

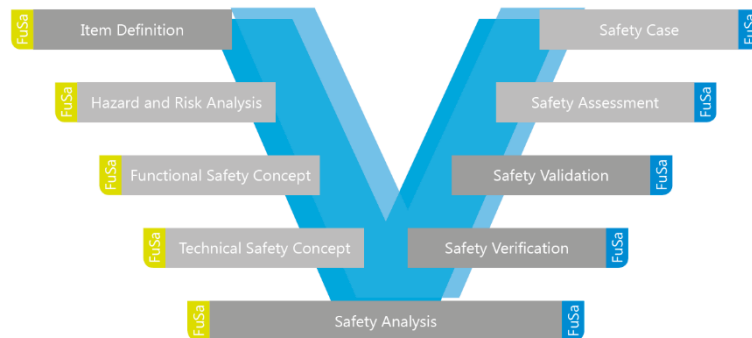
medini® analyze 模块介绍

medini® analyze 是专业的安全分析软件,可支持基于电子和软件的系统功能安全性分析工作,该产品最初用于支持 ISO 26262 汽车领域的安全分析,现在同样也支持其他领域的安全分析,如支持 SOTIF 预期功能安全分析、信息安全分析、半导体领域的安全分析,同时也支持 IEC61508 工业领域、ARP 4761 航空领域以及轨道领域的安全分析等。

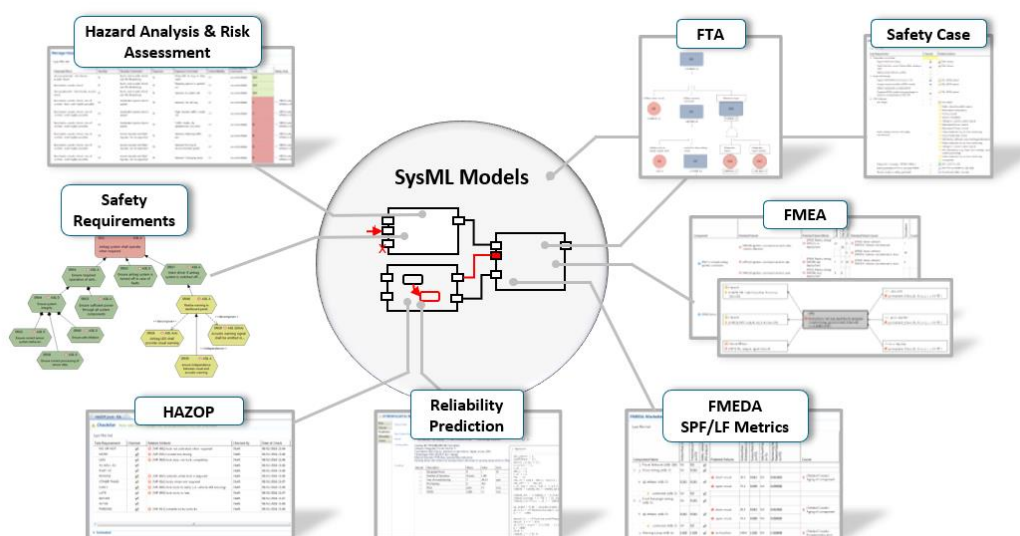
medini® analyze 在同一个工具环境中结合了常用的系统安全分析技术:

- 危害/威胁分析和风险评估 (FHA/PHA/HARA/TARA)
- 故障模式和影响分析 (FMEA)
- 故障树/攻击树分析 (FTA/ATA)
- 危害和可操作性分析 (HAZOP)
- 限制和弱点分析 (LWA)
- 触发条件分析 (TCA)
- 故障模式,影响和诊断分析 (FMEDA/FMECA)
- 硬件安全性分析的诊断覆盖度指标 (DC)
- 半导体的安全性定性和定量分析,以及相关安全产品的导出和集成

