SKY-GO
360 汽车信息安全实验室

智能网联汽车信息安全建设最佳实践

Best Practices of Building Intelligent Cybersecurity Vehicle

360 智能网联汽车安全实验室介绍：

360 智能网联汽车安全实验室（360 天行者团队）是由全球最大的互联网安全公司 360 组建，隶属于亚太安全创新高地—360 安全创新中心，是国内首支专注于汽车信息安全研究领域的顶级安全团队。以跨行业协同为发展理念，目前已经与北京航天航空大学、浙江大学、特斯拉、长安汽车、比亚迪、长城、Visual Threat 等研究机构、汽车生产企业和汽车信息安全相关厂商展开了深度合作和共同研究，组建了多个联合实验室和研究院，建立中国的汽车信息安全研究集群，全面进行基于实战和面向未来的汽车信息安全研究，全方位保护万物互联时代的汽车信息安全。

前言

随着互联网、人工智能、云计算和大数据等技术的应用，今天汽车的智能化、联网化程度越来越高，汽车已经变成名副其实的万物互联时代的智能终端设备。汽车的信息安全已经成为互联网安全的重要组成部分，用于控制汽车的手机应用、内部复杂的传感器控制系统、软件漏洞都有可能成为新的风险点，黑客针对汽车发动大规模攻击只是时间问题。除了可能的远程攻击、未授权监控并获取汽车定位数据等信息外，同时，汽车制造商和车载软件厂商在安全问题的责任划分上，也会对智能汽车的发展产生深远影响，汽车信息安全既主动安全、被动安全、功能安全以后将成为汽车领域中第四大安全问题。

360 结合多年互联网安全经验、汽车安全研究经验及整车厂的安全工作情况，结合《美国交通部现代汽车信息安全最佳实践》编制适用于国内汽车工业企业信息安全建设的最佳实践指南，详细阐述了全生命周期的安全方法，指导企业如何有效开展信息安全生态建设。

目的

本文档的目的，“智能网联汽车信息安全建设最佳实践”旨在识别，解释和定位与关键安全技术，确定相关的安全管理要求。

结合汽车工业企业的业务特性，在联网汽车全生命周期开发过程中，各阶段划分各自风险管理责任，如不能及时解决各阶段的风险问题，风险将传递到下一阶段。因此，如何全局掌控风险，如何避免各阶段风险管控脱节，并有效地管控，则成为汽车工业企业关注的问题。要彻底解决安全问题，需要在业务全生命周期都进行风险识别和处置，通过定义各阶段的关键安全举措及安全技术，使安全风险控制措施 100%覆盖所有业务活动。安全提前介入改变传统安全工作疲于被动处置的低效率而高成本的状态，帮助企业应对到潜在的威胁，权衡存在的风险与威胁，提升用户的安全驾驶体验。

适用范围

本指南定义了智能网联汽车全生命周期的总体安全，适用于指导汽车工业企业、规范供应商、配合第三方安全公司提供业务运行过程中的全方位防护，识别和解释如何使用关键安全技术和过程，评估和减轻与安全和隐私威胁相关的风险。

最佳实践理念与方法

智能网联汽车将汽车内部不同类型的控制器和传感器与互联网系统，业务流程，分析学和人员相连接，通过智能化技术来降低交通事故率。智能网联汽车与传统的汽车系统不同，它们广泛地连接到其他系统和人员，增加了系统的多样性和规模。然而在汽车关键控制系统的安全性依赖于物理分离和网络隔离技术，以及对于关键控制系统中设计和访问规则的复杂性。但是智能网联汽车对于

智能功能需求的开发以及网联程度的接入，打破了汽车控制系统原有的封闭生态，引入了很多来自互联网的安全风险，这些风险可以通过安全的设计，分析和审查，深度的测试和培训来缓解。

360 智能网联汽车信息安全框架，该框架以风险为导向，IT 与 OT 的信任链关系为基础，安全策略为指导方针，从安全配置管理、安全监控与分析、通信与接口防护、终端防护、数据防护贯穿整个车联网的组件控制、传感器控制、应用系统、数据流、操作系统、云端系统，并分别介绍了各层面的安全举措，从而达到车联网系统面临威胁时，可以持续监测、协同联动、快速响应。

