华南地区嵌入式技术和物联网产业发展研讨会（2017年4月嵌入式系统联谊会）

汽车嵌入式系统的功能安全与信息安全

谢国琪 博士

Email：xgqman@hnu.edu.cn
湖南大学信息科学与工程学院

提纲

Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

1. 汽车体系结构

●系统复杂性骤增，功能增加，使得线束的体积(Size)和重量(Weight)、 线束的成本(Cost)和功耗(Power consumption)的也快速增加，给汽车嵌入式系统的设计带了难题。

●为了应对Cost与SWaP (Size, Weight and Power consumption) 问题。新一代汽车嵌入式系统的体系结构从联邦式(Federal)演化为集成式的体系结构(Integrated Architecture)。从计算的视角看，汽车嵌入式系统是一个“异构分布式嵌入式系统”（Heterogeneous Distributed Embedded Systems）

集成的基本特征

- 网络体系结构的集成

- 100多个异构ECU(Electronic Control Unit),
- 大量的传感器，执行器
- 一个或多个中央网关
- 5-6种异构总线：CAN,FlexRay,LIN,MOST,Ethernet
- 所有总线通过网关集成

宝马7系的体系结构

3个 HS-CAN

500Kbps

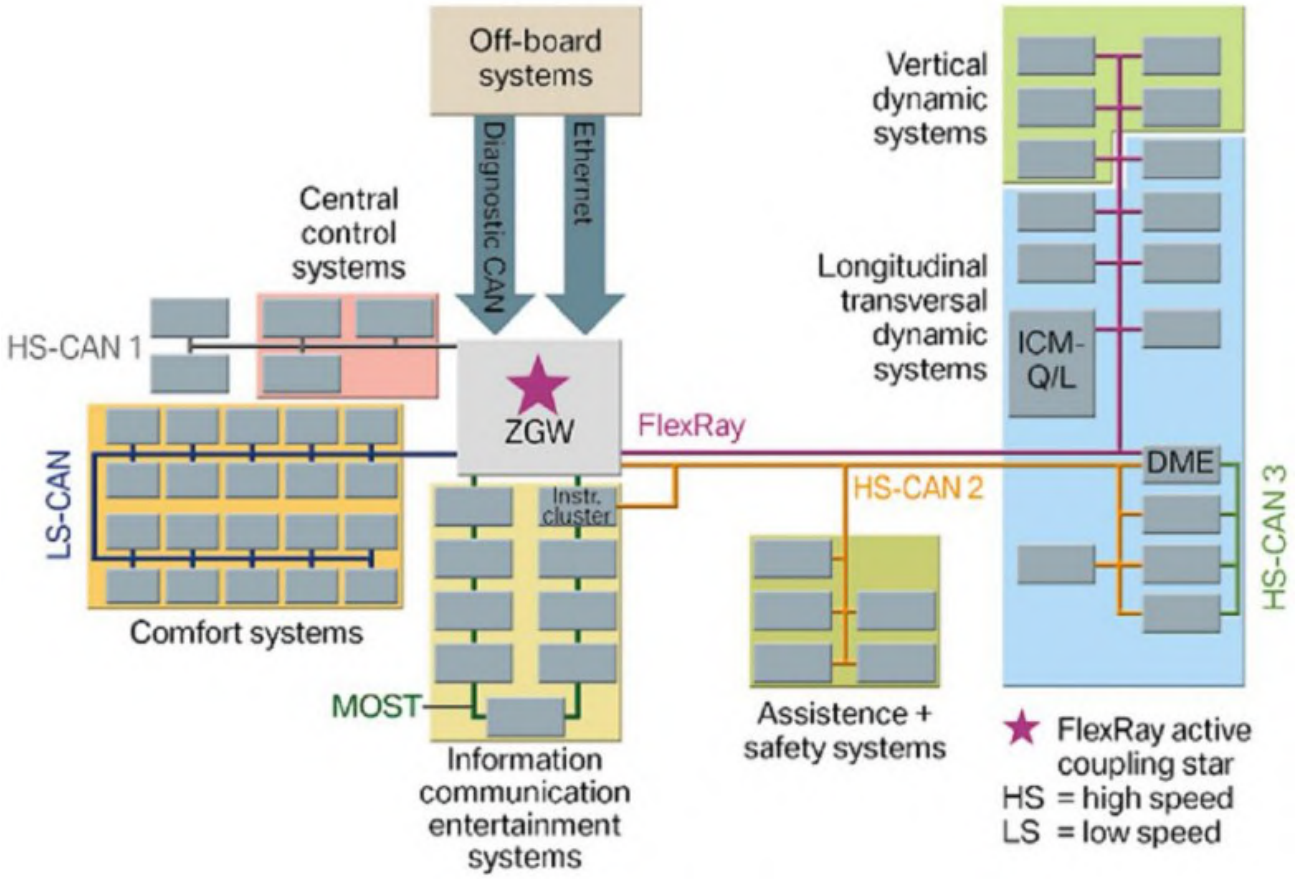
1个LS-CAN

100Kbps

1个FlexRay

1个MOST

1个Ethernet



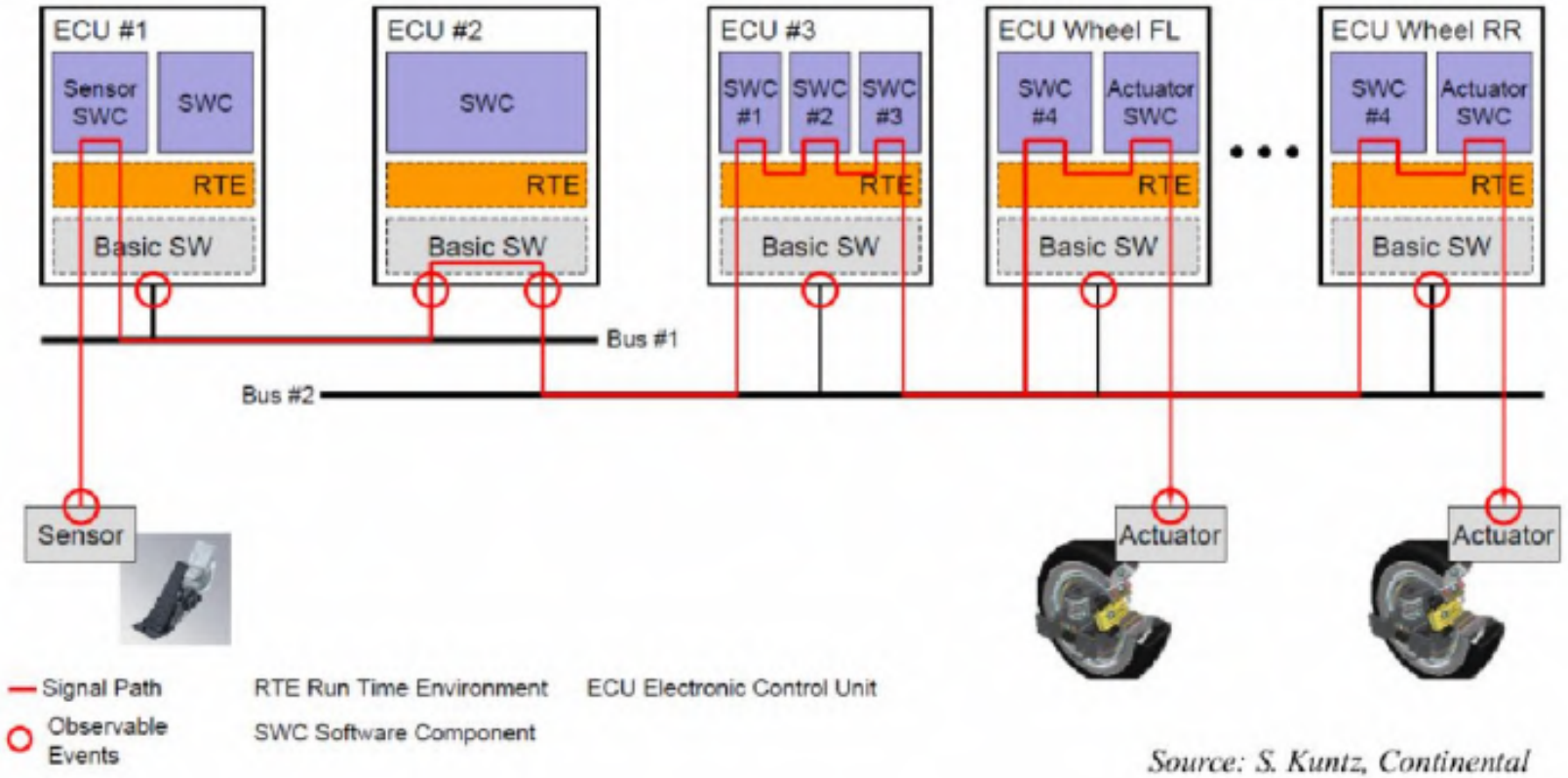
- 功能的集成:
  - 同一系统同时集成多个功能;
  - 一个功能可被不同总线上的ECU执行;
  - 一个ECU可同时支持多个功能执行。

