交控科技
TRAFFIC CONTROL TECHNOLOGY

Shift2Rail项目调研汇报

主讲人：
王霞
西南交通大学 博士在读
系统可信性验证国家地方联合实验室
研究方向：形式化方法、模型检测

2021年8月25日

IP2 Innovation Programme

”Shift2Rail计划”是2014年启动的欧盟史上第一个大型铁路科研创新项目，它的目标为通过加速新技术和先进技术的集成，创新先进的铁路产品，出台以市场为驱动的铁路产品解决方案。

Shift2Rail的**核心目标**为：

■降低铁路运输生命周期成本到50%;

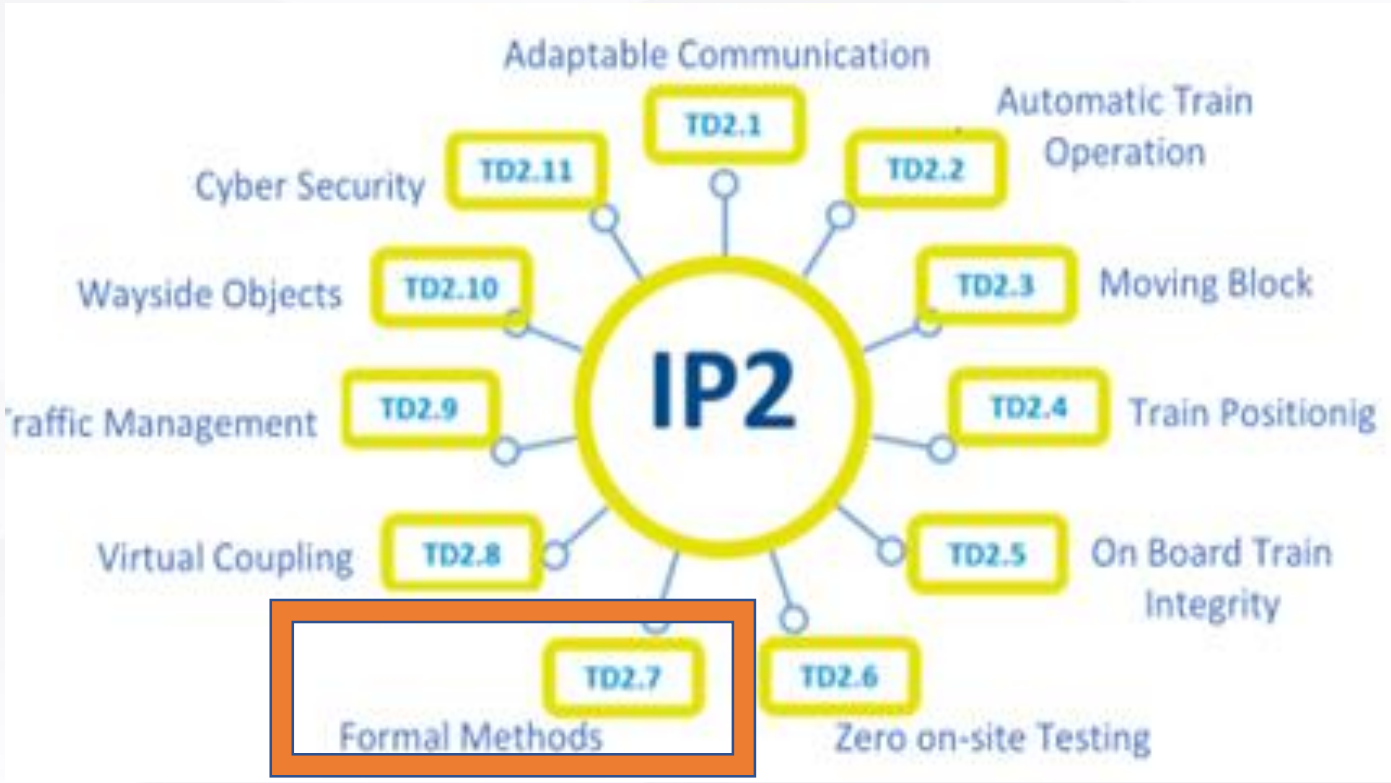
■加倍铁路运力;

■准时性和可靠性尽可能增加50%。

IP2 Innovation Programme

IP2-先进交通管理和控制系统:

致力于先进运输管理与控制系统的创新研究，旨在超越主线铁路ERTMS应用，以期将新的信号和交通管理系统扩展到所有运输部分（市郊、覆盖系统、高速、货运等），共由11个示范技术组成。



