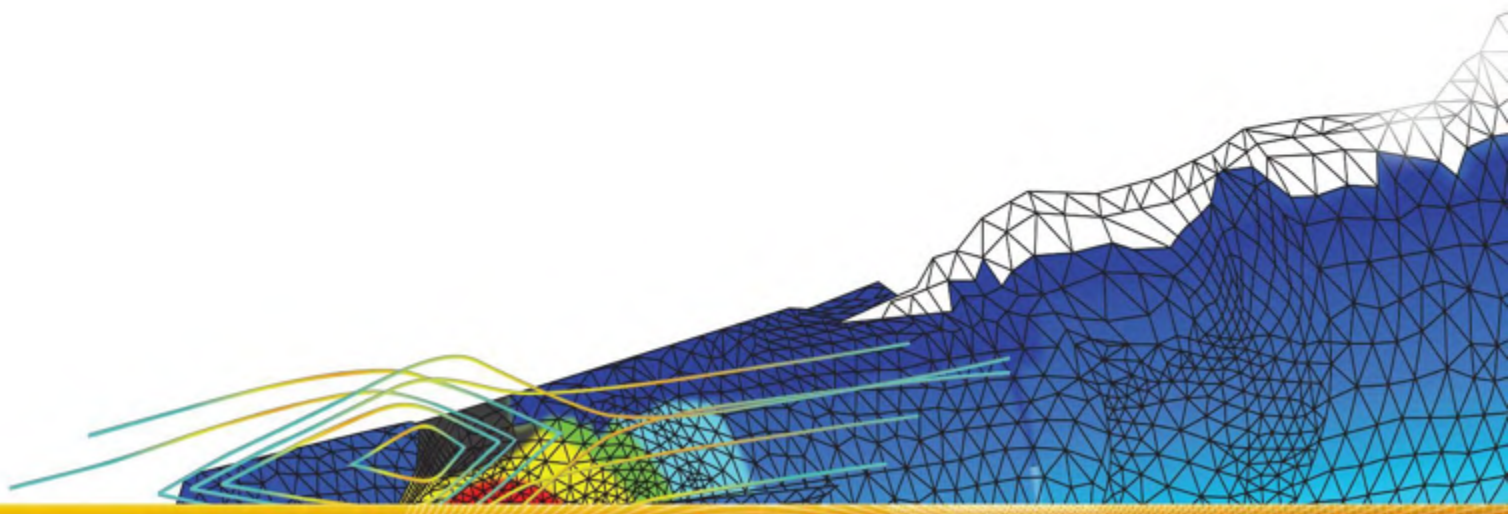
基于模型的车载嵌入式系统设计与高安全性代码生成

应中伟

ANSYS SBU

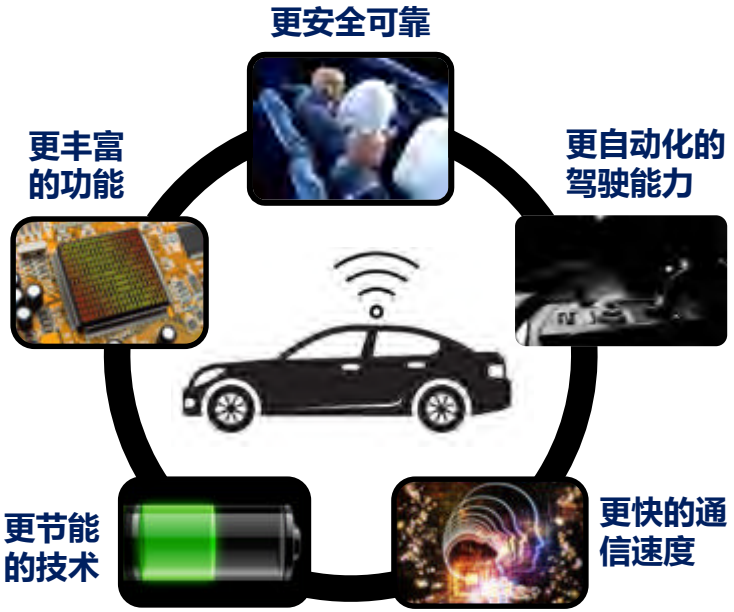
ANSYS

挑战和机遇



汽车行业的发展与趋势（1/3）

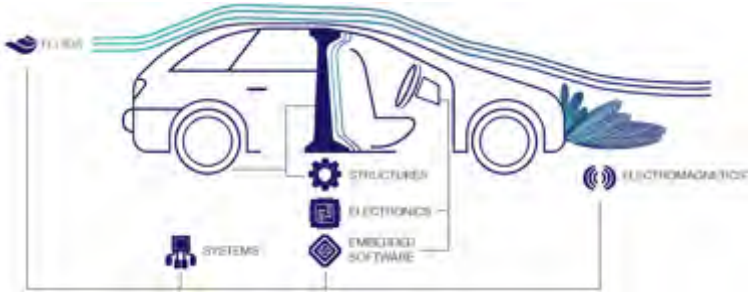
- 当前汽车行业的迅猛发展，得益于国家和用户对于以下三类汽车的迫切需求：
  - ❖ **新能源汽车**
  - ❖ **互联网汽车**
  - ❖ **自动驾驶汽车**



汽车行业的发展与趋势（2/3）

- 越来越多的电子电器系统将成为强安全相关的系统

❖ESP/ESC（车身稳定控制系统）
❖LDWS（车道偏离预警系统）
❖APA （主动停车辅助系统）
❖CCAS（汽车防撞雷达系统）
❖PAS（停车辅助系统）
❖SRS（安全气囊）
❖安全带预紧
❖EMS/CATS（自适应悬架控制）
❖MCU（微控制单元）
❖DDS（司机瞌睡警示系统）
❖整车控制器（新能源）
❖电池管理系统（新能源）
❖电机控制器（新能源）
❖EBS （电子制动系统）
❖ASR（牵引力控制系统）
❖BAS（制动辅助系统）
❖EBD（电子制动力分配系统）
❖EBA（紧急制动辅助系统）
❖TPMS （胎压实时监控系统）
❖ACC（自动巡航系统）
❖PEPS（无钥匙进入系统）
❖EPS（电子助力转向系统）
❖AFS（自适应前照明系统）
❖司机监控系统
❖BCM（车身控制系统）
❖**More and more……**



汽车行业的发展与趋势（3/3）

- **法律的要求**

法律将是自动驾驶发展"绊脚石"？

- Good News：
  - ✓ 《国际道路交通公约（维也纳）》中对于自动驾驶汽车的修正案正式生效。新的修正案规定，在全面符合联合国车辆管理条例或者驾驶员可以人工选择关闭该功能的情况下，将驾驶的职责交给车辆的自动驾驶技术可以明确地被应用到交通运输当中。
  - ✓ 美国国家公路运输安全管理局（NHTSA）正式发布了《自动驾驶汽车法规》。
  - ✓ 日本将放宽无人驾驶汽车与无人机的相关法律法规，允许纯自动驾驶汽车进行路试。自动驾驶汽车（有司机）在2020年可以上高速公路行驶。
- Bad News：
  - ✓ 德国联邦参议院2017年过法律，允许汽车自动驾驶系统未来在特定条件下代替人类驾驶。但法律明确规定，配有自动5月 1 2 日通驾驶系统的汽车内将安装类似"黑匣子"的装置，记录系统运作、要求介入和人工驾驶等不同阶段的具体情况，以明确交通事故责任。如果事故发生在人工驾驶阶段，则由驾驶人承担责任；如果发生在系统运作阶段，或由于系统失灵酿成事故，则由汽车制造商承担责任。
  - ✓ 英国新出台了《汽车技术和航空法案》，旨在在自动驾驶汽车普及之前，帮助保险人和保险公司简化保险流程。据了解，同一保单承保车辆和乘客会给自动驾驶汽车制造商和软件开发商施加更多压力，因为他们必须在发生事故时承担赔偿责任。在发生事故时，为了加快事故赔偿速度，英国政府将首先考虑消费者的权益。

