【密级：公开】

项目白皮书

厚德 明理 慎独 求是

目录

1 产品概述

1.1 产品简介

图 1-1 灵通测欢迎界面

灵通测是一款由 BFS（北京森林工作室）自主研发的跨平台、高兼容、集成化的模糊测试平台。平台主要面向安全测试及漏洞挖掘任务，支持对多平台（Windows/Linux/Android）应用程序、公有/私有通信协议、工控硬件设备等进行模糊测试，通过自动化快速生成大量测试用例挖掘测试对象的潜在缺陷，辅助安全工程师进行产品测试和维护工作。平台已集成目标分析、数据解析、属性修正、任务建模、用例生成、状态监测、实时测控、报告生成等功能，用户可基于 XML 格式灵活构建测试套并调用多元测试接口，形成了多位一体的全方位模糊测试框架。测试过程中，变异权重、变异算子等关键参数支持自定义设置。平台实现了多领域、个性化的测试场景全覆盖，提升了测试过程中的异常覆盖率和漏洞挖掘效率，显著降低测试人工成本，垂直赋能安全防护技术体系、辅助企业快速构建良好安全开发生态。

1.2 产品架构

灵通测模糊测试平台采用 B/S 架构开发，用户可以使用浏览器进行测试任务部署、测试用例分析等操作，有效避免了单机产品复杂的安装部署问题，其系统架构图如**错误!未找到引用源。**所示。系统架构包含 4 层，层内模块间相对独立，可独立维护升级，也可根据用户需求进行定制化开发部署。

业务展现层：平台采用前后端分离模式进行开发，业务展现层提供平台人机

交互接口，通过 API 服务与后端服务进行通信。涵盖了测试种子设置、断点设置、参数设置、监视器设置以及测试可视化、测试报告查阅等功能，实现面向多元测试对象的全自动化模糊测试。

业务逻辑层：共包含测试引擎调度、数据变异、状态模型运行、测试代理及内数据处理 5 大模块。测试引擎调度模块用于处理前端请求并依据路由进行测试任务调度，可根据测试对象的数据计算量进行灵活的多任务并发处理，自动进行测试统筹。数据变异模块用于变异策略选择，依据变异算子指导测试用例生成，可同时满足简单和复杂分层类型数据生成。状态模型运行模块用于维护每一个测试用例的有限状态机、管理测试任务的开始结束，并且支持用户自定义状态操作及操作触发条件。测试代理模块与测试引擎间建立通信，通过为测试对象设置的状态监视器进行多维状态监测、执行控制操作，可同时满足本地、远程动态测试要求。模型内数据处理模块负责对解析的测试套进行数据的分析、转换或修正，其中文件分析与转换支持 17 种类型数据文件，数值修正支持 24 种协议数据。

数据逻辑层：负责数据资源层与业务层逻辑间的交互操作，能够解析测试套配置文件并将其映射为数据模型、状态模型，并完成测试引擎及代理的初始化。测试套配置文件设置为 XML 格式，降低了测试套构建的复杂度、提高了可读性及测试可解释性。

数据资源层：将资源进行独立封装，可适应不同的数据存储方案。支持分布式存储、多节点集群部署，满足企业级高可用、高响应、高稳定、高并发的需求。

1.3 产品特性

1. 规则化测试套构建：测试套配置基于 XML 格式实现，系统依据配置自动生成数据及状态模型，指导测试用例生成，实现与测试端交互。XML 格式配置文件具备良好的语法规范，可解释性强，可有效简化测试配置流程，提升测试前期准备工作效率。
2. 个性化任务定制：除系统内置的百余种建模组件、变异配置外，支持用户自定义测试任务的变异权重和变异算子，可针对性对测试任务的每一个细节内容进行变异，能够满足用户多样化测试需求。同时支持自定义功能扩展插件的二次开发，更好适配不同场景下的测试任务。
3. 多元测试接口：平台测试接口涵盖应用层、系统层、协议层、数据层且支持

