工业信息安全标准化白皮书

（2019 版）

工业信息安全产业发展联盟

2019 年 12 月

版权说明

牵头编写单位：国家工业信息安全发展研究中心

联合编写单位：中国电子技术标准化研究院、广州赛宝认证中心服务有限公司、国家信息技术安全研究中心、清华大学、北京东方国信科技股份有限公司、恒安嘉新（北京）科技股份公司、上海观安信息技术股份有限公司、上海云剑信息技术有限公司、湖北省电子信息产品质量监督检验院、长扬科技（北京）有限公司、北京威努特技术有限公司、中国电子信息产业集团有限公司第六研究所、国网电子商务有限公司、中国科学院大学、北京网藤科技有限公司、北京亚控科技发展有限公司、北京华电天仁电力控制技术有限公司、中国电力企业联合会科技开发服务中心、新华水力发电有限公司、深圳融安网络科技有限公司、北京杉树岭网络科技有限公司、武汉亿博斯特科技有限公司

编写人员：陈雪鸿、李俊、杨帅锋、柳彩云、刘贤刚、李尧、刘克松、方进社、曾珍珍、李霞、叶晓俊、王晨、敖志强、孙广明、傅强、王泽政、谢江、王勇、徐煦、陈斯、黄浚哲、汪义舟、严美玉、黄敏、王绍杰、王栋、张玉清、杨毅宇、张馨元、张硕、陆秋明、成忠庆、陈仲亿、刘森、孙昶辉、王嵘、陈桂耀、汪敦全、梁鼎铭、刘畅、李伟斌、李春、李蜀斌、孙岩、李耀兵、王冲华、江浩、张雪莹、毕婷、赵千、周昊、高建磊、樊佩茹、余果、李赟

编写说明

随着信息化和工业化的深度融合，传统的工业生产系统逐步由单机走向互联，由封闭走向开放，极大促进了工业生产的网络化、协同化，同时也加强了工业互联网安全的级联效应。尤其是电力行业，已经出现了多起因工业互联网安全问题引发的停电事故。在工业互联网安全形势日益严峻的当下，亟需加强工业信息安全标准化工作，奠定两化融合的安全基石。

我国高度重视网络安全，2016 年颁布《网络安全法》，对网络运行安全、监测预警与应急处置、法律责任等方面作出规定，也提出了制定完善网络安全标准的相关要求。为贯彻落实《网络安全法》，推进当前及未来一段时间工业信息安全标准化工作，推动解决标准缺失、滞后、交叉重复、体系化不足等问题，为工业信息安全标准研究与制定提供参考，工业信息安全产业发展联盟组织撰写《工业信息安全标准化白皮书》，旨在厘清工业信息安全概念与内涵，梳理已有的工业信息安全标准及未来拟制定的国家标准，形成全面布局、重点突出的工业信息安全标准体系。与当前已发布的《工业互联网平台标准化白皮书（2018）》《工业互联网标准体系（2.0）》《工业信息安全态势白皮书（2017）》《中国工业信息安全产业发展白皮书》等白皮书相比，本白皮书首次明确界定了工业信息安全相关概念之间的关系，全面分析了当

前工业信息安全标准化工作中存在的问题，并梳理总结了国内外工业信息安全相关标准情况。在此基础上，本白皮书提出了工业信息安全标准体系框架。

工业信息安全产业发展联盟将密切关注工业信息安全领域的技术与标准发展动向，持续推出工业信息安全标准化等系列白皮书，为工业信息安全标准研制和安全防护建设提供参考。

目 录

一、工业信息安全概念和内涵

工业信息安全是近年来的一个新兴概念。2016 年，《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28 号）首次提出工业信息安全，并明确规定要“制定完善工业信息安全管理等政策法规，健全工业信息安全标准体系……提升工业信息安全监测、评估、验证和应急处置等能力”。

工业信息安全是工业领域信息安全的总称，涉及工业领域各个环节，包括工业控制系统安全、工业数据安全、工业云安全等内容。其本质是确保工业生产运营流程不被攻击或破坏，实现稳定的生产过程，完成既定的生产目标，保障生产执行过程的要素不被篡改或盗取。从重要性来看，工业信息安全是网络安全的重要组成，是国家总体安全观在工业领域的重点体现，其事关经济发展、社会稳定和国家安全，做好工业信息安全工作是关系国计民生和国家长治久安的大事；从保障对象来看，工业信息安全涉及工业控制系统安全、工业互联网平台安全、工业物联网安全、工业数据安全、工业云安全等，相关概念的定义如表 1 所示。

表 1 工业信息安全相关概念定义

序号	名词	定义
1	工业信息安全	工业信息安全指对工业领域信息的可用性、完整性、保密性等的保持，涉及工业领域生产和运营的各个环节的安全，包括工业控制系统信息安全、工业数据安全、工业云安全等。
2	工业互联网	工业互联网是满足工业智能化发展需求，在工业（公共）领域中由人、设备和系统、数据等相互连接的网络，是具有低时延、高可靠、广覆盖特点的新型网络基础设施。
3	工业控制系统	工业控制系统是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用于工业部门和关键基础设施中。
4	工业互联网平台	工业互联网平台是边缘数据采集系统、云计算基础设施及其上的开发、应用、服务等软件的集合，是面向工业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，是支撑制造资源泛在连接、弹性供给、高效配置的载体。

5	工业物联网	工业物联网是物联网在工业领域中各类应用的总成，是实现广义工业领域范围的智慧应用及信息共享的基础平台。
6	工业数据	工业数据是指在工业领域中，围绕典型智能制造模式，从客户需求到销售、订单、计划、研发、设计、工艺、制造、采购、供应、库存、发货和交付、售后服务、运维、报废或回收再制造等整个产品全生命周期各个环节所产生的各类数据及相关技术和应用的总称。
7	工业云	工业云是一种面向工业的通过网络将弹性的、可共享的资源和业务能力，以按需自服务方式供应和管理的模式。