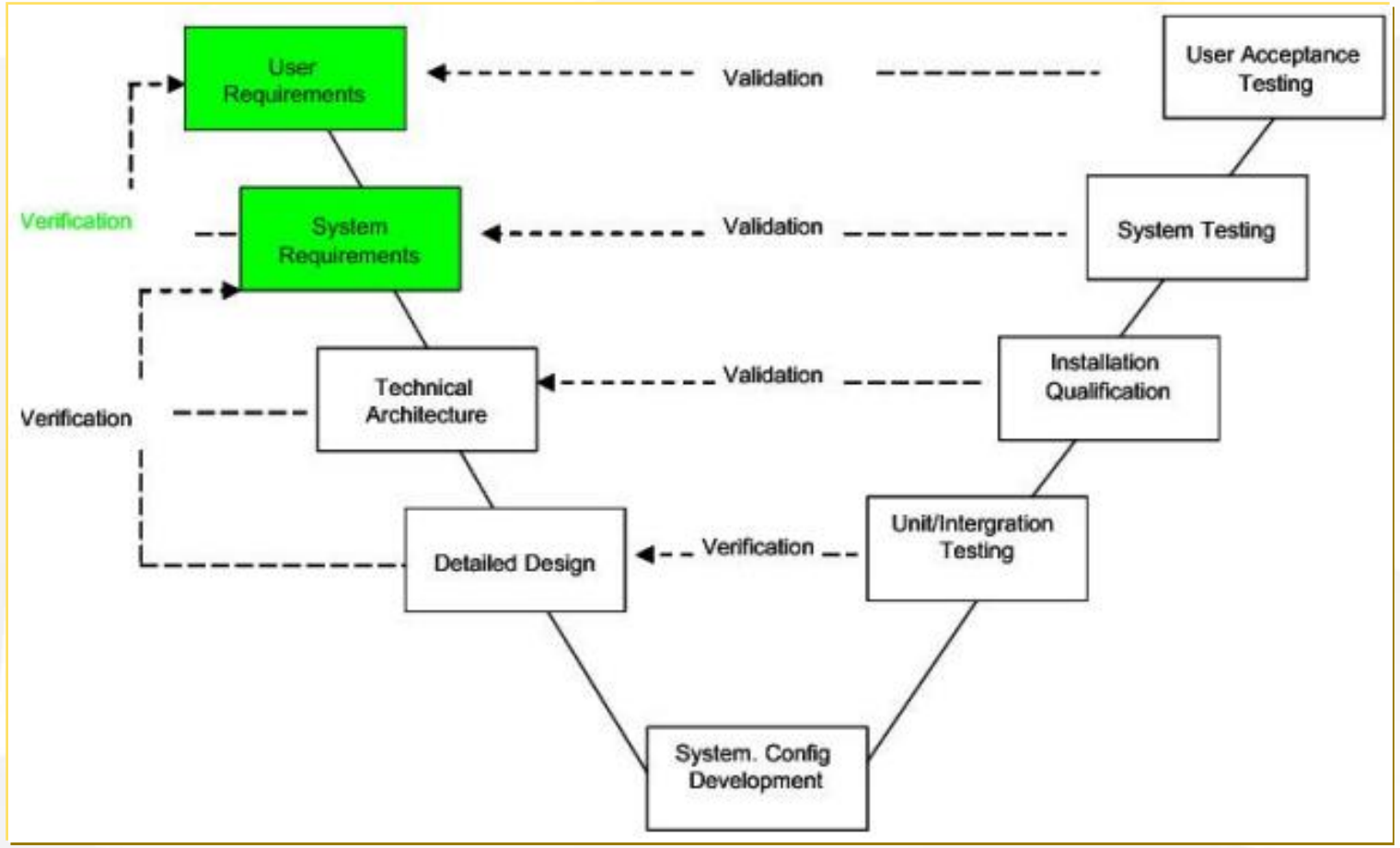
目录

子目录

1.1 形式化方法的引入

对于软件系统的检测手段目前主要有软件分析和软件测试

测试阶段能够发现系统大部份的缺陷，但仍远远不够…



以需求阶段为例

统计指出：软件项目*40%-60%*的祸根都是在**需求阶段**埋下的，需求分析错误引起的成本消耗占预算的*25%-40%*。

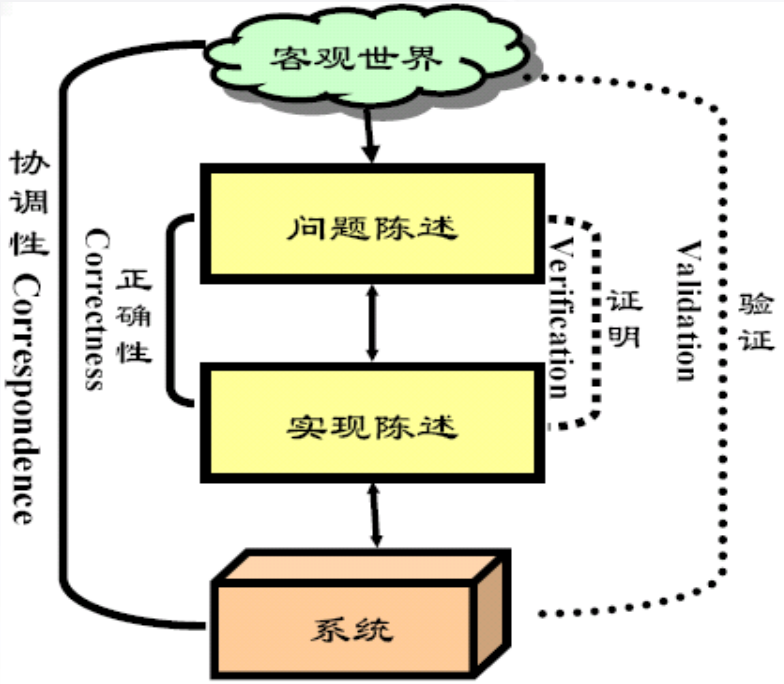
将问题放到后续开发中来修正，比起在需求阶段就立即改正需要多付出*68-200*倍的精力。

形式化方法被引入到了软件开发的各个过程中。

1.1 形式化方法的引入

形式化方法的标准定义是使用数学上严格的技术和工具来对软硬件系统进行规范、设计和验证。其数学理论基础包括数理逻辑、离散数学、集合论、数值分析等，主要应用于系统的需求分析阶段，对系统需求进行分析和验证。

在实践中，尤其是在代码足够复杂的场景中，形式化验证与程序测试方法的验证效果有较大的差距。2009 年，澳大利亚的科学家使用形式化方法对工业级操作系统 seL4 微内核进行了完整功能验证，分别采用了形式化验证和程序测试，结果显示，形式化方法共发现了 460 多个 Bug，而程序测试只发现了 16 个 Bug。



对于出现故障后可能导致人员伤亡、重大经济损失或环境破坏等严重后果的安全苛求系统，由于需求和设计以及最终实现的程序的一致性难以判定，在系统功能模型分析阶段中有必要使用**形式化方法**检查设计缺陷，从而进一步提高所设计产品的可靠性。

1.2 形式化方法在各领域的成功应用

航空航天

1996 年，欧洲航天局首次发射的阿丽亚娜 5 型（Ariane 5）火箭，由于惯性导航系统发送的错误指令，导致火箭在发射仅仅 37 秒后偏离了既定轨道，最终坠毁，欧洲航天局的巨额研发经费因此付之一炬。不久之后，EADS 公司在开发阿丽亚娜火箭任务调度的模型中开始使用形式化方法。美国国际宇航局 NASA 和 英国国防部在 90 年代相继发布了设计标准，其中都包含了形式化方法的使用。 我国的玉兔号月球车控制系统和我国第一个自主研发的空间飞行器嵌入式实时操作系统 SpaceOS 也是通过形式化方法来验证其正确性。

从 2000 年开始，欧盟开始研究如何将形式化方法有效的应用于航空航天系统安全性评估领域。

1.2 形式化方法在各领域的成功应用

国防

美国国防部的 HACMS 项目（High-Assurance Cyber Military Systems，高可信军事网络系统）的目标是开发高可信、黑客无法入侵的军用系统。该项目的一个成果是一个无人机控制系统，这一系统的基础是经过形式化验证的 OS 内核seL4，整个系统在该内核上用 Isabelle 形式化工具开发和验证。开发成功后，团队组织黑客攻击，攻击者知道源码，并能访问系统的一些部分，目标是攻入系统的其他部分。攻击者工作了六周没有达到目的。

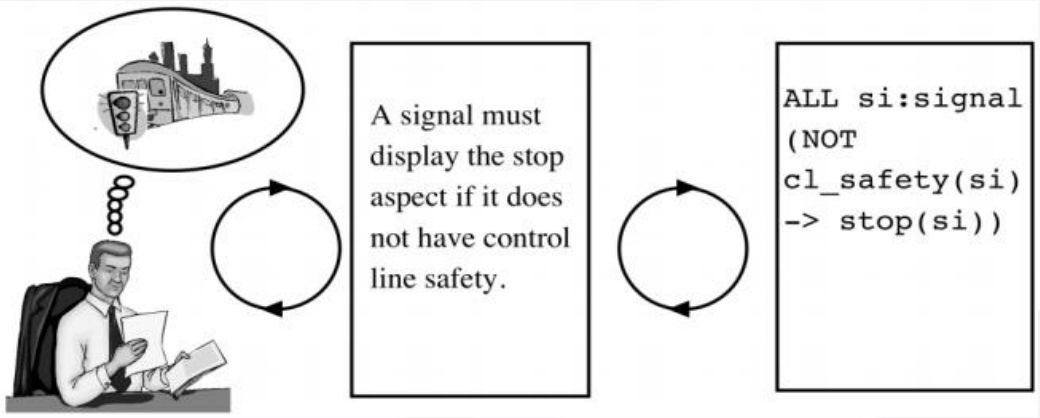
1.2 形式化方法在各领域的成功应用

轨道交通

- 在轨道交通领域，形式化方法最早在1980年被法国巴黎地铁（RATP）得到了应用，在**车载控制软件**开发中使用了**B方法**，并与单编码处理器相结合，并取得了良好效果。
- 2006年9月投用的Roissy机场各候机楼之间的**全自动无人驾驶穿梭车控制系统**也采用了**B方法**的进行形式化开发（**ClearSy and Siemens** ）
- 2012年欧盟进行**open-ETCS系统**（*European Train Control System* ）进行了形式化验证研究。 http://openetcs.org/
- 目前Alstom、Thales等公司在信号与列控产品开发过程都广泛应用了形式化的工具，并与研究机构进行新方法应用合作。如ADVANCE项目， http://www.advance-ict.eu/
- 国内的大部分轨交信号控制系统研究公司近年来均配备了SCADE软件，尝试开展了形式化方法的应用。目前在轨旁设备（**卡斯柯**）、**有轨电车车载安全系统（上海富欣）** 、**列车车载LKJ2000（株洲时代通号）**开发中尝试采用了该软件，通过英国劳氏、德国莱茵等第三方公司的认证。

