ICS 43.040.60

T26

团　　体　　标　　准

T/CAAMTB XX—20XX

电动乘用车共享换电站建设规范 第10部分：数据安全管理，风险预警分析技术要求

Construction requirements for EV shared swap station

Part 10: Technical requirements for data security and data warning analysis

（征求意见稿）

20XX－XX－XX 发布　　20XX－XX－XX 实施

中国汽车工业协会　发布

目　次

前　　言

《电动乘用车共享换电站建设规范》分为十三个部分：

——第1部分：总则；

——第2部分：换电平台和装置技术要求；

——第3部分：换电电池包通信协议要求；

——第4部分：车辆识别系统要求；

——第5部分：电池包技术要求；

——第6部分：换电机构技术要求；

——第7部分：电连接器技术要求；

——第8部分：液冷连接器技术要求；

——第9部分：充电设备、搬运设备、电池仓储系统要求；

——第10部分：数据安全管理，风险预警分析技术要求；

——第11部分：安全防护及应急要求；

——第12部分：换电站规划布局要求；

——第13部分：换电站标识、安全运营、设备运输和安装要求。

本文件为T/CAAMTB XX-20XX《电动乘用车共享换电站建设规范》的第10部分。

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国汽车工业协会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件为首次发布。

电动乘用车共享换电站建设规范

第 10 部分：数据安全管理，数据预警分析技术要求

1 范围

本文件规定了电动乘用车换电过程中的数据上传，包括换电站登入、准备换电（换电握手）、换电过程、换电后电池补能过程、换电后电池置放过程等 5 个过程中换电站和电池采集和上传的数据要求。

本文件适用于电动乘用车共享换电站建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

NB/T 33005-2013 电动汽车充电站及电池更换站监控系统技术规范

NB/T 33007-2013 电动汽车充电站/电池更换站监控系统与充换电设备通信协议

NB/T 33017-2015 电动汽车智能充换电服务网络运营监控系统技术规范

3 术语和定义

本文件没有术语和定义。

4 数据上传要求、数据质量评估

4.1 监控系统

4.1.1 建设原则

有利于实现全系统的信号采集、安全稳定控制和事故/故障处理，提供系统运行的可靠性、经济性，确保充电及电池更换的安全性。系统宜采用数字化、网络化、智能化、集成化的先进高效技术，简化硬件配置，避免重复，实现资源共享。

4.1.2 系统构成

监控系统宜由换电管理平台、站控层、间隔层三部分组成，并用分层、分布、开放式网络实现连接。

换电管理平台宜采用分区分层架构，满足总部、省、地市、站级四级应用。

站控层由计算机网络连接的主机/操作员工作站和各种功能站构成，提供站内运行的人机界面，实现控制、管理间隔层设备等功能，形成全站的监控、管理中心，并具备与换电管理平台通信的功能。

间隔层由站内充电监控单元、电池更换监控单元、供电监控单元、视频及环境监控单元、各种网络、通信接口设备等构成，其中充电监控单元和电池更换监控单元为标配设备，其他为选配设备，可根据换电站功能配置选配。

