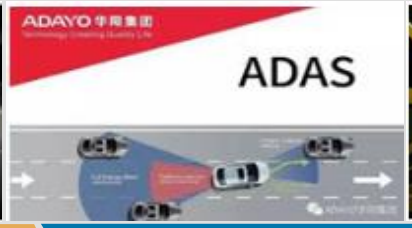
车用嵌入式系统中若干理论挑战与解决方案



报告人：谢国琪

湖南大学信息科学与工程学院

嵌入式与网络计算湖南省重点实验室

湖南大学 HUNAN UNIVERSITY

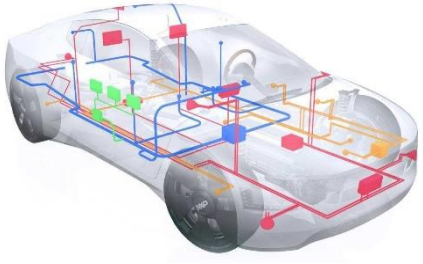
ETCC

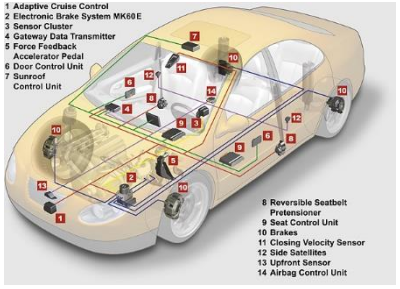
2020年中国嵌入式技术大会

EMBEDDED TECHNOLOGY Conference China 2020

汇报提纲

0. **开发背景**
1. **网络架构**
2. **软件系统**
3. **平台环境**
4. **总结思考**





0.1 背景-软件定义汽车

汽车工业经过一百多年的发展，机械部分已相对成熟，软件成为了带动汽车技术革新的关键

网联化　　自动化　　共享化　　电动化

Connected　Autonomous　Shared　Electric

软件定义汽车是汽车信息化与智能化发展的基础和核心

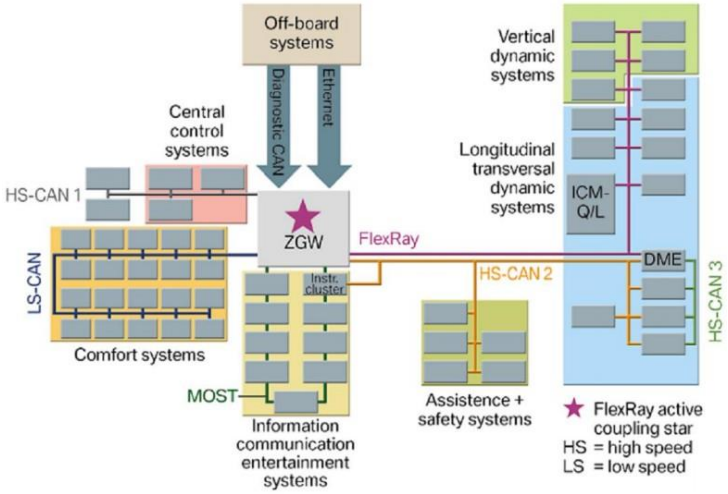
0.2 背景-三高

智能功能	燃油消耗	驾乘体验

三高：高成本敏感性、高安全要求、高开发门槛特性

0.3 背景-新的规范与标准

- 1）2010年起普及采用分布式集成网络架构；
- 2）2011年首次推出车用功能安全标准ISO 26262；
- 3）2017年首次推出AUTOSAR自适应平台标准。



代码量

全球汽车厂商与标准化组织逐步以自底向上的方式对整车网络架构、系统安全保障及软件平台实现提出了新的规范与标准

0.4 背景-催生效果

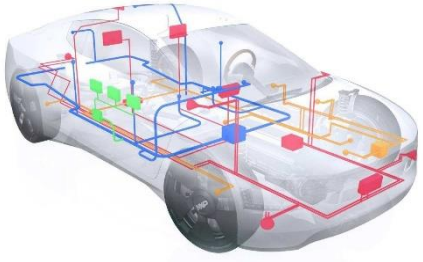
- 1）从架构上减少了车内线束和硬件的体积、重量与功耗（Size, Weight and Power consumption，SWaP）；
- 2）从安全标准上对车用软件系统加强了安全性约束；
- 3）从平台上统一了自动化与自适应软件系统的开发规范。

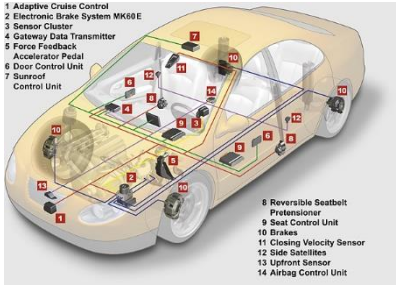
但产生了新的亟待解决的挑战性难题，以我们开发的三个车用嵌入式系统为例进行汇报

- BCM整车E/E架构
- 安全气囊系统
- 自适应前照灯系统

汇报提纲

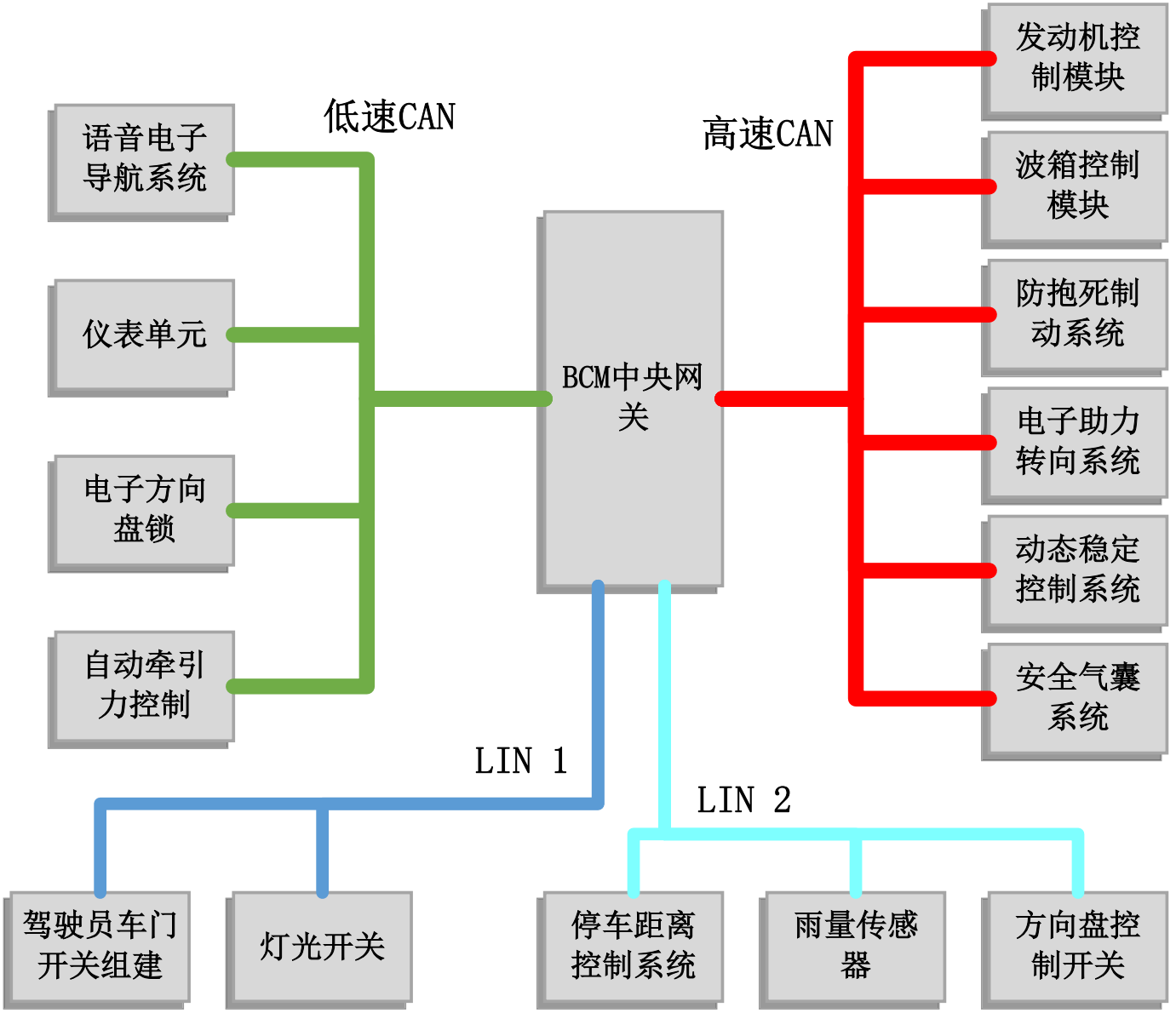
0. 开发背景
1. E/E架构
2. 软件系统
3. 平台环境
4. 总结思考





1.1 BCM整车E/E架构

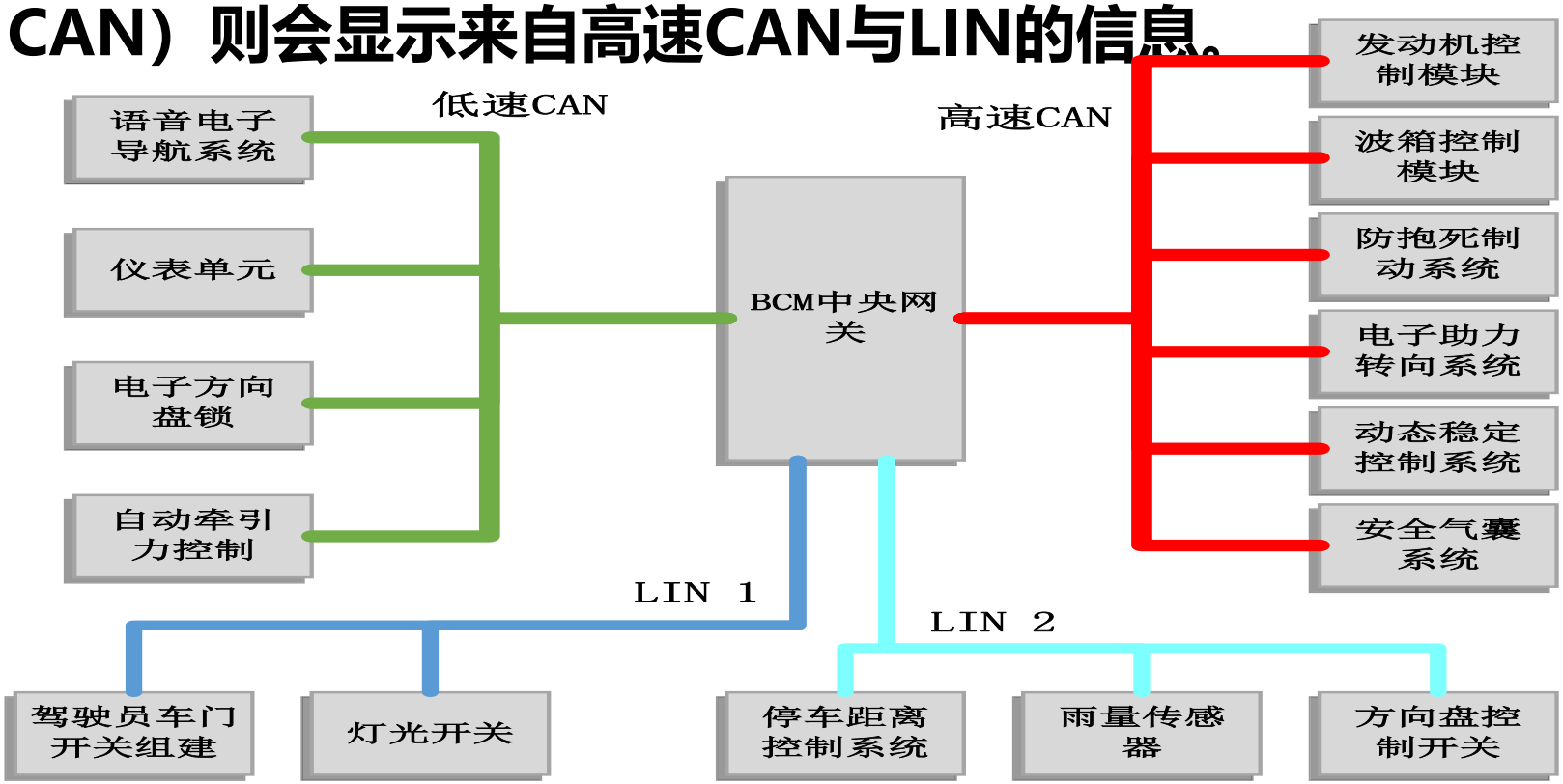
1个高速CAN网络域
1个低速CAN网络域
2个LIN网络域
1个中央网关



1.2 汽车网关的作用

中央网关是多个网络域进行数据交换的枢纽部件。

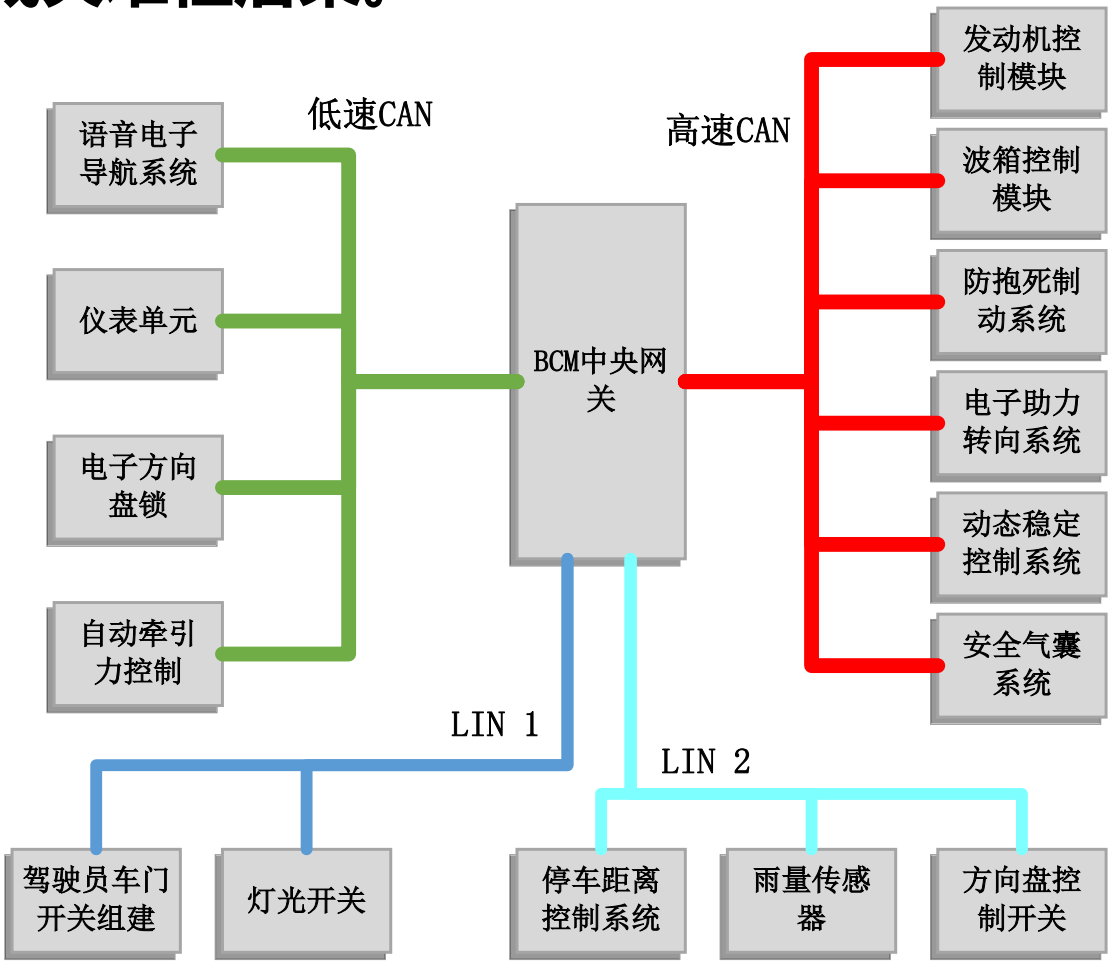
- 例如，通过网关的数据交换，发动机控制模块（高速CAN）从仪表单元（低速CAN）获取输入信号，而仪表单元（低速CAN）则会显示来自高速CAN与LIN的信息。