持续扩展，可实现对公有/私有通信协议、多平台应用程序（Windows、Linux、Mac、Android）、操作系统、工控/车控硬件设备、接口库、API 库等进行系统全面的测试，兼容多格式测试对象，针对性生成测试用例发现潜在缺陷，一站式满足多领域测试需求。

4. 人性化辅助分析：支持对用户提供的未知数据结构和交互流程进行辅助分析，自动生成数据模型和测试流程，帮助用户完成测试套开发。
5. 全异步架构：整个架构基于异步消息、异步方法、异步 HTTP 调用三种方式，保证每个层次模块均能实现异步操作，单节点可并发接收被测端上万条 API 请求，秒级解析模型生成测试用例。
6. 交互式实时数据展示：所有测试信息通过前端界面实时反馈，支持多维图形化展示，帮助测试人员时刻掌握任务状态；同时支持用户自由地进行数据提取、筛选、排序，满足测试推演分析需要。
7. 测试历史可追踪溯源：系统默认设置四十余种监视器全方位审计异常状态且支持持续扩展，自动记录测试全流程，支持异常点快速定位与追踪，任意测试流程重现，有助于漏洞快速发现与定位。

2 产品功能

2.1 测试对象数据模型构建

用户可以根据测试对象本身的结构或收发数据的结构，使用系统提供的数据元素构建测试所需的数据模型，作为后续变异和用例生成的原始种子。

2.2 测试用例生成

系统参照数据模型，按照配置的变异策略对数据模型进行变异，生成新的测试用例。

2.3 测试流程构建

系统可以根据测试对象的运行时状态和收发数据的过程设计测试状态模型，实现高自动化的测试流程。

1. 相关参数配置：提供默认参数配置，且用户可添加参数，新增自定义参数及

其配置。

图 2-1 配置相关参数页面

