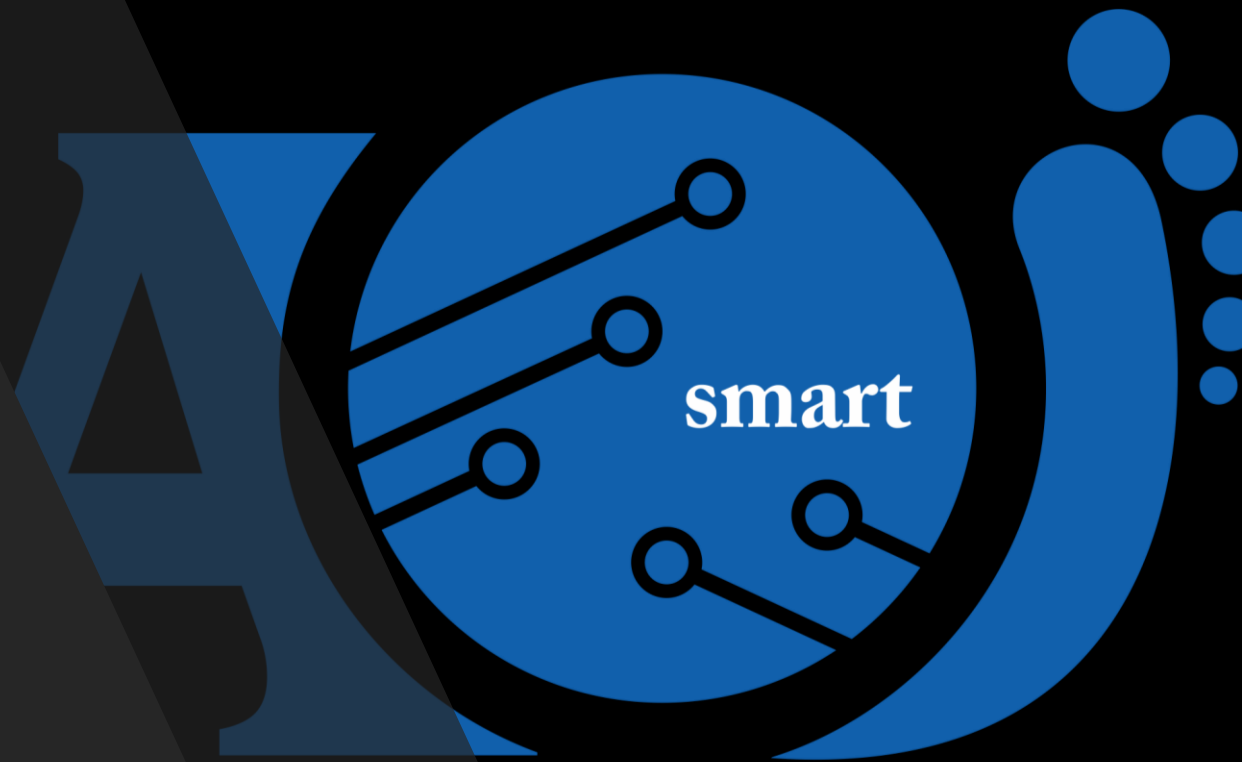


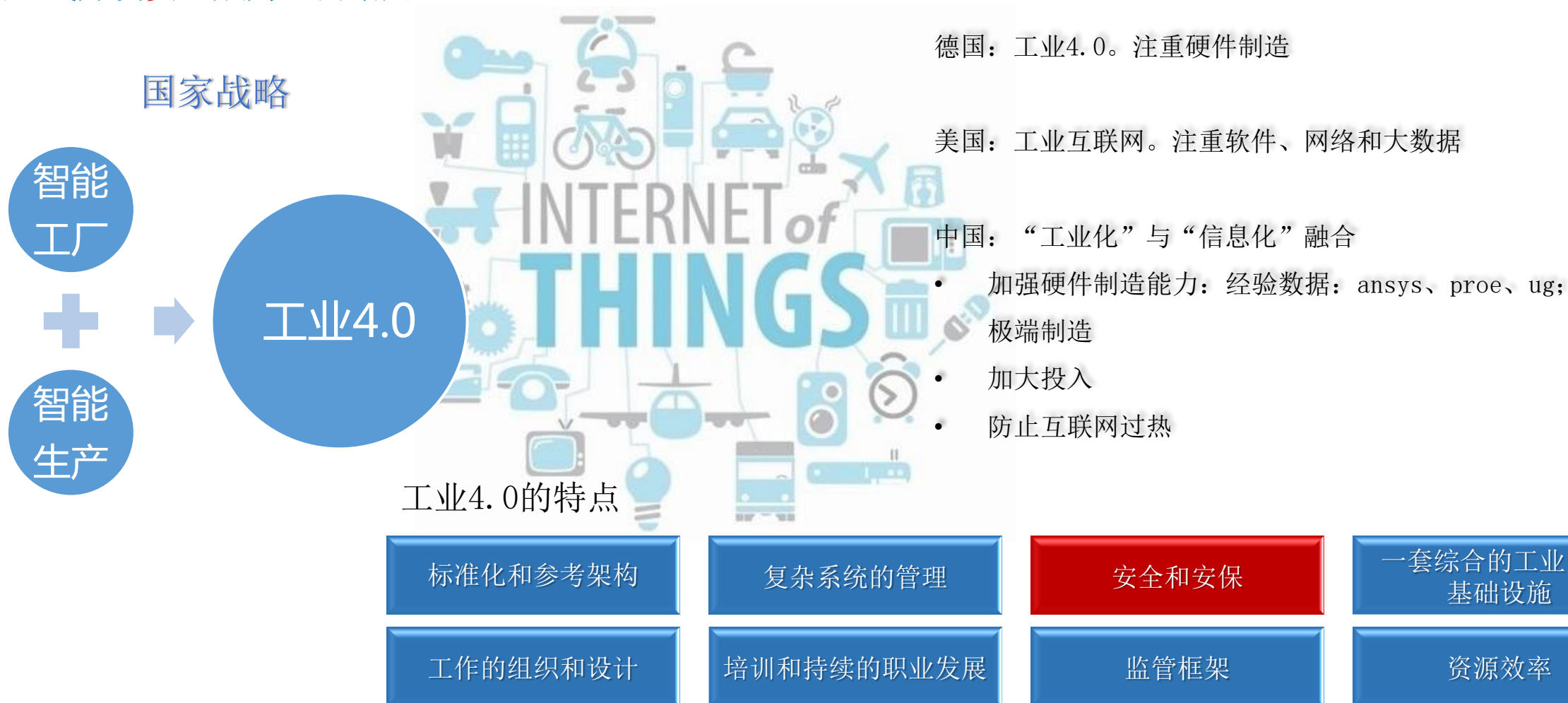
2017. 6

