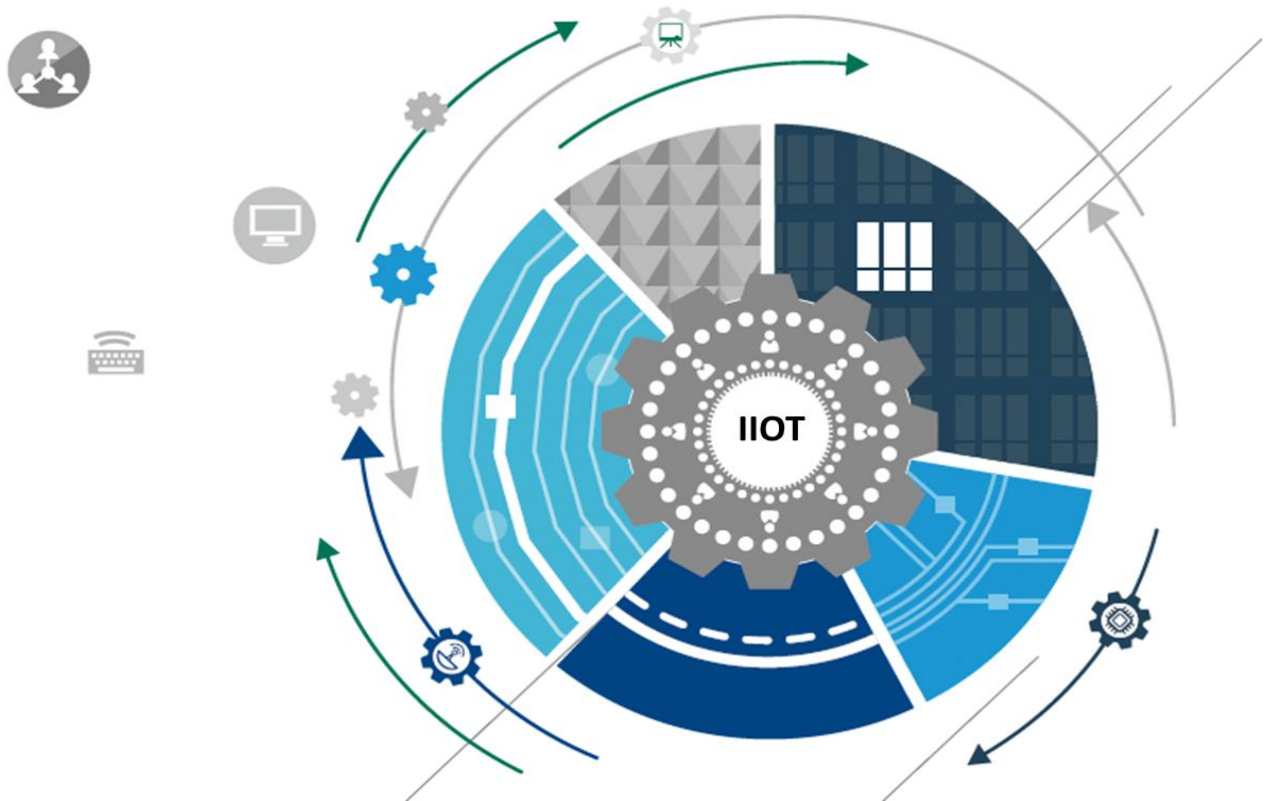


启明星辰集团

工业物联网网络安全解决方案白皮书



目录

1	工业物联网信息安全背景.....	1
1.1	工业物联网基本概念.....	1
1.2	工业物联网发展形势.....	1
1.3	工业物联网安全政策.....	3
1.4	工业物联网重大信息安全事件.....	4
2	工业物联网信息安全威胁.....	6
2.1	工业物联网网络结构.....	6
2.2	工业物联网信息安全威胁分析.....	7
2.2.1	应用层安全威胁分析.....	7
2.2.2	网络层安全威胁分析.....	8
2.2.3	感知层安全威胁分析.....	9
3	工业物联网信息安全需求.....	11
3.1	应用层安全需求.....	11
3.2	网络层安全需求.....	12
3.3	感知层安全需求.....	12
4	工业物联网网络安全解决方案.....	13
4.1	整体方案设计.....	13
4.2	参考依据.....	15
4.3	典型应用场景.....	15
4.3.1	仓储物流场景.....	16

4.3.2	油气开采场景.....	17
4.3.3	智慧办公场景.....	19
5	相关安全产品简介.....	21
5.1	安全产品.....	21
5.1.1	应用层.....	21
5.1.2	网络层.....	23
5.1.3	感知层.....	23
5.2	安全服务.....	24
5.2.1	IIOT 代码审计.....	24
5.2.2	IIOT 漏洞扫描.....	24
5.2.3	IIOT 渗透测试.....	25
6	启明星辰集团介绍及工业物联网积累.....	25

1 工业物联网信息安全背景

1.1 工业物联网基本概念

根据国际电信联盟(ITU)的定义,物联网主要解决物品与物品(Thing to Thing,T2T),人与物品(Human to Thing,H2T),人与人(Human to Human,H2H)之间的互连。但是与传统互联网不同的是,H2T是指人利用通用装置与物品之间的连接,从而使得物品连接更加的简化,而H2H是指人与人之间不依赖于PC而进行的互连。因为互联网并没有考虑到对于任何物品连接的问题,故我们使用物联网来解决这个传统意义上的问题。物联网顾名思义就是连接物品的网络,许多学者讨论物联网中,经常会引入一个M2M的概念,可以解释成为人到人(Man to Man)、人到机器(Man to Machine)、机器到机器从本质上而言,在人与机器、机器与机器的交互,大部分是为了实现人与人之间的信息交互。

与工业互联网的重点不同,工业互联网目标是融合互联网与工业,打破工业生产的全生命周期,从产品的设计、研发、生产制造、营销、服务构成了闭环,彻底改变工业的生产模式。而工业物联网作为物联网技术在工业领域的应用,其特点是将具有感知、监控能力的各类采集、控制传感器或控制器,以及移动通信、智能分析等技术不断融入到工业生产过程各个环节,从而大幅提高制造效率,改善产品质量,降低产品成本和资源消耗,最终实现将传统工业提升到智能化的新阶段。从应用形式上,工业物联网的应用具有实时性、自动化、嵌入式(软件)、安全性、和信息互通互联性等特点。

目前,工业物联网广泛应用于制造业、物流和交通运输业、能源和公用电力事业、航空航天、煤矿、石油和天然气、采矿、冶金等各个工业领域。

1.2 工业物联网发展形势

工业物联网是一个新概念,是传统工业自动化和工业信息化结合发展到一定阶段的产物。

工业物联网突破了传统局域网的限制,将工厂生产、企业管理和市场营销等环节进行了强有力的结合,全方位采集底层基础数据,并进行更深层面的数据分析与挖掘,充分发挥整个企业中机器和人的潜能,提高生产效率。

目前,工业物联网仍处于早期发展阶段,但是由于其广阔的应用前景和巨大的收益潜力,许多大型跨国公司、各国政府及国际组织都已经在工业物联网方面进行了大量投入。国际上已建立了 Industrial Internet Consortium(IIC)、AllSeen Alliance、Open Interconnect Consortium(OIC) 6 等多个工业物联网相关的国际组织。

根据 Accenture 的研究报告指出,全球工业物联网市场规模预计在 2020 年将超过 5000 亿美元,近几年将持续高速增长。而到 2030 年,预计工业物联网为世界经济带来的收益至少在 10 万亿美元,而基于持续增加的投入估计,到 2030 年,工业物联网带来的收益可达到 14 万亿美元。

随着我国“中国制造 2025”、“工业互联网”等战略的实施,未来我国制造业整体信息化水平将大幅提升,制造业数字化、网络化、智能化将取得明显进展,数字化研发设计工具、关键工序制造装备数控化将作为工业物联网的基础在规模以上企业得到广泛应用。

而伴随着市场的不断扩展,物联网技术的不断演进和发展,工业物联网的技术发展趋势也逐步朝着智能化、平台化、边缘化等方向发展,呈现出新的特点,即全面感知、泛在连接、智能处理。

全面感知。工业物联网利用射频识别技术、微机电传感器、二维码等技术手段随时获取工业产品从生产到销售到最终用户使用各个阶段的信息数据,感知范围覆盖整个产业链的各个环节,而传统工业自动化系统信息采集只局限于生产质检阶段,而企业信息化系统则并不过分关注具体生产过程。

