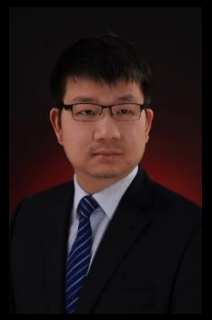
# 面向自动驾驶的安全关键系统资源管理与调度技术研究

黄凯

2023年8月12日

# 研究团队简介



**陈刚**

中山大学教授，博导，中山大学百人计划引进人才。德国慕尼黑工业大学博士。主要研究实时嵌入式系统、安全关键系统等领域

**谭宁**

中山大学副教授，博导，中山大学百人计划引进人才。法国CNRS博士。主要研究机器人系统的建模、设计、仿真、优化、规划与控制

**单云霄**

中山大学副教授。武汉大学博士。主要研究移动机器人、水面航行机器人的感知、规划和控制方法

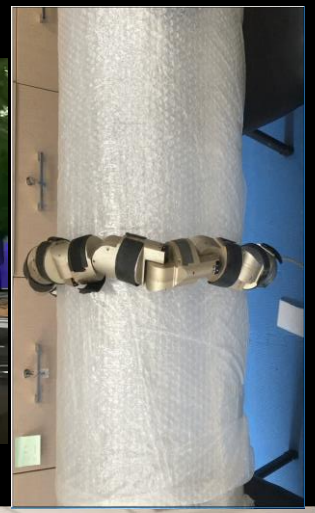
**黎卫兵**

中山大学副教授，中山大学百人计划引进人才。英国利兹大学博士。主要研究机器人运动学和动力学分析以及控制理论

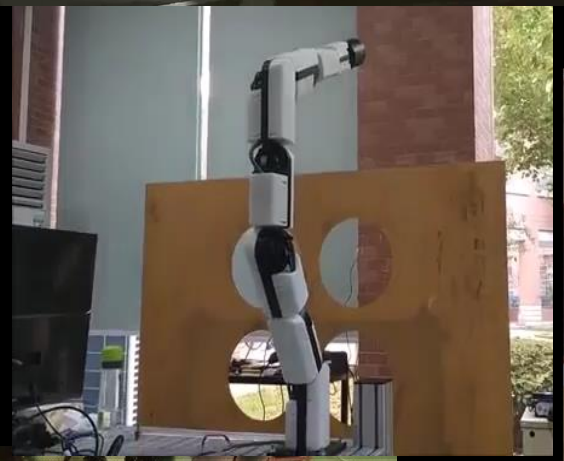
**赵帅**

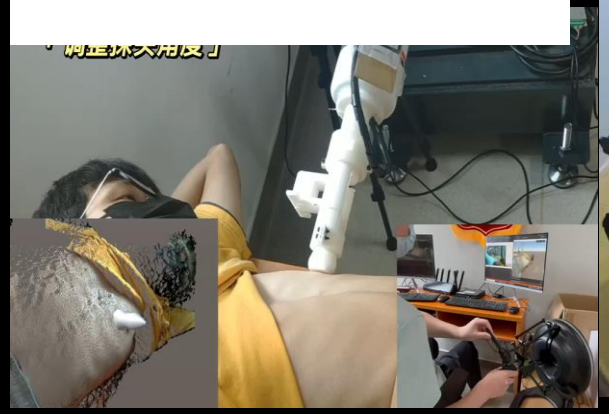
中山大学副教授，中山大学百人计划引进人才。英国约克大学博士。主要研究实时操作系统理论分析软硬件系统协同设计

