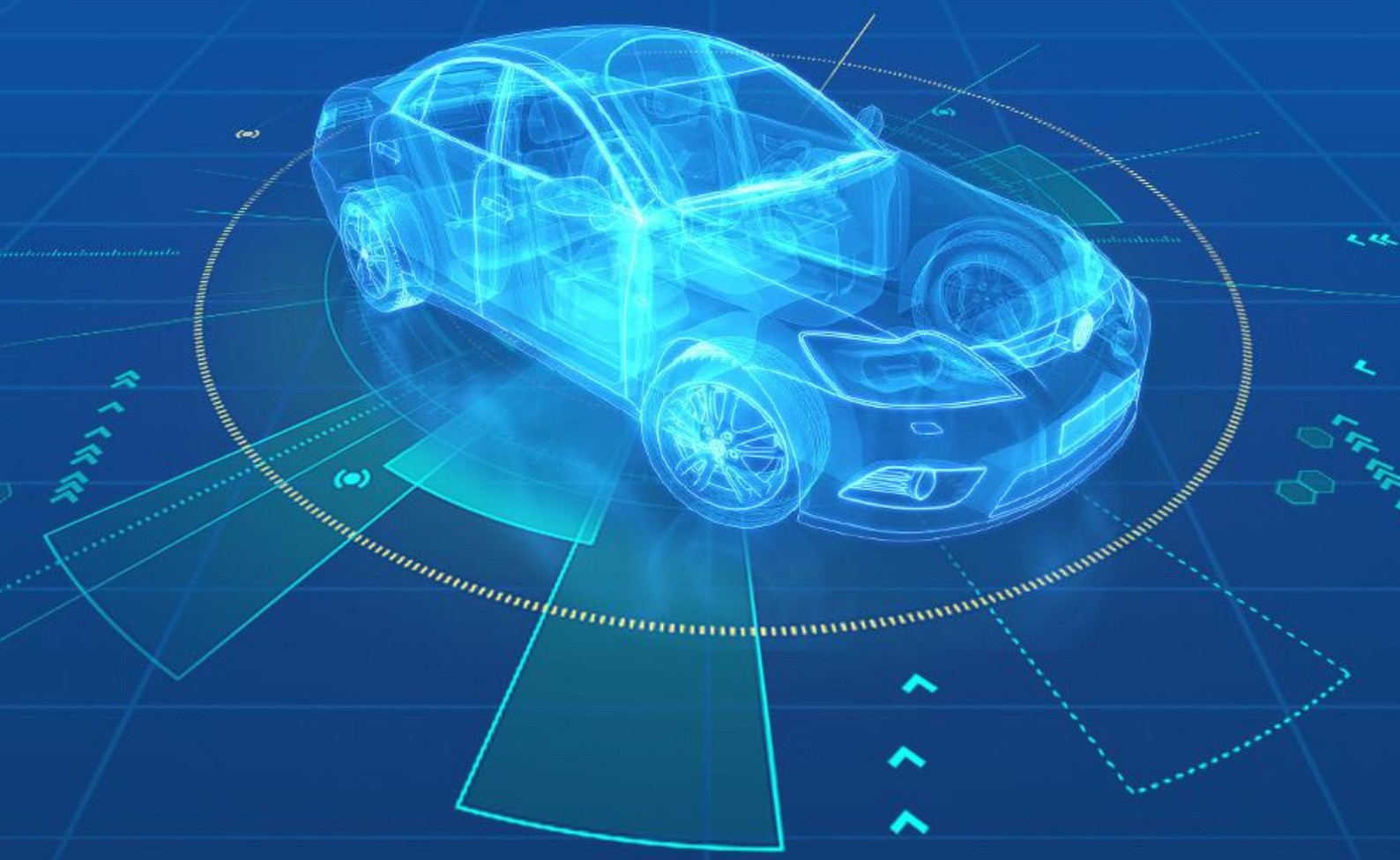
腾讯安全 | 腾讯智慧出行 | 腾讯标准 Tencent Standard

车联网数据安全体系

建设指南



2021年10月

目次

前　言

本指南旨在客观提出数据安全体系建设的一些建议，仅供参考。

本指南内容可能涉及专利，本指南的发布机构不承担识别这些专利的责任。

本指南由腾讯云计算（北京）有限责任公司提出并归口。

本指南起草单位： 腾讯云计算（北京）有限责任公司、北京中安星云软件技术有限公司、北京芯盾时代科技有限公司、杭州世平信息科技有限公司、上海铠射信息科技有限公司、理想汽车

本指南主要起草人：刘海洋、张敏、宋辉、尹晓东、顾益宇、孙菲、朱新新、张文献、张明全、戴平、倪平、武杨、徐永太、贺天明、崔卓

引 言

伴随着以人工智能、5G、云计算、边缘计算、大数据、区块链、物联网等为代表的新一代信息技术向工业领域的不断渗透，汽车行业的信息安全问题日益凸显。汽车智能化、网联化程度逐步提高，车辆开放连接逐渐增多，相关设备系统间数据交互更为紧密，网络攻击、木马病毒、数据窃取等互联网安全威胁频繁发生。一旦车载系统和关键零部件、车联网平台等遭受网络攻击，可导致车辆被非法控制，造成财产损失，还会对数据安全、人身安全、社会安全等产生严重威胁。网络安全已经成为车联网产业健康发展的基础和前提，加强我国汽车行业的工业控制系统信息安全防护建设势在必行。

汽车作为重要的出行工具的同时，车联网也承担着传输和处理大量数据的工作。车辆数据的交互和安全保证离不开车联网，车联网安全运行的关键在于数据安全，因此，如何在保障安全的基础上，促进数据的充分利用，满足合规要求，是车联网领域需要面对和亟待解决的问题。

1. 范围

2. 规范性
引用文件

3. 术语
和定义

1 范围

本指南根据车企对数据使用场景的深入分析，结合相关法律法规、国家及行业标准，提出一些具体的方法和建议。

本指南适用于车企车联网业务中的用户数据流转与使用、车机数据流转与使用、大数据平台、数据提取等车联网数据场景。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《汽车数据安全管理若干规定（试行）》

GB/T 35273—2020《信息安全技术 个人信息安全规范》

YD/T 3751—2020《车联网信息服务 数据安全技术要求》

YD/T 3746—2020《车联网信息服务 用户个人信息保护要求》

《信息安全技术 网络预约汽车服务数据安全指南》（征求意见稿）

3 术语和定义

3.1 车联网 vehicle networking

通过装载在车辆上的传感器、车载终端及电子标签提供车辆信息，采用各种通信技术实现车与车、 车与人、车与路互连互通，并在信息网络平台上对信息进行提取、共享等有效利用，对车辆进行有效的 管控和提供综合服务。

