白皮书

2020

工业互联网安全防护白皮书

NSFOCUS

目录

1. 工业互联网安全体系概论

1.1. 工业互联网发展历程

当前，以数字化、网络化、智能化为本质特征的第四次工业革命正在兴起，工业互联网作为新一代信息技术与制造业深度融合的产物，通过对人、机、物的全面互联，构建起全要素、全产业链、全价值链全面连接的新型生产制造的新型生产制造和服务体系，是数字化转型的实现路径，是实现新旧动能转换的关键力量。为抢抓新一轮科技革命和产业变革的重大历史机遇，世界主要国家和地区加强制造业数字化转型和工业互联网战略布局，全球领先企业积极行动，产业发展新格局正孕育形成。

近年来，我国工业互联网发展态势良好，有力提升了产业融合创新水平，有力加快了制造业数字化转型步伐，有力推动了实体经济高质量发展。工业互联网、5G、数据中心等数字基础设施日益成为新兴基础设施的重要组成部分。在这些高科技领域，既是基础设施，又是新兴产业，既有巨大的投资需求，又能撬动庞大的大消费市场，乘数效应、边际效应显著。

工业互联网平台是工业全要素、全产业链、全价值链连接的枢纽，是实现制造业数据化、网络化、智能化过程中工业资源配置的核心，是信息化和工业化深度融合背景下的新型产业生态体系，构建基于海量数据采集、汇聚、分析和服务体系，支撑制造资源的泛在连接、弹性供给和高效配置的载体，其核心要素包括数据采集体系、工业PaaS、

应用服务体系。在数据采集系统方面，通过智能传感器、工业控制系统、物联网技术、智能网关等技术，把设备、系统、产品等方面的数据进行采集。在工业 PaaS 方面，基于工业互联网平台将云计算、大数据技术与工业生产实际经验相结合形成工业数据基础分析能力。把技术、知识、经验等资源固化为专业软件库，应用模型库、专家知识库等可移植、可服用的软件工具和开发工具，构建云端开放共享开发环境。在应用服务体系方面，面向资产优化管理、工艺流程优化、生产制造协同、资源共享配置等工业需求，为用户提供各类智能应用和解决方案服务。

工业互联网包括网络、平台、安全三大体系。其中，网络体系是基础，工业互联网将连接对象延伸到工业全系统、全产业链、全价值链，可实现人、物品、机器、车间、企业等全要素，以及设计、研发、生产、管理、服务等各环节的泛在深度互联。平台体系是核心，工业互联网平台作为工业智能化发展的核心载体，实现海量异构数据汇聚与建模分析、工业制造能力标准化与服务化、工业经验知识软件化与模块化，以及各类创新应用开发与运行，支撑生产智能决策、业务模式创新、资源优化配置和产业生态培训。安全体系是保障，建设满足工业需求的安全技术体系和管理体系，增强设备、网络、控制、应用和数据的安全保障能力，识别和抵御安全威胁，化解各种安全风险，构建工业智能化发展的安全可信环境。

2017 年 11 月，国务院印发了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》（以下简称《意见》），标志着我国工

业互联网顶层设计正式出台，对我国工业互联网发展具有重要意义。安全是我国发展工业经济和工业互联网的基础和重要保障，构建覆盖工业互联网的各类防护对象、全产业链的安全保障体系，完善满足工业发展需求的安全技术能力和管理机制，才能有效识别和抵御网络安全风险和威胁，从而确保我国工业互联网能够健康有序地可持续发展。

《意见》中提到强化工业互联网安全保障能力，加强工业互联网安全体系研究，技术和管理相结合，建立涵盖设备安全、控制安全、网络安全、平台安全和数据安全的工业互联网多层次安全保障体系。加大对技术研发和成果转化的支持力度，重点突破标识解析系统安全、工业互联网平台安全、工业控制系统安全、工业大数据安全等相关核心技术，推动攻击防护、漏洞挖掘、入侵发现、态势感知、安全审计、可信芯片等安全产品研发，建立与工业互联网发展相匹配的技术保障能力。构建工业互联网设备、网络和平台的安全评估认证体系，依托产业联盟等第三方机构开展安全能力评估和认证，引领工业互联网安全防护能力不断提升。

2019 年 7 月，由工信部等十部委联合印发的《加强工业互联网安全工作的指导意见》中提出：强化平台和工业应用程序 APP 安全，要求工业互联网平台的建设、运营单位按照相关标准开展平台建设，在平台上线前进行安全评估，针对边缘层、IssS 层（云基础设施）、平台层（工业 PaaS）、应用层（工业 SaaS）分层部署安全防护措施，建立健全工业 APP 应用前安全监测机制，强化应用过程中用户信息和数据安全保护。

2020 年 3 月，工信部发布了《工业和信息化部办公厅关于推动工业互联网加快发展的通知》（以下简称《通知》），提出加快工业互联网发展“二十条”。其中第九条提出：建立企业分级安全管理制度，出台工业互联网企业网络安全分类分级指南，制定安全防护制度标准，开展工业互联网企业分类分级试点，形成重点企业清单，实施差异化管理；第十条指出：完善安全技术监测体系，扩大国家平台监测范围，继续建设完善升级安全平台，升级基础电信企业监测系统，汇聚重点平台、重点企业数据、覆盖 150 个重点平台，10 万家以上工业互联网企业，强化综合分析，提高支撑政府决策，保障企业安全能力。

1.2. 工业互联网形态及安全问题

1.2.1. 工业互联网 IaaS 的安全问题

作为工业互联网的基础设施层，工业 IaaS 的安全主要是指对基础设施自身的安全保护，以及因资源虚拟化、多租户服务引发的信息安全问题。具体而言，工业 IaaS 的安全问题涉及接入认证安全、传输安全、数据安全、服务管理安全等方面，所面临的安全威胁主要有设备非法接入、恶意代码注入、会话控制和劫持、弱密码攻击、非法更改或删除平台数据、非法窃取数据或计算资源、虚拟机镜像文件非法访问和篡改、拒绝服务攻击、中间人攻击、SQL 注入攻击等。

1.2.2. 工业互联网 PaaS 的安全问题

工业 PaaS 为用户提供了包括工业应用开发工具、工业微服务组件、工业大数据分析平台、数据库、操作系统、开发环境等在内的软件栈，允许用户通过网络来进行应用的远程开发、配置、部署，并最终在服务商提供的数据中心内运行。工业 PaaS 所面临的安全威胁主要有非法窃取或访问软硬件资源、拒绝服务攻击、恶意软件植入等。可以借助于数据加密、防火墙、访问控制机制、强制执行最小权限规则、反病毒软件和入侵检测工具等技术和管理手段进行安全性增强。

1.2.3. 工业现场设备及工控系统的安全问题

随着工业信息化进程的快速推进以及工业互联网、工业云等新兴技术应用的兴起，信息、网络以及物联网技术在智能电网、智能交通、工业生产系统等工业控制领域得到了广泛的应用。为实现系统间的协同和信息分享，工业控制系统也逐渐打破了以往采用的专用系统、封闭运行的模式，开始在系统中采用一些标准的、通用的通信协议及软硬件系统，甚至有些工业控制系统也能以某些方式连接到互联网中，打破封闭网络的屏障优势，使得工业控制系统面临更多的威胁。由于工业控制系统多被应用在电力、交通、石油化工、核工业等国家的重要行业中，网络攻击行为所导致的工业控制系统安全事故造成的社会影响和经济损失会更为严重。出于政治、军事、经济、信仰等目的，敌对的组织、国家以及恐怖犯罪分子都可能把工业控制系统作为达成其目的的攻击目标。

