# 基于Event-B的分区操作系统内核模型及正确性保障

赵永望
zhaoyw@buaa.edu.cn
北京航空航天大学 计算机学院

2014年1月

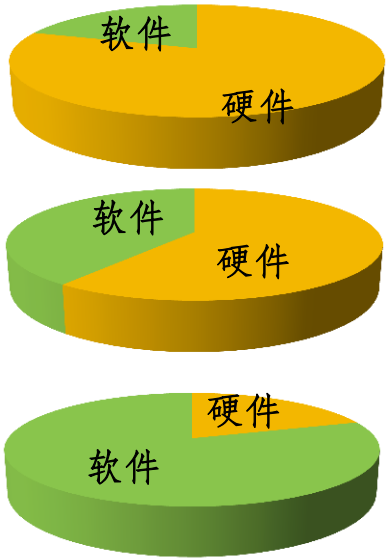
# 报告提纲

- 1. 什么是分区内核
- 2. 分区内核验证的研究现状
- 3. 总体方案
- 4. 分区内核模型
- 5. 隔离内核正确性保障方法
- 6. 小结

# 机载软件的地位和作用

- 以航电系统为例

| 飞机 | 型号 | 航电系统功能 | |
|---|---|---|---|
| | | 硬件(%) | 软件(%) |
| 第二代<br>60年代末 | F-111 | 80 | 20 |
| 第三代<br>70年代末 | F-16 | 60 | 40 |
| 第四代<br>90年代末<br>/21世纪 | F-22<br>F-35 | 20<br>15 | 80<br>85 |




| 飞机型号 | 代码行数(万行) |
|---|---|
| 飞豹战斗机 | 150 |
| F22 | 180(Ada) |
| 波音 | 400 |
| F35 | 1000 |

