工业互联网安全框架

工业互联网产业联盟（AII）

2018 年 11 月

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

前　言

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》，标志着我国工业互联网顶层设计正式出台，对于我国工业互联网发展具有重要意义。安全是工业互联网发展的前提和保障，只有构建覆盖工业互联网各防护对象、全产业链的安全体系，完善满足工业需求的安全技术能力和相应管理机制，才能有效识别和抵御安全威胁，化解安全风险，进而确保工业互联网健康有序发展。

工业互联网安全框架是构建工业互联网安全保障体系的重要指南，是业界专家在工业互联网安全防护方面达成的共识，旨在为工业互联网相关企业应对日益增长的安全威胁、部署安全防护措施提供指导，提升工业互联网整体安全防护能力。

指导单位：工业和信息化部网络安全管理局

牵头编写单位：中国信息通信研究院

参与编写单位：北京奇虎科技有限公司、中国电子信息产业集团有限公司第六研究所、北京神州绿盟信息安全科技股份有限公司、中国移动通信集团公司、树根互联技术有限公司、华为技术有限公司、富士康科技集团、北京匡恩网络科技有限责任公司、中国科学院沈阳自动化研究所、中国电信集团有限公司、思科系统（中国）网络技术有限公司、浙江安恒信息技术有限公司、大唐高鸿数据网络技术股份有限公司、北京安点科技有限责任公司

编写组成员：魏亮、田慧蓉、杜霖、李艺、刘晓曼、陶耀东、李鸿彬、崔君荣、卢凯、赵云飞、吴子建、张峰、马洁、王雨晨、耿涛、黄晋斌、李江力、方宇、黄树强、文博武、章云嘉、叶鹏、赵军凯、邹小蔚、徐斌、王峥

目　录

工业互联网产业联盟

Alliance of Industrial Internet

一、 工业互联网安全概述

（一）工业互联网概念内涵

工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。工业互联网深刻变革传统工业的创新、生产、管理、服务方式，催生新技术、新模式、新业态、新产业，正成为繁荣数字经济的新基石、创新网络国际治理的新途径和统筹两个强国建设的新引擎。

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育。**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。

（二）工业互联网安全框架内容与范围

工业领域的安全一般分为三类，信息安全（Security）、功能安全（Functional Safety）和物理安全（Physical Safety）。传统工业控制系统安全最初多关注功能安全与物理安全，即防止工业安全相关系统或设备的功能失效，当失效或故障发生时，保证工业设备或系统仍能保持安全条件或进入到安全状态。近年来，随着工业控制系统信息化程度的不断加深，针对工业控制系统的信息安全问题不断凸显，业界对信息安全的重视程度逐步提高。

与传统的工控系统安全和互联网安全相比，工业互联网的安全挑战更为艰巨：一方面，工业互联网安全打破了以往相对明晰的责任边界，其范围、复杂度、风险度产生的影响要大得多，其中工业互联网平台安全、数据安全、联网智能设备安全等问题越发突出；另一方面，工业互联网安全工作需要从制度建设、国家能力、产业支持等更全局的视野来统筹安排，目前很多企业还没有意识到安全部署的必要性与紧迫性，安全管理与风险防范控制工作亟需加强。

因此，工业互联网安全框架需要统筹考虑信息安全、功能安全与物理安全，聚焦信息安全，主要解决工业互联网面

临的网络攻击等新型风险，并考虑其信息安全防护措施的部署可能对功能安全和物理安全带来的影响。由于物理安全相关防护措施较为通用，故在本框架中不作重要考虑，主要对工业互联网的信息安全与功能安全进行讨论。

二、 相关网络安全框架分析

（一）传统网络安全框架

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。

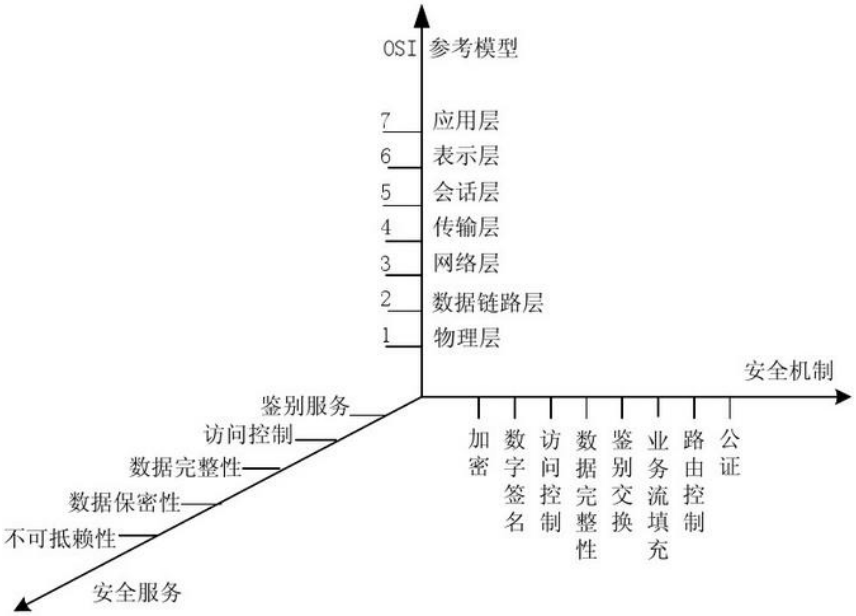

图 1 OSI 安全体系结构

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、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

P2DR 模型是一种基于闭环控制的动态安全模型，适用于需要长期持续安全防护的网络系统。从总体上来讲，该模型与 OSI 安全体系结构一样，都局限于从技术上考虑网络的安全问题，忽视了管理对于安全防护的重要性，在模型的具体实施过程中极有可能因安全策略执行的不当影响安全防护效果。

3、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。

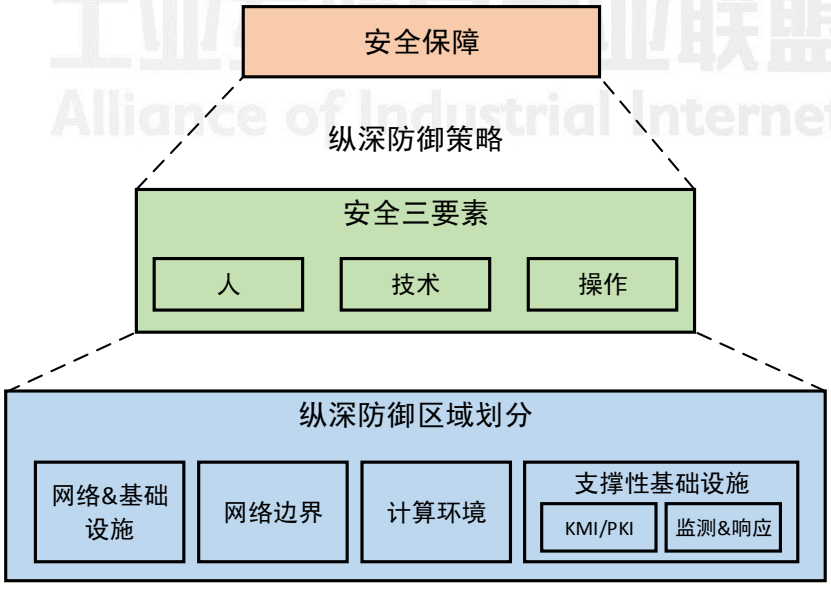

图 3 信息保障技术框架

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、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。