安全，从“根”做起



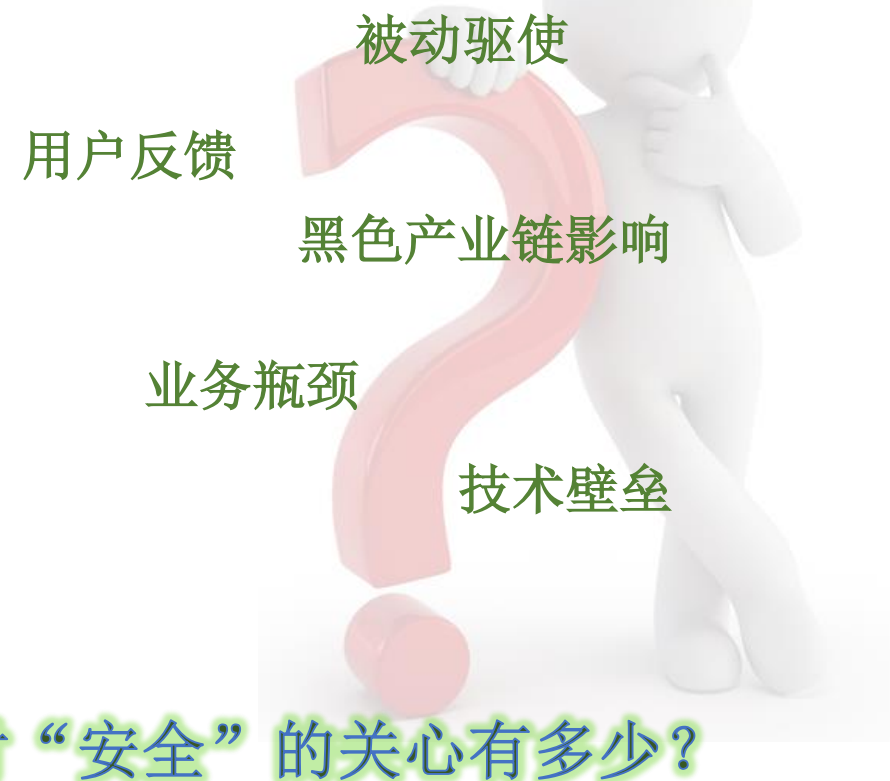
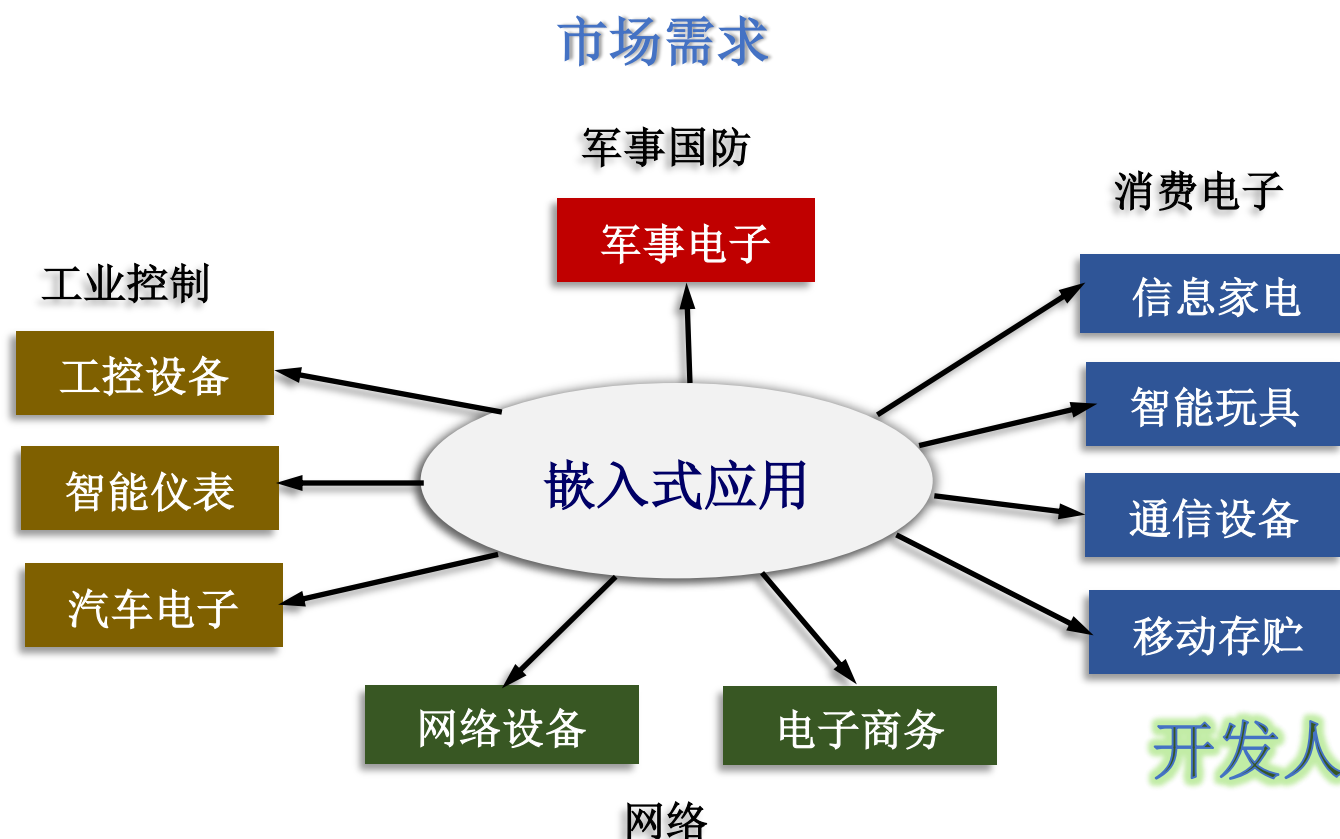
WHY ?

