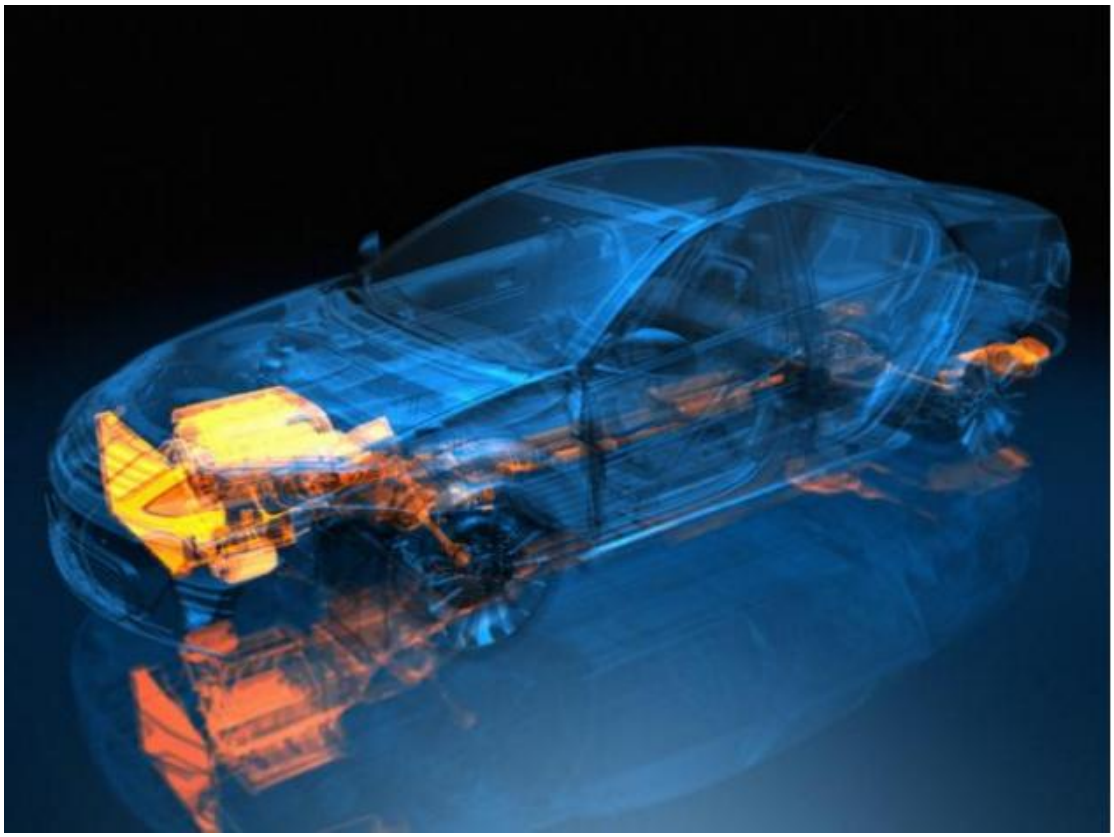
汽车系统建模的发展：EAST-ADL（第 1 部分）

DeJiu Chen, KTH; Lei Feng, Volvo; Henrik Lönn, Volvo; Juha-Pekka Tolvanen, MetaCase



数十年间，汽车嵌入式系统的开发人员已经领略到了建模的好处。模型不仅为沟通提供了更好的理解，也用于原型，分析，模拟和测试正在开发的系统。使用专用生成器，还可以从模型产生高质量的产品级软件代码。典型的代码生成案例是 HMIs 的各种控制工程解决方案和信息娱乐系统。

当前，汽车上关键功能和高级功能的数量显着增长。对开发效率和正确性的要求，结合所涉及的工程学科和工业技术的异质性，更增加了使用现代化的建模方法的必要性。模型可以解决汽车嵌入式系统，从消费者可见功能，到功能架构，硬件架构，软件组件，最后到详细的实现，等不同层次的抽象。由于涉及多个利益相关方并且有不同的关注点，模型也可能涉及各种系统方面，如需求，时间安排和功能安全约束，资源优化方案等。此外，由于开发通常分布在几个组织中，多个工程师也应该能够在与其他设计联系并共享其他设计的同时工作。为了实现并发开发，更快的反馈循环和协作，一个人保留一个可编辑的单图模型在现在是没有意义的。

再联系到系统开发生命周期，这意味着模型不仅仅应用在 V 模型的底部，而且也适用于早期系统规划和设计阶段。一个良好设计的集成模型可以让开发人员使信息和工作管理自动化，并能进行有效的决策，又同时避免昂贵的故障和延迟。特别是，基于模型的方法构成了安全工程的重要基础，因为需要考虑各种系统假

设和设计解决方案，例如由道路车辆的功能安全标准 ISO26262 所规定的各种情况。

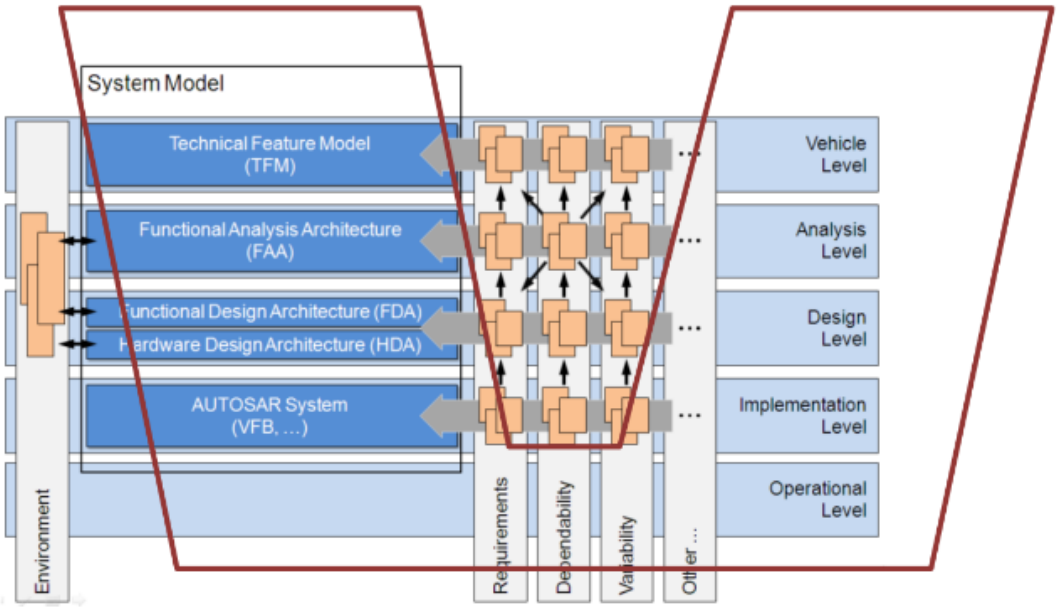


图 1. 在 V 模型中使用建模技术

从对单个功能的建模到对整个架构建模

EAST-ADL 是嵌入式系统规范和分析的领域专用语言。它的目的是解决基于模型的工业规模的汽车嵌入式系统开发的需要，这时，时间和安全往往是关键的要求。语言是特定领域的，因为基本的建模概念是基于领域概念和车辆嵌入式系统的一些关键工业标准而来的。