但经由网关造成的数据传输时延会直接影响安全关键软件系统的实时性，这也使得网关成为整个架构的处理瓶颈。

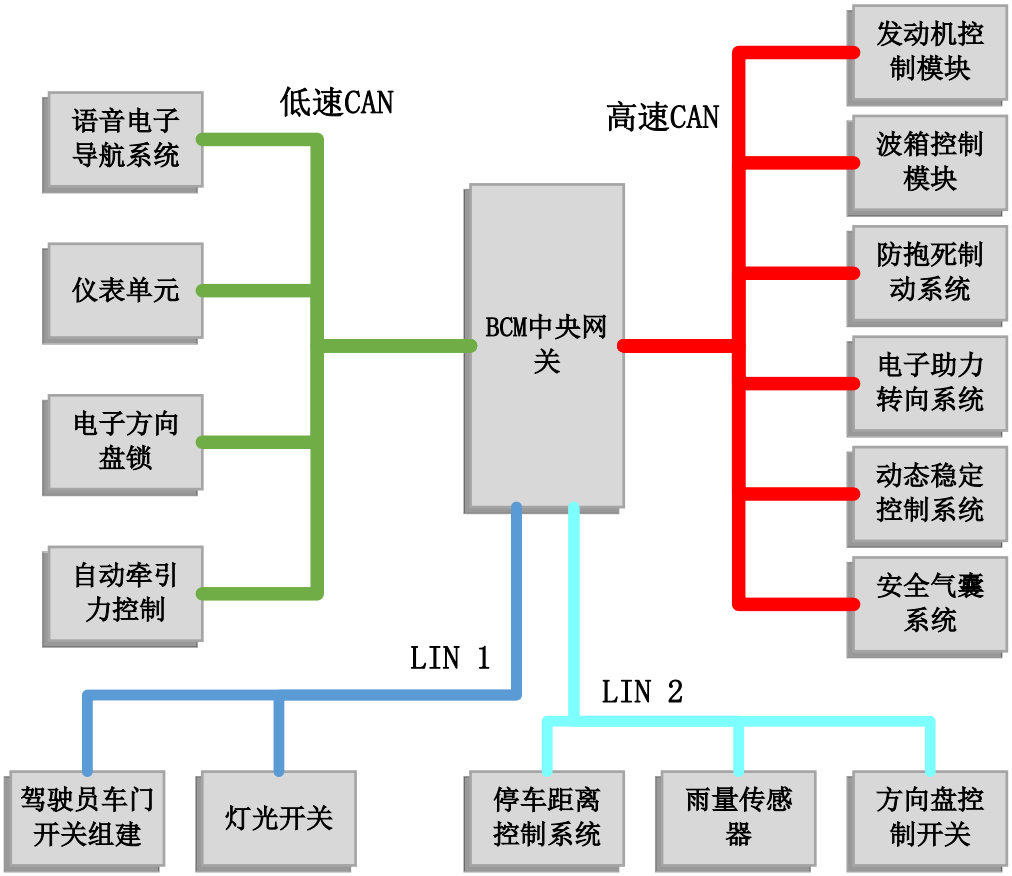
1.3 时延边界

- 要完成从一个网络域到另一个网络域的消息传送，设计者要准确把握网关的**通信时延边界**，避免系统在运行时错过实时性约束而造成灾难性后果。



1.3 时延边界

- 网络域之间需网关来交互信息，出现了两个网络域**相互影响**的现象，使得确定网关的**端到端通信时延边界**或最坏响应时间（Worse Case Response Time, WCRT）相当困难