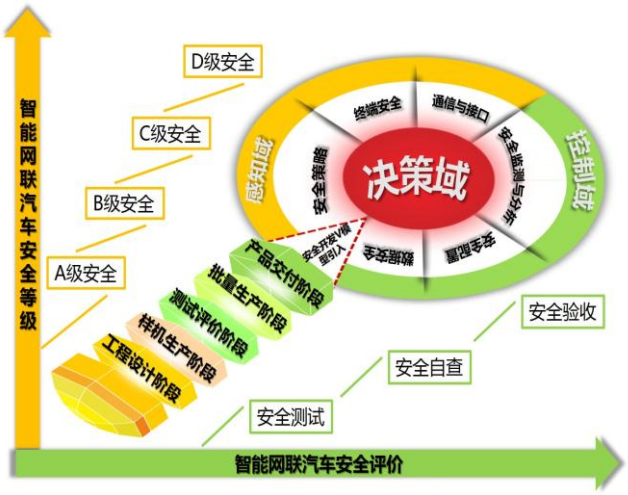

图 2 全生命周期关系视图

图 1 360 汽车信息安全生命周期安全管理

360 智能网联汽车信息安全框架，该框架以风险为导向，IT 与 OT 的信任链关系为基础，安全策略为指导方针，从安全配置管理、安全监控与分析、通信与接口防护、终端防护、数据防护贯穿整个车联网的组件控制、传感器控制、应用系统、数据流、操作系统、云端系统，并分别介绍了各层面的安全举措，从而达到车联网系统面临威胁时，可以持续监测、协同联动、快速响应。

各层面关键安全举措如下：

◎ 终端安全防护：终端访问控制、终端监控分析、终端安全配置管理、终端完整性校验、终端身份识别、终端权限检测、终端环境安全、终端数据安全以及终端安全策略。

◎ 通信安全和接口安全：网络安全配置、网络监控分析、接口安全、安全通信、加密传输、流量控制及安全策略。

◎ 安全监控与分析：终端与接口监控、安全日志监控、供应链监控、行为分析、规则分析、积极预防、检测与恢复、调查取证。

◎ 安全配置管理：安全操作管理、终端身份管理、终端配置管理、通信与接口管理、安全管理、安全变更管理、数据安全管理及安全策略。

◎ 数据安全防护：终端数据防护、通信数据防护、配置文件防护、监控数据防护、数据

◎ 安全策略：配置管理策略、监控与分析策略、通信与接口策略、终端安全策略、数据防护策略、业务安全目标、业务威胁分析

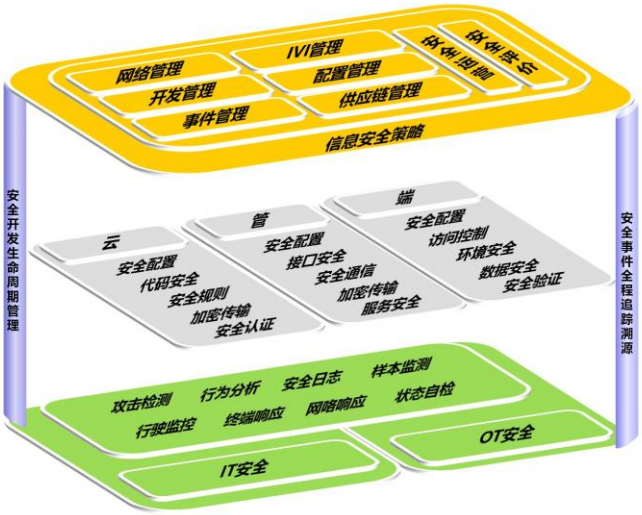

图 3 360 汽车信息安全技术框架

项目策划阶段

智能网联汽车的前期策划是汽车研发和汽车项目立项的重要环节，汽车工业企业为了预防事故，也为分析事故，应自上而下抓安全责任、抓安全责任落实，明确安全责任，着力建立、完善各级各类人员的安全责任制。汽车工业的安全责任制是安全生产的灵魂，认真制订安全责任制、认真执行安全责任制是确保企业安全的关键和灵魂所在。确实把责任落实到实处，安全生产的各项制度、措施、活动计划的有效贯彻执行就有了可靠的保证，安全管理就一定能取得实效，安全生产就有可靠保障，智能网联汽车才能安全稳定。

建立安全组织

汽车工业企业须建立信息安全常设领导机构，全面负责智能网联汽车的信息安全工作。该机构应由企业最高领导负责，各相关部门领导组成。

安全领导机构应为智能网联汽车的安全管理指明清晰的方向，并提供强有力的管理层支持。安全领导机构应通过合理的承诺和充分的资源配置，来推进整个智能网联汽车的信息安全工作。

