汽车制造业信息安全形势与建设分享

分 享 人： 姜明元

合规环境趋紧

01

国家法规

- 《网络安全法》及若干解释
- 《数据安全法》
- 《个人信息保护法》

02

行业监管

- 工信部对汽车制造业的关注加强
- 《工业控制系统信息安全行动计划（2018—2020年）》

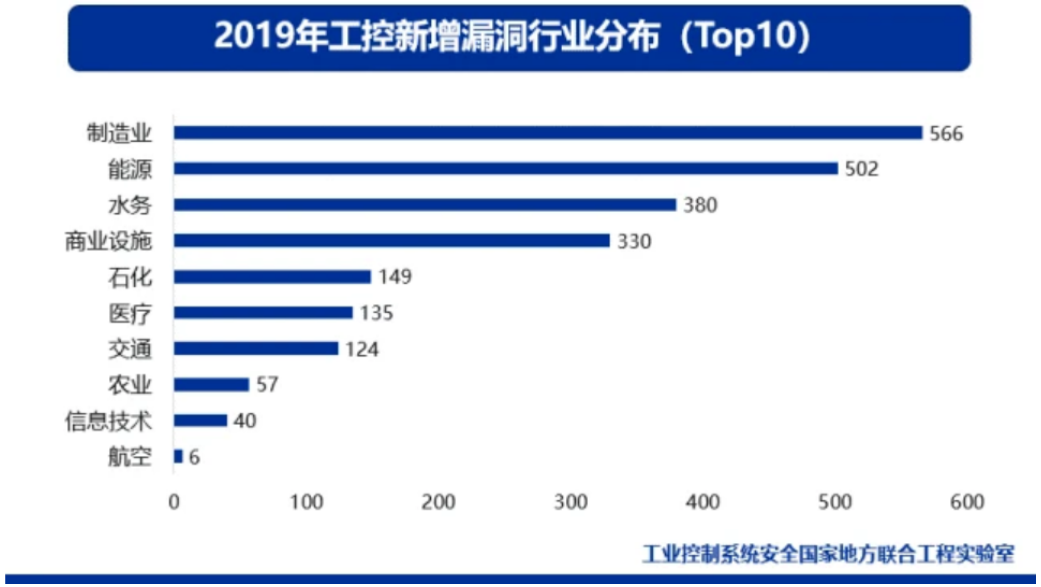
03

准入标准

- 国内车联网安全标准
- TISAX认证
- ISO/SAE 21434《道路车辆-信息安全工程》
- UN/ECE/WP29

外部形势严峻

- 勒索软件等新型攻击模式突破了工控网络的隔离限制，降低了对制造业的攻击门槛；
- “震网”病毒以来，工控系统的安全漏洞呈现逐年增多的趋势，而制造业占比最高；
- 车联网安全成为热门议题，车辆的安全漏洞呈上升趋势。



