面向车车通信的安全计算机时间约束性分析验证

高莺[1]，曹源[2]，孙永奎[3]，马连川[2]，洪春华[3]，张玉琢[3]

（1. 中国铁道科学研究院研究生部，北京 100081；
2. 北京交通大学轨道交通运行控制系统国家工程研究中心，北京 100044；3. 北京交通大学电子信息工程学院，北京 100044）

摘 要：为适应基于通信的列车运行控制（CBTC, communication based train control）系统从车地模式向车车通信模式发展的趋势，针对多周期性应用并发的车载安全计算机的时间约束性，提出了基于时间 Petri 网的安全计算机时间约束性验证方法。以车载 2 乘 2 取 2 安全计算机为例，通过分析安全计算机多周期应用的并发性质，采用时间 Petri 网（TPN, time Petri net）推算其时间可调度区间，并在此基础上进行实例分析。分析和验证结果表明，在单核主频 1GHz 的条件下，车载安全计算机能满足 3 个以上周期性安全关键应用的时间约束性，表明 TPN 在验证和评估安全计算机中周期性应用的时间约束性方面的有效性。

关键词：时间 Petri 网；车车通信；安全计算机；时间约束

中图分类号：U285.49

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2018275

Analysis and verification of safety computer time constraints for train-to-train communications

GAO Ying[1], CAO Yuan[2], SUN Yongkui[3], MA Lianchuan[2], HONG Chunhua[3], ZHANG Yuzhuo[3]

1. Graduate Department, China Academy of Railway Sciences, Beijing 100081, China
2. National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing 100044, China
3. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Abstract: In order to adapt to the development trend of the communication based train control (CBTC) system from train-ground communication mode to train-to-train communication mode, a verification approach for time constraints of multi-period applications concurrence on-board safety computer based on time Petri net was proposed. By taking the double 2 out of 2 on-board safety computer as an example, the multi-period applications concurrence nature of the safety computer was analyzed. Time Petri net (TPN) was utilized to calculate the time schedulable interval. Then several cases were analyzed based on the inference of this approach. The analysis and verification results indicate that onboard safety computer can meet the time constraints of more than three periodic safety-critical applications under the condition of single-core with main frequency of 1GHz, which demonstrates the effectiveness of verifying and evaluating the time constraints of safety computer periodic applications using TPN.

Key words: time Petri net, train-to-train communication, safety computer, time constraint

1 引言

现代轨道交通列车运行控制系统采用分布式、叠加结构，通过地面子系统设备和车载子系统设备之间的通信实现列车运行控制[1]。但是随着现代无线技术发展，系统将从车地协同控制模式向更加智

收稿日期：2018−08−07；**修回日期**：2018−11−29

通信作者：曹源，ycao@bjtu.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2018YFB1201601）；国家自然科学基金资助项目（No.U1534208, No.U1734211）

Foundation Items: The National Key Research and Development Program of China (No.2018YFB1201601), The National Natural Science Foundation of China (No.U1534208, No.U1734211)

能化的车车通信模式发展，以满足日益增长的行车组织要求。车车通信技术旨在尽可能减少地面子系统设备，并将地面子系统功能整合到车载子系统中，使列车运行控制模式由列车和地面子系统协同控制转变为列车之间直接协同控制[2]。由于车车通信技术对车载安全计算机功能的要求愈加苛刻，其软件应用也将愈加庞大，使面向车车通信的安全计算机成为多周期性应用并发的实时控制系统。支持多任务并发的系统虽然具有资源整合共享、降低系统设备复杂度、优化系统结构等诸多优势，但也存在影响系统运行实时性及应用执行时间不确定延时的问题。

时间约束性是安全关键系统重要的特性。安全计算机在规定的时间内完成安全控制逻辑，才能保证行车安全。IEC61508 标准和 EN50128 标准均对安全关键系统的软件功能提出时间约束性要求[3]。由于时间约束性在安全关键系统中的重要性，针对实时系统的时间约束性问题，国内外学者已经提出相关的验证和建模方法。文献[4]中提出了一种实时系统的时间约束建模和一致性验证方法，可针对性地检验系统的时间缺陷。文献[5]中提出了基于时间 Petri 网的实时系统可调度性分析方法，说明了时间 Petri 网能有效地分析实时系统的时间特性。也有学者利用 Petri 网对实时系统进行组合可调度性[6]和独立性[7]分析，说明该方法适用于分析安全关键系统的特性。文献[8]通过分析具有标记的时间 Petri 网系统的可诊断性，说明时间 Petri 网适用于安全关键系统的故障诊断。文献[9]分析了时间约束 Petri 网模型及其可调度性，从而验证了时间 Petri 网能有效描述和分析时间约束性问题。文献[10]研究了基于时间 Petri 网的实时并行设计过程，定量分析了实时并行过程的时域性，说明时间 Petri 网可为并行设计提供可靠的理论依据。