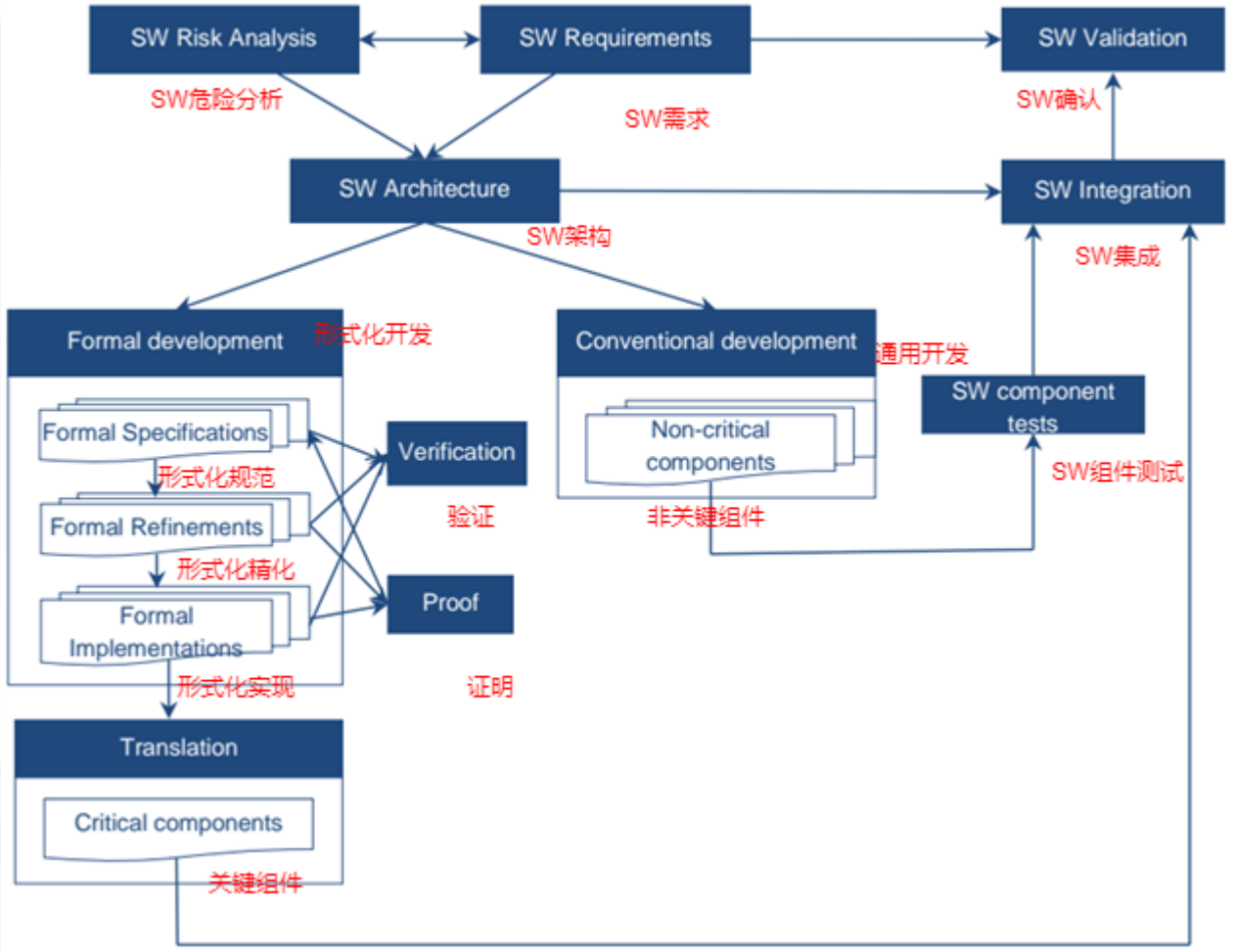
子目录

2.1 形式化规约



左图展示了一个形式化规约过程，其中领域专家制定了一个安全需求。它首先用自然语言表达(“信号必须……”)，然后使用形式化逻辑符号。在这种情况下，形式化是以谓词逻辑(一个多排序的一阶逻辑)表示的。两个谓词*cl_safety*(si)和*stop*(si)用于引用(动态)属性分别称为控制线安全和信号显示停止。谓词是形式化领域专家使用的相关词汇，必须对其进行定义，使这一需求足够具体，以便在验证中使用。ALL是一个量词，涵盖了某一类型的所有个体；在这种情况下，ALL量词用来表示该需求对所有信号都适用。

2.1 形式化建模



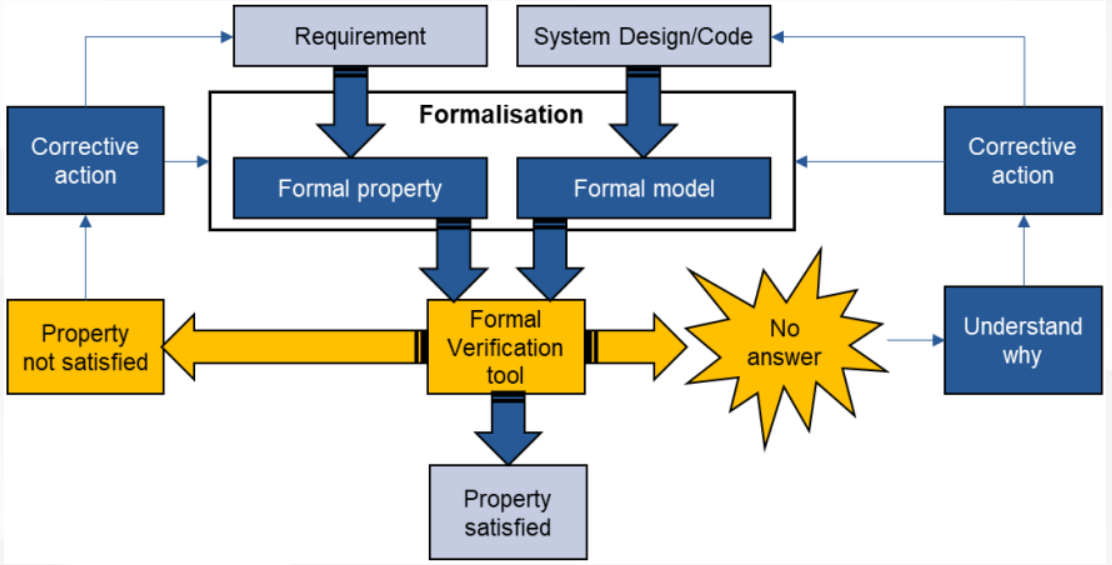
基于精化的形式化建模中，开发人员可先建立一个抽象的系统模型，再逐步对其进行精化，添加系统的各个功能。基于形式化的技术来检查在开发的每个步骤中建立的模型是否满足需求属性。

2.3 形式化验证

形式化验证可以应用于软件、硬件或其组合。在软件和硬件上的应用是最常见的，而应用到“系统的系统”的水平是罕见的(在工业中)。在本节中，我们使用了广义的“系统”一词；它可以指一个软件、一个硬件、一个子系统或系统级的设计，或者一些组合。

要形式化验证给定的属性，需要三个要素:

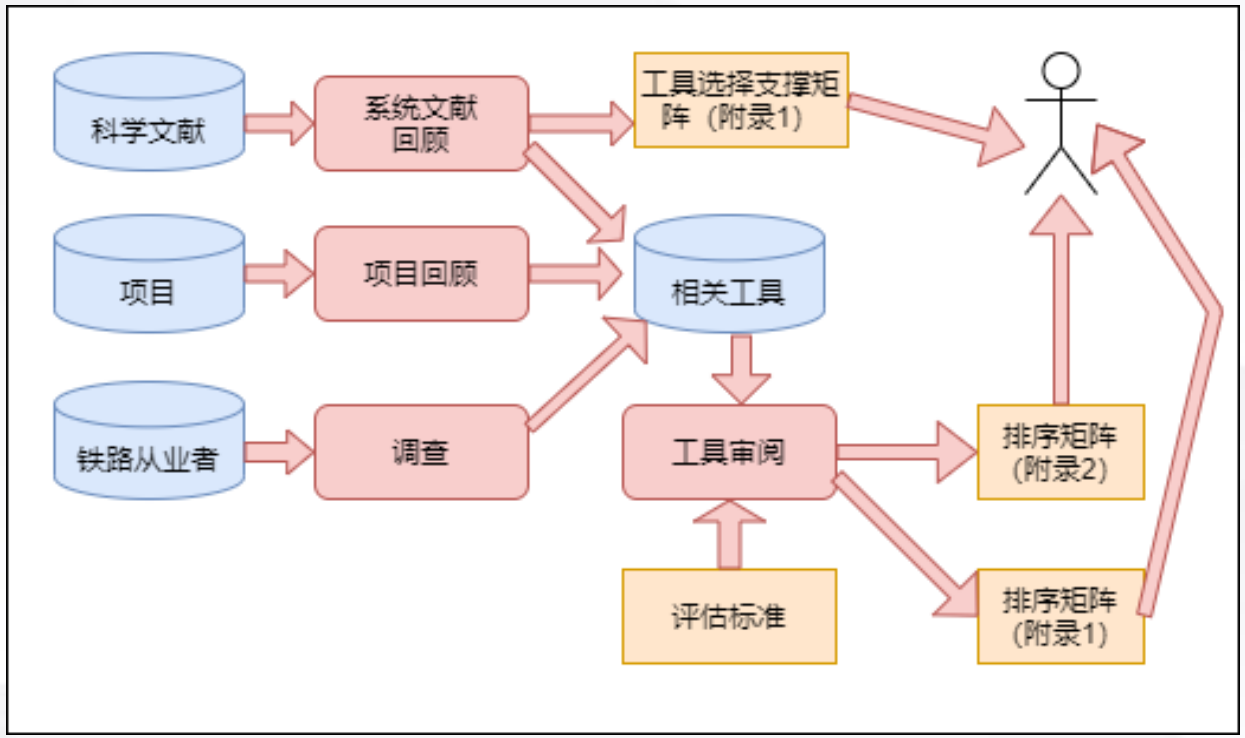
1. 正在验证的系统的形式化模型；
2. 要验证的形式化属性，通常源自系统应确保的需求；
3. 一种形式化验证工具，将形式化模型、形式化属性作为输入，并产生作为输出的答案。