以“震网病毒”为代表的一系列工业控制系统的信息安全事件表明，攻击者正普遍采用被称为高级持续性威胁（Advanced Persistent Threat，简称 APT）的新型攻击手段。攻击者不仅具有明确的攻击目标，而且在攻击时也多采用有组织的多攻击协同模式。由于国内工业控制系统及其工作环境的相对封闭性，国内安全研究团队的研究对象多集中在互联网和传统的信息系统上，在工业控制系统安全方面没有太多的研究成果和实践经验。另一方面，工业控制系统提供商提供的系统或者应用软件更加关注工业控制系统的功能实现，往往忽视信息安全的因素，尤其是在国内的工控系统即使有工控安全的解决方案，往往由于业主方没有明确需求而不会主动配置。在现今工业环境里大量使用计算机设备，例如 MES 系统的数据采集分析与显示的工业计算机、以及对工业控制系统进行控制操作和监控的上位机等等，这些工业主机终端都使用通用操作系统（Windows 或 Linux），采用通用操作系统的优势是使用简单、操作方便，但不可避免的问题是这些操作系统都存在安全风险，尤其是 Windows 系统存在大量漏洞，很容易被黑客攻击或被病毒感染。2010 年发生的 Stuxnet 蠕虫病毒有直接关系，Stuxnet 蠕虫病毒是世界上第一个专门针对工业控制系统编写的破坏性病毒，自此业界对工业控制系统的安全性普遍关注，工业控制系统的安全漏洞数量增长迅速。随着 IT/OT 的不断融合，这些终端设备和工控系统暴露于互联网，被攻击的机会大大增加。工业控制系统脆弱的安全状况以及所面临的日益严重的攻击威胁已经引起了各个国家的高度重视，甚至提升到“国家安全战略”的高度，并在

政策、标准、技术、方案等方面展开了积极应对。在明确重点领域工业控制系统信息安全管理要求的同时，各个国家也在政策和科研层面上积极开展工业控制系统的安全保障工作。

1.3. 工业互联网的网络安全挑战

工业互联网的网络是指工厂内有线网络、无线网络，以及工厂外与用户、协作企业等实现互联的公共网络。

由于 IT 与 OT 的融合，使原有的工厂内外网络边界变的模糊，由于产业模式的创新发展，工厂内外的信息传递更加频繁，这将使黑客更容易入侵到工厂内网络，攻陷生产设备和系统，对生产造成巨大损失。

工业控制系统信息安全目前面临着信息安全与工控系统自身安全融合的要求。目前工控安全产品还处于产品阶段的 1.0 版本的时代，与目前 IT 信息安全和 IT 系统的适配程度相比还有比较大的差距。工业控制系统安全产品是与业务应用相关度比较高的产品。目前的工控安全产品体现在与业务的融合度不够，在深度检测与业务相关的攻击行为的时候往往乏力，缺乏创新性的安全检测思路，防护思路往往缺乏真正有效的方法。

另一方面，随着工业领域中的一些新的应用，如工业云、工业大数据等的普及，工业控制的业态也必将发生一些变化。而信息安全技术与新的业态融合时，必然需要与业务进行融合。而目前工控信息安全技术的融合还没有完全展开，需要在技术方向和应用上有所突破。

2. 工业互联网安全体系与体系能力构建

2.1. 工业互联网安全基本框架

2.1.1. 现今行业内各类工业互联网标准体系

1. OSI 安全体系结构

OSI 安全体系结构是国际标准化组织（ISO）在对 OSI 开放系统互联环境的安全性深入研究的基础上提出的。它定义了为保证 OSI 参考模型的安全应具备 5 类安全服务，包括鉴别服务、访问控制、数据完整性、数据保密性和不可抵赖性，以及为实现这 5 类安全服务所应具备的 8 种安全机制，包括加密、数字签名、访问控制、数据完整性、鉴别交换、业务流填充、路由控制以及公证。OSI 安全体系结构如图 1 所示，安全体系结构中的 5 类安全服务及 8 种安全机制可根据所防护网络的具体要求适当地配置于 OSI 参考模型的 7 个层次中。

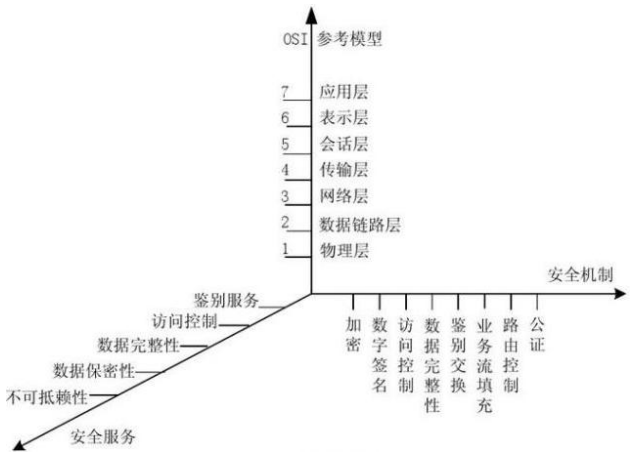

图 1. OSI 安全体系结构

OSI 安全体系结构针对 OSI 参考模型中层次的不同，部署不同的安全服务与安全机制，体现出分层防护的思想，具有很好的灵活性。

然而，OSI 安全体系结构专注于网络通信系统，其应用范围具有一定的局限性。同时，OSI 安全体系结构实现的是对网络的静态安全防护，而网络的安全防护具有动态性，该体系结构对于持续变化的内外部安全威胁缺乏足够的监测与应对能力。此外，OSI 安全体系结构主要从技术层面出发对网络的安全防护问题进行讨论，未考虑管理在安全防护中的地位和作用。面对更复杂更全面的安全保障要求，仅依靠 OSI 安全体系结构是远远不够的。

2. 美国 ISS 公司 P2DR 模型

P2DR（Policy Protection Detection Response）模型是美国 ISS 公司提出的动态网络安全体系模型。P2DR 模型建立在基于时间的安全理论基础之上，将网络安全的实施分为防护、检测和响应三个阶段。在整体安全策略的指导下部署安全防护措施，实时检测网络中出现的风险，对风险及时进行处置，并对处置过程中的经验进行总结以便对防护措施进行调整和完善。这使得防护、检测和响应组成了如图 2 所示的动态安全循环，从而保证网络的安全。

图 2. P2DR 模型

3. 美国国家安全局信息保障技术框架

IATF（Information Assurance Technical Framework，信息保障技术框架）是美国国家安全局于 1998 年提出的，该框架提出保障信息系统安全应具备的三个核心要素，即人、技术和操作。其中，人这一要素包括保障人身安全、对人员进行培训、制定安全管理制度等，强调了人作为防护措施的具体实施者在安全防护中的重要地位。技术这一要素强调要在正确的安全策略指导下采取措施来为信息系统提供安全保障服务并对入侵行为进行检测。操作这一要素则明确了要保证信息系统的日常安全应采取的具体防护手段。此外，该框架将网络系统的安全防护分为网络和基础设施防御、网络边界防御、局域计算环境防御和支撑性基础设施防御四部分。在每个部分中 IATF 都描述了其特有的安全需求和相应的可供选择的技术措施，为更好地理解网络安全的不同方面、分析网络系统的安全需求以及选取恰当的安全防御机制提供了依据。IATF 的具体内容如图 3 所示。