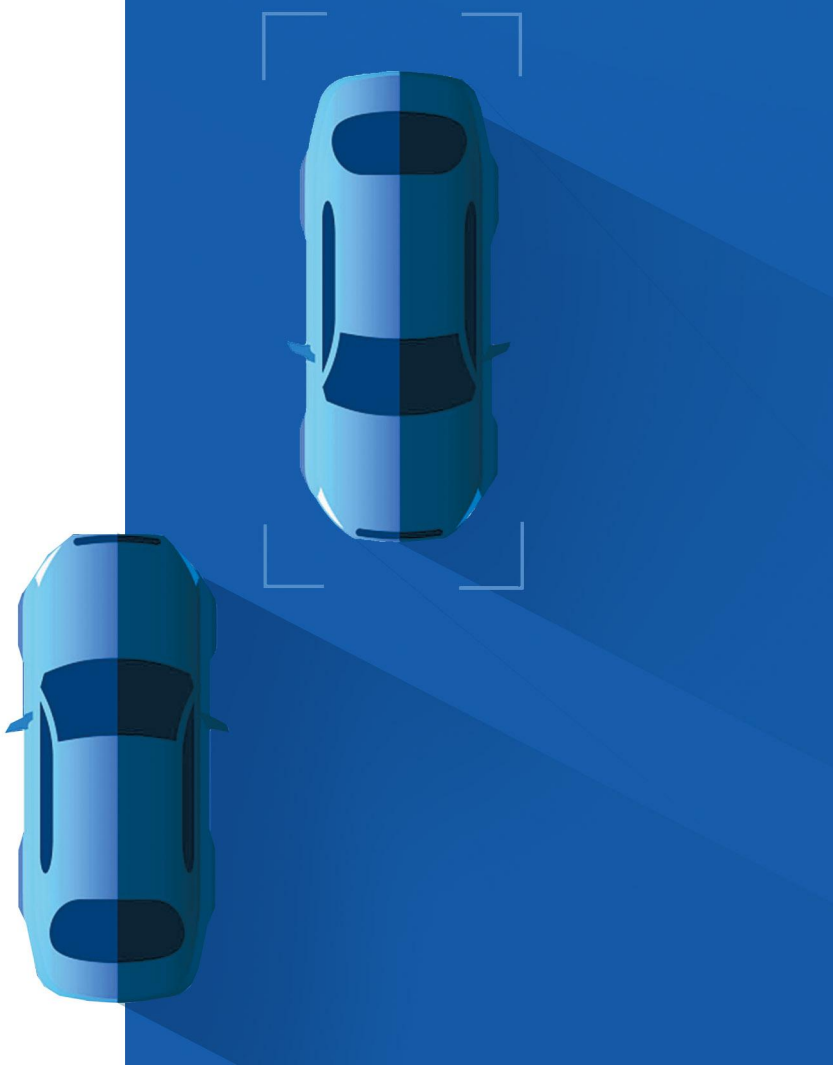
3.2 数据资产 Data Assets

由个人或企业拥有或者控制的，能够为企业带来未来经济利益的，以物理或电子的方式记录的数据资源。

3.3 车联网数据 Internet of vehicles data

车联网数据指涵盖车联网信息服务过程中的除了用户个人信息以外的所有数据，包括但不仅限于来自车辆、移动智能终端、路边设施和车联网服务平台等载体相关的数据。

4. 车联网数据安全需求



4 车联网数据安全需求

随着车联网产业的发展，其数据安全也受到越来越多的重视。一方面车联网是汽车、电子、信息通信、道路交通运输等行业深度融合的产物，其涉及的数据种类多、数据量大、数据处理链条长、数据主体多等特点，导致其数据安全保护工作复杂、难度大。另一方面，车联网数据一旦泄露或被滥用，不仅可能造成经济财产损失，还有可能造成人身伤害，甚至影响国家安全。如车联网核心数据车辆控制信息，即用户信息与车机信息绑定后，为实现智能化用车，需要通过移动终端对车辆进行控制，一旦发生攻击或泄露，车辆将会被非法控制，形成恐慌。因此，车联网企业在满足相关合规要求的同时，还要考虑数据的防泄露、防滥用问题。

4.1 合规

近年来，我国在大力推动车联网产业发展的同时，始终强调数据安全保护工作的重要性，提出了一系列的数据安全要求。

网信办于 2021 年 8 月 20 日发布《汽车数据安全管理若干规定（试行）》于 2021 年 10 月 1 日起实施，该规定对包括汽车设计、制造、服务企业或者机构处理个人信息和重要数据提出了一系列的规定。

工信部于 2021 年 8 月 12 日发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》中指出智能网联汽车生产企业应依法收集、使用和保护个人信息，实施数据分类分级管理，制定重要数据目录，不得泄露涉及国家安全的敏感信息。在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关规定在境内存储。因业务需要，确需向境外提供的，应向行业主管部门报备。

2020 年 2 月，国家发改委、中央网信办、科技部、工信部等 11 个国家部委联合下发了“关于印发《智能汽车创新发展战略》的通知”，明确指出要加强数据安全监督管理，建立起覆盖智能汽车数据全生命周期的安全管理机制，明确相关主体的数据安全保护责任和具体要求。实行重要数据分类分级管理，确保用户信息、车辆信息、测绘地理信息等数据安全可控。完善数据安全管理制度，加强监督检查，开展数据风险、数据出境安全等评估。

根据《中华人民共和国网络安全法》（以下简称《网络安全法》）第二十一条的要求，国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

民法典规定，信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。

信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。

针对 APP 违法违规收集个人信息的合规方面，应及时梳理 APP 权限、个人信息收集、使用、处理等合规现状，找到差距，及时对齐合规要求。

针对关键数据的保护，需要对关键信息进行识别，并进行必要的保护，包括但不限于加密、脱敏、超期后销毁等。

除以上法律法规外，通信行业标准 YDT 3751-2020《车联网信息服务 数据安全技术要求》和 YD/T 3746-2020《车联网信息服务 用户个人信息保护要求》等对车联网信息服务数据安全和用户个人信息保护提出了要求。

4.2 防泄露

车联网数据的应用场景，从数据采集到数据传输、处理、存储等，都需要合理的安全措施进行防护，防止数据泄露。数据泄露不仅对汽车企业名誉带来影响，对于车主的权益也会造成损害，甚至造成人身伤害。

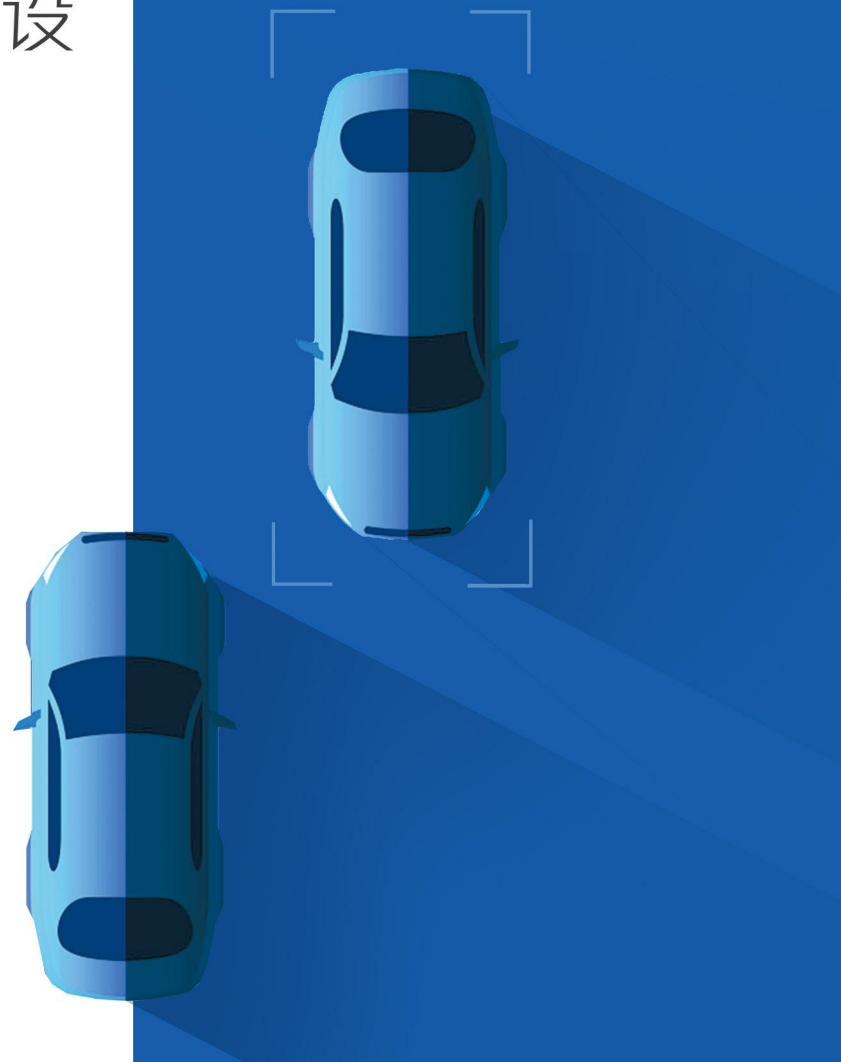
4.3 防滥用

车联网涉及海量数据，且传输链条长，涉及相关方众多，摸清数据资产和数据流转，掌握数据使用情况，防止滥用，包括对过期或不再使用数据的去标识化处理等，对数据安全保护至关重要。

