# 智能汽车网络安全防护技术与实践

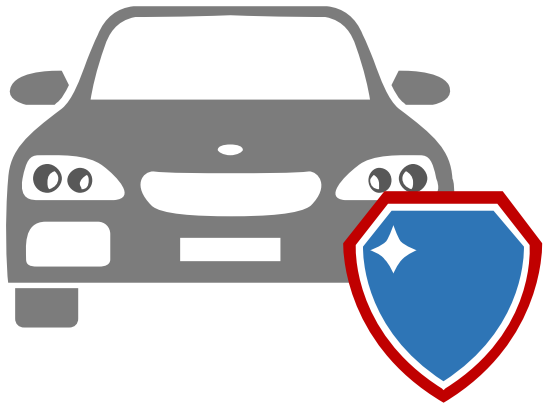
李 允

广东为辰信息科技有限公司

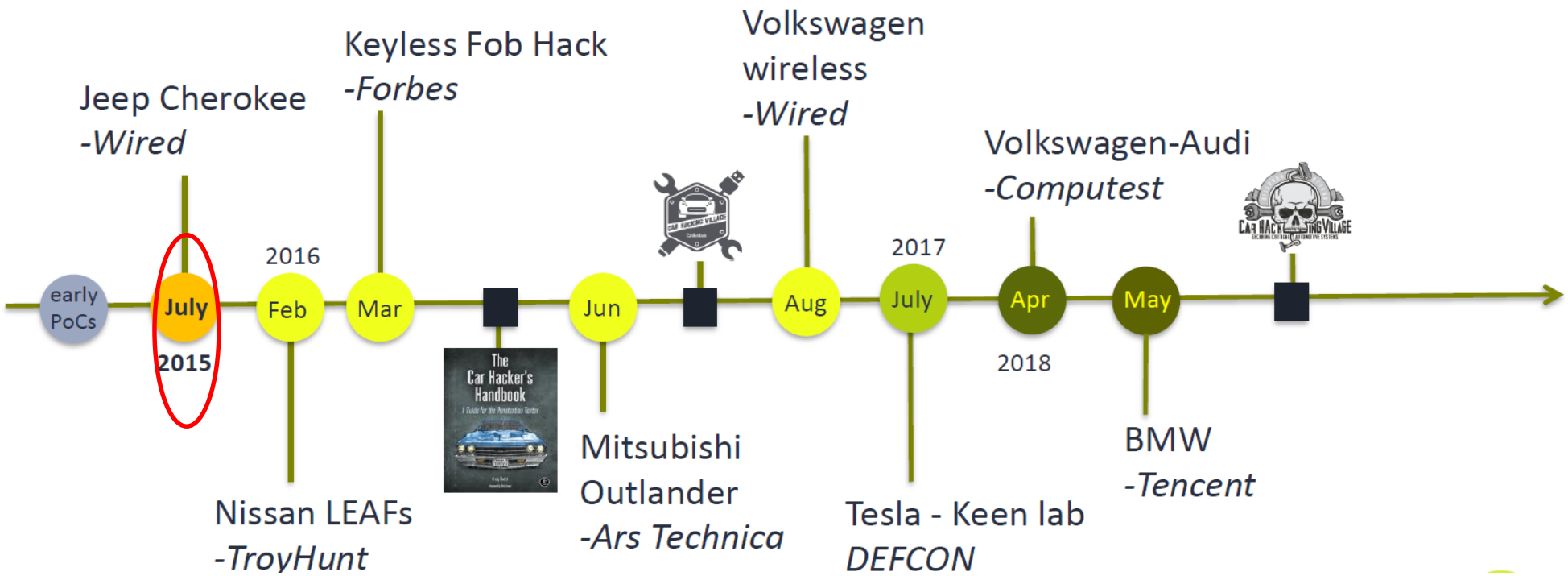
2020.09

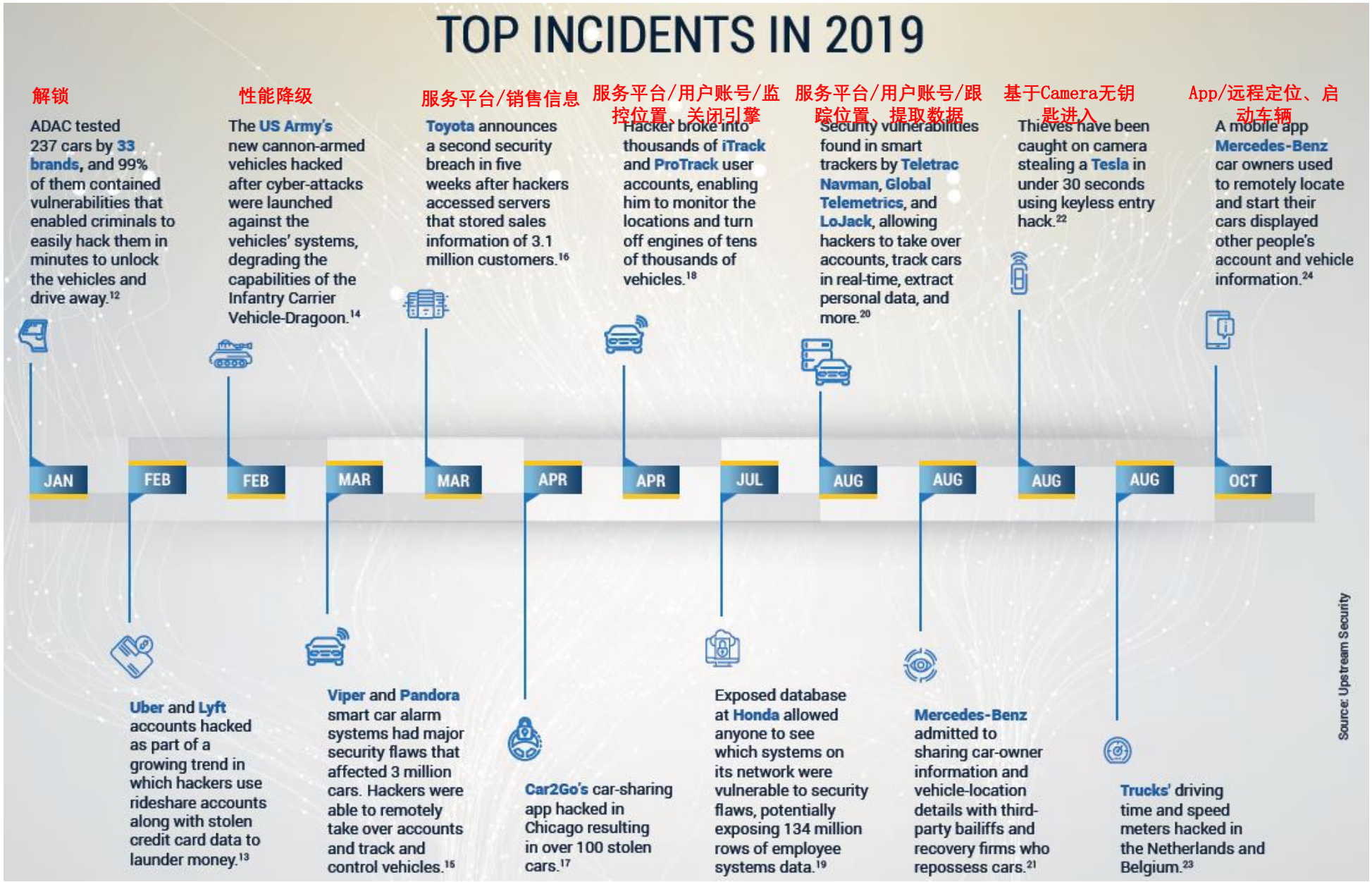
# 主要内容

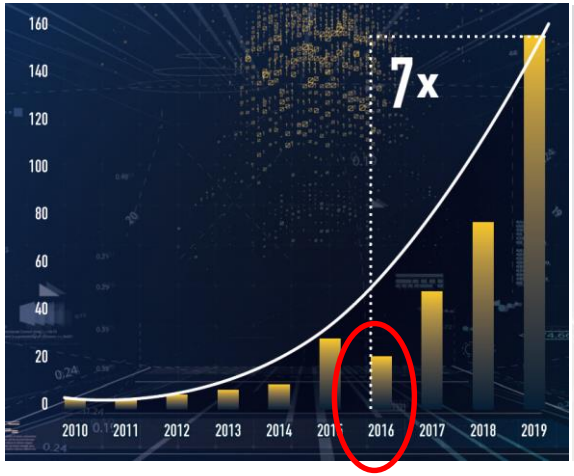
1. 汽车面临日益严峻的网络安全风险
2. 标准、法规与最佳实践
3. 网络安全防护
4. 网络安全与功能安全的融合问题
5. 结束语

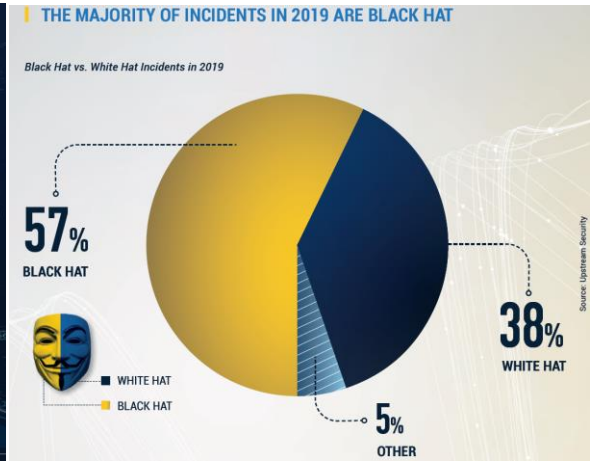


# 1 汽车面临日益严峻的网络安全风险




TOP INCIDENTS IN 2019
解锁
ADAC tested 237 cars by 33 brands, and 99% of them contained vulnerabilities that enabled criminals to easily hack them in minutes to unlock the vehicles and drive away.[12]
JAN
性能降级
The US Army's new cannon-armed vehicles hacked after cyber-attacks were launched against the vehicles' systems, degrading the capabilities of the Infantry Carrier Vehicle-Dragoon.[14]
FEB
服务平台/销售信息
Toyota announces a second security breach in five weeks after hackers accessed servers that stored sales information of 3.1 million customers.[16]
MAR
服务平台/用户账号/监控位置、关闭引擎
Hacker broke into thousands of iTrack and ProTrack user accounts, enabling him to monitor the locations and turn off engines of tens of thousands of vehicles.[18]
APR
服务平台/用户账号/跟踪位置、提取数据
Security vulnerabilities found in smart trackers by Teletrac Navman, Global Telemetrics, and LoJack, allowing hackers to take over accounts, track cars in real-time, extract personal data, and more.[20]
AUG
基于Camera无钥匙进入
Thieves have been caught on camera stealing a Tesla in under 30 seconds using keyless entry hack.[22]
AUG
App/远程定位、启动车辆
A mobile app Mercedes-Benz car owners used to remotely locate and start their cars displayed other people's account and vehicle information.[24]
OCT
FEB
Uber and Lyft accounts hacked as part of a growing trend in which hackers use rideshare accounts along with stolen credit card data to launder money.[13]
MAR
Viper and Pandora smart car alarm systems had major security flaws that affected 3 million cars. Hackers were able to remotely take over accounts and track and control vehicles.[15]
APR
Car2Go's car-sharing app hacked in Chicago resulting in over 100 stolen cars.[17]
JUL
Exposed database at Honda allowed anyone to see which systems on its network were vulnerable to security flaws, potentially exposing 134 million rows of employee systems data.[19]
AUG
Mercedes-Benz admitted to sharing car-owner information and vehicle-location details with third-party bailiffs and recovery firms who repossess cars.[21]
AUG
Trucks' driving time and speed meters hacked in the Netherlands and Belgium.[23]
Source: Upstream Security




2019年发生的信息安全事件是2016年的7倍，且57%属于黑客所为

Source: Upstream Security

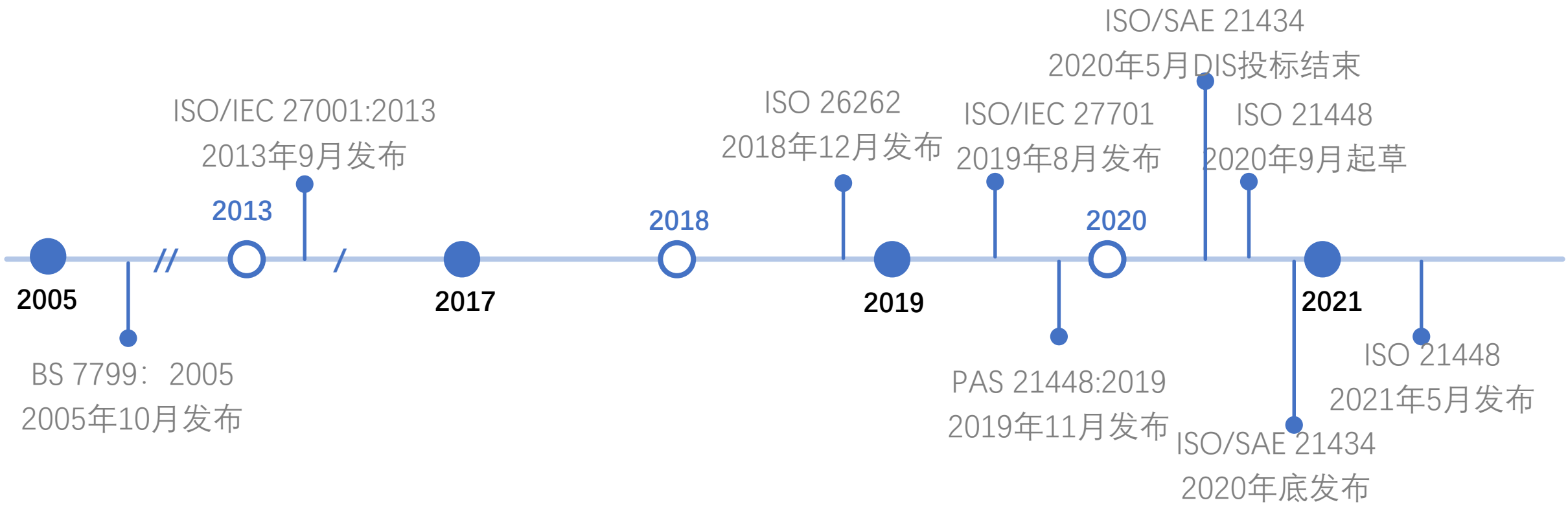


信息安全失效可能导致功能安全方面的危害

2015年7月，菲亚特-克莱斯勒在美国召回140万辆汽车，并对这些汽车的车载软件进行升级，以避免黑客远程控制发动机、转向系统，以及其他车载系统。两名研究人员利用笔记本电脑，通过这辆吉普车的联网娱乐系统侵入其电子系统，完成了行驶速度，空调、雨刮器、电台等方面内容的远程控制，甚至还把车“开进沟里”

甚至影响社会安全和国家安全

# 2 标准、法规与最佳实践


ISO/SAE 21434
2020年5月DIS投标结束
ISO/IEC 27001:2013
2013年9月发布
ISO 26262
2018年12月发布
ISO/IEC 27701
2019年8月发布
ISO 21448
2020年9月起草
2013
2018
2020
2005
2017
2019
2021
BS 7799：2005
2005年10月发布
PAS 21448:2019
2019年11月发布
ISO/SAE 21434
2020年底发布
ISO 21448
2021年5月发布

SAE INTERNATIONAL

| SURFACE VEHICLE RECOMMENDED PRACTICE | J3061™ | JAN2016 |
|---|---|---|
| | Issued 2016-01 | |
| Cybersecurity Guidebook for Cyber-Physical Vehicle Systems | | |

RATIONALE

To provide a cybersecurity process framework and guidance to help organizations identify and assess cybersecurity threats and design cybersecurity into cyber-physical vehicle systems throughout the entire development lifecycle process.