- 系统集成: 集成多个子系统
  - 动力控制子系统;
  - 底盘控制子系统;
  - 安全控制子系统;
  - 车身控制子系统等。

- 功能的分布式

- 每个子系统可包括多个分布式功能（如安全控制子系统包括防抱死制动、线控刹车等功能）

- 某一功能还可能同时跨越多个子系统。



Source: S. Kuntz, Continental

提纲

Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

2.汽车功能安全标准

●背景：汽车自诞生以来，人们就没有停止过对安全驾驶的追求：被动安全(安全气囊)->主动安全(ABS,ESP)->新一代汽车广泛使用的ADAS

●汽车中存在的失效：

- 系统性失效-时限错过导致没有在正确的时间内完成
- 随机硬件失效-硬件出错导致执行中断
- 时序失常-任务的优先约束打乱
- 数据损坏等。

●“风险”即发生伤害或损害的可能性, 及伤害或损害所造成的后果严重性。

- 车辆意外加速、减速与转向；
- 安全气囊非正常弹开；
- 高速行驶时车门突然打开；
- 线控刹车失灵等。

●功能安全(Functional Safety)-避免因系统功能性失效导致的不可接受的风险。

- 避免功能性失效
- 避免不可接受的风险

●IEC 61508:针对工业领域的功能安全标准，

□发布时间：2000年5月

□全程： Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, E/E/PE)。

□目标：该标准要建立一个可应用于各种工业领域的通用功能安全标准。

●ISO 26262:专门针对汽车的功能安全标准，

□发布时间：2011年11月

□全程：道路车辆-功能安全(Road Vehicles-Functional Safety)标准。

□新规则：ISO 26262 针对汽车提出了新的安全完整性等级(Safety Integration Level, SIL)规则

●功能安全的内涵

□实时性(Real-time) —避免因功能性失效造成的不可接受的风险；

□可靠性(Reliability) —避免因随机硬件失效造成的不可接受的风险；

□可控性(Controllability) —避免因驾驶人员控制失效造成的不可接受的风险 （IEC 62608 没有， ISO 26262专门新增的）

提纲

Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

3.汽车信息安全标准

●产生背景：汽车终端信息技术的发展以及无线接口的增多，汽车内部越来也多得越来越多地被暴露在互联网所带来的负面风险之中。攻击者可以通过发动网络攻击，达到访问敏感信息、制造系统故障甚至危害人身安全的目的。

●汽车中存在的信息安全风险：

□欺骗攻击：通过物理接入或无线接口入侵某一个ECU后，利用窃听、伪装、哄骗等攻击形式通过车内网络入侵其他ECU，甚至达到对汽车行驶的控制；

□拒绝服务攻击：另一种是攻击者直接在车内网络上产生大量的无用或错误信息，扰乱汽车的正常行驶。

●汽车信息安全标准SAE J3061

- 全称：信息物理汽车系统网络安全指南 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)