航空电子系统逐渐成为“软件密集型”系统
80%的航空电子功能由软件实现




3

# 综合化航电和机载软件


SWaP需求

**SWaP: Size, Weight, and Power**

独立的专用计算机

独立的管理软件

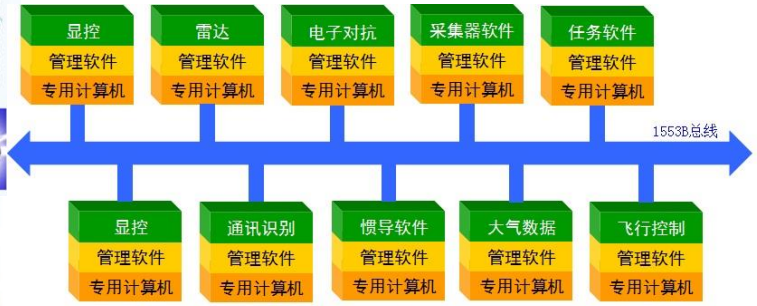
任务总线为通信与控制方式

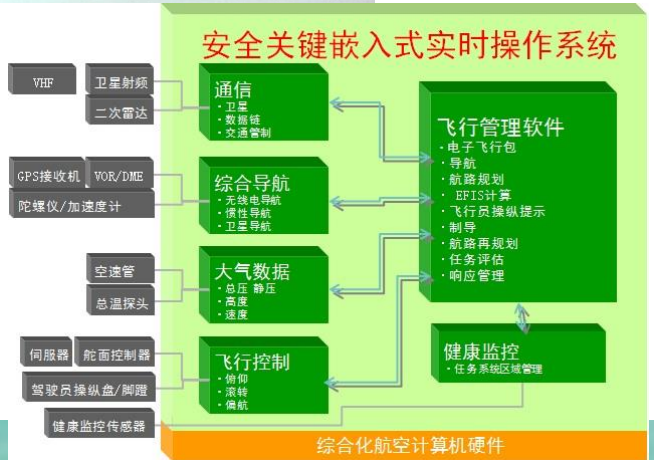


高度综合化的计算机硬件

综合化环境下的任务处理软件

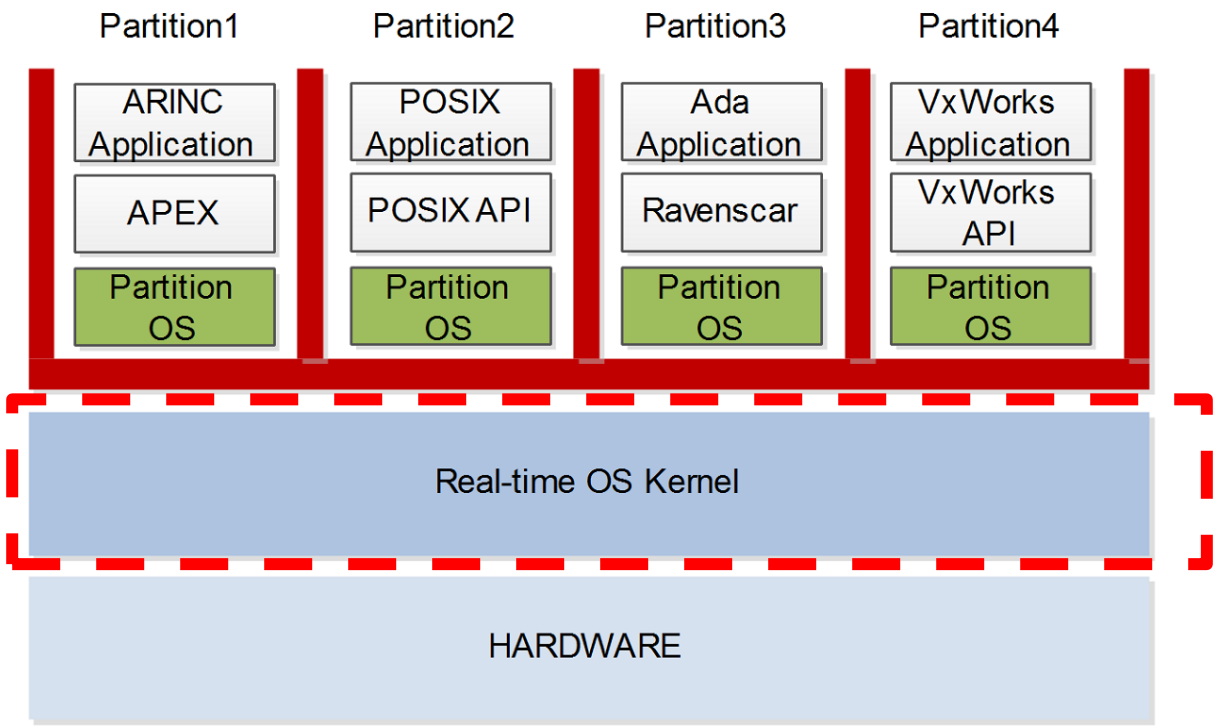
安全关键的嵌入式实时操作系统成为核心



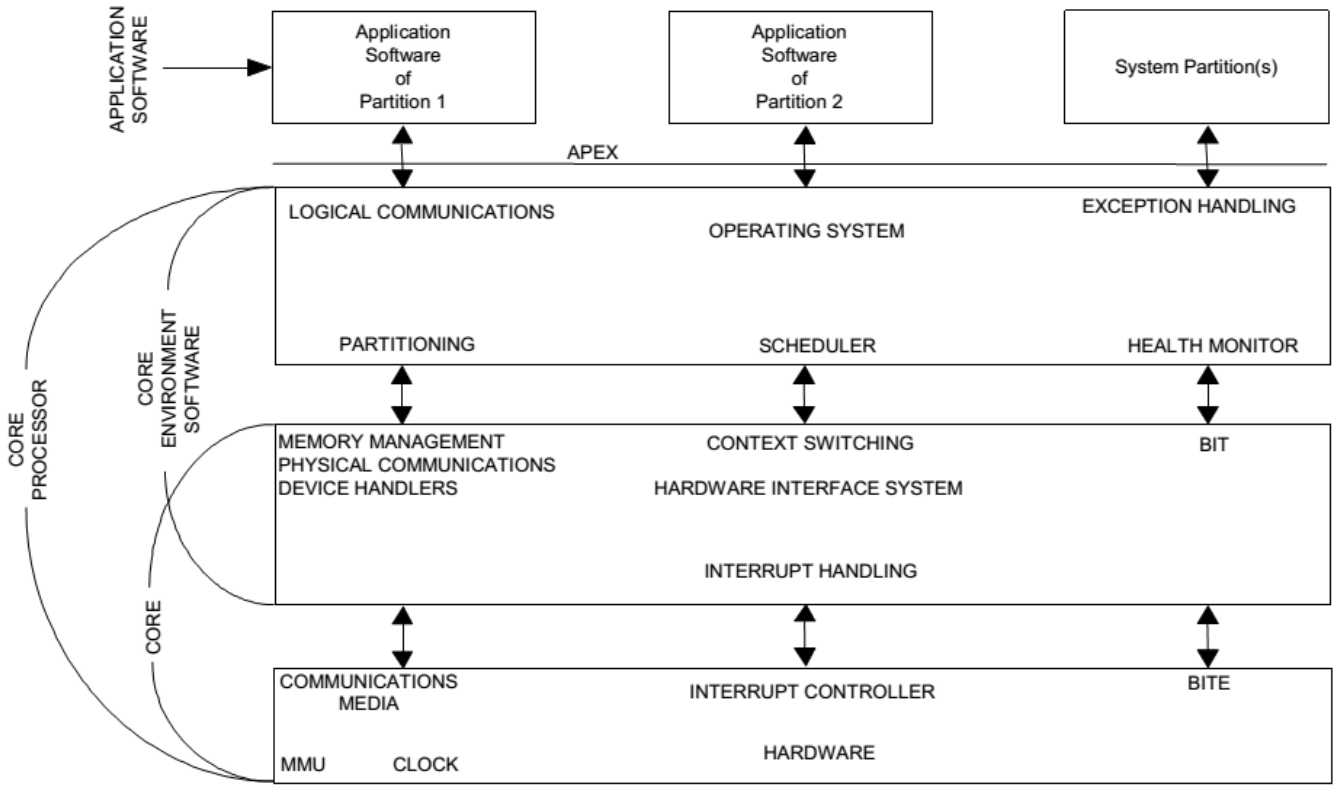
# 分区实时操作系统内核

- 在综合化航电的架构下，实时操作系统支持分区




- 空间隔离
- 时态隔离
- 故障隔离
- 信息流安全性

# ARINC653内核功能




核心服务：

1. Partition Management
2. Process Management
3. Time Management
4. Memory Management
5. Interpartition Communicatio
6. Intrapartition Communicatio
7. Health Monitoring

