
# 上电科信息安全测评服务介绍

上电科2026年版本

# 1. 集团介绍

**上海电器科学研究所（集团）有限公司**创建于1953年，原直属国家机械工业部的事业单位，1999年按照国务院要求，转制为科技型企业，划归上海市。现已成为一家集**科技创新服务、国家产品检测、系统集成解决方案提供和高新技术产品**生产为一体的科技型企业集团。

**智能电网用户端与能源互联网**

用户端能源管理系统
微电网与分布式能源系统
用户端需求响应系统
智能电器与系统
低压直流设备与系统
智能照明与控制系统
电动汽车充换电设施平台

**智慧城市与智能交通**

基于大数据与智能网联的智慧交通
基于智能物联的智慧市政和智慧园区
基于视频AI赋能的智慧公共安全
基于数字孪生的云运维平台
基于VR技术的仿真实训平台

**智能制造与工业互联网**

数字化车间与智能工厂
产品智能柔性制造设备
智能综合试验与测试系统
基于机器视觉的质量系统
面向企业数字化转型服务的工业互联网平台
机器人研发与转化
机器人控制系统测试设备

**检测评估**

检测校准17025
认证服务17065
能力验证17043
检验评估17020
检测标准技术研究
检测数据云服务
在线智能检测
数字认证
数字化评估服务

**智慧节能**

超高效电机
电机绿色设计及制造
电机控制与系统节能
电机系统能耗监测与能效评估
企业能源监测及管理

**船用电气**

船用中低压电器元件
船用中低压成套设备
船用电机及控制系统
船用能量管理
船用电力电子
移动电站
核级配电设备

## 国家级技术创新平台

**国家工业互联网系统与产品质量监督检验中心**
国家汽车电气化产品及系统质量监督检验中心
国家机器人检测与评定中心（总部）
**国家机器人质量监督检验中心**
国家能源智能电网用户端电气设备研发（实验）中心
国家智能电网终端用户设备产业技术创新战略联盟
国家智能电网用户端产品（系统）质量监督检验中心
国家低压电器质量监督检验中心
国家中小电机质量监督检验中心
国家中小型电机及系统工程技术研究中心

## 标委会

全国低压电器标准化技术委员会 TC189
全国熔断器标准化技术委员会 TC340
全国低压设备绝缘配合标准化技术委员会 TC417
全国旋转电机标准化技术委员会 TC26
全国无线电干扰标准化技术委员会 TC79
全国电器设备网络通信接口标委会 TC411
全国机器人标准化总体组
IEC TC125(人员电气运输设备) (主席)
IEC/CISPR、IEC/CISPR B(电磁兼容)(副主席)
IEC/ACOS(风险评估) (专家参与)
IEC/SyC/SM(智能制造) (专家参与)
IEC TC2(电机)

# 2.1 信息安全测评——标准化检测评估项目

## 覆盖系统与产品全生命周期的服务能力

### 信息安全咨询服务

- 安全技术解决方案咨询
- 安全管理体系咨询

### 样品检测（CNAS+CMA）

- 模拟网络环境检测
- 设备和系统检测
- 应用安全检测
- 数据统计及分析

### 工业互联网漏洞挖掘（CNAS+CMA）

- AI算法智能化漏洞挖掘
- FUZZING漏洞挖掘


专注六大安全领域

### 信息安全评估服务（CNAS+CMA）

- 信息安全风险评估
- 信息安全基线检查

### 应用APP安全检测(CNAS+CMA）

- 应用对象（Android应用、iOS应用、微信小程序等），被测应用的运行环境
- 深度静态检测技术、动态检测技术、源代码扫描等，评估应用的安全风险

### 工业互联网信息安全建设与整改

- 针对检测评估过程中发现的问题，提出专业的整改方案
- 并按照客户实际需求修复信息安全隐患，降低信息安全风险

◆ 产品&系统级　　◆ 企业级

# 2.2 产品信息安全测评-定制化测试项目

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的下访问或破坏系统。

## ◆ 1.漏洞扫描的功能主要有：

1. 定期自我检测、评估
2. 启用新软件、新服务后的检查
3. 安全规划评估和成效检验
4. 安全性测试
5. 安全事故分析调查
6. 重大网络安全事件准备
7. 公安、保密部门安全性检查

