2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

# 车联网时代的安全新挑战

奇安信集团 左英男

# 智能网联汽车的发展趋势



网联化

共享化

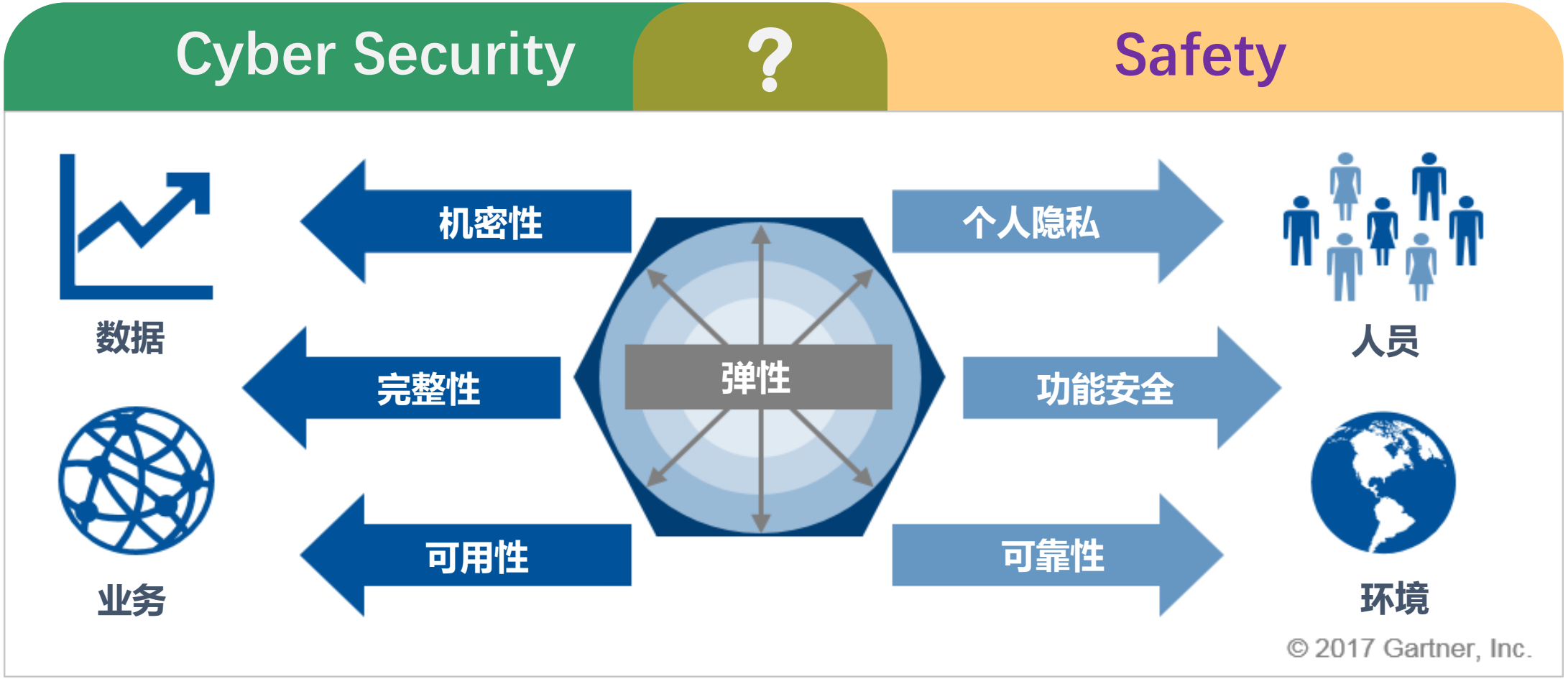
电动化

智能化

**未来的汽车不再是简单的出行工具，而是融入人类日常生活的多场景智能体验终端。**

# 车联网场景下安全内涵发生了改变

智能网联汽车是数字世界和物理世界的交汇点，本质是IT/OT技术的深度融合

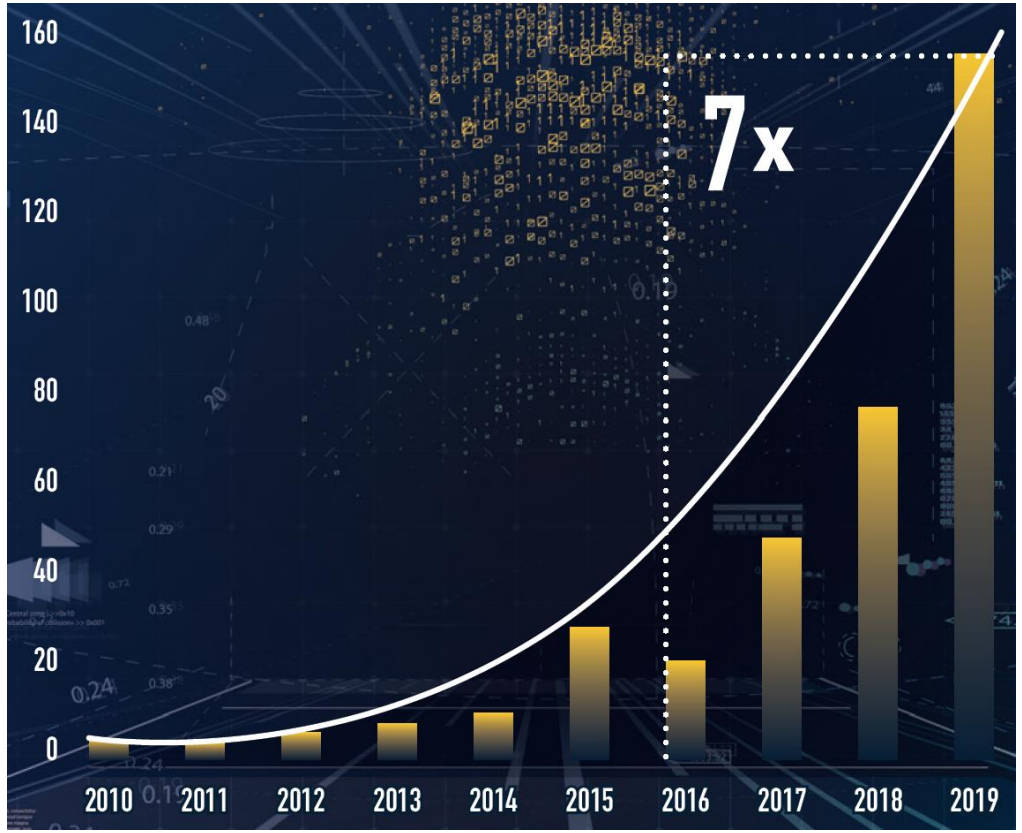


