智能汽车网络安全防护与实践

演讲人：李允　　单位名称：为辰信安

高可信(high dependability)

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

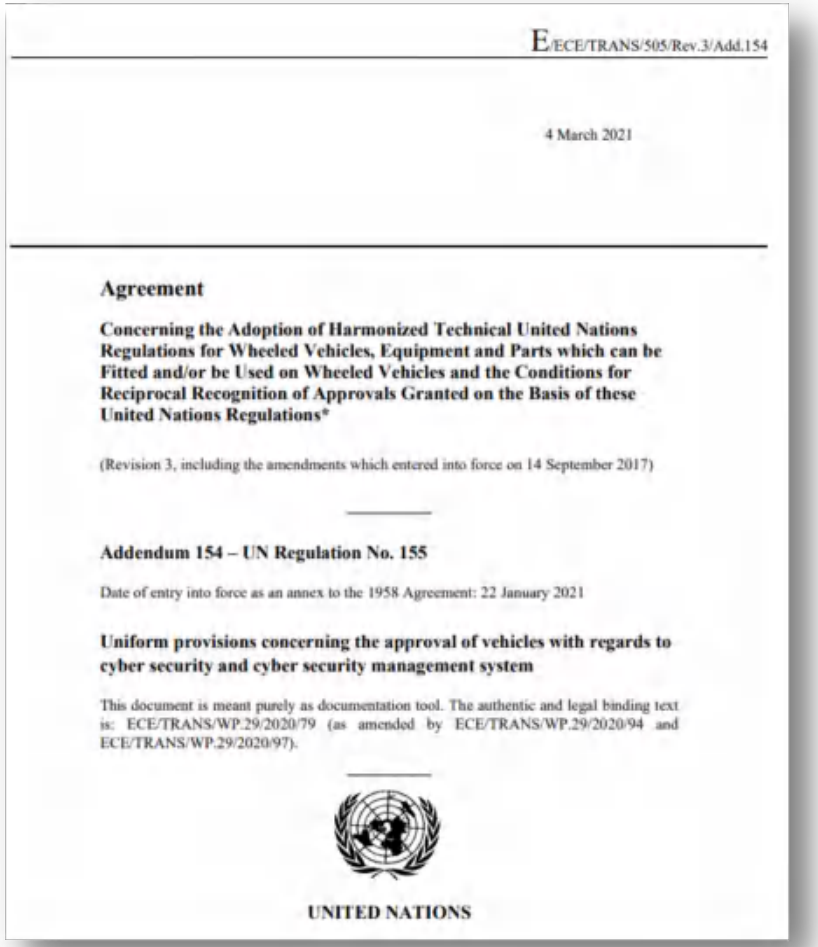
- 网络安全失效可能导致智能汽车**功能安全**方面的危害
- 智能汽车面临前所未有的网络安全**监管要求**

2015年7月，菲亚特-克莱斯勒在美国召回140万辆汽车。两名研究人员利用笔记本电脑远程控制，甚至还把车“开进沟里”

Promon专家利用手机App漏洞成功控制特斯拉汽车

速度与激情里的“僵尸汽车”不再是电影桥段

没有网络安全，就不会有汽车的智能化



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

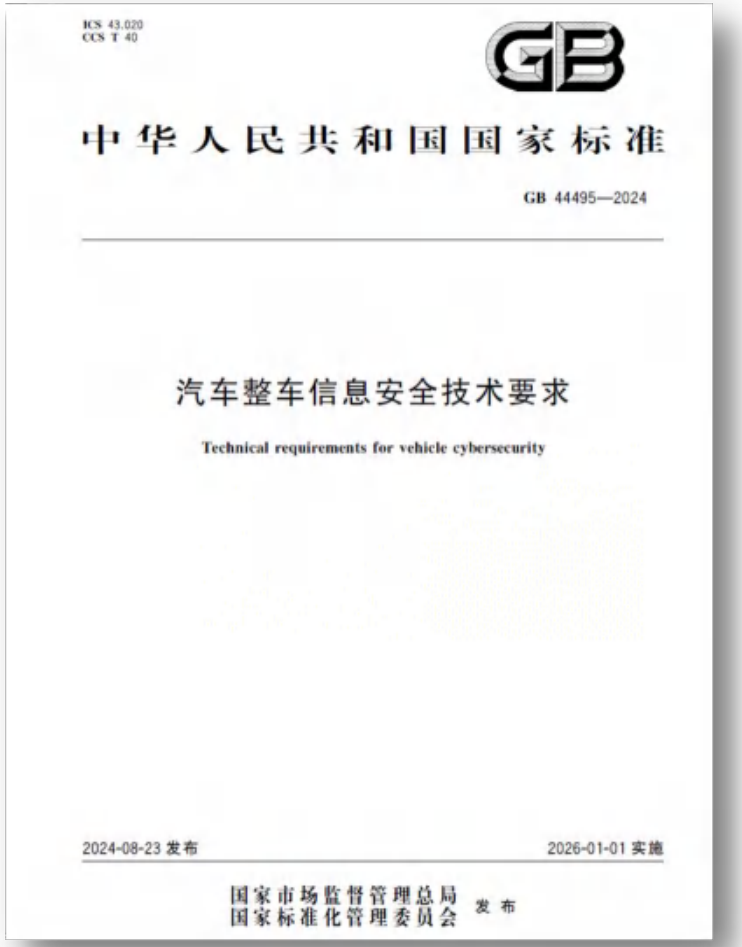
Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS



ICS 43.020
CCS T 40

GB

中华人民共和国国家标准

GB 44495—2024

汽车整车信息安全技术要求

Technical requirements for vehicle cybersecurity

2024-08-23 发布　　2026-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

为辰信安：以可信为根本的产品方案deCORE AUTO

❶ 密码应用deCORE Crypto
密码模块
生产密钥管理系统
数字签名服务系统

❷ 入侵检测与安全运营 deCORE IDPS
IDPS入侵检测与防御系统
VSOC安全运营中心

❸ 新一代EE架构安全
SOA架构安全
SecOC
安全通信测试工具

❹ 数据安全deCORE DS
数据安全咨询
数据分类分级
数据安全监测系统
数据安全共享平台
数据安全防护组件
数据安全测试工具

❺ 云控安全deCORE CCloud
云控网络安全解决方案
云控数据安全解决方案

为辰信安

❻ 数字钥匙deCORE LINK
数字钥匙系统
BLE/UWB定位算法
UWB雷达算法
BLE/UWB模组

❼ 安全测试工具deCORE TSTR
汽车安全合规测试系统
汽车渗透测试工具

❽ 汽车网络靶场deCORE CR
汽车网络靶场
网络安全实训平台（汽车）

❾ 安全咨询
网络/数据安全流程体系建设
网络/数据安全风险评估
网络/数据安全方案设计

❿ 安全测试
渗透测试
符合性测试
软件测试

以可信为目标，把嵌入式操作系统、网络安全作为核心能力

零部件测试工具　　整车测试工具　　自动驾驶测试工具　　V2X测试工具　　OTA测试工具

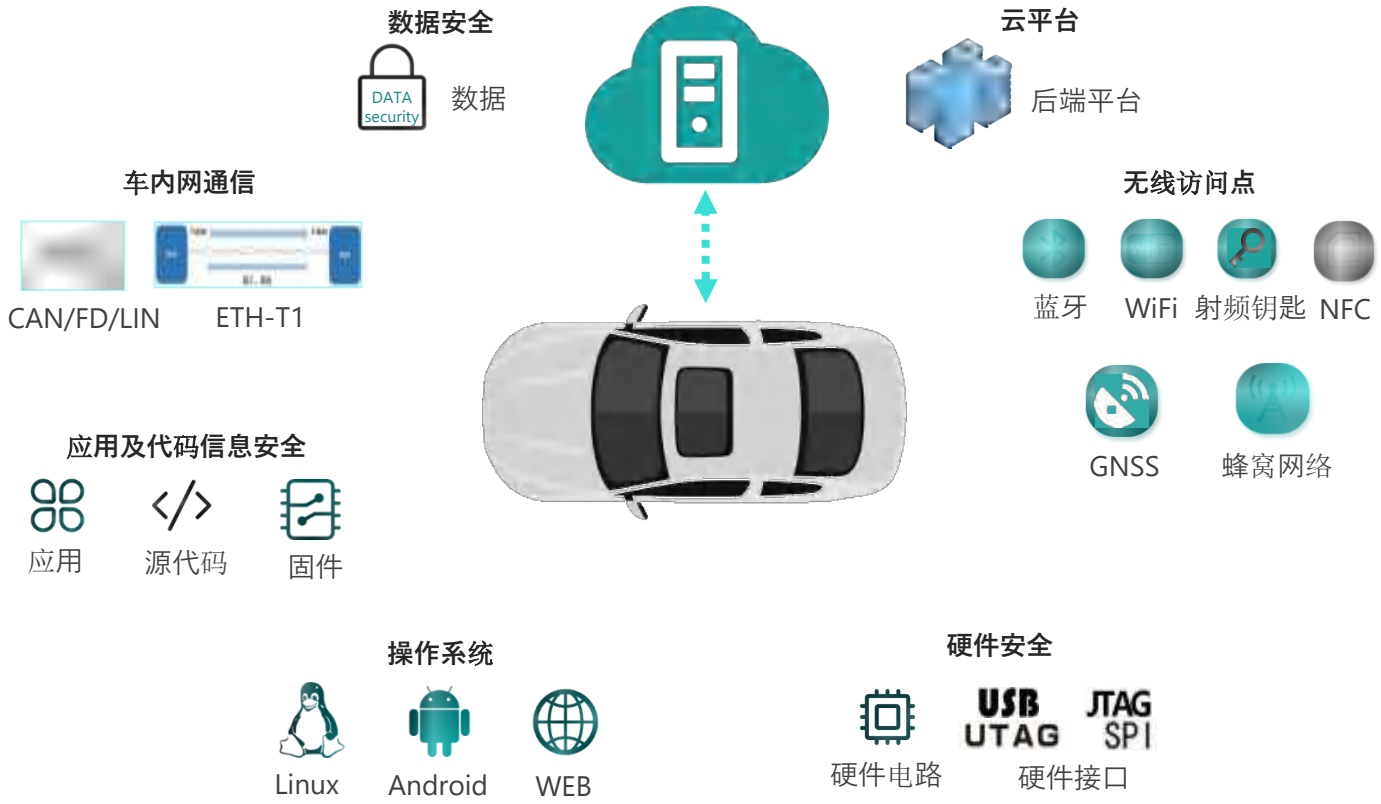
01 汽车面临日益严峻的网络安全风险

02 网络安全是一个系统问题

03 与架构有关的安全思想：隔离与纵深防御

04 如何因应V模型的长尾效应问题

汽车面临日益严峻的网络安全风险



车联网云平台

恶意指令下发、注入攻击、权限提升

功能业务安全

自动驾驶AI算法对抗、数字钥匙破解、恶意远程控制、恶意升级、车路云协同欺骗

应用安全

堆栈溢出、应用功能篡改、业务逻辑缺陷

数据安全

数据泄露、数据破坏、数据篡改

访问点安全

数据监听、信息篡改、协议逆向、业务信号重放

中继攻击、拒绝服务

系统安全

内核漏洞、固件破解、系统组件漏洞、默认口令及弱口令、崩溃攻击

硬件安全

侧信道攻击、密钥读取、故障注入

调试接口恶意调用

车联网高危漏洞预警 | 为辰安全实验室监测到车联网开源组件命令执行漏洞(CVE-2022-30065)