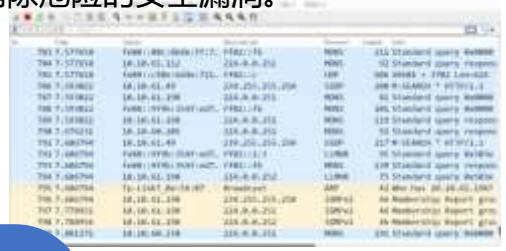
## ◆ 2.漏洞挖掘的主要作用有：

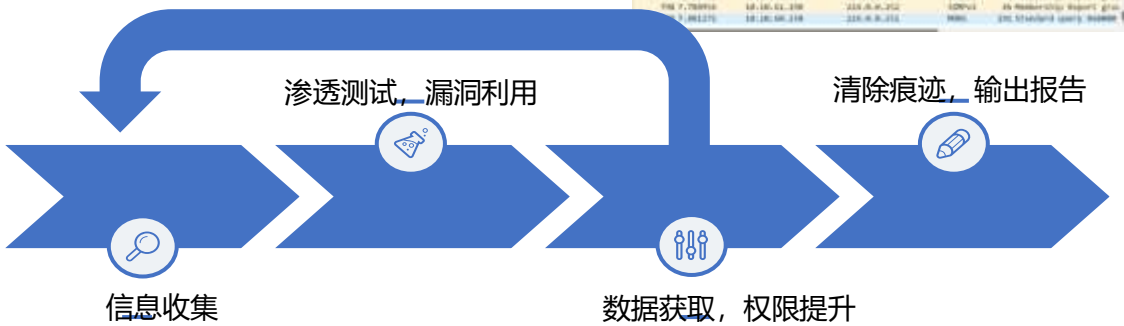
1. 发现未知漏洞、验证安全状况；
2. 采用智能挖掘技术进行安全性测试；
3. 深度挖掘漏洞，定位问题并提供测试细节；
4. 便于问题回溯，提升系统的安全性。