泛在连接。全面感知的实现需要广覆盖、多连接的联网支持,涵盖了包括企业网、互联

网、工控网、移动通信网在内的各类网络连接，它对网络的依赖性更高，比传统工业自动化、信息化系统都更强调数据交互。

智能处理。随着云计算、人工智能、边缘计算、大数据等新一代技术的应用，物联网设备和平台的智能处理需求愈发迫切，对海量生产数据和信息进行分析和处理，并结合大数据技术，深入挖掘数据价值，是未来工业物联网的核心能力。

1.3 工业物联网安全政策

国家“十三五”规划纲要明确提出“发展物联网开环应用”，将致力于加强通用协议和标准的研究，推动物联网不同行业不同领域应用间的互联互通、资源共享和应用协同，通过开环应用示范工程推动集成创新，总结形成一批综合集成应用解决方案，促进传统产业转型升级，提高信息消费和民生服务能力，提升城市和社会管理水平。

2013年2月5日，国务院发布《国务院关于推进物联网有序健康发展的指导意见》，其中重点提到物联网网络信息安全存在潜在隐患急需加强引导加快解决。在基本原则中提出安全可控。强化安全意识，注重信息系统安全管理和数据保护。加强物联网重大应用和系统的安全测评、风险评估和安全防护工作，保障物联网重大基础设施、重要业务系统和重点领域应用的安全可控。

2017年1月17日，工业和信息化部为推动物联网产业健康有序发展，制定信息通信业“十三五”规划物联网分册。在发布的关于印发信息通信行业发展规划(2016-2020年)的通知中发布了《信息通信行业发展规划物联网分册(2016-2020年)》详细内容。规划中将提升安全保障能力作为六大主要任务之一，提出推进关键安全技术研发和产业化和建立健全安全保障体系。

1.4 工业物联网重大信息安全事件

物联网时代，网络安全形势非但没有减弱，相反会越来越严峻。一是连接的设备更多，预防更加困难；二是，物联网和互联网将虚拟世界和现实世界连在一起，未来发生在网络世界的攻击可能变成物理世界真实的伤害。感知层设备作为网络空间与物理空间的连接点，由于数量众多影响范围广而受到黑客的重点关注，多次大规模物联网安全事件中都验证了感知层设备安全性普遍较差这一事实。

- 海康威视弱口令事件

2015年2月27日，江苏省公安厅发布《关于立即对全省海康威视监控设备进行全面清查和安全加固的通知》称，主营安防产品的海康威视其生产的监控设备被曝出严重安全隐患，部分设备已被境外IP地址控制，并要求各地立即进行全面清查，开展安全加固，消除安全隐患。

- 美国东海岸大面积互联网断网事件

2016年10月21日 11:10 UTC(北京时间 19:10 左右)恶意软件 Mirai 控制的僵尸网络对美国域名服务器管理服务供应商 Dyn 发起 DDOS 攻击，从而导致许多网站在美国东海岸地区宕机。安全研究人员表示，造成此次网络宕机事件的罪魁祸首，可能是大量的物联网设备——包括联网的摄像头和数字录像机，这些设备可能因遭到黑客劫持而被利用。

- 其他物联网安全事件

2007年，时任美国副总统迪克·切尼心脏病发作，被怀疑缘于他的心脏除颤器无线连接功能遭暗杀者利用。这被视为物联网攻击造成人身伤害的可能案例之一。

2008年，波兰一名14岁少年用一个改装过的电视遥控器控制了波兰第三大城市罗兹的有轨电车系统，导致数列车脱轨、人员受伤。

2010年，一名前雇员远程入侵了美国得克萨斯州奥斯汀市汽车经销商的电脑系统，招

致大量客户投诉车辆故障,包括喇叭无故半夜鸣响、车辆无法发动等。

2011年,伊朗2011年俘获美国RQ-170“哨兵”无人侦察机,据称就是伊朗网络专家远程控制了这架飞机的操作系统。

2013年,美国知名黑客萨米·卡姆卡尔在“优兔”网站发布一段视频,展示他如何用一项名为SkyJack的技术,使一架基本款民用无人机能够定位并控制飞在附近的其他无人机,组成一个由一部智能手机操控的“僵尸无人机战队”。

2014年,安全研究人员发现了特斯拉Tesla Model S车型汽车应用程序存在设计漏洞,该漏洞可致使攻击者可远程控制车辆,包括执行车辆开锁、鸣笛、闪灯以及车辆行驶中开启天窗等操作。

2015年,HackPWN安全专家演示了利用比亚迪云服务漏洞,开启比亚迪汽车的车门、发动汽车、开启后备箱等操作。

2016年,腾讯科恩实验室利用安全漏洞成功入侵特斯拉汽车,致使特斯拉全球召回问题车辆。

- 物联网恐成WannaCry下一个目标



图1 WannaCry勒索病毒

令人想哭的 WannaCry 勒索病毒，导致不少 Windows 系统用户成为受灾户，上一波瞄准的是个人计算机(PC)，安全专家指出，物联网(IoT)恐成为下一个目标。

据 IoT Institute 报导，试想黑客在酷寒的冬季控制你家的恒温器，要挟你再不付赎金就没暖气，或者黑客为了赎金不惜攻击电网、工业设施或医疗院所，又或者黑客控制你的智能车门锁，除非付赎金否则开不了车门。

根据国际权威咨询机构预测，到 2020 年，25%的企业安全事件都将会和物联网相关，物联网的安全问题亟待解决！

2 工业物联网信息安全威胁

2.1 工业物联网网络结构

工业物联网层模型由物联网感知延伸层（感知层）、物联网网络业务层（网络层）、物联网应用层（应用层）组成。

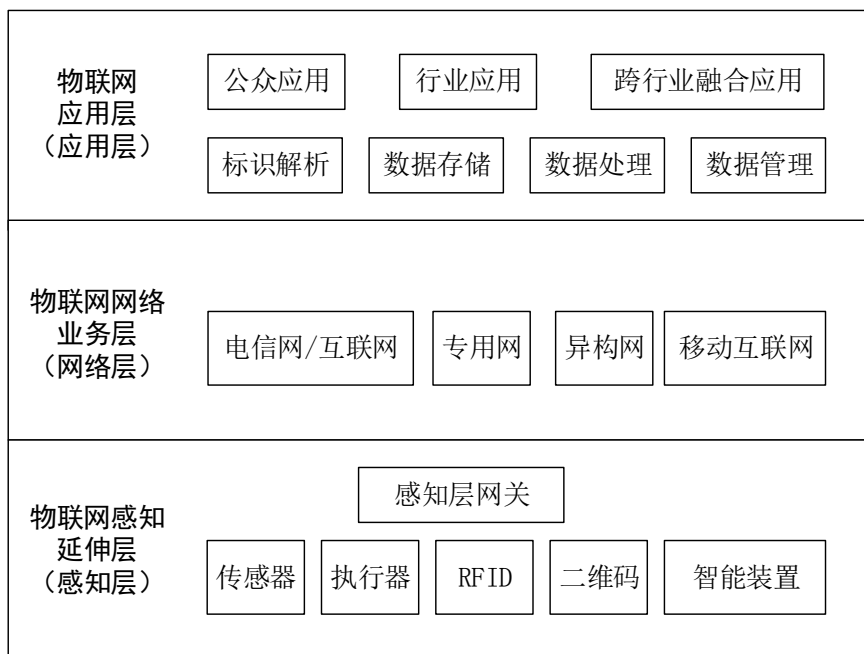


图 2 工业物联网网络结构示意图

- 感知层

感知层包括感知层网关和传感器、RFID 等感知设备，也包括这些感知设备与感知层网

关之间的短距离通信（通常为无线）。感知层网关是将感知设备所采集的数据传输到数据处理中心的关键出口，简单的感知层网关只是对感知数据的转发（因电力充足），而智能的感知层网关可以对数据进行适当处理、数据融合等。

- 网络层

网络层主要实现物联网数据信息和控制信息的双向传递，包括互联网、移动网、专用网等，常包括几种不同网络的融合。

- 应用层

应用层指对感知数据进行集中处理的平台，其中应用支撑是为应用服务提供基础支撑服务的系统，包括标识解析、数据存储、数据处理、数据管理等。对大型物联网应用系统来说，应用层一般是云计算平台，该平台的任务包括收集合法感知网络的真实数据，存储并管理这些数据，管理终端用户对这些数据的访问和使用，以及建立审计、授权、访问控制等机制。

