重磅发布 | 触点互动工控仿真测试解决方案

一、 工控领域的仿真测试需求及现状

近年来，工业控制领域的技术正逐步和 IT 和 CT 技术融合，底层通信技术从传统的串口大规模转向以太网和工业以太网技术，无线技术从 WiFi 演进到和 5G 融合。工控系统或 PLC 开发逐步通过采用 IT 行业主流的技术实现，包括类似于 MQTT 这些标准协议栈，OPCUA 这种 IT 框架技术都得到了广泛的应用。

随之而来的是，工控领域的测试需求出现了井喷式的爆发。因为 IT 网络技术的引进，需要对 PLC、DCS 的网络接口通信能力进行功能、性能和安全性测试，以确保入网工控设备能够符合运行标准要求。5G 技术的引进，需要对融合 5G 模组的工业控制系统的功能、性能以及稳定性也进行验证，看 5G 技术是否能够有效替代传统的有线通信技术。另外，工控安全行业的蓬勃发展，又带来了大量对工控安全设备本身的功能、性能以及攻击防护能力的测试需求。

然而，目前市场上并没有一款成熟的工控测试产品，能够帮助甲方或者工控设备研发人员进行高效、易用的设备测试。大量的工控产品测试还是采用人工方式，用 PC 端模拟工具加上 PCAP 数据比对的方式进行验证。这种初级的测试方法，已经不能适应当前工控技术 IT 化、CT 化带来的要求，无论从测试准确度，测试效率，新技术适配上面都已经远远不能适应现在的现状。国外的高端进口工控测试工具，价格又极其昂贵，很多客户无法承受。

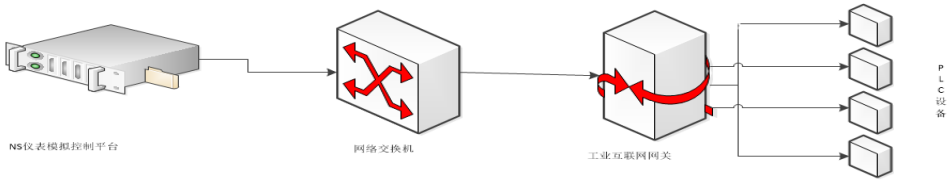
二、 触点互动工控测试方案

2.1 测试工具优势

触点互动的 XproNetworkSimulator 系列网络仿真测试工具(简称 XproNS 或者 NS)，可以在标准 X86 平台上仿真主流的工控协议栈和工控 PLC/DC 等设备，以非常简单易用的方式实现对工控设备的功能、性能、安全性测试，也可以对工控安全设备进行功能、性能和安全防护能力测试。完美地解决了目前工控行业的测试工具匮乏，测试效率不高的痛点。

2.2 测试 PLC 设备

单臂模式NS仪表测试PLC设备



XproNS 仪表模拟工业互联网管理平台，将指令或数据发送到工业互联网网关设备，转发给 PLC，或者直连 PLC 设备，通过 XproNS 发送工控指令直接控制 PLC 设备。通过这一拓扑可以验证 PLC 设备的协议栈的协议一致性，包括常见的 Modbus，Coap，MQTT，IEC 104，IEC61850 等协议。

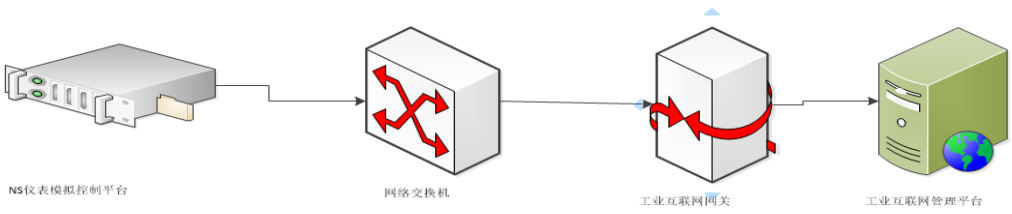
XproNS 支持主流的工控协议，同时允许管理员按照标准工控协议进行具体指令的定义来模拟和真实工控环境一模一样的指令动作。