4.1.3 系统功能

换电管理平台应具备客户服务、收费账务、清分结算、资产管理、配送管理、综合统计分析及系统管理功能。

换电管理平台应建立数据库，可进行实时数据和历史数据查询，且便于数据统计，汇总，分析。

换电管理平台应具有站点监控，站点管理，电池状态管理，电池健康策略管理，车辆管理，交易规则设置功能。

站控系统应具备站内设备监视、设备状态报警、站内设备控制与操作、事件顺序记录功能。

站控系统应建立实时数据库，具备人机交互界面、统计计算及制表打印功能。

站控系统应具备计量及交易计算、记录功能。

间隔层应具备充电监控、电池更换监控、供电监控、视频及环境监控功能。

间隔层应具备就地数据采集、控制、显示、传输、时间同步等功能。

4.1.4 站控系统通信协议结构

站控系统与间隔层各监控单元之间的通信协议结构宜参照 NB/T 33007-2013 第 4 章的规定。

间隔层内部宜采用 CAN 通信方式。

4.1.5 站控系统与上级平台通信协议结构

优选 json 和 mqtt 协议。

服务端平台对接收到的数据进行校验，当校验正确时，服务端平台做正确应答。当校验错误时，服务端平台做错误应答。服务端平台的应答信息错误时，客户端应重发本条实时信息。

平台交换数据和用户自定义数据存在时，完成平台交换数据和用户自定义数据的上报。

向服务端平台上报信息的时间周期应可调整。

当终端发送数据为加密状态时，客户端平台应先进行数据解密，并重新加密后发送至服务端平台，如平台间传输无加密需求则无需重新加密。

补发机制：当数据通信链路异常时，客户端平台应将实时上报数据进行本地存储。在数据通信链路恢复正常后，在发送实时上报数据的空闲时间完成补发存储的上报数据。

传输规则：协议应采用大端模式的网络字节序来传递字和双字。

数据包结构：一个完整的数据包应由起始符、命令单元、识别码、数据加密方式、数据单元长度、数据单元和校验码组成。

4.1.6 指标要求

参照 NB/T 33017-2015 第 10 章、NB/T 33005-2013 第 7 章部分。

换电管理平台响应速度。

系统容量、并发量。

系统实时性指标。

连续运行要求。

年可用率。

接收终端数据的成功率。

4.1.7 换电站路由服务

统一接收站控系统的硬件设备数据，通过 mqtt 协议实时转发至监控系统。

4.2 站控系统数据要求

4.2.1 通用规范

区分上传与下载数据。

区分本地保存和云端交互数据。

站控主机与云端交互数据应分为上传数据和下载数据，上传数据包括实时信息、换电过程信息、补发信息和告警信息，下载数据包括配置信息和控制。

本地保存的补发信息，数据保存时长至少不应低于24小时。数据采集的间隔时间应不大于1s。

4.2.2 电池箱数据

参照 NB/T 33005-2013 附录 B,应包含：电池箱电压、电池箱充电电流、电池箱充电功率、电池箱充电时间、电池箱充电电能、单体蓄电池电压、单体蓄电池荷电、电池箱温度、电池箱标识、电池箱类型、电池箱参数、电池箱故障代码等信息。

应包含绝缘电阻、绝缘等故障信息、故障前后实时信息（周期 10ms）以用于故障分析。

宜包含功率、电流请求信息、充放电状态、车辆运行状态、GPS 等实时信息（10s）、数据产生时间。

应具有数据续传功能。

4.2.3 充电设备数据

参照 NB/T 33005-2013 附录 B,应包含充电机直流输出电压、充电机直流输出电流、充电机温度、充电机状态、充电机故障代码等信息。

宜包含充电机交流侧开关状态、充电机直流侧开关跳闸/熔断器熔断、监控单元故障、监控单元与站内监控系统通信中断、充电架空置/就位状态、充电架充电进行/充电完成状态等信息。

4.2.4 换电系统数据

参照 NB/T 33005-2013 附录 B,应包含换电过程数据/信号，如：启动/停止/工作状态。

应具有远程控制功能。

4.2.5 供电设备数据

参照 NB/T 33005-2013 附录 B,应包含：功率，电压，电流，温度等，工作状态。

4.3 监控上级平台系统数据要求

4.3.1 通用规范

区分上传与下载数据。

区分本地保存和云端交互数据。

站控主机与云端交互数据应分为上传数据和下载数据，上传数据包括实时信息、换电过程信息、补发信息和告警信息，下载数据包括配置信息和控制。

部分数据需要进行本地保存，本地保存数据包括补发信息，数据采集周期不应超过30分钟，数据保存周期不应超过1小时。

数据采集的间隔时间应不大于1s。

云端在相关定义和要求下，可通过远程对站控主机下达控制命令。

4.3.2 电池类数据

参照 NB/T 33005-2013 附录 B, 应包括电池包电压、工作电流、SOC、SOH、剩余容量、充电次数、换电次数、电池累计运行里程、电池充电总容量、电池充电总能量、电池换电站内充电总容量、电池换电站内充电总能量、电池输出总容量、电池输出总能量、站内输出总容量、站内输出总能量。