在轨道交通领域，时间 Petri 网主要用于分析列车运输调度问题。文献[11]提出基于时间 Petri 网的推理算法，验证了时间约束的列车运行调整方案的可行性。文献[12]提出了基于模糊时间 Petri 网的列车运行时间不确定问题的处理方法。然而，目前国内外针对安全计算机安全性方面的研究，主要集中在硬件安全设计方法，如 2 乘 2 取 2 架构、3 取 2 架构等。同时为了确保轨道控制设备的安全性和可靠性，车载安全计算机只采用经过反复验证的计算机硬件，其性能远低于主流的计算机。由于车载安全计算机硬件安全结构和性能等方面的限制，同时也缺乏针对多周期性应用时间约束性的验证和评估方法，导致其系统软件设计更加保守化，严重制约轨道交通控制技术的发展。因此本文以目前安全计算机硬件结构和性能现状入手，针对面向车车通信的车载安全计算机多周期性应用的时间约束性问题，首次采用时间 Petri 网建模验证，以说明多周期性应用能够满足车载安全计算机时间约束性的安全需求。

2　车车通信系统

CBTC 系统是目前国内外大部分城市轨道交通使用的信号系统技术。CBTC 系统主要采用车载子系统与地面子系统相互协作实现列车行车控制和移动闭塞功能，因此线路中存在许多区域控制器（ZC, zone controller）、计算机联锁（CBI, computer-based interlocking）等地面设备。然而，复杂的地面设备导致子系统之间接口复杂化，系统维护成本高，运营灵活性差等诸多问题。为解决以上问题，国内外开始研究轨道交通信号系统车车通信技术，以简化系统复杂度，精简轨旁设备，提高并优化系统性能，如法国里尔地铁 1 号线已经采用了以目标控制器和列车为核心的控制系统[2]。

在基于车车通信的列车运行控制系统中，区域控制器、联锁设备的功能被智能化的目标控制器和车载设备所取代，从而改变现有 CBTC 系统以地面控制设备为核心的架构，使车载系统成为行车控制核心。通过现代无线通信（如 wlan、LTE-M）和移动控制算法[13-14]等技术实现列车与列车之间，列车与目标控制设备之间直接协同控制，降低系统对轨旁设备的依赖，减少系统控制流中间环节，如图 1 所示。基于车车通信的列车运行控制系统能够降低系统复杂度，降低维护成本，提高运营的灵活度，并将全面提高对车载安全计算机的性能需求。多个独立控制功能模块整合到车载安全计算机中，使其设计面临多应用并发和系统实时性之间的矛盾。列车运行控制系统作为安全关键实时控制系统，其应用逻辑设计基本采用周期性时限执行的控制算法，对执行的时间约束性要求高。而目前 CBTC 系统的车载安全计算机只考虑简单应用需求场景，缺少对多个独立功能模块整合的并发系统的研究，针对该问题，本文对安全计算机多应用并发性进行时间约束性分析，对 CBTC 系统由车地通信模式向车车通信模式转换有一定的指导意义。

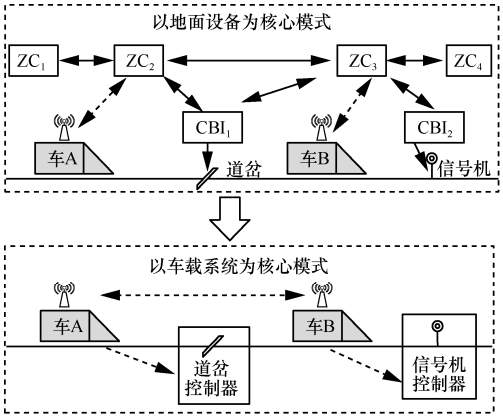


图 1 车车通信系统架构

3 时间约束性分析

3.1 时间 Petri 网

Petri 网概念最早于 1962 年由德国 Carl Adam Petri 提出，直观的图形表示特点和完善的数学理论基础使其特别适合描述异步并发系统。随着时间因素在实际应用分析中愈加重要，出现 TPN 分支理论[9]。TPN 也是 IEC61508 和 EN50128 软件完整性等级 SIL4 所推荐的建模方法。下面以图 2 为例分析 TPN 模型的参数含义。

如图 2 所示的 TPN 模型描述的是在 T_0 时刻库所 s_n 开始等待接收托肯，由于传输延时，托肯到达库所存在延时。

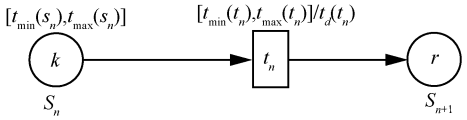


图 2 基本 TPN 模型片段

设在$[T_0+t_{\min}(s_n),T_0+t_{\max}(s_n)]$时域内的$T_1$时刻，获得托肯，库所$s_n$使能$t_n$变迁。只有使能后，$t_n$才能被触发。$t_n$使能后，$t_n$变迁在时间$[T_1+t_{\min}(t_n),T_1+t_{\max}(t_n)]$内的$T_2$时刻被触发。由于变迁$t_n$的处理延时为$t_d(t_n)$，则在$T_3$时刻触发结束。同样考虑传输延时的问题，在一定延时后，托肯进入库所s_{n+1}，从而实现从库所s_n经t_n变迁到达库所s_{n+1}，如图 3 所示。

设$T^f_{\text{start}}(t_n)$为t_n最早可能触发开始时间，$T^l_{\text{end}}(t_n)$为t_n最晚可能触发结束时间，$T_a(s_n)$为表示托肯到达库所的延时，描述接收资源的通信延时，$T_l(s_n)$为托肯离开库所的延时，描述发送资源的通信延时。