安全分析的技术活动

safety validation

controllability analysis

failure mode and effects analysis

driving situation analysis

hardware diagnostic coverage metrics

hazard analysis

change management

risk assessment

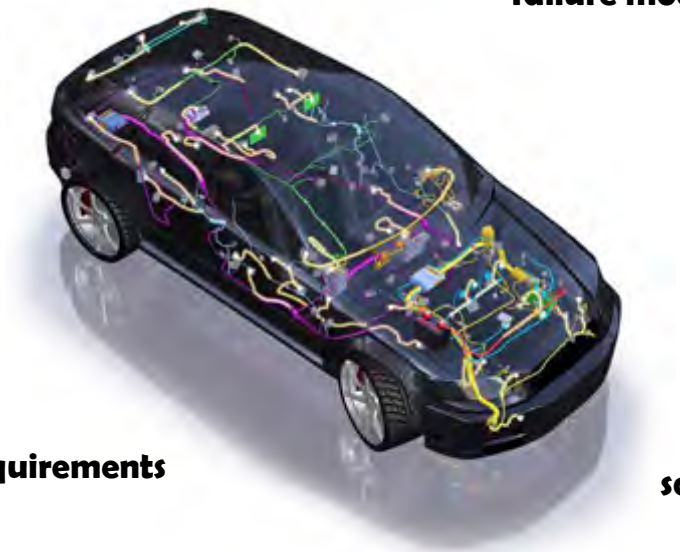
fault tree analysis

safety goals

configuration management

safety requirements

safety architecture



functional safety concept

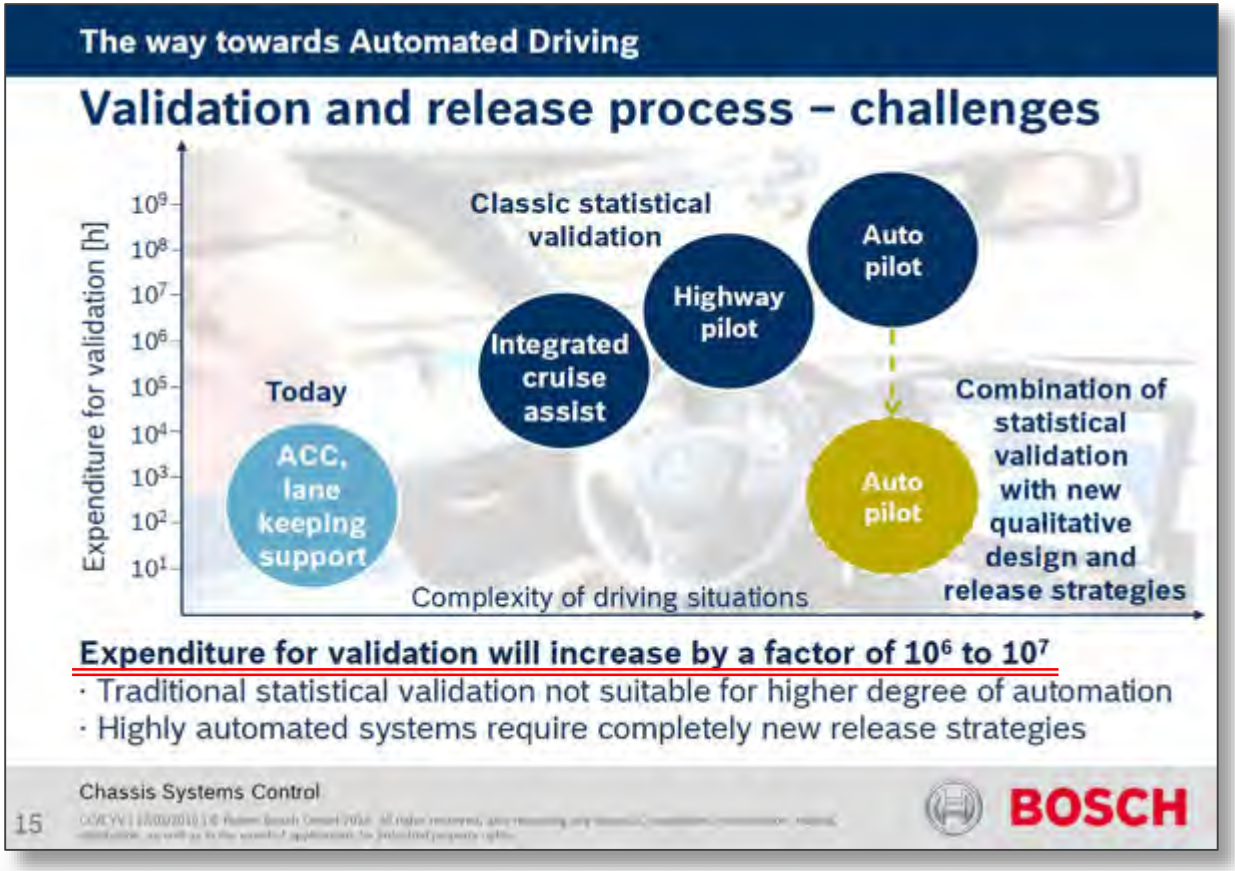
Safety standards like ISO 26262 require to perform multiple analysis methods in a consistent, thorough manner

软件安全性

- **近义词辨析**
  - **可靠性：**
    - 在规定的条件下和规定的时间内，**软件或硬件不引起**功能故障的性能指标；
  - **安全性：**
    - 是软件或硬件在运行中完成规定功能而**不致引起系统**发生不可接受风险的能力。
- **软件安全性的关键要素**
  - 一个单独的软件本身不存在安全性的问题。软件安全性**是系统安全性的一部分**；
  - **软件工程化**（ 软件开发技术和软件项目管理 ）改进的是软件可靠性；
  - **安全性保证技术**是改进软件安全性的重要手段：
    - 其核心就是确保**安全性需求**得以**正确、完备、一致的开发、实现和确认**。

传统方法所面临的困难和挑战

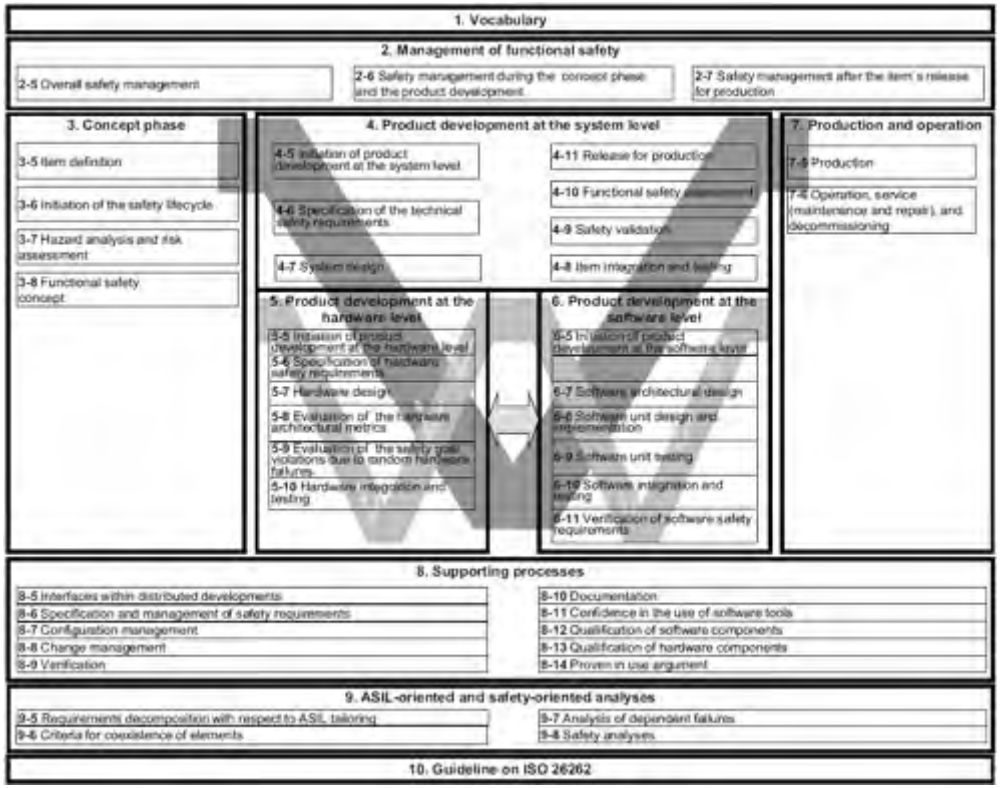
- BOSCH关于传统验证手段对于自动驾驶技术有效性的预测



汽车安全性国际标准（1/2）

- **ISO 26262是汽车的一个安全性国际标准**
  - ISO26262是从电子、电气及可编程器件功能安全基本标准**IEC61508派生出来**的。经历了大约6年左右的时间，于**2011年11月正式颁布**，成为国际标准；
  - 越来越多的国际知名品牌车企对于电子电气部件的采购已经明确提出了新的要求：**部件需要符合ISO26262标准并获得独立的第三方认证**。
  - 标准主要定位在汽车行业中特定的**电气器件、电子设备、可编程电子器件**等专门用于**汽车控制领域**的**部件和系统**。它旨在**提高**汽车电子、电气产品**功能安全性能**；
  - 标准的核心价值在于：它可以通过系统的功能**安全研发管理流程**，以及针对汽车电子控制系统硬件和软件的**系统化验证和确认方法**，**保证电子系统的安全功能在面对各种严酷条件时不失效**，从而保证驾乘人员以及路人的安全。

