ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL 151—2025

低碳汽车制造工厂 工业内网渗透测试与安全防护规范

Specification for Intranet Penetration Testing and Security Protection of Low-Carbon Automotive Manufacturing Plants

征求意见稿

2025 - - 发布　　2025 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

低碳汽车制造工厂 工业内网渗透测试与安全防护规范

一、引言

随着汽车制造行业向低碳化、智能化、网联化深度转型，工业互联网、物联网技术在冲压、焊接、涂装、总装等核心工艺环节广泛应用，生产网络与信息网络的融合程度不断加深。这一趋势在提升生产效率、降低碳排放的同时，也显著扩大了网络攻击面，使得工业内网面临前所未有的安全威胁。针对工业控制系统的网络攻击可能导致生产中断、质量缺陷、设备损坏，甚至引发安全事故，直接危及人员生命财产安全与低碳目标的实现。当前，低碳汽车制造工厂在工业内网安全方面普遍存在网络边界模糊、安全防护措施不足、渗透测试不规范、应急响应机制不健全等问题。为系统性地提升工业内网的安全水位，特制定本标准。本标准聚焦于工业内网渗透测试的方法论、实施流程、风险评估以及与之配套的安全防护体系建设，为低碳汽车制造工厂构建纵深防御能力提供标准化指引。

二、范围

本标准规定了低碳汽车制造工厂工业内网渗透测试与安全防护的术语和定义、总体原则、渗透测试流程、渗透测试内容与方法、安全防护体系架构、安全防护技术要求、安全管理要求、应急响应与持续改进以及附则。本标准适用于采用低碳制造工艺（如轻量化材料应用、绿色涂装、能源回收等）的汽车制造工厂，对其工业内网（包括生产控制网、制造执行系统网络、工业物联网等）进行渗透测试的方案设计、组织实施、结果评估，以及后续安全防护体系的规划、建设与运维。参与工厂工业网络安全工作的运营单位、系统集成商、安全服务提供商及评估机构可参照使用。

三、规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

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

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 30976.1-2019 工业控制系统信息安全 第1部分：评估规范

GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 36637-2018 信息安全技术 工业控制系统信息安全防护能力评价方法

《中华人民共和国网络安全法》（2017年6月1日起施行）

《中华人民共和国数据安全法》（2021年9月1日起施行）

《工业控制系统信息安全防护指南》（工信部信软〔2016〕338号）

《网络产品安全漏洞管理规定》（工信部联网安〔2021〕66号）

四、术语和定义

下列术语和定义适用于本标准。

（一）低碳汽车制造工厂

在汽车生产制造全过程中，通过应用清洁能源、节能技术、环保材料及资源循环利用等手段，显著降低能源消耗与温室气体排放的现代化汽车制造工厂。

（二）工业内网

支撑低碳汽车制造工厂生产运营的专用网络环境，包括连接可编程逻辑控制器、分布式控制系统、数据采集与监视控制系统、工业机器人、智能传感器、制造执行系统等工业控制设备与系统的网络总称。