从概念定义来看，工业互联网安全属于工业信息安全的子集。工业互联网的两大属性是“工业”和“互联”，而在实际工业生产经营过程中，无论是离散工业还是流程工业中，均存在未连入工业互联网的工业系统和设备，其信息安全属于工业信息安全范畴，但尚不属于工业互联网安全。工业互联网覆盖工业云、工业数据、工业控制系统、工业物联网及其他新兴的工业互联网形态。其中，工业云是工业互联网平台及工业物联网的基础技术，而工业互联网平台是传统工业云平台的迭代升级。工业互联网平台除工业云外，还包括边缘

层、工业应用以及平台上的工业数据，并且与工业物联网有交叉关系。此外，工业控制系统的硬件构件与工业物联网之间也存在交叉关系。各相关对象之间的安全关系如图 1 所示。**图 1 主要对概念范围和边界进行区分，对各概念的交叉和包含关系进行直观展示，而非严格的集合图。**

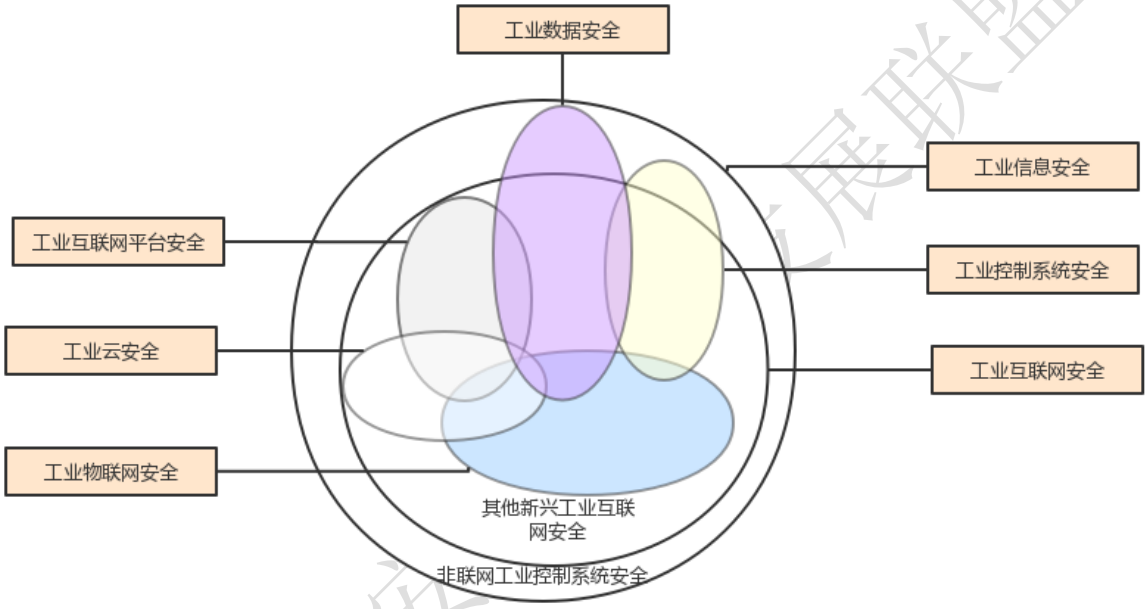

图 1 工业信息安全概念关系图

综上所述，与传统计算机网络安全相比，工业信息安全在保障目标对象、安全需求等方面具有其特殊性。例如，工业信息安全的主要目的是确保工业（产业）发展的安全，其保护需求往往融合考虑了信息安全、功能安全和生产安全等多种安全需求，更侧重于维护生产运行过程的可靠稳定。工业属性带来的保护场景多样、安全措施通用性较差等给工业信息安全带来了挑战，传统的网络安全保障体系已难以做到全面有效防护，亟需建立针对性强、特色鲜明的工业信息安

全保障体系。

二、工业信息安全标准现状、发展趋势和问题

（一）工业信息安全标准化发展现状及趋势

1. 国外工业信息安全标准的发展现状及趋势

1.1 发展现状

1.1.1 国际工业信息安全标准多为电力领域工控安全标准

工控安全国际标准主要集中在电力系统信息安全领域，国际电工委员会（IEC）、电气和电子工程师协会（IEEE）和国际自动化协会（ISA）等都致力于工控安全国际标准建设。IEC 在 2016 至 2019 年间发布的电力系统信息安全相关标准有 10 个，例如 2018 年 11 月发布了《电力系统管理及信息交换：数据和通信安全性第 4 部分：MMS 及其衍生物的概要（IEC 62351-4）》，为基于制造消息规范的应用程序握手期间的身份验证明确了传输层和应用层的安全要求；IEEE 于 2013 年更新发布了《变电站 IED 网络安全功能标准（IEEE 1686-2013）》，解决了 IED 访问、操作、配置、固件修订和数据检索方面的安全问题，且研究制定了新版本的《变电站串行链路网络安全的机密协议试行标准（IEEE P1711）》，为变电站串行链路定义了一种安全通信加密协议，保护了异步串行通信的完整性和（可选）保密性。此外，通用的工业

信息安全国际标准方面，IEC 和 ISA 一直积极研制《工业过程测量、控制和自动化 网络与系统信息安全（IEC 62443）》，于 2018 年 1 月发布了 IEC 62443-4-1，2019 年 2 月发布了 IEC 62443-4-2 部分。IEC 62443 从信息安全的通用方面、针对用户的信息安全程序、针对系统集成商保护系统所需信息安全技术要求、针对制造商提供的单个部件的信息安全技术要求四个方面，提出工控安全要求。