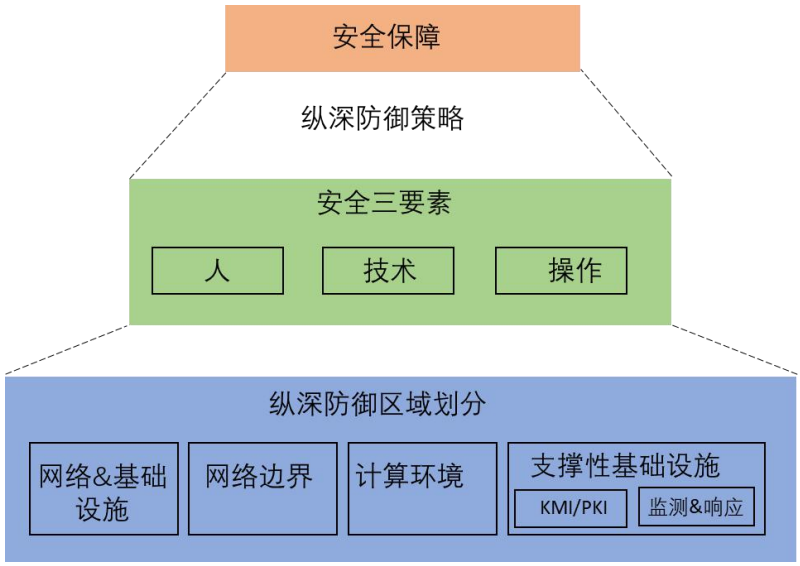

图 3. 信息保障技术框架

IATF 通过对上述四个部分分别部署安全保障机制，形成对网络系统的纵深防御，从而降低安全风险，保障网络系统的安全性。但

IATF 与 OSI 安全体系结构一样，实现的都是对网络系统的静态安全防护，并未对网络系统部署动态持续的安全防护措施。

4. 国际电工委员会 IEC62443

IEC62443 是国际电工委员会工业过程测量、控制与自动化/网络与系统信息安全工作组（IEC/TC65/WG10）与国际自动化协会（ISA99）共同制定的工业控制系统安全防护系列标准。该标准将工业控制系统按照控制和管理的等级划分成相对封闭的区域，区域之间的数据通讯通过管道进行，通过在管道上安装信息安全管理设备来实现分级保护，进而实现如图 4 所示的控制系统的网络安全纵深防御。

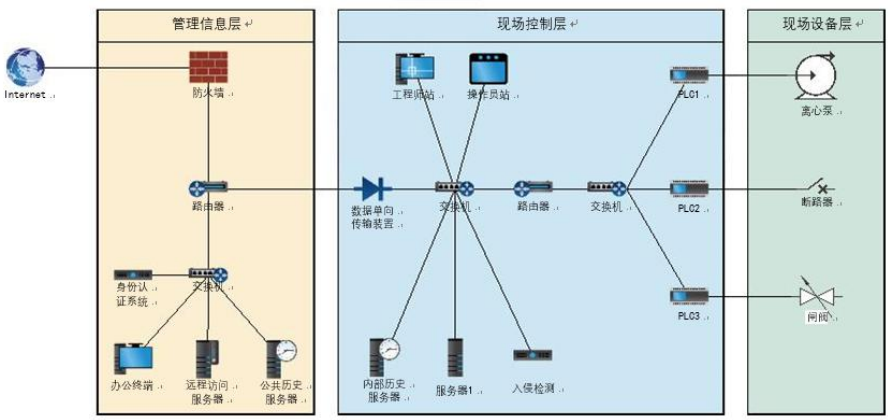

图 4. IEC62443 实施案例

IEC62443 系列标准中对于安全技术与安全管理的实施均提出了要求，但从总体上来看，与 OSI 安全体系结构和 IATF 一样，实现的都是静态安全防护。而工业互联网的安全防护是一个动态过程，需要根据外部环境的变化不断进行调整。在工业互联网安全框架的设计中，需要将动态防护的理念纳入其中。

2.1.2. 美国安全框架

2016 年 9 月 19 日，美国工业互联网联盟（IIC）正式发布工业互联网安全框架（IISF）1.0 版本，拟通过该框架的发布为工业互联网安全研究与实施提供理论指导。IISF 的实现主要从功能视角出发，定义了如图 5 所示的六个功能，即端点保护、通信&连接保护、安全监测&分析、安全配置管理、数据保护以及安全模型&策略，并将这六个功能分为三个层次。其中顶层包括端点保护、通信 &连接保护、安全监测&分析以及安全配置管理四个功能，为工业互联网中的终端设备及设备之间的通信提供保护，对用于这些设备与通信的安全防护机制进行配置，并监测工业互联网运行过程中出现的安全风险。在四个功能之下是一个通用的数据保护层，对这四个功能中产生的数据提供保护。在最下层是覆盖整个工业互联网的安全模型与策略，它将上述五个功能紧密结合起来，实现端到端的安全防护。

图 5. 美国工业互联网安全实施框架

美国 IISF 聚焦于 IT 安全，侧重于安全实施，明确了具体的安全措施，对于工业互联网安全框架的设计具有很好的借鉴意义。

2.1.3. 德国安全框架

德国工业 4.0 注重安全实施，由网络安全组牵头出版了《工业 4.0 安全指南》、《跨企业安全通信》、《安全身份标识》等一系列指导性文件，指导企业加强安全防护。德国虽然从多个角度对安全提出了要求，但是并未形成成熟的安全体系框架。但安全作为新的商业模式的推动者，在工业 4.0 参考架构（RAMI 4.0）中起到了承载和连接所有结构元素的骨架作用。

德国 RAMI 4.0 从 CPS 功能视角、全生命周期价值链视角和全层级工业系统视角三个视角构建了如图 6 所示的工业 4.0 参考架构。从 CPS 功能视角看，安全应用于所有不同层次，因此安全风险必须做整体考虑；从全生命周期价值链视角看，对象的所有者必须考虑全生命周期的安全性；从全层级工业系统视角看，需要对所有资产进行安全风险分析，并对资产所有者提供实时保护措施。

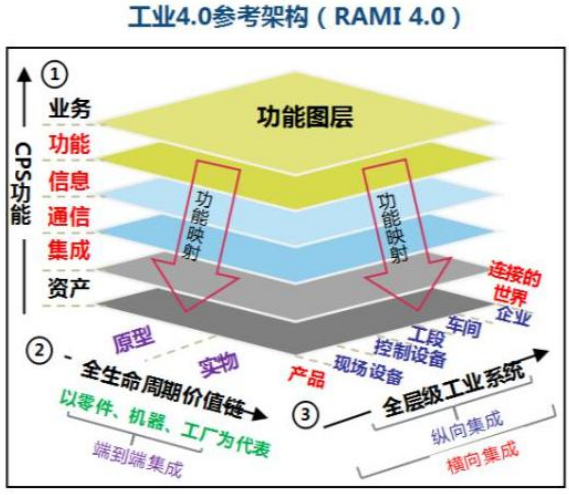

图 6. 工业 4.0 参考架构（RAMI 4.0）

德国 RAMI 4.0 采用了分层的基本安全管理思路，侧重于防护对象的管理。在工业互联网安全框架的设计过程中可借鉴这一思路，并

且从实施的角度将管理与技术相结合，更好地指导工业互联网企业部署安全实施。

2.1.4. 我国工业互联网安全框架 2.0

为解决工业互联网面临的网络攻击等新型风险，确保工业互联网健康有序发展，工业互联网安全功能框架充分考虑了信息安全、功能安全和物理安全，聚焦工业互联网安全所具备的主要特征，包括可靠性、保密性、完整性、可用性和隐私和数据保护，如图 7 所示。