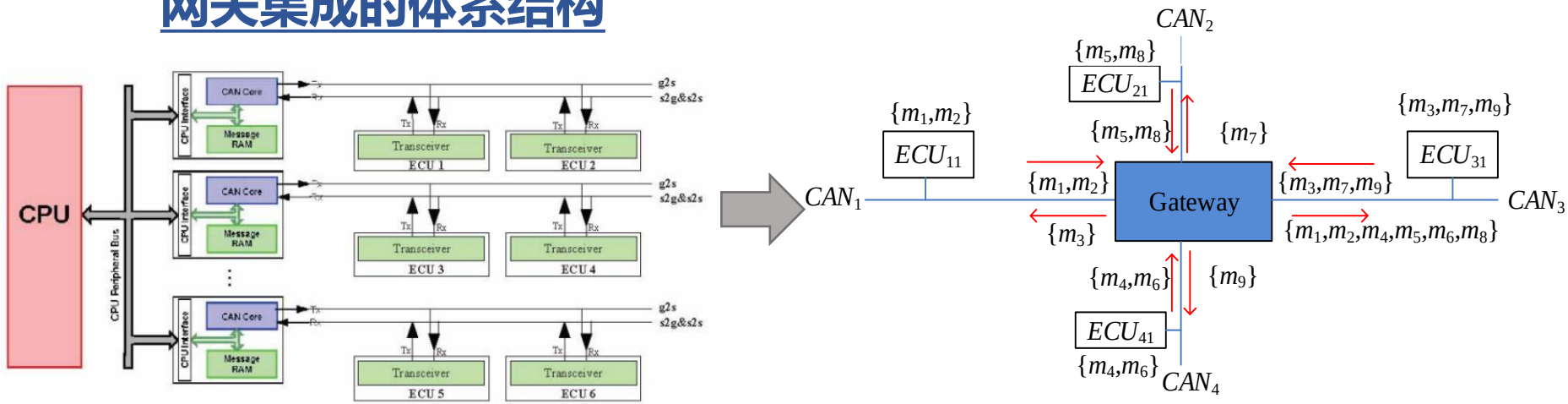


1.4 理论挑战：网关时延边界确定难

- 从联邦架构（之前）→集成体系结构（现在）。
- 以CAN集群为例的中央网关互连的集成体系架构。

实验测量手段：结果不稳定，不安全（安全隐患大）
实时分析技术：结果正确性难以保证（难度大）

网关集成的体系结构



1.5 解决方案

在分析单核汽车网关精确WCRT 的基础上，研究多核汽车网关的WCRT分析技术，进而研发出一种新型的实时汽车网关。

需要分析的时间：

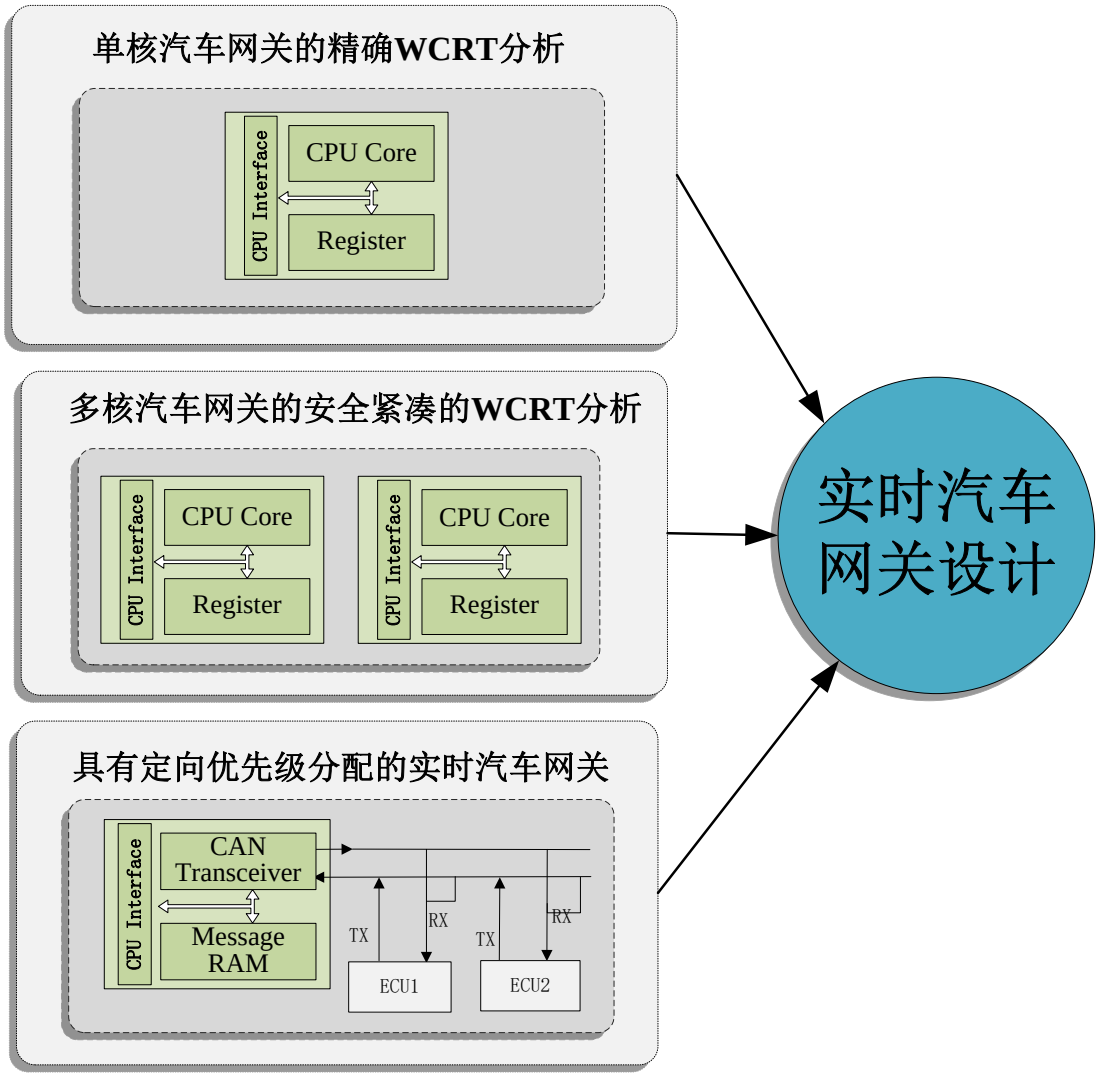
最坏响应时间（Worst Case Response Time, WCRT）

需要分析的部件：

网关:（单核，多核）

需要新的功能：

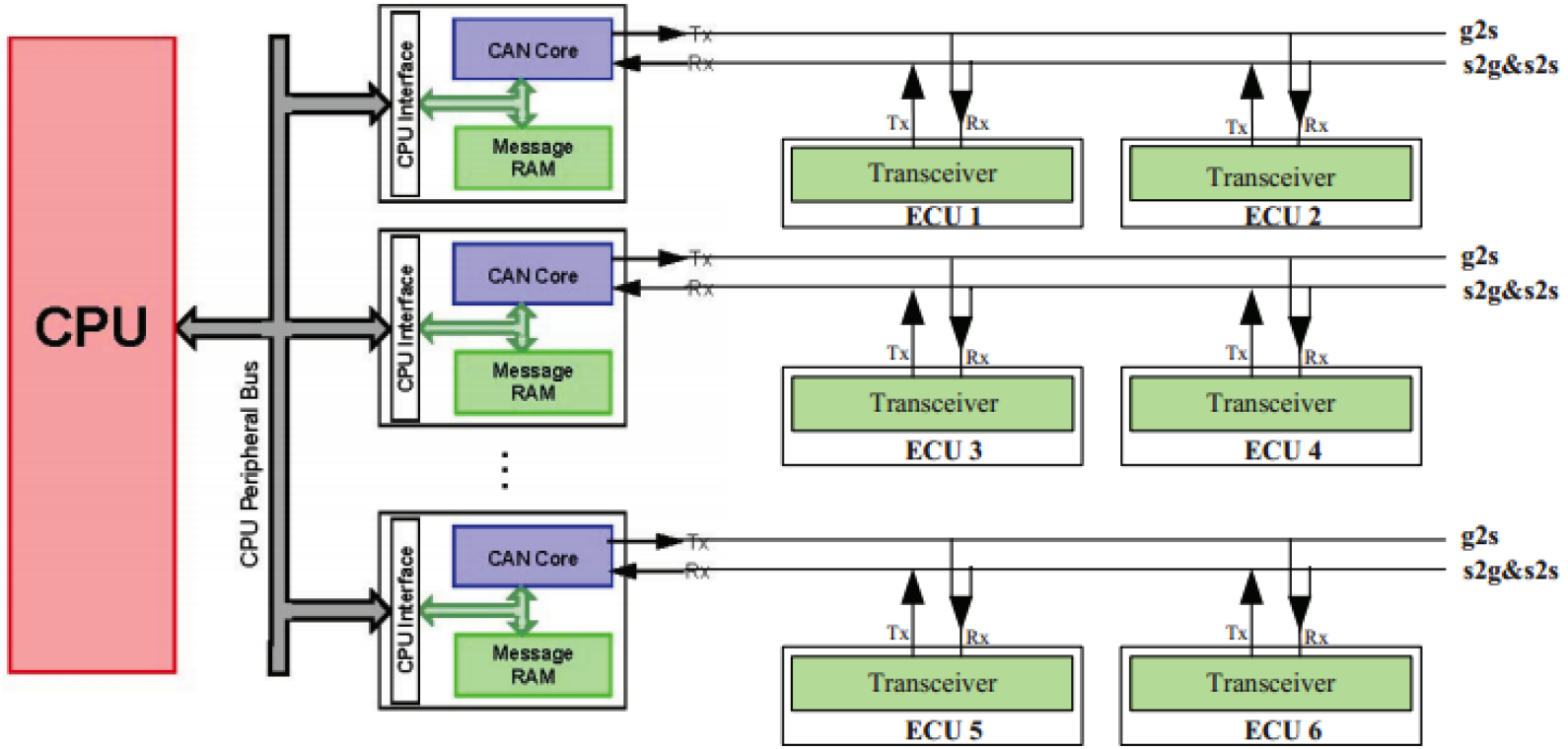
改善分析：定向优先级分配



1.6 单核网关的精确分析

●通过分析中央网关内部的结构与传输特性，提出了**轮搜索方法**，快速地找到时延上界与下界；

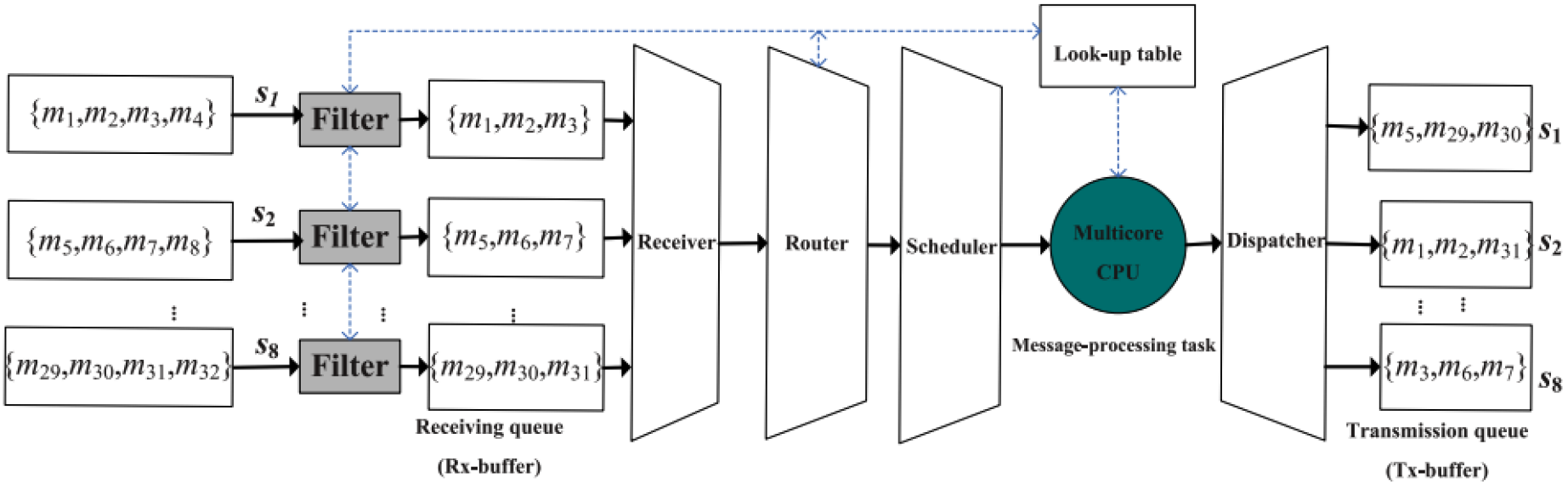
●通过**精化候选技术**，去除多达99.99999%的组合，快速地获得了单核汽车网关的精确WCRT。



1.7 多核网关的近似分析

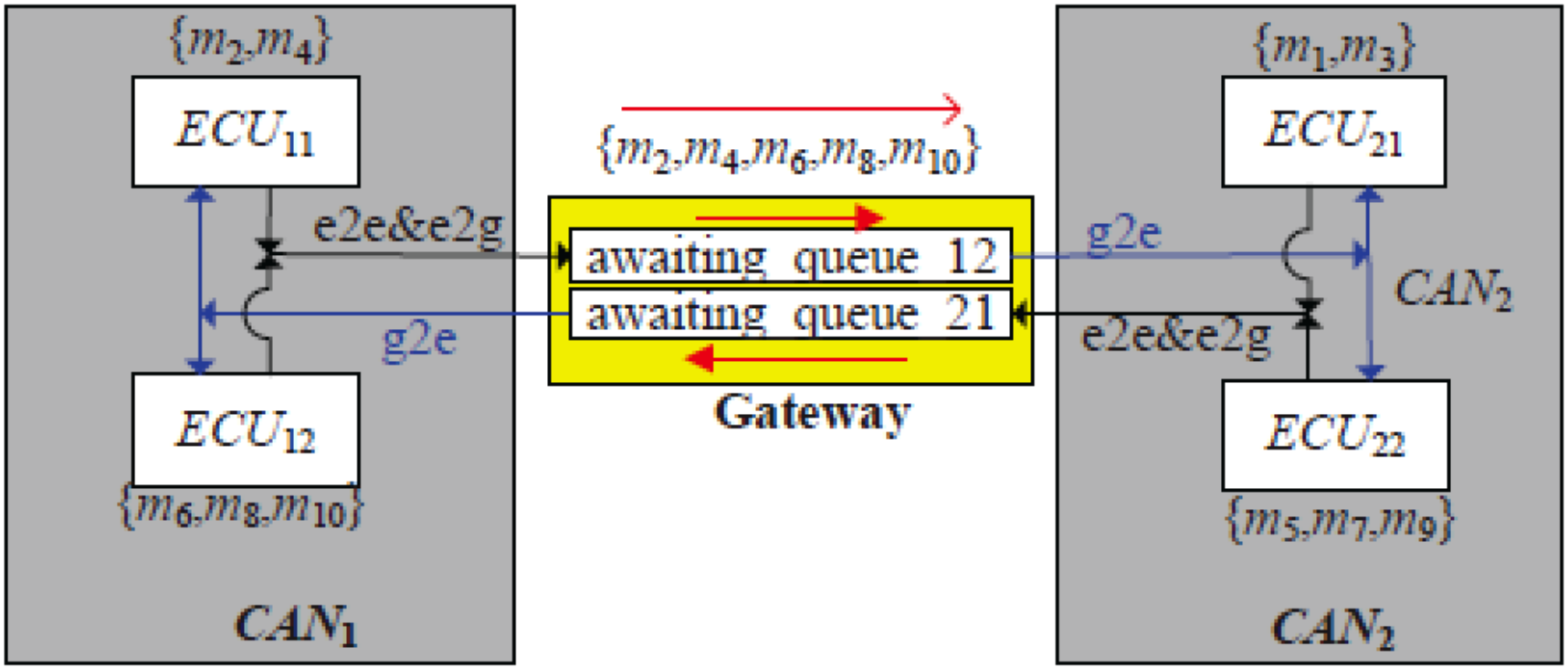
●针对多核汽车网关的**全局和分区调度**下的WCRT分析技术，根据实际消息集

●评估了两种分析技术的时延结果得出：**分区调度优于全局调度**，且使用四核网关可消除大规模CAN集群下网关传输时延。

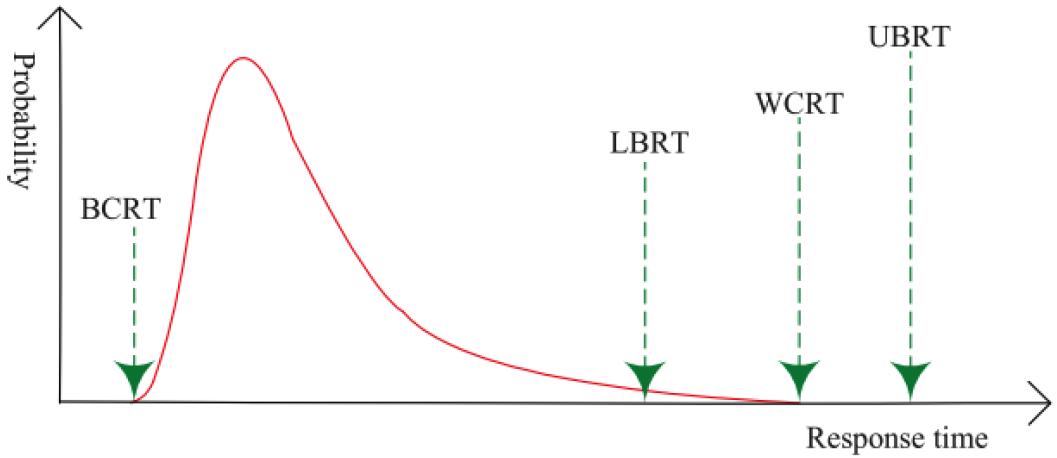


1.8 定向优先级分配

- 修改网关设计，将CAN控制器的队列移除，在网关内部增加等待队列
- 在等待队列里面定向调整部分CAN消息的优先级，提高可调度下



1.9 研究成果



面向集成架构的实时分析：

- 针对单核汽车网关的精确时间分析技术
- 针对多核汽车网关的安全紧凑时间分析技术
- 具备紧凑时间分析与定向优先级分配的实时汽车网关

G. Xie, G. Zeng, R. Kurachi, H. Takada, R. Li, K. Li, "Exact WCRT Analysis of Message-Processing Tasks on Gateway-Integrated In-Vehicle CAN Clusters," **ACM Transactions on Embedded Computing Systems**, 17(6): 95, Jan. 2019.

G. Xie, G. Zeng, R. Kurachi, H. Takada, Z. Li, R. Li, K. Li, "WCRT Analysis and Evaluation for Sporadic Message-Processing Tasks in Multicore Automotive Gateways," **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems**, 38(2): 281-294, Feb. 2019.

G. Xie, H. Gong, Y. Han, S. Chakraborty, W. Chang, "A Real-Time CAN-CAN Gateway with Tight Latency Analysis and Targeted Priority Assignment," **The 41st IEEE Real-Time Systems Symposium (RTSS)**,, Dec. 2020.