- 发布时间：2016年1月

- 信息安全定义：避免因入侵攻击而导致的不可接受的伤害和风险

●信息安全的内涵

□完整性(Integrity) —避免欺骗攻击造成的不可接受的风险；

□可用性(Availability) —避免拒绝服务攻击造成的不可接受的风险；

□机密性(Confidentiality) —避免信息的窃听攻击造成的不可接受的风险（不是SAE J3061所关注的重点 ）。

提纲

Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

4.AUTOSAR自适应平台标准

- 之前的AUTOSAR 静态平台标准
  - 汽车开放系统架构（AUTomotive Open System Architecture, AUTOSAR）
  - 发布日期：2003年7月
  - 创始成员：宝马、博世、大陆、戴姆勒-克莱斯勒、西门子威迪欧、大众
  - 加入成员：福特公司、标致雪铁龙、丰田、通用
  - 目标：为汽车电子构架开发一套开放的行业标准，其分层软件架构中的基础软件模块层能够应用于不同厂家生产的车辆以及不同供应商提供的功能部件。
  - 最新版本：AUTOSAR 4.3

●由于汽车是高度安全关键的嵌入式系统，AUTOSAR一直对汽车中的功能采用静态规划的方式实现其安全性

●静态的含义

□所有功能只释放一次或严格的周期释放

□系统调度严格按照预先设定的方式进行，不再改变

●静态的局限

□车道偏离警示、碰撞避免、线控刹车等功能需与物理世界进行实时的动态交互，它们都是动态释放的。

□基于静态规划的AUTOSAR平台标准已不太适应汽车中这些动态安全关键功能的执行。

●AUTOSAR发言人Simon Furst多次指出AUTOSAR新平台标准将全面支持动态规划（Planned Dynamics）

□动态调度：系统能够自适应的响应动能的动态释放，分配，以及错误报告；

□动态通信：功能能够通过面向服务的通信机制实现动态通信；

□动态部署：系统功能安全功能的要求实现动态重配置。

●是一个支持并行计算、安全性、关键性和功能集成的异构计算平台

提纲

Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

1. 汽车网络体系结构的时间分析

●实时系统的开发生命周期：建模，分析，设计，实现几个阶段

●分析的结果将作为设计阶段（验证、调度、优化）的时间输入参数

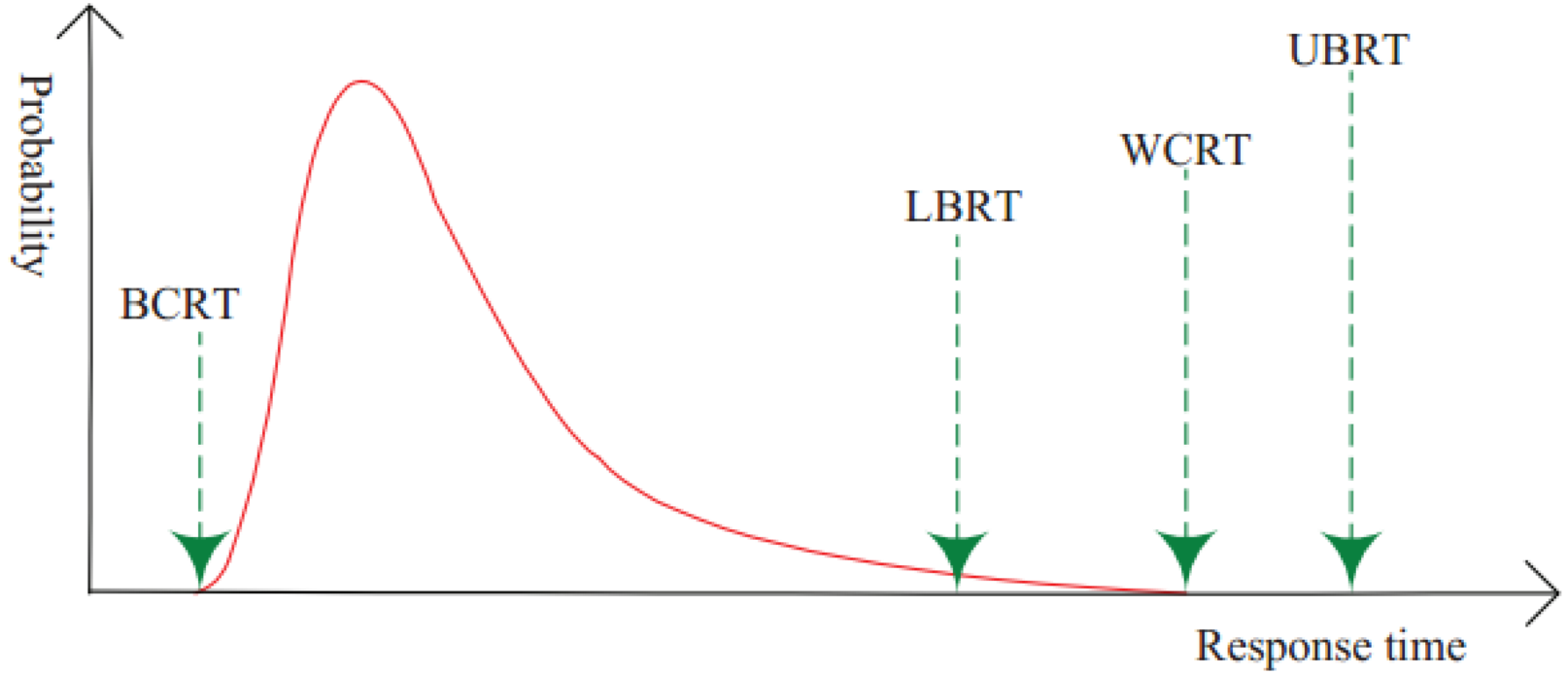
●最坏执行时间(Worst Case Execution Time, WCET)

