第三期 S2R 调研报告

--关于形式化方法在轨道交通行业的发展趋势调研

1. 引言

在科技发展中，存在许多对系统安全性和可信性要求很高的系统，如核发电站控制系统、航空领域、轨道交通领域的各类控制系统。这些系统结构庞大、设计十分复杂，且随着社会的发展，各种科技不断进步，这类控制系统的规模不断扩张。系统规模的持续扩张不断增加了系统缺陷存在的可能性，一旦这些缺陷被触发，严重时甚至会造成难以估量的重大经济损失以及人员伤亡。

保证系统的安全性和可信性比较主流的方法有仿真、测试和形式化方法。相对于形式化方法而言，仿真和测试可以直观的看到执行结果，且前期开发成本较低，但是只能证明有错误，发现问题的能力有限，不能达到完备。因此，人们开始关注形式化方法在安全苛求系统研究中的优势。

形式化方法是一种基于数学的特殊技术，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。一般来说，使用形式化方法开发的整个过程主要包含了形式化规约、形式化建模和形式化验证。如图 1 所示。

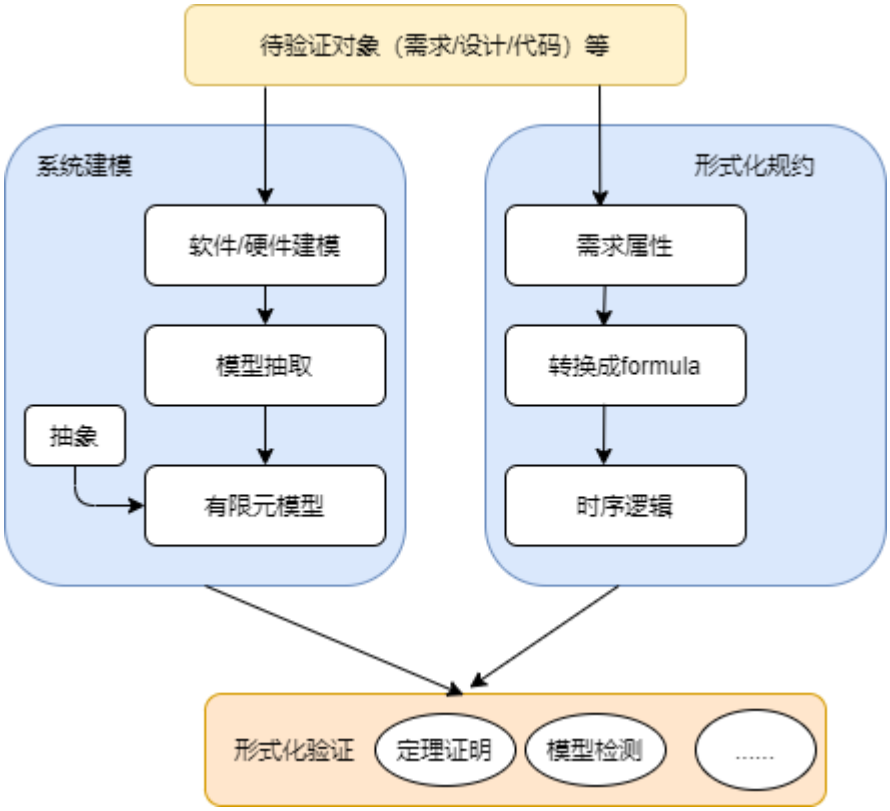

图 1 形式化开发流程

形式化规约是由形式化规约语言严格描述的系统模型或者系统需要满足的性质（属性）。形式化建模是以数学理论为基础在某一个或者某些层次上对系统进行抽象，模拟系统行为的过程。形式化验证，即建模后引入相应的理论和方法对模型的形式化规约属性进行分析或验证。最常用的验证方法是演绎式的定理证明和算法式的模型检测。基于定理证明的形式化验证将“系统满足其规约”这一论断作为逻辑命题，通过一组推理规则，以演绎推理方式对该命题开展证明。另一种方法是模型检测，相对于测试，模型检测遍历地验证了所有可能的行为，特别是在属性没有满足的情况下提供了反例。

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。更吸引人注意的是，在以高验证成本著称的形式化验证领域，完全验证 seL4 微内核只需要 600 万美元的验证成本，而以测试的方式通过 CC EAL6 级认证的成本竟高达 8700 万美元。