- Defines a complete lifecycle process framework that can be tailored and utilized within each organization's development processes to incorporate cybersecurity into cyber-physical vehicle systems from concept phase through production, operation, service, and decommissioning.
- Provides high-level guiding principles.
- Provides information on existing tools and methods.
- Provides the foundation for further standards development.

DRAFT INTERNATIONAL STANDARD

**ISO/SAE DIS 21434**

ISO/TC 22/SC 32 Secretariat: JISC

Voting begins on: 2020-02-12 Voting terminates on: 2020-05-06

# Road vehicles — Cybersecurity engineering

ICS: 43.040.15

## 2.1 SAE J3061; ISO/SAE 21434

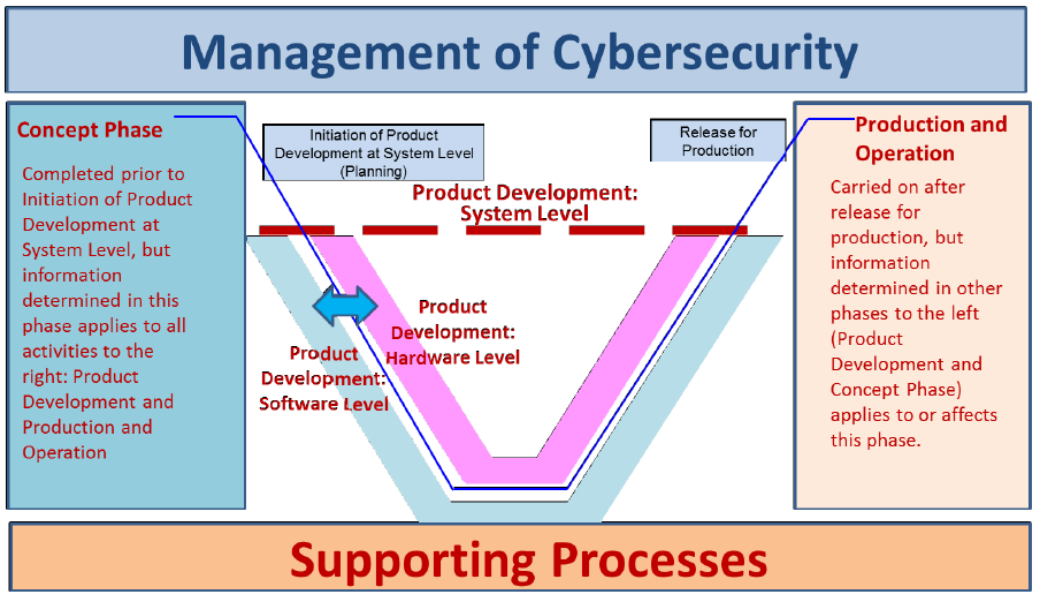



*Figure 3 - Overall Cybersecurity process framework*

**5. Overall cybersecurity management**

- 5.4.1 Cybersecurity governance
- 5.4.2 Cybersecurity culture
- 5.4.3 Cybersecurity risk management
- 5.4.4 Organizational cybersecurity audit
- 5.4.5 Information sharing
- 5.4.6 Management systems
- 5.4.7 Tool management
- 5.4.8 Information security management

**6. Project dependent cybersecurity management**

- 6.4.1 Cybersecurity responsibilities & their assignment
- 6.4.2 Cybersecurity planning
- 6.4.3 Tailoring of the cybersecurity activities
- 6.4.4 Reuse
- 6.4.5 Component out of context
- 6.4.6 Off-the-shelf component
- 6.4.7 Cybersecurity case
- 6.4.8 Cybersecurity assessment
- 6.4.9 Release for post-development

**7. Continuous cybersecurity activities**

- 7.3 Cybersecurity monitoring
- 7.4 Cybersecurity event assessment
- 7.5 Vulnerability analysis
- 7.6 Vulnerability management

**8. Risk assessment methods**

- 8.3 Asset identification
- 8.4 Threat scenario identification
- 8.5 Impact rating
- 8.6 Attack path analysis
- 8.7 Attack feasibility rating
- 8.8 Risk determination
- 8.9 Risk treatment decision

**Concept phase**

**9. Concept phase**

- 9.3 Item definition
- 9.4 Cybersecurity goals
- 9.5 Cybersecurity concept

**Product development phases**

**10. Product development**

- 10.4.1 Refinement of cybersecurity requirements and architectural design
- 10.4.2 Integration and verification
- 10.4.3 Specific requirements for software development

**11. Cybersecurity validation**

**Post-development phases**

**12. Production**

**13. Operations and maintenance**

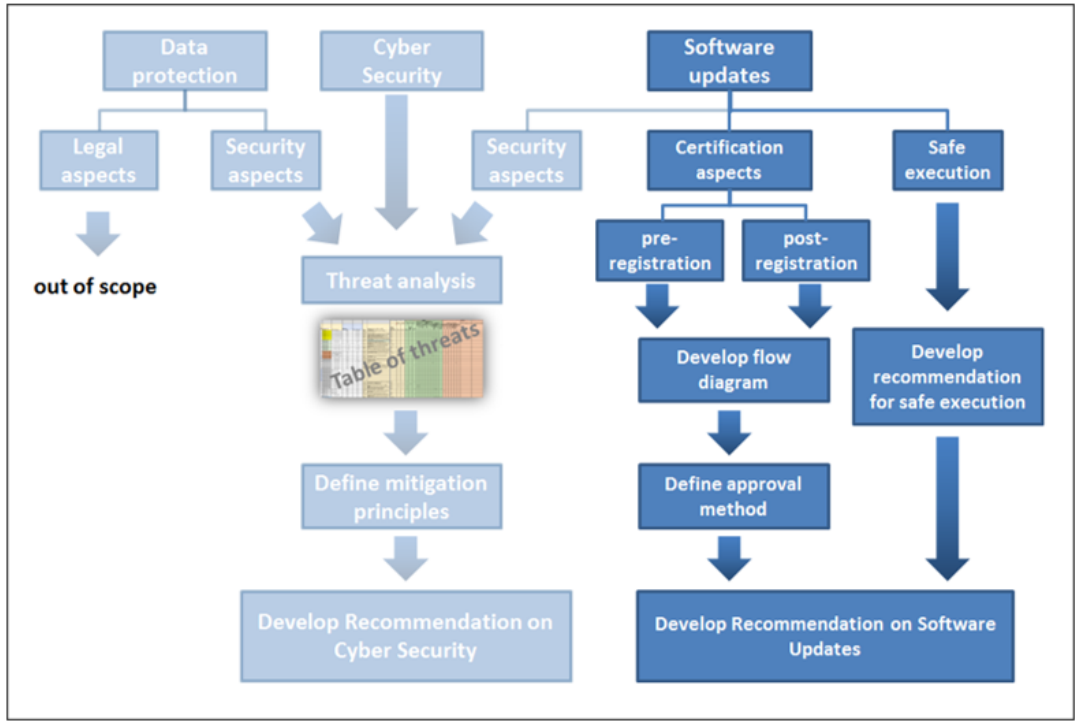
- 13.3 Cybersecurity incident response
- 13.4 Updates

**14. Decommissioning**

**15. Distributed cybersecurity activities**

- 15.4.1 Demonstration and evaluation of supplier capability
- 15.4.2 Request for quotation
- 15.4.3 Alignment of responsibilities

- UNECE WP.29 CS/OTA 信息安全法规
- CSMS是特定车型后的整车型式认证的前提条件
- OEM必须实现获得CSMS认证证书，并且在特定车型开发&量产项目尚，能够充分证明CSMS充分且有效运行后，才具备资格申请后续的特定车型所对应的整车型式认证




**7.2. → Requirements for the Cyber Security Management System**

| 7.2.2.1 Lifecycle Phases | 7.2.2.2 CSMS Scopes | 7.2.2.3 Response & Mitigation | 7.2.2.4 Continual Monitoring | 7.2.2.5 Supplier & Organizations |
|---|---|---|---|---|
| • 开发阶段<br>• 生产阶段<br>• 生产后阶段 | • 网络安全管理<br>• 风险识别、评估、分类、处置<br>• 网络安全验证、测试<br>• 更新风险评估<br>• 监控/检测/响应<br>• 分析网络安全攻击 | • 威胁、漏洞响应<br>• 威胁、漏洞缓解 | • 首次注册后的车辆<br>• 基于车辆数据和日志，分析、检测安全威胁、漏洞和攻击的能力 | • 供应商<br>• 服务提供商<br>• 分支机构 |

## 2.2 WP.29

TISAX（Trusted Information Security Assessment Exchange）最早起源于大众内部对其合作伙伴的信息安全审计，目的是对敏感信息的共享和保护，目前已扩展到所有的德国汽车主机厂（宝马、戴姆勒等）和各级供应商，成为一种通用的评估和交换机制，目的是为了实现德国汽车行业信息安全评估的相互接受，全球所有供应商（包括零部件厂商、外围服务商等）均应建立和维持信息安全管理体系，并通过与之相应级别的TISAX审计，作为必须准入条件。

成熟度等级

| | |
|---|---|
| 5 | 优化级（Optimizing） |
| 4 | 量化级（Predictable） |
| 3 | 已建立级（Established） |
| 2 | 已管理级（Managed） |
| 1 | 已执行级（Performed） |
| 0 | 无实施（Incomplete） |

## 信息安全 41

- 信息策略和组织
  - 信息安全策略
  - 信息安全组织
  - 资产管理
  - 信息安全风险管理
  - 评估
  - 事件管理
- 人力资源
- 物理安全和业务连续性
- 身份和访问管理
  - 身份管理
  - 访问管理
- IT安全和网络安全
  - 加密
  - 操作安全
  - 系统采购，需求管理和开发
- 供应商关系
- 符合性

## 原型保护 22

- 物理和环境安全
- 组织的要求
- 车辆、零部件的处理
- 测试车辆的要求
- 活动和拍摄的要求

## 数据保护 4

- 数据保护要求
- 个人可识别信息保护
- 数据保护有效性
- 数据保护符合性

# 2.3 TISAX

## ISO/IEC 27001《信息安全管理体系 要求》

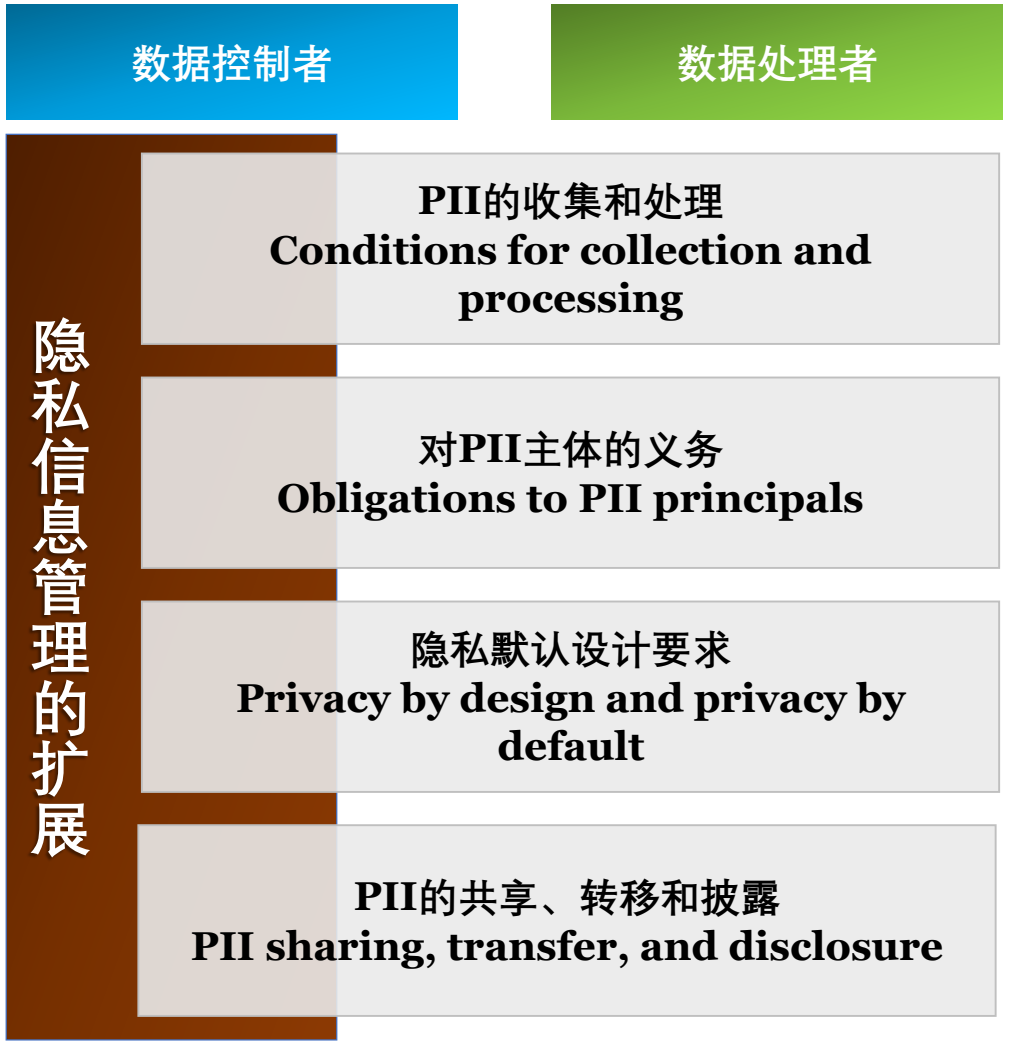
信息安全管理体系的基础，是信息安全建设的基本思路，基于PDCA方法论，为组织提供信息安全管理体系建设的方向和指引。

ISO/IEC 27001给出了信息安全的“What to do”，给出了普适性的安全要求，不同组织可以根据自身的风险状况和能力，选择适宜的安全措施。

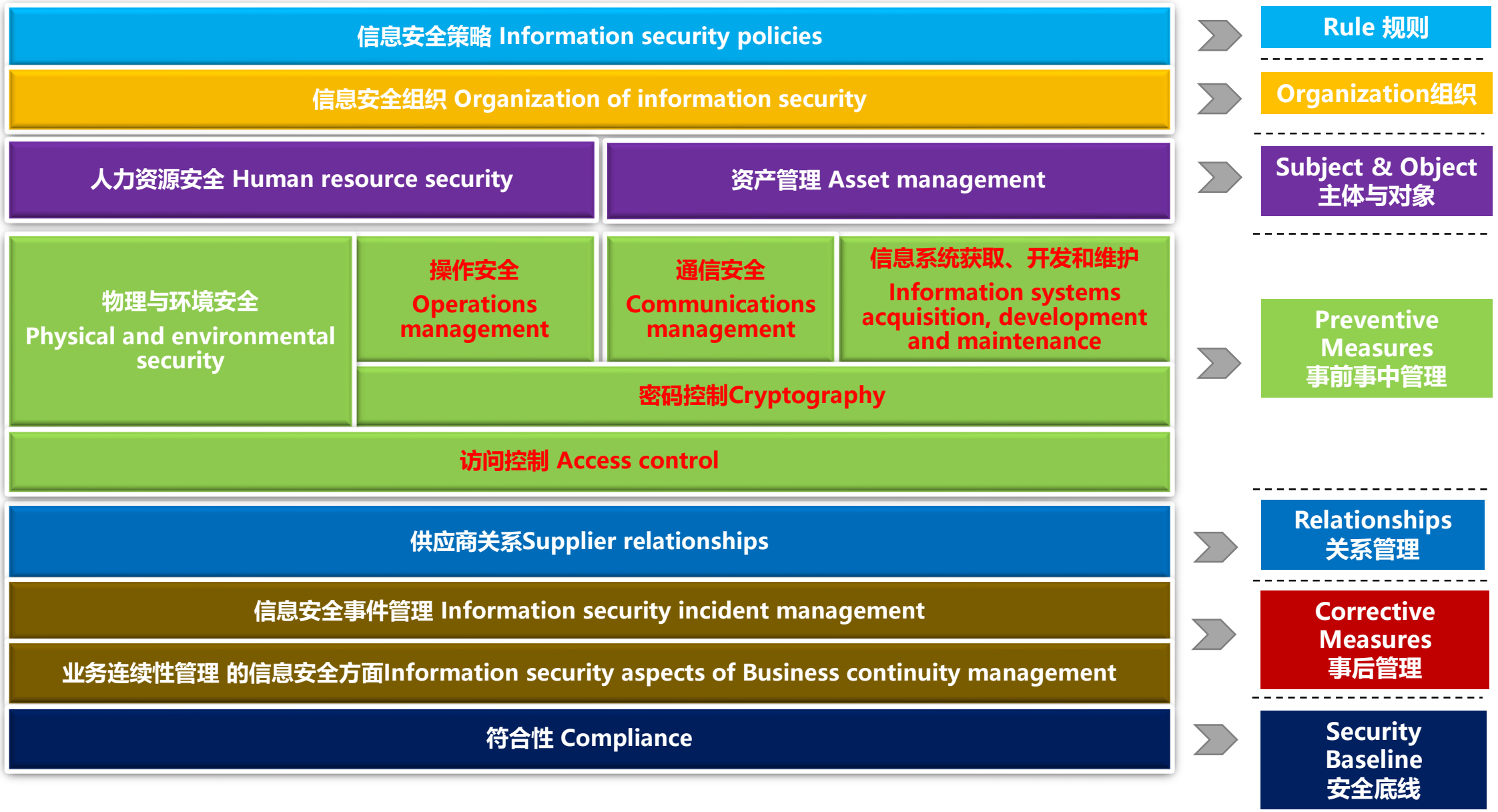
## ISO/IEC 27002《信息安全控制实践指南》

作为ISO/IEC 27001的实践指南，ISO/IEC 27002基于14个控制域、114个控制项，分别详细阐述了信息安全应该如何入手，构建起组织的信息安全框架。