XproNS 支持的性能测试指标：

- ✧ PLC 设备注册成功率
- ✧ PLC 设备注册平均延时
- ✧ PLC 设备注册最大延时
- ✧ PLC 设备注册最小延时

2.3 测试工业互联网平台

单臂模式NS仪表测试工业互联网平台



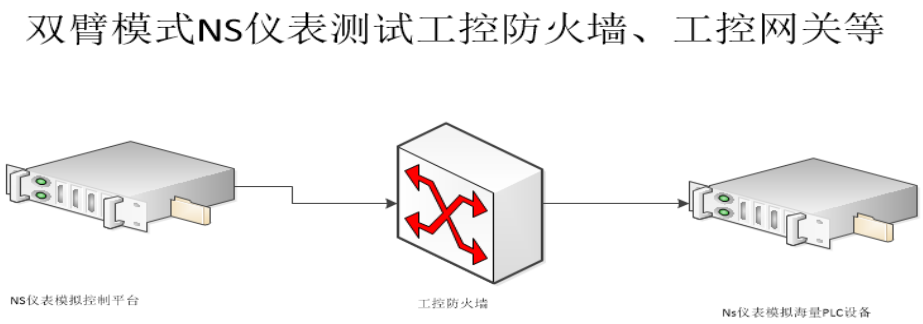
XproNS 仪表模拟海量 PLC 设备对接工控网关设备，网关设备再通过公网接入工业互联网平台。XproNS 仪表模拟 PLC 设备采集数据，并把采集到的数据按照规定模型上报给工业互联网平台。在工业互联网平台上可以看到海量的仿真 PLC 设备和这些海量 PLC 生成的海量仿真数据。

通过这一测试，可以在不需要真实 PLC 设备的情况下，迅速验证工控网关和工业互联网平台的工控 PLC 接入性能和扩展性。支持的对接协议包括 MQTT、 LWM2M、 OPCUA 等流行工业互联网接入协议。

支持的性能测试指标：

- ✧ 控制指令成功率
- ✧ 控制指令重传次数
- ✧ 控制指令平均延时
- ✧ 控制指令最大延时
- ✧ 控制指令最小延时
- ✧ 控制指令往返平均延时
- ✧ 控制指令往返最大延时
- ✧ 控制指令往返最小延时
- ✧ 控制指令返回设备数量成功比例

2.4 测试工控安全网关型设备



XproNS 仪表模拟海量的 PLC/DCS 和上位机，用于复现一个真实的工厂或者电网的工控环境。同时串接或者并接工控安全设备，来测试工控安全设备的相关安全防护能力、功能、性能和稳定性。XproNS 最多可以支持数万个 PLC 的模拟，同时可以混合多种工控协议来模拟真实的多协议流量场景。可以测试的设备包括：工控防火墙、工控 IDS、工控网闸、工控态势感知系统等。

支持的测试指标：

- ✧ 协议识别成功率
- ✧ 协议指令解析成功率
- ✧ MODBUS 新建/并发性能测试
- ✧ OPCUA 新建与并发性能测试
- ✧ MQTT 性能测试
- ✧ COAP 新建/并发性能测试
- ✧ HANDLE 新建/并发性能测试
- ✧ ……

三、 XproNS 支持的工控协议列表

支持的测试拓扑模式	协议名称
单臂模式、双臂模式、单双臂模式	HANDLE
	OPCUA
	MQTT
	LWM2M
	MODBUS
	COAP
	IEC104
	IEC61850
	telnet
支持双臂模式	AMQP
	ANSI
	BACnet
	BECKHOFFADS
	BITCOIN
	CAN

	CIP
	COTP
	CQL
	DICOM
	DJIUA
	DNP3
	DRDA
	ESIO
	Ethercat
	EtherNet/IP
	fins
	GOOSE
	GRYPHON
	HART-IP
	HollySys
	IEC 60870-5-104
	IEEE_C37.188
	LONTALK
	MMS
	MONGODB
	MYSQL
	NTP
	OMRON
	OMRONFINS
	OPC_TCP(opcda、opcae)
	OPENSAFETY
	PCWORX
	PGSQL
	proconos
	profinet
	RTPS
	SBUS
	Siemens S7
	Siemens S7-plus
	SIP
	SNMP
	SV
	SYNPHASOR
	TDS
	TNS
	XMPP