1.1.2 美国体系化开展工业信息安全标准化工作

美国国家标准与技术研究院（NIST）、美国国土安全部（DHS）等机构致力于美国工业信息安全标准的建设，在工业信息安全标准方面不断加强投入。在工控安全方面，发布了一系列工控安全的指南和规范性文件，包括《工业控制系统信息安全指南（NIST SP 800-82）》《系统保护轮廓—工业控制系统（NIST IR 7176）》《中等健壮环境下的 SCADA 系统现场设备保护概况》等。在电力、石油、天然气、核电等领域，美国也发布了一系列典型行业的工控安全标准，例如《管道 SCADA 安全（API1164）》《智能电网安全指南（NIST IR 7628）》等。此外，2007 年美国 ISA 成立安全复合型研究院 ISCI，专门从事安全标准的符合性认证工作，目前 ISCI 已经推出嵌入式设备安全保证（EDSA）认证、系统安全保证认证（SSA）和安全开发生命周期保证认证（SDLA）。

在物联网安全方面，美国政府多措并举加强物联网安全。

2015 年，美国联邦贸易委员会发布《物联网产品安全高级指南》，投入 1.6 亿美元推动“智慧城市”计划，将物联网应用试验平台建设作为首要任务。2016 年 2 月，成立物联网标准组织“Open Connectivity Foundation”，致力于物联网产业标准制定。2016 年 5 月，NIST 发布了《网络物理系统框架》。2016 年 9 月，美国白宫再次追加预算 8000 万美元，集中于城市服务等领域的物联网技术应用。2016 年 11 月美国国土安全部发布《确保物联网安全的战略原则》，面向物联网设备和系统开发商、管理者及个人提出了一组网络安全实践准则建议。具体到工业物联网安全方面，美国成立工业互联网联盟（IIC），负责对工业物联网安全进行研究，已发布了一系列成果。如 2016 年 9 月 19 日，IIC 发布工业物联网安全框架（IISF），定义了工业互联网可信体系的五大关键特性，即信息安全、功能安全、可靠性、弹性和隐私安全，拟通过该框架的发布为工业互联网安全研究与实施部署提供指导。

在工业数据和工业云安全方面，NIST 于 2012 年 6 月启动了大数据相关基本概念、技术和标准需求的研究，2013 年 5 月成立了 NIST 大数据公开工作组（NBG-PWG），2015 年 9 月发布了《NIST 大数据互操作框架（第一版）（NIST SP 1500）》系列标准。2013 年 7 月，发布了《NIST 云计算标准路线图（第二版）（SP500-291）》。

1.1.3 欧盟各国工业信息安全标准以基础设施为重心

近年来，欧盟发布了“欧洲关键基础设施保护项目（EPCIP）”，成立了工控安全应急响应组（ICS-CSIRT），负责对各类工控安全事件响应分析、共享信息，协调各成员国实施关键基础设施保护计划。此外，欧盟国家根据各自国情关注特定领域的工控安全标准建设，例如荷兰国际仪器用户协会（WIB）2006 年发布《过程控制域（PCD）—供应商安全需求》，挪威石油工业协会（OLF）2009 年发布《过程控制、安全和支撑 ICT 系统的信息安全基线要求（OLF Guideline NO.104）》和《工程、采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施（OLF Guideline NO.110）》，瑞典民防应急局（MSB）2010 年发布《工业控制系统安全加强指南》。德国作为传统汽车产业强国，对自动驾驶技术与产业发展持积极态度。2017 年 6 月，德国颁布《道路交通法第八修正案》与《自动驾驶道德准则》，成为自动驾驶领域立法的“先行者”。此外，作为工业 4.0 的先行者，德国还发布了《工业 4.0 安全指南》，对工业 4.0 背景下的风险分析、网络划分、用户账户、安全协议等进行约定，旨在确保工业 4.0 中设施设备、系统运行等方面的安全。

1.2 发展趋势

随着新工业革命时代的到来，美国、欧盟等发达国家和

组织将在未来的一段时间内，加快工业互联网网络安全、数据安全、平台安全、关键信息基础设施安全等方面的标准研究和制定，逐步完善工业信息安全标准路线图。

一是继续完善各领域标准工作计划。2019 年 5 月，美国能源部发布《能源行业网络安全多年计划》，为能源部网络安全、能源安全和应急响应办公室（CESER）勾画了一个“综合战略”,确定了美国能源部未来五年力图实现的目标和计划。将来，发达国家将会继续进行统筹规划，在工业信息安全各个领域勾画标准蓝图，指导标准研究制定。

二是加快研制重点行业领域标准。在统筹规划的基础上，发达国家将进行分类施策，主抓重点行业领域及易受威胁领域的工业信息安全标准，如电力领域。加快指导制定相关行业领域标准，“分行业、分重点”实现标准先行。

三是加快研究关键信息基础设施安全标准。美国、欧盟一直以来都将关键信息基础设施保护作为重点，随着当前关键信息基础设施安全形势日趋严峻，“网络战”成为各国关注的焦点，发达国家将继续加强关键信息基础设施安全标准研制，强化关键信息基础设施保护。

四是瞄准新技术新应用安全需求，开展标准研制工作。随着工业互联网、人工智能、工业大数据等技术的快速发展，美国、欧盟等发达国家将会针对相关技术、应用及时研制标准，规范新技术新应用的发展，同时确保其在新技术新应用