应包括电池单体电压、单体温度、最高温度、最高电压、梯级利用代码、规格代码、追溯信息代码、故障信息等。

应包含数据实际产生时间。

4.3.3 换电站数据

上传信息包括换电站运行状态数据、运营数据、车辆信息数据、消防状态数据、整站相关子系统运行状态数据。

下载信息包括：换电站配置数据、换电站远程操作数据、换电站系统更新数据等。

4.4 数据质量

4.4.1 主要技术指标

数据上传周期应在 30 秒以内。

4.4.2 可靠性指标

a) 模拟量测量综合误差 ≤1%；
b) 系统可用率 ≥99.9%；
c) 遥测合格率 ≥98%；
d) 遥控正确率 ≥99.99%；
e) 遥信正确率 ≥99%；
f) 站控层平均故障间隔时间（ MTBF ） ≥20000h；
g) 间隔层平均故障间隔时间（ MTBF ） ≥30000h。

4.4.3 系统实时性指标

a) 模拟量越死区传送时间（至站控层显示屏） ≤2s；
b) 开关量变位传送时间（至站控层显示屏） ≤1s；
c) 开关量信号输至画面显示相应时间 ≤2s；
d) 系统控制操作响应时间（从发出指令到现场变位信号返回） ≤4s；
e) 实时数据扫描周期 ≤2s；
f) 画面实时数据更新周期 ≤3s；
g) 动态画面响应时间 ≤2s。

5 换电站与服务平台通信

5.1 数据包结构

起始字节	定义	数据类型	描述及要求
0	起始符	/	/
2	命令标识	/	/
3	应答标识	/	/
4	唯一识别码	/	换电站ID
	数据加密方式	/	/
	数据单元长度	/	/
	数据单元	/	/
	校验码	/	/

5.2 命令和应答定义

5.2.1 命令标识

编码	定义	方向
0x01	换电站登入	上行
0x02	实时信息上报	上行
0x03	补发信息上报	上行
0x04	换电操作过程上报	上行
0x05	换电站登出	上行

5.2.2 应答标识

编码	定义	说明
0x01	成功	/
0x02	错误	/
0x03	重复	/

5.3 换电站登入

电池进入换电站后，登入信息传输，换电站应上传换电站相关信息，如下表所示

名称描述	数据类型	长度/字节	描述及要求
数据采集时间	Uint64	8byte/	换电站登入时间,毫秒时间戳
登入流水号	String	/	换电站每登入一次，流水号自动加1，从1开始循环，循环周期为天
换电站id	String	/	/
换电站型号	uint32	8/	/
换电站名称	String	/	/
服务商名称	String	/	/

5.4 实时信息上报

5.4.1 实时信息上报格式

数据表示内容	数据类型	长度/字节	描述及要求

数据采集时间			
换电站数据			
换电站报警数据			
电池数据（1）			
...			
电池数据（n）			

5.4.2 换电站数据

数据表示内容	数据类型	字节	描述及要求
换电站状态	Uint	1	1. 换电中；2. 故障；3. 空闲；4. 消防中；5.未知
1号电池充电状态	Uint	1	0，空闲；1，标准充电中；2，柔性充电中；3，故障；4，OTA中；5，保留
2号电池充电状态	Uint	1	0，空闲；1，标准充电中；2，柔性充电中；3，故障；4，OTA中；5，保留
n号电池充电状态	Uint	1	0，空闲；1，标准充电中；2，柔性充电中；3，故障；4，OTA中；5，保留
1号电池充电输出电流	float	4	/
2号电池充电输出电流	float	4	/
n号电池充电输出电流	float	4	/
1号电池充电输出电压	float	4	/
2号电池充电输出电压	float	4	/
n号电池充电输出电压	float	4	/
1号电池充电请求电流	float	4	/
2号电池充电请求电	float	4	/

流			
n号电池充电请求电流	float	4	/
1号电池充电请求电压	float	4	/
2号电池充电请求电压	float	4	/
n号电池充电请求电压	float	4	/
1号电池充电输出功率	float	4	/
2号电池充电输出功率	float	4	/
n号电池充电输出功率	float	4	/
换电站实时功率	float	4	/
进线 n 路 A 相电流	float	4	有多路，则上传每路信息
进线 n 路 B 相电流	float	4	有多路，则上传每路信息
进线 n 路 C 相电流	float	4	有多路，则上传每路信息
进线 n 路 A 线电压	float	4	有多路，则上传每路信息
进线 n 路 B 线电压	float	4	有多路，则上传每路信息
进线 n 路 C 线电压	float	4	有多路，则上传每路信息
浪涌保护器状态	uint	1	0，分断；1，闭合；
UPS 前端供电断路器状态	uint	1	0，分断；1，闭合；
网络供电断路器状态	uint	1	0，分断；1，闭合；

