工业互联网产业联盟
Alliance of Industrial Internet

工业互联网标识解析
——安全风险分析模型研究报告

工业互联网产业联盟（AII）
2020年4月

Industrial Internet

工业互联网标识解析—
安全风险分析模型研究报告
（2019年）

工业互联网产业联盟（AII）

2020 年 4 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

当前，工业互联网已成为推动传统工业转型升级的重要着力点，工业互联网标识解析作为工业互联网的重要网络基础设施，是我国工业互联网建设的重要任务，是支撑工业互联网实现身份管理、实现数据互联互通的枢纽，其安全是工业互联网安全的重要内容。

2017 年 11 月 27 日，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“指导意见”），将“推进标识解析体系建设”列为主要任务之一，提出“加强工业互联网标识解析体系顶层设计，制定整体架构”，明确提出“重点突破标识解析系统安全”。2019 年，工业和信息化部等十部委联合印发《关于加强工业互联网安全工作的指导意见》，其中特别就工业互联网标识解析体系安全工作推进进行了重点部署，要求标识解析系统的建设运营单位同步加强安全防护技术能力建设，确保标识解析系统的安全运行。

本报告从工业互联网标识解析体系架构安全、身份安全、数据安全、运营安全等多个视角，阐述工业互联网标识解析体系可能存在的安全风险，并建立统一的安全风险分析模型，从根源上把控风险，为工业互联网标识解析安全体系建设贯彻落实提供参考和指引，并推动业界达成广泛共识，共同推进工业互联网标识解析安全、健康、持续发展。

组织单位：工业互联网产业联盟标识特设组

编写单位：（排序不分先后）

中国信息通信研究院、广东鑫兴科技有限公司、恒安嘉新（北京）科技股份公司、瓦戈科技有限公司、大唐移动通信设备有限公司、亚信科技（成都）有限公司、中兴通讯股份有限公司、江苏中天互联科技有限公司、深圳奥联信息安全技术有限公司、南京中新赛克科技有限责任公司、上海市数字证书认证中心有限公司、北京亚鸿世纪科技发展有限公司、北京天地和兴科技有限公司、北京信安世纪科技股份有限公司、北京泰尔英福网络科技有限责任公司、兴唐通信科技有限公司、中国科学院计算机网络信息中心、复旦大学、中国联通网络技术研究院、中国电子科技信息安全有限公司、北京顶象技术有限公司、新疆天衡信息系统咨询有限公司、北京万维物联科技发展有限公司、北京航天智造科技发展有限公司、深圳市标准技术研究院、浙江鹏信信息科技股份有限公司、重庆工业大数据创新中心有限公司、上海观安信息技术有限公司、用友网络科技股份有限公司、许继集团有限公司、南京埃科法物联技术有限公司。

编写人员：（排名不分先后）

区景安、刘阳、马宝罗、张振涛、戴清平、王桂温、许道远、朱向赟、徐晖、毕晓宇、汤凯、吴天飞、白顺东、崔久强、熊翱、池程、汪毅、郑宁、汤永田、焦靖伟、覃汐赫、

渠立孝、李媛红、李龙、贾雪琴、赵闪、王姝、胡鹏辉、王大鹏、赛玉华、泮晓波、史博、张森、钱侃、林晨、滕斌、张俊毅、张开颜、朱斯语、武林娜、邢镔、梁栋、胡龙珍、李朋、梁栋、杨杨、刘溪伟、艾舒欣、乔帅飞、崔婷婷。

目录

1 标识解析体系安全风险研究的背景和意义

1.1 研究背景

工业互联网标识解析体系是工业互联网网络体系的重要组成部分。目前，北京、上海、广州、重庆、武汉五大国家顶级节点自 2018 年底上线运行，系统功能逐步完备，与 Handle 国际根节点、OID(Object Identifier，对象标识符)国际体系等实现对接。当前，我国工业互联网标识服务体系持续完善，标识应用成效初步显现。截至 11 月 29 日，已部署并上线试运行的工业互联网标识节点达 34 个，涵盖 16 个行业，标识注册总量突破 12 亿，接入标识服务节点的企业超过 800 家。中国信息通信研究院将持续夯实基础，在汇聚产业数据的基础上，推动工业互联网创新应用向更广范围、更深层次发展。

随着工业互联网标识的逐步推广应用，标识解析开启了一个自主机器和智能过程的崭新时代，正在为我们带来巨大的社会和经济机遇。然而，互联互通必将会带来不可避免的副作用，即我们暴漏于网络入侵的威胁之中。因此，标识解析安全也就成为工业互联网标识解析体系部署过程中最需要引起关注的问题。工业互联网标识解析作为工业互联网实现互联互通的“中枢神经”，存储了更多的敏感数据，一旦服务受限或遭遇攻击，将会对国民经济造成重要影响，甚至对国家安全构成一定的威胁，加快推进工业互联网标识解析

体系安全防控能力建设迫在眉睫。

1.2 研究意义

为落实《指导意见》工作要求，加快推进工业互联网标识解析安全技术研究、标准制定、未来创新发展趋势和手段建设，工业互联网产业联盟标识特设组开展了工业互联网标识解析安全风险调研，搜集、分析国内外的最新动态和资料，组织编写了《工业互联网标识解析-安全风险分析模型》研究报告，希望在规划设计阶段，通过对工业互联网标识解析安全风险进行分析，提前识别出受保护对象的风险点、风险事件、风险事件的起因、可能的影响后果、适合的保护措施、标准法规的符合性、贯彻实施的可行性等等，从而建立统一的风险分析模型和方法论，做到提前把控，防范于未然。

2 现有标识解析体系面临的安全风险

当前工业互联网标识解析技术基于 DNS(Domain Name System,域名系统)主要可区分为两条路径：改良路径和变革路径。变革路径是采用不同于 DNS 的标识解析技术，包括 Handle 体系、UID 体系，以及一些其他类型的体系。改良路径仍基于互联网 DNS 系统，对现有互联网 DNS 系统进行适当改进实现标识解析，这类标识解析技术是在 DNS 技术上叠加一套标识服务，然后再往下保存标识 ID 和与标识相关的映射。

2.1 DNS 风险分析

2.1.1 DNS 安全概述

在网络环境中，设备标识是设备之间通信的基础。为了实现工业互联网内实体之间的信息交互，工业互联网中的每个实体对象都需要被赋予统一的标识，通过建立类似互联网域名解析系统的工业互联网标识解析体系，实现工业互联网中实体之间标识信息的识别，进而实现工业各环节信息互通以及信息的查询与共享。为了保证建立工业互联网的标识解析体系的安全性，需要充分考虑该体系所对应的安全风险模型。深入分析当前技术发展比较成熟且得到广泛应用的 DNS 标识解析体系所面临的安全风险，并以此作为建立工业互联网标识解析体系风险模型建立的参考。

在网络环境中，通信实体之间的连接是通过每个实体在网络中唯一的 IP 地址实现的。DNS 域名解析服务是互联网最基础、最核心的服务，它为整个网络中的其它服务器提供域名到 IP 地址解析。通常网络用户使用域名访问网站，DNS 为用户提供将主机名和域名转换为 IP 地址，从而实现网络中基于 TCP/IP 的通信。在 DNS 域名解析体系中，采用层次树状结构命名方式。域可以划分为顶级域或者一级域，一级域之后可以划分为二级域、三级域。用户发出的域名解析请求一般通过若干 DNS 服务器以直接解析或者递归/迭代查询方式解析获得。