例如，建模的基础架构和基本方法与 AUTOSAR 一致。与嵌入式系统的其他系统描述语言相比，EAST-ADL 对系统开发生命周期进行了更全面的观察，并在明确阐述一些关键工程问题的同时，为信息管理提供了各种模型间细粒度的可追溯性。正如本文所展示的，这推动了一种更系统的架构设计方法。做为分析的优势，EAST-ADL 模型可以与各种现有的建模技术和工具集成。对于最终的产品实现，使用 EAST-ADL 制定的系统架构定义通常由更详细的软件和硬件解决方案（如 AUTOSAR，JasPar 或内部架构）实现。

示例：从特性和需求开始

接下来我们使用一个小例子来检查 EAST-ADL 及其应用：具有 ABS 的反馈制动系统。典型的开发起点是车辆的特性 – 如图 2 所示。这里，EAST-ADL 的特性模型通过捕获特性组合定义了正在开发的制动系统，并特别展示出了一些与制动相关的关键汽车功能及其相关功能（dependencies）：例如，可选的 AdvancedBraking 特性是由 ABSBraking 及可选的 ESPBraking 专门提供的，但是如果选择了 ESPBraking 制动特性，则 ABSBraking 特性也需要。虽然这个例子显示了一些车辆功能，但功能模型可以通过解决功能及其关系（如功能依赖和排除）来指定和管理与整个产品系列相关的每个车辆的内容。为了定制的目的，诸如模型和市场的市场方面可以组织在特征模型中，并且追溯到更多的技术特征（例如特定硬件平台的选择）。

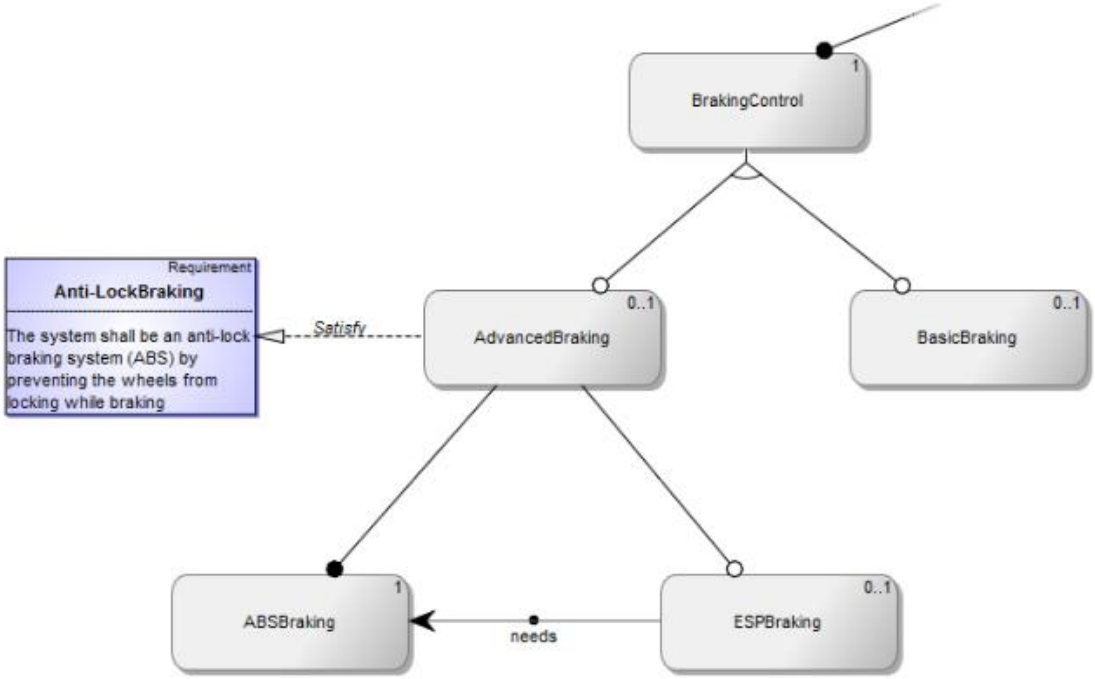


图 2. 具有 ABS 的反馈制动系统的特性模型（局部）

与车辆特征的组合平行，我们可以从车辆级别要求的说明开始。 EAST-ADL 支持捕获不同类型的需求，包括与质量有关的超功能问题，以及它们与系统开发生命周期中各种文物的绑定。 要求也可以从现有需求管理工具导入，并与 EAST-ADL 型号对齐。 例如，在图 2 中，AdvancedBraking 功能满足 Anti-LockBraking 要求。 与特征或其他类型的模型元素的这种关系可以随后被并入到可能使用的外部需求管理工具中。

实现独立架构

EAST-ADL 的核心部分，顾名思义，侧重于多层次的系统设计在体系结构方面的规范。作为实现预期车辆功能的第一步，汽车嵌入式系统的完整电气功能可以被指定为独立于实现的功能分析架构。这种架构规范的特征在于一些相互作用的抽象应用功能的组合。这些功能中的每一个都由其输入输出接口，执行模式以及相关的行为和功能外限制来指定。图 3 显示了 ABS 相关功能架构规范的一部分。这里 ABS_1 功能与 Brake_1 的制动力请求 相连， 这是一个抽象的驱动设备（FunctionalDevice）。然后该制动致动装置提供表示实际制动转矩的物理能量流。

