汽车网络安全左移实践

——基于信任构建汽车安全的探索

北京豆荚科技有限公司

简介目录

1
豆荚与汽车安全

2012年

研究可信计算
可信操作系统 TEE OS

2019年

探索ISO21434的TARA方法论
从事汽车安全咨询的业务

ISO21434对R155起到实施支撑作用

2018年

调研WP.29 R155草案
车载ECU对可信计算的需求

2020年 UN/WP.29 R155

全球第一个汽车信息安全强制法规

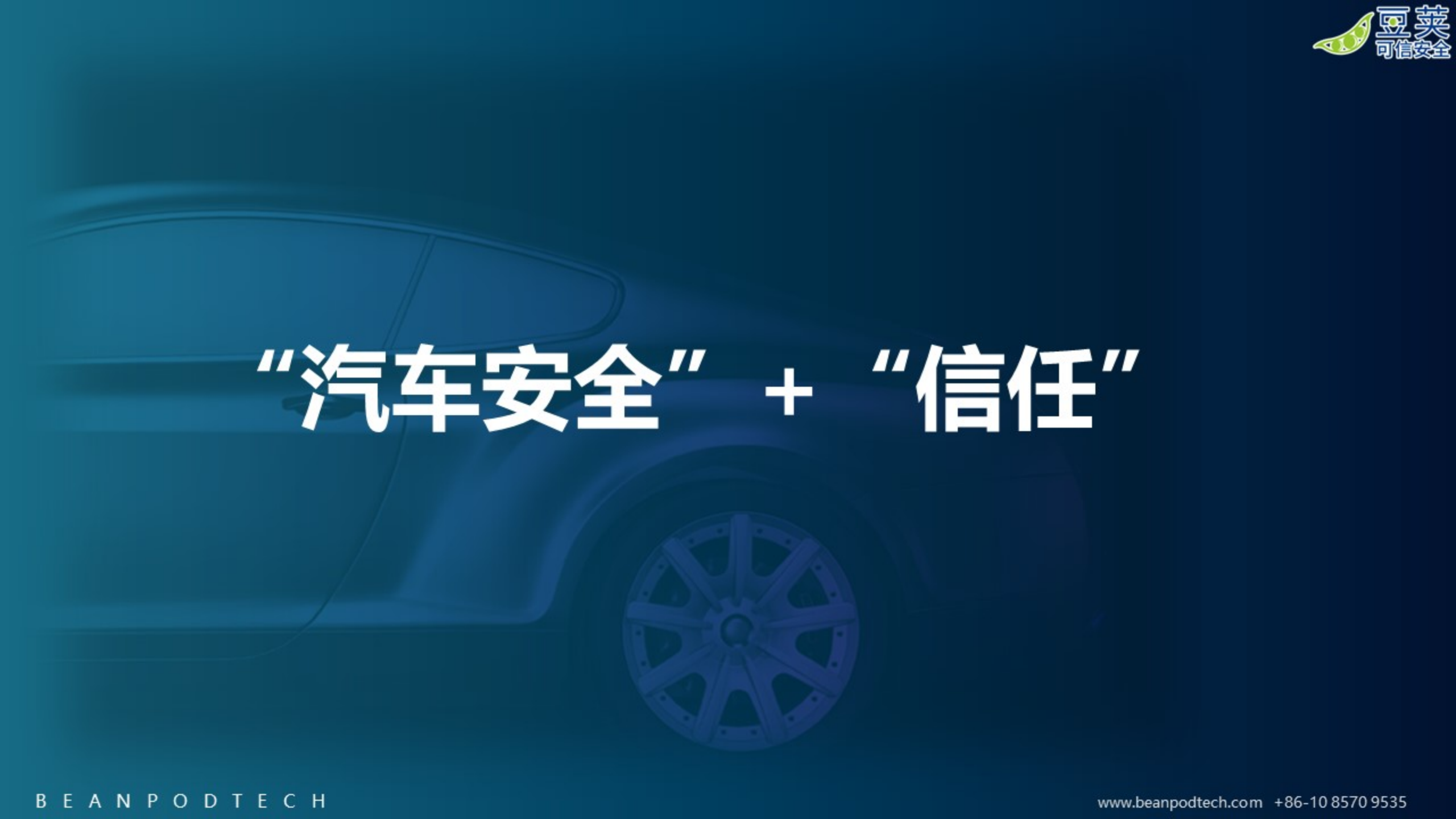
基于威胁分析与风险评估（TARA），
形成整车信息安全的7大领域：

1. 数据与隐私安全
2. 业务与功能安全
3. 应用与平台安全
4. 环境安全
5. 通信安全
6. 后台与移动安全
7. 生产与售后安全

资产的7大安全属性：

1. 机密性
2. 完整性
3. 可用性
4. 新鲜性
5. 抗抵赖性
6. 真实性
7. 授权性

10 8570 9535


“汽车安全” + “信任”

2
谈谈“信任”

trustworthy

信任与安全的关系

- 系统安全工程是为了解决漏洞的一系列方法、技术、规程，本质上是提供必要的**信任**证明，以抵御复杂的网络攻击。

— 摘自《NIST SP 800-160 系统安全工程 v1 p9》

- 零信任是一种以资源保护为核心的网络安全范式，其前提是**信任**从来不是隐式授予的，而是必须进行持续**评估**。

— 摘自《NIST SP 800-207 零信任架构 p13》

通过信任构建安全示例

安全启动

- 加载代码的安全可信
- 可信的密钥 + 密码算法

用户登录

- 身份的安全可信
- 可信的认证因子（口令、验证码、生物特征等）

安全诊断

- 诊断仪和车的信任
- 27服务（29服务）的“挑战-应答”机制

数据安全

- 全磁盘加密FDE
- 可信的用户身份 + 可信的密码算法（不信任设备）

通过信任构建安全示例

防火墙的基本工作原理 → 黑白分明

假定防火墙的引擎及规则配置是值得信任的，

则黑白名单规则会按照意愿生效

基于**信任链**的思想，需要为假设做出证明，证明引擎值得信任

这是一个**复杂的系统性安全工程**

3
关于“信任根”

RoT (Root of Trust)

信任根

信任根 RoT (Root of Trust) 是平台中的一个计算引擎 + 一段代码 + 可能的数据，它提供基础安全服务，如：机密性、完整性、可用性、标识、真实性、授权性、度量性等。