DNS 在网站运行和维护中起着至关重要的作用,通过 DNS 可以访问属于网络的任何应用。但 DNS 协议设计之初对于安全性考虑不足，DNS 查询协议缺乏认证控制机制，传输的信令与数据因未被加密保护，容易被攻击者截获或者篡改，用户收到响应后无法验证数据的完整性。此外，攻击者可以通过伪装正常的 DNS 查询的方式攻击 DNS 服务器，例如通过拒绝服务攻击使得 DNS 系统面临劫持、欺骗、拒绝服务、缓存污染等严重的安全威胁。

2.1.2 DNS 安全风险

- **DDoS 攻击**

DNS DDoS 攻击主要针对 DNS 系统，利用“肉鸡”等各种网络资源发送 DNS 服务请求,以耗尽 DNS 服务资源,达到 DNS 解析服务无法正常的处理 DNS 解析请求。例如，攻击者可以通过控制僵尸网络发起大量域名查询请求，或者攻击者可以通过利用工具软件伪造源 IP 发送海量 DNS 查询请求，耗尽 DNS 服务能力或者 DNS 服务的网络资源，从而达到 DNS 正常用户无法获得解析结果的目的。

- **缓存污染**

DNS 服务器分为授权 DNS 服务器和缓存 DNS 服务器。缓存 DNS 服务器提供递归解析服务，通过向授权 DNS 服务器查询,将资源记录暂时存储到缓存中,供后续用户访问时使用。

由于 DNS 协议不支持以快速和安全的方式将数据更新，

也无法验证服务器的合法性和缓存的有效性，将导致 DNS 缓存不一致和缓存数据（特别是一些密钥等敏感数据）未及时更新而产生风险。攻击者可以利用这个弱点将无效信息传播到 DNS 服务器或缓存的方式发起缓存污染攻击，缓存投毒攻击就是利用了协议的这些不足之处实施攻击。

- **DNS 重定向**

一般用户发送 DNS 请求到 LOCAL DNS 中，LOCAL DNS 先查看缓存中是否有结果，如果无结果，LOCAL DNS 发起递归请求，从授权 DNS 获取相应的解析结果，在 LOCAL DNS 与授权 DNS 交互过程中，攻击者发送伪造的响应包给 LOCAL DNS，抢先在授权 DNS 应答，从而 LOCAL DNS 将缓存的错误的结果并发送给用户，使得用户的访问被导向了攻击者的网站。攻击者通过 DNS 查询时将 LOCAL DNS 缓存中注入伪造的域名资源记录实现重定向的目的。

- **DNS 欺骗**

DNS 查询通常使用 UDP 协议，一般 DNS 查询使用五元组：源 IP、源端口、域名、目的 IP、目的端口进行数据校验，这种校验方法无法验证数据来源的真实性和报文的完整性。鉴于这种设计缺陷，如果 LOCAL DNS 在递归解析过程中接收到错误的信息，只要五元组能够校验准确，就将把接收到的错误的信息当着正确的解析结果处理。

攻击者通过控制 DNS 服务器或者冒充域名服务器，将查

询的 IP 地址设为攻击者的 IP 地址，或者构造虚假的 DNS 服务器响应数据包以匹配这些参数，将用户引导至错误的网站、甚至是钓鱼网站。

- **DNS 劫持**

DNS 劫持又称为域名劫持。攻击者将在目标网络范围内拦截域名解析请求或者窃听 DNS 会话，分析请求的域名，猜测 DNS 服务器响应 ID 返回虚假的 IP 给用户或者劫持在 DNS 的服务器上的 DNS 应答响应后直接返回一个恶意的 IP 地址或者不执行反馈 IP 的响应，使得用户访问到假冒的网络或者得不到网络响应。

2.2 基于 DNS 改良路径的标识解析技术风险分析

改良路径采用基于互联网 DNS 系统的标识解析技术，目前主要是类似于 DNS 的自动网络服务系统的对象名称解析服务（ONS）和由 ISO/IEC、ITU 国际标准组织共同提出的对象标识符（OID)。

2.2.1 ONS 安全概述

在工业互联网应用中，ONS(Object Name Service,对象名称解析服务)标识解析服务是其中一个重要的环节，作为用户访问工业互联网的最初入口，如果错失安全防守，则可能将大量的查询用户引导至有安全问题的服务、网站等资源，带来巨大的信息泄露，造成不可估量的损失。

首先，ONS 保存了工业互联网中所有标识的解析信息，一旦 ONS 服务受到骇客攻击，泄露的解析信息将会暴露所有标识及相关应用服务资源入口，将整个服务体系暴露在攻击者面前。

其次，ONS为用户提供应用服务资源入口，必须要保证其返回结果的真实性，并保护解析结果的隐私。否则接收到错误信息的用户将被诱导到存在安全问题的应用服务资源，对生产、流通和使用环节的业务造成重大的影响，或无法即时发现仿冒的或有缺陷的产品。

2.2.2 ONS 安全风险

国内外很多学者已经意识到 ONS 安全对于 EPC 网络的重要性，并对关于 ONS 的安全威胁做了很多研究，同样相关的研究也适用于工业互联网的 ONS 服务。

结合 ONS 服务的解析原理和流程，可以分析出**ONS 的安全危险主要存在以下几个方面:**

- **缺少对 ONS 服务器的认证**

缺少对 ONS 解析服务器的认证会导致用户无法确定所获取的信息是来自真实的 ONS 服务器还是伪造的 ONS 服务器。一旦用户访问了伪造的 ONS 服务器，将获得不可信的应用服务资源入口，带来极大的安全隐患。

- **缺少对用户的认证**

ONS 服务记录保存了不同的应用服务资源入口，对于不

同权限的用户应返回不同的结果。而 DNS 服务本身并不会验证用户身份，只返回所有信息。因此缺少对用户的认证将允许任何人包括攻击者可以任意访问 ONS 服务资源，使 DDoS 攻击成为可能。

- **缺少机密性的传输机制**

ONS 的解析过程依赖于 DNS 服务，而 DNS 查询请求和返回报文均为明文，没有采取任何安全机制。明文传输带来两个方面的威胁，首先攻击者可以侦听访问请求和返回结果，导致用户隐私的泄露；然后攻击者可以有机会拦截返回结果，进行修改后再返回给用户，从而将存在安全问题的应用服务资源入口清单提供给用户使用，实现侵入用户终端窃取用户机密的目的。

- **缺乏数据完整性检查**

ONS 没有为用户提供验证其返回结果数据完整的方法，攻击者可以把截获到的信息进行篡改并发送，从而将错误的应用服务资源入口提供给用户，将用户引导至假冒的资源服务。

- **DNS 系统安全缺陷**

ONS 架构与服务设计建立在 DNS 基础之上。标识在解析时，首先根据标准约定的规则进行域名转换，通过 DNS 查询获取域名对应的 NAPTR 记录，才能获得对应的应用服务资源入口。因此这样的系统架构也继承了 DNS 系统全部的安全缺

陷，主要包括 DDoS 攻击、恶意网址重定向攻击、中间人攻击、域名欺骗、缓存污染、单点故障等。

2.2.3 OID 安全概述

OID 是由 ISO/IEC、ITU-T 共同提出的对象标识机制，用分层的树状结构对任何类型的对象进行全球无歧义的唯一标识，几十年来在网络通信、安全、卫生、气象等领域得到了广泛的应用。从地区来看，OID 已经在全球 200 多个国家中得到使用，并由各个国家自主管理各自的国家标识分支。我国在 2006 年成立了国家 OID 注册中心，负责 OID 中国国家分支节点（1.2.156 与 2.16.156）的相关标准制定、标识注册管理、标识解析等相关的工作，并且在农业、林业、交通、智能制造等新领域得到了进一步的应用，制定了一系列的行业标准。

