工业互联网标识解析安全白皮书（2020）

工业互联网安全系列研究报告

国家工业信息安全发展研究中心
CHINA INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

NISIA
工业信息安全产业发展联盟
National Industrial Security Industry Alliance

版权申明

本白皮书版权属于国家工业信息安全发展研究中心和工业信息安全产业发展联盟，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或观点的，应注明“来源：国家工业信息安全发展研究中心和工业信息安全产业发展联盟”。违反上述声明者，将追究其相关法律责任。

国家工业信息安全发展研究中心

序

国家工业信息安全发展研究中心（工业和信息化部电子第一研究所）简称国家工信安全中心，是工业和信息化部直属事业单位，是我国工业领域国家级信息安全研究与推进机构。为加快推进工业信息安全技术研发和保障能力建设，更好地推动工业信息安全事业发展，国家工信安全中心于2018年9月成立保障技术所。

自成立以来，保障技术所始终坚持贯彻落实总体国家安全观，以护航制造强国和网络强国建设为重点，围绕新一代信息技术与制造业融合带来的安全需求，以“风险可发现、可防范、可处置”为保障目标，面向工业控制系统、工业互联网、工业云、工业大数据、新一代信息技术等领域开展核心安全技术攻关，2018年以来承担40余个工控安全、工业互联网安全专项和重大课题，构建保障技术平台和专业技术力量，有力支撑主管部门完成工控安全、工业互联网安全等相关监督指导工作，帮助工业互联网企业提升安全保障能力。保障技术所建立了扎实的技术与服务能力，包括工业信息安全技术保障平台建设、工业信息安全实验室建设支撑、工业互联网安全技术服务与咨询、工业互联网数据安全监测与防护、工业数据安全交换共享、工业互联网标识解析建设与安全认证、标准研究与对标评估、安全评估评测等。

保障技术所联合业界单位，推出了《工业互联网平台安全》《工业互联网边缘计算安全》《工业互联网标识解析安全》《工业互联网数据安全》等系列白皮书，可为业界开展工业互联网安全相关工作提供参考。由于成稿仓促，加之水平有限，报告中难免有疏漏和错误之处，恳请批评指正。在此对于给予白皮书编制和发布等提供指导、支持、帮助的单位和个人一并表达感谢。

编写组

2020年12月

国家工业信息安全发展研究中心

白皮书编写说明

工业互联网标识解析是工业互联网的重要网络基础设施，为工业设备、机器、物料、零部件和产品提供编码、注册与解析服务，并通过标识实现对异主、异地、异构信息的互联互通、安全共享及智能关联，是实现工业互联网快速发展的重要基石。我国高度重视工业互联网标识解析自主可控发展，积极建设国际根节点、国家顶级节点与二级节点。国家陆续印发《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》、《工业互联网发展行动计划（2018-2020年）》、《工业互联网网络建设及推广指南》等系列文件指导工业互联网标识解析建设，并同步强调安全保障能力，2019年工信部发布《关于加强工业互联网安全工作的指导意见》，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，确保标识解析系统安全运行。

随着工业互联网的快速发展，工业互联网标识数量将数以千亿计，并发解析请求可达千万量级，如此大量级的标识解析服务需求对安全保障能力提出了非常高的要求，标识解析安全是工业互联网安全的重要建设内容。为了保证工业互联网的稳定运行，标识解析系统中的数据在传递过程中需提供完整性和一致性保护，对于敏感数据，还需提供机密性和隐私性保护，对于标识解析系统数据的更新，还需具备数据源认证能力以及对标识解析数据的访问控制能力。亟需综合各类安全技术对标识解析的开放式架构与协议进行加固改造，加强

对工业互联网标识解析服务节点的规模化跨域认证和标识数据、服务的信息保护，支持工业互联网标识解析业务单位身份管理、访问控制、安全认证、安全防护功能以及保障工业互联网标识解析节点批量接入认证能力。实现对标识的隐私保护、源认证、可查询性、数据完整性校验、密钥管理等能力，支持对标识解析请求端的基于身份、属性等方式的细粒度访问控制等能力，提升标识解析的安全性。

在这样的背景下，国家工业信息安全发展研究中心会同工业信息安全产业发展联盟组织编写了《工业互联网标识解析安全白皮书（2020）》，希望提高业界对工业互联网标识解析安全风险及相关防护技术的重视和共识，以推动工业互联网标识解析安全发展，为工业互联网健康发展保驾护航。

白皮书主要分为五个部分。第一部分为概述，主要介绍典型的标识解析技术、工业互联网标识解析的政策支持情况以及整体建设情况。第二部分介绍了工业互联网标识解析安全现状及建设意义。第三部分描述了工业互联网标识解析的安全特征和安全挑战。第四部分提出了工业互联网标识解析安全框架，以标识解析流程为主线，从防护对象、安全角色、脆弱性与威胁、防护措施以及安全管理等视角进行介绍，此框架全面梳理了工业互联网标识解析安全的各方面内容，可对安全保障能力建设提供参考。第五部分分析了工业互联网标识解析安全所涉及的关键技术。第六部分对工业互联网标识解析安全进行了展望。

编写组

主编: 陈雪鸿、李俊

编写单位和成员:

国家工业信息安全发展研究中心	王冲华、余果、周昊、樊佩茹、林晨、李红飞、刘东东、张雪莹、李耀兵、杨帅锋、王允成、江浩、张莹
杭州海康威视数字技术股份有限公司	王滨、王星
中国科学院信息工程研究所	熊刚、苟高鹏
深圳奥联信息安全技术有限公司	程朝辉、蔡先勇
广州大学	殷丽华、李超
亚信科技(成都)有限公司	刘东红、吴天飞
奇安信集团	王弢、崔君荣
北京电子科技学院	姚栋、阎亚龙、赵洪
北京三未信安科技发展有限公司	高志权、高嵩
北京炼石网络技术有限公司	白小勇、岳小杰
航天信息股份有限公司	宁红宙、王永宝
任子行网络技术股份有限公司	沈智杰
鹏城实验室	乔延臣

国家工业信息安全发展研究中心

哈尔滨工业大学（威海）	王佰玲、刘扬
威海天之卫网络空间安全科技有限公司	刘红日、孙云霄
北京天融信网络安全技术有限公司	张超
北京亚鸿世纪科技发展有限公司	古元
大唐微电子技术有限公司	王勇、贾小勇
阿里云计算有限公司	郑景鑫、宋林健
北京邮电大学	谢人超、黄韬
北京交通大学	陶耀东
中国电子科技网络信息安全有限公司	滕斌、曹国江
北京天地和兴科技有限公司	宋晓龙
中国移动通信集团山东有限公司威海分公司	战明明、姜成恒
杭州安恒信息技术股份有限公司	冀宗玉
博智安全科技股份有限公司	傅涛、郑轶
中国电子技术标准化研究院	陈勇、刘小慧

目录
CONTENTS

一、工业互联网标识解析概述 …… 1

（一）工业互联网标识解析体系架构 …… 1

（二）典型标识解析技术 …… 3

（三）我国工业互联网标识解析政策支持情况 …… 7

（四）我国工业互联网标识解析整体建设情况 …… 9

（五）研究内容和范畴 …… 10

二、工业互联网标识解析安全现状与建设意义 …… 12

（一）主流标识解析框架安全防护能力分析 …… 13

（二）工业互联网标识解析安全保障能力建设意义 …… 15

三、工业互联网标识解析安全需求特征和挑战 …… 17

（一）工业互联网标识解析安全需求特征 …… 18

（二）工业互联网标识解析安全挑战 …… 22

四、工业互联网标识解析安全框架 …… 26

（一）业务流程视角 …… 27

（二）防护对象视角 …… 27

（三）安全角色视角 …… 29

（四）脆弱性与威胁视角 …… 30

（五）防护措施视角 …… 35

（六）安全管理视角 …… 41

国家工业信息安全发展研究中心

五、工业互联网标识解析安全关键技术 43
（一）标识解析建设安全 44
（二）标识解析国密融合 45
（三）标识解析安全接入 45
（四）标识解析访问控制 47
（五）标识解析数据治理 47
（六）标识解析威胁检测 49
（七）标识解析网络测量 49
（八）标识解析监测审计 50
（九）标识解析安全编排 51
（十）标识解析安全代理 51
（十一）标识解析云化安全 52
六、工业互联网标识解析安全发展展望 53
（一）围绕安全运营、顶层设计、政策指导、标准引领等方面建立健全工业互联网标识解析安全管理机制 53
（二）从完整性、健壮性、服务质量等方面加快提升工业互联网标识解析安全评估能力 54
（三）着眼统一整体与各层细节等角度建设工业互联网标识解析安全风险监测体系 55
（四）着力安全技术新应用、新技术赋能标识解析安全、标识解析助力工业互联网安全等方向推进工业互联网标识解析安全技术创新 55
（五）从人才培养、产业链协同、生态创新等方面促进工业互联网标识解析安全产业创新发展 57

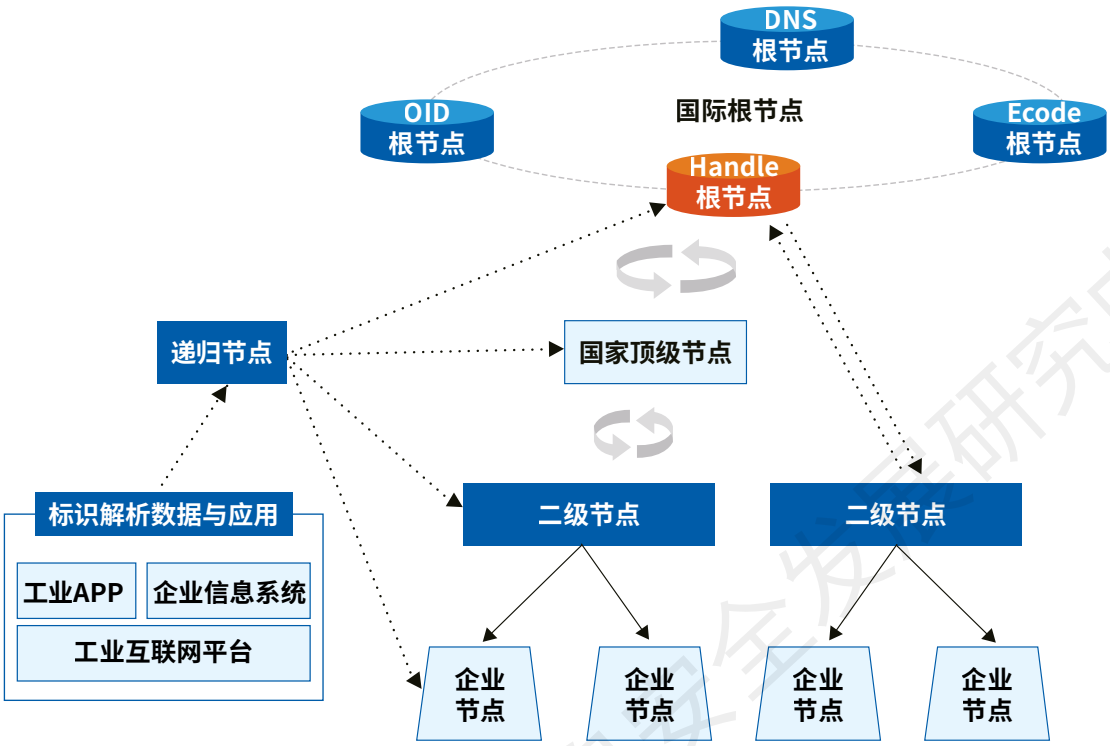
一、工业互联网标识解析概述

工业互联网标识解析是工业互联网实现全要素互联互通的重要网络基础设施，为工业设备、机器、零部件和产品提供编码、注册与解析服务，是平台、网络、设备、控制、数据等工业互联网关键要素实现协同的“纽带”。类似域名解析系统DNS之于互联网，工业互联网标识解析是工业互联网的神经中枢，是整个网络互联互通、资源调度、生产协调的重要基础设施。然而，工业互联网的发展对标识解析提出更高的要求。一方面标识的对象更为广阔。随着工业互联网的发展，需要标识的对象已从以往的域名，延伸到一个身份、一个零部件、一个产品、一个作品、一个交易、一个服务等更为具体、更为广阔的对象。另一方面信息的管理更为复杂多变。由于工业互联网中对象的多样性，使得标识相对应的信息结构更加复杂多变，因此标识层的信息管理需要扩展以支持数据安全交互与安全共享。