定义 1 可调度性。若考虑变迁t_n和库所托肯到达的时间，且变迁t_n满足式(1)，则称其具有强可调度性。若不考虑库所托肯到达的时间，则称为弱可调度性[9]。

$$\begin{cases} T^l_{\text{end}}(t_n)-T^f_{\text{start}}(t_n)\geqslant t_d(t_n) \\ T^l_{\text{end}}(t_n)=\min\{t_{\max}(s_n)-T_l(s_n), \\ \qquad t_{\min}(s_n)+t_{\max}(t_n)-T_l(s_n)\} \\ T^f_{\text{start}}(t_n)=\max\{t_{\min}(s_n),T_a(s_n)\}+t_{\min}(t_n) \end{cases} \tag{1}$$

变迁满足可调度性是指在一定的可调度范围内，通过调度调整能够实现满足时间约束性变迁，而不是在任何时间点都能实现变迁[9]。

3.2 安全计算机 TPN 模型

目前，国内外车载安全计算机基本采用分布式 2 乘 2 取 2 容错结构，每系独立划分为通用计算域、安全管理域[3]。实时系统的应用运行在通用计算域，并由安全管理域监督。安全计算机应用运行采用基于时间触发式的调度机制，在限定周期内完成一次应用执行逻辑，即周期性控制算法。为提高控制精确度，将一个应用执行周期T划分 3 个子周期：数据输入子周期、应用运算子周期、数据输出子周期。每个子周期在规定时间内完成相应逻辑处理后，向安全管理域报告运行状态，由安全管理域根据时间约束性判断应用执行逻辑是否满足安全要求，如图 4 所示。

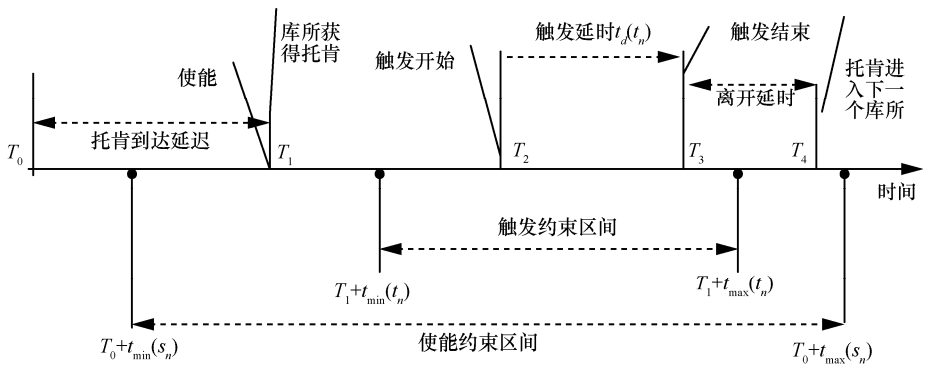


图 3 TPN 片段时间流描述

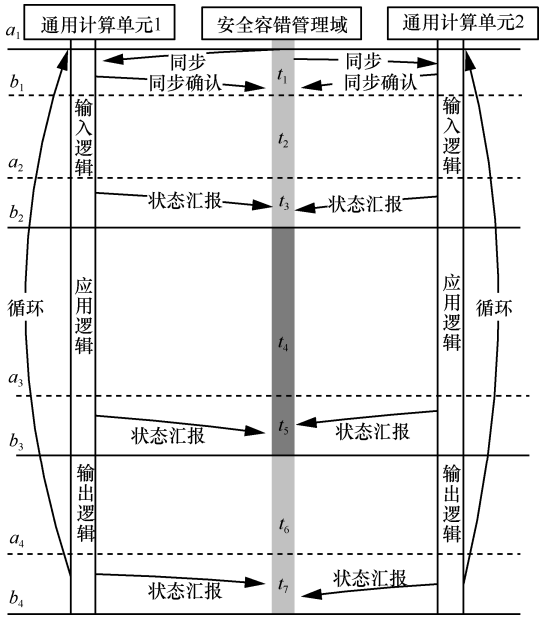


图 4　安全计算机时间调度算法

若应用出现故障不满足时间约束关系，则容错安全管理域能够及时有效地发现应用故障，从而采取有效安全措施防止事故发生。由安全计算机控制过程可知，车载安全计算机中系统应用在安全控制逻辑中被周期性调用执行，只要周期性应用不满足时间约束要求，就会触发安全计算机安全处理逻辑，使系统导向安全。根据图 4 安全控制逻辑流程，对时间触发式控制算法建立 TPN 模型，如图 5 和表 1 所示。