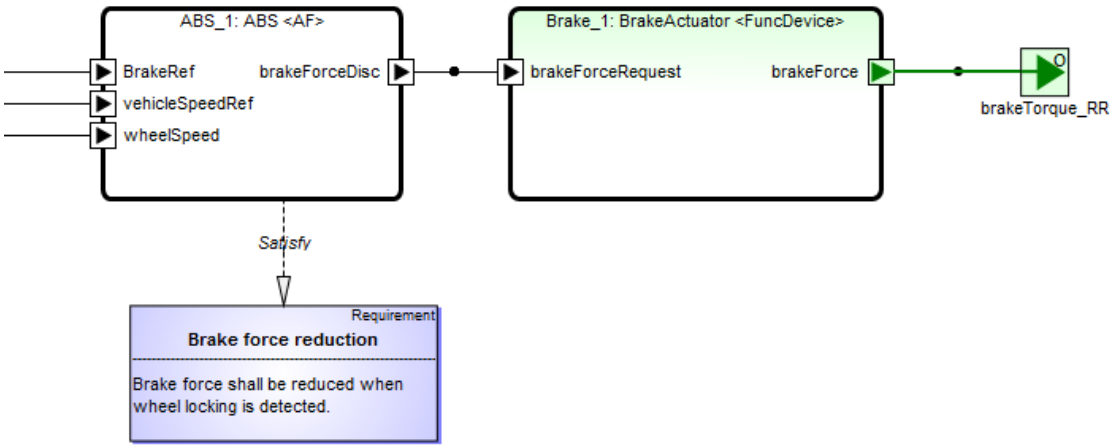


图 3. 与 ABS 相关的功能分析架构

EAST-ADL 遵循用于组件定义和实例化的类型原型模式。例如，诸如 ABS 和 BrakeActuator 的功能类型　可以针对不同的制动器实例被多次实例化（在这种电动车辆中实际上有四个制动功能原型 – 四个制动器中的每一个各有一个）。

与特征模型类似，可以将各种要求映射到各个架构元素，从而能够跟踪和分析系统如何满足各种需求。这里的　ABS_1 功能满足了从中得到的制动力减小要求要素已经在特征模型中提出（图 2）。这是因为 *ABS_1* 功能与轮速监控，ABS 控制，四轮刹车扭矩驱动等功能一起构成实现 *ABSBrake* 功能的控制回路　。ABSBraking 功能专门设计了 AdvancedBraking 功能，从而继承了这些要求。基于 EAST-ADL，工具支持使跟踪能够看到例如满足特定要求的所有功能。可以在如图 3 所示的功能体系结构模型中指定映射和跟踪，或者在图 4 中的单独视图中指定满足特定要求的功能。

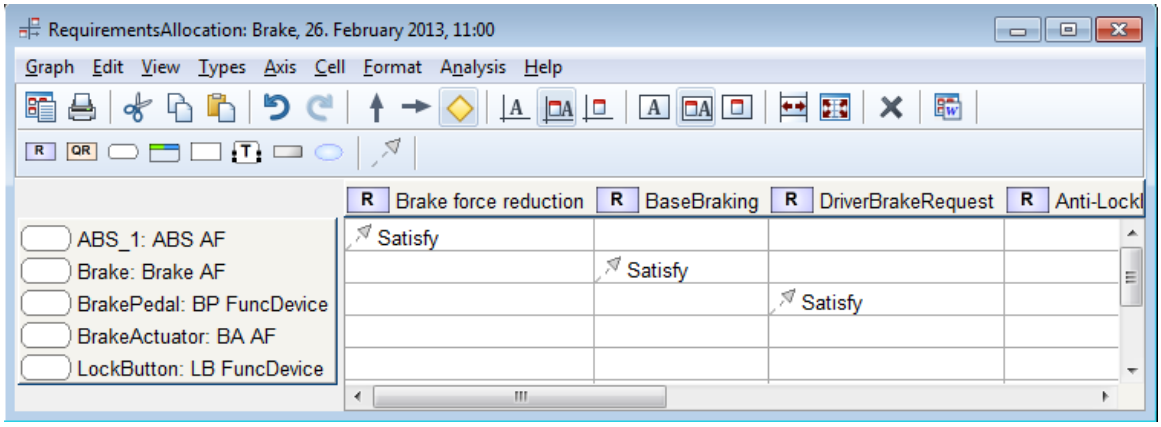


图 4. MetaEdit +工具中 regenerative breaking 功能所满足的要求

转向设计架构

在技术架构规范中首先考虑了抽象功能的具体实现，称为功能设计架构。它指定了在特定软硬件平台上实现的分析架构的改进（例如，通过抽象应用程序功能的分配和分割）。这个图示如图 5 所示。这里 BrakeRR 设计功能接收三种不同的数

据：请求的转矩，车轮速度和车速。此功能连接到本地设备管理器，将信号发送到硬件功能。然后，这个硬件功能可以为 BrakeTorque_RR 提供物理能量。

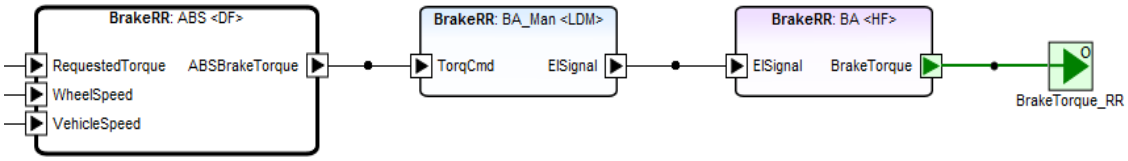


图 5. 再生破坏的设计功能

与功能并行，EAST-ADL 允许设计硬件架构，包括传感器，执行器，电源和 ECU。图 6 显示了硬件架构的一部分，其中 BrakeRR 功能从映射到 HW 架构的功能设计。传感器 Encoder_RR 通过 IOConnection 向 ECU_RR 节点提供每分钟的转数，然后 ECU_RR 节点将请求发送到位于右后方的制动器。所有的硬件组件都有一个端口供电。ECU 节点组件也通过通信端口连接到网络。