2.2.4 OID 安全风险

传统标识体系大多基于 DNS 技术体系构建，将自身的标识空间映射到 DNS 空间，以利用无所不在的 DNS 的解析服务能力，在此基础之上构建相应的标识管理与应用体系，例如 ITU-T 定义的 OID 体系。

(1)DNS 技术体系固有的安全问题

DNS 体系作为重要的基础互联网基础设施，设计之初如同互联网本体一样，并未考虑安全性方面的需求，导致其成

为各种网络攻击的重要目标与手段，主要包括:

- **针对 DNS 服务器的 DDOS 攻击**

包含基于主机耗尽型的 DNS 查询拒绝服务攻击与基于宽带耗尽型的 DNS 反弹式拒绝服务攻击（DNS reflector attacks，又称 DNS amplification attacks）。

- **针对用户的 DNS 劫持**

包含 DNS 服务器地址劫持、hosts 文件劫持、缓存投毒、kaminsky 缓存投毒攻击、入侵 DNS 服务器等方式。

（2）OID 管理与应用体系固有的安全问题

OID 解析体系采用了 DNS 技术，相应的 DNS 体系具有的缺陷都会在 OID 体系之中存在。除此之外，OID 本身在运营与管理过程中，也会存在各种技术性或非技术性的风险。

- **标识缺乏认证能力**

当前 OID 解析体系继承了 DNS 的名字解析能力，同样也继承了 DNS 缺乏认证能力的缺陷，需要结合其他的认证手段才能提供认证能力，如 PKI 体系。但 PKI 体系太过于重量级，并且主要面向组织与主机身份提供证书服务，难以面向海量的 OID 对应对象进行证书发放；另外，由于 OID 授权用户的认证方式相当多元化，例如用于防伪领域时，根据不同的商品的特点，需要采用不同的认证方式，OID 体系本身无法从顶层设计规定统一的认证方式。

- **解析系统缺乏解析权限控制能力**

OID 解析系统仅仅提供标识的匿名查询能力，无法对解析进行更细粒度的权限控制，以满足某些特殊行业或者应用领域更高的安全性需求。解析流量无法采用加密的方式进行传输，为攻击者提供了了解用户行为并进行针对性攻击的手段。

- **标识对应身份缺乏可信背书**

OID 授权用户可以定义标识的身份内涵，但授权用户（例如企业本身）本身并不具备很强的信用能力，往往需要独立的第三方（如监管部门）进行背书，才能够提供足够的信用，使得面向公众提供的服务具备足够的可信度。服务于 OID 标识的信用体系成熟需要时间，以支撑大规模的可信标识应用。

- **OID 国际顶级解析节点对接风险**

当前 OID 国际顶级解析节点 oid-res.org 在国内没有备份节点，由于各国发展水平的不一致，当与国际 OID 根节点对接时，会产生对接风险。

- **太长的授权链条容易导致信用淡化，监管弱化**

标识上级节点对下级节点，从管理上到技术上，都缺乏穿透式监管能力，对于下级 OID 节点的行为缺乏可视性与可控性。相应的信任关系，将会随着 OID 节点的链条加长，呈现快速弱化的趋势。

- **标识授权用户缺乏运营标识管理系统等基础设施的技术**

能力与经验

缺乏授权节点的认证标准与认证体系，随着应用规模的不断扩大，标识层次的不断增加，对于下级叶子节点的控制比较弱，难以保证参与者水平的一致性。另外，很多标识授权用户，本身缺乏运营标识管理系统的技术能力与经验，在监管比较弱的情况下，将会很容易出现标识滥用、滥发等异常情况，不利于工业互联网标识领域信用体系的建立以及长期的健康发展。

2.3 基于 DNS 变革路径的标识解析技术风险分析

变革路径采用不同于互联网 DNS 系统的标识解析技术，目前主要是数字对象名称管理机构（DONA 基金会）提出的 Handle 系统，未来还可能出现新的技术方案。

2.3.1 Handle 安全概述

Handle 系统最初是由美国 CNRI（The Corporation for National Research Initiatives）提出并实现的一种建立在 Internet 架构之上的通用分布式信息系统，用于提供有效的、可扩展的、可靠的全球名字服务。在这个分布式的环境中，每个 Handle 标识都有自己的管理者和管理机构。

Handle 系统定义了一套成熟兼容的编码规则、拥有一套稳定的后台解析系统和一个自主可控的全球分布式管理架构。编码结构为权威域（前缀）/本地命名（后缀），前后

缀之间用“/”分隔。由美国国家创新研究所（CNRI）开发，后由 DONA 进行管理和运营。Handle 在全球设立若干的根节点，根节点之间平等互通。Handle 系统支持可靠的标识解析，为客户端的请求提供了诸如数据保密性、服务完整性和不可抵赖性等安全服务。目前 Handle 技术在国内已经成功应用在产品溯源、数字图书馆等领域。

2.3.2 Handle 安全风险

Handle 标识解析技术提供了一套完整的安全机制，通过用户身份验证、管理鉴权等方式，有效地保证了数字对象及其服务的完整性，同时又能有效地防止通过伪造用户要求或者篡改服务器响应而产生的不安全行为。尽管如此，Handle 系统在以下几个方面仍存在安全风险。

- **隐私保护**

通常情况下，存储在 Handle 系统的大多数标识数据都是开放的，除非 Handle 管理员另有授权。当新增标识数据时，Handle 管理员须根据标识数据属性将这些标识标记为可读，或者将其存储为加密的标识数据，以保证标识数据只能在受控目标对象范围内被读取。Handle 服务器生成的日志文件是另一个薄弱环节，客户隐私易遭受攻击，Handle 标识解析系统的运营者须加强对这些信息的保护。

- **缓存和代理服务器**

代理和缓存服务器都可以带来性能提升并能够提供其

它增值服务，二者都将自己定位为“中间人”，因而也会很容易受到“中间人攻击”。因为缓存的内容很容易被恶意利用，缓存服务器还带来其它潜在安全威胁。对缓存的潜在攻击可以导致私人数据曝光，或当用户认为他们的信息已经从网络中移除时，仍然保留他们的信息。因此，缓存内容应该被视作敏感信息进行保护。

- **镜像**

Handle 系统在镜像站点之间复制内容可能存在延迟。因此，在发送任何时间敏感的数据时，应考虑将请求发送到基层服务站点。服务管理员在选择镜像站点时必须谨慎，每个镜像站点必须遵守同样的安全程序，以此来保证数据的完整性，也可以使用软件工具来确保镜像站点之间数据的一致性。

- **DDoS 攻击**

与所有公共服务一样，Handle 系统也会遭受拒绝服务攻击。目前没有通用的解决方案可以用来预防此类攻击。网络态势感知技术可用来感知此类攻击，也可以用于当攻击发生时通知管理员。无状态 Cookies 是减轻 DDoS 对主机攻击效果的工具之一。

3 标识解析安全风险分析模型

3.1 设计思路

本报告中的工业互联网标识解析安全风险分析模型是

在充分借鉴传统互联网和国内外工业互联网安全框架基础上，结合我国工业互联网标识解析体系的特点提出的，旨在为相关单位在工业互联网标识解析体系建设初期开展安全风险防范工作提供参考和指导，做到从根源上把控风险，防范于未然，从而提升工业互联网标识解析体系安全防护能力。对于工业互联网标识解析安全风险分析模型设计，可以从以下三方面进行阐述:

第一，建立统一的标识解析安全风险分析模型。

标识解析体系架构是一个树形分层型架构，它在物理上、操作上和管理上的种种漏洞均会构成安全的脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性更使单纯的技术防不胜防。攻击者使用“最易渗透原则”，必然在系统中最薄弱的地方进行攻击，因此，必须充分、全面、完整地对标识解析体系的安全需求进行分析。目前国内还没有针对标识解析体系安全风险全周期性、系统性、多层次的研究和认识，因此，亟需建立统一的标识解析安全风险体系，才能更好的对整个标识解析体系进行严格、规范的安全防护和管理。

第二，相关解析技术安全风险共性分析及借鉴。

当前工业互联网标识解析技术无论是改良路径或是变革路径主要基于 DNS 技术思想，而随着传统互联网应用不断成熟、壮大，DNS 自身的局限愈发明显，其遭受的攻击愈发

的多样性。而另一方面工业互联网标识解析真正应用分析场景还未来临，通过对已知的 DNS 安全威胁，结合工业互联网已有风险类型，对节点、数据、管理等对象分析，提炼共性风险特征，这在工业互联网标识解析安全风险分析模型的设计中是值得思考并充分借鉴。

第三，采用多维度多层次法研究模型。

要建立全面的标识解析安全风险体系，就要多维度、多层次横纵交叉分析，才能有效避免遗漏。本报告的研究结合国内外标识解析体系安全领域的现状，以 DNS、Handle、OID、ONS 四种常用标识解析技术为出发点，技术与管理相结合，针对安全风险分析、风险管理、风险措施三个视角，定义了架构、身份、数据、运营 4 个不同标识解析安全风险分析对象；参照传统互联网存在安全风险点，结合工业互联网应用场景，进行分析、筛选、增减，形成不同维度下的一系列风险类型，为后期不同对象做风险评价形成基础模型。

综上所述，工业互联网标识解析安全风险分析模型是基于建立系统性的模型作为设计理念，分析并借鉴国内外相关标识解析技术安全风险共性，采用多维度、多层次研究方法开展研究工作。

3.2 风险模型

工业互联网标识解析安全风险分析模型从风险分析视角、风险管理视角和风险措施视角三个视角进行构建，如图

1 所示。

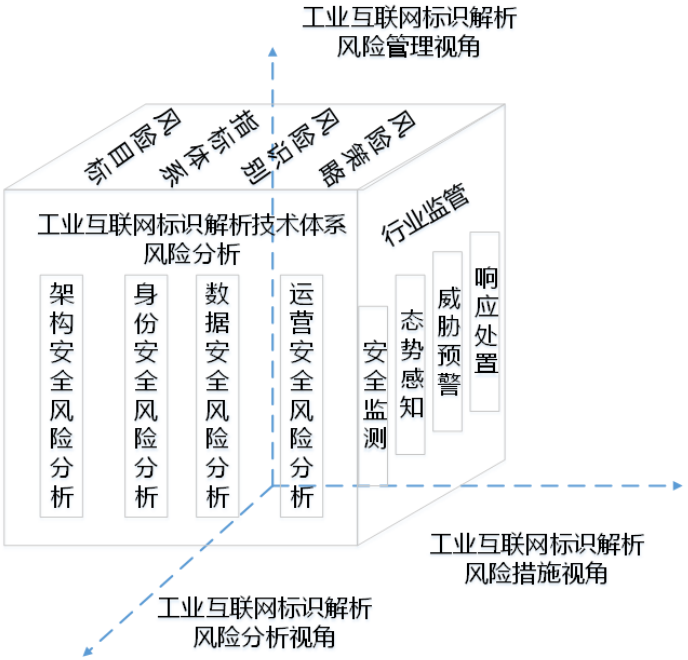

图1 安全风险分析模型总体架构

其中，风险分析视角包括架构安全风险分析、身份安全风险分析、数据安全风险分析和运营安全风险分析四大风险分析重点；风险管理视角包括风险目标、指标体系、风险识别和风险策略四大环节；风险措施视角包括行业监管、安全监测、态势感知、威胁预警和响应处置五个部分。

工业互联网标识解析安全风险分析模型的三个风险分析视角相对独立，但彼此之间又相互关联。三者相辅相成构成一个有机整体。

3.2.1 风险分析视角

风险分析视角主要包括架构安全风险分析、身份安全风险分析、数据安全风险分析、运营安全风险分析四大风险分

析对象，如图 2 所示。

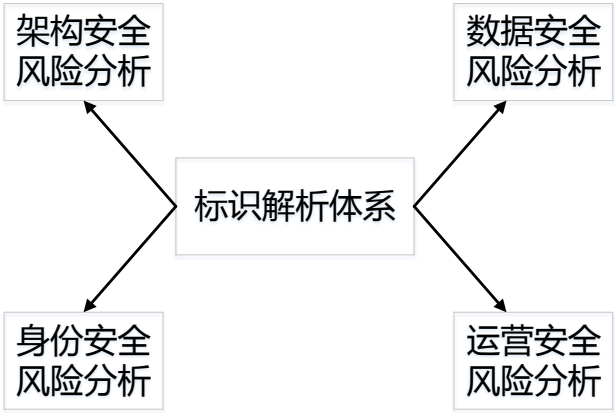

图2 风险分析视角模型

具体内容包括:

架构安全风险分析: 主要包括节点可用性风险、节点间协同风险、关键节点关联性风险等架构安全风险分析;

身份安全风险分析: 包括涉及人、机和物等三种角色的身份欺骗、越权访问、权限紊乱、设备漏洞等四种身份风险分析;

数据安全风险分析: 包括涉及标识注册数据、标识解析数据和日志数据的数据窃取、数据篡改、隐私数据泄露、数据丢失等数据安全风险分析;