# 例1：网联化带来的安全新挑战

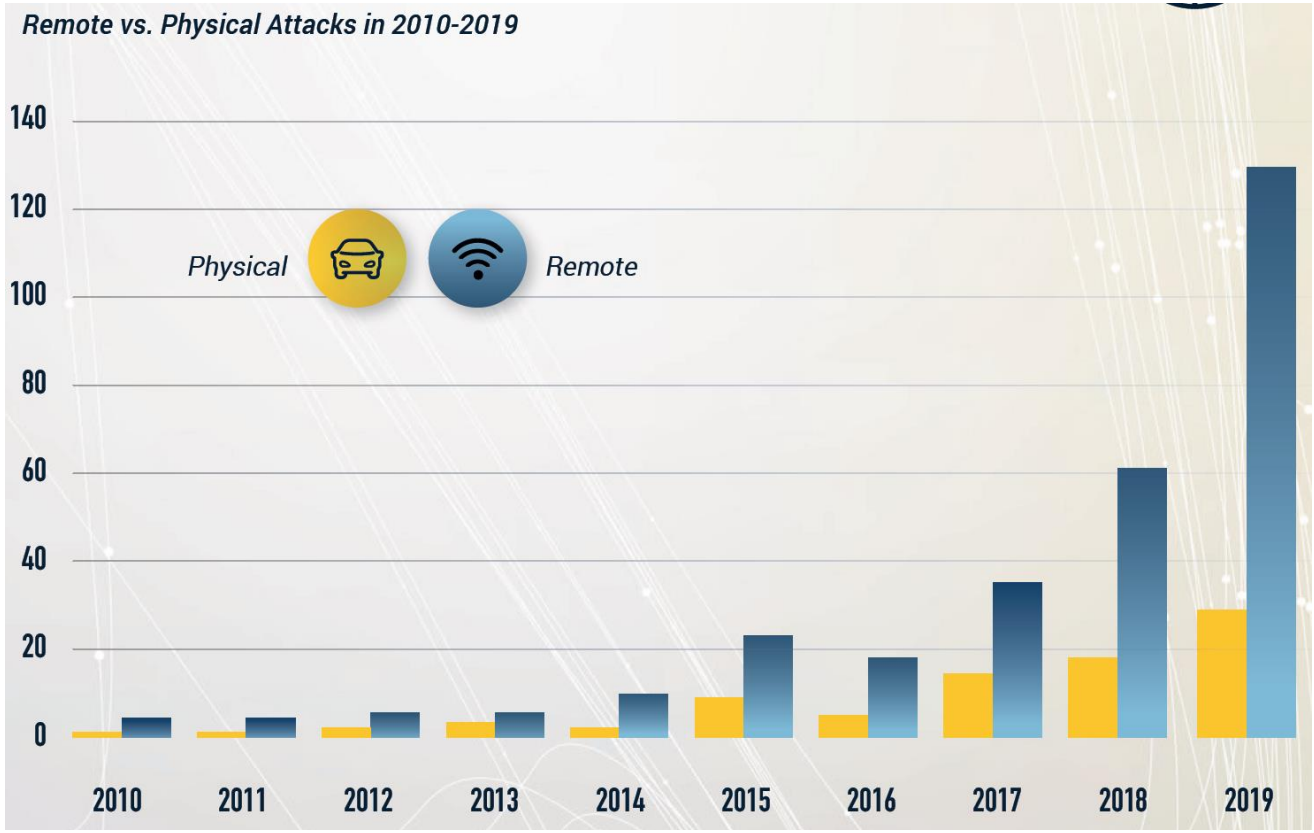


# 例1：网联化带来的安全新挑战






过去10年网络安全事件的数量

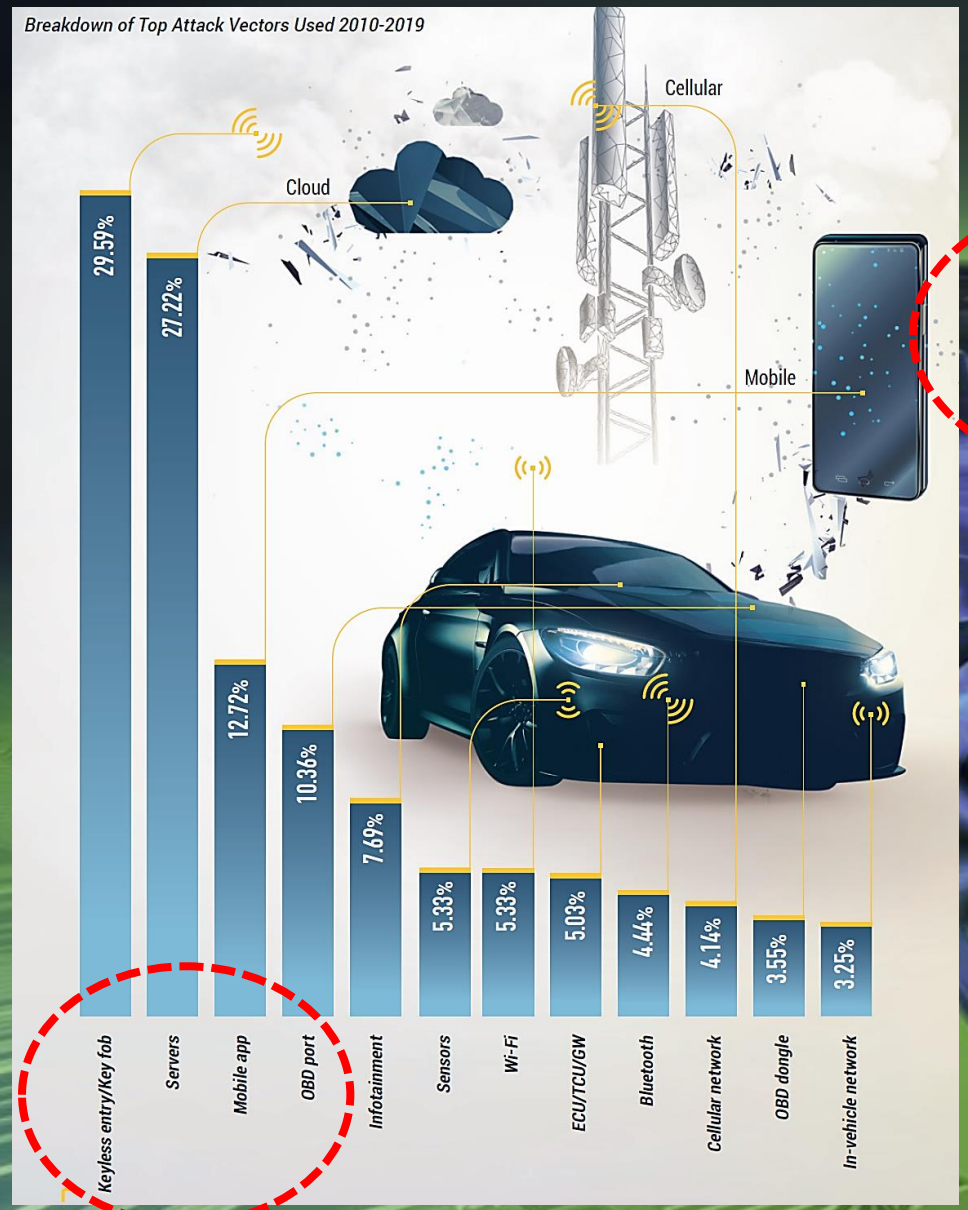


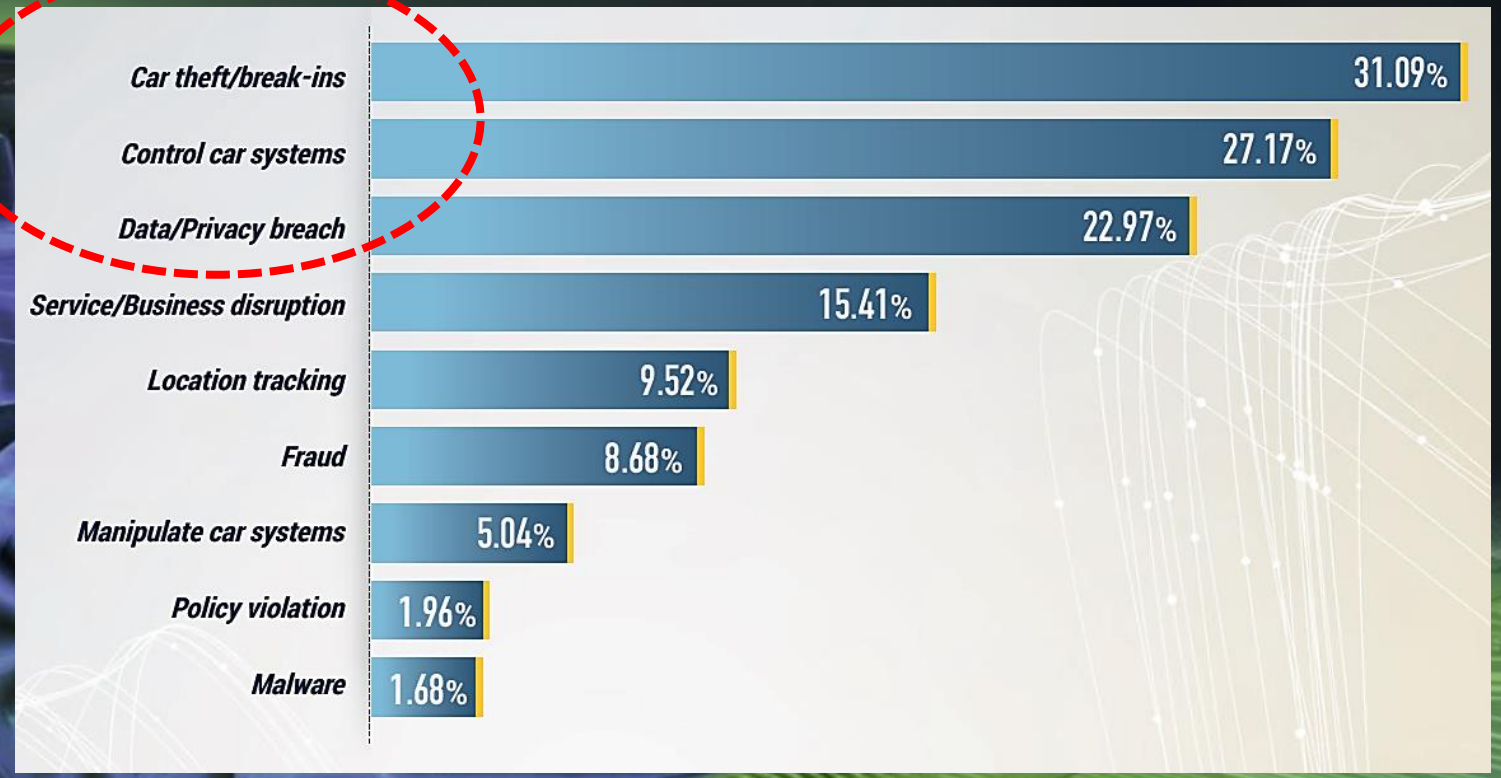

过去10年物理攻击和远程攻击

Upstream Security：*Global Automotive Cybersecurity Report 2020*

# Top攻击向量&后果

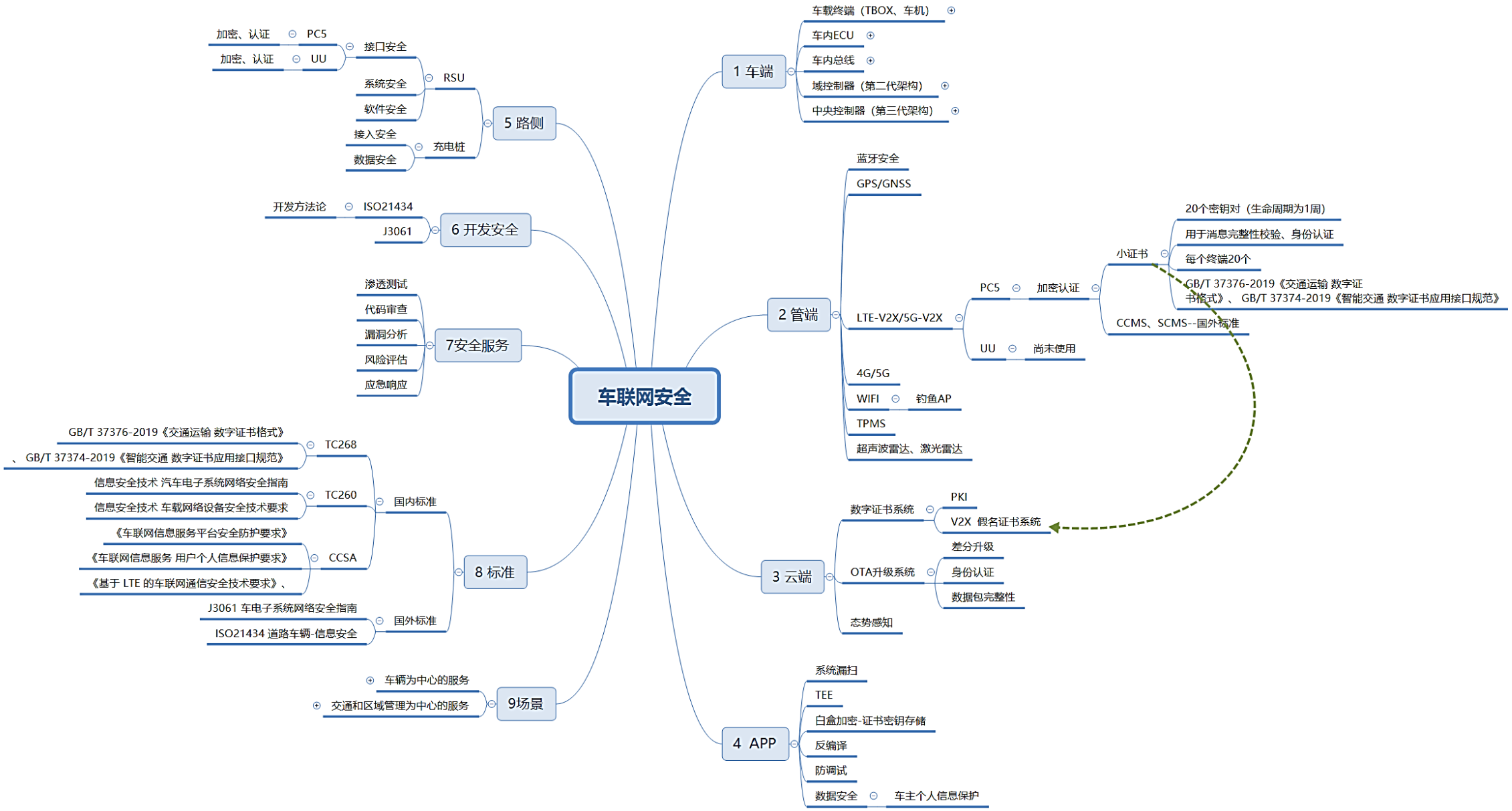



Breakdown of Top Attack Vectors Used 2010-2019
Cellular
Cloud
Mobile
29.59%
27.22%
12.72%
10.36%
7.69%
5.33%
5.33%
5.03%
4.44%
4.14%
3.55%
3.25%
Keyless entry/Key fob
Servers
Mobile app
OBD port
Infotainment
Sensors
Wi-Fi
ECU/TCU/GW
Bluetooth
Cellular network
OBD dongle
In-vehicle network