（三）渗透测试

在授权和可控的前提下，模拟恶意攻击者的思维和技术，对工业内网中的系统、网络、应用程序进行的安全性测试与评估，旨在发现其中存在的安全漏洞和脆弱性。

（四）安全防护体系

为保障工业内网安全而建立的一系列技术措施、管理策略与运行机制的集合，形成纵深防御能力。

（五）工业防火墙

专门用于工业控制网络环境，能够识别和解析工业协议，并根据安全策略对网络流量进行访问控制的安全设备。

（六）安全运营中心

负责对工业内网进行集中安全监控、分析、预警和响应的组织单元与技术平台。

五、总体原则

（一）安全与生产并重

安全防护措施的部署与渗透测试的实施必须以不影响生产系统的连续性与稳定性为前提，任何操作均需经过充分评估与授权。

（二）预防为主，综合防范

构建以识别、防护、检测、响应、恢复为核心的主动防御体系，强调事前预防与事中控制，降低安全风险。

（三）重点防护，纵深防御

针对冲压、焊接、涂装、总装等核心生产区域及其控制系统进行重点防护，构建从网络边界到核心控制设备的纵深防御体系。

（四）动态感知，持续改进

通过持续的监控、定期的渗透测试和风险评估，动态感知安全威胁，并基于评估结果持续优化安全防护策略与技术措施。

（五）合规性与针对性结合

安全防护与测试活动既要符合国家网络安全等级保护制度及相关标准要求，又要紧密结合低碳汽车制造工厂的特定业务场景与技术架构。

六、渗透测试流程

（一）测试前准备

成立由工厂运营方、安全专家及必要时的系统供应商组成的联合测试团队。明确测试范围、目标、时间窗口及中止条件。测试范围应至少覆盖工厂级监控网络、车间级控制网络以及关键现场总线网络。必须获取工厂最高管理层的书面授权，授权书需明确测试边界与行为规范。制定详细的测试方案与应急预案，并在测试前 3 个工作日通知可能受影响的业务部门。

（二）信息收集

在授权范围内，通过被动扫描、公开信息源查询、社会工程学（需特别授权）等方式，收集目标网络的拓扑结构、IP 地址段、开放的端口与服务、使用的工业协议（如 PROFINET, EtherNet/IP, MODBUS TCP）、设备型号与版本信息、系统架构等。

（三）威胁建模与漏洞分析

基于信息收集结果，构建工业内网的威胁模型，识别潜在攻击路径。利用专业的工业漏洞库（如

CNVD, CNNVD, NVD）及漏洞扫描工具，对识别出的资产进行漏洞扫描与分析。对于高可用性要求的核心控制系统，漏洞扫描应在离线测试环境或生产系统的维护窗口期进行，且扫描策略应为非侵入式。

（四）漏洞利用与验证

在严格可控的环境下，对中、高风险漏洞进行模拟利用，以验证漏洞的真实性与危害程度。严禁对在线运行的核心控制系统（如焊接机器人控制器、喷涂机器人 PLC）进行可能引发停机的攻击测试。此类验证应在仿真环境中进行。

（五）后渗透测试

在成功利用漏洞获取初步访问权限后，测试权限提升、横向移动、持久化驻留等攻击链后续环节的可能性，以评估整个内网的安全状况。

（六）报告编制与评审

测试结束后 10 个工作日内，应出具详细的渗透测试报告。报告内容应包括：执行摘要、测试过程与方法、发现的漏洞清单（附详细描述、风险等级、CVSS 评分、受影响资产）、漏洞利用证据、风险分析、整改建议。报告需经过测试团队与工厂运营方共同评审确认。

（七）复测

在工厂完成高危漏洞整改后，应在 1 个月内安排复测，以验证整改措施的有效性。

七、渗透测试内容与方法

（一）网络架构安全测试

测试网络分区隔离的有效性，检查不同安全区域（如生产监控区、过程控制区、现场设备区）之间

的访问控制策略是否合理。尝试跨越 VLAN 或工业防火墙进行非授权访问。

（二）工业协议安全测试

针对 MODBUS TCP、OPC UA、PROFINET 等常用工业协议，测试其通信的机密性、完整性与可用性。检查是否存在协议滥用、未授权命令执行、中间人攻击等风险。

（三）主机与设备安全测试

对工业上位机、工程师站、操作员站、HMI 及 PLC 等控制器进行安全配置检查与漏洞扫描。测试内容包括但不限于：弱口令检查、不必要的服务与端口、补丁管理状况、防病毒软件部署等。其中，口令策略应强制要求长度不少于 8 位，且为数字、字母、特殊字符混合组成，并定期（如 90 天）更换。

（四）无线网络安全测试

对工厂内的 Wi-Fi、4G/5G 等无线接入网络进行安全评估，测试其认证机制、加密强度及接入控制策略，防止通过无线网络渗透至工业内网。

（五）物理安全与社会工程学测试

（需单独授权）测试对关键工业控制区域的物理访问控制有效性，或通过模拟钓鱼邮件、电话欺诈等方式，评估员工的安全意识水平。

八、安全防护体系架构

（一）安全分区

根据 GB/T 30976.1，将工业内网划分为多个逻辑安全区域，如企业管理区、生产监控区、过程控制区、现场设备区、DMZ 区等。区域间通过工业防火墙、网闸等设备进行隔离，并遵循"最小权限"原则