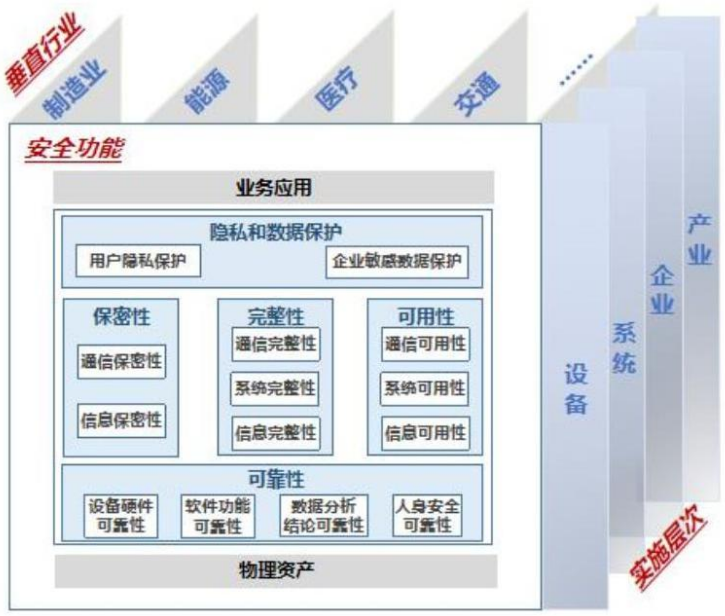

图 7. 工业互联网功能视图安全体系框架

可靠性指工业互联网业务在一定时间内、一定条件下无故障地执行指定功能的能力或可能性。一是设备硬件可靠性，指工业互联网业务中的工业现场设备、智能设备、智能装备、PC、服务器等在给定的操作环境与条件下，其硬件部分在一段规定的时间内正确执行要求功能的能力。二是软件功能可靠性，指工业互联网业务中的各类软件产品在规定的条件下和时间区间内完成规定功能的能力。三是数据

分析结论可靠性，指工业互联网数据分析服务在特定业务场景下、一定时间内能够得出正确的分析结论的能力。在数据分析过程中出现的数据缺失、输入错误、度量标准错误、编码不一致、上传不及时等情况，最终都可能对数据分析结论的可靠性造成影响。四是人身安全可靠性，指对工业互联网业务运行过程中相关参与者的人身安全进行保护的能力。

保密性指工业互联网业务中的信息按给定要求不泄漏给非授权的个人或企业加以利用的特性，即杜绝有用数据或信息泄漏给非授权个人或实体。一是通信保密性，指对要传送的信息内容采取特殊措施，从而隐蔽信息的真实内容，使非法截收者不能理解通信内容的含义。二是信息保密性，指工业互联网业务中的信息不被泄漏给非授权的用户和实体，只能以允许的方式供授权用户使用的特性。

完整性指工业互联网用户、进程或者硬件组件具有能验证所发送的信息的准确性，并且进程或硬件组件不会被以任何方式改变的特性。一是通信完整性，指对要传送的信息采取特殊措施，使得信息接收者能够对发送方所发送信息的准确性进行验证的特性。二是信息完整性，指对工业互联网业务中的信息采取特殊措施，使得信息接收者能够对发送方所发送信息的准确性进行验证的特性。三是系统完整性，指对工业互联网平台、控制系统、业务系统（如 ERP、MES）等加以防护，使得系统不被以任何方式被篡改即保持准确的特性。

可用性指在某个考察时间，工业互联网业务能够正常运行的概率或时间占有率期望值，可用性是衡量工业互联网业务在投入使用后

实际使用的效能。一是通信可用性，指在某个考察时间，工业互联网业务中的通信双方能够正常与对方建立信道的概率或时间占有率期望值。二是信息可用性，指在某个考察时间，工业互联网业务使用者能够正常对业务中的信息进行读取、编辑等操作的概率或时间占有率期望值。三是系统可用性，指在某个考察时间，工业互联网平台、控制系统、业务系统（如 ERP、MES）等正常运行的概率或时间占有率期望值。

隐私和数据保护指对于工业互联网用户个人隐私数据或企业拥有的敏感数据等提供保护的能力。一是用户隐私保护，指对与工业互联网业务用户个人相关的隐私信息提供保护的能力。二是企业敏感数据保护，指对参与工业互联网业务运营的企业所保有的敏感数据进行保护的能力。

3. 绿盟工业互联网安全体系

绿盟采用“平台+服务”的业务模式，建设工业互联网安全体系，产品包括工业互联网安全监测、主机安全防护、蜜网、工控安全工具（漏洞扫描、网站篡改、资产探测、高危漏洞验证等）、工业威胁情报、移动 APP 评估检测、安全服务等，可直接服务电力、轨道交通、化工、汽车、生物医疗行业等。

根据工信部等十部委联合发布的《加强工业互联网安全工作的指导意见》的相关指导规范要求，绿盟科技整合公司现有技术构建工业互联网安全管理体系，建设并完善工业互联网平台安全保障体系。

针对工业互联网：边缘层、工业 IaaS 层、工业 PaaS 层、工业 SaaS 层进行分层部署安全防护措施，健全工业互联网平台和工业 APP 应用前的安全风险监测机制，强化平台和 APP 应用过程中的用户信息、网络和数据安全防护能力。