通过以上技术, medini® analyze 可以在完整开发生命周期中支持系统安全的相关活动。



medini® analyze 是一款基于模型的安全分析工具,其安全分析技术主要是基于 SysML 模型进行,基于模型的方法确保了分析的一致性、可跟踪性以及高效性。



medini® analyze 包含 5 个不同功能组合的套件。此外，还有一个连接包提供与工程过程中其他工具的集成。

Modules	Safety PRO	Safety PREMIUM	CyberSecurity Pro	Connectivity Package	ENTERPRISE	Semiconductor ENTERPRISE
System Design (SysML)	✓	✓	✓		✓	✓
Requirements Modeling	✓	✓	✓		✓	✓
HARA/FHA/PHA	✓	✓			✓	✓
FMEA	✓	✓			✓	✓
Qualitative FTA	✓	✓			✓	✓
Limitation and Weakness Analysis	✓	✓			✓	✓
Triggering Condition Analysis	✓	✓			✓	✓
Guideword Analysis			✓		✓	✓
Threat Identification			✓		✓	✓
TARA			✓		✓	✓
Attack Tress			✓		✓	✓
DC Configurator – FMEDA Import		✓			✓	✓
Quantitative FTA		✓			✓	✓
FMEDA/ HW-Metrics		✓			✓	✓
Failure Rate Prediction with SN29500, IEC 62380, MIL 217F/RIAC 217Plus, FIDES, GJB299C		✓			✓	✓
MATLAB/ Simulink Integration				✓	✓	✓
Task Management Integration				✓	✓	✓
Requirements Management Integration (DOORS/DNG, PTC, Jama)				✓	✓	✓
Qualification Automation					✓	✓
View only mode	✓	✓	✓		✓	✓
SCADE Architect tool					✓	✓
Semiconductor Design Import						✓
DC Configurator – FMEDA Export						✓

medini® analyze safety pro高级套件

medini® analyze 高级套件提供用于安全分析的 SysML 架构模型的所有基本建模功能。此外，还可以创建和维护安全目标及需求模型。对于安全分析，该套件包含危险和可操作性分析（HAZOP）、危害分析与风险评估表（HARA）、定性故障树分析（FTA）和定性故障模式和影响分析（FMEA）、相关失效分析（DFA）、**限制和弱点分析（LWA）**、**触发条件分析（TCA）**以及其他一般功能，如任务管理、追溯性管理、变更管理和审查评估以及报告生成、比较与合并功能，同时该套件还支持模板的定制以及团队合作。

SysML Modeling 系统建模

medini® analyze 中使用 SysML 语言对执行安全分析的系统功能和架构进行建模。为了便于应用，这里对 SysML 语言进行了简化和裁剪。

medini® analyze 提供以下建模能力：

- 通过图形和表格编辑器进行 SysML 建模
- 在定制版本中使用块定义图和内部框图对功能依赖性和故障的功能架构进行图形化建模
- 易于使用的实例/类型概念，没有继承或聚合
- 使用活动图对功能和过程的行为建模
- 支持建立部件库，允许从库模型导入元素到实际模型，以便重复使用
- 在库更改时自动更新，例如如果库包含类型定义，并且这些类型的实例在导入模型中使用
- 可以根据各行业中定义的规则，基于需求分配的安全等级的计算和可视化，即考虑元素的潜在独立性或非独立性。
- 可以定义 SysML 模型元素的故障模式和故障率

Requirements and Goal Modelling 需求与目标建模

medini® analyze 可用于推导和管理安全需求。为此，该工具有其特有的用于需求定义的模块。

- 图形和表格编辑器，来编辑安全目标 and 需求，用于获取和管理功能和技术安全需求

- 将需求分配给系统架构、硬件、软件模型以及功能模型，保证安全需求、系统设计与安全分析的交互迭代
- 对工具中其他图表上的需求进行追溯管理并进行可视化的显示

Hazard Analysis and Risk Assessment (HARA/FHA)危害分析与风险评估

危害分析与风险评估由日志表支持。在表中分析功能使用情景下的故障行为、危害及其后果。工具支持场景库的创建以及安全等级的计算，并可以创建或链接安全目标。这包括：

- 通过表格对操作场景、故障和危害事件的管理
- 通过拖放和链接进行表格的创建
- 矩阵形式管理，易于组合故障和操作场景
- 符合行业安全标准的安全等级确定
- 安全目标的推导和链接
- 支持建立危害集合及场景库，便于重用