ISO 27002是一个有关最佳实践的指南，告知组织做好信息安全的“How to do”。



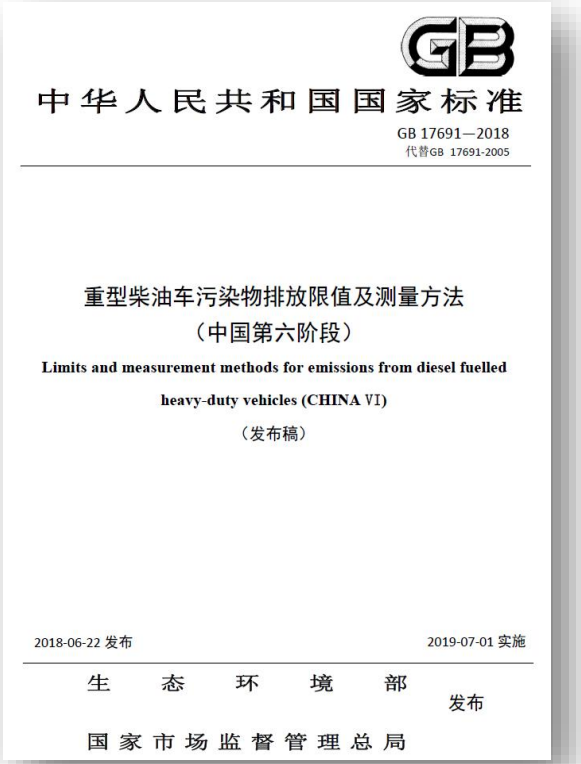

# 2.4 ISO27001/ISO27701




ISMS Control Domains 信息安全管理体系控制域

## 全国汽车标准化技术委员会（TC114）

| 批次 | 序号 | 标准项目/当前阶段 | 当前阶段 |
|---|---|---|---|
| 第一批 | 1 | 《汽车信息安全通用技术要求》 | 征求意见 |
| | 2 | **《电动汽车远程服务与管理系统信息安全技术要求》** | 征求意见 |
| | 3 | 《车载信息交互系统信息安全技术要求》 | 征求意见 |
| | 4 | **《汽车网关信息安全技术要求》** | 征求意见 |
| | 5 | 《电动汽车充电系统信息安全技术要求》 | 立项 |
| 第二批 | 6 | 《汽车软件升级通用技术要求》 | 立项 |
| | 7 | **《汽车诊断接口信息安全技术要求》** | 提交立项 |
| | 8 | 《汽车信息安全应急响应管理指南》 | 提交立项 |
| | 9 | 《汽车信息安全风险评估规范》 | 提交立项 |
| 第三批 | 10 | **《汽车整车信息安全技术要求与测试方法》** | 预研 |
| | 11 | **《道路车辆 信息安全工程》** | 提交立项 |
| | 12 | 《车载计算平台标准化需求研究》 | 预研 |
| | 13 | 《汽车电子控制单元（ECU）信息安全防护技术要求研究》 | 预研 |


中华人民共和国国家标准

GB 17691—2018

代替GB 17691-2005

重型柴油车污染物排放限值及测量方法

（中国第六阶段）

Limits and measurement methods for emissions from diesel fuelled heavy-duty vehicles (CHINA VI)

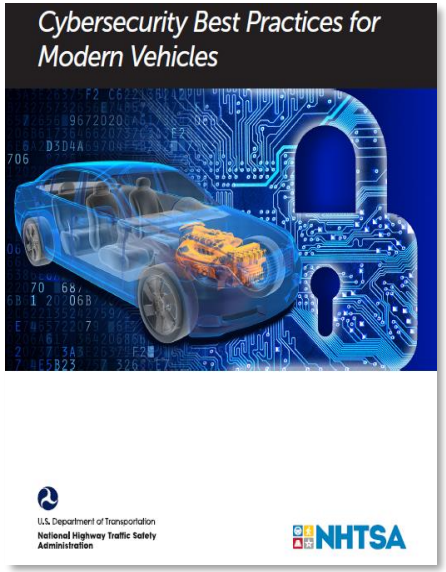
（发布稿）

2018-06-22 发布　　2019-07-01 实施

生　态　环　境　部　发布

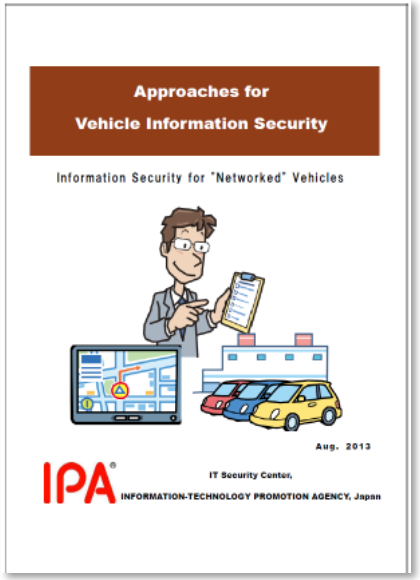
国家市场监督管理总局

## 2.5 国内标准发展情况


Cybersecurity Best Practices for Modern Vehicles
U.S. Department of Transportation
National Highway Traffic Safety Administration
NHTSA


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS
NOVEMBER 2019


The Key Principles of Cyber Security for Connected and Automated Vehicles
HM Government


Approaches for Vehicle Information Security
Information Security for "Networked" Vehicles
Aug. 2013
IPA
IT Security Center,
INFORMATION-TECHNOLOGY PROMOTION AGENCY, Japan

# 2.6 最佳实践

SAE INTERNATIONAL

| SURFACE VEHICLE RECOMMENDED PRACTICE | J3061™ | JAN2016 |
|---|---|---|
| | Issued 2016-01 | |
| Cybersecurity Guidebook for Cyber-Physical Vehicle Systems | | |

**①知道系统潜在的漏洞**（vulnerabilities）

- 是否存在敏感数据、个人身份信息（Personally Identifiable Information, PII）
- 在safety-critical functions中所扮演的角色
- 是否同车辆外部有联接或是通信
- 是否可能作为跳板去攻击其他系统
- 是否有信息（时间、功耗等）可用于侧信道攻击（side channel attack）
- 执行威胁分析与风险评估

**②明白系统的关键安全原则**

- 保护个人身份信息
  - 对用户数据采用保守的默认访问设置
  - 在收集、传输任何数据前需要得到认可
  - 阻止非授权访问
- 使用最小权限原则；纵深防御（Defense in Depth）；禁止在全面分析和测试之前对标定、数据进行修改
- 禁止车主有意或是无意对可能导致潜在漏洞的内容进行非授权修改：改变标定设置或是软件，以改变动力性能；在不通知用户或是告知用户存在风险的情况下，通过DVD或是手机把软件安装在信息娱乐系统中

**③考虑车主对系统的使用**

- 最小化收集数据：使用数据中最不敏感的内容（姓名的敏感度要低于社会保障号码）
- 采用用户控制策略：车主负责管理敏感数据，可在必要的时候由车主授权。也包括制造商管理隐私的设置问题
- 保护个人身份信息的存储、使用和传输
- 在收集、存储或是共享个人信息时，提供必要的通知信息，以便车主能够进行正式的决策
- 为经销商、服务热线、网页和车主提供必要的材料，以便车主能够掌握隐私数据方面的情况，并告知车主系统在相关方面的能力和局限性，提供通常的安全实践

**④在概念（concept）和设计阶段实现安全**

- 设计feature时，融入安全，并从生命周期的概念阶段开始
- 分析系统面临的威胁。对于确定的威胁，识别漏洞，并确定合适的安全控制（cybersecurity controls）
- 开展安全分析，确定、配置系统的最优安全等级

**⑤在开发和验证中实现安全**

- 通过评审，对设计是否符合安全需求进行评估
- 执行测试，对feature的安全需求是否得到满足进行确认
- 与feature或是软件进行**重刷写**可能带来的任何风险，需要最小化或是彻底规避

**⑥在应急响应（incident response）中实现安全**

- 修订或是创建应急响应过程
- 在出现安全事件的情况下，确定更新软件或是标定

**⑦车主发生变化时的安全考虑**

- 确定系统中是否有数据或是车主身份信息需要被擦除
- 提供擦除个人信息的方法


## POLICIES

17

- Security by design
- Privacy by design
- Asset management
- Risk and threat management

## ORGANISATIONAL PRACTICES

15

- Relationships with suppliers
- Training and awareness
- Security management
- Incident management

# GOOD PRACTICES

## TECHNICAL PRACTICES

50

- Detection
- Protection of networks and protocols
- Software security
- Cloud security
- Cryptography
- Access control
- Self-protection and Cyber Resilience
- (Semi-) autonomous systems self protection and cyber resilience
- Continuity of operations

### 4.4.7 Self-Protection and Cyber Resilience

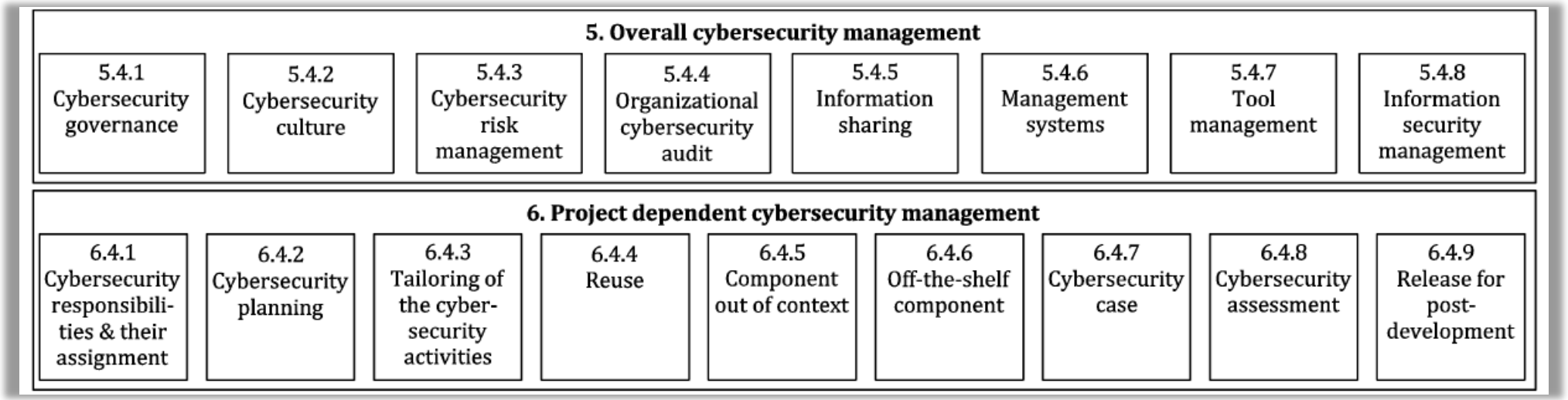
- 差分监测：GNSS系统，获得准确的定位数据
- 不同层级（设备、网络、后台）加固，减少攻击面
- 接口健壮性，如应对缓冲区溢出或fuzzing
- 运行时应用隔离，使用可信软件技术
- 网络分段：物理和逻辑的技术

### 4.4.8 (Semi-) Autonomous Systems Self Protection and Cyber Resilience

- 考虑使用惯性导航
- 保护传感器：防止通过攻击的方式影响车辆对环境的感知能力
- 防止AI和ML的对抗攻击、伪造数据
- 数据冗余：传感器数据融合
- 硬件冗余

| 生命周期过程 | 技术 |
| --- | --- |
| 管理：组织架构、文化 | |

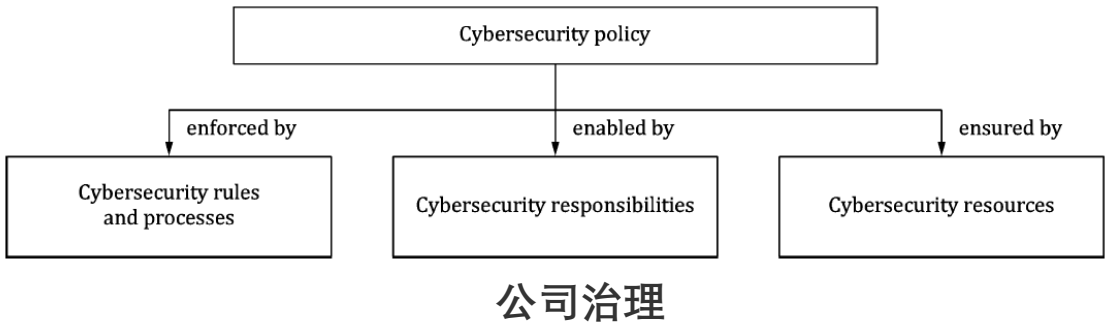
| 标准/规范 | 最佳实践 | 信息共享、威胁情报与应急响应 | 测评体系 | 第三方安全公司 |
| --- | --- | --- | --- | --- |


5. Overall cybersecurity management
5.4.1 Cybersecurity governance
5.4.2 Cybersecurity culture
5.4.3 Cybersecurity risk management
5.4.4 Organizational cybersecurity audit
5.4.5 Information sharing
5.4.6 Management systems
5.4.7 Tool management
5.4.8 Information security management
6. Project dependent cybersecurity management
6.4.1 Cybersecurity responsibili-ties & their assignment
6.4.2 Cybersecurity planning
6.4.3 Tailoring of the cyber-security activities
6.4.4 Reuse
6.4.5 Component out of context
6.4.6 Off-the-shelf component
6.4.7 Cybersecurity case
6.4.8 Cybersecurity assessment
6.4.9 Release for post-development