（一）工业互联网标识解析体系架构

目前全球存在多种标识解析技术，我国工业互联网标识解析体系采用以DOA技术为核心、兼容Handle、OID、Ecode、GS1等主流标识技术的融合型方案，其架构由国际根节点、国家顶级节点、二级节点、企业节点和递归节点等要素组成。其中，**国际根节点**是指标识解析体系的最高层级服务节点，一方面不限于特定国家或地区提供面向全球范围公共的根层级的标识服务，另一方面面向国内不同层级节点提供数据同步与注册解析等服务。**国家顶级节点**是指一个国家或地区内部的顶级节点，其与国际根节点及二级节点连接，面向全国范围提供顶级标识解析服务。**二级节点**是面向特定行业或者多个行业提供标识服务的公共节点，负责为工业企业分配标识编码及提供标识注册、标识解析、标识数据服务等，其分为行业二级节点和综合类二级节点两种类型。**企业节点**是指一个企业内部的标识服务节点，能够面向特定企业提供标识注册、标识解析服务、标识数据服务等，并与二级节点连接。**递归节点**指标识解析体系的关键性入口设施，负责对标识解析过程中的解析数据进行缓存等操作，减小解析数据处理量，提高解析服务效率。我国工业互联网标识解析整体架构如下图1所示。

图1. 工业互联网标识解析体系架构



（二）典型标识解析技术

目前，国内外现存多种标识解析技术，根据其演进方式可分为DNS域名解析技术、基于改良路径的标识解析技术、基于革新路径的标识解析技术三类。

1.DNS域名解析技术

DNS标识解析是一种分布式网络目录服务，主要用于将服务器名称和IP地址进行关联，实现域名与IP地址的相互转换。域名系统定义了网络设备的命名语法和规范，以利于通过名称委派域名权限，通过使用DNS的命名方式来为遍布全球的网络设备分配域名。

DNS采用层次树状命名方法，不同层次之间用点“.”分隔：主机名.次级域名.顶级域名.根域名，每一个域名服务器只对域名体系中的一部分进行管辖，采用递归或迭代的查询方式提供解析服务，广泛应用于Web和电子邮件等应用之中。域名与地址管理机构ICANN具有域名系统管理、IP地址分配、协议参数配置以及主服务器系统管理等职能，现由IANA和其他实体与美国政府约定管理。中国互联网络信息中心CNNIC是我国域名注册管理机构和域名根服务器运行机构，负责运行和管理国家顶级域名.CN、中文域名系统，提供域名注册、域名解析和WHOIS查询等服务。

2.基于改良路径的标识解析技术

基于改良路径的标识解析技术通过对现有DNS架构进行扩充，以DNS上层应用的形式提供工业互联网标识解析服务。典型的架构包括：对象标识符（Object Identifier，OID）技术、产品电子代码（Electronic Product Code，EPC）技术、物联网统一标识（Entity code for IOT，Ecode）技术等。

OID标识解析由ISO/IEC与ITU-T国际标准化组织于上世纪80年代联合提出，采用分层树形结构，其编码由一系列数字、字符或符号组成，层数无限制，支持对用户、网络服务及其它物理或逻辑对象等进行唯一命名。其解析系统采用递归解析方式，需依托DNS，通过域名与名称权威指针（Naming Authority Pointer，NAPTR）记录完成解析操

作。在安全方面，解析客户端可以选择是否使用DNSSEC，目前未提供其它安全保障方案。OID技术已在信息安全、医疗卫生、网络管理等领域有应用实践。

EPC技术于1999年由美国麻省理工学院Auto-ID中心（现为EPCglobal，属于GS1组织）首次提出，EPC标签数据标准（TDS）规定了其数据格式与编码方案。EPC解析系统采用迭代解析方式，同样依托DNS，通过NAPTR记录完成解析。EPC系统主要从EPC、EPC标签和读取器、服务发现、网络信息四个方面增强其安全性。EPCglobal在中国的分支机构由中国物品编码中心负责成立，为国际EPCglobal系统成员提供服务，负责制定EPC物联网标准以及EPC码在中国的分配与管理。

Ecode技术由中国物品编码中心主导、中国自主研发，编码为层次编码结构，由多段数字组成，可用于标识物联网对象。采用迭代解析方式，依托DNS，通过NAPTR记录提供解析服务。在安全方面，除使用DNS安全增强外，Ecode编码中含校验码。目前，该标识技术已在产品追溯查询、防伪验证、产品营销等领域有应用实践。

总体而言，基于改良路径的系统便于实现且部署较快，仅需在现有的DNS架构上进行扩展便可提供解析服务。但将其应用于工业互联网场景会使得大量请求涌入DNS服务，可能导致DNS系统过载，对DNS系统的正常运行造成影响。

3.基于革新路径的标识解析技术

基于革新路径的标识解析技术不依托于DNS，而是直接基于TCP协议或UDP协议进行服务的新型标识技术，如数字对象标识解析技术（DOA/Handle）、泛在识别技术（Ubiquitous ID，UID）。

DOA/Handle技术是基于数字对象理念的下一代全球分布式标识服务与数据管理体系框架，由互联网之父Robert Kahn于1994年提出，目前由DONA基金会维护。Handle标识解析体系能够为网络中的数字对象提供永久标识、动态链接和数据安全治理等基础服务。Handle具有全球唯一两段式结构码，即全球统一管理的Handle前缀和自定义编码（后缀），这两部分用“/”分隔，其可兼容OID、Ecode、GS1、DNS、UID等标识技术。Handle具有独立解析体系，标识解析系统由国际并联根节点（GHR）、辅根节点（ARS）、行业节点（LHS1）、下级的各授权节点（LHSn）、缓存/递归解析服务节点等组成，可作为现有互联网的扩展、并与其完全兼容，从Handle编码解析到信息所在服务器或设备的IP地址，最后解析到具体信息。在安全方面，Handle具有部分内嵌的安全机制，能够自主管理信息、访问权限及用户身份等，保证信息的安全与可控，具备用户数据主权保护能力，不依赖于任何平台、系统、数据库。目前中国部署有自主可控的全球Handle根节点及下级节点网络体

系，由国家工业信息安全发展研究中心（CIC）牵头的“MPA中国联合体”全权负责管理和运营，Handle技术在国内已经成功应用在产品溯源、供应链管理、智慧城市、工业互联网等领域。

UID技术通过泛在标识编码（ucode）标识客观实体、空间、地址、概念等物理或逻辑对象，并通过关系模型为ucode间建立关联。命名空间采用分层结构进行管理，由顶级域和二级域两层组成，每个编码长度固定，由版本、顶级域代码、类代码、二级域代码和标识码5个字段组成。ucode采用递归解析方式，其解析系统由关系数据库节点、关系数据库前端、关系词汇引擎和信息服务4个核心组件组成。该技术主要应用于日本实时操作系统内核项目，为场所和物品植入的IC电子标签分配唯一的标识编码。

基于革新路径的系统一方面弥补了现有DNS技术安全设计上的部分缺陷，另一方面其服务较为轻便，更契合工业互联网场景。然而革新路径难以利用现有基础设施，需重新部署，所以建设成本较高、周期较长。

（三）我国工业互联网标识解析政策支持情况

工业互联网标识解析体系建设是我国工业互联网建设的重要任务，我国积极推进标识解析国际根节点、辅根节点、国家顶级节点、二级节点建设，同时高度重视安全保障能力建设。2017年，国务院发布《关于深化“互联网+先

进制造业”发展工业互联网的指导意见》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”，“构建标识解析服务体系，支持各级标识解析节点和公共递归解析节点建设”，明确指出“重点突破标识解析系统安全”。各地方也将标识解析体系建设作为落实工业互联网创新发展战略、加快数字化转型的重要抓手。2018年，工业和信息化部设立了工业互联网专项工作组并印发《工业互联网发展行动计划（2018-2020年）》提出以供给侧结构性改革为主线，以全面支撑制造强国和网络强国建设为目标，着力建设先进网络基础设施，打造标识解析体系，发展工业互联网平台体系，同步提升安全保障能力，突破核心技术。2019年1月，工信部发布《工业互联网网络建设及推广指南》提出在2020年初步构建工业互联网标识解析体系，建设一批面向行业或区域的标识解析二级节点以及公共递归节点，制定并完善标识注册和解析等管理办法，标识注册量超过20亿。2019年8月，工信部等十部门发布《加强工业互联网安全工作指导意见》，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；地方通信管理局监管本行政区域内标识解析系统、公共工业互联网平台等的安全工作。2019年12月工信部发布《工业互联网企业网络安全分类分级指南（试行）》将工业

互联网企业分为三类，其中标识解析系统建设运营机构是主要的工业互联网基础设施运营企业。2020年3月工信部发布《关于推动工业互联网加快发展的通知》将增强完善工业互联网标识体系作为加快新型基础设施建设的四大方向之一，将标识解析等新技术的应用纳入企业上云政策支持范围。

（四）我国工业互联网标识解析整体建设情况

根节点建设方面，2014年，国家工业信息安全发展研究中心-北京中数创新-北京西恩多纳（CIC-CDI-CHC）联合体成为首个全球MPA（Handle标识解析全球根节点所在国家管理机构），可自主行使Handle资源顶级管理权限，负责推进部署中国的Handle全球根节点管理、建设、运营和应用推广等工作。我国同步推进基于Handle、OID等多种标识解析技术的工业互联网标识解析国际根节点建设。2019年10月，DONA理事会2019年会和第六届国际根节点MPA协调组会议在北京召开，来自美国、中国、德国、英国、沙特和ITU（国际电信联盟）等的各国MPA代表出席，从会议了解，其他MPA国家的标识解析应用到工业互联网的较少，与其他国家相比，我国工业互联网标识解析建设起步较早，推广应用度最高。