形式化方法的发展已有较长的历史，对于轨道交通、航空航天、人工智能等安全苛求系统而言，如何利用形式化方法保证系统功能的安全可信一直受到国内外相关学者的关注。

2. 形式化方法在安全苛求领域的研究现状

将形式化方法用于开发安全苛求型和任务关键型产品，已经在工业界进行了大量的试验。使用形式化方法的著名工业案例是 Maeslant Kering Storm Surge Barrier 控制系统，其中使用了 Z 和 Promela 形式化符号，以及巴黎地铁车载设备，其中采用了 B 方法。计算机硬件巨头企业如 NVIDIA, IBU, AMD 和 CADENCE 等也都是形式化方法的使用者。这里具体介绍形式化方法在轨道交通、航空航天以及国防系统中的成功应用。

2.1 轨道交通

由于形式化方法自证是正确的，因此非常适合应用于安全苛求的轨道交通系统的各种研发活动,也被业界视为最具有潜力和应用前景的可信构建方法。

在轨道交通领域，很多与安全相关的系统功能需求或者是具有高安全要求场景的国际标准，都需要采用形式化方法描述其系统规范及验证系统的某些功能属性。如 IEC61508 中提出，在系统的安全完整性等级为 SIL4 级的时候，强烈推荐利用形式化证明方法对系统进行验证。EN50128 标准明确表示强烈推荐在信号系统设计与验证的过程中使用形式化方法与技术。表 1 显示了 EN50128 对各类软件确认方法的建议。

表 1 EN50128 软件确认方法建议

技术方法	SIL1	SIL2	SIL3	SIL4
有限状态自动机	强力推荐	强力推荐	强力推荐	强力推荐
时间 Petri 网	强力推荐	强力推荐	强力推荐	强力推荐
形式化方法	推荐	推荐	强力推荐	强力推荐
数据流图	推荐	推荐	推荐	推荐
性能建模	推荐	推荐	强力推荐	强力推荐
原型/激励	推荐	推荐	推荐	推荐

结构图	推荐	推荐	推荐	推荐

近年来，不少领域专家专注于形式化方法在轨道交通行业的应用，如Eugcnio[6]等建立了联锁系统继电器逻辑控制模型，用布尔逻辑抽象出系统需求，用定理证明推演联锁系统中复杂逻辑转换的正确性，把复杂逻辑关系转变成了较为简单的数学逻辑问题。Thierry Lecomte[7]等提出了基于 B 方法的安全苛求系统开发，目的在于寻求在故障模式中仍然保证系统可以正确的实现的功能。通过法国铁道系统的实例，将建模与验证在系统设计的初期阶段实施，减小了故障发生的可能性，同时尽可能地降低了系统测试成本。Zafar[8]利用 Z 语言对联锁系统进行建模，模型描述了移动闭塞情况下的各种场景。交通领域联合研究中心，与 Freiburg, Oldenburg 和 Saarbriicken 联合，致力于复杂系统的安全性研究，尤其是对交通运输复杂系统的分析与自动验证。

2.2 航空航天

航空航天系统中控制软件的规模和复杂性正在迅速增加，这种发展使其在整个航天器系统范围内的验证复杂化，采用基于模型的安全性分析对航空航天系统进行系统层级的建模和分析受到了航空界的广泛关注和推广。

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，先后进行了 ESACS(Enhanced Safety Assessment for Complex System)、ISSAC(Improvement of Safety Activities on Acronautical Complex Systems)和 MISSA(More Integrated Systems Safety Assessment)等较大的三个规模的研究项目。该系列研究应用基于模型检验方法完成了对 A320 液压系统、A340 高升力系统的控制模块、Airbus 系列飞机起落架系统的前轮转弯模块等案例研究。

由 ESA 资助的 COMPASS 将形式化方法应用在航空系统中，采用最先进的时态逻辑模型检查技术来实现无线状态转换系统。Bozzano 在文献中介绍了 COMPASS 项目[9]，该项目旨在提供一种集成的系统和软件协同工程方法，通过使用统一的规范和分析方法，来评估基于航空航天的记载计算机的系统级正确性、安全性和可信性。