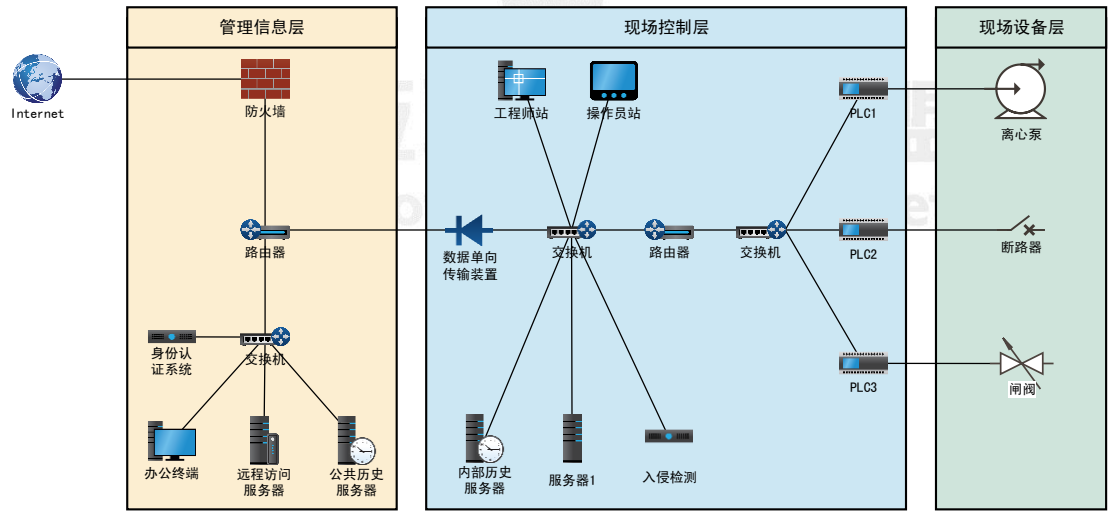

图 4 IEC62443 实施案例

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。

（二）工业互联网安全框架

1、美国工业互联网联盟（IIC）的 IISF

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。

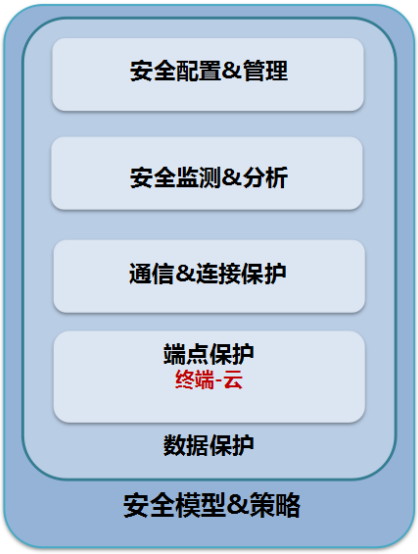

图 5 美国工业互联网安全实施框架

总的来看，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、德国工业 4.0 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。

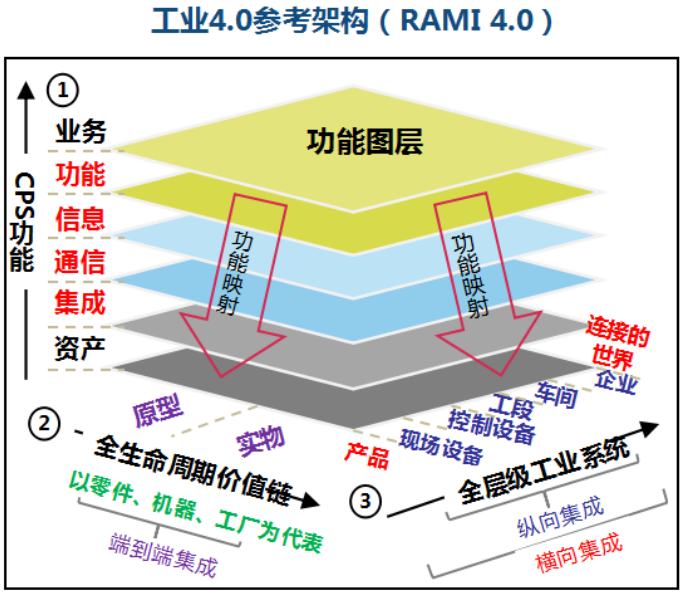

图 6 工业 4.0 参考架构（RAMI 4.0）

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。

（三）相关框架共性分析及经验借鉴

通过对以上相关网络安全框架的分析，总结出以下三方面的共性特征，在工业互联网安全框架的设计中值得思考并充分借鉴。

1、分类别部署安全防护措施

上述相关网络安全框架中大多都体现出分类别部署安

全防护措施的思想。例如在 OSI 安全体系结构中根据网络层次的不同部署相应的安全防护措施，IATF、IEC62443 通过划分不同的功能域来部署相应的安全防护措施，美国 IISF 与德国工业 4.0 框架中则根据资产类型的不同分别阐述其安全防护措施。工业互联网安全框架在设计时可根据防护对象的不同部署针对性的安全防护措施，更好地发挥安全防护措施的防护效果。

2.构建动态安全模型成为主流

P2DR 模型、美国 IISF 及德国工业 4.0 框架中均强调对安全风险进行持续的监测与响应，充分说明相对安全观已成为目前安全界的共识。为应对不断变化的安全风险，工业互联网安全框架的设计需将动态与持续性安全防护纳入其中。

3.技术手段与管理手段相结合

IATF、IEC62443、美国 IISF 及德国工业 4.0 框架等在设计过程中均强调了技术手段与管理手段相结合的重要性。设计工业互联网安全框架时，需充分借鉴技管相结合的思路，双重保障，从而更好地帮助工业互联网相关企业提升安全防护能力。

三、 工业互联网安全框架设计

（一）设计思路

本工业互联网安全框架是在充分借鉴传统网络安全框架和国外相关工业互联网安全框架的基础上，并结合我国工业互联网的特点提出的，旨在指导工业互联网相关企业开展安全防护体系建设，提升安全防护能力。对于工业互联网安全框架的构建，可以从以下三方面进行阐述:

第一，明确安全防护对象是前提。安全防护对象的确定是一个根本问题，是明确工业互联网安全防护工作范畴的基础，并为防护工作的实施指明方向。在传统网络安全框架与国外相关工业互联网安全框架中，都明确界定了防护对象。2016 年 8 月工业互联网产业联盟（AII）发布的《工业互联网体系架构（版本 1.0）》中的安全体系部分也从防护对象角度提出了工业互联网安全的五大重点方向，即设备安全、控制安全、网络安全、应用安全和数据安全。因此本框架充分借鉴这一思路，将设备、控制、网络、应用、数据作为工业互联网安全防护的研究对象。

第二，部署安全防护措施是关键。工业互联网安全框架的实施离不开安全防护措施的部署。在诸多传统网络安全框架中都将安全防护措施作为框架的重要组成部分。OSI 安全框架中阐述的安全服务与安全机制即是针对不同防护对象

部署了相应的防护措施。在 P2DR 等安全模型中引入了动态安全的理念，除了部署静态的安全防护措施外，还增加了监测响应、处置恢复等环节，形成了动态、闭环的安全防护部署机制。设计工业互联网安全框架的过程中，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。

第三，落实安全防护管理是重要保障。在网络安全防护领域有“三分技术、七分管理”的传统。传统网络安全框架 IATF、IEC62443 等均强调了管理对于网络安全防护的重要性。国外工业互联网安全相关框架也将管理与技术相结合，强调技术与管理并重。设计工业互联网安全框架的过程中，需要将技术与管理有效结合，构建科学完备的安全防护管理体系，指导工业互联网相关企业提升安全防护管理水平。

综上所述，工业互联网安全框架的构建需要包含防护对象、防护措施以及防护管理三个方面，从三个不同的视角指导企业开展工业互联网安全防护工作。

（二）安全框架

工业互联网安全框架从防护对象、防护措施及防护管理三个视角构建。针对不同的防护对象部署相应的安全防护措施，根据实时监测结果发现网络中存在的或即将发生的安全问题并及时做出响应。同时加强防护管理，明确基于安全目