顶级节点建设方面，2018年底，北京、上海、广州、武汉、重庆等地市政府与相关单位签署合作协议，共同推动工业互联网标识解析体系顶级节点建设工作，融合

Handle、DNS、OID、Ecode等多种标识解析方案，并同步开展了多个典型行业二级节点和行业应用示范。2019年10月由国家工业信息安全发展研究中心主办的国际DOA技术应用论坛在北京召开，论坛开幕式上举行了“工业互联网根顶对接和Handle二级节点启动建设仪式”，标志Handle标识解析**国际根节点与国家顶级节点的对接**迈向新的阶段。目前，五个国家顶级节点与Handle国际根节点、OID国际标识体系等已经实现互联互通，可与国际工业互联网标识解析体系接轨。

二级节点与企业节点方面，截至2020年10月，我国已上线运行工业互联网标识解析二级节点75个，覆盖航天装备、建筑材料、食品、装备制造、工业配件、船舶制造、定制家居等20多个行业以及综合行业，标识注册量突破73亿，接入企业超过6500家，工业互联网标识解析生态初显。国家工业信息安全发展研究中心连续两年对Handle服务节点状况进行应用及安全状况评估，监测数据显示，2020年初我国Handle运行节点达172个，同比去年年初增加5倍。

（五）研究内容和范畴

本白皮书立足工业互联网标识解析在海量数据管理、服务质量保障、跨域访问管控、多标识体系兼容、安全机制扩展等方面的安全需求特征，分析当前标识解析面临的安全挑战。以标识解析业务流程视角为主线，从防护对象、安全角

色、脆弱性与威胁、防护措施以及安全管理等视角出发，明确防护对象，厘清安全角色，针对架构、协议、身份、数据、运营、应用六个方面分析工业互联网标识解析体系脆弱性与威胁，梳理安全防护措施，提出工业互联网标识解析安全框架。最后，针对工业互联网标识解析安全现状及面临的风险，汇编总结标识解析安全关键技术，展望标识解析安全发展路径。

国家工业信息安全发展研究中心

二、工业互联网标识解析安全现状与建设意义

工业互联网推动当前以“人与人”连接为核心的互联网走向“人-机-物”全面互联，极大扩展了网络空间的边界和功能，打破了工业控制系统传统的封闭格局，使工业互联网控制层、设备层、网络层、标识解析层、平台层等安全问题大量暴露出来，线上线下安全风险交织叠加放大，给安全防护能力建设带来了新的挑战。

国家工业信息安全发展研究中心发布的《2019年工业信息安全态势展望报告》显示，目前网络安全风险不断向工业领域转移，安全形势愈加复杂，风险日益加大，工业互联网正在成为网络安全的主战场。作为工业互联网的关键“纽带”，标识解析也将成为攻击的重点目标。DNS因其应用时间久、应用规模广，是当前标识体系安全事件频发的主要对象。工业互联网标识解析体系正处于高速发展，类似DNS之于互联网，工业互联网标识解析是工业互联网重要信息基础设施，其受攻击的影响范围更广，需保障其安全性。接连发生的乌克兰停电事件、美国Dyn公司域名系统瘫痪事件及“永恒之蓝”病毒肆虐全球已经为我们敲响警钟。

（一）主流标识解析框架安全防护能力分析

1.DNS安全防护能力分析

DNS协议在设计之初并未考虑太多安全因素，导致DNS服务的安全性在互联网环境日益复杂的当今备受挑战，面临劫持、隐私泄露、缓存投毒、中间人攻击、反射攻击等风险。

当前提出多种安全协议增强DNS安全。DNSSEC使用签名技术保证DNS报文完整性和真实性，作用于递归服务器与各级权威服务器之间。DoT和DoH对报文进行加密传输，作用于客户端与递归服务器之间，通过代理的方式将客户端的产生的DNS流量进行加密。根据IETF标准RFC7830，通过DNS数据填充，防止根据固定大小的DNS查询应答来推测DNS内容的隐私窃听。针对DNS协议无状态的特性，RFC 7873中提出了DNS Cookie技术，在DNS查询之前交换了Cookie，可以抵御常见的拒绝服务、放大、伪造和缓存投毒攻击。**当前DNS增强协议未得到广泛应用，且增强的DNS协议仍存在安全挑战。**

2.基于改良路径的标识解析安全防护能力分析

首先，基于改良路径的标识解析服务需要依托DNS提供，所以DNS系统本身的故障会导致其服务失败。其次，此类标识解析系统继承了DNS系统存在的已有安全问题，包括架构脆弱、易被缓存投毒、单点故障、负载过重和易被特殊权力机构绑架等。另外，其安全保障主要依赖于DNSSEC，

在数据源身份鉴别与完整性保护能力有所提升，但难以兼顾可用性，且仍存在数据泄露风险。此外，此类标识解析体系高度依赖DNS，大规模应用后会给现有DNS基础设施带来压力。

3.基于革新路径的标识解析安全防护能力分析

DOA/Handle技术体系可不依赖于DNS服务，定义权限认证机制，支持数据、访问权限、用户身份等自主管理，保证身份安全、数据安全与行为安全，具备较高的安全性与可靠性，具体体现在以下三方面：一是管理员与权限设计，为每个Handle标识设置一个或多个管理员，任何管理操作只能由拥有权限的Handle管理员执行，并在响应请求前进行身份验证与权限认证。二是客户端身份安全与操作合法，客户端发起解析和管理请求均需进行身份验证，Handle服务器会根据权限对客户端进行差异化解析，只响应客户端权限范围内的管理请求。三是服务器身份安全，客户端可以要求Handle服务器使用私钥对其响应进行签名，从而验证服务器身份。

UID体系从物理标签安全、接入与访问控制、通信安全、资源管理、安全更新等方面采取措施，加强其安全防护能力。

基于革新路径的标识解析体系能够较好地满足工业互联网标识解析在安全等方面的核心需求，但是**在海量标识数据治理、多主体身份认证、细粒度权限管控以及全流程安全等方面仍需加强。**

（二）工业互联网标识解析安全保障能力建设意义

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，日益成为新工业革命的关键支撑和深化“互联网+先进制造业”的重要基石，对未来工业发展产生全方位、深层次、革命性影响。作为工业互联网的重要网络基础设施，保障工业互联网标识解析安全具有重要意义。

1.标识解析安全是工业互联网安全的重要基础

工业互联网标识解析能够支撑工业数据流通和信息交互，支持工业互联网中设备、人、物料等的全生命周期管理，是打破信息孤岛、实现数据互操作、挖掘海量数据的基础。标识解析安全是工业互联网健康发展的前提和保障，一旦标识解析体系遭入侵或攻击，波及范围不仅是单个企业，更可延伸至其他工业互联网关键要素乃至整个工业互联网生态。做好标识解析安全保障工作**是确保工业互联网应用生态、工业互联网关键要素等安全的重要保证。**

2.可支撑提升工业互联网整体安全防护水平

标识解析体系可助力工业互联网安全保障能力建设。随着工业互联网标识解析的普及应用，在保障标识解析自身安全的同时，标识的不可篡改、不可伪造、全球唯一等安全属性优势逐渐凸显，标识可在数据可信采集、统一身份认证、安全接入认证、密码基础设施服务、恶意行为分析等方面赋能工

业互联网安全保障能力建设。**构建标识解析体系安全可推动工业互联网安全保障能力建设。**标识解析安全建设可作为应用示范，推动工业互联网整体安全建设，推行标识解析安全管理机制及技术标准可带动工业互联网整体安全管理与技术创新，标识解析安全体系构建有利于加快产业应用协调发展。

3.有助于推动工业互联网信息技术创新发展

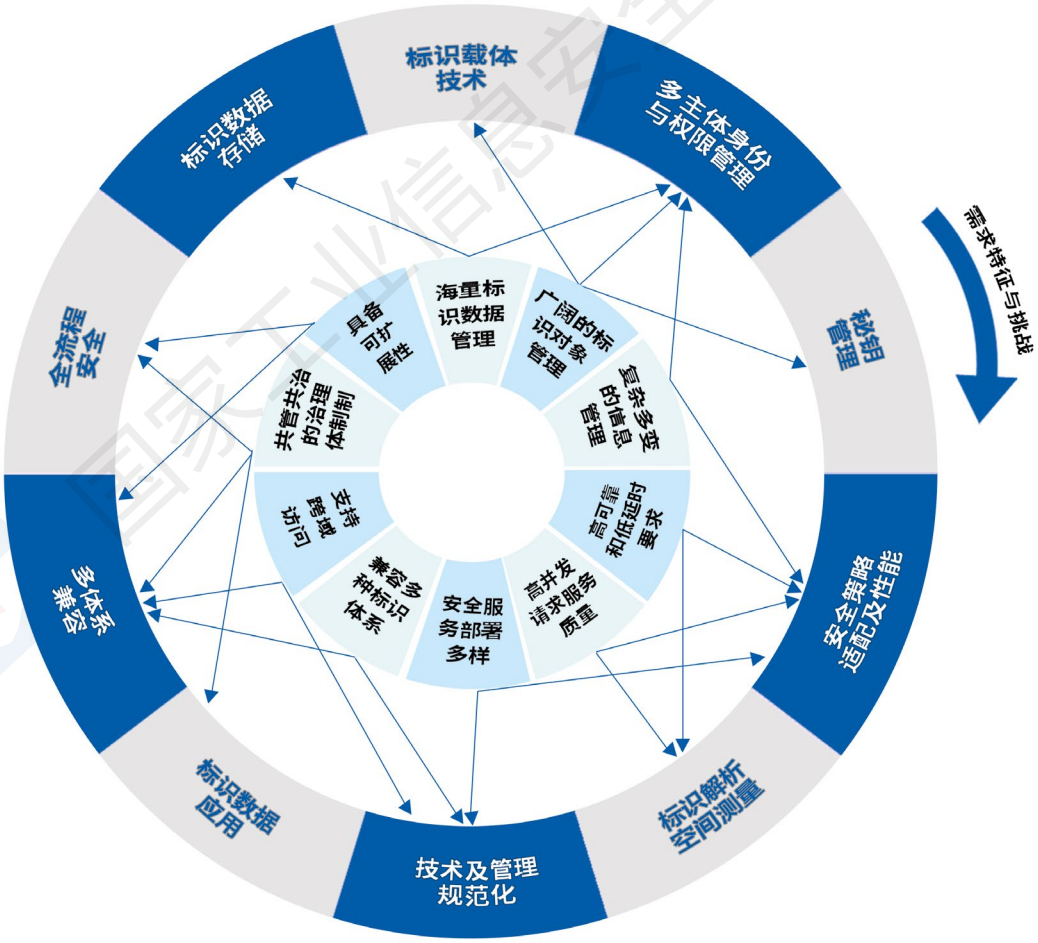
标识解析体系安全构建有利于提高工业互联网核心技术抗冲击能力，有利于把握工业互联网持续发展主动性，推动工业互联网其他核心技术在此基础上建立独立自主研发生态，提升工业互联网整体关键技术自主能力，摆脱技术的依赖性，提升我国工业互联网核心信息技术创新发展水平。