# Our robots



Robustness Tests





# 内容提纲

- 冗余系统实现与自动驾驶场景下案例分析
- 自动驾驶中系统资源在线调度与循迹案例分析
- 总结与展望

# 内容提纲

- 冗余系统实现与自动驾驶场景下案例分析
- 自动驾驶中系统资源在线调度与循迹案例分析
- 总结与展望

# 一. 冗余系统实现与自动驾驶场景下案例分析

自动驾驶系统面临的问题与挑战：

（1）可靠性问题

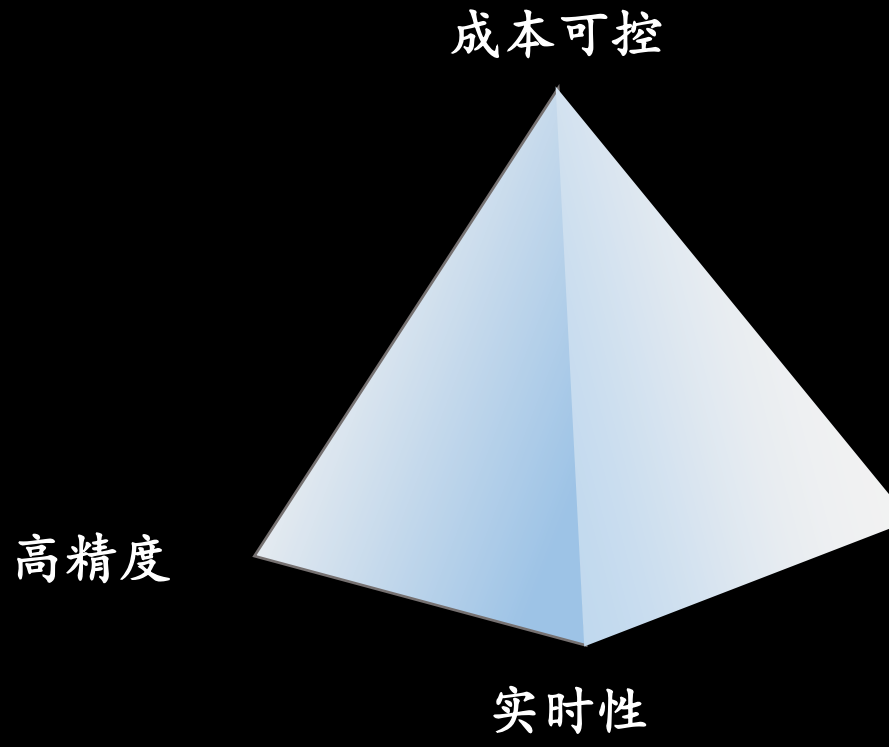
安全事故时有发生，围绕自动驾驶系统的诉讼和纠纷仍旧难以彻底理清。

（2）成本问题

高性能自动驾驶需要车载大量高精度传感器和配套的实时计算系统，
为自动驾驶产品的商业化和大众化设置了非常高的经济门槛。

# 一. 冗余系统实现与自动驾驶场景下案例分析

期待的自动驾驶系统：



# 一.冗余系统实现与自动驾驶场景下案例分析

**功能性**

GPS循迹能力

车道线检测

障碍物检测

局部路径规划

其他功能算法

**影响性能的因素**


自动驾驶平台

**非功能性**

有限计算时间

系统可靠级别

驾驶平稳性

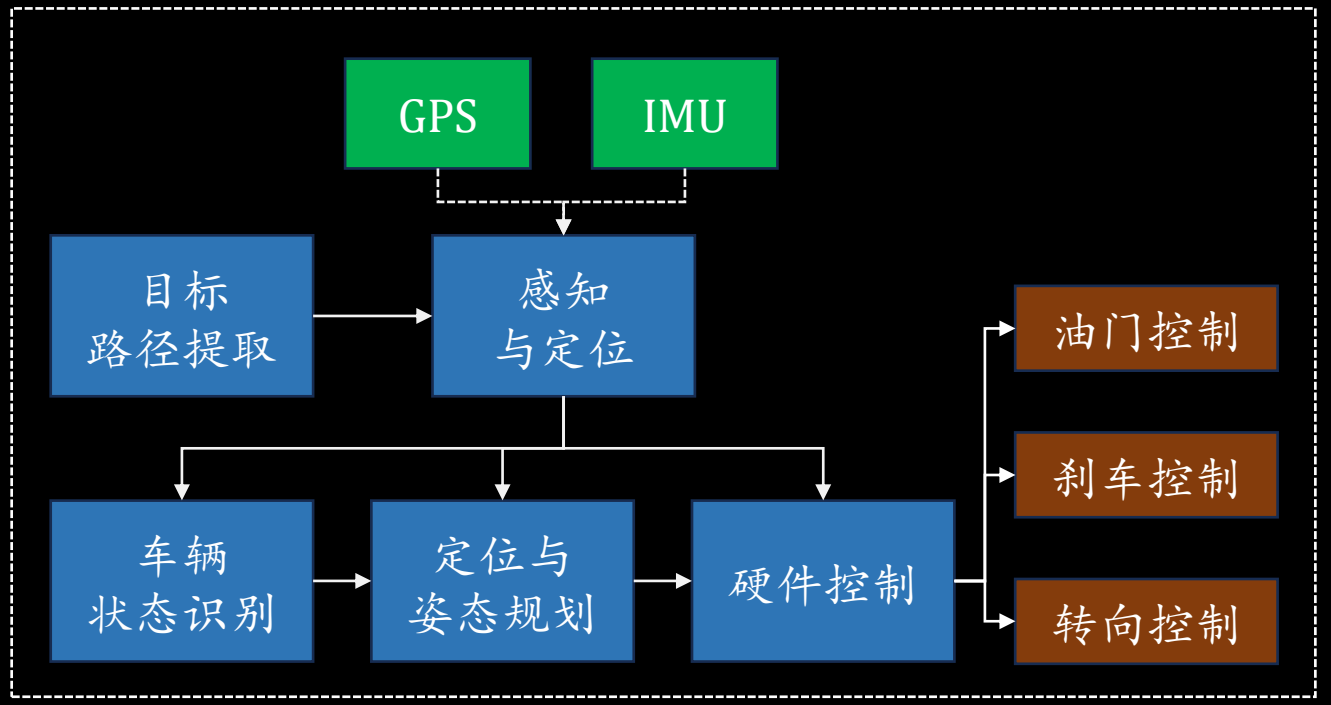
资源能耗效率

其他指标

# 一. 冗余系统实现与自动驾驶场景下案例分析

以自动驾驶循迹控制器为例：

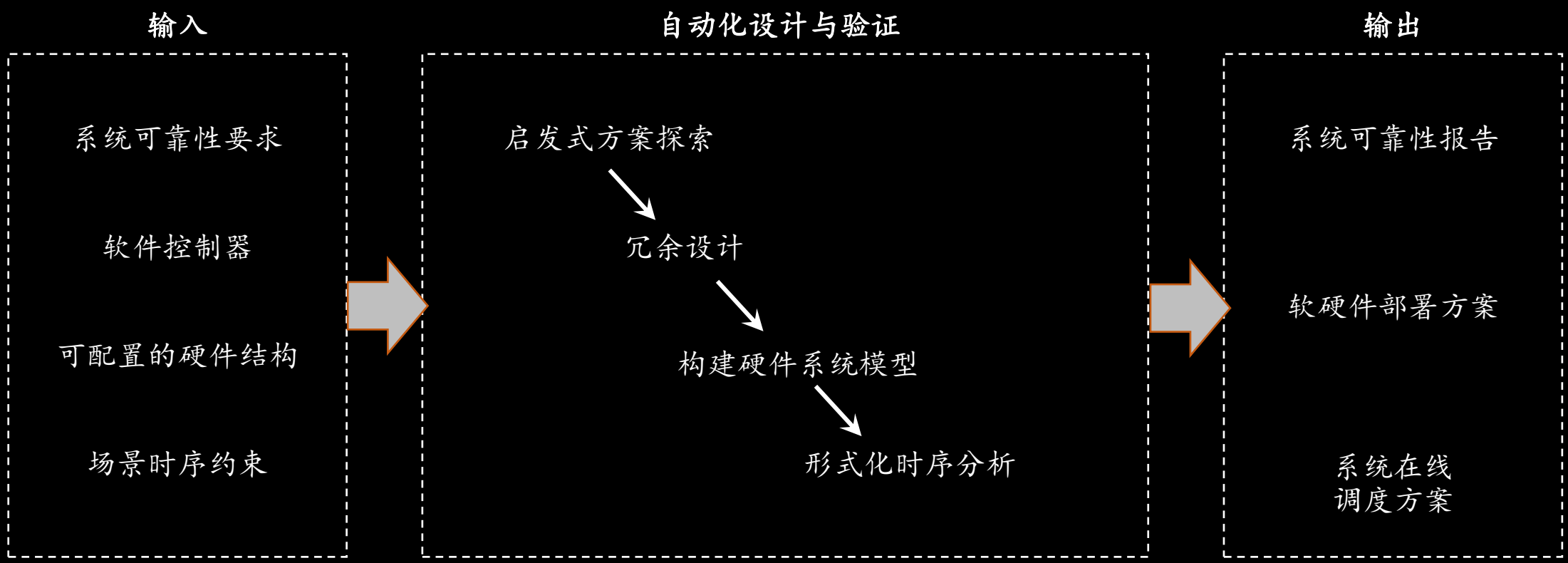
中山大学无人系统研究所
自动驾驶实验平台




一种典型的自动驾驶循迹控制器结构

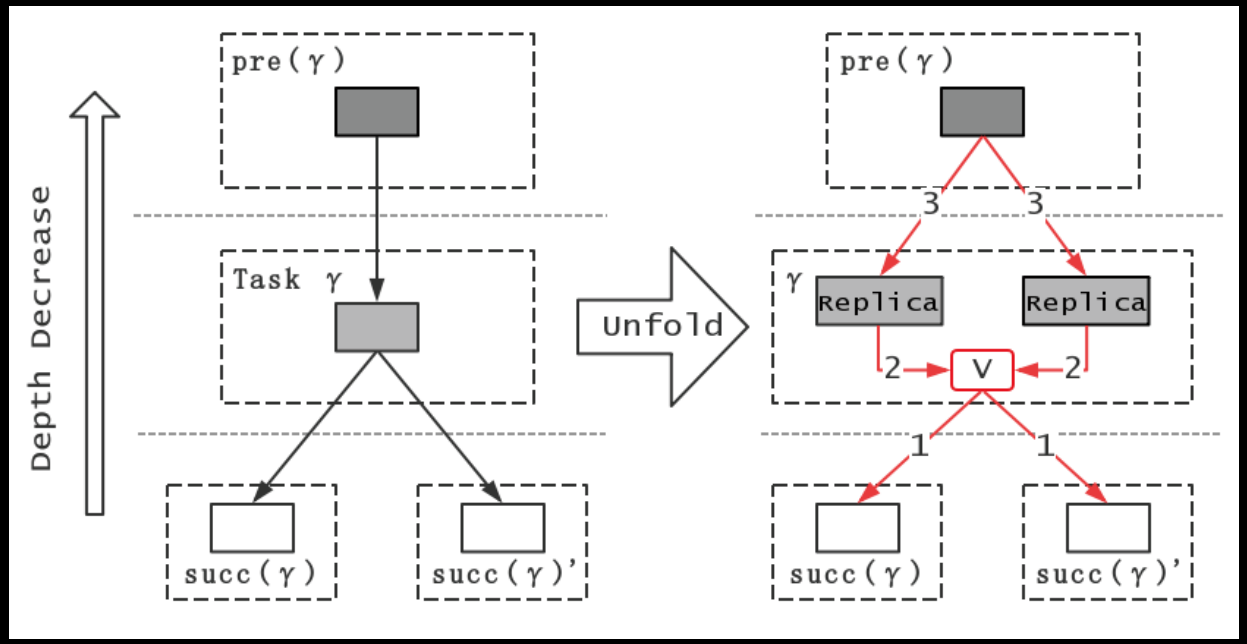
# 一. 冗余系统实现与自动驾驶场景下案例分析

为了提高系统可靠性，提出一种自动化的冗余控制设计流程：



# 一. 冗余系统实现与自动驾驶场景下案例分析

冗余的实现方法

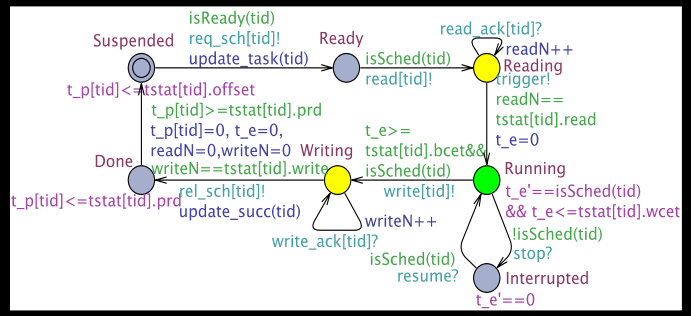


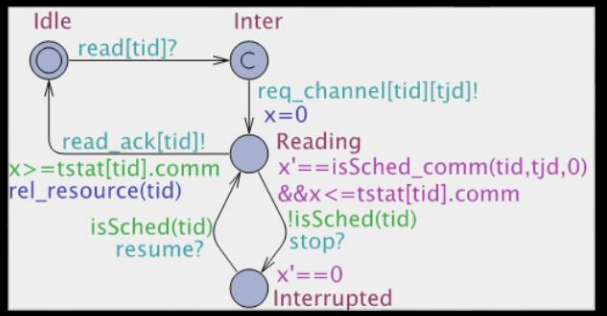

**模型折叠:**

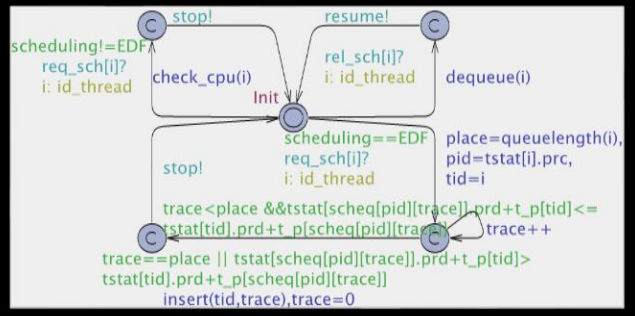
通过反向遍历控制器任务拓扑图
来添加冗余备份与相应的投票器。

# 一. 冗余系统实现与自动驾驶场景下案例分析

冗余的验证方法：Timed Automata 时间自动机



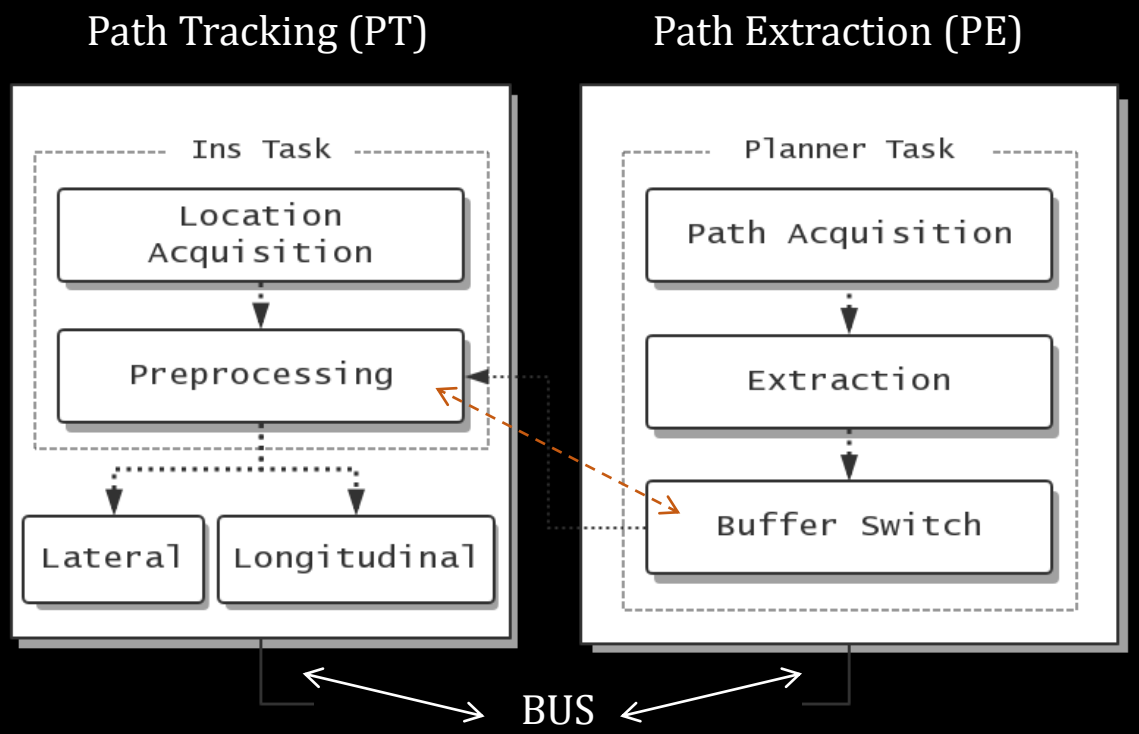




任务模型　　通讯模型　　调度模型

# 一. 冗余系统实现与自动驾驶场景下案例分析

仍然以现有的自动驾驶循迹控制器为例，结合AUTOSAR的开发模型进行分析。



# 一. 冗余系统实现与自动驾驶场景下案例分析

不同场景中任务执行频率的要求

| Speed | Path Tracking (PT) | | | Path Extraction (PE) | | |
|---|---|---|---|---|---|---|
| | Straight | Turn | U-Turn | Straight | Turn | U-Turn |
| 10km/h | 100 | 100 | 120 | 10 | 10 | 12 |
| 20km/h | 100 | 100 | 181 | 10 | 10 | 19 |
| 30km/h | 100 | 107 | N/A | 10 | 11 | N/A |
| 40km/h | 120 | N/A | N/A | 12 | N/A | N/A |
| 60km/h | 197 | N/A | N/A | 20 | N/A | N/A |