标的可持续改进的管理方针，从而保障工业互联网的安全。工业互联网安全框架如图 7 所示。

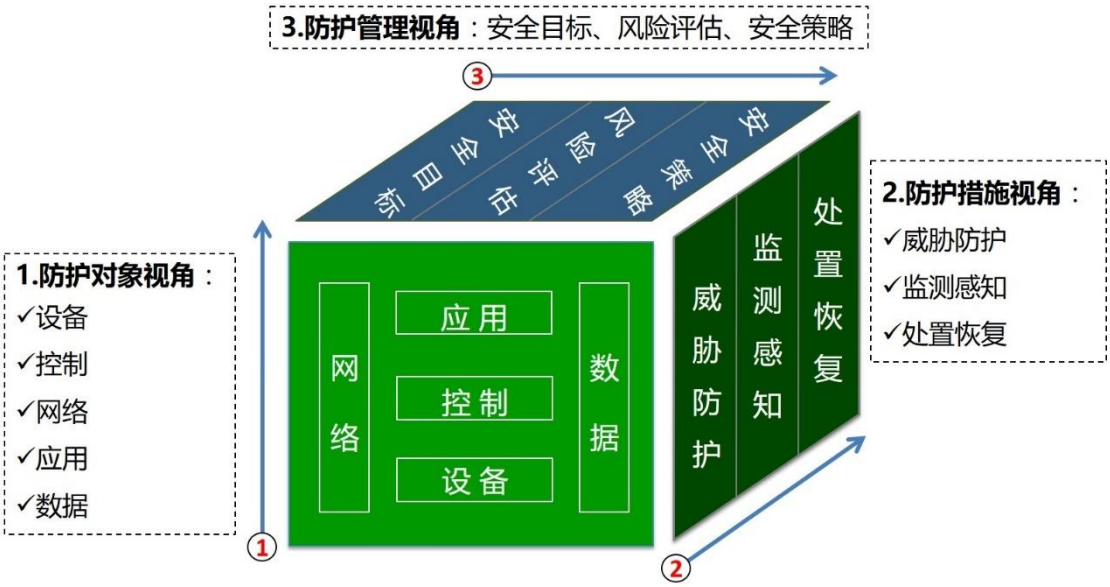

图 7 工业互联网安全框架

其中，防护对象视角涵盖设备、控制、网络、应用和数据五大安全重点；防护措施视角包括威胁防护、监测感知和处置恢复三大环节，威胁防护环节针对五大防护对象部署主被动安全防护措施，监测感知和处置恢复环节通过信息共享、监测预警、应急响应等一系列安全措施、机制的部署增强动态安全防护能力；防护管理视角根据工业互联网安全目标对其面临的安全风险进行安全评估，并选择适当的安全策略作为指导，实现防护措施的有效部署。

工业互联网安全框架的三个防护视角之间相对独立，但彼此之间又相互关联。从防护对象视角来看，安全框架中的每个防护对象，都需要采用一系列合理的防护措施并依据完备的防护管理流程对其进行安全防护；从防护措施视角来看，

每一类防护措施都有其适用的防护对象，并在具体防护管理流程指导下发挥作用；从防护管理视角来看，防护管理流程的实现离不开对防护对象的界定，并需要各类防护措施的有机结合使其能够顺利运转。工业互联网安全框架的三个防护视角相辅相成、互为补充，形成一个完整、动态、持续的防护体系。

本工业互联网安全框架与美国 IIC 的 IISF 虽呈现视角有不同，但设计思路有共通之处，在防护内容上也具有一定的对应关系。图 8 展示了工业互联网安全框架与美国 IIC 的 IISF 之间的映射关系。其中，防护对象视角中的五大防护对象对应了美国 IIC 的 IISF 中的端点保护、通信&连接保护以及数据保护中所界定的防护对象；防护措施视角中的三类安全技术手段与美国 IIC 的 IISF 中的端点保护、通信&连接保护、数据保护、安全监测&分析以及安全配置管理中提出的防护技术手段相对应；防护管理视角中的内容与美国 IIC 的 IISF 中的安全模型&策略具有对应关系。由此可以看出，二者均从指导企业开展工业互联网安全工作出发，强调技管结合、动静互补，持续提升企业的工业互联网安全防护能力。工业互联网安全框架的提出，有助于深化我国工业互联网产业联盟与其他国际组织的合作与交流，对于我国企业与国际接轨、开拓海外市场也具有积极意义。

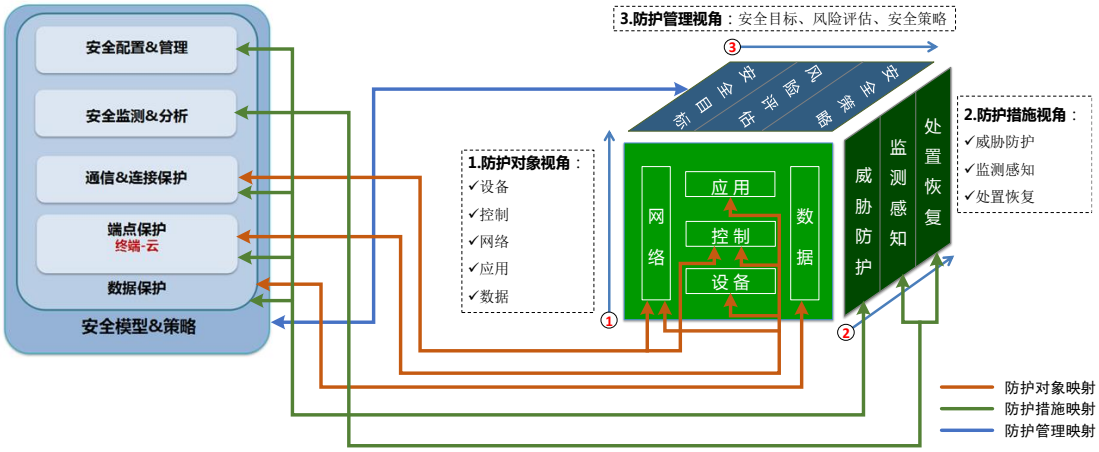

图 8 工业互联网安全框架与美国 IIC 的 IISF 的映射关系

（三）防护对象视角

防护对象视角主要包括设备、控制、网络、应用、数据五大防护对象，如图 9 所示。具体内容包括：

1、设备安全：包括工厂内单点智能器件、成套智能终端等智能设备的安全，以及智能产品的安全，具体涉及操作系统/应用软件安全与硬件安全两方面。

2、控制安全：包括控制协议安全、控制软件安全以及控制功能安全。

3、网络安全：包括承载工业智能生产和应用的工厂内部网络、外部网络及标识解析系统等的安全。

4、应用安全：包括工业互联网平台安全与工业应用程序安全。

5、数据安全：包括涉及采集、传输、存储、处理等各个环节的数据以及用户信息的安全。

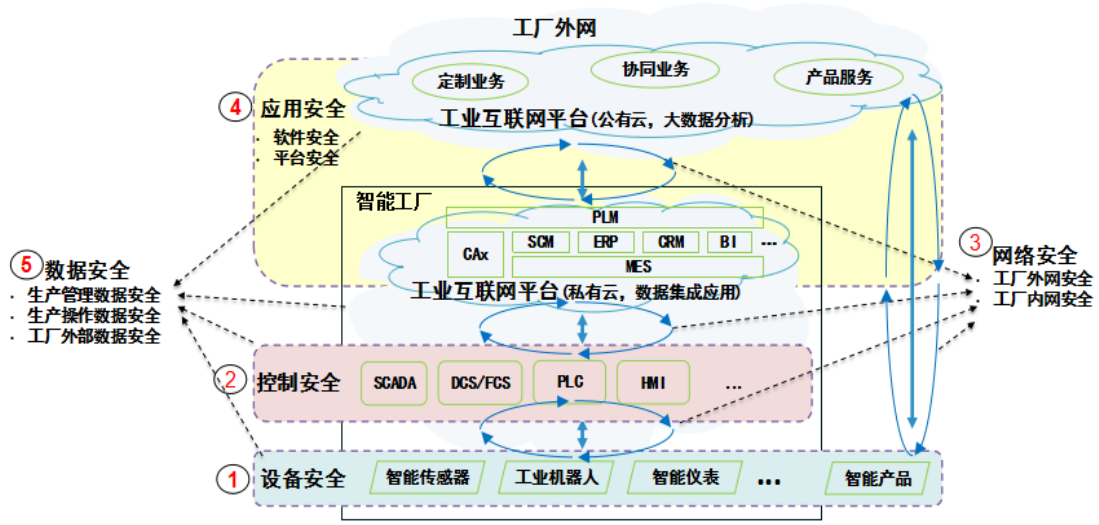

图 9 防护对象视角

（四）防护措施视角

为帮助相关企业应对工业互联网所面临的各种挑战，防护措施视角从生命周期、防御递进角度明确安全措施，实现动态、高效的防御和响应。防护措施视角主要包括威胁防护、监测感知和处置恢复三大环节，如图 10 所示。