2. 配置数据监控：提供代理和监视器自定义配置，可为测试套添加一个或多个代理，且配置一个或多个监视器。

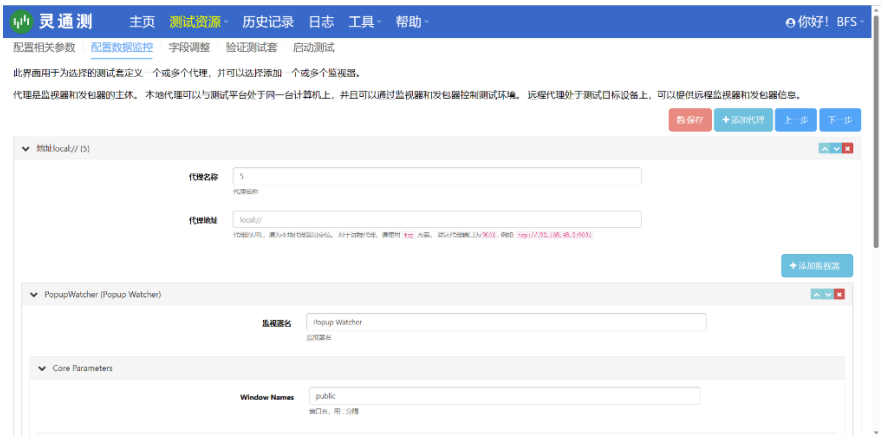

图 2-2 配置数据监控页面

3. 字段调整：快速查找字段，自定义字段测试用例生成频率，提升测试定制化程度。

图 2-3 字段调整页面

2.4 测试对象状态监视

系统提供了丰富的监视接口，可以满足多领域的监视需求，提供充分的测试对象的运行状态和数据。

实时测试状态监视：用户实时可视测试运行过程的核心信息和详细日志，对测试流程可知、可控。

图 2-4 实时测试状态页面

2.5 测试对象通信与交互

系统提供了丰富的通信交互接口，可以满足用户与测试对象的交互需求。

2.6 测试辅助功能

系统不仅可以详细记录测试流程中的交互数据和过程，复现历史测试流程，追踪测试对象的状态，辅助用户分析测试对象的潜在缺陷；还可以对用户提供的

未知数据结构和交互流程进行分析，自动生成数据模型和测试流程，辅助用户开发测试套。

1. 验证测试套：验证用户配置参数是否有误，陈列可能对测试任务产生影响的内容，辅助用户修改测试参数配置，构建更合理的配测试套项目。

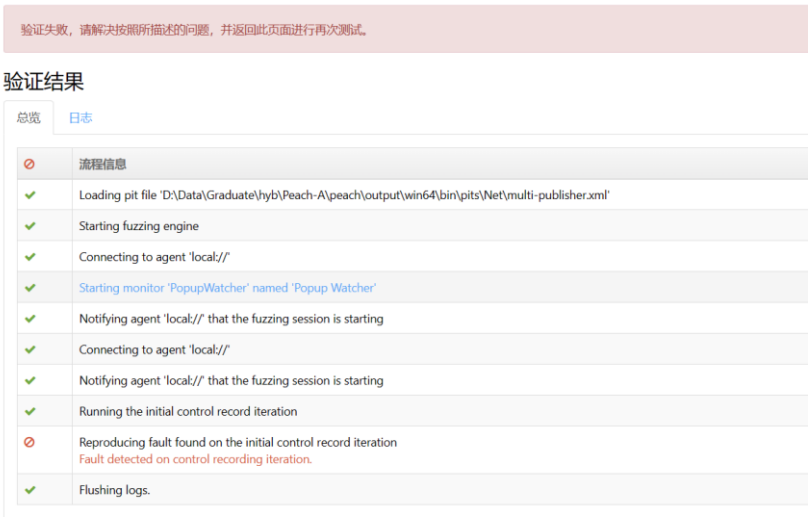

图 2-5 测试套验证失败示例

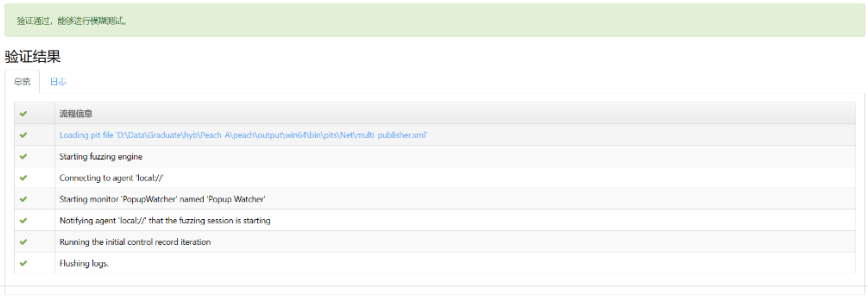

图 2-6 测试套验证通过示例

2. 历史记录查询：系统保存用户测试项目结果，提供丰富的历史记录查询内容，包括 8 项统计数据：故障总览、突变因子、突变记录、相关元素、状态统计、数据集、存储变化时间轴、Bucket。