不同任务的执行时序信息

| Type | Path Tracking | | | Path Extraction |
|---|---|---|---|---|
| tasks | ins | lateral | longitudinal | planner |
| WCET | 0.3662 | 0.6674 | 0.5932 | 6.9216 |
| BCET | 0.1230 | 0.0790 | 0.1300 | 1.8620 |

# 一. 冗余系统实现与自动驾驶场景下案例分析

## 在不同场景下两种冗余资源映射策略的比较实验

任务执行频率 | 冗余方案 | 不同的资源映射与相应的系统可靠性分析

空间域冗余方案

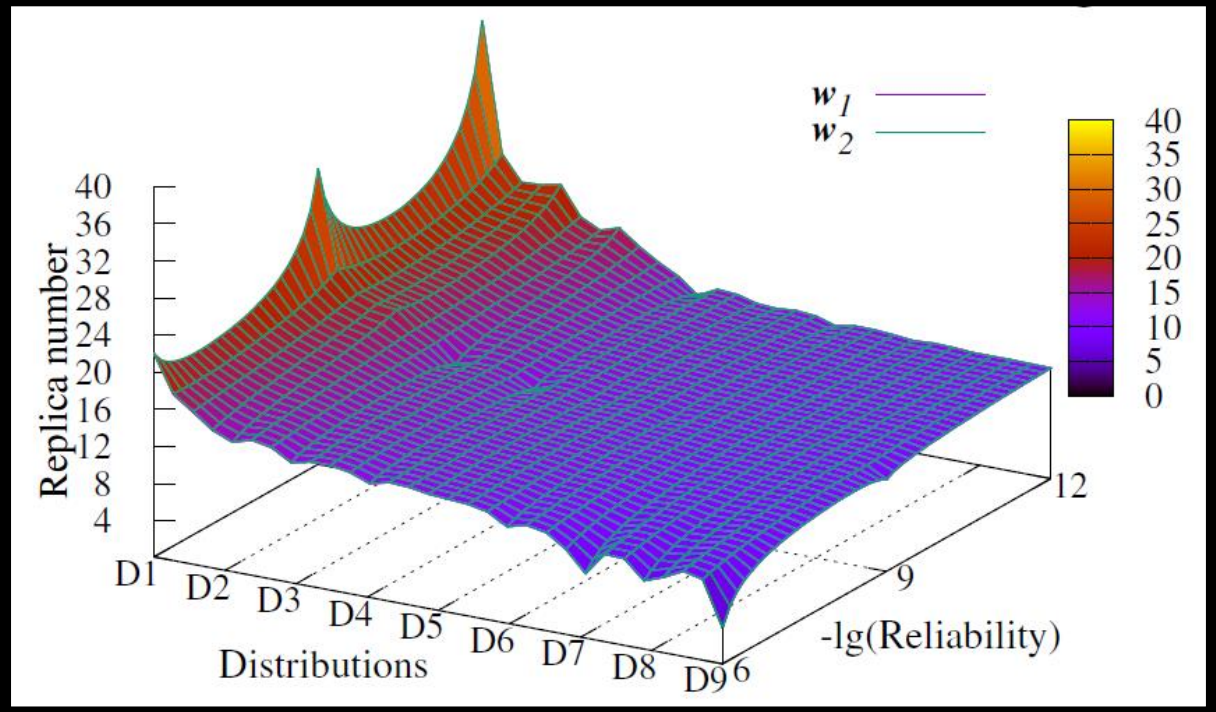
| Frequency (Hz) | Replica | $\|P\|$ | Constraint solving | | | | Model checking | | | | Greedy algorithm | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | fixed map. | | flexible map. | | fixed map. | | flexible map. | | fixed map. | | flexible map. | |
| | | | sat. | cost | sat. | cost | sat. | cost | sat. | cost | sat. | cost | sat. | cost |
| (100,10) | $t_i \times 1$ | 1 | Y | 0.041 | Y | 0.037 | Y | 0.010 | Y | 0.010 | Y | 0.003 | Y | 0.003 |
| | $t_i \times 3$ | 3 | Y | 0.161 | Y | 0.189 | Y | 7148.820 | Y | 7218.180 | Y | 0.003 | Y | 0.004 |
| (120,12) | $t_i \times 1$ | 1 | Y | 0.036 | Y | 0.035 | Y | 0.010 | Y | 0.010 | Y | 0.003 | Y | 0.003 |
| | $t_i \times 3$ | 3 | Y | 0.095 | Y | 0.090 | Y | 5464.94 | Y | 6714.620 | Y | 0.003 | Y | 0.004 |
| (107,11) | $t_i \times 1$ | 1 | Y | 0.040 | Y | 0.039 | Y | 0.010 | Y | 0.010 | Y | 3.579 | Y | 3.073 |
| | $t_i \times 3$ | 3 | Y | 0.098 | Y | 0.103 | Y | 7083.540 | Y | 8520.740 | N | 32.574 | N | 32.251 |
| (197, 20) | $t_i \times 1$ | 1 | Y | 0.070 | Y | 0.073 | Y | 0.020 | Y | 0.010 | Y | 0.003 | Y | 0.004 |
| | $t_i \times 3$ | 3 | Y | 0.198 | Y | 0.189 | Y | 7183.370 | Y | 8494.460 | N | 30.043 | N | 30.681 |

时-空域混合冗余方案

| Frequency (Hz) | Replica | $\|P\|$ | Constraint solving | | | | Model checking | | | | Greedy algorithm | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | fixed map. | | flexible map. | | fixed map. | | flexible map. | | fixed map. | | flexible map. | |
| | | | sat. | cost | sat. | cost | sat. | cost | sat. | cost | sat. | cost | sat. | cost |
| (100, 10) | $t_i \times 3$ | 1 | Y | 189.207 | Y | 228.648 | Y | 4.790 | Y | 2.650 | N | 106.903 | N | 110.818 |
| | | 2 | Y | 0.472 | Y | 1.127 | Y | 0.012 | Y | 0.013 | Y | 0.003 | Y | 0.006 |
| (120, 12) | $t_i \times 3$ | 1 | Y | 152.501 | Y | 150.642 | Y | 3.510 | Y | 2.540 | N | 132.833 | N | 117.347 |
| | | 2 | Y | 1.140 | Y | 1.235 | Y | 0.014 | Y | 0.013 | Y | 0.004 | Y | 0.004 |
| (107, 11) | $t_i \times 3$ | 1 | Y | 102.439 | Y | 101.999 | Y | 3.500 | Y | 2.560 | N | 119.581 | N | 142.081 |
| | | 2 | Y | 1.167 | Y | 1.088 | Y | 0.011 | Y | 0.012 | Y | 0.004 | Y | 0.004 |
| (197, 20) | $t_i \times 3$ | 1 | N | 5708.326 | N | 4232.964 | N | 3.180 | N | 2.370 | N | 75.561 | N | 75.964 |
| | | 2 | Y | 4.506 | Y | 3.564 | Y | 0.014 | - | - | Y | 0.004 | Y | 0.003 |