Checklists and HAZOP 检查单和危险和可操作性分析

检查单在工具中用于多种开发活动，例如用于验证和确认活动、安全计划、进度跟踪以及相关失效分析（DFA）等，危险和可操作性分析（HAZOP）可基于引导词系统性的对故障进行分析这包括：

- 具有分层结构的检查项和可自定义属性的检查单定义
- 直接链接到建模元素（例如用于将证据链接到检查项目）
- 检查单模板，用于轻松实例化实际的检查单（例如，在项目中多次应用相同的检查单）
- 相关失效分析模板，根据标准提供相关失效分析内容
- HAZOP 的预定义模板，根据标准提供相应引导词

Failure Mode and Effect Analysis (FMEA)故障模式和影响分析

FMEA 是一种归纳式安全分析技术，对于元件的给定故障模式来分析其潜在原因和影响，从而可以定义原因效应链（故障网）。FMEA 方法可以评估与故障模式相关的风险并且定义用于防止和检测这些故障模式的措施。这包括：

- 设计和处理 FMEA 的标准模板
- 可定制的 FMEA 表布局
- 跨抽象层的端到端因果/效应链
- 自动计算风险优先级编号（RPN）
- 支持从系统架构模型自动生成 FMEA 表，并自动填充表，保持与来自 SysML 模型元素和功能元素的一致性
- 自动包含结构和功能元素的所有故障模式
- 支持 Excel 和 MSR-FMEA 导入（例如 APIS IQ-FMEA，PLATO SCIO）已有 FMEA 表格
- 连接到需求管理和任务管理（需要连接包）
- 根据 VDA 质量手册的网格图形化失效
- 可以建立安全措施集
- 使用风险矩阵进行评估和优化

Qualitative Fault Tree Modeling and Analysis (FTA) 定性的故障树建模与分析

故障树分析是一种演绎式安全分析方法，从非预期事件（顶级事件，TLE）开始，调查使得非预期事件发生必须保持的条件，并定性评估故障树，以发现引起 TLE 所必须发生的基本事件（条件）的最小集合，包括：

- 定性故障树的图形编辑器，支持通过逻辑门级连接的顶级事件、中间事件、基本事件、房屋事件、未开发事件和条件事件 - AND 门，OR 门，XOR 门，投票门。为了使图的可见性更好，还支持传输门。
- 自动图布局，支持通过多个图处理大型故障树
- 通过从架构模型中拖放架构元素或故障模式创建事件和子树
- 自动评估最小割集
- 从子集到系统设计元素的无缝导航
- 子树的折叠和展开以提高可见性
- 大纲视图，以方便的方式涵盖所有事件和多个发生的事件
- 从属故障和常见原因分析

Limitation and Weakness Analysis (LWA) 限制和弱点分析

限制和弱点分析是预期功能安全分析中的一种安全分析方法，通过对传感器或算法的标称特性进行分析，从而系统性地分析该特性可能存在的限制或弱点，并对存在的限制和弱点进行收集。这包括：

- 对传感器或算法进行标称特性的建模
- 标称特性与运行场景特性结合，系统性的分析限制和弱点
- 通过收集表对限制和弱点进行收集，用于复用及数据库的建立
- 支持与故障树结合，分析导致故障的弱点和限制
- 支持对限制和弱点衍生相关的预期功能安全需求

Triggering Condition Analysis (TCA) 触发条件分析

触发条件分析是预期功能安全分析中的一种安全分析方法，通过对传感器或算法的限制和弱点以及传感器的仿真测试数据进行分析，找到限制或弱点可能产生的触发条件。这包括：

- 通过因果分析的方式，确定限制和弱点的触发条件
- 通过仿真模拟测试数据对触发条件进行分析
- 通过收集表对触发条件进行收集，用于复用及数据库的建立
- 支持与故障树结果，分析导致故障的触发条件
- 支持对触发条件衍生相关的预期功能安全需求
- 支持对触发条件进行详细的建模，作为后续测试验证的输入