资料来源：工业控制系统安全国家地方联合工程实验室

业务发展压力

数字化转型过程中的技术创新与变革引发新的安全风险

新技术的引入、新系统的上线不仅是对传统业务形态的颠覆，也是对原有安全策略的挑战。

“走出去”战略对数据管控边界提出挑战

全球化业务扩展、跨界跨行业合作过程中，对数据共享与控制能力上需要有新的解决方案

不断演变的工作形态需有相适应的安全能力

核心商业机密的非结构化转变，新的办公形式加大对移动办公、协同办公场景的需求

面对挑战

01. 历史包袱重

02. IT基础薄弱

03. 获取资源难度大

04. 面对变革转型压力

05. 人员结构复杂

06. 自主可控有限

主要风险

公司涉密数据遭到泄露

- 员工违规操作与不当行为，泄露公司涉密数据
- 外部入侵公司网络，窃取公司涉密数据
- 合作第三方未尽到涉密数据保护义务
- 新业务发展引发新的数据泄露风险

生产因安全事件导致中断

- 工控环境感染病毒导致设备停摆
- 设备或系统操作不当导致停产
- 外部人员入侵工控网络，恶意停止设备运转

安全合规问题使业务推进受阻

- 未达行业信息安全标准无法上市
- 违反跨境数据传输、个人隐私保护相关法规面临较重处罚

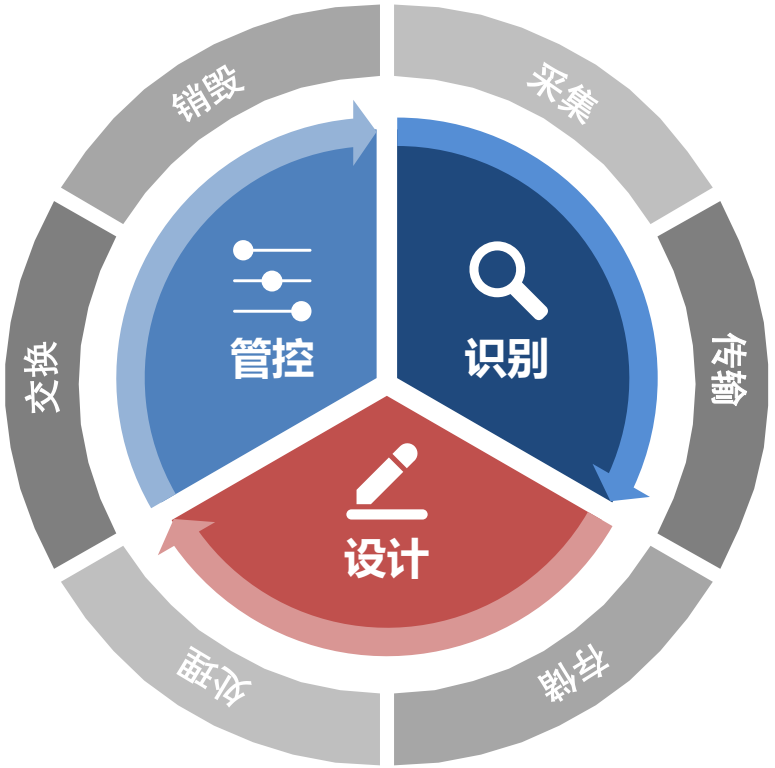
公司研发或产品存在安全漏洞

- 已上市车辆产品出现安全漏洞
- 供应链引发的产品安全漏洞
- 运营中的信息系统发现信息安全漏洞

数据防泄漏

持续优化监控

- 风险监控
- 技术管控措施