□最坏响应时间(Worst Case Response Time, WCRT)

当该任务在给定的任务集的硬件平台上执行时，产生的所有可能的响应时间中最大的那个响应时间就是该任务的WCRT

●响应时间分布

■ 图中曲线所示为响应时间的概率分布，从图可以看出，响应时间的分布绝大部分处于靠近最好响应时间(Best Case Response Time, BCRT)，而WCRT则是一个非常微小的点。



1. 汽车网络体系结构的时间分析

- 实时系统的开发生命周期：建模，分析，设计，实现几个阶段
- 分析的结果将作为设计阶段（验证、调度、优化）的时间输入参数
- 最坏执行时间(Worst Case Execution Time, WCET)
  - 最坏响应时间(Worst Case Response Time, WCRT)

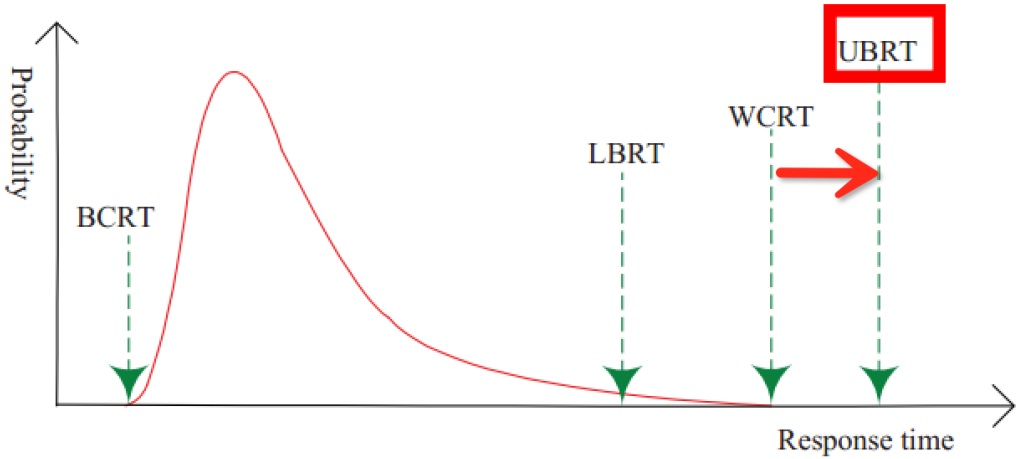
当该任务在给定的任务集的硬件平台上执行时，产生的所有可能的响应时间中最大的那个响应时间就是该任务的WCRT