图 2-7 历史记录故障总览页面

图 2-8 故障详情

图 2-9 历史记录突变因子页面

图 2-10 历史记录相关元素页面

3. 变异复现：基于突变记录，开展单轮或多轮变异复现，实现用例解析。

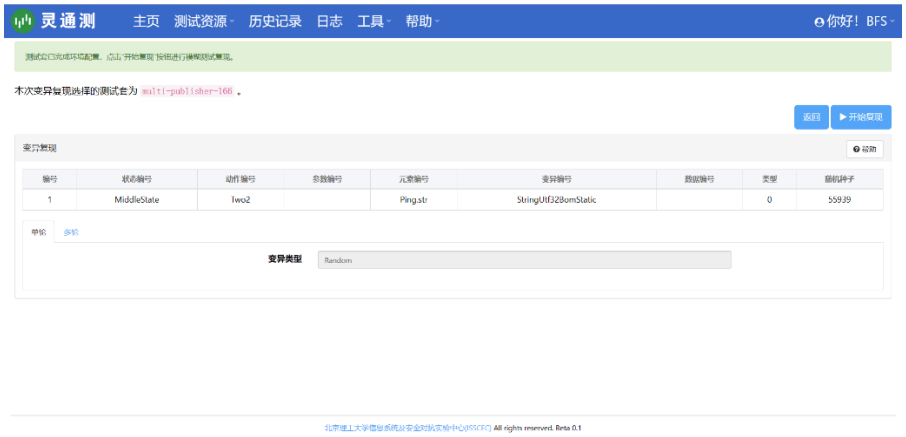

图 2-11 变异复现页面单轮设置

图 2-12 变异复现页面多轮设置

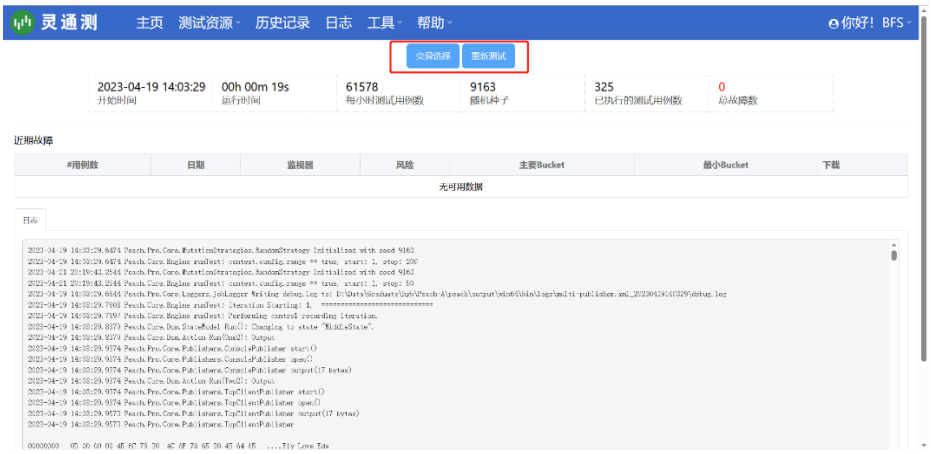

图 2-13 变异复现运行页面

2.7 二次开发接口

系统考虑了可扩展性和用户自定义的需求，用户可以根据需要编写并使用自定义的功能模块、测试辅助的脚本和新的测试套，极大地扩展了平台的适用范围，延长了平台的生命周期。

1. 协议逆向工具：根据用户上传的协议文件，提供专属测试套生成。解析用户文件内容，获取特定类型协议；解析协议内容，为协议构建数据模型和状态模型；生成测试套文件，构建平台测试资源。