Car theft/break-ins 31.09%
Control car systems 27.17%
Data/Privacy breach 22.97%
Service/Business disruption 15.41%
Location tracking 9.52%
Fraud 8.68%
Manipulate car systems 5.04%
Policy violation 1.96%
Malware 1.68%

# 车联网安全涉及“云管端”的方方面面

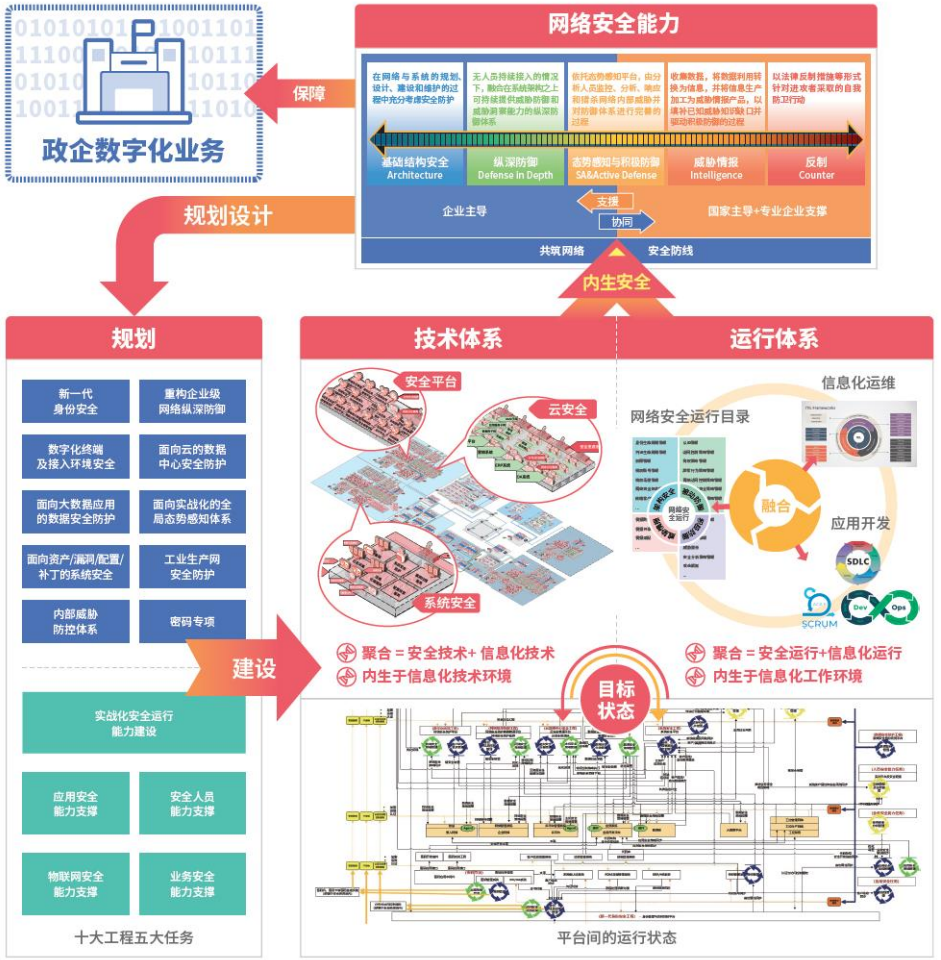




# 车联网安全体系规划与设计的原则

## 新一代网络安全框架（内生安全框架）

- 同步规划、同步建设、同步运营
- 从”局部整改”到”整体规划”
- 从”外挂修补”到”内生融合”
- 技术体系与运行体系并重
- 网络安全与功能安全融合




新一代企业网络安全框架（内生安全框架）

# 例2：智能化带来的安全新挑战




BAIR
BERKELEY ARTIFICIAL INTELLIGENCE RESEARCH

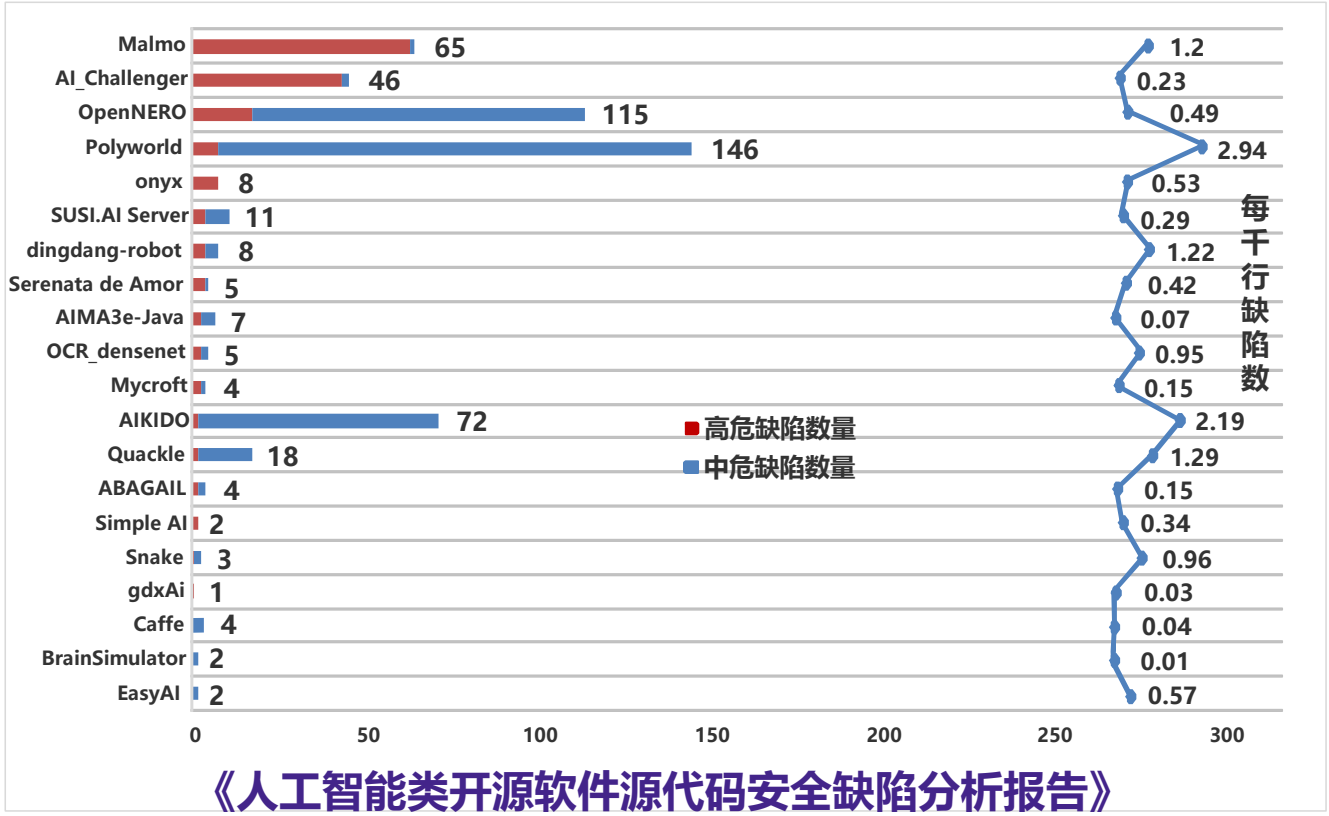
设计者为算法定义了
**错误**
的目标函数

选用的算法模型
**表达能力有限**
不能完全表达实际情况

设计者定义了
**计算成本非常高**
的目标函数

# 例2：智能化带来的安全新挑战






《人工智能类开源软件源代码安全缺陷分析报告》

CNCERT/CC 国家互联网应急中心 + 奇安信代码卫士 Qi An Xin CodeSafe

| 开源项目名称 | 版本号 | 主要编程语言 | 功能说明 | 代码行数 |
|---|---|---|---|---|
| dingdang-robot | 0.2.1 | Python | 工作在 Raspberry Pi 上的中文语音对话机器人 | 6,574 |
| Serenata de Amor | 1.0.0 | Python | 公共社会管理的 AI 项目 | 11,877 |
| Snake | 1.0.0 | Python | AI 的贪吃蛇游戏 | 3,123 |
| Simple AI | 0.8.1 | Python | AI 算法工具包 | 5,963 |
| EasyAI | 1.0.0 | Python | 一个 AI 游戏框架 | 3,487 |
| Mycroft | 0.8.5 | Python | 可编程的开源语音助手 | 27,236 |
| AI_Challenger | 1.0 | Python | 开放数据集和编程比赛的 AI 挑战平台 | 198,422 |