Team Work Capabilities - Project Compare and Merge 团队工作能力-项目比较与合并

medini® analyze 支持同一项目上的团队同步工作。为此，它在 medini® analyze 项目级别提供比较和合并功能，包括：

- 项目比较，支持 2 路和 3 路差分分析
- 团队协作的项目合并功能
- 与配置管理系统集成（SVN，PTC Integrity 等）
- 管理模型版本，支持团队同步

Common Features 通用功能

- 包含外部文档并通过 URI 链接到外部资源
- 完整的端到端可追溯性、基于跟踪的导航、跟踪矩阵和快速跟踪来链接任何建模元素
- 定义 medini 分析中任何类型的信息元素之间的类型化和非类型化跟踪
- 通过轨迹导航到项目的其他模型中的相关元素
- 在任何图表中可视化跟踪元素
- 过滤器和层次结构，以支持大型跟踪矩阵的使用
- 通过图形可视化跟踪（可定制的依赖关系查看器）

- 可定制的工作产品/文档生成
- 定制具有用户定义属性的任何模型元素 - 简单类型化属性，引用其他模型元素的属性和派生属性与规则以导出其值
- 基于 OCL 的验证引擎验证规则，用于检查是否符合安全标准
- Java 脚本 API
- 可自定义的自动编号功能，以确保一致的编号，例如，安全要求
- 项目模板，可能包含特定的模型结构、预定义的建模元素、通过其他属性定制的模型元素类型、模型验证的特定约束

medini® analyze safety premium 超级套件

medini® analyze premium 超级套件包含 safety pro 高级套件的所有功能。此外，它包含对可靠性预测的支持，意味着元素故障率可以基于手册、任务剖面 and 应力参数来确定。FTA 评估和 FMEA 也可用于定量分析，如硬件故障度量或随机硬件失效率（PMHF）的确定。

可靠性预测

对于硬件级的安全分析，重要的是处理随机硬件故障。medini® analyze 可用于基于其特性导出硬件元件的基本故障率。它包含进一步的机制来将这种故障率分布在故障模式或复杂硬件元素的部分上。这种故障率和故障率分布的确定是执行更详细的安全分析的前提条件，例如根据安全标准所要求的硬件故障度量和随机硬件失效率（PMHF）的计算。

- 使用手册（SN 29500、MIL-HDBK-217F/RIAC-217Plus、IEC 62380、FIDES、IEC61709、GJB/Z 299C 等）来确定基本故障率，
- 自定义缩放功能
- 支持项目级/元件级设置 mission profile
- 支持在类型和/或实例级别定义的应力参数（温度，电压等）
- 支持从 Excel 导入 BOM，通过拖放轻松重构、自动绑定到库中定义的元素类型

FMEDA 和硬件指标

FMEDA 是一种用于分析安全机制的诊断覆盖率和其余未被安全机制覆盖的安全相关部分的故障率的安全分析方法。基于这些计算，medini® analyze 可以计算完整的基于 SysML 的架构模型的指标。包括：

- FMEDA 安全故障比例（SFF）计算
- 计算单点故障度量（SPFM）和潜在故障度量（LFM）
- 从 SysML 架构模型自动同步故障模式和故障率数据
- 子模块失效率分布
- 原因/效应链的定义和故障率的自动计算
- 支持从 ISO26262 选取推荐的安全机制，并自动填充诊断覆盖率
- 安全机制对安全需求和软硬件设计的可追溯性
- DC Configurator 导入功能：可以导入供应商导出的 medini 工程，从而读取、重用供应商的 FMEDA 结果数据以及其他导出的工程数据。