图 2-14 协议逆向工具数据处理页面

图 2-15 协议逆向工具文件生成页面

2. 最小集生成工具：为用户上传的目标测试程序提供最大代码覆盖率所需的最小示例文件子集。

图 2-16 最小集生成工具页面

3. 风暴攻击工具：提供测试套代理自定义功能，可为测试套配置一个或多个代理，并可以选择添加一个或多个监视器。自定义代理后，可即刻配置测试参数、开展测试。

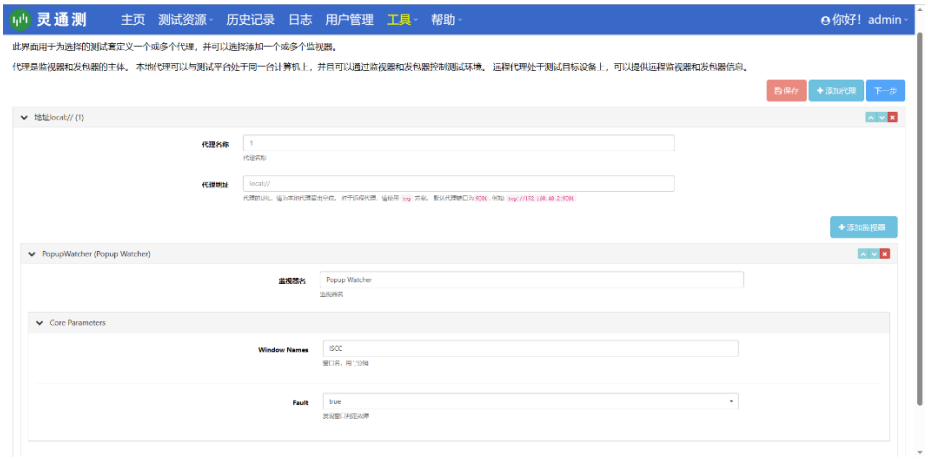

图 2-17 风暴攻击工具代理配置页面

图 2-18 风暴攻击工具测试参数配置页面

2.8 详细功能列表

功能	子功能	描述
数据模型构建	数据元素调用	支持使用数字、十六进制数值、字符串、无格式数据、外部文件数据等数据类型构建数据模型。
	数据元素修正	动态计算并修正数据元素的值，比如计算数据元素的长度、计算数据元素的校验和等。

	数据元素转换	转换引用元素的初始值，并替换初始值，比如 SSL 证书转换、散列算法转换等。
	数据元素分析	分析引用元素的初始值，提取目标信息后替换初始值，比如 HTML 响应包分析等。
测试用例生成	变异策略与变异算子生成	根据策略变异数据模型的元素，生成大量测试用例，策略内包含众多变异算子，比如元素复制、元素删减、字节修改、元素位置变换等。
	变异权重预设	用户可以微调数据模型中每个元素的变异权重,从而精准控制变异位点和变异程度。
测试流程构建	状态模型构建	根据测试对象的运行时状态和收发数据的过程设计测试状态模型，可以模拟测试对象的主动行为，比如输入、输出、条件判断、状态转移等。
	临时数据存储	使用字典保存状态模型执行过程中的临时数据，比如测试执行状态，测试对象返回的数据等。
测试对象状态监视	网络状态监视	用于监视诸如路由器、交换机等网络通信设备的存活或连接状态，包含 ping 监视器、socket 监视器等。
	操作系统状态监视	用于监视不同操作系统下的程序运行状态，包含 gdb 监视器、windbg 监视器、Android adb 监视器等。
	工控设备状态监视	用于监视工控设备状态的监视器，包含 Apc 电源监视器，串口监视器等。
测试对象通信与交互	无线协议通信与交互	用于与无线设备的通信交互，支持蓝牙、WiFi 等协议。
	工控协议通信与交互	用于与工控设备的通信交互，支持 I2C、CAN 等协议。

	网络协议通信与交互	用于与网络通信设备的通信交互，具有不同层的通信封装接口，包含链路层发包器、IP 协议发包器、TCP 发包器等。
	操作系统通信与交互	用于在不同操作系统上与程序进行交互，包含 AndroidMonkey 发包器、命令行发包器等。
	Web 接口通信与交互	用于与 Web 接口进行通信交互，包含 Rest 发包器、Websocket 发包器等。
	串口通信与交互	用于与串口通信的设备进行交互，如 USB 接口数据交互等。
测试辅助功能	测试用例解析	详细记录每一个用例的生成过程和每一轮测试流程，用户根据历史回顾追踪测试对象的状态，分析测试对象的潜在缺陷。
	测试用例复现	用户可以选择测试历史中的测试用例重新运行，复现历史测试中的场景。
	异常定位	在测试过程中如果监视到测试对象出现异常，则回溯测试流程，确认复现异常的最小测试用例集。
	测试远程代理	数据生成和测试流程调度在本地执行，监视、通信和交互功能运行在远端，双方通过 socket 通信，该功能可用于嵌入式设备的测试。
	未知数据结构解析	分析用户提供的未知数据结构和交互流程，自动生成数据模型和测试流程，辅助用户开发测试套。该模块主要用于网络协议的逆向分析。
二次开发接口	测试脚本自定义开发接口	提供 python2 编程接口，用于编写脚本辅助测试，比如数值计算、编码计算等复杂的操作。