其代码和数据的可信证明由自身完成不依赖于其他实体。

— 摘自Global Platform《Root of Trust Definitions and Requirements V1.1》

常见的信任根

HSM

硬件安全模块

TEE

可信执行环境

TPM

可信平台模块

信任根与7大领域

1、数据与隐私安全

如：车内音视频的机密性（加密存储）

2、业务与功能安全

如：蓝牙钥匙的控车指令的真实性（MAC密钥）

3、应用与平台安全

如：关键业务代码的完整性（代码验签）

4、环境安全

如：外部环境实体的真实性（唯一性标识及其完整性保护）

5、通信安全

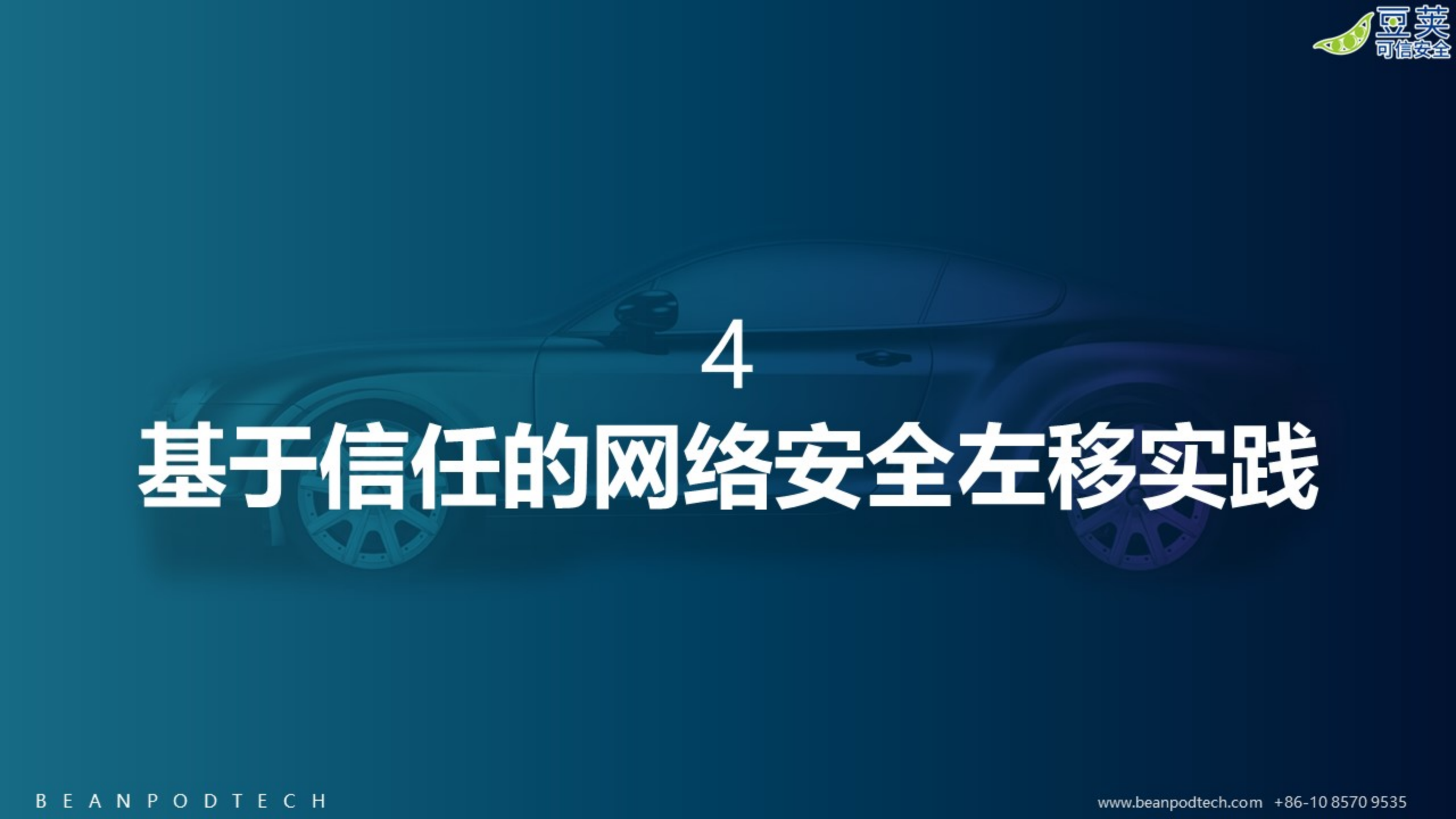
如：车内通信的真实性和新鲜性（SecOC验签）

6、后台与移动安全

如：执行环境的机密性与可用性 （机密容器、keystore）

7、生产与售后安全

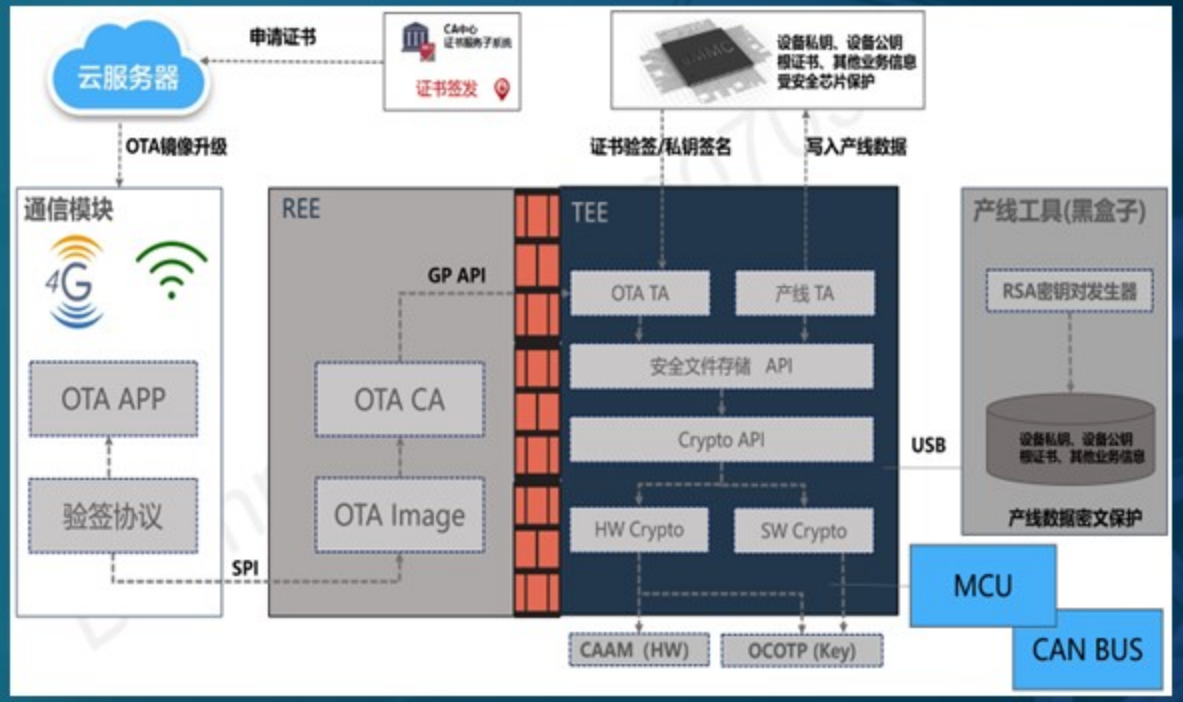
如：诊断的真实性与授权性 （PKI）



4

基于信任的网络安全左移实践

豆荚基于信任的实践 – OTA安全



- TEE部署于TBOX
- 方案目标举例：通信安全、OTA安全
- 方案核心点：