- 流程化管理措施



数据需求识别

- 涉密数据定义与识别
- 保护策略的定义
- 数据使用业务场景的识别

管控方案设计

- 管控措施
- 监控措施
- 接口设计

安全防护能力建设

通过安全运营、安全治理保障防护手段有效

物理环境

- 出入控制
- 机房管理
- 监控

网络安全

- 网络隔离
- 访问控制
- 无线安全
- 异常监测

主机安全

- 运维管控
- 设备加固
- 漏洞管理
- 日志收集

数据安全

- 数据备份
- 防泄密保护
- 数据加密
- 数据脱敏

业务终端

- 终端准入
- 防病毒
- 白名单

信息系统

- 权限控制
- 接口安全
- 开发安全

合规与认证

ISO 27001

- 通用性标准
- 多个标准参考依据
- 必须无重大偏差
- 适用于各行业，包括整车厂

TISAX

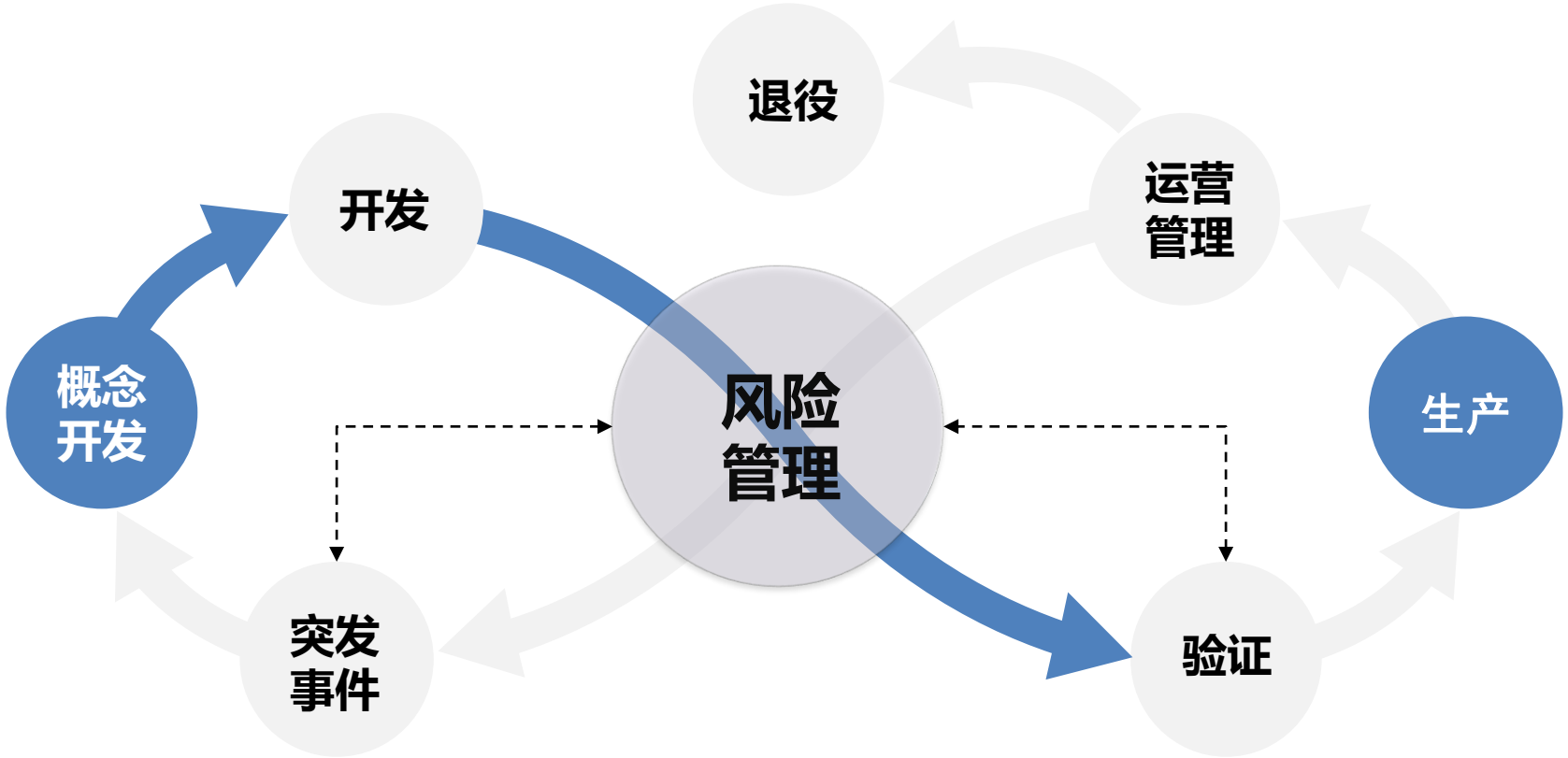
- 27001扩展要求
- VDA准入门槛
- 包含部分隐私保护内容
- 必须所有满足控制项
- 适用于零部件、供应链厂商

ISO 21434

- 为车辆研发提供参考
- 2020年2月发布草案，2021年计划转化为国标
- 汽车生命周期各个阶段的安全保障

整车研发

参考ISO21434搭建整车生命周期业务。包括网络安全整体管理、风险管理，开发过程、运营维护。



几点建议

- 组织建设
- 自主能力
- 安全运营
- IT整体能力兼顾
- 审计与检查
- 安全意识提升
- 共享交流

分享完毕