	功能模块自定义开发接口	提供 python2 和 C#编程接口，用于开发自定义的功能模块，如远程代理、发包器、监视器等。

3 产品优势

1. **直观**

规范的测试套构建：基于高通用性的 XML 格式定义测试套，规范化复杂的测试套建模流程，易于用户理解和调试。

实用的操作面板：通过图形化的一键操作进行测试任务创建、调度、监控，支持导出包含详细测试用例统计信息、异常交互报文的测试多格式文档（Pdf/Word/Excel/Html），便捷测试人员使用。

友好的 UI 交互：设计人性化的专业操作界面，将冗余海量的测试数据进行图形化展示，对关键信息进行显示标识，重点突出、精简操作。

2. 健壮

稳定高效的分层架构设计：对工作流进行切割分层，各层次间独立性高。系统采用全异步处理，解耦各功能模块，保证系统的稳定性和高效性。

多领域测试接口支持：从实际网络安全测试需求出发，能够同时满足网络协议测试、二进制程序测试、安卓程序测试、以太网设备测试、无线通信设备测试等不同测试需求，保证系统强健的任务兼容性。

3. 弹性

功能插件可拓展：支持用户自定义开发插件，满足个性化测试需求。

跨平台测试：可完美兼容 Windows、Linux、Mac、Android 等主流平台的测试对象，实现测试任务全覆盖。

测试配置可按需调配：用户可通过配置文件，按照实际需求制订测试规则、分配测试资源，精准控制测试用例的运行方式。

自适应测试用例生成：支持多种异常种类，如常规异常、二进制异常、组合异常等，用户可自定义异常级别和种类生成相应数目的测试用例，满足多样化测试要求。

4. **全面**

全自动化测试：系统结合生成式和变异式方法进行用例生成，对已知的测试

协议或接口进行建模，并根据已知的数据样本启发用例突变，自动化生成批量测试用例并记录，以供测试使用及检索。

详细的测试工作流回溯：系统详细记录测试全流程的配置信息、测试用例、交互报文、历史日志，支持查询定位、回顾分析测试任务节点并进行异常复现或任务调整，有助于漏洞快速发现与定位。

深入的缺陷覆盖：平台支持构建符合各协议规范的数据模型及其状态机，并对数据模型字段进行全面测试，重点关注漏洞高发区数据元素，基于变异算子生成测试用例，深入挖掘潜在缺陷。

全流程测试辅助：平台在每一个测试流中都会提供当前解析的测试状态模型数据，辅助测试人员进行数据推演分析。

实时全局监控：实时掌握平台系统资源的消耗情况、测试对象核心状态，支持智能化调配节省软硬件资源。

国际化标准评估：平台对标国际通用的 CVSS 打分模型评价漏洞危险程度，保证测试结果的客观准确。

4 应用场景

操作系统内核漏洞挖掘

操作系统作为统筹管理计算机资源的软件，在整个通信架构中占据核心地位，也因此成为安全威胁的重要来源。据全球各大漏洞库的数据显示，操作系统漏洞占据了相当大的比例：例如，美国国家漏洞数据库（NVD）统计数据显示，操作系统漏洞占比达 21.8%，排名第二；同样，中国国家信息安全漏洞库（CNVD）发布的统计数据也显示，操作系统漏洞占较大，达到了 19.3%，排名第二。

灵通测平台完美兼容 Windows、Linux、Mac 等主流操作系统内核环境，结合静态调用分析和动态变异测试，依据系统嵌套调用关系智能化生成测试用例，并利用系统状态参数监测缺陷异常，实现全面深入、准确高效的系统漏洞挖掘方案。