1. TEE作为密码模块的信任根保护TLS密钥，集成国密算法；
2. 基于P11提供快速，零开发集成；
3. 固件明文不暴露在不可信的Linux环境所访问的普通RAM区域。

豆荚基于信任的实践 - ZT-V

汽车EE架构SOA化带来的网络安全问题

EEA的SOA化 + 车载平台的持续开放

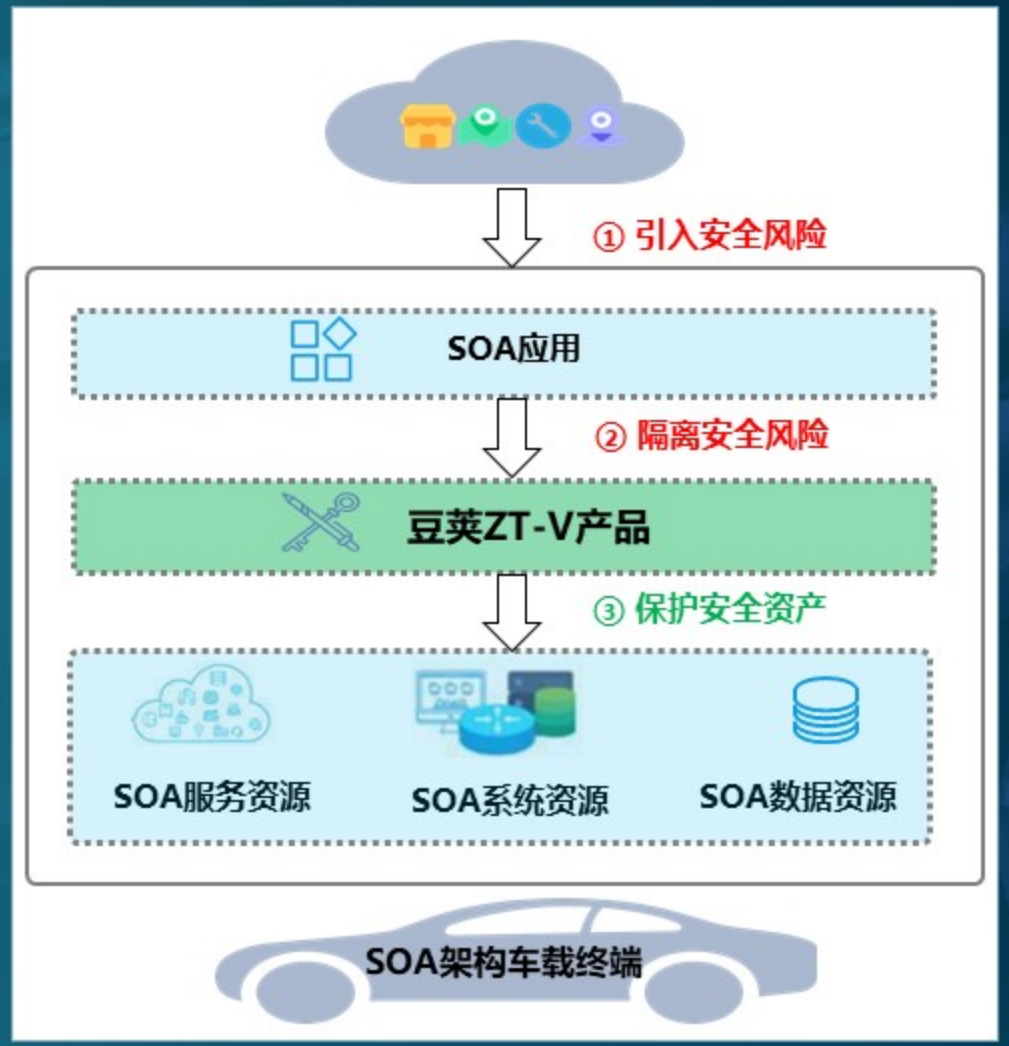
↓

导致增加了大量的不可控的安全风险

↓

传统的汽车安全设计理念乏力

豆荚基于信任的实践 - ZT-V



问题的核心焦点是“***访问资源和服务的风险***”