# 形式验证需求

- 机载软件适航认证DO-178C要求采用形式化方法
- CC对安全关键软件的要求

国际信息技术安全评估通用标准
Common Criteria
ISO/IEC 15408

| CC级别 | 需　求 | 功能规约 | 高层设计 | 低层设计 | 代码实现 |
|---|---|---|---|---|---|
| EAL1 | 非形式化 | 非形式化 | 非形式化 | 非形式化 | 非形式化 |
| EAL2 | 非形式化 | 非形式化 | 非形式化 | 非形式化 | 非形式化 |
| EAL3 | 非形式化 | 非形式化 | 非形式化 | 非形式化 | 非形式化 |
| EAL4 | 非形式化 | 非形式化 | 非形式化 | 非形式化 | 非形式化 |
| EAL5 | 形式化 | 部分形式化 | 部分形式化 | 非形式化 | 非形式化 |
| EAL6 | 形式化 | 部分形式化 | 部分形式化 | 部分形式化 | 非形式化 |
| EAL7 | 形式化 | 形式化 | 形式化 | 部分形式化 | 非形式化 |
| 完全验证 | 形式化 | 形式化 | 形式化 | 形式化 | 形式化 |

EAL1—功能测试
EAL2—结构测试
EAL3—系统地测试和检查
EAL4—系统地设计、测试和复查
EAL5—部分形式化设计和测试
EAL6—部分形式化验证的设计和测试
EAL7—形式化验证的设计和测试

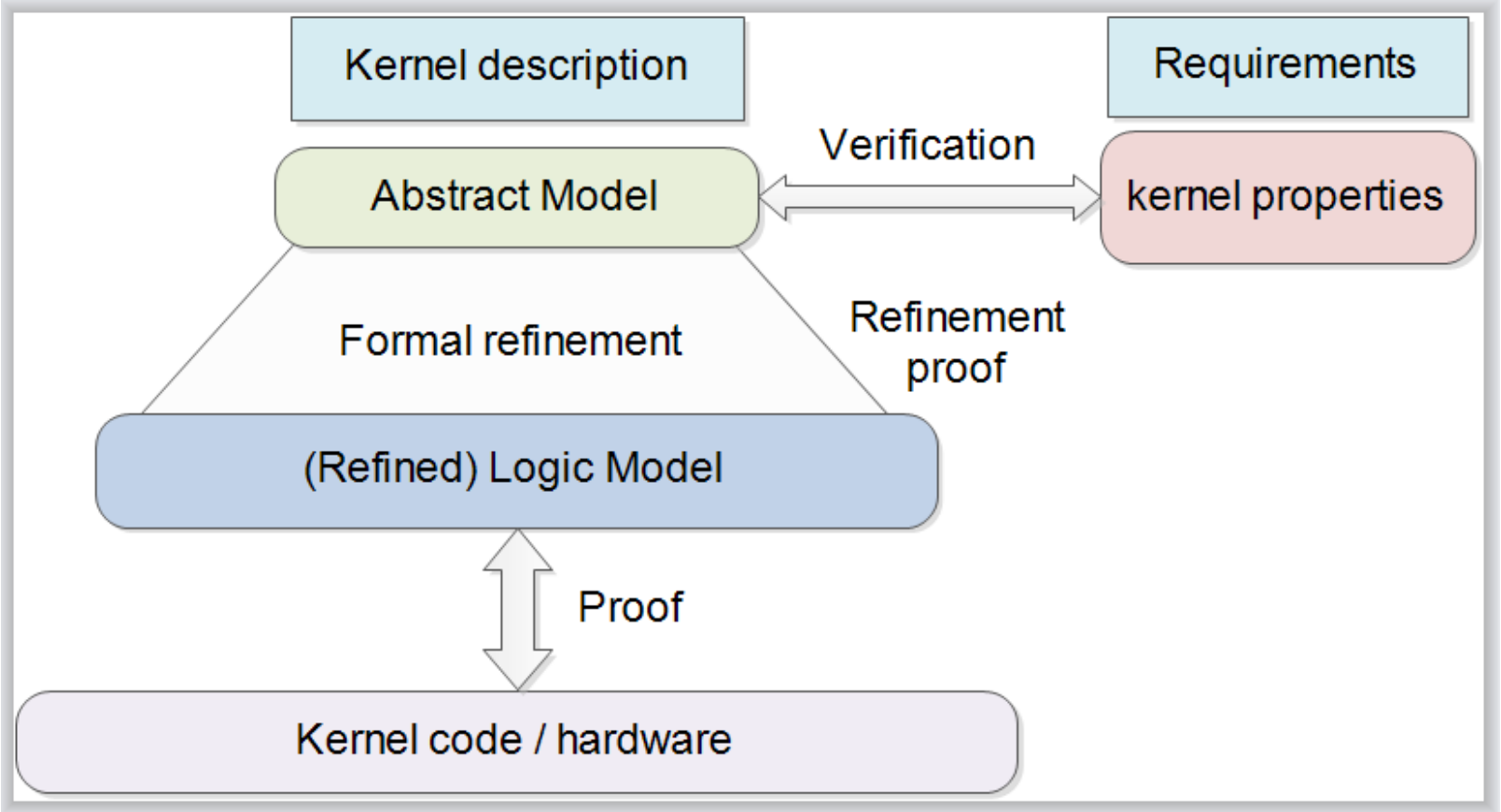
# 形式验证需求

- **提高可靠性、降低安全认证成本**
  - **“Crash-Proof Code”**
    - **one of the 10 breakthrough technologies in 2011 by “MIT Technology Review”**
  - **澳大利亚国家信息通信技术研究中心**
  - **对L4内核进行形式验证**
    - L4内核：构造OS的基本机制，包括线程、消息传递、中断、虚拟内存、访问控制等
    - 内核包含8700行C代码（其中1200行为内核启动代码），600多行ARM汇编代码
  - **20万行手写Isabelle/HOL证明代码，形式验证工作量25人年**
  - **共发现460多个Bug(C代码中160多个，设计中150个，规约中150个)，而在测试中只发现16个Bug**
  - **完全形式化验证成本：600万美元**
    - 走CC EAL6级认证，10000美元/行代码成本计算，需8700万美元
    - 而且CC EAL6认证比完全形式化验证的软件可靠性确保度低