通信协议缺陷测试

协议是通信中重要组成部分，用于规定设备间数据传输的格式和规则，由于通信协议的多元性和广泛性，通信协议缺陷可以被用来窃取敏感数据、篡改网络流量等，严重威胁隐私安全。

灵通测平台可同时支持公有、私有协议的测试，用户只需通过配置文件构建测试套即可实现自动化报文生成与交互；同时平台可在黑盒、灰盒场景实现自动化协议识别、报文分段等复杂工作，满足多种测试需求。

软件安全合规认证

在智能微服务如火如荼的今天，软件与用户生活已紧密洽接，如支付应用与用户财务挂钩、购物应用与用户信息挂钩，软件安全不仅关乎业务持续性，同时与大批用户隐私数据安全有直接联系。

灵通测平台能够面向软件开发，基于应用程序安全规范对初代软件产品进行模糊测试，提前发现软件缺陷、避免漏洞危害；同时也能够面向软件安全合规性检查，辅助软件合规认证。

物联网设备安全测试

物联网（IoT）将独立电子、电气化设备接入网络实现了万物互联，智能家居、车联网、智能健康监测等概念产品以数据包为媒介在用户与设备间快速传递信息，但由于缺乏必要的安全防范，这些设备很容易被不法分子劫持。

灵通测平台提供了从协议到软件到设备全套的测试接口，能够便捷实现体系化安全测试并形成统计分析测试报告，帮助物联网开发人员及时发现设备潜在安全威胁。

雷达通信设施安全测试

雷达是一种利用电磁波探测目标并测量其距离、速度、方位等参数的无线电设备，被广泛应用于民用和军事领域，如航空、航天、地质勘探、交通管理、防御安全等领域，必须保证其设备的安全稳定、精确可靠。

灵通测平台提供了多样化的 API、库、协议测试接口，无需用户干预、无需暴力测试，能够生成大量用例，智能进行设备逻辑检查、设计缺陷挖掘，为雷达通信设备测试提供高效方案。

工控设施安全审查

工控设备涵盖工业自动化系统中用于监测、控制和操作生产过程的设备，如传感器、执行器、PLC（可编程逻辑控制器）、DCS（分布式控制系统）、SCADA（监控与数据采集系统）等，其在生产过程中扮演着至关重要的角色。

灵通测平台支持针对工控关键设施进行一键测试，全面摸排设施潜在隐患，

助力工业系统安全体系建设、故障灾难预防，保证系统服务持续性、可用性、安全性。

车控设备缺陷审计

车控系统是构建智能网联汽车生态的重要基石，负责支撑和保障着智能驾驶功能集中运行的性能和安全，重要性日益凸显。

灵通测平台针对系统的核心控制元件和网络组件进行查验，自动化统计异常数据评估风险等级，满足不同场景下企业级车载设备的测试需求，保障车控系统稳定可靠。

企业等保测评

等级保护测评是评估企业信息安全风险和确定安全控制措施的核心步骤，对于保护敏感信息和防范信息安全风险至关重要。

灵通测平台能够对企业中基础信息网络、物联网设备、云计算设备、移动互联软件等关键等保对象进行精准测试，帮助企业进行基础设施自查，助力等保测评认证。

5 术语表

术语	解释
XML	可扩展标记语言，标准通用标记语言的子集，可以用来标记数据、定义数据类型，是一种允许用户对自己的标记语言进行定义的源语言。
测试套	许多测试用例的集合。测试套将服务于同一个测试目的或同一运行环境下的一系列测试用例有机组合，以达成测试目标。
变异权重	在随机变异中起到判断是否对可变异对象进行变异的依据之一，程序根据随机种子给每个可变异对象赋予权重，可变异对象的权重越大，在随机选择变异对象的过程中，被选中的可能也越大。
变异算子	又称变异器，在模糊测试的过程中作为变异动作的直接作用方，用于让数据模型产生数据变异或让状态模型产生状态变异。

I2C	由 Philips 公司开发的一种简单、双向二线制同步串行总线。
CAN	控制器域网。