为辰信安 2023-02-16 09:00 发表于北京

CVE-2022-30065 Detail

Description

A use-after-free in Busybox 1.35-x's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

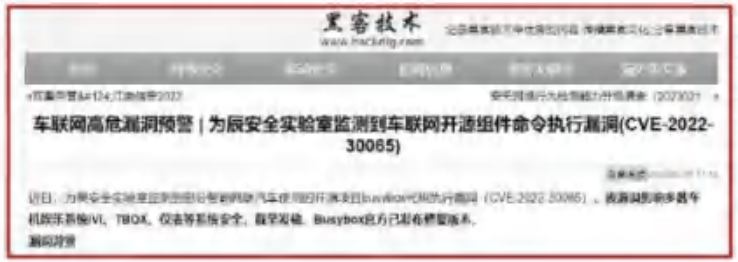
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

- 可导致程序崩溃、权限提升，从而**使车辆的业务功能失效**，严重可导致车辆停止工作或者丧失控制权，系统崩溃时被执行其他攻击的风险激增。
- 可配合其它远程漏洞，通过非法控车，获取例如像**车辆定位数据、车主身份信息、车辆操作历史等一系列敏感信息。**黑客可利用这些信息来实施身份盗窃、勒索、追踪等恶意行为。
- 配合信息泄露漏洞如用于维持权限，则意味着黑客可以在系统中长期潜伏并继续进行攻击活动，而不被发现或清除。**黑客可以利用这个漏洞来获取管理员权限并修改系统配置，或者在受感染的车辆上执行恶意代码。**这可能会对车辆和驾驶员的安全造成严重威胁。

此前，由**为辰安全实验室**监测到的车联网高危漏洞开源组件命令执行漏洞(CVE-2022-30065)，**被国外头部智能汽车信息安全研究机构Upstream列入《H1'2023 Automotive Cyber Trend Report》报告。**

In February 2023, a thorough technical analysis and POC of CVE-2022-30065 affecting the open-source project BusyBox—which provides tools that interface with the Linux kernel—was published on a popular Chinese security blog.[15] An exploit of this vulnerability might result in program crashes and privilege escalation, invalidating the system's functions. When the system crashes, the risk of other attacks also increases. Combined with other vulnerabilities, it can provide access to sensitive information including vehicle location data, owner identity information, and the history of vehicle operation. Black hat threat actors can use this information to carry out malicious acts, such as identity theft and tracking.[16,17]


黑客技术 www.hacking.com

车联网高危漏洞预警 | 为辰安全实验室监测到车联网开源组件命令执行漏洞(CVE-2022-30065)

Early warning of high risk vulnerability affecting connected vehicles - code execution vulnerability of BusyBox component found in numerous in-vehicle infotainment systems (CVE-2022-30065)

H1'2023 Automotive Cyber Trend Report原文

高危漏洞预警|为辰安全实验室监测到BlackBerry系统命令执行漏洞(QNX-2024-001/CVE-2024-35213)

[illegible] Jeewintek 为辰信安 2024年06月13日 17:10 [illegible]

BlackBerry Home myAccount

Details

QNX-2024-001 Vulnerability in SGI Image Codec Impacts BlackBerry QNX Software Development Platform (SDP)

June 12, 2024 • Security Advisory

ARTICLE NUMBER

000139914

OVERVIEW

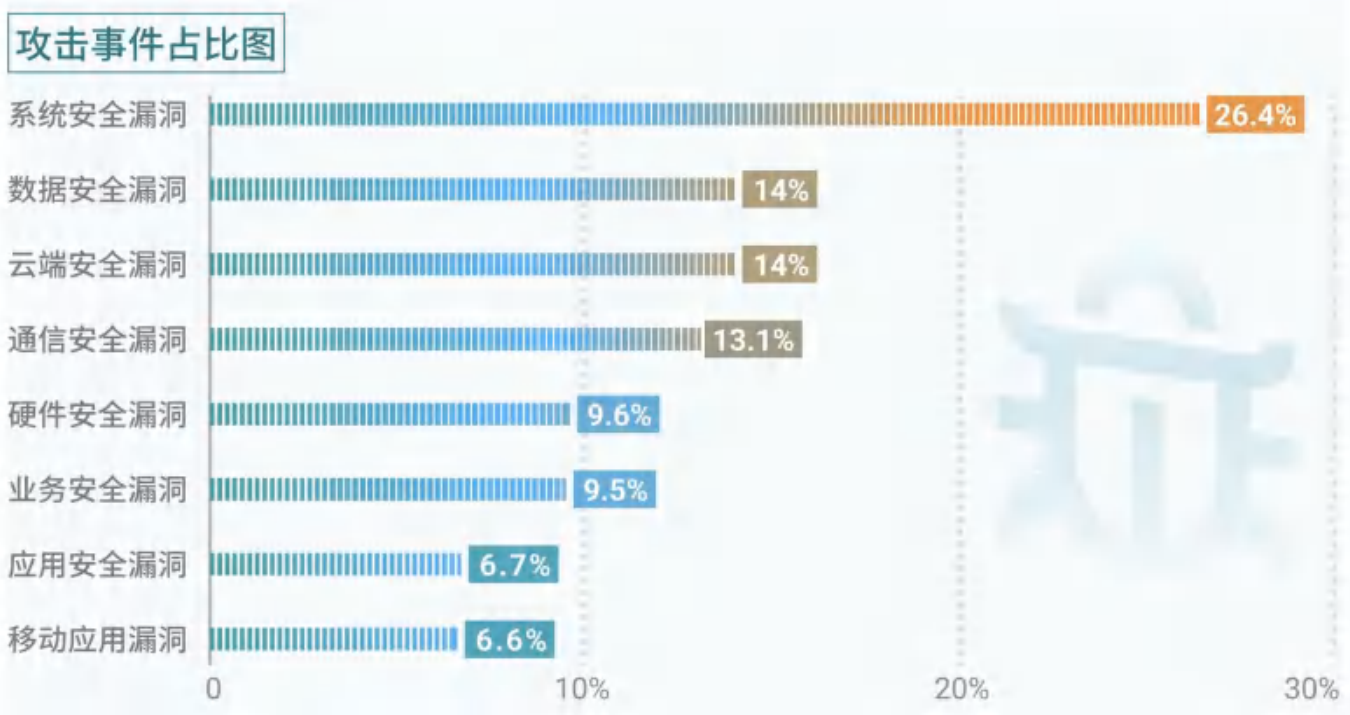
This advisory addresses an improper input validation vulnerability in the SGI Image Codec of affected versions of the QNX Software Development Platform that could potentially allow a successful attacker to cause a denial-of-service condition or execute code in the context of the image processing process. BlackBerry is not aware o any exploitation of this vulnerability.

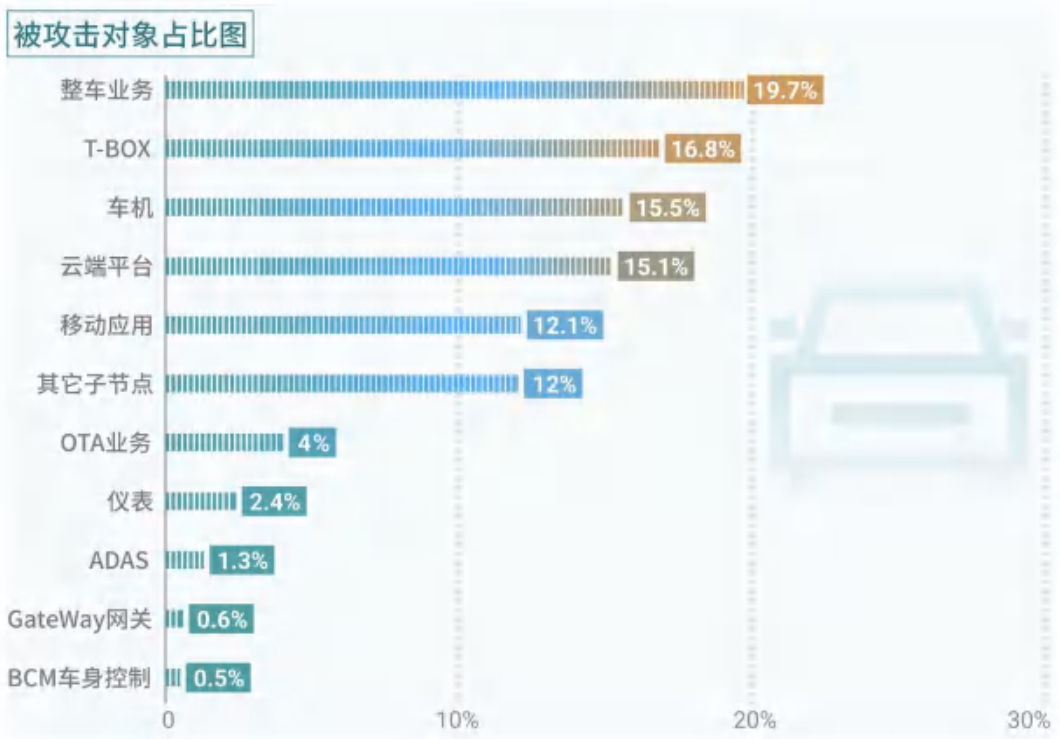
BlackBerry investigates all reports of security vulnerabilities affecting supported products and services. A security advisory is issued once the investigation is complet and the software update is released. Installing the recommended update(s) in this advisory will help maintain the security of your BlackBerry QNX product(s).