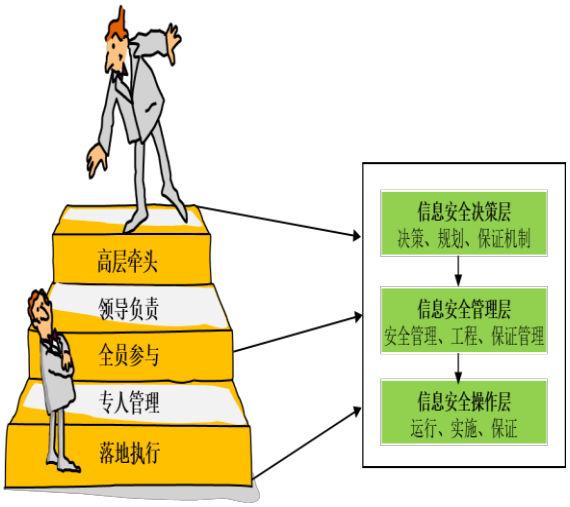

图 4 安全组织示意图

明确安全职责

为明确安全责任，划分（界定）安全管理与具体执行之间的工作职责，汽车工业企业必须建立安全责任制度。安全责任分配的基本原则是“谁主管，谁负责”。企业拥有的每项网络与信息资产，必须根据资产归属确定“责任人”。“责任人”对资产安全保护负有完全责任。“责任人”可以是个人或部门，但“责任人”是部门时，应由该部门领导实际负责。