嵌入式开发安全成为热门话题？

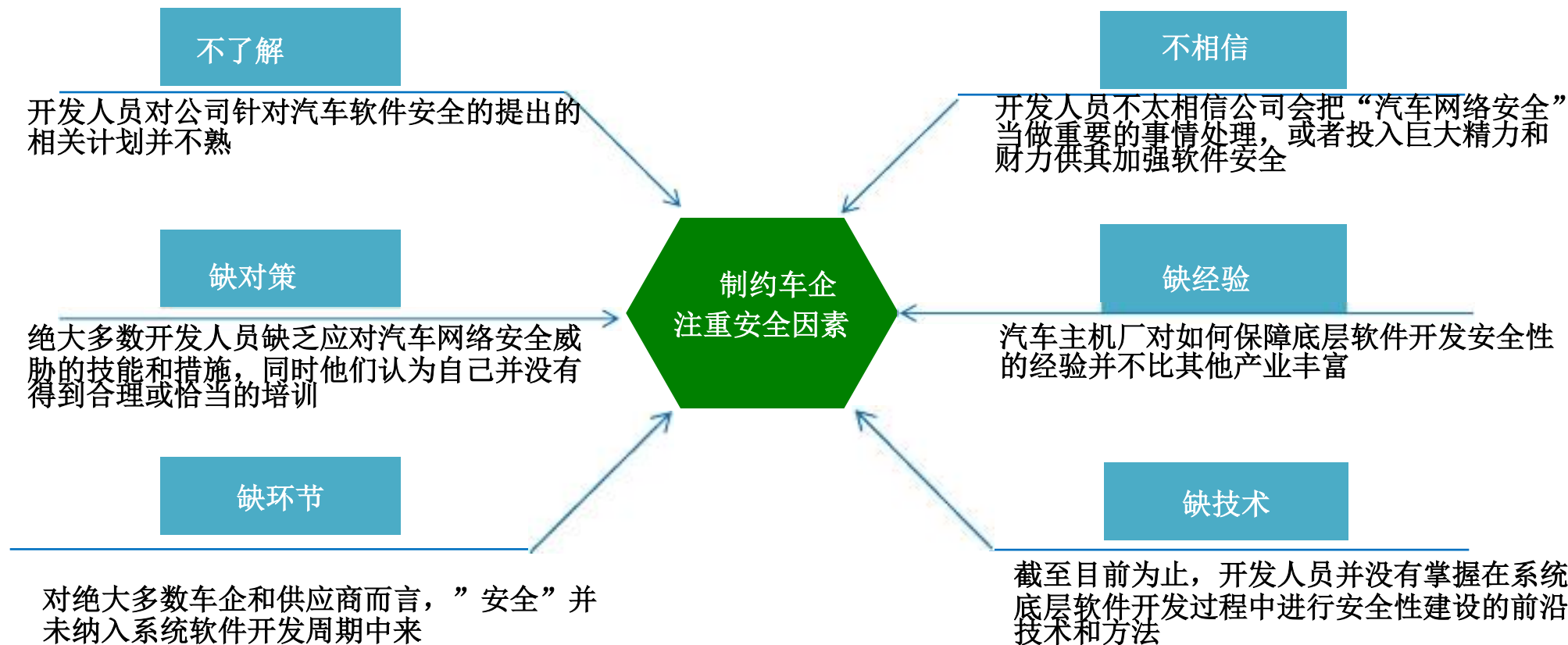


WHO ?

嵌入式开发安全成为热门话题？



WHY ?



参考标准

- IEC 61508 电气/电子/可编程电子安全系统的功能安全 [功能安全标准](#)