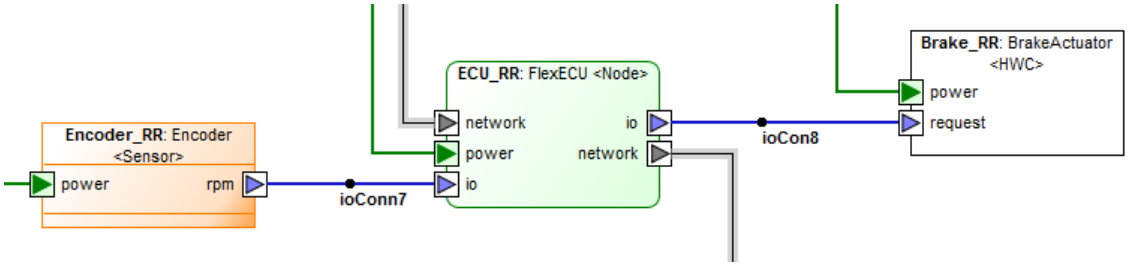


图 6. 再生破坏的硬件体系结构摘录

图 7 显示了对节点的功能分配。

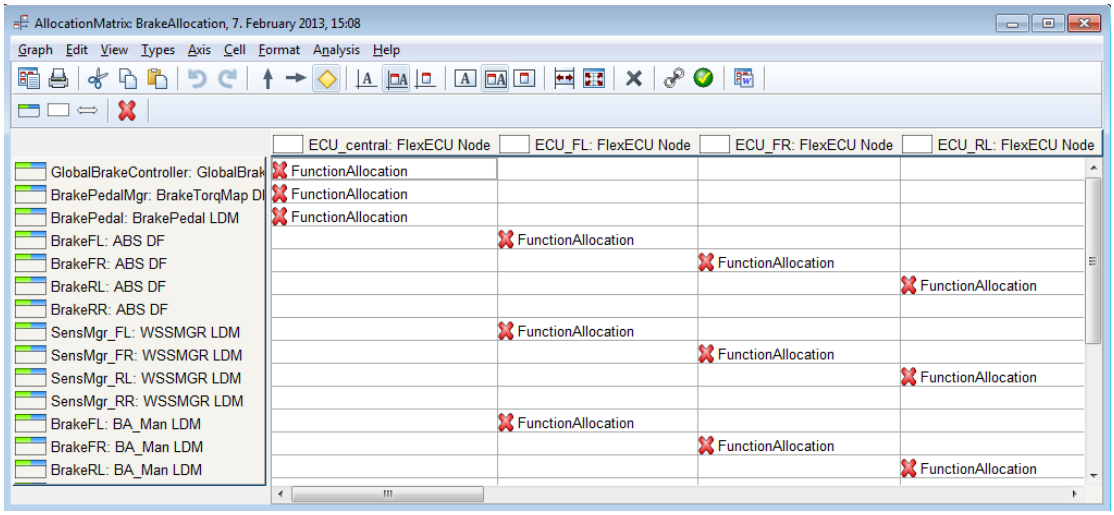
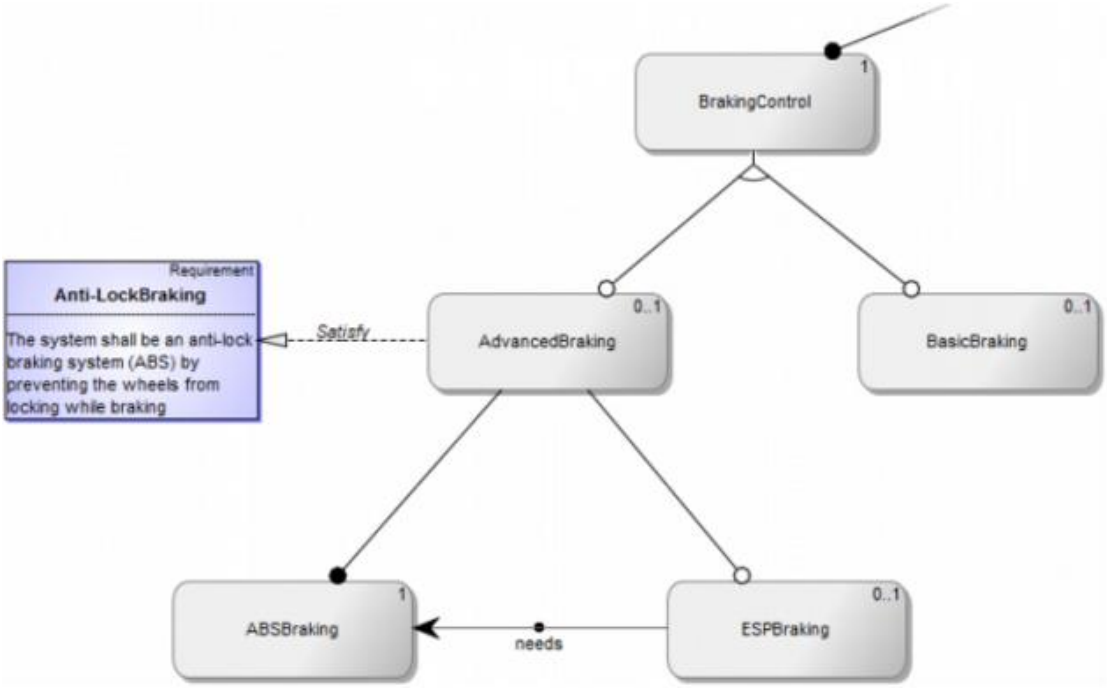


图 7 功能到节点映射表

第二部分将介绍行为描述和分析，可靠性建模和映射到现有软件架构。

北京怡然瑞丰科技有限公司 张劲松
E-mail：theseus.zhang@yeerichtek.com Tel：13391680017

汽车系统建模进展：EAST-ADL（第 2 部分）



几十年前，汽车嵌入式系统的开发人员已经获得了建模的好处。模型不仅为沟通提供了更好的理解，也用于对原型，分析，模拟和测试进行系统开发。使用专用生成器，也可以从模型生产高质量的生产级软件代码。代码生成的典型案例是 HMI 的各种控制工程解决方案和信息娱乐系统。

行为描述和分析

使用 EAST-ADL，开发人员可以根据需求工程，质量预测，设计验证和验证，安全工程的需求，捕获并形成各种行为问题。为了形式化行为描述，EAST-ADL 提供了一个集成了离散事件和连续时间行为模型的混合系统模型。所有行为描述与要求，系统设计和约束规范以及验证和验证案例无缝地进行管理。图 8 显示了一个功能类型 ABS 由 ABS_BehaviorConstraint 约束的示例。

