojekt mit ikv

- Welche Funktionalität bietet das medini™ analyze Werkzeug?
 - auch im Vergleich zu anderen System Safety Werkzeugen
- Wie lässt sich der GM „System Safety Engineering“ Prozess in medini™ analyze abbilden?
 - Konfigurierbarkeit und Flexibilität des Werkzeugs
- Welche Vorteile bieten sich hinsichtlich Traceability und Konsistenzhaltung?
 - sowie allgemeine Performanz- und Usability-Aspekte.



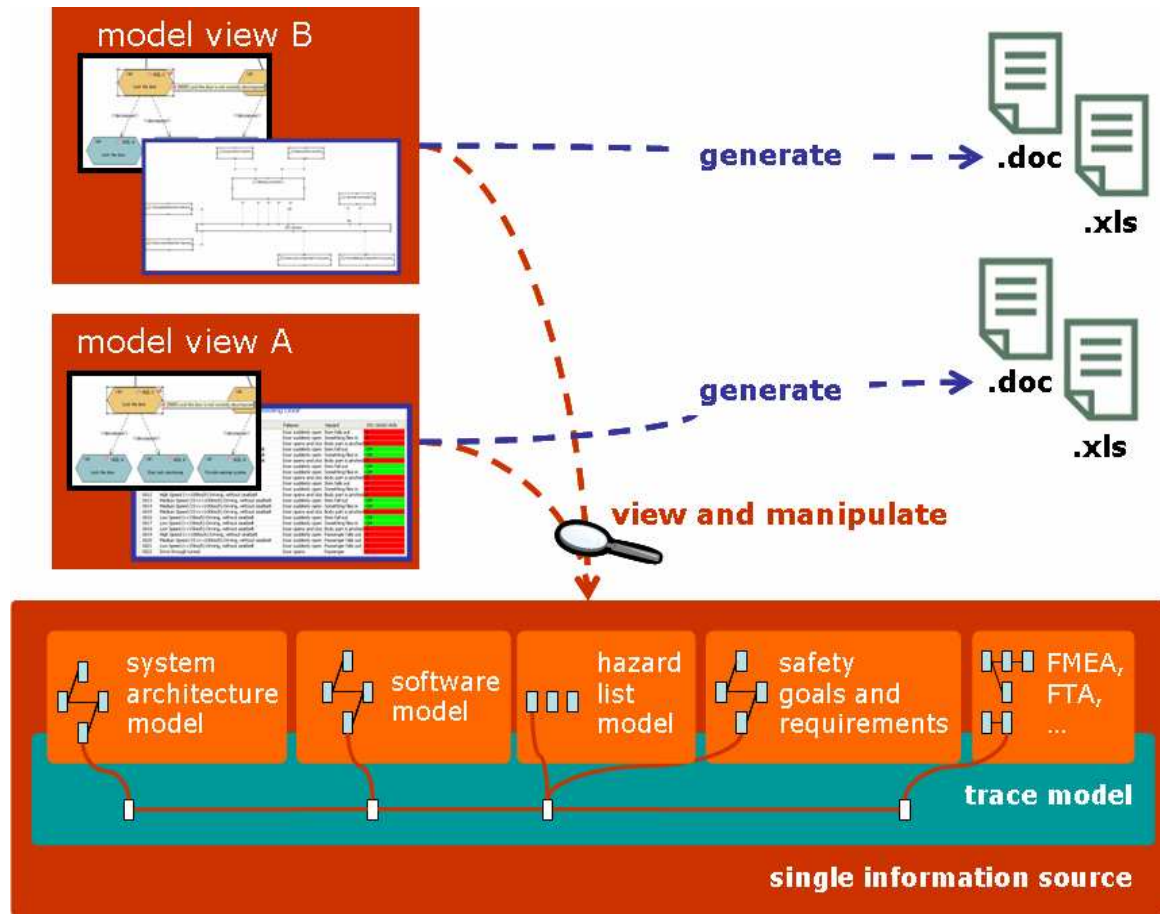
medini™ analyze



medini™ analyze

Integrierte Werkzeuglösung für Funktionale Sicherheit

- Unterstützt ISO 26262 Workflows und Arbeitsprodukte
- Realisiert „single-source-of-information“ Prinzip
- Konsistenzprüfung über Sicherheitsanalysen/ Systemmodellen
- Modellbasierter Ansatz mit verschiedenen Sichten, Suchfunktionen, Impact Analyse, etc.