国家工业信息安全发展研究中心

三、工业互联网标识解析安全需求特征和挑战

工业互联网标识解析作为工业互联网数据交换与共享的重要基础，在海量数据管理、服务质量、多标识体系兼容等多方面具备其独有的需求特征，标识解析所特有的业务流程和实现架构也为安全需求的实现提出了新的挑战（如图2）。

图2. 工业互联网标识解析安全需求特征与挑战



（一）工业互联网标识解析安全需求特征

工业互联网标识解析是工业互联网的重要基础设施，类似DNS服务器，是攻击者的重要目标。与消费互联网和传统物联网不同，工业互联网的通信主体多样、对安全性要求更高，为了支撑标识解析安全防护能力，标识解析安全需要满足以下十大需求特征：

特征1：支持海量数据管理

工业互联网中标识解析包含海量工业设备、资源产生的海量标识数据，是传统互联网域名解析体系的百万倍甚至更大量级。需要提供多粒度、多权限的海量标识数据管理、轻量级的数据加密存储、高性能的数据安全检索、标识数据安全分类分级与隐私保护等能力。

特征2：保障高并发请求服务质量

工业互联网标识解析系统面向的用户广泛，在同一时间解析系统可能面对数以万计的标识解析请求，在解析的过程中需要保证数据的一致性，支持标识数据同时期的更新、修改、删除操作，保证高并发下稳定、可信的查询服务质量。需要提供标识数据的安全同步机制，实现数据的安全更新，并根据应用场景动态调整安全策略，降低安全保障机制对业务质量的影响。

特征3: 同时保障高可靠与低延时

工业互联网区别于传统消费互联网的一大重要特征是低延时，工业互联网的超时响应甚至未响应可能会影响生产安全甚至生命安全。需要提供低开销的身份验证和数据安全传输机制，并针对解析服务需求进行差异化服务，在保证标识解析服务低延时响应的同时保障服务的高可靠性。

特征4: 需兼容多种标识体系

当前工业互联网标识解析体系中兼容了多个标识解析体系，如DNS、Handle、OID等，需要协调各技术体系的安全防护能力，消除体系中的安全短板，实现兼容的安全、协同的安全、整体的安全。需要提供兼容不同标识协议的统一安全防护框架，依据不同的协议标准和服务需求，进行安全服务的灵活编排和动态部署，实现跨协议兼容的安全认证和统一认证，满足兼容系统的整体安全需求。

特征5: 支持广阔的标识对象管理

随着工业互联网的发展，需要标识的对象已从以往的域名，延伸到一个身份、一个零部件、一个交易、一个服务等更为具体、更为广阔的对象。需要提供标识身份验证和身份伪造监测、异构对象的权限访问控制、异常行为分析和操作行为审计等功能，对多类型的标识对象进行身份和权限的管理。

特征6: 共管共治的治理机制

作为支撑工业互联网应用的重要基础设施，工业互联网标识解析需要支持多主体参与、跨地域部署，实现多边共管共治的治理机制。我国工业互联网标识解析既需要支持网际兼容国际可互联互通，又需要保证在极端条件下网内自主可独立。需要实现自主可控的标识解析安全管理系统，设计不同主体、不同域间进行协调的安全标准接口。

特征7: 适用于复杂多变的信息管理

工业互联网对象多样，行政上来自不同的国家和地区，数据所有者错综复杂且实时变化，数据源包括物料、设备、网元、服务、操作员等，加上多标准、多协议、多命名格式共存，给对象的检索与管理带来巨大挑战。标识解析需要全面支持与对象标识相关的各类信息管理。需要实现异构标识数据统一管理、标识合法性检测、标识关联性分析和异常标识检测。

特征8: 解析安全服务部署方式多样

依据应用场景不同的解析服务需求和安全需求，工业互联网标识解析系统和标识解析安全服务需要以不同的形式部署，包含硬件部署、软硬件融合部署以及云化部署等多种形式，为系统的统一管控带来了挑战。需要提供标识解析服务和安全服务功能模块化精准划分方法、动态部署调配方

案，设计跨平台、跨系统的管控协议，实现多种部署方式的统一管控、联合管控。

特征9：支持跨域访问

工业互联网标识解析服务存在大量跨信任域的应用场景，对跨信任域的标识解析请求需要细粒度、轻量级、支持跨域访问的标识解析访问控制机制。需要提供统一的跨域安全认证平台，设计细粒度权限快速查验机制，实现跨行业、跨领域、跨解析协议的公认信任体系。

特征10：具备可扩展性

工业互联网标识解析服务应具备可扩展性。在架构层面，可根据实际需求进行扩充，保证该体系在未来海量数据及新增标识方案场景下依旧满足需求。在协议层面，应支持无缝添加其他新型标识解析协议子域。在系统层面，需保证系统扩展时命名空间可容纳未来海量数据接入，同时保证服务可靠和安全有效，设计多体系安全隔离的防护体系，在确保扩展性的同时，减少安全短板对整体系统安全的影响。

（二）工业互联网标识解析安全挑战

当前产业界以及学术界已经开始认识到工业互联网标识解析安全的重要性和价值，并开展了积极有益的探索，但是目前关于工业互联网标识解析安全的探索仍处于产业发展的初期，缺乏系统性的研究。针对上述安全需求，本白皮书就工业互联网标识解析环境中的多体系兼容、标识载体技术、多主体身份与权限管理、安全策略适配及性能、密钥管理、标识数据存储、标识数据应用、技术及管理规范化、全流程安全、标识解析空间测量等方面总结出当前工业互联网标识解析体系面临10个最主要的安全挑战。

挑战1：多体系兼容

在工业互联网标识解析体系中，由于多种标识编码体系并存，无法引入一种统一的模式支持不同的标识编码体系。在不改变现有标识编码体系协议设计的前提下，需要进行统筹考虑并设计安全机制，实现对标识解析安全防护能力的多标识体系兼容。

挑战2：标识载体技术

标识载体是承载标识编码资源的标签，需要主动或被动地与标识数据读写设备、标识解析服务节点、标识数据应用平台等发生通信交互。主动标识载体安全、被动标识防伪、载体标识数据安全更新等是保障标识解析数据安全的第一道关口，是工业互联网标识解析安全建设的重要挑战。

挑战3: 多主体身份与权限管理

工业互联网标识解析体系涉及众多领域，应用行业分布广泛，二级节点的运营服务机构较多，标识对象、标识用户海量，需要对身份及权限进行细颗粒度的管理，在身份可信、隐私数据保护、防止越权、防止非法操作技术实施上存在较大挑战。

挑战4: 安全策略适配及性能

工业互联网标识解析具有不同应用场景、应用特性、地域特性、行业特性，安全需求的动态特性明显，工业应用对数据采集的实时性、计算的效率、存储量、稳定性都有较高的要求。如何结合不同的应用场景来动态设置和快速调整、分派安全策略尚未明确，保障安全策略适配的同时不影响业务处理能力，兼顾高可靠与低时延、兼顾安全运营与高并发服务是安全建设需要解决的关键问题。

挑战5: 密钥管理

由于标识解析机制的灵活性和工业互联网应用的多样性，导致了数据的多样多源，随着业务场景动态变化，加上设备数量的快速扩展，传统的密钥管理方法难以适用于标识解析体系的密钥管理。在海量、多源、异构环境下，实现标识对象、用户、运营机构密钥的统一适配与管理存在挑战。

挑战6: 标识数据存储

标识数据海量、解析体系与存储架构多样性等特点，导致标识数据存储对软硬件可靠性、可用性要求很高。在分布式部署架构中，数据传输链路长，各节点安全性与数据同步安全性都需要保障，特别是对敏感信息的加密解密工作量巨大，保障数据安全性的同时兼顾系统性能存在挑战。

挑战7: 标识数据应用

从数据来源看，工业互联网标识解析数据的所有者众多且跨行业、跨地区，数据请求与操作量级大，各企业数据多标准、多协议、多命名格式共存，给对象的检索与理解难度极高。针对工业互联网标识解析流量的大数据分析，是推进工业互联网发展、焕发标识数据生命力的主要手段。然而当前工业企业数据安全问题突出，在大数据采集与分析过程中，保障数据主权及隐私安全，激发企业数据共享动力，是当前安全建设的一大挑战。

挑战8: 技术及管理规范化

规范化的技术及管理更有利于工业互联网解析应用的推广，现阶段标识解析技术较为碎片化，建设和管理依据不足，实现协议的标准化、安全机制的标准化、安全管理的体系化存在挑战。

国家工业信息安全发展研究中心

挑战9: 全流程安全

工业互联网标识解析体系在标识注册、节点接入、数据管理、解析查询的各个环节中存在端到端的数据流动，涉及数据的产生、采集、传输、存储、处理、销毁等全生命周期的安全问题，存在被恶意篡改、窃取等安全威胁。构建标识解析全流程的安全监测手段来摸清数据资产、梳理数据使用、管控数据风险等存在挑战。

挑战10: 标识解析空间测量

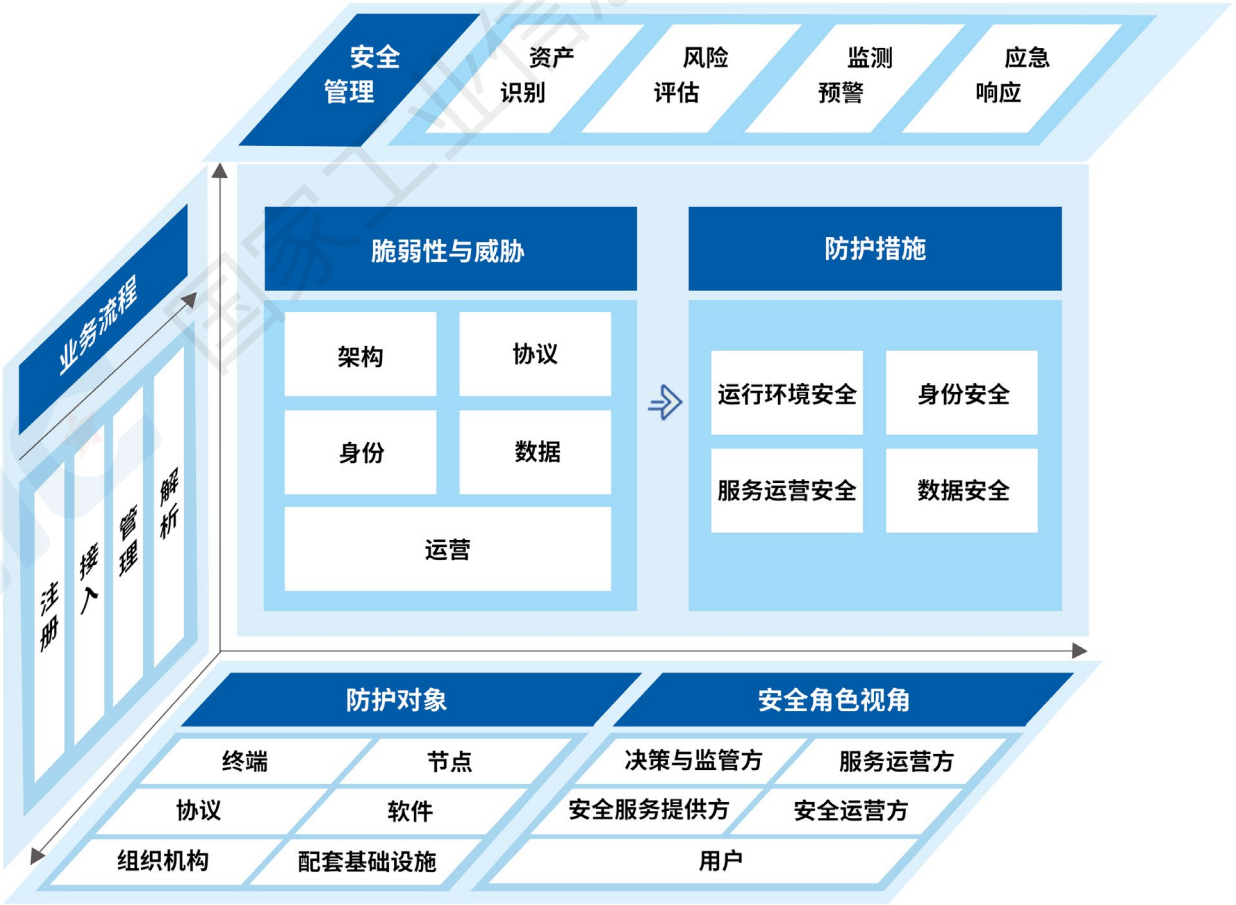
工业互联网标识解析空间测量旨在通过对实际标识解析网络的测量和运行状况的评估,建立基于测量的标识解析行为分析模型，为性能提升、系统优化设计与实施流量工程提供指导。而标识解析跨域、多类型、海量、异构的特点为标识解析空间测量带来挑战。