# 分区内核验证的现状

1. Partitioning Kernel Protection Profile (PKPP)
   - 2003年，洛克希德马丁，空军研究实验室，OpenGroup草案
2. Separation Kernel Protection Profile (PKPP)
   - 2007年，美国国家安全局正式颁布
3. 美国国防部：a Mathematically Analyzed Separation Kernel (MASK) 项目
4. Rockwell Collins公司的GWV安全策略及信息流安全验证
5. 美国海军研究中心ED separation kernel形式验证
6. 英国约克大学Grand Challenge Verified Software项目下Separation Kernel形式模型与验证
7. 美国Critical Software公司Partitioning Kernel的B模型及验证
8. 德国Verisoft XT项目对PikeOS的Separation Kernel验证
9. 澳大利亚NICTA：seL4作为Separation Kernel，验证安全性

# 总体方案

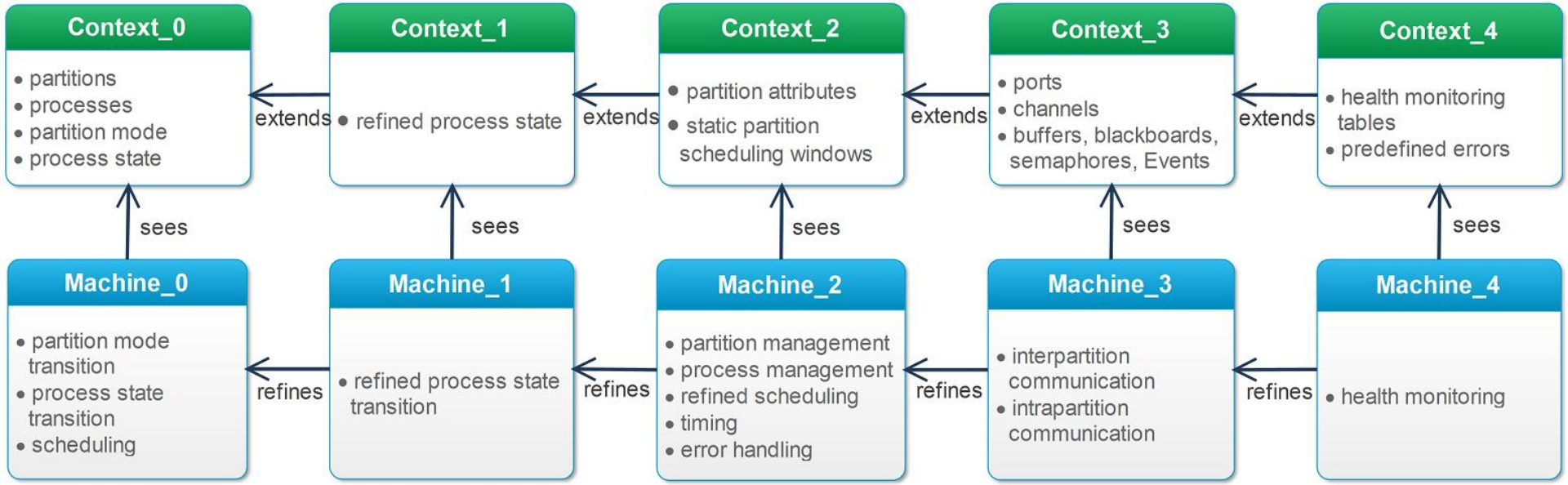



Refinement及证明

B方法：refinement及proof obligation

Proof obligation的正确性：定理证明器Coq

# 分区内核的Event-B模型



# 分区与进程

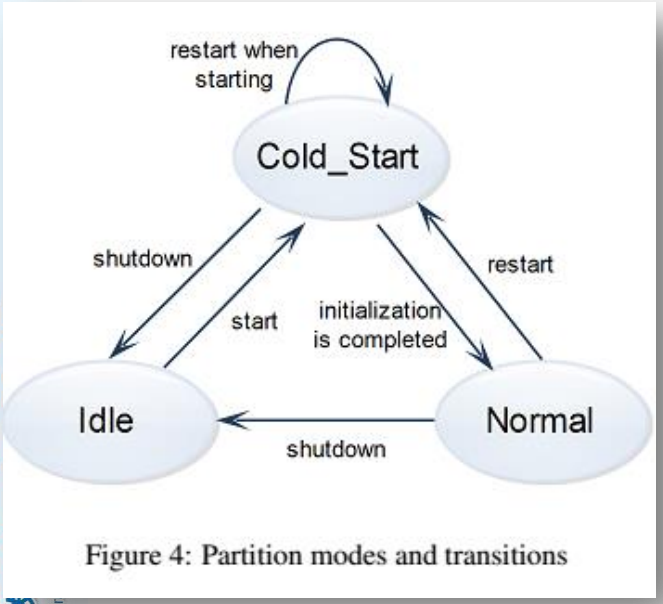



Figure 4: Partition modes and transitions

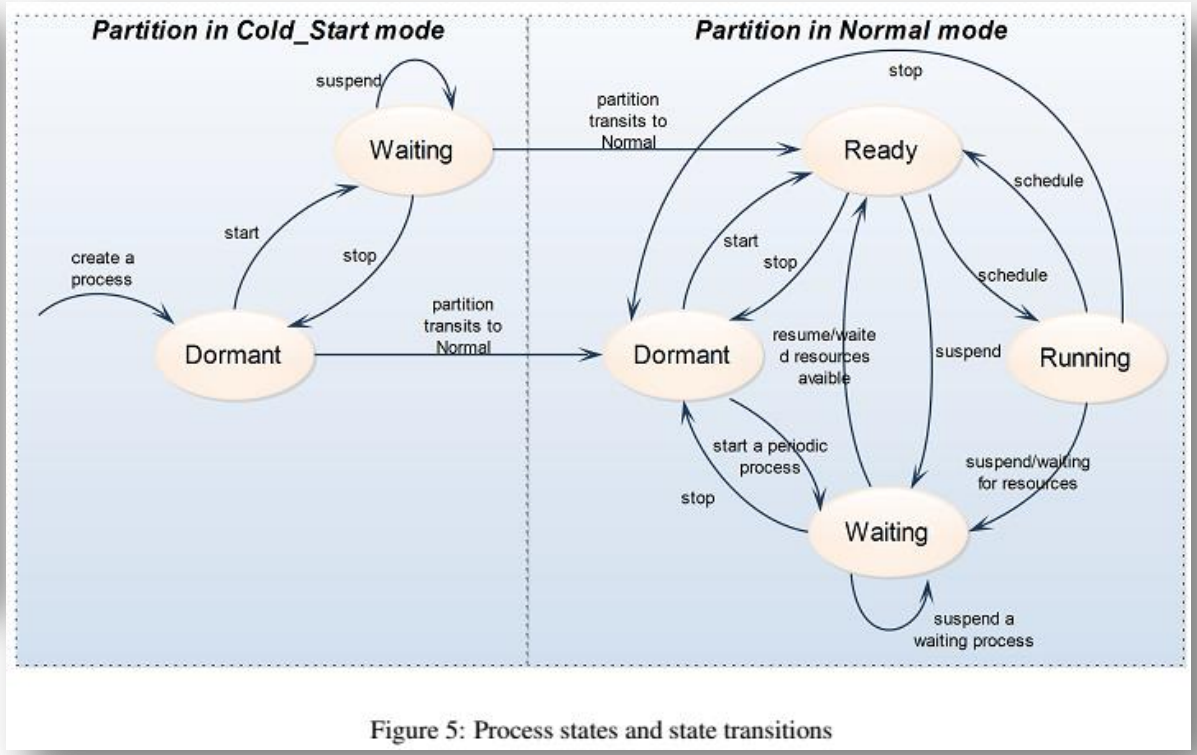



Figure 5: Process states and state transitions