1.9 研究成果

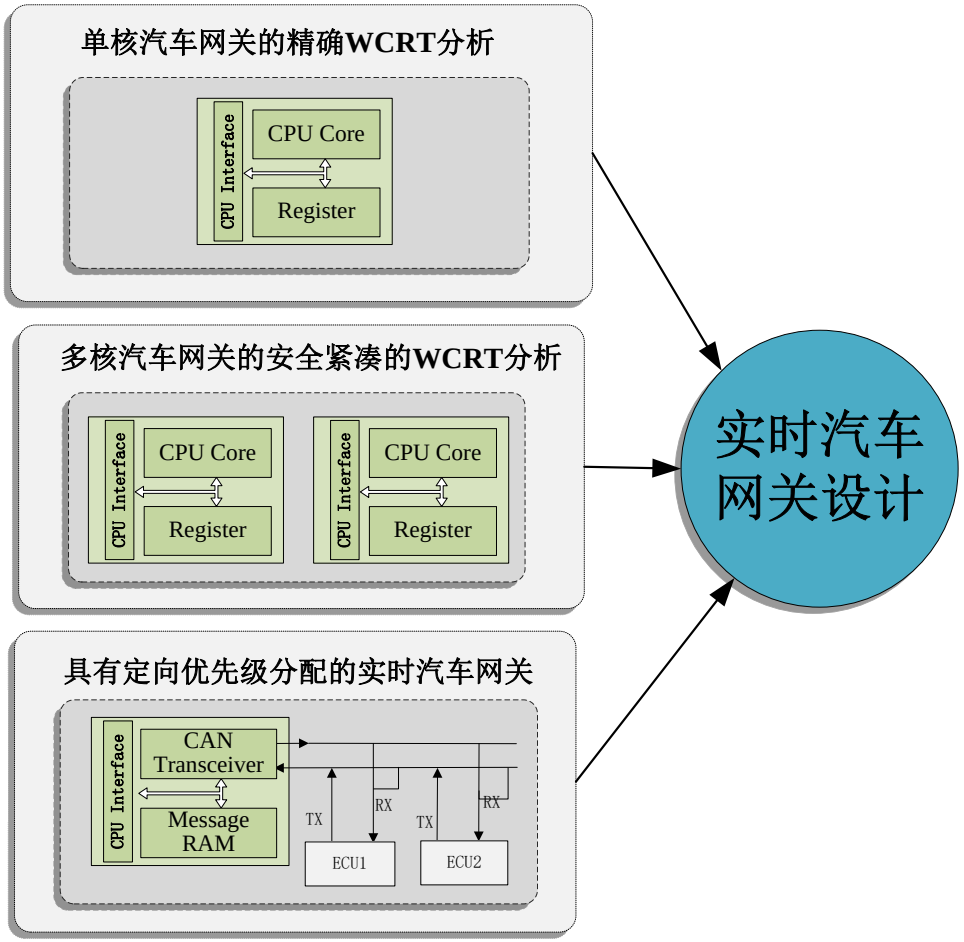
●三项WCRT结果组合串联起了从源端->网关->目的端的整个分析过程

●基于源端->网关->目的端的整个分析结果，改进E/E架构设计，确保端到端通信时延可安全确定的目的。

需要分析的时间：
最坏响应时间（Worst Case Response Time, WCRT）

需要分析的部件：
网关:（单核，多核）

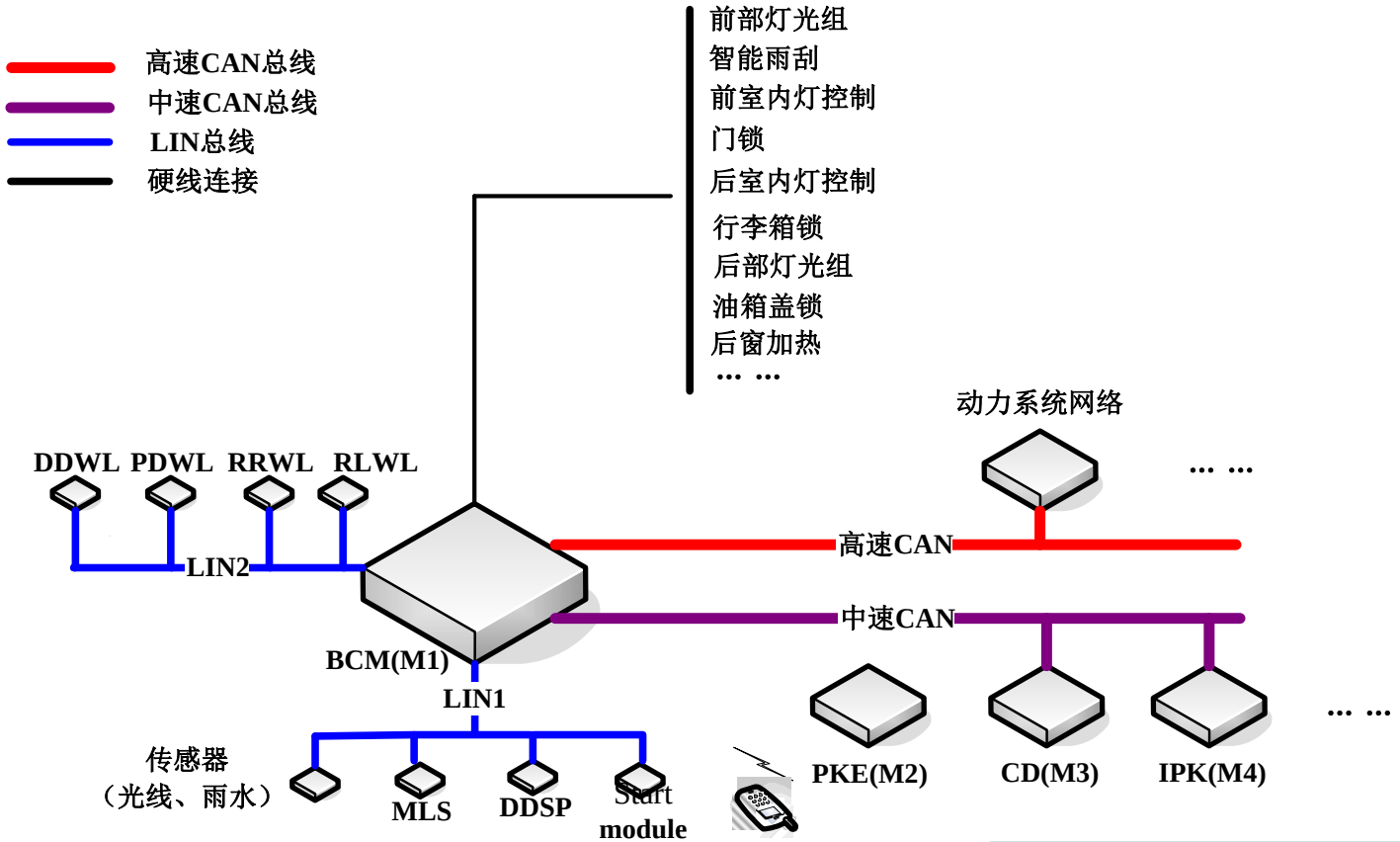
需要新的功能：
改善分析：定向优先级分配



1.10 开发成果

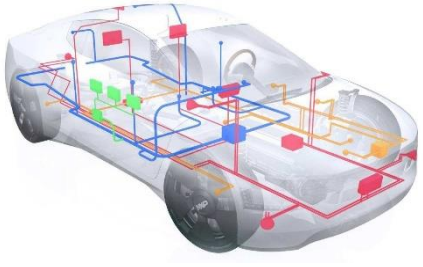
●基于上述三项WCRT分析成果，我们最终成功研发完成了BCM整车E/E架构，并用于实车。

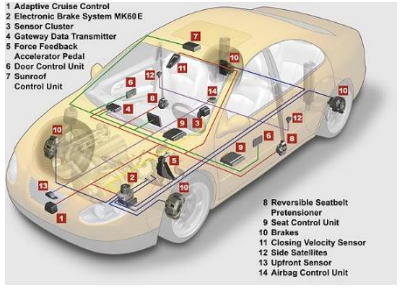
●以上成果解决了以BCM整车网络架构下实时通信时延边界计算的准确性问题，**排除了测量手段所引起的安全隐患。**