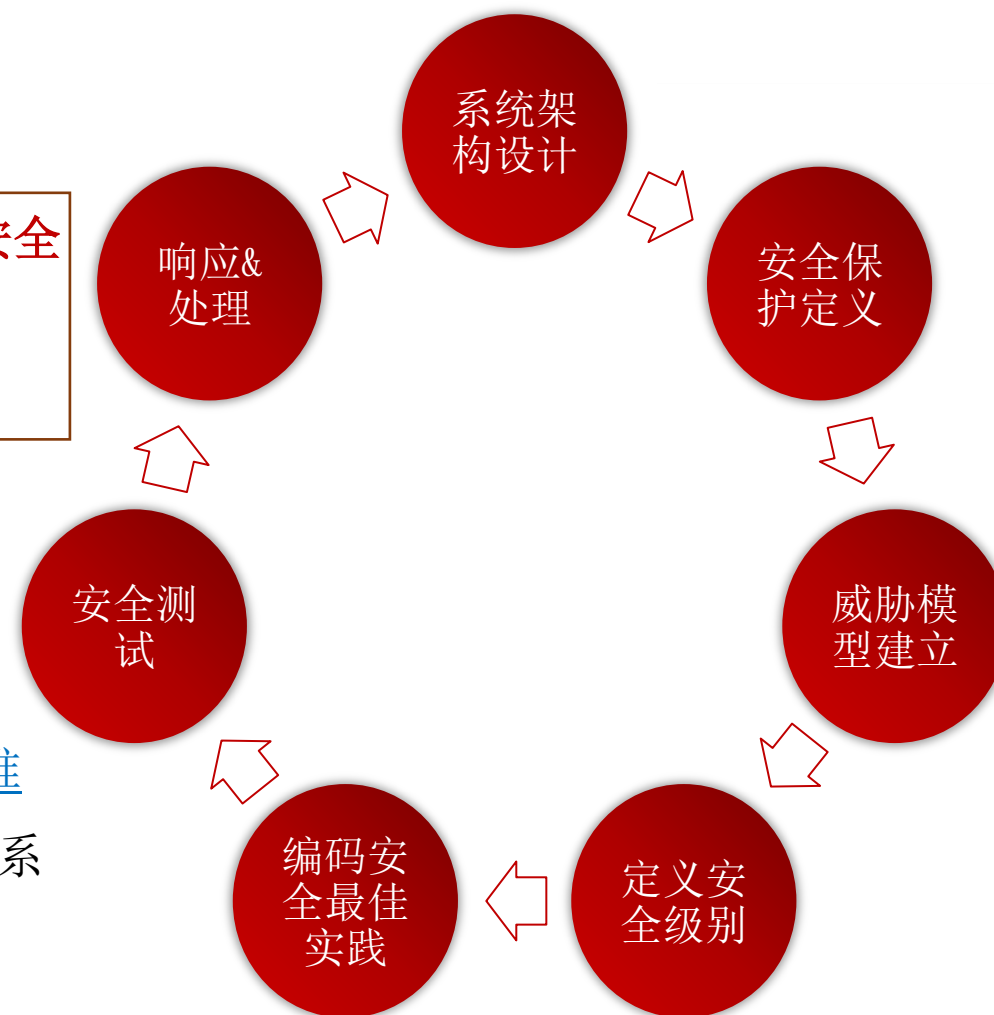
目标是

26262 汽车电子电气系统功能安全 [汽车行业](#)
避免由系统功能性故障导致的不可接受的风险，关注系统故障后的行为，而不是系统的原有功能或性能

- DB44/T 1558-2015 实时嵌入式软件安全性测试规范 [地方标准](#)
- IEC 62443 工业过程测量/控制和自动化网络与系统信息安全体系
- ISO/IEC 27034

功能安全

[功能安全标准](#)