Gefährdungsanalyse mit medini™ analyze

The screenshot displays the medini analyze software interface for a hazard analysis of a driver airbag system. The interface is divided into several main sections:

- Model Browser (Left):** Shows a hierarchical tree of the project structure, including ISO 26262 Documents, Company Style, Item Definition, Preliminary Architecture, Airbag System components (Front Sensors, ACU, Driver Airbag, Front passenger Airbag), Driver Airbag functions, AirbagSystem Functions, and Hazard Analysis and Risk Assessment.
- Manage Hazardous Events for Driver Airbag (Top Center):** A table listing hazardous events (HE001-HE004) with columns for ID, Location, Road Conditions, Malfunction behavior, Hazard Description, Potential Effect, Severity, Exposure, Controllability, ISO 26262 ASIL, and Safety Goal.
- Functional Block Diagram (Center):** A diagram showing the ACU (Airbag Control Unit) connected to Driver Airbag and Front Passenger Airbag. The ACU contains a Micro controller, Power Resistor, and Inflation Watchdog. It is connected to a CAN bus, which in turn connects to Acceleration Sensor, Impact Sensor, and Speed Sensor.
- Function Details (Right):** A panel for the function "[F001] Deploy Airbag - AirbagSystem1.4". It includes general information (ID: F001, Name: Deploy Airbag), a description, and related functions (Requires: [F002] Detect Collision, [F003] Ignite Gas Generator; Contributes to: empty).
- Problems View (Bottom):** A table showing identified errors related to hazardous events HE005.

ID	Location	Road Condi...	(Mal)function behavior of E...	Hazard Description	Potential Effect	Severity	Exposure	Controllability	ISO 26262 ASIL	Safety Goal
HE001	Highway	ALL	[MF001] Unintended Deployment	Driver hit by airbag	Distraction/injury of driver. Potential accident	S3	E4	C2	A	[G001] Prevent unintended deployment (ASIL C)
HE002	Parking	no influence	[MF001] Unintended Deployment	Driver hit by airbag	Injury of driver	S1	E3	C2	QM	
HE003	Highway	ALL	[MF002] Airbag does not deploy when required	Driver hits dashboard or steering wheel	Serious injuries	S3	E1	C3	A	[G002] Ensure that Airbag deploys in crash situation (ASIL A)
HE005	Highway	ALL	[MF003] Late Deployment	Driver hits dashboard or steering wheel	Serious injuries	S3	E1	C3	A	
HE004	Accident site	no influence	[MF001] Unintended Deployment	Airbag may hit persons inside car or rescue people	Injuries or serious injuries	S2	E3	C2	A	[G003] Prevent unintended deployment after crash (ASIL A)

Description	Problem ID	Location
The Hazardous-Event HE005 : Driver hits dashboard or steering wheel [A] is safety related and has no safety goal assigned	0002	Driver Airbag Hazards::<HazardousEvent>
Hazardous-Event HE005 : Driver hits dashboard or steering wheel [A] has no justification given for the estimated ranking of exposure for the ISO ASIL	0010	Driver Airbag Hazards::<HazardousEvent>