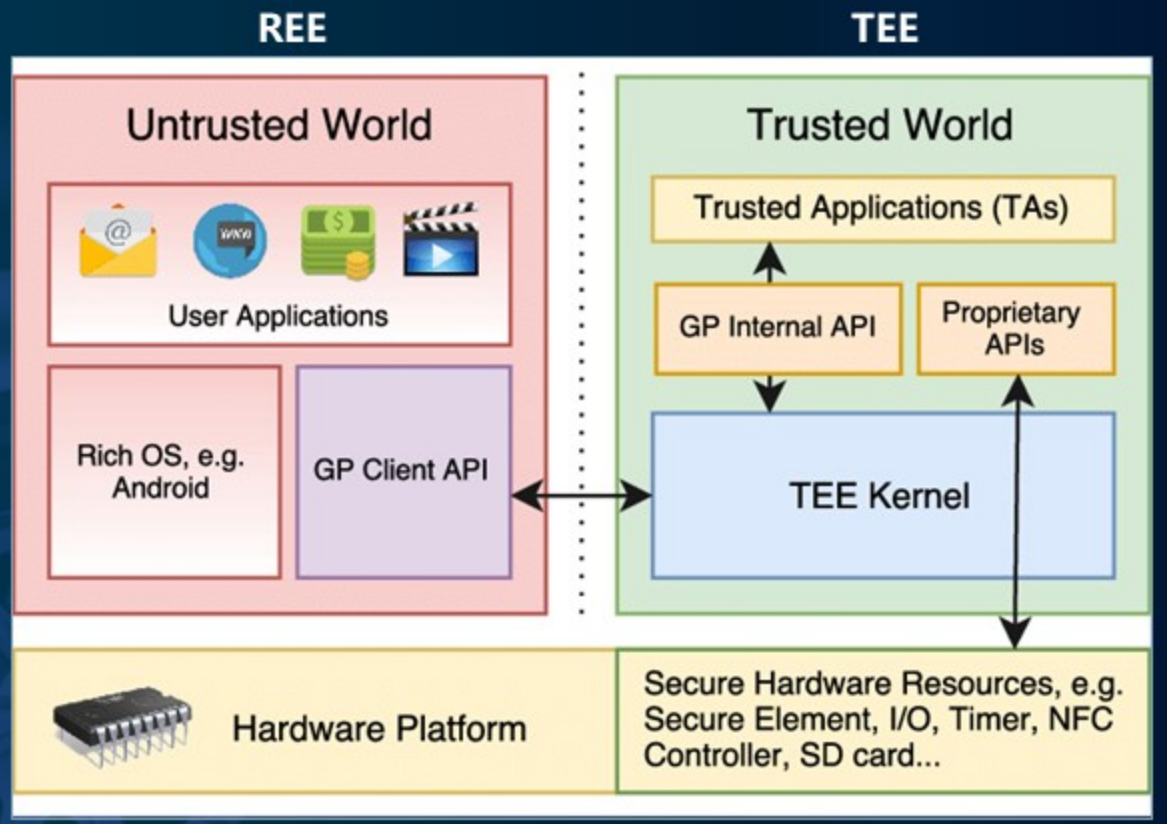
- 解决方法：

结合零信任思想，融合“**信任根**、服务隔离、身份认证、可用保护、审计、访问策略、**可信度量**”等关键技术提出了“基于零信任的SOA安全方案” — ***ZT-V***

