



medini™ analyze functional safety analysis for ISO 26262

product version 1.6 – April 2012

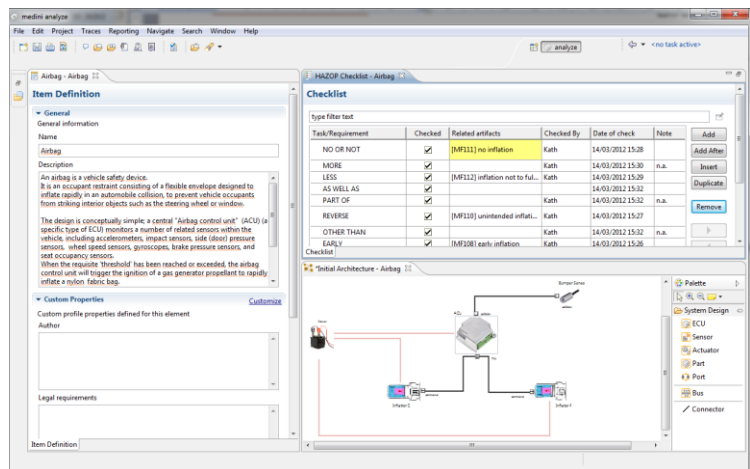


- safety analysis and design according to ISO 26262 for software controlled safety related functions
- integration of architectural/functional design with functional safety analysis methods
- support of driving situation analysis, hazard and risk analysis, Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), probabilistic analysis and hardware failure metrics
- traceability for all safety relevant information and decisions throughout the whole development process
- generation of ISO 26262 work products
- integration with DOORS, Rhapsody, EA, MATLAB/Simulink/Stateflow, MKS Integrity, MS Office, SVN, ClearCase, Rational Team Concert and more



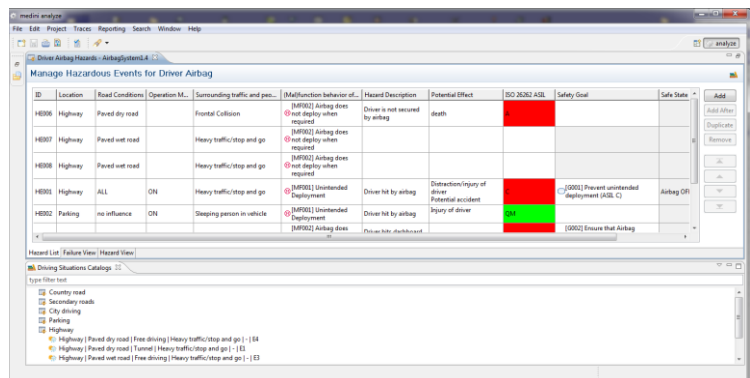
item definition

- dedicated form for the item description
- customizable with user attributes
- definition of functions and malfunctions of an item and their relations,
- HAZOP analysis with predefined checklists
- initial item architecture with SysML
- inclusion of external documents and linking to external resources via URI



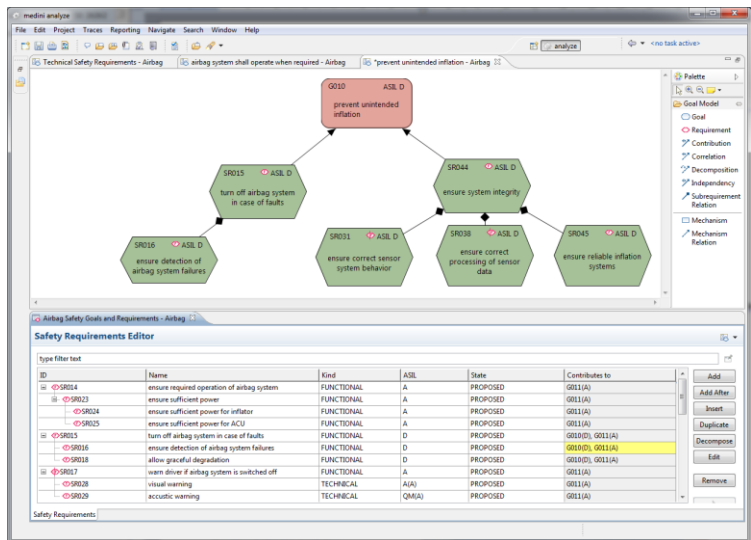
hazard analysis, risk assessment and ASIL determination