汇报提纲

0. 开发背景
1. 网络架构
2. **软件系统**
3. 平台环境
4. 总结思考



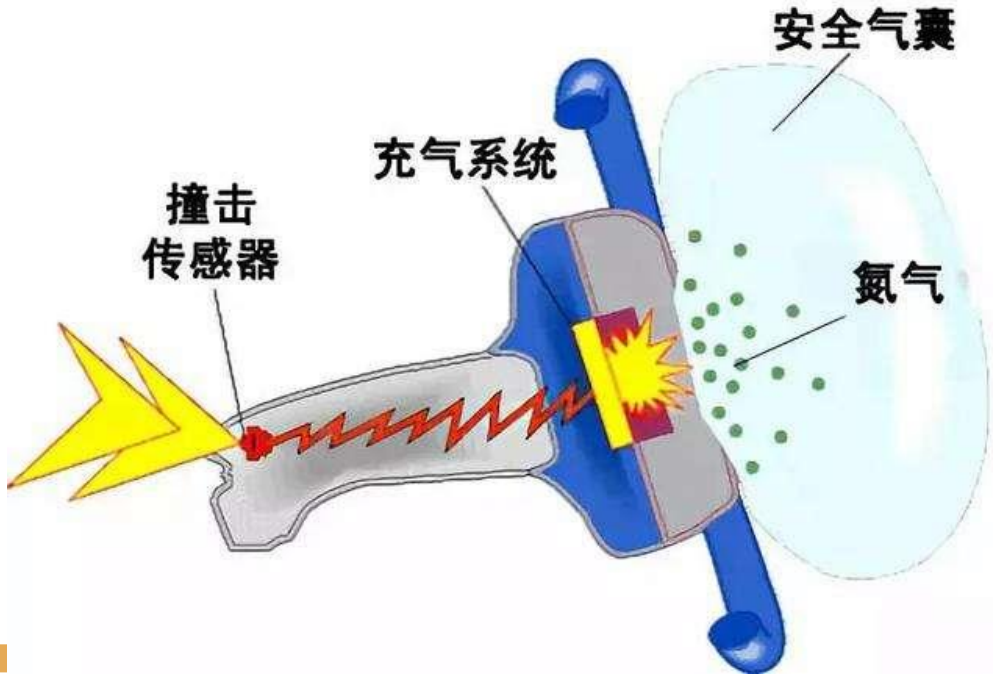


2.1 安全气囊系统

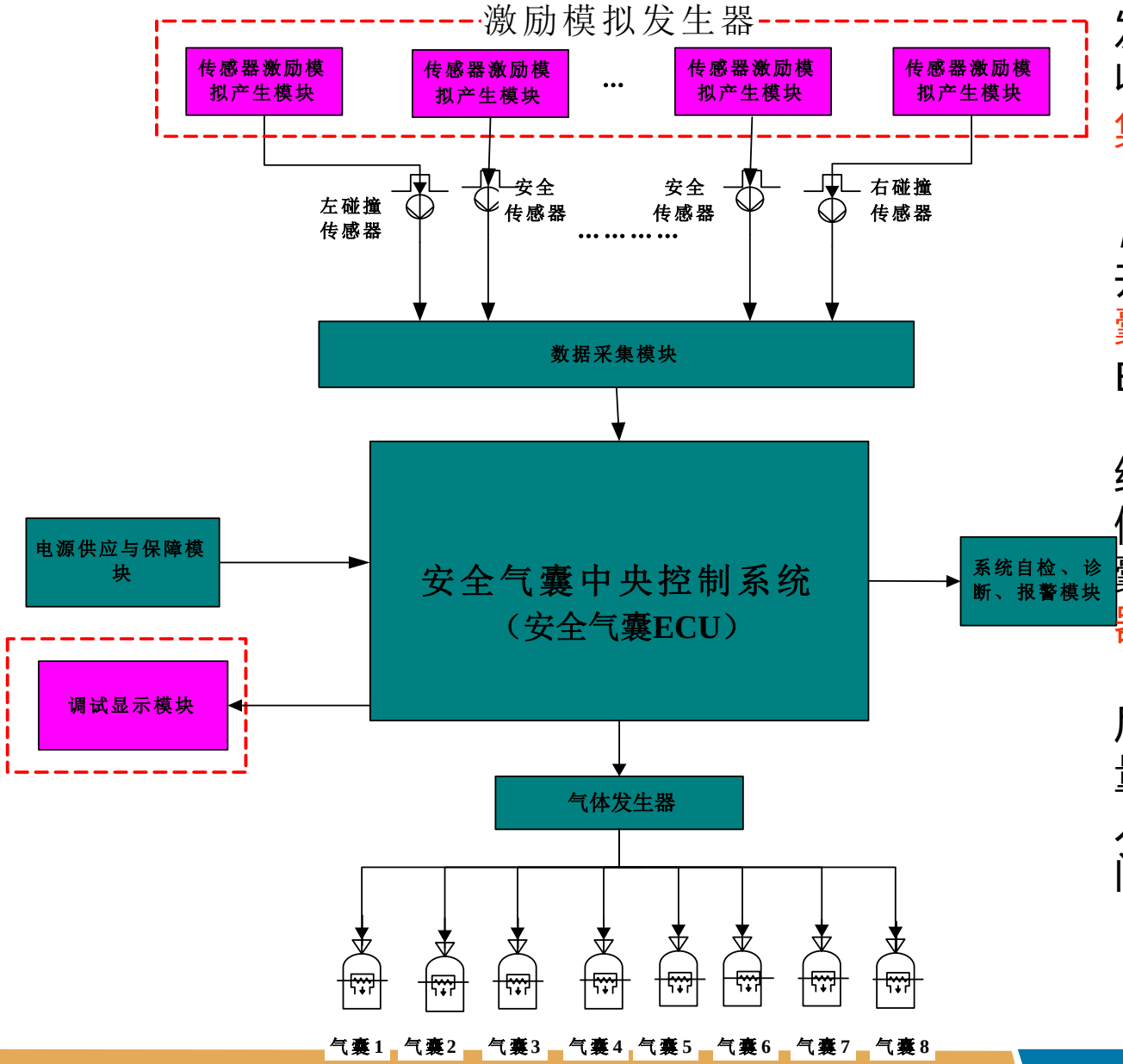
●安全气囊系统是现代轿车上几乎必备的安全技术装置之一。

●在车辆前端发生剧烈碰撞时，安全气囊会瞬间从方向盘内弹出，以防止驾驶者的头部和胸部撞击方向盘或仪表板等硬物。

●安全气囊自面市以来，已挽救了许多人的生命。研究表明，当轿车发生正面碰撞时，安全气囊可使驾驶者死亡率降低30%。



2.2 开发安全气囊系统



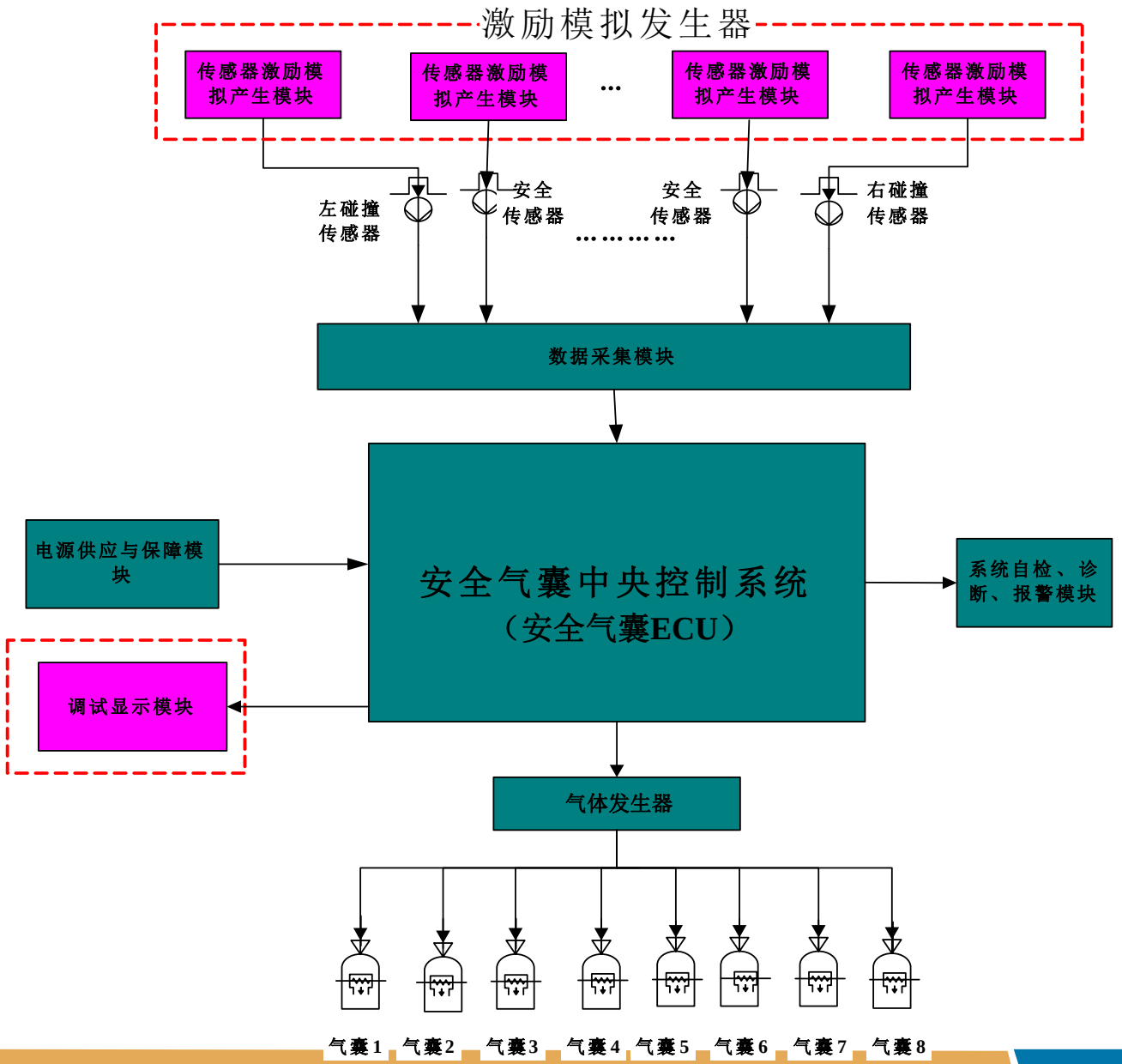
1）当汽车在行驶过程中发生碰撞时，安全传感器接收撞击信号并发送给数据采集模块；

2）只要达到规定的强度，安全传感器便产生动作，并由数据采集模块向安全气囊中央控制系统（安全气囊ECU）发出信号；

3）安全气囊中央控制系统接收到信号后，与其原存储信号进行比较，若达到气囊打开条件，则向气体发生器发送点火信号；

4）气体发生器接到信号后引燃气体发生剂，产生大量气体，经过滤并冷却后进入气囊，使气囊在极短的时间内突破衬垫迅速展开。

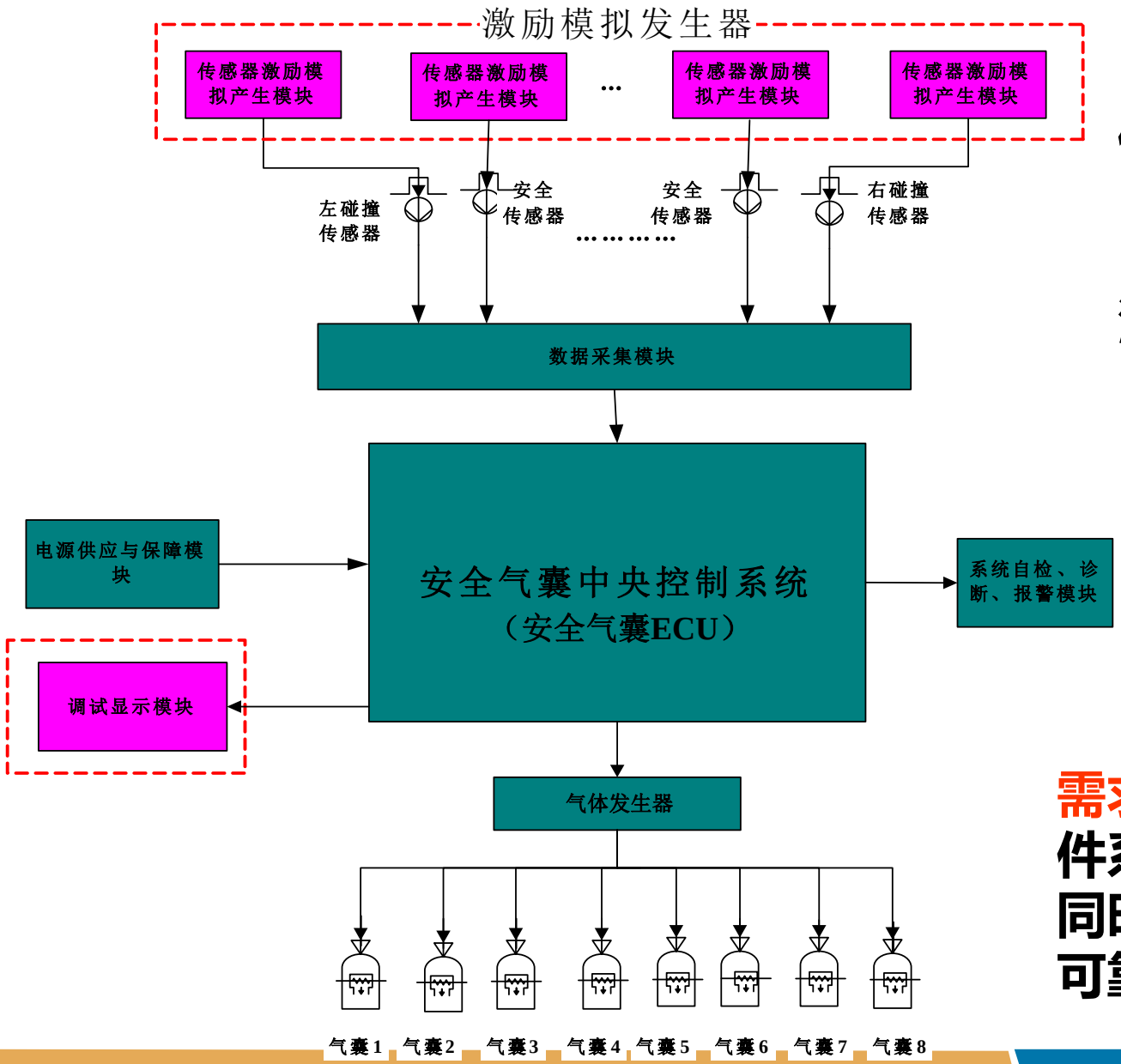
2.3 安全气囊系统的质量评价指标



1）可靠性目标：气体发生器是否能从气囊ECU准确地收到弹出信号

2）实时性约束：发送碰撞到气囊弹出的时间段是否满足规定的时延约束

2.3 安全气囊系统的质量评价指标



- 若信号接收的概率太低，可靠性就降低
- 若时延太长，便无法满足实时性约束

需求： 满足安全关键软件系统的安全目标需要同时满足实时性约束与可靠性目标。

2.4 理论挑战：安全系统重复开发几率高

- ISO 26262：对于安全关键软件系统，需要在系统完成后再通过检查和测评来进行安全验证与确认操作，若完成的软件系统无法满足安全目标，则需重新设计与实现，直到满足安全目标为止。

先实现、再验证与确认：重复开发几率高，设计负担重、周期长与成本高等风险，这些风险开发时难以降低或避免。

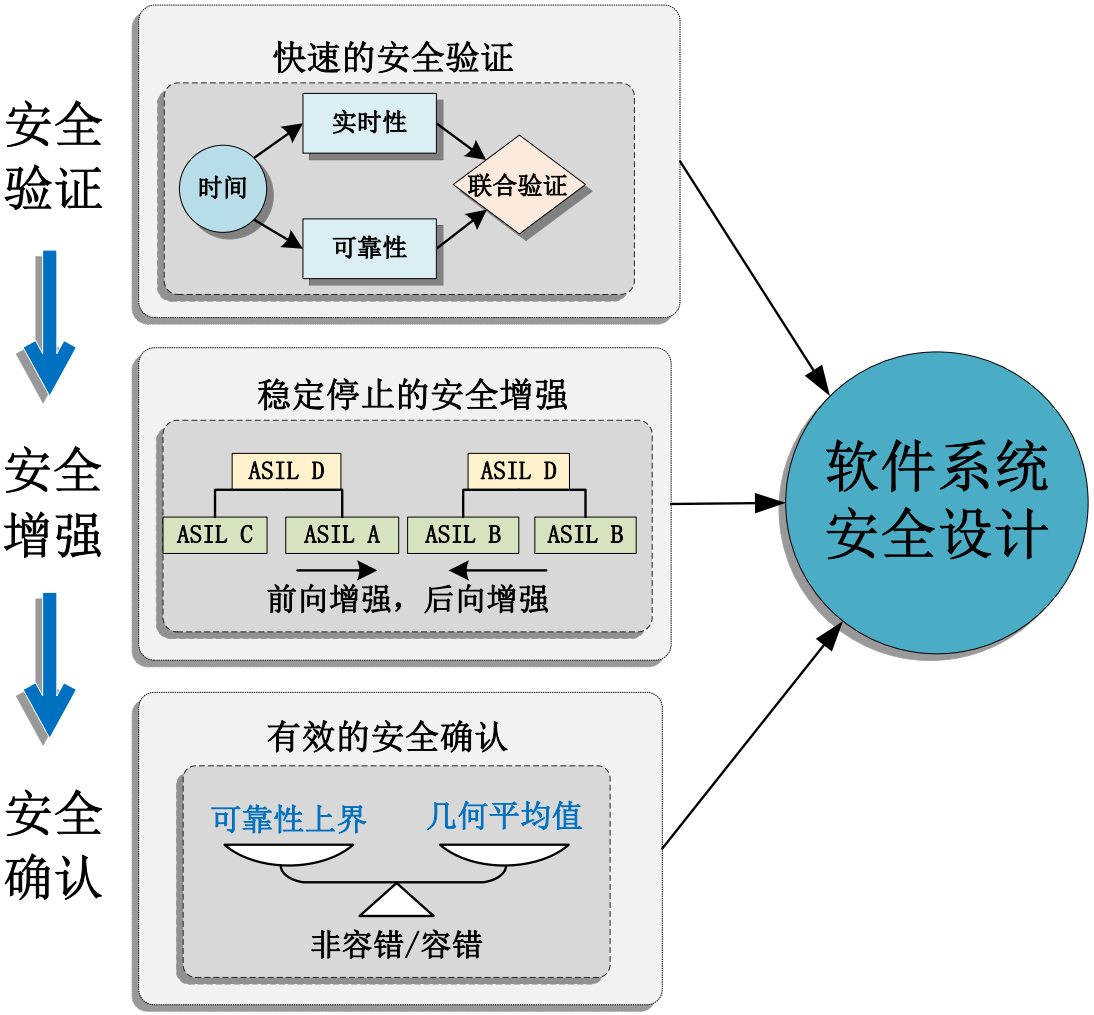
2.5 解决方案

- 在软件系统设计的早期阶段就预先验证与确认实现安全目标所需要达到的条件，有效了避免上述困境

功能安全验证（功能安全评估）：判断软件系统是否达到其功能安全需求

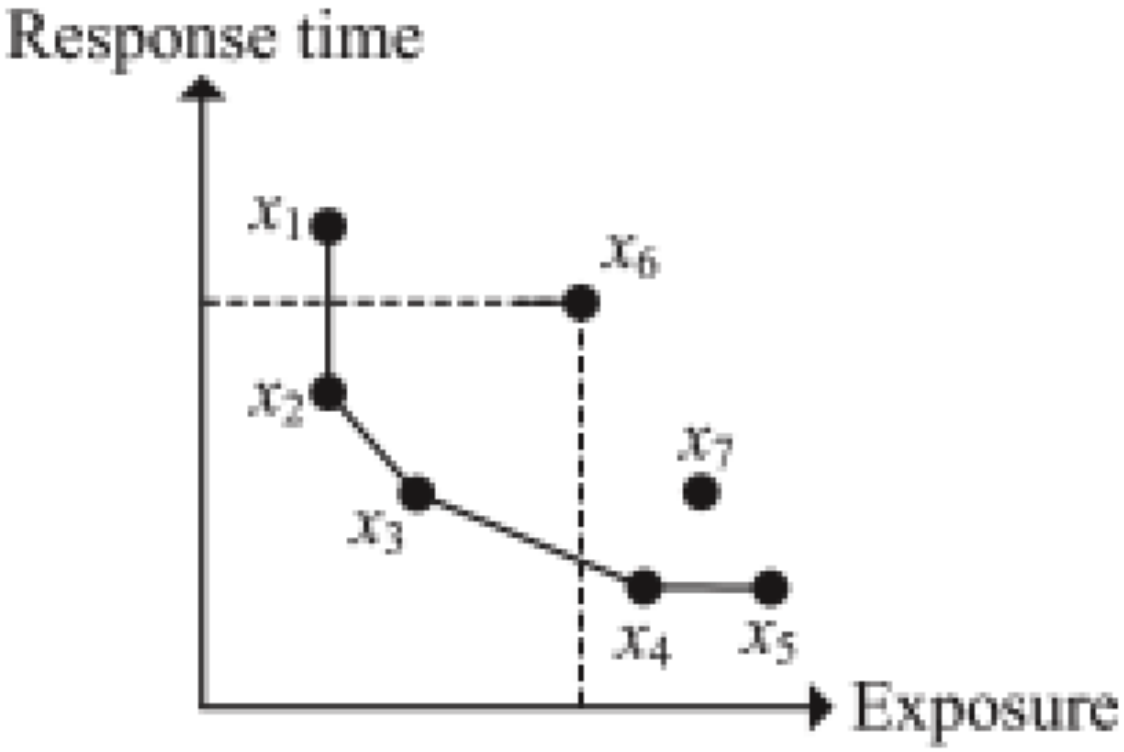
功能安全增强：增加安全值（如通过增加可靠性值来降低暴露率）以控制风险

功能安全确认（功能安全保证）：由检查和测试以足够的完整性级别实现安全目标



2.6 安全验证

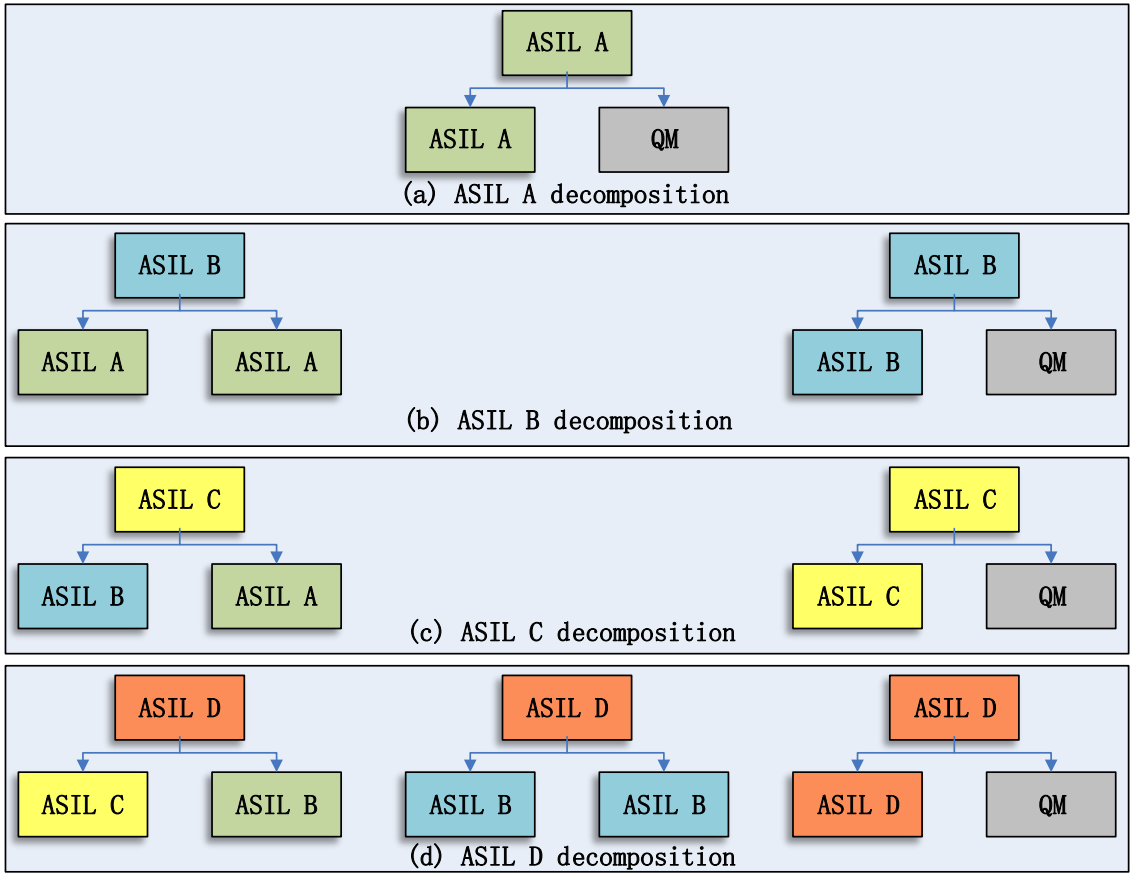
- **量化出安全目标中的两个核心条件（即实时性约束与可靠性目标）**
- **安全验证算法：依据这两个条件构建对偶问题，快速判别安全目标获得满足的可能性**