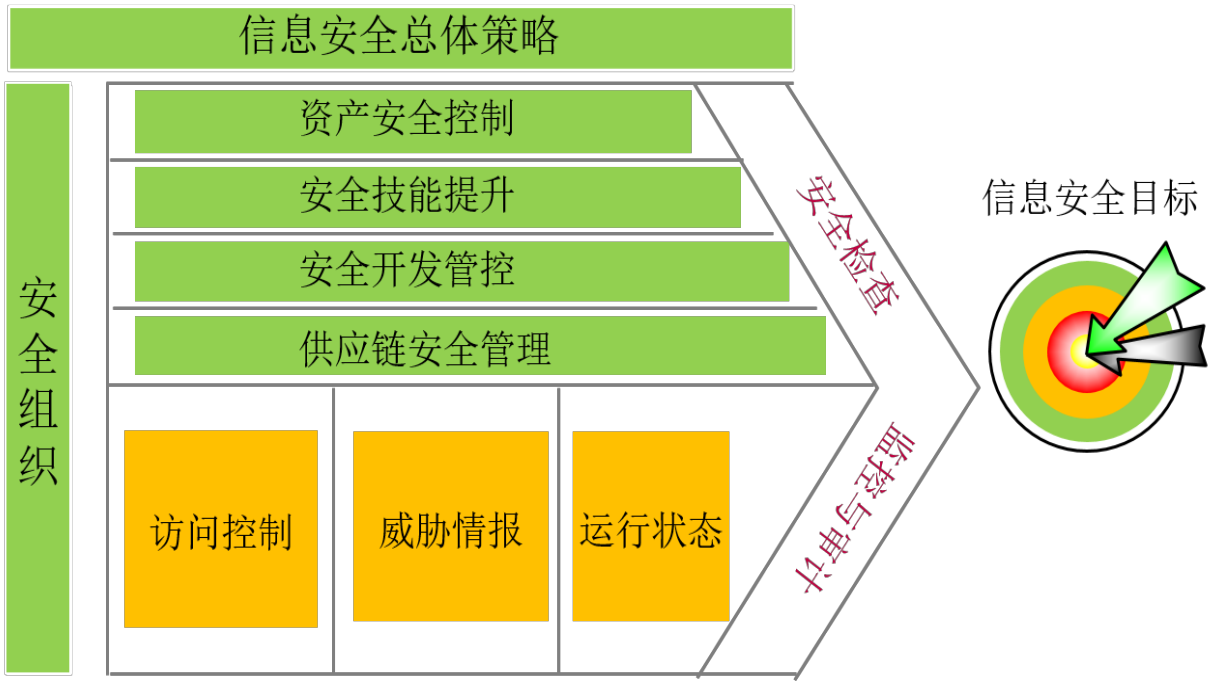

图 5 安全责任与目标示意图

汽车全生命周期安全管理

信息安全是需要建立在设计阶段而不是在开发最后再进行考虑。设计之初考虑信息安全需要一个合适的生命周期过程，这个生命周期过程包括从概念阶段到生产、运营、服务和废弃阶段。SAE J3061 提供了一种可用于汽车工业企业特定过程的全生命周期流程框架，该流程框架类似于在 ISO 26262 公路车辆功能安全中描述的流程框架。这两个过程虽然不同但却有关联，为了维持组织安全过程输出和网络安全过程输出的持续性和完整性，二者都需要集成通信。一个组织可以通过两个过程间适当等级的相互作用来任意维持分离的过程，或者尝试直接集成这两个过程。

确立信息安全目标

评估类别	汽车安全评价类型		汽车网络安全等级 VCSL 安全评价			
			VSCL A	VSCL B	VSCL C	VSCL D
安全设计	TAP:安全威胁和风险分析		TAP1	TAP2	TAP3	TAP4
	SDA:安全设计分析		SDA1	SDA2	SDA3	SDA4
	DEV:安全扩展分析		--	--	DEV1	DEV2
	DEP:安全部署及可行性分析		--	DEP1	DEP2	DEP3
测试评价	VPT:渗透测试		VPT1	VPT2	VPT3	VPT4
	VUL:漏洞扫描		--	VUL1	VUL2	VUL3
	SFT:系统模糊测试			SFT1	SFT2	SFT3
	控制安全	CEA:总线终端攻击	--	--	CEA1	CEA2
		TSA:传输安全验证	--	--	TSA1	TSA2
		ORA:组织架构梳理	--	--	ORA1	ORA2
平行对标	自动驾驶等级(J3016)		L1-L2	L2-L3	L3-L4	L4-L5

策划阶段需要确定汽车信息安全的目标，结合研发设计车辆的功能需求，定义所谓的“汽车网络安全等级”，360 智能网联汽车安全实验室在以往的测试评价中会定义四个安全测试级别，从而决定在安全设计和开发阶段中的工作范围。

VCSL(ICVehicle Cyber Security Level) 智能网联汽车网络安全等级分为四类，后续会根据 SAEJ3016 内部对自动驾驶等级的对于到不同的信息安全等级上。建议 DA 级别且不联网的汽车可以参考使用 VSCL A 级别要求；PA、CA 级别需要做到 VSCL B,或者 VSCL C 级，因为这两个

级别汽车的监视、责任还是归属于驾驶员的。能够在发生攻击的情况下由人工介入，而 CA 级别是不需要人员来监视的则更最好能够实现 VSCL C 级的安全要求。对于 HA、FA 的汽车的控制、监视、责任都由系统来负责，所以要求达到 VCSL D 级别。

工程设计阶段

汽车工程设计阶段需要对设计的汽车进行功能划分，根据功能特性进行威胁建模，完成威胁建模后。要从计划阶段就开始导入信息安全对策,根据智能网联汽车的关键技术，如图定义关键信息安全技术，如特定访问权限、密钥安全管理、OBD 接口安全、FOTA 安全管理、车机安全管理、网络服务安全、安全边界划分、车内安全通讯、安全日志、接口安全等这一点非常重要。在这一阶段,汽车的理念、配备的功能都将明确,需要考虑各项功能安全性的重要程度,为与重要程度相符的对策分配预算。而且,在选择车辆配备的功能然后转交给开发阶段的时候,一定要提交包括信息安全在内的需求。

