

基于 UML 的列车自动防护系统需求建模研究

刘攀峰¹ 邱昕夕² 陈祥献¹ 黄 海¹ 段会龙¹

(浙江大学生物医学工程与仪器科学学院 杭州 310027)¹ (浙江大学信号系统研发中心 杭州 310027)²

摘 要 针对列车自动防护系统(ATP)对软件的高安全性的需求,提出并实现了一种基于 UML 的需求建模方法。该方法借鉴了形式化语言的特点,在经典的状态机模型上做了改进,引入了超级状态机,并定义了精确的规则和语义,实现了对复杂的 ATP 系统的形式化建模。在某城市地铁线路的信号系统的应用表明,此方法建立的需求模型避免了语言描述的二义性,降低了软件故障率,提高了 ATP 系统的安全性,且更易于开发和维护。

关键词 列车自动防护,需求建模,统一建模语言,形式化方法,安全性

中图法分类号 TP301 **文献标识码** A

UML Based Software Requirement Modeling for Automatic Train Protection

LIU Pan-feng¹ QIU Xin-xi² CHEN Xiang-xian¹ HUANG hai¹ DUAN Hui-long¹

(College of Biomedical Engineering and Instrument Science, Zhejiang University, Hangzhou 310027, China)¹

(Zhejiang University Signal System Research and Development Center, Hangzhou 310027, China)²

Abstract To meet the needs of high safety of automatic train protection system, this paper proposed and implemented an optimized UML-based requirement modeling method. By learning from the formal method, this paper improved the classical state machine model, and introduced a super-state machine with a series of accurate pre-defined rules, to implement the formal modeling of ATP system. Applied the method to an urban rail transit signal system, the result shows that the model established in this paper reduces the software failure by avoiding the ambiguity, meanwhile, it greatly improves the safety and reliability and makes the system more easily to develop and maintain.

Keywords Automatic train protection, Requirement modeling, UML, Formal method, Safety

在现代公共交通系统中,城市轨道交通系统以其高速便捷等特点显示出越来越突出的作用和地位。列车运行防护系统(ATP)作为轨道交通系统的关键子系统,担当着保障行车安全和提高列车运行效率的重任,具有很高等级的安全性要求,在铁路应用标准 EN50128 中指出 ATP 系统的安全性等级为 SIL4^[1]。近年来,基于形式化和基于模型的设计方法为提高列车运行控制系统的安全性提供了有效途径^[2,3],但是系统安全不仅要从设计阶段保证,更要从需求阶段保证。很多研究重点在于提高设计阶段的安全性,而忽略了需求分析阶段作为系统开发生命周期的第一个阶段对系统安全性的至关重要的作用。有报告指出,在软件生命周期中,一个错误发现得越晚,修复错误的费用越高,被检查出来的错误的 56% 产生的根源可以追溯到需求阶段^[4]。有研究者关注于在建模中引入形式化方法来减少描述的二义性^[5],但形式化方法过于依赖数学符号与逻辑推理,比较繁杂且不容易理解。而对于复杂的 ATP 系统,单纯的一个说明或公式系统不能准确地刻画实际需求,在具体的项目中必须根据实际情况考虑需求的形式化程度。与形式化方法相比,统一建模语言(UML)具有简洁、可视化、标准化的特点,而且更具综合性,易于被开发人员掌握,不需要进行大量的培训,可以有效地提高开发效

率^[6,7]。

基于以上原因,本文结合各种方法的优缺点^[5],提出一种半形式化的面向对象的需求分析建模方法:基于 UML 的 ATP 软件需求建模方法。该方法借鉴了形式化语言的特点,在 UML 模型上做了改进,可以精确地描述需求,并且可以使用模型验证工具对其进行验证。此外,建立的需求模型可以实现需求分析到软件框架设计阶段的平滑过渡,并为后续的软件架构设计和软件测试提供精确的依据。