配置访问控制列表。

（二）网络通信防护

在生产控制网络内部及与其他网络的连接处部署工业防火墙，深度解析工业协议，实现基于“白名单”的精细访问控制。对跨越不同安全区域的敏感数据（如生产配方、工艺参数）进行加密传输。关键控制指令的通信应使用校验码或数字签名技术保障完整性。

（三）计算环境防护

对工业上位机、服务器等主机系统实施安全加固，包括拆除或禁用非必要软硬件、严格账户与权限管理、部署兼容性好的主机防护软件。操作系统、数据库及工业应用软件的漏洞补丁，应在测试验证后，于计划停机期内及时安装。对于无法打补丁的系统，应部署虚拟补丁等补偿性控制措施。

（四）物理与环境安全

对中央控制室、关键设备间等核心区域实施严格的物理访问控制，如采用门禁系统、视频监控、专人值守等措施，并记录访问日志，日志保存时间不少于 180 天。

九、安全防护技术要求

（一）入侵检测与防御

在网络关键节点部署工业入侵检测系统，具备对异常网络流量、已知攻击特征及违反工业协议规范的行为进行检测和告警的能力。检测规则库应至少每周更新 1 次。

（二）安全审计

部署统一日志审计系统，集中收集网络设备、安全设备、操作系统及工业应用的操作日志、安全事

件日志。对关键用户行为（如权限变更、组态下载、程序修改）和重要系统事件进行记录和分析，审计记录保存时间不应少于 12 个月。

（三）恶意代码防范

在保证系统兼容性与稳定性的前提下，在工程师站、操作员站等 Windows 主机部署防病毒软件，病毒库应至少每天更新 1 次。禁止在稳定性要求极高的实时控制设备（如某些型号的 PLC）上安装防病毒软件。

（四）集中安全管理

建议建立安全运营中心或采用统一的安全管理平台，实现对各安全组件（防火墙、IDS、审计系统等）的策略配置、状态监控、事件关联分析与统一运维。

十、安全管理要求

（一）安全策略与制度

制定覆盖网络、系统、数据、物理及人员安全的全面管理制度，包括但不限于：《网络安全管理办法》、《账户与权限管理制度》、《变更管理规定》、《渗透测试管理办法》等，并每年至少评审和更新 1 次。

（二）人员安全管理

对所有接触工业内网的员工、承包商进行背景审查和安全培训，签订保密协议。实施岗位职责分离，关键操作（如控制逻辑修改）需双人复核。定期开展安全意识教育，每年至少 1 次。

（三）供应链安全

在与设备供应商、系统集成商、服务提供商签订的合同中，明确其安全责任与义务。对引入的第三方设备、软件和服务进行安全评估。

（四）安全运维管理

建立规范的资产台账和网络拓扑图，并及时更新。所有系统变更需通过正式的变更管理流程审批。严格管理移动存储介质的使用。

十一、应急响应与持续改进

（一）应急预案

制定针对不同安全事件（如病毒爆发、网络攻击导致停机、数据泄露）的应急预案，明确指挥体系、处置流程、恢复步骤及沟通机制。预案应至少每年组织 1 次桌面推演或实战演练。

（二）应急响应

设立 7x24 小时应急响应联络点。一旦发生安全事件，立即根据预案启动响应，遏制攻击、消除影响、恢复系统，并按照规定及时向主管监管部门和上级单位报告。

（三）持续改进

建立网络安全度量体系，定期（如每季度）评估安全防护体系的有效性。将渗透测试、风险评估、应急演练、安全审计中发现的问题纳入持续改进流程，不断完善安全防护措施。工厂应每年至少进行 1 次全面的工业内网风险评估。

十二、附则

本标准由广西电子商务企业联合会负责解释。本标准自发布之日起试行，试行期为一年。试行期满

后，根据实施反馈情况进行修订和完善。各低碳汽车制造工厂及相关单位可依据本标准制定具体的实施细则。若本标准与国家新颁布的法律法规或强制性标准有不一致之处，应以国家法律法规和强制性标准为准。本标准所引用的规范性文件如有更新，其最新版本适用于本标准。广西电子商务企业联合会将根据技术发展和应用需求，适时组织对本标准的复审与修订工作，以保障其持续的先进性和适用性。本标准的有效实施，有赖于工厂管理层、运营团队、安全专业人员及所有员工的共同参与和严格执行，共同构筑低碳汽车制造工厂的网络安全防线。