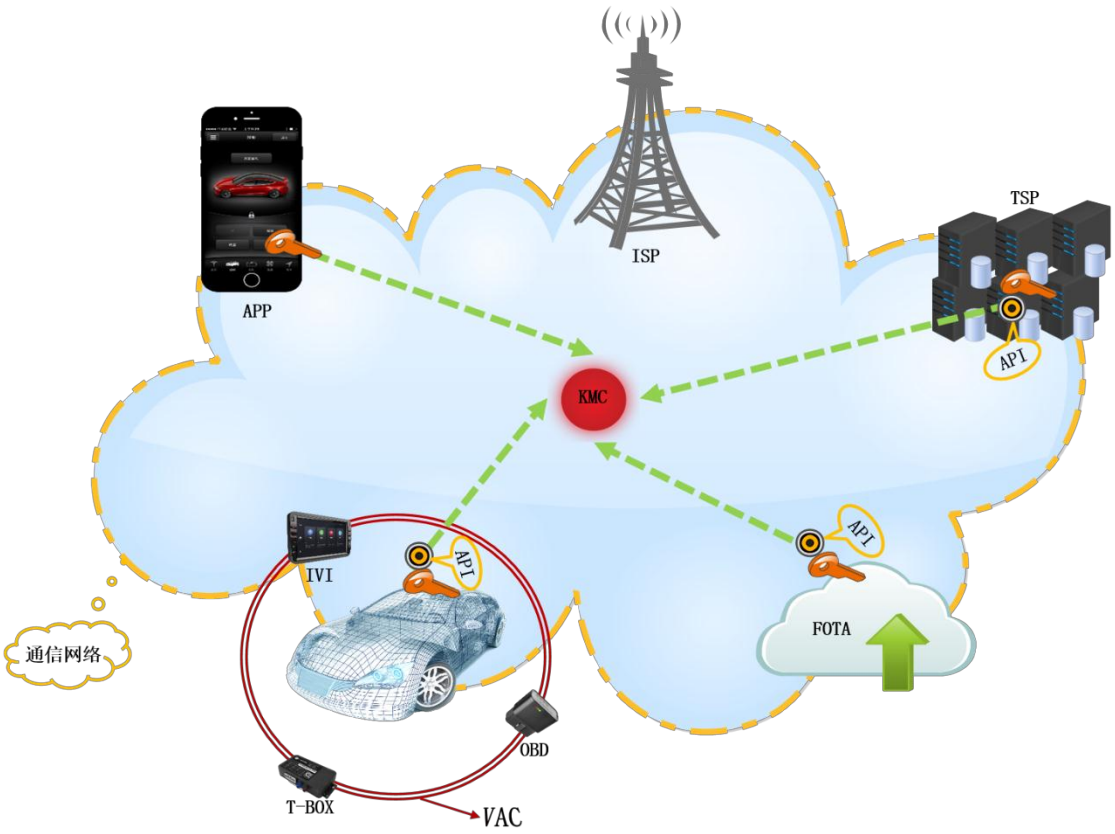

图 6 关键技术架构图

特定访问权限

开发人员具备 ECU 的最高权限，通过调试端口或串口可随便访问 ECU。应针对具体的开发需求，开放特定的访问权限，可根据实际场景，划分普通权限、限制权限或高级限制权限；根据确定的权限等级，进行对应的权限管理。包括: 如果行驶状态为停止，运行状态为未运行，则将权限等级确定为普通权限；或者，如果行驶状态为正在行驶，运行状态为未运行，则将权限等级为限制权限；或者，如果行驶状态为正在行驶，运行状态为运行关键任务，则权限等级为高级限制权限。

密钥安全管理

密钥管理是对密钥材料的产生、登记、认证、注销、分发、安装、存储、归档、撤消、衍生和销毁等服务的实施和运用。密钥管理的目标是安全地实施和运用这些密钥管理服务，因此密钥的保护是极其重要的。

密钥管理程序依赖于基本的密码机制、预定的密钥使用以及所用的安全策略，密钥管理还包括在密码设备中执行的那些功能。

OBD 接口安全

OBD 是车载智能设备的核心，其通过接口读取汽车运行状况数据，从数据维度、车型维度、时间维度、地域维度等多角度，深入分析、比较用户驾驶行为，发现驾驶行为共性和个性，甚至对潜在的一些故障风险给出预警。OBD 数据采集及控制权限应规范限制，如：修改 ECU、控制刹车、通过修改 OBD 数据来切换车辆的状态等，可针对不同的操作行为配置时间阀值,对 OBD 接口接入终端设备进行身份认证。

FOTA 安全更新

空中升级（Over-the-air）首当其冲的是安全问题。OTA 在端与端之间进行，类似云服务器等升级来源在一端，车辆的信息娱乐系统在另一端。因此，就相当于这两端都在与一个“确定的可信机构”进行密钥交换。在 OTA 升级前需先验证安全漏洞的有效性，避免由于升级安全漏洞而导致系统不可用，如果安装失败了，系统必须能够激活“恢复(restore)”功能，以便能够恢复至升级前的状态；“清除(removal)”功能，将系统恢复至升级前的状态。并定级验证 fota 的代码安全。