子目录

3.1 铁路行业中形式化方法的应用调研

系统文献调查（SLR）、行业项目和铁路从业者的反馈。



该调研中，根据出版物中考虑的经验所涉及的系统类型和开发过程的阶段等特征，对114篇关于形式化方法和铁路的科学出版物进行了系统的文献审查。文献回顾与项目回顾和从业者调查相辅相成，以确定在铁路环境中使用的最成熟的形式化方法和工具。

3.1铁路行业中形式化方法的应用调研

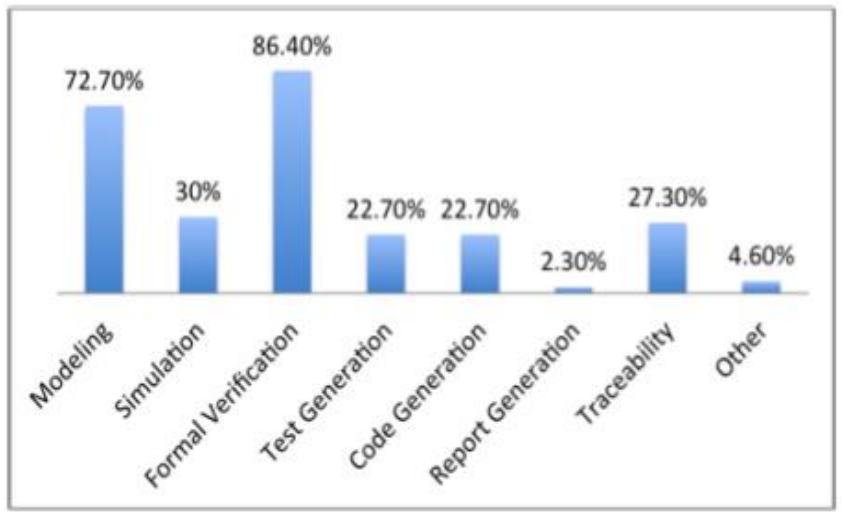
基于对过去二十年中在铁路应用中使用形式化方法和工具的项目的搜索。已经检查了每个项目的可用文档，以列出作为语言和工具使用或推荐的形式化方法。

从1998年至今的14个项目已经解决了在铁路应用中，使用形式化方法和工具的问题。下表报告了这些项目，他们根据所考虑的不同类型的铁路系统进行了划分：ERTMS/ETCS/CBTC、分布式铁路信号和联锁。

	ETMS/ETCS/CBTC
CRYSTAL	http://www.crystal-artemis.eu/
Deploy	http://www.deploy-project.eu/
DITTO	http://cs.swansea.ac.uk/dittorailway/
EuRailCheck	https://es.fbk.eu/projects/eurailcheck-era-formalization-and-validation-etcs
MBAT	http://www.mbat-artemls.eu/home/69-abstract.html
OpenCOSS	http://opencoss-project.eu
OpenETCS-ITEA2	http://openetcs.org/
PERFECT	EUROPA - Performing Enhanced Rail Formal Engineering Constraints Traceability | TRIMIS - European Commission
	Distributed railway signalling
SafeCap	http://gow.epsrc.ac.uk/NGBOVIewGrant.aspx?GranRef=EP/I010807/1
	Interlocking
ADVANCE	http://www.advance-ict.eu/
EULYNX	http://eulynx.eu/
EuroInterlocking	http://test.swissrequirementsengineering.ch/en/projects/euro-interlocking-project
INESS	http://www.iness.eu
RobustRail	http://www.robustrails.man.dtu.dk

3.1铁路行业中形式化方法的应用调研

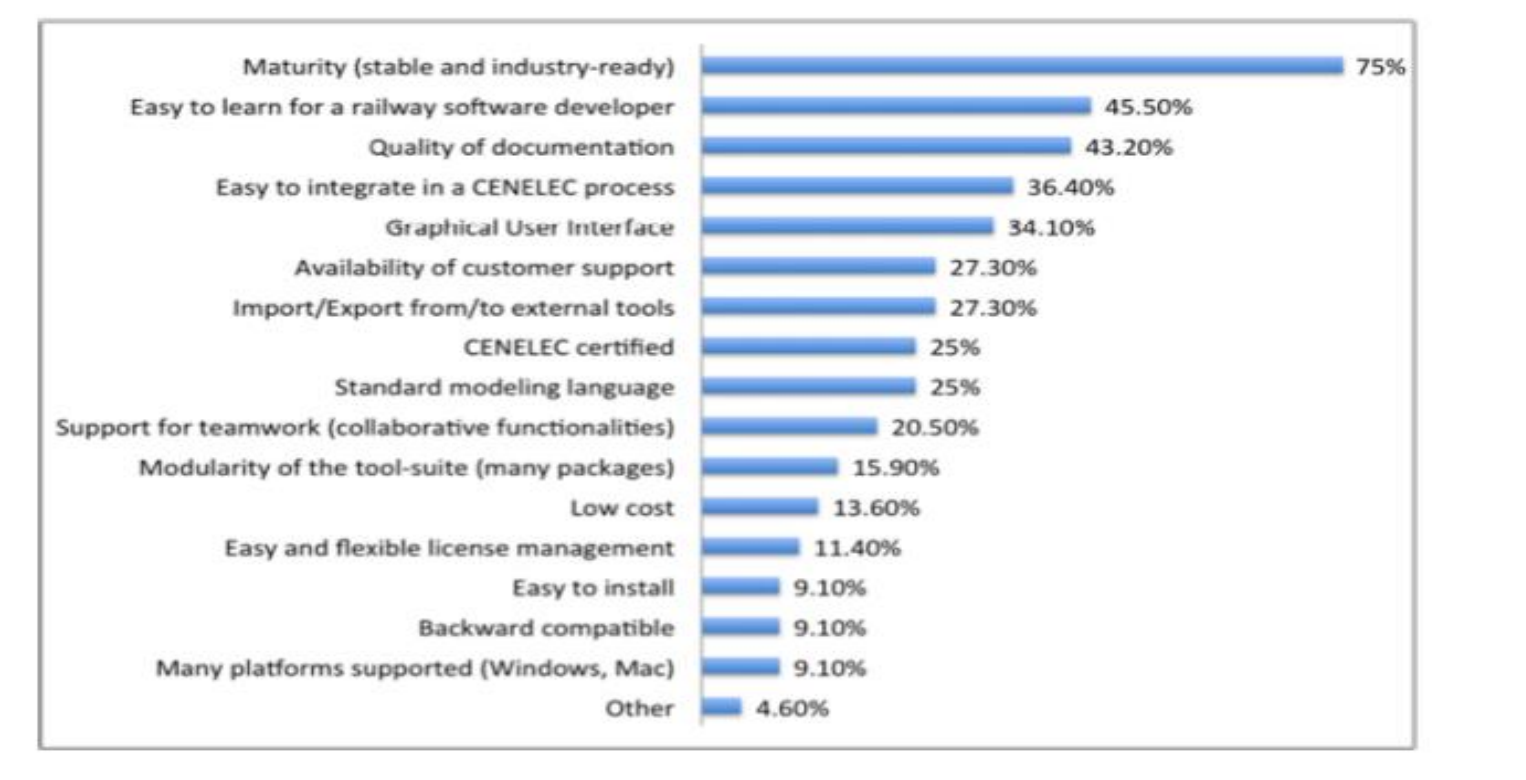
下图显示了形式化方法最相关的功能特征。大多数受访者都认为最相关的功能特征是形式化验证（86.4%的受访者），其次是建模（图形/文本）（72.7%）。形式化工具的这些传统功能特征之后是仿真（30%）和可追溯性（27.3%）。



与开发过程的后期活动相关的功能特性，例如测试生成和代码生成，也被相当多的受访者（22.7%）认为是相关的。这些数字表明，形式化工具被视为主要在开发过程的早期阶段发挥作用，用于规范和形式化验证。这些也是形式化方法不能被任何其他方式替代的阶段—就像测试、代码开发和跟踪一样。

3.1铁路行业中形式化方法的应用调研

下图报告了最相关的质量方面，75%的受访者认为工具的成熟度（稳定性和行业准备度）是最相关的质量方面，其次是铁路软件开发人员的可学习性（45.5%）、文档质量（43.2%）和抑制集成在CENELEC过程中（36.4%）。



3.2 形式化方法支撑工具对比

●Simulink(2017b)：Simulink是一个基于模型的开发工具，允许用户以输入输出块的形式图形化地绘制系统模型图，这些图被认为是按顺序执行的。这些块可以通过包含在Simulink中的工具Stateflow以分层状态机的形式进一步精化。Simulink支持图表的图形仿真，Simulink设计验证器(Simulink中也包含的一个包)允许对图表上的属性进行形式化验证。Simulink附带了几个包，也用于模型的代码生成。