# 两级调度

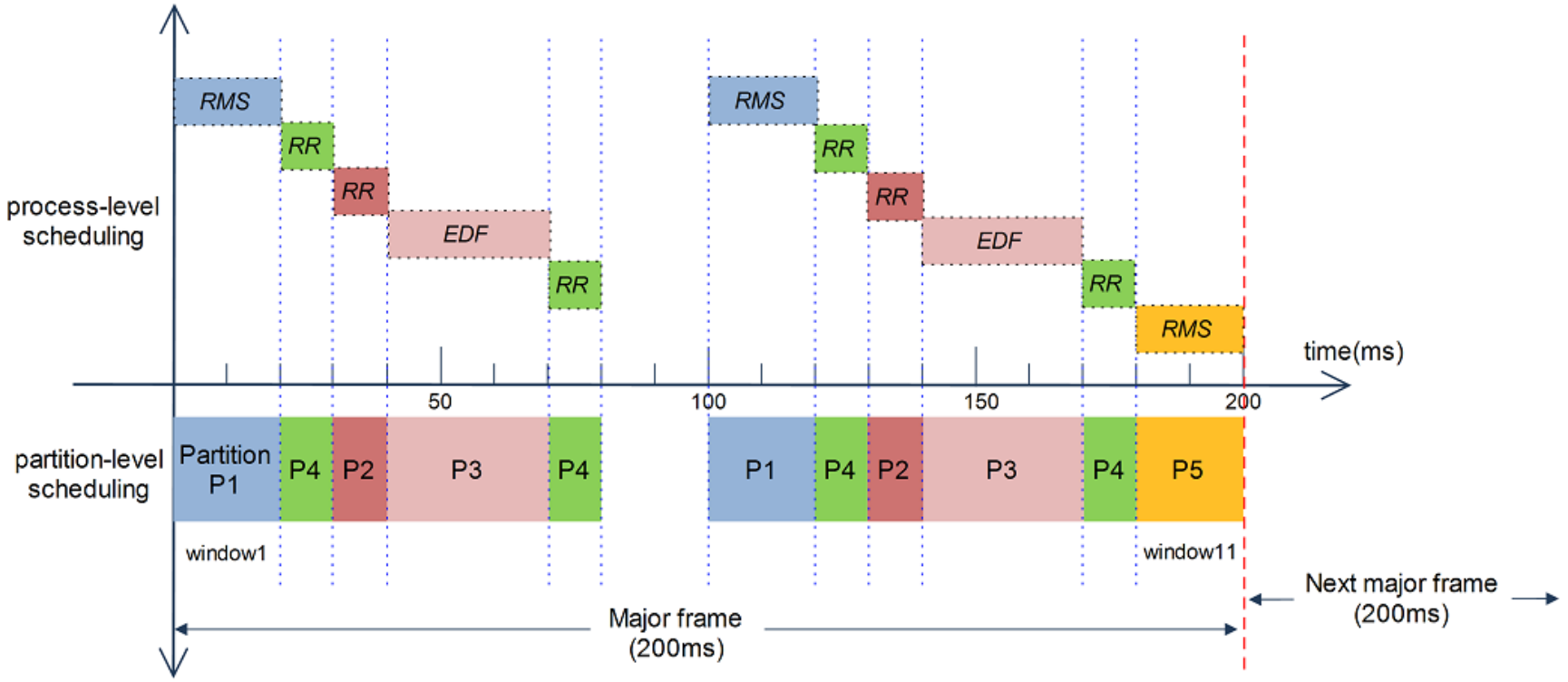



Figure 6: Two-level scheduling

# 分区通信

- 分区间：队列端口和采样端口通信
- 分区内：buffer、blackboard、semaphore、event

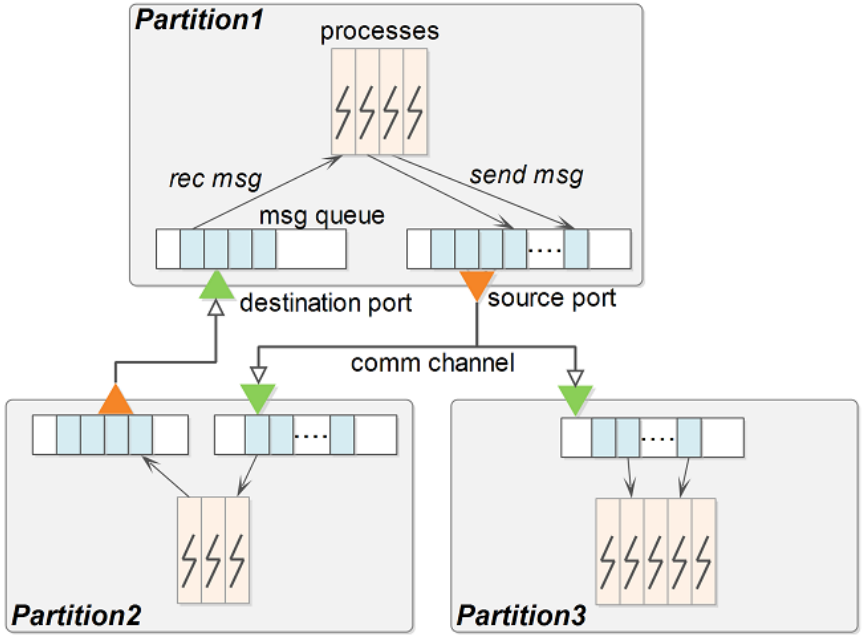



Figure 7: Interpartition communication (queuing mode)

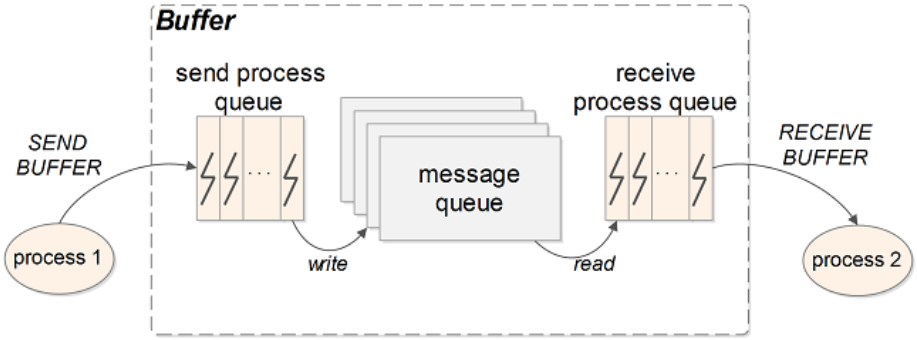



Figure 8: Intrapartition communication (buffer)

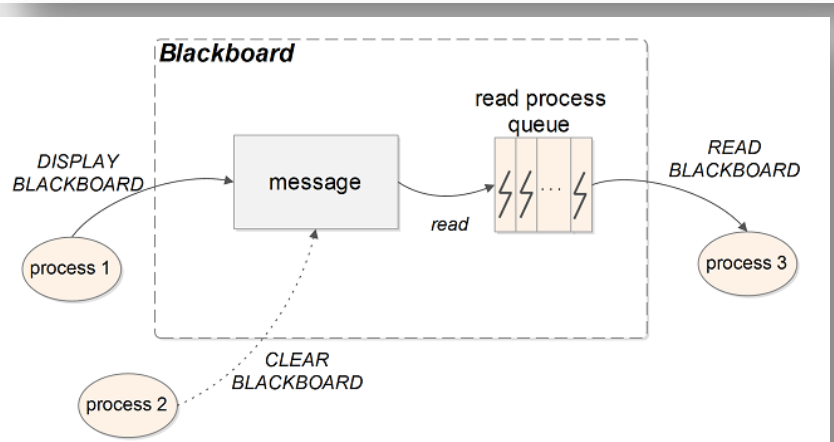



Figure 9: Intrapartition communication (blackboard)