1 基于 UML 的软件需求建模

1.1 软件需求建模

在 EN50128 中,定义了一个 V-模型的软件开发生命周期^[1],描述了安全相关软件的开发过程中主要包含需求分析阶段、框架设计阶段、模块设计阶段及编码阶段。由于目前列车自动防护系统软件需求的分析方法主要依赖于分析者的经验和对系统的熟悉程度,很难满足 EN50128 标准^[1]对软件需求的清楚准确、无二义性、可验证、可测试等特性的要求,因此,本文提出在需求分析阶段后进行需求建模,以实现需求分析到软件框架设计阶段的平滑过渡,如图 1 所示。

刘攀峰(1989—),女,硕士生,主要研究领域为城市轨道交通列车自动防护子系统,E-mail:lylpf0122@163.com;邱昕夕(1968—),男,高级工程师,E-mail:qiuxinxi@zdwjxd.com(通信作者);陈祥献(1967—),男,副教授,主要研究领域为城市轨道交通信号系统、虚拟仪器、普适计算等;黄 海(1959—),男,教授,主要研究领域为信号处理及其应用。

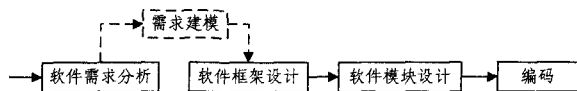


图1 软件开发流程图

需求模型通常使用图形符号来创建,并辅以文字说明描述,从而避免了需求分析中自然语言的不一致性和二义性。因此,使用需求建模的方法可以以简洁、准确、结构清晰的方式描述软件需求,提高系统安全性。

1.2 UML 建模技术

统一建模语言 UML 作为一种用于描述可视化和构架软件系统的半形式化建模语言,它不仅统一了 Booch、OMT 和 OOSE 等方法中的基本概念,而且吸取了面向对象技术领域中其他流派的长处,其中包括非 OO 方法的影响,从而更具综合性^[6,7],很适合对大规模、复杂的软件系统进行建模。此外,UML 多种类型的图形表示(如用例图、类图、序列图、状态图、活动图等)适用于系统开发过程中从需求分析到系统完成后测试等系统开发的不同阶段^[8]。

UML 状态图的重点在于说明对象的状态及其状态之间的转移。状态图主要用于描述一个对象在其生存期间的动态行为,表现为一个对象所经历的状态序列、引起状态转移的事件,以及因状态转移而伴随的动作。一般可以用状态机进行建模来描述控制流,用状态图显示状态机。

1.3 改进的 UML 状态机建模技术

ATP 系统是一个庞大而复杂的系统,包含许多复杂的逻辑状态的转换,可能的状态数也很多,在状态分析和 UML 建模中很容易引入错误。因此,本文采用分层次结构化的状态机模型,即超级状态机的方法来设计模型。所谓超级状态机方法,是用一个超级状态来封装一系列独立的状态,这个超级状态在高层模型中被当作一个状态,在下一级模型中就展开成了一系列状态^[9]。

UML 所建立的面向对象的系统模型是一种半形式化的模型,这种模型由一系列的图形符号构成,这些符号并没有严格的形式化的定义。本文借鉴形式化语言的特点,提出通过一系列预先定义的详细准确的语义和规则将 UML 模型的语言描述形式化的方法。这种语义表达和规则,简洁易于理解,汲取了形式化语言精确性的特点,却不像形式化语言那么抽象和繁杂,易于掌握和学习。例如在建立的需求模型中有一条规则定义,如图 2 所示。由图可知,从状态 State_1 到状态 State_2 的转换条件表示为 $T[A, B, \sim C, \sim D]$ 。规则 $T[A, B, \sim C, \sim D]$ 表示满足条件 A 和 B 并且不满足条件 C 和 D,即当满足条件 A、B 且不满足条件 C、D 时可以由状态 State_1 转换到 State_2。

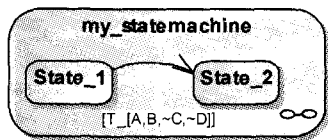


图2 超级状态机示意图

经过这两点改进的 UML 状态机建模方法,可以将需求中复杂的条件清晰化、简单化,建立精确的需求模型,实现 ATP 需求分析的准确描述。下节将以 ATP 系统软件设计实例来说明整个建模过程。