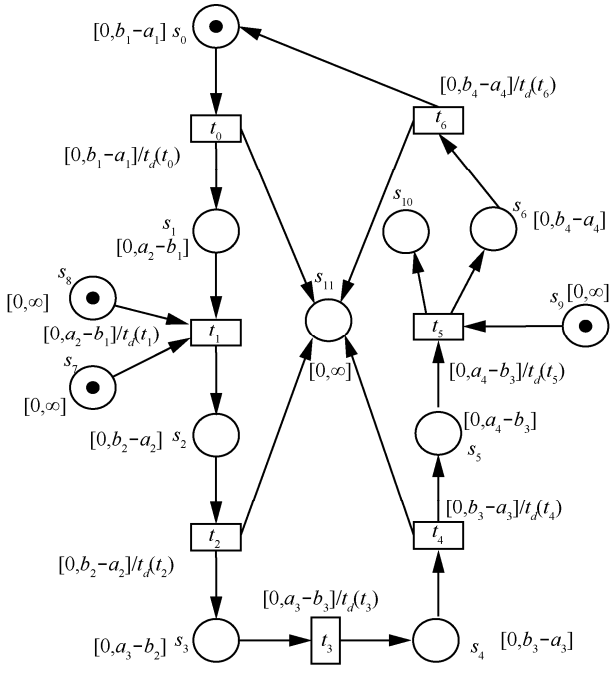


图 5　安全计算机时间调度算法 TPN 模型

表 1　　TPN 模型变迁含义

变迁	含义
t_0	发送同步确认信息至容错安全管理域
t_1	输入数据 2 取 2 逻辑对比
t_2	发送输入数据对比结果
t_3	执行系统应用逻辑阶段
t_4	应用逻辑运算结束状态汇报给容错安全管理域
t_5	输出数据 2 取 2 逻辑对比
t_6	发送输出数据对比结果

由图 5 可知 TPN 模型能直观描述安全计算机平台逻辑的时间约束特性。由于多任务多应用的复杂并发系统存在有限的资源（输入输出资源、CPU 资源等）复用问题，需要增加调度机制实现多个应用并发管理。假定单应用的 TPN 模型变迁都是可调度的，即在单任务的简单控制系统中，满足时间约束性要求的条件下，只要增加的调度变迁是可调度的，则多应用并行就能在满足时间约束关系条件下成功变迁。

3.3　调度变迁可调度条件

3.3.1　应用调度变迁

在多个周期性应用并行模式下，应用通过多线程（或多任务）调度机制实现并发执行。由于系统基于嵌入式实时操作系统，线程上下文切换开销时间与应用逻辑处理时间相比可忽略不计。设应用执行调度变迁为 k，系统各应用的变迁运算处理耗时为 t_i，则 n 个应用并行情况下，最长可能变迁延时为

$$t_d = \sum_{i=1}^{n} t_i \tag{2}$$

在应用执行阶段只负责数据逻辑处理，数据获取和传输都在其他时间段执行，因此 $T_a(s_k)$=0，$T_l(s_k)$=0，并且托肯的使能时间约束区间与触发约束区间相同。同时该变迁的某个时间约束段可能属于多个应用的时间约束区间，这种情况下该时间约束区取各个应用中最短的时间约束区间，即

$$\begin{aligned} t_{\max}(s_k) &= t_{\max}(t_k) = \min\{t_{\max}(n)\} \\ t_{\min}(s_k) &= t_{\min}(t_k) = \max\{t_{\min}(n)\} \end{aligned} \tag{3}$$

且由定义 1 可知，若要满足强可调度，则变迁 k 需满足式(4)。

$$\begin{aligned}T(k)&=T_{end}^{l}(t_k)-T_{start}^{f}(t_k)\\&=\min\{t_{\max}(s_k)-T_l(s_k),t_{\min}(s_k)+\\&\quad t_{\max}(t_k)-T_l(s_k)\}-\\&\quad\{\max\{t_{\min}(s_k),T_a(s_k)\}+t_{\min}(t_k)\}\\&=\min\{t_{\max}(t_i)\}-\max\{t_{\min}(t_i)\}\\&\geqslant\sum_{i=1}^{n}t_i\end{aligned}\tag{4}$$

3.3.2 输入调度变迁

在多应用并发执行模式下，每个应用输入变迁增加了数据排队到达的调度延时，则到达延时为

$$T_a(s_k)=\sum_{i=1}^{n}\alpha_i+T_c\tag{5}$$

其中，α_i 为各应用输入数据传输的排队延时，T_c 为外部通信延时（如无线通信延时）。

输入变迁 k 负责将接收的外部数据交给应用执行变迁处理，因此其离开库所延时 $T_l(s_k)$=0 。由定义 1 可知若要满足可调度性，则各变迁 k 需满足

$$\begin{aligned}T(k)&=T_{end}^{l}(t_k)-T_{start}^{f}(t_k)\\&=\min\{t_{\max}(s_k)-T_l(s_k),t_{\min}(s_k)\\&\quad+t_{\max}(t_k)-T_l(s_k)\}\\&\quad-\{\max\{t_{\min}(s_k),T_a(s_k)\}+t_{\min}(t_k)\}\\&=\min\{t_{\max}(t_i)\}-\max\{t_{\min}(t_i)\}-\sum_{i=1}^{n}\alpha_i-T_c\\&\geqslant\sum_{i=1}^{n}t_i\end{aligned}\tag{6}$$

3.3.3 输出调度变迁

输出变迁的 TPN 模型可看成输入变迁的逆过程，主要不同的是离开延时 $T_l(s_k)$ 。设每个应用排队离开的延时为 β_i，同样设外部通信延时为 T_c，则排队离开的调度延时为

$$T_l(s_k)=\sum_{i=1}^{n}\beta_i+T_c\tag{7}$$

由定义 1 可知输出变迁若要满足可调度性，需满足

$$\begin{aligned}T(k)&=T_{\text{end}}^{l}(t_k)-T_{\text{start}}^{f}(t_k)\\&=\min\{t_{\max}(s_k)-T_l(s_k),t_{\min}(s_k)+\\&\quad t_{\max}(t_k)-T_l(s_k)\}-\\&\quad\{\max\{t_{\min}(s_k),T_a(s_k)\}+t_{\min}(t_k)\}\\&=\min\{t_{\max}(t_i)\}-\max\{t_{\min}(t_i)\}-\sum_{i=1}^{n}\beta_i-T_c\\&\geqslant\sum_{i=1}^{n}t_i\end{aligned}\tag{8}$$