# 内核建模的完成情况

Table 3: Statistics of Event-B machines

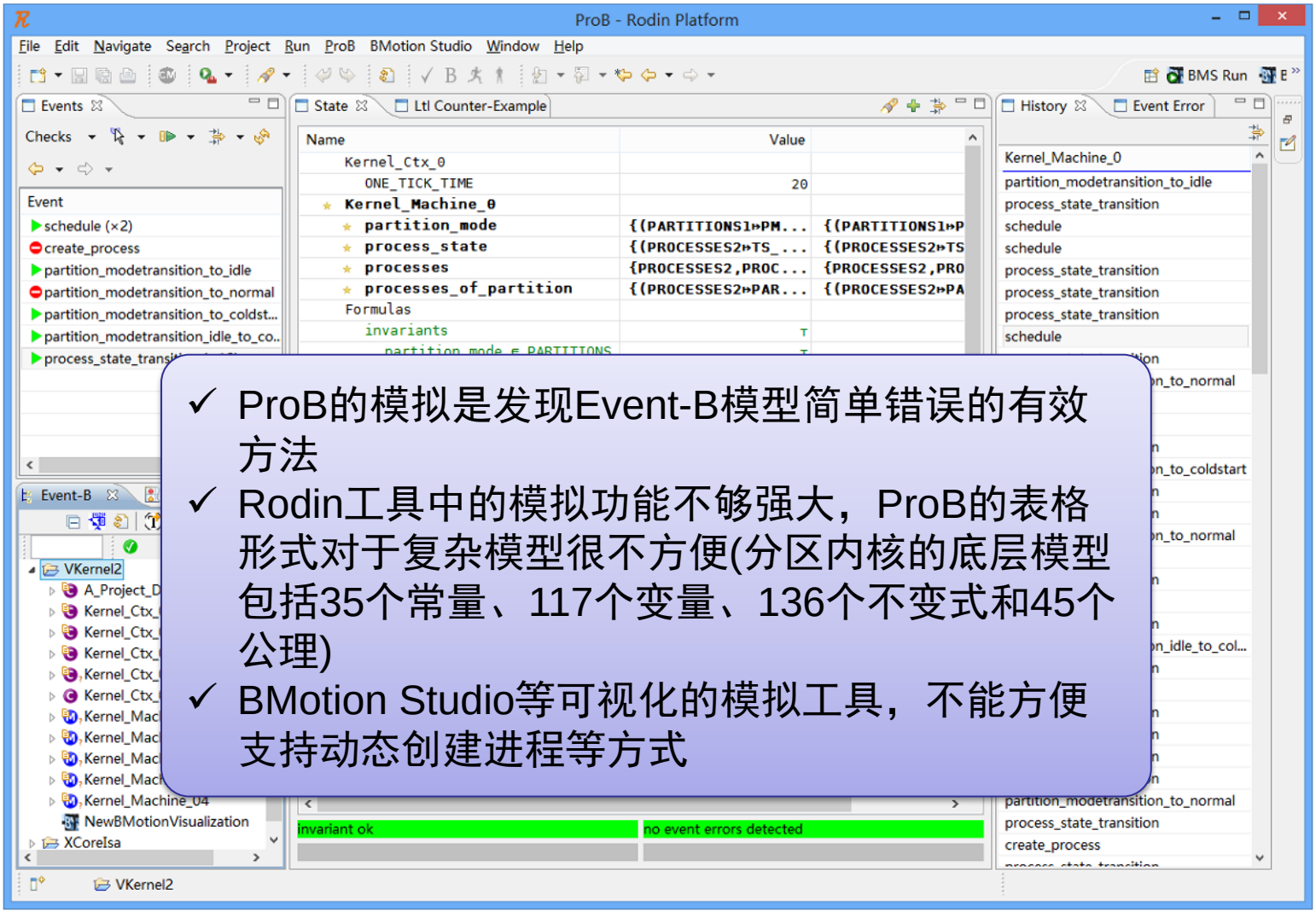
| Machine | LOC | Events | Invariants |
|---|---|---|---|
| Machine_0 | 168 | 8 | 11 |
| Machine_1 | 108 | 8 | 5 |
| Machine_2 | 619 | 36 | 31 |
| Machine_3 | 776 | 76 | 25 |
| Machine_4 | 421 | 86 | 5 |
| Total | 2092 | 214 | 77 |

Table 4: Statistics of ARINC 653 services and models

| ARINC 653 services | Amount of services | Modeled | Events |
|---|---|---|---|
| Partition Management | 2 | 2 | 8 |
| Process Management | 14 | 14 | 20 |
| Time Management | 4 | 4 | 4 |
| Memory Management | 0 | 0 | 0 |
| Interpartition Communication | 10 | 8 | 14 |
| Intrapartition Communication | 22 | 18 | 27 |
| Health Monitoring | 4 | 4 | 10 |
| Total | 56 | 50 | 83 |