参考标准



参考国际主流的应用安全最佳实践

安全组织

通过安全开发生命周期改进

Microsoft®



微软 SDL
安全开发生命周期



SAMM
企业软件保证 成熟度模型

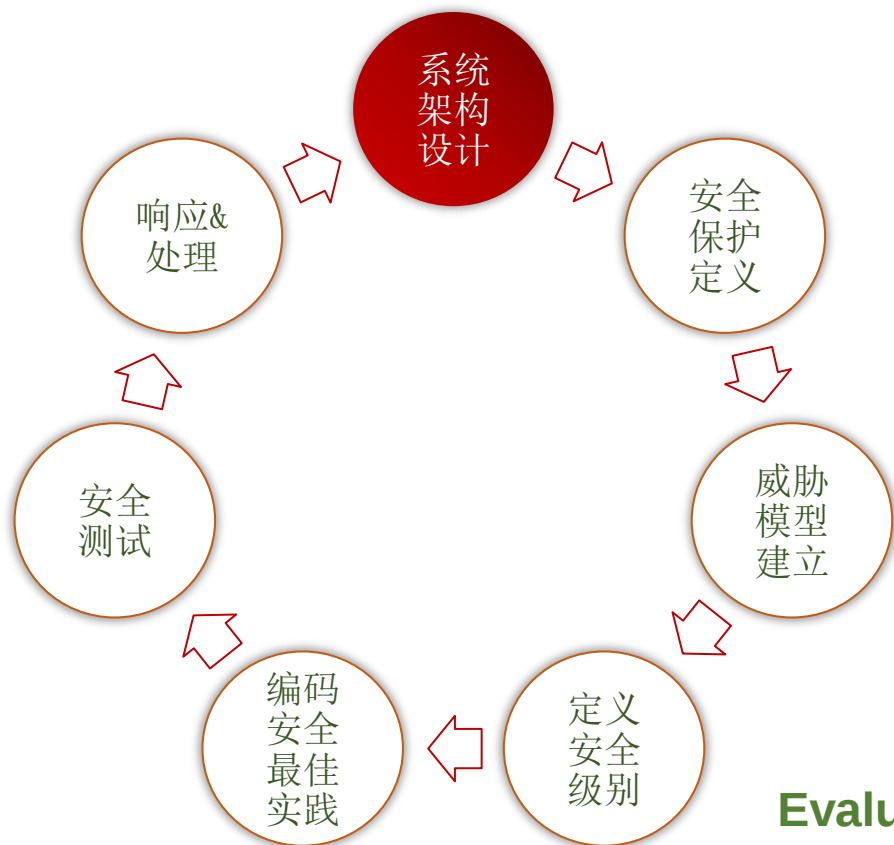
NIST



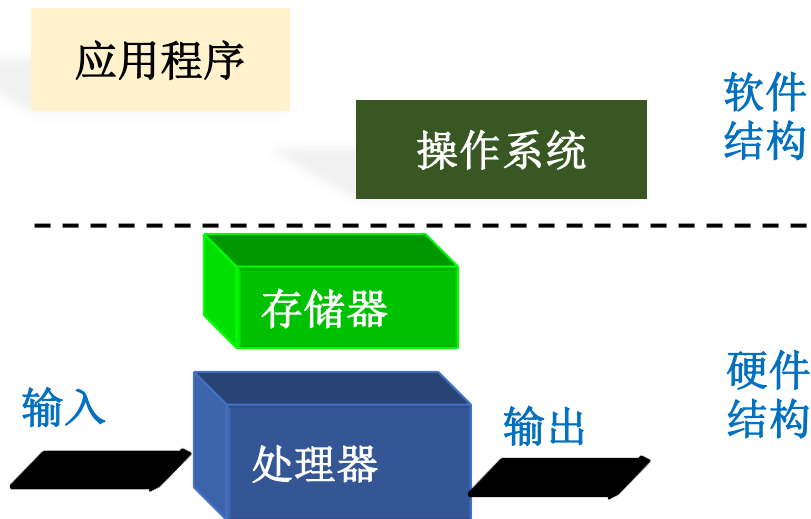
NIST SP800-64

Security Considerations in the System Development Life Cycle

开发安全生命周期



嵌入式系统架构的组成



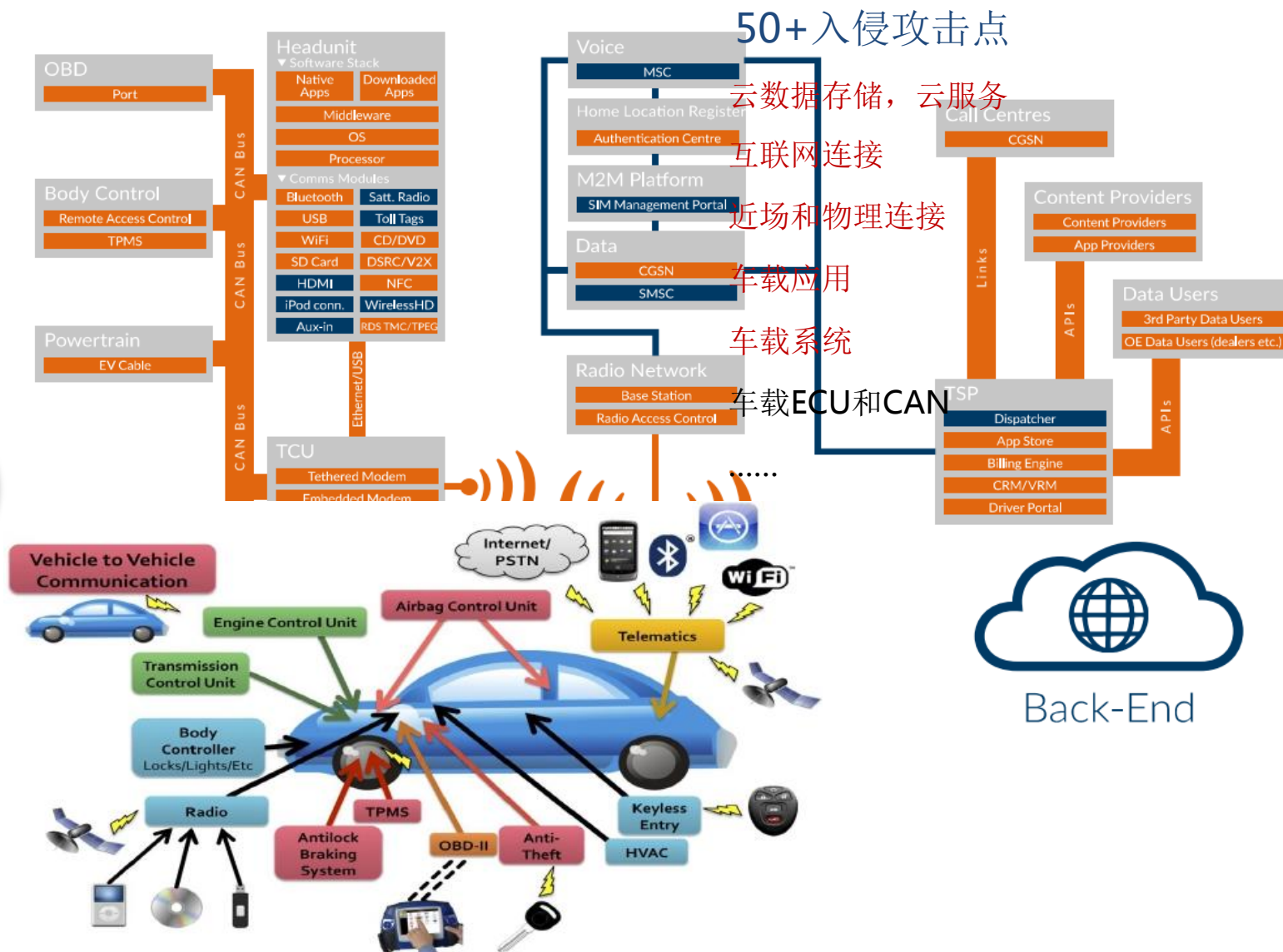
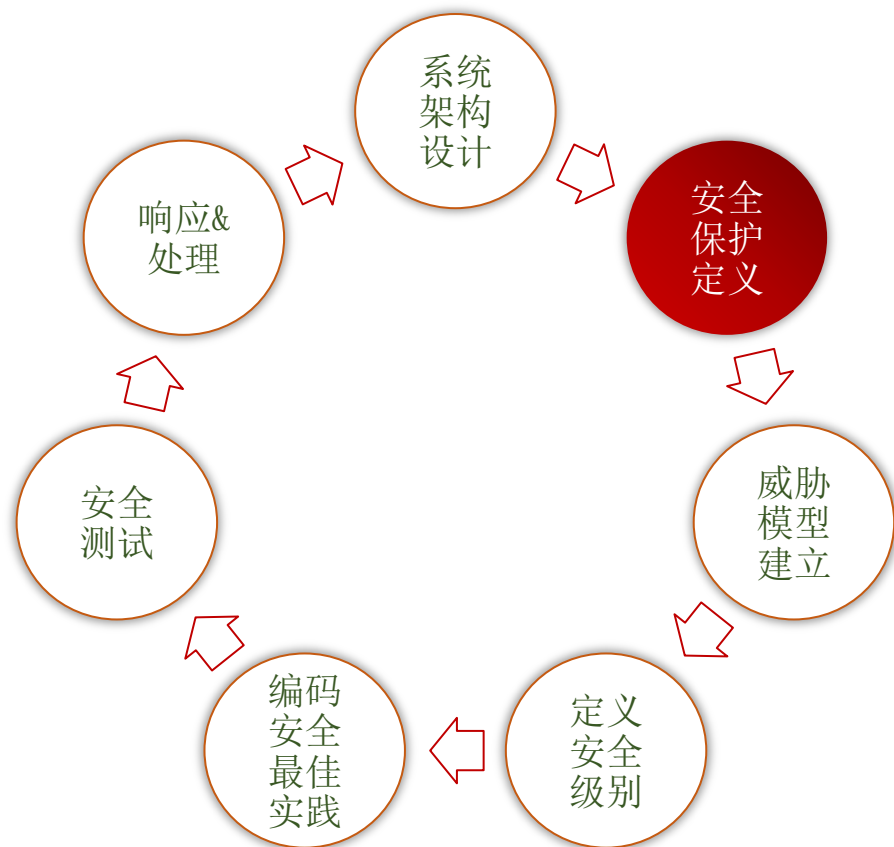
□ 开发标准