5. 总体思路

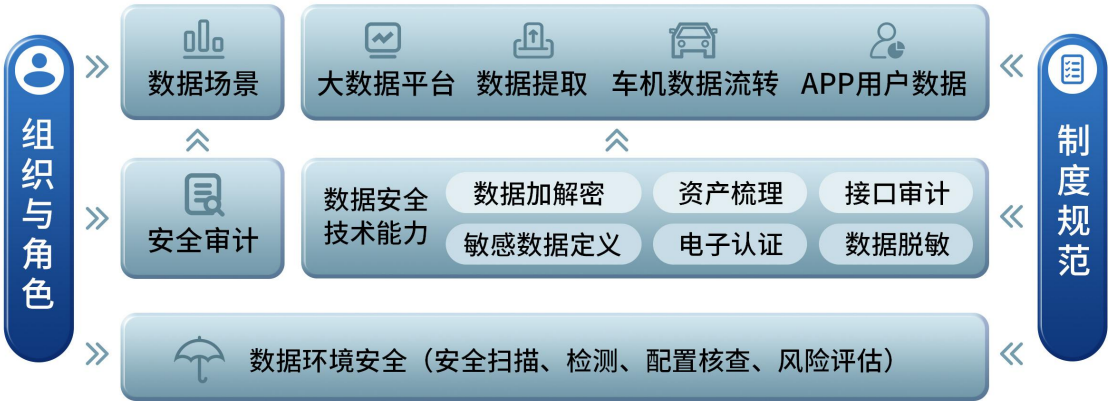
6. 组织建设

7. 制度体系建设



5 总体思路

由于数据安全与业务息息相关，传统的单点风险解决方式已不再适用，车联网又是新兴行业，具有业务迭代快、互联网暴露面大的特征，因此，建议车联网企业的数据安全防护采用体系化方式进行建设，包括组织、制度、能力、审计四个维度，如下图所示：



一、 组织建设

数据安全管理角色需要有一定的权利，以及获得高级别管理者的授权或直接由其担任，才能顺利开展数据安全管控工作。因此，确立组织和角色是开展数据安全体系建设的前提。

二、 制度规范体系

制度与规范是日常数据安全管理工作的标准，是数据安全技术运用的依据，制度与规范要符合实际状况，切实可行、覆盖全面。

三、 技术保障能力建设

结合车联网数据场景特点，建议建设能力包括数据加解密、资产梳理、接口审计、敏感数据定义与识别、电子认证、数据脱敏等。并通过平台的方式对能力进行统计管理和使用；

四、 安全审计

安全审计一方面可以在海量数据访问过程中及时发现违规操作和疑似风险，同时还可以稽核数据安全要求的执行情况，并对数据安全管控的投入提供依据；

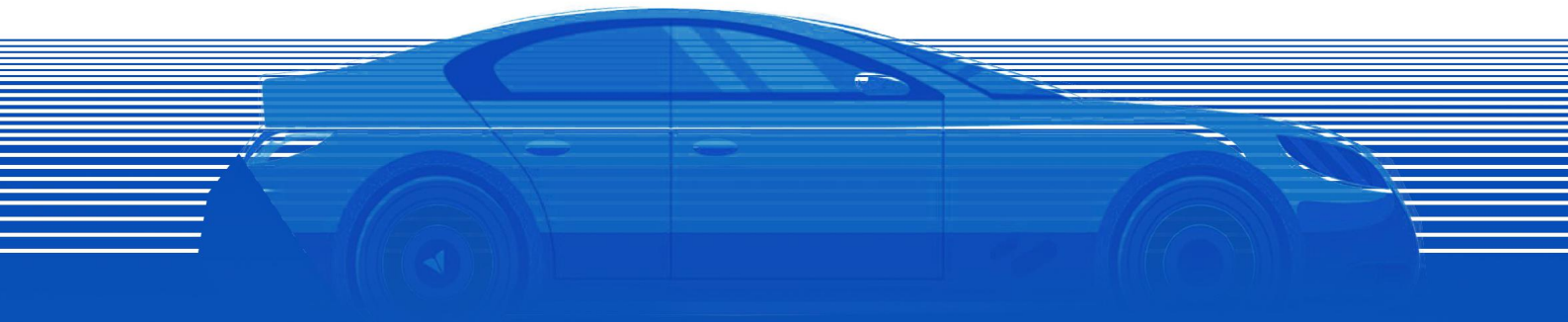
6 组织建设

组织建设是车联网企业有效开展数据安全建设的基础保障，组织建设过程中必须明确责任归属、职责划分、落地负责、监管考核的角色与内容。组织首先有必要成立专门的数据安

全机构，这个机构可以是实体的，亦可以是虚拟的（一般以此为主），持续有效开展车联网企业数据安全的策略制定与执行、监督与贯彻，做到谁负责、谁落实、谁监管。

数据安全机构成员一般由数据利益相关者和专业人员构成，此处所指的利益相关者不仅仅是数据的使用者（业务口），还有可能包含：数据本身的拥有者、数据本身代表方（用户方）、数据责任人（组织指派负责人）。

组织架构早期的构建可以由熟悉应用或者安全的业务部门发起，采用循序渐进的方式完善整个组织的角色构成，逐步建立一个涵盖信息化、管理、安全、执行等部门的综合组织机构。一般组织内部的成员由企业的 IT、法务、财务、信息化、市场、产品等部门重要人员组成，车联网企业的数据安全组织机构中可以包括主管的 VP、董事会成员等，有条件的车联网企业可以在内部组织建设的过程中设立“数据安全官”（CSO）。

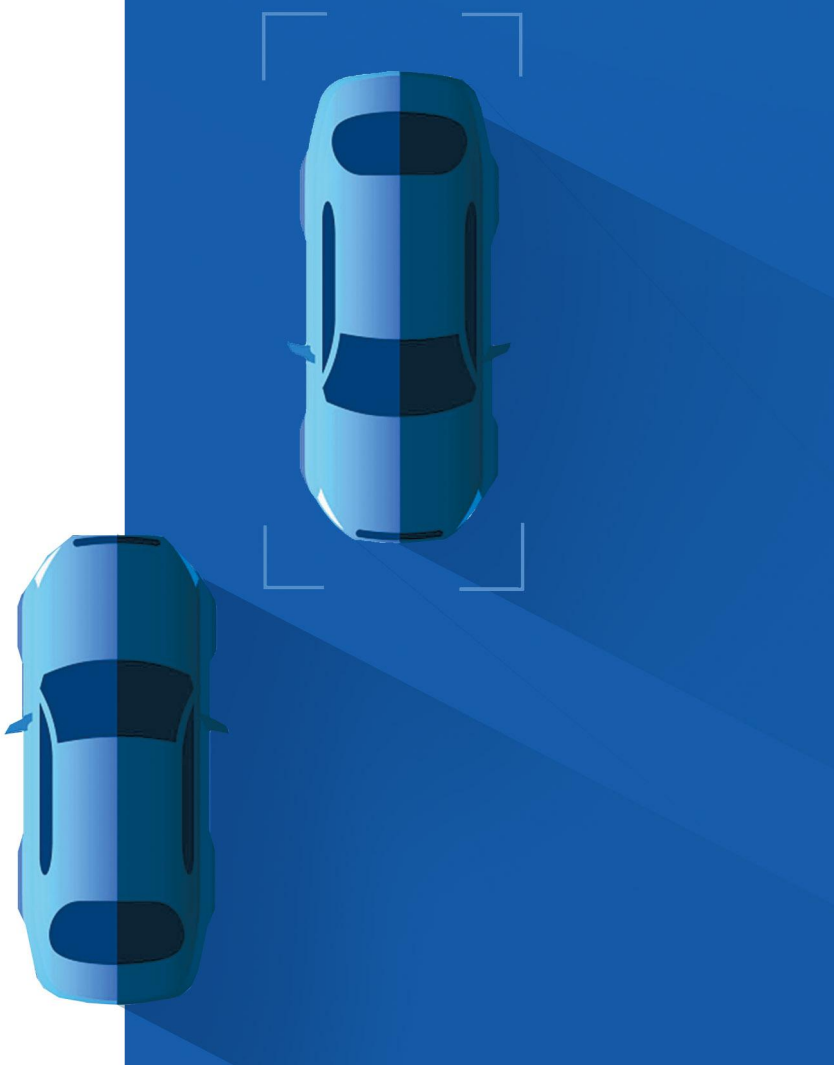


7 制度体系建设

由于车联网涉及到大量的用户数据、隐私信息，以及终端（车端）的位置信息、行驶轨迹等重要数据，车联网企业在制度体系建设过程中，需构建一种“双向构建”制度体系建设模式，即：一是要把国际国内监管合规架构的要求作为企业内部制度体系的准则，车联网制度体系的建设不能脱离车联网领域的网络数据安全标准，主要围绕车联网云平台数据安全、V2X通信数据安全、智能网联汽车数据安全、车联网移动 App 数据安全等开展制度体系的建设；二是要从车联网自身实际的需要出发，内部建立明确的数据安全管理制度，对重要的、敏感的数据（特别是用户个人信息）进行分类分级之后，落实到实际的制度条款之中。