急停开关状态反馈	uint	1	0，分断；1，闭合；
水冷系统供电断路器状态反馈	uint	1	0，分断；1，闭合；
N 号 温湿度传感器通信状态	uint	1	0，断开；1，连接；
充电区域温度	unt	1	/
充电区域湿度	int	1	/
水冷水箱温度	uint	1	/
加热器运行状态	uint	1	0，disable；1，enable；
内循环泵运行状态	uint	1	0，disable；1，enable；
压缩机高压压力	int	4	/
压缩机低压压力	int	4	/
蒸发器出水温度	int	1	/
压缩机排气温度	int	1	/
水箱温度控制上限	int	1	/
水箱温度控制下限	int	1	/
水冷模式控制	int	1	/

5.4.3 换电站报警数据

数据表示内容	数据类型	字节	描述及要求
N号BMS绝缘故障	bool	/	有多路，则上传每路信息
N号 BMS高压继电器过温故障	bool	/	有多路，则上传每路信息
N号 BMS充电连接器过温故障	bool	/	有多路，则上传每路信息
N号 BMS充电连接器故障	bool	/	有多路，则上传每路信息
N 号 BMS 电池包温度过高	bool	/	有多路，则上传每路信息
N 号 BMS 电池包温度	bool	/	有多路，则上传每路信息

过低			
N 号 BMS 电流过大	bool	/	有多路，则上传每路信息
N 号 BMS_电池类型不匹配告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池一致性告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池温差过大告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池包过压告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池包限压告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池单体电压过高告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池单体电压过低告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池单体温度过高告警	bool	/	有多路，则上传每路信息
N 号 BMS_电池单体温度过低告警	bool	/	有多路，则上传每路信息
N 号 BMS_禁止充电告警	bool	/	有多路，则上传每路信息
N 号 BMS_热管理失控告警	bool	/	有多路，则上传每路信息
N 号 BMS 电池包温度过高	bool	/	有多路，则上传每路信息
	bool	/	有多路，则上传每路信息
n 号模块交流过压	bool	/	有多路，则上传每路信息
n 号模块交流欠压	bool	/	有多路，则上传每路信息
n 号交流过压关机	bool	/	有多路，则上传每路信息
n 号直流输出过压	bool	/	有多路，则上传每路信息
n 号直流输出过压关机	bool	/	有多路，则上传每路信息
n 号模块输出欠压	bool	/	有多路，则上传每路信息
n 号模块风扇故障	bool	/	有多路，则上传每路信息
n 号模块环境过温	bool	/	有多路，则上传每路信息
n 号模块 PFC 过温保护 1	bool	/	有多路，则上传每路信息
n 号模块 PFC 过温保护 2	bool	/	有多路，则上传每路信息
n 号模块 DC 过温保护 1	bool	/	有多路，则上传每路信息
n 号模块 DC 过温保护	bool	/	有多路，则上传每路信息

2			
n 号模块 PFC 故障	bool	/	有多路，则上传每路信息
n 号模块泄放电路异常	bool	/	有多路，则上传每路信息
n 号通信故障	bool	/	有多路，则上传每路信息
n 号模块启动失败	bool	/	有多路，则上传每路信息
n 号模块停止失败	bool	/	有多路，则上传每路信息
n 号模块交流输入故障	bool	/	有多路，则上传每路信息
n 号模块直流输出短路	bool	/	有多路，则上传每路信息
n 号模块其他故障	bool	/	有多路，则上传每路信息

5.4.4 电池数据

名称描述	数据类型	长度/字节	描述及要求
电池所在仓位编号	uint	16	仓位编号
事件编号	uint	32	事件编号共12位，前8位为本次事件起始日期，后4位流水号，每发生一次新事件，流水号自动加1，每日首次事件从0001开始循环累加。 例：202101010001
事件类型	uint	16	1.充电事件；2. 静置事件；3.放电事件
总电流	float	32	总电流-1000A~1000A
总电压	float	32	总电压0～1000V
soc	float	32	荷电状态
均衡状态	uint	16	当前均衡是否开启
绝缘阻值	uint	32	绝缘状态
继电器状态	uint	32	0：断开；1：闭合
事件充入电量	uint	32	0~2000 kWh
事件放出电量	uint	32	0~2000 kWh