# 3.1 网络安全管理

## **整体网络安全管理：**公司治理，公司文化

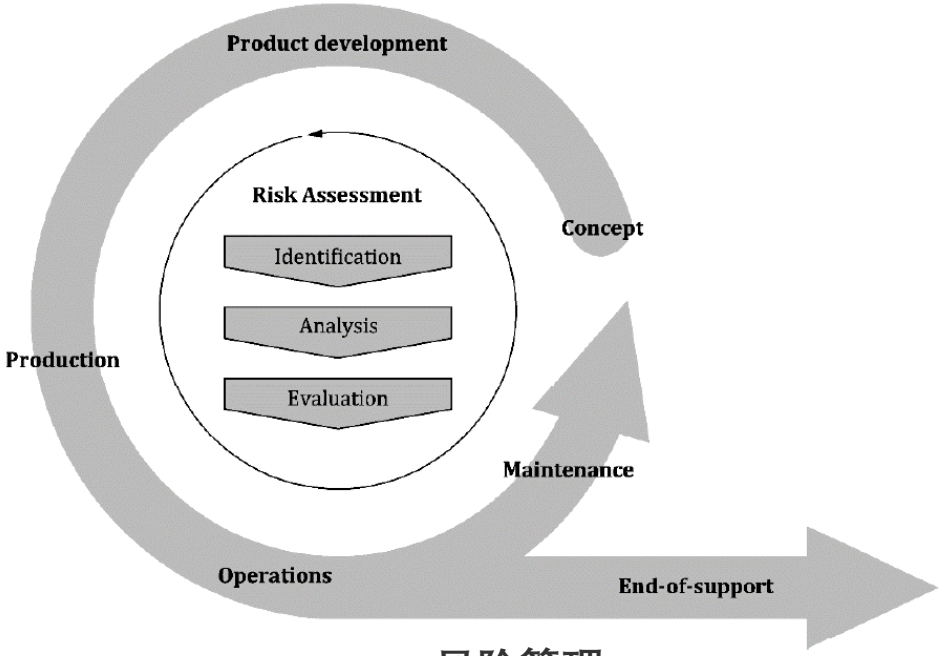
- 方针（安全风险；管理风险的承诺；风险处置），组织相关规则、过程（漏洞披露、生命周期）
- 分配职责、机构：实施安全活动
- 为实现安全提供支持：资源、管理
- 安全文化：意识、能力、持续改进
- 组织级**安全审计**
- **信息共享**管理
- 建立和维护支持安全活动的**管理系统**
- 提供证据证明所使用**工具**不影响网络安全




**公司治理**

## 项目网络安全管理

- 为项目安全活动分配职责
- 计划：安全活动
- **安全案例**：所达到网络安全程度的证明材料
- **安全评估**：判断所达到的网络安全程度
- **发布决策**：进入开发后阶段




**风险管理**

### 4.2.1 Security by design

- 采用设计安全方法：车辆和基础设施
- 确保安全在**概念阶段的初期**就被考虑
- **开发和运行阶段**的活动考虑安全/基于方法的
- **安全角色**：领导产品过程团队的安全相关任务

### 4.2.2 Privacy by design

- 采用本地和国际的隐私相关法规
- 隐私影响评估：识别隐私相关的风险，并采用合适的措施进行缓解
- **隐私审计**：每年至少一次，确保符合隐私相关方针

### 4.2.3 Asset Management

- 使用工具进行资产管理：自动发现、识别、分类
- **维护资产目录**
- 对车辆来说，根据变更过程引入新的设备或软件变更

### 4.2.4 Risk and Threat Management

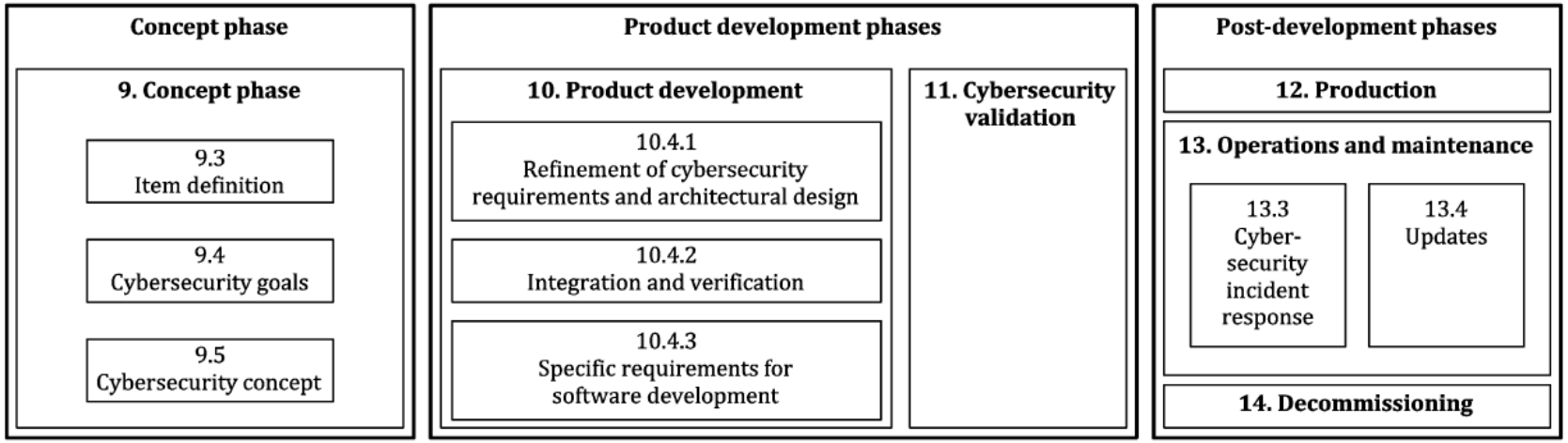
- 风险管理方法：针对汽车领域不断出现的威胁和攻击
- 设计的早期就进行风险分析：至少每年更新
- 监控投放市场车辆的安全漏洞：每六个月或更频繁
- 安全评估：渗透测试/事件驱动：更新升级后新的威胁或漏洞
- 建立威胁情报过程：新攻击类型/攻击源、新漏洞的信息能够得到及时通知
- 安全控制：至少一年一次评估，并通过补丁缓解风险
- 安全假设：至少每半年检查一次

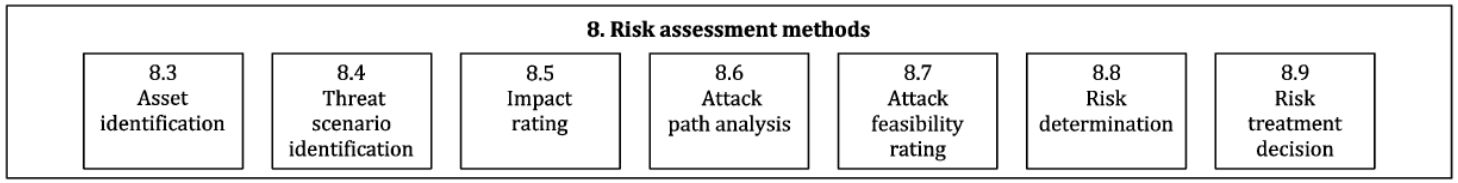
### 4.3.2 Training and Awareness

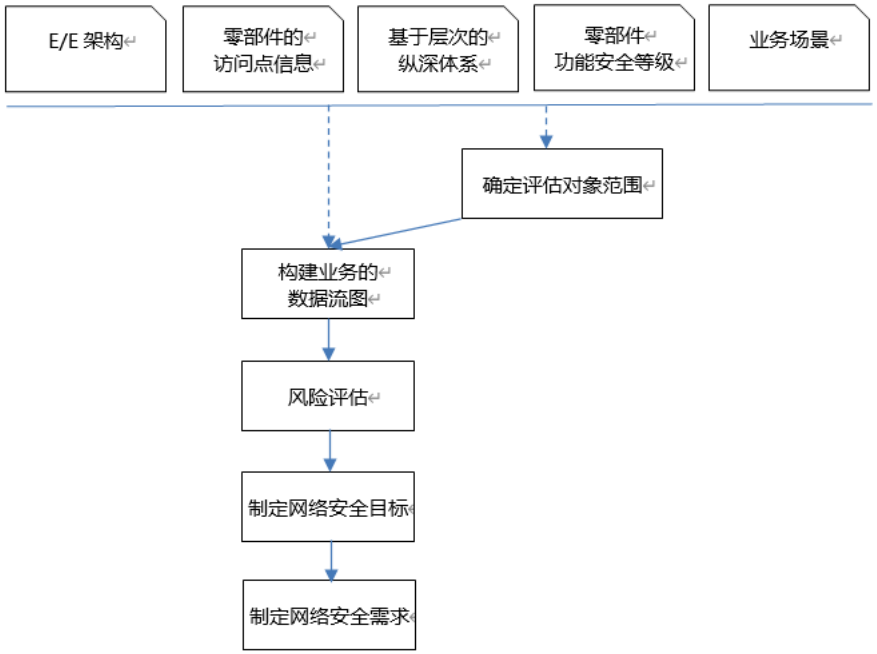
- **共享相关信息**：分公司、供应商和第三方伙伴，参考ISAC
- 对员工采用**系统的培训方法**
- 安全培训是持续的、有规律的，且经常更新
- 提升车主、驾驶人员和乘客的**安全意识**：如何预防

### 4.3.3 Security Management

- SOC：角色、职责、能力；监控预防潜在威胁
- 具有**安全技能**的团队：多样性、宽范围能力
- **信息安全管理系统**：覆盖车辆生命周期
- 特别工作组：领导安全相关战略决策和资源保障




- **评审**：验证方法；检查文档或工作产品/基于特定目标或原则；检查表
- **分析**：系统而方法的手段，对工作产品进行研究；检查内在的脆弱性、人因错误、已知系统缺陷，以及结合需求的一致性、正确性、完整性；可采用业界标准方法、最佳实践识别漏洞：静态代码分析/MISRA-C/CERT-C
- **仿真**：确认正在设计中系统需求或设计规格的一致性、正确性和完整性
- **原型**：基于早期样品，确认正在设计中系统需求或设计规格的一致性、正确性和完整性
- **功能测试**：在测试环境中，确认功能是否满足需求
- **接口测试**：基于功能测试，验证输入、输出是否满足需求
- **渗透测试**：以发现漏洞为目的，加固系统、抵御威胁为目标；黑盒、灰盒、白盒
- **漏洞扫描**：可作为渗透测试或分析的技术手段之一
- **模糊测试**：把大量随机数据（自动或半自动）注入系统，寻找脆弱性/溢出、段和堆错误；可以作为渗透测试的手段之一

# 3.2 生命周期

United Nations ECE/TRANS/WP.29/GRVA/2020/3

Economic and Social Council

Distr.: General
1 December 2019

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Working Party on Automated/Autonomous and Connected Vehicles*

Fifth session
Geneva, 10–14 February 2020
Item 5 (a) of the provisional agenda
Connected vehicles:
Cyber security and date protection as well as software updates

→ → Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems

## Part A. Vulnerability or attack method related to the threats

4.3.1 Threats regarding back-end servers related to vehicles in the field
4.3.2 Threats to vehicles regarding their communication channels
4.3.3. Threats to vehicles regarding their update procedures
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack
4.3.5 Threats to vehicles regarding their external connectivity and connections
4.3.6 Threats to vehicle data/code
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened

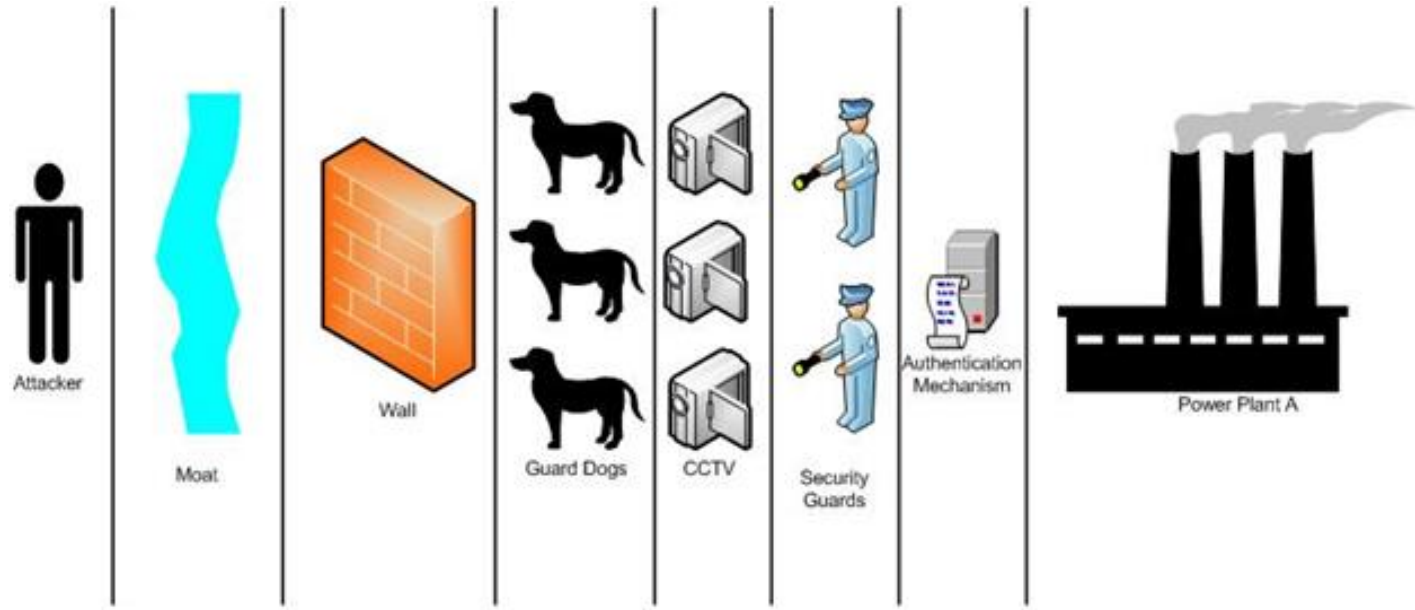
## Part B. Mitigations to the threats intended for vehicles

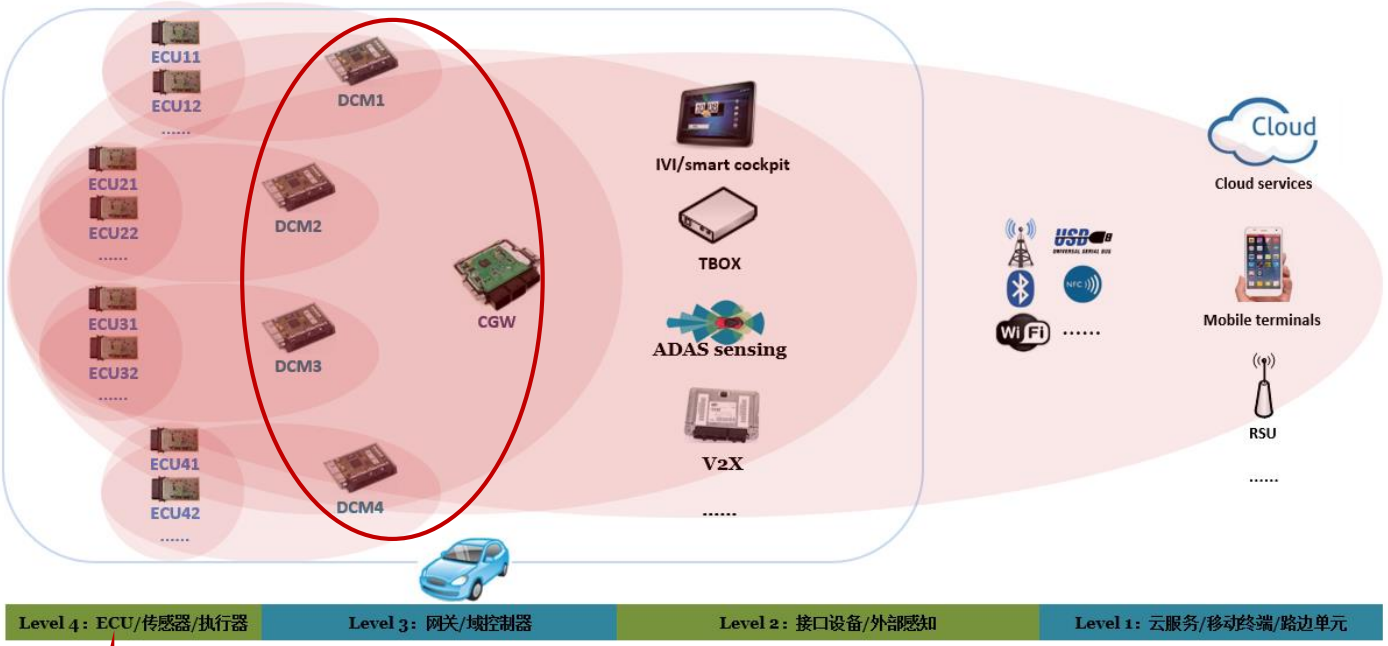
| *Table A1 reference* | *Threats to "Vehicle communication channels"* | *Ref* | *Mitigation* |
|---|---|---|---|
| 4.1 | Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation | M10 | The vehicle shall verify the authenticity and integrity of messages it receives |
| 4.2 | Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road) | M11 | Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules) |