- table-based management of driving situations and hazardous events
- customizable with user attributes
- support for driving situation catalogues with drag & drop
- ISO 26262 compliant ASIL determination
- specification of driving situations and hazards based on predefined parameters
- comprehensive traceability to item definition and item functions as well as to safety goals and safety analysis artifacts
- derivation of safety goals



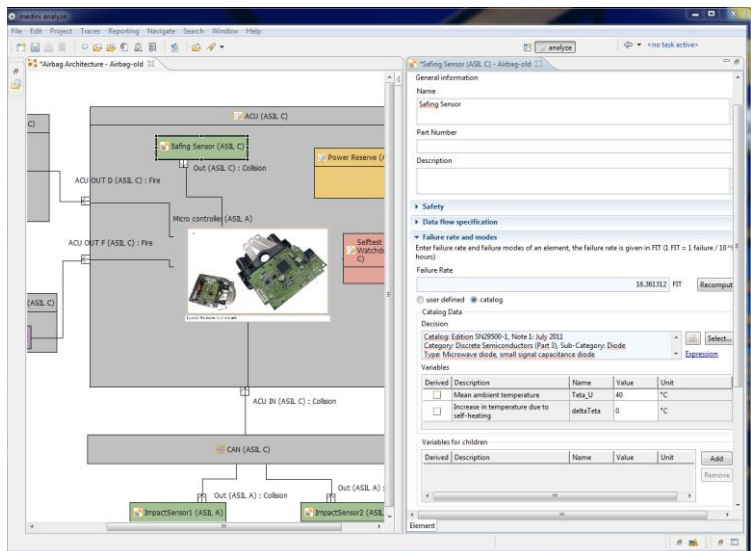
safety goal analysis and management

- graphical and table editors for safety goals and requirements
- customizable with user attributes
- capture and manage functional and technical (HW/SW) safety requirements
- support for structured requirements and for ASIL decomposition
- validation rules to check compliance with ISO 26262
- allocation of requirements to system architecture, HW and SW models and to function model
- import and export from/to requirements management systems (e.g. DOORS, MKS integrity)



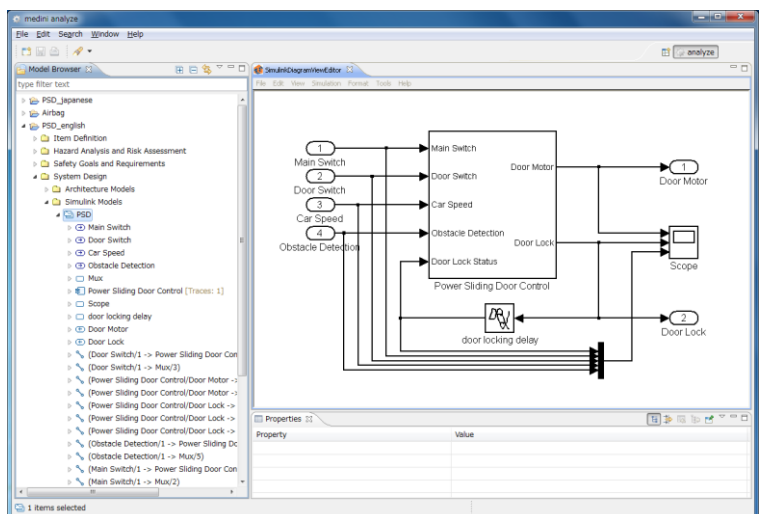
system architecture modeling (SysML)

- graphical SysML editor for architecture models
- import and round-trip of SysML models from IBM Rational Rhapsody and Enterprise Architect
- specification of failure modes and failure rates for elements of the system architecture
- failure rate determination using catalogs and handbook data (e.g. SN 29500)
- single source for safety analysis such as FTA, FME(D)A and Hardware Metrics
- computation and visualization of the resulting ASIL for components considering argumentation of independence



function behavior modeling

- import, round-trip and visualization of MATLAB Simulink and Stateflow models
- associate elements of MATLAB model to elements of system architecture model
- traceability to requirements and to safety analysis such as FTA and FMEA
- validation of the HW/SW mapping
- automatic creation of FTA models from MATLAB Simulink models using structural path analysis
- consistent update of MATLAB models in case of design change



Failure Mode and Effects Analysis (FMEA)

- standard templates for FMEA/FMEDA
- customizable with user attributes
- automatic population of the table with components and functions from the system models
- automatic inclusion of all failure modes/rate data of the system model
- automatic computation of Risk Priority Numbers (RPN) to prioritize which items require additional quality planning or action
- FMEDA with Safe Failure Fraction (SFF) computation
- Excel import for legacy integration