运营安全风险分析: 包括物理环境管理、访问控制管理、业务连续性管理、人员管理、机构管理、流程管理等方面的运营安全风险分析。

3.2.2 风险管理视角

风险管理视角旨在指导构建持续改进的风险管控管理

机制，提升风险管控整体水平，主要包括风险目标、指标体系、风险识别、风险策略四个部分，如图 3 所示。

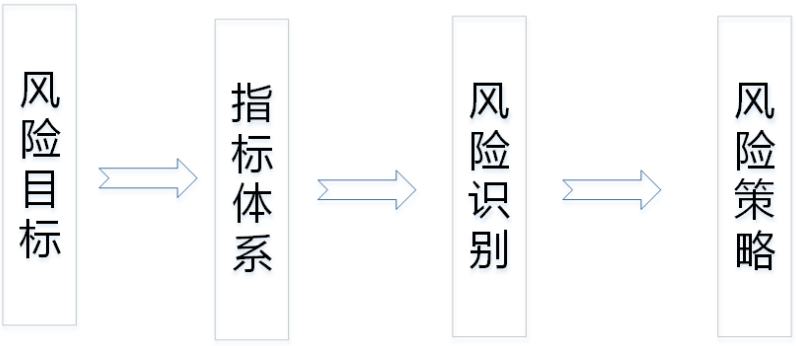

图3 风险措施视角模型

风险目标：需要确立工业互联网标识解析风险评估和业务保障的对象，即风险目标；

指标体系：根据风险目标，确定风险评估指标体系；

风险识别：针对风险目标，识别可能的风险；

风险策略：针对风险目标可能的风险，指定响应的安全防护策略。

3.2.3 风险措施视角

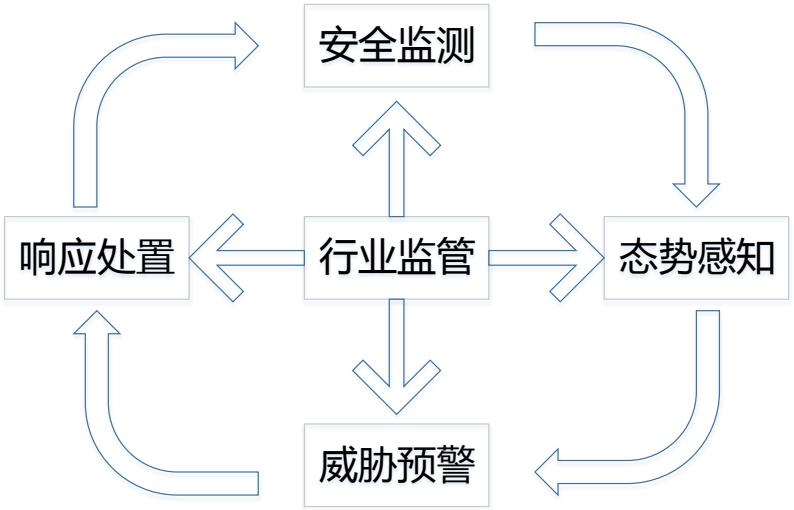

图4 风险措施视角模型

针对工业互联网标识解析体系面临的各种风险，风险措施视角从全生命周期角度明确方法指引，实现闭环管理和风险管控。风险措施视角主要包括行业监管、安全监测、态势感知、威胁预警和响应处置五大环节，如图 4 所示。

行业监管：统一领导，统一指挥，建立联动监管机制；

安全监测：针对四大风险分析对象，进行风险监测；

态势感知：部署响应的监测措施，实时感知安全风险；

威胁预警：针对态势感知发现的风险，进行风险预警；

响应处置：建立响应处置机制，及时应对安全风险。

4 标识解析安全风险的重点分析

4.1 架构安全风险分析

4.1.1 架构风险概述

工业互联网标识解析体系架构面临的风险很多，主要包括节点可用性风险、节点之间协同风险、关键节点关联性风险等。

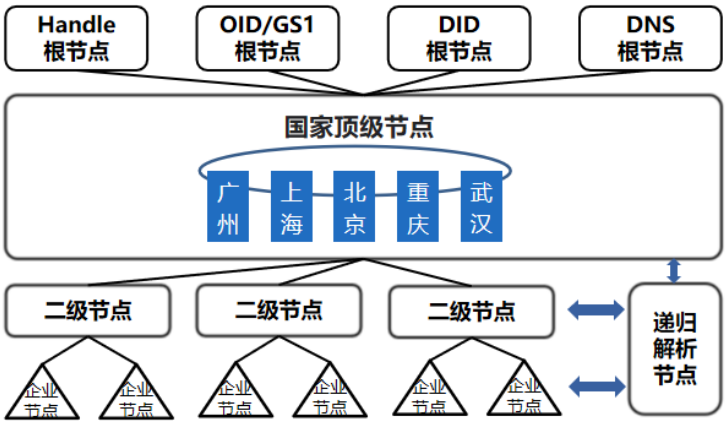

图 5 工业互联网标识解析体系架构

标识解析体系系统从架构上而言，是一个树形分层型架构，从逻辑上而言是一个分布式信息系统，如图 5 所示。主要包括查询客户端、解析服务器、镜像服务器、代理服务器、缓存服务器，该架构安全性在事务的每一步都依赖于这些部件的安全性，当体系架构的某一层节点出现问题时，就会对于整个架构的安全性产生一定程度的威胁。

4.1.2 架构风险分析

4.1.2.1 节点可用性风险

节点可用性风险是指解析体系架构的每一层中每种节点在可用性方面面临的风险，如果节点受到攻击，那么该节点的可用性会受到威胁，造成节点功能失效或者不可达。具体而言，节点的可用性风险主要包括以下方面。

- **DDoS 攻击**

标识解析系统是工业互联网的“中枢神经系统”，是关键基础信息设施，往往存在被 DDoS 攻击的风险。DDoS 攻击

通过僵尸网络利用各种服务请求耗尽被攻击节点的系统资源，造成被攻击节点无法处理合法用户的请求。而针对标识解析系统的 DDoS 攻击又可按攻击发起者和攻击特征进行分类。

- **按攻击发起者分类**
  - **僵尸网络：**控制僵尸网络利用真实标识协议栈发起大量标识查询请求。
  - **模拟工具：**利用工具软件伪造源 IP 发送海量标识查询。
- **按攻击特征分类**
  - **Flood 攻击：**发送海量标识查询报文导致网络带宽耗尽而无法传送正常标识查询请求。
  - **资源消耗攻击：**发送大量非法标识查询报文引起标识解析服务器持续进行迭代查询，从而达到较少的攻击流量消耗大量服务器资源的目的。

4.1.2.2 节点间协同性风险

节点间协同性风险是指对于解析体系的分布式特点，如果在解析过程中，节点协同性出现问题，就会造成数据同步或者复制内容过程出现延迟现象，导致数据不一致或者数据完整性出现问题。节点间协同性面临的主要风险包括：

- **代理服务器延迟**

代理服务器是指安装在本地网络边缘，作为用户终端向服务器发起请求的安全控制终端，实现用户发起查询的安全

性校验，提供标识匹配、标识转换等功能。如果代理服务器受到攻击，那么会导致解析服务器的应答延时增大，重则无法正常提供解析服务。

- **镜像服务器延迟**

各解析服务器的镜像站点之间复制内容可能存在延迟，导致数据不一致的问题，系统客户端应注意镜像站点之间内容复制的可能延迟。对于任何时间敏感的数据，应该考虑将解析请求发送到主服务站点。

- **数据完整性**

服务管理员必须仔细选择镜像站点。为了确保数据完整性，每个镜像站点必须遵循相同的安全过程。可以使用软件工具来确保镜像站点之间的数据一致性。

4.1.2.3 关键节点关联性风险

关键节点关联性风险是指标识解析体系架构中某些关键节点出现问题，将会导致影响其他节点的功能，最终削弱其稳定性或者健壮性。关键节点关联性风险主要表现为以下几种形式:

- **缓存击穿**

高并发场景下，如果某个缓存服务器中的标识缓存失效，则会导致解析请求都会直接落到下游的标识解析服务器，对其造成极大的压力，很可能使标识解析服务器的解析服务停止响应甚至瘫痪。

- **缓存穿透**

当请求访问的标识数据是一条并不存在的解析请求数据时，一般这种不存在的数据是不会写入缓存，所以访问该标识数据的请求都会直接落地到标识解析服务器，当这种请求量很大时，同样会给标识解析服务器带来风险。

- **反射/放大攻击**

攻击者大量向解析服务器发送大范围标识查询请求，并将该标识查询请求的源 IP 地址伪造成想要攻击的目标 IP 地址。标识解析服务器在接收到请求后会对该请求进行解析查询，并将大范围域名查询的响应数据发送给攻击目标。由于请求数据比响应数据小得多，攻击者就可以利用该技术有效的放大其掌握的带宽资源和攻击流量。

4.2 身份安全风险分析

4.2.1 身份风险概述

身份安全是工业互联网标识解析的门户，用户使用系统首先要进行身份认证，身份的重要性不言而喻。本节从人、机、物的角度分析标识解析系统中各种角色的身份以及其对应的风险点。不同的角色拥有不同级别和不同种类的权限，标识解析系统中各种风险点都可造成权限或信任受到侵害。

- **人员**

从人的角度可以对标识解析系统进行角色划分，主要包括标识数据管理员、普通用户、标识管理员、第三方监管员。

(1) 标识数据管理员：标识数据管理者;

(2) 普通用户：标识数据查询方;

(3) 标识管理员：标识管理者;