| OpenNERO | 1.0.0 | C++ | 面向 AI 研究和教育的开放平台 | 234,302 |
| Polyworld | 2.6.0 | C++ | AI 仿人工生命系统 | 49,673 |
| AIKIDO | 0.2.0 | C++ | 一个解决机器人运动规划和决策问题的 C++库 | 32,830 |
| Quackle | 1.0.3 | C++ | 填字游戏的 AI 分析工具 | 13,908 |
| Caffe | 0.9999 | C++ | 一个深度学习开发框架 | 92,761 |
| SUSI.AI Server | 2.1.0 | Java | 一个智能开源个人助理程序 | 37,400 |
| gdxAi | 1.8.1 | Java | 基于 libGDX 的游戏开发框架 | 35,200 |
| onyx | 1.1.4 | Java | 一个使用人工智能，机器学习和深度学习等技术的 android 库，可了解在应用中显示的内容 | 15,100 |
| AIMA3e-Java | 3.0.0 | Java | Russell 和 Norvig 的 AI 算法的 Java 实现 | 97,600 |
| ABAGAIL | 1.0.0 | Java | 机器学习和人工智能的算法包 | 26,700 |
| Malmo | 0.35.6 | Java | 一个基于 Minecraft 的 AI 实验和研究平台 | 54,100 |
| OCR_densenet | 1.0.0 | Java | 采用 densenet 的图片文字识别软件（第一届西安交通大学人工智能实践大赛第一名） | 5,267 |
| BrainSimulator | 0.6.0 | C# | AI 架构的可视化原型设计开发平台 | 295,300 |

# 车联网产业安全生态：协同共治安全漏洞



6万+
已注册白帽子数量

6000+
已注册机构数量


40万+
已发现漏洞总数

8万+
漏洞影响企业数

网络安全产业

**车联网厂商**

- 安全意识相对薄弱
- 安全开发能力不足
- 漏洞研究人才匮乏

+

**网络安全厂商**

- 智能汽车型号繁多
- 获取成本相对较高
- 功能安全认知有限

**以用户知情为宗旨的**
**漏洞披露和协同治理机制**

车联网产业

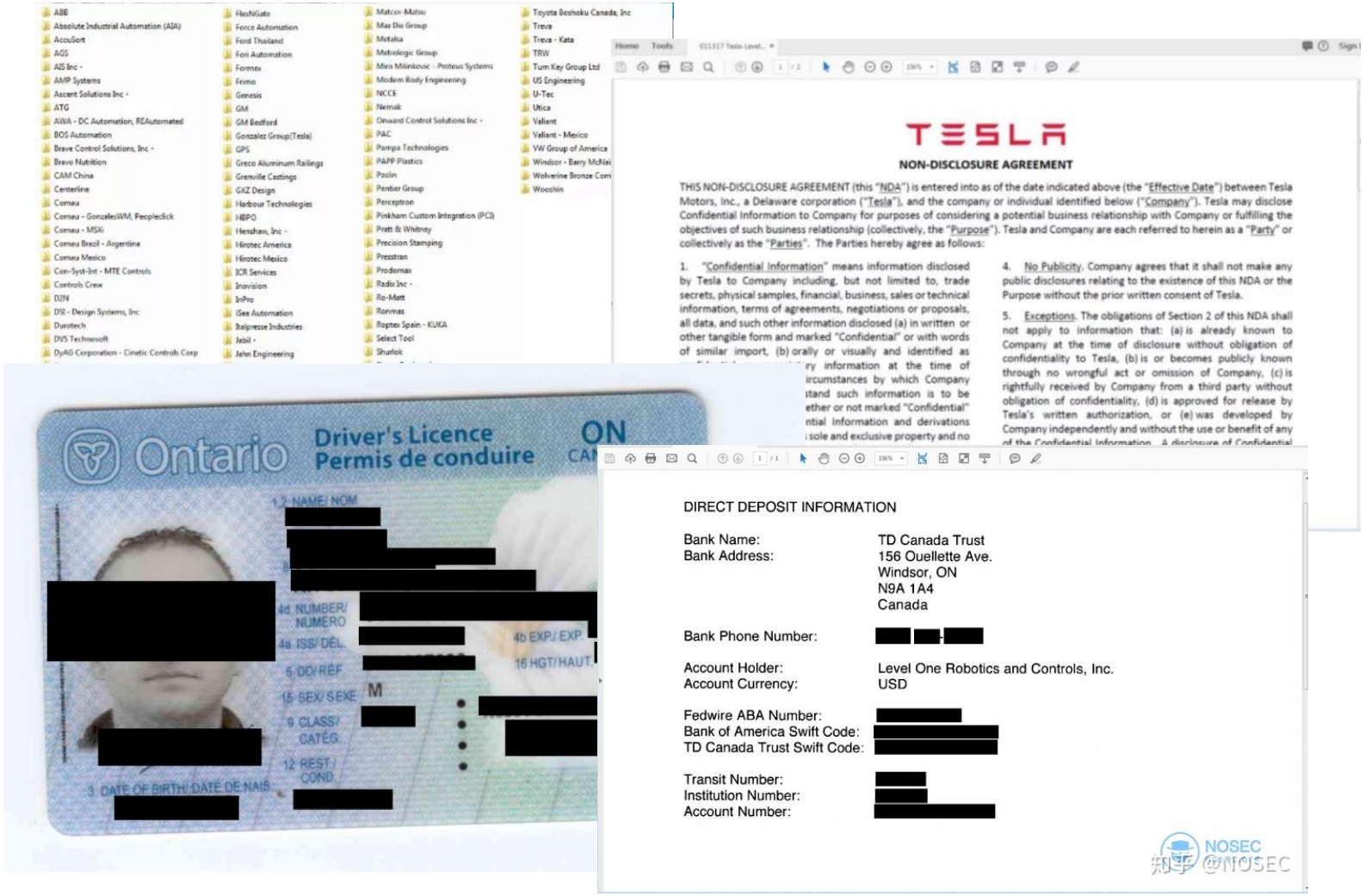
# 例3：共享化带来的安全新挑战



## Level One Robotics& Controls

大众、特斯拉、丰田、福特、通用等百余家汽车厂商机密文件被曝光。内容及车厂发展蓝图规划、制造细节，到客户合同、工作计划，甚至员工的驾驶证和护照的等隐私信息，共计**15.7G**，近**5万**个文件。