汽车安全性国际标准（2/2）



Part 1: Vocabulary

Part 2: Management of functional safety

Part 3: Concept phase

Part 4: Product development at the system level

Part 5: Product development at the hardware level

Part 6: Product development at the software level

Part 7: Production and operation

Part 8: Supporting processes

Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

Part 10: Guideline on ISO 26262

行业认证要求所带来的困难和挑战

- **与传统软件项目相比，一个DO-178 DAL A认证级项目将花费3倍的时间：**

Table-1 - Breadown by Safety Level

	NoCert	DAL A
Concept/Definition	9	9
System Design/Requirements, Functions and System Architecture	6	12
System Requirements allocated to Software	6	15
Plan	6	15
Sofware Design	18	40
Coding	16	35
Testing	18	90
Integration SW/SW - HW/SW	18	35
Reviews	3	55
Total	**100**	**306**

困难和挑战

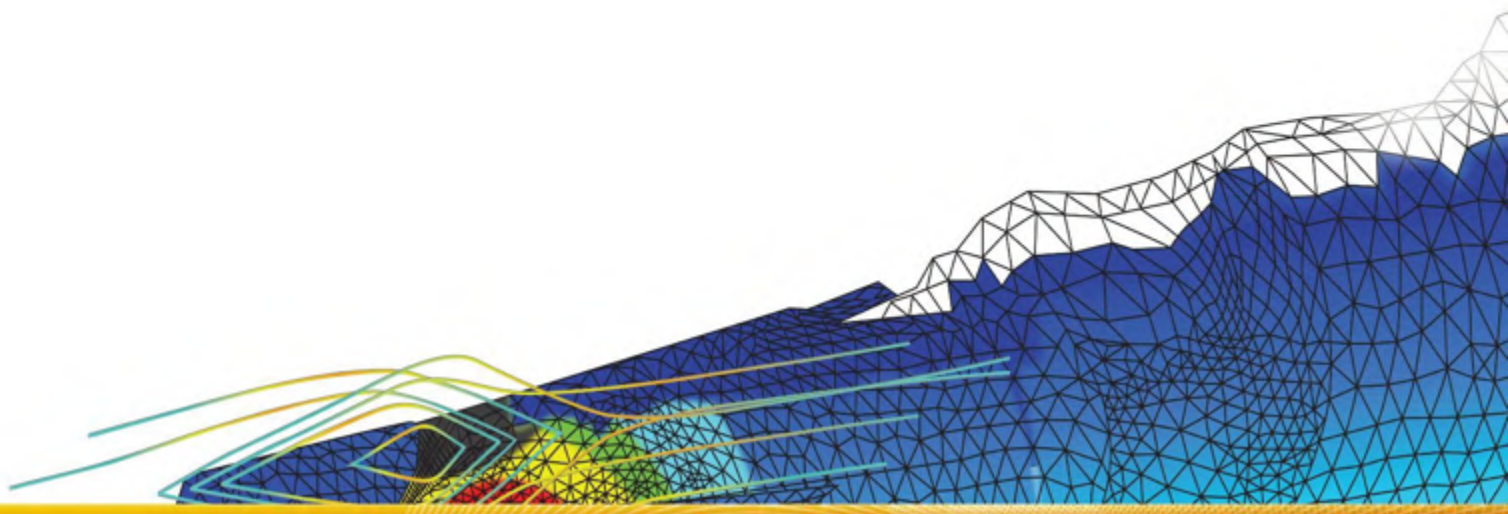
MORE TIME

MORE RISK

Realize Your Product Promise®

ANSYS

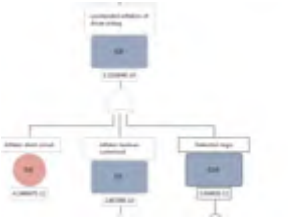
高安全性车载控制系统解决方案



ANSYS SBU Products Help to Cope

Functional Safety

medini™ analyze



Ensure system safety by providing state-of-the-art safety, quality and reliability *analysis methods* in an integrated model based approach

System Development

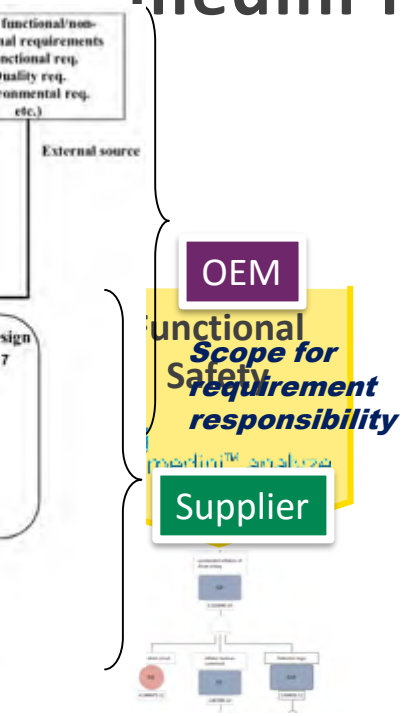
Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation

Embeded Software

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements

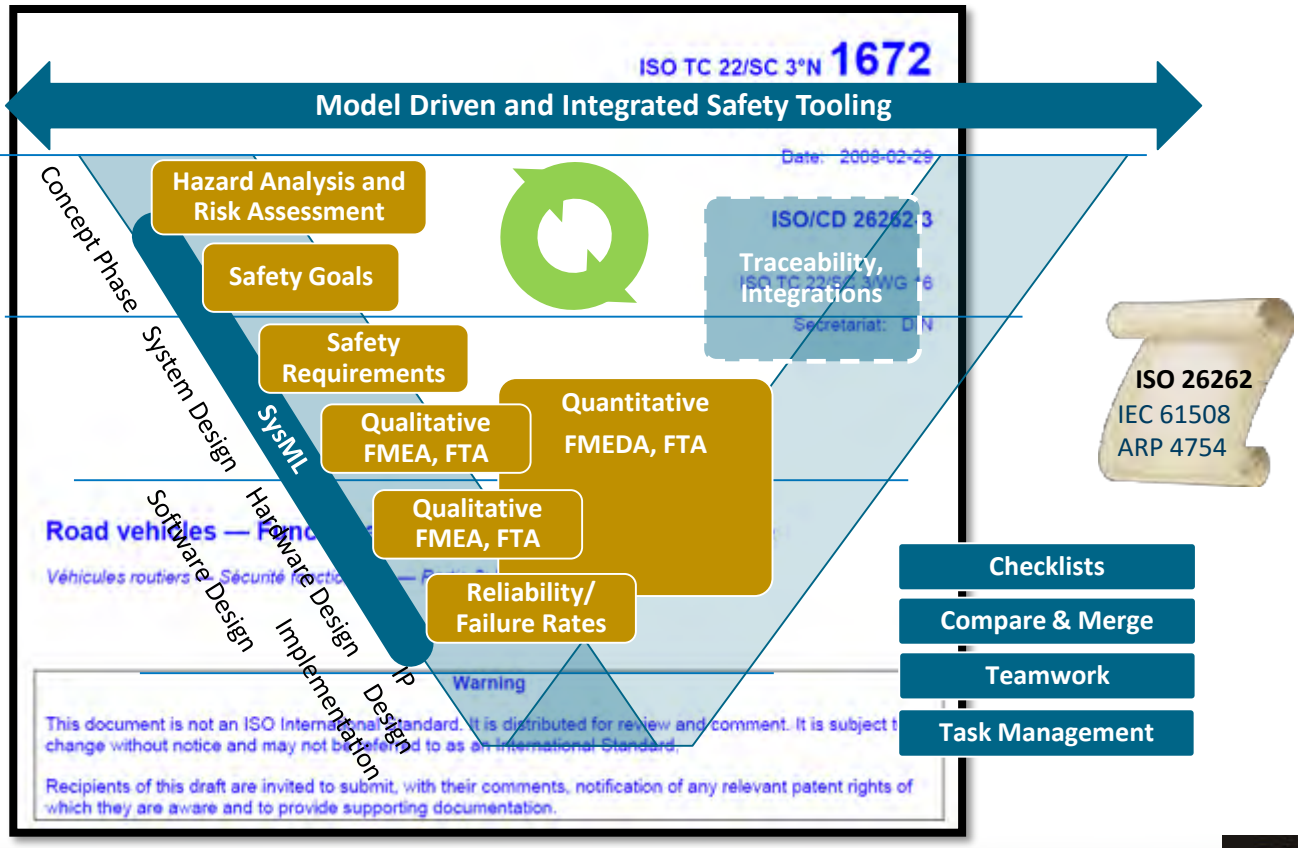
Safety standards like ISO 26262 require to perform multiple analysis methods in a consistent, thorough manner