# 一. 冗余系统实现与自动驾驶场景下案例分析

冗余设计方案生成与可靠性分析实验

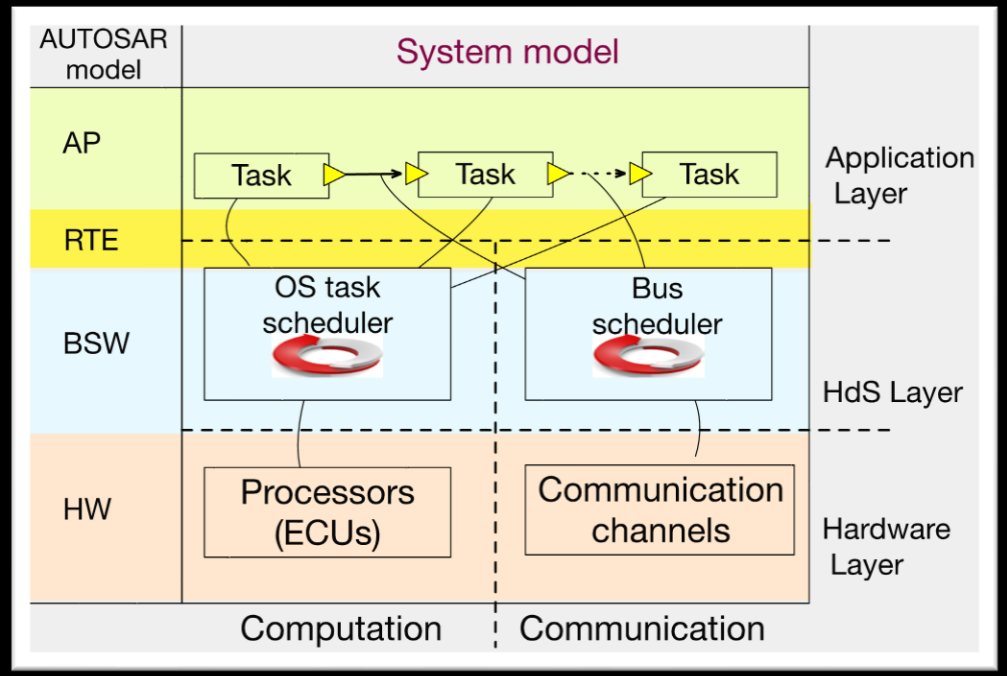


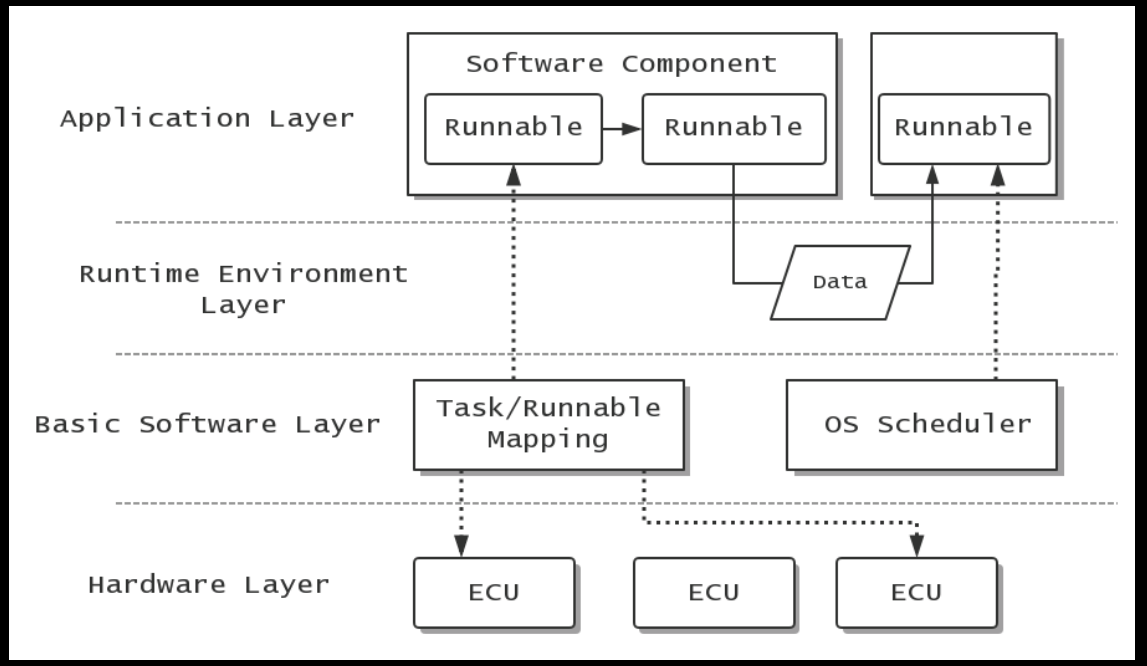

冗余模块为不同任务设置了不同重要程度和可靠性权重，并由此计算不同冗余设计方案下系统可靠性的分布情况。

实验结果给出了在不同可靠性配置方案下保证特定可靠性水平需要的冗余部署数量。

# 一. 冗余系统实现与自动驾驶场景下案例分析

自动驾驶系统已经拥有工业级的通用层级式开发模型 AUTOSAR



# 一. 冗余系统实现与自动驾驶场景下案例分析

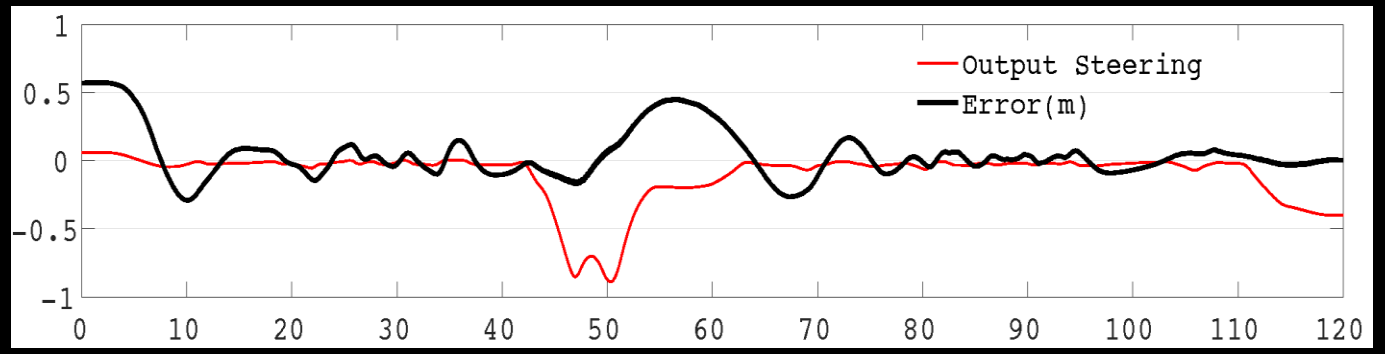
在中山大学校内试验场地
进行实车测试的路径


实车运行控制器时的端到端延迟

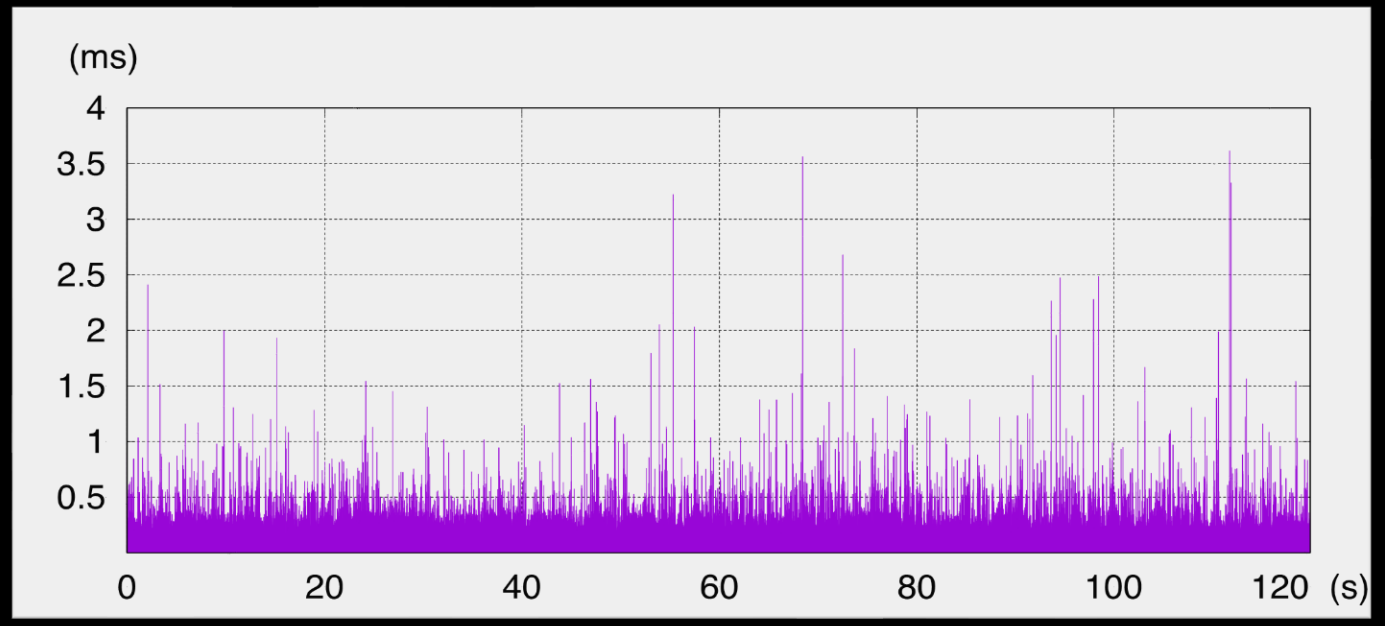
| Type | PT | PE |
|---|---|---|
| Deadline | 5.0 | 50.0 |
| Minimal | 0.5234 | 20.3281 |
| Maximal | 3.7870 | 25.3125 |
| Average | 0.6188 | 23.9560 |

# 一. 冗余系统实现与自动驾驶场景下案例分析

车辆横向转弯控制的
在线变化图




控制器端到端延迟的
在线分布



# 内容提纲

- 冗余系统实现与自动驾驶场景下案例分析
- 自动驾驶中系统资源在线调度与循迹案例分析
- 总结与展望

# 二. 冗余系统实现与自动驾驶场景下案例分析

AUTOSAR 模型支持 2 种软件触发方式：

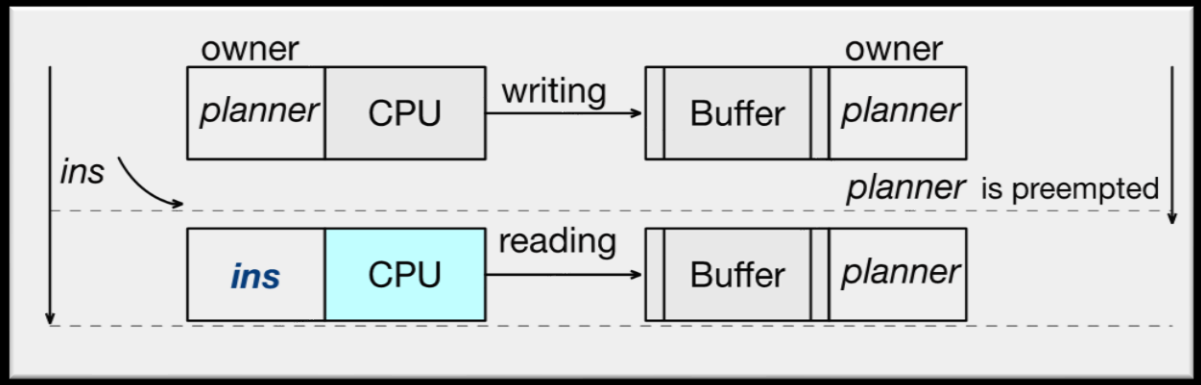
| 时间触发 | 事件触发 |
| --- | --- |
| 确定的 | 非确定的 |
| 可预测行为 | 有限的可预测性 |
| 离线调度 | 在线调度，优先级主导 |
| 简单的容错冗余可决定性（可分析性） | 复杂的冗余模块同步 |

# 二. 冗余系统实现与自动驾驶场景下案例分析

结合时序和频率信息使用时间自动机模型在不同调度算法下的死锁检测结果

| Freq | Proc | FIFO | | | | FP | | | | EDF | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | No Replica | | Replica | | No Replica | | Replica | | No Replica | | Replica | |
| | | DL | costs | DL | costs | DL | costs | DL | costs | DL | costs | DL | costs |
| (10,100) | 1 | N | 0.013 | Y | 19.08 | Y | 0.014 | Y | 18.97 | Y | 81.50 | Y | 73.20 |
| | 2 | N | 0.014 | N | 499.5 | N | 0.014 | N | 499.6 | N | 114.7 | N | 501.4 |
| (20,200) | 1 | Y | 0.814 | Y | 6.655 | Y | 0.763 | Y | 6.719 | Y | 0.765 | Y | 6.732 |
| | 2 | N | 1.358 | N | 257.6 | N | 1.361 | N | 255.0 | N | 37.50 | N | 256.6 |