2 ATP 系统软件需求建模

2.1 ATP 系统功能概述

ATP 子系统连续、自动地对轨道区段状态及列车位置进行检测,以保证系统对列车进路的安全控制和对列车运行速度及间隔的安全控制。在其他子系统出现异常时,ATP 系统能够导向安全,并且具有完善的降级运行功能。ATP 子系统具有在各种驾驶模式下对列车运行的超速防护功能^[10]。

ATP 系统应用软件通过安全平台软件提供的接口来获取可靠的数据和安全的数据输出。结合 ATP 系统功能的特点,ATP 系统软件可划分为以下几个模块:底层平台管理、系统初始化模块、数据库服务、业务处理、列车定位、列车测速、门控与发车、目标点计算、ATP 曲线计算和列车监控模块。其中,列车监控模块主要负责完成列车的模式管理功能及列车运行状态的监控。下面仅以列车模式管理功能为例,说明本文所描述的 ATP 软件需求建模的过程。

2.2 需求描述

ATP 应用软件的列车模式管理功能保证了对驾驶模式的控制和模式之间的转换。车载设备应周期性地检查列车当前运行模式所具备的条件是否满足,如果不满足则采取相应的安全措施。列车所允许的驾驶模式转换应能通过人工或自动的方式完成。ATP 系统应用软件设计了如下控制模式:

- ATO:列车全自动驾驶模式
- ATPM:ATP 防护的人工驾驶模式
- ATB:自动折返模式
- RM_F:受限的人工驾驶模式(向前)
- RM_R:受限的人工驾驶模式(向后)
- IATPM:点式 ATP 驾驶模式
- IATO:点式 ATO 自动驾驶
- EBM:紧急制动模式
- NRM:人工驾驶模式

2.3 需求建模过程

根据以上所描述的功能需求和各个模式所要实现的功能及相互关系,可利用超级状态的方法将模式进一步划分层次,如图 3 所示。在 CBTC 模式下,车载设备能够接收区域控制器发送的移动授权信息以及相关的地面设备状态数据;在点式 IATP 模式下,车载设备仅根据相关的地面设备状态数据运行;在 RM 模式下,由司机人工驾驶列车,车载设备仅提供列车运行最高限速。如图 4 所示,列车模式管理功能模块的外部接口输入有:列车自动运行系统(ATO)状态数据、列车 IO 数据、区域控制器(ZC)有效数据、测速数据和定位数据;此功能模块的输出为列车当前的运行模式。

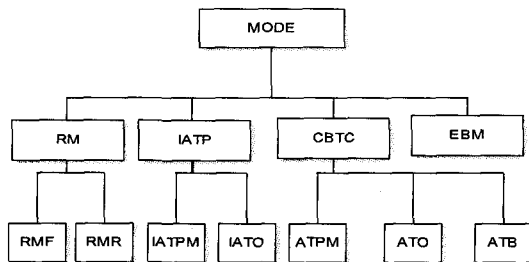


图3 ATP 列车运行模式图

具体来说,ATP 软件系统需要从列车 IO 接口获取离散的安全输入数据,从测速定位模块获取速度信息及列车定位信息;从轨道数据库 DSU 获得有效的线路数据库数据;从 ZC 接口获取 ZC 的状态数据及 MAL 数据;从 ATO 获取相关工作状态数据。根据各个模式的功能特点分析得出此模块的模式运行需要判断以下运行必备条件:

1. 与 ZC 的链接状态是否正常
2. ATO 工作状态是否健康
3. 列车定位功能是否正常
4. 本端 CC 激活且另端 CC 未激活
5. ATB Key 是否有效
6. 是否存在有效的点式移动授权
7. 是否存在有效的 ZC 移动授权
8. 测速功能是否正常
9. 模式开关 2 是否处于 NORMAL 位置
10. 方向控制器是否处于 FWD 位置
11. 方向控制器是否处于 REV 位置
12. 列车完整性是否正常
13. 车门未旁路且车门状态合法
14. 线路数据库是否可用
15. 是否处于紧急制动状态