国际标准研制中的领先地位。

2. 国内工业信息安全标准的发展现状及趋势

2.1 发展现状

当前，我国工业信息安全标准加快推进，主要呈现以下三个特点：

（1）工业控制系统安全标准制定推进成效显著。我国在21 世纪初期便开展对于工业控制系统安全标准的研制工作，一批工业控制系统基础类安全标准已发布和实施。例如我国于 2011 年发布了《GB/T 26333-2010 工业控制网络安全风险评估规范》，2014 年发布了《GB/T 30976.1-2014 工控系统信息安全第 1 部分：评估规范》《GB/T 30976.2-2014 工控系统信息安全第 2 部分：验收规范》等标准，填补了我国工业控制系统安全标准的空白，使工业控制系统安全工作有标准可依。此外，我国通过在信息系统安全等级保护中增加工控安全等保扩展要求、建立新标准体系等多种方式，进一步加紧更新细化完善工控安全标准，并研究制定了《GB/T 32919-2016 信息安全技术工业控制系统 安全控制应用指南》《GB/T 36323-2018 信息安全技术工业控制系统 安全管理基本要求》《GB/T 36324-2018 信息安全技术工业控制系统信息安全分级规范》《GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》等标准 30 余项。

（2）工业互联网网络、数据、平台安全标准正在加紧研制，但目前还难以满足工业互联网发展的安全需求。随着《关于深化“互联网+先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》等政策文件的发布实施，工业互联网安全体系架构进一步明确，但工业互联网安全标准化工作还在起步阶段。从《工业互联网综合标准化体系建设指南》的内容来看，《20170373-T-604 工业通信网络和系统安全术语、概述和模型》《2017-0960T-YD 工业互联网网络安全总体要求》《2018-0179T-YD 工业互联网安全接入技术要求》等网络安全标准，《20181369T-YD 工业互联网数据安全保护要求》等数据安全标准，《2018-1396T-YD 工业互联网平台安全防护要求》《GSJCPZT0247-2019 工业互联网 安全体系框架》《GSJCPZT0246-2019 工业互联网平台质量管理要求》等平台安全标准正在加紧制定中。

（3）工业信息安全体系框架类标准亟待填补。目前，尚未有正式发布的工业信息安全体系框架类标准。随着工业互联网的快速发展，工业信息安全概念的范围逐渐扩展，各类工业信息安全标准逐步推进。同时，工业领域新技术新应用标准也在加紧研制中，但相关标准间缺乏严格的逻辑关联，亟需开展工业信息安全体系框架类标准制定，为工业信息安全标准的研制提供思路和方向。

2.2 发展趋势

未来，我国工业信息安全标准将主要呈现“体系化、国际化、影响扩大化”三方面的趋势。

2.2.1 标准研制体系化

下一步，国内工业信息安全领域标准将逐步制定和完善，工作管理和技术支撑体系将更加健全，以“安全促发展，发展保安全”的产业生态体系将逐步形成。具体而言，相关行业企业、科研院所将通过深入分析新背景下工业领域面临的信息安全问题和标准化需求，借鉴其他国外信息安全标准体系的先进经验，建立网络安全、平台安全、数据安全、设备安全、应用安全等相关标准，以及面向安全服务、行业需求等的系列标准。此外，各行业将积极向电力行业看齐，制定符合本行业特征的工业信息安全标准规范，以指导和规范本行业的工业信息安全工作。

2.2.2 标准合作国际化

我国的工业信息安全标准化工作起步较晚，大多数的工业信息安全国际标准是在欧美发达国家的标准基础上制定产生的，借鉴国外的成熟先进经验对我国的工业信息安全标准化建设十分必要。

未来，我国的工业信息安全标准化工作者将积极参与国际标准化活动，密切关注国际工业信息安全标准的发展动态，

加强与国外专家的技术交流和沟通，在翻译和消化国外类似标准规范的同时，有计划、有重点地参与和主动承担国际标准的起草工作，包括标准试验验证和讨论等，逐步使我国的工业信息安全标准化工作与国际标准化工作的计划、进度以及试验验证等接轨。

2.2.3 标准影响扩大化

未来，标准的研制将对“产学研用”均有更大的推动作用。

“产”：标准的制定、发布将大力促进产业的发展，推动产业往更安全、更可靠、更成熟的方向前行。

“学”：标准的广泛制定和应用需求将吸引更多工业信息安全人才投身标准建设中，为标准工作添砖加瓦。

“研”：工业信息安全标准的技术要求、管理要求等将为学术研究提供参考，推动工业信息安全技术深挖，引导未来新技术新应用发展，促进学术研究和标准研究相互借鉴和融合。

“用”：标准在引导未来新技术新应用发展的基础上，更加注重实用性和可操作性。标准的宣贯培训和试点示范将会增多，对行业企业的指导作用将逐步加强，在行业企业中的应用将更为广泛。

（二）工业信息安全标准化工作存在的问题

当前，我国工业信息安全标准化工作整体而言还处于起

步阶段，存在“合作交流较少、概念统一性差、体系建设不足、落地应用困难”等问题。具体有以下表现：

“合作交流较少”：当前，我国有多个标准化技术委员会致力于工业信息安全标准的研制，有助于工业信息安全标准的全面快速发展。但是各标准化技术委员会、标准工作组之间合作交流较少，一定程度上存在标准交叉、重复的现象。

“概念统一性差”：当前，我国工业信息安全相关标准中的概念统一化不足，基本概念和术语界定存在不一致。此外，部分引入的国外标准中，其术语定义更多是根据字面意思直接翻译外文，与我国相关概念的实际内涵有偏差，导致实际应用困难。

“体系化建设不足”：当前，我国工业信息安全标准建设不完善，一定程度上存在新旧标准关系不清、衔接性差、关联性不强的问题，通用标准和具备工业特色的标准还未有效衔接互补。

“落地应用困难”：一是行业标准缺乏，不同行业工业信息安全需求差异大，通用性国家标准很难满足行业需求，导致在实际应用中标准落地的指导性意义不强；二是标准宣贯不足，企业在标准应用中存在理解偏差等问题，导致标准应用不合规。