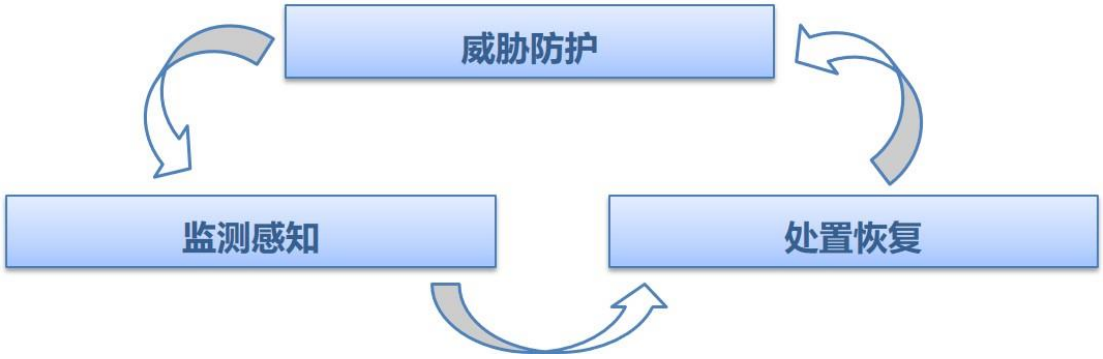

图 10 防护措施视角

1、威胁防护：针对五大防护对象，部署主被动防护措施，阻止外部入侵，构建安全运行环境，消减潜在安全风险。

2、监测感知：部署相应的监测措施，实时感知内部、外部的安全风险。

3、处置恢复：建立响应恢复机制，及时应对安全威胁，并及时优化防护措施，形成闭环防御。

（五）防护管理视角

防护管理视角的设立，旨在指导企业构建持续改进的安全防护管理方针，在明确防护对象及其所需要达到的安全目标后，对于其可能面临的安全风险进行评估，找出当前与安全目标之间存在的差距，制定相应的安全防护策略，提升安全防护能力，并在此过程中不断对管理流程进行改进。防护措施视角的内容如图 11 所示。

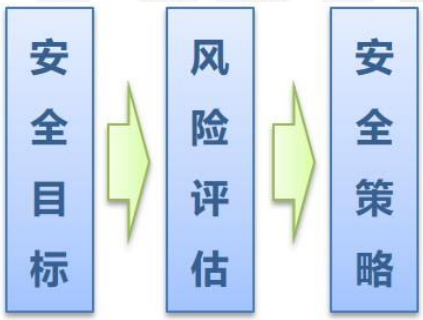

图 11 防护措施视角

1、安全目标

为确保工业互联网的正常运转和安全可信，应对工业互联网设定合理的安全目标，并根据相应的安全目标进行风险评估和安全策略的选择实施。工业互联网安全目标并非是单一的，需要结合工业互联网不同的安全需求进行明确。工业互联网安全包括保密性、完整性、可用性、可靠性、弹性和

隐私安全六大目标，这些目标相互补充，共同构成了保障工业互联网安全的关键特性。

（1）保密性：确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

（2）完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。

（3）可用性：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

（4）可靠性：确保工业互联网系统在其寿命区间内以及在正常运行条件下能够正确执行指定功能。

（5）弹性：确保工业互联网系统在受到攻击或破坏后恢复正常功能。

（6）隐私安全：确保工业互联网系统内用户的隐私安全。

2、风险评估

为管控风险，必须定期对工业互联网系统的各安全要素进行风险评估。对应工业互联网整体安全目标，分析整个工业互联网系统的资产、脆弱性和威胁，评估安全隐患导致安全事件的可能性及影响，结合资产价值，明确风险的处置措施，包括预防、转移、接受、补偿、分散等，确保在工业互

联网数据私密性、数据传输安全性、设备接入安全性、平台访问控制安全性、平台攻击防范安全性等方面提供可信服务，并最终形成风险评估报告。

3、安全策略

工业互联网安全防护的总体策略，是要构建一个能覆盖安全业务全生命周期的，以安全事件为核心，实现对安全事件的“预警、检测、响应”动态防御体系。能够在攻击发生前进行有效的预警和防护，在攻击中进行有效的攻击检测，在攻击后能快速定位故障，进行有效响应，避免实质损失的发生。

安全策略中描述了工业互联网总体的安全考虑，并定义了保证工业互联网日常正常运行的指导方针及安全模型。通过结合安全目标以及风险评估结果，明确当前工业互联网各方面的安全策略，包括对设备、控制、网络、应用、数据等防护对象应采取的防护措施，以及监测响应及处置恢复措施等。同时，为打造持续安全的工业互联网，面对不断出现的新的威胁，需不断完善安全策略。

四、 工业互联网安全防护措施实施

工业互联网安全框架在实施过程中的重点是针对防护对象采取行之有效的防护措施。为此，本章针对工业互联网安全的五大防护对象面临的安全威胁，分别介绍其可采取的

安全防护措施，并对监测感知与处置恢复两类贯穿工业互联网全系统的防护措施进行介绍，为企业部署工业互联网安全防护工作提供参考。

（一）设备安全

工业互联网的发展使得现场设备由机械化向高度智能化发生转变，并产生了嵌入式操作系统+微处理器+应用软件的新模式，这就使得未来海量智能设备可能会直接暴露在网络攻击之下，面临攻击范围扩大、扩散速度增加、漏洞影响扩大等威胁。

工业互联网设备安全指工厂内单点智能器件以及成套智能终端等智能设备的安全，具体应分别从操作系统/应用软件安全与硬件安全两方面出发部署安全防护措施，可采用的安全机制包括固件安全增强、恶意软件防护、设备身份鉴别与访问控制、漏洞修复等。

1、操作系统/应用软件安全

（1）固件安全增强

工业互联网设备供应商需要采取措施对设备固件进行安全增强，阻止恶意代码传播与运行。工业互联网设备供应商可从操作系统内核、协议栈等方面进行安全增强，并力争实现对于设备固件的自主可控。

（2）漏洞修复加固

设备操作系统与应用软件中出现的漏洞对于设备来说是最直接也是最致命的威胁。设备供应商应对工业现场中常见的设备与装置进行漏洞扫描与挖掘，发现操作系统与应用软件中存在的安全漏洞，并及时对其进行修复。

（3）补丁升级管理

工业互联网企业应密切关注重大工业互联网现场设备的安全漏洞及补丁发布，及时采取补丁升级措施，并在补丁安装前对补丁进行严格的安全评估和测试验证。

2、硬件安全

（1）硬件安全增强

对于接入工业互联网的现场设备，应支持基于硬件特征的唯一标识符，为包括工业互联网平台在内的上层应用提供基于硬件标识的身份鉴别与访问控制能力，确保只有合法的设备能够接入工业互联网并根据既定的访问控制规则向其他设备或上层应用发送或读取数据。此外，应支持将硬件级部件（安全芯片或安全固件）作为系统信任根，为现场设备的安全启动以及数据传输机密性和完整性保护提供支持。