2.2 工业物联网信息安全威胁分析

2.2.1 应用层安全威胁分析

工业物联网应用层存在的安全威胁主要有以下几方面：

- a) 隐私威胁

隐私泄露：隐私泄露是指用户的隐私信息暴露给攻击者，例如用户的病历信息，个人身份信息、兴趣爱好、商业机密等信息。

恶意跟踪：隐私信息的获取者可以对用户进行恶意跟踪。例如，攻击者可以通过标签的位置信息获取标签用户的行踪或者利用标识信息来确定并跟踪贵重物品的数量及位置信息等。

- b) 业务滥用

物联网中可能存在业务滥用攻击，例如非法用户使用未授权的业务或者合法用户使用未定制的业务等。

c) 身份冒充

物联网中存在无人值守设备,这些设备可能被劫持,然后用于伪装成客户端或者应用服务器发送数据信息、执行操作。例如针对智能家居场景中,针对自动门禁远程控制系统,通过伪装成基于网络的后端服务器,可以解除告警、打开门禁进入房间。

d) 信息窃听/篡改

由于物联网通讯需要通过异构、多域网络,这些网络情况多样,安全机制相互独立,因此应用层数据很可能被窃听、注入和篡改。

e) 抵赖和否认

通信的所有参与者可能否认或抵赖曾经完成的操作和承诺。

f) 重放威胁

攻击者向目标(感知设备或物联网应用服务器)发送已接收过的消息,来达到欺骗系统的目的。

g) 拒绝服务攻击

目前的认证方式是应用终端与应用服务器之间的 1 对 1 认证。而在物联网中,终端设备数量巨大,当短期内这些数量巨大的终端使用业务时,会与应用服务器之间产生大规模的认证请求消息。这些消息将会导致应用服务器过载,使得网络中信令通道拥塞,引起拒绝服务攻击。

2.2.2 网络层安全威胁分析

工业物联网网络层存在的安全威胁主要有以下几方面:

a) 网络拥塞和拒绝服务攻击

由于物联网设备数量巨大,如果通过现有的认证方法对设备进行认证那么信令流量对通信网络来说是不可忽略的,尤其是大量设备在很短时间内接入网络,很可能会带来网络拥塞,而网络拥塞会给攻击者带来可趁之机,从而对服务器产生拒绝服务攻击。

b) 中间人攻击

攻击者可以发动中间人攻击,使得物联网设备与通信网络失去联系,或者诱使物联网设备向通信网络发送假冒的请求或响应,从而使得通信网络做出错误的判断而影响网络安全。

c) 伪造网络消息

攻击者可以利用感知层网络的安全性等特点,伪造通信网络的信令指示,从而使得物联网设备断开连接或者做出错误的操作或响应。

2.2.3 感知层安全威胁分析

工业物联网终端接入带来的安全威胁主要有以下几方面:

a) 非授权读取设备信息

对于任意类型的感知设备或感知层网关,包括物联网终端、传感器节点和传感器网关,可能被攻击者物理俘获或逻辑攻破,攻击者可以利用专用工具分析出感知设备所存储的机密信息。

b) 路由攻击

恶意感知设备拒绝转发特定的消息并将其丢弃,以使得这些数据包不再进行任何传播。另一种表现形式是攻击者修改特定感知设备传送来的数据包,并将其可靠地转发给其它感知设备,从而降低被怀疑的程度当恶意感知设备在数据流传输路径上时选择转发攻击最有威胁。

c) 节点欺骗

攻击者通过假冒网络中已有的感知设备或感知层网关,可以向感知网络注入信息来发动多种形式的攻击,包括监听感知网络中传输的信息,向感知网络中发布假的路由信息,重放已发送过的数据信息,传送假的数据信息等。

d) 恶意代码攻击

木马、病毒、垃圾信息的攻击,这是由于终端操作系统或应用程序的漏洞所引起的安全威胁。

e) 隐私泄露

与用户身份有关的信息泄露,包括个人信息、使用习惯、用户位置等,攻击者综合以上信息可进行恶意目的的用户行为分析。

f) 网络中断

路由协议分组,特别是路由发现和路由更新消息,会被恶意感知设备中断和阻塞。攻击者可以有选择地过滤控制消息和路由更新消息,并中断路由协议的正常工作。

g) 网络拦截

路由协议传输的信息,如“保持有效”等命令和“是否在线”等查询,会被攻击者中途拦截,并重定向到其他感知设备,从而扰乱网络的正常通信。

h) 篡改

攻击者通过篡改路由协议分组,破坏分组中信息的完整性,并建立错误的路由,造成合法感知设备被排斥在网络之外。

i) 伪造

感知层网络内部的恶意感知设备可能伪造虚假的路由信息,并把这些信息插入到正常的协议分组中,对网络造成的破坏。

j) 拒绝服务

拒绝服务主要是破坏网络的可用性,减少、降低执行网络或系统执行某一期望功能能力的任何事件。如试图中断、颠覆或毁坏感知层网络,另外还包括硬件失败、软件 bug、资源耗尽、环境条件等。包括在网络中恶意干扰网络中协议的传送或者物理损害感知设备,消耗感知设备能量。

3 工业物联网信息安全需求

3.1 应用层安全需求

工业物联网应用层安全需求包括：

a) 身份鉴别

为防止假冒用户使用未授权的业务应用或者合法用户使用未定制的业务应用，用户请求使用业务前必须经过严格的身份鉴别；为防止末端感知设备身份伪造和克隆等攻击，需对感知设备进行身份鉴别。

b) 组认证

物联网应用通常对应大量的末端节点，这些末端节点可能构成一个组，物联网应用服务器需要提供对这些末端节点进行组认证的能力。

c) 隐私保护

保护行为或者通信信息不泄密，这些信息包括通信内容、用户地理位置和用户身份等。

d) 数据完整性

考虑到物联网络中恶意末端节点可能注入、篡改应用层消息。因此，物联网应用层需要避免未授权的删除、插入和复制操作。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的完整性保护。

e) 数据保密性

在物联网络中各种数据和消息只能让授权用户查看。保密性保护可以避免非授权访问和应用层数据内容非授权阅读。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的保密性保护。

f) 防抵赖

提供不可抵赖性机制，保证通信各方对自己行为及对行为发生的时间的不可抵赖性。例如通过进行身份认证和数字签名，数字时间戳等机制避免对行为发生的抵赖。

g) 抗重放

提供抵御重放攻击的机制。

3.2 网络层安全需求

工业物联网网络层安全需求包括：

a) 组认证

基于组的形式对感知设备进行认证，避免大规模设备认证造成的网络信令拥塞并防止可能的拒绝服务攻击。

b) 身份鉴别

感知设备、感知层网关与网络的需采用多种鉴别方式实现双向身份鉴别。

3.3 感知层安全需求

工业物联网感知层安全需求包括：

a) 物理安全防护

需要采取措施保护感知设备或感知层网关避免失窃，或被攻击者物理上获得或复制。

b) 访问控制

需要采取访问控制的方式，防止末端节点被逻辑攻破，或向其它末端节点或网络设备泄露用户或末端节点信息。

c) 身份鉴别

为确保采集数据来源的合法性及有效性，同时避免非法感知设备接入网络，需对感知设

备进行身份鉴别；为控制合法感知层网关的接入，阻断非法感知层网关的连接，需对感知层网关进行身份鉴别。

d) 数据保密性

感知设备所存储的数据或所传送的数据要加密。

e) 数据完整性

需要采取措施防止感知设备所存储的数据或所传送的数据被篡改。

f) 可用性

需要采取措施保护感知设备，例如采用防病毒软件，防火墙等措施，使之不会被逻辑攻破或被病毒攻击导致不工作。

g) 隐私保护

需要保护感知设备所存储的用户隐私，并防止与用户身份有关的信息泄露。

h) 数据源认证

避免感知设备或感知层网关被恶意注入虚假信息，确保信息来源于正确的物联网设备。

i) 新鲜性

保证接收到数据的时效性，确保没有恶意感知设备重放过时的消息。

4 工业物联网网络安全解决方案

4.1 整体方案设计

通过前述章节对工业物联网应用层、网络层、感知层的安全威胁进行全面的分析，以及第 3 章梳理出各个层次包括身份鉴别、访问控制、安全审计、入侵防范、通信完整性、保密性等多个方面的综合安全需求，据此设计工业物联网网络安全整体解决方案，实现由端至云覆盖应用、网络、感知各层次的安全防护保障体系。

