标题：智能制造安全监测与运营管理平台

引言/导读

360 企业安全技术（北京）集团有限公司是 360 公司继个人安全市场后专注于为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务的网络安全公司，法定代表人为齐向东，注册资本 1.33 亿人民币，总部设立在北京市朝阳区酒仙桥路 6 号院 2 号楼（电子城.国际电子总部），同时公司在上海、成都、广州、大连等地设有分支机构。公司拥有 4000 余名网络安全技术、产品和服务人员。截止目前已经为 90%部委、72%央企、100%大型银行以及上百万中小企业提供了网络安全产品和服务。

本项目采用物联网、大数据、云计算、人工智能等工业互联网先进技术，在实现供水设备智能互联的基础上，通过对采集数据的实时分析、深度学习和数据挖掘，整合供水设备从设计、生产、安装、运营、维保、报废到优化的全生命周期八大环节的数据，开发基于目标用户的设备个性化需求系统、设备标准化设计系统、设备最优化智能生产系统、移动施工管理系统、设备远程监管系统、设备故障预警系统、故障专家自诊断系统、维保快速响应系统等服务应用，并通过 APP、Web 等人机交互工具为不同用户提供多层次、多元化的用户界面，构建供水设备全生命周期的一体化管理平台。

一、关键词

安全监测、运营管理

二、发起公司和主要联系人联系方式

发起单位：360 企业安全技术（北京）集团有限公司

主要联系人：崔君荣 cuijunrong@360.net 陶耀东 taoyaodong@360.net

三、合作公司

上海威派格智慧水务股份有限公司

四、测试床项目目标和概述

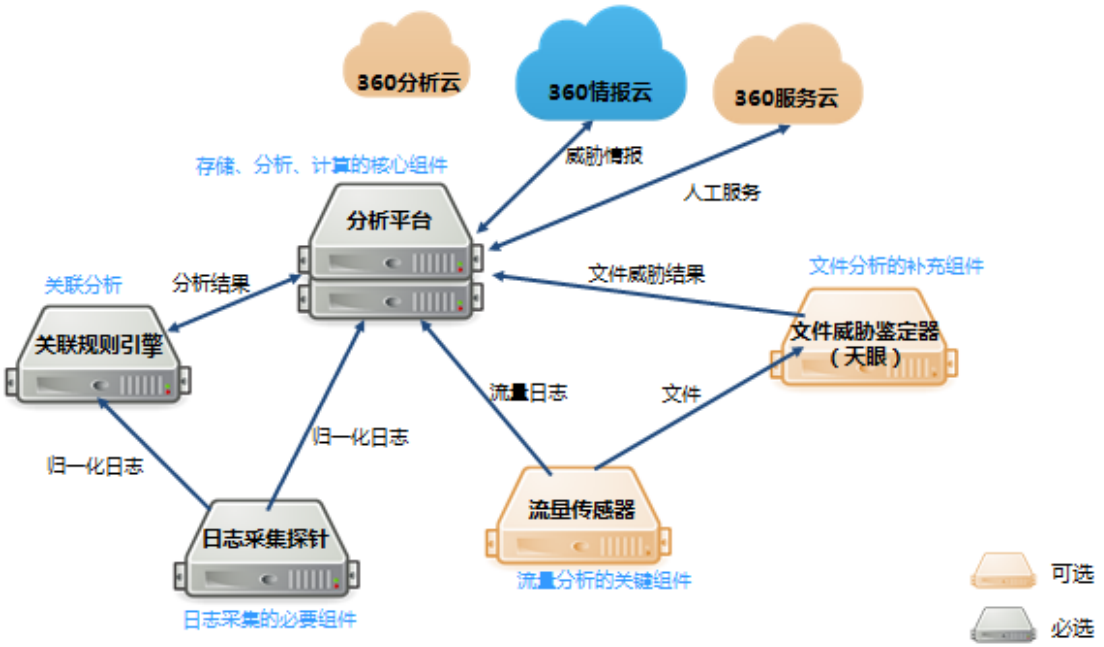
- 主要目标

“智能制造安全监测与运营管理平台”主要实现对智能制造企业工控系统通信数据和安全日志进行快速、自动化的关联分析，及时发现智能制造行业工控系统异常和针对工控系统的威胁，通过可视化的技术将这些威胁和异常的总体安全态势展现给用户，通过对告警和响应的自动化发布、跟踪、管理实现安全风险的闭环管理。

通过建设智能制造安全监测与运营管理平台，实现企业内网 IT 和 OT 安全的统一管理，企业内部通过全网流量监测，提前洞悉企业内部各种工业安全威胁，降低智能制造企业在进行工业互联网转型过程中的安全门槛，促进智能制造相关产业高速发展。