最大单体电压	float	32	0～15V，65534:异常，65535:无效
最小单体电压	float	32	0～15V，65534:异常，65535:无效
最高温度	float	32	-40℃～+210℃,254:异常，255:无效
最低温度	float	32	-40℃～+210℃,254:异常，255:无效
最大单体电压编号	uint	16	1～250，254:异常，255:无效
最小单体电压编号	uint	16	1～250，254:异常，255:无效
最高采样温度编号	uint	16	1～250,254:异常，255:无效
最低采样温度编号	uint	16	1～250,254:异常，255:无效
单体电压列表	float	32	0V～60.000V，65534:异常，65535:无效
温度列表	float	32	-40℃～+210℃,254:异常，255:无效
平均电压	float	32	0V～60.000V，65534:异常，65535:无效
平均温度	float	32	-40℃～+210℃,254:异常，255:无效
进水温度	float	32	-40℃～+210℃,254:异常，255:无效
出水温度	float	32	-40℃～+210℃,254:异常，255:无效
电池故障等级	uint	8	0：正常；1：故障；
电池过压故障	uint	8	0：正常；1：故障；
电池欠压故障	uint	8	0：正常；1：故障；
电池温度过高故障	uint	8	0：正常；1：故障；
电池过流故障	uint	8	0：正常；1：故障；
电池电压一致性故障	uint	8	0：正常；1：故障；
电池温度一致性故障	uint	8	0：正常；1：故障；
电池绝缘故障	uint	8	0：正常；1：故障；

电池高压互锁故障	uint	8	0：正常；1：故障；
电池总压过压故障	uint	8	0：正常；1：故障；
电池总压过低故障	uint	8	0：正常；1：故障；

5.5 换电操作过程上报

5.5.1 换电握手过程

名称描述	数据类型	精度及范围	描述及要求
开始换电时间	String	系统时间，精确到毫秒	开始换电时间
结束换电时间	String	系统时间，精确到毫秒	结束换电时间
车辆电池实际soc	Uint	1个字节	车辆电池实际soc
服务电池实际 soc	Uint	1个字节	服务电池实际soc
握手结果	uint	1个字节	0：握手失败；1：握手成功
车辆id	String	/	准备换电车辆vin或车辆id
车型	String	/	准备换电车辆车型
车辆供应商	String	/	准备换电车辆车辆供应商
电池编号	String	/	车辆准备换电换入电池id
电池供应商	String	/	换入电池供应商
电芯结构	uint	1个字节	换入电池电芯结构（如圆柱/方壳/软包）
电芯类型	uint	1个字节	换入电池电芯化学体系（如三元/磷酸铁锂）
电芯容量	float	4	换入电池单体电芯容量
电池生产日期	date	/	换入电池电池pack生产日期
电池热管理类型	uint	1个字节	换入电池包热管理方式

电芯数量	byte	/	换入电池包电芯数量
累积充电电量	float	4	电池累计充入电量
累积里程	float	4	电池在所有车辆上行驶里程累积值
累积换电次数	uint	4	电池在所有换电站换电次数累积值
累积服役时间	uint	4	电池在所有车辆/换电站服役时间
电池健康状态	uint	1个字节	电池管理系统或换电站计算得到的健康状态值

5.5.2 换电操作过程

换电站确认后，在换电过程中，需要采集如下信息，并且立即上传。

名称描述	**数据类型**	**精度及范围**	**描述及要求**
操作流水号	string	/	唯一标示的换电id流水号
被操作电池编号	string	/	本次操作的电池编号
操作模式	string	/	0：换入，1：换出，
操作状态	string	/	0：操作启动；1：操作中； 2：操作完成；3：操作失败
操作失败原因	string	/	换电过程中产生的换电故障信息