4 时间约束性验证

4.1 可调度验证方法

根据输入、输出、应用调度变迁的可调度性条件，对并发系统的应用并发数量与其时间约束特征进行分析。假设系统的周期性应用数为 n，计算机性能度量修正参数为 t_{arr}，以安全计算机实验平台单核 1GHz 主频的处理器性能为基准，应用逻辑运行时间基本在 1~10 ms 范围，因此可取其最大值 t_{arr}=10 ms 作为性能指标。

假定输入输出调度器均基于先到先服务策略，由文献[15]可知输入输出排队延时与并发应用数 n 之间存在关系 $\sum_{i=1}^{n}\alpha_i\propto(n^2),\sum_{i=1}^{n}\beta_i\propto(n^2)$，则输入输出排队延时 T_s 为

$$T_s=\sum_{i=1}^{n}\alpha_i=\sum_{i=1}^{n}\beta_i=t_{arr}n^2\tag{9}$$

根据实时操作系统调度策略，由于各应用具有相同优先级，采用 Round-Roin 调度（也称轮询调度），则 $t_d\propto(n)$，由式(2)可得

$$g(n)=t_d=\sum_{i=1}^{n}t_i=t_{arr}n\tag{10}$$

其中，$g(n)$ 为 n 个应用并行情况下，最长可能变迁延时。

设关于变量 n 的可触发区间函数为 T(n)，表示最早可能触发开始到最晚可能触发结束的时间长度，则有

$$f(n)=T_{\text{end}}^{l}(t_n)-T_{\text{start}}^{f}(t_n)\tag{11}$$

由 TPN 可调度性和定义 1 可知，$f(n)-g(n)\geqslant0$ 表示该变迁具有可调度性，否则不具有可调度性。并可用 $R(n)=f(n)-g(n)$ 表示 n 个应用并发执行情况下该变迁的可调度时间范围。$R(n)$ 值越大，说明调度范围越大，系统的时间冗余度越高，安全性也越高，但是资源利用率越低。

首先分析计算机性能参数 t_{arr} 与并发系统的应用数 n 之间关系。由于 CBTC 系统采用无线（如 WLAN）和有线（如光纤通信）通信组网方式实现各个子系统的协同控制，由文献[16-17]可知，其通信延时在 40~50 ms，因此可设外部通信延时 T_c=50 ms。虽然外部通信延时与列车速度等现实因素有一定的关系，但要保证列车安全运营，无线基站的布置满足列车运营需求即可，所以本文没有重

点阐述列车速度等因素对通信传输速率的影响。CBTC 系统中安全计算机控制周期时间为 200 ms，其时间约束区间为 0~200 ms。则一个周期内可调度时间范围为

$$\begin{aligned} R(n) &= f(n) - g(n) \\ &= 3(\min\{t_{\max}(t_i)\} - \max\{t_{\min}(t_i)\}) \\ &\quad - 2T_c - \sum_{i=1}^{n}\alpha_i - \sum_{i=1}^{n}\beta_i - t_d \\ &= 500 - 2t_{arr}n^2 - t_{arr}n \end{aligned} \tag{12}$$

令 t_{arr}={10, 1, 0.1}，表示不同计算性能的安全计算机，绘制不同计算性能下，$R(n)$ 与应用数 n 的关系图，如图 6 所示。当 t_{arr}=10ms 时，在满足现有的系统应用时间约束的条件下，可最大支持的并发应用数 $n=4$，而目前 CBTC 系统中安全计算机实际只运行一个应用功能，其资源利用率 η 只有 25%。而当计算机性能提高到 t_{arr}=0.1 ms 时，并发应用数最大可达 $n=49$，表明计算机性能的提升会为安全计算机提供更大的设计冗余空间，并可进一步优化系统性能。同时，由图 6 可知，随着 n 的增大，时间冗余度也相应降低，为保证系统安全可靠运行，在系统设计时需要考虑一定的时间可调度冗余性。

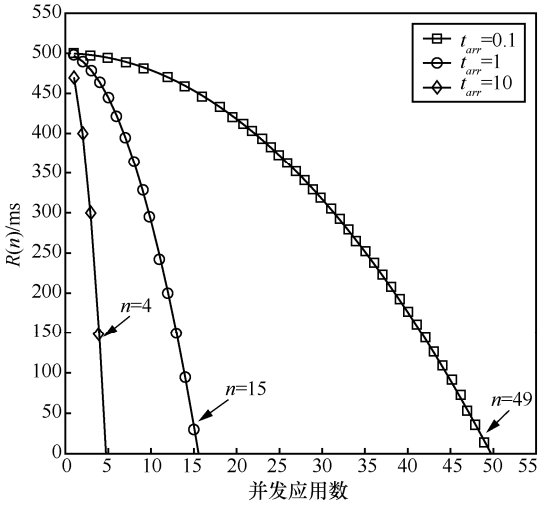


图 6 不同计算计算性能下 $R(n)$ 与 n 的关系

上述分析基于每个应用均与外部子系统应用进行通信的假设，而实际在车车通信系统中，各个控制功能模块之间的交互变成了计算机内部线程的交互，数据通信延时将会极大地降低，从而系统性能能得到进一步优化，安全性也能得到进一步提升。假设计算机性能参数 t_{arr}=10 ms，则可调度时间范围为

$$\begin{aligned} R(n) &= f(n) - g(n) \\ &= 3(\min\{t_{\max}(t_i)\} - \max\{t_{\min}(t_i)\}) - \\ &\quad 2T_c - \sum_{i=1}^{n}\alpha_i - \sum_{i=1}^{n}\beta_i - t_d \\ &= 600 - 2T_c - 20n^2 - 10t_{arr} \end{aligned} \tag{13}$$