Component	Failure Rate (in FIT)	Potential Failure Modes	Failure Category	Failure rate distribution (in %)	Failure Rate Fraction (in FIT)	Potential Failure Effects	Safety	Risk Priority	Potential Failure Causes	Current Design Controls	
ACU	0.0										
Micro controller	100.0	AIR	Safe/Undetected	100.0	100.0						
Power Reserve	20.0	AIR	Dangerous/Undetected	100.0	20.0						
Safest Watchdog	10.0	AIR	NoEffect	100.0	10.0						
Safing Sensor	16.361312	stuck at value	Safe/Undetected	25.0	4.090328	delivers wrong data	4	4	N	sensor is dirty	2 shielding
		lower signal value	Dangerous/Undetected	25.0	4.090328						
		higher signal value	Dangerous/Undetected	25.0	4.090328						
		intermittent signal	Dangerous/Undetected	25.0	4.090328						
Out	0.0										
ACU OUT D	1.0										
ACU OUT F	1.0										
ACU IN	1.0										
Driver Airbag	0.0										
Initiator	9.0	short circuit	Dangerous/Undetected	100.0	9.0						
Front Passenger Airbag	0.0										

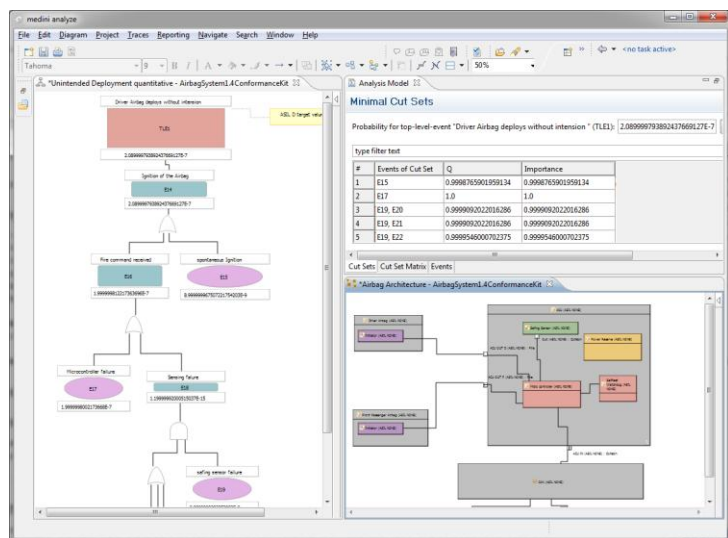
ISO 26262 Part 5 Hardware Metrics

- calculation of Single Point Fault Metric and Latent Fault Metric
- evaluation of HW metrics based on safety goal and ASIL
- automatic synchronization of failure mode and failure rate data from architecture model
- extensible catalog of safety mechanisms according to part 5 of ISO 26262
- specification of properties for applied safety mechanisms
- rich validation and consistency checks
- traceability of safety mechanisms to requirements and SW/HW implementation

Component Name	Failure Rates (in FIT)	Safety Related	Potential Failure Modes	Failure rate distrib.	Violates safety goal	SM prevents violation	SFF Coverage (in %)	SFF (in FIT)	Multiple failures violate safety goal	SM prevents FM from being	LF Coverage (in %)	LF (in FIT)
ACU	0.0											
Micro controller	100.0	AIR	100.0			Self-test by software (limited number of patterns (one channel)) Self-test supported by hardware (one channel)	99.0	1.0			0.0	-
Power Reserve	20.0	AIR	100.0			Voltage or current control (input) Voltage or current control (output)	99.0	-		Voltage or current control (input)	80.0	4.0
Safest Watchdog	10.0	AIR	100.0				0.0	-			0.0	10.0
Safing Sensor	16.361312		stuck at value	25.0			0.0	-			0.0	-
			lower signal value	25.0			Failure detection by on-line monitoring	0.0	-		0.0	-
			higher signal value	25.0				0.0	-		0.0	-
			intermittent signal	25.0				85.0	0.838656		0.0	3.272824
Out	0.0											
ACU OUT D	1.0											
ACU OUT F	1.0											
Driver Airbag	0.0											
Initiator	9.0											
Front Passenger Airbag	0.0											