绿盟工业互联网安全体系能力框架由安全基础设施、安全运营、安全管理和政府/行业安全监管四个组成部分构建一体化动态综合防御体系，总体安全体系架构如图 8 所示。

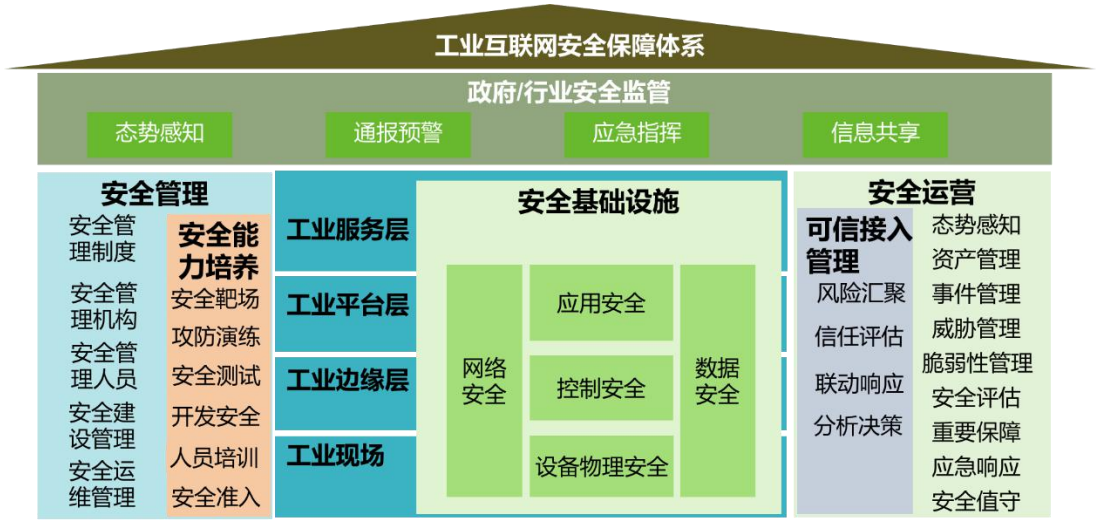

图 8. 总体安全体系架构

通过工业互联网网络安全防护体系，围绕工业互联网平台、网络、数据、主机、接入等方面构建工业互联网整体安全防护保障体系。从工业互联网平台边缘层、工业 IaaS 层、工业 PaaS 层、工业 SaaS 层面临的突出安全风险进行深度分析，应用工业互联网平台安全防护核心技术，形成抗 DDoS、虚拟机逃逸、镜像篡改、数据窃取与篡改等安全防护手段。利用纵深防御安全能力模型，形成边界安全、业务和应用安全、数据安全的工业互联网平台整体解决方案，从形成一套完整的工业互联网安全方案：防攻击、防病毒、防入侵、防窃密、防

控制等综合安全防御能力；同时，通过实现对工业互联网平台流量、主机、设备等进行全面、可靠的网络安全监测分析，形成对工业互联网的综合安全态势监管能力保障，从威胁识别、通报预警、风险评估、应急响应、溯源分析等方面对工业互联网平台各类威胁进行研判分析和处置，构建工业互联网企业对其安全的可视化监管、风险管控、处置和分析的全方位安全运营体系，为工业互联网平台可持续运营提供先导性的安全决策与分析手段；另外，通过完善对工业物联网设备的安全接入和认证能力，借鉴“零信任”网络安全防护体系建设思想，从平台边缘层用户、设备和数据接入层面，有效提升工业互联网平台的接入安全保障水平。

3.1. 绿盟工业互联网安全体系设计原则

绿盟工业互联网安全体系能力架构设计遵循以下原则：

1. 体系化纵深防御原则

在工业互联网环境中，OT 与 IT 相融合，原有的可信边界日益削弱，它本身在物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性，需要从预防、防护、检测、响应等方面多维度考虑安全防护设计，构建纵深防御体系。

2. 动态防护原则

除考虑静态的安全防护措施外，还要考虑动态、闭环的安全防护部署机制。需要结合工业互联网安全防护的特殊要求，采取静态防护与动态防护措施相结合的方式，及时发现并加以有效处置安全事件。

3. 最小特权

泛在联接是工业互联网的重要特征，它要实现人、机、物的全面联接，在工业互联网平台环境中，最小特权原则尤为重要，可以减少各对象之间潜在的相互影响，从而减少、消除对特权无意的、不必要的或者不适当的使用。

4. 平衡性原则

对任何网络，绝对安全难以达到，也不一定是必要的，所以需要建立合理的实用安全性与用户需求评价与平衡体系。安全体系设计要正确处理需求、风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。

5. 遵从性原则

工业互联网系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互联互通、信息共享。

6. 技术与管理并重原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

3.2. 工业互联网平台安全防护体系构建

安全技术架构如图 9 所示：

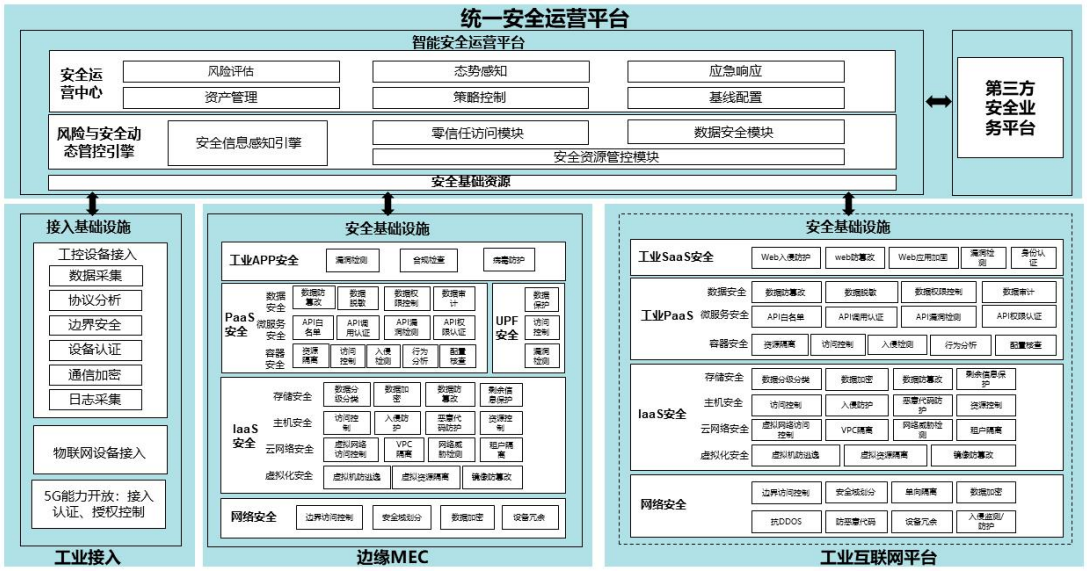

图 9. 安全技术架构

安全基础设施：

工业互联网平台安全基础设施的防护可划分为边缘、网络、平台 IaaS、平台 PaaS 层及平台 SaaS 层五个层面。

1. 边缘层安全

为了工业互联网场景中各类设备安全可信接入，采用安全网关接入的形式实现数据采集安全和传输安全。

2. 网络安全

通过采用划分隔离、访问控制、机密性与完整性保护、异常监测、入侵防范、安全审计和单向隔离等技术手段实现云平台的网络架构安全、网络传输过程中的机密性和完整性防护，以及通信环境的可信验证。实现对来自云平台内外部的双向网络攻击的检测、告警、阻断和审计。

3. 平台 IaaS 层安全

IaaS 层包括支撑工业互联网平台运行的各类物理及虚拟资源，如服务器、存储、网络、虚拟化等。

通过虚拟化安全、主机安全、虚拟化网络安全和存储安全设计解决因资源虚拟化、多租户服务引发的信息安全问题。

4. 平台 PaaS 层

PaaS 层包括数据分析服务、平台微组件应用开发环境等。通过容器安全、微服务安全和数据安全设计为 PaaS 服务提供安全防护

5. 平台 SaaS 层

SaaS 层包括面向各类工业应用场景的应用等，是平台的门户，通过身份认证、数据加密、漏洞检测、web 防护等技术对 SaaS 层提供安全防护。

6. 智能安全运营体系：

通过安全信息感知系统、安全资源管控系统对安全基础资源的数据采集与管控。通过大数据分析平台进行多维度安全风险关联分析支撑安全运营决策。

智能安全运营平台具有资产管理、基线配置、策略控制、态势感知、风险评估、零信任服务和应急响应能力。

3.3. 绿盟工业互联网安全能力体系

绿盟基于工业互联网安全建设迫切性分析，总结概括工业互联网的安全能力主要为：

数据接入安全：防止数据泄漏、被侦听或篡改，保障数据在源头和传输过程中安全。

平台安全：确保工业互联网平台的代码安全、业务和应用安全、数据安全、网站安全。

访问安全：通过建立统一的访问机制，限制用户的访问权限和所能使用的计算资源和网络资源实现对工业互联网平台重要资源的访问控制和管理,防止非法访问。

一些新安全技术正在工业互联网领域的创新中获得快速发展。

3.4. 绿盟工业互联网安全体系能力框架实施对象

针对工业互联网安全体系能力的实施对象我司进行如下划分：

安全基础设施：面向工业设备、控制、网络、数据和应用五个对象在平台侧提供安全防护能力，并为安全运营提供技术支撑。

安全运营：可信管理模块对接入访问进行风险汇聚、信任评估、联动响应和分析决策，为企业提供可信接入能力，动态避免对资源的非授权访问。而态势感知、资产管理、事件管理、威胁管理、脆弱性管理、安全评估、重要保障、应急响应和安全值守模块则基于安全运营平台为安全预警、安全监测、安全响应处置提供支撑。如有政府/行业监管要求，安全运营平台可与监管平台对接。