●SCADE(19.0)：SCADE是一个基于模型的开发工具，类似于Simulink，通过输入输出块的方式支持系统建模。与Simulink不同，块的执行是同步的，即在每个执行步骤中，所有的块同时执行它们的计算。像在Simulink中一样，这些块可以用分层状态机进一步精化，该工具允许用SCADE设计验证器进行仿真和形式化验证。SCADE还附带了几个包，例如SCADE Architect，它允许用高级块来建模系统架构，类似于用SysML/UML语言所能做的。

3.2 形式化方法支撑工具对比

● UPPAAL(4.1)：UPPAAL是一个集成的工具环境，用于建模、确认和验证实时系统，这些系统被建模为时间自动机网络，并通过数据类型进行扩展。它适用于可以被建模为具有有限控制结构和实值时钟的不确定过程集合的系统，通过通道或共享变量进行通信。典型的应用领域包括实时控制器和通信协议，尤其是那些定时方面至关重要的领域。该工具由Department of Information Technology at Uppsala University, Sweden and the Department of Computer Science at Aalborg University in Denmark合作开发。

● ProB(1.10.2018)：ProB是B方法的动画器、约束求解器和模型检测工具(参见Clearsy的B Method网站http://www.methodeb.com/en/)。它允许B规范的全自动动画，并可用于系统地检查一个规格的大范围错误。ProB的约束求解能力也可以用于模型死锁检查和测试用例生成。B语言植根于谓词逻辑、算术和集合论，并为数据结构(如高阶)关系、函数和序列提供支持。除了B语言之外，ProB还支持Event-B、CSPM、TLA+和Z。ProB可以安装在Rodin中，它附带了BMotionStudio，可以轻松生成特定领域的图形可视化。(参见ProB组件的概述，请参见)。商业支持由分拆公司Formal Mind (http://formalmind.com)提供。

3.2 形式化方法支撑工具对比

● Atelier B(4.2.1):由ClearSy开发，Atelier B是一个工业工具，允许在操作上使用B方法来开发无缺陷的成熟软件(形式化软件)。它用于为阿尔斯通和西门子在世界各地安装的各种地铁开发安全自动化系统，也用于通用标准认证以及ATMEL和ST微电子开发系统模型。此外，它还被用于许多其他行业，如汽车行业。Atelier B也用于航空和航天领域。

● NuSMV (2 . 6 . 0): NuSMV是SMV符号模型检测器的再实现和扩展，是第一个基于二元决策图(BDDs)的模型检测工具。该工具被设计为用于模型检测的开放架构。它旨在对工业规模的设计进行可靠的验证，用作其他验证工具的后端和形式化验证技术的研究工具。NuSMV是由ITCIRST(Istituto Trentino di Cultura in Trento, Italy)、Carnegie Mellon University, the University of Genoa and the University of Trento 联合开发的一个项目。从版本2开始，它结合了基于BDD的模型检测和基于SAT的模型检测。它的最后一个进化，叫做nuXmv，也允许无限测试系统的验证。

3.2 形式化方法支撑工具对比

● SPIN(6.4.8):SPIN(Simple Promela解释器)是一种高级且非常高效的工具，专门针对多线程软件的验证。该工具是从1980年开始在计算科学研究中心的Unix组的贝尔实验室开发的。2002年4月，该工具被授予ACM系统软件奖。系统规范支持的语言叫做Promela (PROcess MEta LAnguage)。

● UMC(4.6): UMC是一个验证框架，它是在ISTICNR的FM&&T实验室开发的，用于系统设计的定义、探索、分析和模型检测，系统设计表示为一组通信(UML)状态机。它目前的状态仍然是一个主要用于教学和研究目的的实验框架。即使没有为真正的工业软件开发做好准备，它也可以在基于UML的早期设计中消除歧义、制作动画和验证方面发挥作用。

3.2 形式化方法支撑工具对比

根据调查，总结出，

A. Simulink和SCADE适用于早期原型开发和面向代码生成的详细设计，在针对形式化验证时需要使用其他工具。

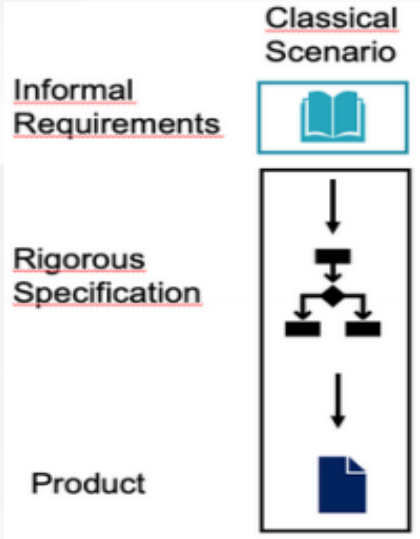
B. 当需要专注于验证定量、实时属性和概率方面时，UPPAAL是合适的。

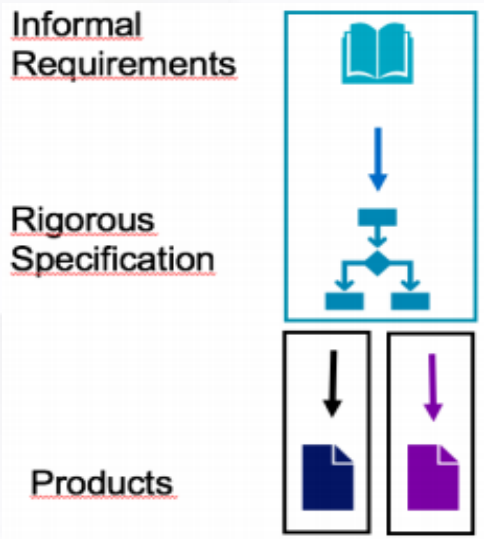
C. 当系统或系统的组成具有大的状态空间，并且需要验证时态逻辑属性时，NuSMV和SPIN是合适的。

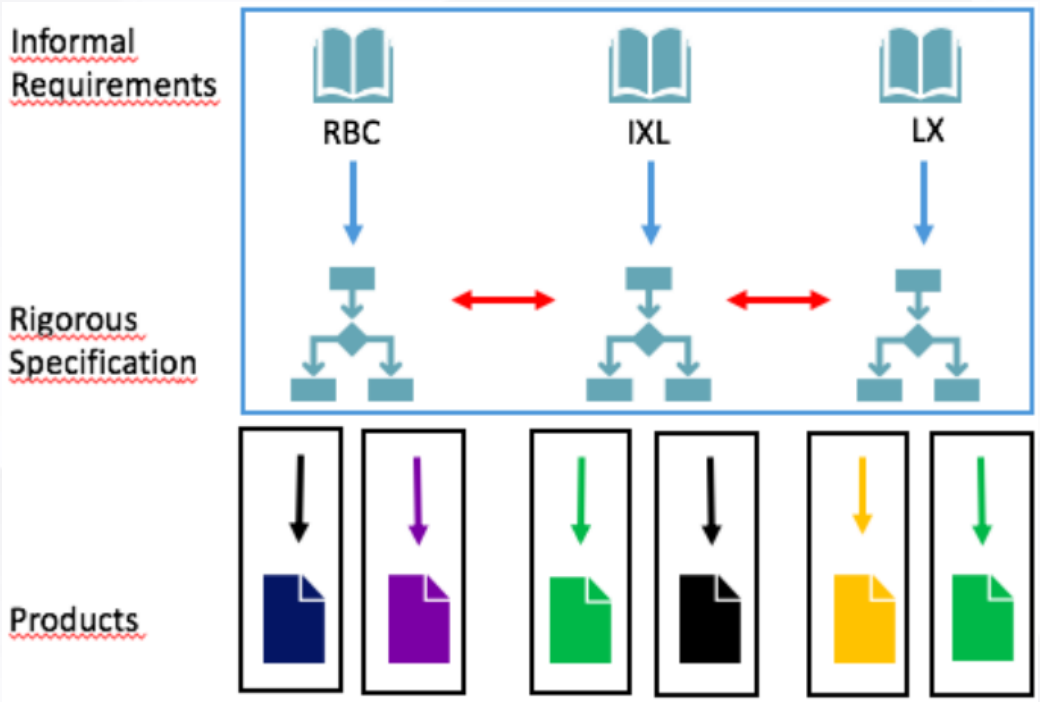
D. Atelier B和ProB是自上而下开发的正确选择(即。从最初的设计到代码)，并且具有某种程度上互补的验证能力，其中Atelier B支持不变式检查，而ProB支持模型检测。