## ◆ 3.渗透测试

对其软件和系统进行设计时，应力争消除危险的安全漏洞。其中，渗透测试支持以下安全活动：

1. 找出系统的弱点；
2. 确定安全控制的可靠性；
3. 支持符合数据隐私和安全规范。





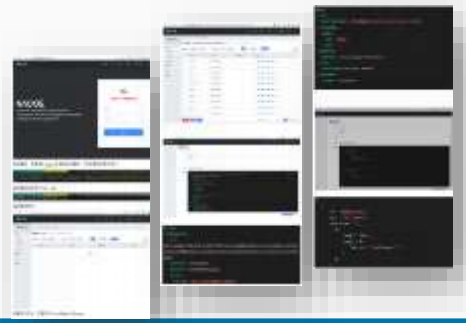

**GS应用系统及操作系统、数据库**

漏洞扫描&渗透测试

**检测结论：**系统包含Web、服务器等角度风险共12项：其中包含3项高危风险、3项中危风险、6项低危风险，涉及1例框架级权限与账户体系层面高危漏洞，1例框架级输入与输出层面中危漏洞。**判定结论为高风险。**

渗透测试

**测试结论：**最终问题在于nacos系统暴露在公网上，且存在漏洞，导致可以添加账户登入，查看微服务配置，拿到ak，sk等**重要敏感配置信息**，扩大攻击面和利用面。



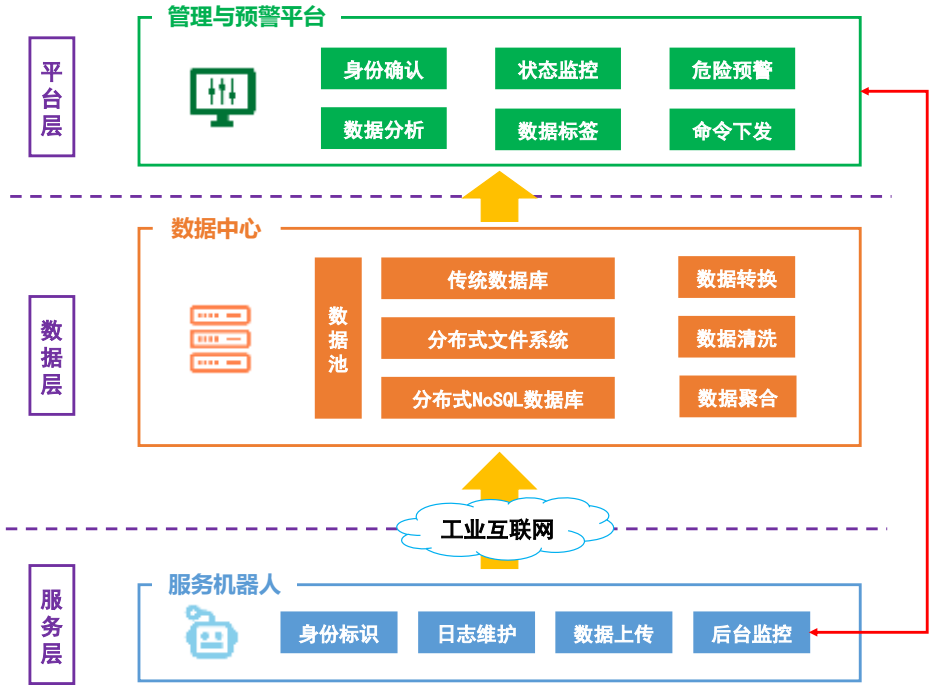
**TT云对象存储、微服务注册与发现中心**

# 2.3 产品信息安全测评——典型行业案例

## 服务机器人

- ***实现对服务机器人安全的全面监测预警***
- 全面获取服务机器人在线使用行为信息，包括服务机器人在线状态、业务访问情况等
- 充分利用大数据深度挖掘技术，实现安全态势感知，对服务机器人异常使用行为进行预警，如脱离既定位置、高频移动等

### 服务机器人信息安全监测与管理平台架构




### 服务机器人信息安全标准

STIEE

◆ 服务机器人信息安全标准生成

- 由上电科提出的服务机器人信息安全标准从流程级到高安全级分为五个等级
- 随后生成服务机器人信息安全测评要求和方法



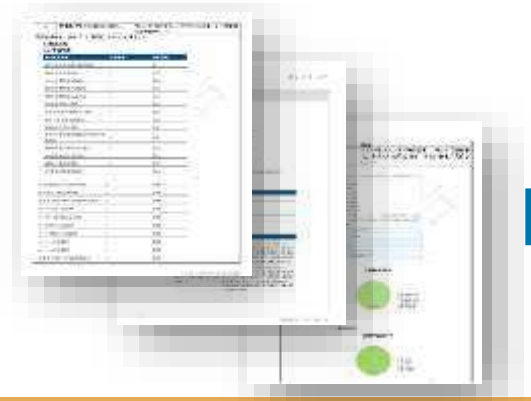
两份试验用样品

# 2.3 产品信息安全测评——典型行业案例

## 充电桩和充电平台


典型场景


建模建标



迭代交付

上海市电动汽车充放电设施
聚合交易平台项目建设方案

场景扩展

从设备到系统方案

### 设备入场

### 充电桩信息安全测试

### 智慧电能场景下的安全检测

截至2026年07月，充电桩业务共已检测超过180单，依据 T/CEC 208-2019对充电桩信息安全进行检测。检测内容包括但不限于充电桩内部存储机制，充电桩与平台间通信，日志留存，与人员权限等。

### 智能充电桩行业信息安全普遍分析

**41% 高风险项**

- 操作系统未保证代码可控、本体代码未保证完整性且不具备认证机制
- 本地和传输数据不能保证数据有效性、完整性、保密性
- 无身份认证及权限划分
- 未关闭非系统运行和维护所必需的网络通信端口
- 审计记录未定期备份且可修改
- 外部访问接口无安全保护措施