安全管理：在网络安全防护领域有“三分技术、七分管理”的传统。有效的安全防护体系架构必须讲管理与技术相结合。企业需要注重安全能力培养，包括安全靶场建设、定期攻防演练、安全测试、开发安全、人员培训和设备安全准入机制的不断完善。企业在制度、

机构、人员、建设与运维管理方面需要不断持续改进，做到目标明确、责权清晰，保障企业业务的健康发展。

4. 工业互联网安全能力云化

4.1. 工业互联网安全能力云化需求

工业互联网安全云化是指工业互联网应用层的应用服务安全。其中，工业 APP 涉及专业工业知识、特定工业场景，集成封装多个低耦合的工业微服务组件，功能复杂、安全设计规范缺乏，可能存在安全漏洞和缺陷，面临的工业 APP 漏洞、API 通信安全、用户管控、开发者恶意代码植入等应用安全问题更为突出。

4.2. 工业互联网云化安全与信息安全能力融合

绿盟为了保证工业云化应用的安全，利用云计算技术简历一套云安全集中管理系统，通过安全资源池的方式部署 WAF 等安全防护产品，为同业软件提供应用实施深度防御、Web 应用安全过滤、敏感信息防泄漏、网页防篡改等安全防护，抵御针对应用软件的外部攻击、具备了各种安全防护手段的按需提供能力。

云安全集中管理系统遵循以业务为中心，风险为导向的，基于安全域的纵深主动防护思想，综合考虑云平台安全威胁、需求特点和相关要求，对安全防护体系架构、内容、实现机制及相关产品组件进行了优化设计。采用“软件定义安全 SDS”架构，将虚拟化安全设备和传统硬件安全设备进行资源池化的整合。通过该平台实现安全设备

服务化和管理的集中化，以及安全能力的“按需分配、弹性扩展”，满足客户的合规性需求，提高云上安全运维效率。

平台的实现主要分为三个层面如图 10 所示，最底层：安全资源池；中间层：平台控制层；最上层：平台应用层；

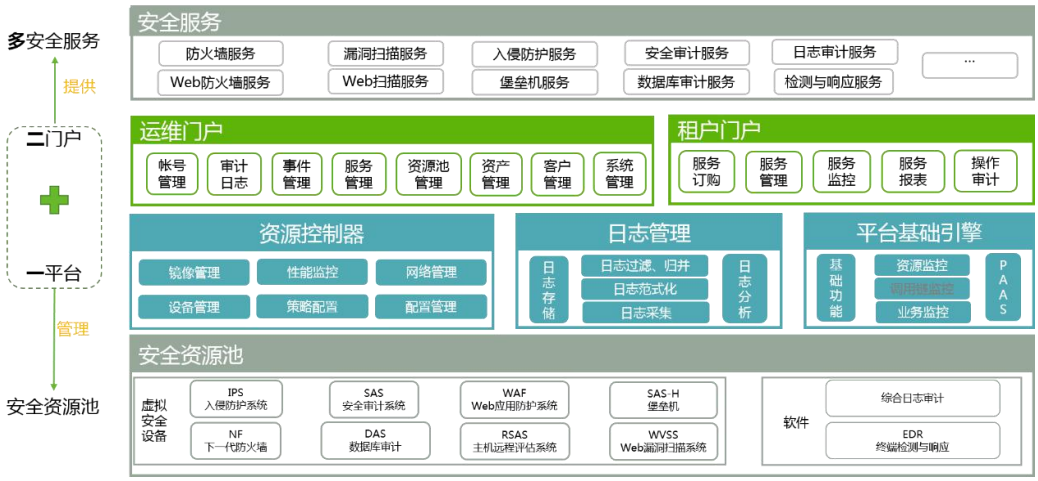

图 10. 云安全集中管理系统架构图

4.2.1. 安全资源池

支持虚拟化安全产品、软件类安全产品以及硬件安全产品等不同类型的的安全能力的纳入，并接受安全资源池的统一管理，对外提供相应的安全能力。目前该方案提供的安全资源池包含了虚拟化类型安全能力有：下一代防火墙、入侵防护系统、web 应用防火墙、网络安全审计、系统扫描器、web 扫描器、堡垒机、数据库审计；软件类型安全能力有：终端检测与响应 EDR。

4.2.2. 平台控制层

4.2.2.1. 资源池控制器

资源池控制器可对安全资源池中所有安全能力进行集中调度管控，实现对安全能力的策略管理、配置管理、性能监控、服务编排、网络管理等功能，还可根据应用场景的不同灵活配置和扩展。

运维门户可通过控制器实现安全服务的开通，针对虚拟化的安全设备可以控制设备的生命周期管理，实现启动、关闭、重启和删除等操作。资源池控制器还可以对接云内网络设备，实现引流的全自动化流程，当租户下发了防护策略后把云内流量自动按需牵引到安全资源池内做检测和防护。

4.2.2.2. 日志分析模块

日志分析模块可以收集安全资源池中各类安全设备日志，通过采集、范式化、过滤和归并等一系列处理流程，实现各种安全设备日志的统一管理和存储。在日志管理的基础上，进行一些分析规则的配置，对标准化事件进行分析，符合规则的进行告警，并区分不同租户或者业务系统推送到门户进行呈现。

平台基础引擎采用 WEB 前端与后端业务逻辑分离设计，为门户提供基础功能支持。为平台基础提供 PAAS 功能层服务包括消息中间件、数据服务等；平台基础引擎采用微服务设计，借助容器化实现各个功能组件，利用容器管理系统可快速实现对资源、业务、调用链的监控。

4.2.3. 平台应用层

4.2.3.1. 租户门户

为满足用户细粒度的安全需求和自主可控、可管理的安全目标；用户可根据自己的业务情况，在租户界面服务市场中自行按需选择满足自己安全需求的安全能力，实现安全的自主可控；同时在租户安全服务界面自主实现安全服务细粒度的策略配置和下发；用户还可以通过服务监控、服务报表了解自己购买服务的运行情况和业务系统的安全风险。

4.2.3.2. 运营管理门户

通过运维门户对安全资源池的资源进行统一管理，对资源池中安全能力抽象形成安全服务并进行组合和发布；能通过运维门户对安全资源池进行统一的监控、对事件告警进行统一的查看，也可以查看整个安全资源池的运行状态、服务使用率，实时掌握安全资源池动态。在运维门户上也可以实现对整个 NCSS 各个组件模块运行稳定性的整体监控，保障整个系统的正常运行。