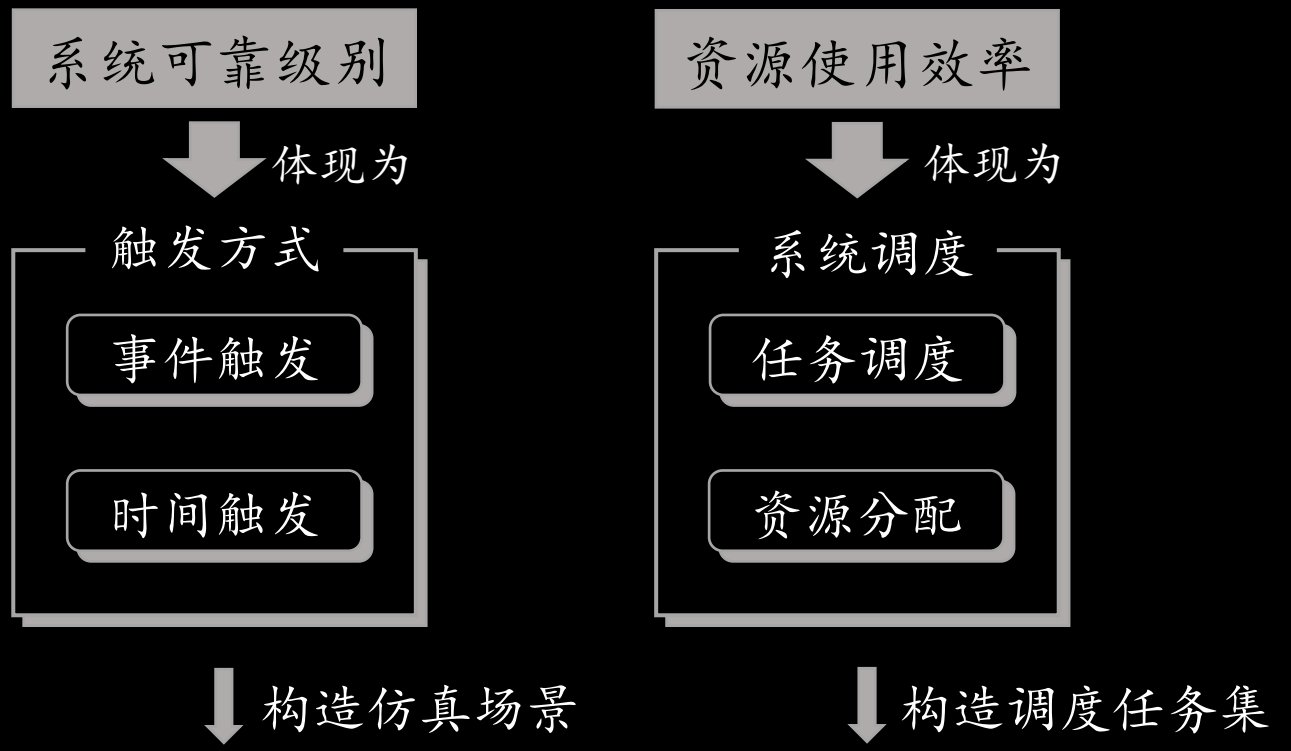
（PT任务优先级高于PE任务）




死锁场景

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

影响**非功能性指标**的重要因素



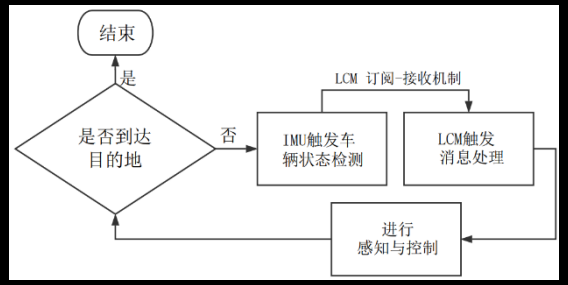
# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 探索触发方式对驾驶平稳性的影响

功能开发便利性

↓

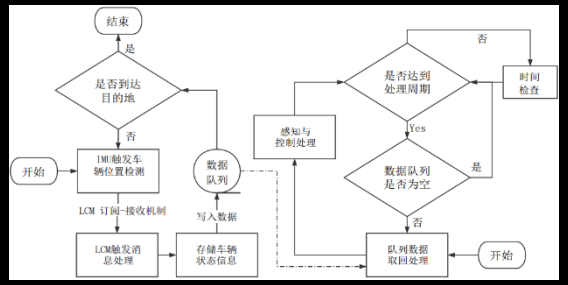
**事件触发**模式




系统行为的确定性

↓

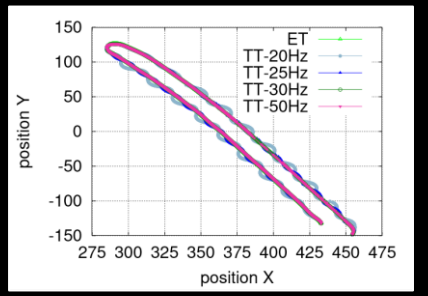
**时间触发**模式




API
接入

API
接入

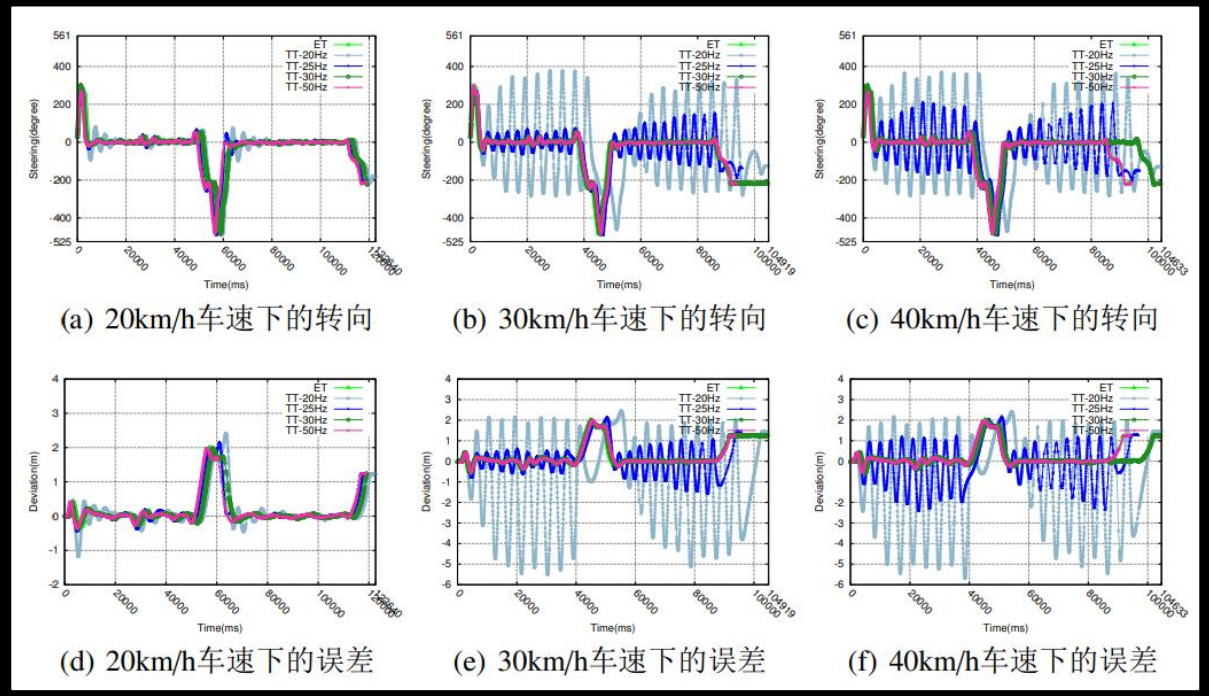
AirSim仿真环境




比较时间/事件触发
不同频率系统性能

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

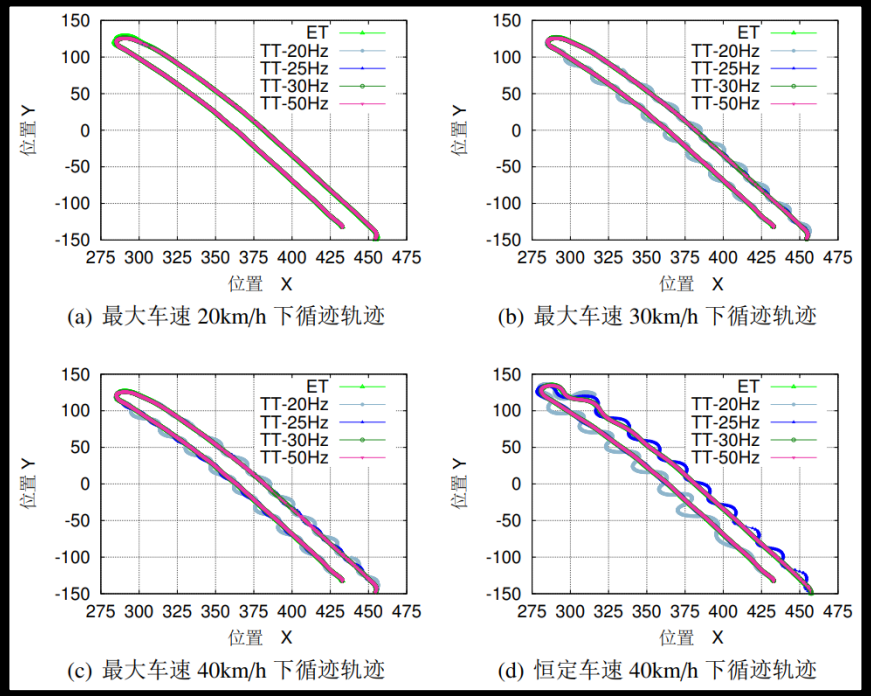
## 探索触发方式对驾驶平稳性的影响




(a) 20km/h车速下的转向　(b) 30km/h车速下的转向　(c) 40km/h车速下的转向

(d) 20km/h车速下的误差　(e) 30km/h车速下的误差　(f) 40km/h车速下的误差

在不同车速和触发频率下的
实时转向误差




(a) 最大车速 20km/h 下循迹轨迹　(b) 最大车速 30km/h 下循迹轨迹

(c) 最大车速 40km/h 下循迹轨迹　(d) 恒定车速 40km/h 下循迹轨迹

在不同车速和触发频率下的
最终循迹轨迹

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

启发：

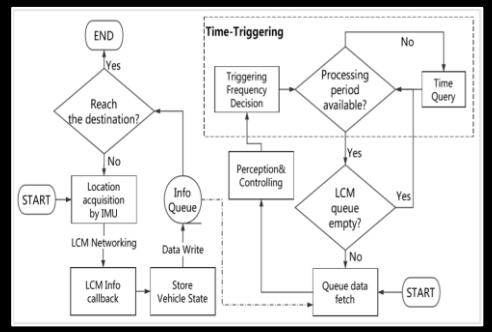
具有可靠性的时间触发实现需要尽可能提高触发频率以满足复杂驾驶场景的误差性能要求。