由于车联网数据的特殊性，一旦发生安全事件，所造成的损失不是传统意义上网络边界突破或者业务连续性中断，而是一种持续性的影响，而且影响的周期可能会比较长，因此，制度体系建设一定要明确追责机制，要有明确的责任方与可以量化的后果，同时在制度中明确行之有效的补救措施与应急预案。

8. 能力建设



8 能力建设

结合车联网领域数据使用特点和自身使用需要，建议建设并加强六个方面的能力，包括数据脱敏、数据加解密、电子认证、数据资产梳理、接口审计、安全扫描与检测。

8.1 数据脱敏

车联网企业在业务运营中，会涉及大量的隐私数据。数据脱敏能力的建设，对企业有效地使用这些数据，使其在能够安全、高效地服务于企业运营各个环节的同时，保障各方隐私不被泄露，具有重大的意义。

数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。在涉及客户安全数据或者一些商业性敏感数据的情况下，在不违反系统规则的前提条件下，对真实数据进行改造并提供测试或分析使用，如车架号、定位信息、车况信息、驾驶信息、身份证号、手机号、车牌号等敏感信息都需要进行数据脱敏。从而实现在不泄露敏感数据的前提下保障业务的正常运行。

从使用场景上区分，数据脱敏能力的建设，包括静态数据脱敏和动态数据脱敏两类。静态数据脱敏主要用在从数据库或者数据仓库中，批量导出包含敏感内容的数据，经过脱敏处理后，再导入到其他目标库中。动态数据脱敏主要用在持续在线的业务场景中，实时、高效地对传输过程中的数据进行脱敏处理，如 CRM 系统等。

脱敏系统可以整合一定的工单管理能力，可以很好地提升工作效率，与角色、权限管理结合之后，能够有效地控制敏感数据的流动，保障数据安全。

在脱敏能力的建设过程中，建议关注以下几点：

1 针对不同角色和用户、不同敏感数据类型，以及不同的库、表、列，设置不同的脱敏算法；

2 对于脱敏算法的设置，能够灵活地修改和配置，提高安全性；

3 脱敏引擎预留相关接口，能够扩展自定义的脱敏算法；

4 脱敏算法本身具有一定的安全性、健壮性，不易被破解或还原；

不同的数据，数据脱敏之后数据类型有可能改变，对业务的可用性、连续性和稳定性需要仔细测试与验证。

8.2 数据加解密

数据安全可信主要指数据来源真实性、不可抵赖性，数据内容的完整性和一致性，数据存储、传输和交互的机密性等几方面。数据安全防护的目标如下：

一、 *数据安全涉及到交互主体和交互过程包括但不限于：*

1 车辆智能终端与行车电脑之间的指令交互；

2 车辆智能终端与车主移动终端 APP 的数据交互；

3 车辆智能终端与平台端数据交互；

4 平台端与车主移动终端；

5 平台端与 CP/SP 系统之间；

二、 *需要保护的数据可能涉及的内容包括但不限于：*

1 车辆敏感数据：包括但不限于车辆信息、车主信息、行车轨迹、业务服务等私密内容；

2 车辆控制指令信息：包括但不限于远程遥控汽车解锁上锁、开关空调、灯光控制、玻璃升降、导航及定位、整车体检及电话通讯等功能等；

3 平台业务数据：包括但不限于业务订购/消费、对账计费、支付结算等；

三、 *数据保护的安全功能包括：*

1 数字签名功能：需要利用数字证书和数字签名技术，来保护源发数据的来源真实性、不可抵赖性、数据内容的完整性等，防止未知来源的指令执行、数据内容非法插入篡改、数据和指令伪造等；

2 数据加解密功能：需要通过数字证书和加解密技术（对称加解密、非对称加解密、数字信封等）实现数据生成、数据传输、数据接收过程、数据存储、数据处理等各环节和过程的机密性，防止敏感信息泄密；

8.2.1 基于公钥体系的强安全加密认证

目前有许多数学方法和技术手段可以达到安全加密认证的目标，业内通用的就是增加安全算法来提高信息系统的安全等级。

1 通过 3DES、AES、SM4 等对称加密算法来确保数据的保密性。通常优势是：计算速率高、消耗资源少、商用环境普适性强。通常劣势是：密钥分发困难、端到端的密钥维护量大。

2 通过 Hash（哈希函数，如 SHA−256）和 MAC（消息认证代码算法，如 CMAC 和 HMAC 的方式形成信息摘要从而快速地检查信息完整性。

3 通过非对称算法（如基于 RSA 和 SM2 等公钥算法数字签名）实现信息的真实性和不可否认性。通常优势是：密钥分发容易、端到端密钥维护便捷。通常劣势是：计算速率稍低、消耗资源较多、商用环境普适性差。

根据车联网各环节的保护信息的重要程度和破坏后造成的严重后果的严重程度，指导算法类型、密钥管理、安全加密认证流程，可灵活应用公钥密码算法密钥分发管理方便、安全强度高，对称密钥计算速度快、计算资源消耗少、普适性强的特点，确保算法类型、算法强度与实际需求和产业现状相匹配，综合平衡好安全和业务需求的关系。

8.2.2 国产密码算法支持

国家商用密码管理办公室制定的一系列密码标准包括 SSF33、SM1（SCB2）、SM2、SM3、SM4、SM7、SM9 及祖冲之密码算法等。其中 SSF33、SM1（SCB2）、SM4、SM7 及祖冲之密码是对称算法；SM2、SM9 是非对称算法；SM3 是 Hash 算法。

其中 SM2（椭圆曲线公钥密码算法）就是 ECC 椭圆曲线密码机制，但在签名、密钥交换方面不同于 ECDSA、ECDH 等国际标准，而是采取了更为安全的机制。另外，SM2 推荐了一条 256 位的曲线作为标准曲线。SM2 使用国家密码管理局批准的 SM3 密码杂凑算法和随机数发生器，根据总则选取有限域和椭圆曲线，并生成密钥对。

对于采用 Nbit 密钥的对称加密，其加密强度是由其密钥的长度来实现的，一般需要尝试 2N−1 次才能找到密钥（平均值）。

对于采用公钥算法的非对称加密情形与此不同，其加密强度由数学逻辑和密钥长度同时保证，如对于 ECC 椭圆形曲线加密（SM2 就是 ECC 椭圆曲线密码机制），平均猜测次数至少要达到点数的平方根之后才能找到私有密钥。但在找到私钥之前，一般需要先解开极其复杂的数学方程才能进行密钥推算。

保密级别	对称密钥长度/bit	RSA密钥长度/bit	ECC/SM2密钥长度/bit	解密时间
80	80	1024	160	2010年
112	112	2048	224	2030年
128	128(SM1/4/7)	3072	256(SM2)	2040年
192	192	7680	384	2080年
256	256	15360	512	2120年

注：密钥长度安全性对比

如图所示：国产密码算法 SM2 在密钥长度、加密效率、加密安全性均优于国际通用算法 RSA。随着车联网安全加密认证的发展，国际主流方案也逐步采用 ECC 算法。

安全加密认证技术采用最新的国产密码算法，包括车载端密钥和算法、加密传输通道的密钥协商和算法、平台端的密钥和算法，以及身份安全标识的数字证书均采用最新的国产密码算法，可以有效推动国产化密码算法在车联网行业中的产业化应用，才能进一步构建完整的基于国产化密码算法的车联网安全加密认证技术产品良好生态，自主可控的完整供应链体系。

8.2.3 基于国产密码算法双向认证

对称加密算法通常优势是：计算速率高、消耗资源少、商用环境普适性强；通常劣势是：密钥分发困难、端到端的密钥维护量大。

非对称算法通常优势是：密钥分发容易、端到端密钥维护便捷。通常劣势是：计算速率稍低、消耗资源较多、商用环境普适性差。

将这两种加密方式结合使用，用公共密钥体系做端到端的身份鉴别（证书或签名），在双方之间创建和加密传输共享会话临时密钥，双方通过使用这个共享会话密钥的对称加密进行通信，如此，就能充分利用这两种加密的长处：对称加密的性能、速度，以及公共密钥加密的安全性和便利性。

算法选择方案建议选择经过论证、安全强度较高的算法，例如 RSA2048 以上、SM256、SHA256 以上。

TLS（Transport Layer Security）是为网络通信提供安全及数据完整性的一种安全协议，TLS 在传输层对网络连接进行加密。传统的 TLS 协议分为两种方式，单向认证和双向认证。
无论是单向还是双向，都应建议使用 CRL 吊销列表，确保被认证的密钥处于安全可用状态，并根据车辆的状态及时更换或吊销其认证密钥。