子目录

4.1 形式化开发标准化接口设计





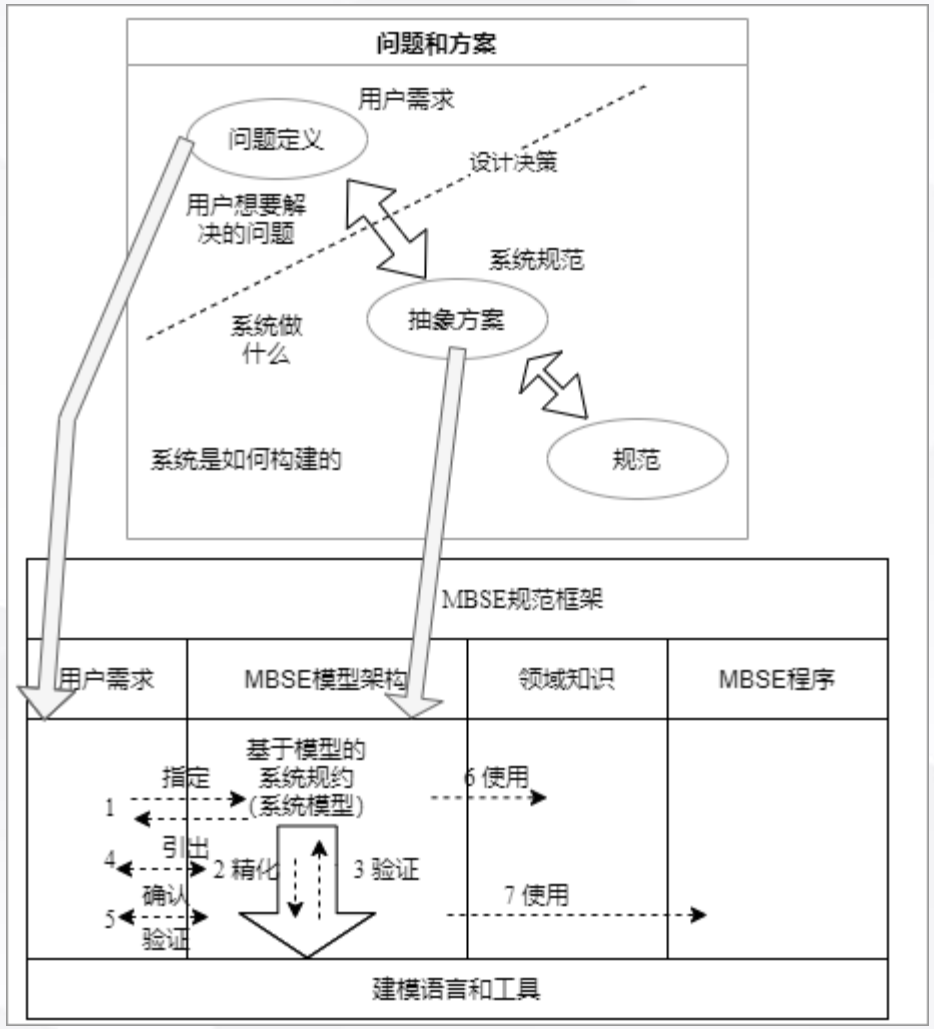


4.1 形式化开发标准化接口设计

“标准接口”旨在成为由基础设施管理者（用户）传达给开发人员的标准参考。其中标准接口包括两个方面：

首先是不同的供应商同意的不同设备之间的接口需求。标准接口由Eulynx推广和开发。 Eulynx计划旨在为信号系统定义模块化架构，包括单个组件的标准化接口。

第二个方面是需要为标准接口的规范使用标准化的符号，UML是主要的标准化建模语言，由一组集成的图形形成，旨在帮助系统和软件开发人员指定、可视化、构建和记录软件系统的产品。



4.2 MBSE架构支撑平台

ProB用于详细仿真、分析和验证

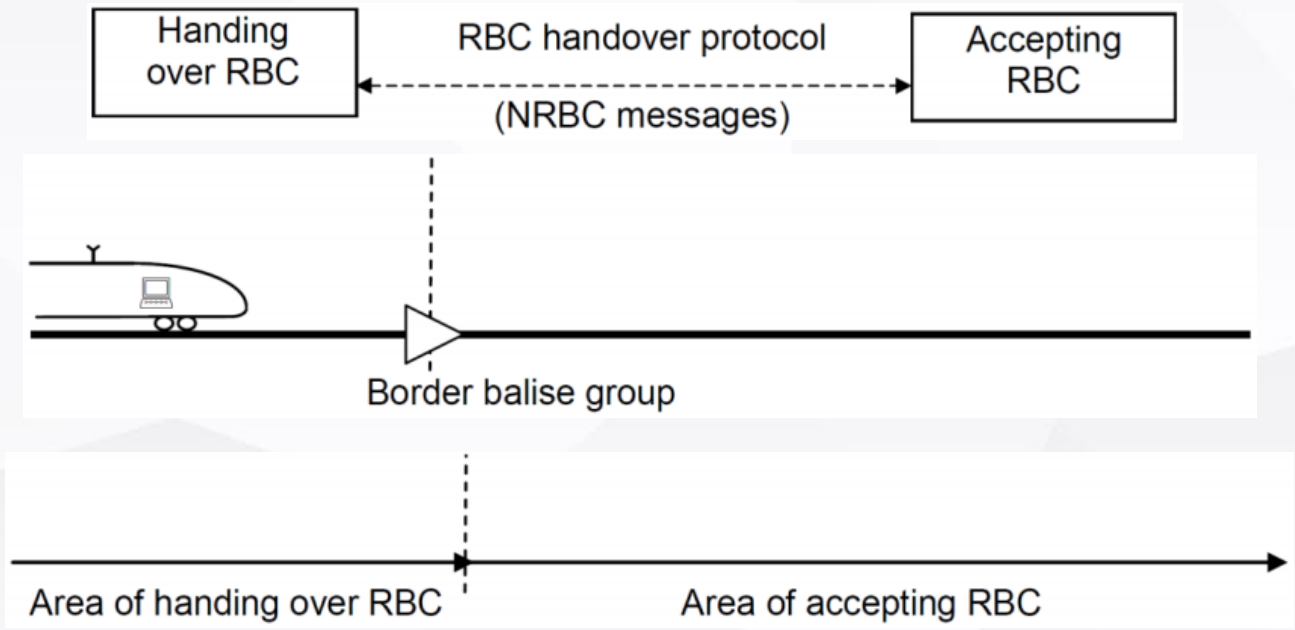
关于ProB在4SECURail项目中的计划使用，这个框架受到一些限制，因为它是围绕一个特定的规范符号(Event-B)产生和发展的。特别是:

- 它不允许对多个相互作用的状态机进行显式建模。
- Event-B状态机不同于UML/SysML状态机。在目前的技术水平下，已经提出了多种从UML到ProB状态机的转换建议，但是目前还没有工业上可用的产品支持这种映射。
- 当系统由许多相互作用的异步状态机组成时，模型检查不太可能扩展。

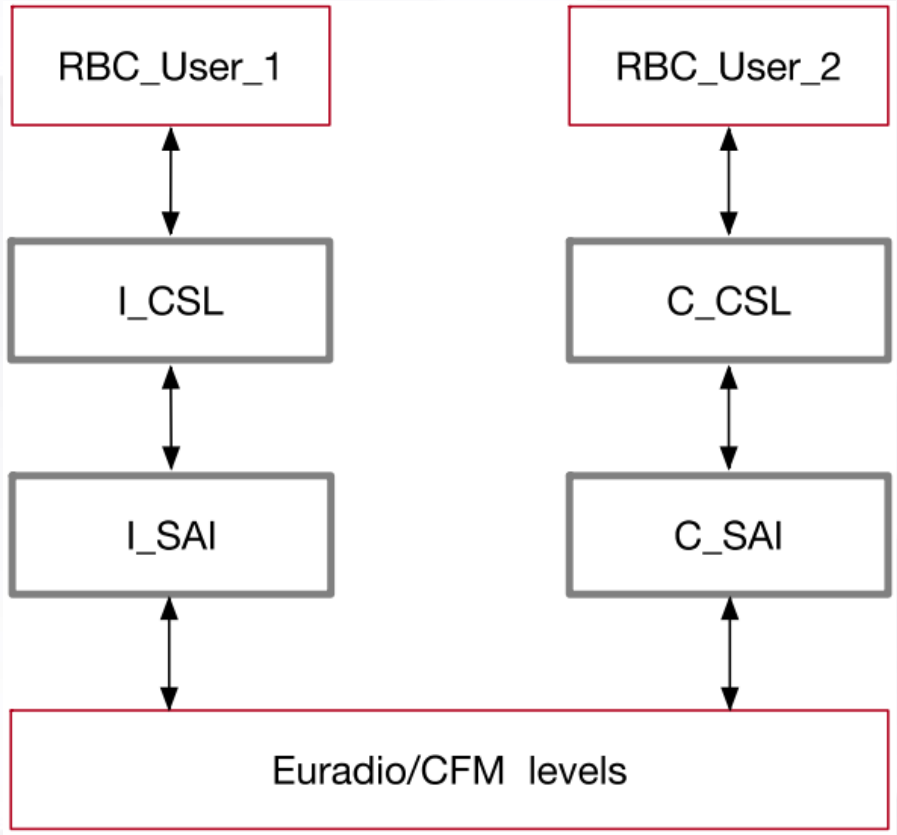
UML设计的ProB编码可以直接从系统的文本UMC表示中获得，并且两个规范符号的一致性可以被形式化地验证。ProB会在出现错误时提供反馈，或者使用执行跟踪来解释属性。为了提供这种反馈的图形表示，提供了一个用于根据序列图描述这些执行轨迹的简单工具。