该漏洞为具有严重危害漏洞，官方CVSS评分9.0，受影响范围广泛，对受影响的车载终端及智能设备可能造成重大安全风险——

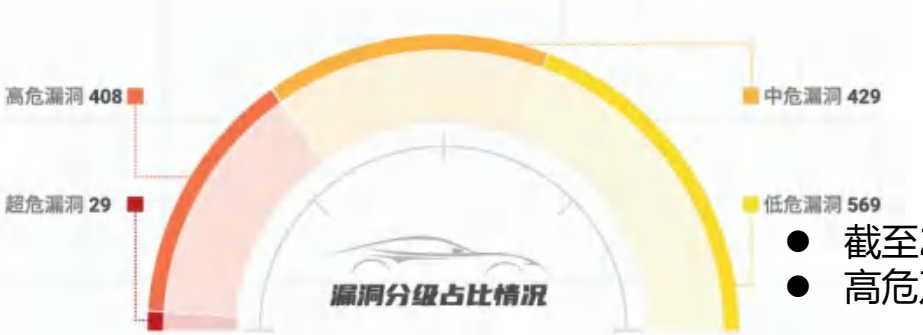
- **可导致程序崩溃、权限提升**，致使车辆的业务功能失效，严重可导致车辆停止工作或者丧失控制权，系统崩溃时被执行其他攻击的风险激增。
- **可配合其它漏洞进行非法控车，获取**例如像**车辆定位数据、车主身份信息、车辆操作历史**等一系列敏感信息。黑客可利用这些信息来实施**身份信息窃取、勒索、追踪**等恶意行为。
- **配合其他木马，可用于维持权限**，这意味着黑客可以长期潜伏在系统中并持续进行攻击活动，却不被发现或清除。黑客可以利用这个漏洞获取管理员权限并修改系统配置，或在受感染的车辆上执行恶意代码，从而对车辆和驾驶员的安全造成严重威胁。

在为辰安全实验室研究过的1000+车型与零部件中，监测到的攻击事件及被攻击对象态势



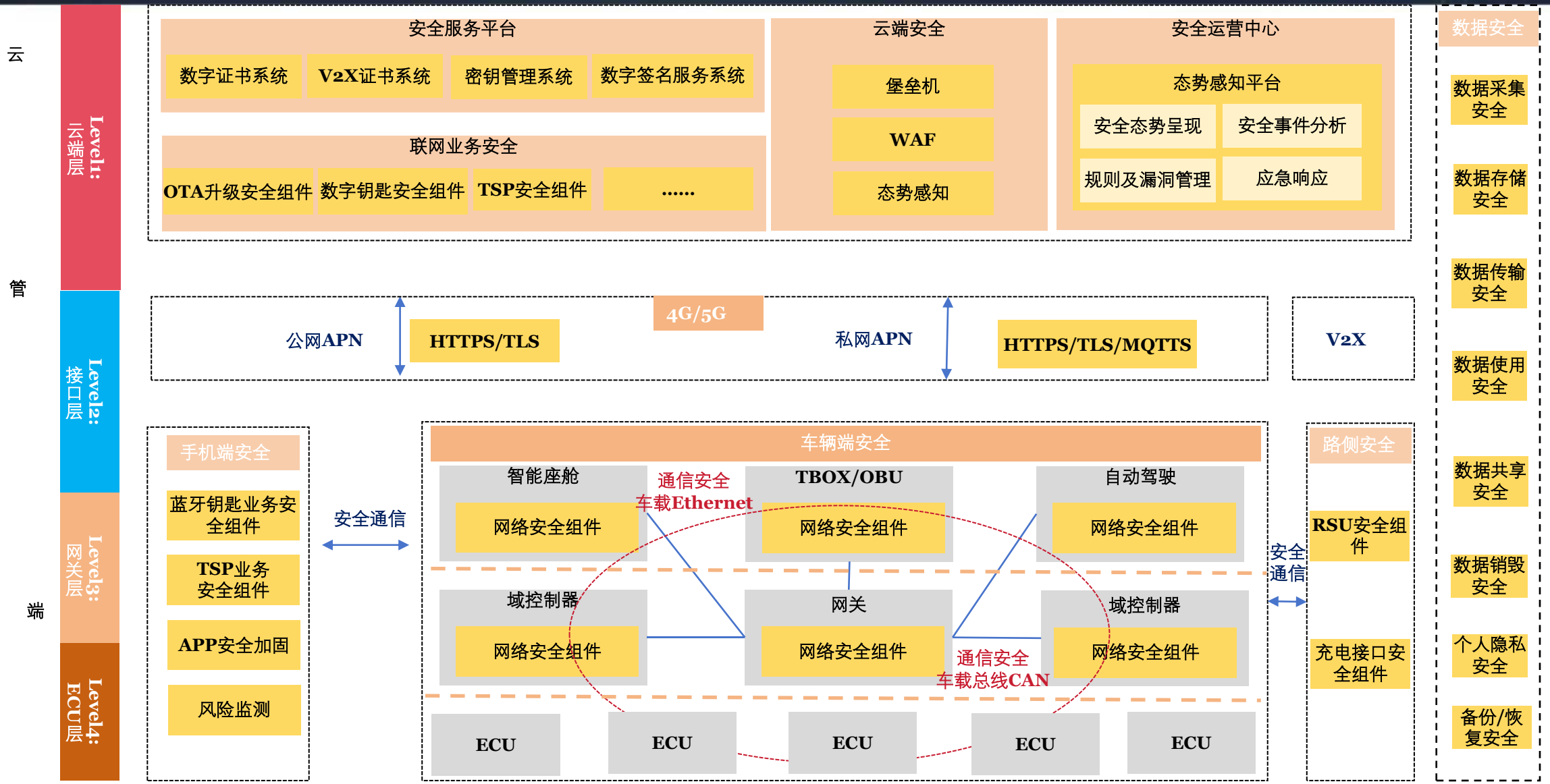


来源： 为辰安全实验室



- 截至2023年，为辰安全实验室共计监测漏洞1435个
- 高危及超危漏洞437个

网络安全是一个系统问题



技术：基于网联体系的网络安全

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”。

- **ISMS**：信息安全，**Information security Management System**
- **CSMS**：网络安全，**Cybersecurity Management System**

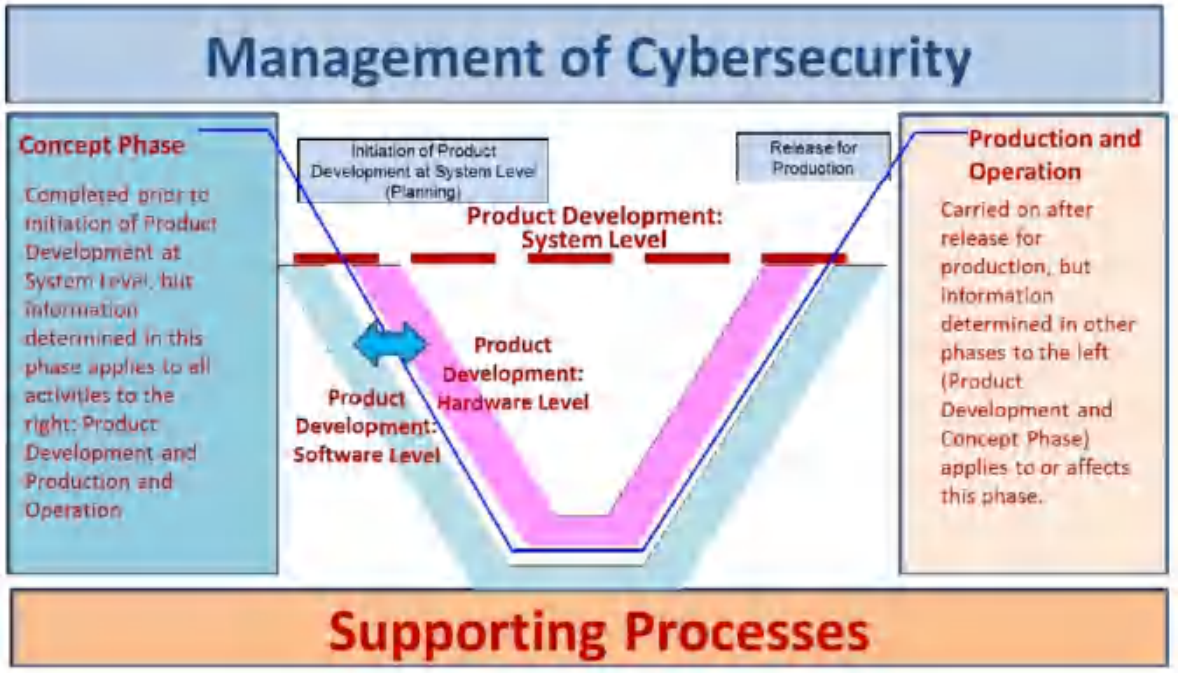
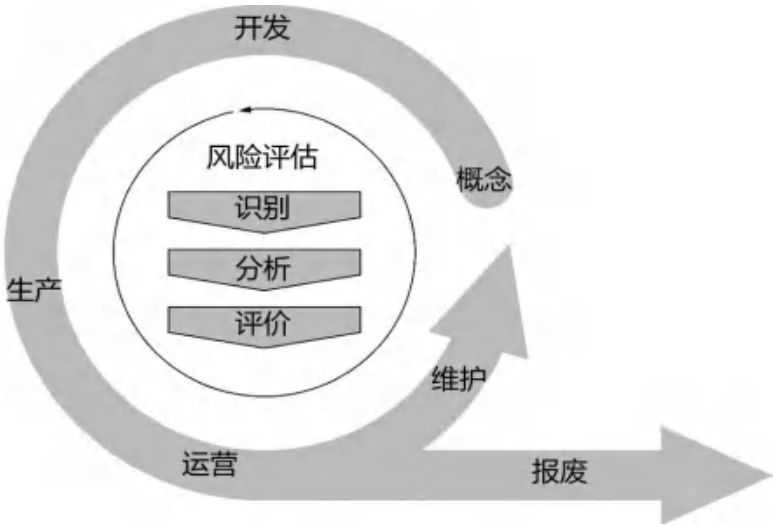