但是，高频触发带来了更高的资源需求，并在嵌入式平台上**引发资源竞争**。

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

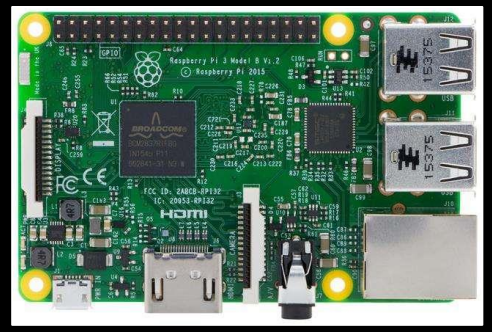
引入混合安全关键系统理论

复杂功能




资源需求量大

嵌入式平台



有限计算能力

软件部分

硬件部分

系统特征

- 软件反馈实时性
- 不同任务**关键性**
- 功能模块周期性

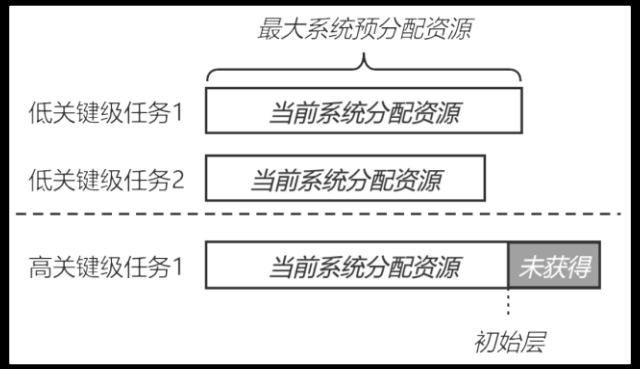
符合

混合关键级系统理论

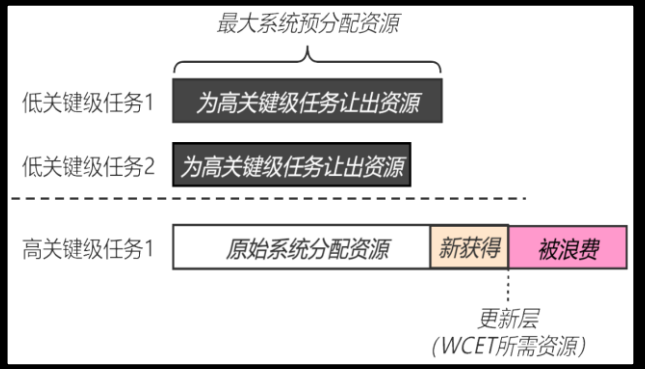
# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 现有混合关键级理论与三大缺陷

原始状态




由于**高关键级任务运行资源枯竭且未结束**，系统更新预算资源配置。




模式切换

**悲观性**

基于低概率WCET的离线预算分配

**资源浪费**

完成后未耗尽的预算被完全忽视

**激进丢弃**

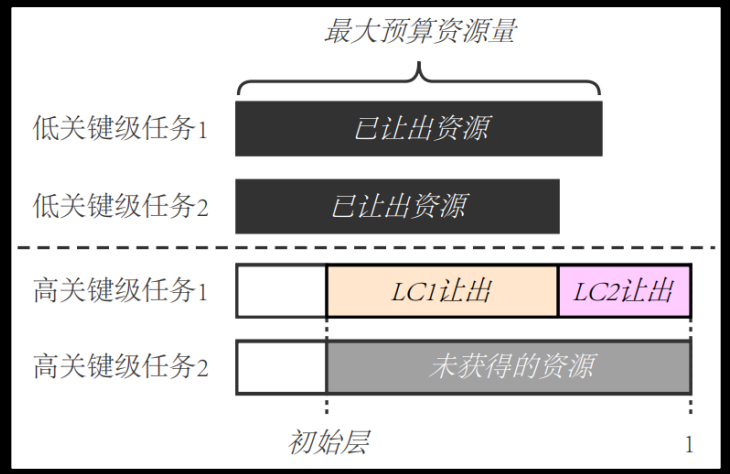
无预算任务将直接放弃执行

问题：如何充分为低关键级任务分配资源保证其执行?

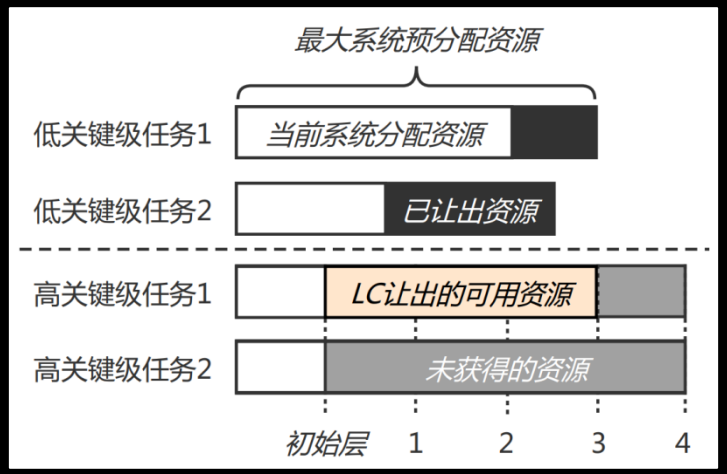
# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 解决悲观性：两层系统模型的多层拓展

两层模型




拓展




多层模型 MST

优点

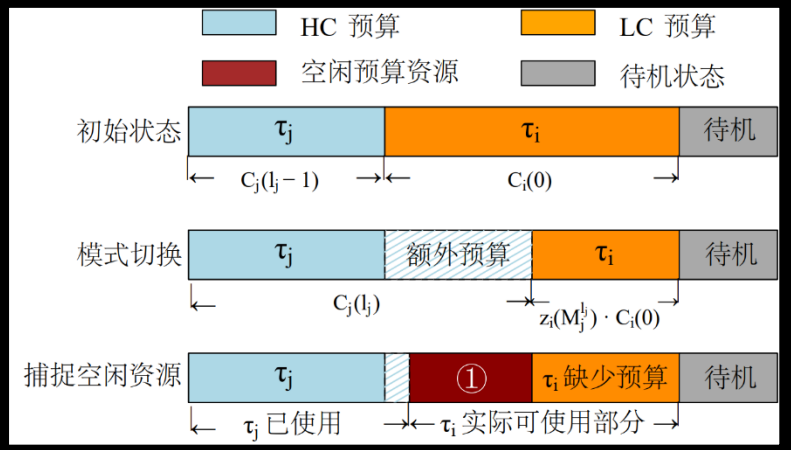
- 更细粒度资源调配
- 尽可能保留低关键级任务的可用预算

确保

- 系统可调度性(U≤1)
  - 离线状态可调度
  - 模式切换后可调度
  - 资源转移保持平衡
- 系统资源平衡

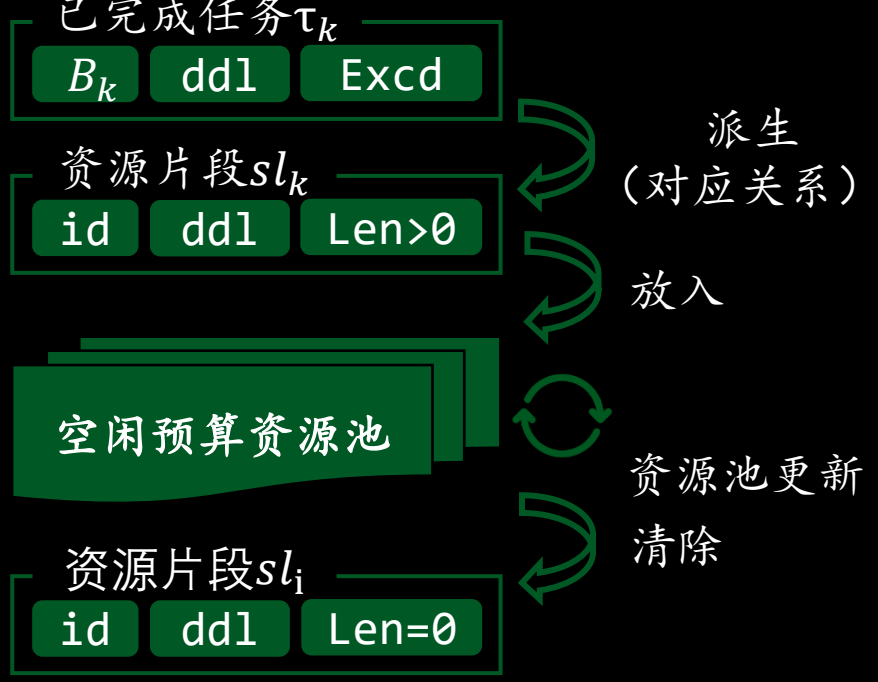
# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 解决资源浪费：在线空闲预算管理机制