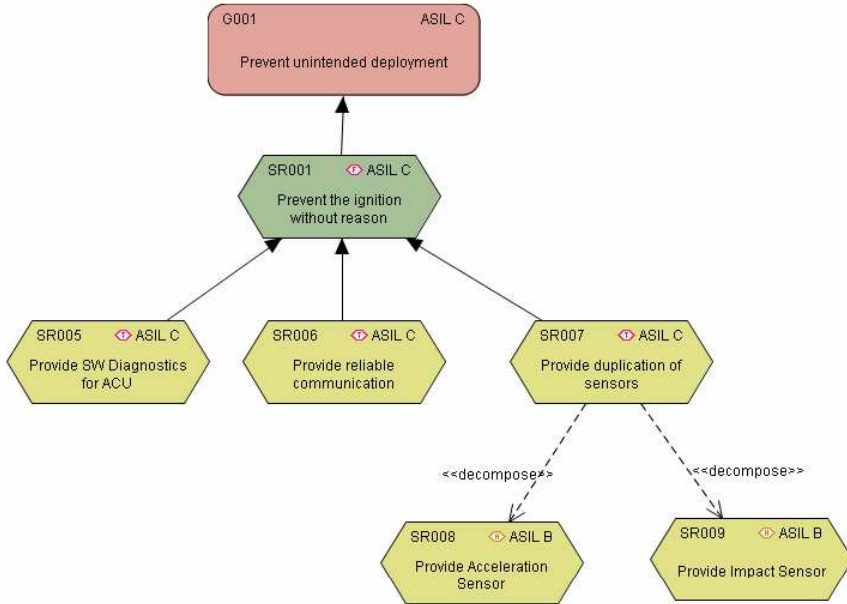
medini analyze

File Edit Diagram Project Traces Reporting Search Window Help

Tahoma 9 B I A 100%

SVN Reposito... analyze

*AB Safety Goals - AirbagSystem1.4



```

    graph TD
      G001[G001 ASIL C  
Prevent unintended deployment]
      SR001{{SR001 ASIL C  
Prevent the ignition  
without reason}}
      SR005{{SR005 ASIL C  
Provide SW Diagnostics  
for ACU}}
      SR006{{SR006 ASIL C  
Provide reliable  
communication}}
      SR007{{SR007 ASIL C  
Provide duplication of  
sensors}}
      SR008{{SR008 ASIL B  
Provide Acceleration  
Sensor}}
      SR009{{SR009 ASIL B  
Provide Impact Sensor}}

      SR001 --> G001
      SR005 --> SR001
      SR006 --> SR001
      SR007 --> SR001
      SR008 -.-> SR007
      SR009 -.-> SR007
      style SR008 stroke-dasharray: 5 5
      style SR009 stroke-dasharray: 5 5
  
```

AB Safety Goals - AirbagSystem1.4

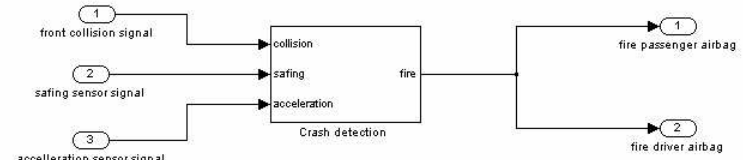
Safety Requirements Editor

ID	Name	Description	Kind	
SR001	Prevent the ignition without reason		FUNCTIONAL	Add
SR006	Provide reliable communication		TECHNICAL	Add After
SR007	Provide duplication of sensors		TECHNICAL	Insert
SR005	Provide SW Diagnostics for ACU	Self-check using redundant communication	TECHNICAL	Duplicate
SR002	After a crash is detected and airbags are fired once, switch OFF airbag system.	handle this in the algorithms	TECHNICAL	Edit
SR011	ensure that fire command is issued only once		FUNCTIONAL	Remove
SR008	Provide Acceleration Sensor		HARDWARE	
SR009	Provide Impact Sensor		HARDWARE	

Safety Requirements

ACU - AirbagSystem1.4

File Edit View Simulation Format Tools Help



```

    graph LR
      FCS[1 front collision signal] --> C[collision]
      SSS[2 safing sensor signal] --> S[safing]
      ACS[3 acceleration sensor signal] --> A[acceleration]
      C --> CD[Crash detection]
      S --> CD
      A --> CD
      CD --> FPA[1 fire passenger airbag]
      CD --> FDA[2 fire driver airbag]
  