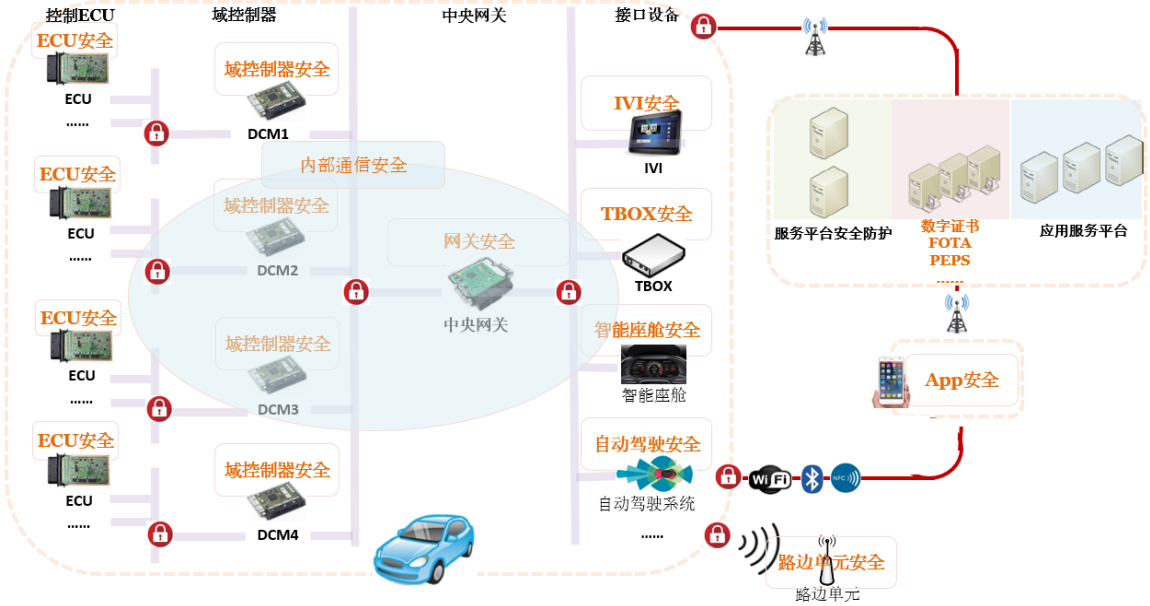
## Part C→ → Mitigations to the threats outside of vehicles

| *Table A1 reference* | *Threats to "Back-end servers"* | *Ref* | *Mitigation* |
|---|---|---|---|
| 1.1 & 3.1 | Abuse of privileges by staff (insider attack) | M1 | Security Controls are applied to back-end systems to minimise the risk of insider attack |
| 1.2 & 3.3 | Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) | M2 | Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP |
| 1.3 & 3.4 | Unauthorised physical access to the | M8 | Through system design and access control it should |

# 3.3 网络安全防护技术


Attacker
Moat
Wall
Guard Dogs
CCTV
Security Guards
Authentication Mechanism
Power Plant A




① **端到端**。智能汽车全要素覆盖：车辆、云服务、移动终端、路边单元，解决如下安全问题：真实性；完整性；机密性；可用性；防抵赖；可授权

② **纵深防御**。车辆内部（访问点防护；接口设备安全防护；基于网关、域控制器的安全防护；总线通信安全防护；零部件安全防护）；车外系统安全防护

纵深防御、全要素覆盖


检测防御：监控与应急响应

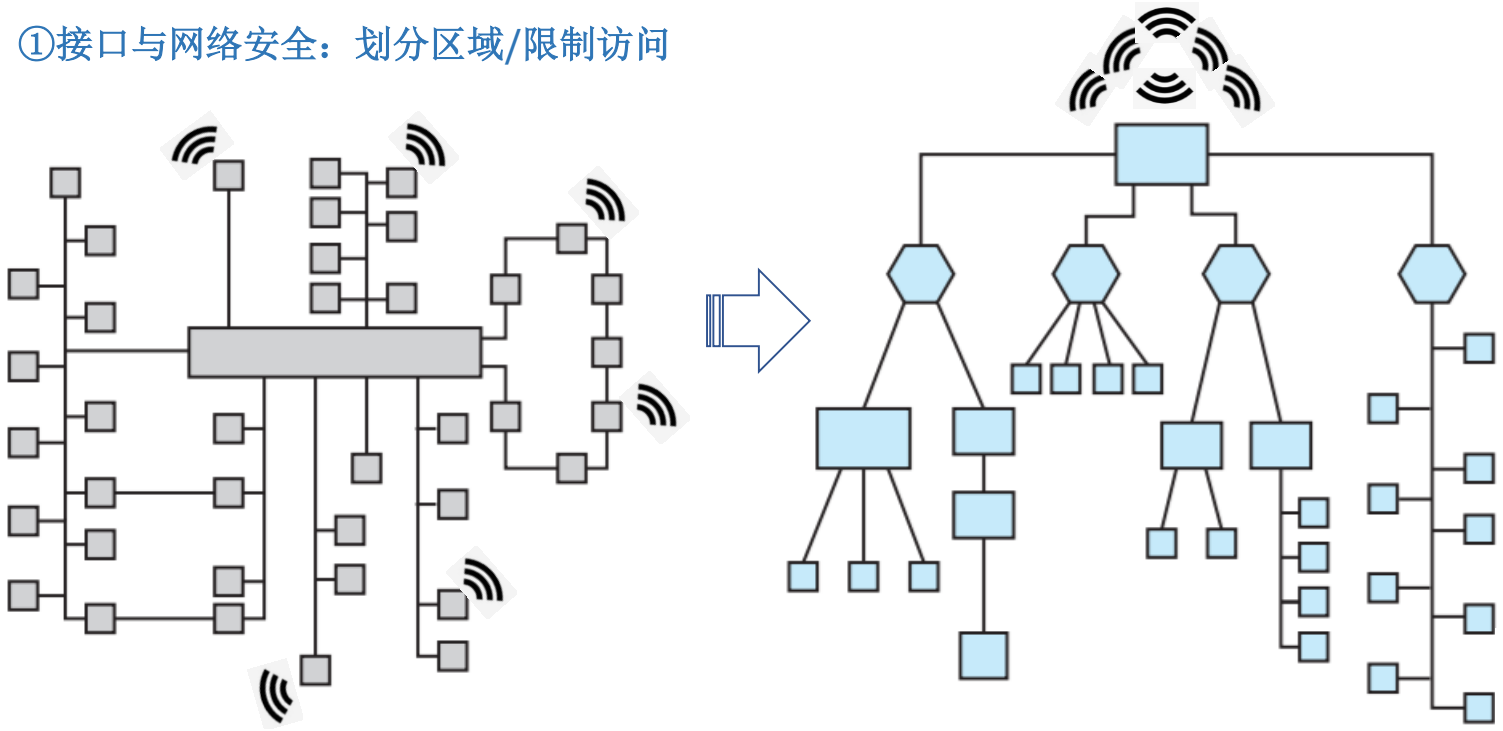
接口与网络安全：外部访问点/划分区域/隔离；可用性/网络出现DOS攻击，或flood攻击，在下一个网关就可以限制流量的速率

数据传输安全：身份真实性、数据完整性、数据保密性、抗重放

零部件安全：防配置篡改；防非法软件植入

基于以太网的E/E架构网络安全防护

## ①接口与网络安全：划分区域/限制访问



限制具有外部访问点的ECU数量

访问点：WLAN, bluetooth, cellular, wireless key, OBD ...

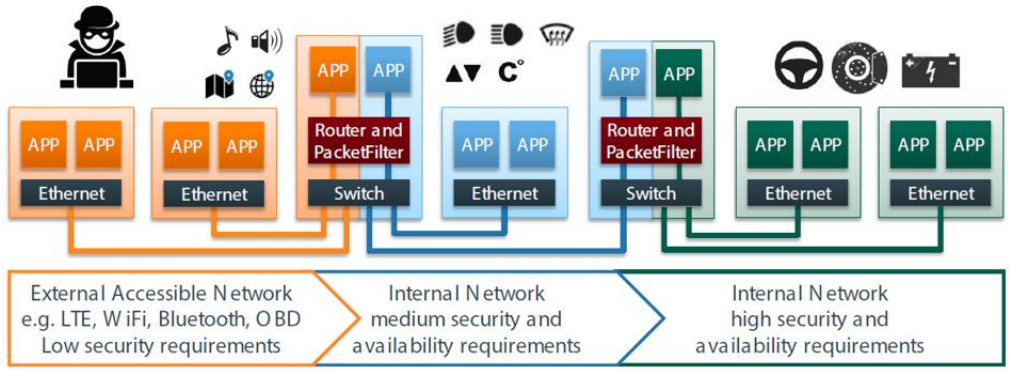
重点防护与外部有访问点的接口设备

接口设备采用状态防火墙，诊断通信不直接与ECU交互；基于中央网关，且与中央网关之间采用基于TLS的安全通信

功能安全

| ASIL等级 | 零部件 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| QM | | | | | | | | |
| A | ARC | HUD | VSP | ALM | DSM | IEM&RVM | | |
| | HMT | MCU | ACM | BMS | PDU | IPEU | WPT | EGSM |
| | DCM | PDM | NTDM | PLGM | SCM | OLM | ESCL | SCAM |
| | LIN设备 | | | | | | | |
| B | TBOX | CGW | IDCM | ADCM | VDCM | BDCM | | |
| C | | | | | | | | |
| D | APA | 底盘 | | | | | | |