此次泄露的原因主要由于Level One未对自己的RSYNC服务设置密码，导致任何人都可以在不需要密码的情况下访问这些敏感文件。最终造成数据泄露。



# 传统的数据安全防护技术



ICS 35.040
L 80

中华人民共和国国家标准

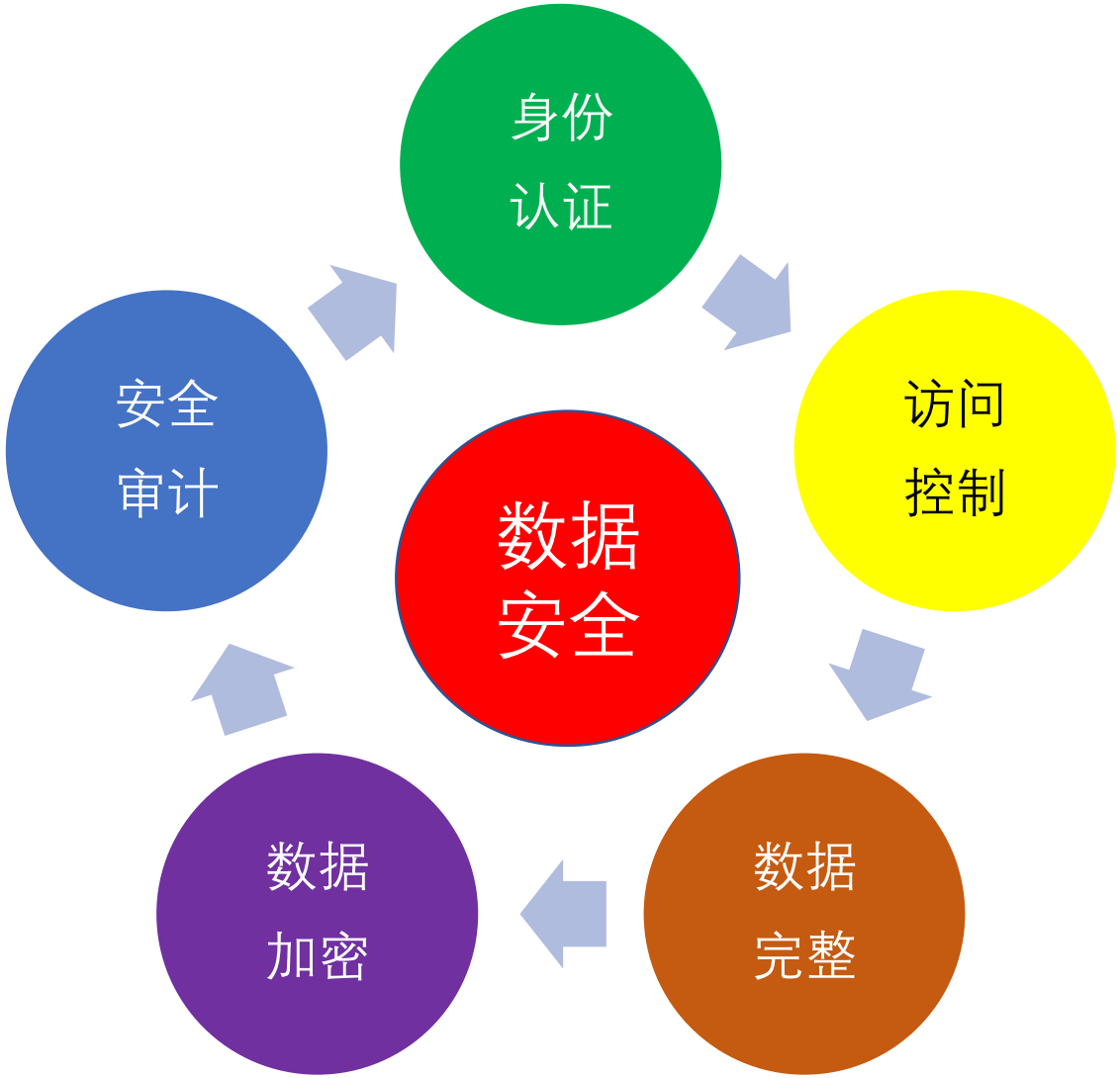
GB/T 22239—2019
代替 GB/T 22239—2008

信息安全技术
网络安全等级保护基本要求

Information security technology—
Baseline for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布