□ 接口：输入输出，操作效率

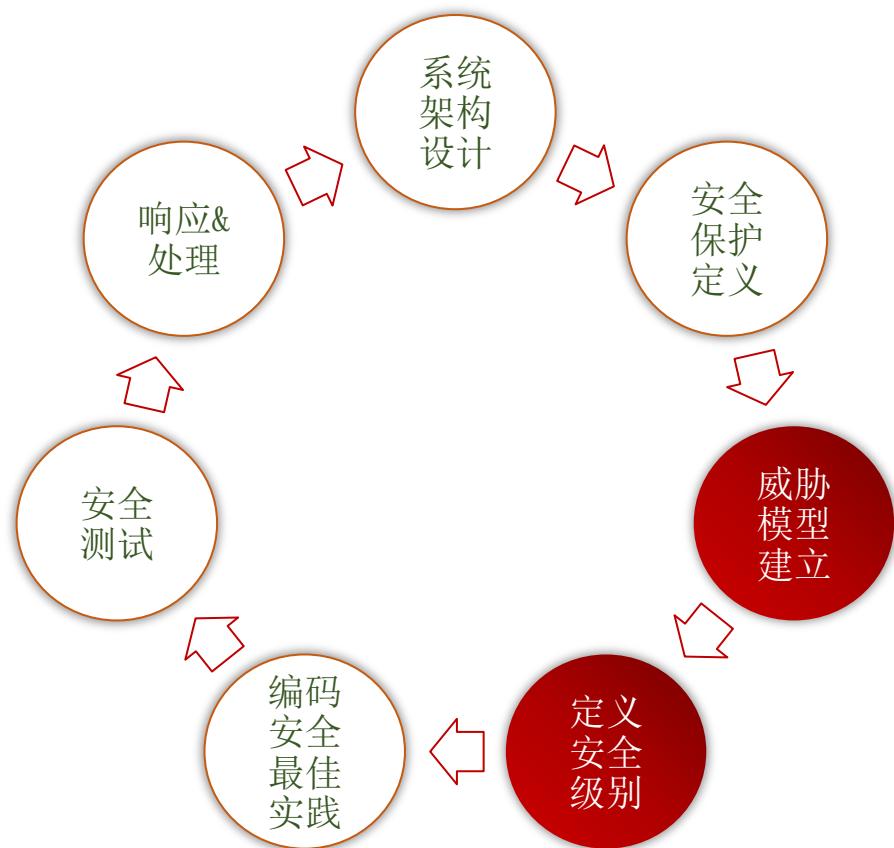
Evaluation of the available security technologies, working closely with suppliers. 评估现有的安全技术，与供应商合作

Advice on efficient use of security technologies and management of the associated risks. 使用技术和管理方法帮助控制风险