车载系统安全管理

针对车载操作系统和智能网联汽车的安全防护产品，应实现车机杀毒、清理、加速、联网防火墙、车身控制监控、车机 root 检测、车机 adb 调试检测，并对车机体检结果分析、车机联网控制行为、车机应用调用行为、车机 root 检测分析、汽车控制数据分析。

网络接入服务安全

车载终端、T-BOX 等汽车网络接入设备运行的网络服务应该仅开放必要的基本功能和服务，保护端口，以防止未获授权者使用。IP、端口将成为黑客利用的载体，应删除任何不必要的网络服务。

安全边界划分

安全边界划分是改善安全重要的措施，充分的分析威胁可利用载体攻击智能网联汽车的

途径，并通过逻辑及物理隔离限制每个组件、车载网络、车载接口等，可采取黑白名单的方式进行有效控制。

车内安全通信

车载网络运行的关键数据能立即影响智能网联汽车控制系统，应具备欺骗检测能力，防止由于正常指令而导致错误的执行动作，严格隔离车载网络与非信任网络的通信，且重要安全通信须提供身份验证及消息验证机制。

安全日志要求

智能网联汽车业务需要有能力在安全审计跟踪日志中记录车载网络、车机、APP、TSP等里发生的安全相关事件。应严格限制日志的访问权限，实现细粒度审计规则，其中包括汽车控制信号、驾驶行为、连接行为、操作行为，完整的安全日志可以有效分析安全性，以及审核内部人员的合规性，全面呈现整体安全趋势。

API 接口安全

智能网联汽车业务整体架构开放接口较多，首先确保接口编码安全，接口间通信应采用加密方式，通过数字证书进行安全认证，必要时可通过安全规则进行限制，并实时监听接口,有异常及时发现。

样机生产阶段

样机在生产制造阶段,汽车厂商及零部件厂商开始设计硬件和软件安装到汽车上,这是采取信息安全对策的最重要环节。

汽车工业企业在安全开发过程中应参照《SAE J3061》、《Security Development Lifecycle》、《ISO 26262》的高级指导原则控制安全开发风险。充分考虑安全需要一个合适的生命周期过程，这个生命周期过程包括从概念阶段到生产、运营、服务和废弃阶段。应当明确安全目标、可能面临的风险，并且将相应的计划整体构形成规划文档。应考虑如何在开发流程中集成安全性，找出关键的安全性对象，以及在尽量提升代码安全性的同时尽量减少对计划和日程的影响，同时加强供应商产品

的质量安全管理。在此过程中，需要考虑如何使安全功能和保证措施与供应商产品相互集成。

供应商质量监控

智能网联汽车业务承载多个零部件，涉及多个层面，其中承载大量的代码程序。安全缺陷是软件产品中存在的可能导致软件与其设计目标不一致，并且可能违反软件文档所定义的安全政策的软件缺陷。

这些程序大部分都是由供应商实施开发，对于供应商提交的产品管理，汽车企业应首先应慎重选择应用程序编程语言，尽量选择安全编程语言，并形成全编程基本规则与手册要求供应商参考安全框架进行开发，在系统编码的过程中，提高安全编码质量和安全性，避免出现智能网联汽车业务的安全隐患和漏洞。

安全开发控制

安全开发控制过程中，360 汽车安全实验室推荐使用汽车行业、软件开发领域常用的 V 字开发模型，在整个过程中需要重点关注安全需求的提出，安全功能的验证和回归测试。同时各组织开发过程中（从概念阶段到生产、操作、服务和废弃阶段），将网络安全考虑在信息物理汽车系统中。

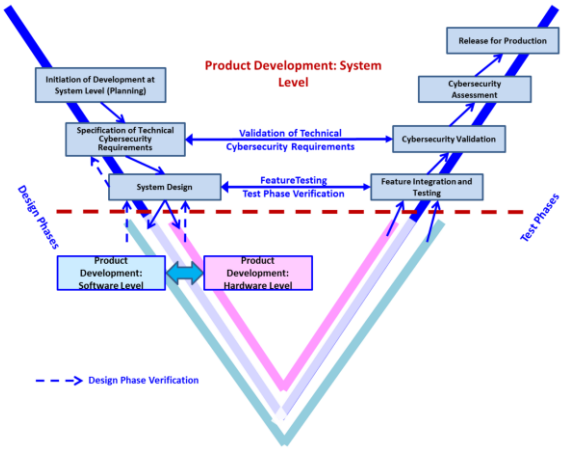

图 7 汽车安全开发框架

智能网联汽车的安全设计和构建时，应遵循安全开发风险管理体系的相关规定执行，提升产品成熟度过程能力。应当根据业务的特点，规划全局性的信息系统应用安全架构，明确系统各个模块之间、应用系统与操作系统、