三、工业信息安全标准体系

2019 年以来，我国工业信息安全标准体系建设取得积极

进展。3 月，工业和信息化部和国家标准化管理委员会联合发布《工业互联网综合标准化体系建设指南》，其中第三章明确提出工业互联网标准体系框架，该体系框架从设备安全、控制系统安全、网络安全、数据安全、平台安全、应用程序安全、安全管理 7 个方面对工业互联网安全标准进行规划。8 月，工信部、教育部等十部门联合印发《加强工业互联网安全工作的指导意见》，指出要建立工业互联网安全标准体系，推动工业互联网设备、控制、网络（含标识解析系统）、平台、数据等重点领域安全标准的研究制定，建设安全技术与标准试验验证环境，支持专业机构、企业积极参与相关国际标准制定，加快标准落地实施。

（一）总体思路及目标

本白皮书根据《加强工业互联网安全工作的指导意见》等文件精神，以及《工业互联网综合标准化体系建设指南》和网络安全等级保护 2.0 安全框架的具体要求，按照**多维考虑、纵向分层、横向分类**的总体思想，构建工业信息安全标准体系框架，以指导标准编写单位体系化开展标准研制。其中纵向分层指按照工业企业、边缘接入、工业云平台、工业应用等自下而上的层次，纵向覆盖工业领域的相关安全标准。横向分类是指从多个维度分类提出工业信息安全标准，包括但不限于以下四个维度：

基础共性类：制定框架类、术语类标准规范；

安全防护类：制定设备和控制安全、平台安全、数据安全、标识解析安全、网络和通信安全、应用安全、安全管理等相关安全标准；

安全服务类：制定检查评估、检测认证、应急响应、监测预警、运维服务等安全服务类标准；

垂直行业类：制定汽车等典型行业应用标准。

（二）工业信息安全标准体系框架

工业信息安全标准体系主要由基础共性类标准、安全防护类标准、安全服务类标准、垂直行业类标准组成，如图 2 所示。

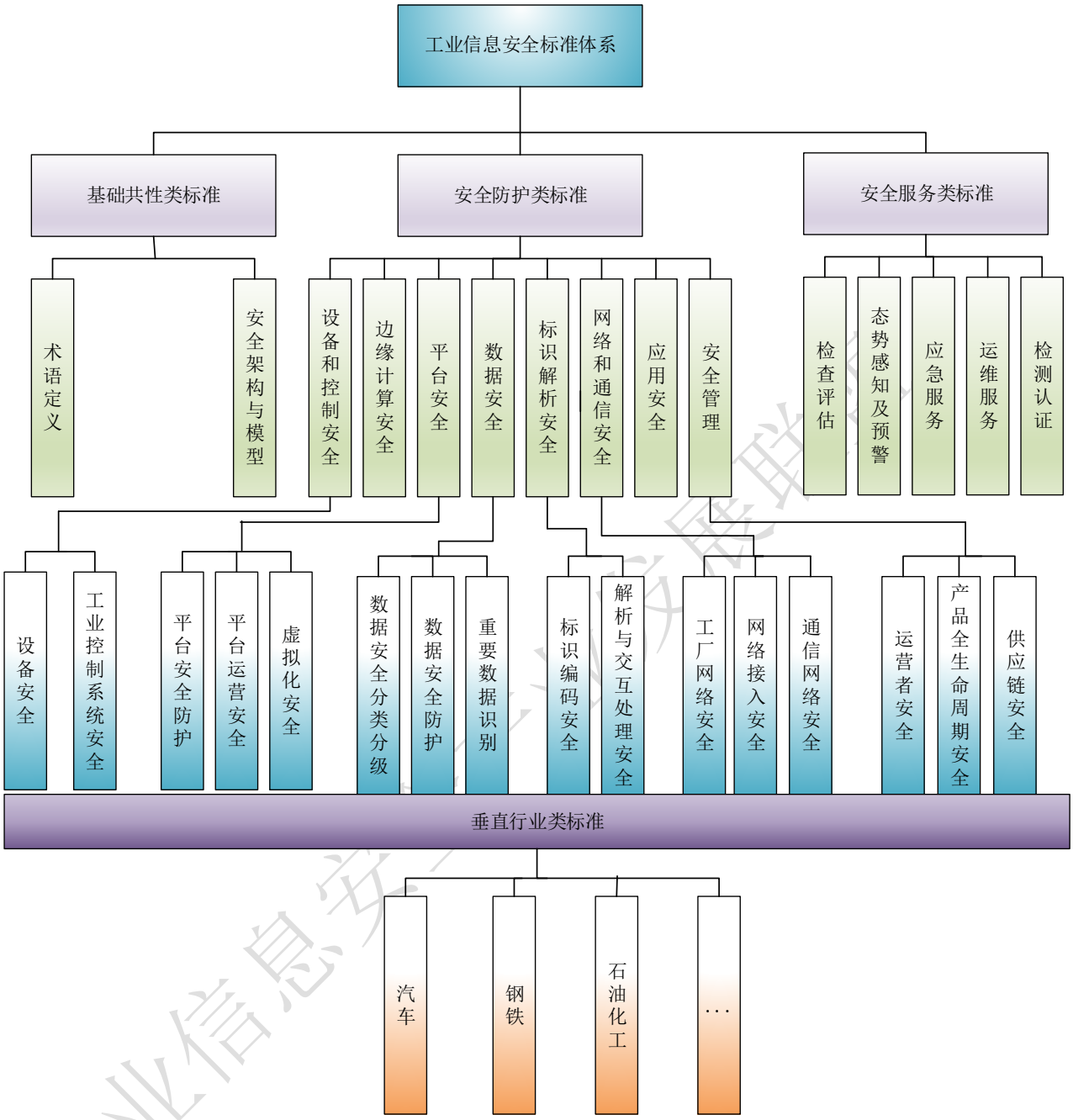

图 2 工业信息安全标准体系框架

1. 基础共性类标准

包括术语定义、安全架构与模型等标准，主要目的是规范工业信息安全相关概念、体系架构，明确界定工业信息安全的对象、边界、各部分的层级关系和内在联系，为其它相关标准的制定提供参考。