则根据式（13）可绘制不同通信延时下，$R(n)$ 与应用数 n 的关系图，如图 7 所示。通信延时减小，系统的时间冗余度能够得到提高，有利于提高系统的安全性。

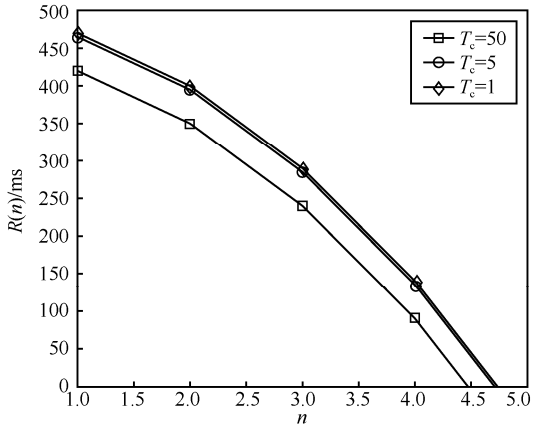


图 7　不同通信延时下 $R(n)$ 与 n 的关系

根据上述分析可知并行应用数与其可调度区间关系。可调度区间代表时间约束的冗余度，时间冗余度越高，说明系统容错能力越强，系统安全性越高，但系统性能利用率越低。通过 TPN 建模可以对时间约束冗余度 $R(n)$ 与应用数 n 建立联系，从而定量地确定系统并发设计要求。通过对安全计算机性能以及通信延时这 2 个方面进行分析，表明安全计算机性能的提升及通信延时的降低能够增加可调度区间，即满足软件综合化的时间约束关系，且能进一步优化时间约束参数，同时也表明在当前硬件条件下，车载安全计算机可满足多个周期应用调度需求。另外，TPN 模型能准确描述系统时间约束关系和影响时间特性的主要因素，为进一步优化时间参数提供理论依据。

4.2　时间约束特性实例设计

为了验证基于 TPN 的时间约束性分析评估方法在评估安全计算机性能及周期性应用并发数关系上的有效性，本文在车载 2 乘 2 取 2 安全计算机硬件设备条件下，测试 3 个周期性应用的时间运行关系，验证该安全计算机是否满足 3 个周期性应用

的时间约束性。限于安全性和可靠性方面考虑，该安全计算机平台的硬件采用已验证的单核主频 1 GHz 的 PowerPC 系列的处理器。同时分别设计 3 个周期性应用 A/B/C，其周期分别为 35 ms、40 ms、50 ms。通过记录每个应用的周期开始和结束时间，以及应用执行的开始和结束时间来确定多应用并发情况下是否满足周期性时间约束。

首先说明面向车车通信的安全计算机与目前 CBTC 系统中安全计算机的主要差别。CBTC 系统主要由分散的子系统 ZC 和 CBI 完成控制功能，而车车通信系统将这些功能集中到车载系统。CBTC 系统中的车载安全计算机只执行车载列车超速防护（ATP, automatic train protection）功能，而车车通信系统中，车载安全计算机除了实现车载 ATP 安全关键功能外，还将整合 CBTC 系统中 ZC 和 CBI 的 ATP 安全苛求功能，如轨旁设备控制命令下达、车门管理等，如图 8 所示。功能的整合必然使得车载安全计算机成为复杂的并发系统，而车载计算机是典型的安全关键实时控制系统，不仅需要保证处理逻辑功能的正确性，还必须具有严格的周期性特征，即必须在严格限定的时间内执行相关命令，否则可能造成严重的安全事故。

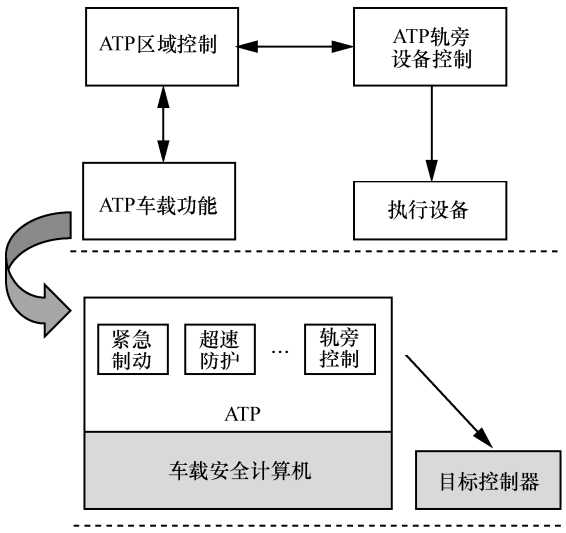


图 8　车车通信车载安全计算机结构

4.3　调度时刻特性分析

根据上述实例设计，获得周期性应用的运行时间特性数据，依据时间变量关系将其整理成离散点图，如图 9 所示。其中，3 个周期性应用分别为应用 A、应用 B 和应用 C，横轴表示应用在系统调度中的运行时刻表，每个片段表示应用在计算机中被选中调度的实际运行时长。案例设计中，记录应用在其每个控制周期内的运算开始和结束时间点，表示周期内的有效执行时间。