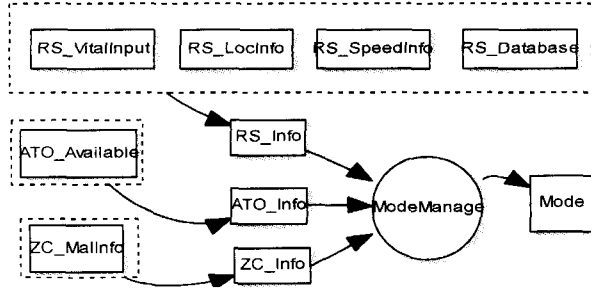


图 4 列车模式管理功能模块数据流图

根据对需求的分析可得出在各个模式下的运行必备条件,如表 1 所列。表中各行表示上述的 15 个必备条件,各列表示 ATP 的各个工作模式。

表 1 ATP 各个工作模式的必备条件

	ATB	ATO	ATPM	IATO	IATPM	RMF	RMR	EBM	NRM
1	★	★	★	—	—	—	—	—	—
2	★	★	—	★	—	—	—	—	—
3	★	★	★	★	★	—	—	—	—
4	★	★	★	★	★	★	★	—	—
5	★	—	—	—	—	—	—	—	—
6	—	—	—	★	★	—	—	—	—
7	★	★	★	—	—	—	—	—	—
8	★	★	★	★	★	★	★	—	—
9	★	★	★	★	★	★	★	—	—
10	★	★	★	★	★	★	×	—	—
11	×	×	×	×	×	×	★	—	—
12	★	★	★	★	★	★	★	—	—
13	★	★	★	★	★	—	—	—	—
14	★	★	★	★	★	—	—	—	—
15	×	×	×	×	×	×	×	★	—

注:★必备条件;×不能存在的条件

由此表可以看出,各个模式下的必要条件各不相同。此外,该功能模块的模式有以下几个特点:每个周期都有一个控制模式状态存在,每个模式下都会执行一定的操作,各个控制

模式之间可以通过一定的条件触发进行转换。如当列车在 RMF 模式下运行时,如果 ATP 曲线计算模块计算得出 IATP 模式可用,而且从列车 IO 接口采集获得的模式选择开关位于 IATP 模式,则列车控制模式由 RMF 模式转换到 IATP 模式。基于以上特点,可以用状态机模型对列车模式管理模块进行建模。各个模式之间的状态转换图如图 5 所示,图中对各个模式之间的转换条件都做了清晰的标示。例如 RM 模式与 CBTC 模式之间的转换条件 $T_{[1,3,7,13,14]}$ 表示:当满足表 1 中 1,3,7,13,14 条件时,列车模式管理模块会将当前列车的模式由 RM 模式切换到 CBTC 模式,再根据条件 2 和 5 判断其应该为 ATPM,ATO 或者 ATB 模式。

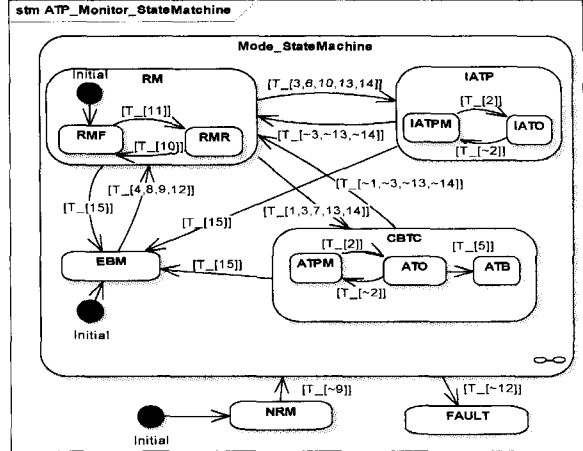


图 5 ATP 工作模式状态机模型

3 结果及分析

本研究使用沈阳 1 号线线路数据为对象,开发了 ATP 自动防护系统软件,并在仿真平台上进行了功能模拟。图 5 所示模型中,共有 20 条转换规则,分别对应 ATP 系统的 12 条需求。结果证明,用以上状态机模型开发的代码可以满足 91% 以上的需求,而未使用此模型开发的系统只满足了 75% 的需求描述。因此使用该方法设计的需求模型可以满足列车在各个场景下的模式转换,很好地满足了需求。