```

Trace Matrix

Configuration

Traces	ACU	front collision signal	safing sensor signal	acceleration sensor signal	Crash detection	collision	safing	acceleration	Logical Operator	acceleration compare	acceleration threshold	collision compare	collision threshold	safing compare	safing threshold	fire	fire passenger airbag	fire driver airbag
AB Safety Goals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR001] Prevent the igniti...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR006] Provide reliable c...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR007] Provide duplicati...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR005] Provide SW Diag...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR002] After a crash is d...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR011] ensure that fire ...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR008] Provide Acceler...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[SR009] Provide Impact S...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Allocate Requirements - AirbagSystem1.4

Sicherheitsanforderungen,
Traceability und
Systemmodelle
in medini™ analyze

FMEA Worksheet

Worksheet Header

Review RPN FMEDA

Add component/function Add Failure mode Add Failure effect Add failure cause Add current design control Add recommended action Add taken action Remove

Components/Functions	Failure Ra...	Potential Failure Modes	Failure Category	Failure rat...	Failure Ra...	Potential Failure Effects	Severity	Max. Severity	Risk Class	Potential Failure Causes	Occurrence	Current Design Controls Prevention	Cu
ACU	0.0												
Micro controller	200.0	All	SafeDetected	100.0	200.0	calculation error	7	7	N	communication problem	4		HW
Power Reserve	20.0	All	DangerousUndetected	100.0	20.0								
Selftest Watchdog	10.0	signal pulse/spike	NoEffect	100.0	10.0	calculation error	7	7	N	communication problem	3		SW
Driver Airbag Initiator	9.0	short circuit	SafeDetected	100.0	9.0	unintended deployment	10	10	S	cabling	6		nor
Front Passenger Airbag Initiator	9.0	short circuit	SafeDetected	100.0	9.0	unintended deployment	10	10	S	cabling	6		
CAN	100.0	delayed signal	DangerousDetected	100.0	100.0	late deployment none rthelvnent	3 3		N N	cabling overhaul	6 6		

Total Failure Rate: 362 (in FIT) Undetected Dangerous Failure Rate: 28 (in FIT) No Part Failure Rate: 8,5 (in FIT) Safe Failure Fraction: 92,2%

Custom Properties

Customize

FMEA Editor

DC for Unintended Deployment: [G001] Prevent unintended deployment (ASIL C) - AirbagSystem1.4

Diagnostic Coverage and Hardware Metrics

Safety Goal Details

Diagnostic Coverage Worksheet Details

Show Single-Point Fault Metric Show Latent Fault Metric

Component Name	Failure Ra...	Safety Related	Potential Failure Modes	Failure rat...	Violates safety goal	SM prevents violation	SPF Coverage (in %)	SPF (in FIT)	Multiple failures violate safety goal	SM prevents FM from bei...	LF Coverage (in %)	LF (in FIT)
ACU	0.0	<input checked="" type="checkbox"/>										
Micro controller	200.0	<input checked="" type="checkbox"/>	All	100.0	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Self-test by software: limited number of patterns (one channel) Self-test supported by hardware (one-channel) 	99.0	2.0	<input type="checkbox"/>		0.0	198.0
Power Reserve	20.0	<input checked="" type="checkbox"/>	All	100.0	<input type="checkbox"/>	<ul style="list-style-type: none"> Voltage or current control (input) Voltage or current control (output) 	99.0	0.2	<input type="checkbox"/>			
Selftest Watchdog	10.0	<input checked="" type="checkbox"/>	All	100.0	<input type="checkbox"/>		0.0	10.0	<input checked="" type="checkbox"/>			
Driver Airbag	0.0	<input checked="" type="checkbox"/>										

Total

Total Failure Rate: 375 (in FIT)
Total Safety Related: 375 (in FIT)
Total Not Safety Related: 0 (in FIT)