目前标准的 TLS 协议支持的非对称算法为 RSA 和 ECC，对称算法支持为 3DES、AES 等，这些都是国际上通用的算法，没有使用国密算法，在安全性上存在隐患。

应根据《中华人民共和国密码行业标准 SSL VPN 技术规范 GM/T 0024—2014》中定义的国密 SSL 协议（主要分为记录层协议、密码规格变更协议、报警协议和握手协议），研制开发 TSL 握手协议，将其中的算法修改为国密算法，使得项目可以支持基于国产密码算法的安全双向认证。

8.3 电子认证

8.3.1 强身份认证

车联网电子认证要求主要目标在于实现各场景的安全身份标识，通过 PKI/CA 手段对于参与交易的实体进行安全的身份标识，包括但不限于车端设备（T-BOX、HU 等）、云平台服务器（智能网联汽车运营服务平台）、接入 SP/CP 服务器、车主移动端 APP、授权用户移动端 APP、平台管理员等主体。

8.3.1.1车端身份认证

车端安全身份认证需求主要包括：

1 车端可信身份标识和车云双向认证：实现车端设备的可信身份标识，并基于安全身份标识实现与云端的双向认证。

2 车端和移动 APP 近场通讯双向认证：基于车端设备可信身份标识，实现与移动 APP 端可信身份标识的近场通讯双向认证。

基于上述车端安全身份认证需求，对车端设备进行识别、验证后，以车架号、车机号等唯一硬件标识，为车端设备颁发设备证书，该设备证书支持硬件密码芯片的安全存储和操作系统文件级安全等两种方式。

车端数字证书一般通常包括车载 T-BOX 和 HU 设备，车载 T-BOX 的数字证书通常在车辆生产环节即预先刷写安装，HU 设备可以在车主使用过程中激活，在线申请、下载安装数字证书。

8.3.1.2移动端身份认证

移动端（互联网或蓝牙）安全加密认证需求主要包括：

1 移动 APP 和车端近场通讯双向认证：基于通讯双方的可信身份标识，实现移动 APP 和车端近场通讯双向认证。

2 移动 APP 远程车控安全认证和指令保护：基于通讯参与方的可信身份标识，实现移动 APP 和云端平台、云端平台和车端的安全认证、指令来源真实性验证、指令信息完整性和机密性等安全保护。

3 用户可信身份标识和车云双向认证：车主通过移动端 APP 进行车辆控制业务操作，移动端安全加密认证主要包括车主身份识别认证、车主安全身份标识、车主应用登录安全认证和移动端与平台端的通讯双向认证。

4 车辆使用授权可信身份标识和认证：车主授权另外的车辆使用者场景下，对于被授权方的身份识别认证、安全身份标识、应用登录安全认证和移动端与平台端的通讯双向认证。

5 通过蓝牙方式与车辆进行连接同样需要经过认证机制，确保双向身份可信。

基于以上要求，对车主持有的智能手机进行识别、验证后，为车主颁发个人数字证书，该数字证书以数据电文形式存在，内置在智能手机终端中。

8.3.1.3服务器身份认证

服务器身份认证需求主要包括：

1 云端可信身份标识和车云双向认证：实现云端平台的可信身份标识，并基于安全身份标识实现与车端的双向认证。

2 平台接入端的可信身份标识和安全认证：实现对接入平台的 CP/SP 进行安全可靠标识，并基于安全身份标识实现与接入端的双向认证。

3 平台管理端的可信身份标识和安全认证：实现对访问平台的运营管理端用户进行可信身份标识，并基于安全身份标识实现安全认证。

基于上述要求，对平台及内部子系统的服务器 IP 地址和硬件属性信息进行识别、验证后，以服务器 IP 地址和硬件属性信息等作为服务器的唯一标识项，为服务器颁发数字证书，通过该数字证书进行服务器身份的安全标识。

并且为 CP/SP 系统的服务器 IP 地址和硬件属性信息进行识别、验证后，以服务器 IP 地址和硬件属性信息等作为服务器的唯一标识项，为服务器颁发数字证书，通过该数字证书进行服务器身份的安全标识。

8.3.1.4用户身份识别

用户身份识别安全需求主要为用户可信身份标识和车云双向认证：车主通过移动端 APP 进行车辆控制业务操作，包括车主身份识别认证、车主安全身份标识、车主应用登录安全认证和移动端与平台端的通讯双向认证。

因此，对于用户身份识别，在为车主颁发个人数字证书前需对车主自然人实名身份信息进行核验， 以自然人公民身份证号码为中心，融合多种身份认证技术、实现不同电子身份认证互通，成为符合行业要求、服务车联网、全面互联互通的自然人身份统一认证平台，为各类车联网活动提供统一、可靠、持续的身份认证服务。

用户身份识别平台为接入平台的外部应用提供身份认证服务，对个人用户的身份信息通过与身份认证源进行交互来获取，同时平台提供相应的管理功能，包括身份标识管理、认证等级策略管理、匿名身份标识管理、身份源管理、应用管理以及系统配置，从而通过核心的身份决策单元来通过对认证等级策略、访问控制策略和身份信息的计算来核定用户的身份信息和认证等级信息，同时对于应用管理者提供应用接入中心服务。

8.3.2 加密传输

业务层面的数据安全主要从数据的产生、初加工、传输、再加工、存储、利用等周期的各环节来保障数据来源（数据产生主体）的真实性、数据内容的完整性（没有经过非法篡改、伪造、删减等）和一致性（确保接收的数据确定就是发送方想要发送的数据）、数据内容的保密性（传输过程、存储过程、利用过程）。

常见的数据安全相关攻击有如下方面：伪造指令攻击（无法有效确定指令来源和指令的正确性）、敏感信息内容获取（利用传输过程、存储过程的漏洞获取敏感信息）、数据内容篡改和欺诈误导系统和用户错误操作等。

通过 PKI/CA 的数字签名技术，可以有效的鉴别数据来源的真实性、数据内容的完整性和一致性；通过 PKI/CA 的数据加解密技术，可以有效的进行数据内容全周期的安全加密保护，防止敏感信息泄密。

数据安全防护的内容主要为通过数字签名技术确保数据和指令交互主体的安全认证，对于数据和指令来源的可靠性进行安全认证，包括但不限于：

1 车辆智能终端与行车电脑之间的指令交互；

2 车辆智能终端与车主移动终端（手机、平板电脑）的数据交互；

3 车辆智能终端与智能网联汽车运营服务平台数据交互；

4 智能网联汽车运营服务平台与车主移动终端（手机、平板电脑）；

5 智能网联汽车运营服务平台与 CP/SP 系统之间；

8.3.3 抗抵赖

为满足车联网多主体交互的安全认证机制，实现业务数据的完整性和不可抵赖性，建设基于 PKI/CA 体系的平台，提供综合的数字证书应用集成服务，配合车联网环境下各实体提供包括访问控制、数字签名验签、时间戳、安全数据网关等多项功能，从而确保业务操作和数据的完整性、有效性、时效性，并能为后期责任认定提供权威合法的电子证据。

8.4 数据资产梳理

数据资产梳理，是指对车企的数据资产进行全面清查、摸排，构建企业级的数据资产目录的过程。数据资产梳理是数据安全体系建设及数据资产管理中的一项基础性工作，其重要性体现在：

1 认识数据是一切数据资产价值的源头，只有进行数据资产梳理，了解数据所代表的含义，才能进行数据资产管理和数据安全体系建设。

2 通过对数据资产的盘点和梳理，挖掘数据背后隐藏的价值，进而支持企业的运营和决策分析。

3 资产梳理是保障数据安全的基础，通过数据资产梳理完成对数据的分类和敏感等级划分，是建立数据安全体系的第一步。

支撑数据资产梳理工作的数据资产梳理工具一般具备以下能力：

1 能够根据车企数据特点，制定和使用数据分类模板。对车企的数据字典进行收集和整理，统一数据描述规范，并结合企业内部特征，制定合适的数据分类模板，使用这些模板进行资产梳理和盘点。

2 能够自动探查和发现内部数据存储位置。数据资产一般分布在数据库、云平台（公有云、私有云）、大数据平台、文件服务器、工作终端等设备中，数据资产梳理工具应具备数据源自动扫描功能，可以自动发现数据存储位置。

3 能够对数据含义进行自动识别和解析。通过内置的业务模板和数据标准，数字资产梳理工具应可以自动识别数据格式，并在此基础之上，通过自然语言处理和特征分析等方法，对数据进行语义内容识别；另外，还需要实现表格分类、关联关系分析等功能，使得数据内部关系透明化。