此外,通过此方法建立的 ATP 软件需求模型精确、可靠,提高了 ATP 系统的安全性,降低了软件故障失效率,更易于开发、测试和维护。表 2 中比较了传统的开发方法和本文中的需求建模的方法。从表中的数据可以看出,由于采用了需求建模的方法,所开发的系统开发周期大大缩短了,同时与需求相关的缺陷数大大降低了。因此,该方法很大程度上提高了系统的安全性,很好地满足了系统需求。

表 2 传统开发方法与使用需求建模方法开发周期比较

系统	传统方法	本文方法
开发周期	10 个月	6 个月
需求条数	38	38
代码行	3538	3980
构件个数	8	11
需求相关缺陷数	89	35

结束语 在计算机软件越来越多地应用于安全相关领域的今天,本文提出采用 UML 技术对 ATP 应用软件进行需求建模的方法,在体现了面向对象需求分析技术的优势和特点的同时,还使 ATP 应用软件复杂的需求得到直观、明晰的描

述,有效地解决了文字描述的二义性等固有问题;并且使软件开发及维护阶段的工作能够顺利进行,提高了开发效率,确保了软件产品的质量。本文所提出的开发方法,为实际的 ATP 软件的需求分析以及相关的开发研制工作提供了一个新的思路。但本文未使用模型验证工具对所建立的需求模型进行验证,这将是后续研究的重点。

参考文献

[1] CENELEC. Railway applications-Communications, signaling and processing systems-Software for railway control and protection systems[S]. EN 50128:2001 / IEC 62279:2002

[2] Behm P, Benoit P. a successful application of B in a large project [J]. Lecture Notes in Computer Science, 1999, 1(1708): 369-387

[3] Wang Hai-feng, Gao Chun-hai, Liu Shuo. Model-based software development for automatic train protection system[C]//Computational Intelligence and Industrial Applications, 2009. PACIIA, 2009: 463-466

[4] Tavalato P, Vincena K. A Prototyping Methodology and Its Tool[M]//Budde R, et al., eds. Approaches to Prototyping. Berlin: Springer-Verlag, 1984: 434-436

[5] 王黎, 毋国庆, 吴怀广. 面向行为的需求建模研究及实现[J]. 计算机科学, 2011, 38(4): 175-181

[6] Hull E, Jackson K, Dick J. Requirements Engineering [J]. Springer, 2010, 3(6): 47-76

[7] 史英海. UML 在航天器姿态与轨道控制应用软件需求建模中的应用[J]. 空间控制技术与应用, 2008, 34(3): 42-45

[8] 周慧华, 郑明辉. 一种改进的软件工程需求建模框架[J]. 微机发展, 2004, 14(2): 75-77

[9] 萨默维尔, 程成. 软件工程[M]. 北京: 机械工业出版社, 2007: 106-109

[10] IEEE Recommended Practice for Communications-Based Train Control(CBTC) System Design and Functional Allocations[S]. IEEE 1474. 3-2008

(上接第 451 页)

比较图 10 和图 11, 在同样的初始条件下, PSO-BP 算法较纯 BP 神经网络控制效果要好一些。原因是采用 PSO-BP 会得到更好的训练精度, 由于误差较大的作用得到的 i_d 、 i_q 、 ω 控制曲线有时候会发生抖动现象, 而不是一条平整的直线。

令 $\rho = (k+1)d_n - d_{n+1}$, 以 $u_{1n-1} = u_{1n} + \rho$ 代替 u_{1n} 代入式 (20), 得:

$$\begin{cases} i_{dn+1} = i_{dn} + \Delta t \cdot K_{i_d}^2 \\ i_{qn+1} = i_{qn} + \Delta t \cdot K_{i_q}^2 \\ \omega_{n+1} = \omega_n + u_{1n} + \rho + e_{n-1} \end{cases} \quad (21)$$

采用 PSO-BP 算法对式 (21) 进行仿真, 得到如图 12 所示的混沌控制效果图。图 13 是控制量 u_{1n-1} 的行为效果图。在同样的条件下, 采用纯 BP 神经网络的混沌控制效果如图 14 所示, 其行为效果图如图 15 所示。