1.1 术语和定义

主要规范工业信息安全相关术语、概念，划分工业信息安全相关概念定义边界，统一定义语义，方便行业企业制定其它标准。

1.2 安全架构与模型

主要规范工业信息安全标准体系、体系架构及参考架构，明确各研究对象之间的关系。

2. 安全防护类标准

包括工业信息安全涉及的设备安全、控制安全、边缘计算安全、平台安全、数据安全、标识解析安全、网络和通信安全、应用安全、安全管理。

2.1 设备和控制安全

包括设备安全和控制安全两部分。设备安全主要规范工业领域中的关键设备及产品安全。控制安全主要规范工业控制系统自身安全及控制协议安全。在开展相关标准研制时，

可分别按照离散工业和流程工业的特点，对设备及控制系统提出相应的安全标准。

2.2 边缘计算安全

主要规范工业领域中的边缘设备安全、边缘智能安全等。包括边缘云安全、边缘网关安全、边缘设备接口安全等相关标准。

2.3 平台安全

主要提出工业互联网平台运行安全、工业微服务安全、平台互通安全等相关标准。

2.4 数据安全

主要提出工业领域数据安全分类分级、安全防护、安全共享、安全评估、重要数据识别、数据安全成熟度模型等相关标准。

2.5 标识解析安全

主要规范标识解析及解析中的数据交互安全要求，包括编码与存储、标识数据采集、标识解析、异构标识互操作等过程中的安全标准。

2.6 网络和通信安全

主要包括工业内外网接入安全、现场总线通信安全、工业无线通信安全等相关标准。

2.7 应用安全

主要包括工业 APP 等应用的开发安全、测试安全、运行安全等。

2.8 安全管理

主要包括工业运营者安全要求、产品全生命周期安全及供应链安全等标准。其中，工业运营者安全包括工业信息安全各相关主体的安全管理要求，如工控厂商安全管理要求、集成商安全管理要求、设计院安全管理要求、用户企业安全管理要求等。产品全生命周期安全包括产品建设、运行、维护等全生命周期的安全管理要求。供应链安全要求主要规范工业生产经营过程中的供应链安全管理。

3. 安全服务类标准

主要规范工业领域安全服务的方法、流程等要求。包括检查评估、态势感知及监测预警、应急响应、检测认证、运维服务等。

3.1 检查评估

主要规范工业领域系统、设备、产品等的安全检查、安全评估要素、方法和流程，提出安全检查指标、评估方法、评估模型等。

3.2 态势感知及预警

主要规范工业控制系统、工业现场等的安全态势感知、监测预警服务的安全要求。包括态势感知及监测预警系统建设规范、态势感知及监测预警技术规范、态势感知及监测预警体系建设等标准。

3.3 应急服务

主要规范工业控制系统、工业现场、工业互联网平台、工业数据等出现安全问题时的应急服务安全要求。包括应急服务流程、应急服务规则、应急处置方式等标准。

3.4 运维服务

主要规范工业控制系统、工业现场、工业互联网平台、工业数据等的安全运行维护操作规程、操作方式等。

3.5 检测认证

主要为工业控制系统、工业互联网平台、工业数据等的安全检测认证提供标准参考。

4. 垂直行业类标准

在基础共性类标准、安全防护类标准、安全服务类标准的基础上，面向汽车、钢铁、石油化工等重点行业领域，结合行业特色和需求，研制更具针对性、对行业更有指导作用的工业信息安全国家标准。

（三）重点标准化方向

未来，工业信息安全标准化工作应坚持“统筹规划、重点突出、急用先行”的原则，加快急需工业信息安全标准研制和标准体系建设，加强标准落地应用。

表 2 工业信息安全重点标准化方向

标准类别		标准名称	标准内容
基础共性类	安全架构与模型	工业信息安全　工业互联网安全体系框架	基于工业互联网的架构、安全防护需求等，从设备和控制安全、平台安全、数据安全、网络和应用安全等维度，研究提出工业互联网安全体系框架。
安全防护类	设备和控制安全	工业信息安全　工业互联网设备安全接入要求	针对工业控制设备、智能终端等工业互联网设备接入工业互联网平台时存在的安全问题及接入需求，从设备接入前安全评估、接入过程安全控制、接入后安全检测等方面，提出工业互联网设备安全接入要求。

	工业互联网平台安全	工业信息安全　工业互联网平台服务安全要求	针对工业互联网平台提供的服务，提出工业互联网平台服务安全要求，包括平台开发服务安全、工业 APP 服务安全等。
	边缘计算安全	工业信息安全　边缘计算安全要求	对工业互联网平台底层的边缘计算过程提出安全要求，包括边缘计算中的数据安全要求、边缘计算节点安全要求等。
	数据安全	工业信息安全　工业互联网数据分类分级与安全防护指南	从落实主体安全责任的角度，对工业互联网数据提出分类方法，从数据遭破坏产生的后果影响程度提出数据分级方法，从安全管理和技术的角度，对工业互联网数据提出不同级别的安全防护要求。
		工业信息安全　工业互联网数据交换共享安全	针对工业互联网数据交换与共享中的互信互任、权限控制、责任界定、安全共享等方面，提出工业互联网数据安全交换共享模型和要求。