4 能够对数据进行分级分类。在数据资产管理的实际操作中，对数据进行正确地分类，能够避免大部分一刀切的控制方式，同时能对数据的安全管理采用更加精细的措施，使数据在共享使用和安全使用之间获得平衡。数据资产的分类原则和分级方式一般定义如下：

a) 数据分级分类的原则：分类——依据数据的来源、内容和用途对数据进行分类；分级——按照数据的价值、内容敏感程度、影响和分发范围不同对数据进行敏感级别划分。

b) 数据分级分类方式：根据梳理出的数据资产，进行敏感数据的自动探测，通过特征探测定位敏感数据分布在哪些数据资产中；针对敏感的数据资产进行分级分类标记，分类出敏感数据所有者（部门、系统）根据已分类的数据资产由业务部门进行敏感分级，将分类的数据资产划分公开、内部、敏感等不同的敏感级别。

5 能够分类展示数据，划分敏感等级。采用规范的数据分类方案对数据进行分类管理，并根据敏感程度划分敏感等级，帮助企业全面清晰地厘清数据资产、确定数据重要性以及敏感程度，对数据资产实现规范化管理，更好地完成对数据的维护和补充。

6 能够生成数据资产地图和可视化数据报告。数据资产梳理工作的成果，能够以完整、全面、直观的数据资产地图，以及可视化数据报告来呈现。包括：数据资产位置分布地图、数据分类分级报告、数据质量报告、数据资产报告等。能够帮助车企管理人员清晰地了解内部数据情况，掌握数据资产状况。

8.5 接口审计

接口审计关注的目标，重点在于数据 API 网关与车机系统，以及其他包含隐私数据的系统和功能模块。其中，车机系统的接口审计包括所有与车机交互的数据接口，如支撑 V2X 的私有云，以及第三方应用的上行数据接口。

接口审计依赖调用行为、接口响应行为、网络流量统计等详细的日志记录，内容包括使用者的身份、IP 地址、主机信息、访问时间、服务响应、流量大小等。通过日志记录，可以为管理者提供详实、不可抵赖的安全审计功能。以备在安全事件发生时，能够及时预警、迅速定位事件起因与产生源头。

8.6 大数据平台安全

大数据平台的安全问题，一般来自于两个方面，一方面是支撑大数据组件的系统平台自身存在的漏洞，另一方面是大数据组件本身提供的一些功能可能会诱发的隐患。这些隐患大概包括以下几点：

1 安全配置。常见的 Hadoop 组件发行版本，如 Apache、CDH、HDP 等，默认的配置中，安全配置并不完善。

2 组件自身脆弱性。Hadoop 开源以来，最初并没有考虑安全方面的问题，例如组件间的身份认证、鉴权等要依赖 kerberos。

3 分布式架构带来的问题。与传统的数据库集中式的架构不同，分布式的组件部署，带来如越权访问、网络扫描、暴力破解、账户冒充、嗅探监听等安全问题。

针对上述特点，大数据平台的安全扫描与监测能力的建设关注以下几个方面：

1 大数据组件的管理。大数据集群节点间的组网信息，平台环境的物理参数，以及组件的部署信息，对这些信息的管理是后续一系列工作的基础。

2 集群节点的漏洞扫描，安全配置扫描。从平台硬件资源层加强漏洞检测、版本更新补丁、大数据组件的安全基线扫描，加强主机口令、操作管理，减少非法登录。定期备份系统和文件数据，能够快速修复主机的系统问题。制定有效的身份、认证、授权、审计等配置方面检查方法。形成具备操作指导性质的文档、手册，或者可执行脚本。

3 从网络层面加强平台访问行为监测。大数据平台一般部署在企业内网，与外网物理隔离，杜绝安全隐患。其次，在企业网络内部，大数据平台的组件与其他内部网络（如办公网络）之间，可以部署网络防火墙、安全网关等，能够更好地监测未经授权的可疑访问行为，也可以做到及时地报警与阻断。

4 集群节点系统资源监测。各个组件节点的系统资源监测对于维持大数据平台的可用性非常重要，可以部署具备集中控制和监控节点资源利用情况的管控系统，以便管理员能够在中央控制端进行统一的管控。

5 制度建设。从社会工程学的角度来看，建立大数据平台的建设、管理以及使用等方面的保障制度和规范，应当是重中之重，各种技术防范措施做的再好，如果没有良好地制度和规范来约束使用这些技术平台的相关人员，那么所有的数据安全保障系统将形同虚设。

8.7 容灾备份

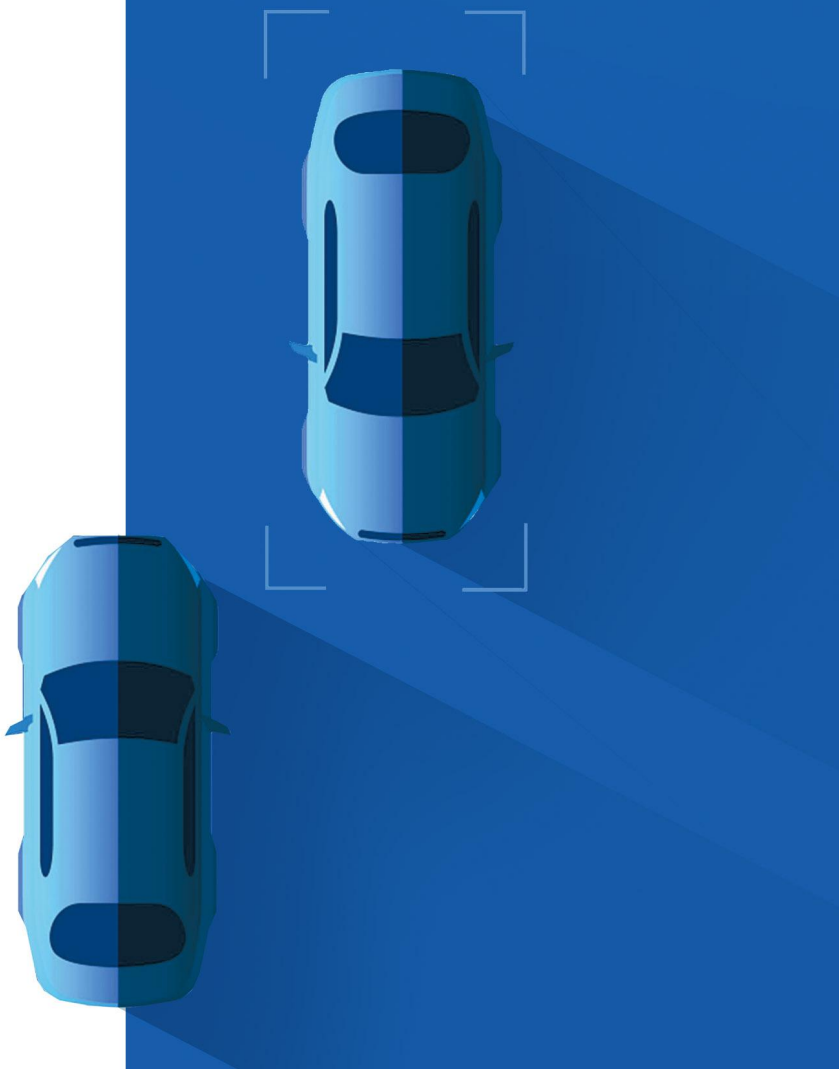
车联网运营过程中会产生大量的车辆数据、驾驶数据、车主操作等数据，这些数据一旦丢失或被破坏，不仅造成车企具大的损失，也会给车主带来诸多不便。因此，车企在为车主提供智能网联汽车服务的同时，也要考虑建设数据的容灾备份能力。

容灾系统的目的在于保证系统数据和服务的“连续性”，即当系统发生故障时，仍然能够正常地提供数据和服务，以使应用系统不会终断。

从技术上看，衡量容灾系统有两个主要指标：RPO（Recovery Point Object）和 RTO（Recovery Time Object），其中 RPO 代表了当灾难发生时允许丢失的数据量；而 RTO 则代表了系统恢复的时间。

常用的灾备组合方式有建设机房内的本地备份系统和建设异地的备份系统两种，而后者则是一个较为理想化的容灾系统一体化解决方案，能够在很大程度上避免各种可能的错误。

9. 安全审计



9 安全审计

车联网 V2X 模式，已经形成了一个完整的信息生态系统，软件、硬件、数据、通信整个都包含在车联网这个大的信息系统环境之中，因此安全审计在这个环境下是必不可少的，车联网安全审计的前提还是要遵循合规，通过安全审计，实现车联网数据的机密性、完整性、可控性、抗抵赖性、可用性就显得尤为重要。