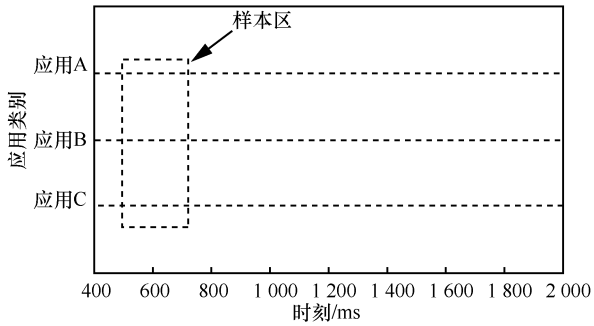


图 9　各应用周期调度实际运行时刻

由图 9 可知，安全计算机安全苛求应用实际运行时间是离散化的，而非连续的。这与宏观上观察的安全计算机应用存在本质区别。在周期调度策略中，就安全计算机安全关键应用对资源的竞争力而言，其逻辑不可能完全保证自身的有效运行时间，必须依靠安全计算机平台的调度策略来保证。

取局部样本分析，如图 10 所示。周期性调度策略会根据每个应用声明的调度周期，在时间约束内灵活调度多个应用安全并行。从图 10 的实际测试结果可知，在目前软硬件条件下，安全计算机平台能满足 3 个应用周期性调度。

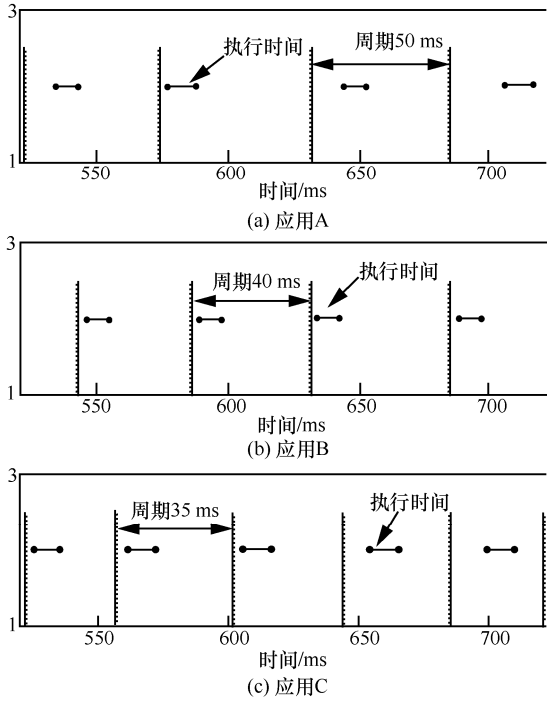


图 10　各应用局部时间特性

图 10 中每个应用都能在其周期约束内完成运行逻辑。每个周期内应用实际执行时间占整个周期时间的比率为 10%~30%，符合前面分析结果。同时各个阶段的有效运算时长比率存在波动，图 10 中应用的执行时间在每个周期内不尽相同，但执行时长都约束在 10%~30%比率内。造成该现象的原因是多应用并行存在资源竞争，导致任务阻塞，从而增加处理延时。这种情况符合实时操作系统多任务调度特性，也是多应用并行影响原有系统的时间约束性的主要表现。

5　结束语

针对 CBTC 系统的发展趋势，研究了面向车车通信的车载安全计算机中多个周期性应用并发能否满足时间约束性要求的问题。列车运行控制系统的功能整合，导致多个安全关键的周期性应用在车载安全计算机上并发运行。然而限于目前车载安全计算机的硬件性能，需要对安全计算机能否满足多周期性应用的时间约束性进行验证和评估。本文以目前的安全计算机硬件结构和性能入手，首次采用 TPN 分析多个周期性应用的并行时间特性。通过建立 TPN 模型，分析了可调度性区间，结果表明目前使用的 2 乘 2 取 2 车载安全计算机性能满足 3 个周期性应用的时间约束性要求。同时，论证了在满足各周期性应用时间约束条件下，计算机性能、通信延时与可支持的周期性应用数之间的关系。

基于车车通信的列车运行控制是未来城市轨道交通列车运行控制的发展方向，而车载安全计算机必然也会变得更加复杂化和多功能化。因此，研究车载安全计算机支持多个周期性应用的关键技术具有实际意义。在将来的研究中，我们将考虑更多现实环境因素，并对 TPN 加以改进，应用于合适的应用场景。

参考文献：

[1] 郑升, 曹源, 张玉琢, 等. 通用型列控系统的安全计算机设计与验证[J]. 北京交通大学学报, 2014, 38(3): 128-134.
ZHENG S, CAO Y, ZHANG Y Z, et al. Design and verification of general train control system's safety computer[J]. Journal of Beijing Jiaotong University, 2014, 38(3): 128-134.