- 总体概述

智能制造安全监测与运营管理平台主要包括流量传感器、日志采集探针、关联规则引擎和分析平台 4 个硬件模块。如下图所示：



平台组成架构

1） 流量传感器

流量传感器的功能主要是采集工控网络中的工业协议流量数据，将原始的工控网络全流量转化为按 session 方式记录的格式化流量日志，全流量日志会加密传输给分析平台存储用于后期的审计和分析。

2） 日志采集探针

日志采集器的主要功能是对工控网络内工控设备（PLC/DCS/RTU/HMI 等）、安全设备、工业以太网、上位机、服务器等设备通过主动采集或被动接收等方式对日志进行采集并进行归一化预处理，方便数据流后面的关联规则和数据分析能够快速使用。同时日志采集器还负责对内网资产进行扫描识别，收集资产数据。

3） 关联规则引擎

关联规则引擎主要负责对来自日志采集器的大量日志信息进行实时流解析，并匹配关联规则，对异常行为产生关联告警。

4） 分析平台

分析平台用于存储流量传感器和日志采集器提交的流量日志、设备日志和系统日志，并同时提供应用交互界面。分析平台底层的数据检索模块采用了分布式计算和搜索引擎技

术对所有数据进行处理，可通过多台设备建立集群以保证存储空间和计算能力的供应。

五、测试床解决方案架构

(一) 测试床应用场景

本平台主要面向智能制造领域，对中小企业建设具有监测、预警的管理平台，利用平台的实时监测能力，有效加强企业的工业互联网安全水平。

水务是一个涉及到国计民生的行业，近年来中国水务向数字化、自动化、智慧化的方向发展。为保证供水生产设备的安全运行、预防系统突发性重大事故的发生，并在事故发生后迅速有效地控制和处理，最大限度地减少事故损失和相关系统的影响，在企业内部建立安全运营管理平台，以数据为驱动，以安全分析为工作重点，立足于安全策略防护，充分利用大数据平台的数据收集、查询能力进行持续的监控与分析；在持续监控的基础上，实现安全管理体系、预警监测体系、安全服务体系、纵深安全防护之间的有效协同和共同作用，最终形成可以有效落实的体系化安全解决方案。

(二) 测试床重点技术

该平台数据采集部分，除了对智能制造行业传统的 Syslog、Flow、各种系统日志和安全设备日志以外还突破性的针对原始流量日志（依赖于流量传感器或 360 下一代防火墙）和终端日志（依赖于天擎 EDR 模块）进行采集。依赖于更加原始的日志信息，平台可以发现隐藏更深的各种威胁，同时能够提供完整的事件回溯分析能力。

平台在数据的存储和分析中大量使用大数据相关技术，在标准化组件中可以依赖于分布式全文检索技术提供接近 PB 级日志量的存储和快速计算，同时能够提供良好的可靠性保证，以解决意外断电、磁盘故障可能对系统带来的可靠性问题。

平台使用多种分析引擎针对不同的管理目标提供相应支撑，关联分析、统计分析、快速搜索等功能相较于传统产品具有明显的性能优势。

平台最外层提供友好、高效的交互管理页面，既满足了使用需求，又能够提升工作效率。再结合威胁情报、安全服务等来自于 360 特有的安全知识输入，该平台可以极大的提升本地安全运营的效率。

(三) 技术创新性及先进性

通过全网流量监测，发现工业网络中的各类威胁和高级威胁，并进行情报挖掘与云端关联分析，提前洞悉企业内部各种工业安全威胁，并将威胁情报以可机读格式推送到本地系统，供本地威胁检测和分析时使用。

(四) 测试床解决方案架构

该平台将建设成一个以多种安全问题管理为目标、以智能制造工业数据为核心、威胁情报为特色、打通安全运营中的检测、响应、预警、防御多个领域环节的完整安全体系，能够覆盖安全管理与运营的各个环节，功能架构图如下：

平台功能架构

六、预期成果

(一) 测试床的预期测试结果，针对测试项（重点）

1、工控系统关键资产管理

该平台能够提供对企业内网资产的扫描发现、手工管理、资产变更比对、资产信息整合展示等基本功能。同时，提供长期的服务、流量、威胁相关的监控，所有资产相关的监控数据均可在资产详情页查看。

2、工控系统操作行为监测

该平台能够实时监测工控系统控制器下装、上传、启动、停止等关键操作行为，包括智能制造行业常用西门子 S7-300、施耐德昆腾、罗克韦尔 Control Logix 等系列工控系统。

3、威胁发现及时性提升

利用多种新型威胁监测手段，再结合威胁情报的使用，该平台能够更快的发现隐藏在各类日志中的安全问题。更早的发现威胁，一方面可以帮助企业或单位在安全管理上更为从容，无需面临可能被通报追查的窘境，另一方面可以留下更多挽回损失的机会，为快速的弥补安全问题提供宝贵的时间窗口。

4、安全运营

该平台可以在多种安全功能基础之上提供安全运营，帮助用户快速的、宏观的了解整个企业的安全情况。对各种威胁采取措施控制指令下发至控制系统，形成监控、分析、控制的闭环。