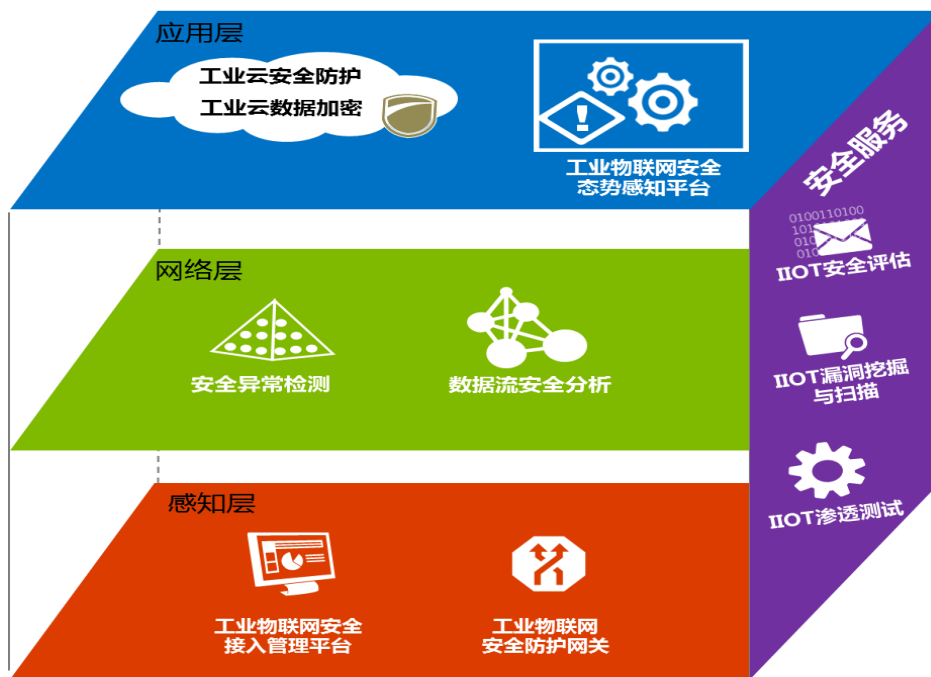


图 3 工业物联网网络安全整体解决方案

方案整体由安全技术防护和安全服务保障两大部分组成：安全技术措施依据各层次业务特点、安全需求特点精确部署。

工业物联网感知层各类设备分布范围广，面临物理攻击、伪造、仿冒等多种类型安全威胁，在感知层部署物联网安全接入与防护措施，提供访问控制、安全认证与准入、数据传输加密等安全能力，确保感知层物联网设备的安全性及可视化管理。

工业物联网网络层是汇集各类感知终端传输数据的通道，各类异常行为、拒绝服务攻击、中间人攻击对网络层的安全性构成了极大的威胁，通过在网络层部署安全异常检测系统和数据流安全分析系统实时监测网络层入侵攻击以及流行为异常等网络层威胁。

工业物联网应用层包含云平台 and 各类应用系统，是工业物联网的业务核心，各类虚拟化应用、大数据分析、移动应用、Web 应用都在该层实现。在应用层的主要以云安全防护为基础，云数据加密为保障，通过工业物联网安全态势感知平台实现整体安全的监测、管理、控制和运营，将网络安全的感知和防护范围扩大到整个工业物联网的每个环节，有效构建工业物联网安全运营体系。

4.2 参考依据

- GB/T35317-2017 《公安物联网系统信息安全等级保护要求》
- GB/T35318-2017 《公安物联网感知终端安全防护技术要求》
- GB/T35592-2017 《公安物联网感知终端接入安全技术要求》
- GB/T 25070 信息安全技术 网络安全等级保护物联网安全设计技术指南
- YD/T 2437-2012 物联网总体框架与技术要求
- YDB 101-2012 物联网安全需求
- 信息安全技术 网络安全等级保护安全设计技术要求（征求意见稿）
- 信息安全技术 网络安全等级保护测评要求（征求意见稿）
- 信息安全技术 物联网数据传输安全要求（征求意见稿）
- 信息安全技术 物联网感知终端应用安全技术要求（征求意见稿）
- 信息安全技术 物联网感知层网关安全技术要求（征求意见稿）
- 信息安全技术 物联网安全参考模型及通用要求（征求意见稿）
- 《物联网白皮书（2011年）》，工业和信息化部电信研究院
- 《物联网白皮书（2016年）》，CAICT 中国通信院
- 《工业物联网白皮书（2017年）》，中国电子技术标准化研究院

4.3 典型应用场景

工业物联网的行业应用范围非常广泛，这里选取了三个比较典型的应用场景，根据其场景业务特点，分析了各个场景中的安全问题和需求，将工业物联网网络安全解决方案在场景中的应用进行了详细阐述。

4.3.1 仓储物流场景

仓库是现代物流的一个重要组成部分，在物流系统中起着至关重要的作用，高效率的仓库可以有效加快物资流动的速度，降低物流成本，保障各项生产的顺利进行，并可以实现对资源的有效控制和管理。仓库的发展经历了不同的历史时期和阶段，从原始的人工仓库到目前互联网时代的智能仓库，通过互联网、物联网等各类新兴技术的应用实现对仓库效率的大幅提升。

随着仓储物流行业的快速发展，物流仓库实体平台与“互联网+物流”的网络化平台的结合及其跨区域整合将进一步加强，使用智能技术驱动物流仓库创新，颠覆传统物流模式，利用机器人和物联网技术相结合，将仓库建设成为智能、高效的智慧仓库系统是目前物流仓库的主要发展趋势。智慧物流仓库的建设，可根据物流仓库的实际需求以及已有的信息化平台，通过增加硬件设施和深化信息调度，实现仓储管理信息化、自动化、智能化、标准化、可视化。以信息系统平台和硬件设施为支撑，以成品出入库和物料搬运为主体业务，打造物流仓库的智慧管理，将仓储、搬运、信息、人员等资源柔性调度，实现智能化。结合智慧物流系统（IWMS）实现“智能物流”，通过互联网、云计算、物联网技术的运用，整合物流仓库资源，从而构建智能化的柔性物流仓库体系。

4.3.1.1 安全性分析

在智慧仓储的场景中，物联网的应用主要包括平台层的物资管理系统，网络层的 WiFi、ZigBee、4G-LTE 等组网技术，感知层的各类传感器、智能终端以及机器人等操作设备，在此场景下，其攻击面广泛，攻击路径众多对物联网网络安全的防护范围和防护粒度提出了挑战；另外智慧仓储管理系统是保障物流系统稳定运行的重要系统，一旦系统遭受攻击，不仅影响物流系统的正常运行，也可能影响到企业或者行业的商业利益，且仓储数据也具有非常

重要的价值，一旦泄露或者遭受破坏，后果也非常严重。

因此，智慧仓储的物联网网络安全防护应是能够覆盖端侧、网络和云平台的体系化防护部署，不仅需要各类物联网终端设备进行防护，也要在云端实现整体安全态势的监测和管控。

4.3.1.2 解决方案的应用

根据对智慧仓储物联网的安全性分析，工业物联网网络安全解决方案在该场景中的应用

设计如下图所示：

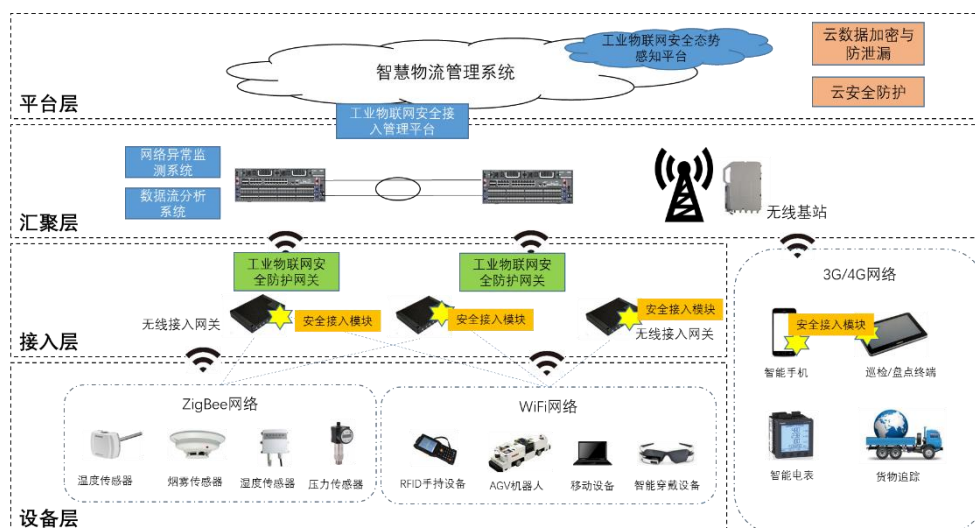


图 4 智慧仓储物联网安全防护示意图

该方案在防护范围和防护粒度上能够满足智慧仓储物联网的安全防护需求，无需对现有物联网网络架构进行大范围调整，可移植性较高，能够实现从端到云的一体化安全防护。

4.3.2 油气开采场景

目前，油气田的开采模式主要是从多个地面井口采集上来后集中汇聚到一个大型集气站，对采集上来的油气进行汇集、脱水、过滤和加压，最后进入天然气的长输管线。油气进入长输管线之前主要包括两大部分：井口 RTU 控制系统和天然气集气站的控制系统，包括 PLC，