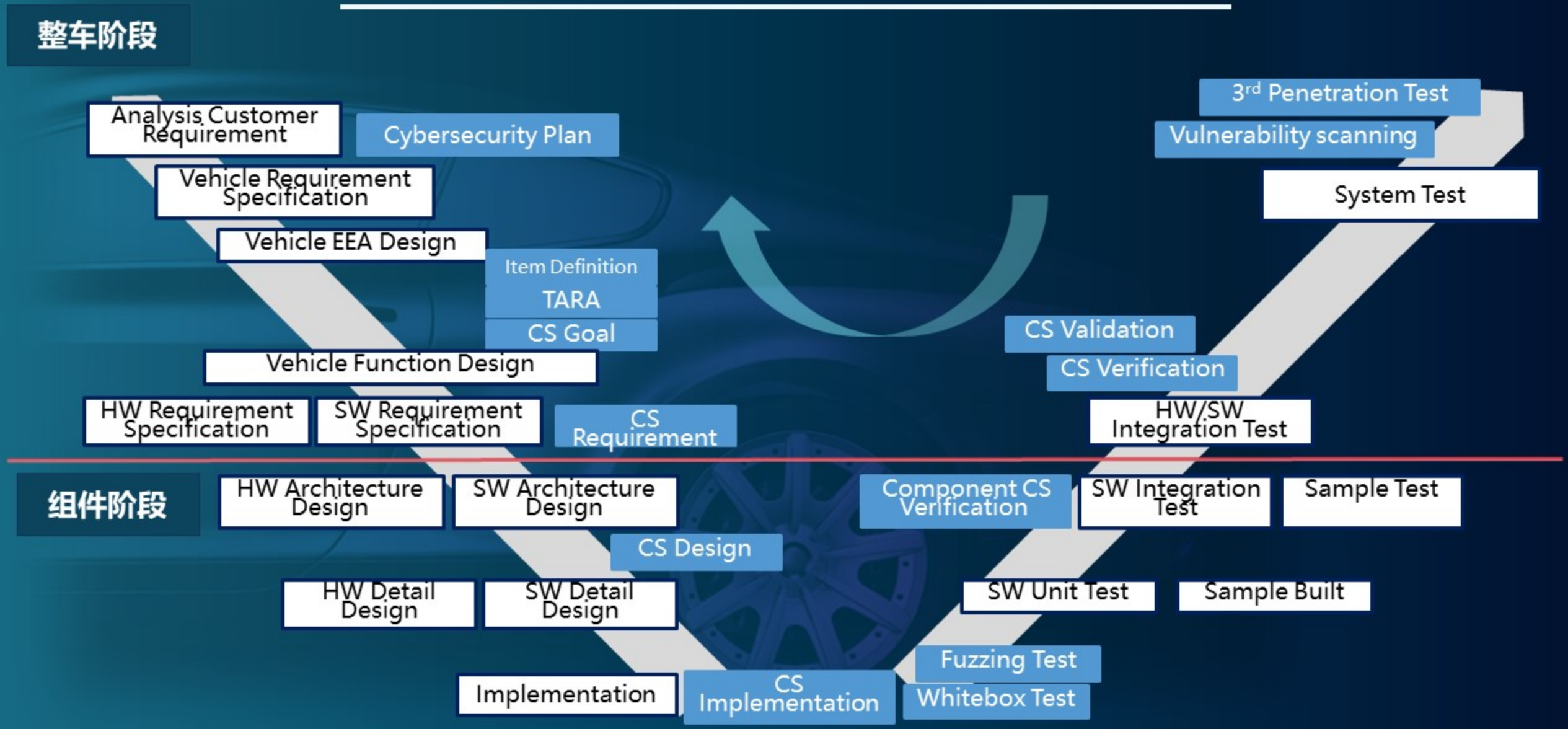
豆荚基于信任的实践 - TEE

目前，在汽车领域的使用场景：

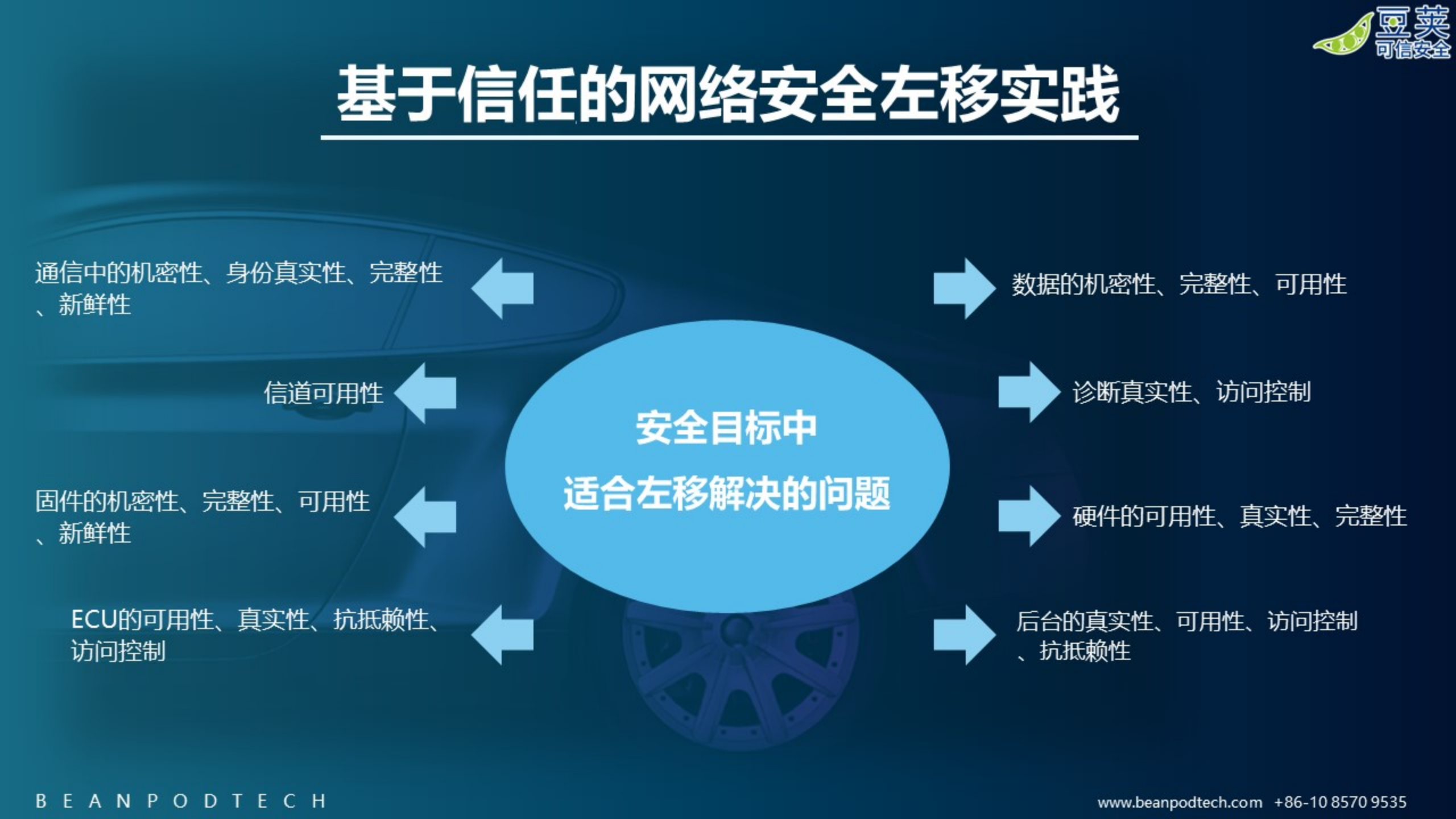
- 基于密钥保护的能力
- 基于敏感代码保护的能力
- 需要防UI劫持的场景
- 需要对资源做隔离的场景
- CCC车钥匙的场景
- 需要内容保护的场景
- 需要安全支付的场景