9.1 安全审计时效性

从车联网安全审计的时效性分析，覆盖事前、事中、事后三个环节，尤其是在事前、事中要重点安全审计，重点围绕车联网安全管理系统开展安全审计的各个工作流程。

事前安全审计，重点核实审计车端身份的准确性（人）、车载使用数据的一致性（车）、车联网沿线设备的安全性（路）、车联网安全管理系统的稳定性（云），确保车联网运行前总体的安全与稳定。

事中安全审计，重点审计黑客的攻击、CA 签名的不一致性以及道路设备与车载软件的匹配性，事中安全审计是比较重要的，审计的日志及结果都要做严格的记录与归总，特别是发生一些异常行为的时候，要进行及时的预警与处置。

事后安全审计，在车联网领域的主要作用在于事后复盘，明确车联网领域存在哪些不足或者缺陷风险，为后续车联网领域数据安全持续改进提供数据支撑。

9.2 安全审计对象

从车联网安全审计的对象分析，包括车联网领域主机审计、设备审计、行为审计、内容审计、应用审计。

这几个过程围绕着车联网数据的全生命周期展开，主机审计重点关注的是车联网终端（车端）的非法接入（外联）控制问题，同时车端的操作审计也是主机审计的重要着力点，很多的车联网主机既是数据的使用者，亦是数据的生产者，更是最易被攻击的突破口，安全审计当以主机审计为先；设备审计—V2X 车联网，“车–路–云”都是由有诸多的硬件设备组成，这些基础设施既是车联网链路上的重要支点，也是数据流经的必然节点，因此对于设备的安全审计也是至关重要的，特别是对一些重要的“路”节点设备，要利用专用的审计能力进行定向、连续的审计；行为审计——网络行为审计也是安全审计不可或缺的部分，一些通过网络

协议（http、smtp/pop3、ftp 等）作为数据传输载体，极易变成攻击的对象，在网络层进行安全审计，不仅仅是对异常行为的审计，更是能够通过对协议的解析实时、动态的发现针对车联网数据安全的攻击行为，确保车联网数据不会在网络上被侦听或者泄露，同时能够实时预警；内容审计——内容审计面向的对象主要是数据库内的结构化数据、车载端接入的非结构化数据进行综合的审计，特别是对一些异常的数据调用操作进行重点的“行为+内容”的综合评估，实现针对数据内容的 UEBA；应用审计——应用审计涉及到中间件、后台服务，这些是车联网应用能够有效运作的纽带，也是比较容易被攻击的对象，特别是其中短暂驻留的车联网数据，要进行安全审计。同时应用上线之前需要进行代码审计，确保上线之前的业务应用在代码层面不存在漏洞，避免因为应用存在漏洞而导致的数据泄露风险。

9.3 安全审计内容

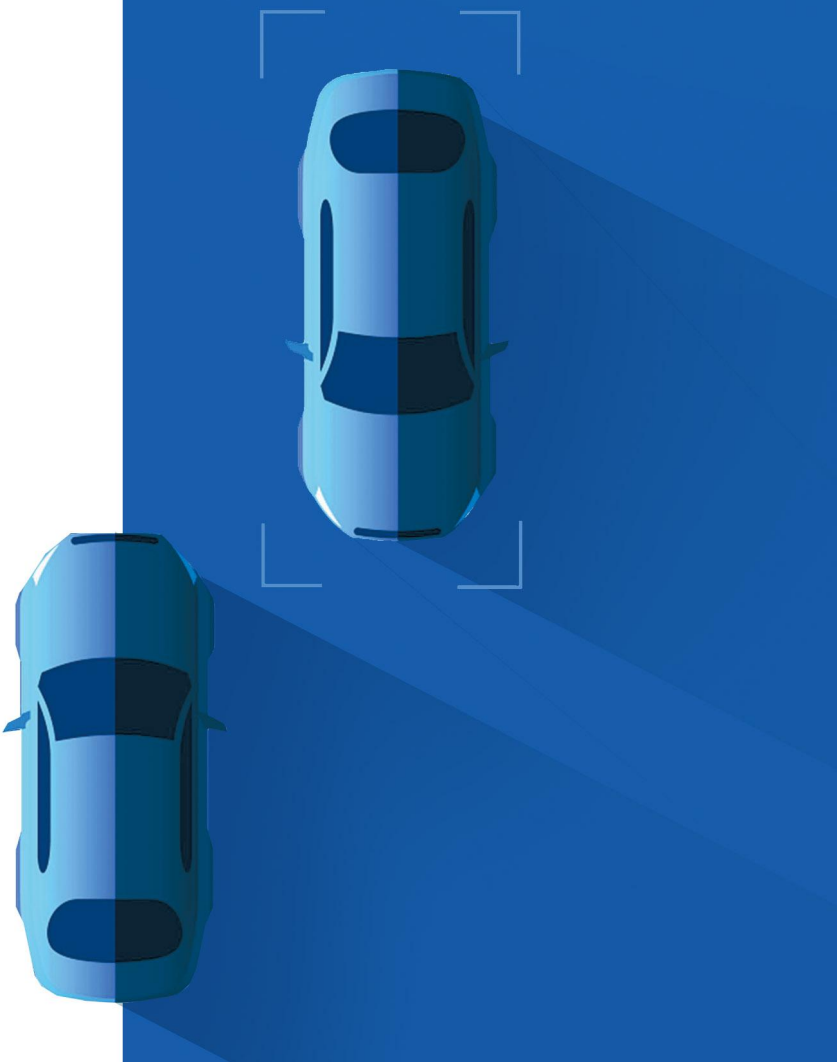
从车联网安全审计内容分析，安全审计包含：合规审计、日志审计（安全事件审计）、制度审计。

安全合规性审计要求车联网数据安全在建设与运行 IT 系统中的过程是否符合相关的法律、标准、规范、文件精神的要求，能够作为风险控制的主要手段之一，可以有效检查数据安全策略的落实情况。

日志审计，也是指对数据安全事件安全审计的一种形式，每一个车联网的端点都需要有相应的日志采集及上报能力，特别是涉及到数据流转的节点，要根据策略定义的审计记录事件结果进行汇总，并进行数据备份或生产报告，以便进行事后追溯与问题分解应对。

制度审计，这是内容审计的重要组成部分，在数据安全体系建设过程中，制度的建设是非常有必要的，制度在车联网各阶段运转过程中是否有落实到位，可以依托组织机构进行持续的跟踪与审计，出具阶段性的制度安全审计报告，以备在实际的车联网运转过程中能够实现数据安全的有责任人、有职划分、有监管到位。

10. 场景安全



10 场景安全

场景安全包括车联网四个典型的数据场景，包括数据提取、大数据平台、车机数据流转和 APP 用户数据流转，本指南将从场景描述、风险分析、制度规范、技术工具、参考文件五个方面进行阐述。

10.1 数据提取

10.1.1 场景描述

车联网数据依据产品需求采集完成以后按规定将原始数据存储至生产库，并通过备份系统备份至备份库，供数据需求者以及后续产品迭代使用。例如，数据提取的方式由需求者将特定 SQL 或提取需求提交给 DBA，DBA 提取后通过中间服务器或邮件发送给需求者，需求者收到后将数据导入自己的目标库。

10.1.2 风险分析

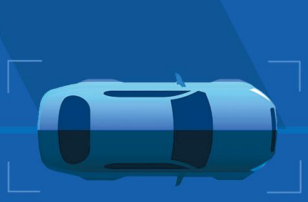
数据提取过程中如果涉及的人员过多、手工多于自动化则会造成数据暴露面过大，导致数据泄露的风险。另外，如果缺少对数据提取命令的审核和审计，数据需求者存在无意或故意窃取数据的可能。

10.1.3 制度规范

源数据存储时采用加密存储。整个数据提取流程完全自动化完成，拒绝人工拼写 SQL 执行。所有提取行为采用严格审计行为。对数据提取的 SQL 的进行事前校验，参照 SQL 白名单对 SQL 的合法性进行校验，只能通过变更 SQL 白名单来变更 SQL，对于 SQL 发起的主体依据规则进行鉴权。能够检测数据传输过程中的完整性，如果检测到完整性被破坏时应重新获取数据。