medini for Model-based Safety Analysis (1/3)



Ensure system safety by providing state-of-the-art safety, quality and reliability *analysis methods* in an integrated model based approach

- **功能安全分析和设计过程**



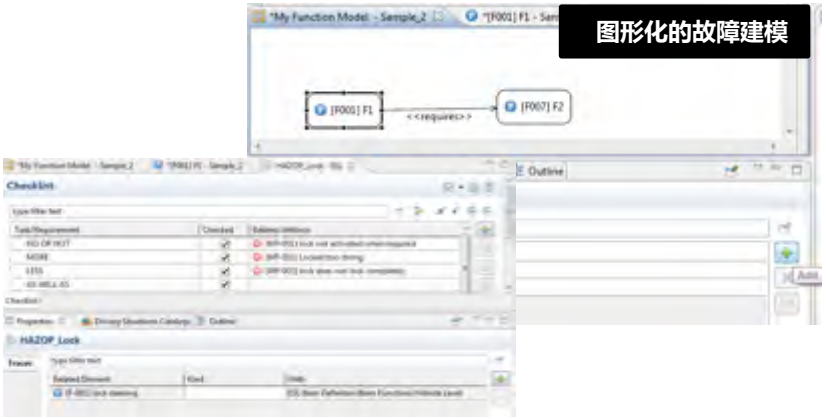
medini for Model-based Safety Analysis（2/3）

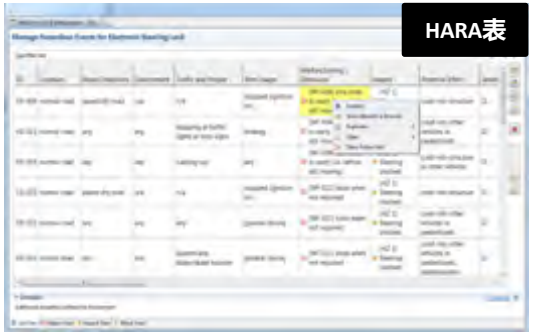
Functional Safety

medini™ analyze

Ensure system safety by providing state-of-the-art safety, quality and reliability *analysis methods* in an integrated model based approach

- **功能安全分析和设计方法**
  - ❖ 概念阶段（Concept Phase）
    - ❑ **目标：**
      - ✓ 危害分析
      - ✓ 确定安全目标
    - ❑ **medini功能方法：**
      - ✓ 驾驶状况和危险事件管理
      - ✓ 危害和可操作性分析（HAZOP）
      - ✓ 危害分析和风险评估（HARA）
      - ✓ 支持符合ISO 26262标准的ASIL测定与风险图，自动计算ASIL等级

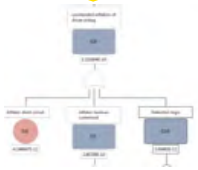




medini for Model-based Safety Analysis（2/3）

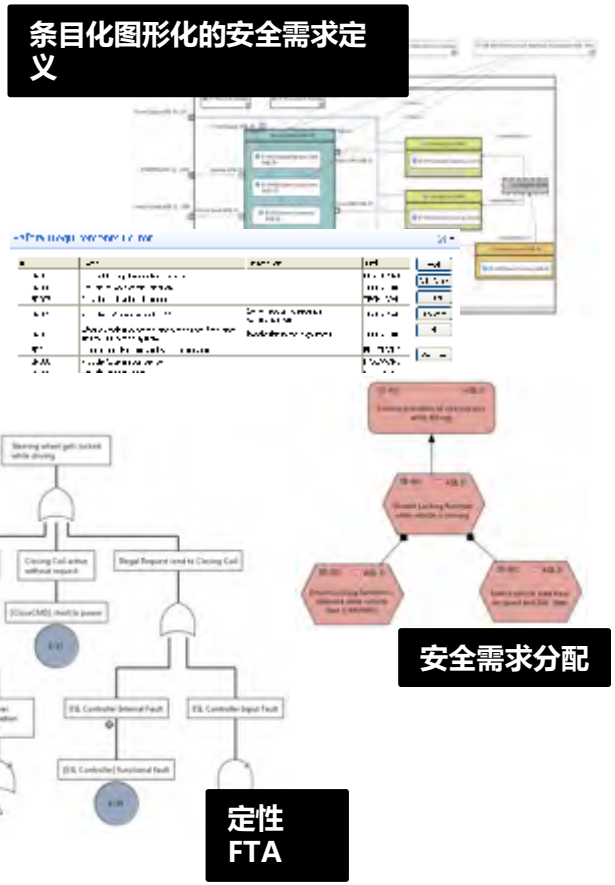
Functional Safety

medini™ analyze



Ensure system safety by providing state-of-the-art safety, quality and reliability *analysis methods* in an integrated model based approach

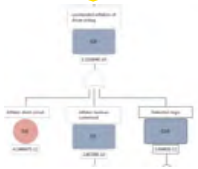
- **功能安全分析和设计方法**
  - ❖ 功能安全概念阶段（FSC）
    - ❑ **目标：**
      - ✓ 从功能安全目标推导功能安全需求
      - ✓ 把功能安全需求分配给子系统
    - ❑ **medini功能方法：**
      - ✓ **基于条目和图形的安全需求定**
      - ✓ **可视化的需求分配和追踪管理**
      - ✓ **故障树分析（FTA）**



medini for Model-based Safety Analysis（2/3）

Functional Safety

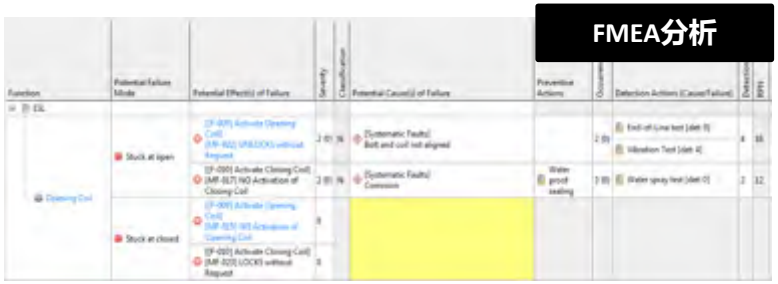
medini™ analyze



Ensure system safety by providing state-of-the-art safety, quality and reliability *analysis methods* in an integrated model based approach

- **功能安全分析和设计方法**
  - ❖ 技术安全概念阶段（TSC）
    - ❑ **目标：**
      - ✓ 按照功能安全概念规定技术安全需求
      - ✓ 对技术安全需求规定必要的安全机制
      - ✓ 技术安全需求应分配给系统设计元素（软硬件）
    - ❑ **medini功能方法：**
      - ✓ 故障模式和影响分析（FMEA）
      - ✓ 故障树分析（FTA）
      - ✓ 事件树分析（ETA）
      - ✓ 故障模式，影响和诊断分析（FMEDA）
      - ✓ 硬件安全性分析的诊断覆盖度指标
      - ✓ 支持单点故障分析
      - ✓ 支持潜在故障硬件度量
      - ✓ 支持故障率等级
      - ✓ 支持依据故障率手册的可靠性预测