基于信任的网络安全左移实践

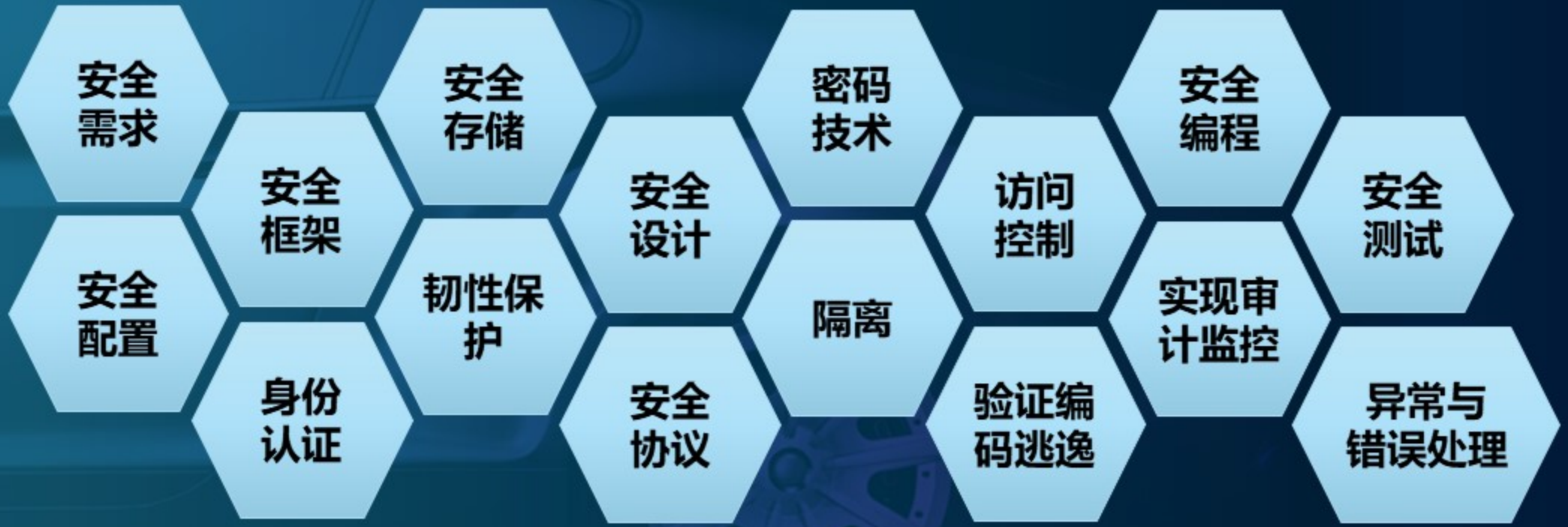


基于信任的网络安全左移实践



基于信任的网络安全左移实践

针对以上安全目标，常见的控制手段：



基于信任的网络安全左移实践

上述的安全目标和控制手段中，豆荚提供服务

谢谢观看

北京豆荚科技有限公司
WWW.BEANPODTECH.COM

Add：北京市海淀区中关村南大街乙12号天作国际B座1911室

Tel：010-85709535

E-Mail：business@beanpodtech.com