案例 1

天融信网络安全技术有限公司

主标题：面向关键基础设施的工业互联网安全监测与态势感知系统

副标题：安全赋能助力产业发展

引言：

天融信科技集团创始于 1995 年（简称天融信），自 1996 年推出填补国内空白的首台自主知识产权防火墙起，如今已成长为中国领先的网络安全、大数据与云服务提供商。天融信自成立至今为工业企业提供了大量优质的解决方案，覆盖电力、轨道交通、航空航天、军工、能源、石油化工、机械制造、国防工业、汽车、电子等行业领域。目前获得包括 CCID、工业互联网产业联盟等颁发的优秀解决方案、优秀应用案例等多个奖项。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

工业互联网概念的提出和近年来的快速发展满足了“管控一体化”、工业智能化等工业企业发展需要，是工业企业提升信息化技术、创新应用的必然趋势，在现阶段和未来工业互联网行业蓬勃发展的背景环境下，如何构建全方位的、融合传统 IT 网络安全技术与工业 OT 网络安全技术的综合技术保障体系是工业互联网企业共同面对的技术难题。

现阶段对于某省区域的工业互联网企业的安全状态，目前缺乏必要的监管技术措施，难以从全局角度洞悉该区域的工业互联网企业的网络安全态势，对于各

工业互联网企业的相关安全信息，也无法进行有效的整合和利用，及时发现潜在的安全威胁。

面向省级的工业互联网安全监测与态势感知系统是构建全方位的工业互联网安全综合保障网络体系的重要基础。通过打造企业内部工业互联网态势感知系统，完成态势的细粒度分析，并将态势感知系统与省级工业互联网安全监测与态势感知系统联动，实现省级工业互联网安全全面及实时的监测。

一、项目概况

本案例是在某省区域建设企业级态势分析系统和省级工业互联网安全态势感知平台，实现省级工业互联网安全全面及实时的监测，并与国家平台实现数据共享与交换。通过项目的实施，有助于推动互联网与该省工业深度融合，优化产业结构，提升产业竞争力，打造经济发展新动能，打造工业互联网产业新生态。

1. 项目背景

工业互联网推进工业生产过程不断灵活化、柔性化，企业、用户、产品之间将高度协同、开放、共享，工业互联网安全边界越发模糊，攻击面不断扩大，未来安全将向设备、网络、控制、数据、应用全方面渗透。安全是保障工业互联网发展的重要前提，亟需从技术、管理、服务等多角度协同构建工业互联网安全发展环境。

我国也高度关注工业互联网安全的新形势。中央领导从总体国家安全观的高度指出，安全是发展的前提，发展是安全的保障，安全和发展要同步推进。这个论述，把安全提到了一个前所未有的新高度。在工业互联网时代，网络安全至关重要，企业必须高度重视网络和大数据安全问题，否则后果将是灾难性的。

2017 年 11 月国务院推出《关于深化“互联网+先进制造业”发展工业互联网的指导意见》该意见提出以“强化安全保障”为指导思想、“安全可靠”为基本原则，明确“建立工业互联网安全保障体系、提升安全保障能力”的发展目标，部署“强化安全保障”的主要任务，为工业互联网安全保障工作制定了时间表和路线图。意见提出以来，国内工业互联网建设的顶层设计逐步加强，相关工作有序推动，国家和地方政府密集出台了一系列的相关政策来推动工业互联网的落地

实施。为贯彻落实国务院《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，前瞻布局工业互联网，全面支撑制造强国和网络强国建设，工业和信息化部、财政部决定联合开展 2018 年工业互联网创新发展工程项目工作。我司为了响应国家的工业互联网建设需求，申报了 2018 年工业互联网创新发展工程。

2. 项目简介

本案例是在某省区域建设企业级态势分析系统和省级工业互联网安全态势感知平台。通过建设企业级态势分析系统，向省级工业互联网安全监测与态势感知平台提供监测数据；通过构建省级工业互联网安全监测与态势感知平台，实现数据共享与交换，通过接口向国家工业互联网网络安全监测与态势感知技术平台提供监测数据。通过该项目的实施，有助于推动互联网与该省工业深度融合，优化产业结构，提升产业竞争力，打造经济发展新动能，打造工业互联网产业新生态。