Figure 3 - Overall Cybersecurity process framework

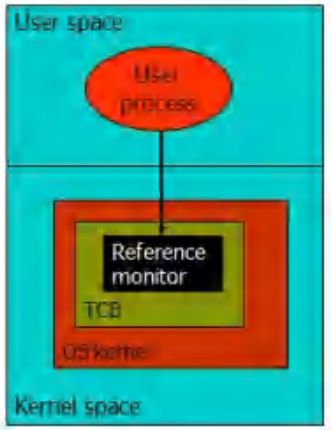
管理：信息安全与网络安全



作为智能网联汽车网络安全管理的一部分，TARA贯穿其概念、开发、生产、运营、维护和报废的整个生命周期

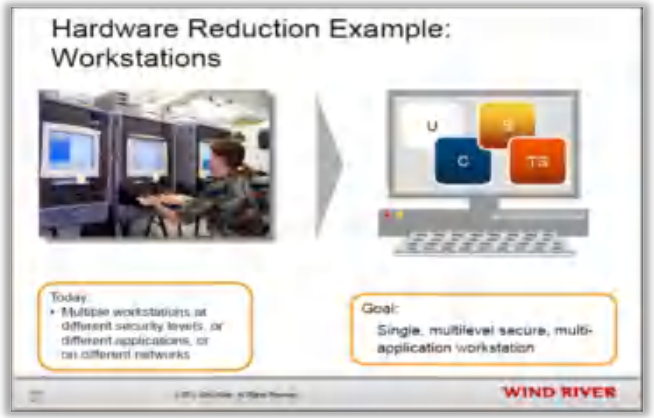
车辆端生命周期：基于车辆生命周期的网络安全活动

与架构有关的安全思想：隔离与纵深防御



之前系统的问题1

- 基于单体安全内核，需要为整个系统提供安全支持
- 除安全内核外，TCB包括有助于系统安全的所有安全功能
- 很多应用特定的功能也放到TCB中，导致TCB增长到最后，消耗了整个系统
- 整个系统的评估变得非常困难



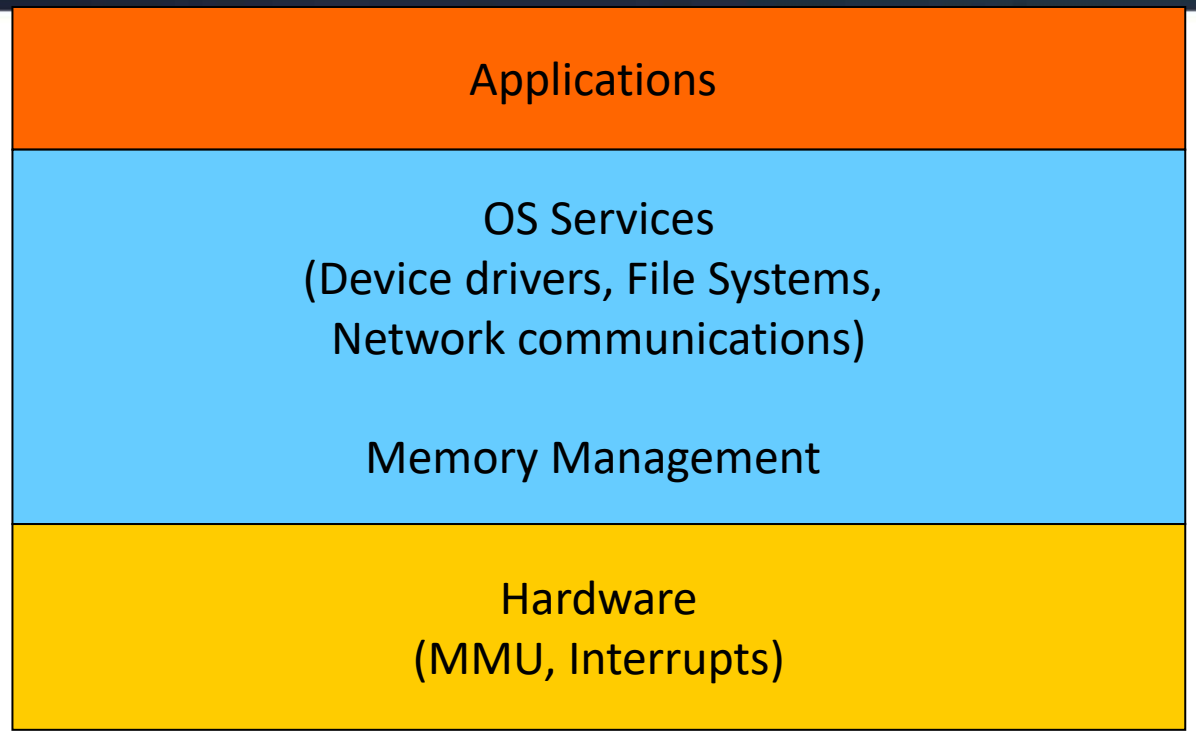
之前系统的问题2

物理隔离

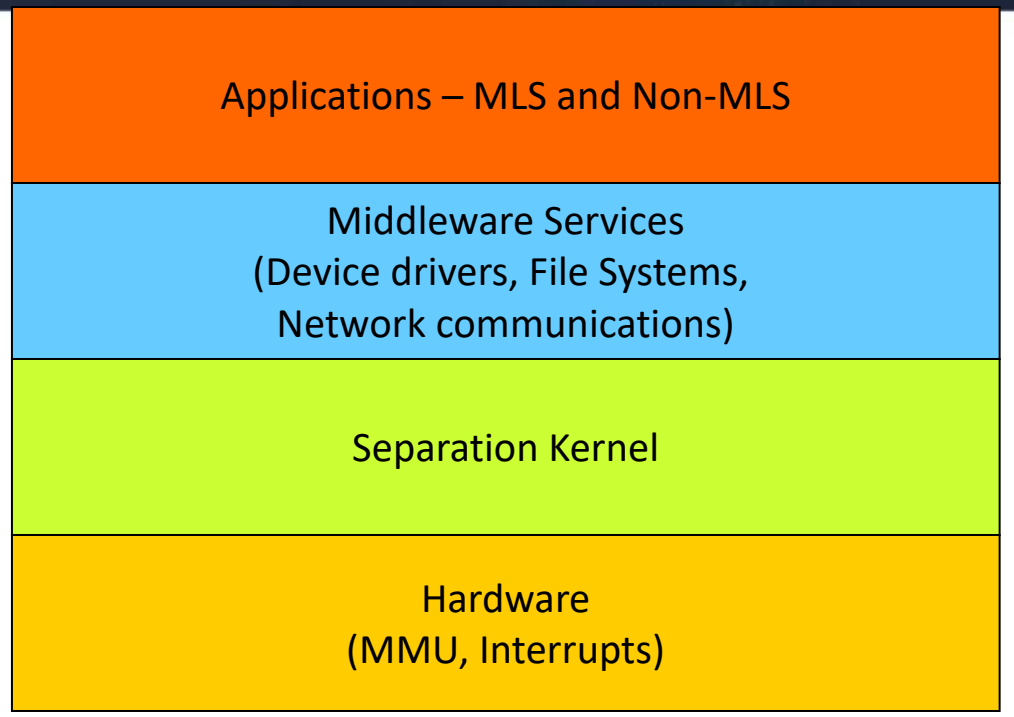
- Modern warfare is about sharing information现代战争需要信息共享
- Information must be shared securely to not compromise the mission安全共享信息，还不影响任务

MILS（Multiple Independent Levels of Security/Safety）

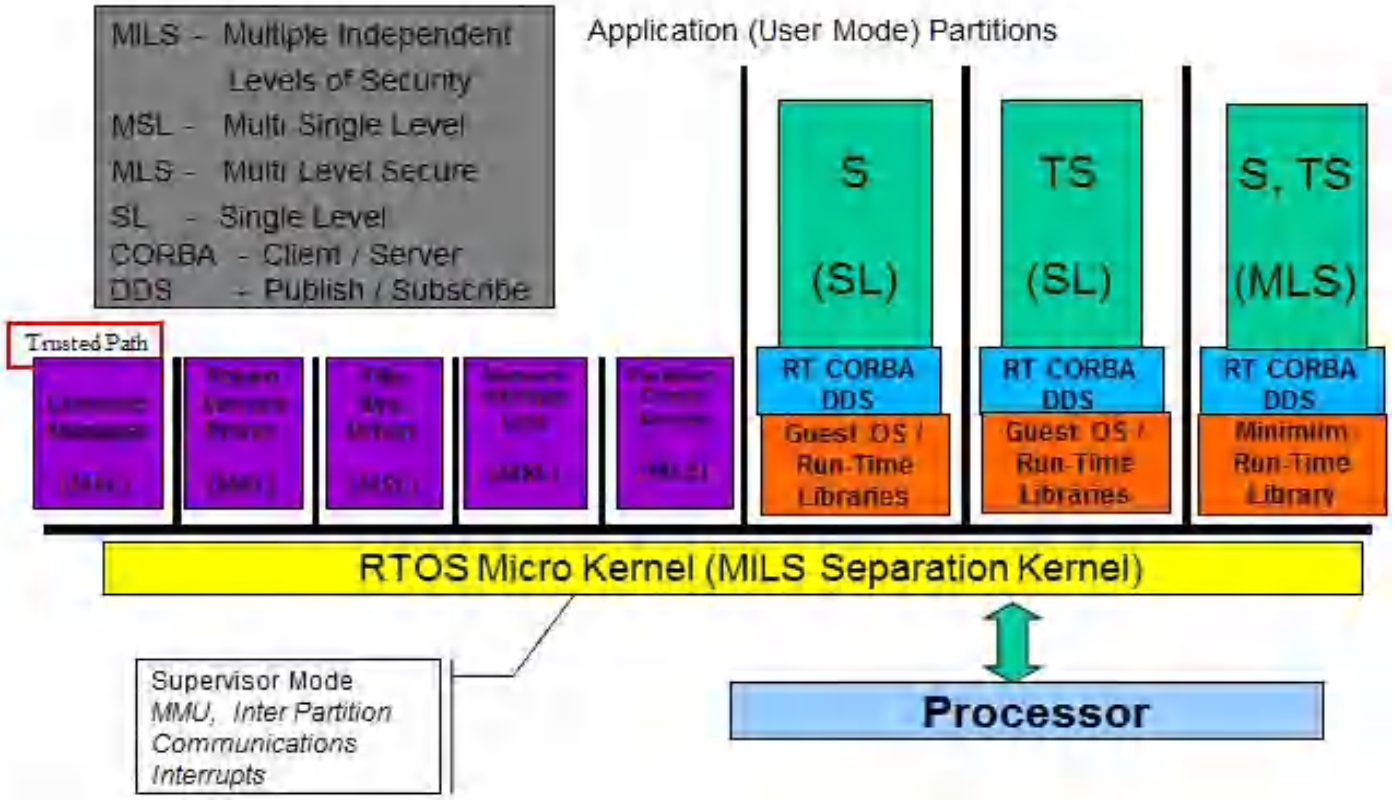
- the concept of separation, as introduced by John Rushby隔离的概念，由John Rushby提出
- Each level is responsible for its own security domain and nothing else每个层次只负责自己的安全
- Makes evaluation possible评估变得可能
- Fits in with small is beautiful thinking小而美