2.7 安全增强

- 基于稳定停止的安全增强算法：及时补救安全验证未通过的功能点

- 是后向增强、前向增强、复制的后向增强、复制的前向增强的有机组合，且能快速收敛



2.8 安全确认

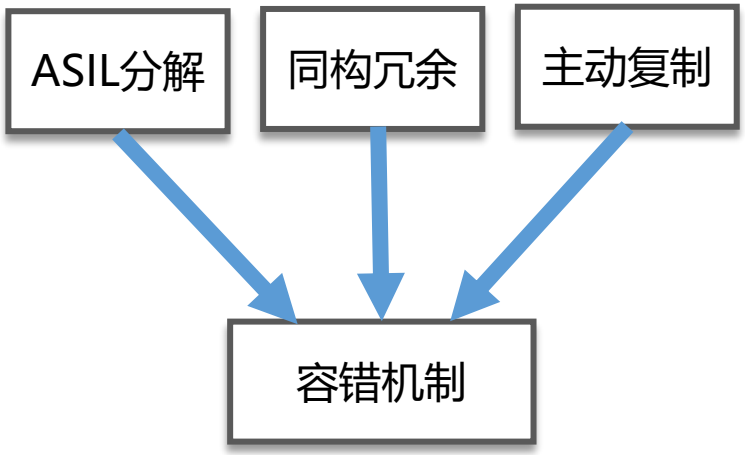
1）**基于几何平均值的安全确认算法，使组件之间的可靠性值呈集中趋势，从而以更平衡的方式来提高安全确认的精度。**

$$GM = \sqrt[|N|]{t_1 \times t_2 \times \cdots \times t_{|N|}}.$$

严重性	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

2.9 研究成果

基于冗余的容错机制



- 快速联合的功能安全验证算法
- 稳定停止的功能安全增强算法
- 基于几何平均值的功能安全确认算法

G. Xie, G. Zeng, Y. Liu, J. Zhou, R. Li, K. Li, “Fast Functional Safety Verification for Distributed Automotive Applications During Early Design Phase,” **IEEE Transactions on Industrial Electronics**, 65(5): 4378 - 4391, May 2018.

G. Xie, H. Peng, Z. Li, J. Song, Y. Xie, R. Li, K. Li, “Reliability Enhancement Towards Functional Safety Goal Assurance in Energy-Aware Automotive Cyber-Physical Systems,” **IEEE Transactions on Industrial Informatics**, 14(12): 5447-5462, Dec. 2018.

G. Xie, G. Zeng, J. An, R. Li, K. Li, "Resource Cost-Aware Fault-Tolerant Design Methodology for End-To-End Functional Safety Computation on Automotive Cyber-Physical Systems," **ACM Transactions on Cyber-Physical Systems**, 3(1):4, Jan. 2019.

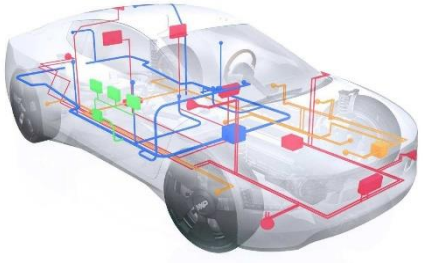
2.10 开发成果

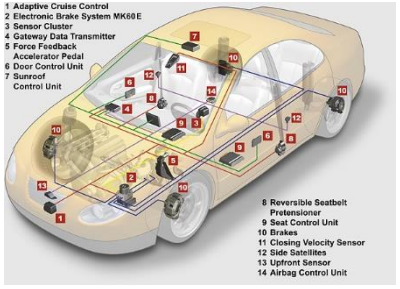
基于上述软件系统安全设计成果（验证、增强与确认），为国内某汽车厂商成功研发了中高档轿车安全气囊系统

安全气囊系统在无锡国家进出口检疫局（安全气囊检测国家授权单位）进行 “台车实验”的现场。

汇报提纲

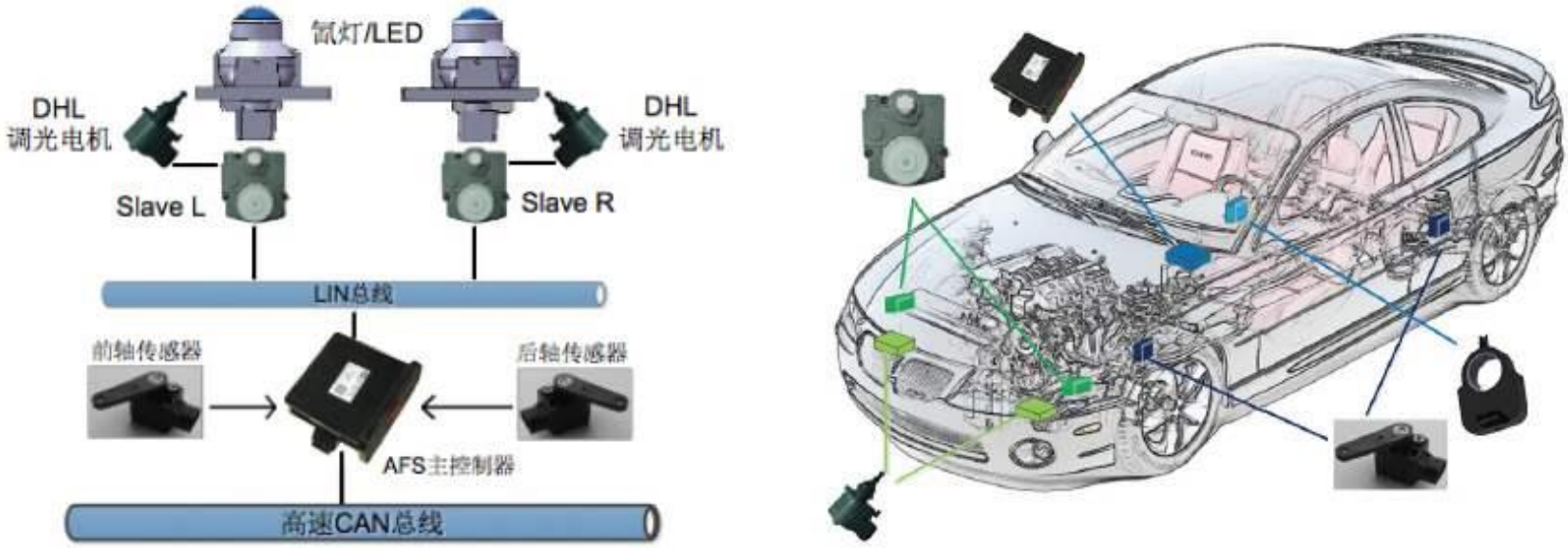
0. 开发背景
1. 网络架构
2. 软件系统
3. 平台环境
4. 总结思考





3.1 自适应前照灯系统

一种**智能灯光调节**系统，它通过感知驾驶员操作（方向盘转角）、车辆行驶状态（车速）、车身悬架高度、GPS、陀螺仪信息、路面变化及天气环境等信息，**自适应地控制前照灯的照明亮度**、照射范围和照明角度，为驾驶员提供舒服的道路照明效果。