FMEA分析



将ASIL调整到目标的ASIL

medini for Model-based Safety Analysis（3/3）

- **功能安全分析和设计目标**

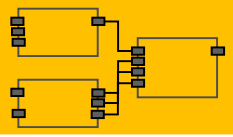
Functional Safety

medini™ analyze

Ensure system safety by providing state-of-the-art safety, quality and reliability *analysis methods* in an integrated model based approach

Hazard Analysis & Risk Assessment

System Architecture Model



HW Architectural Metrics

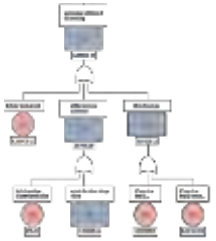
Extended with analysis related properties

Safety Requirements

FMEA

HAZOP

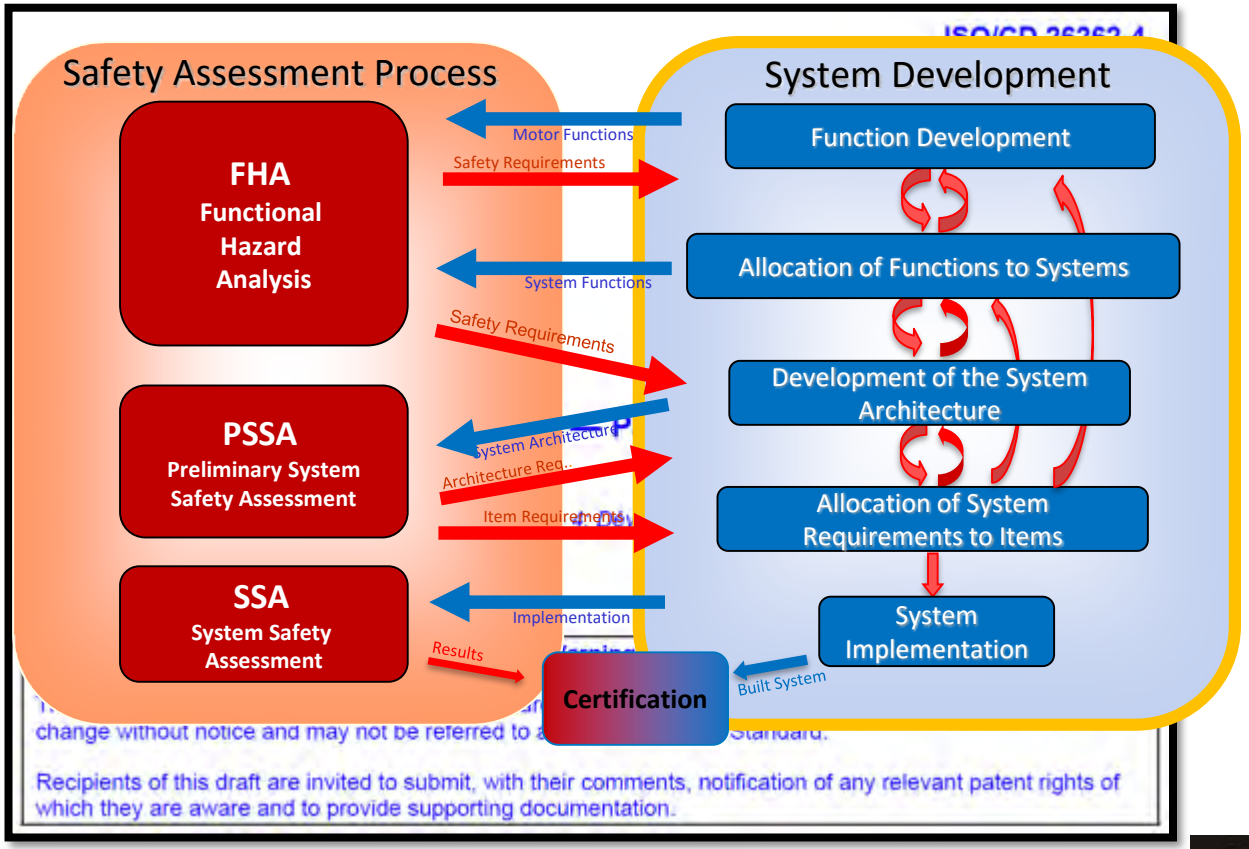
FTA



SCADE Architect for System Development (1/4)

- **系统开发流程**

Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation

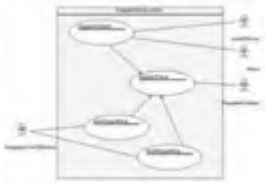


SCADE Architect for System Development (2/4)

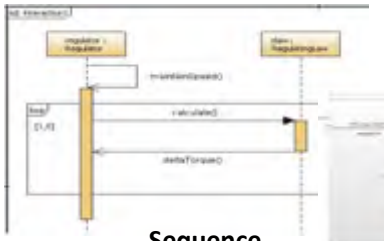
- **系统建模能力**
  - ❖ 基于SysML建模语言

System Development

Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation



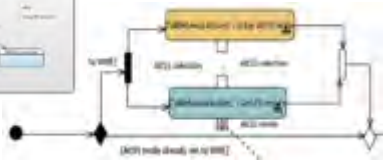
Use Case



Sequence

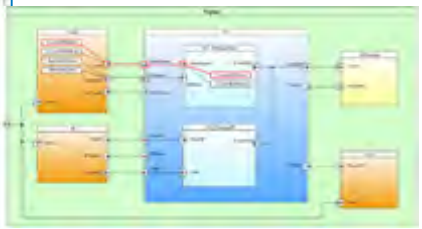
State Machine

Parametric



Activity

Block Definition



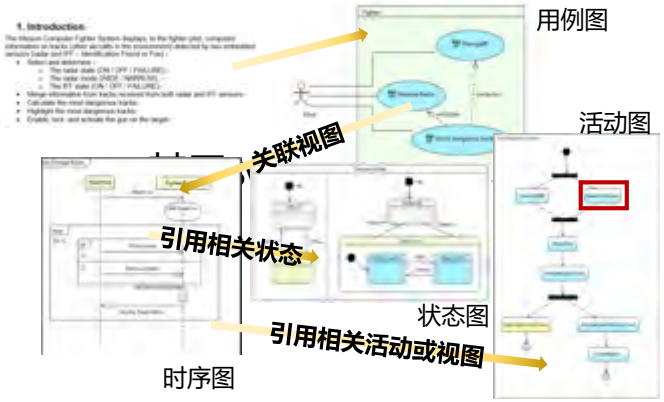
Internal Block

Tables

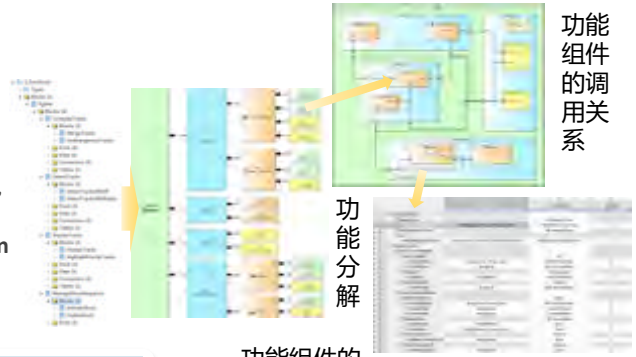
SCADE Architect for System Development (2/4)

System Development

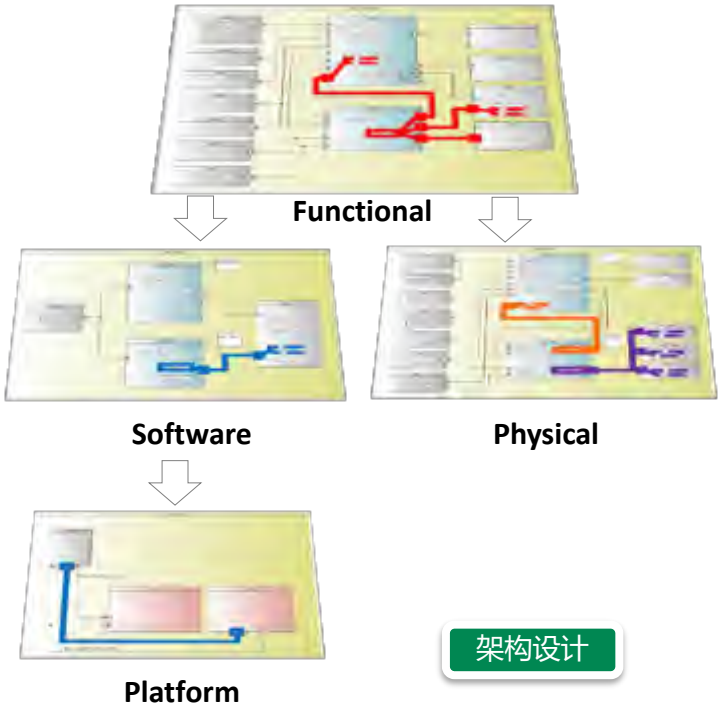
Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation