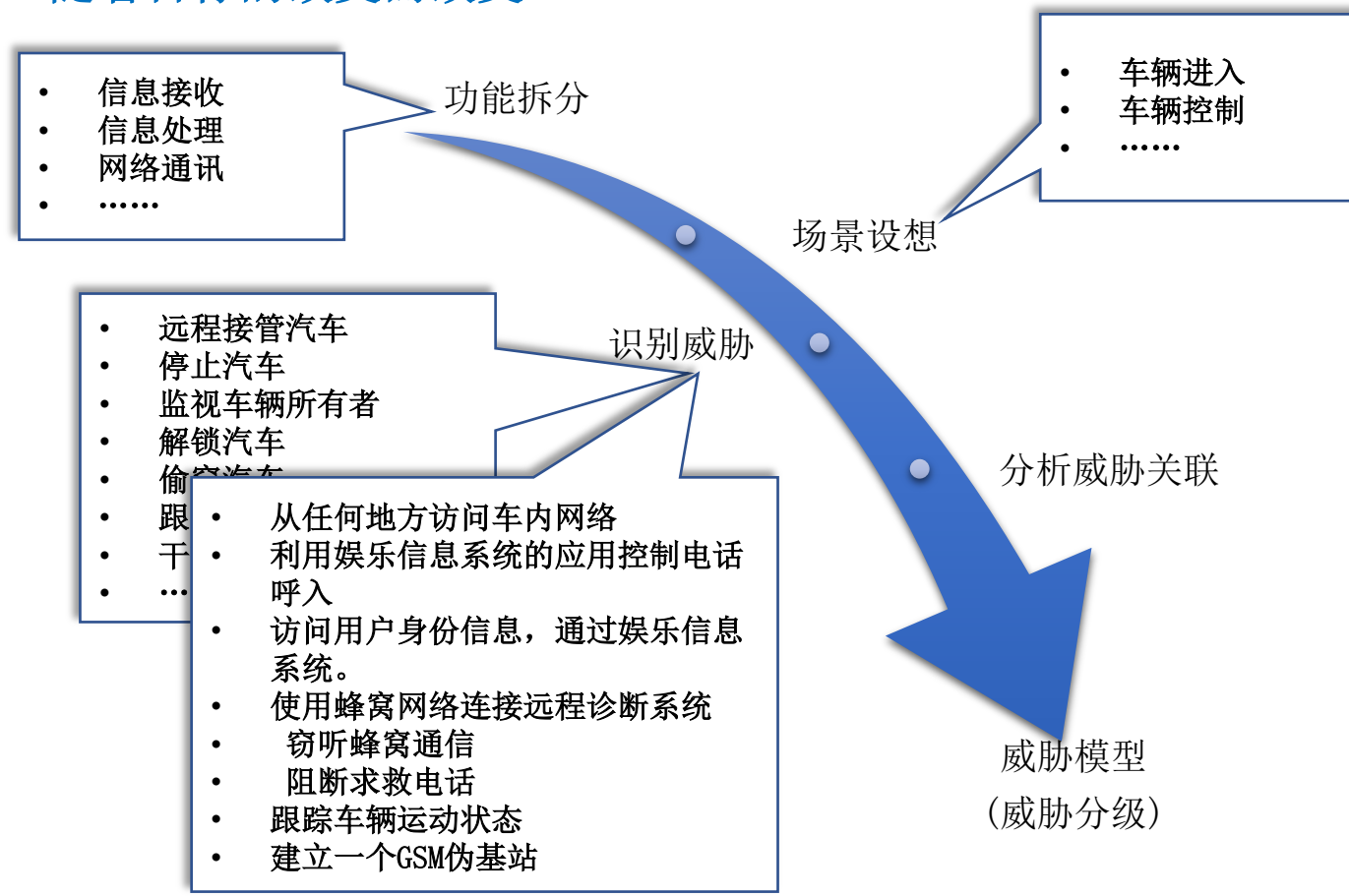
开发安全生命周期



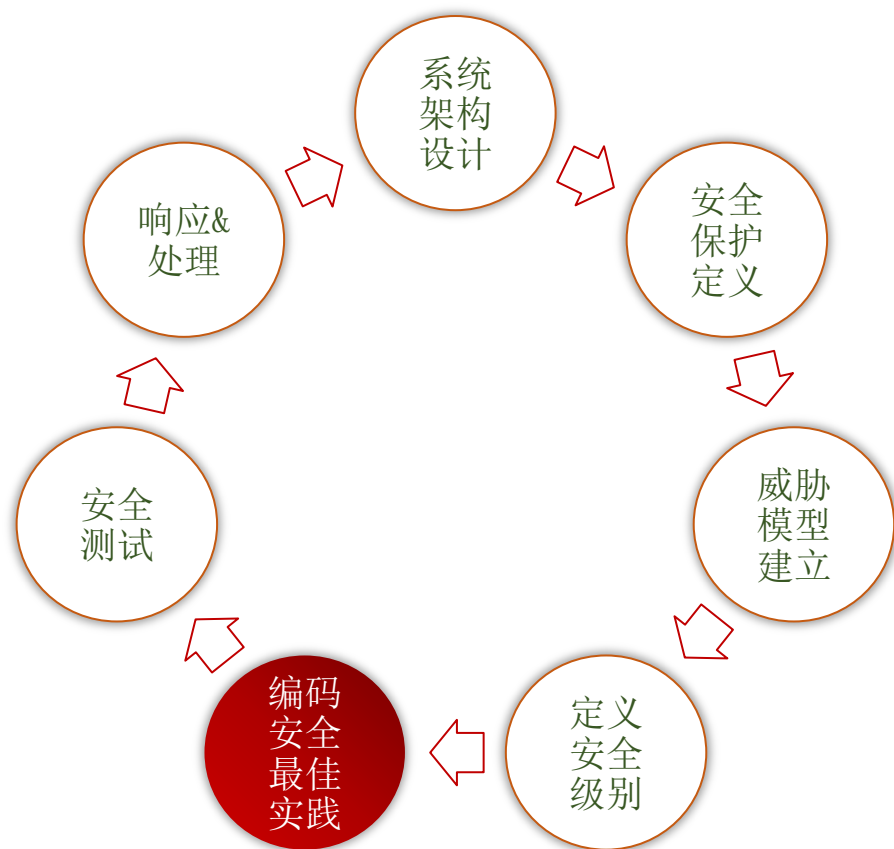
开发安全生命周期



一个好的生命周期是：在产品开发之前创建一个威胁模型，随着产品穿过整个生命周期持续更新威胁模型。威胁模型是一个活的文档，随着目标的改变而改变



开发安全生命周期



安全编码规范：代码质量，处理效率，技术安全漏洞规避

不安全的DES方法

相同对称加密密钥

重放攻击

无篡改检验（TCU）

VIN信息泄露

不加密的数据传输

数据校验不足

任意号码呼叫接收

缓存溢出

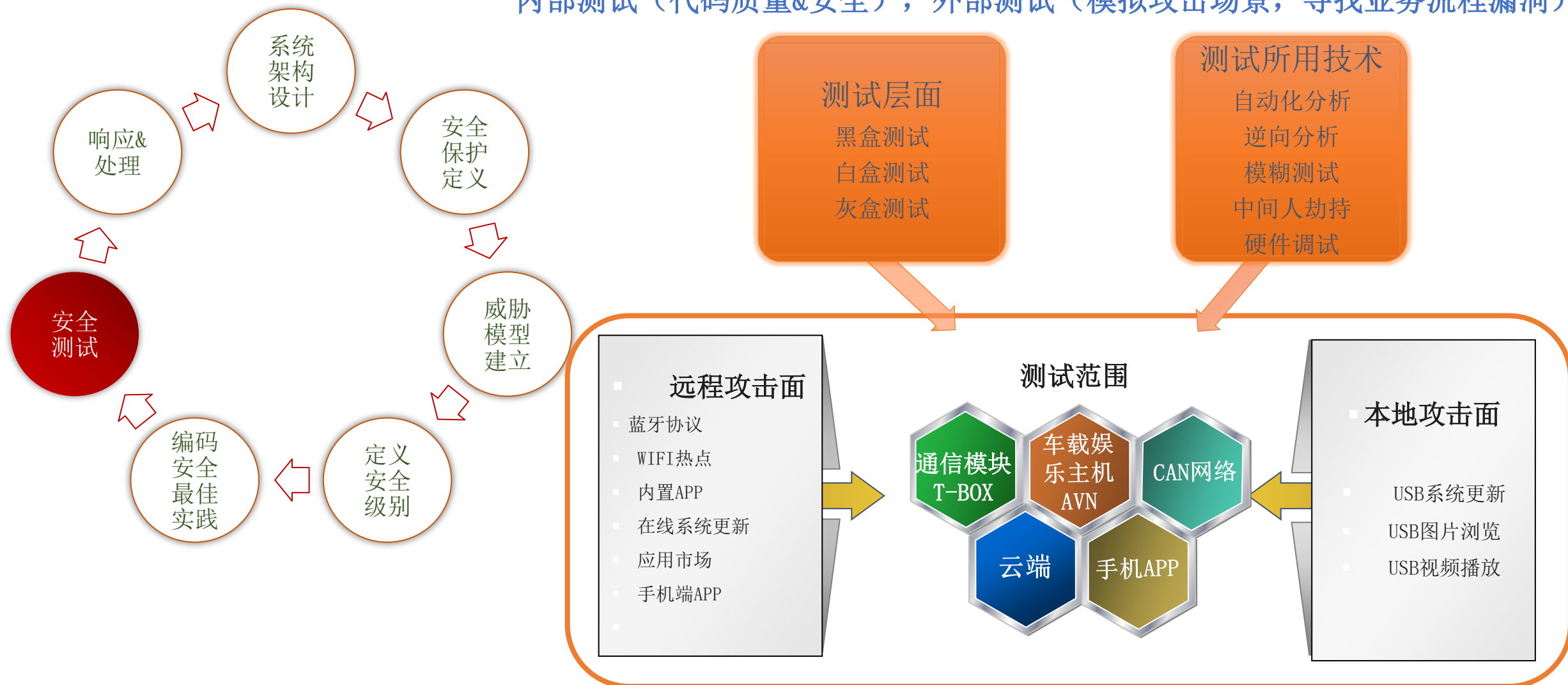


- ❑ 函数
- ❑ 命名规范
- ❑ 变量，宏，常量
- ❑ 安全
 - ✓ 程序效率
 - ✓ 字符串操作安全
 - ✓ 格式化输出安全
 - ✓ 文件I/O安全
 - ✓ 容错性
 - ✓ 可重用性



开发安全生命周期

内部测试（代码质量&安全），外部测试（模拟攻击场景，寻找业务流程漏洞）



其它参考信息



由于智能化、网联化汽车在全球发展还处于探索期，世界各汽车标准制定机构标准制定还处于初期阶段，目前多为零散规定：

国内待制定标准		