国家工业信息安全发展研究中心

四、工业互联网标识解析安全框架

工业互联网标识解析安全框架（如图3）以标识解析业务流程视角为主线，从防护对象、安全角色、脆弱性与威胁、防护措施以及安全管理等视角出发，明确防护对象，厘清安全角色，针对架构、协议、身份、数据、运营、应用六个方面分析工业互联网标识解析体系脆弱性与威胁，梳理保障运行环境、身份、服务运营以及数据四方面安全性的防护措施，从风险评估、监测预警、应急响应三个方面给出安全管理建议。

图3. 工业互联网标识解析安全框架



（一）业务流程视角

工业互联网标识解析业务流程主要包括注册、接入、管理和解析。

注册：指在标识解析系统中申请并获得标识编码的过程，包括节点注册（针对一段标识）、标识注册（针对单个标识）。在注册过程需要确认注册申请方、注册受理方身份，保障注册消息安全传输。

接入：指在标识解析系统中完成编码与解析数据配置的过程，包括节点接入、标识对象（具有联网解析功能的设备）接入。在接入过程需要确认新接入对象、接入点身份，保障接入配置消息安全传输。

管理：指在标识解析系统中对标识数据进行增加、删除、修改、查询的过程，包括数据更新、数据同步等。在管理过程需要确认管理操作者身份及权限合法，保障操作数据安全传输。

解析：指在标识解析系统中查询标识编码获得对应解析数据的过程，包括解析标识对应企业节点信息、解析标识对应属性值等。在解析过程需要确认解析请求方和解析服务提供方身份及权限合法，保障解析数据安全传输。

（二）防护对象视角

遵照工业互联网标识解析“注册、接入、管理、解析”的业务流程，工业互联网标识解析安全防护对象包括：终端、节点、协议、软件、组织机构以及配套基础设施。防护对象的范畴也是本白皮书研究的工业互联网标识解析安全边界，如图4所示。

终端：标识载体及客户端。

节点：包括标识解析根节点、顶级节点、二级节点、递归节点及企业节点服务器。

协议：标识注册、解析、安全保障过程中使用的相关通信协议。

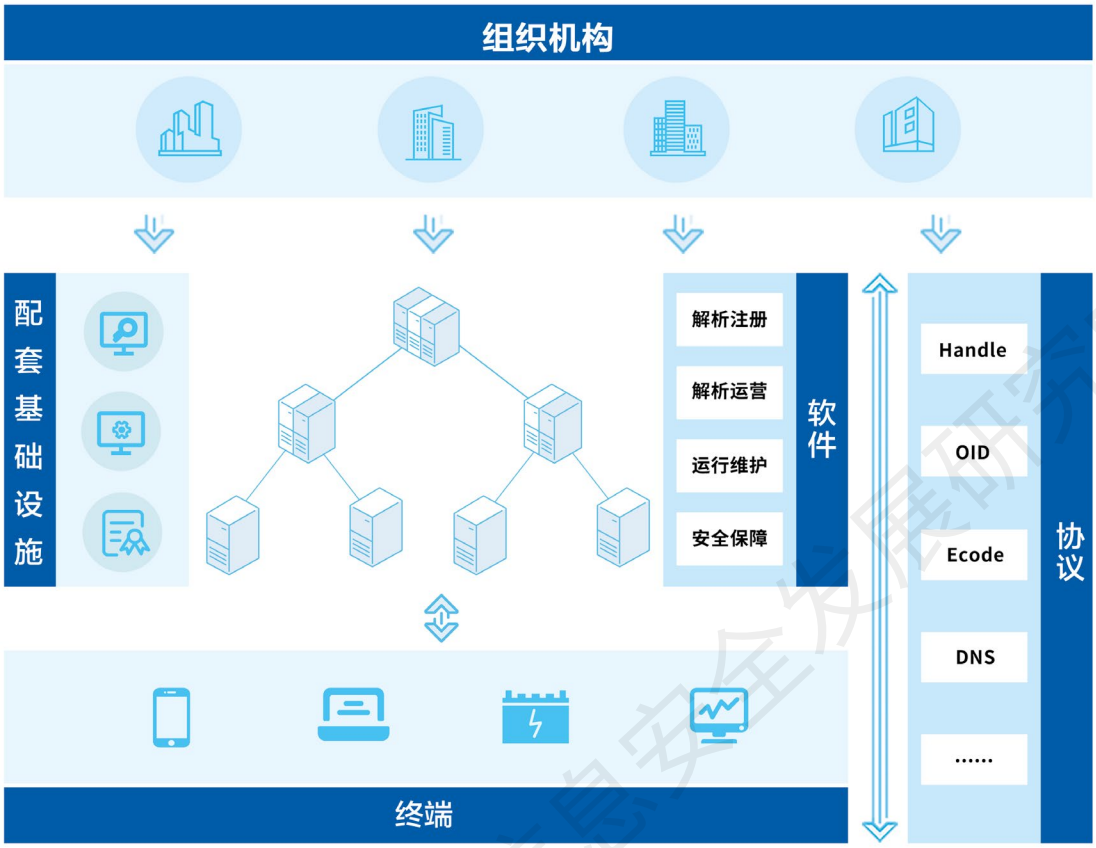
软件：提供标识注册、解析、运行维护、安全保障等服务的软件。

组织机构：平台系统建设、运营、监管、使用的机构。

配套基础设施：包括CA、密钥管理中心等安全服务基础设施、路由等网络基础设施、搭载软件系统的云平台等。

国家工业信息安全发展研究中心

图4. 标识解析防护对象



（三）安全角色视角

工业互联网标识解析安全建设与保障过程中涉及的角色包括标识解析决策与监管方、标识解析服务运营方、标识解析安全服务提供方、标识解析安全运营方、标识解析用户。

标识解析决策与监管方，负责对工业互联网标识解析安全架构的设计建设方案进行决策，对工业互联网标识解析安全建设、运营、使用情况实施监督管理。

标识解析服务运营方，负责提供标识解析服务，使用安全服务保障标识解析服务安全。

标识解析安全服务提供方，负责提供工业互联网标识解析安全产品和集成、建设等服务。

标识解析安全运营方，负责对工业互联网标识解析安全事件进行监测、预警、响应和恢复。

标识解析用户，包括联网解析企业、个人及具有联网解析功能的终端，需安全、合法使用标识解析服务。

（四）脆弱性与威胁视角

脆弱性与威胁视角针对标识解析在架构、协议、身份、数据、运营以及应用六个方面分析其脆弱性与威胁。

1.标识解析架构

工业互联网标识解析架构包括终端、节点、协议、软件、组织机构以及配套基础设施多类对象，其架构脆弱性与威胁可分别从各类对象本身和体系架构进行分析。

从对象角度分析，终端是标识解析服务的入口，节点是标识解析体系的关键组成，协议是标识解析通信的基础，软件直接提供标识解析服务，组织机构是标识解析软件硬件的管理与操作者，配套基础设施是标识解析服务的重要支撑，以上各类对象都可能成为标识解析体系的脆弱点。

从体系结构角度分析，首先，标识解析体系的树形分层体系结构为拒绝服务攻击提供了可能，一旦上层节点被破坏将造成叶子节点之间不可达。其次，当其节点数据被篡改时，将为整个标识解析体系带来不同程度的影响。例如，国际根

服务器被篡改可能会误导客户端请求，将其引导至错误的顶级、二级或企业节点，被破坏节点授权的下级节点也将不可信。企业节点服务器被篡改可能会返回错误的标识解析结果。中心节点数据被篡改可能导致更大范围的污染扩散。

2.标识解析协议

工业互联网标识解析体系中使用了多种通信协议，这些通信协议的安全特性参差不齐，架构也存在较大的差异。尤其，多数标识解析协议在设计之初没有过多的考虑安全性，一方面要保证协议自身的设计安全，另一方面要保障协议的实现安全。

工业互联网标识解析在协议方面可能存在多种脆弱性。一是源端身份鉴别问题，若在通信时未进行双向身份鉴别，则易滋生身份伪造。二是数据传输完整性问题，若对数据缺乏一致性校验，则易受到中间人篡改。三是数据传输保密性问题，若对通信数据采取明文传输，则易被窃听，造成隐私泄露。四是协议设计缺陷，若设计协议不严谨，易造成重放攻击、等待时间设置过长、侧信道攻击等威胁。五是协议实现问题，在协议的工程实现过程中容易出现代码安全、SDK安全等问题。六是密码算法安全，若协议中选用的密码算法被破解，或密码算法实现过程有误，则直接影响传输数据安全。

3.标识解析身份

工业互联网标识解析涉及的主体类型多样，人、机构、软件系统、硬件设备等主体的身份信息与权限级别各异，身份认证以及基于身份的管理控制存在挑战。身份安全是建立安全通信、提供可靠服务的基础，一旦身份信息被伪造、权限策略被篡改或绕过，将影响通信安全、数据安全及服务可控性，工业互联网标识解析场景中的典型攻击威胁包括伪造节点的中间人攻击、越权访问标识数据。

伪造节点的中间人攻击。攻击者可能拦截标识解析请求，冒充请求方向服务方发出请求，冒充服务方给原请求方返回响应。攻击方可能篡改响应内容，也可能观察请求与响应消息中的敏感信息。攻击者用类似的手段可以冒充客户端窃取标识属性数据，冒充物品提供虚假物品信息返回给企业节点认证等。