●最坏响应时间的安全性

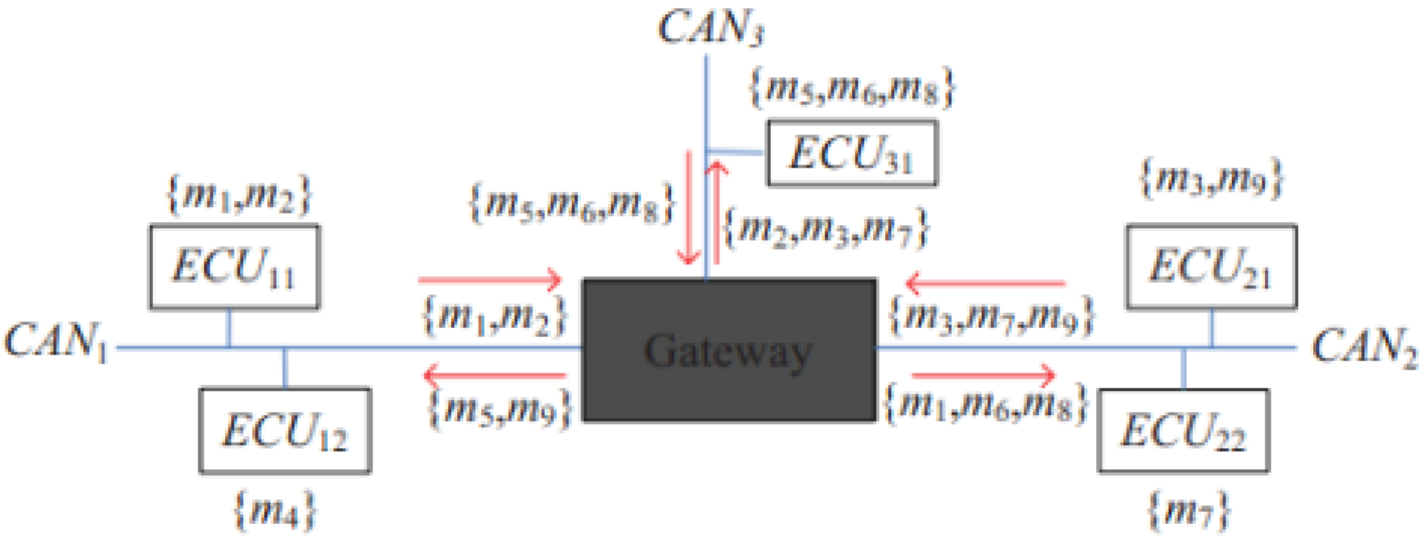
- ■ 一方面，我们必须在调度之前要找到WCRT
- ■ 另一方面，我们不能在伪多项式时间内找到WCRT

➢ **如何解决？**

✓ 既然精确的WCRT不好找，那么我们可以一个近似的WCRT，并且这个近似的值大于等于精确的WCRT的，我们称之为WCRT上界（Upper Bound on WCRT, UBRT）



●汽车内部：CAN Cluster (Multi-domain CAN Systems)



●分析对象：

□ECU中的任务， 多核ECU

□CAN总线上的消息， 端到端CAN消息

□网关中处理消息的任务， 单核，多核网关

●汽车中时间分析面临的新挑战

□模型挑战

✓通用实时系统中的模型无法映射到汽车中

✓汽车中ECU,网关,总线都需要分析，但又都是相互影响的

□分析方法挑战

✓通用实时系统中的方法（例如，忙周期）应用于汽车显得悲观

✓需要提出新的面向汽车体系结构的分析方法

提纲

Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

2. 汽车自适应平台的调度技术

- ISO 26262 定义了汽车安全完整性等级（Automotiv Safety Integration Level, ASIL）
- ASIL A 为最低级， ASIL D 为最高级
- 严重度Severity
- 暴露率Exposure
- 可控性 Controllability

表 1 严重度、暴露率、可控性分类

严重度		暴露率		可控性	
S0	无伤害	E1	很低的概率	C0	完全可控
S1	轻度和中度伤害	E2	低概率（1%）	C1	简单可控(>99%驾驶员)
S2	严重伤害（有生还可能）	E3	中度概率（1%-10%）	C2	一般可控（>90%驾驶员）
S3	致命伤害	E4	高概率(>10%）	C3	很难控制（<90%驾驶员）

●汽车混合关键级系统(Automotive Mixed-Criticality Systems)

□概念：将多个不同关键级别的功能集成到同一资源共享的硬件平台上并在该平台上执行。“关键级”强调某个功能的重要性和风险程度，并经过第三方的严格认证

严重度	暴露率	可控性		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

●汽车信息物理系统(Automotive Cyber-physical Systems, ACPS)