定量 FTA 分析

除了故障树的定性分析外，medini 也支持故障树的定量分析。包括：

- 基本事件的概率模型：固定概率、是否修复的失败率的指数分布、具有测试/监测间隔的指数分布、Weibull 分布
- FTA 事件与 SysML 模型元素的绑定和同步（例如故障模式）
- 安全机制的失效概率（1-（诊断率））

- 每个事件的概率图表
- 使用概率计算最小子集分析：不可用性，不可靠性，不可用性和每小时不可靠性的平均值，子集的概率
- 子事件的重要性，如 Birnbaum, Fussell-Vesely, Criticality
- 支持指定任务时间
- 设计更改后自动重新计算概率

medini® analyze cybersecurity pro 高级套件

medini® analyze 信息安全高级套件提供用于信息安全分析的 SysML 架构模型的所有基本建模功能。此外，还可以创建和维护信息安全目标及需求模型。对于信息安全分析，该套件包含危险和基于引导词的分析（Guideword Analysis）、威胁识别、威胁分析与风险评估表（TARA）、攻击树分析（ATA）以及其他一般功能，如任务管理、追溯性管理、变更管理和审查评估以及报告生成、比较与合并功能，同时该套件还支持模板的定制以及团队合作。

SysML Modeling 系统建模

medini® analyze 中使用 SysML 语言对执行信息安全分析的系统功能和架构进行建模。为了便于应用，这里对 SysML 语言进行了简化和裁剪。

medini® analyze 提供以下建模能力：

- 表示评估对象（TOE）的 SysML 系统模型的图形编辑
- 使用块、部件、端口和连接对系统架构和设计进行结构化建模
- 使用活动、操作以及设计配置进行功能和流程建模
- 使用依赖项编辑器实现功能网、配置和其他关系的可视化和编辑
- 将 SysML 元素标记为资产
- 为资产分配安全属性（保密性、完整性、可用性等）
- 通过 ANSYS SCADE Architect、IBM® Rational® Rhapsody 和 Sparx Systems Enterprise Architect 实现系统设计模型的导入和往返操作
- 确保 SysML 需求模型和安全分析工具（如 TARA 或攻击树）的可追溯性

Requirements and Goal Modelling 需求与目标建模

medini® analyze 可用于推导和管理信息安全需求。为此，该工具有其特有的用于需求定义的模块。

- 针对安全需求应用图形和表格编辑器
- 使用图表实现需求层次结构和可追溯性的可视化
- 将需求分配至系统架构、硬件与软件模型以及功能模型
- 与导入、导出和往返需求管理系统（如 IBM Rational Doors、IBM Rational Doors Next Generation、PTC Integrity 和 Jama）的操作兼容，包括自定义属性映射

Threat Identification 威胁识别

威胁识别是信息安全分析中重要的一环，工具可系统性的找出与资产相关的信息安全威胁这包括：

- 通过向 STRIDE 类别应用映射，借助从资产及其安全属性获得的潜在威胁自动创建威胁集合
- 选择威胁以进行后续评估
- 根据 HEAVENS 项目中的定义预估潜在威胁的可能性

Threat Analysis and Risk Assessment(TARA)威胁分析和风险评估

威胁分析和风险评估表格通过分析威胁，识别资产面临的相关威胁、并据此建模，而风险评估可以对每一个威胁的影响力和可能性评级，如此便能优化后续开发阶段的风险和威胁管理措施，这包括：

- 创建威胁分析和风险评估的定制化表格，并拖放威胁集合中的数据以填充表格
- 估算威胁影响以及其可能性级别
- 计算总体信息安全级别
- 定义风险处理策略（缓解、避免、接受、转移）
- 描述和分配信息安全措施和信息安全需求，以便进一步细化处理策略

Attack Tree Analysis (ATA)攻击树分析

攻击树分析是一种演绎式信息安全分析方法，从威胁开始，分析威胁发生必须的条件，并定性评估攻击树，以发现引起威胁所必须发生的基本事件（条件）的最小集合，包括：这包括：