Single-Point Fault Metric

Total Single-Point Fault Failure Rate: 12,8 (in FIT)
Single-Point Fault Metric: 96,5% (expected ≥97%)

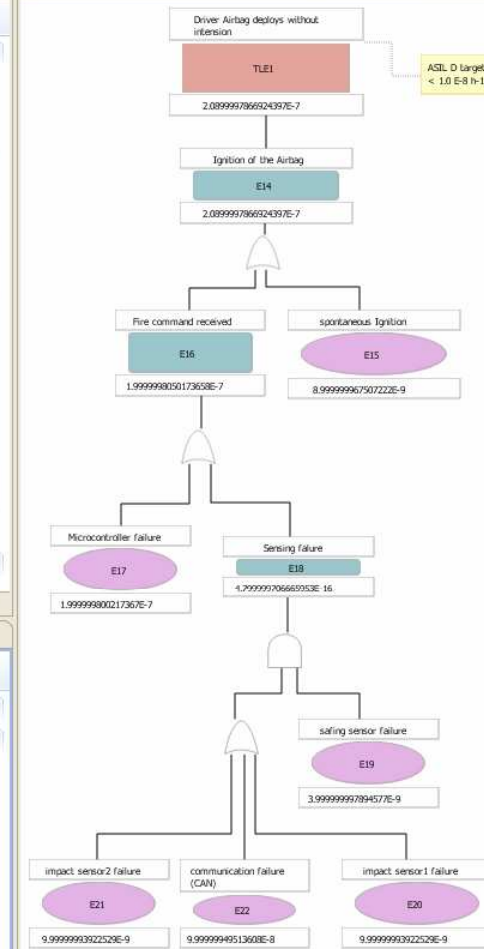
Latent Fault Metric

Total Latent Fault Failure Rate: 115 (in FIT)
Latent Fault Metric: 68,2% (expected ≥80%)

Custom Properties

Diagnostic Coverage and Hardware Metrics

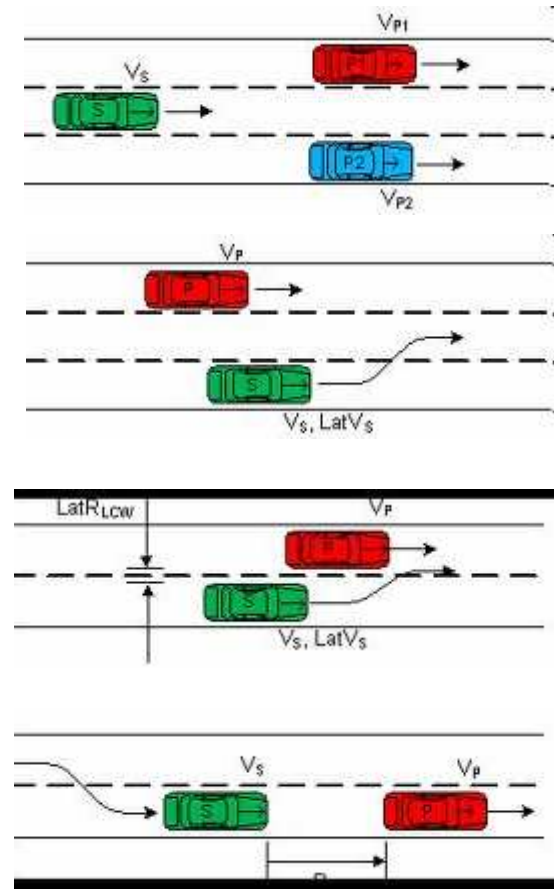
*Unintended Deployment quantitative - AirbagSystem1.4



FTA, FME(D)A und Diagnostic Coverage in medini™ analyze

Pilotierung vom „Lane Centering Assistance“ Feature

- Ziel der Pilotierung:
 - „Einsatz einer integrierten, modellbasierten Werkzeugkette zur Konsistenzprüfung aller während der Sicherheitsanalyse erstellten Artefakte“
- ➔ Abbildung der GM/Opel Dokumenten-Templates auf das Werkzeug
- ➔ Eingabe existierender Daten
- ➔ Durchführung der Konsistenzprüfungen
- ➔ Qualitative Auswertung im Hinblick auf werkzeugbedingte Verbesserung während der Sicherheitsanalyse