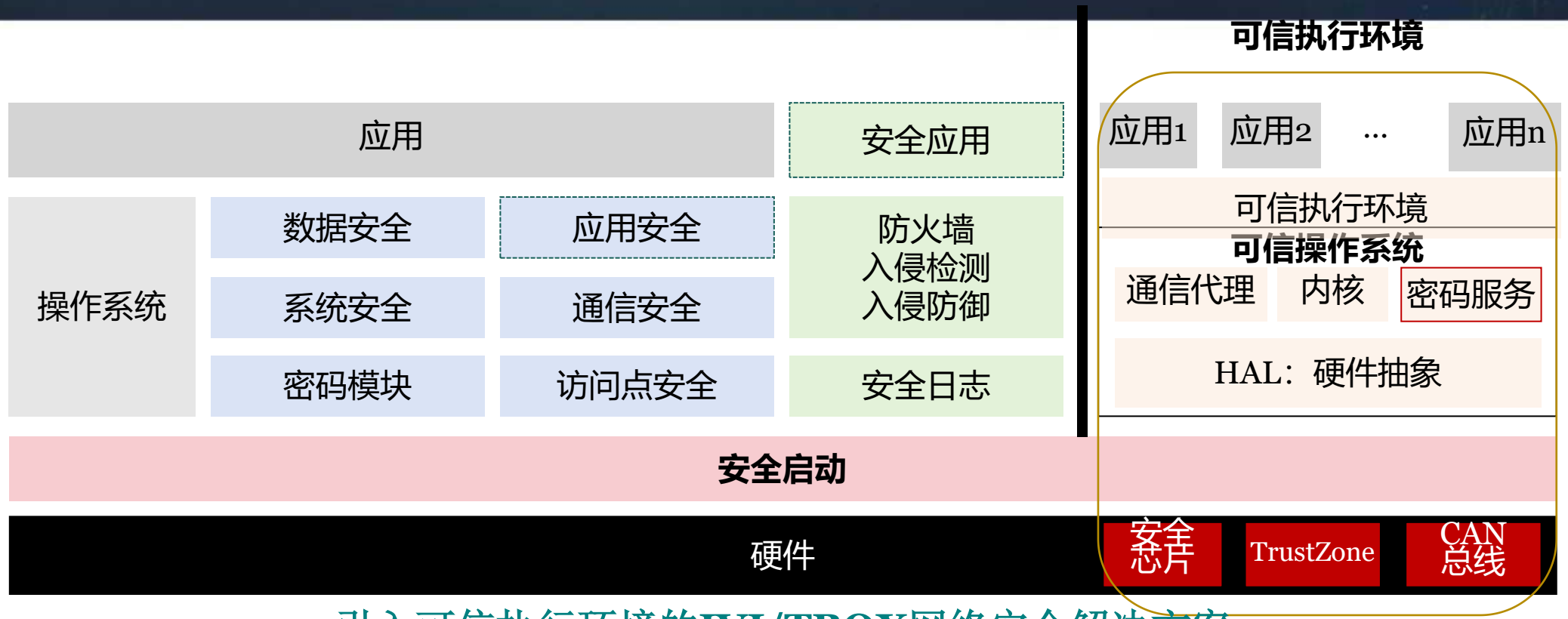


Normal architecture



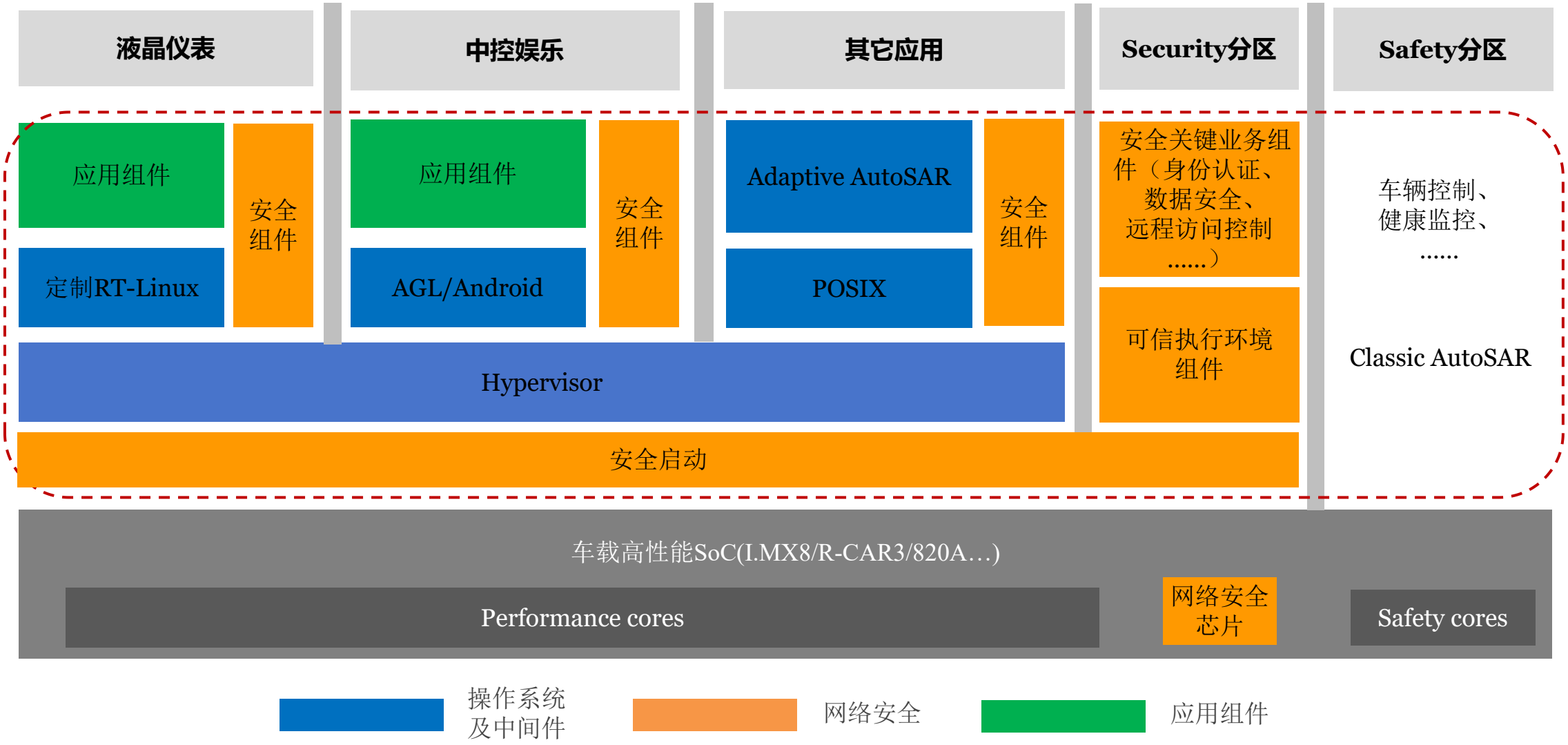
MILS architecture


MILS - Multiple Independent Levels of Security
MSL - Multi Single Level
MLS - Multi Level Secure
SL - Single Level
CORBA - Client / Server
DDS - Publish / Subscribe
Application (User Mode) Partitions
S (SL)
TS (SL)
S, TS (MLS)
Trusted Path
RT CORBA DDS
RT CORBA DDS
RT CORBA DDS
Guest OS / Run-Time Libraries
Guest OS / Run-Time Libraries
Minimum Run-Time Library
RTOS Micro Kernel (MILS Separation Kernel)
Supervisor Mode
MMU, Inter Partition Communications
Interrupts
Processor

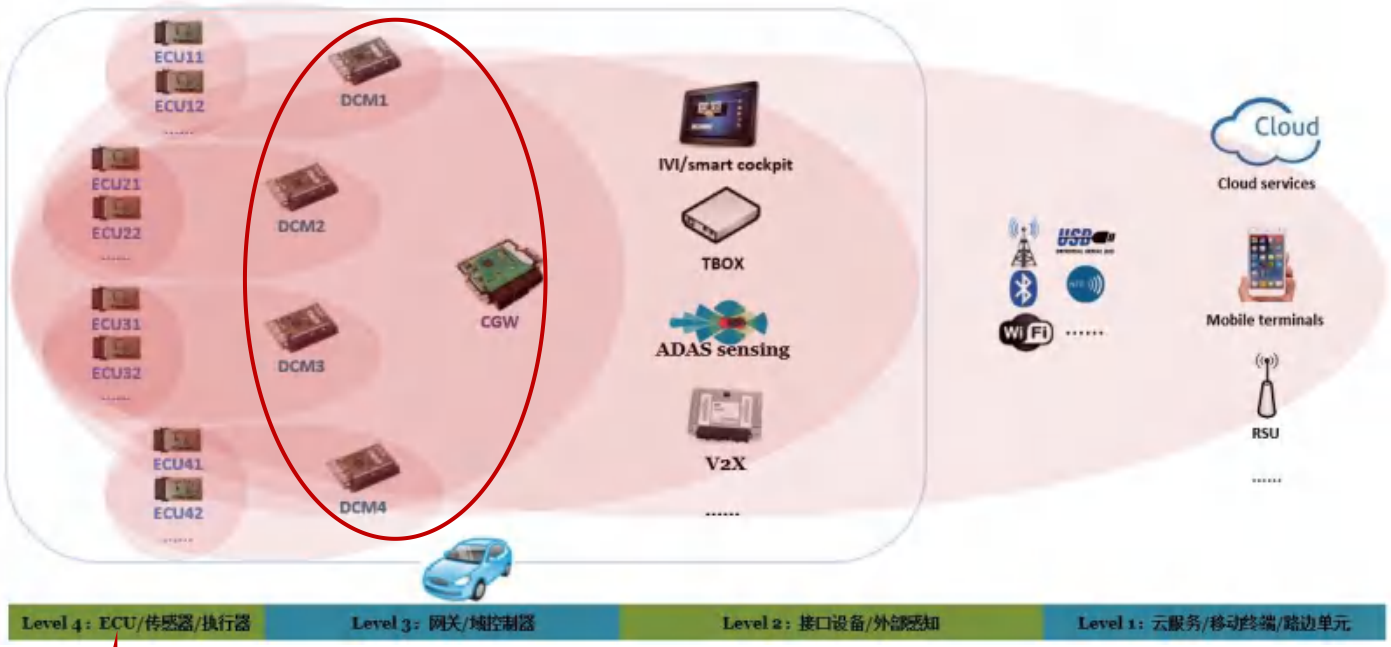


引入可信执行环境的IVI/TBOX网络安全解决方案

- 把高等级安全方面的应用（身份认证、远程控制等）纳入可信执行环境进行管理和运行，抵御Linux/Andorid潜在漏洞可能对安全应用带来的安全风险，提升系统的安全防御能力
- **分域隔离**：对访问CAN总线等方面的关键IO设备，通过可信执行环境进行管理和控制，实现车内网络与车外网络的隔离，提升系统的安全防御能力
- **动态度量**：对关键代码和关键数据，进行运行时度量，防止非法篡改