在线空闲预算资源示意

空闲预算资源管理方法：

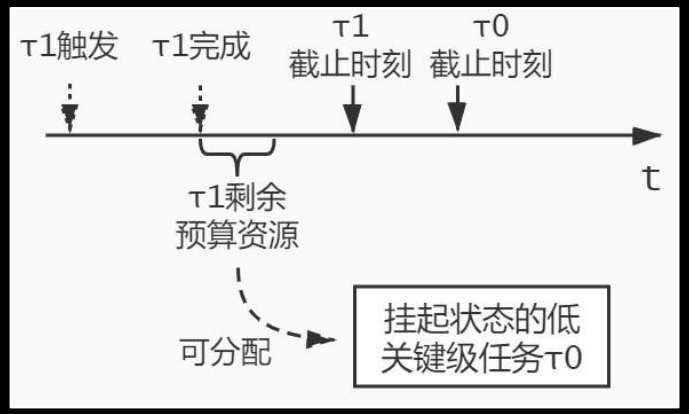


# 二. 自动驾驶中系统资源在线调度与循迹案例分析

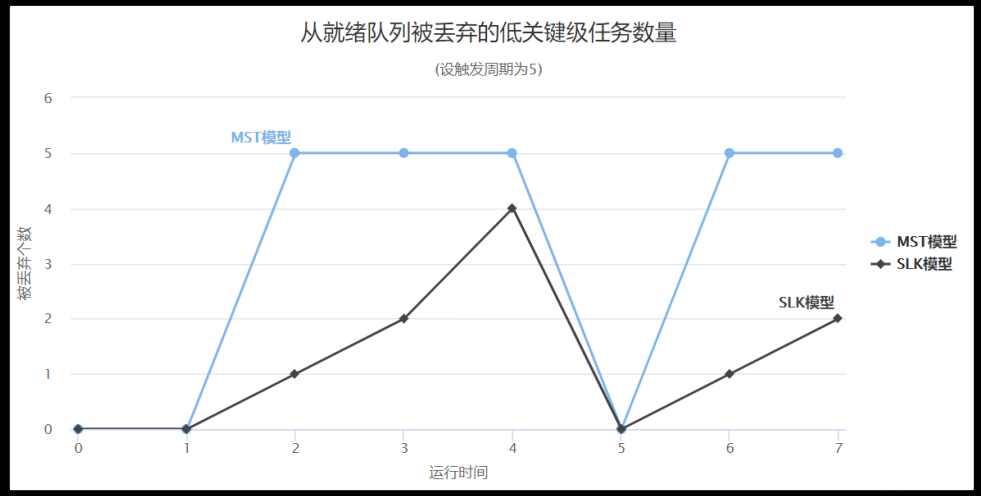
## 解决激进丢弃：多步式任务丢弃策略

**多步式丢弃策略**

在单一调度周期内只丢弃一个尚无预算资源可用的低关键级任务并检查新产生的空闲预算片段是否可用。

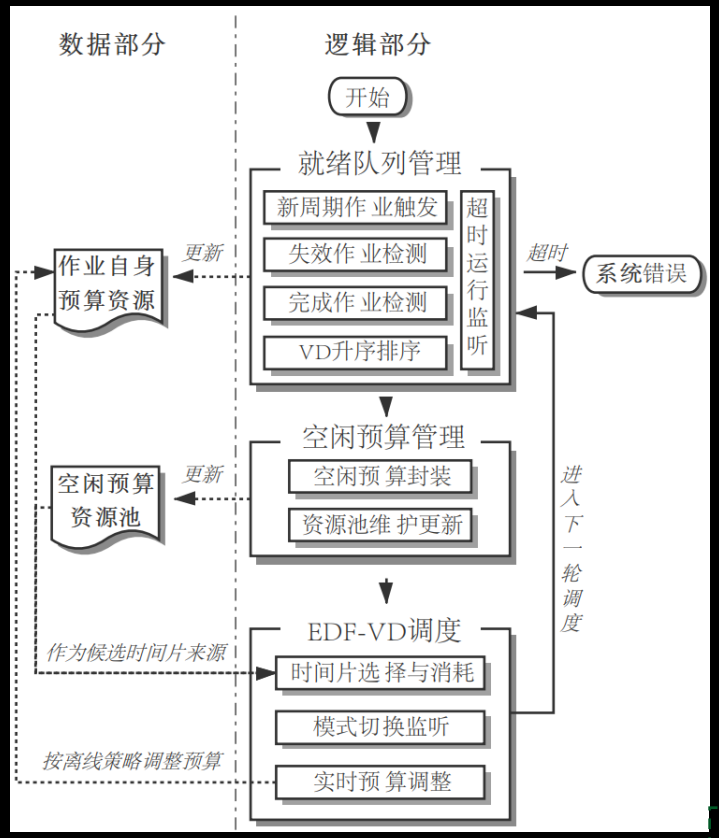



剩余可用预算带来的
延迟丢弃




多步丢弃SLK模型与激进丢弃MST模型
的性能退化对比

# 二. 自动驾驶中系统资源在线调度与循迹案例分析




在线空闲预算资源示意

进入EDF-VD调度阶段

优先使用空闲预算资源 — 满足 $sl_k.ddl \leq \tau_i.ddl$ 即具有可用性

其次使用自身预算资源 — HC任务预算不足时触发模式切换并更新预算总量

尝试消耗时间 — 无有效时间片则尝试调度就绪队列中的下一个任务

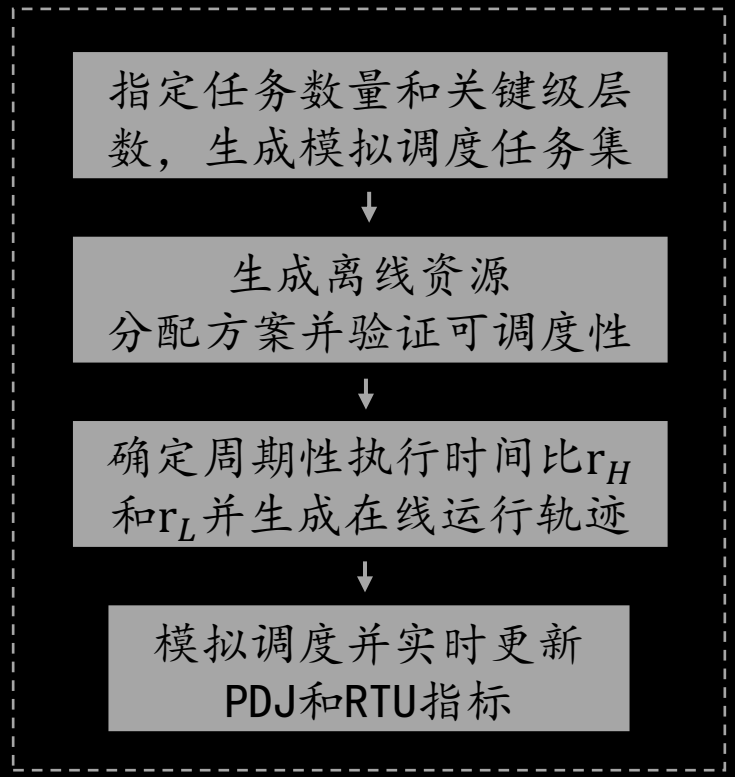
确保时间片消耗量为

$$\min(floor(t_{cur}) + 1 - t_{cur}, toExec_i - Excd_i, sl_k.len)$$

便于下次调度前在就绪队列中插入周期性触发的新任务

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 实验设计与指标说明




模拟调度实验流程

**PDJ指标**

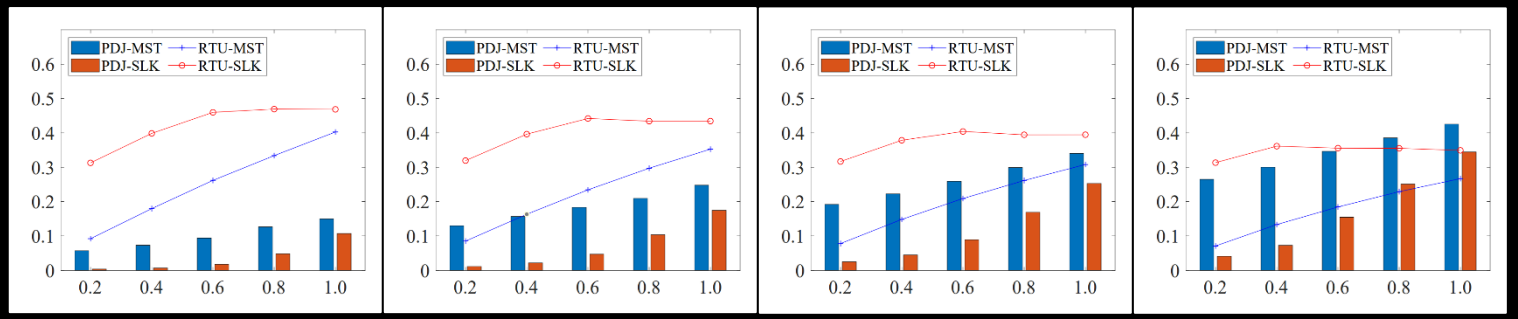
指在给定模拟时间区间内**被丢弃低关键级任务数量占低关键级任务触发总数的比例**，用于衡量给定周期内系统性能退化的程度。

**RTU指标**

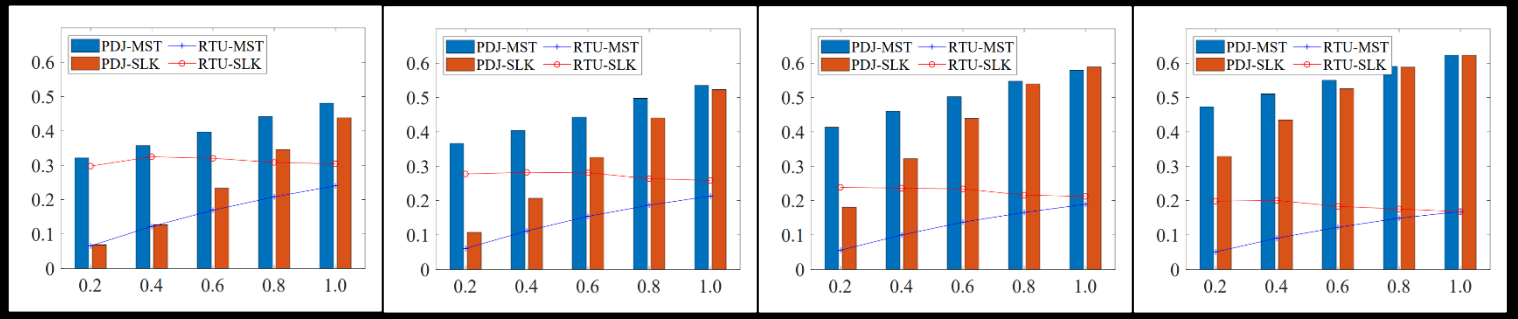
指在给定模拟时间区间内**低关键级任务消耗的时间片资源总数占总模拟时间的比例**，用于衡量低关键级任务的实际资源分配。