# 中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见

2020-04-09 19:00 来源： 新华社 【字体：大 中 小】 打印

新华社北京4月9日电

完善要素
会主义市场经
会创造力和市
意见。

一、总体

- 确权—数据没有独占性
- 定价—数据没有稀缺性
- 流动—数据价值会衰减

**大数据安全和隐私保护的挑战更大**

## 六、加快培育数据要素市场

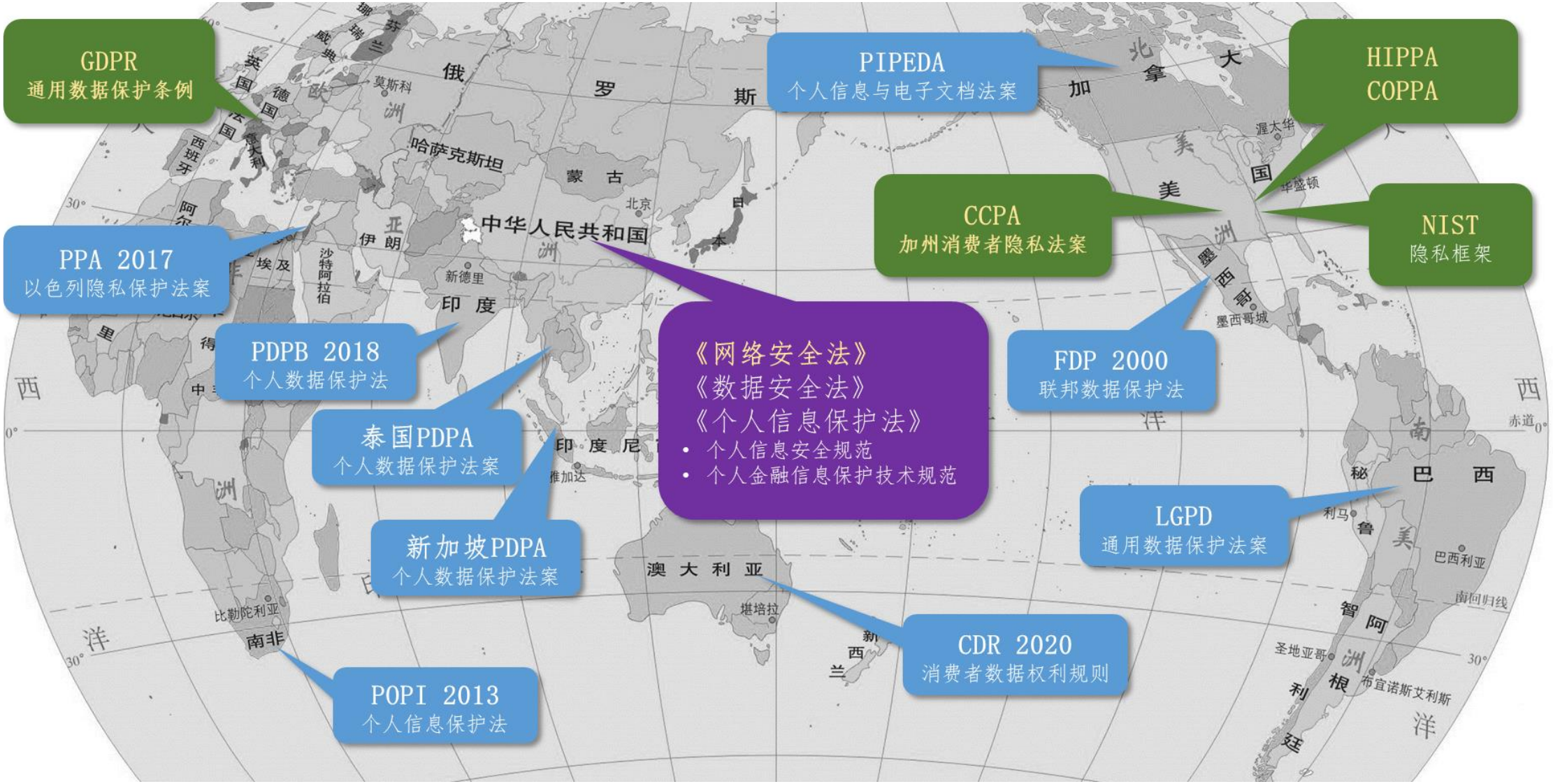
（二十）推进政府数据开放共享。优化经济治理基础数据库，加快推动各地区各部门间数据共享交换，制定出台新一批数据共享责任清单。研究建立促进企业登记、交通运输、气象等公共数据开放和数据资源有效流动的制度规范。

（二十一）提升社会数据资源价值。培育数字经济新产业、新业态和新模式，支持构建农业、工业、交通、教育、安防、城市管理、公共资源交易等领域规范化数据开发利用的场景。发挥行业协会商会作用，推动人工智能、可穿戴设备、车联网、物联网等领域数据采集标准化。

（二十二）加强数据资源整合和安全保护。探索建立统一规范的数据管理制度，提高数据质量和规范性，丰富数据产品。研究根据数据性质完善产权性质。制定数据隐私保护制度和安全审查制度。推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。

