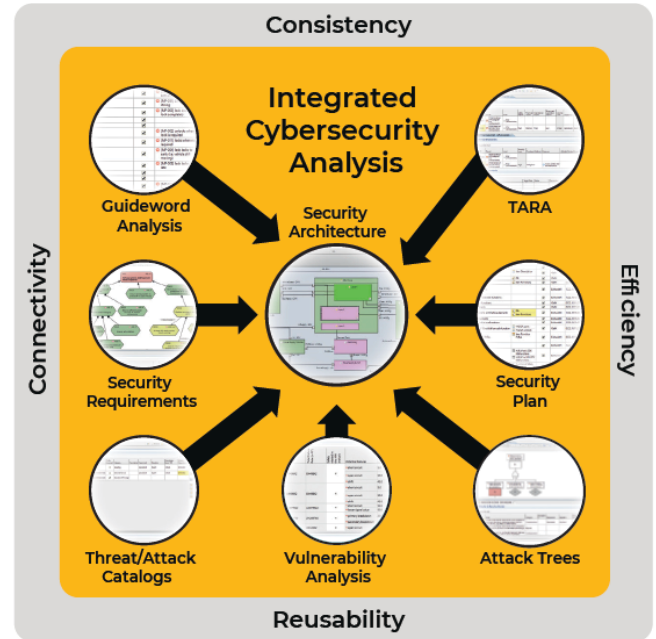


Ansys medini analyze for Cybersecurity

Cybersecurity Threat Analysis and Risk Assessment

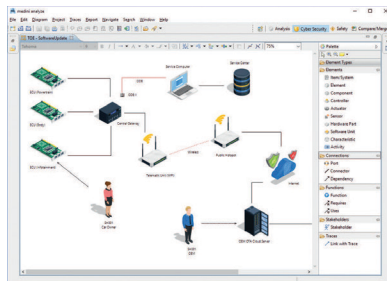
Main Features

- ✓ Model-based and integrated tool supporting analysis context establishment, asset identification, threat identification, attack trees and threat assessment and treatment
- ✓ Cybersecurity analysis and design of cybersecurity related functions and systems according to e.g. ISO 21434, UN-ECE R.155 (WP.29), DO-356a, ISO 27005
- ✓ Integration of architectural/functional design models with cybersecurity analysis methods
- ✓ Capture and management of cybersecurity requirements
- ✓ Support of complete end-to-end traceability
 - Customizable work product/document generation
 - Teamwork with detailed compare and merge
 - Integration with IBM Rational DOORS, PTC Integrity, Jama, MS Office, SVN and others



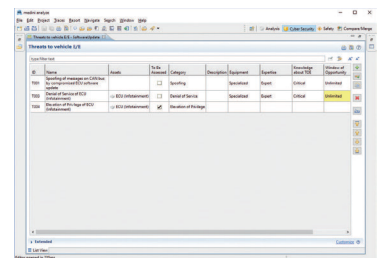
Analysis Context Establishment and Asset Identification

- ✓ Graphical editor for system models based on SysML to model the Item Definition or the Target of Evaluation (TOE)
- ✓ Structural modelling of system architecture and design using blocks, parts, ports, and connections
- ✓ Function and process modelling using activities, actions and dataflows, allocations to design
- ✓ Dependency Editor allowing to visualize and edit function nets, allocations, and other relations
- ✓ Marking of SysML elements as assets
- ✓ Assigning of security attributes (confidentiality, integrity, availability, etc.) to assets
- ✓ Import and round-trip of system design models from Ansys SCADE Architect, IBM® Rational® Rhapsody, Sparx Systems Enterprise Architect, MagicDraw
- ✓ Traceability of SysML models to requirements and security analysis such as Threat Analysis and Risk Assessment (TARA) or Attack Trees



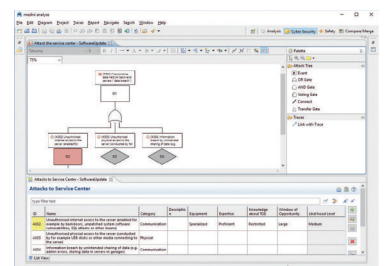
Threat Identification

- ✓ Threat collections filled automatically with potential threats or threat scenarios that are derived from the assets and their security attributes by applying a mapping to the STRIDE categories
- ✓ Selection of threats or threat scenarios for later assessment
- ✓ Pre-estimation for the feasibility of potential threats or threat scenarios according to the definitions of the HEAVENS project or of the ISO 21434 (user-defined approaches for feasibility estimation is possible too)



Attack Trees and Attack Collections

- ✓ Graphical editor to describe attack scenarios that lead to potential threats or threat scenarios
- ✓ Automatic layout and support to handle large attack trees by multiple diagrams
- ✓ Creation of events and subtrees by drag & drop of attacks, threats, vulnerabilities and other system model elements
- ✓ Attack collections to gather the attacks forming the attack scenarios
- ✓ Pre-estimation of the feasibility of every single attack in the collection