10.1.4 技术工具

对车联网数据运用加密技术进行存储，通过脱敏技术对脱敏后的数据进行共享，基于角色的细粒度管控措施对数据共享行为进行管控。



10.2 大数据平台

10.2.1 场景描述

由于监管要求，需要将存储在 TSP 数据库及备份库中的原始数据，通过监管数据报送员进行报送，通过互联网发送至监管方。基于对原始数据处理生成再生库，对数据进行分析或者对功能研发迭代需要用到原始数据。

10.2.2 风险分析

通过人工操作将原始数据通过互联网进行报送，由于人工介入过多导致风险系数提升，互联网不确定性因素也有潜在的风险。以及对原始数据进行处理生成再生库的过程，由于没有对原始数据做处理，再者对再生库中的数据缺乏有效的审计，无法清晰了解再生库中的数据使用情况，均会加大数据泄露的风险。

10.2.3 制度规范

原始数据上报需要通过特殊流程进行上报。数据处理时需要通过大数据平台进行处理，杜绝个人直接访问原始数据。研发及数据分析使用高仿真脱敏数据进行分析，避免直接接触原始数据。对大数据组件进行鉴权、严格审计，依据规范保障大数据环境的安全。

10.2.4 技术工具

运用大数据脆弱性检测工具检测数据存储环境。运用数据脱敏工具对敏感数据进行高仿真脱敏。整个数据分析过程运用数据分析平台进行分析，并对大数据组件进行审计。

10.3 车机数据流转

10.3.1 场景描述

车机系统能够处理的数据包含视频、图片、车机数据、车辆基本信息、其他 ECU、语音、VIN、GPS 等数据。数据会通过互联网上传至车企私有云和车机系统应用厂商。

10.3.2 风险分析

车机系统本身存在漏洞，引发视频、图片、车机数据、车辆信息、其他 ECU、语音、VIN、GPS 等数据的泄露。缺乏对运维人员的有效监控措施，TSP 运维以及 TSP 数据库的审计等存在泄露风险。车机应用数据回传缺乏有效监测，无法知晓是否有数据违规回传行为。

10.3.3 制度规范

通过安全机制、接口鉴权，对密钥证书格式、消息签名、加密流程、密钥协商等方面进行校验，定期对车机系统进行安全扫描，并由专人定期进行巡检。对车机系统的 API 调用进行审计，对身份及设备进行鉴别。TSP 运维人员和 TSP 数据库中的敏感数据进行隔离，并对运维行为进行管控，以及对 TSP 数据库审计。限定车机应用回传数据内容，并对回传内容进行审计。

10.3.4 技术工具

车机系统安全扫描工具：自动对车机系统进行漏洞和脆弱性扫描，发现潜在风险，并给出修复建议；

接口管控系统：数据从车机端向互联多端发送数据时需要对接口内容和合规性进行管控，及时发现违规调取数据的接口并识别返回内容是否正常，并对调取数据对象的身份进行认证，确保合法可信；

数据库运维管理系统：由于工作需要，一般运维人员的权限较大，数据库运维管理系统主要是针对运维人员的操作进行管控，高危操作和批量操作需要提前申请，否则拒绝执行；

数据库审计系统：通过数据库协议解析对数据库的访问行为进行审计，包括操作对象、操作时间、操作结果、影响范围等；

10.4 APP 用户数据流转

10.4.1 场景描述

手机和车机联网通过互联网进行数据共享，有用户信息、购买信息、用户行为、车辆操控数据、通讯录、通话记录等。

10.4.2 风险分析

APP 端的用户数据属于个人信息，且存在敏感信息（如交易信息）和隐私信息（如行驶轨迹信息），这些数据在流转过程中存在以下风险：

一、 APP 程序本身的漏洞被利用，被窃取数据；

二、 端到端传输时未采用加密手段则很容易从报文中解析出原始数据；

三、 数据交换双方未做认证则会造成伪身份情况，使数据发送到非法的终端上；

四、 数据明文存在在数据库中，一旦被拖库或被高权限人员指导出，则会造成严重的数据泄露事件；

10.4.3 制度规范

对 APP 安全加固与定期检测、数据加密传输、双向强身份认证、数据环境检测、应用检测、应用间数据交换管控、数据加密存储、数据库审计。

10.4.4 技术工具

APP 加固工具：对 APP 程序进行安全加固，包括代码的强壮性和搞攻击性；

数据加密工具：通过密码算法对存入数据库的数据进行加密处理；

数据库审计工具：解析数据库协议，及时发现数据库访问风险，审计内容包括访问对象、访问时间、访问结果等；

数据环境检测工具：对应用系统的运行环境进行检测，扫描是否存在操作系统漏洞、中间件漏洞、脆弱性代码等问题；

身份认证系统：通过数字证书技术对数据交换双方的身份进行可信认证；

11. 数据安全体系建设趋势

11 数据安全体系建设趋势

结合目前信息化发展态势，各行业相关数据安全相关要求，未来车联网领域数据安全体系建设会向数据资产管理智能化、数据安全能力平台化、数据安全分析中心化三个方向发展，满足监管要求的同时，真正加强自身数据安全防护能力。

11.1 数据资产管理智能化

车联网企业的核心数据主要由用户数据和车辆数据组成。车辆的不断增加，会使车辆数据成倍的增加，导致核心数据将会迅猛增长。在此过程中，随着人员变动、应用程序的迭代，数据资产将会变的越来越模糊，甚至出现僵尸库、无名资产等现象，若这些资产存在敏感数据，将会成为数据安全的隐患。采用咨询方式对全网数据进行梳理，不仅工作量大，且未必准确，一些僵尸库和无名资产还是缺少清理的依据。

通过人工智能和机器学习技术辅助管理数据资产，可以实时掌握数据资产变化情况、使用状况、敏感数据分布情况等，为数据资产清理提供依据（例如：6 个月未被访问过的数据库可以考虑下架、无名资产可以根据访问关系进行认责等）。另外，通过人工智能技术可以在海量数据中快速识别出敏感数据，大大降低数据资产的管理难度。通过人工智能和机器学习技术管理数据资产，具有效率高、准确率高的特点。因此，车联网企业数据资产管理智能化是必然趋势。

11.2 数据安全能力平台化

数据安全技术已发展 15+年，防护产品已趋于成熟。近几年国家和行业推出了一系列的数据安全法律法规，车联网企业为满足合规及自身需要，或多或少的已建设了一些数据安全能力，采购了数据安全产品。但随着法律法规越来越精细化、车联网业务越来越复杂化，现有的防护方式带来以下等问题：

- ✓ 数据安全产品存在边界，不能全部解决所有合规要求，很难决策；
- ✓ 多个数据安全产品与车联网应用程序集成导致应用臃肿；
- ✓ 各业务条线自行建设数据安全能力，造成冗余；
- ✓ 多个数据安全产品增加运维压力、重复功能，且很难联动，实现整体防御；
- ✓ 出现问题，采购产品，又出现问题，再采购产品，安全产品反成负担；

综上所述，通过建设数据安全能力平台，不仅可以打破数据安全能力孤岛，将散落在各部门或各业务线中的数据安全能力进行整合，还可以使数据安全防护标准化、规范化，数据安全管理统一化。

数据安全能力平台化的核心价值：

一、高扩展性：由于平台采用了组件化，各模块间为松耦合关系，因此，可以通过简单的集成便可增加新的功能组件。另一方面，基于平台可以根据需要随时进行扩容，提升性能；

二、降本增效：将数据安全产品组件化，并通过平台化统一管理，不仅可以充分发挥各数据安全能力的作用，而且可以按需进行数据安全产品的扩充另外，新技术的接入成本也会大大降低；各部门或各业务线无需自行建设数据安全能力，由平台实现统筹；

11.3 数据安全分析中心化

在大数据时代，通过将相关日志进行统一收集、汇总、清洗，生成规则、模型、画像，无疑是快速发现潜在安全风险最有效的方法，即数据安全分析中心化（也可称为数据安全态势感知）。常规的态势感知一般指的是网络安全侧的，数据安全会涉及但不完善，很难发现深层次的数据安全风险。数据安全态势感知需要从应用用户、应用程序、数据库帐号、数据表（必要时到字段级）进行关联分析，分析要素包括操作类型、影响行数等。

数据安全相关的日志进行统计汇总后，结合安全专家经验和业务特征，可以生成具有车联网行业特征、车联网企业管理特征的安全规则、安全模型、行为画像，在海量的数据操作过程中，快速甄别数据安全风险和违规操作，并实现追踪溯源和取证，整体提供数据安全防御能力，并为数据安全投入提供依据。

腾讯安全 | 腾讯智慧出行 | 腾讯标准 Tencent Standard