(4) 第三方监管员：负责监管标识数据。

- **机器**

从机器的角度划分标识解析系统的角色，包括国际根节点、国家顶级节点、二级节点、企业节点、递归解析节点、工业互联网客户端。

(1) 国际根节点：包括 13 个国际根节点，中国拥有一个国际根节点。负责向全球范围提供公共根区数据管理和根解析服务;

(2) 国家顶级节点：包括现有的 5 个国家顶级节点。负责国内顶级标识编码注册和标识解析服务以及标识备案和认证等;

(3) 二级节点：主要指行业节点或省级节点。负责行业或区域内的标识编码注册和标识解析服务以及标识业务管理和应用对接服务;

(4) 企业节点：每一个企业自己的节点，也叫做三级节点。负责企业的标识编码注册和标识解析服务;

(5) 递归解析节点：为工业互联网终端提供统一入口，通过缓存等技术提高标识解析服务性能;

(6) 工业互联网客户端：标识数据的使用者和标识解析

节点的管理终端。

- **物**

工业互联网终端：标识数据的生产者。

4.2.2 身份风险分析

针对人、机、物三种身份，每种身份对应的主要风险点如下表所示：

身份类别	具体身份	风险点
人员	标识数据管理员	身份欺骗、越权访问、权限紊乱
	普通用户	身份欺骗、越权访问、权限紊乱
	标识管理员	身份欺骗、越权访问、权限紊乱
	第三方监管员	身份欺骗、越权访问、权限紊乱
机器	国际根节点	身份欺骗、设备漏洞
	国家顶级节点	身份欺骗、设备漏洞
	二级节点	身份欺骗、设备漏洞
	企业节点	身份欺骗、设备漏洞
	递归解析节点	身份欺骗、设备漏洞
	工业互联网客户端	身份欺骗、设备漏洞
物	工业互联网终端	身份欺骗、身份标识与产品关联出错、设备漏洞

4.2.2.1 身份欺骗

身份欺骗在工业互联网标识解析系统中也可以叫标识欺骗，因为标识解析系统所有的身份都是以标识来表示。下面从人、机器、物的角度来对身份欺骗进行分析。

从人员的角度来看，身份欺骗是通过伪造合法身份来获得合法身份所对应的权限。这既可以是非法用户伪造身份变成合法用户，也可以是合法用户伪造身份变成其他用户，比如普通用户伪造身份变成标识管理员、标识数据管理员伪造身份变成第三方监管等。

从机器的角度来看，身份欺骗是伪造身份导致设备或服务器被假冒欺骗。这既可以在国际根节点与国家顶级节点之间发生，也可以在二级节点与企业节点之间发生，工业互联网客户端与企业节点之间也同样存在身份欺骗。以二级节点与企业节点之间身份认证为例，二级节点认证企业节点，一个非法的企业伪造自己的身份，欺骗二级节点让认证通过。

从物的角度来看，身份欺骗是伪造产品或者终端设备的身份以提供虚假的信息。以企业节点认证工业互联网终端为例，工业互联网终端伪造自己的身份，将物品 A 伪造成物品 B，以物品 B 的身份被企业节点认证，以后一直提供物品 B 的信息给企业节点。

身份欺骗出现的原因多种多样，主要原因是没有进行标识鉴别，除此之外还诸如中间人攻击、嗅探、伪造证书等。

下面以标识未曾鉴别和中间人攻击为例进行说明。

黑客用普通用户的标识伪造成标识管理员登录系统，如果系统没有进行标识鉴别直接解析登录，那么普通用户就拥有了标识管理员的权限，黑客就能进行各种意想不到的操作，对系统造成不可预测的威胁。

中间人攻击的模式为二级节点-中间人-企业节点 A，二级节点认证企业节点 A 时，中间人冒充企业节点 A 与二级节点通信，使得二级节点认为与之通信的是企业节点 A，同时又伪造成二级节点和企业节点 A 通信，最终达到身份欺骗的目的。

4.2.2.2 越权访问

越权访问主要是指能访问超过用户本身权限的资源。比如标识管理员它应该只有管理标识的功能没有普通用户的功能，如果标识管理员出现了普通用户的功能，这就是越权访问。这是两个不同的权限，一个权限只能对应一种身份。

越权访问的出现有以下几个原因:

（1）系统本身访问控制设计混乱，造成权限不明。在做访问控制设计的时候，权限管理这一块条理不清楚，从而出现越权访问的设计漏洞。

（2）遭遇攻击，提升了原角色权限。比如低权限的数据库用户，登录数据库后，利用数据库的漏洞或者不合理的函数，提升权限；WEB 页面进行 SQL 注入攻击，对数据库进

行非法访问，提升用户权限等。

4.2.2.3 权限紊乱

使用标识解析服务的设备和人员众多，最小时间和资源范围授权有效但授权繁杂，对权限的分配、职责的分割、特殊权限的限制、权限的撤销等管理上的疏漏或为非法利用，攻击者可以通过注入、渗透等方式绕过权限管理，从而进入系统。

4.2.2.4 身份标识与产品关联出错

身份标识与产品关联出错是指身份标识与产品没有一一对应，导致产品数据收集出现错误。比如一个大闸蟹的身份标识却贴在茅台酒上，导致服务端误以为收集的是大闸蟹的数据，实际却是茅台酒的。

4.2.2.5 设备漏洞

设备漏洞主要是指标识解析系统中的服务器、客户端或者终端可能存在安全漏洞或使用含已知漏洞的组件，导致攻击者通过已知漏洞绕过设定的访问控制策略，远程控制、入侵或篡改设备以及设备标识数据。

4.3 数据安全风险分析

4.3.1 数据风险概述

工业互联网标识解析涉及标识注册数据、标识解析数据

和日志数据等共三类数据进行数据安全风险分析。在网络安全中，数据安全的能力包括数据的完整性、机密性和可用性三个维度。根据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，标识解析数据安全涉及到数据采集、数据传输、数据存储、数据使用、数据交换和数据销毁等环节。基于以上数据安全维度，标识解析数据安全风险有：数据窃取、数据篡改、隐私数据泄露和数据丢失四类风险。

4.3.2 数据风险分析

4.3.2.1 数据窃取

工业互联网标识解析数据窃取风险主要是破坏数据的机密性，数据被非授权用户获得，使得**标识注册数据、标识解析数据或日志数据**外泄。数据窃取风险可能发生在数据采集、数据传输、数据交换和数据存储环节。

- **数据采集**

数据采集主要发生在工业互联网设备端，存在设备和计算安全、网络和通信安全等不可控风险。标识解析的注册数据和解析数据的采集、传输都在不可控的设备当中进行，存在着采集数据被窃取的风险。数据过程运行在设备当中，存在着数据过程被调试、监听，导致采集的数据被窃取的风险。例如针对硬件的拆解、估计得篡改将会导致计算设备不可控导致数据窃取；针对软件接口（如 GDB）、硬件接口（如 JTAG）等的非法调试也会导致数据窃取风险。

- **数据传输**

目前，大多数工业互联网设备依托 HTTP 传输工业标识解析数据，少量设备采用 SSL/TLS 等方式加密传输，但是由于设备端普遍性能较低，加密算法不可控等因素，导致数据在传输过程中被窃取。数据在传输过程中对数据保护不到位，如存在：明文传输、双方未进行身份校验、数据未进行完整性校验等情况，攻击者通过通信链路取通信数据，并进行非法活动，造成严重的业务风险与数据泄露。攻击者可以通过截取传输过程当中的数据，窃取数据内容。

上述风险都会带来数据过程的异常，导致数据被窃取，在数据采集过程当中，需要对数据过程进行有效的安全防护，对设备端程序进行抗破解、抗反编译处理；对设备漏洞进行早期发现和防护；对软硬件调试接口进行封锁，避免数据过程当中的安全风险。