国内也有不少研究者开展这类工作，如程永江[10]等使用 UPPAAL 工具对飞机着陆过程构造了模型，然后对模型的需求规范进行了验证，验证结果表明模型不存在死锁的问题，最终可以保证飞机安全和及时地着陆。Qingfan Gu[11]等针对综合化航空电子系统安全性分析存在的失效模式和动态时效问题，研究了基于模型驱动航空电子系统安全性的分析技术。

2.3 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。

3. 轨道交通中形式化方法的应用（Shift2Rail 调研）

3.1 轨道交通中常用的形式化支撑工具

Shift2Rail TP2.7 D4.1 中通过审查文献和问卷调查的方式，选择了 8 种工具来作为轨道交通控制系统形式化建模的优选子集，即 Simulink、SCADE、UPPAAL、ProB、Atelier B、NuSMV、SPIN 和 UMC。根据图 2 显示，在轨道交通中，最常用的形式化工具是 B 方法相关的工具，如 Atelier B 和 ProB。B 方法的早期应用案例是开发了巴黎地铁的信号系统和一些控制系统，包括巴黎地铁 14 号线的自动驾驶系统等。据粗略统计，目前全世界有数十条地铁线路的自动驾驶系统是用 B 方法开发的。此外，B 方法还被应用到其他安全攸关领域，如汽车和航空等领域，同时也被西门子和阿尔斯通等公司广泛使用。据了解，在我国从欧洲引入的

高铁信号控制系统和设备中，有一些软件也是用 B 方法开发的。紧随在 B 方法之后的是 Simulink、UPPAAL、NuSMV、SPIN 等工具。

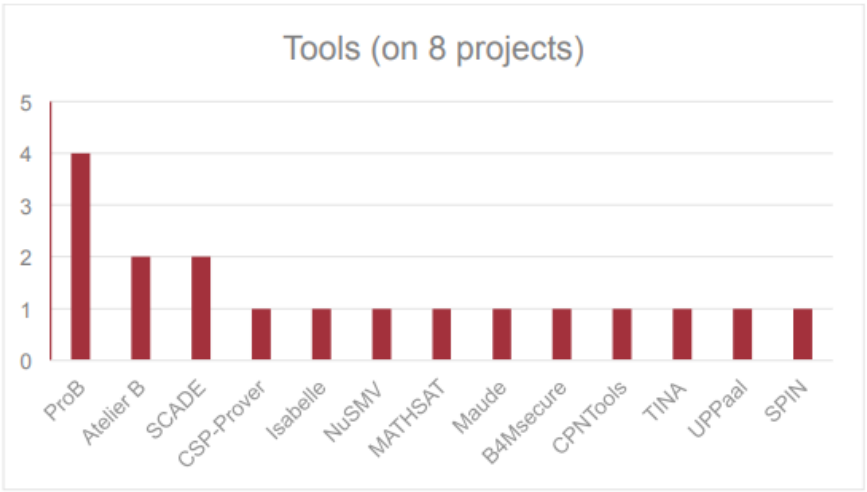

图 2 轨道交通中优选形式化工具

图 3 报告了应用形式化工具的文章数量的调查结果。值得注意的是，被检查的文章通常结合了不同的技术，因此，不同的技术并不相互排斥。例如，将基于模型的开发与模型检测结合。

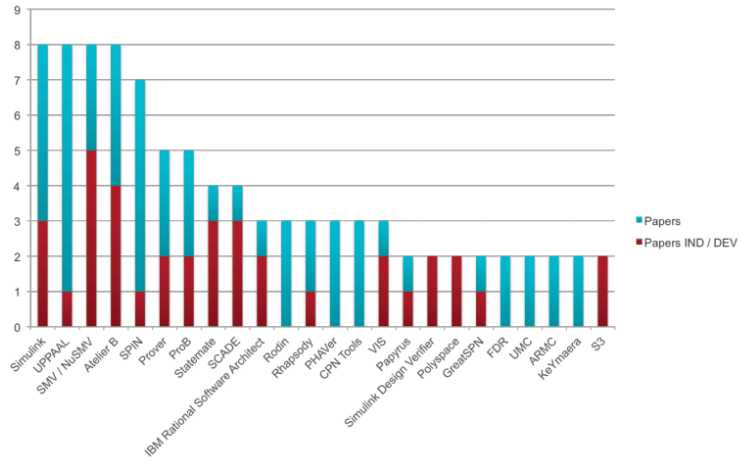

图 3 调研论文中讨论的形式化工具（Shift2Rail TD4.1）

3.2 形式化方法在轨道交通系统各开发阶段的应用

在对形式化从业者进行问卷调查中显示，大部分受访者认为最相关的功能特征是形式化验证（见图 4， 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%）。实际上，需仿真（通常以图形规范的动画形式化）来快速检查模型的行为；安全苛求