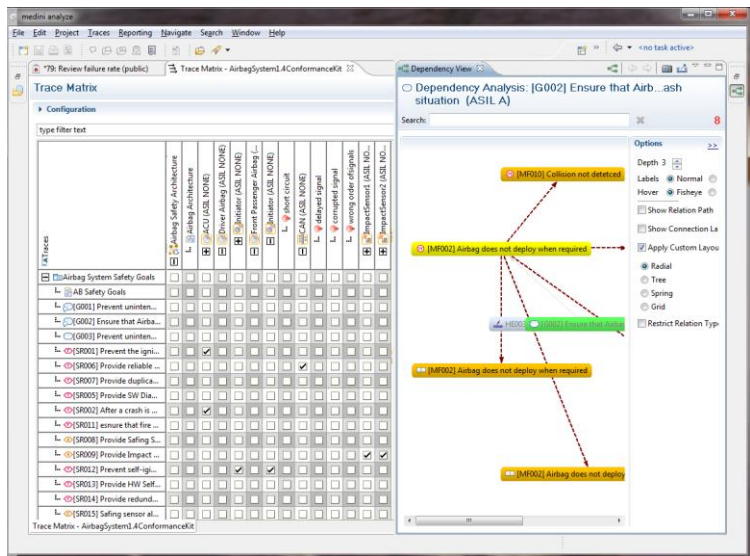
Fault Tree Analysis (FTA)

- graphical editor for quantitative and qualitative FTA
- automatic layout and support to handle large fault trees by multiple diagrams
- creation of events and subtrees by drag&drop of architecture elements or failure modes from architecture model
- determination and evaluation of minimal cut-sets to find out their probability
- importance measures such as Birnbaum, Fussell-Vesely, Criticality
- seamless navigation from cut-sets to elements of the system design
- automatic re-calculation of probabilities after design changes



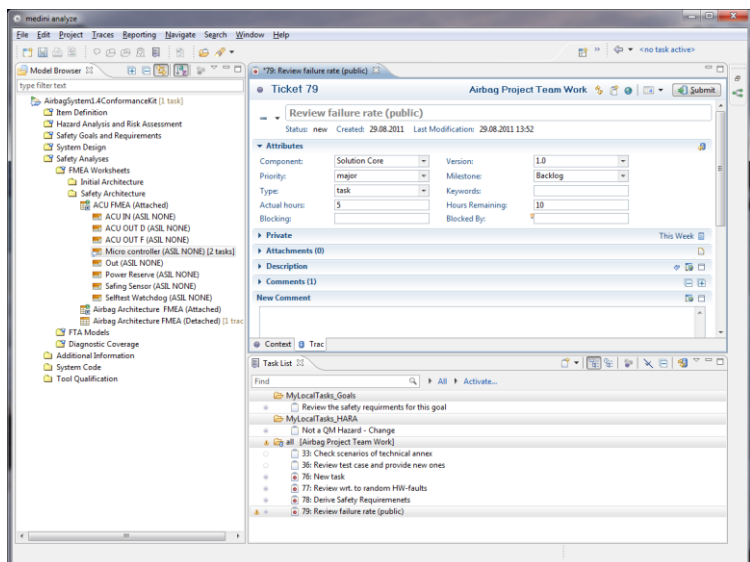
sophisticated traceability

- definition of typed and untyped traces between information elements of any type within medini analyze
- definition of traces using trace-matrix or by quick-trace functionality
- follow-trace to navigate quickly to related elements in other models
- filters and hierarchies to support the usage even of large trace matrices
- customizable graphical visualization of traces to identify element relationships and for impact analysis



team work and integrated task management

- integration with configuration management systems (SVN, Clearcase, MKS Integrity etc.)
- management of model versions, support of team synchronization
- comprehensive consistency checks
- integration with issue tracking systems (Bugzilla, Trac, RTC, Outlook etc.)
- creation of tasks/comments for arbitrary model elements
- navigation from tasks to elements and vice versa
- context visualization for active tasks
- documentation of all decisions at the tasks
- scheduling, user assignment, e-mail notification and much more



licensing

- attractive product tailoring due to individually licensable components
- single user, dongle and network floating licenses available

system requirements

- supported platforms: Microsoft® Windows 2000/XP/Vista®/Windows 7
- required disc space: 250 MB
- recommended memory size: 2 GB

*do you need more information?
do you have questions?
do you want a trial?*

contact us at
www.ikv.de

+49(30)3480 770
information@ikv.de