DCS 控制系统，在集气站部署有实时历史服务器，负责数据的采集与控制系统，并将生产数据上传到石化企业的 ERP 系统。

4.3.2.1 安全性分析

目前油气开采物联网系统的网络拓扑示例如下：

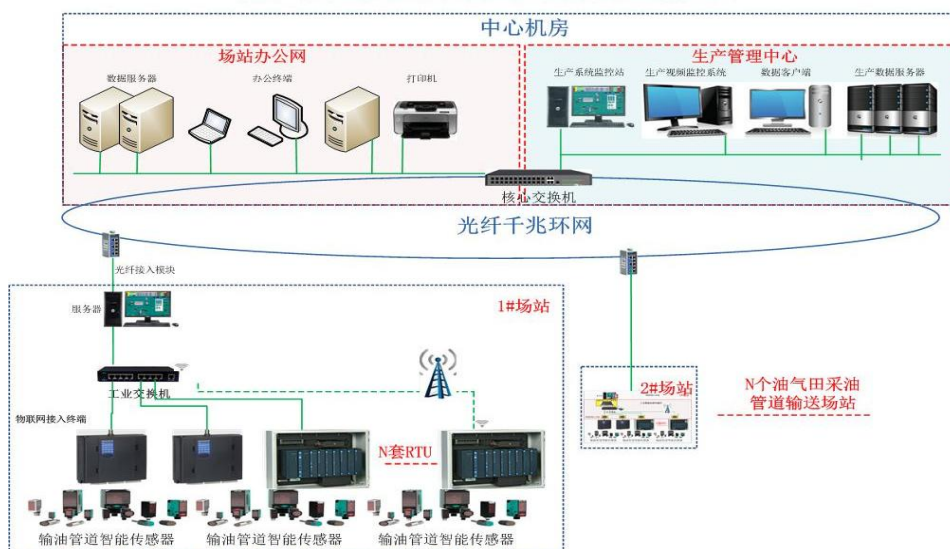


图 5 油气开采物联网系统网络结构示意图

如拓扑示意图所示，目前，油气开采物联网系统的信息安全需求主要包括如下几个方面：
RTU 设备位置分散，存在 RTU 终端被非法接入的安全风险；主要服务器与 RTU 设备之间通讯存在被恶意攻击、数据窃取、恶意篡改、非法远程访问等安全风险；系统缺乏对各类访问行为和控制指令进行安全分析和过滤，无法对拒绝服务攻击等典型攻击行为进行有效的防护；大量独立分散的终端设备缺乏集中的工业物联网可视化安全管理和控制机制。

4.3.2.2 解决方案的应用

根据对系统安全需求的详细分析以及国家等级保护标准的基本要求，结合启明星辰在工控安全和工业物联网安全方面的最佳实践，油气开采工业物联网安全防护解决方案设计如下：

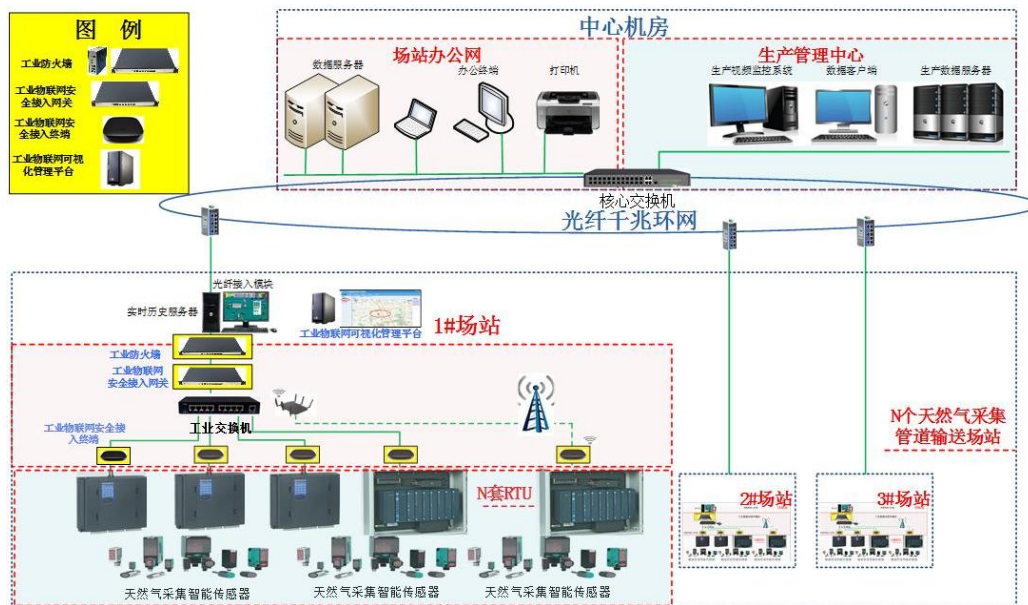


图 6 油气开采物联网系统安全防护解决方案示意图

如上图所示，工业物联网解决方案在此场景中主要是工业物联网网络边界安全防护、工业物联网终端设备接入安全和工业物联网安全可视化管理三部分内容的的应用。

4.3.3 智慧办公场景

4.3.3.1 安全性分析

随着企业信息化应用的不断提升，移动办公、智能办公越来越多的走进各大企业的办公环境，大量的物联网设备接入到企业的核心办公网络，物联网设备包括非智能终端（也称“哑终端”，一般没有数据处理的能力，只能通过网络上报传感数据，或接受操控数据，如门禁、摄像头等）和智能终端设备（例如工业机器人、业务一体机、智能平板等），这些物联网终端设备不仅改变了人们的工作方式，也对企业网络安全提出了新的重大挑战：物联网设备众多，资产情况难以掌握，存在违规接入的风险，同时缺失运维手段、事件监测通报以及应急处理机制；物联网设备在户外、分散安装、易被接触到而又没有纳入管理，导致物理攻击、篡改和仿冒；物联网设备，普遍存在弱口令、漏洞、大量开放端口等安全风险，容易被恶意

代码感染形成僵尸主机,进而构成僵尸网络;物联网设备网络协议多种多样并存在大量漏洞,增加了终端感染病毒、木马或恶意代码入侵的渠道,增加了网络层的安全风险。

通过对哑终端和智能终端的入侵或冒用,以此为跳板可以直接威胁到企业的核心业务系统。如 Mirai 通过对摄像头入侵,向 DNS 运营商 DYN 发起了大规模的 DDOS 攻击,致使整个美国网络访问大规模中断;在某国有大型企业中,黑客通过门禁卡的入侵进而攻破了核心业务服务器。由此可见物联网设备安全日渐成为网络安全的防护短板。

4.3.3.2 解决方案的应用

针对物联网的安全风险,在智慧办公场景下,其安全需求主要包括如下几个方面:由于大多数智能设备是后期加装到办公网络中的,因此,其资产状况在很多企业中并不清晰,很多网络拓扑中也很少涉及此类物联网设备,因此,梳理出网络中的各类物联网设备的资产状况,并实现可视化呈现是非常必要的;由于物联网设备的用途、类型和品牌等不尽相同,需要对物联网设备建立身份安全基线并进行审批,以实现物联网设备的仿冒攻击防护;需要实现对物联网设备的安全态势评估,并有效给出防护建议和手段;需要从网络层和应用层来实现物联网设备的通信协议管控。工业物联网网络安全解决方案在智慧办公场景下的应用设计如下图所示:

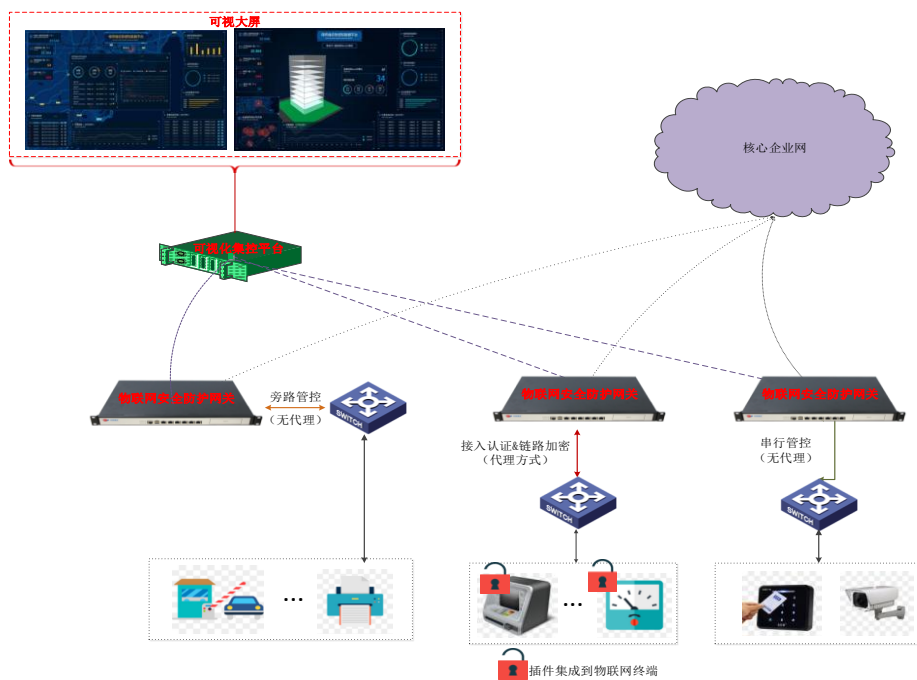


图 7 智能楼宇物联网防护示意图

5 相关安全产品简介

5.1 安全产品

5.1.1 应用层

5.1.1.1 工业云安全防护

■ 产品简介

工业云安全防护产品是针对数据中心、云计算中心，面向虚拟化平台、云计算平台推出的，具有集成多种安全产品的虚拟安全资源池、基于软件定义网络架构的智慧流管理平台、在云或虚拟化平台上进行导流的虚拟导流管理系统三大部件的，具备良好用户体验与易用性，能够为用户构建已知威胁、未知恶意威胁、威胁审计的新一代安全防御体系产品。

5.1.1.2 工业云数据加密

■ 产品简介

工业云数据加密定位于核心敏感数据加密，目前主要应用于工业物联网云数据库加密防泄露。

5.1.1.3 工业物联网态势感知平台

■ 产品简介

工业物联网态势感知平台可针对工业物联网整体网络中所发生的入侵行为、病毒传播实时监测，对大规模爆发的网络入侵行为、病毒传播等事件及时通报，对网络潜在的安全风险以及恶意攻击行为进行分析预警。该系统可实现对工业物联网整体安全情况进行实时统一监测，准确、及时发现存在的安全漏洞等安全隐患，对重大安全事件实时报警，可高度可视化图形界面显示物联网安全趋势。



图 8 工业物联网态势感知平台主页

5.1.2 网络层

5.1.2.1 安全异常监测系统

■ 产品简介

安全异常监测系统产品通过旁路部署监测工业物联网网络层流量,提供特有的物联网安全检测策略,并可针对工业物联网中特定操作数据进行记录和异常行为检测。可检测工业物联网网络中发生的僵尸网络、缓冲区溢出攻击、DDOS、扫描探测、欺骗劫持等各类入侵攻击,实现工业物联网网络安全与异常行为的告警。

5.1.2.2 数据流安全分析系统

■ 产品简介

数据流安全分析系统集成网络访问行为监控、网络流量管理、监控、分析于一体,可应用于网络流量分析、网络流量审计、异常流量分析、故障定位等,充分满足运维人员、安全服务人员的需求。

5.1.3 感知层

5.1.3.1 工业物联网安全防护网关

■ 产品简介

工业物联网安全防护网关主要用于对感知层接入设备的安全管控,通过安全防护网关实现对接入设备的安全访问控制、通讯链路加密等功能,精准阻断来自上层网络的非法指令等可能的攻击行为,基于设备指纹识别阻止仿冒终端设备接入等来自感知层的入侵行为,保障终端侧设备双向通信安全。

5.1.3.2 工业物联网接入管理平台

■ 产品简介

工业物联网接入管理平台可以同时实现对多台物联网安全防护网关的集中管控,对工业物联网感知层设备进行统一综合管理,整体呈现工业物联网接入层设备接入状态、连接关系、安全状态,高度可视化集中呈现感知层设备安全现状。

5.2 安全服务

5.2.1 IIOT 代码审计

■ 服务内容：

针对物联网的源码检测服务是根据漏洞库和安全编码规范,在阅读源码的过程中跟踪关键数据流和逻辑控制流,检查安全控制措施是否到位,是否存在安全隐患,从根本上发现和修补程序存在的安全威胁,进一步保障信息安全,势在必行。

源代码安全检测的最核心的元素是输入。在源代码程序中有很多的输入,包括系统内外部,由于用户的输入被应用程序处理,然后分析,进而展示,那每一个有可能被恶意利用或者造成代码纰漏的输入都是可疑的。据统计,在漏洞里面,由输入数据引起的安全问题高达90%。跟随用户输入梳理整体程序逻辑流发现其中的安全漏洞是及其行之有效的方式。

5.2.2 IIOT 漏洞扫描

■ 服务内容

漏洞扫描是用各种商用安全评估系统或扫描器,根据其内置的评估内容、测试方法、评估策略及相关数据库信息,从系统内部对主机、网络、数据库等系统进行一系列的设置检查,

使其可预防潜在安全风险问题，如弱口令、用户权限设置、用户帐户设置、关键文件权限设置、路径设置、密码设置、网络服务配置、应用程序的可信性、服务器设置以及其他含有攻击隐患的可疑点等。它也可以找出黑客攻破系统的迹象，并提出修补建议。

5.2.3 IIOT 渗透测试

■ 服务内容

渗透测试，也叫白客攻击测试，它是一种从攻击者的角度来对主机系统的安全程度进行安全评估的手段，在对现有信息系统不造成任何损害的前提下，模拟入侵者对指定系统进行攻击测试。渗透测试通常能以非常明显，直观的结果来反映出系统的安全现状。该方法也越来受到国际/国内信息安全业界的认可和重视。为了解服务系统的安全现状，将在许可和控制的范围内，对应用系统进行渗透测试。

具体来说针对公网提供服务的物联网提供远程渗透测试：从远程模拟黑客针对客户进行渗透测试，包括但不限于端口开放性扫描、端口远程连接性测试、远程漏洞测试、远程弱口令鉴权等攻击方式，并根据测试结果提供测试分析报告和整改建议。

对工业物联网系统提供内网渗透测试：在客户内网模拟内部拥有接入权员工对内网服务器等系统模拟内部员工攻击或者内部员工被渗透后扩大测试范围进行人工测试，测试方法包括接入设备渗透、网络层面渗透、应用层面渗透、系统层面渗透等攻击方法，并根据测试结果提供测试分析报告和整改建议。

6 启明星辰集团介绍及工业物联网积累

启明星辰信息技术集团股份有限公司（以下简称：启明星辰）成立于 1996 年，由留美博士严望佳女士创建，是国内规模最大的面向政府及企业的网络安全解决方案与服务供应商。2010 年 6 月 23 日，启明星辰在深交所中小板正式挂牌。



图 9 启明星辰大厦

作为国家级网络安全研究基地，启明星辰集团已积累了 200 多项技术发明专利和软件著作权，参与制订国家及行业网络安全标准 20 多项，填补了我国信息安全科研领域的多项空白，承担并完成了包括国家发改委产业化示范工程，国家科技部 863 计划、国家科技支撑计划、工业和信息化部电子发展基金等国家级、省部级和地方科研项目近百项。同时启明星辰拥有“国家级企业技术中心”、“国家规划布局内重点软件企业”、“中国自主创新品牌 20 强”、“涉及国家秘密的计算机信息系统集成甲级资质”等认定。