[2] 徐纪康. 基于车车通信的新型 CBTC 系统分析[J]. 铁道通信信号, 2014, 50(6): 78-80.
XU J K. Analysis of a new CBTC system based on train-train communication[J]. Railway Signalling & Communication, 2014, 50(6): 78-80.

[3] 梁靓, 曹源, 马连川, 等. 安全计算机通信管理机制的形式化验证与实现[J]. 通信学报, 2016, 37(11): 196-202.
LIANG L, CAO Y, MA L C. Formal verification and implementation of safety computer communication management mechanism[J]. Journal on Communications, 2016, 37(11): 196-202.

[4] 白晓颖, 汪明, 陆皓, 等. 实时系统时间约束验证[J]. 清华大学学报(自然科学版), 2012, 52(9): 1286-1292.
BAI X Y, WANG M, LU H, et al. Verifying timing constraints in real-time systems[J]. Journal of Tsinghua University, 2012, 52(9): 1286-1292.

[5] TSAI J J P, YANG S J, CHANG Y H. Timing constraint Petri nets and their application to schedulability analysis of real-time system specifications[J]. IEEE Transactions on Software Engineering, 1995, 21(1): 32-49.

[6] XU D X, HE X D, DENG Y. Compositional schedulability analysis of real-time systems using time Petri nets[J]. IEEE Transactions on Software Engineering, 2002, 28(10): 984-996.

[7] SINGH L K, RAJPUT H. Dependability analysis of safety critical real-time systems by using Petri nets[J]. IEEE Transactions on Control Systems Technology, 2017, 26(2): 415-426.

[8] BASILE F, CABASINO M P, SEATZU C. Diagnosability analysis of labeled time Petri net systems[J]. IEEE Transactions on Automatic Control, 2017, 62(3): 1384-1396.

[9] 宋巍, 窦万春, 刘茜萍. 时间约束 Petri 网及其可调度性分析与验证[J]. 软件学报, 2007, 18(1): 11-21.
SONG W, DOU W C, LIU X P. Timing constraint Petri nets and their schedulability analysis and verification[J]. Journal of Software, 2007, 18(1): 11-21.

[10] 宋玉银, 褚秀萍, 蔡复之. 基于时间 Petri 网的实时并行设计过程建模研究[J]. 计算机集成制造系统, 1999, 5(6): 17-22.
SONG Y Y, CHU X P, CAI F Z. Research of the process modeling of real-time concurrent design based on time Petri net[J]. Computer Integrated Manufacturing Systems, 1999, 5(6): 17-22.

[11] 叶阳东, 杜彦华, 高军伟, 等. 时间 Petri 网的时间知识推理算法及在铁路智能运输系统中的应用[J]. 铁道学报, 2002, 24(5): 5-10.
YE Y D, DU Y H, GAO J W, et al. A temporal knowledge reasoning algorithm using time Petri nets and its applications in railway itelligent transportation system[J]. Journal of the China Railway Society, 2002, 24(5): 5-10.

[12] 叶阳东, 王娟, 贾利民. 基于模糊时间 Petri 网的列车运行时间不确定性问题的处理[J]. 铁道学报, 2005, 27(1): 6-13.
YE Y D, WANG J, JIA L M. Processing of temporal uncertainty of train operation based on fuzzy time Petri nets[J]. Journal of the China Railway Society, 2005, 27(1): 6-13.

[13] CAO Y, MA W G, MA L C. Local fractional functional method for solving diffusion equations on cantor sets[J]. Abstract and Applied

Analysis, 2014: 1-6.

[14] CAO Y, MA L C, MA W G. Mobile target tracking based on hybrid open-loop monocular vision motion control strategy[J]. Discrete Dynamics in Nature and Society, 2015: 1-10.

[15] HYYTIÄ E, AALTO S. On Round-Robin routing with FCFS and LCFS scheduling[J]. Performance Evaluation, 2016, 97: 83-103.

[16] CAO Y, MA L C, XIAO S, et al. Standard Analysis for Transfer Delay in CTCS-3[J] Chinese Journal of Electronics, 2017, 26(5): 1057-1063.

[17] 朱力, 宁滨. 基于IEEE 802.11g标准的CBTC车地通信系统设计[J]. 中国铁道科学, 2010, 31(5): 119-124.
ZHU L, NING B. The design of the CBTC train-ground communication system based on IEEE 802.11g standard[J]. China Railway Science, 2010, 31(5): 119-124.

[作者简介]

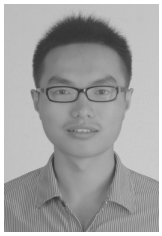
高莺（1985−），女，山东烟台人，中国铁道科学研究院博士生、工程师，主要研究方向为安全分析。

曹源（1982−），男，回族，河南开封人，博士，北京交通大学副教授、博士生导师，主要研究方向为通信的列车控制技术。

孙永奎（1993−），男，河南商丘人，北京交通大学博士生，主要研究方向为铁路信号系统故障诊断。

马连川（1970−），男，河北唐山人，北京交通大学副教授，主要研究方向为列控系统安全计算机技术。

洪春华（1990−），男，福建福州人，北京交通大学硕士生，主要研究方向为列控系统安全计算机技术及形式化验证。



张玉琢（1990−），男，河南信阳人，北京交通大学博士生，主要研究方向为 Petri 网理论及在列车运行控制系统的应用。