3. 项目目标

通过建设工业互联网省级安全监管平台，可以从监管层面全局洞悉工业互联网企业的网络安全态势，解决工业互联网关键基础设施制造行业面临的网络安全保障问题。围绕关键信息基础设施的工业互联网监测，企业级态势感知系统，构建省级安全监测与态势感知平台。一方面通过采用主动探测的方式，发现互联网中工业相关安全信息，形成互联网工业网络安全底图，另一方面通过打造企业内部工业互联网态势感知系统，实现对网络安全的态势觉察、跟踪、预测和预警，并将态势感知系统与平台联动，实现省级工业互联网安全全面及实时的监测。平台能够汇聚安全感知各维度信息，实时感知生产系统和设备的运行状况、风险隐患及企业管理运行情况等信息，实现对监测信息的分类汇聚、精准研判，及时对潜在的网络安全威胁和风险进行预警，不断的提升智能制造系统的网络安全的防护水平。

二、项目实施概况

通过建设分布式工业互联网数据采集系统、数据处理及存储系统等子系统，

构建省级工业互联网安全监测与态势感知平台和企业级态势分析系统，从监管层面实现省级工业互联网安全全面及实时的监测。

1. 项目总体架构和主要内容

图 1 项目总体结构

该项目通过打造企业内部工业互联网态势感知系统，实现对网络安全的态势觉察、跟踪、预测和预警，同时向省级工业互联网安全监测与态势感知平台提供监测数据。工业互联网企业级态势分析系统针对工业互联网设计，可以提供安全监测、威胁情报、安全审计、资产管理、安全处置等功能，通过对工业互联网流量的采集、分析、监测，结合特定的安全策略，快速有效识别出工业互联网中存在的网络异常事件和网络攻击行为并进行实时告警。

省级工业互联网安全监测与态势感知平台的核心系统包括工业互联网数据采集子系统、数据处理及存储子系统、实时数据分析子系统、离线数据分析子系统和工业互联网态势应用子系统等。其中，工业互联网数据采集子系统主要实现对工业互联网资产、安全漏洞、安全事件以及流量等数据的采集；工业互联网数据处理及存储子系统主要实现接收并处理工业互联网数据采集系统采集的网络数据，存储在数据仓库和分布式文件系统中；数据分析子系统实现对数据的建模和分析；工业互联网态势应用子系统主要实现对数据的不同维度的展示。

通过省级工业互联网安全监测与态势感知平台的设计，实现省级工业互联网安全全面及实时的监测，并向国家工业互联网安全监测与态势感知技术平台提供监测数据，实现监测数据的共享与交换。

该平台的建设通过主动探测、流量监测、企业侧采集等技术手段，打造了态势感知、安全检测、安全预警、快速处置、追踪溯源等功能于一体的态势感知系统，构建“国家-省-企业”立体全方位的安全保障管理体系，实现对该省工业互联网业务发展及网络安全的态势研判。

图 2 系统总体技术架构

系统的设计思想是通过一套完整的面向海量数据应用（网络监测数据、专项数据、安全数据等）的数据管理平台框架，从“数据收集、数据汇总、数据分析、数据展示”全过程对网络安全态势进行分析和展现，平台以各类组件库及组件为基础，遵循体系化、层次化、迭代过程的设计，融入具体业务应用特性，实现对多类异构数据的集中统一处理，展现有价值的数据信息视图。

网络安全态势感知系统包括三个层次：业务系统层、数据存储中心层、数据采集层:

（1）业务系统层:通过安全监测、安全预警、快速处置、追踪溯源等业务功能，提供多维度态势统计分析与展示，不但支持全网态势、工控态势、威胁态势、安全底图态势、安全处置态势等，而且还包括针对客户关注的专享态势，如资产态势、脆弱性态势、攻击态势、僵木蠕态势、网站监测态势等展示。