5. 工业互联网数据安全

5.1. 工业互联网中的工业数据特点

5.1.1. 工业数据的形态、特点

工业大数据存在 “多模态、高通量、强关联”的特性。我司在工业领域总结了多种不同类型的数据，数据模态多样，结构关系复杂。高通量是指数据持续不断地产生，采集频率高，通量大。强关联是指工业场景下的数据有非常强的机理支撑，不同学科之间的数据是在机理层面的关联，而不是数据字段上的关联。

而对工业大数据的分析应用，也不是将深度学习、强化学习的方法放到这里就可以有结果。需要获知研究对象的机理模型与定量领域知识，而这在当前基础上前进很困难。需要找出数据在输入、输出之间的统计关系，对机理和模型不确定、不清晰的部分加以补足，这是工业大数据应用的基础。

智能制造在不断获得数据的驱动，从智能制造到工业互联网，核心都是利用数据和模型，优化制造资源的配置效率。

工业互联网并不等同于智能制造，区别在于数据的跨界和业务的边界上是否有所突破。当下，太多人过于重视平台能力，而真正的工业互联网讲的是生态，资源优化从描述、诊断向预测、决策不断深入，从单机设备、生产线、产业链再到产业生态不断拓宽。

5.1.2. 工业数据的应用场景

工业大数据的三个典型应用场景，也是实现工业互联网的目标，包括智能装备、服务型制造和跨界融合。

第一个层次是设备级的，就是提高单台设备的可靠性、识别设备故障、优化设备运行等；

第二个层次更多是针对产线、车间、工厂，提高运作效率，包括能耗优化、供应链管理、质量管理等；

第三个层次是跨出了工厂边界的产业跨界，实现产业互联。

5.2. 工业数据安全风险及安全能力需求分析

5.2.1. 工业数据面临的安全风险

数据是工业互联网运营最有价值的环节，工业互联网最核心的价值之一就是实现数据的共享与实时利用。工业互联网采集、存储和利用的数据资源存在数据体量大、种类多、关联性强、价值分布不均、不同领域数据保护利用存在较大差异等特点，因此工业互联网数据安全存在责任主体边界模糊、分级分类保护难度较大、事件追踪溯源困难等问题。同时，工业大数据技术在工业互联网中的广泛应用，使得工业互联网面临着数据加密存储技术尚不完善，鉴权技术发展尚不成熟，平台用户信息、企业生产信息等敏感信息存在泄露隐患，数据交易权属不明确、监管责任不清等问题，工业大数据应用存在安全风险。

5.2.2. 工业数据安全能力需求

工业数据安全需要能够提供工业敏感数据发现与识别，数据防泄漏，数据脱敏，数据审计等功能，向工业互联网业务平台提供接口，实现对企业工业数据的分类分级，使工业企业具备对自身敏感数据的发现与管理能力。

5.3. 基于敏感数据识别与防泄漏的工业数据安全

绿盟基于敏感数据识别与防泄漏的数据安全能力可以提供工业互联网敏感数据发现与识别，数据防泄漏，数据脱敏，数据审计等功能，向工业互联网业务平台提供接口，实现对企业工业数据的分类分级，使工业企业具备对自身敏感数据的发现与管理能力，如图 11 所示。

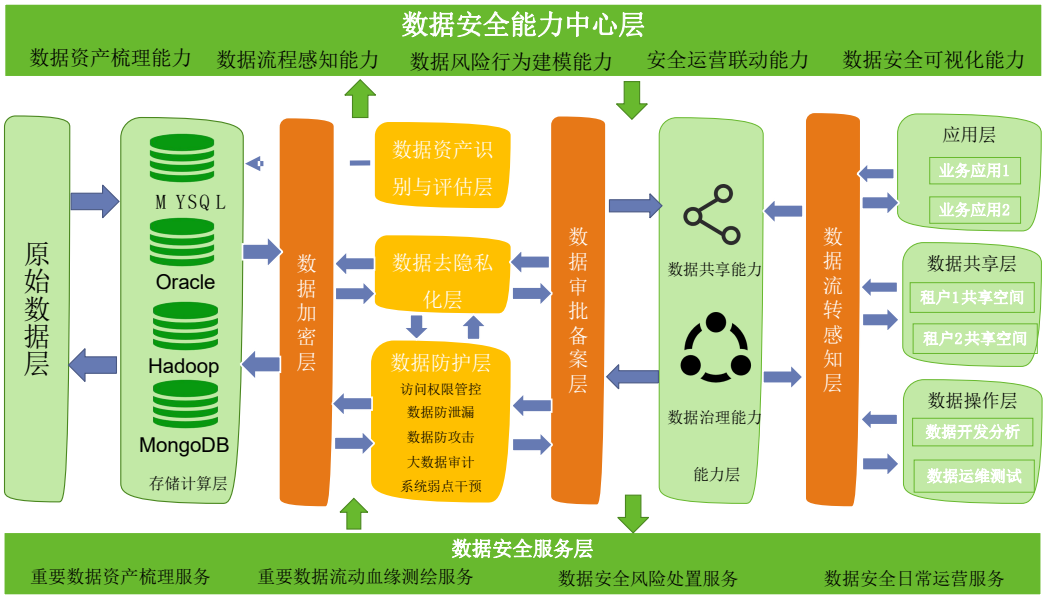

图 11. 数据安全子系统架构

5.3.1. 敏感数据发现与识别

敏感数据发现与识别系统的整体架构如图 12 所示：

图 12. 敏感数据发现与识别系统架构示意图

基础平台包含专用硬件平台和基础软件平台，包含了绿盟科技定制操作系统、文件系统、硬盘加密解密、应用程序加密解密、输入输出加密解密、IPv4/IPv6 网络服务、内置数据库、Web 服务、程序运行环境等功能。

系统服务层包含数据处理引擎和系统服务引擎。数据处理引擎是系统内部的数据接口，提供了数据库访问、数据缓存、数据同步等功能。数据处理引擎屏蔽了数据库系统操作的细节，减少数据库的连接，优化数据库的访问，缓存常用和计算复杂的数据，集中处理数据的逻辑，降低了其他功能模块的维护工作量。系统服务引擎是系统内部的功能接口，提供了系统还原点备份与恢复、任务数据导入导出等功能。系统服务引擎解耦了前台操作和后台操作，后台功能以特定的权限运行，增加了系统的安全性。

系统核心层包含组件发现、漏洞扫描、配置核查、敏感数据发现、流量获取和协议解析等，有较多可扩展的模块和插件。报表引擎是报表展示的核心处理模块，能够提供 HTML、WORD、EXCEL、PDF 等多种报表格式。调度引擎是扫描工作的协调中心，根据用户操作的不同可能有立即执行的任务、定时执行的任务、周期执行的任务等，检测出任务的类型和优先级，进行漏洞扫描或者配置检查、口令猜测。状态引擎是系统状态的协调中心，主要包含系统资源状态信息、系统的授权证书信息、BDB 配置项、任务执行进度信息、升级进度信息等。证书系统提供了产品可授权使用的信息，包含购买用户、设备 HASH 值、授权 IP 数、授权使用模块、授权起止信息等。升级系统提供了产品更新的能力，为扫描插件更新、产品功能更新、产品反馈修改等提供了可能。

系统接入层包含了用户通过浏览器访问 Web 页面、通过串口访问控制台、通过数据接口进行数据交互等方式，其中数据接口包含第三方平台管理数据接口、SNMP Trap。