（2）运维管控

工业互联网企业应在工业现场网络重要控制系统（如机组主控 DCS 系统）的工程师站、操作员站和历史站部署运维管控系统，实现对外部存储器（如 U 盘）、键盘和鼠标等使用 USB 接口的硬件设备的识别，对外部存储器的使用进行

严格控制。同时，注意部署的运维管控系统不能影响生产控制区各系统的正常运行。

（二）控制安全

工业互联网使得生产控制由分层、封闭、局部逐步向扁平、开放、全局方向发展。其中在控制环境方面表现为信息技术（IT）与操作技术（OT）融合，控制网络由封闭走向开放；在控制布局方面表现为控制范围从局部扩展至全局，并伴随着控制监测上移与实时控制下移。上述变化改变了传统生产控制过程封闭、可信的特点，造成安全事件危害范围扩大、危害程度加深、信息安全与功能安全问题交织等后果。

对于工业互联网控制安全防护，主要从控制协议安全、控制软件安全及控制功能安全三个方面考虑，可采用的安全机制包括协议安全加固、软件安全加固、恶意软件防护、补丁升级、漏洞修复、安全监测审计等。

1、控制协议安全

（1）身份认证

为了确保控制系统执行的控制命令来自合法用户，必须对使用系统的用户进行身份认证，未经认证的用户所发出的控制命令不被执行。在控制协议通信过程中，一定要加入认证方面的约束，避免攻击者通过截获报文获取合法地址建立会话，影响控制过程安全。

（2）访问控制

不同的操作类型需要不同权限的认证用户来操作，如果没有基于角色的访问机制，没有对用户权限进行划分，会导致任意用户可以执行任意功能。

（3）传输加密

在控制协议设计时，应根据具体情况，采用适当的加密措施，保证通信双方的信息不被第三方非法获取。

（4）健壮性测试

控制协议在应用到工业现场之前应通过健壮性测试工具的测试，测试内容可包括风暴测试、饱和测试、语法测试、模糊测试等。

2、控制软件安全

（1）软件防篡改

工业互联网中的控制软件可归纳为数据采集软件、组态软件、过程监督与控制软件、单元监控软件、过程仿真软件、过程优化软件、专家系统、人工智能软件等类型。软件防篡改是保障控制软件安全的重要环节，具体措施包括以下几种:

①控制软件在投入使用前应进行代码测试，以检查软件中的公共缺陷。

②采用完整性校验措施对控制软件进行校验，及时发现软件中存在的篡改情况。

③对控制软件中的部分代码进行加密。

④做好控制软件和组态程序的备份工作。

（2）认证授权

控制软件的应用要根据使用对象的不同设置不同的权限，以最小的权限完成各自的任务。

（3）恶意软件防护

对于控制软件应采取恶意代码检测、预防和恢复的控制措施。控制软件恶意代码防护具体措施包括:

①在控制软件上安装恶意代码防护软件或独立部署恶意代码防护设备，并及时更新恶意代码软件和修复软件版本和恶意代码库，更新前应进行安全性和兼容性测试。防护软件包括病毒防护、入侵检测、入侵防御等具有病毒查杀和阻止入侵行为的软件；防护设备包括防火墙、网闸、入侵检测系统、入侵防御系统等具有防护功能的设备。应注意防止在实施维护和紧急规程期间引入恶意代码。

②建议控制软件的主要生产厂商采用特定的防病毒工具。在某些情况下，控制软件的供应商需要对其产品线的防病毒工具版本进行回归测试，并提供相关的安装和配置文档。

③采用具有白名单机制的产品，构建可信环境，抵御零日漏洞和有针对性地攻击。

（4）补丁升级更新

控制软件的变更和升级需要在测试系统中经过仔细的测试，并制定详细的回退计划。对重要的补丁需尽快测试和

部署。对于服务包和一般补丁，仅对必要的补丁进行测试和部署。

（5）漏洞修复加固

控制软件的供应商应及时对控制软件中出现的漏洞进行修复或提供其他替代解决方案，如关闭可能被利用的端口等。

（6）协议过滤

采用工业防火墙对协议进行深度过滤，对控制软件与设备间的通信内容进行实时跟踪，同时确保协议过滤不得影响通信性能。

（7）安全监测审计

通过对工业互联网中的控制软件进行安全监测审计可及时发现网络安全事件，避免发生安全事故，并可以为安全事故的调查提供详实的数据支持。目前许多安全产品厂商已推出了各自的监测审计平台，可实现协议深度解析、攻击异常检测、无流量异常检测、重要操作行为审计、告警日志审计等功能。

3、控制功能安全

要考虑功能安全和信息安全的协调能力，使得信息安全不影响功能安全，功能安全在信息安全的防护下更好地执行安全功能。现阶段功能安全具体措施主要包括:

（1）确定可能的危险源、危险状况和伤害事件，获取已

确定危险的信息（如持续时间、强度、毒性、暴露限度、机械力、爆炸条件、反应性、易燃性、脆弱性、信息丢失等）。

（2）确定控制软件与其他设备或软件（已安装的或将被安装的）以及与其他智能化系统（已安装的或将被安装的）之间相互作用所产生的危险状况和伤害事件，确定引发事故的事件类型（如元器件失效、程序故障、人为错误，以及能导致危险事件发生的相关失效机制）。

（3）结合典型生产工艺、加工制造过程、质量管控等方面的特征，分析安全影响。

（4）考虑自动化、一体化、信息化可能导致的安全失控状态，确定需要采用的监测、预警或报警机制、故障诊断与恢复机制、数据收集与记录机制等。

（5）明确操作人员在对智能化系统执行操作过程中可能产生的合理可预见的误用以及智能化系统对于人员恶意攻击操作的防护能力。

（6）智能化装备和智能化系统对于外界实物、电、磁场、辐射、火灾、地震等情况的抵抗或切断能力，以及在发生异常扰动或中断时的检测和处理能力。

（三）网络安全

工业互联网的发展使得工厂内部网络呈现出 IP 化、无线化、组网方式灵活化与全局化的特点，工厂外网呈现出信息

网络与控制网络逐渐融合、企业专网与互联网逐渐融合以及产品服务日益互联网化的特点。这就造成传统互联网中的网络安全问题开始向工业互联网蔓延，具体表现为以下几个方面：工业互联协议由专有协议向以太网/IP 协议转变，导致攻击门槛极大降低；现有一些 10M / 100M 工业以太网交换机（通常是非管理型交换机）缺乏抵御日益严重的 DDoS 攻击的能力；工厂网络互联、生产、运营逐渐由静态转变为动态，安全策略面临严峻挑战等。此外，随着工厂业务的拓展和新技术的不断应用，今后还会面临 5G/SDN 等新技术引入、工厂内外网互联互通进一步深化等带来的安全风险。

工业互联网网络安全防护应面向工厂内部网络、外部网络及标识解析系统等方面，具体包括网络结构优化、边界安全防护、接入认证、通信内容防护、通信设备防护、安全监测审计等多种防护措施，构筑全面高效的网络安全防护体系。

（1）优化网络结构设计

在网络规划阶段，需设计合理的网络结构。一方面通过在关键网络节点和标识解析节点采用双机热备和负载均衡等技术，应对业务高峰时期突发的大数据流量和意外故障引发的业务连续性问题，确保网络长期稳定可靠运行。另一方面通过合理的网络结构和设置提高网络的灵活性和可扩展性，为后续网络扩容做好准备。