功能安全等级



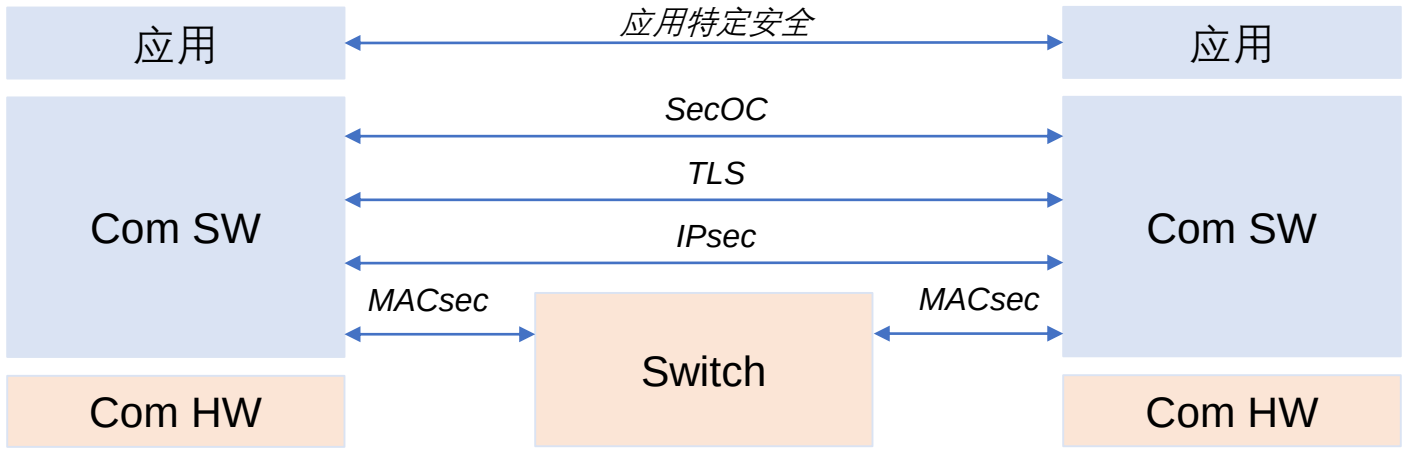

### 网络设计/网络拓扑

把网络划分为多个不同的安全区域，区域之间采用受限通信方式

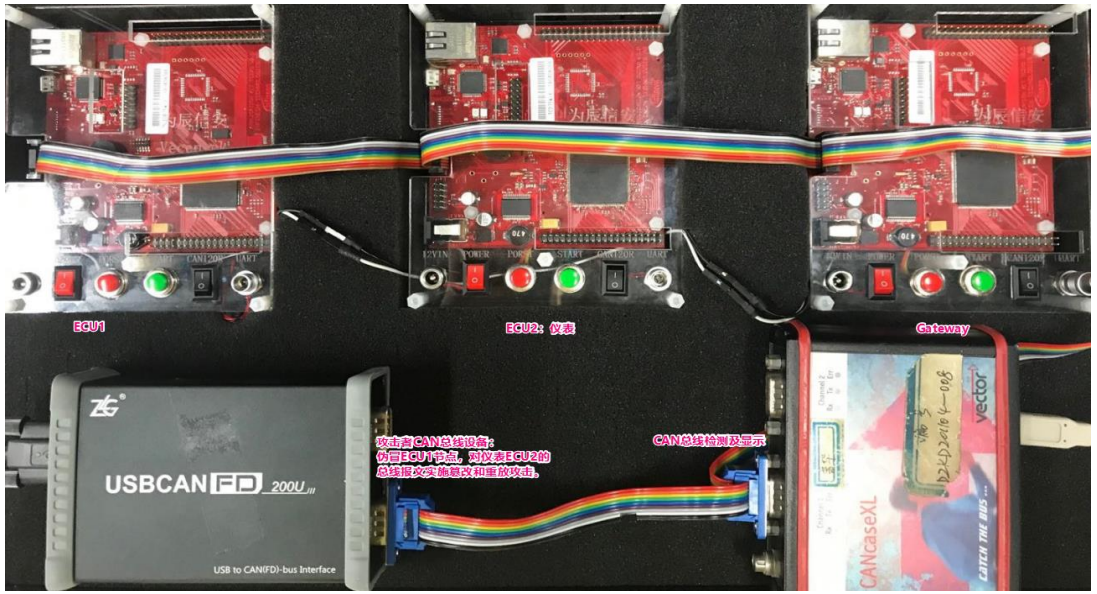
安全区域划分：限制具有外部访问点的ECU数量；功能安全等级

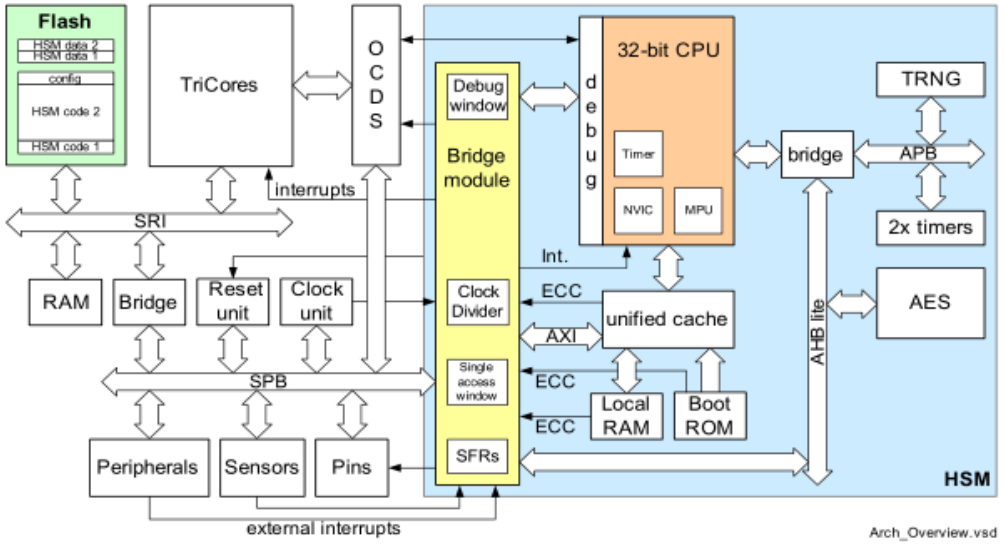
合法、授权数据可以跨域：VLAN通信；物理隔离

## ②数据传输安全

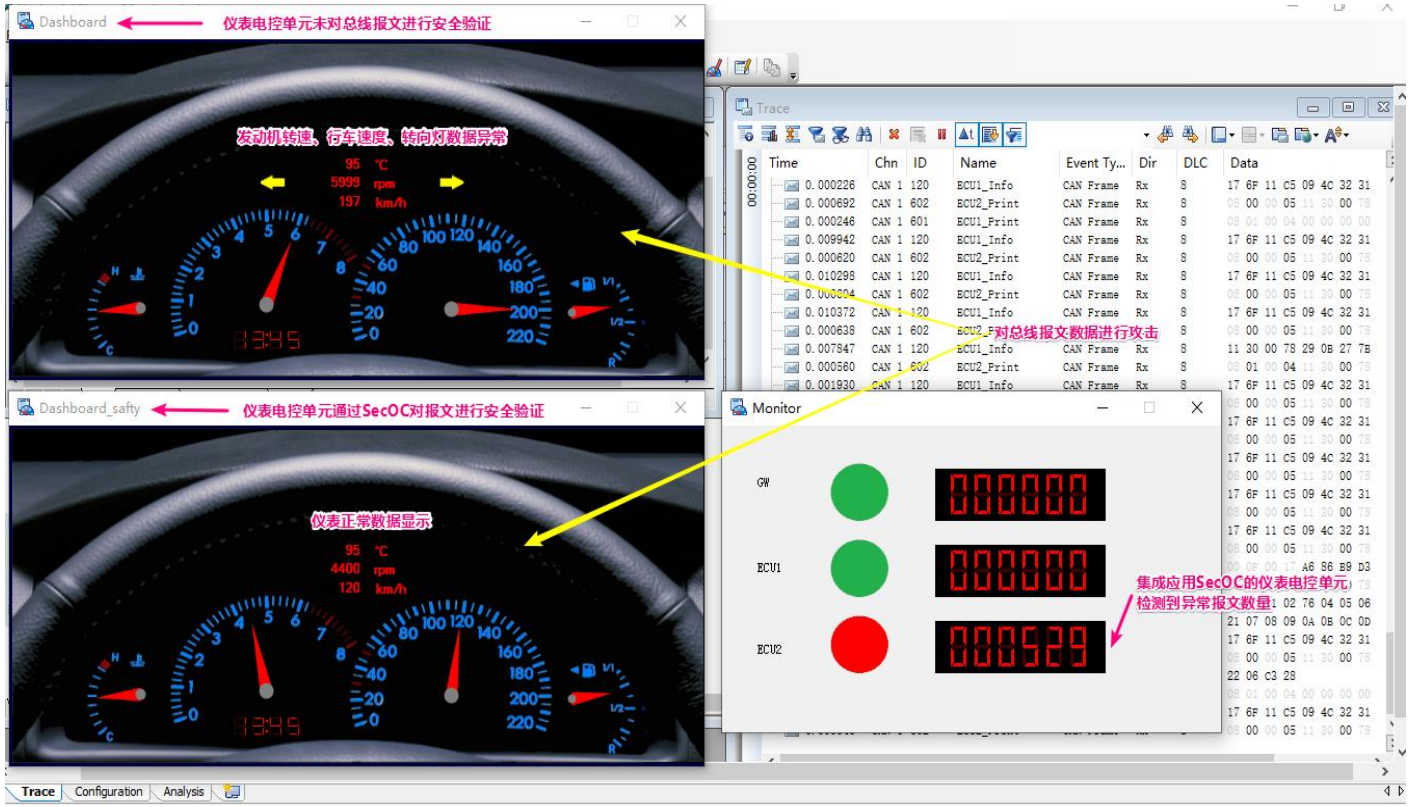



| 协议 | 标准 | 类型/协议层次 | 真实性 | 保密性 |
|---|---|---|---|---|
| MACsec | IEEE 802.1AE | Hop-by-Hop<br>Data-Link | √ | √ |
| IPsec AH | IETF RFC 4302 | End-to-End<br>IP | √ | x |
| IPsec ESP | IETF RFC 4303 | End-to-End<br>IP | √ | √ |
| TLS | IETF RFC 5246 | End-to-End<br>TCP | √ | √ |
| SecOC | AUTOSAR | End-to-End<br>PDUs | √ | x |