需求分析



功能开发



架构设计

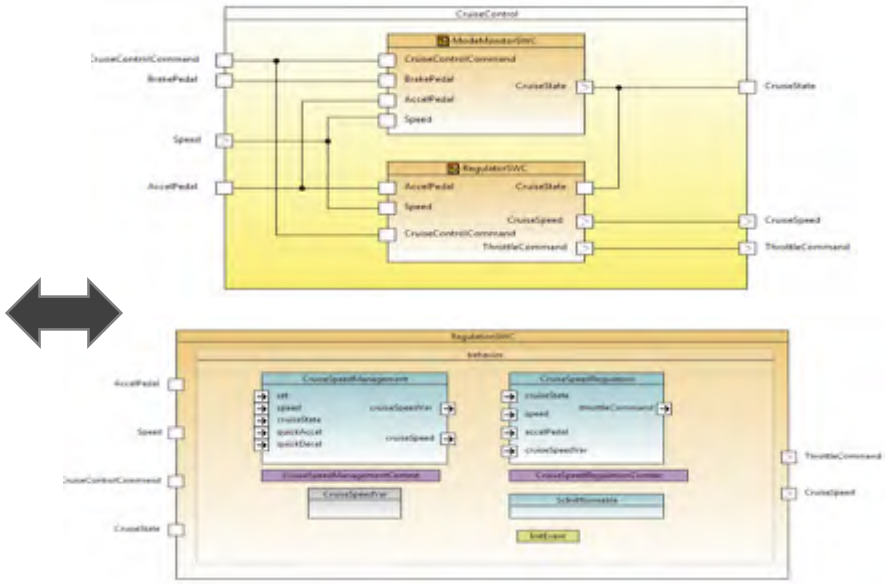
SCADE Architect for System Development (3/4)

- **基于AUTOSAR的汽车架构设计**
  - ❖ 基于汽车行业的专业模型库

System Development

Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation

AUTOSAR Model



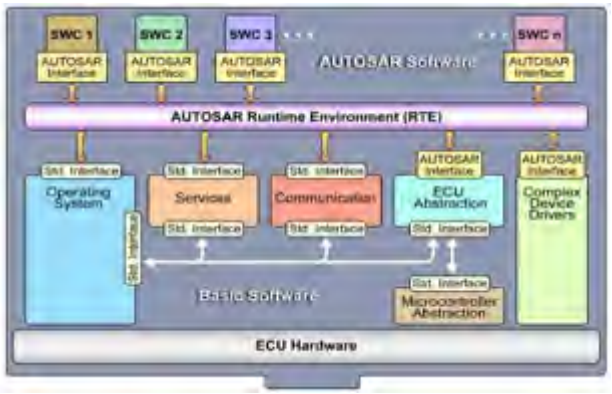
SCADE Architect

SCADE Architect for System Development (3/4)

- **基于AUTOSAR的汽车架构设计**
  - 基于汽车行业的专业模型库
  - 支持AUTOSAR 4.2.2标准
  - SWC描述文件的导入和导出

System Development

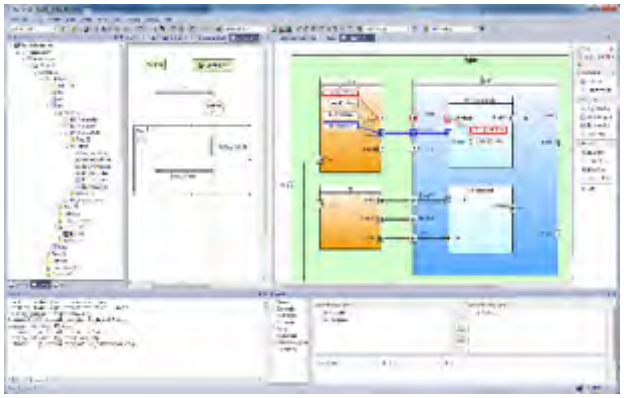
Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation



AUTOSAR Authoring Tool (AAT)

ARXML

SCADE Architect

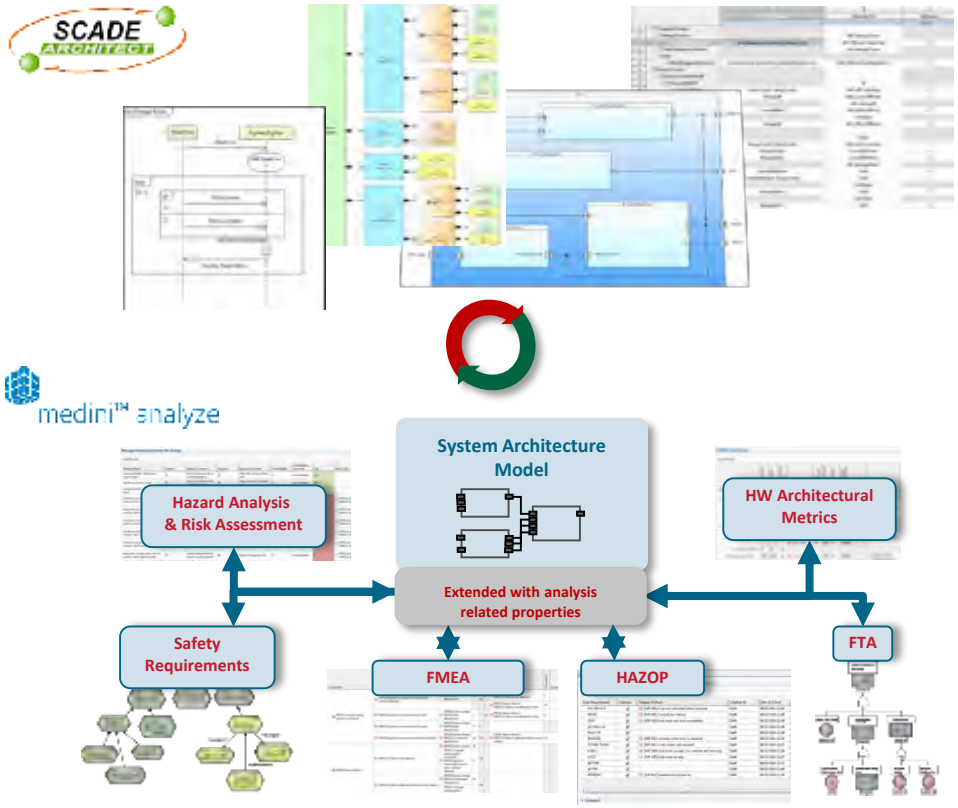


SCADE Architect for System Development (4/4)

- 与安全性分析工具medini的无缝集成

System Development

Simulate driving scenarios with detailed physics. Virtually test control algorithms, sensor accuracy and vehicle dynamics. Validate safety assumptions by simulation