4.3 RBC/RBC接口案例研究原理

4SECURail提出的形式化方法演示器的案例研究是4SECURail切换协议，该协议由UNISIG指定到SUBSET039 FIS中用于RBC/RBC切换和SUBSET-098 RBC/RBC安全通信接口。需要一个切换程序来管理两个相邻RBC之间的列车控制监督的交换。当列车接近移交RBC监管区域的末端时，与(新的)接受RBC进行信息交换以管理责任交接，如图所示。



4.3 RBC/RBC接口案例研究原理

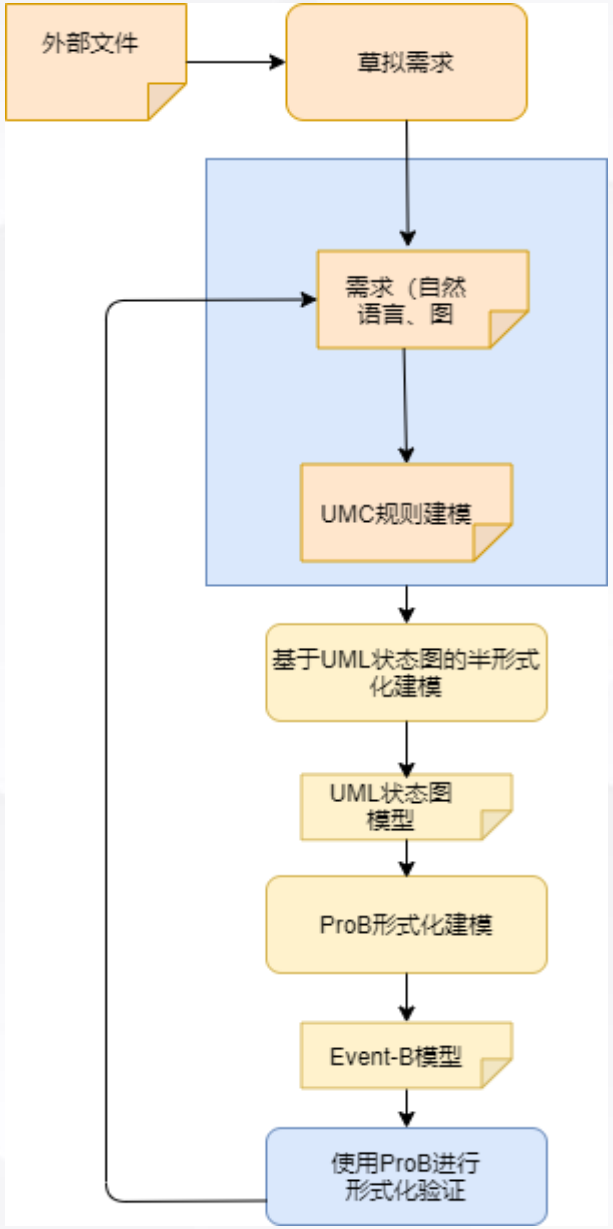


在CSL（通信监督）之上，RBC用户层包括了所有应用功能(例如，行车许可的评估、与机载设备的通信、RBC-RBC移交事务的实际管理)以及生成/接收通信信息，而协议层则专门用于格式化和与通信伙伴交换此类信息。案例研究的要求中不包括对RBC_User功能的说明。此外，低于SAI(SUBSET-098的欧洲无线电和通信功能模块)的较低级别也不属于案例研究的要求。

因此，演示器将应用于CSL和SAI级别，而RBC_User、ER和通用CFM被视为外部环境。左图显示了系统的整体结构。请注意，在通信的两侧，一侧被配置为安全连接的“发起方”，而另一侧被配置为“被呼叫方”。

4.3 RBC/RBC接口案例研究原理

整个基于标准接口的形式化开发过程可以参见右图。

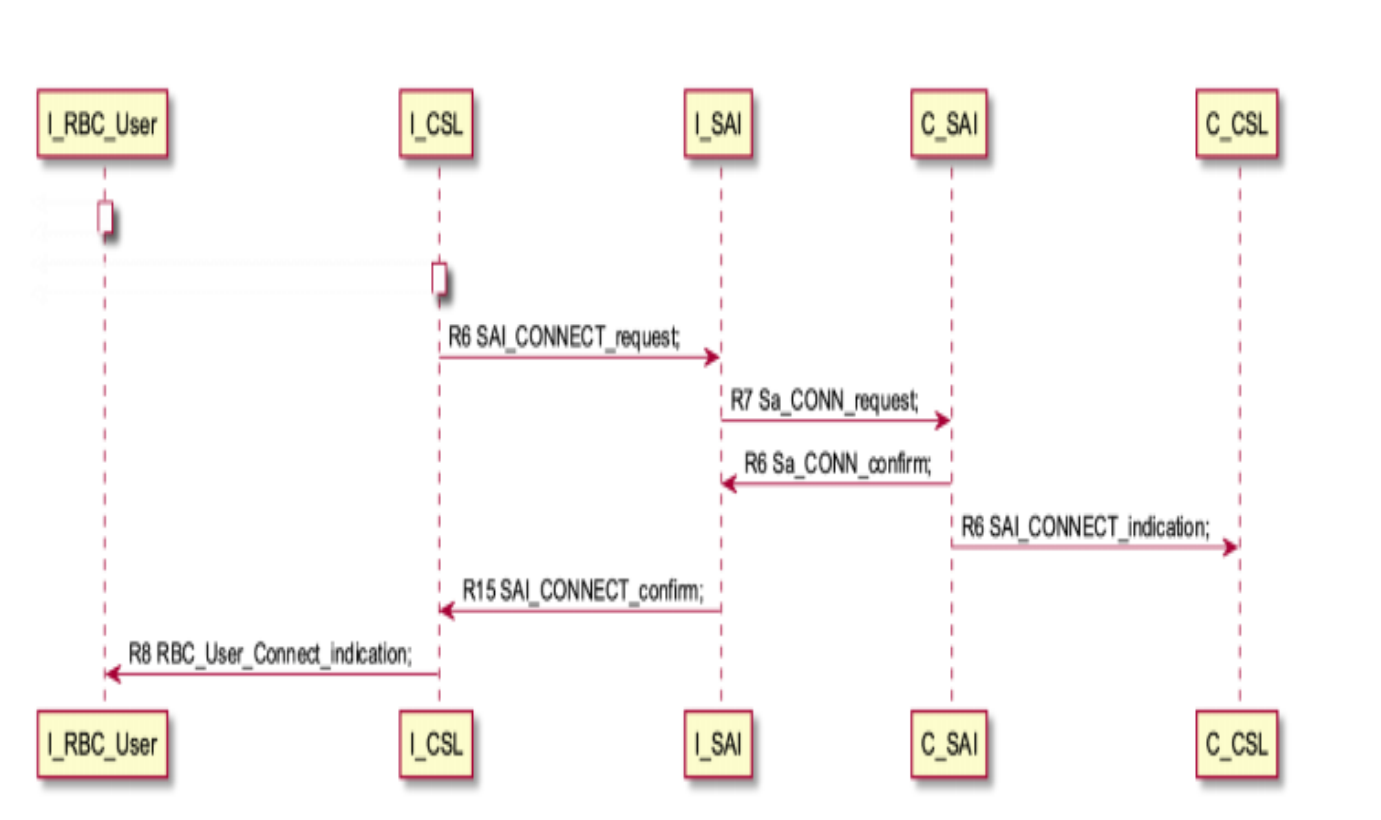


4.3 RBC/RBC接口案例研究原理

```
-- when connecting handle connection confirmation
--
R8_ICSL_IRBC_rbcuserconnectindication:
  NOCOMMS -> COMMS
     { SAI_CONNECT_confirm   /
         RBC_User.RBC_User_Connect_indication;
         connect_timer := max_connect_timer;
         receive_timer := 0;
         send_timer := 0; }
```