启明星辰集团现有员工 3000 余人，在北京、上海、深圳、成都等地设有研发中心。集团拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测/防御管理、网络审计、终端管理、运维管理等技术领域，共有百余个产品型号，整体安全解决方案可帮助客户建立起完善的安全保障体系。集团在全国各省市自治区设立三十多家分支机构，拥有覆盖全国的渠道和售后服务体系。

多年来，启明星辰保持了我国入侵检测、漏洞扫描、统一威胁管理、安全管理平台市场占有率第一位，也是安全性审计、安全专业服务的领导者。近年来，集团在云计算安全、大数据安全、物联网和移动互联网安全领域积极投入布署，建立了自主的核心能力，并逐步形成了信息安全产业生态圈，启明星辰已对网御星云、杭州合众、书生电子、赛博兴安进行了全资收购，旗下投资参股公司达到 30 多家。自此，集团成功实现了对网络安全、数据安全、应用业务安全等多领域的覆盖，并为打造一个可控的安全生态体系不断努力。投资及控股的

公司如下图所示。

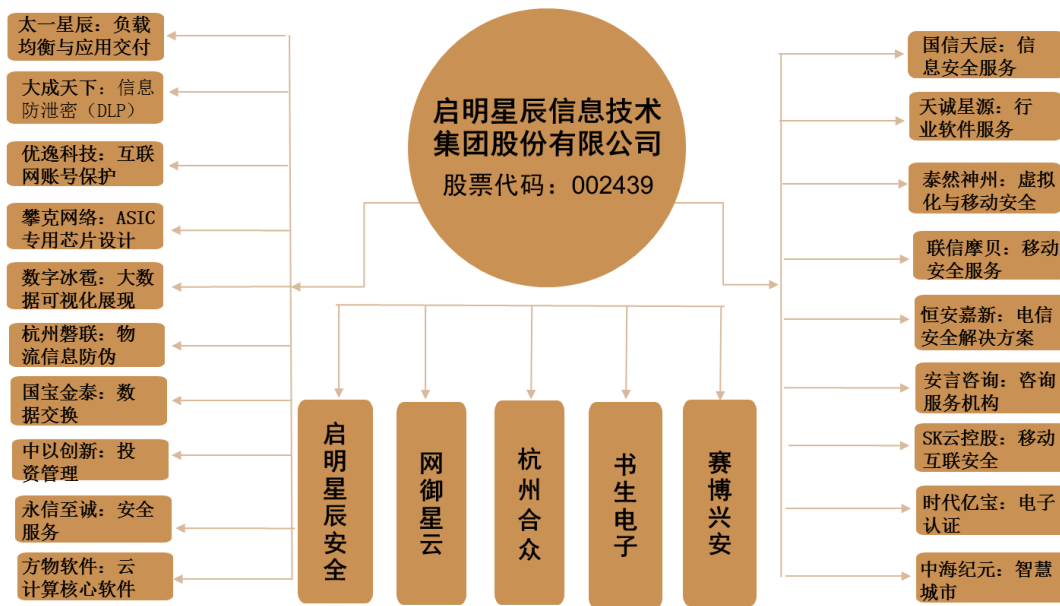


图 10 启明星辰集团组成

作为信息安全产业的领军企业，启明星辰以用户需求为根本动力，通过不断耕耘，已经成为在政府、电信、金融、能源、交通、军队、军工、制造等国内高端企业级客户的首选品牌。作为北京奥组委独家中标的核心信息安全产品、服务及解决方案提供商，奥帆委唯一信息安全供应商，启明星辰得到了国家主管部门的大力嘉奖。

启明星辰将秉承诚信和创新精神，继续致力于提供具有国际竞争力的自主创新的安全生产产品和最佳实践服务，帮助客户全面提升其 IT 基础设施的安全性和生产效能，为打造和提升国际化的民族信息安全产业第一品牌而不懈努力。

启明星辰公司一直以振兴民族软件产业为己任，先后承担并实施完成了多项包括工信部电子信息产业发展基金招标项目、科技部 863 项目、国家发改委产业化示范工程、北京市科技重大项目等国家级/省部级重点信息安全科研项目，并获得了工业和信息化部“优秀电子发展基金授牌”以及国家发改委“产业化示范工程”授牌。公司也由此走出了一条从国家科研项目实施到核心技术积累，再到推出自主创新产品，直至工程示范、产业化的高科技企业发展成功之路。

早在 2010 年伊朗震网病毒事件发生后，启明星辰已将工控安全作为一个重要的方向进行深入安全研究，产品研发部门着手进行工业防火墙、工控漏扫等一系列的工控安全产品研发工作。2014 年初，集团成立了贯穿前中后场的工控安全部，开展全集团的工业物联网信息安全业务。

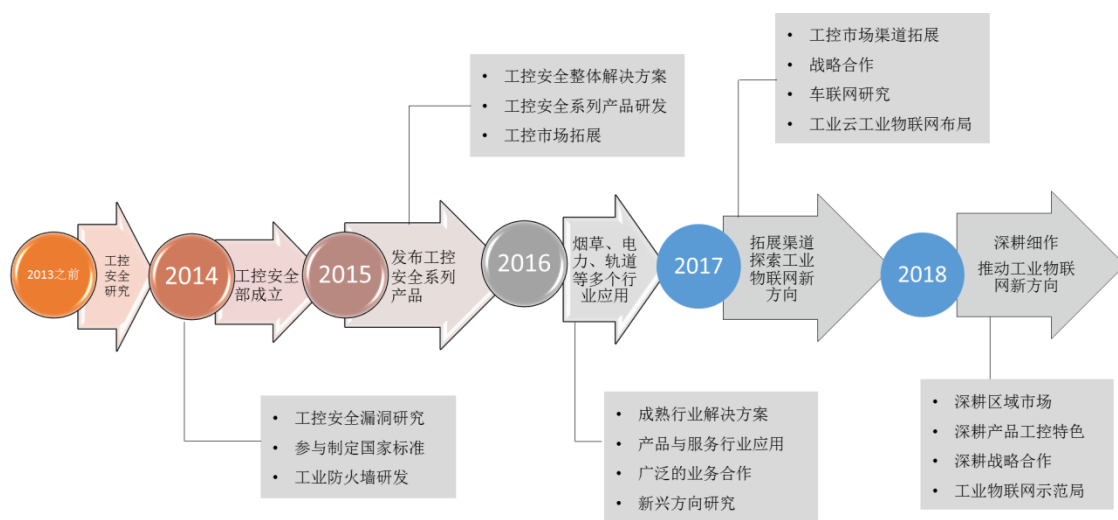


图 11 启明星辰工业互联网业务发展历程

启明星辰工控安全技术和产品研发方面始终坚持创新和自主可控的理念，经过在电力、石油化工、先进制造、轨道交通、烟草等多个行业的广泛应用和打磨，启明星辰的工业防火墙、工业网闸、工控异常监测与审计、工控漏洞扫描、工控安全管理平台等多款产品已不断深度完善，基本夯实了已有技术的工业协议深度防护、异常流量自学习、关键设备运维审计、工控漏洞挖掘等多项核心技术，且与各行业应用场景无缝联接，已在多个行业根据行业业务特点沉淀出切实可行的安全解决方案，在所属行业内产生了标杆示范效应。

石油行业，已开展多个油田、炼化厂两网隔离，实现注、采、输从井口到场站各类地面设备运行状况、设施工艺参数等数据安全传输到数据中心；电力行业，主要针对各级调度的电力监控系统、智能变电站、用采系统、电厂生产控制系统、电网配网的安全防护。参照 36 号文要求，我司已有多个电力工控系统的防护案例。实现了工控网络入侵检测、敏感指令检测、异常流量监测，工控系统边界安全防护，运维操作审计，操作站安全管理等安全技

术建设；轨道交通行业，综合监控系统和信号系统均有多个建设样板工程，重点解决了对车站级到中央级的严格访问控制，车地之间、自动化系统之间的安全通信，自动发现网络中的活跃主机、端口，以及接口间的访问关系，对工控网络的各种入侵、病毒、木马攻击行为，发现 PSCADA、BAS 等系统指令异常，统一实时监测安全状态；烟草行业，我司作为烟草行业工控安全标准制定参与者，扎实走稳每一步，已落实卷烟厂、复烤厂、醋纤公司、商业公司物流系统等众多工控安全项目；先进制造行业，针对机床类的精密加工场景，重点解决其普遍存在的网络无安全域划分、机床近端防护措施缺失、运维操作无审计纪录、缺少违规异常发现机制等问题。