越权访问标识数据。企业节点对标识的属性信息定义基于用户的、基于角色的或基于属性的权限，只允许符合权限的用户操作。攻击者可能通过水平越权访问与他拥有相同权限的用户的资源，通过垂直越权问高级别用户的资源。

4.标识解析数据

工业互联网标识解析数据是标识解析应用的关键资源要素，需要在采集、传输、存储、使用等各个环节保障其保密性、完整性、真实性、不可抵赖性，其中数据传输过程主要由

协议脆弱性带来的安全问题，采集、存储、使用过程的脆弱性与威胁分析主要如下：

数据采集。标识解析系统的数据来源广泛、结构杂乱。从主体看，工业互联网通信主体来自不同的国家和企业，数据所有者错综复杂且实时变化，包括物料、设备、网元、服务、操作员等，具有更高的复杂性和多源异构性。一方面，在数据采集过程中会涉及到大量重要工业数据和用户隐私信息，访问控制及安全维护难度大，可能因访问控制策略配置不当造成隐私泄漏。另一方面，工业互联网标识数据载体类型多样，安全水平参差不齐，可能因标识载体被破坏导致采集数据失真。

数据存储。超千亿规模的标识数据量以及支撑系统运行的基础数据和日志数据将是长期负担，对数据的安全存储提出了更高的要求。当前标识解析平台分布式部署，节点众多，数据传输链路长，一方面数据可能在各节点被破坏，另一方面数据同步压力大，可能在同步过程中遭到缓存污染。

数据使用。当前主要通过接口使用千亿级工业互联网数据的过程存在多种安全隐患，由于数据处理节点多、类型复杂、部署分散，接口安全运维难度大，容易出现访问控制不严谨、安全策略不一致、行为审计不严格等问题。当接口被大规模调用时，会消耗系统资源，影响系统的正常访问，甚至导致系统瘫痪；当接口被非法或越权使用时，数据可能被伪造、

篡改、泄漏，影响数据完整性与保密性。当前针对工业互联网标识数据的探测行为日益增多，如果攻击者掌握了某一类资源的特征，很可能会利用这一特征对可探测资源进行批量枚举攻击，影响工业互联网资源的数据安全。

5.标识解析运营

随着工业互联网标识对象数量、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，需要厘清决策与监管方、标识解析服务运营方、安全服务提供方、安全运营方等主体在标识服务运营、标识安全保障、标识服务监管等环节的安全责任。按以上角色和流程分析运营方面的脆弱性与威胁情况如下：

标识服务运营。当决策方或标识解析服务运营方对标识编码资源分配不合理时，会使标识编码资源难以满足应用需求，同时出现资源闲置与紧缺情况；当标识解析服务运营方未对标识注册申请进行有效管控时，可能出现标识资源被抢注、滥用等情况；当标识解析服务运营方未对人员、机构进行有效管理时，可能出现人员误操作、机构非法运营等情况，引发标识资源失信、标识解析结果失真等安全问题。

标识解析安全保障。当安全服务方、安全运营方在设计、建设和运营标识解析安全服务的过程中未考虑工业互联网场景下应用高并发、低时延、高可靠性、可用性需求时，可能出现安全控制措施影响业务连续性的情况；当安全运营方未

对物理环境、人员身份、系统运行、资源使用采取有效的安全保障策略，未对风险制定完整的评估、监测、响应方案，未能落实技术加制度的安全管理手段时，可能造成标识解析安全保障缺失的情况。

标识解析服务监管。当标识解析服务运营方、监管方未对标识内容进行深入有效监管时，标识数据可能被用于存储有害信息或作为攻击支撑。

6.标识解析应用

标识解析架构可能被恶意利用，对其他系统造成攻击威胁。一方面，标识解析可能为僵尸网络提供温床，攻击者通过注册解析节点建立C&C信道，僵尸主控机通过C&C信道进行信号传输并控制僵尸主机，进而实现一系列恶意行为，如分布式拒绝服务攻击、隐私信息窃取等。另一方面，攻击者可能伪造成受害者发起大量正常标识解析请求，利用标识解析应答流量对受害者造成拒绝服务攻击。此外攻击者还可能对其恶意数据包进行二次封装，伪造成正常标识解析流量穿透防火墙，对目标进行隧道攻击。

（五）防护措施视角

针对标识解析在架构、协议、身份、数据、运营、应用六方面的脆弱性与威胁，防护措施视角以“注册、接入、管理、解析”的业务流程为主线，从物理环境、主机、网络、协议、系统、身份、数据等多方面采取技术加管理的防护措施，保障

标识解析运行环境安全、身份安全、服务运营安全、数据安全，符合《网络安全等级保护2.0》、《网络安全审查办法》、《密码法》、《数据安全法（草案）》等相关法规要求。

1.运行环境安全

为保障工业互联网标识解析终端、节点、平台系统的运行环境安全，应从物理环境、设备及软件系统、网络等方面部署安全防护措施，提升安全防护能力。

物理环境安全防护方面，建立机房安全管理制度，对机房所在区域采取访问授权、视频监控等物理安全防护措施，并定期巡查通信线路。对核心软硬件所在区域采取安全域隔离、访问控制、视频监控、专人值守等物理安全防护措施。防火、防盗、防静电、温湿度控制、防尘、电力供应、电磁防护。

设备及软件系统方面，一是做好资产管理，建立标识解析系统基础设施资产清单，做好资产分类、定级与标识管理，及时修复重要系统的安全漏洞。二是做好恶意代码防范，建立恶意代码防护及其相应的维护机制，通过手动或自动方式及时更新，防止非特权用户绕过。三是做好漏洞与补丁升级，密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证。

网络安全防护方面，一是做好安全域划分，分离安全区域，通过网络边界防护设备对边界进行安全防护，通过防

火墙、网闸等防护设备对安全区域之间进行逻辑隔离安全防护。对核心系统（如标识解析节点服务系统）搭建独立的计算平台、存储平台、内部网络环境及相关维护、安防、电源等设施，并经由受控边界与外部网络相连。二是做好入侵防范，建设端口扫描、木马后门、DDoS、缓冲区溢出等网络入侵行为检测及报警能力，并记录攻击源IP、攻击类型、攻击时间。对进出关键系统的数据信息进行过滤，并能根据系统能力对网络流量及并发数进行限制，对关键入侵行为进行阻断。三是做好安全审计，对重要设备运行情况、网络流量信息、系统管理及维护等信息进行记录，对记录进行留存并加以保护，防止篡改和未授权访问，以支持将来的调查和访问控制监视。

2.身份安全

为保障工业互联网标识解析终端、节点、组织机构身份可信，防止伪造身份的中间人攻击、重放攻击以及越权访问，应从终端、协议、平台系统等方面采取防护措施，提升身份管理与应用安全。

组织机构方面，加强机构实体身份认证，对于新申请加入的组织机构做好相关身份与资质审查，建立身份信息标识，保证操作过程身份可校验，防止机构身份伪造。

终端方面，一是加强标识载体安全，通过防伪、标识绑定等技术防止被动及主动标识载体中的标识编码被篡改、伪

造，二是提升客户端安全，通过软件安全防护技术，防止客户端被破坏，避免其身份被篡改、伪造、恶意利用。

协议方面，采用具有认证机制的通信协议，在各级节点间、客户端与服务端间等通信过程中，对主体身份、消息进行安全认证，支持配套的认证密钥建立。

平台系统方面，建设支持多种认证方式的身份与权限管理平台，对工业互联网标识解析涉及的多主体对象的身份及权限进行统一管理，对用户访问的全过程实行严格的向正确的用户实行相应的权限控制，包括从登入到登出的过程。

3.服务运营安全

为保障工业互联网标识解析服务运营方提供“注册、接入、管理、解析”服务的安全性，同时保证服务质量，应建立健全安全管理支撑、标准规范指引、技术手段保障、资源管理协同的安全的服务运营体系，提升服务运营安全，保障标识解析体系安全、稳定、持续运行。

建立和完善规范的运营管理制度。对标识解析注册机构、运营服务机构、监管方、安全服务提供方、安全运营方等制定相应的管理制度和运营规范，明确各机构的职责、权益、工作流程，制定发布工业互联网标识解析安全相关政策文件，面向各级解析节点提出安全保障技术要求及风险评估规范。在影响国计民生和公共安全的关键领域中，建立标识解析服务的准入审查机制，加强标识解析服务运营及应用的安

全性、可控性和透明性的审查。

制定运营安全的技术规范。建立健全工业互联网标识解析安全标准体系，先行制定接入安全、运营安全等相关技术规范和标准，加快标识解析安全管理、安全防护、安全评估等标准立项与制定。

综合采用安全技术手段建设立体化防护体系。针对物理环境、终端设备、软件系统、网络设施等对象，在服务及运维等过程采取多样安全防护技术，建设立体化防护体系，保障物理环境安全、通信网络安全、区域边界安全、计算环境安全和服务安全。保证标识解析业务不间断运行，保持主备服务器间的数据同步与更新，定期进行日志备份，做到操作可追溯，历史数据可统计。

加快形成资源管理的协同机制。完善标识注册备案机制，加强标识解析注册与服务机构的认证和管理，做好解析节点授权管理及标识资源使用，利用云计算、大数据等新手段实现数据资源共享、机构高效协同、责任边界明确的标识解析服务协作机制。

落地技术应用，落实制度要求。按照制定的管理制度规范要求，做好安全审计，对每个用户账号的操作、行为、标识资源使用情况、系统重要安全事件进行审计，留存记录并加以保护；做好身份鉴别，在标识解析系统运营维护、配置和补丁管理、系统升级、主机登录、标识解析服务资源访问等过程中

使用身份认证管理，对于关键设备、系统和平台的访问采用多因素认证；做好会话认证，对所有的通信会话提供真实性保护，防止中间人攻击、会话劫持；做好访问控制，依据安全策略控制业务用户、管理用户对系统文件、数据库、标识资源等客体的访问，对重要信息资源设置敏感标记，并依据安全策略控制用户对有敏感标记重要信息资源的操作，实现规范化的技术应用、体系化的运营管理、立体化的安全保障。

4.数据安全

为保障工业互联网标识解析各主体在“注册、接入、管理、解析”业务流程中产生的数据安全性，防止数据被篡改、丢失和泄露，应从存储、传输、使用等方面采取防护措施，确保数据可用性、完整性和保密性。

数据分类分级，建立分级管理规范。将工业互联网标识数据进行分类分级，对其存储、传输、使用过程制定对应的操作规范，定义不同类别、不同等级数据的安全防护要求。

数据分级管理，采用针对性数据安全防护手段。针对标识解析体系中涉及核心工业参数配置等的重要文件、目录及注册表进行保护，不允许进行修改、删除以及目录、文件重命名等操作，阻止异常修改并记录相应日志。对标识数据以及其他有重要价值的敏感数据存储时，采用密码算法或其他措施实现存储数据的保密性。确保敏感信息在入库（结构化数据）或落盘保存（非结构化数据）后以密文形式存在。对重要

数据进行传输时，除了加密之外，应对标识数据的有效性、完整性进行检验，保证标识数据未被篡改或伪造。对数据进行使用时，需根据数据类别与等级进行访问控制。

数据访问控制，设计细粒度数据使用控制策略。针对数据本身重建安全访问机制，以应用层为抓手设计数据访问控制策略，对访问主体（包括人、设备以及节点等）和被访问数据实现细粒度访问控制，结合数据加密方案实现数据访问过程动态脱敏。