Safety process seamlessly integrated with system development

Safety analysis results always consistent

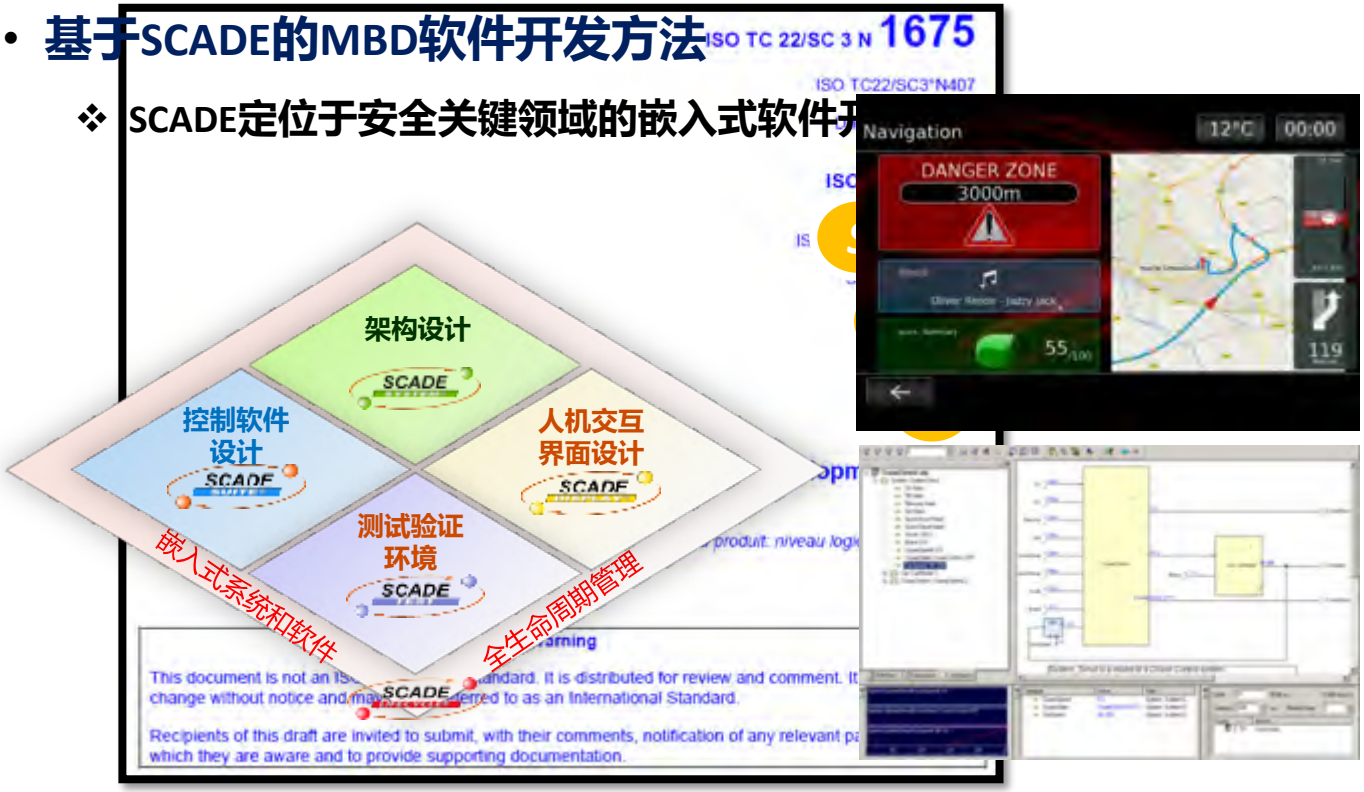
Safety requirements discovered and considered early in the design process

SCADE for Model-based Software Development (1/5)

Embeded Software

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements

- 基于SCADE的MBD软件开发方法
  - ❖ SCADE定位于安全关键领域的嵌入式软件开



SCADE for Model-based Software Development (2/5)

- **基于SCADE的MBD软件开发过程**

Embeded Software

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements

SCADE for Model-based Software Development (3/5)

- **满足ISO 26262的ASIL C\D软件开发要求**

Embeded Software

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements

❖ **模型语言——直接满足ISO 26262 中对建模和编码的考虑和要求**

SCADE语言是同步且形式化的语言（起源于同步语言Lustre）

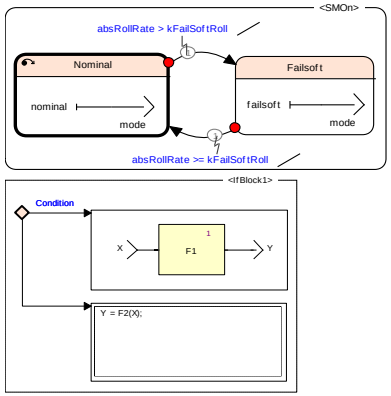
- ❑ SCADE语言简单稳定，确定性、强类型、明确的语义
- ❑ SCADE模型的解释不依赖于读者和运行环境，仅由数学逻辑唯一确定

包含安全结构和表述的语言子集（Correct/Safety by construction）

- ❑ 完全符合安全关键软件的编码要求
- ❑ 内嵌的防御性建模机制
- ❑ 模块化、低耦合的建模机制

经过30年的验证研究

图形化的表述，无需学习语言



SCADE for Model-based Software Development (4/5)

- **满足ISO 26262的ASIL C\D软件开发要求**
  - ❖ **测试验证——完全支持ISO 26262 中的测试验证要求**

Embeded Software

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements

语法检查：确保语言语法正确

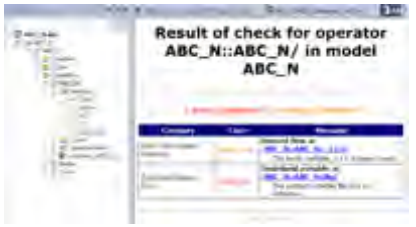
仿真调试：软件功能仿真和调试

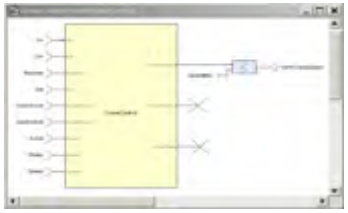
时间堆栈分析：与目标平台的符合性

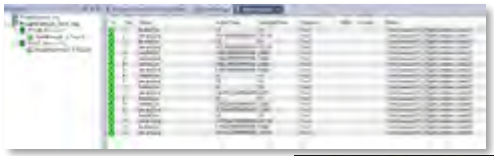
形式化验证：安全性需求验证

黑盒功能测试：确保单元功能的正确性

模型和代码覆盖率：评估验证的完备程度



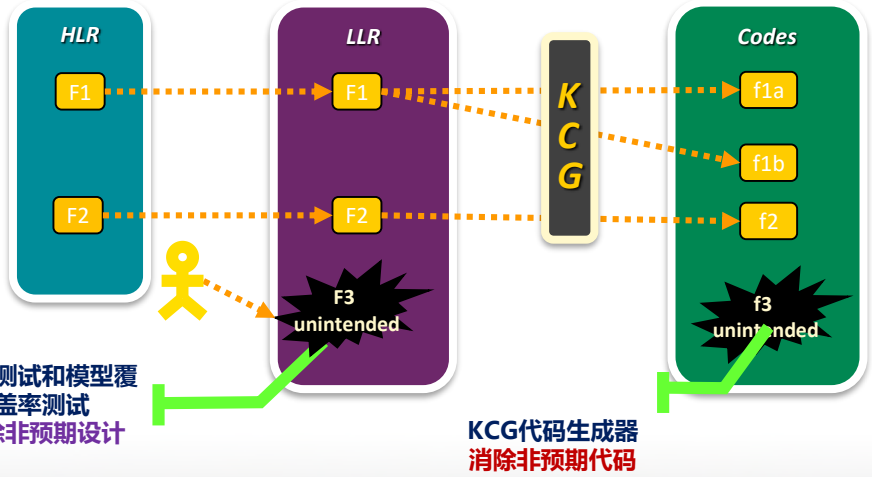


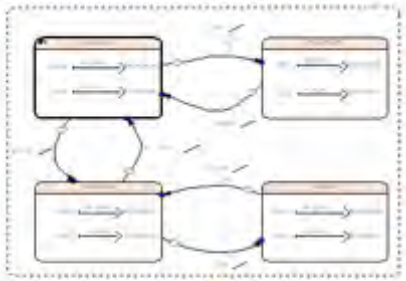


SCADE for Model-based Software Development (5/5)

- 满足ISO 26262的ASIL C\D软件开发要求
  - ❖ 认证级工具链——获得ISO 26262 ASIL D、IEC50128、DO-178C认证
    - ❑ 生成工具（TCL3）
      - ❖ SCADE Suite C/ADA Code Gneration 代码生成器
        - ✓消除代码的人工走查工作
        - ✓消除代码级的单元、集成测试工作
        - ✓消除代码级的覆盖率测试工作

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements





```
[...]
void Button_ABC_N(inC_Button_ABC_N *inC,
    outC_Button_ABC_N *outC)
{
 /* ABC_N::Button::SM1::SSM_SM1_dispatch_sel
    */
 SSM_Button_SM1_ST SSM_SM1_dispatch_sel;

 if (outC->init)
 {
  outC->init = kcg_false;
  SSM_SM1_dispatch_sel =
  SSM_SM1_Unselected__ABC_N;
 }
 else
```