（2）网络边界安全

根据工业互联网中网络设备和业务系统的重要程度将整个网络划分成不同的安全域，形成纵深防御体系。安全域是一个逻辑区域，同一安全域中的设备资产具有相同或相近的安全属性，如安全级别、安全威胁、安全脆弱性等，同一安全域内的系统相互信任。在安全域之间采用网络边界控制设备，以逻辑串接的方式进行部署，对安全域边界进行监视，识别边界上的入侵行为并进行有效阻断。

（3）网络接入认证

接入网络的设备与标识解析节点应该具有唯一性标识，网络应对接入的设备与标识解析节点进行身份认证，保证合法接入和合法连接，对非法设备与标识解析节点的接入行为进行阻断与告警，形成网络可信接入机制。网络接入认证可采用基于数字证书的身份认证等机制来实现。

（4）通信和传输保护

通信和传输保护是指采用相关技术手段来保证通信过程中的机密性、完整性和有效性，防止数据在网络传输过程中被窃取或篡改，并保证合法用户对信息和资源的有效使用。同时，在标识解析体系的建设过程中，需要对解析节点中存储以及在解析过程中传输的数据进行安全保护。具体包括：

①通过加密等方式保证非法窃取的网络传输数据无法被非法用户识别和提取有效信息，确保数据加密不会对任何其他工业互联网系统的性能产生负面影响。在标识解析体系

的各类解析节点与标识查询节点之间建立解析数据安全传输通道，采用国密局批准使用的加密算法及加密设备，为标识解析请求及解析结果的传输提供机密性与完整性保障。

②网络传输的数据采取校验机制，确保被篡改的信息能够被接收方有效鉴别。

③应确保接收方能够接收到网络数据，并且能够被合法用户正常使用。

（5）网络设备安全防护

为了提高网络设备与标识解析节点自身的安全性，保障其正常运行，网络设备与标识解析节点需要采取一系列安全防护措施，主要包括:

①对登录网络设备与标识解析节点进行运维的用户进行身份鉴别，并确保身份鉴别信息不易被破解与冒用;

②对远程登录网络设备与标识解析节点的源地址进行限制;

③对网络设备与标识解析节点的登录过程采取完备的登录失败处理措施;

④启用安全的登录方式（如 SSH 或 HTTPS 等）。

（6）安全监测审计

网络安全监测指通过漏洞扫描工具等方式探测网络设备与标识解析节点的漏洞情况，并及时提供预警信息。网络安全审计指通过镜像或代理等方式分析网络与标识解析系

统中的流量，并记录网络与标识解析系统中的系统活动和用户活动等各类操作行为以及设备运行信息，发现系统中现有的和潜在的安全威胁，实时分析网络与标识解析系统中发生的安全事件并告警。同时记录内部人员的错误操作和越权操作，并进行及时告警，减少内部非恶意操作导致的安全隐患。

（四）应用安全

工业互联网应用主要包括工业互联网平台与工业应用程序两大类，其范围覆盖智能化生产、网络化协同、个性化定制、服务化延伸等方面。目前工业互联网平台面临的安全风险主要包括数据泄露、篡改、丢失、权限控制异常、系统漏洞利用、账户劫持、设备接入安全等。对工业应用程序而言，最大的风险来自安全漏洞，包括开发过程中编码不符合安全规范而导致的软件本身的漏洞以及由于使用不安全的第三方库而出现的漏洞等。

相应地，工业互联网应用安全也应从工业互联网平台安全与工业应用程序安全两方面进行防护。对于工业互联网平台，可采取的安全措施包括安全审计、认证授权、DDOS 攻击防护等。对于工业应用程序，建议采用全生命周期的安全防护，在应用程序的开发过程中进行代码审计并对开发人员进行培训，以减少漏洞的引入；对运行中的应用程序定期进行漏洞排查，对应用程序的内部流程进行审核和测试，并对公

开漏洞和后门并加以修补；对应用程序的行为进行实时监测，以发现可疑行为并进行阻止，从而降低未公开漏洞带来的危害。

1、平台安全

（1）安全审计

安全审计主要是指对平台中与安全有关的活动的相关信息进行识别、记录、存储和分析。平台建设过程中应考虑具备一定的安全审计功能，将平台与安全有关的信息进行有效识别、充分记录、长时间的存储和自动分析。能对平台的安全状况做到持续、动态、实时的有依据的安全审计，并向用户提供安全审计的标准和结果。

（2）认证授权

工业互联网平台用户分属不同企业，需要采取严格的认证授权机制保证不同用户能够访问不同的数据资产。同时，认证授权需要采用更加灵活的方式，确保用户间可以通过多种方式将数据资产分模块分享给不同的合作伙伴。

（3）DDoS 防御

部署 DDoS 防御系统，在遭受 DDoS 攻击时，保证平台用户的正常使用。平台抗 DDoS 的能力应在用户协议中作为产品技术参数的一部分明确指出。

（4）安全隔离

平台不同用户之间应当采取必要的措施实现充分隔离，

防止蠕虫病毒等安全威胁通过平台向不同用户扩散。平台不同应用之间也要采用严格的隔离措施，防止单个应用的漏洞影响其他应用甚至整个平台的安全。

（5）安全监测

应对平台实施集中、实时的安全监测，监测内容包括各种物理和虚拟资源的运行状态等。通过对系统运行参数（如网络流量、主机资源和存储等）以及各类日志进行分析，确保工业互联网平台提供商可执行故障管理、性能管理和自动检修管理，从而实现平台运行状态的实时监测。

（6）补丁升级

工业互联网平台搭建在众多底层软件和组件基础之上。由于工业生产对于运行连续性的要求较高，中断平台运行进行补丁升级的代价较大。因此平台在设计之初就应当充分考虑如何对平台进行补丁升级的问题。

（7）虚拟化安全

虚拟化是边缘计算和云计算的基础，为避免虚拟化出现安全问题影响上层平台的安全，在平台的安全防护中要充分考虑虚拟化安全。虚拟化安全的核心是实现不同层次及不同用户的有效隔离，其安全增强可以通过采用虚拟化加固等防护措施来实现。

2、工业应用程序安全

（1）代码审计

代码审计指检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。工业应用程序在开发过程中应该进行必要的代码审计，发现代码中存在的安全缺陷并给出相应的修补建议。

（2）人员培训

企业应对工业应用程序开发者进行软件源代码安全培训，包括：了解应用程序安全开发生命周期（SDL）的每个环节，如何对应用程序进行安全架构设计，具备所使用编程语言的安全编码常识，了解常见源代码安全漏洞的产生机理、导致后果及防范措施，熟悉安全开发标准，指导开发人员进行安全开发，减少开发者引入的漏洞和缺陷等，从而提高工业应用程序安全水平。

（3）漏洞发现

漏洞发现是指基于漏洞数据库，通过扫描等手段对指定工业应用程序的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。在应用程序上线前和运行过程中，要定期对其进行漏洞发现，及时发现漏洞并采取补救措施。

（4）审核测试

对工业应用程序进行审核测试是为了发现功能和逻辑上的问题。在上线前对其进行必要的审核测试，有效避免信息泄露、资源浪费或其他影响应用程序可用性的安全隐患。

（5）行为监测和异常阻止

对工业应用程序进行实时的行为监测，通过静态行为规则匹配或者机器学习的方法，发现异常行为，发出警告或者阻止高危行为，从而降低影响。

（五）数据安全

工业互联网相关的数据按照其属性或特征，可以分为四大类：设备数据、业务系统数据、知识库数据、用户个人数据。根据数据敏感程度的不同，可将工业互联网数据分为一般数据、重要数据和敏感数据三种。工业互联网数据涉及数据采集、传输、存储、处理等各个环节。随着工厂数据由少量、单一、单向向大量、多维、双向转变，工业互联网数据体量不断增大、种类不断增多、结构日趋复杂，并出现数据在工厂内部与外部网络之间的双向流动共享。由此带来的安全风险主要包括数据泄露、非授权分析、用户个人信息泄露等。