北京怡然瑞丰科技有限公司 张劲松
E-mail：theseus.zhang@yeerichtek.com Tel：13391680017

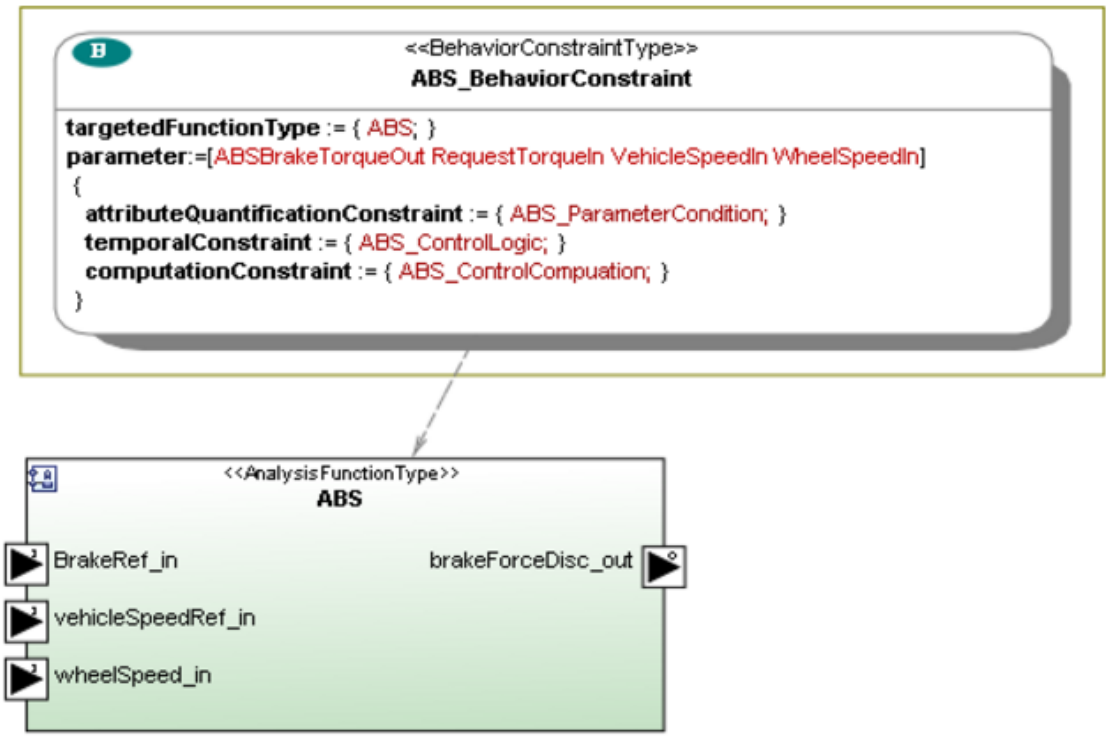


图 8. 注释 ABS 功能的行为约束

EAST-ADL 正式捕获三类行为约束。工程师在其特定的设计和分析环境中，决定要应用的确切类型和约束程度。这些类别的行为约束是：

属性量化约束- 与价值属性的声明和相关的绝对量化相关（例如，U = I * R）。
时间约束- 涉及行为约束的声明，其中考虑到时间表上的行为历史。
计算约束- 与逻辑变换（用于数据分配）和逻辑路径方面的数据的因果依赖关系的声明有关。
让我们考虑 ABS 功能要满足的属性量化约束的一个例子。在图 9 中，VehicleSpeedIn 和 WheelSpeedIn 是从端口接收的两个监视变量。这两个外部变量与常量 WheelRadius 根据量化条件[SlipRateQuantification]决定估计的 SlipRate。

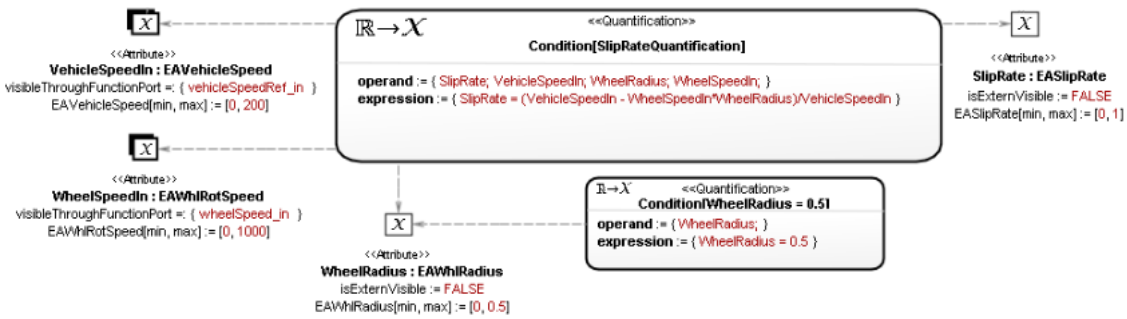


图 9. 对 ABS 功能注释属性量化约束

在图 10 中，通过根据状态机捕获 ABS 控制逻辑来进一步阐述行为约束。state invariants 和 transition guards 由一些属性量化规范精确定义，如 Conditon [VehicleSpeedIn> ABSVehicleSpeedThreshhold]和 Conditon [SliprateThreshhold <= SlipRate <= 1]。