●汽车中的传感器与执行器通过对周围的物理环境进行全面的3600的信息采集、以及与周围行驶的汽车及基础设施进行实时交互，来实现对汽车的精确化、智能化和集成化控制

●高级辅助驾驶系统（Advanced Driver Assistance Systems, ADAS）是包括车道偏离警告、夜视、自适应巡航控制等多个功能的系统，它的实现依赖于汽车中的多种传感器对其周围的物理环境进行全面的信息采集

●汽车信息物理系统(Automotive Cyber-physical Systems, ACPS)

□汽车中的传感器与执行器通过对周围的物理环境进行全面的3600的信息采集、以及与周围行驶的汽车及基础设施进行实时交互，来实现对汽车的精确化、智能化和集成化控制

□高级辅助驾驶系统（Advanced Driver Assistance Systems, ADAS）是包括车道偏离警告、夜视、自适应巡航控制等多个功能的系统，它的实现依赖于汽车中的多种传感器对其周围的物理环境进行全面的信息采集

●ACPS的特征：

□异构性，动态行，并行性。CPS中许多事件是同时发生的；物理过程是很多动态与并行过程的组合；动态与并行是CPS的固有特征；CPS总是面临时序动态与并行问题的挑战- 《嵌入式系统导论-CPS方法》

□功能安全： 实时性，可靠性，可控性

□信息安全： 完整性，可用性，机密性

提纲

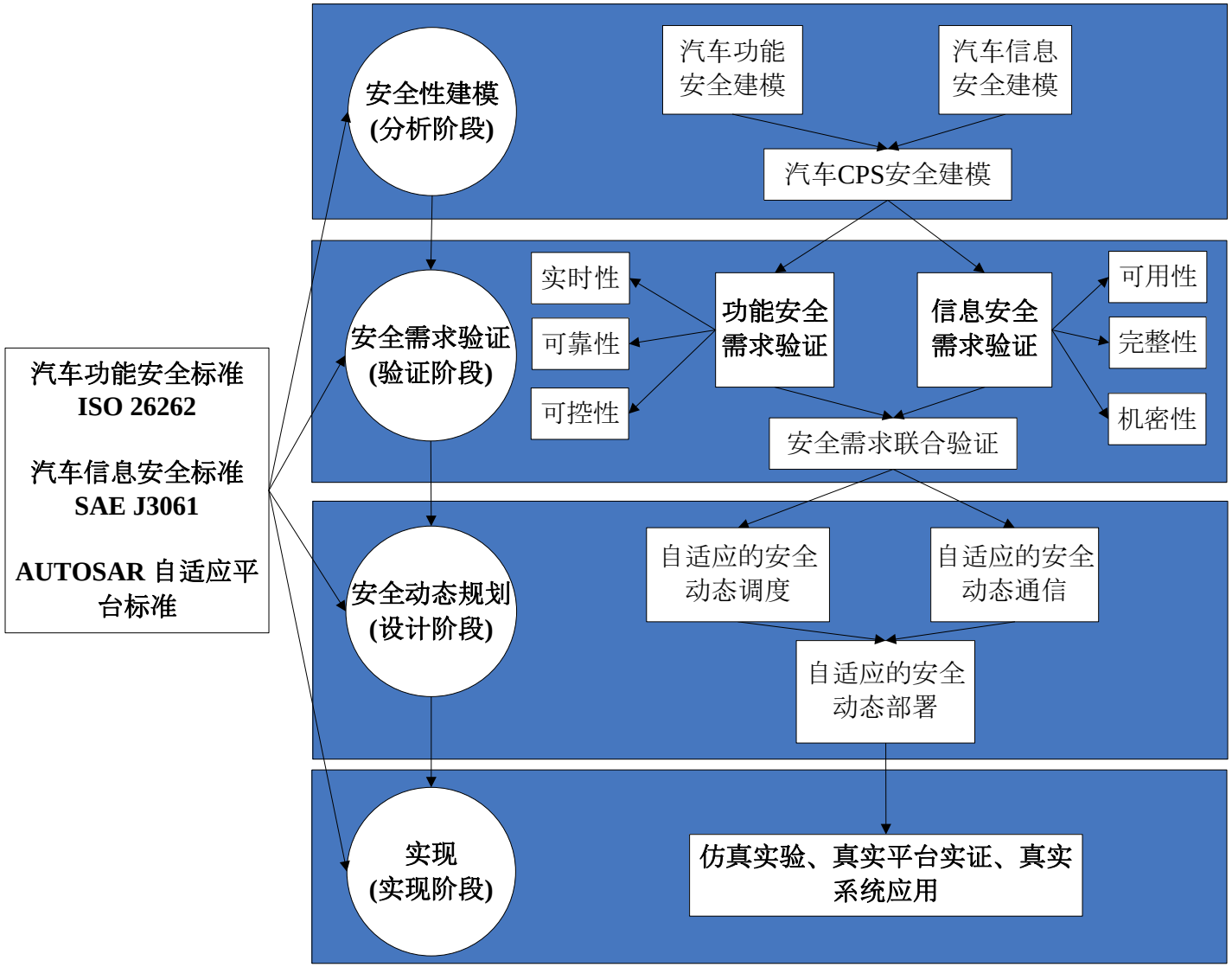
Part I. 汽车嵌入式系统的结构与标准

- ✓ 汽车体系结构
- ✓ 汽车功能安全标准
- ✓ 汽车信息安全标准
- ✓ AUTOSAR自适应平台标准

Part II.基于结构与标准的研究工作

- ✓ 汽车网络体系结构的时间分析
- ✓ 汽车自适应平台的调度技术
- ✓ 汽车软件工程的设计方法学

3. 汽车软件工程的设计方法学



●非功能属性优化

- 成本：考虑到大众市场， 汽车是成本极敏感的产业
- 能耗： 考虑到绿色环保，汽车也是能耗极敏感的产业

- 在满足功能安全和信息安全需求的前提下，优化这些属性

- 成本分类：
  - 资源成本：计算，通信资源的消耗
  - 硬件成本：ECU, 总线的配置类型与数量
  - 开发成本： 开发功能的程序员劳动力

以上3个成本在汽车中都需要优化

- 能耗优化：如果实现节能

近来发表的论文

1. **Guoqi Xie, Gang Zeng, Zhetao Li, Renfa Li, and Keqin Li. Adaptive Dynamic Scheduling on Multi-functional Mixed-Criticality Automotive Cyber-Physical Systems [J]. *IEEE Transactions on Vehicular Technology*, 2017**