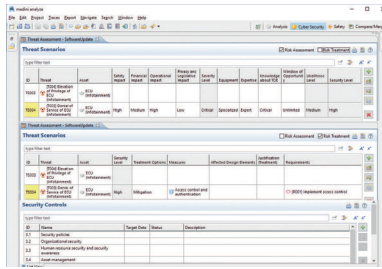


Ansys medini analyze for Cybersecurity



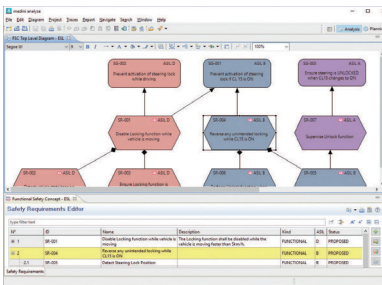
Threat Assessment and Treatment

- ✓ Customizable table for threat assessment and treatment filled by Drag&Drop from any threat collection
- ✓ Estimation of the impact and feasibility levels (user-defined approaches for impact and feasibility estimation is possible too)
- ✓ Calculation of an overall security level (risk level)
- ✓ Definition of treatment strategies to handle the risk (mitigation, avoidance, acceptance, transfer)
- ✓ Description and assignment of security measures and security goals to further detailize the treatment strategies



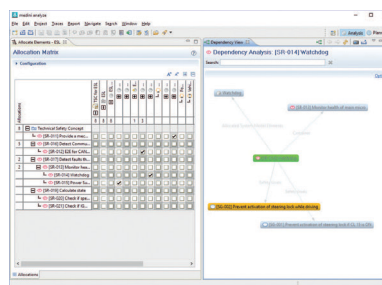
Requirement Analysis and Management

- ✓ Graphical and table editors for security requirements
- ✓ Visualization of requirement hierarchies and traceability using diagrams
- ✓ Allocation of requirements to system architecture, HW and SW models and to function models
- ✓ Import, export, and round-trip from/to requirements management systems (e.g. IBM® Rational® DOORS®, IBM® Rational® DOORS® Next Generation, PTC Integrity, Jama) including custom attribute mapping
- ✓ Support for general requirements exchange via ReqIF/RIIF



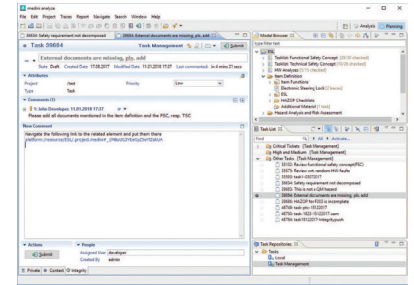
Rich Traceability

- ✓ Definition of traces between information elements of any type within Ansys medini analyze
- ✓ Definition of traces using trace-matrix or by quick-trace functionality
- ✓ Navigation via traces to related elements in other models
- ✓ Visualization of traced elements at any diagram
- ✓ Filters and hierarchies to support the usage even of large trace matrices
- ✓ Impact analysis by graphical visualization of traces (customizable dependency viewer)



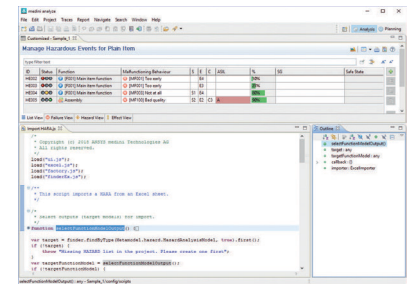
Teamwork and Integrated Task Management

- ✓ Project compare with 2-way and 3-way difference analysis
- ✓ Project merge functionality for team collaboration
- ✓ Integration with configuration management systems (TortoiseSVN, IBM® Rational® ClearCase, PTC Integrity etc.)
- ✓ Management of model versions, support of team synchronization
- ✓ Integration with issue tracking systems (e.g. Bugzilla, Trac, RTC, Redmine, Jira, Mantis, PTC Integrity, Microsoft® Outlook)
- ✓ 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, email notification



Reporting and Customization

- ✓ Reporting functionality to generate PDF, Word, Excel, or HTML documents for all project content
- ✓ Default report for the security concept including, TOE, TARA, Attack Trees and security requirements
- ✓ Customizable reporting framework to build corporate reports for security related work products
- ✓ Profiling mechanism to add custom fields, references, and queries to all models and analyses
- ✓ Extensible model validation rules to check consistency across all project data
- ✓ Scripting API with integrated JavaScript engine for adding automation features and building tool extensions



Ansys medini analyze is a product of Ansys

FOR INFORMATION:

EnginSoft | Alessandro Mellone
a.mellone@enginsoft.com
Tel. 0461 979 340
www.enginsoft.com

Licensing

- ✓ Attractive product tailoring
- ✓ Network floating licenses
- ✓ Trial licenses on request

System Requirements

- ✓ Supported platforms: Microsoft® Windows 8/10 (64-bit version)
- ✓ Required disc space: 500 MB
- ✓ Recommended memory size: 4GB