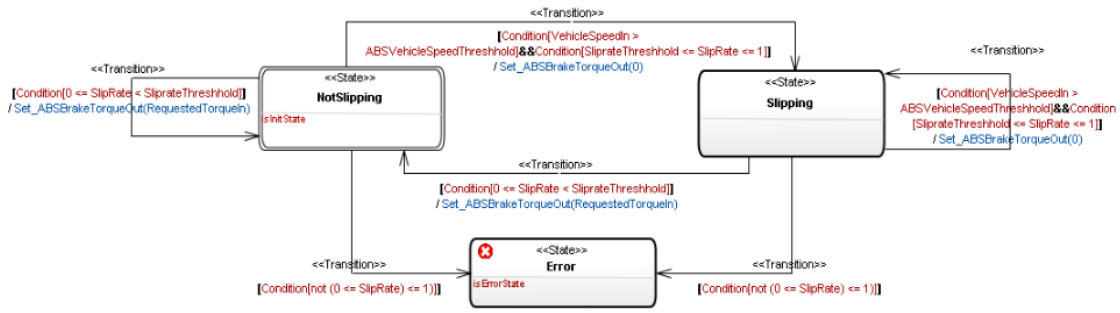


图 10.注释 ABS 功能的时间约束

图 11 显示了 ABS 功能的相关计算约束。该规范声明对计算 ABS 制动转矩请求的变换 *Set_ABSBrakeTorqueOut*（）允许的两次　调用。

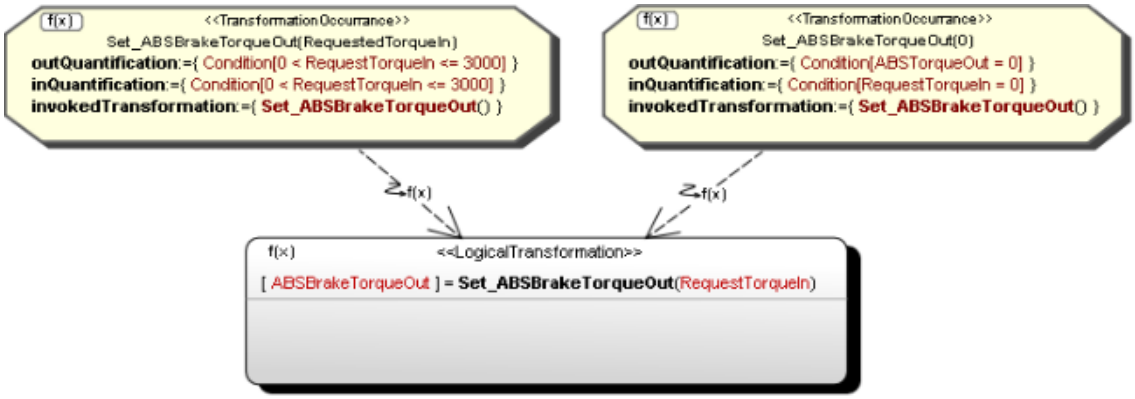


图 11.注释 ABS 功能的计算约束

关于应用功能的执行，EAST-ADL 通过其时序模型，可以将整体时序约束的映射指定为多任务处理的各个功能的时序属性。对于每个系统功能，这样的定时属性包括优选的触发策略（例如，时间或事件触发）和相关的时序约束（例如响应时间，优先级和同步）。如果被触发，每个系统功能都会根据运行到完成语义运行。

EAST-ADL 旨在通过成熟的分析方法和工具获得大部分分析杠杆。为此，从 EAST-ADL 行为模型转换为支持外部分析工具的模型包括 SPIN，UPPAAL，Matlab / Simulink 和 Modelica。

我们来考虑使用模型检查器 SPIN 彻底验证行为模型与要求的一个示例。可验证的要求包括断言，死锁自由，期望状态的可达性，避免或遵守给定执行模式以及线性时间逻辑（LTL）语句。我们已经定义了 EAST-ADL 行为结构和用于指定 SPIN 模型的 PROMELA 语言之间的通用映射规则。

映射规则作为MetaEdit+中的算法实现，将EAST-ADL的行为模型自动转换为SPIN模型。图 12 显示了 ABS 功能的 PROMELA 代码部分。断言语句 assert（0）指导 SPIN 搜索执行路径以达到语句，路径指示车轮的锁定状态。在模型检查术语中，路径是一个反例，给设计者提供如何达到给定状态的提示。

```
        /* The ABS function at each wheel satisfies the run-to-completion semantics */
proctype abs(byte id; chan RequestedTorqueIn, VehicleSpeedIn, WheelSpeedIn, ABSBrakeTorqueOut)
{
    byte reqTorq, vehSpd, whlSpd, ABSBrakeTorq; /* Local variables */

    do
    :: trig_abs[id] ? _ ->                  /* The execution trigger */
        read_Inport(RequestedTorqueIn, reqTorq);    /* Read all inports and save the values */
        read_Inport(VehicleSpeeddIn, vehSpd);       /* in local variables */
        read_Inport(WheelSpeedIn, whlSpd);
                /* Note: the vehSpd in this process is the estimate from the average */
                /* of the speeds of the 4 wheels. */
        if
        :: vehSpd > ABSVehicleSpeedThreshold &&
            vehSpd - whlSpd*WheelRadius > vehSpd*ABSSlipRateThreshold ->
                                            /* If locked, release the brake */
            ABSBrakeTorq = 0;               /* Set_ABSBrakeTorqueOut(0) */
            assert(0)                       /* Flag an error when a wheel is locked */
        :: else ->      /* If not locked, apply the full torque demand */
            ABSBrakeTorq = reqTorq      /* Set_ABSBrakeTorqueOut(RequestedTorqueIn) */
        fi;

        write_Outport(ABSBrakeTorqueOut, ABSBrakeTorq)      /* Write the outports */
    od
}
```

图 12. ABS 功能的 PROMELA 代码段

为了说明通过 SPIN 的分析杠杆，此断言的验证结果如图 13 所示，带有 SPIN 打印输出的屏幕快照。顶行显示了 SPIN 模型检查器的版本以及应用的算法选项的以下两行。在较低的部分我们可以看到该验证的内存使用情况：实际使用量为 154 MB。最后一行表示执行时间，即 4.63 秒。不熟悉 SPIN 的读者可以方便地忽略其他细节。SPIN 可以通过跟踪变量值可视化计数器示例，并通过消息序列图检查流程通信。当车轮速度被制动转矩减小但没有计算出最新的车速估计并向车轮广播时，发生图 13 中所示的锁定状态。这种情况在当前架构中是可能的，因为进程是异步的，并且可以以任何顺序发生。如果要在确定控制决策前确保 ABS 功能总是接收到最新的速度估计值，则必须在软件架构中执行更严格的执行和通信协议。

```
(Spin Version 6.2.2 -- 6 June 2012)
Warning: Search not completed
    + Partial Order Reduction
    + Compression

Full statespace search for:
    never claim             - (not selected)
    assertion violations    +
    cycle checks        - (disabled by -DSAFETY)
    invalid end states  +

State-vector 220 byte, depth reached 249, errors: 1
  2111709 states, stored
  1104578 states, matched
  3216287 transitions (= stored+matched)
       18 atomic steps
hash conflicts:     36667 (resolved)

Stats on memory usage (in Megabytes):
  475.276   equivalent memory usage for states (stored*(State-vector + overhead))
   90.391   actual memory usage for states (compression: 19.02%)
            state-vector as stored = 29 byte + 16 byte overhead
   64.000   memory used for hash table (-w24)
    0.009   memory used for DFS stack (-m250)
  154.332   total actual memory usage


nr of templates: [ 0:globals 1:chans 2:procs ]
collapse counts: [ 0:5276 2:18 3:30 4:39 5:56 6:238841 ]

pan: elapsed time 4.63 seconds
To replay the error-trail, goto Simulate/Replay and select "Run"
```

图 13. SPIN 验证结果

除了 ABS 功能中的断言之外，我们还可以检查整个制动系统的许多其他属性，包括 ABS 功能，驾驶员制动指令，车轮和车身动力学。

可靠性建模

作为一个整体系统的财产，安全是关于故障和故障的情况以及它们对系统的影响。EAST-ADL 旨在在 ISO 26262 参考安全生命周期涵盖的所有阶段中精确地表达安全要求和相关信息以及标称系统模型。这意味着对于任何安全要求，EAST-ADL 基于 ISO / DIS 26262 的 ASIL（汽车安全完整性等级）分类方案，提供了对其分配，精确含义和完整性等级的支持。