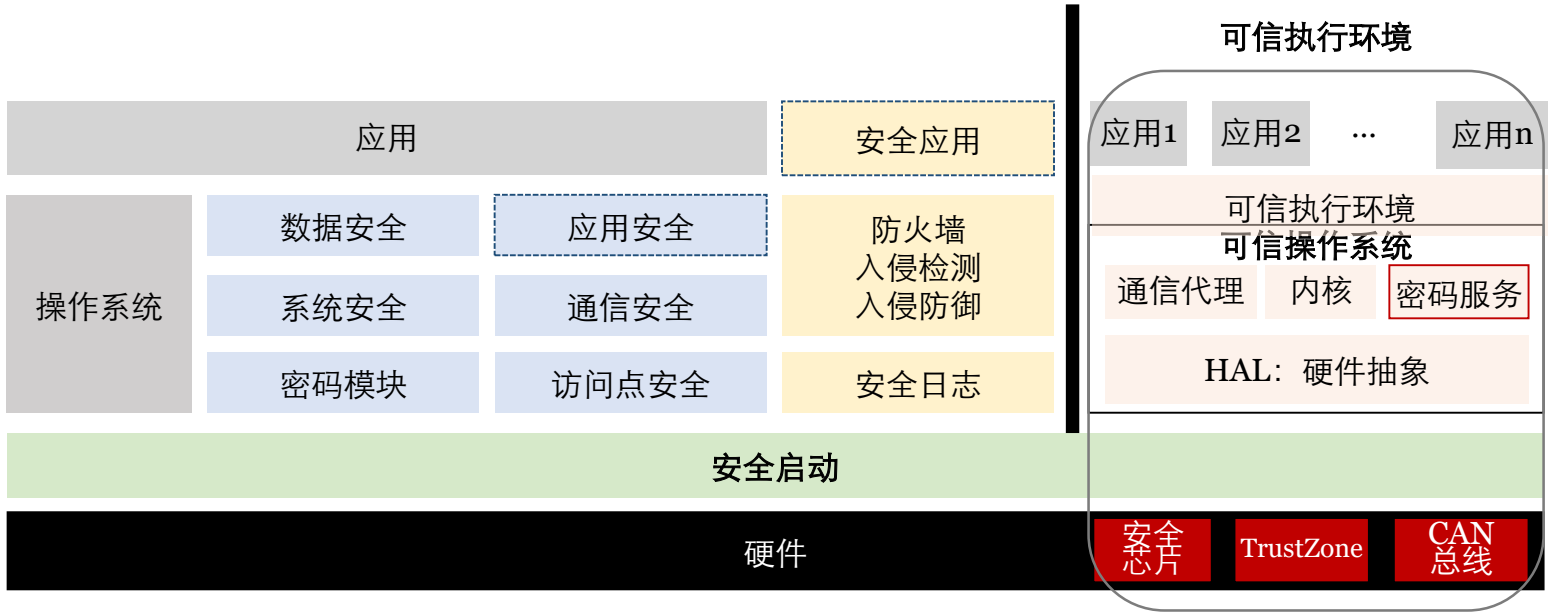




Tricores是非安全核，HSM是安全核，Tricores与HSM的资源相互隔离，HSM通过中断和寄存器来控制Tricores，数据传递则是通过共享内存来实现



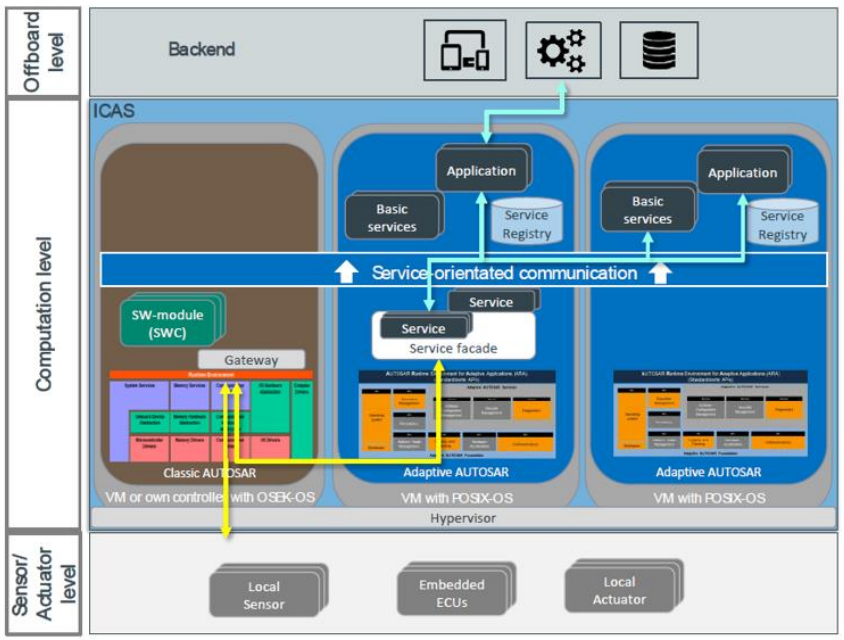

基于AurixTC275的SecOC展示环境

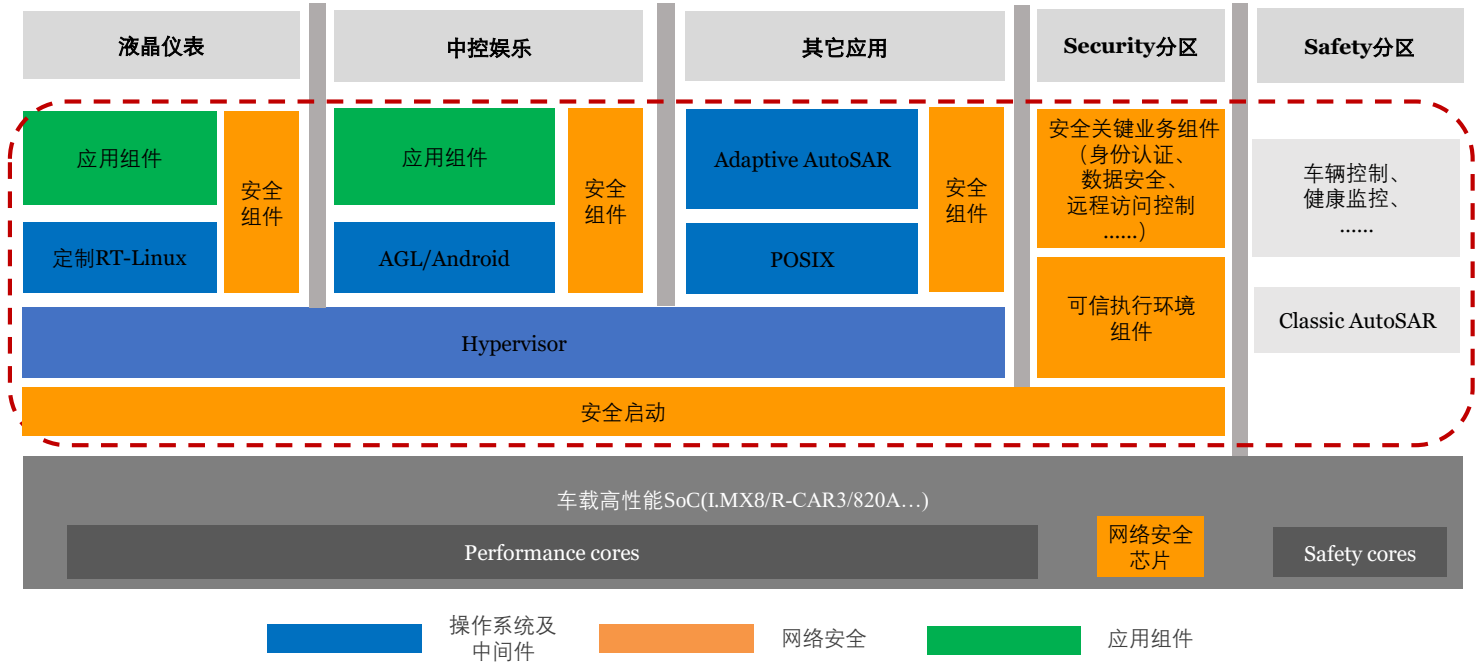
## ③零部件安全




### 以太网交换安全

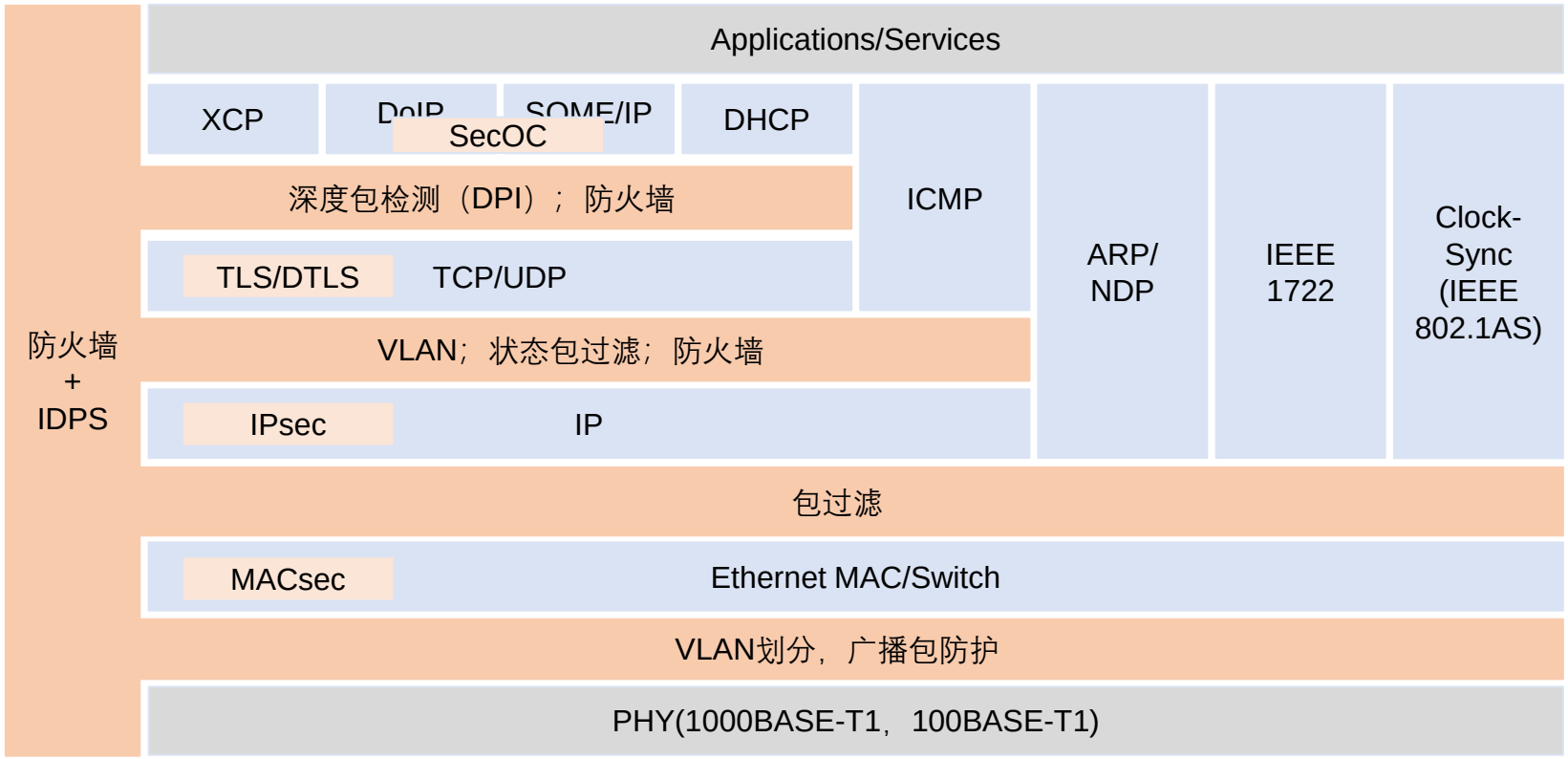
数据篡改：VLAN配置、防火墙规则；交换配置




下一代零部件安全：智能座舱、中央网关、域控制器、自动驾驶、……

## ④检测与防御：通信监控/防火墙 + IDPS




**合法、授权数据通信才能跨越domain和VLAN**

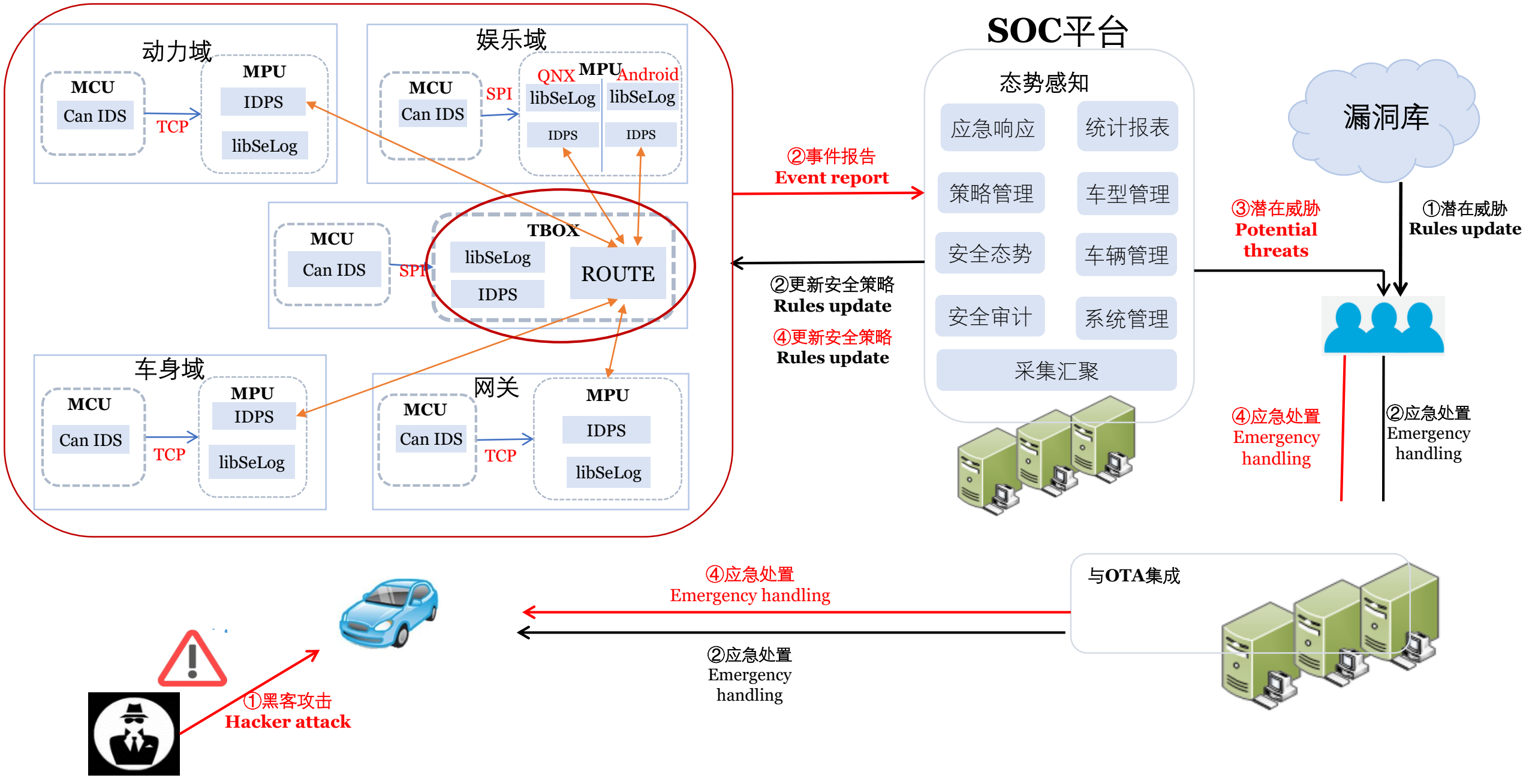
基于业务的VLAN划分

| VLAN Tag | VLAN ID | Use Case |
|---|---|---|
| VLAN_00 | 100 | OTA业务 |
| VLAN_01 | 101 | 诊断业务 |
| VLAN_02 | 102 | 车辆信息和事件上报 |
| VLAN_03 | 103 | 车辆控制 |
| VLAN_04 | 104 | 高清地图下载 |

IP地址分配

| Node | VLAN_00 | VLAN_01 | VLAN_02 | VLAN_03 | VLAN_04 |
|---|---|---|---|---|---|
| THU | 192.168.100.1 | 192.168.101.1 | 192.168.102.1 | 192.168.103.1 | 192.168.104.1 |
| GW | 192.168.100.2 | 192.168.101.2 | 192.168.102.2 | - | - |
| A | 192.168.100.3 | 192.168.101.3 | 192.168.102.3 | 192.168.103.3 | 192.168.104.3 |
| B | 192.168.100.4 | 192.168.101.4 | 192.168.102.4 | 192.168.103.4 | - |
| C | 192.168.100.5 | 192.168.101.5 | 192.168.102.5 | 192.168.103.5 | - |
| Tester | - | 192.168.101.6 | - | - | - |

**VLAN划分与配置**


动力域
MCU
Can IDS
TCP
MPU
IDPS
libSeLog
娱乐域
MCU
Can IDS
SPI
MPU
QNX
Android
libSeLog
libSeLog
IDPS
IDPS
MCU
Can IDS
SPI
TBOX
libSeLog
IDPS
ROUTE
车身域
MCU
Can IDS
TCP
MPU
IDPS
libSeLog
网关
MCU
Can IDS
TCP
MPU
IDPS
libSeLog
SOC平台
态势感知
应急响应
统计报表
策略管理
车型管理
安全态势
车辆管理
安全审计
系统管理
采集汇聚
②事件报告
Event report
②更新安全策略
Rules update
④更新安全策略
Rules update
漏洞库
①潜在威胁
Rules update
③潜在威胁
Potential threats
④应急处置
Emergency handling
②应急处置
Emergency handling
与OTA集成
④应急处置
Emergency handling
②应急处置
Emergency handling
①黑客攻击
Hacker attack


汽车网络安全态势感知
2020-07-15 17:18:03
安全事件类型
SYSTEM_SECURITY_EVENT
UDP端口扫描
TCP ACK Flood
EVENTCODE_SIGN_IN
通信测试
TCP ACK 端口扫描
带选项的IP包（严格选路）
带选项的IP包（记录路径）
TCP 源端口为0
Data ack and push flood
EVENTCODE_CONFIG
攻击事件(次)
概览
29
车辆总数
1
今日增加
49895
累计事件
0
今日事件
零部件
IVI
TBOX
被攻击区域TOP5
四川省
广东省
北京市
陕西省
攻击滚动实时展示列表
序号 VIN 设备编号 攻击IP 攻击类型 车辆位置 时间 攻击源位置
13 123456789 IVI EVENTCODE_SIGN_IN 四川省 成都市 2020-07-14 11:02:59
14 123456789 IVI EVENTCODE_SIGN_IN 四川省 成都市 2020-07-14 10:46:24
15 123456789 IVI EVENTCODE_SIGN_IN 四川省 成都市 2020-07-14 10:45:05
16 123456789 IVI EVENTCODE_SIGN_IN 四川省 成都市 2020-07-14 10:44:37
17 123456789 IVI 172.16.10.78 SYSTEM_SECURITY_EVENT 四川省 成都市 2020-07-13 16:48:53 四川省 成都市
18 123456789 IVI 172.16.10.78 SYSTEM_SECURITY_EVENT 四川省 成都市 2020-07-13 16:48:37 四川省 成都市


2020-06-10 12:45:12
车辆总数：8901
今日注册车辆：180
车联网实时网络安全事件监控
Internet of Vehicles real-time network security event monitoring
今日活跃车辆：2530
事件累计：134,230
今日攻击事件 49
事件信息详情
车型：
车辆：
时间：
被攻击
设备：
IP地址：
端口：
攻击
IP地址：
端口：
地址：
攻击类型：
威胁等级：
车辆位置：
事件原始内容：
当前攻击步骤
1·网关
2·车载电脑
3·车身动力地盘
4·网关
5·Tbox
序号 车辆标识 设备类型 攻击IP 攻击类型 车辆所在地 时间
1 SD234J3J423455 IVI 202.23.341.123 TEST 北京 2020-06-12 17:45:45
2 SD234J3J423234 IVI 202.21.121.12 IcmpDos 山东 2020-06-12 16:21:19
3 SD234J3J423412 IVI 202.23.123.10 TEST 重庆 2020-06-12 16:09:40
4 SD234J3J423457 IVI 201.45.102 modify-cert 江苏 2020-06-12 14:23:07
5 SD234J3J1113455 IVI 202.23.341.168 http-alert 重庆 2020-06-12 09:05:38

# 4 网络安全与功能安全的融合问题

## 高可信(high dependability)

- Reliability *R(t)* = probability of system working correctly provided that is was working at *t*=0 可靠
- Maintainability *M(d)* = probability of system working correctly *d* time units after error occurred. 可维护
- Availability: probability of system working at time *t* 可用
- Safety: no harm to be caused 安全可靠
- Security: confidential and authentic communication 安全保密

Dependable computing/可信计算

## Trusted Computing （TCG）

- *An entity can be trusted if it always behaves in the expected manner for the intended purpose.*
  一个实体在实现给定目标时，若其行为总是如同预期，则该实体是可信的
- 着重终端可信：密钥和数据的安全存放和使用、终端运行环境的完整性度量
- 不能保证终端内容和行为的可信
- 可信内涵：从主体（用户）视角出发，强调行为与设定目标的符合性





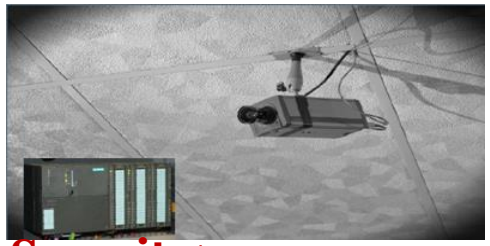


Trusted computing/信赖计算

## 两个概念之间的区别

- 功能安全考虑的是非故意行为引发的风险；网络安全考虑的是恶意行为引发的风险
- 功能安全考虑的是保护外部环境不受设备的伤害，需要进行危害分析；网络安全考虑的是设备不受外部环境的伤害，需要进行威胁分析

**Safety**:
保护外部环境不受设备的伤害



**Security**:
保护设备不受外部环境的伤害

## 两个概念之间的联系

- 功能安全和网络安全都达不到100%，强调的是没有不可接受的风险
- 网络安全主要是为功能安全提供保障。没有网络安全，也就谈不上功能安全
- 网络安全的软硬件，也需要符合功能安全的要求

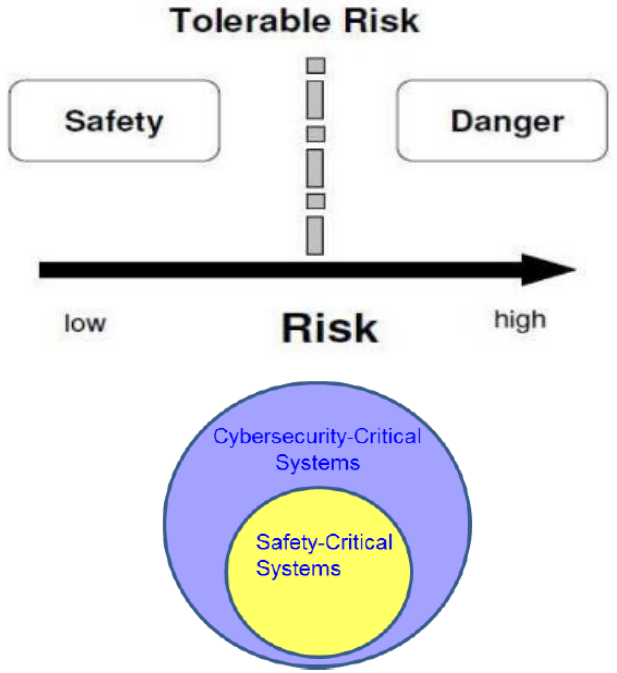



*Figure 1 - Relationship between safety-critical and Cybersecurity-critical systems*

## 开展功能安全和网络安全融合工作的基础

- 功能安全和网络安全都已成为汽车的重要属性，且相互之间具有紧密联系
- SAE J3061、ISO21434沿用了与ISO26262大致类似的工程过程，拥有部分相同的活动
- SAE J3061提供了网络安全活动与功能安全活动之间的通信路径

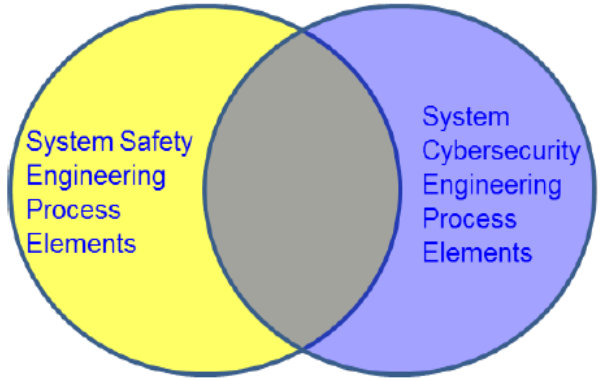



*Figure 2 - Relationship between system safety and system Cybersecurity engineering elements*

根据SAE J3061，有两种方式来协同具有密切联系的功能安全与网络安全工程过程：

- 利用已有safety过程，开发security过程，并在safety和security两者中具有内在联系性的地方，维护两者之间的一致性
- 基于已有safety过程，融入security活动，形成集成的过程

## 概念阶段

- 作为概念阶段的第一个活动，把功能安全和网络安全的需求融合在一起，形成统一的item definition
- 设立四个同步点：TARA与HARA；concept；requirements；review
- 可制定独立的计划，但需要在计划中体现四个同步点，并进行统一的计划跟踪工作
- TARA与HARA的融合，确保safety goal与security goal具有一致性和整体性：
  - 对分析方法进行整合，尽量采用比较一致的方法
  - 把HARA中涉及到的数据、软硬件实体、通信等相关内容纳入**TARA的资产**
  - 把威胁带来的危害，同HARA的危害进行结合，并根据HARA对危害的分析结果，确定**威胁的影响等级**
  - 用HARA分析出来具有ASIL等级要求的危害，核实是否有潜在的**攻击路径**带来相应的危害
  - 结合HARA的ASIL等级，确定网络安全功能所对应**软硬件需要满足的ASIL等级**
  - 需要就网络安全措施对功能安全的**影响**进行评估；网络安全措施需要考虑功能安全带来的**约束特性**