（2）数据存储与分析层:提供数据的转换、存储、分析功能。数据转换支持

的数据类型包括结构化、半结构化、非结构化的数据，提供清洗、归一化、过滤、归并、打标签等数据转换方式；数据存储提供分布式文件存储、数据仓库、NoSQL数据库、关系型数据库等存储方式，实现对事实数据、结果数据、知识数据的存储；数据分析提供分析引擎、分析组件、分析模型等。

（3）数据采集层：通过部署分布式的采集探针实现对安全数据、威胁监测数据、网络监测数据等数据等的采集，安全数据经过数据汇入后存储到存储计算引擎中。

2. 网络、平台或安全互联架构

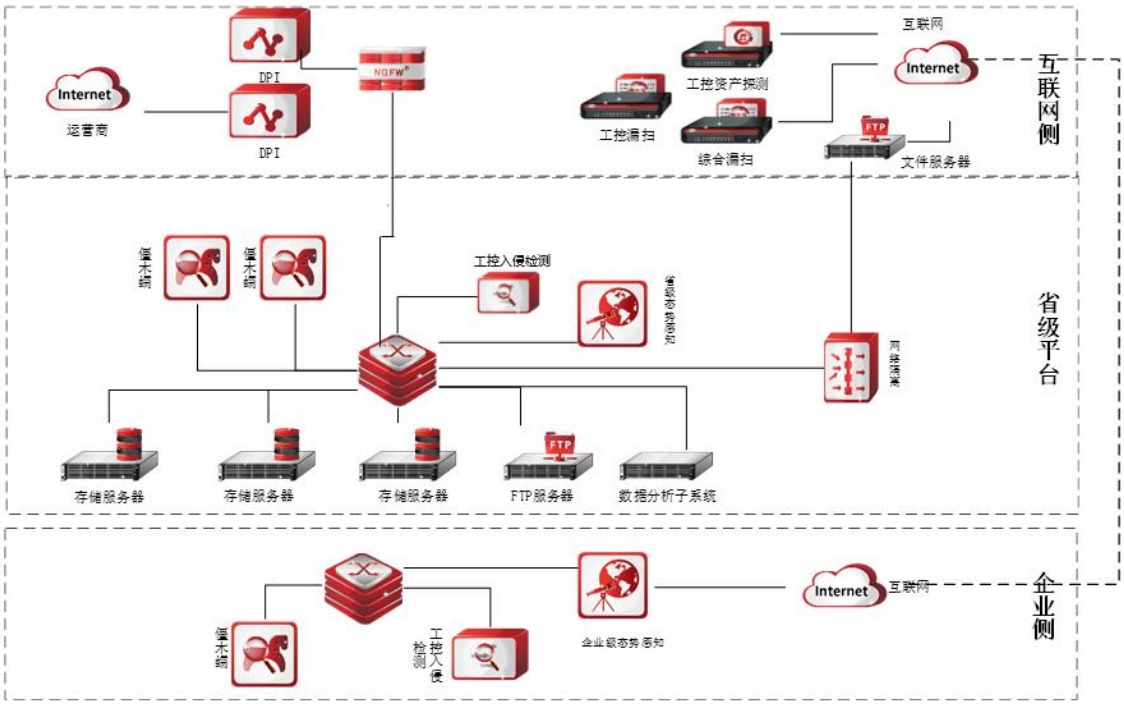

图 3 项目建设示意图

本项目主要是在互联网侧、省级平台和企业侧实施的部署：在互联网区（运营商）部署漏扫产品，通过网络隔离设备导入内网 FTP 服务器，再接入省级平台，向省级平台传输监测数据，部署 DPI 流量分析设备，可为工控入侵检测提供原始工控流量，为僵木蠕提供全网抽样流量；省级的态势感知平台部署在核心区，通过对接收的企业侧和互联网侧的检测数据进行综合分析，实现省级工业互