# 正确性保障

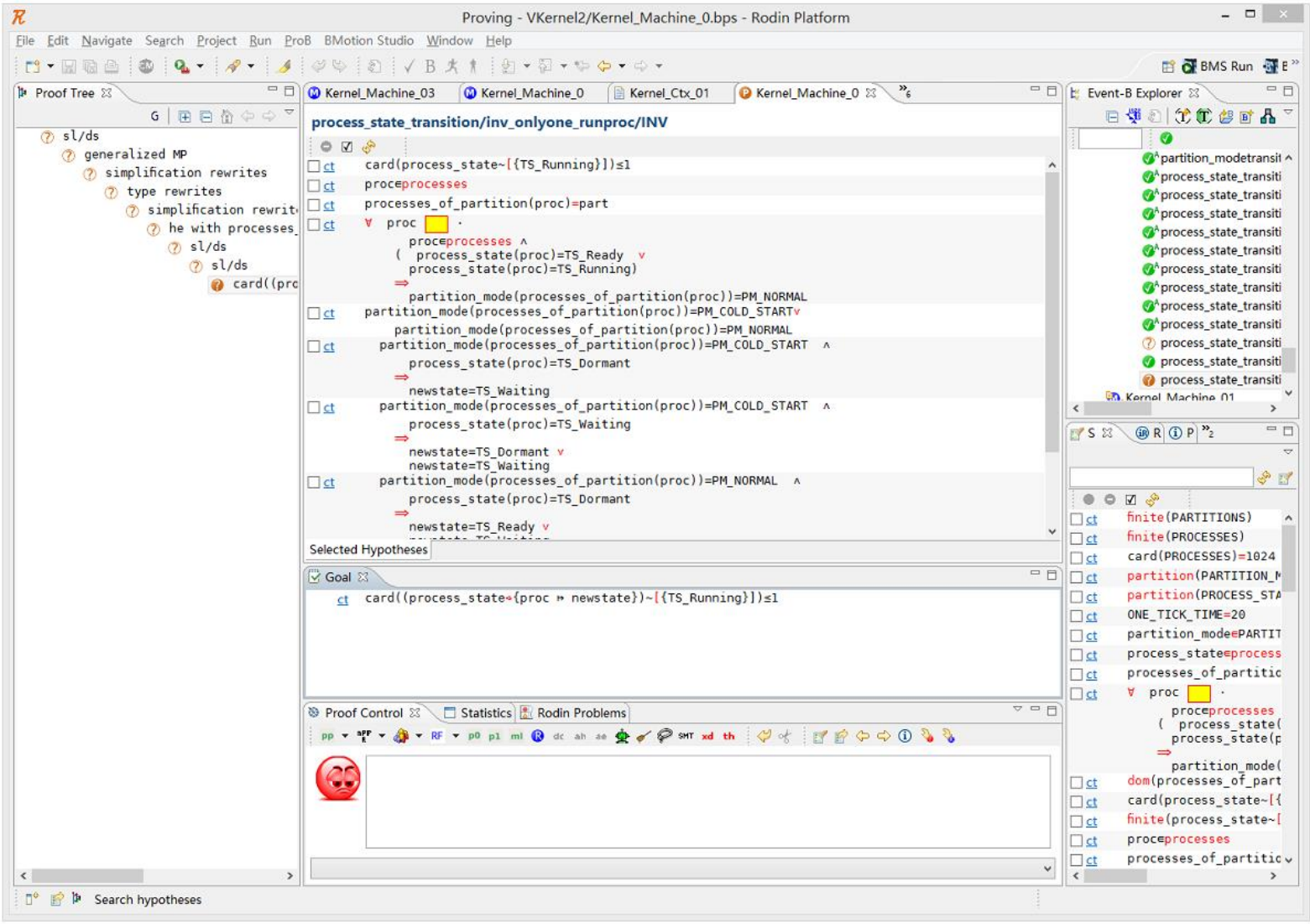
- **Simulation in Rodin/ProB plugin**




- ✓ ProB的模拟是发现Event-B模型简单错误的有效方法
- ✓ Rodin工具中的模拟功能不够强大，ProB的表格形式对于复杂模型很不方便(分区内核的底层模型包括35个常量、117个变量、136个不变式和45个公理)
- ✓ BMotion Studio等可视化的模拟工具，不能方便支持动态创建进程等方式

# 正确性保障

- Theorem Proving



# 正确性保障

- **Theorem Proving**
  - **Rodin内置证明器不能自动证明的定理中，40%-50%可通过第三方证明器自动完成**

Table 5: Generated proof obligations and proving results

| Context/Machine | Proof obligation generated | Auto-proved | manual proved |
|---|---|---|---|
| Context_0 | 2 | 0 | 2 |
| Context_1 | 0 | 0 | 0 |
| Context_2 | 0 | 0 | 0 |
| Context_3 | 2 | 0 | 2 |
| Context_4 | 0 | 0 | 0 |
| Machine_0 | 84 | 62 | 22 |
| Machine_1 | 48 | 39 | 9 |
| Machine_2 | 350 | 202 | 148 |
| Machine_3 | 415 | 86 | 329 |
| Machine_4 | 487 | 103 | 384 |
| Total | 1388 | 492 | 896 |

# 结 论

- 本文的模型是公开资料中最完整的符合ARINC 653的分区内核模型
- 模型实现了ARINC653的完整功能和接口
- 采用Event-B进行分区内核建模，开发效率高、证明义务自动生成、证明的自动化程度高
- 一种分区内核实现的参考模型
  - 结合硬件模型后，可自动生成代码
  - 提供规约和性质，可用于验证已有的分区内核
  - 可提供分区内核认证的证据材料



# 谢谢！

# 请批评指正！