数据操作审计，实现全流程数据操作过程管理。对于数据新建、访问、修改、删除等行为，记录完整的数据操作过程及主体身份信息，形成审计日志，并结合数字签名技术防止日志篡改，确保数据操作全流程可追溯。

（六）安全管理视角

安全管理视角从风险评估、监测预警、应急响应三个方面建设全面有效的工业互联网标识解析安全管理体系。

1.综合性风险评估能力

对工业互联网标识解析终端、节点、协议、软件、组织机构、配套基础设施六大防护对象进行识别与评估，在架构、协议、身份、数据、运营、应用六个层面分析其脆弱性、威胁、控制措施，分析脆弱性在相关环境下被威胁所利用的可能性以及利用后造成的影响，综合评估风险等级。

2.动态的监测预警能力

综合运用态势感知、威胁情报等技术手段，在关键解析节点部署安全态势监测与安全审计系统，重点针对物理环境、访问控制、运营人员、关键流程等风险点进行实时、动态监测，确保标识解析体系持续稳定运行。引入专项安全技术和服务，强化各解析节点服务对抗DDoS、缓存污染、标识劫持、标识解析重定向等攻击的能力。

3.联动的应急响应机制

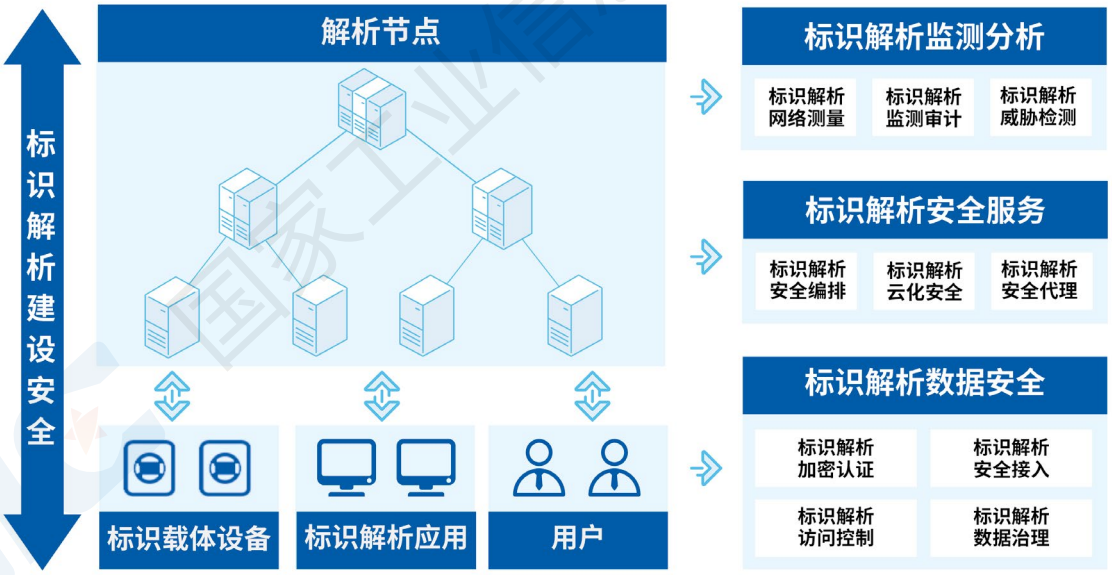
加强标识解析系统运行过程的安全监测和管理，完善重大网络安全事件触发响应机制。完善容灾和数据备份恢复机制。由于工业互联网标识解析体系涉及大量工业数据，一旦数据丢失或损坏将造成不可估量的损失，因此，应对数据进行多级保存、多点备份。可根据企业不同的业务类型与系统特点，对备份能力等级进行划分，依照等级的不同采取不同的备份策略与应对措施。同时，企业可制定适合自身的备份恢复策略，并对制定的策略进行有效性与实用性方面的验证。此外，还需完善应急响应团队的人才储备，通过定期演练检验应急响应团队、计划、流程、机制的有效性和完备性，提高重大突发事件的多方协同应对能力。

国家工业信息安全发展研究中心

五、工业互联网标识解析安全关键技术

针对工业互联网标识解析安全现状及面临的风险，本白皮书从安全建设、国密融合、安全接入、访问控制、数据治理、威胁检测、网络测量、监测审计、安全编排、安全代理以及云化安全等多个方面汇编总结工业互联网标识解析安全关键技术（如图5），为工业互联网标识解析安全建设者与研究者提供参考。

图5. 工业互联网标识解析安全关键技术



（一）标识解析建设安全

工业互联网标识解析建设过程中涉及的安全问题是构建工业互联网标识解析安全保障体系的基础，需要结合标识解析系统特性，规范化开发流程中的每一个环节，保证建设流程的安全。

标识解析服务具有应用需求差异性、安全服务多样性以及多体系共存等特性。需要设计可灵活调度、扩展性强、兼容性强的标识解析系统和安全服务框架。需要开发高可靠、低处理开销、多协议兼容的标识解析功能模块，体积小、安全性强、易于调度的安全服务模块。测试时需要充分考虑各种应用场景需求和业务需要，制定全面的测试评估方案。系统部署时要依据使用场景，综合使用软硬件部署和虚拟化部署方案。依据上述特征需求，建立标准化的安全开发流程。

安全开发流程保障安全建设。安全开发流程可通过规范的安全概要设计或方案设计、安全编码、安全测试、安全部署实现。在需求分析与设计阶段注意架构设计合理性、业务流程完整性、评估第三方软件安全风险；在开发阶段注意提供安全的函数，结合代码安全审计工具做好各模块审计工作，检查是否存在因设计缺陷导致攻击的可能，以及是否满足应用需求；在测试阶段注意结合自动化测试与手动测试方法在软件正式投入使用前对其进行深度测试，测试实现是否

符合设计预期；在**部署阶段**注意安全策略配置的适用性，同时避免弱口令等基础安全问题。

（二）标识解析国密融合

标识解析系统中数据需要采用合适的保护措施，在数据采集、传输和数据存储等过程中保障数据安全，避免数据窃取、篡改、丢失等安全风险。标识数据涉及大量工业核心数据，需要采用自主可控的安全方案。将国密算法深度融入到数据采集设备、传输设备和存储设备的软件代码和硬件实现中，在数据产生的源头处对数据进行签名认证和加密，减少安全风险环节，有效保护解析数据。

数字签名技术可对传输与存储数据进行签名，以便通信双方、服务双方进行身份认证与数据完整性校验。**数据加密技术**可对传输与存储数据进行加密，防止数据泄露。标识解析安全建设方可根据使用场景需要选择对称、PKI、IBC等多种方案。应按照国家密码管理有关规定使用和管理标识解析系统中所使用的密码设施，并按规定生成、管理和使用密钥。

（三）标识解析安全接入

标识解析系统对于接入网络的设备与标识解析节点应该具有可信的唯一标识，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。安全芯片提供随机数生成、唯一ID、密钥相关的管理服务，可作为设备的信任根，支撑设备安全接入。对接入对象进行身份认证，验证实体身份合法、消息可信，是实现安全接入的主要技术手段。

基于安全芯片的主动标识载体。标识载体是指承载标识编码资源的标签，是标识技术应用的关键环节。主动标识载体能够主动与标识数据读写设备、标识解析服务节点、标识数据应用平台等发生通信交互。基于安全芯片的主动标识载体能够满足接入安全需求，首先，安全芯片有一定的计算和存储能力，能够提供安全存储环境、安全运行环境、密码算法计算、随机数生成、自身安全防护等方面支持。其次，安全芯片可支撑工业互联网数据的可信采集，结合5G、NB IOT等通讯技术，利用其联网通信功能，能够主动向标识解析服务节点或标识数据应用平台等发起连接。此外，安全芯片支持密码算法防护，利用隐藏技术、掩码技术等手段，在原理和技术上保障密码算法的安全性。另外，在安全芯片中存储工业互联网标识、密钥等关键信息，运用安全芯片内的COS对关键信息进行严格的管理，结合适当的监管和密钥分发机制，能够防御外部攻击，保证访问者的合法性，数据保密性、不可抵赖性和不可篡改性，也可应对标识被随意读取、复制、盗用等威胁。

身份认证。通信双方的身份认证以及基于身份的消息加

密能够有效保障通信安全，防止身份被伪造、数据被篡改、隐私被泄露。通过基于口令的认证、基于生物特征的认证、基于PKI体系的数字证书、基于IBC的认证等方案等实体认证技术能够建立标识解析服务提供方与使用方、标识解析同级/跨级节点之间、标识解析终端设备与管理平台之间的信任。基于实体身份进行消息认证，能够保障标识解析请求与响应过程消息的完整性与可靠性。

（四）标识解析访问控制

访问控制是保障工业互联网标识解析不同角色安全访问标识数据的关键技术，一方面对标识解析的访问控制需要具备动态性、粒度可调节、灵活性等特点，另一方面对标识解析的访问控制需要具备应对大规模高并发访问请求的服务能力，以及抗拒绝服务攻击能力。根据不同标识解析业务需求，选择基于ACL、角色、属性、规则、业务场景、信任等要素的访问控制以及集成访问控制技术可实现灵活的标识解析访问控制，通过负载均衡技术、拒绝服务攻击防护技术可应对大量甚至过量的访问请求。

（五）标识解析数据治理

数据治理是组织中涉及数据使用的一整套管理行为，是对数据资产管理行使权力和控制的活动集合。标识管理是工业互联网标识解析数据治理的核心内容，可从异构标识、可

循环标识、关联标识、标识数据智能分析、对等解析等方面研究标识管理方案。隐私保护是工业互联网标识解析数据治理全过程的安全要求，可以在标识编码、发布、存储、分析、使用等过程结合隐私保护方案。

工业互联网标识解析数据管理技术包括：统一标识有效性管理技术、异构数据标识技术、可循环标识管理技术、映射与关联信息收集技术、标识数据智能分析技术、对等解析技术等。

标识数据隐私保护技术包括：标识编码隐私保护技术、数据发布隐私保护技术、数据存储隐私保护技术、数据分析挖掘隐私保护技术、数据使用隐私保护技术。标识编码隐私保护方案主要有两种，一是层级式的结构化标识编码方案，该方案有利于实现标识编码的分级查询和安全管理，二是扁平化的随机数形式的标识编码方案，该方案具有去中心化特性，在网络攻击和防御方面具有良好的表现。数据发布隐私保护技术包括泛化技术、k-匿名模型及k-匿名改进模型。数据存储隐私保护技术包括基于同态加密的隐私存储、多级索引技术、安全多方计算技术等。数据分析挖掘隐私保护技术包括抑制技术、假名化技术、随机化、差分隐私模型等。数据使用隐私保护技术包括基于角色控制和属性控制确保数据访问的风险控制。