SCADE for Model-based Software Development (5/5)

Embeded Software

Develop qualified, AUTOSAR compliant safety critical control and HMI software with model based development tools. Fulfill ISO 26262 requirements

- 满足ISO 26262的ASIL C\D软件开
  - ❖ 认证级工具链——获得ISO 26262 AS
    - ❑ 生成工具（TCL3）
      - ❖ SCADE Suite C/ADA Coc
        - ✓消除代码的人工走查工
        - ✓消除代码级的单元、集
        - ✓消除代码级的覆盖率测
    - ❑ 验证工具
      - ❖ SCADE Reporter 详细设计
      - ❖ SCADE MTC 模型覆盖率分
      - ❖ SCADE Test Environmen
        - ✓消除以上工具执行结果
  - ❖ 从而减少开发、验证时间，减少认证
  - ❖ 具备极高的认证信用，远大于100个设备级项目的认证

CERTIFICATE

No. Z10 16 11 55460 008

Holder of Certificate: Esterel Technologies
14 & 15, Place Georges Pompidou
78180 Montigny-le-Bretonneux
FRANCE

Factory(ies): 55460

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): Code Generator SCADE Suite KCG 6.6

Parameters: The code generator, classified as T3 offline support tool according to IEC 61508-4 and EN 50128, is qualified for the use in safety-related software development according to IEC 61508, EN 50128 and ISO 26262.

The report EM90205C is a mandatory part of this certificate.

Tested according to: IEC 61508-1:2010 (SIL 3)
IEC 61508-3:2010 (SIL 3)
EN 50128:2011 (SIL 3/4)
ISO 26262-8:2011 (ASIL D)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: EM90205C

Valid until: 2021-11-14

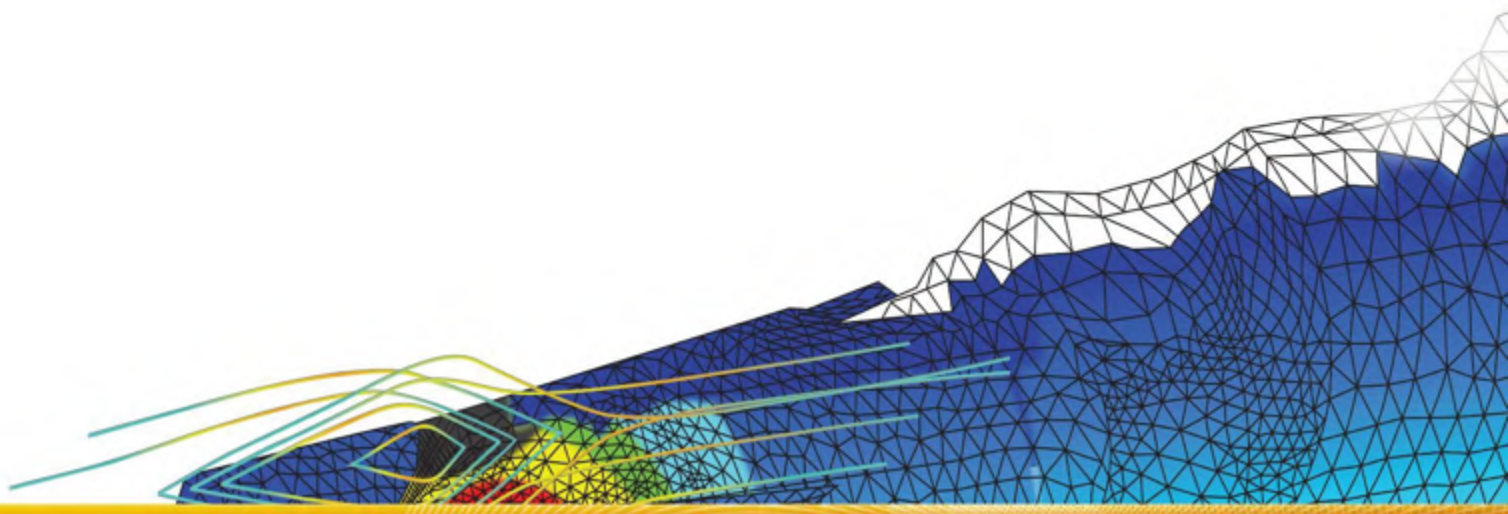
Date, 2016-11-18 (Peter Weiss)

Page 1 of 1

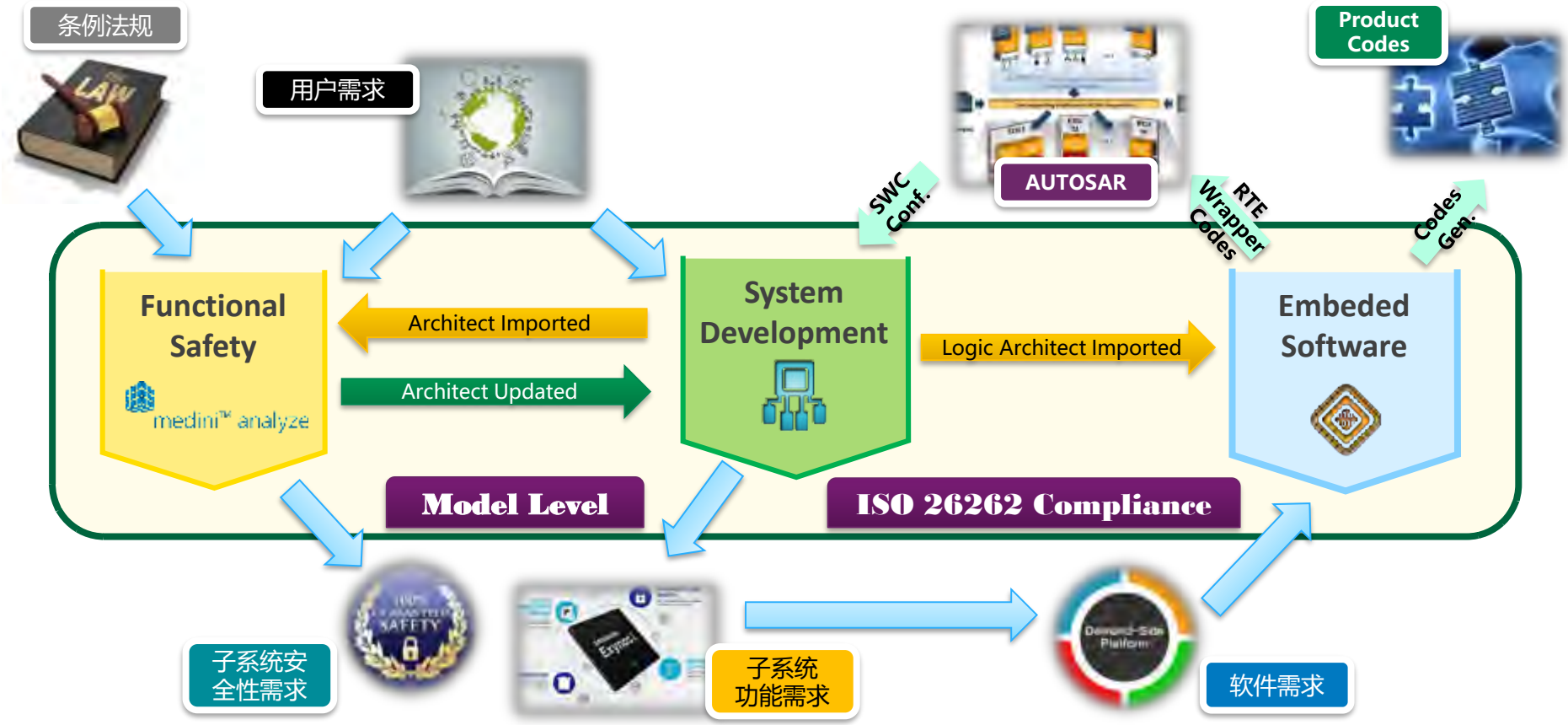
ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

ANSYS

总结



Completed MBD for Automotor E/E System



Benefit for Automotor Development

Saving Times for Safety & System & Software Development

Promote Quality of Embeded Software

Saving Times & Reducing Risks for ISO 26262 Certification

感谢聆听