数据库之间、应用系统与其他软件之间的接口关系以及相关的安全需求，安全开发流程必须遵照执行。

软件开发中，应当详细检查输入数据长度以免发生缓存区溢出，编程中防止隐蔽通道的产生，检查数据类型的正确性，保证检查点不会被用户绕过，语法验证，执行校验和验证等。还应当测试可能的各种攻击情景，弄清楚对代码的攻击或者以非授权的方式修改数据是如何进行的。应该由成对的程序员执行互相的调试和代码检查，一切过程都应该有文档记录，最终保证安全功能完成开发要求。

测试评价阶段

试验工程既包括性能试验和可靠性试验，也要包括安全性试验，智能网联汽车的安全性试验是整车关键元素，贯穿在信息系统的整个生命周期中。汽车工业企业在安全开发过程中应参照《信息安全技术 信息安全风险评估规范 GB/T 20984 2007》开展风险评估以确定系统的安全目标，并通过渗透测试和代码审计深度分析代码安全性，以确定系统安全措施的有效性，确保安全保障目标始终如一得以坚持。

全面风险评估

安全风险评估可以应用于整个智能网联汽车生态链，也可应用于 TSP、APP、TBOX 等特定系统组件或服务。通过标准统一的评估程序和方法，量化安全风险，确定安全风险的危险级别，从而采取合理措施防范或降低安全风险。应对新出现的威胁和漏洞，评估现有控制措施的有效性及合理性，必须周期性地进行安全风险评估并调整控制措施，且应在不同的层面进行，为高风险领域优先分配资金、人力等资源。

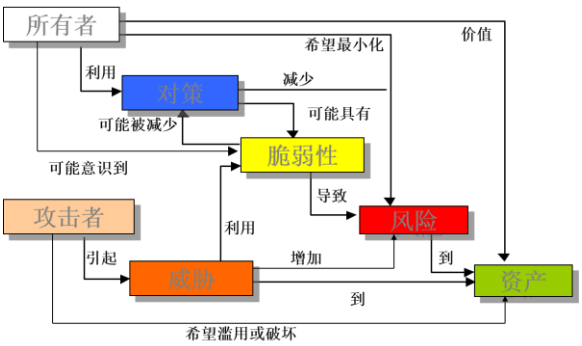

图 8 风险评估示意图

专项渗透测试

通过模拟汽车黑客操作执行对汽车进行整体破解，包括但不限于车联网 APP、TSP 包括 CP/SP 的接入系统、T-BOX 的整体层面、IVI 的系统、应用及接口、车联网控制协议、总线协议、汽车网关、汽车传感器、无线钥匙验证模块、自动驾驶路径规划系统，主要发现由于编码错误、系统配置错误或其他运行部署弱点导致的潜在漏洞。

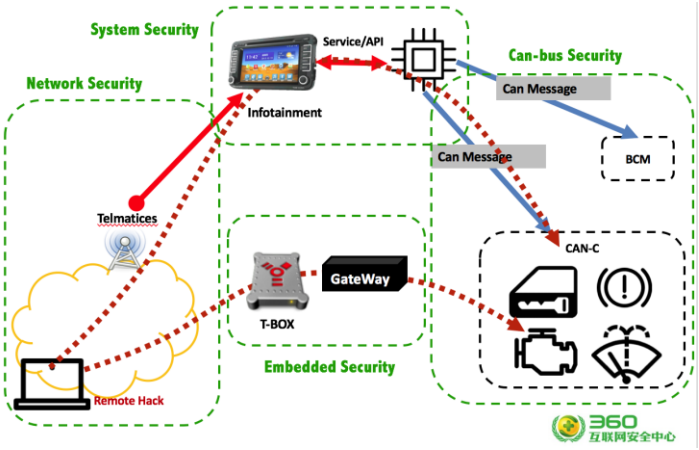

图 9 渗透测试流程图

适配安全加固

针对智能网联汽车 APP 端可能存在的反编译、易篡改、易注入等问题，通过加固保护核心代码和业务逻辑不泄露，加强基础平台应用的安全性。

定期自查

车厂应建立内部审核程序和网络安全的相关操作文档。周期性的针对汽车设备零配件供应商进行自查。以满足整车厂网络安全规范要求，约束供应商信息安全要求。

批量生产阶段

面向市场需求开展批量生产时，汽车工业企业须加强关键技术环节的安全性验收工作，其中包括 CAN-BUS、FOTA、APP、TSP 平台等安全验证，衡量现有安全措施的整体状况，验证是否应该继续执行现有安全措施，确保现有的安全措施符合企业内部的安全标准、策略和要求。