具有多域融合特性的下一代零部件网络安全解决方案：智能座舱、中央网关、自动驾驶



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

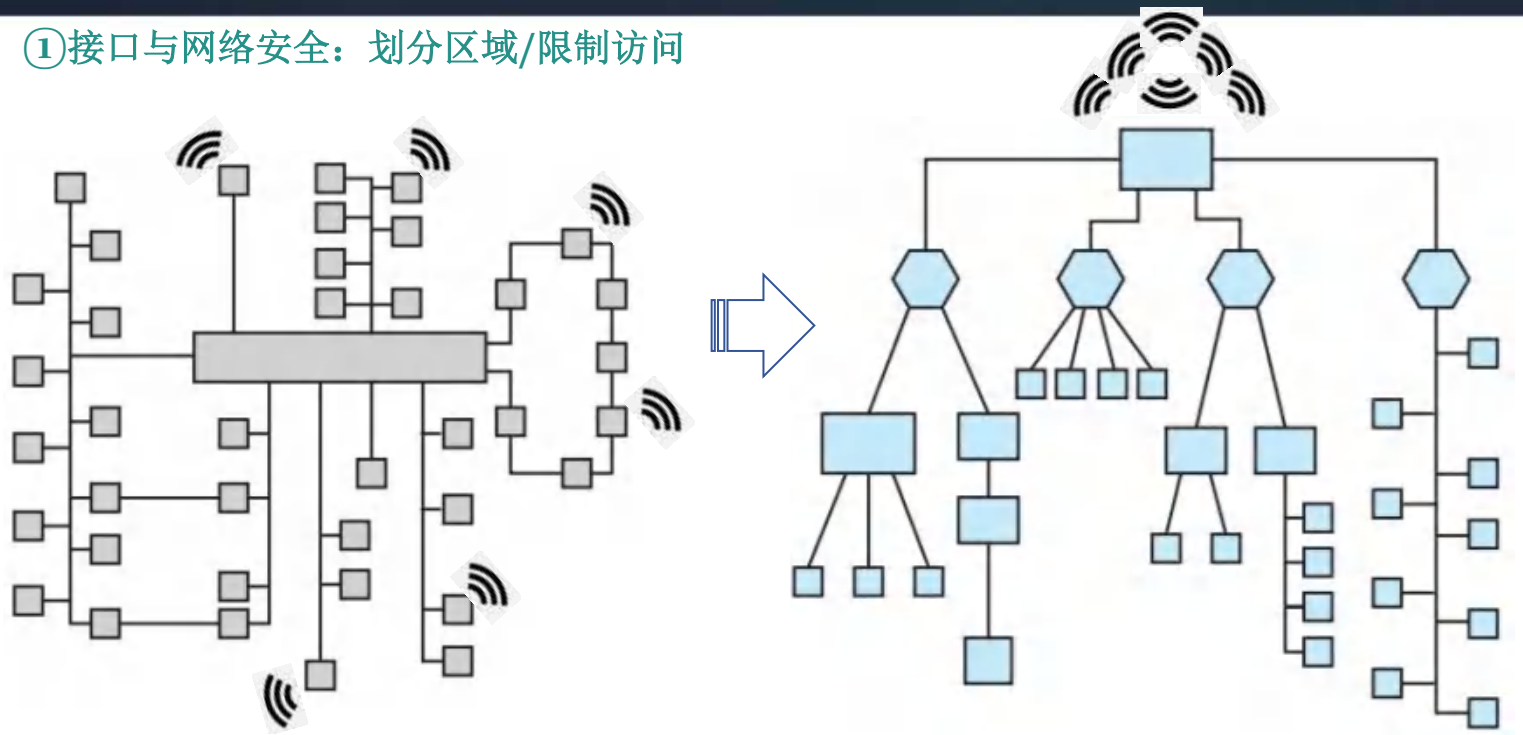
检测防御：监控与应急响应

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

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

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

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

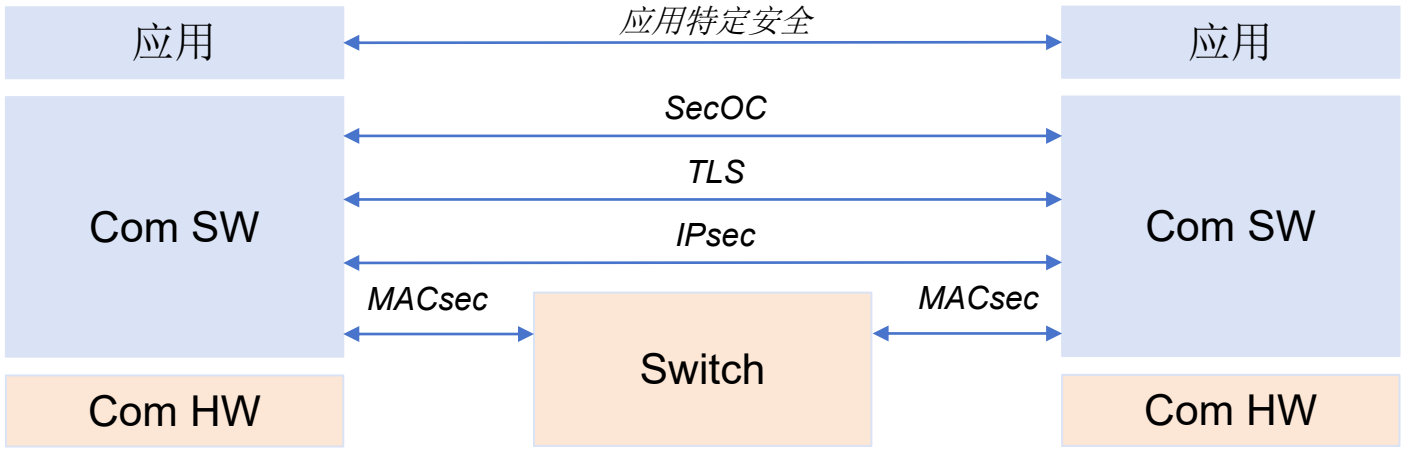
网络设计/网络拓扑

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

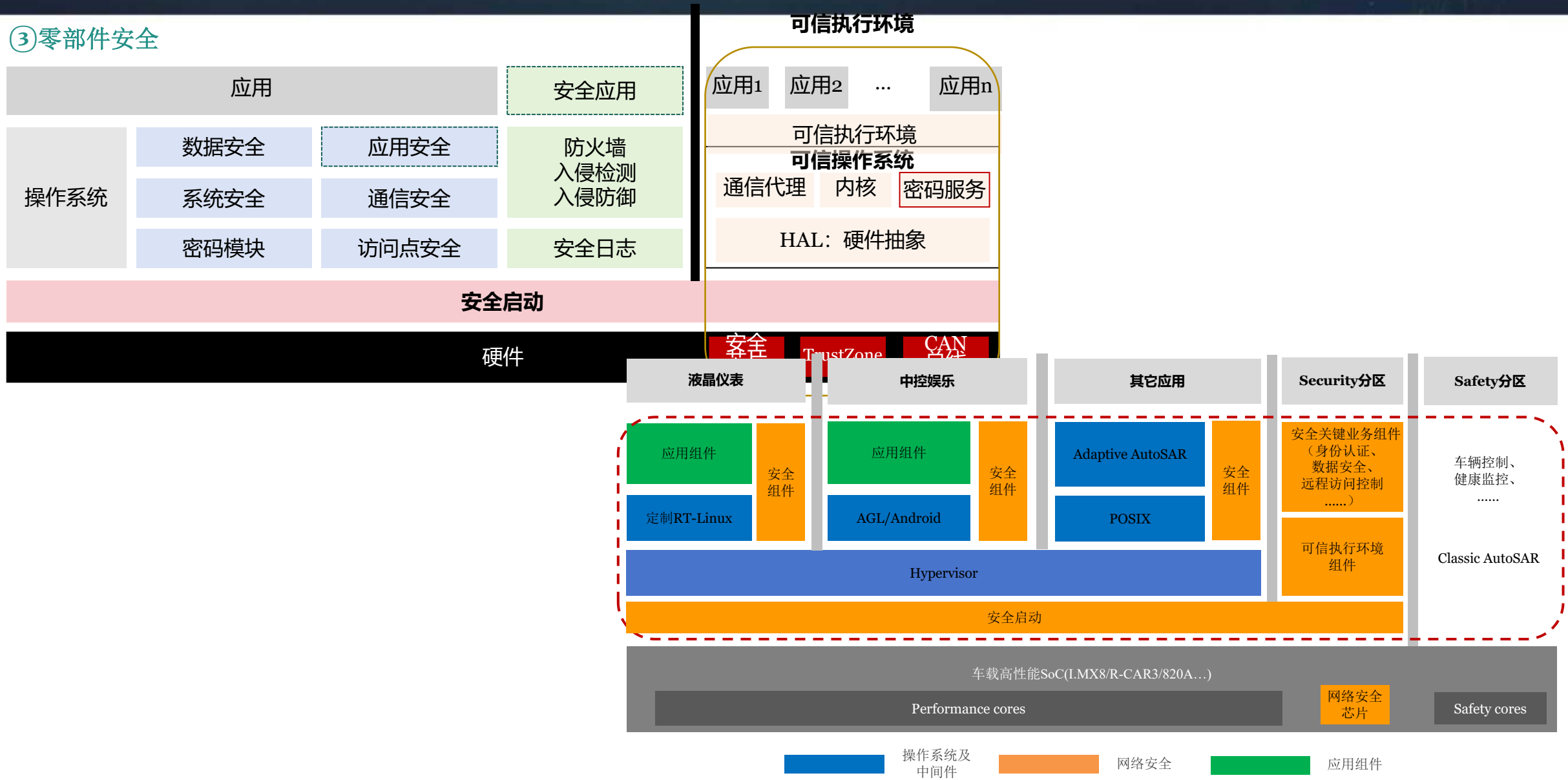
合法、授权数据可以跨域：VLAN通信；物理隔离

②数据传输安全



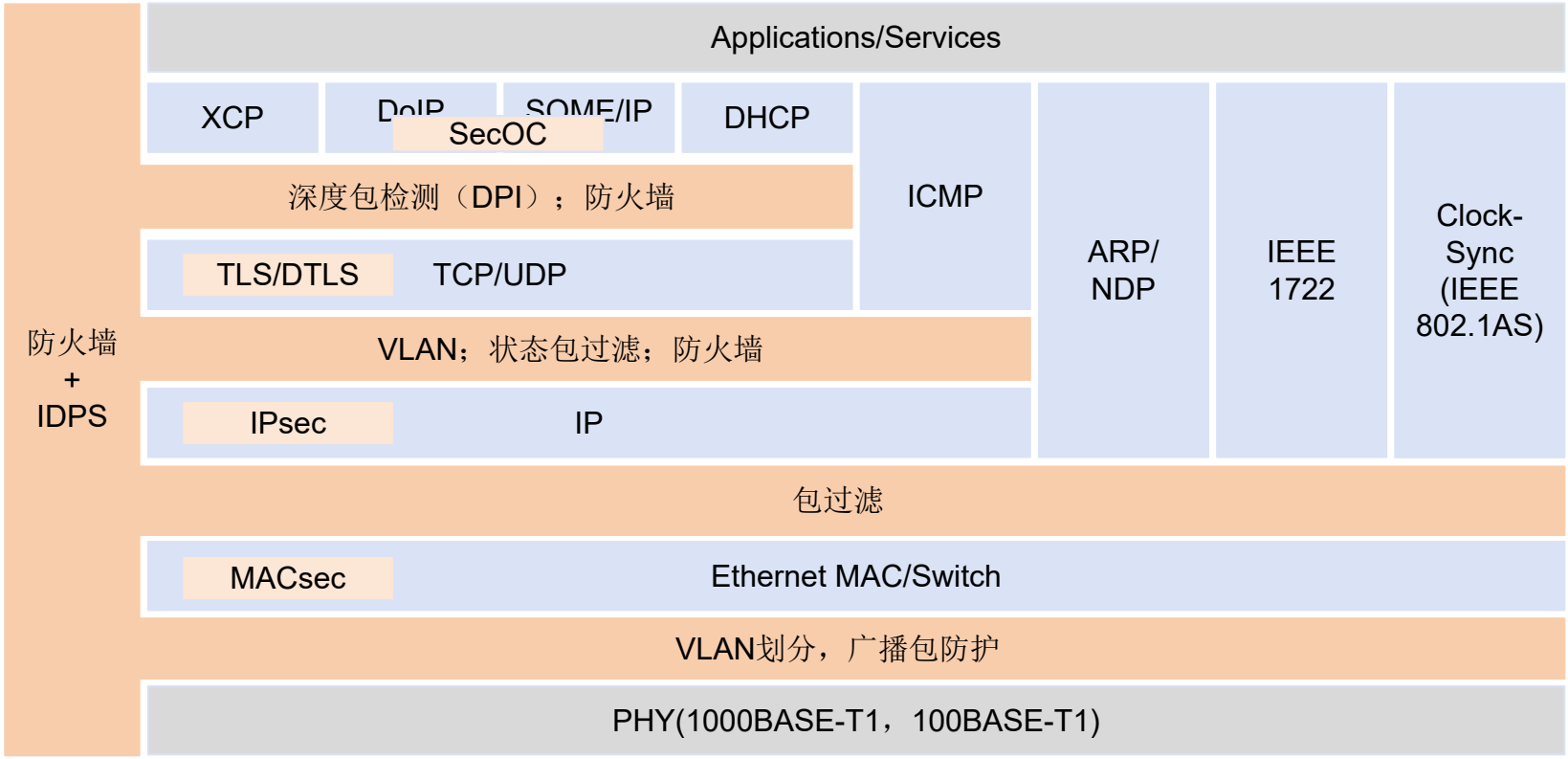
协议	标准	类型/协议层次	真实性	保密性
MACsec	IEEE 802.1AE	Hop-by-Hop Data-Link	√	√
IPsec AH	IETF RFC 4302	End-to-End IP	√	x
IPsec ESP	IETF RFC 4303	End-to-End IP	√	√
TLS	IETF RFC 5246	End-to-End TCP	√	√
SecOC	AUTOSAR	End-to-End PDUs	√	x