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 在线调度过程模拟结果




(a) $r_H$ = 0.3　(b) $r_H$ = 0.4　(c) $r_H$ = 0.5　(d) $r_H$ = 0.6




(e) $r_H$ = 0.7　(f) $r_H$ = 0.8　(g) $r_H$ = 0.9　(h) $r_H$ = 1.0

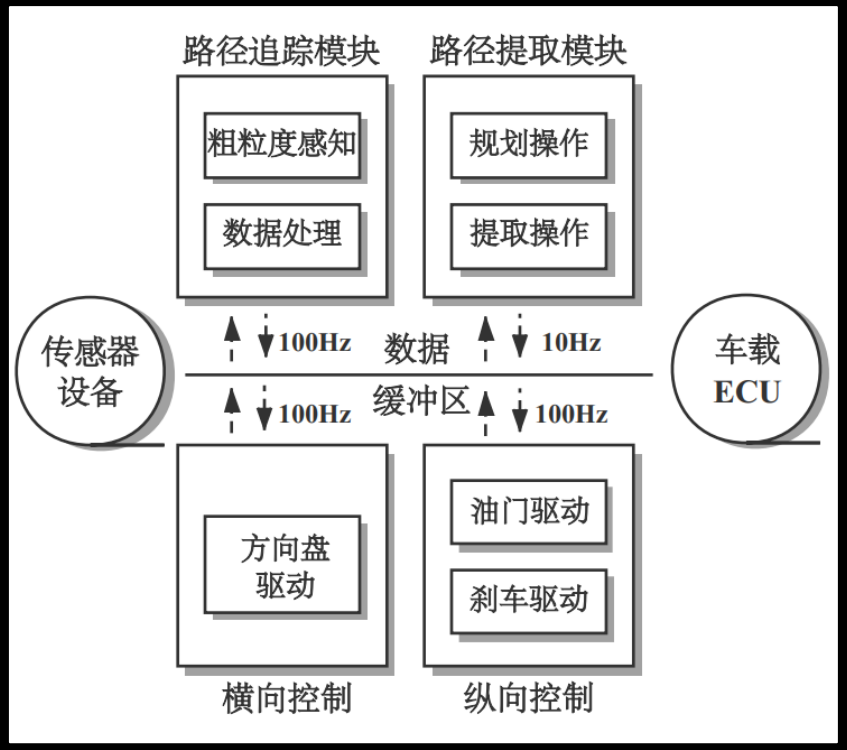
不同$r_H$和$r_L$取值对应MST和SLK模型的系统性能

在$r_H$从0.3增大至1.0的过程中，与MST模型相比下SLK模型在绝大多数场景中的任务丢弃情况更好（即**更低的PDJ指标**），缓解了系统性能退化，因此在模拟时段内的**系统性能更优**。

在$r_H$从0.3增大至1.0的过程中，与MST模型相比下SLK模型为低关键级任务分配了更多的系统资源（即**更高的RTU指标**），帮助低关键级任务提升了完成周期性执行的概率，在模拟时段内的**系统资源使用效率更高**。

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 以自动驾驶循迹控制器为分析案例




单核系统上的循迹控制器结构

表1. 循迹应用任务集信息（ms）

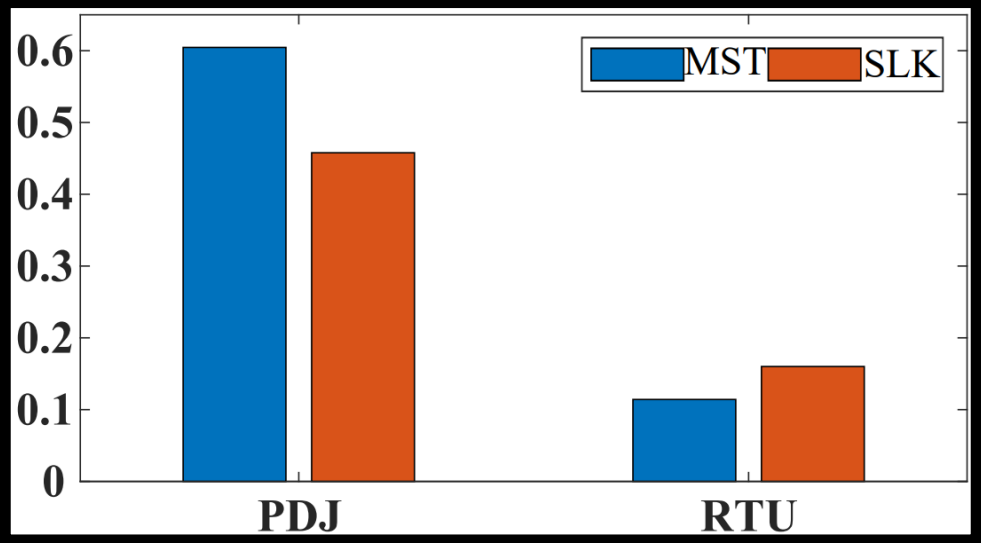
| 功能模块 | WCET下界 | WCET上界 | 周期 | 关键级 |
|---|---|---|---|---|
| 路径追踪 | 8 | – | 10 | 低 |
| 路径提取 | 50 | – | 100 | 低 |
| 纵向控制 | 1.0 | 3 | 10 | 高 |
| 横向控制 | 0.8 | 4 | 10 | 高 |

表2. 低关键级任务对误差的影响(m)

| 功能模块 | 完成对误差影响 | 丢弃对误差影响 |
|---|---|---|
| 路径追踪 | -0.05 | +0.02 |
| 路径提取 | Error归零 | +0.02 |

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 循迹控制器的性能指标




循迹控制任务集使用MST和SLK
模型的性能比较

**指标分析**

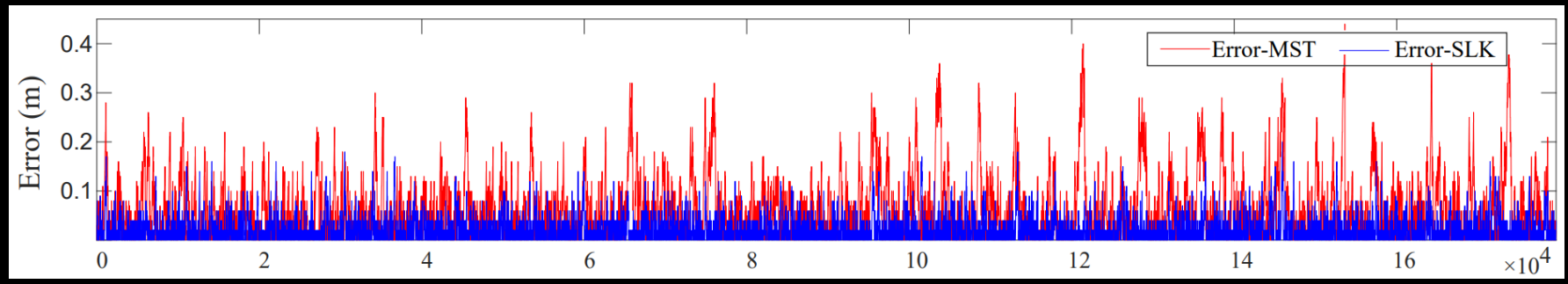
（SLK较MST）

PDJ性能： 降低24%

RTU性能： 提升40%

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

循迹控制器在调度期间的实时误差分布




循迹控制任务集使用MST和SLK模型进行
调度的实时循迹误差

现象 → 分析

**SLK模型具有更小的最大循迹误差**

- SLK模型最大误差为0.2m
- MST模型最大误差为0.44m

**SLK模型具有更平滑的误差分布**

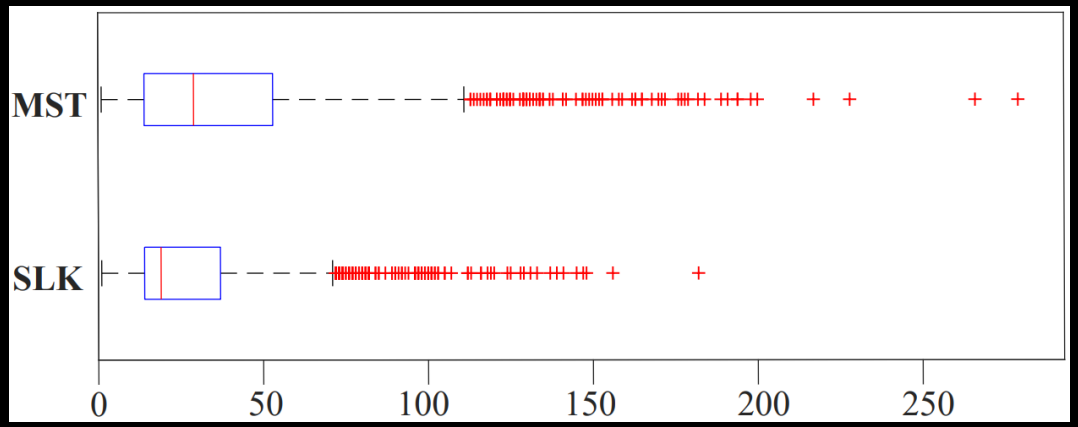
- SLK模型更快消除最大误差
- MST模型误差消除存在波动

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 循迹控制器的连续偏移长度分布

### 偏移与连续偏移

在循迹过程中，车辆在滑动窗口范围内出现的误差增大现象称为**偏移**。相邻的偏移将合并为**连续偏移**，并更新连续偏移的长度。




循迹控制任务集使用MST和SLK模型进行调度的持续偏移长度分布

SLK模型的最大和平均连续偏移长度均小于MST模型的相关指标，说明SLK模型的循迹偏移分布得更加稀疏。

**得出结论**

SLK模型的系统性能退化过程更加平缓，一定程度避免了用户体验的断崖下降。

# 二. 自动驾驶中系统资源在线调度与循迹案例分析

## 空闲资源调度的优势

针对两层系统模型的悲观资源分配、在线资源调配缺乏灵活性、激进任务丢弃等问题，通过多层模型拓展、空闲预算管理、多步式丢弃等方法，提升了混合关键级系统的输出性能。

# 三. 总结与展望

自动驾驶技术是未来智能交通的重要组成部分，它为道路交通带来了全新的前景。其中，安全关键系统理论扮演着至关重要的角色，它涉及一系列技术和方法，旨在确保自动驾驶车辆在各种复杂道路环境中的安全性和可靠性。

References:


- Junjie Yang, Guangyi Xu, Gang Chen, Nan Guan, Kai Huang: Efficient runtime slack management for EDF-VD-based mixed-criticality scheduling. J. Syst. Archit. 117: 102119 (2021)
- Rongjie Yan, Di Zhu, Fan Zhang, Yiqi Lv, Junjie Yang, Kai Huang: Resource-Aware Design for Reliable Autonomous Applications with Multiple Periods. FM 2018: 294-311
- Rongjie Yan, Junjie Yang, Di Zhu, Kai Huang: Design Verification and Validation for Reliable Safety-Critical Autonomous Control Systems. ICECCS 2018: 170-179