（六）标识解析威胁检测

威胁检测是保障标识解析系统安全运行的核心技术，通过收集标识解析系统运行数据，采用多种异常检测和威胁感知方法，分析系统安全事件并上报处理。威胁检测流程包括威胁分析数据收集、异常数据检测和威胁事件提取。在数据收集方面，用于分析的数据包括解析流量数据、设备运行数据、用户行为数据等。通过网络数据采样、数据镜像获取、接口数据拉取等方式进行收集。异常数据检测方面，分为传统的数据分类分析和机器学习分析两种。传统数据分析利用分类、聚类算法，依据确定的阈值标准，将正常数据和异常数据进行划分。机器学习方式使用贝叶斯分类、决策树等方法进行自动化的异常分类分析。威胁事件提取方面，利用已有的异常分类信息，与已有威胁特征库比对确定威胁事件，学习记录未匹配事件特征。

（七）标识解析网络测量

网络测量是遵照一定方法和技术，利用软件和硬件工具来测试或验证表征网络性能指标的一系列活动的总和。工业互联网标识解析空间测量是了解工业互联网标识解析动态变化情况、获取其性能特征的重要手段，能够为建立准确的行为模型和评价标准提供依据，有助于对工业互联网标识解析实施科学管理和有效控制，提高标识解析的应用能力和安全性。

从不同角度出发可以对测量技术进行分类，测量对象包括：网络的拓扑结构、逻辑拓扑关系或具有地理信息的拓扑，以及时延、吞吐量、丢包率等性能信息；测量方式包括单点测量与多点测量、主动测量与被动测量等。

利用测量到的拓扑数据构建标识解析网络全局视图，反映各级节点、终端设备的拓扑连接关系，确定不同种类服务的分布情况和运行状态。将性能测量结果映射到网络视图中，实时测量分析网络节点状态、链路负载问题、业务运行情况，进一步确定解析网络中的性能瓶颈、不稳定节点和潜在的安全风险位置，为业务行为分析和模型构建、标识解析系统状态管控、解析系统设计优化及动态调节和安全策略实时部署提供支撑。

（八）标识解析监测审计

标识解析安全监测与审计包括辨别、分析和记录标识数据及标识流量中的安全问题。通过分析标识数据内容，结合人工与自动化方法对标识数据进行内容审查，分析其中是否存储不良、有害信息，对相关标识进行标记并追责。通过对上层交换机镜像的标识流量或标识解析节点服务器产生的业务流量进行采集、读取标识流量采集的数据包解码生成固定格式的日志、对标识节点进行多维度业务指标监测并形成日志文件，分析流量、流量解码日志、监测日志中反映的

系统活动、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，实时分析安全事件并告警。

（九）标识解析安全编排

安全编排是依据不同标识解析应用需求，为不同的解析服务分派不同的安全策略，在保证安全策略适配的同时，不影响业务可用性及服务质量的安全技术。针对标识解析服务特性各异、安全需求多样、服务质量要求严格的特点，使用安全服务链编排技术，根据业务需求为不同标识解析服务编排不同的服务链。分析业务安全需求，构建安全服务需求模型；将安全策略进行分解，拆分成为安全服务元组件并分析组件资源需求，将安全服务需求和服务元组件进行映射，形成安全服务链。结合网络状态感知结果和服务组件资源需求，将服务链映射到安全设备上，选取最优的传输路径，并利用虚拟化技术进行安全服务组件的动态部署和灵活调配，实现标识解析安全服务的按需编排、动态编排。

（十）标识解析安全代理

标识解析系统在身份认证、传输加密等过程中需要使用大量密钥数据。针对动态业务场景、海量解析设备、多元异构环境，需要实现灵活、易部署、安全的密钥管理。利用云化密钥技术，通过软件实现密码算法的运算，密钥通过管理互

通协议与远端的硬件密钥管理系统交互，形成“软件+硬件”的组合模式，弥补纯硬件模式下的不足。通过云密钥管理技术实现了密钥的全生命周期管理，对于系统的传统化部署、云化部署，都能充分保证密钥的安全使用，且通过专用的代理加密技术，可以完成密钥的自动化备份与恢复，实现了标识解析密钥的动态管控、安全管理。

（十一）标识解析云化安全

标识解析系统根据应用需求和服务需要，会采用软硬件结合、云化混合部署等方案，将标识解析系统功能以服务的形式部署在云平台上，降低部署使用开销、提高服务扩展能力。解析数据上云后存在使用不透明、管理困难的问题，存在泄漏风险，解析功能上云后存在隔离安全问题。利用云访问安全代理技术，对上云标识数据使用进行全程跟踪，建立数据流动视图，检测数据使用情况。利用微服务隔离技术，对不同级别的标识解析功能进行安全隔离，避免数据泄露。实现标识解析云化部署的功能安全和数据安全。

六、工业互联网标识解析安全发展展望

工业互联网标识解析处于快速发展过程中，随着标识解析体系的快速落地与融合应用，其安全发展必将愈发得到工业界与学术界的重视。本白皮书提出的工业互联网标识解析安全框架可为我国工业互联网标识解析安全研究、安全建设以及安全应用提供一定参考。当前相关政策与管理机制还未配套完备，其安全防护技术及产品也正处于研究与落地的初步阶段。立足我国工业互联网标识解析发展和安全现状，从规范安全管理机制、提升安全评估能力、建设安全监测体系、激发安全防护技术创新、促进产业协同发展等方面入手，着力推动标识解析安全保障能力建设，可以加强以下工作。

（一）围绕安全运营、顶层设计、政策指导、标准引领等方面建立健全工业互联网标识解析安全管理机制

一是规范标识解析节点运营管理。对标识解析节点运行服务相关机构制定相应管理办法，规范标识解析各级节点的建设、接入和运营管理。

二是统筹建立标识资源管理与协调机制。完善标识注册

备案机制，加强标识解析注册与服务机构的认证和管理，做好解析节点授权管理，规范标识资源使用，建立稳定的标识体系协作机制，稳步推进国际根节点、顶级节点、二级节点的互联互通。

三是完善政策制度与规范指导。制定发布工业互联网标识解析安全相关政策文件，面向各级解析节点提出安全保障技术要求及风险评估规范，指导各级节点做好安全防护工作。

四是加快标准研制。建立健全工业互联网标识解析安全标准体系，先行制定标识解析编码规范、标识解析互联互通要求、标识解析隐私保护、标识解析接入安全、运营安全等相关标准，加快标识解析安全管理、安全防护、安全评估等标准立项与制定。

（二）从完整性、健壮性、服务质量等方面加快提升工业互联网标识解析安全评估能力

一是完整性评估。从数据完整性、协议完整性与系统完整性等角度开展标识解析完整性评估，确保标识与解析数据在通信过程的真实性、不可否认性。

二是健壮性评估。立足基础设施与架构安全、系统运维安全、容灾恢复和安全管理制度四个方面，开展标识解析健壮性评估，确保系统出现安全事件时的恢复能力。

三是服务质量评估。从标识解析安全认证能力、安全监

测能力、系统安全防护能力、恶意代码检测能力、应急响应能力与容灾备份能力等角度开展标识解析服务质量评估。

（三）着眼统一整体与各层细节等角度建设工业互联网标识解析安全风险监测体系

一是加强标识解析各节点安全监测与防护能力。在关键解析节点部署安全态势监测与安全审计系统，实时、动态监测标识解析系统运行安全状态，加强各解析节点服务抗DDoS、缓存污染、标识劫持、标识解析重定向等攻击的能力。

二是建设体系化的标识解析安全监测平台。通过统一监测平台协同收集各层次的安全风险监测数据，通过体系化的监测手段挖掘潜在安全风险，通过关联的流量数据分析安全事件。促进各标识解析基础设施和安全平台的数据及响应形成联动，提升风险监测能力与安全响应能力。

（四）着力安全技术新应用、新技术赋能标识解析安全、标识解析助力工业互联网安全等方向推进工业互联网标识解析安全技术创新

一是集合多种方案加强标识解析网络通信安全。可使用TLS1.3等技术对标识解析流量进行加密，或使用隧道协议封装标识解析流量，抵御网络传输过程中的中间人攻击等威胁，防止数据泄露。

二是充分利用密码技术加固标识解析安全。使用符合国家密码管理规定的密码算法和产品对标识解析的开放式协议架构进行加固改造，加强对工业互联网标识解析服务节点的规模化跨域认证和标识数据、服务的信息保护。逐级建立认证体系，支持工业互联网标识解析身份管理、访问管理以及节点批量接入认证能力，构建从根节点自上而下的完整信任链。

三是应用安全技术加强标识数据安全治理。建立工业互联网标识数据的可信环境，加强对标识数据的隐私保护、标识的源认证、标识的可查询性、标识数据完整性校验、支持对标识解析请求端的基于身份、属性等方式的细粒度访问控制等能力，强化对工业互联网标识数据的使用管理。

四是结合新技术优势建设标识解析。可利用区块链技术实现工业互联网标识解析数据的可信共享与应用，解决传统标识解析架构单点故障、权力不对等问题，支撑可信的对等解析。可利用人工智能技术助力安全检测、支撑威胁感知、支持应急响应、辅助分析决策以及赋能威胁分析，提高标识解析的安全水平。可利用国产安全芯片从源头上解决工业互联网的信任问题。可基于可信计算能构建主动免疫的防护体系。

五是通过标识解析助力工业互联网安全。可利用标识构建工业互联网标识密码体系，支撑标识密码、无证书密码等

技术的应用；可利用标识保障工业数据采集安全，实现基于标识的身份、数据加密、访问控制；可利用标识提升工业互联网边缘设备接入安全，实现基于标识的边缘对象接入认证与综合管控；可利用标识助力工业互联网资源安全治理，基于标识实现包括资产识别、可信接入、数据安全操作与确权共享等环节的安全治理；可利用标识解析流量进行工业互联网恶意行为检测，从标识解析流量中发现攻击行为与恶意程序；可利用标识数据支撑攻击溯源，将网络行为关联信息存储到标识数据中，可作为攻击者身份追溯的凭证，助力关联行为分析，从而支撑恶意行为溯源。

（五）从人才培养、产业链协同、生态创新等方面促进工业互联网标识解析安全产业创新发展

一是培养复合型安全人才队伍。结合政府、科研单位、高校、企业等各方力量，整合国内外优势资源，培养标识解析安全、工业互联网安全、网络空间安全等多领域交叉人才，培养具有工业互联网安全领域应用能力的高水平人才队伍，为推动产业发展提供鲜活能量。

二是激发安全产业链新动力。促进标识解析安全技术及产品在工业互联网领域的推广应用，为具有自主知识产权的安全标识载体、安全服务平台等提供应用支持，加强跨域、跨界企业交流合作，促进产业链协同创新。

三是促进安全生态新模式。充分发挥我国工业互联网标识解析建设的领先优势，加速战略布局，整合相关行业资源，探索完善工业互联网标识解析体系建设、加固工业互联网标识解析安全体系架构、标识赋能工业互联网安全保障能力建设的发展思路，打造标识数据、标识载体、标识解析节点、标识解析系统赋能工业互联网安全的应用生态新模式，助力基于标识解析体系的工业互联网安全能力建设。

国家工业信息安全发展研究中心

联系地址：北京市石景山区鲁谷路35号　　联系电话：010-88686237