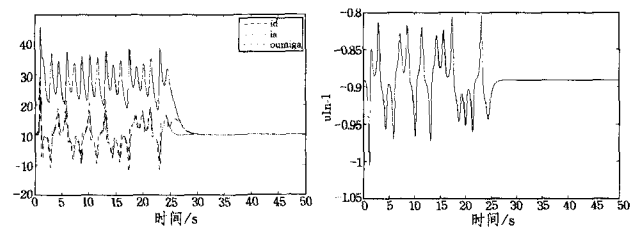


图 12 PSO-BP 混沌控制到平衡点 (0,0,0)

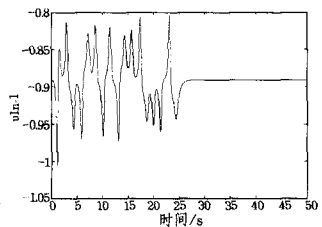


图 13 采用 PSO-BP 的 u_{1n-1} 行为效果

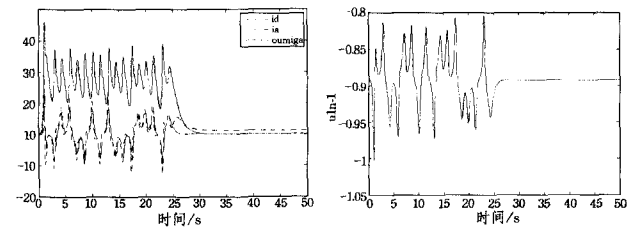


图 14 BP 混沌控制到平衡点 (0,0,0)

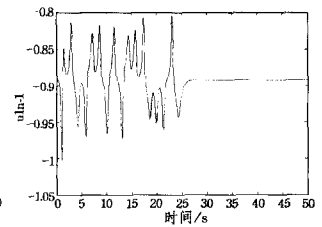


图 15 采用 BP 的 u_{1n-1} 行为效果

比较图 12 和图 14 可见, 采用 PSO-BP 算法可以将控制效果很好地稳定到平衡点 (0,0,0) 上, 得到的最后曲线几乎是一条直线, 没有抖动现象, 采用 BP 算法则会出现控制曲线上的抖动, 由于较大误差的存在, 使得按本文的控制原理来控制难以达到平衡点 (0,0,0); 再比较图 13 和图 15, 由于两种算法的误差精度不同, u_{1n-1} 行为效果也出现了差异, 采用 PSO-BP 算法可以使 u_{1n-1} 最后稳定在某个值, 而采用纯 BP 神经网络时, u_{1n-1} 在很小的范围内不断变动。

结束语 微粒群优化算法有很大的研究价值, 本文利用它的优点用于优化神经网络, 并在混沌控制上得到了应用。通过 PSO-BP 算法和纯 BP 神经网络对永磁同步电机的混沌控制进行比较, 证明了 PSO-BP 算法比纯 BP 神经网络更加优越, 可以得到几乎理想的结果, 说明了 PSO-BP 算法在实际中会得到更满意的效果, 应用上具有更大的可行性。

参考文献

[1] 刘希玉, 刘宏. 人工神经网络与微粒群优化[M]. 北京: 北京邮电大学出版社, 2008(3): 263-267

[2] 谭文, 王耀南. 混沌系统的模糊神经网络控制理论与方法[M]. 北京: 科学出版社, 2008, 5: 58-60

[3] Shi Y, Eberhart R C. A modified particle swarm optimizer[C]//Proc. of the IEEE CEC. 1998: 69-73

[4] 高尚, 杨静宇. 群智能算法及其应用[M]. 北京: 中国水利水电出版社, 2007, 12: 6-8

[5] Lee C-Y, Shen Yi-xing, Cheng J-C, et al. Neural Networks and Particle Swarm Optimization Based MPPT for Small Wind Power Generator[J]. Engineering and Technology, 2009, 60: 17-23

[6] 李磊, 秦卫阳, 张劲夫. 采用 BP 神经网络进行混沌运动控制[J]. 振动与冲击, 25(5): 89-91

[7] 徐丽娜. 神经网络控制[M]. 哈尔滨: 哈尔滨工业大学出版社, 1999, 5: 48-53

[8] 张波, 李忠. 永磁同步电动机的混沌模型及其模糊建模[J]. 控制理论与应用, 2002, 19(4): 545-548