EAST-ADL 涵盖了安全要求的规范及其系统可靠性的影响，包括：

1.整体系统的安全目标以车辆级视角为特征

2.功能安全概念源于安全目标及其对高级系统功能的分配

3.从功能安全要求和对硬件和软件特定设计解决方案的分配中得出的技术安全概念

4.硬件和软件安全要求分配给硬件和软件架构的执行级别。

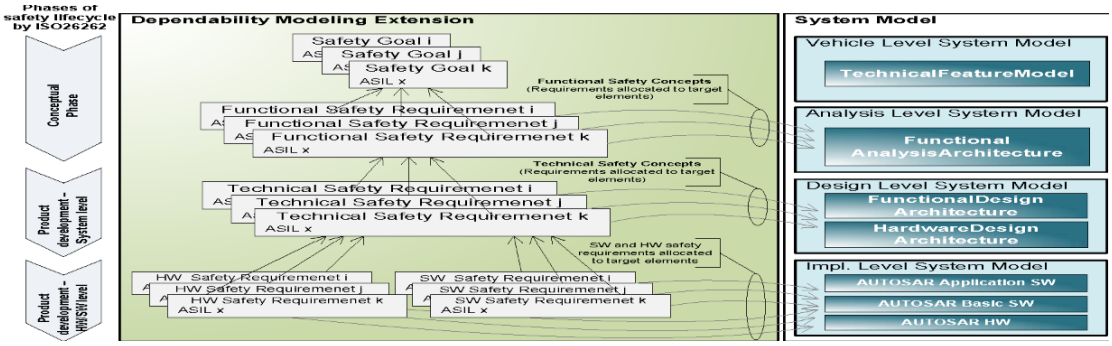
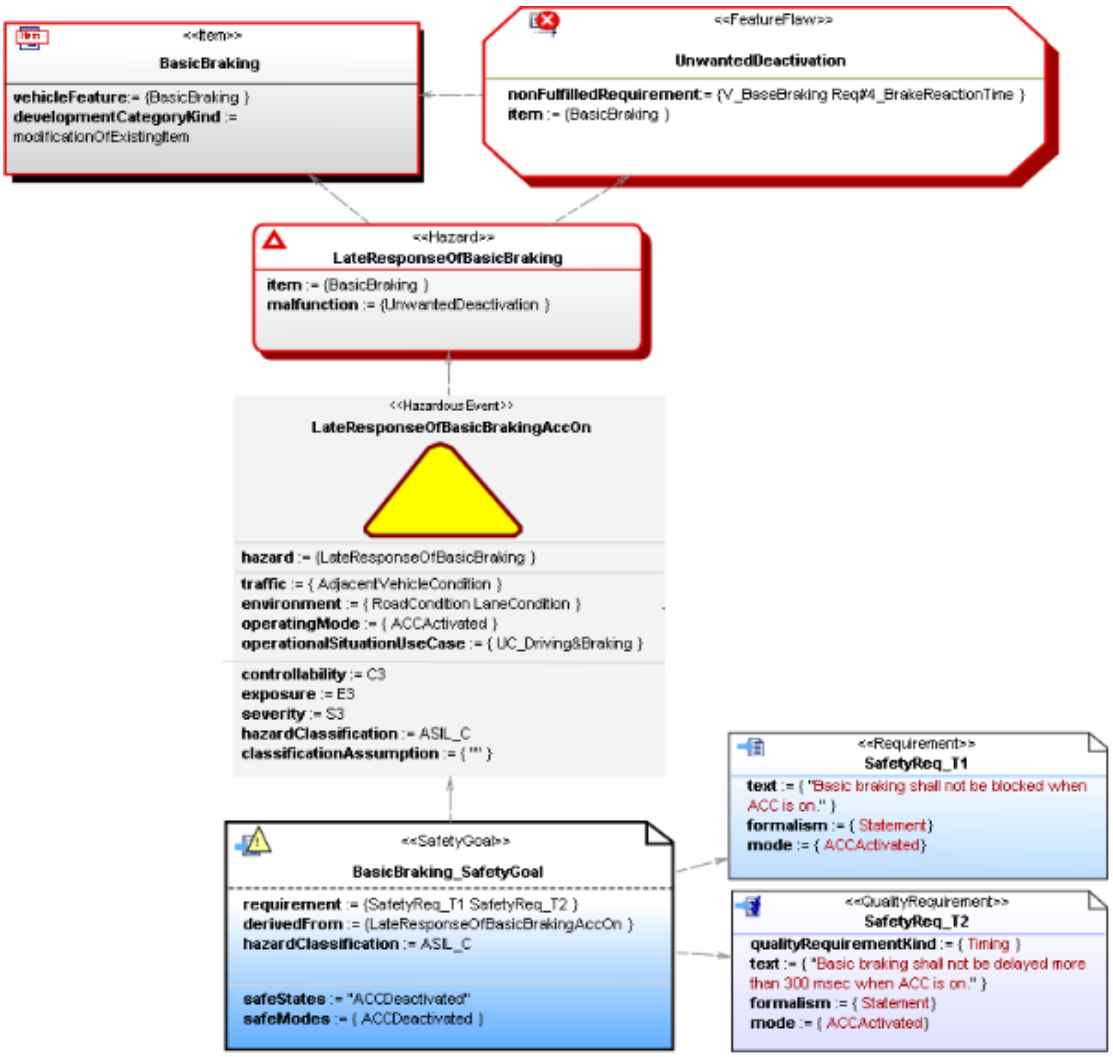


图 14. EAST-ADL 对安全要求及其对系统工件分配的支持的概述

随着安全要求的规范，EAST-ADL 允许系统功能的形式化和各种抽象层次的安全分析操作情况。

图 14 显示了 PHA（初步危害分析）建模支持的一部分，其重点是危害识别和风险评估，从而确定安全目标。根据 ISO / DIS 26262，一个项目是指在功能安全方面特别关注的功能，组件或系统。使用 EAST-ADL，通过检查代表目标系统项目的系统功能的潜在故障，在车辆级执行 PHA。为了塑造顶级安全要求，每个危险定义都捕获潜在的危险物品行为以及在特定操作情况下发生的这些物品行为触发的相关危险事件。



北京怡然瑞丰科技有限公司 张劲松
E-mail：theseus.zhang@yeerichtek.com Tel：13391680017

图 15.通过初步安全分析（PHA）得出制动功能的危险事件和安全目标

为了促进安全工程任务，EAST-ADL 工具可以从名义功能架构模型中创建初始误差模型。图 15 显示了 MetaEdit +工具，如何从与再生破坏相关的功能设计产生相应的可靠性和错误模型。这些自动生成的误差模型可以为支持安全分析和识别架构设计变化的标称架构提供跟踪。