联网安全全面及实时的监测；在某省企业区域部署企业级的态势分析系统及僵木蠕、工控审计等探针，向省级态势感知平台提供监测数据。

本项目在某省区域建成面向关键基础设施的省级工业互联网安全监测与态势感知平台 1 套，实现了分布式工业互联网数据采集、大容量分布式工业互联网数据处理及存储、在线实时数据分析、离线批量数据分析及网络安全态势感知应用，并且向国家工业互联网安全态势感知与风险预警平台上报有关数据，建设内容包含省级面向关键基础设施的工业互联网安全监测与态势感知系统 1 套和企业级态势分析系统，目前系统接入了工业企业互联网专线流量 110G，监测了 30000+个工业 IP、3200 个域名和 83 家工业互联网云服务平台。

3. 具体应用场景和应用模式

基于数据分析、数据存储、数据处理等技术，构建工业互联网安全态势感知体系，实现工业互联网企业的全面及实时的监测，可用于多种安全应用场景：

- 企业工控网监测场景

基于工控安全探针设备，采集工控网的数据，对工控协议进行深度解析，对企业工控网的通讯内容进行完整性、功能码、地址范围、值范围多维度的检测和审计，及时发现违规操作、异常指令等安全威胁，并进行及时告警。

- 企业 IT 网监测场景

基于 IT 安全探针设备，采集并分析企业 IT 系统数据，实现恶意程序检测、APT 检测、WEB 安全检测等多种攻击监测，并进行报警，实现对企业 IT 网的安全防护。

- 企业级态势分析

构建企业级态势分析系统，围绕企业内部工业网络数据，构建态势应用包括态势感知数据交互式检索、工控数据实时监测、态势分析模型、安全风险快速处置、工业安全问题追踪溯源等功能。

- 集团级/省级态势分析

构建集团级/省级安全监测与态势感知分析系统，从多个维度分析并可以可视化/集团/全省安全态势，根据集团/全省工业互联网安全状态，针对不同的安全问题，进行针对性的安全预警。

4. 安全及可靠性

本项目的工业互联网安全监测与态势感知分析系统，具有自主知识产权，符合国家法律政策及相关部委监管法规的要求。根据项目的建设需求，完成产品在互联网侧、企业侧、省级的安全应用，涉及网络安全、数据安全、主机安全、控制安全、应用安全等多方面的安全防护应用，已形成立体的工业互联网安全防护与分析体系，一方面通过采用主动探测的方式，发现互联网中工业相关安全信息，形成互联网工业网络安全底图，另一方面通过打造企业内部工业互联网态势感知系统，实现对网络安全的态势觉察、跟踪、预测和预警，并将态势感知系统与平台联动，实现省级工业互联网安全全面及实时的监测，满足工业互联网企业的安全建设需求，提升工业互联网安全运营水平。。

5. 其他亮点

- 采用了工业互联网安全人工智能分析技术

  利用人工智能算法实现对各种工业控制网络的自动学习、自动适应和自动规则生成。通过人工智能的数据分析构建工业场景的行为模型，实现对通用的工业控制协议和安全大数据的有效建模，有效得利用了机器学习、模式识别、数据挖掘、高性能算法设计。
- 采用了可扩展数据建模技术

  平台的多维数据分析功能都是基于多维分析技术来实现，提供可扩展的数据建模框架，利用丰富的过程组件，实现可视化的数据建模定义。

三、下一步实施计划

就本项目而言，目前录入到该省级平台里的工业企业信息描述较少，难以对规模以上的重点企业进行标注，所以下一步计划在省内继续推广该项目，使更多的企业信息可以录入到省级平台，使省级平台更有效地实现对省工业互联网业务发展及网络安全态势研判，有效提升该省工业互联网的综合管理和安全保障能力，加速推动互联网与该省工业深度融合，优化产业结构，打造经济发展新动能，打造工业互联网产业新生态，推进该省工业企业进入新的发展阶段。