对于工业互联网的数据安全防护，应采取明示用途、数据加密、访问控制、业务隔离、接入认证、数据脱敏等多种防护措施，覆盖包括数据收集、传输、存储、处理等在内的全生命周期的各个环节。

1.数据收集

工业互联网平台应遵循合法、正当、必要的原则收集与使用数据及用户信息，公开数据收集和使用的规则，向用户

明示收集使用数据的目的、方式和范围，经过用户的明确授权同意并签署相关协议后才能收集相关数据。授权协议必须遵循用户意愿，不得以拒绝提供服务等形式强迫用户同意数据采集协议。

另外，工业互联网平台不得收集与其提供的服务无关的数据及用户信息，不得违反法律、行政法规的规定和双方约定收集、使用数据及用户信息，并应当依照法律、行政法规的规定和与用户的约定处理其保存的数据及个人信息。

2.数据传输

为防止数据在传输过程中被窃听而泄露，工业互联网服务提供商应根据不同的数据类型以及业务部署情况，采用有效手段确保数据传输安全。例如通过 SSL 保证网络传输数据信息的机密性、完整性与可用性，实现对工业现场设备与工业互联网平台之间、工业互联网平台中虚拟机之间、虚拟机与存储资源之间以及主机与网络设备之间的数据安全传输，并为平台的维护管理提供数据加密通道，保障维护管理过程的数据传输安全。

3.数据存储

（1）访问控制

数据访问控制需要保证不同安全域之间的数据不可直接访问，避免存储节点的非授权接入，同时避免对虚拟化环境数据的非授权访问。

①存储业务的隔离

借助交换机，将数据根据访问逻辑划分到不同的区域内，使得不同区域中的设备相互间不能直接访问，从而实现网络中设备之间的相互隔离。

②存储节点接入认证

对于存储节点的接入认证可通过成熟的标准技术，包括 iSCSI 协议本身的资源隔离、CHAP（Challenge Handshake Authentication Protocol）等，也可通过在网络层面划分 VLAN 或设置访问控制列表等来实现。

③虚拟化环境数据访问控制

在虚拟化系统上对每个卷定义不同的访问策略，以保障没有访问该卷权限的用户不能访问，各个卷之间互相隔离。

（2）存储加密

工业互联网平台运营商可根据数据敏感度采用分等级的加密存储措施（如不加密、部分加密、完全加密等）。建议平台运营商按照国家密码管理有关规定使用和管理密码设施，并按规定生成、使用和管理密钥。同时针对数据在工业互联网平台之外加密之后再传输到工业互联网平台中存储的场景，应确保工业互联网平台运营商或任何第三方无法对客户的数据进行解密。

（3）备份和恢复

用户数据作为用户托管在工业互联网服务提供商的数

据资产，服务提供商有妥善保管的义务。应当采取技术措施和其他必要措施，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

工业互联网服务提供商应当根据用户业务需求、与用户签订的服务协议制定必要的数据备份策略，定期对数据进行备份。当发生数据丢失事故时能及时恢复一定时间前备份的数据，从而降低用户的损失。

4.数据处理

（1）使用授权

数据处理过程中，工业互联网服务提供商要严格按照法律法规以及在与用户约定的范围内处理相关数据，不得擅自扩大数据使用范围，使用中要采取必要的措施防止用户数据泄露。如果处理过程中发生大规模用户数据泄露的安全事件，应当及时告知用户和上级主管部门，对于造成用户经济损失的应当给予赔偿。

（2）数据销毁

在资源重新分配给新的租户之前，必须对存储空间中的数据进行彻底擦除，防止被非法恶意恢复。应根据不同的数据类型以及业务部署情况，选择采用如下操作方式:

①在逻辑卷回收时对逻辑卷的所有 bit 位进行清零，并利用“0”或随机数进行多次覆写;

②在非高安全场景，系统默认将逻辑卷的关键信息（如元数据、索引项、卷前 10M 等）进行清零；在涉及敏感数据的高安全场景，当数据中心的物理硬盘需要更换时系统管理员可采用消磁或物理粉碎等措施保证数据彻底清除。

（3）数据脱敏

当工业互联网平台中存储的工业互联网数据与用户个人信息需要从平台中输出或与第三方应用进行共享时，应当在输出或共享前对这些数据进行脱敏处理。脱敏应采取不可恢复的手段，避免数据分析方通过其他手段对敏感数据复原。此外数据脱敏后不应影响业务连续性，避免对系统性能造成较大影响。

（六）监测感知

监测感知是指部署相应的监测措施，主动发现来自系统内外部的安全风险，具体措施包括数据采集、收集汇聚、特征提取、关联分析、状态感知等。

（1）数据采集

数据采集指对工业现场网络及工业互联网平台中各类数据进行采集，为网络异常分析、设备预测性维护等提供数据来源。

（2）收集汇聚

对于数据的收集汇聚主要分为两个方面。一是对

SCADA、MES、ERP 等工业控制系统及应用系统所产生的关键工业互联网数据进行汇聚，包括产品全生命周期的各类数据的同步采集、管理、存储及查询，为后续过程提供数据来源。二是对全网流量进行监听，并将监听过程中采集到的数据进行汇聚。

（3）特征提取

特征提取是指对数据特征进行提取、筛选、分类、优先级排序、可读等处理，从而实现从数据到信息的转化过程，该过程主要是针对单个设备或单个网络的纵向数据分析。信息主要包括内容和情景两方面，内容指工业互联网中的设备信号处理结果、监控传输特性、性能曲线、健康状况、报警信息、DNC 及 SCADA 网络流量等;情景指设备的运行工况、维护保养记录、人员操作指令、人员访问状态、生产任务目标、行业销售机理等。

（4）关联分析

关联分析基于大数据进行横向大数据分析和多维分析，通过将运行机理、运行环境、操作内容、外部威胁情报等有机结合，利用群体经验预测单个设备的安全情况，或根据历史状况和当前状态的差异进行关联分析，进而发现网络及系统的异常状态。

（5）状态感知

状态感知基于关联分析过程，实现对工业互联网相关企

业网络运行规律、异常情况、安全目标、安全态势、业务背景等的监测感知，确定安全基线，结合大数据分析等相关技术，发现潜在安全威胁、预测黑客攻击行为。

（七）处置恢复

处置恢复机制是确保落实工业互联网信息安全管理，支撑工业互联网系统与服务持续运行的保障。通过处置恢复机制，在风险发生时灾备恢复组织能根据预案及时采取措施进行应对，及时恢复现场设备、工业控制系统、网络、工业互联网平台、工业应用程序等的正常运行，防止重要数据丢失，并通过数据收集与分析机制，及时更新优化防护措施，形成持续改进的防御闭环。处置恢复机制主要包括响应决策、备份恢复、分析评估等。

1.响应决策

对于工业互联网灾难恢复过程中的决策与响应，需预先制定相应的处置策略，针对不同风险等级制定相应预案措施。处置恢复工作需要在处置恢复组织的领导下进行，通过实时监测工业互联网系统各类数据，在突发灾难时通过相应机制进行应对。

（1）处置恢复组织架构

①处置恢复规划领导组:是实施处置恢复规划工作的组织领导机构，应由单位高层领导担任组长，领导和决策处置

恢复规划中的重大事宜。

②处置恢复现场实施组:负责对处置恢复工作进行需求分析、规划并确立处置恢复策略，制订处置恢复预案。

③处置恢复日常运行组:负责灾难备份中心日常管理,处置恢复预案的教育、培训、演练、维护和管理，突发事件发生时的损失控制和损害评估，灾难发生后恢复技术支持及外部协作等。