5.6 补发信息上报

补发信息主要补发换电操作过程消息、实时消息。实时消息主要发电池数据和告警信息。告警信息主要补发BMS相关的告警值。

名称描述	数据类型	长度/字节	描述及要求
编码	Int	/	补发信息上报编码
补发时间	string	/	当前系统时间戳
补发消息类型	Int	/	0x01：换电操作过程消息 0x02：电池数据 0x03：告警信息
数据	string	/	换电操作过程消息/电池数据/告警信息

5.7 换电站登出

名称描述	数据类型	长度/字节	描述及要求
数据采集时间	Uint64	8byte/	换电站登出时间
登出流水号	String	/	登出流水号与当前登入流水号一致

6 故障监控及处置措施

换电站故障项	处置措施
换电站故障一级	风险提示，无措施
换电站故障二级	设备停机
换电站故障三级	整站停止运营
电池故障项	处置措施
电池故障一级	无措施
电池故障二级	暂停充电直至故障消失
电池故障三级	停止充电
电池过压故障	停止充电
电池欠压故障	停止充电
电池温度过高故障	停止充电
电池过流故障	停止充电
电池电压一致性故障	停止充电
电池温度一致性故障	停止充电
电池绝缘故障	停止充电
电池高压互锁故障	停止充电（可恢复）
电池总压过压故障	停止充电
电池总压过低故障	停止充电

换电站分别对换电站故障、电池故障、电池预警分别执行相应处置措施。

预警项	处置措施
电池绝缘异常预警	禁止换出
压差异常预警	禁止换出
温差异常预警	禁止换出

7 数据安全管理

7.1 基本要求

应根据平台系统的重要程度以及遭到破坏后的危害程度，参照 GB/T 22240 的规定确定其安全保护等级，并具备 GB/T 22239 规定的基本安全保护能力。

应根据平台系统的应用、数据和技术架构，将系统信息进行分等级管理，根据其重要程度划分安全信息区域，采取不同的系统安全保护措施，实现同等级信息集中管理。

7.2 数据信息完整性

应确保采取的数据信息管理和技术措施以及覆盖范围的完整性。

应能够检测网络设备操作系统、主机操作系统、数据库管理系统和应用系统的系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性措施采取必要的恢复措施。

应具备完整的用户访问、处理、删除数据信息的操作记录能力。

在传输数据信息时，经过不完全网络时，应对传输的数据提供完整性校验。

应具备完善的权限管理测试，支持权限最小化原则、合理授权。

7.3 数据信息保密性

数据信息保密性安全规范用于保障业务平台重要业务数据信息的安全传递与处理应用，确保数据信息能够被安全、方便、透明的使用。为此，业务平台应采用加密等安全措施开展数据信息保密性工作。

系统应采用密码技术保证通信过程中车架号、电池追溯码、车主信息等关键数据和隐私信息的保密性。（GB/T 22239，8.1.2.2 修改）

系统接口传输协议采用加密技术，确保数据信息传输的安全性。

应采用加密有效措施实现重要业务数据信息传输保密性。

应采用加密实现重要业务数据信息存储保密性。

7.4 数据信息备份与恢复

数据信息备份数据信息备份应采用性能可靠、不宜损坏的介质，如光盘、硬盘等备份数据信息的物理介质应注明数据信息的来源、备份日期、恢复步骤等信息，并置于安全环境保管。

系统应提供重要数据的本地数据备份或者云端数据定期备份功能，防止未经授权的备份数据访问。

系统应具备故障后数据恢复功能，应能实现本地数据和云端数据的同步。

运维操作员应根据不同业务系统实际拟定需要测试的备份数据信息以及测试的周期。

本地数据和云数据操作时需要具备相应权限，不同权限的人员只能对数据执行授权范围内的数据操作。

对于因设备故障、操作失误等造成的一般故障，需要恢复部分设备上的备份数据信息，遵循异常事件处理流程，由运维操作员负责恢复。

应尽可能地定期检查和测试备份介质和备份信息，保持其可用性和完整性，并确保在规定的时间内恢复系统。

应确定重要业务信息的保存期以及其它需要永久保存的归档拷贝的保存期;恢复程序应定期接受检查及测试，以确保在恢复操作程序所预定的时间内完成。

7.5 应用安全

系统应能对登录的用户进行身份标识和鉴别,只有在系统注册后合法用户才能接入。(前半句 GB/T 22239，7.1.4.1）

系统应对登录的用户分配账户和权限。