四、项目创新点和实施效果

1. 项目先进性及创新点

（1） 项目先进性

基于大数据／机器学习／深度学习技术的网络安全态势感知系统是当前国际网络安全研究和开发的热点，我们开发的面向关键信息基础设施的工业互联网网络态势感知系统，将把互联网网络安全研究的最新成果与工业互联网关键基础设施的具体情况结合起来，将会为工业互联网关键基础设施制造领域提供安全上的保障，可以支持超过 1000 个点的数据采集能力，每秒最大可入库 20000 条各类安全数据，系统数据存储能力可达到 100T，建成了大容量分布式工业互联网数据处理及存储系统，实现了工业互联网资产、安全漏洞、安全事件以及流量等数据的预处理、分析和存储。

（2） 项目创新点

- 基于图计算的关联分析技术

将来自多个数据源的安全信息表示为一系列动态变化的图，通过图计算的方式，识别出网络行为模式的变化，识别出网络潜在的安全风险以及主要的风险源。

- 基于时间窗置信区间的检测模型技术

平台采用了基于时间窗置信区间的检测模型和方法，可以在运行中自适应实际环境，自动剔除历史时间窗内的异常历史数据，实现历史时间窗数据与网络实际正常流量行为特征的高度吻合，提高对异常行为报警的准确性。

- 先进的事件归并技术

平台的事件归并技术可以根据用户指定要归并的信息的特征、字段等信息进行归并，只有具有该特征、字段的信息才可以被归并，即当多个信息的指定特征、字段的内容一致时，产生一个归并信息。同时，用户可以自己指定是否丢弃原始信息。

2. 实施效果

通过构建企业的工业互联网安全态势感知系统，可以使企业全局洞悉工业互联网的网络安全态势，并结合工业互联网威胁情报中心与响应中心的情报，及时

发现可能面临的安全威胁和风险，采取及时的响应，通过监管与运营的结合，有效指导了工业企业在网络安全建设过程中存在的不足，优化企业网络安全建设思路，进而强化企业网络安全建设效果，降低因网络安全造成的非计划停机比例，增大攻击成本从而降低企业遭受攻击频率，间接降低了企业因事故造成的财产损失，并且可以向省级工业互联网安全监测与态势感知平台提供监测数据。

通过构建省级安全监测与态势感知平台，可以实现省级平台与国家平台的数据共享与交换，并且可以从工控资产态势、工业产业态势、全网态势、威胁态势等多个维度查看分析工业企业和工业互联网平台企业网络的安全态势，可以有效提升某省工业互联网的综合管理和安全保障能力，通过与国家级安全态势感知平台对接，形成上下联动、政企协同的某省工业互联网监测体系。该项目适用于工业企业对自身生产业务有安全状态监测需求、省级单位对下属工业企业的安全状态监测需求等应用场景。

本项目成果拥有自主知识产权，符合国家法律政策及相关部委监管法规的要求，满足该省工业互联网信息安全建设需求，可提高省级的工业互联网信息安全管理水平。本项目的成功实施，将作为后续该省制造业数字化转型的重要参考，快速推动该省制造业深化改革节奏，具备很深远的市场推广和示范型意义，为后续全国其他省份工业互联网平台建设起到示范性效应，具有广阔的应用前景和推广价值：

- 项目提供了结合企业、区域监管、国家监管的多级监管运营结构实践场景，对建设单位后续区域安全运营进行了理论基础支撑，根据本项目实践场景，建设单位后续可以推出一系列如安全公共服务平台、区域安全运营平台等；
- 该项目有效促进建设单位对于国家工业互联网安全发展思路的理解，对后续有效支撑国家在工业互联网安全领域的产业发展与建设提供了理论基础支撑，并对企业后续参与其他省份省级监管平台设计与建设提供了实践依据，促进建设单位在相关领域的能力发展；
- 从分析展示层面，省级可以集中监管各企业单位业务板块工控系统网络安全实时状态，能有效的降低信息安全人力需求；
- 加强顶层设计，有效提升用户单位生产控制系统网络应对网络攻击风险

的能力；

- 有利于优化产业结构，提升产业竞争力；
- 有利于提高用户工控系统信息化建设水平；
- 有利于国家相关部门对工控系统信息安全态势的管控。