约90%充电桩存在高风险信息安全隐患

**24% 中风险项**

- 充电设备不具备异常告警功能
- 未采用最小化安装方式配置软件
- 未采用权限划分最小特权原则

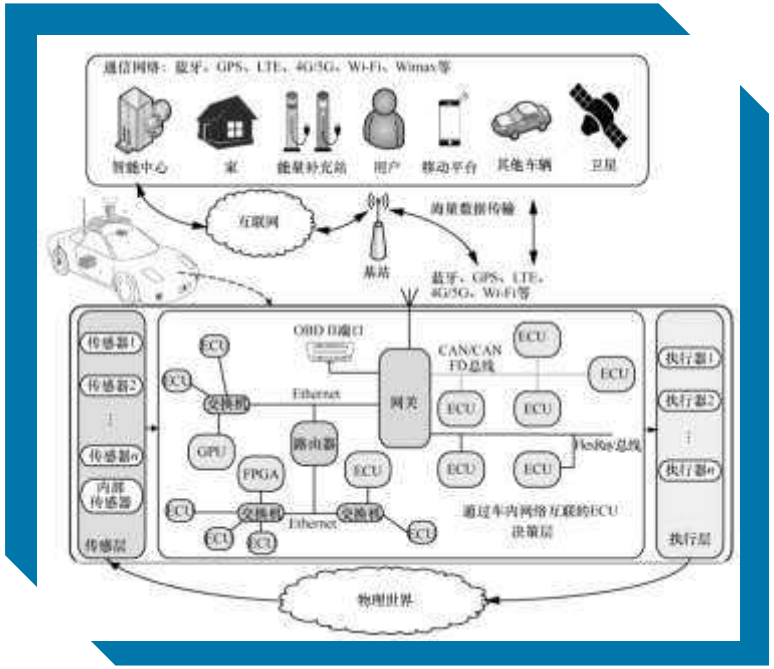
**35% 低风险项**

- 物理防护不到位
- 充电设备不具备控制接入的开关
- 本地审计日志留存能力不足

约30%充电桩存在中低风险信息安全隐患

# 2.3 产品信息安全测评——典型行业案例

## 智能网联车

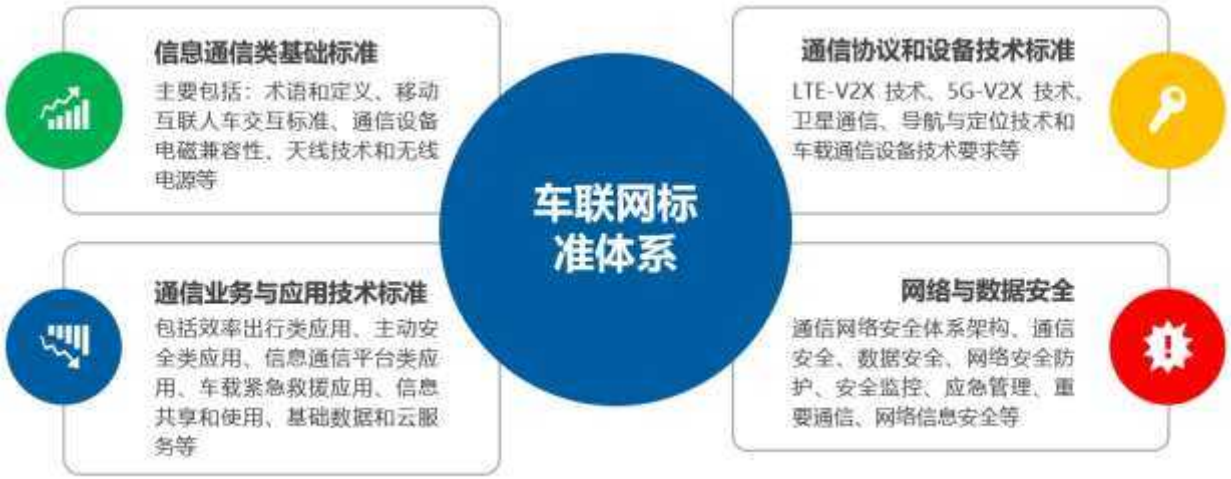



| 产品类别 | 占比 |
|---|---|
| T-box | 55% |
| 雷达 | 6% |
| 天线 | 22% |
| 收音机 | 11% |
| 其他 | 6% |