产品交付阶段

智能网联汽车及面向互联网提供的服务平台投放市场到实际使用，汽车工业企业须从两方面着手安全，一方面，真正做到安全事件提前预警，及时获取安全预警信息的来源，确保信息来源的准确性、全面性，与第三方合作伙伴协同全面分析预警信息的严重程度、紧急程度和发展趋势，与实际运行环境相结合，确定安全预警信息的适当防护措施；另一方面，要真正的将安全事件预防、发现、处置到威胁情报共享全环节的打通，踏实落地的安全运营，缩短事件实际发生到响应的时间差，提升检测效率，提升数据化监测能力，为后期决策奠定基础，持续改进。

实时漏洞预警

运用技术手段对智能网联汽车资产进行全面的安全漏洞监测、可用性、篡改、敏感词监测并且结合安全运营中心以及网络安全设备产生的数据进行态势分析，周期性进行智能网联汽车资产的漏洞扫描与验证，及时跟踪来自互联网发布的行业信息安全预警信息，实时了解安全态势和安全问题。

数据安全运营

通过实时漏洞预警可以有效的动态感知网络中的威胁。而发现威胁，才是安全运营的目的所在。将系统数据和控制数据进行全面关联分析，能发现和定位恶意行为，对受害车辆及攻击目标实现定位，最终判断入侵途径及攻击者背景。

安全事件响应

定义检测、响应恶意攻击事件并限制后果的策略，焦点在于智能网联汽车业务或网络遭受影响时信息安全的响应。事件响应是短暂的、小范围的、现场的，这和以业务连续性和灾难恢复为代表的其他应急计划有很大区别，后者更关注面临大的灾难时组织如何恢复并维持系统操作和业务，以免中断造成的严重后果。

结论

攻击智能网联汽车有可能导致环境的损害，人身的伤亡或人命的损失。与此同时，还有隐私数据泄露的可能，中断操作和破坏系统等。攻击汽车联网系统的影响力是广泛的，同时还会导致品牌和声誉受损。汽车信息安全不是单凭汽车工业企业的努力就能做到的。还要从不同的企业角色来共同支撑汽车信息安全生态，总体提升国内智能网联汽车信息安全能力，使得我国自主品牌汽车在国际上更具备竞争力。

相关引用

- ✓ ISO 26262 标准根据安全风险程度对系统或系统某组成部分确定划分由 A 到 D 的安全需求等级（Automotive Safety Integrity Level 汽车安全完整性等级 ASIL），其中 D 级为最高等级，需要最苛刻的安全需求。
- ✓ SAE J3061 识别和评估网络安全威胁，并将网络安全设计理念渗透到信息物理汽车系统整个生命周期开发过程中，提供了一种信息安全流程框架和指南。
- ✓ IIC 工业物联网如何使用技术和过程来识别，评估和减轻与安全和隐私威胁相关的风险。
- ✓ 美国交通部 DOT 汽车信息安全白皮书探索并采取方法共同应对可能出现不合理安全或安全风险的网络威胁。这包括制定最佳实践，以确保机动车辆的生态系统安全。

360 车联网安全中心于 2016 年 11 月 24 日在上海举行的 SyScan360 亚太前瞻信息安全技术年会上宣布正式成立，该中心由 360 公司联合多家高校、汽车及零部件企业组建，是国内第一个专业从事汽车及车联网的安全保护的跨行业合作机构。

360 车联网安全中心旗下拥有 2 个汽车信息安全攻防研究团队、3 个实验室、1 个联合研究院和一个汽车信息安全专业安服团队，推出了 360 汽车卫士、CANPICK 等多个汽车安全防护和检测产品，基于安全大数据的 360 车联网安全运营平台目前也已经投入运行，这是国内第一个进入时效运营的汽车信息安全综合运营平台，可以向汽车行业和网络安全行业输出车联网安全威胁情报。