工业安全产业观察

INDUSTRY OBSERVER

聚焦技术前沿 聚合产业生态 聚积工业力量

2021年（下）
www.ICSISIA.com

工业控制系统信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

联盟动态

政策与规划

产业生态

智库研究

成员资讯

官方微信

ICSISIA 2021下半年新增5家成员单位

2021年7月，工业控制系统信息安全产业联盟（ICSISIA）理事会正式通过5家新的成员单位加入，现有理事单位共计130家。

安徽信科共创信息安全测评有限公司
必维欧亚电气技术咨询服务（上海）有限公司
防特网信息科技（北京）有限公司
杭州迪普科技股份有限公司
上海宽域工业网络设备有限公司

2021年度工业安全系统典型应用案例征集遴选结果公示

为贯彻《工业控制系统信息安全防护指南》、落实“十四五”规划纲要“统筹发展和安全”等政策要求，充分发挥先进典型的引领示范作用，加快提升工业互联网安全防护能力，强化工业互联网安全综合保障能力，进一步推动我国工业安全产业高质量发展，工业控制系统信息安全产业联盟（ICSISIA)于2021年5月20日启动了2021年工业安全系统典型应用案例征集评选活动。经前期的积极推荐、专家评审等阶段，2021年度工业安全系统典型应用案例遴选结果公示。

2021年工业安全系统典型应用案例公示名单

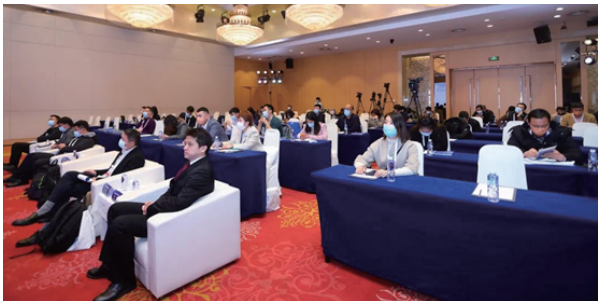
（排名不分先后）

序号	案例名称	申报单位
1	基于AI的钢铁行业工业控制系统安全防护建设	北京六方云信息技术有限公司
2	某新能源企业工控系统网络安全综合防御体系建设案例	北京珞安科技有限责任公司
3	智慧水务场景化工控安全建设项目	北京启明星辰信息安全技术有限公司
4	大连LNG工业控制系统安全防护	北京神州绿盟科技有限公司 国家管网集团大连液化天然气有限公司
5	某钢铁企业工业互联网安全集成项目	北京圣博润高新技术股份有限公司
6	卡奥斯-双湃工业安全态势感知平台	北京双湃智安科技有限公司 青岛海尔工业智能研究院有限公司
7	油气管道工业控制系统网络安全防护方案	北京天地和兴科技有限公司
8	基于行为基线分析的制造企业安全防护体系设计与应用	北京天融信网络安全技术有限公司
9	锌电集团工业控制系统安全解决方案	北京网御星云信息技术有限公司
10	钢铁行业自动化工业网络安全防御解决方案	长扬科技（北京）有限公司
11	发电行业网络靶场平台建设	烽台科技（北京）有限公司 国核自仪系统工程有限公司
12	智能制造企业工业互联网平台安全防护建设	杭州安恒信息技术股份有限公司
13	轨道交通综合监控系统解决方案	杭州立思辰安科科技有限公司
14	即插即用不改变原应用的油田生产数据安全传输及数据库授权加密存储	南京讯石数据科技有限公司
15	大唐三门峡电厂2X1000MW机组网络安全改造项目	宁波和利时信息安全研究院有限公司
16	冶金企业网络安全防护平台建设	奇安信科技集团股份有限公司
17	基于等保2.0的石化企业工控网络安全技术防护应用	青岛海天炜业过程控制技术股份有限公司
18	广西广投新材料集团网络安全项目（II标段）	深圳融安网络科技有限公司
19	省级天然气管道工控系统网络安全及防护体系研究与应用项目	浙江国利网安科技有限公司
20	电力行业高仿真虚拟化融合工控安全实验室	浙江木链物联网科技有限公司

“十四五”加持 共建工业安全生态——2021世界智能制造大会智能制造安全保障论坛举办

由江苏省人民政府、工业和信息化部、中国工程院、中国科学技术协会共同主办的2021世界智能制造大会12月7日～10日在南京拉开帷幕。

大会首日，以“‘十四五’加持 共建工业安全生态”为主题的智能制造安全保障论坛在国际博览中心隆重举办。论坛由国际智能制造联盟、中国自动化学会、中国光学工程学会承办，智能制造推进合作创新联盟、工业控制系统信息安全产业联盟、边缘计算产业联盟、OICT学院协办，汇聚众多业内资深专家、杰出企业代表，共同探讨智能制造目标下工业安全的技术创新、方案应用、产业生态、发展前瞻。中国自动化学会副秘书长、武汉大学教授张俊主持论坛。