**车载T-box、5G制式条件下通信安全测试**

衍生的信息安全测试有：

1、车载T-Box 通信安全测试
2、车载定位系统安全测试
3、紧急呼叫系统安全测试
4、无钥匙进入系统安全测试
5、 WIFI/蓝牙安全测试
6、 V2X信息安全测试/5G




### 智能网联汽车场景下的信息安全与通信安全

某公司ESCL产品

**测试结论**

模糊测试以及渗透测试共测试15项，其中7项符合，4项不符合，4项不适用，不符合项目有：
1）产品不具备加密通信功能；
2）会话无法自动关闭；
3）产品未记录审计日志；
4）产品不具备防恶意指令嵌入的机制。

**整改建议**

从成本效益出发，对产品提出实际可行的整改建议，满足信息安全相应要求：
1）建议增加会话超时功能，实现会话在固定时间不活动后，自动关闭；
2）建议增加输入验证功能，对输入的数据、信息或命令进行验证与把控。

某公司BNCM产品

渗透测试共测试14项，其中14项符合，0项不符合，0项不适用。

产品目前已满足信息安全相关要求，建议后期产品运行维护过程中配合相应监控、审计流程，实现产品全生命周期信息安全。

# 2.3 产品信息安全测评——典型行业案例

## 医疗器械

医疗器械信息安全受国际国内法规条例监管，如：

- 美国食品药品监督管理局
- 《YY/T 1843-2022医用电气设备网络安全基本要求》
- 《医疗器械网络安全注册技术审查指导原则》


医疗器械试验样品

漏洞扫描 → 渗透测试 → 用户文档集核查 → 网络安全能力要求

漏洞扫描报告

查验用户文档集，核对其是否满足4.2的标识、管理职能等要求以验证符合性。

# 2.3 产品信息安全测评——典型行业案例

## 无线电设备

**适用范围**

所有进入欧盟市场的无线电设备

**法律地位**

RED指令下的强制性协调标准

**市场意义**

CE认证的必要前提，市场准入关键




无线电设备试验样品



# 2.4 企业信息安全测评——网络安全分级评估

## 01 制定评定规则

工业和信息化部选择重点行业或区域开展分类分级试点，细化**联网工业企业分级评定参考规则**，形成评定规则。

1 2

## 02 企业自评

1 2 3 4 5 6

依托工业互联网企业网络安全分类分级管理服务平台，联网工业企业在线填报问卷，形成**自评报告**。

## 03 核查确认

地方主管部门可自行或组织第三方专业服务机构对企业提交的自评报告**真实性、完整性**进行核查，发现信息不真实、不完整的，通知企业予以补正后进行确认。

3 4 5 6

## 04 级别变更

1 2 3

当联网工业企业网络安全风险程度发生**重大变化**时，应主动重新定级

1 **定级咨询服务**

系统调查、系统定级、定级报告、专家评审、协助备案

2 **风险评估服务、差距评估服务**

测评准备、方案编制、现场评估、报告编制

3 **安全规划与整改方案设计服务**

安全需求分析、安全策略设计、解决方案设计、安全建设规划

4 **整改集成实施服务**

技术整改、管理整改、安全加固、安全培训

5 **协助测评服务**

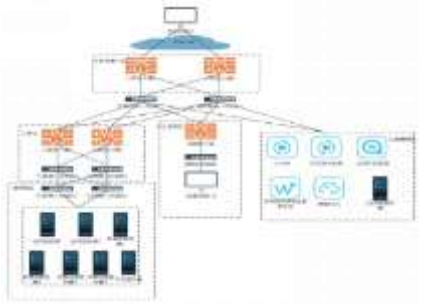
测评准备、协助测评

6 **安全运维服务**

安全巡检、应急响应、安全通告、售后服务


**某租赁住房管理系统等级测评报告**

本次测评按照测评项汇总并分析后，共发现安全问题44个，其中高风险问题0个，中风险问题31个，低风险问题13个；选取的测评指标总数为211个，不适用指标为13 个，测评结论为中。