		工业信息安全　工业互联网数据安全评估指标体系	根据工业互联网数据特点，从安全性、可控性、透明性等方面提出数据安全评估指标体系。
	标识解析安全	工业信息安全　标识解析与交互处理安全要求	根据工业互联网标识解析面临的安全问题，提出标识解析过程以及标识在各解析节点间的交互安全要求。
安全服务类	安全测试与评估	工业信息安全　工业互联网安全测试与评估指南	面向工业互联网平台、工业数据等，提出安全测试和评估的内容、方法和工作流程。

四、下一步工作建议

下一步应重点从以下三个方面，加快开展工业信息安全标准化工作:

一是定期更新。根据标准化工作进展、行业企业建议以及新技术新应用的发展情况，定期更新发布《工业信息安全标准化白皮书》，及时梳理新技术新概念新标准，为制定工业信息安全标准提供体系化参考，提高白皮书的实效性和实用性。

二是加强标准研制与落地。按照标准体系开展急需专用标准研制，加强标准宣贯培训和试点应用，切实发挥标准的指导作用，为解决行业、企业在工业信息安全管理和防护中

的痛点、难点提供标准参考。

三是加强沟通交流。应充分发挥各标准化技术委员会的作用，加强沟通合作。同时，标准承研单位应在标准研制过程中积极与相关标准化技术委员会进行沟通确认，充分考虑标准的衔接性和实用性，避免出现标准重复、冲突等现象。

附件 1：缩略语

DCS　Distributed Control System　集散控制系统

DHS　Department of Homeland Security　（美国）国土安全部

DISA　Defense Information Systems Agency　（美国）国防信息系统局

EDSA　Embedded device security Authentication　嵌入式设备安全保证

ERP　Enterprise Resource Planning　企业资源计划

ESD　Emergency Shutdown Device　紧急停车系统

IEC　International Electrotechnical Commission　国际电工技术委员会

IED　Intelligent Electronic Device　智能电子设备

IEEE　Institute of Electrical and Electronics Engineers　（美国）电气和电子工程师协会

ISA　International Society of Automation　国际自动化学会

ISO　International Organization for Standardization　国际标准化组织

MES　Manufacturing Execution System　制造执行系统

MMS　Manufacturing Message Specification　制造报文规范

MSB　Myndigheten för samhällsskydd och beredskap　瑞典民防应急局

NIST　National Institute of Standards and Technology　美国国家标准技术研究院

OLF　Norwegian Oil Industry Association　挪威石油工业协会

PCD　Process Control Domain　过程控制域

PLC　Programmable Logic Controller　可编程逻辑控制器

SAE　Society of Automated Engineers　自动机工程师学会

SCADA　Supervisory Control And Data Acquisition　数据采集与监控

SDLA　Security Development Lifecycle Authentication　安全开发生命周期保证认证

SIS　Safety Instrumented System　安全仪表系统

SSA　System Security Assurance　系统安全保证认证

V2X　Vehicle to Everything　车联网

WIB　荷兰国际仪器用户协会

附件 2：已发布、制定中的工业信息安全标准

附表 1 国外工业信息安全标准

序号	标准号	标准或技术文件名称（中文）	发布国家或组织机构
工业控制系统安全标准			
1	SP800-82	工业控制系统（ICS）信息安全指南	NIST
2	NIST IR 7628	智能电网安全指南	NIST
3	Version 1.1	改善关键基础设施网络安全框架	NIST
4	API1164	管道 SCADA 安全	NIST
5	IEC 62443	IEC 62443 工业通讯网络—网络和系统安全	IEC
6	无	工业控制系统安全评估指南	DHS&CPNI
7	无	工业控制系统远程访问配置管理指南	DHS&CPNI
8	AGA PeportNo.12	SCADA 通信加密保护规范	AGA
9	RG5.71	核设施网络安全措施	美国核管理委员会
10	无	过程控制和 SCADA 安全指南	英国 CPNI
11	M 2784-X-10	过程控制域（PCD）—供应商安全需求	WIB
12	OLF Guideline NO.104	过程控制、安全和支撑 ICT 系统的信息安全基线要求	OLF
13	OLF Guideline NO.110	工程、采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施	OLF
14	MSB 766	工业控制系统安全加强指南	MSB
15	IEC62210	电力系统控制和相关通信：数据和通信安全	IEC
16	AMURNA115	工业自动化系统的信息技术安全：制造工业中采取的约束措施	德国 NAMUR
序号	**标准号**	**标准或技术文件名称（中文）**	**发布国家或组织机构**
工业互联网安全标准			
1	无	工业互联网安全框架	IIC
2	无	工业 4.0 安全指南	德国

3	无	工业 4.0 与工业控制系统（ICS）行业的网络安全	ECS
云安全标准			
序号	**标准号**	**标准或技术文件名称（中文）**	**发布国家或组织**
1	ISO/IEC 27017:2015	基于 ISO/IEC27002 的云计算服务的信息安全控制措施使用规则	ISO/IEC JTC1/SC27
2	ISO/IEC 27018:2014	公共云计算服务的数据保护控制措施实用规则	ISO/IEC JTC1/SC27
3	ISO/IEC 27036-4:2016	供应商关系的信息安全—第四部分：云服务安全指南	ISO/IEC JTC1/SC27
4	NIST Special Publication 800-125	完全虚拟化技术安全指南	NIST
5	NIST Special Publication 800-144	公共云计算中安全与隐私	NIST
6	无	云计算—信息安全保障框架	ENISA/WG GROUP
7	无	政府云的安全和弹性	ENISA/WG GROUP
8	无	关键领域的云计算安全指南	SCA 标准建议
数据安全标准			
序号	**标准号**	**标准或技术文件名称（中文）**	**发布国家或组织**
1	NIST Special Publication 1500-4	大数据互操作性框架：大数据安全和隐私	NIST 数据组
2	NIST Special Publication 800-171B	非联邦系统和组织中受控非密信息的保护—关键程序和高价值资产的增强安全保护	NIST 数据组