UMC规则例子

我们可以要求解释上图所示的转换是何时触发的（即，当信号*SAI_CONNECT_confirm*导致发送*RBC_User_connect_indication*时），答案可以用序列图来观察，如右图所示(图形布局是由UMC使用PlantUML在线服务自动生成的)。



UMC生成的序列图

4.3 RBC/RBC接口案例研究原理

UMC状态机设计的每个转换规则定义都映射到Event-B的等效操作上

UMC transition

```
R8_ICSL_IRBC_rbcuserconnectindication:
NOCOMMS -> COMMS
 { SAI_CONNECT_confirm /
   RBC_User.RBC_User_Connect_indication;
   connect_timer := max_connect_timer;
   receive_timer := 0;
   send_timer := 0; }
```

Event-B Operation

```
R8_ICSL_IRBC_rbcuserconnectindication =
 PRE
   ICSL_STATUS = NOCOMMS &
   icsl_buff /= [] &
    first(icsl_buff) =  SAI_CONNECT_confirm
THEN
  ICSL_STATUS := COMMS;
  irbc_buff := irbc_buff <- RBC_User_Connect_indication;
  icsl_connect_timer := icsl_max_connect_timer;
  icsl_receive_timer := 0;
  icsl_send_timer := 0;
  icsl_buff := tail(icsl_buff)
END;
```

4.3 RBC/RBC接口案例研究原理

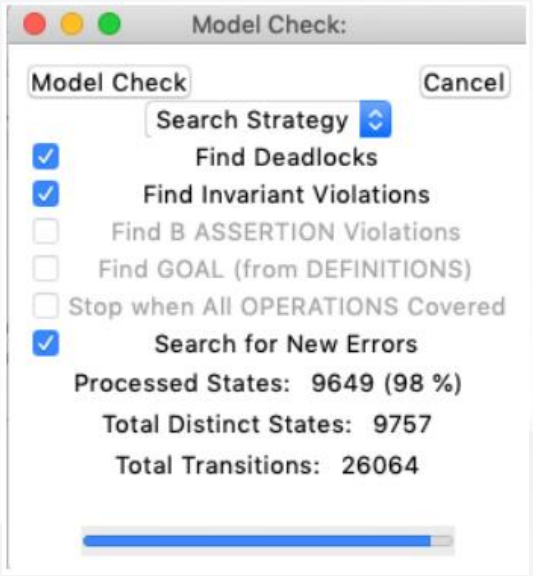
➢ 需求属性列举

REQ_001	如果被配置为发起方，当被开启时(在NOCOMMS状态下的通信)，CSL负责向底层发送命令以建立与相邻RBC的安全连接，并在安全连接被认为丢失时(在NOCOMMS状态下的通信)命令重新建立。
REQ_012	如果配置为启动器，在启动时，当检测到安全连接丢失时，CSL应向SFM发送安全连接初始化命令(SAI_CONNECT.request)。
REQ_002	发送建立连接的命令后，发起方应启动计时器。如果定时器在连接建立之前到期，将生成新的连接请求。
REQ_006	安全连接的丢失应由底层SFM的CSL读数报告检测。
REQ_007	如果从底层收到安全连接丢失的报告，CSL应考虑在NOCOMMS中进行通信。

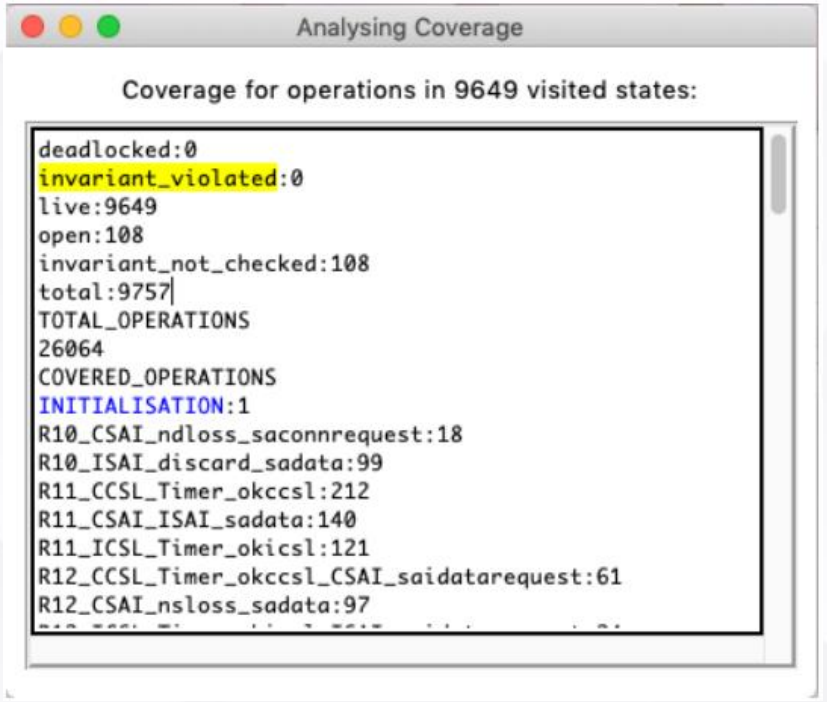
4.3 RBC/RBC接口案例研究原理

形式化验证示例

每个场景中每个UML转换的Event-B模型(即，是否将执行转换)可以通过模型检测来明确检查。



系统模型检测的ProB默认界面



验证后可以分析的覆盖率报告

子目录

5.1 形式化方法的长短期效益

	短期效益	长期效益
减少或补充昂贵的测试和安全审查阶段	关键系统属性的遍历验证	替换效率较低的方法
通过发现或避免早期错误而减少成本	需求“为了”更高程度的洞察力	由于发现的错误更少而降低了成本
更改的自动验证使检测问题更容易	减少短期维护成本	减少长期维护成本
以计算机可读格式记录的关键系统需求	建立清楚的需求（而不是人类思维的形式）	帮助减少长期维护成本

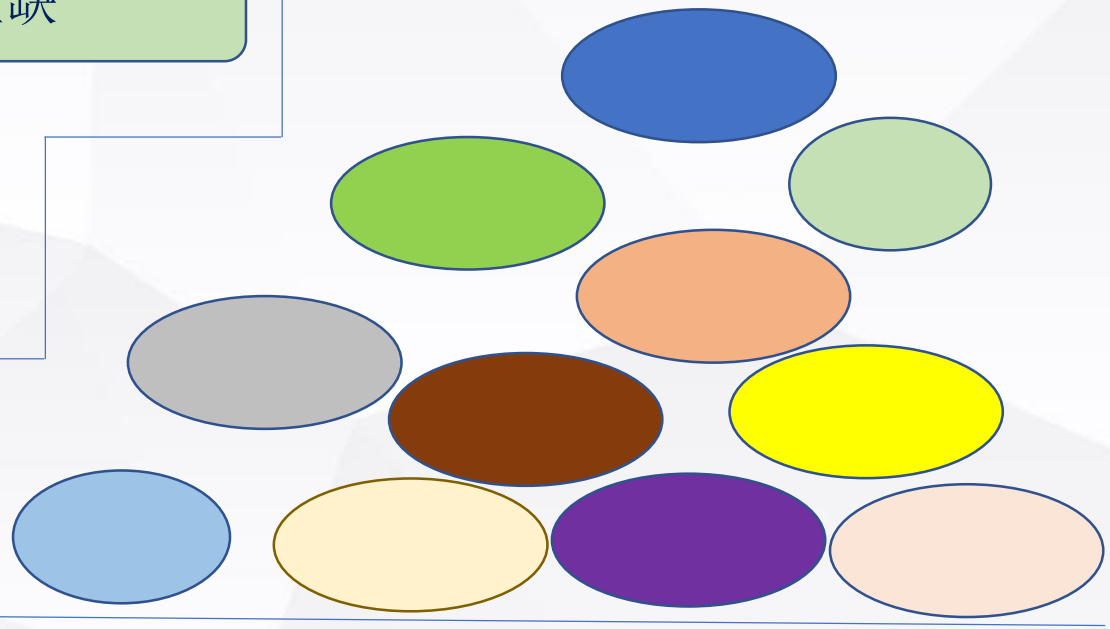
5.1 面临的挑战

缺乏一套成熟的应用体系

专业人员的短缺

模型检测的状态空间爆炸问题

前期成本高，一般只有在高安全苛求的领域得以应用



交控科技 TRAFFIC CONTROL TECHNOLOGY

谢谢大家！

交控科技

2021年8月25日