启明星辰截止目前工控安全产品销量上亿元，在行业内处于第一梯队，在国家对智能制造的大力推动下，工业互联网将是其不可或缺的一环，信息安全更是重中之重，目前我们已在继续扎实传统的工控安全技术基础上，不断研究新的工业物联网安全、工业互联网安全及车联网安全的相关防护技术。

启明星辰建设了覆盖工控系统、物联网、车联网等内容的《面向互联网+工业及智能设备信息安全工程实验室》。实验室目前配备有西门子、施耐德、三菱、和利时等国内外主流自动化厂商控制设备及软件系统，高度仿真涉及轨道交通、先进制造、石油炼化、烟草等多个行业工艺生产流程控制，并以此为基础开展工控设备攻防研究及展示、工控安全产品专业适配测试等工作。

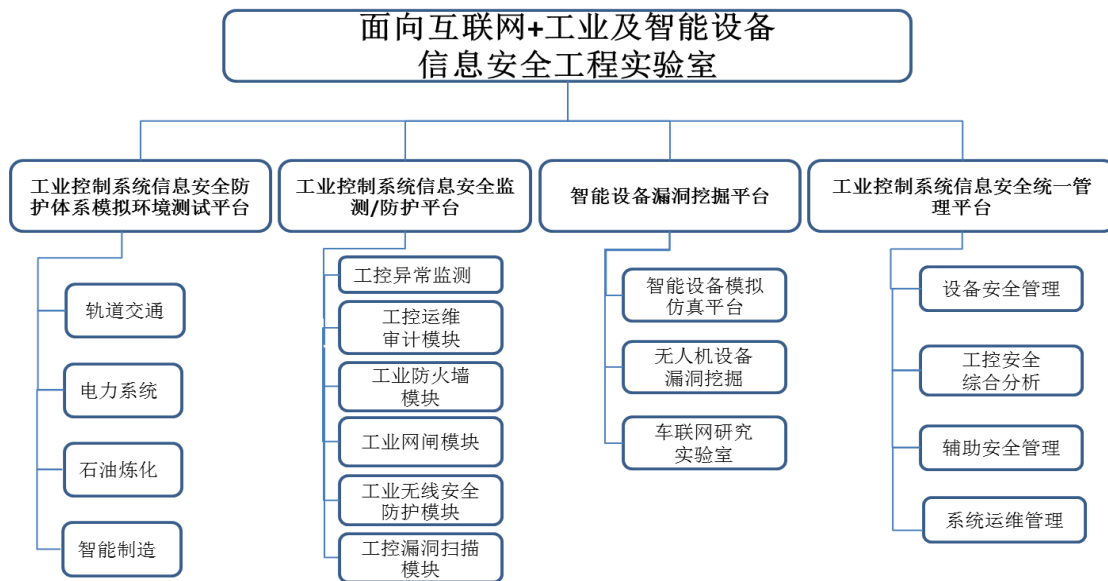


图 12 面向互联网+工业及智能设备信息安全工程实验室组成



图 13 面向互联网+工业及智能设备信息安全工程实验室现场

启明星辰拥有业界享有盛名的信息安全攻防技术的专业团队——积极防御实验室 (ADLab)，该实验室吸收了 70 余名研究网络安全黑客动态和漏洞机理方面的专家，其核心成员在国际网络安全业界具有相当的知名度，他们先后获得了国际网络安全组织和微软亚洲最具价值专家的荣誉和称号。截至目前，启明星辰 ADLab (积极防御实验室) 通过国际 CVE 组织发布的 Windows、Linux、Unix 操作系统的安全漏洞数量居亚洲首位，确立了在网络安全领域的核心地位，也成为安全产品的核心技术保障。ADlab 长期以来密切跟进国

内、国际漏洞机理研究的最新进展，探寻各种操作系统、应用软件以及物联网设备的安全性特征。

- 智能硬件领域安全研究成果
 - 某品牌路由器后门
 - 某品牌摄像头漏洞+海康摄像头漏洞
 - 无人机 GPS 劫持
 - 某品牌智能插座远程控制漏洞
 - 某品牌智能冰箱远程控制漏洞
- 移动互联网领域安全研究成果
 - Android 内核漏洞
 - 某品牌手机漏洞

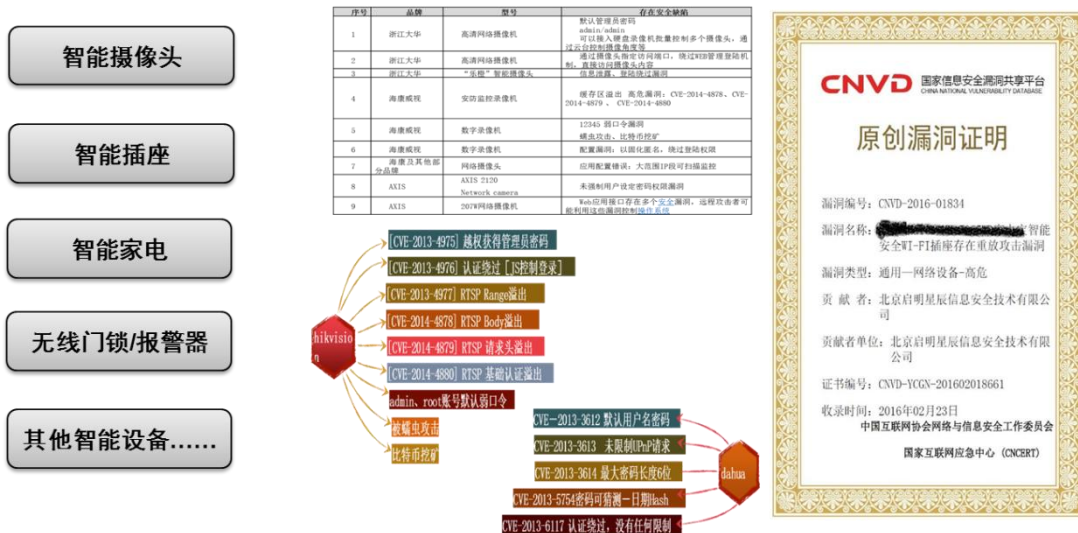


图 14 启明星辰工业物联网安全研究成果

启明星辰近年来积极跟进智能汽车、车联网安全方向，由公司内各领域安全专家对车载系统安全、T-Box 安全、TSP 安全、APP 安全及汽车通讯协议安全进行深入安全研究，并取得了一系列安全研究成果，如在某合资品牌车联网系统发现远程控制过程中身份验证问题，劫持 Authorization 即可获取到对汽车的控制权；某车用智能后视镜 App 设计缺陷导致诸

如用户定位、形式轨迹等隐私信息泄露等。通过对车联网安全研究成果的深入思考，结合多年安全防护经验积累，形成了覆盖车载终端、移动终端、网络通信及车联网云平台的体系化解决方案。

启明星辰积极参与业内重要组织，与国家相关部委、研究机构、高校以及产业界同仁携手推动国内工业物联网安全产业发展，目前已加入工业物联网领域的重要组织包括：

- 军民融合物联网专业委员会——成员单位
- 工业互联网产业联盟——成员单位
- 工信部互联网产业联盟——成员单位
- 国家工业信息安全产业发展联盟——成员单位
- 边缘计算产业联盟——成员单位
- 中国仪器仪表学会——会员单位
- 中国仪器仪表学会物联网分委会——理事单位
- 云安全联盟大中华区——会员单位
- 车载信息服务产业应用联盟——成员单位
- 智能网联汽车产业联盟——成员单位

启明星辰积极参与国家标准制定组织全国工业过程测量和控制标准化技术委员会（TC124）和全国信息安全标准化技术委员会（TC260）的工业物联网安全相关标准制定，目前已参与国家重要的物联网相关安全标准包括：

- 信息安全技术 网络安全等级保护基本要求 第4部分 物联网安全扩展要求
- 云安全联盟（CSA）—物联网安全技术指南
- 智能网联汽车产业联盟-车载端信息安全技术要求与测试方法
- 车载信息服务产业应用联盟—车联网网络安全防护指南细则

目前已参与国家重要的工控安全相关标准包括:

- 工业控制系统信息安全
- 集散控制系统（DCS）安全类系列标准
- 可编程序控制器（PLC）系统信息安全要求
- 信息系统安全等级保护基本要求：对工业控制系统的扩展安全要求
- 中国石化工业控制系统信息安全防护技术规范
- 电力监控系统网络安全防护导则
- 烟草行业工业控制网络安全技术规范