2. **Guoqi Xie, Yuekun Chen, Yan Liu, Yehua Wei, Renfa Li, and Keqin Li. Resource Consumption Cost Minimization of Reliable Parallel Applications on Heterogeneous Embedded Systems[J]. *IEEE Transactions on Industrial Informatics*, 2017**
3. **Guoqi Xie, Junqiang Jiang, Yan Liu, Renfa Li, and Keqin Li. Minimizing Energy Consumption of Real-Time Parallel Applications on Heterogeneous Systems[J]. *IEEE Transactions on Industrial Informatics*, 2017**
4. **Guoqi Xie, Gang Zeng, Yuekun Chen, Yang Bai, Zhili Zhou, Renfa Li, and Keqin Li. Minimizing Redundancy to Satisfy Reliability Requirement for a Parallel Application on Heterogeneous Service-oriented Systems[J]. *IEEE Transactions on Industrial Informatics*, 2017**
5. **Guoqi Xie, Gang Zeng, Renfa Li, and Keqin Li. Energy-aware Processor Merging Algorithms for Deadline-constrained Parallel Applications in Heterogeneous Cloud Computing[J]. *IEEE Transactions on Sustainable Computing*, 2017**
6. **Guoqi Xie, Gang Zeng, Liangjiao Liu, Renfa Li, and Keqin Li. High Performance Real-time Scheduling of Multiple Mixed-criticality Functions in Heterogeneous Distributed Embedded Systems [J]. *Journal of Systems Architecture*, 2016, 70: 3-14**
7. **Guoqi Xie, Gang Zeng, Liangjiao Liu, Renfa Li, and Keqin Li. Mixed Real-Time Scheduling of Multiple DAGs-based Applications on Heterogeneous Multi-core Processors [J]. *Microprocessors and Microsystems*, 2016, 47:93-103**

谢谢大家，

欢迎各位专家批评指正！