附表 2 国内工业信息安全标准

工业控制系统安全标准				
序号	标准号或计划号	标准名称	所处状态	类型
1	GB/T 36323-2018	信息安全技术 工业控制系统安全管理基本要求	已发布	国家标准
2	GB/T 36324-2018	信息安全技术 工业控制系统信息安全分级规范	已发布	国家标准
3	GB/T 36466-2018	信息安全技术 工业控制系统风险评估实施指南	已发布	国家标准
4	GB/T 36470-2018	信息安全技术 工业控制系统现场测控设备通用安全功能要求	已发布	国家标准
5	GB/T 32919-2016	信息安全技术 工业控制系统安全控制应用指南	已发布	国家标准
6	GB/T 30976.1-2014	工业控制系统信息安全 第 1 部分：评估规范	已发布	国家标准
7	GB/T 30976.2-2014	工业控制系统信息安全 第 2 部分：验收规范	已发布	国家标准
8	GB/T33009.1-2016	工业自动化和控制系统网络安全集散控制系统（DCS）第 1 部分：防护要求	已发布	国家标准
9	GB/T33009.2-2016	工业自动化和控制系统网络安全集散控制系统（DCS）第 2 部分：管理要求	已发布	国家标准
10	GB/T33009.3-2016	工业自动化和控制系统网络安全集散控制系统（DCS）第 3 部分：评估指南	已发布	国家标准
11	GB/T33009.4-2016	工业自动化和控制系统网络安全集散控制系统（DCS）第 4 部分：风险与脆弱性检测要求	已发布	国家标准
12	GB/T33008.1-2016	工业自动化和控制系统网络安全可编程序控制器（PLC）	已发布	国家标准
13	GB/T 26333-2010	工业控制网络安全风险评估规范	已发布	国家标准
14	GB 30439	工业自动化产品安全要求	已发布	国家标准
15	GB/T 37934-2019	信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求	已发布	国家标准
16	GB/T 37954-2019	信息安全技术 工业控制系统漏洞检测技术要求及测试评价方法	已发布	国家标准
17	GB/T 37953-2019	信息安全技术 工业控制网络监测安全技术要求及测试评价方法	已发布	国家标准
18	GB/T 37993-2019	信息安全技术 工业控制系统专	已发布	国家标准

		用防火墙技术要求		
19	GB/T 37980-2019	信息安全技术 工业控制系统安全检查指南	已发布	国家标准
20	GB/T 37955-2019	信息安全技术 数控网络安全技术要求	已发布	国家标准
21	GB/T 37962-2019	信息安全技术 工业控制系统产品信息安全通用评估准则	已发布	国家标准
22	GB/T 37941-2019	信息安全技术 工业控制系统网络审计产品安全技术要求	已发布	国家标准
23	GA/T 1390.5-2017	信息安全技术 网络安全等级保护基本要求 第 5 部分：工业控制系统安全扩展要求	已发布	行业标准
24	JB/T 11962-2014	工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术	已发布	行业标准
25	DL/T 1941-2018	可再生能源发电站电力监控系统网络安全防护技术规范	已发布	行业标准
26	DL/T 1936-2018	配电自动化系统安全防护技术导则	已发布	行业标准
27	DL/T 1931-2018	电力 LTE 无线通信网络安全防护要求	已发布	行业标准
28	GB/T 21109.1-21109.3	过程工业领域安全仪表系统的功能安全	已发布	国家标准
29	GB/Z 34066-2017	控制与通信网络 CIP Safety 规范	已发布	国家标准
30	GB/T 36006-2018	控制与通信网络 Safety-over-EtherCAT 规范	已发布	国家标准
31	GB/T 36047-2018	电力信息系统安全检查规范	已发布	国家标准
32	GB/T 36572-2018	电力监控系统网络安全防护导则	已发布	国家标准
33	GB/T 37138-2018	电力信息系统安全等级保护实施指南	已发布	国家标准
34	20171279-T-469	工业控制系统产品信息安全 第 2 部分：安全功能要求	制定中	国家标准
35	20171280-T-469	工业控制系统产品信息安全 第 3 部分：安全保障要求	制定中	国家标准
36	20173583-T-469	信息安全技术 工业控制系统信息安全防护能力评价方法	制定中	国家标准
37	20170374-T-604	工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术	制定中	国家标准
38	20171744-T-469	信息安全技术 工业控制系统安全防护技术要求和测试评价方法	制定中	国家标准
39		信息安全技术 工业控制系统网络组件安全保障要求	研究项目	

40		工业控制系统安全控制成熟度模型	研究项目	
41		工业控制系统通信安全技术要求研究	研究项目	
42		工业控制系统信息安全实施指南	研究项目	
工业互联网安全标准				
序号	**标准号或计划号**	**标准名称（中文）**	**所处状态**	**类型**
1	GB/T 35673-2017	工业通信网络 网络和系统安全 系统安全要求和安全等级	已发布	国家标准
2	GB/T33007-2016	工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序	已发布	国家标准
3	JB/T 11961-2014	工业通信网络 网络和系统安全 术语、概念和模型	已发布	行业标准
4	JB/T 11962-2014	工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术	已发布	行业标准
5	2018-1369T-YD	工业互联网 数据安全保护要求	制定中	行业标准
6	AII/003-2018	工业互联网 安全总体要求	已发布	联盟标准
7	AII/004-2018	工业互联网平台 安全防护要求	已发布	联盟标准