系统开发的主要指南强制要求软件开发产品之间的可追溯性（对模型的需求，代码模型等）。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。

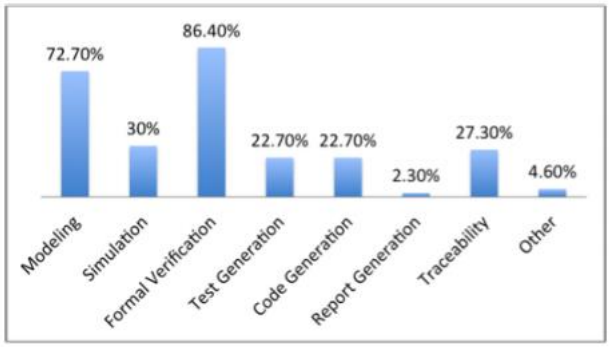

图 4 形式化工具在项目研究中的使用占比

图 5 报告了在调查的文献中，形式化方法在系统开发各阶段的应用。该结果表明，使用形式化方法对系统控制逻辑的高级定义进行架构设计的使用率较高，而后续阶段的使用率较少。事实上，测试、需求和组件涉及阶段都被考虑在内，但数量要少得多。值得注意的是，行业中往往涵盖需求阶段和后期开发阶段，如验证、实施和维护。这表明工业界有意用形式化方法覆盖更多的开发阶段，更接近于实现层次的开发阶段有更大的意图，其中形式化方法可以用来保证具体实现的正确性。

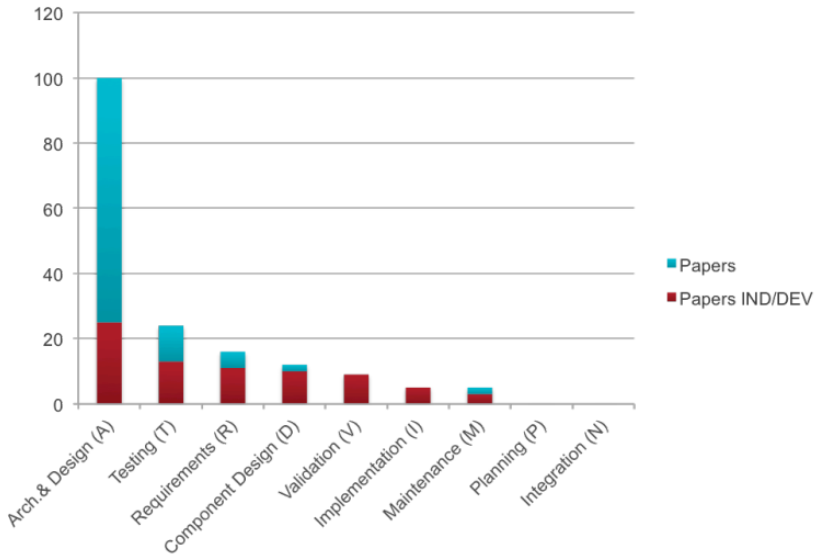

图 5 形式化方法在系统开发阶段的应用

4. 智能信号系统的形式化及标准接口设计

形式化方法可以通过发现或避免早期错误而减少成本，补充昂贵的测试和安全审查阶段，缩短系统维护周期，这些优点对于轨道交通系统的研发而言都是非常有益的。但是就目前而言，形式化方法的应用仍然面临着许多挑战，例如相关专业的人才欠缺，生成文档难理解等。

在典型的客户端/开发人员场景中，通常的做法是生成普通的非形式化系统需求文档。开发人员可以使用该文档来构建系统的初始可执行规范，然后将其精化为最终产品。在实际工作中，不仅向单个开发人员提供相同的严格/可验证规范，也可能为多个应该生产等效产品的不同开发人员提供相同的规范。铁路信号系统是由许多子系统组成的(每个子系统可能由不同的供应商开发)，这种情况更复杂（见图 6），它们之间必须正确地相互作用。因此需要建立起标准接口，以供提交给不同的开发人员。