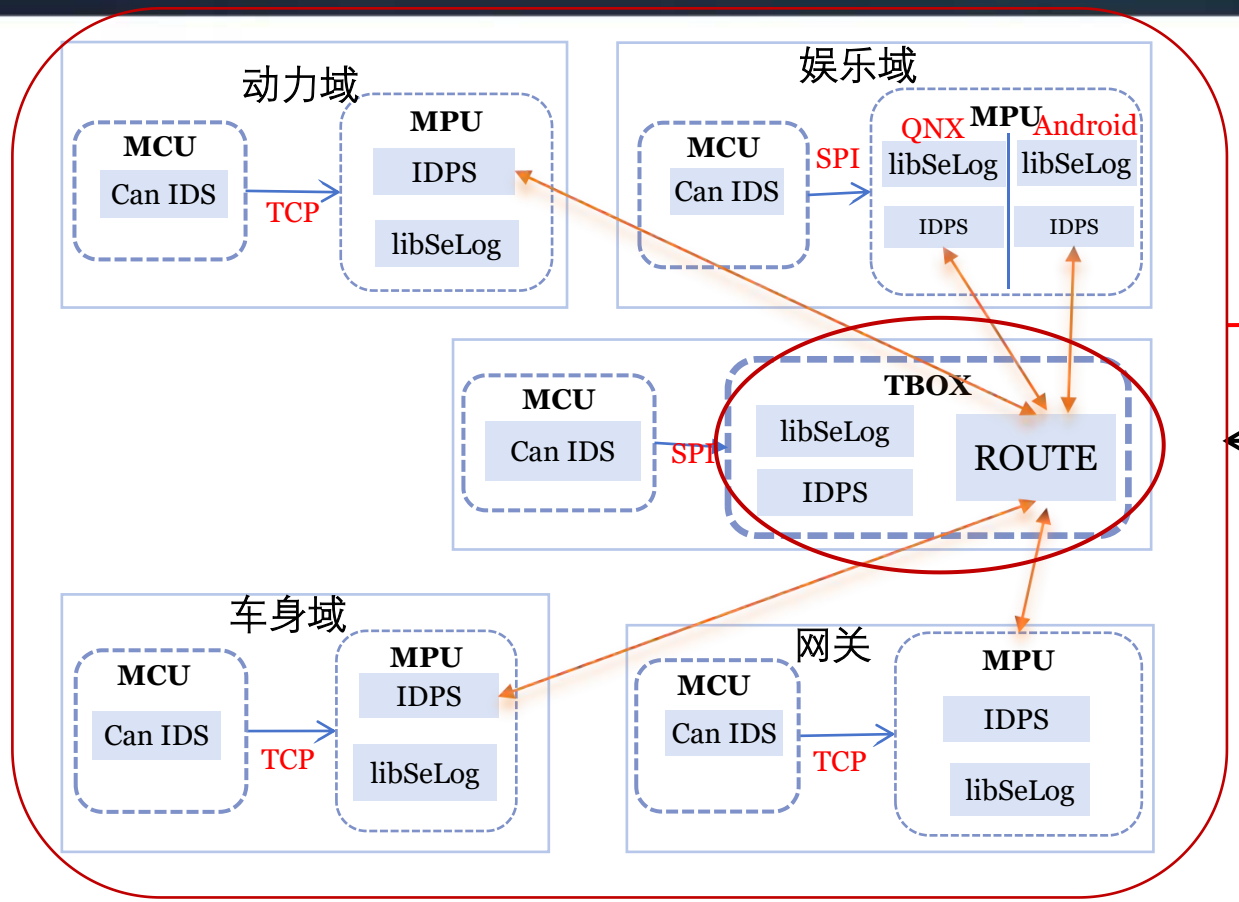
③零部件安全

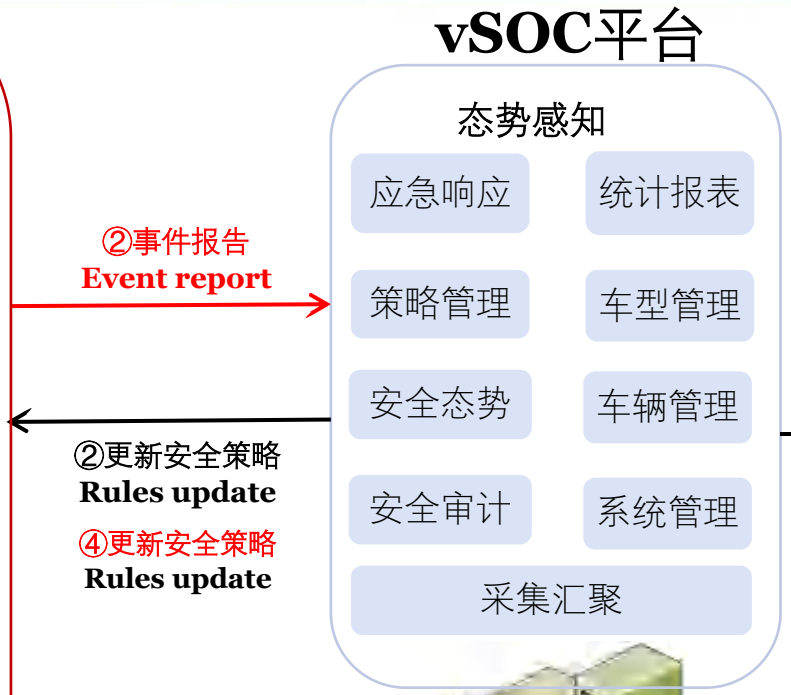


下一代零部件安全：智能座舱、中央网关、域控制器、自动驾驶、……

④检测与防御：通信监控/防火墙 + IDPS







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

③潜在威胁
Potential threats

①潜在威胁
Rules update

④应急处置
Emergency handling

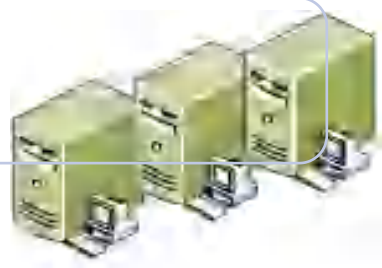
②应急处置
Emergency handling

①黑客攻击
Hacker attack

④应急处置
Emergency handling

②应急处置
Emergency handling

与OTA集成




汽车网络安全态势感知
23
245
108


汽车网络安全态势感知
IVI
TBOX


亚马逊云科技
智慧汽车
安全 & 合规
为质信安增强墙 VSOC
联合解决方案
亚马逊云科技
构建无限
智慧汽车
亚马逊云科技
亚马逊云科技

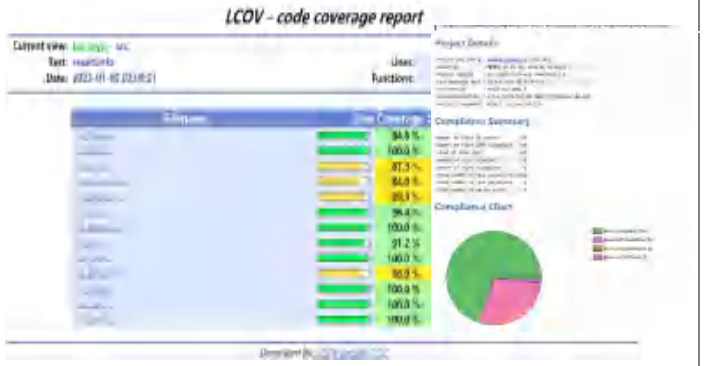
如何因应V模型的长尾效应问题

- 通过虚实结合技术构建汽车网络安全靶场，为智能汽车网络安全攻防演练、安全防护技术验证、安全产品功能验证等提供环境支撑和服务，提高智能汽车网络安全测试评估能力和安全防护能力，加强智能汽车网络安全应急保障工作
- 从攻防演练中的不同角度出发，划分为试验导调，资源管理，进攻方，防守方，检测方等5个角色

汽车网络靶场体系架构

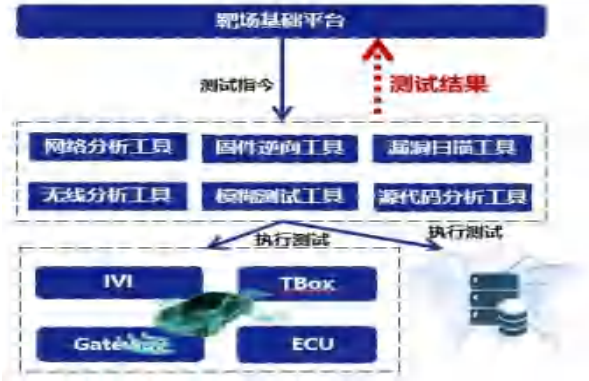
①安全开发验证

基于汽车网络靶场，在规划阶段、概念阶段和开发阶段可以加快安全组件的集成和验证效率（如安全组件或整体安全策略），利用靶场搭建目标网络运行环境和攻防场景，进行开发与验证，以期找到存在的漏洞和缺陷



②安全测试

基于汽车网络靶场，搭建目标测试环境和攻防场景，开展合规验证、渗透测试，涵盖国际/国内标准、法规和企业安全规范的要求

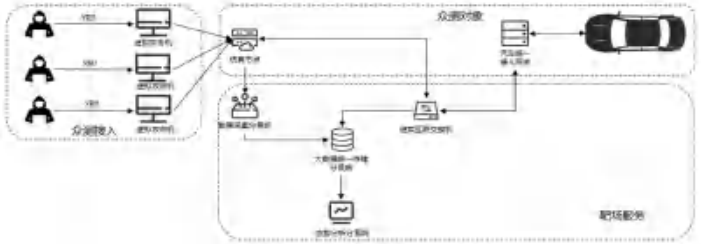


③攻防演练

基于汽车网络靶场，构建出各种逼真可控的虚实仿真与实车环境，通过各种攻防训练与竞技、实车对抗，可以发现并完善存在的安全问题，提高网络安全水平

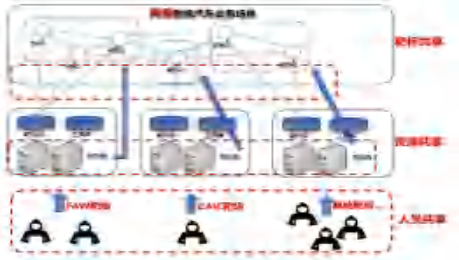
④安全众测

基于汽车网络靶场，引入多家安全测试机构、白帽子进行众测，集多方资源进行漏洞挖掘、积累测试方法和漏洞库。弥补自主试验室和单一测试机构测试用例固化，测试技术单一的问题



⑤联邦靶场互联互通

基于汽车网络靶场，与鹏城国家靶场等其他异域异构靶场互联互通，多场景多方协同共享资源，利用不同靶场的服务器资源，分布式仿真，实现靶标共享、资源共享、人员共享，打造开放式的网络安全生态

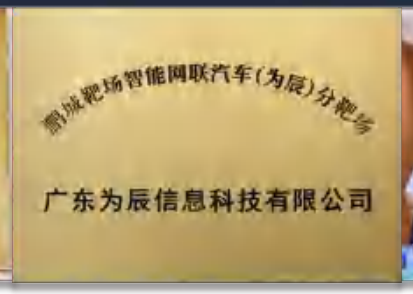


⑥应急响应中心

基于汽车网络靶场，提供漏洞提交，安全事件收集、威胁检测，配合应急响应规则，触发风险预警、溯源分析、漏洞验证为应急响应提供决策依据

基于网络靶场的车联网漏洞挖掘竞赛-数十支参赛队伍，数百名名选手参赛

漏洞挖掘



30+ OEM/Tier-1/检测机构等联盟成员

20场 “护车行动”攻防赛事

2020-2021

2020.7 深圳/鹏城实验室，组织首届“网络靶场与智能汽车安全论坛”