Pilot Projekt: Arbeitsprodukte

- Werkzeuganpassung erfolgte größtenteils durch Konfiguration des Werkzeugs (Profilmechanismus)
- Umfang der Arbeitspakete/Zeit des Pilotprojekt limitiert auf:
 - System Safety Program Plan (SSPP)
 - Preliminary Hazard and Risk Analysis (PHA)
 - Safety Goals und High level Safety Requirements
 - Architekturmodelle und Funktionales System Safety Concept
 - Single element fault analysis (SEFA) als spezifische FMEA
 - Qualitative FTA



Ergebnisse des Pilotprojekts – Traceability und Konsistenzhaltung

- Traceability zwischen *allen* sicherheitsbezogenen Artefakte sowie Systemmodellen
 - z.B. Hazards, Sicherheitsziele und -anforderungen, FTA, FMEA
 - Allokationen zu Systembeschreibungen (Anforderungen/ASIL)
- Prävention von Fehlern bei der Erstellung der Arbeitsprodukte durch:
 - spezifische Editoren zum strukturierten Vorgehen
 - standardisierte Auswahlmöglichkeiten
 - Gewährleistung der Konsistenz durch referenzielle Integrität
- Automatisierte Konsistenzprüfung zum Entdecken von Inkonsistenzen innerhalb der Dokumente, z.B.
 - falsche Zuordnungen bei der ASIL Bestimmung
 - fehlende Elemente in der SEFA (FMEA)
 - ➔ *In Excel nur mit unverhältnismäßig hohem Aufwand(!)*

Ergebnisse des Pilotprojekts – Konfigurierbarkeit und Flexibilität

- Werkzeug hilft bei der Erstellung der vom GM „System Safety Engineering“ Prozess geforderten Arbeitsprodukte
 - Anpassbarkeit ist gegeben
 - GM-spezifische Templates wurden entwickelt und eingesetzt
- Integration möglich in bestehende Werkzeugumgebungen
 - z.B. IBM Rational Tool-chain über Eclipse, DOORS über RIF, MS Office Produkte



Ergebnisse des Pilotprojekts – Performanz und Usability

- Hin- und herwechseln zwischen verschiedenen Werkzeugen wird vermieden
- Visualisierung der Abhängigkeiten zwischen Elementen steigert das Verständnis
- Zusammenhänge können graphisch oder tabellarisch dargestellt werden (→ *Trace Matrix*)
- Suche und Navigation über alle Arbeitsprodukte erleichtert das Vorgehen

- Erwartete Verbesserungen bei einer unternehmensweiten Einführung einer Werkzeugkette wie medini™ analyze
- Einhaltung von Unternehmensrichtlinien und “*Best Practices*”
- Unterstützung bei Arbeitsabläufen über verschiedene Phasen der Sicherheitsanalyse hinweg (“*workflow support*”)

Zusammenfassung, Ausblick

- Das Pilotprojekt hat bestätigt, dass ein Werkzeug wie medini™ analyze die Konsistenz und Qualität der System Safety Arbeitsprodukte wirkungsvoll unterstützt
- Eine Effizienzsteigerung ist nach der Lernphase zu erwarten durch die Werkzeugautomatisierung bzgl. Traceability, Validierung, Workflow support
 - abhängig von der Usability und der Integration des System Safety Werkzeugs in die bestehenden Werkzeugumgebungen
- medini™ analyze wird bei der Adam Opel AG in ausgewählten Projekten pilotweise eingesetzt und ist Kandidat bei der Auswahl eines globalen Werkzeugs zur Unterstützung des GM „System Safety Engineering“ Prozesses



Danke für Ihre Aufmerksamkeit!



Wir leben Autos.



ikv