AFS 系统（上下左右调节功能）

3.2 AUTOSAR经典平台标准

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

□自适应系统普及：自适应前照灯系统、自适应巡航控制系统、自适应安全气囊系统等软件系统被并应用于商用轿车中

□响应滞后：若仍采用AUTOSAR经典平台标准来运行这类”自适应软件系统”，可能存在响应滞后的现象

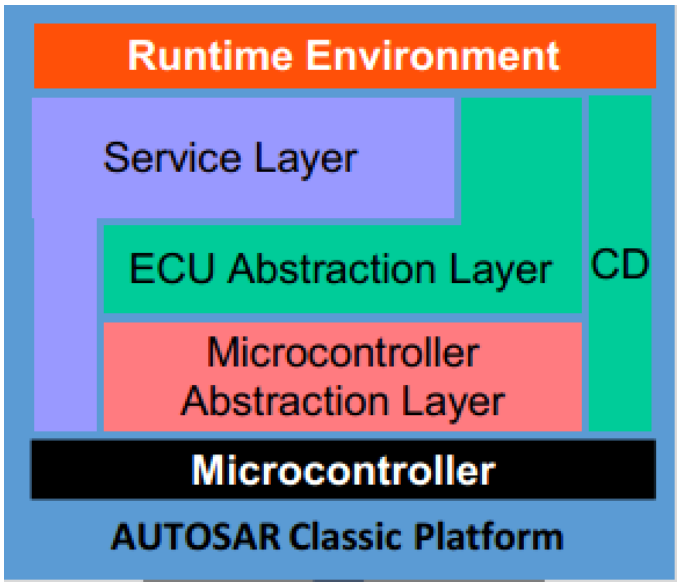
3.3 AUTOSAR 自适应平台标准

首次发布时间：2017年5月

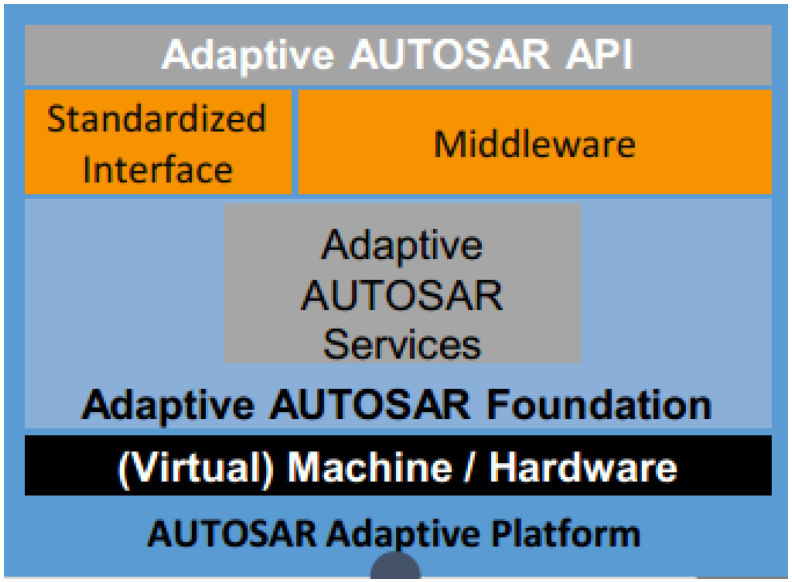
发布原因：为了支持汽车日益增长的动态释放的自治功能， 自动驾驶

之前的标准：已改为AUTOSAR经典平台（AUTOSAR Classic Platform）

2003年



2017年



3.4 理论挑战-自适应平台与开发环境实现难

- 第一种是实现全新的AUTOSAR自适应平台

✓ 优点：与标准更契合
✓ 缺点：成本高且容易与现有开发环境冲突

- 第二种是对现有AUTOSAR经典平台进行升级改造

✓ 优点：成本低且与现有开发环境易兼容，
✓ 缺点：难以找准突破口；若没有找准升级改造的突破口，则可能造成“牵一发而动全身”的后果

3.5 自适应平台标准要求

AUTOSAR新平台标准全面支持**动态规划**（Planned Dynamics）。

口动态调度：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；

口动态通信：功能能够通过面向服务的通信机制实现动态通信；

口动态部署： 系统能够根据自身需求的变化来实现自适应的动态重配置（重映射与重调度）

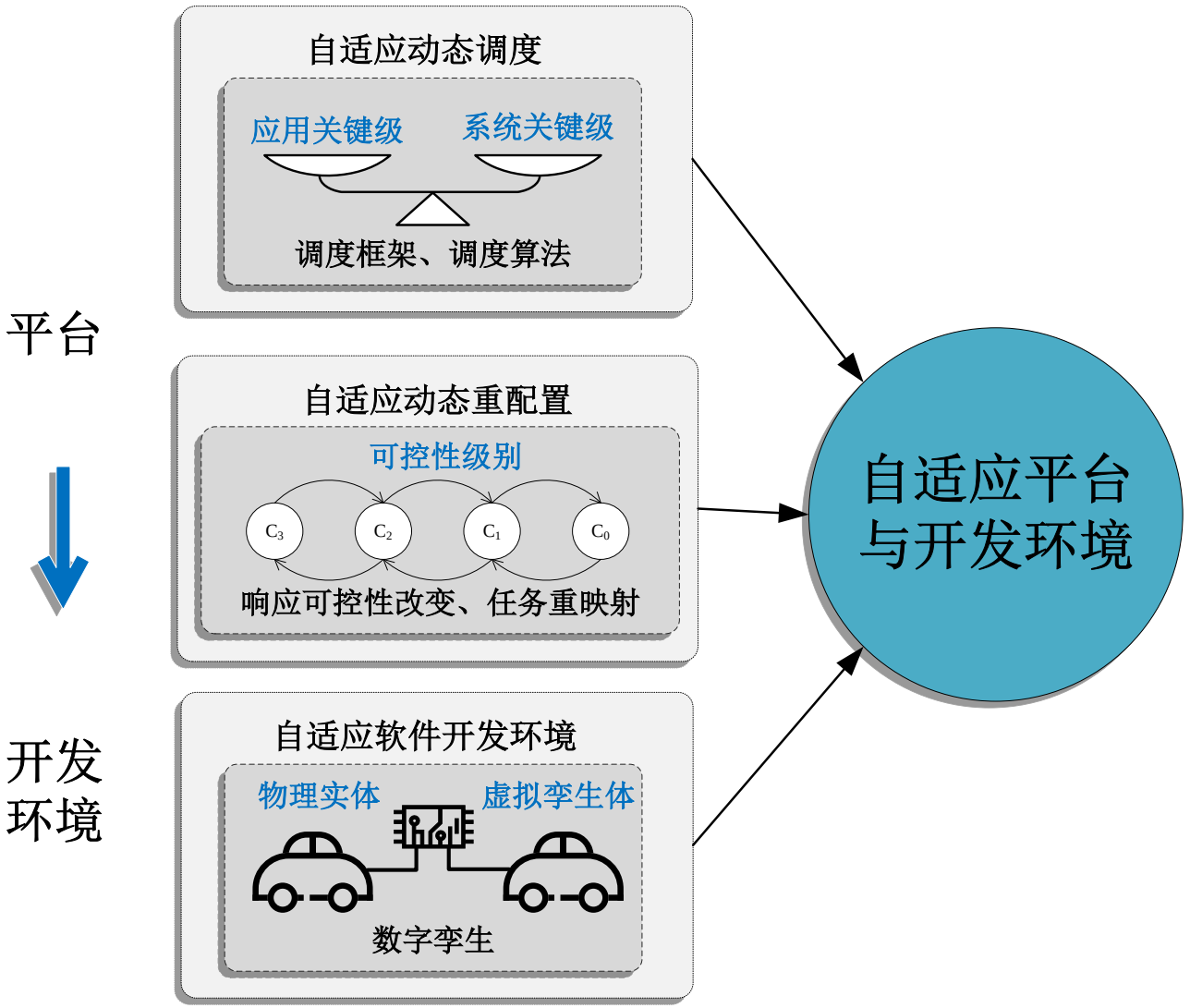
是一个支持并行计算、安全性、关键性和功能集成的异构计算平台

3.6 解决方案

动态调度：平台能够自适应的响应软件系统的动态释放、分配及错误报告

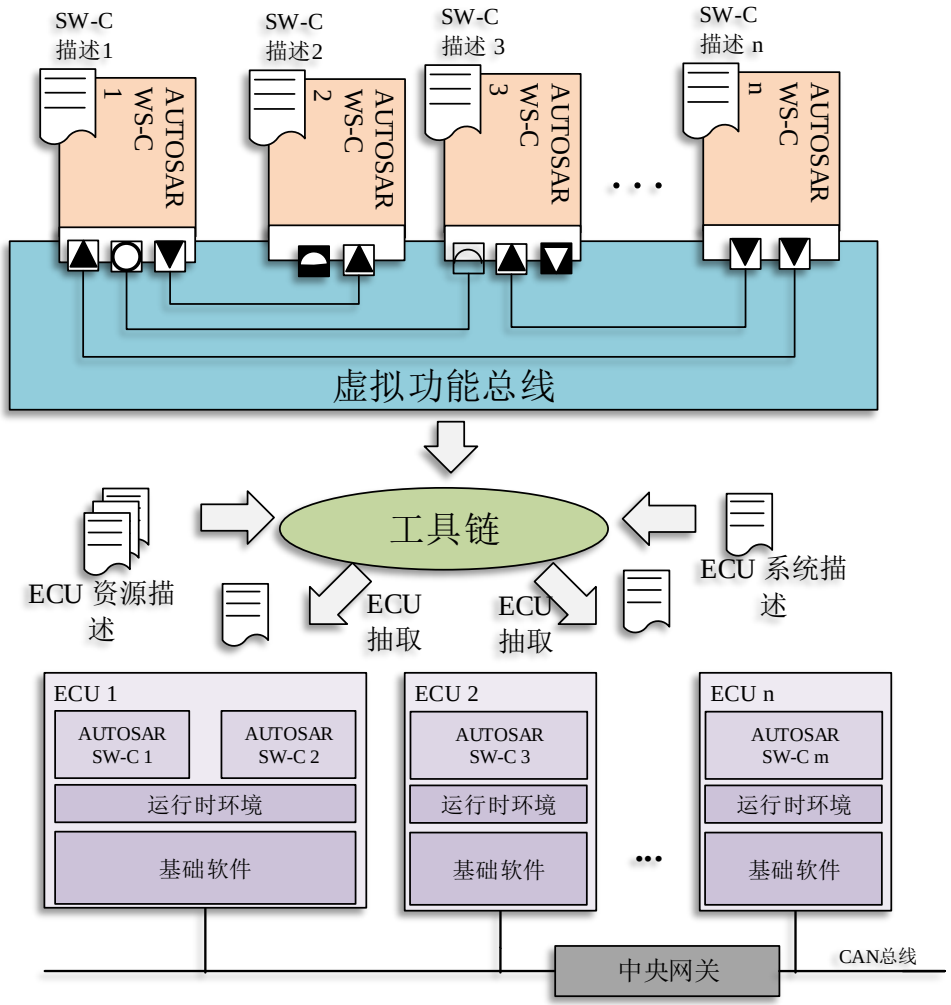
动态重配置：软件系统能够根据自身需求的变化来实现自适应的动态重映射与重调度

自适应开发环境：开发过程具备高扩展性与高灵活性，且可方便地满足开发过程中各种变化的设计需求



3.7 自适应调度

- **模式切换：** 根据各软件系统的关键级别及平台实时负载情况，自适应地切换 “平台关键级”，实现了自适应动态调度框架与算法。

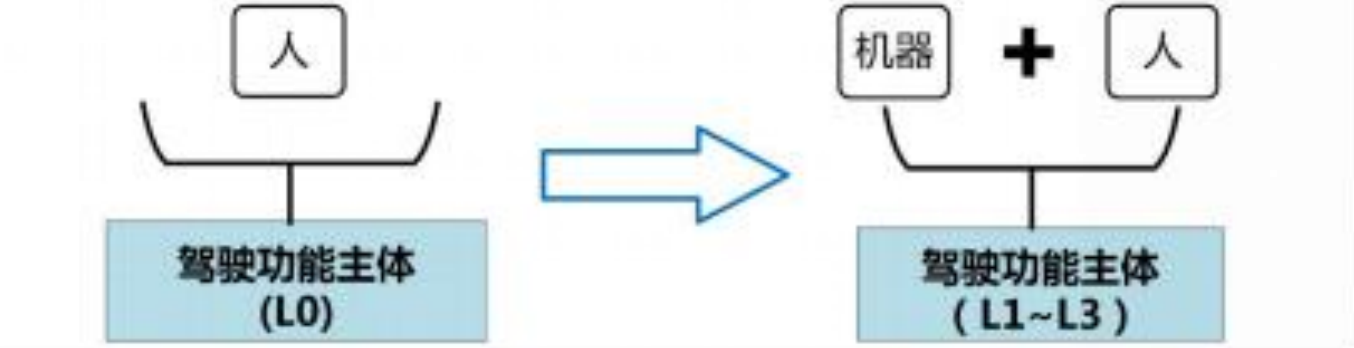


3.8 自适应重配置

- 感知驾驶员与平台之间的**人机交互**，在满足安全关键软件系统的功能安全目标的前提下减少其冗余配置，并提高平台的运行性能

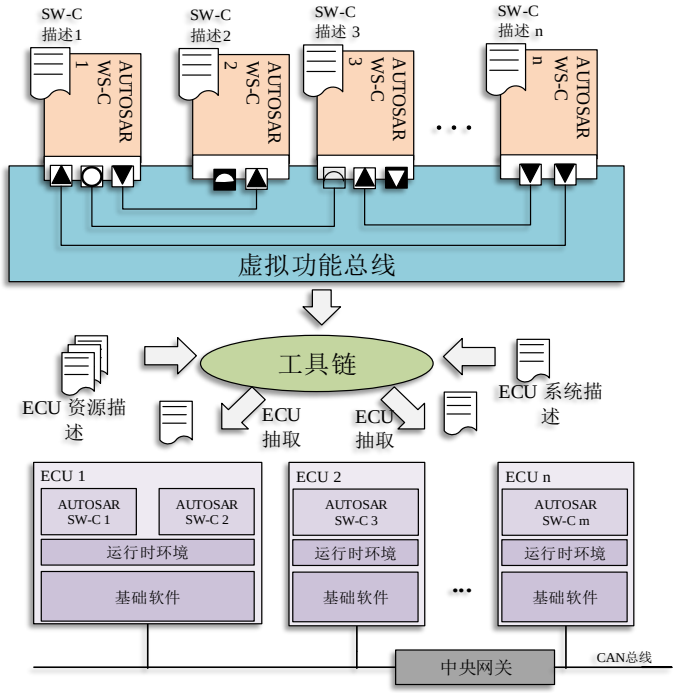
自动驾驶分级（SAE）

SAE分级	SAE命名	功能			区域	
		驾控主体	感知接管	监控干预	道路条件	环境条件
Level 0	完全人类驾驶	人	人	人	任何	任何
Level 1	辅助驾驶	人|机器	人	人	限定	限定
Level 2	部分自动驾驶	机器	人	人	限定	限定
Level 3	有条件自动驾驶	机器	机器	人	限定	限定
Level 4	高度自动驾驶	机器	机器	机器	限定	限定
Level 5	完全自动驾驶	机器	机器	机器	任何	任何

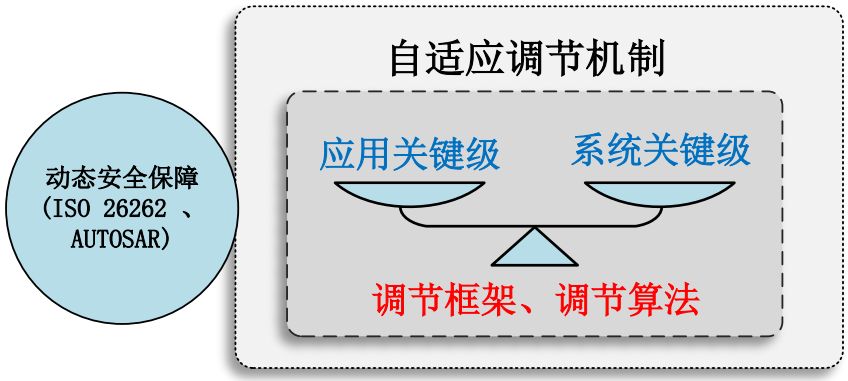


3.9 研究成果

提出自适应调节框架



形成动态保障机制



- 关键级调节驱动的自适应动态调度
- 人机交互感知的自适应功能安全处理

G. Xie, G. Zeng, Z. Li, R. Li, K. Li, "Adaptive Dynamic Scheduling on Multifunctional Mixed-Criticality Automotive Cyber-Physical Systems," **IEEE Transactions on Vehicular Technology**, 66 (8): 6676 - 6692, Aug. 2017.

G. Xie, Y. Bai, W. Wu, Y. Li, R. Li, K. Li, "Human-Interaction-Aware Adaptive Functional Safety Processing for Multi-Functional Automotive Cyber-Physical Systems," **ACM Transactions on Cyber-Physical Systems**, 3(4): 39, Aug. 2019.

3.10 自适应软件开发环境

●**汽车厂商希望**：提高车用嵌入式软件系统的开发效率来应付激烈的市场竞争。

●**实际开发过程存在的问题**：开发周期长、可伸缩性差、测试完整性低等问题。

●**启用数字孪生技术：**

3.11 需要解决2个关键问题

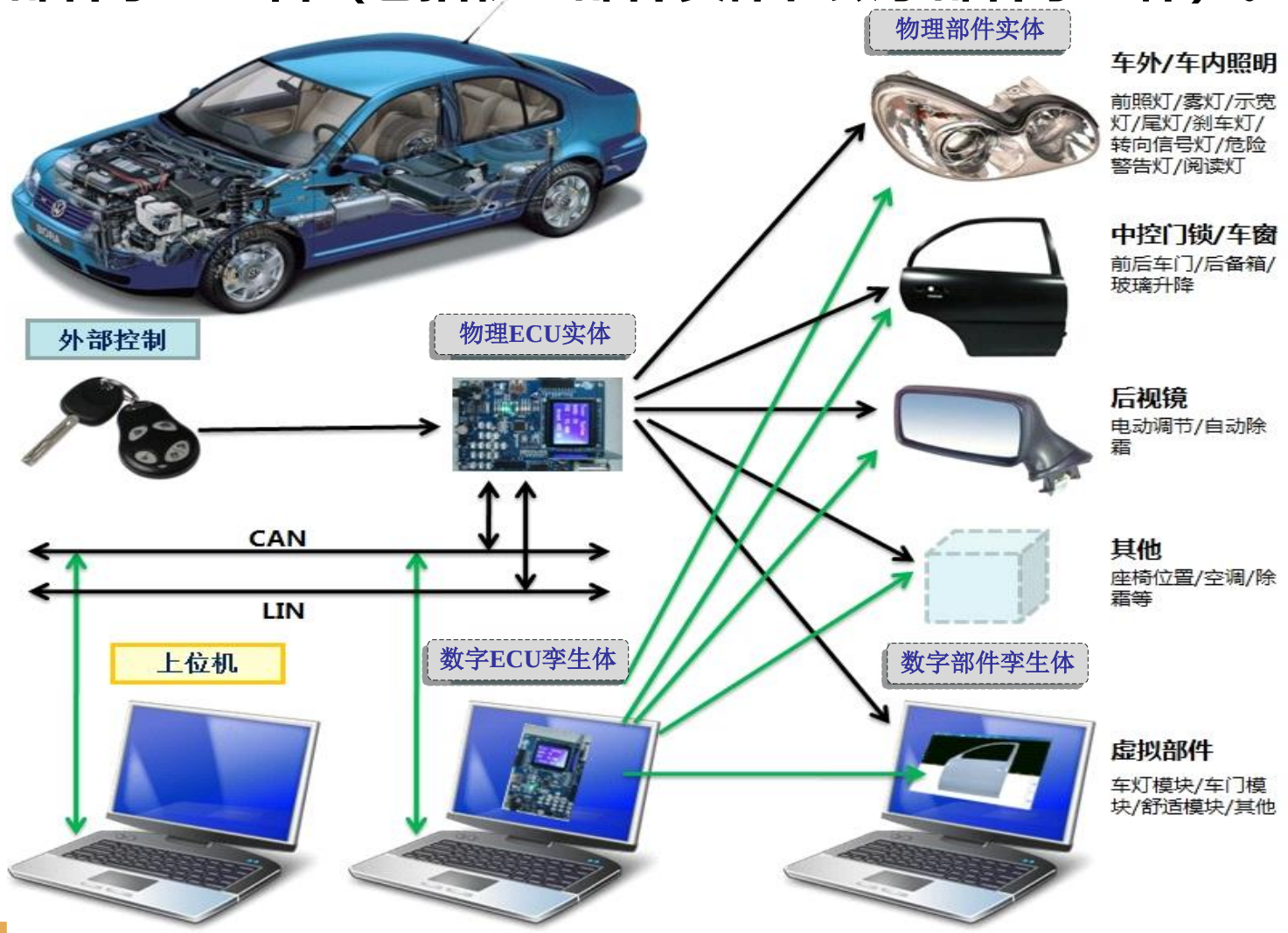
●**关键问题1（克隆）**：即每个物理实体（ECU，汽车部件和测试源）需要克隆一个等同的数字孪生体； 即实现孪生体的生产