在工业互联网标识解析体系中，标识查询和标识解析等过程都涉及到对工业标识数据的使用，而经过标识的数据很可能包含工业企业生产制造相关的核心设备、关键流程、企业管理等重要数据，如果没有有效的安全防护措施，数据使用应采取适当的安全控制措施以防止由于数据分析而可能带来的数据价值泄漏风险。

- **数据存储**

标识解析系统以及载体系统存在漏洞，导致攻击者入侵

节点服务器或相关数据存储服务器，导致攻击者获得服务器控制权限从而导致数据信息泄露。

内部员工权限管理不当或安全意识不到位，可能存在内部员工窃取数据获取利益，或内部员工被辞退后主动泄露管理身份信息、服务器配置信息等行为。若一系列流程设置不当可能会导致无关或恶意人员直接接触到解析服务器、数据服务器等重要设备，存在直接拷贝数据、盗走硬盘、主机等行为。

4.3.2.2 数据篡改

工业互联网设备在接入工业互联网络时，攻击者有机会通过物理方式或者远程接入互联的设备，对设备当中存储的数据进行读取、修改等操作。存在着数据被恶意篡改、伪造等风险，数据处理算法和过程被破解，进而导致标识解析的注册数据、解析数据和日志被篡改。

在数据传输过程当中，有可能出现如下风险:

如果对数据没有进行有效的签名校验，在传输过程当中，攻击者可以对数据进行篡改，伪造数据，而数据传输双方都无从得知。会导致数据应有方使用错误的数据，带来不可预知的风险。

通过对数据传输过程的数据伪造和篡改，攻击者可以实现中间人攻击。伪造数据发送方的身份，给数据接收方提供伪造的数据和身份信息，导致接收方进行错误的数据处理，

进而导致错误的业务行为，带来严重的业务风险。

4.3.2.3 隐私数据泄露

在标识数据使用过程中，在没有有效的安全防护措施的情况下，很容易导致工业企业关键设备数据、产品数据、管理数据、客户数据等隐私数据的泄露，而泄露的隐私数据会给不法分子带来可乘之机，经过标识的工业数据具有识别和路由信息，以此为跳板，进而会泄露企业更大范围的核心数据。一方面数据的泄露给网络攻击提供了入口，工业企业运行所需的各类网络设备、主机、服务器等设备被攻克后，企业内部信息堡垒将会被逐个攻破；另一方面重要数据泄露带来重大损失，在国家重要领域，核心保密工业工艺、设计流程等数据泄露的情况下，很可能会给企业乃至国家带来不可估量的损失。

4.3.2.4 数据丢失

在标识数据使用过程中，如果没有安全的保护措施和合理的备份情况下，不法分子通过对缓存或代理服务器进行攻击获取了权限后恶意删除数据，服务器遇到自然灾害造成数据丢失，操作人员误删数据，导致工业企业关键设备数据、关键产品数据、用户数据等重要数据丢失并无法恢复，对工业企业造成巨大的损失。

- **内部人员风险**

由于缺乏相关分类分级及审批流程制度，导致相关人员（管理人员、运营人员、运维人员等）能够在该流程的操作过程中接触到非权限范围内的数据与设备，调用权限之外的接口与功能，从而删除数据或服务系统重要文件，造成数据不可恢复或不可用，从而无法正常提供服务。

- **设备异常**

由于相关设备采集设备发生异常断电、异常关机、高温损毁、组件不兼容等情况而导致相关数据丢失。

- **恶意攻击**

相关设备遭受内部或外部攻击，例如 DDoS、系统漏洞、协议漏洞、架构漏洞，导致服务器宕机、系统被恶意破坏、数据被恶意删除等后果，使得数据异常或丢失。

- **程序异常**

工业互联网标识解析系统在使用过程中发生异常，例如采集程序异常、网络异常、服务端数据存储异常导致数据丢失或不可用。

- **备份异常**

相关数据在备份、还原的操作过程中发生出现备份数据损坏、备份流程未执行、备份数据未进行完整性校验等情况，异致相关数据操作失败。

- **不可抗因素**

不可抗力是指不能预见、不能避免并不能克服的客观情

况。标识解析节点的建设者、运营者、维护中若没有建立完备的异地备份及恢复流程，发现该类情况会导致数据丢失、服务无法运行。

4.4 运营安全风险分析

4.4.1 运营风险概述

随着标识生态的形成，参与者角色不断丰富，规模不断扩大。用户体量和系统规模的持续壮大，给标识解析体系的运营带来新的挑战。来自内部与外部的风险，都将影响整个工业互联网标识解析体系的安全可控运营。

4.4.2 运营风险分析

运营风险管理起到对二级节点运营风险进行识别、衡量、监督、控制和报告的作用。运营风险主要存在于对物理和环境管理、访问控制、业务连续性、人员、分支机构以及流程等各方面的管理中。

4.4.2.1 物理环境管理风险

对标识解析体系运营所涉及的业务范围内的物理和环境方面的控制和管理不到位，可能会引起未授权的访问、损害和干扰。

评估标识解析体系运营各区域所需要安全级别要求，对不同的区域实施不同的安全控制措施，以确保需要保护的信息在安全的区域内受控。

4.4.2.2 访问控制风险

访问控制风险包括物理访问控制风险以及系统访问控制风险。

物理访问控制风险包括未授权的物理访问、强行进入等。对不同安全区域的物理环境实施不同的安全访问控制措施可以有效规避此类风险。

系统访问控制风险主要涉及：**1）用户的非授权登录、访问，**授权访问控制措施不严、访问权限设置不合理等。**2）对网络访问的授权和认证管控风险；3）对关键应用的访问控制风险。**对于这些访问控制策略的设置需考虑“最小权限”原则及身份认证要求等。

4.4.2.3 业务连续性管理风险

标识解析体系的运营过程中，意外（如事故）情况发生或其他类型灾难发生，可能导致服务业务中断或恶化，进而对机构运营产生负面影响。业务连续性计划的缺失或缺乏维护，设备、系统、数据和重要信息等备份策略是否科学，同样可能将业务中断的潜在可能性提高。

4.4.2.4 人员管理风险

标识解析体系的运营具有高可靠性和高安全性的要求，所有有权使用或控制那些可能影响标识分配、标识解析、业

务管理、数据管理等操作的员工、第三方服务人员等（统称“人员”）都会影响系统的正常运营，统称为可信角色。

- **角色鉴别风险**

对于将要成为可信角色的人员，需进行严格、合理的角色鉴别，确保其能够满足所从事工作职责的要求。角色鉴别风险包括对人员物理身份的真实性和可靠性的识别与鉴别风险，及更进一步的背景调查中存在的风险，如不同角色的背景要求以及背景调查的开展、人员与相应角色可信要求的匹配度评估等。

- **关键岗位角色管理风险**

针对标识服务运营中的关键岗位角色，需进行合理的角色管理控制，确保角色职责权限清晰可控。关键岗位角色管理风险存在于可信角色必要的背景调查、培训、考核、离退等机制，后续的跟踪、评估和培训制度，以及对关键岗位角色之间的权限分离等机制中。

- **人员操作风险**

针对标识服务中的敏感操作，需建立、维护和执行严格的人员操作控制流程，确保某些敏感操作由多名可信人员共同完成。人员操作风险包括人员的错误操作、越权操作、以及互相牵制、互相监督机制的缺失等。