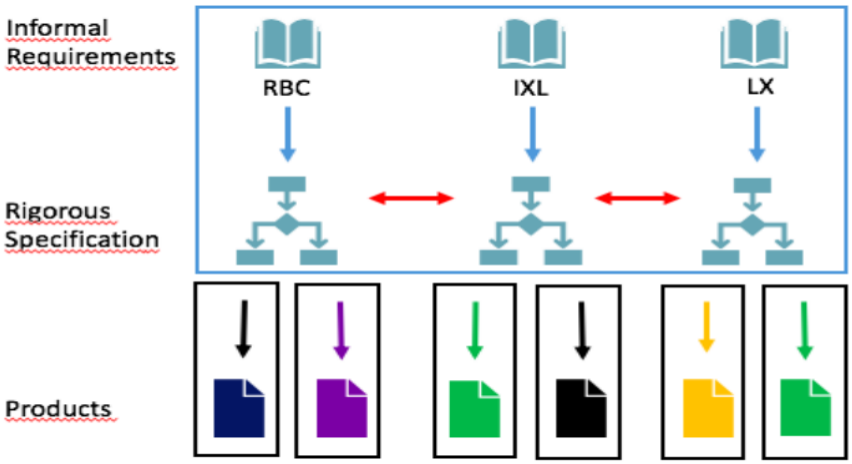

图 6 轨道交通信号系统的开发模式

4SECURial 项目中将形式化方法和标准接口的使用确定为两个关键概念，以缩短开发和交付信号系统所需的时间，并降低采购、开发和维护的高成本。需要用形式化方法来确保正确的行为、互操作性和安全性，用标准接口来促进市场竞争和标准化，降低长期的生命周期成本。标准接口旨在成为由基础设施管理者（客户）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。

该项目定义此“标准接口”规范的目的是在整个欧洲(单一欧洲铁路区域，SERA)创建可互操作的铁路。而这也是将形式化方法快速纳入系统开发设计阶段的一种有效方式。

5. 总结

随着人工智能技术的引进，运能的不断扩增，以及速度的逐步提升，以轨道交通为代表的高安全苛求领域控制系统的安全设计不容小觑。在下一代列车控制系统研发中，为确保安全可信性，控制系统的研发必须采用可信构造技术。而形式化方法在安全苛求型系统的研发中已成为一种趋势。因此，掌握形式化方法的技术，并将其正确的应用到列车控制系统的研发中，很有可能会为企业甚至是国内轨道交通的发展带来非常可观的收益。

参考文献：

[1] Guy Katz, Clark Barrett, David L. Dill, et al. Reluplex: An efficient SMT solver for verifying deep neural networks[C]. CAV 2017, pp.97-117.

[2] Ruediger Ehlers. Formal verification of piece-wise linear feed-forward neural networks[C]. ATUA 2017. pp. 269-286

[3] 王戟, 詹乃军, 冯新宇,等. 形式化方法概貌[J]. 软件学报, 2019, 30(001):33-61.

[4] 陈铭宋，鲍勇翔，孙海英，等.基于通信的列车控制系统可信构造：形式化方法综述[J].软件学报，2017. 28(5):1183-1203

[5] CCF 形式化专家委员会.人工智能系统的形式化验证技术研究进展与趋势. 2019-2020 中国计算机科学技术发展报告. pp:492-539

[6] Roanes-Lozano E, Hernando A , Alonso J A , et al. A logic approach to decision taking in a railway interlocking system using Maple[J]. Mathematics and computers in simulation, 2011, 82(1): p.15-28.

[7] Lecomte T. Safe and Reliable Metro Platform Screen Doors Control/Command Systems[C]// International Symposium on Formal Methods. Springer Berlin Heidelberg, 2008.

[8] Zafar N A. Formal specification and validation of railway network components using Z notation[J]. IET Software, 2009, 3(4):312-320.

[9] Bozzano M, Cimatti A, Katoen J P, et al. The COMPASS Approach: Correctness, Modelling and Performability of Aerospace Systems. 2009.

[10]程永江, 周清雷. 基于 uppaal 的飞机着陆控制系统模型验证[J]. 计算机工程与设计, 2009(23):227-229.
[11]Gu Q, Wang G, Ming Z. Model-based Safety Analysis for Integrated Avionics System[C]// Aiaa Aviation Technology, Integration, & Operations Conference. 2015.