# 世界各国数据安全和隐私保护相关法规





# 车联网平台：构建以数据为中心的安全体系



**时间维度：**

数据生命周期（采集、传输、存储、使用、销毁）的安全风险

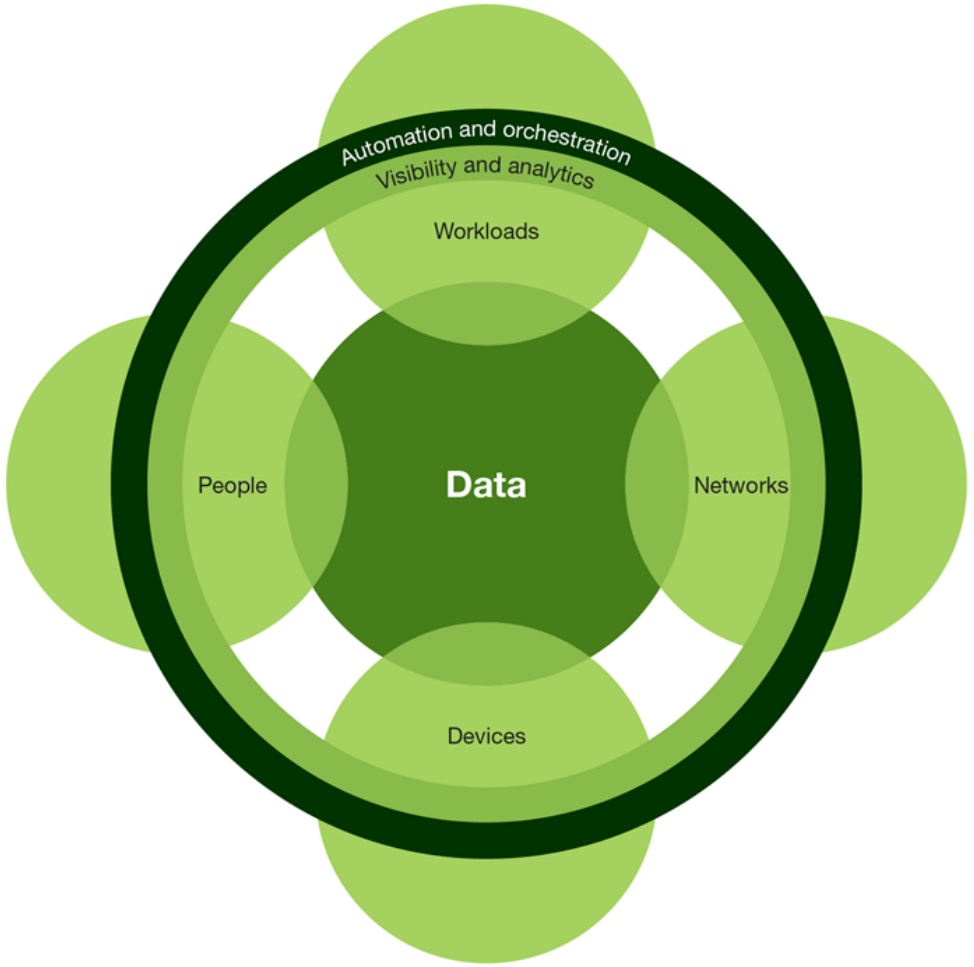
**空间维度：**

数据的暴露面，数据流转各个环节的安全风险

**价值维度：**

大数据时代，对所有的数据都提供完善的安全保护是不现实的，需要对数据的重要程度进行分类分级，

**没有不可接受的风险就是安全。**




**可见：**

数据分布可视、数据流转可视、访问行为可视

**可控：**

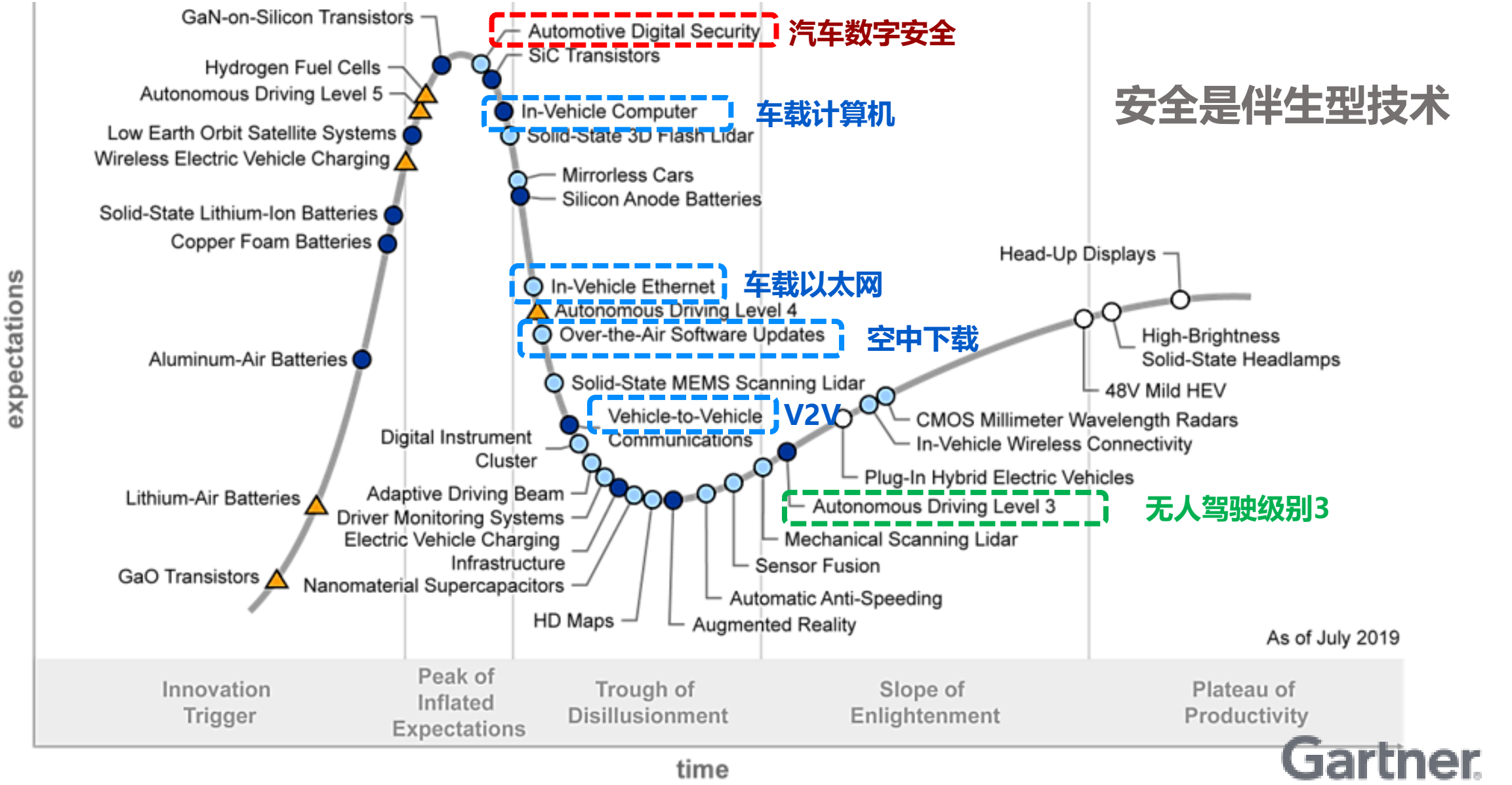
风险驱动，减少大数据的暴露面，强化访问控制

**可管：**

发现、保护、检测、响应手段有机结合，实现数据全生命周期可管理

# Hype Cycle for Automotive Electronics, 2019






安全是伴生型技术

Gartner

# Hype Cycle for Automotive Electronics, 2019



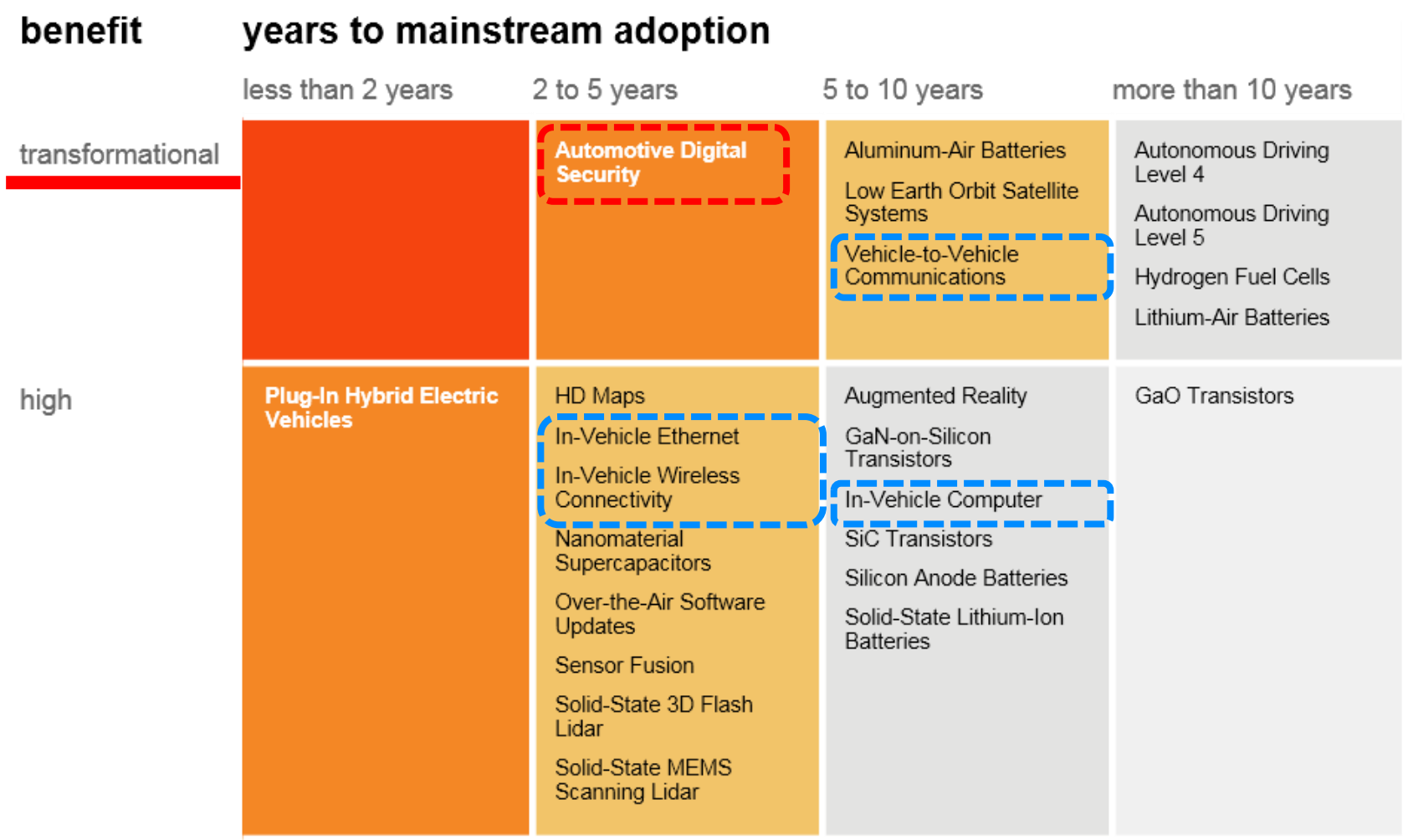
1. 汽车数字安全：针对内外部威胁，保护汽车内所有的物理资产（汽车硬件）和数字资产（例如软件、信息）

2. 早期针对无钥匙进入系统、OTA等的网络攻击，驱动早期的汽车数字安全投入

3. 数字设备的信息物理融合特性导致功能安全和信息安全融合

4. 长期来看

   **数字安全提升汽车的价值**



# 山高水远，来日方长


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音