（2）灾难风险分析与管理

工业互联网较传统信息系统架构更为复杂，处置恢复组织应根据工业互联网系统架构进行风险识别，并对风险按照类别与等级、风险影响程度、风险发生几率和风险时长等因素进行评估，依照风险处置优先级别制定防范措施与解决预案，将实际情况与之进行匹配，并进行适当的调整以满足实施的有效性。

（3）灾难数据监测

工业互联网系统架构包括多个层级与数据接口，针对可能发生的风险所在的层级，应采取相应的措施降低灾难发生的几率。处置恢复日常运行组可以通过对设备层、网络层、控制层、应用层、数据层等部署监测机制，对工业互联网系统运行中的数据状态进行定期监测，感知潜在的安全风险与系统异常，由处置恢复实施组通过恢复策略进行相应处置。

（4）灾难恢复决策

应建立灾难恢复的处理决策与异常处置规则，当发生突发灾难事件时，若灾难事件超出解决范围或响应时间过长，处置恢复实施组应遵循规则向上级组织进行汇报与处理。针对异常的灾难恢复事件，处置恢复领导小组应召集专业人员评估突发事件，确认突发事件对工业互联网系统造成的影响程度，进而确定下一步采取的措施，并将最新信息通知给处置恢复实施组，确保处置恢复工作的及时性。

（5）灾难恢复响应

应建立灾难恢复的响应规则，在事件发生时，处置恢复实施组收到处置恢复领导小组的决策后根据相应的处置恢复策略及时做出响应，迅速进行灾难恢复工作。当处置恢复实施组无法进行响应或响应时间过长时，应及时向处置恢复领导小组进行汇报，保障灾难恢复工作的持续性。

2.备份恢复

为确保工业互联网平台持续运作，应对重要系统进行灾难备份。企业应根据系统备份能力进行分级，按需求目标制订相应的备份恢复预案。为确保备份恢复预案顺利进行，企业可建立专门的灾难备份中心与处置恢复组织，根据处置恢复策略进行维护管理，并定期进行灾难恢复预案演练，确保预案的有效性。

（1）备份能力等级的定义

根据企业不同的业务类型与系统特点，对备份能力等级

进行划分，依照等级的不同采取不同的备份策略与应对措施。

（2）备份能力的需求确立

企业通过对其业务影响程度的分析与风险评估，确定工业互联网系统的备份能力等级需求及备份前所需的资源。

（3）备份恢复策略制定

依据企业现有的或行业通用规范准则制定适合自身的备份恢复策略，有条件的情况下可对制定的策略进行有效性与实用性方面的验证。

（4）灾难备份中心的建设、运行和维护管理

有条件的企业可建立专门的灾难备份中心，在灾难发生时迅速进行备份恢复工作，确保将损害降到最低。企业根据业务需求，成立专职的或兼职的灾难备份中心的运行和维护管理团队进行日常维护或危机处理。

（5）处置恢复预案的演练与管理

企业应定期对制定的处置恢复计划进行验证及防灾演习，来不断适应环境或技术的变化，确保计划的有效性。

3.分析评估

分析评估风险是工业互联网系统优化防护措施、形成闭环防御不可缺少的一个重要环节。通过分析识别系统面临的风险来制定相应的响应预案，并依据安全事件处理评估结果进行持续修正，从而达到改进处置恢复策略的目的。

（1）风险分析

企业可采用定性或定量的分析方法对安全事件造成的各种影响进行等级判断:

①定量分析：以量化方法，评估业务功能的中断可能给企业带来的直接经济损失和间接经济损失。

②定性分析：运用归纳与演绎、分析与综合以及抽象等方法评估业务功能的中断可能给企业带来的非经济损失，包括企业声誉、顾客忠诚度、社会与政治影响等。

（2）风险定义与预案制定

通过对工业互联网系统面临的内外部风险进行识别和定义，结合企业自身安全框架分析评估风险发生的可能性，从而制定适合企业自身需要的处置恢复机制。

（3）处置恢复效果评估

当企业发生安全事件后，要及时分析事件的影响范围与程度，评估企业处置恢复方案的适用性与有效性。

（4）处置恢复方案改进

通过分析结果，对工业互联网系统面临的风险进行确认，分析总结此次事件处置恢复所消耗的资源成本以及风险造成的损失，检验处置恢复预案的落实与管理是否符合处置恢复目标的要求，并通过实际案例的处理经验不断改进处置恢复准则。

五、 工业互联网安全发展趋势与展望

本工业互联网安全框架的提出，对于企业开展工业互联网安全防护体系建设，全面提升安全防护能力具有重要的借鉴意义。工业互联网安全防护作为未来工业互联网发展的一个重点关注方面，要求工业互联网安全框架在工业互联网快速发展中不断更新与完善。未来工业互联网安全防护工作有以下几个方面值得关注。

一是安全防护智能化将不断发展。未来对于工业互联网安全防护的思维模式将从传统的事件响应式向持续智能响应式转变，旨在构建全面的预测、基础防护、响应和恢复能力，抵御不断演变的高级威胁。此外，未来将有更多企业建成安全数据仓库，利用机器学习、深度学习等人工智能技术分析处理安全大数据，不断改善安全防御体系。工业互联网安全架构的重心也将从被动防护向持续普遍性的监测响应及自动化、智能化的安全防护转移。

二是工业互联网平台安全在工业互联网安全防护中的地位将日益凸显。工业互联网平台作为工业互联网发展的核心，汇聚了各类工业资源，因而在工业互联网安全防护未来的发展过程中，对于平台的安全防护将备受重视。届时，工业互联网平台使用者与提供商之间的安全认证、设备和行为的识别、敏感数据共享等安全技术将成为刚需。基于云访问

安全代理、软件定义安全、远程浏览器等技术的安全解决方案和模型将有效提升工业互联网平台的安全可视性、合规性、数据安全和威胁保护能力。

三是对工业互联网大数据的分类分级保护、审计和流动追溯将成为防护热点。工厂数据由少量、单一、单向向大量、多维、双向转变，具体表现为工业互联网数据体量大、种类多、结构复杂，并在 IT 和 OT 层、工厂内外双向流动共享。工业大数据的不断发展，对数据分类分级保护、审计和流动追溯、大数据分析价值保护、用户隐私保护等提出了更高的要求。未来对于数据的分类分级保护以及审计和流动追溯将成为防护热点。

四是对于工业互联网现场设备的安全监测与威胁处置要求越发迫切。工业互联网现场设备的智能化发展将使安全问题在工业互联网生产场景中被逐步放大，仅靠拦截将无法应对新形势下的安全挑战。未来要力争在对于工业互联网现场设备的安全监测、内存保护、漏洞利用阻断等终端防护技术方面将取得创新突破，有针对性地保护工业互联网现场设备，并对攻击行为进行快速响应。

五是信息共享和联动处置机制呼声日高。面对不断变化的网络安全威胁，企业仅仅依靠自身力量远远不够，需要与政府和其他企业统一认识、密切配合已成为安全界的共识。未来通过建立健全运转灵活、反应灵敏的信息共享与联动处

置机制，打造多方联动的防御体系，能够进一步提升工业互联网企业安全风险发现与安全事件处置水平。

六是态势感知将成为保障工业互联网安全的重要技术手段。鉴于工业互联网对于国民生产及社会稳定的重要意义，对于工业互联网的安全防护，必须做到在安全威胁对其正常运行造成实质性影响之前及时发现并妥善处置，这就要求今后的工业互联网需具备完备的安全态势感知机制，分析工业互联网当前运行状态并预判未来安全走势，实现对工业互联网安全的全局掌控，并在出现安全威胁时通过网络中各类设备的协同联动机制及时进行抑制，阻止安全威胁的继续蔓延。

综上所述，工业互联网安全框架需紧密结合工业互联网安全发展的五大趋势，针对防护对象，从防护措施和防护管理视角加强安全防护，并不断进行丰富和完善，从而更好地指导企业开展工业互联网安全防护工作，提升工业互联网安全防护能力。