- 进行图形编辑，以便描绘导致潜在威胁的情况
- 提供自动布局和支持，以通过多个图表处理大型攻击树
- 通过拖放攻击、威胁、漏洞和其他系统模型元素创建活动和子树
- 将构成攻击场景的攻击编译为攻击集合
- 预估每次攻击的可能性

Team Work Capabilities - Project Compare and Merge 团队工作能力-项目比较与合并

medini® analyze 支持同一项目上的团队同步工作。为此，它在 medini® analyze 项目级别提供比较和合并功能，包括：

- 项目比较，支持 2 路和 3 路差分分析
- 团队协作的项目合并功能
- 与配置管理系统集成（SVN，PTC Integrity 等）
- 管理模型版本，支持团队同步

Common Features 通用功能

- 包含外部文档并通过 URI 链接到外部资源
- 完整的端到端可追溯性、基于跟踪的导航、跟踪矩阵和快速跟踪来链接任何建模元素
- 定义 medini 分析中任何类型的信息元素之间的类型化和非类型化跟踪
- 通过轨迹导航到项目的其他模型中的相关元素
- 在任何图表中可视化跟踪元素
- 过滤器和层次结构，以支持大型跟踪矩阵的使用
- 通过图形可视化跟踪（可定制的依赖关系查看器）
- 可定制的工作产品/文档生成
- 定制具有用户定义属性的任何模型元素 - 简单类型化属性，引用其他模型元素的属性和派生属性与规则以导出其值
- 基于 OCL 的验证引擎验证规则，用于检查是否符合安全标准
- Java 脚本 API
- 可自定义的自动编号功能，以确保一致的编号，例如，安全要求
- 项目模板，可能包含特定的模型结构、预定义的建模元素、通过其他属性定制的模型元素类型、模型验证的特定约束

medini® analyze connectivity package 连接包

medini® analyze 连接包包含与开发过程中常用的其他工具的桥接和集成--- 包括建模工具（Sparx Systems Enterprise Architect, MathWorks Simulink, IBM Rational Rhapsody）、需求管理工具（IBM Rational DOORS, PTC Integrity）以及用于变更管理和问题跟踪的工具（例如 Redmine）。

连接功能包括：

- 包括自定义属性映射的需求管理系统（例如 IBM DOORS、DOORS NG、PTC Integrity）的导入，导出和往返
- 从 IBM Rhapsody 和 Enterprise Architect 导入和导出模型
- 与问题跟踪系统集成（例如 Bugzilla, Trac, RTC, Redmine, Jira, Outlook）
- 为任意模型元素创建任务/注释
- 从任务到元素的双向导航
- 活动任务的上下文可视化
- 记录任务中的所有决策
- 计划、用户分配、电子邮件通知

medini® analyze enterprise 企业套件

medini® analyze 企业套件包含了 safety 和 cybersecurity 超级套件和连接包的所有功能。此外，它捆绑了一个 SCADE Architect 高级建模器以及工具鉴定服务。

medini® analyze enterprise for semiconductors 半导体企业套件

medini® analyze 半导体企业套件组合了企业套件和以下所有功能：

- 芯片设计人员和安全分析人员之间无缝交换 IP 设计数据。
- 芯片的基本故障率的推导（基于 IEC 62380、SN29500、IEC61709 等）。
- 基于设计数据（例如，Die 面积，gate 计数）自动确定永久故障和瞬态故障分布。
- 基于硬件设计的 FMEA, FMEDA 和 FTA 分析，包括自动计算 SPF / LF 指标，安全故障分数。
- 设计更改时，分析数据的“闭环”更新。
- 重复使用和改编以前设计的 FMEDA 数据。
- 将故障列表以 XML 格式导入相关 EDA 工具，在 EDA 工具中执行完故障注入测试与仿真后，将仿真后的数据导入 medini，可自动更新 FMEDA 中诊断覆盖率数据。
- DC configurator 导出功能：导出可配置的 FMEDA 结果数据，并将安全数据以 medini 工程的形式移交给集成商。