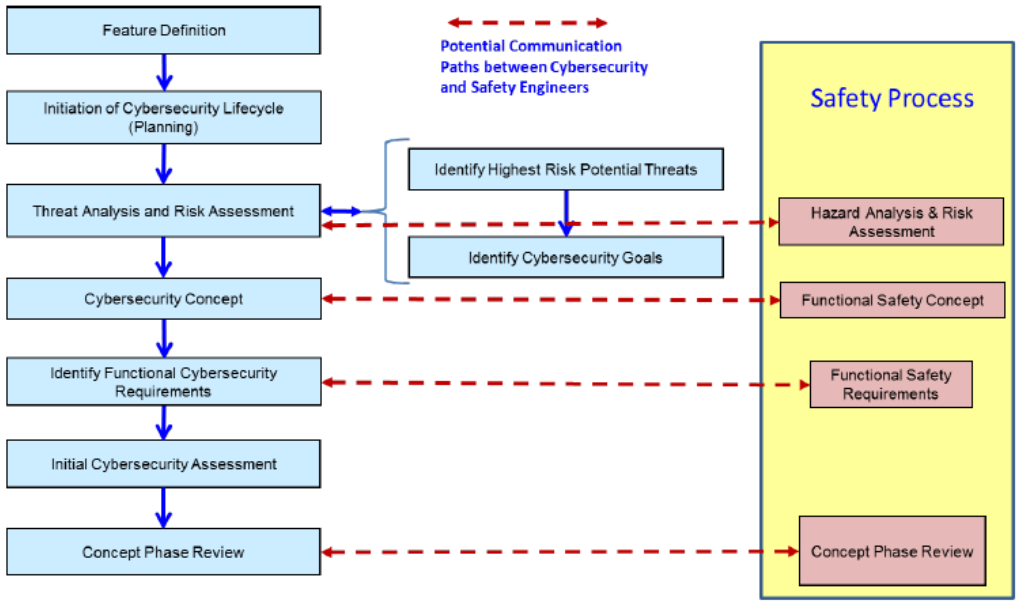
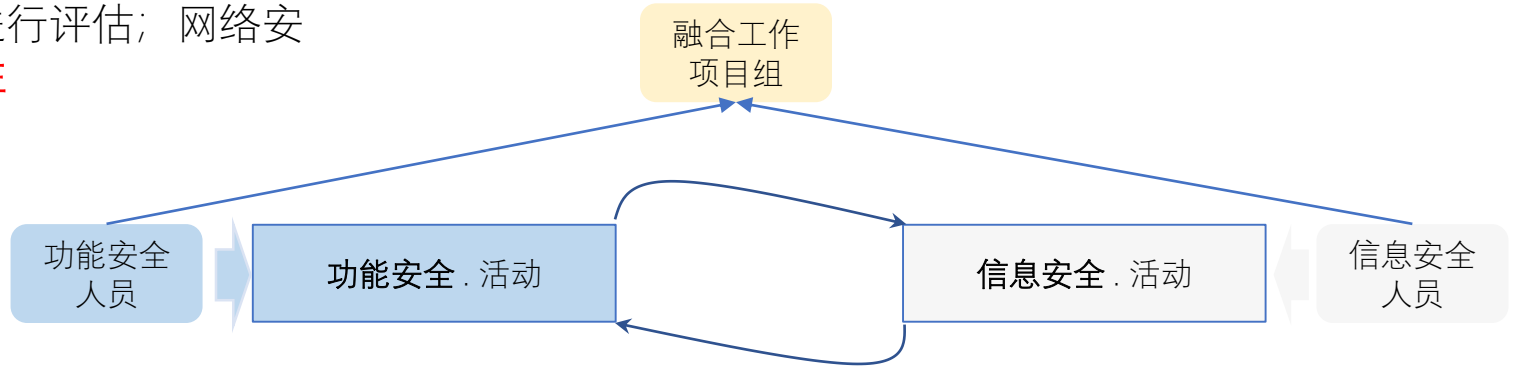
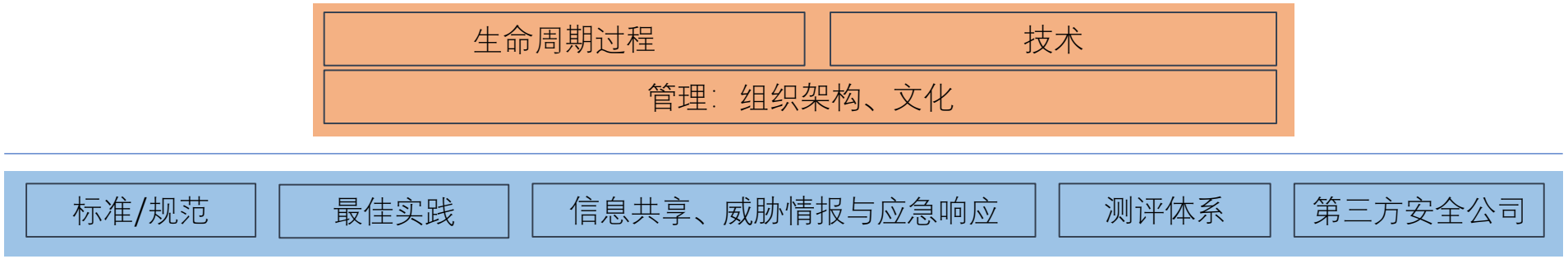



*Figure 14 - Concept phase activities with potential communications paths between Cybersecurity and safety activities*

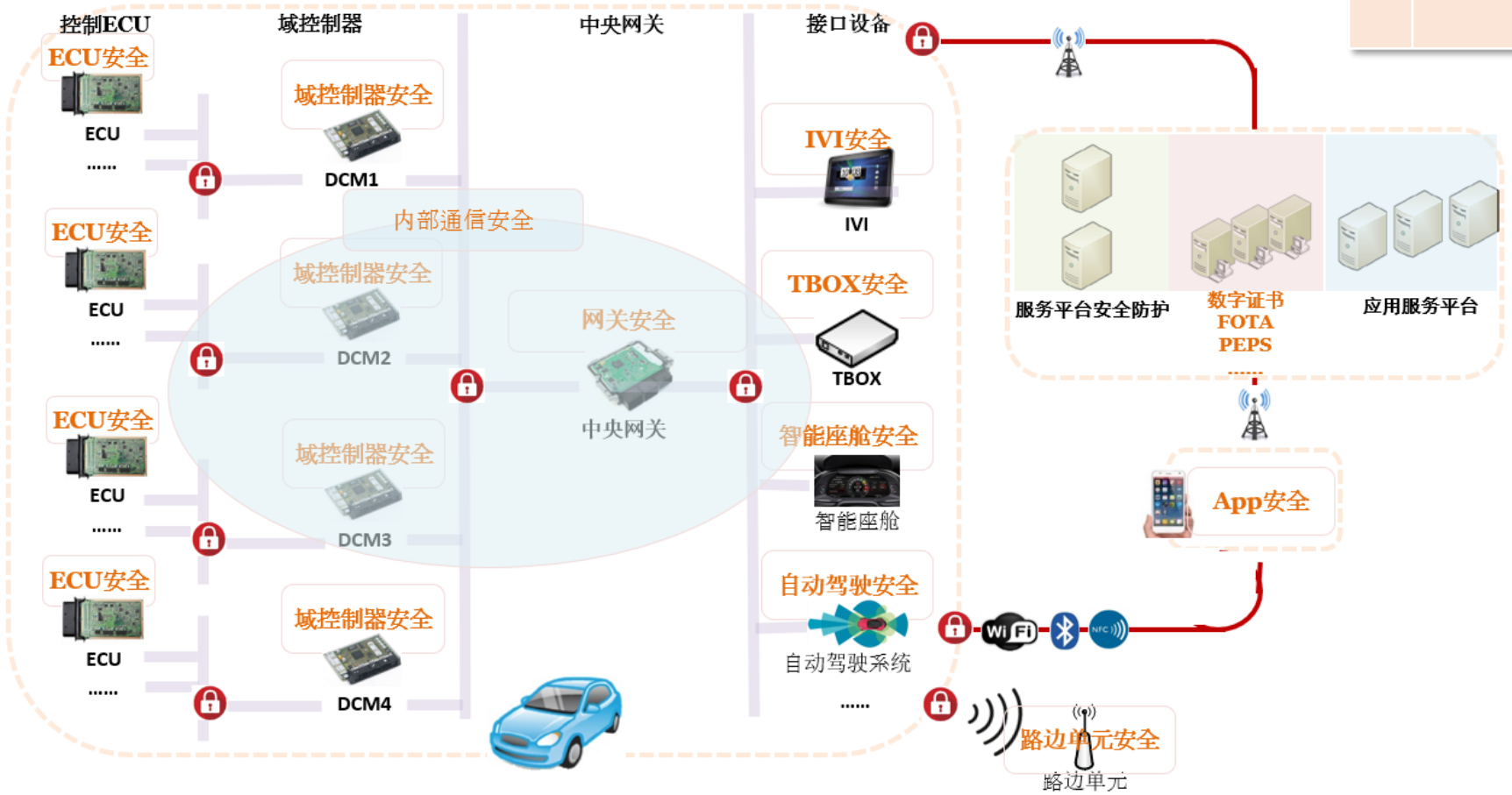


# 5 结束语

- 网络安全是一个系统问题：多层次纵深防御




# 我们提供的产品与服务




## 覆盖智能汽车全要素

| 01 | 零部件 | 02 | 车辆内部通信 | 03 | 关键业务 |
|---|---|---|---|---|---|
| | IVI、TBOX、智能座舱、中央网关、自动驾驶系统、域控制器、控制类型ECU、..... | | CAN、CAN FD、以太网 | | FOTA、蓝牙钥匙、V2X、国六B、..... |

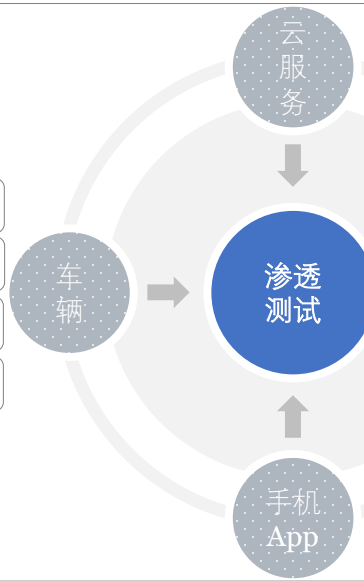
**智能汽车网络安全解决方案 deCORE AUTO**

# 我们提供的产品与服务

01 信息收集 | 02 威胁建模 | 03 风险评估 | 04 用例设计 | 05 模拟攻击 | 06 漏洞分析 | 07 测试报告

WEB应用（对注入、跨站、越权、CSRF、中间件、规避交易、信息泄露、业务等 数十个检测项进行安全检测）

服务器（中间件、组件漏洞、系统漏洞进程、数据库、集群化配置、基础配置、应用配置、安全配置基线等 数十个检测项进行安全检测）




IVI | TBOX
智能座舱 | 中央网关
域控制器 | 控制类型ECU
.....

FOTA | secOC
国六B | V2X
蓝牙钥匙 | .....

安卓应用（对客户端、组件、本地数据、敏感信息、业务等数十 个检测项目进行安全检测）

iOS应用（对客户端、策略、通信、敏感信息、业务等 数十个检测项目进行安全检测）


实车仿真展示区 | 测试工位区1 | 零部件区 / 工具设备区 / 台架 | 测试工位区2 | 会议/培训室

# 渗透测试与能力建设

知识赛


2019第一届网安知识赛
00:36:22:25

攻防赛

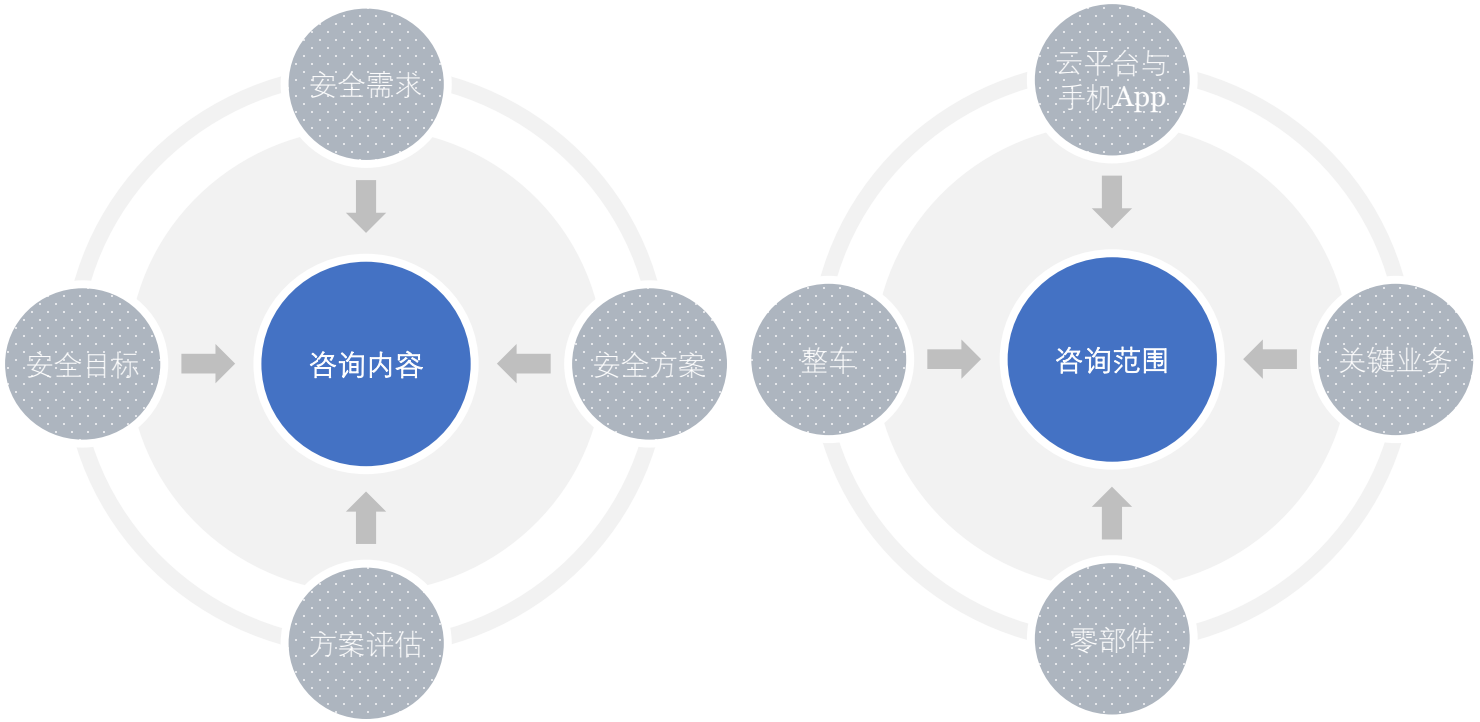

攻防演练大屏展示
12:45:00-12:50:00
32,456
00:46:38.00

夺旗赛


CTF
比赛倒计时: 00:30:56
确认解题
正在解题
题目描述

E/E架构 | 零部件的访问点信息 | 基于层次的纵深体系 | 零部件功能安全等级 | 业务场景

01构建业务的数据流图 | 02风险评估 | 03制定网络安全目标 | 04制定网络安全需求 | 05 评审供应商安全方案




# 安全咨询

为辰信安

# 汽车产业的可信合作伙伴!