- **人员控制风险**

即人员在任职前、中、后的管理控制风险，主要存在于

关键岗位角色入职前的背景调查程序、调查内容、调查方式，以及人员入职前的培训考核方式、业务工作能力评估和人员离职管理等方面。

4.4.2.5 分支机构管理风险分析

分支机构管理风险主要指在标识解析体系众多环节上提供相应标识服务的实体/机构的生命周期管理风险。

- **分支机构的授权风险**

包括对众多二级节点运营主体，以及负责面向包括二级节点在内的工业互联网应用场景提供软件、硬件产品及应用集成解决方案的技术提供方等机构的审核、评估和授权风险。

- **分支机构的运行风险**

包括直属类型分支机构的运营管理基础设施及运行维护能力风险,以及代替主体机构所提供服务的服务受理、系统运作和管理规范风险等。

- **分支机构的违约风险**

分支机构在提供服务时，违反与主体机构约定的客户服务内容或协议规定，从而影响服务的质量，引起客户投诉，可能进一步导致违规风险。

- **分支机构的服务终止风险**

分支机构作为代替主体机构提供服务的实体,存有相关运营服务运行的关键数据，分支机构服务的终止可能影响业

务承接和业务的连续性。

4.2.2.6 流程管理风险

系统的运营是由一系列业务流程所组成的集合，缺乏必要的业务流程管理，会导致运营人员在执行工作时，只是依据经验执行，具有较大的随意性，给系统运营带来风险。

- **业务流程管控风险**

由于业务流程涉及到业务层面的各个环节，环节越多，所涉及的部门和人员就越多，系统就越复杂，统一规划和管理就越难，任何一个业务流程脱节都会对整个运营产生影响。

- **二级节点管理风险**

主要包括二级节点申请流程管理风险，如对建设方案、业务规划方案、网络安全保障方案、服务承诺等的审核、评估和授权等，以及二级节点运行管理风险，如标识注册、监测及备案，以及安全数据上报和应急处置等。

5 标识解析安全风险技术演进趋势与产业推动展望

5.1 演进趋势

我国工业互联网标识解析建设刚刚起步，安全保障能力建设相关工作相对滞后，工业互联网标识解析体系正面临新的风险变化，存在诸多安全风险，突出表现在架构安全风险、身份安全风险、数据安全风险和运营安全风险四个方面。

标识解析架构安全风险。国际上目前存在 Handle、OID、DNS 等多种标识解析方案，但散而弱，并未成熟，对其协议安全性的考虑则更为滞后，在探索推进工业互联网标识解析系统的过程中应同步规划部署相应的安全措施，需考虑整体架构的安全和实际运行中与 DNS 系统的互联互通，当体系架构中的一层节点出现问题时，就会对整个架构的安全性产生一定程度的威胁，如节点可用性风险、节点之间协同风险、关键节点关联性风险等。以及面临的 DDOS、缓存感染、系统劫持等网络攻击。

标识解析身份安全风险。工业互联网标识解析身份安全风险主要包括人、机、物等标识解析系统中各种角色的身份风险。中国信息通信研究院曾对部分工业互联网平台进行了安全评估，发现用户口令、身份认证、通信加密等方面均存在大量安全问题。工业互联网标识解析身份安全仍面临多种风险威胁，如身份认证安全和访问控制安全，用户客户端安全和标识解析服务器身份的真实性核验，身份认证在不同层级间的节点互信、标识源的真实性验证、用户终端与标识解析节点间的互信等方面都存在被窃听或攻击的风险。

标识解析数据安全风险。工业互联网数据种类多样，涉及标识注册数据、标识解析数据和日志数据等，在工业互联网标识数据的采集、传输、存储、使用和销毁等全生命周期流转中数据流动方向和路径复杂，暴露面多且复杂。工业互

联网标识的解析数据可能存在于顶级节点、二级节点、企业节点和业务终端等各个环节，离散的数据保护措施无法支撑数据全生命周期数据保护，需要全面考虑数据窃取、数据篡改、数据丢失或泄露至境外等各种风险。

标识解析运营安全风险。运营风险主要存在物理和环境管理、访问控制、业务连续性管理、人员管理、分支机构管理以及流程管理中。当前，工业互联网安全标准体系尚未健全，安全接入、数据保护、平台防护等方面的标准尚未出台，同时工业企业普遍存在重发展轻安全的情况，对工业互联网安全缺乏足够认识，企业运营方面仍存在关键岗位角色监管不严格、人员管理机制不健全、越权访问、伪造标识分支机构等诸多安全风险。

5.2 产业推动展望

立足于我国工业互联网标识解析存在的架构风险、身份风险、数据风险和运营风险，以及政策标准体系不完善、安全保障能力弱、节点接入安全授权与可信认证缺失等安全问题现状，未来标识解析安全工作将主要围绕以下几个方面进行推动。

一、提早布局。加强核心技术创新研究，重点突破标识解析安全核心技术的研究，将更多的安全因素纳入标识解析体系框架设计中，在标识解析体系建设初级从根源上把控风险，防范于未然；加快推进安全风险预警和态势感知平台建

设，提升标识解析体系安全防御能力。

二、全面分析。加快推进标识解析安全风险分析模型、标识解析节点安全接入认证、标识解析体系安全防护等报告的研究、发布；强化工业互联网标识解析安全创新成果转化和产业发展力度，推动产业快速发展。

三、逐项突破。在认证、加密、隐私等重点方向开展技术验证；逐步推广使用国产密码算法和符合国家密码管理部门规定的安全认证产品对标识解析的开放式协议架构进行加固；推动科研院所和高校等设立重点实验室，积极探索人工智能、区块链、零信任、大数据等新技术在标识解析安全防护能力建设中的创新应用。

四、重视标准。积极开展标识解析安全体系标准和安全运营规范等方面的研究制定工作，加快推动标识解析节点接入认证、解析体系安全防护、安全管理等标准研究工作。

五、人才培养。强化工业互联网标识解析安全人才培养，加强安全宣传教育，鼓励企业和高校安全专家在智能+学院、专题会议等重要活动中发表主题演讲。建议高等院校、科研机构和安全企业建立人才联合培养机制，加快推进复合型安全人才的培养和选拔，依托工业互联网产业联盟平台，组织开展技能大赛等活动，提升工业互联网标识解析安全从业人员的技能水平。

六、协同推进。针对工业互联网标识解析安全可能存在

的风险，中国信通院在国家顶级节点建设中围绕安全风险防控已经采取了一些手段措施。但仅凭借单一或部分力量很难构建标识解析安全产业生态，需要产业各界积极参与，投入更多的人力、物力。同时调动政产学研用的积极性，发挥产业与技术优势，群策群力、找准位置、形成合力，推动技术共享合作纵深发展，共建工业互联网标识解析安全产业生态。

6 小结

本报告主要针对工业互联网标识解析体系可能存在的安全风险进行了深入的分析研究，并从风险分析、风险管理、风险措施三个视角综合分析后，构建了统一的标识解析安全风险分析模型。但任何新生技术体系都需要一个不断完善的过程，不仅关乎技术本身，还涉及使用者如何驾驭这种技术。

为最大限度的减少工业互联网标识解析体系安全隐患，构筑标识解析安全产业生态，后续研究将针对现有安全风险分析模型进行持续滚动研究，适时开展相应的标识解析体系安全防护、标识解析节点安全接入认证、基于国密算法的标识数据安全加密、标识解析安全技术标准和安全运营规范等方面的研究工作。同时呼吁产业各界更加关注、多投入标识解析安全发展，发挥产业和技术优势，加强交流合作与资源共享，共同构建标识解析安全防护整体框架，持续优化工业互联网标识解析安全环境和产业生态。

联系我们

工业互联网产业联盟 秘书处

地址：北京市海淀区花园北路52号，100191

电话：010-62305887

邮箱：aii@caict.ac.cn

网址：http://www.aii-alliance.org