5.3.2. 数据防泄漏

绿盟数据防泄漏以自然语言处理技术作为内容识别核心引擎，虚拟文件驱动加密作为核心基础技术，可帮助企业对结构化和非结构化数据进行数据治理（文档资产统计、密级标识等）、安全管控（数据加密、权限管理，数据脱敏、边界防护、应用准入、行为审计、数据防护等）、追踪溯源（文档操作、介质操作、用户操作、系统操作等）

和态势感知（趋势分析、风险预警、溯源、风险人员画像）。防护范围覆盖终端数据、存储数据、网络数据、业务系统数据、邮件数据。最终实现掌握数据分布、风险看的见、泄漏防的住的整体效果，如图13所示。

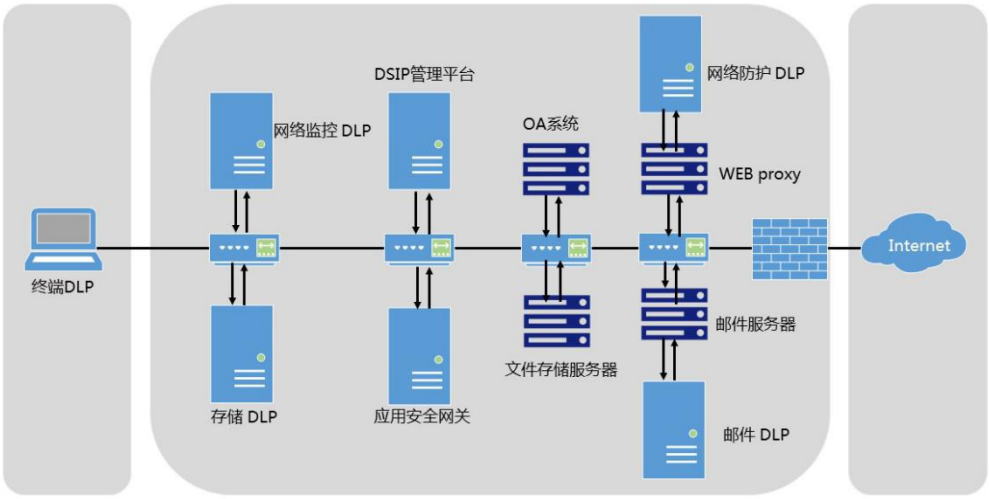

图 13. 数据泄露防护系统（DLP）示意图

整个数据泄露防护系统由安全智能管理平台（简称：SIP）及终端数据安全、网络数据安全、应用系统数据安全四大功能模块组成。帮助用户做到事前主动防御、事中检测响应、事后追踪溯源、全程态势感知。

6. 工业互联网安全态势感知

绿盟根据国家对工业互联网安全态势感知的建设思路，建设业务监测与态势感知一体化的平台。平台涵盖资产图谱绘制，发展趋势预测，安全态势感知，威胁溯源处置等主要功能，着力构建内外一体，部、省、企业三级协同联动的弹性架构，服务于工业互联网主管部门

对工业互联网新技术、新产品、新模式、新业态的监管，提升安全态势感知和综合保障能力。

绿盟工业互联网安全态势感知是在大数据框架的基础上为工业环境提供安全监控及响应的安全运营中心。它具有一定的智慧能力，具备持续的检测、响应和预测的自适应体系架构；同时它可以高效地基于情境上下文和外部威胁情报，协助安全专家发现安全问题，并能通过实际的运维手段实现安全闭环管理。

通过部署在工业互联网设施系统的多维感知设备，实时工业互联网基础设施数据，通过关联分析、深度学习等大数据分析方法，为用户提供风险评估量化与排名、事件关联分析、深度威胁挖掘、设备状态管理等态势感知功能。同时平台还能够通过全网主动探测的方法，对工业互联网设施的存活、状态、脆弱性、安全性进行检测，实时向用户动态反馈我国各区域工业互联网设施网络安全状况，依据安全态势发展趋势为用户提供安全策略和建议。

7. 工业互联网安全监测评估及应急处置服务能力

7.1. 安全监测评估服务能力

绿盟安全监测评估技术从等级测评价格参考规范，加强对托管数据中心的等级保护管理，加强商用密码和数字证书的安全管理和测评，测评报告的专家评审等方面进行设计，采用配置一体化、便携式、高性能专用硬件装备，集检查对象信息收集、合规评估、资产安全评估、

流量安全评估、无线 WiFi 评估、主机恶意代码评估于一体的综合评估工具集，为用户提供标准、专业的检查指导，多样的评估功能，并支持对评估结果数据的关联分析、统计对比，可帮助用户快速分析展示合规现状，定位工业网络安全风险。

7.2. 应急处置服务能力

绿盟工业互联网应急处置服务工具通过扩展硬件接口和软件能力，实现对 PLC，工业机器人等工控硬件软件产品的日志获取。

建立基线，通过大数据分析，实现复杂环境下大量信息的清洗和分析。在日志流量等方面的处理有长足进步。

使用先进的数据分析比对方法，实现对异常行为的识别，并对众多异常行为进行关联，最终发现是某种安全事件。

建立完善的匹配处置库，能够根据收集到的信息，得出安全事件的重要性、当前发生的可能性和匹配度。能够智能的给客户提出包含多种处置建议的处置方案。

能定位到问题资产，让客户定点对相关资产进行处理，节省处理安全事件的时间。

8. 工业互联网安全展望

现阶段，从国家到企业对工业互联网安全的重视程度越来越高，安全投入呈现增加趋势，工业互联网安全市场将有巨大需求，总体来说工业互联网企业对安全的投入呈现一个良好的趋势。

工业互联网安全建设最大的难处在于在没有发生安全事故的情况下，企业高层较难理解安全建设段时间内给企业带来的收益，工业互联网安全建设的投入产出比不被企业决策层理解。

现今工业企业针对工业防火墙、工业主机防护、工业安全集中管控平台三类产品的需求最高，可见工业企业首要关注的问题仍然停留在工业网络安全建设方面。通过三年行动计划，国家正在加速推动安全监测、安全评估、安全服务等安全能力及服务平台的建设。

工业互联网是互联网和新型工业制造业全方位的深度融合所形成的的新型的产业和应用生态体系。工业互联网的建设需要对有较为成熟的工控业务背景，能够从业务场景的角度切入，从而对工业互联网进行全方位的安全规划。由于安全企业对工控业务的理解度不足，现今更多的工控厂商或者工业制造厂商与安全厂商深度合作，建设安全实验室、学校等，来进行安全人才的培养。在工业信息安全保障方面，制定工业数据安全规范，研制工业互联网大数据分级分类、工业APP 管理、工业互联网建设评价等关键标准，围绕平台数据收集、存储、传输、共享等各个环节，明确差异化安全机制和策略。建设工业互联网大数据中心，建立中央、地方、行业企业多层次数据管理机制，打破数据孤岛和基础设施捆绑。强化平台安全监测预警能力，搭建国家、地方、企业多级协同联动的态势感知网络，实现对重要和关键平台接入设备、控制系统、运行数据的风险实时监测，感知边缘层、IaaS 层、PaaS 层和 SaaS 层等的安全状态，切实提升工业互联网安全防护水平。

安全企业需要不断深入的与更多的工业企业、工业互联网平台企业工业集成商以及国安家监管部门进行深度生态合作，从业务场景的角度为不同行业的工业企业客户提供更加优质以及切实符合客户需求的安全解决方案及安全服务。

NSFOCUS

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com

绿盟科技官方微信