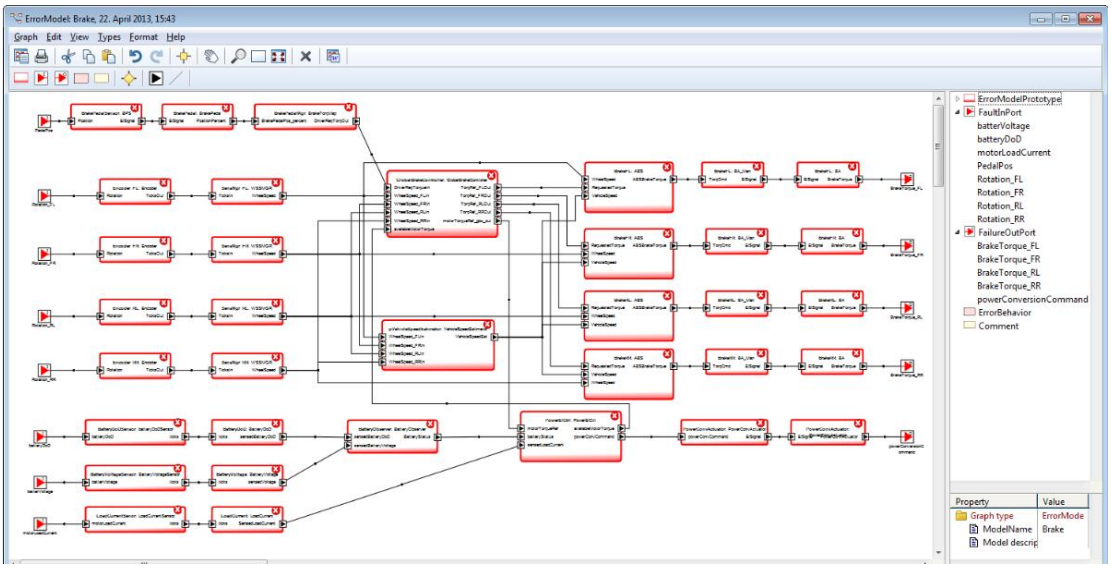


图 16.再生破坏功能设计中自动生成的误差函数

映射到现有的软件架构和实现

在汽车领域，AUTOSAR 通常用于定义软件架构，并使用各种行为建模工具来生成代码。EAST-ADL 为模型提供了一个本体论，将系统实现与设计分离，但不能替代与软件架构相关的工具和符号。实现级别的软件组件，可运行和框架是设计级别的功能和连接器的实现。描述实施的模型可以根据 EAST-ADL 提供的车辆的整体视图进行规划和管理。也可以基于设计级别模型来合成实现元素。考虑图 16 中的再生破坏的示例：建模工具提供了选择哪些功能是基于 AUTOSAR 的实现中排除的选项。这里本地设备管理器 BrakeRR 被标记为不基于 AUTOSAR，排除项也在图中显示。这种建模功能很重要，因为在实践中不同的平台需要一起生活。可以通过提供更详细的选项来提供对 AUTOSAR 和其他平台的映射，以及如何制作映射到软件架构以及报告关于成功创建平台的任何缺失信息。

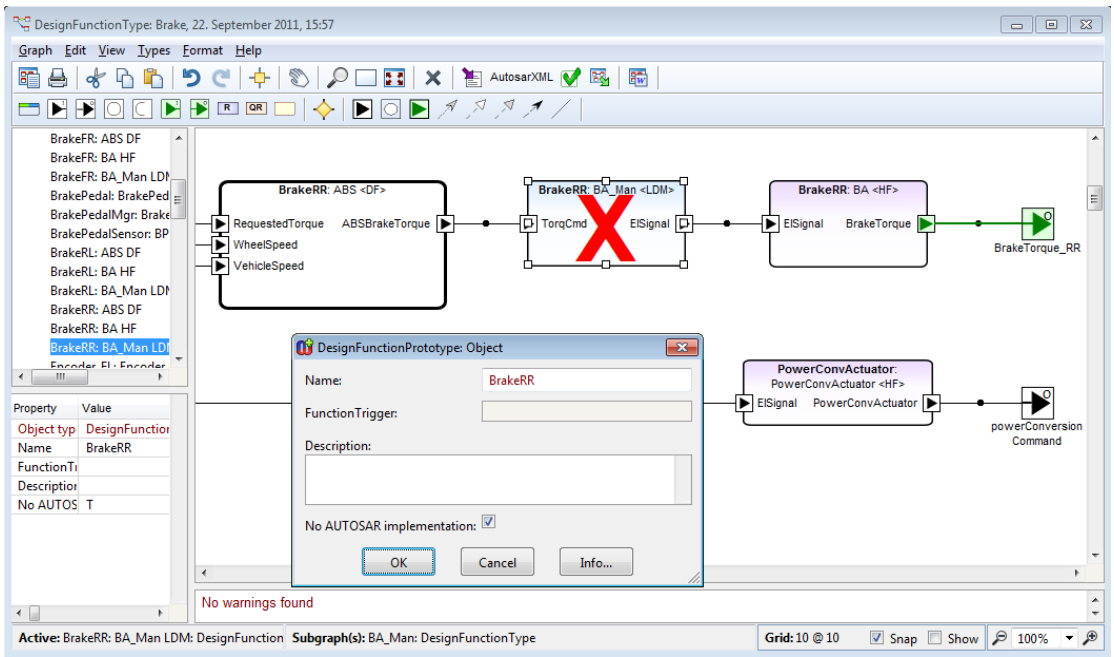


图 17. 从 MetaEdit +中的 EAST-ADL 模型中选择要映射到 AUTOSAR 的功能

概要

从 V 模型看，EAST-ADL 用于组织工程信息，并提供从早期到实施的要素之间的关系。它是针对需求和变体，功能，功能架构和硬件架构的综合信息模型。时序，可靠性和其他非功能注释可满足完整的多方面建模和分析。由于支持早期阶段模型，因此可以在抽象解决方案中进行验证和验证。我们演示了使用 SPIN 进行行为分析以及生成 AUTOSAR 模型。类似的其他集成链接从 MetaEdit +实现，从 EAST-ADL 到 UPPAAL，Matlab / Simulink 和 Modelica。

EAST-ADL 提供了在行业中使用通用本体和交换格式的机会。它与 AUTOSAR 和 COTS 工具对齐，用于行为建模。该语言是模块化和可扩展的，用于新的建模需求。使用通用语言，工具，方法和协作实践的进展将更加有效。现在的挑战是形成一个关键的群体，其中有足够的工具集可用，允许足够的用户组来应用 EAST-ADL。我们已经看到它发生在 AUTOSAR 工具和平台上。通过 ISO26262，新的传动系统技术，嵌入式系统的复杂性日益增加，开发早期阶段需要采用同样的协作方式，以及解决需求，可靠性和其他非功能方面。