●**关键问题2（交互）**：物体实体与数字孪生体可以紧密交互。

目标：可以使物理ECU和数字ECU（由桌面计算机虚拟）都能使用一致的信号来控制实际物理部件与虚拟孪生部件。

3.12 汽车中的数字孪生

1）ECU孪生组合（包括物理ECU实体和数字ECU孪生体）；
2）部件孪生组合（包括物理部件实体和数字部件孪生体）。

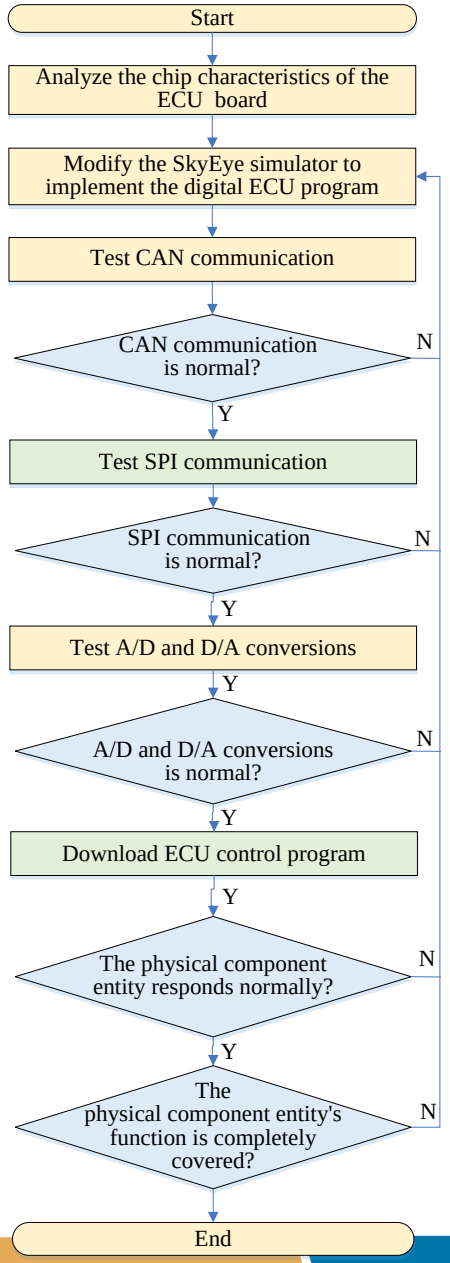


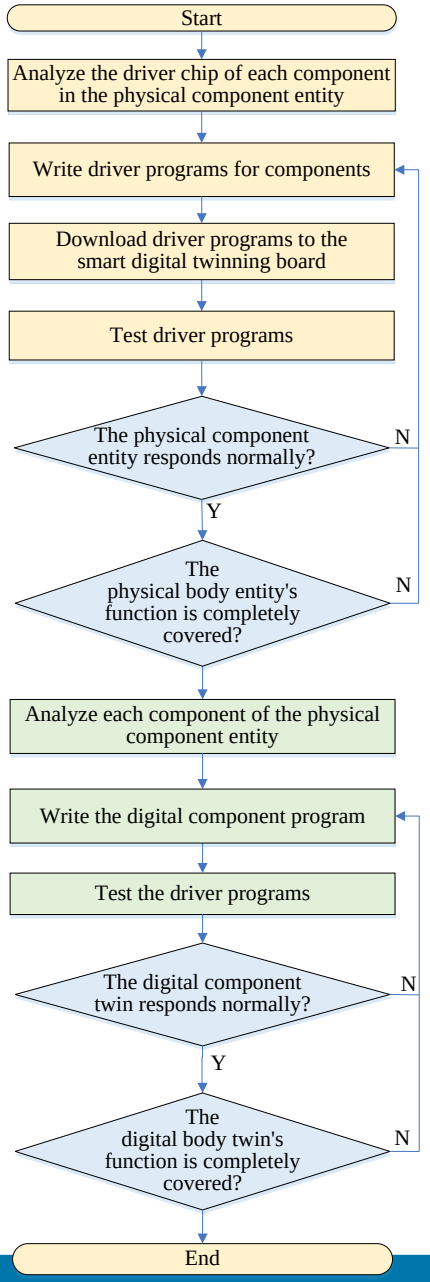
3.13 解决第1个关键问题

集成的数字孪生克隆流程

1、针对数字ECU孪生体的克隆流程

2、针对数字部件孪生体的克隆流程



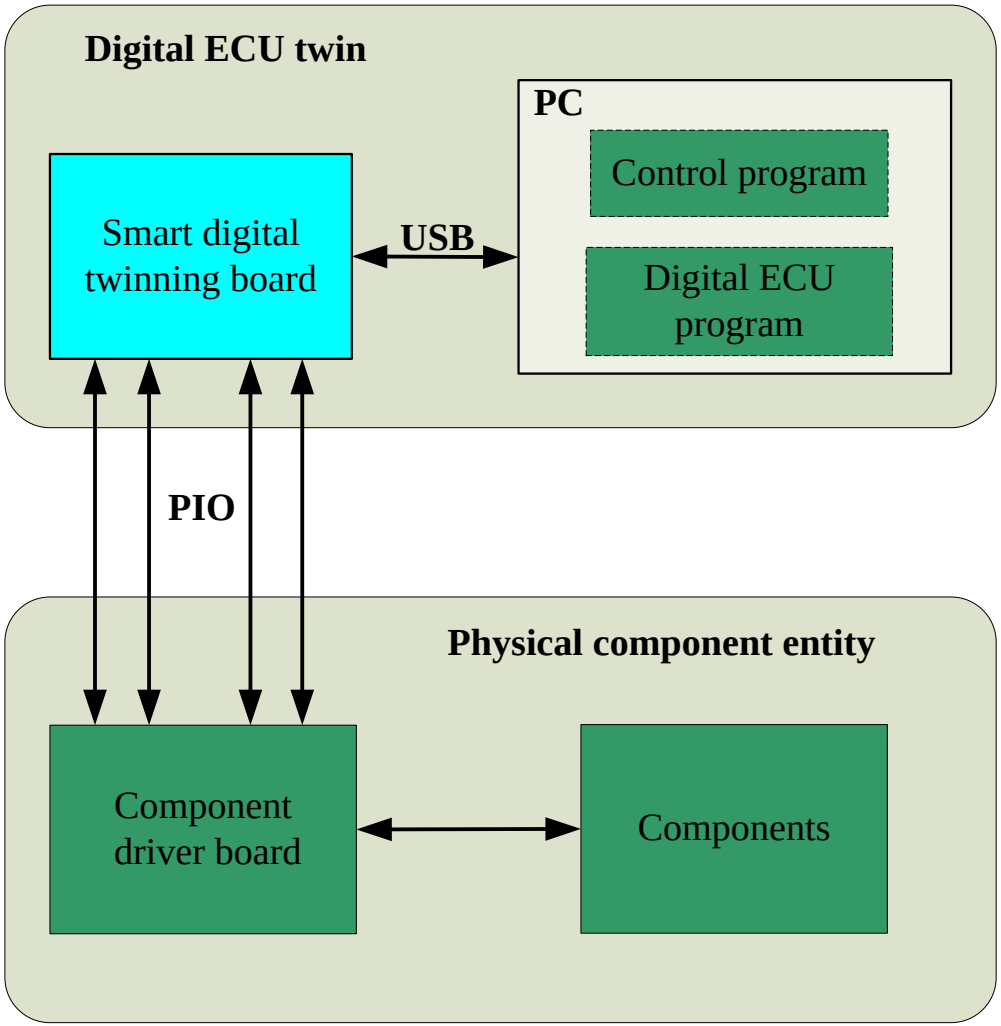


3.13 解决第2个关键问题

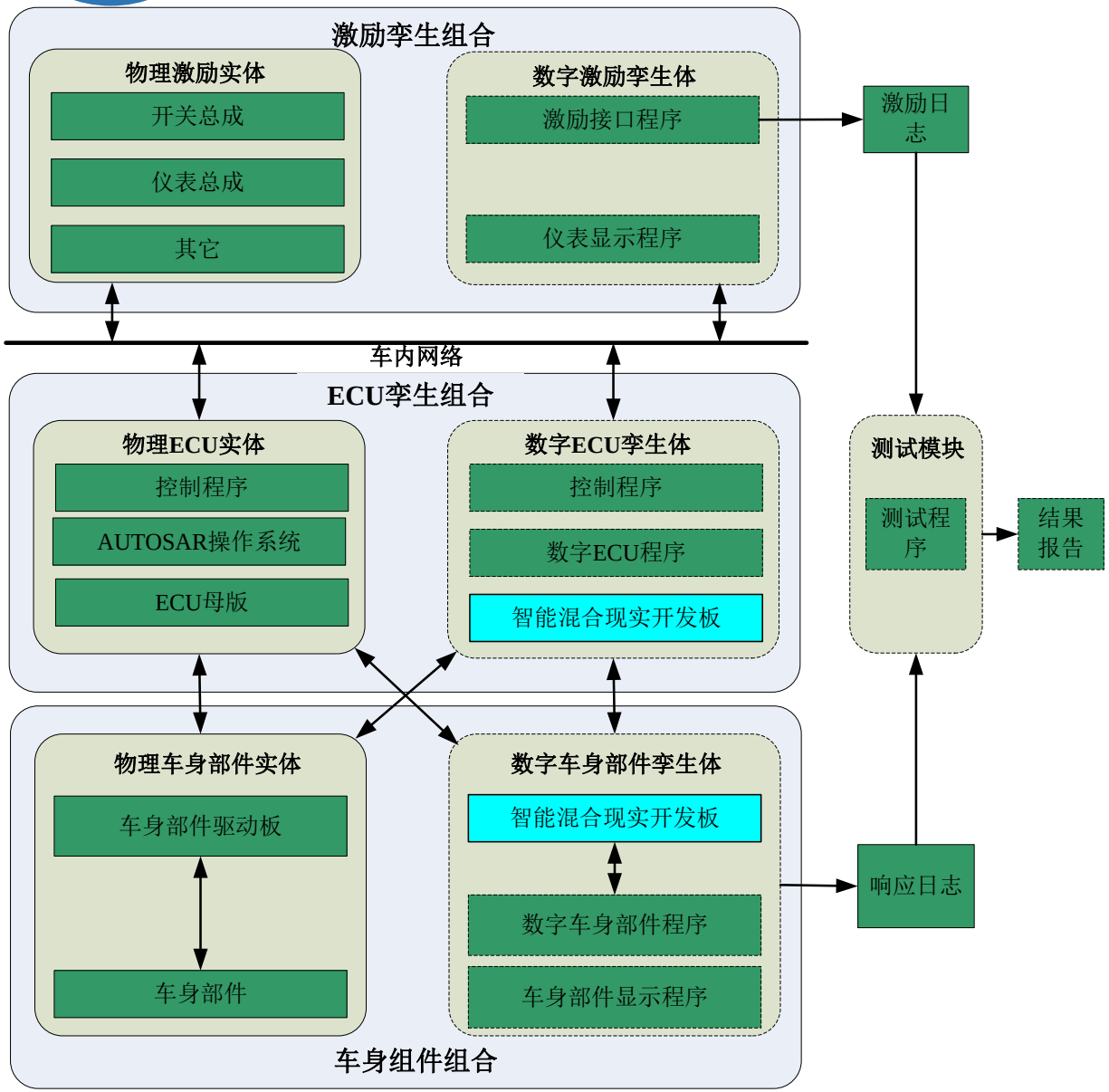
开发智能数字孪生开发板

信号控制：物理ECU实体和数字ECU孪生体都可以通过该开发板来控制物理或数字部件，二者控制信号完全一致

路由：智能数字孪生开发板是自适应开发环境的核心，它是“数字孪生体”与“物理实体”之间的路由。



3.14 开发环境基本组成



1）ECU孪生组合（包括物理ECU实体和数字ECU孪生体）

2）部件孪生组合（包括物理部件实体和数字部件孪生体）

3）物理激励实体：电灯开关总成，车窗开关总成和仪表总成等

4）测试模块：通过对比激励日志与响应日志进行比较来获得结果

3.15 开发环境特点

（1）低成本。支持以SkyEye的形式实现数字ECU孪生体，无需重新制作ECU电路板即可快速轻松地修改设计，节省了时间和成本。

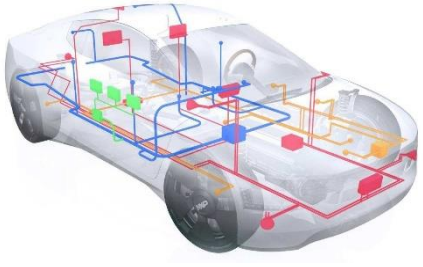
（2）低复杂性。可以轻松测试物理ECU实体中的控制程序，驱动程序和操作系统的有效性；可以轻松确定部件驱动芯片的选择和部件的选择，快速构建和测试用于车用软件系统的产品解决方案。

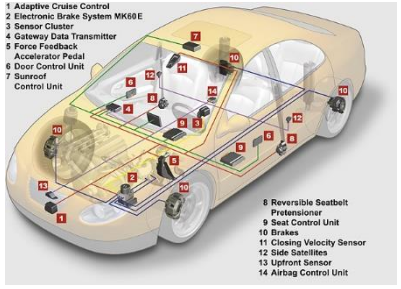
（3）高扩展性。方便程序员扩展或更改软件系统设计方案和产品解决方案；数字和物理实现都可以完全反映软件系统的功能，为开发人员提供便利。

（4）高灵活性。可以直观地显示测试响应，并能将响应记录自动保存到日志文件中，轻松实现无人值守的自动测试和统计。

汇报提纲

0. 开发背景
1. 网络架构
2. 软件系统
3. 平台环境
4. 总结思考





4.1 总结思考-理论挑战

三个理论挑战反映了低成本控制与高安全目标难以兼得的现实：

(1) 其一是低成本架构下难以保证通信安全

(2) 其二是高安全标准下难以保证低成本开发

(3) 其三则是低成本且高安全的平台与环境难以实现。

4.2 总结思考-解决方案

1、三个解决方案构造了低成本高安全的车用嵌入式系统设计理论与应用，最终做到：

（1）通信时延边界可安全确定

（2）安全目标可一次确认

（3）自适应系统易于开发

2、三个解决方案相互支撑，共同为车用嵌入式系统设计与实现提供了一套理论、方法、平台与开发环境：

（1）实时E/E架构设计构建好低时延的实时通信，为车用系统的安全实现奠定基础；

（2）软件系统安全设计在早期设计阶段以低成本的方式提前确认好安全目标；

（3）自适应平台与开发环境实现则为自适应软件系统开发提供了良好的平台环境与测试条件。

车用嵌入式系统中若干理论挑战与解决方案

谢谢大家！

湖南大学
HUNAN UNIVERSITY

2020年中国嵌入式技术大会
EMBEDDED TECHNOLOGY
Conference China 2020

湖南大学　谢国琪