2022.1 深圳/鹏城实验室“首届智能汽车网络安全大赛”

2022.2 北京/ 举办CVVD车联网漏洞挖掘赛

2022.3 上海/AutoSec网络安全论坛开展汽车攻防体验嘉年华

2022.4 深圳/成立护车联盟

2022.12南京/举办“创安杯”智能汽车信息安全公开赛

2022

2022.4 线上/ 2022CICV漏洞挖掘赛初赛

2022.5 天津/2022WIDC世界智能驾驶挑战赛

2022.7 沈阳/2022智能网联汽车国际大会

2022.7 深圳/第二届“鹏城杯”联邦靶场协同攻防演练赛

2022.8 北京/2022CICV漏洞挖掘赛决赛

2022.9 北京/2022全国智能驾驶测试赛

2022.10 线上/第二届“创安杯”初赛

2022.12 北京/工信部“铸网2022”车联网网络安全实网演练赛

2023

2023.3 南京/第二届“创安杯”决赛

2023.4 沈阳/2023世界智能驾驶挑战赛-信息安全攻防赛预赛

2023.5 天津/发布基于网络靶场的智能汽车全生命周期安全测评方法

2023.7 沈阳/第三届中国（沈阳）智能网联汽车国际大赛-信息安全攻防赛

2023.11 线上/鹏城实验室第三届“鹏城杯”CTF线上解题赛

2023.11 深圳/鹏城实验室第三届“鹏城杯”联邦靶场协同攻防演练赛

基于鹏城实验室，率先形成的汽车网络靶场，已开展20余场次攻防演练活动

第四届“鹏城杯”

联邦网络靶场协同攻防演练

为加速推进我国网络安全战略与数字化进程落地，创新信息系统安全防护与网络安全技术研究模式，促进各行业网络安全建设的融合与协作，由鹏城实验室牵头主办的第四届“鹏城杯”联邦网络靶场协同攻防演练正式启动。本次活动汇集了能源、金融、交通、水利、市政、电信、政府部门等二十余家关键信息基础设施行业的特色场景，创新引入协同攻防、红蓝对抗和异地参赛等多种竞赛机制，与参赛队伍和行业专家深入探讨联邦靶场技术和生态建设，展示各分靶场单位在网络靶场建设方面的最新成果。所有选手的决赛得分，计入众测资质等级评估体系，对于满足分数标准的选手，发放相应众测资质等级证书。

组织单位

主办单位

鹏城实验室、中国网络空间安全人才教育论坛、中国网络空间新兴技术安全创新论坛、华中科技大学、西安电子科技大学、广州大学

协办单位

（单位名称按首字笔划排序）

一汽－大众汽车有限公司、工业和信息化部电子第五研究所、山东省计算中心（国家超级计算济南中心）、广东为辰信息科技有限公司、广东省机场管理集团有限公司、中山市政务服务和数据管理局、中汽创智科技有限公司、中汽研汽车检验中心（天津）有限公司、中国石化安全工程研究院有限公司、中国电信股份有限公司研究院、中国汽车工程研究院股份有限公司、中国移动通信集团有限公司、中国第一汽车集团有限公司研发总院、中国联合网络通信有限公司研究院、中国联合网络通信集团有限公司、北京六方云信息技术有限公司、四川亿览态势科技有限公司、西南交通大学、西部智联数字科技（重庆）有限公司、网络空间安全产业协会、全聚合数字技术有限公司、齐鲁工业大学、软极网络技术（北京）有限公司、国汽（北京）智能网联汽车研究院有限公司、南方电网科学研究院有限责任公司、浙江国利网安科技有限公司、深圳市环境水务集团有限公司、深圳市南山区政务服务和数据管理局、深圳市燃气集团股份有限公司、博维资讯系统有限公司、博智安全科技股份有限公司、联通智网科技有限公司

参赛对象

比赛面向全国招募参赛人员，邀请
高校、企业、研究机构等有关单位的网络安全研究人员参赛。

赛程安排

初赛

时间：2024 年 11 月 9 日
模式：CTF 线上解题赛

决赛

时间：2024 年 11 月 22 日 - 24 日
模式：联邦靶场协同攻防模式

THANK YOU!