标准类型项目名称技术归口单位		
车联网服务技术要求	车辆远程服务系统通用技术要求	全国智能运输系统标准化技术委员会
危险报警	车辆运行碰撞危险报警系统性能要求	全国智能运输系统标准化技术委员会
专用短程通信	车路协同专用短程通信第1部分:总体技术要求	全国智能运输系统标准化技术委员会
	车路协同专用短程通信第2部分:媒体接入控制层和物理层	全国智能运输系统标准化技术委员会
	车路协同专用短程通信第3部分:网络层和应用层	全国智能运输系统标准化技术委员会
	车路协同专用短程通信第4部分:设备应用	全国智能运输系统标准化技术委员会
数据标准	交通运输数字证书格式	全国智能运输系统标准化技术委员会
要素标识标准	交通运输物联网标识规则	全国智能运输系统标准化技术委员会
	交通运输物联网标识应用分类及编址	全国智能运输系统标准化技术委员会
安全规范	交通运输信息安全规范	全国智能运输系统标准化技术委员会
信息交换标准	跨区域交通出行服务信息交换	全国智能运输系统标准化技术委员会
信息安全技术	全国信息安全标准化技术委员会提出并归口	GB/T20274.1-2008信息安全技术信息系统安全保障评估框架第1部分:简介和一般模型；
	全国信息安全标准化技术委员会提出并归口	GB/T20274.2-2008信息安全技术信息系统安全保障评估框架第2部分:技术保障