(二) 商业价值

传统工业领域安全防护常用的分层分域的隔离与边界防护思路以及传统的 IT 安全手段已不能有效识别和抵御所有可能的攻击。安全监测与运营管理平台为智能制造中小企业的工业控制系统信息安全保障提供了一种有效解决方案。

(三) 经济效益

通过该平台的部署，可以实时监控企业内网的流量，及时发现智能制造网络空间的可疑行为和风险，大大提高了整个工业控制过程自动化领域的信息安全保障水平，同时提高用户对自己使用的工业控制系统信息安全的自主把控能力。本平台作为智能制造行业工业互联网建设和正常运行的重要支撑和保护，其建设具有良好的经济效益。

(四) 社会价值

智能制造行业工业控制系统在我国经济生产生活中起着举足轻重的作用，如果工业控制的信息被窃取或者被修改，可能造成人身伤亡、财产损失等严重后果，更严重的甚至会影响到国家安全。本平台建成后，将快速面向智能制造中小企业，形成良好的工业互联网

和网络安全产业生态，加快工业物联网在工业信息化产业中的布局，降低企业工业控制信息化的复杂度，从而让工业充分享受信息化产业带来的便利，社会效益十分显著。

七、测试床技术可行性

(一) 物理平台

平台主要包括流量传感器、日志采集探针、关联规则引擎和分析平台 4 个硬件模块。主要部署在网络出口交换机旁，或者其他需要监听流量的网络节点旁，接收镜像流量，极大的避免了硬件接入至企业厂区内部对生产本身的影响。

(二) 软件平台

所用设备操作系统为 linux。

八、和 AII 技术的关系

(一) 与 AII 总体架构的关系

安全监测和运营管理平台在工业互联网体系架构中提供安全服务，网络边缘侧接入的终端类型广泛，数量巨大，承载的业务繁杂，被动的安全防御往往不能起到良好的效果。因此，需要采用更加积极主动的安全防御手段，包括基于大数据的态势感知和高级威胁检测，以及统一的全网安全策略执行和主动防护，从而更加快速响应和防护。再结合完善的运维监控和应急响应机制，则能够最大限度保障系统的安全、可用、可信。

(二) AII 安全（可选）

智能制造安全监测与运营管理平台是安全产品，能够连接工控防火墙、工业安全审计、工业主机防病毒软件、工控交换机等设备，统一管理安全事件。

同时，该平台在出厂时已经通过公司内部安全审查和评估。

(三) 详细清单（可选）

配置和控制接口

模块	接口

流量传感器	2×1GE 管理口（电），2×1GE 监听口（电），2×1GE 监听口（光口，可插千兆光模块）
日志采集探针	4×1GE 电口
关联规则引擎	4×1GE 电口
分析平台	4×1GE 电口

数据通讯接口

工控通信协议 MODBUS/TCP、OPC DA、S7 等。

(四) 安全联系人

孙树海 sunshuhai@360.net

(五) 与已存在 AII 测试床的关系

参考工业互联网产业联盟成果发布——测试床，现有 34 个测试床，主要集中在智能服务平台、通信设备制造、家电协同制造等方面。现有成果没有从安全角度考虑建设测试床，因此，智能制造安全监测与运营管理平台的部署是非常有必要的，同时需要亟待落实。

九、交付件

智能制造安全监测与运营管理平台是一个总系统，主要包括流量传感器、日志采集探针、关联规则引擎和分析平台，部署在智能制造同一个网段中。

十、测试床使用者

智能制造安全监测与运营管理平台建设成功后，可应用于工业控制系统安全国家地方联合工程实验室进行展示，同时可用于威派格智慧水务生产设备系统的安全监测、分析预警、安全态势展现、威胁情报发布与使用。

十一、 知识产权说明

1.项目实施过程中所产生的知识产权，

①各方独立完成的成果所有权归各自所有；共同完成的成果所有权，按照参与方的贡献大小进行分配。

②共同完成的项目成果转让，须经参与各方同意的前提下进行，任何一方不得私自开展。

2. 独立完成的知识产权成果各方可独立组织成果鉴定。

3. 共同完成的项目成果申报各级奖项，应根据各方贡献大小排名。具体事宜另行商定。

十二、 部署，操作和访问使用

流量传感器通常部署在网络出口交换机旁，或者其他需要监听流量的网络节点旁，接收镜像流量。关联规则引擎、日志采集器和分析平台部署在流量传感器同一个网段即可。

十三、 资金

自筹

十四、 时间轴

项目建设周期为两年。2018 年完成流量传感器、日志采集探针等技术的开发，2019 年实现新探针、新应用开发技术模式，2020 年基本完成。

十五、 附加信息

该平台通过以大数据和威胁情报为核心的智能制造安全监测和运营管理平台建设，实现威胁检测、可视化展现、闭环响应的工业安全运营，推动水务设备制造及智能制造行业的发展。