# 2.5 扩项标准清单

| 编号 | 标准号 | 标准名称 | 授权范围 | 授权机构 |
|---|---|---|---|---|
| 1 | GB/T 34975-2017 | 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法 | 5.1 5.2 | 中国合格评定国家认可委员会 |
| 2 | GB/T 37931-2019 | 信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法 | 7.1.1 7.1.2 7.1.3 7.2.1 7.2.2 7.2.3 | |
| 3 | GB/T 37954-2019 | 信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法 | 7.1 7.2 7.3 | |
| 4 | GB/T 37953-2019 | 信息安全技术 工业控制网络监测安全技术要求及测试评价方法 | 7.1 7.2 | |
| 5 | EDSA-406-2.01 | EDSA-406 ISA安全遵从协会-嵌入式设备安全保证-测试IPv4或IPv6上IETF TCP传输协议实现的健壮性 | TCP.T00 TCP.T01 TCP.T02 TCP.T03 TCP.T04 TCP.T05 TCP.T06 TCP.T07 TCP.T08 TCP.T09 TCP.T10 TCP.T11 TCP.T12 TCP.T13 TCP.T14 TCP.T15 TCP.T16 TCP.T17 TCP.T18 TCP.T19 TCP.T20 TCP.T21 TCP.T22 TCP.T23 TCP.T24 | |
| 6 | T/CEC 208-2019 | 电动汽车充电设施信息安全技术规范 | 5.2.1 5.2.2 5.2.3 | |
| 7 | GB/T 41578-2022 | 电动汽车充电系统信息安全技术要求及试验方法 | 5.2 5.3 5.4 5.5 | 中国计量认证 |
| 8 | Q/GDW 10597-2022 | 应用软件系统通用安全技术要求及测试规范 | 6.1 6.2 6.3 6.4 6.5 6.6 6.7 6.8 6.9 6.10 6.11 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 7.11 7.12 7.13 | |
| 9 | GB 40050-2021 | 网络关键设备安全通用要求 | 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.9 5.10 | |
| 10 | YY/T 1843-2022 | 医用电气设备网络安全基本要求 | 4.1 4.2 4.3.1 4.3.2 4.3.3 4.3.4 4.3.5 4.3.6 4.3.7 4.3.8 4.3.9 4.3.10 4.3.11 4.3.12 4.3.13 4.3.14 4.3.15 4.3.16 | |
| 11 | IACS UR E27 | 船载系统和设备网络韧性统一要求 | 2.1 2.2 2.3 2.4 3.1 3.2 3.3 4.1 4.2 | |
| 12 | IEC 62443-4-1:2018 | 工业自动化和控制系统信息安全<br>第4-1部分：产品安全开发生命周期要求 | 9.2 9.3 9.4 9.5 9.6 | |
| 13 | EN 18031-1:2024 | 无线电设备通用安全要求第1部分：联网的无线电设备 | 6.1 6.2 6.3 6.4 6.5 6.6 6.7 6.8 6.9 6.10 6.11 | 中国合格评定国家认可委员会 中国计量认证 美国实验室认可协会 |
| 14 | EN 18031-2:2024 | 无线电设备通用安全要求第2部分：具有数据处理功能的无线电设备，即联网的无线电设备、儿童监护无线电设备、玩具无线电设备和可穿戴无线设备 | 6.1 6.2 6.3 6.4 6.5 6.6 6.7 6.8 6.9 6.10 6.11 | |
| 15 | EN 18031-3:2024 | 无线电设备通用安全要求第3部分：<br>带支付功能的无线电设备 | 6.1 6.2 6.3 6.4 6.5 6.6 6.7 6.8 6.9 | |

# 3 联系我们



上海电器设备检测所有限公司
地址：上海市武宁路505号（曹杨路800号）
Email：marketing@seari.com.cn
市场部：021-62574990-644