会议现场

中国自动化学会副秘书长、武汉大学教授张俊主持论坛

中国科学院院士、中国自动化学会特聘顾问/会士、北京控制工程研究所研究员吴宏鑫为论坛作开幕致辞，他强调，提升我国智能制造的安全防护水平成为实现制造业高质量发展的重要基础。自主可控是保障网络安全、信息安全的前提。工业企业已经意识到安全保障的重要性，更要加大力度，完善提高智能制造的安全技术和管理水平。

中国科学院院士、中国自动化学会特聘顾问/会士、北京控制工程研究所研究员吴宏鑫

中国工程院院士沈昌祥带来题为“打造工业控制安全可信主动免疫新生态“的报告。能源局电力行业信息安全等级保护测评中心第三实验室副主任黄益彬、中国电子技术标准化研究院网络安全研究中心副主任李琳、菲尼克斯（中国）投资有限公司智能技术与工程部总监张龙、中国信息通信研究院安全研究所两化安全部主任柯皓仁、江苏启明星辰信息安全技术有限公司副总经理雷慧桃、博智安全科技股份有限公司副总裁胡志锋、布里斯托大学助理教授、信息物理融合系统安全专家Sridhar Adepu分别带来精彩报告。

随着全球新一轮科技革命和产业变革深入发展，为制造业高端化、智能化、绿色化发展提供了历史机遇。工业控制系统作为工业核心组成部分，其安全事关工业生产运行、国家经济安全和人民生命财产安全。本次会议通过线上、线下相结合的方式，为观众呈现了一场关于智能制造安全保障政策、技术、产品和解决方案的盛宴。希望业内同仁以自主可控、安全可信作为工作目标，为建设我国成为网络强国而共同努力。

OICT学院V期刊创刊号发布，聚焦工业互联网，聆听专家与企业声音

今天，工业互联网发展已经到了非常重要的历史机遇期，我国把发展工业互联网作为制造业高质量发展，特别是经济社会高质量发展的一个重要抓手。

近年来，特别是工业互联网创新战略实施以来，在产学研用各方的积极参与、共同推动下，我国工业互联网发展在网络、平台、安全、应用等方面都取得了显著成效。

尽管工业互联网的成绩已经初见端倪，但显然我国工业互联网的发展之路仍任重而道远。

扫描二维码，即可观看OICT学院V期刊第一期视频。

2021年度优质工业安全服务商评选活动启动

由中国自动化学会主办，智能制造推进合作创新联盟、中国仪器仪表行业协会、工业控制系统信息安全产业联盟、边缘计算产业联盟、全国机械安全标准化技术委员会、全国工业过程测量控制和自动化标准化技术委员会协办，控制网（www.kongzhi.net）&《自动化博览》、OICT学院承办的2022中国自动化产业年会（CAIAC2022）暨第十七届中国自动化产业世纪行将以“绿色驱动 数字赋能，智领自动化新未来”为主题，全方位探讨在新一轮科技革命和产业变革背景下，中国自动化产业如何推动制造业实现绿色低碳发展，引领中国工业的数字化转型之路。“2021中国自动化领域年度人物、年度团队、年度企业、年度创新成长企业、年度最具影响力工程项目、年度最具价值解决方案、年度最具竞争力创新产品、用户信赖产品、年度优质工业安全服务商”9大奖项评选已启动。

扫描二维码，即可下载“2021年度优质工业安全服务商”推荐表进行推荐。

发改委等四部门联合印发《能源领域5G应用实施方案》，强调加大安全保障能力建设

2021年6月，国家发展改革委、国家能源局、中央网信办、工业和信息化部近日联合印发《能源领域5G应用实施方案》。在能源安全方面，强调加大相关基础设施和安全保障能力建设，构建5G应用安全保障体系。依托先进密码、身份认证、加密通信等技术，研究适用于能源领域5G应用场景下的用户、数据、设备与网络之间信息传递、保存、分发的信息通信安全防护体系，确保5G融合应用相关网络基础设施和核心系统安全。健全能源领域5G应用安全技术标准，建立网络稳定运行保障机制、电力终端入网安全认证机制、网络切片隔离安全、分场景的业务安全测评和监测机制，提升5G网络作为能源基础通讯网络的可靠性，避免在极端条件下影响能源领域安全生产。鼓励国家级权威测评机构开展能源领域5G应用网络安全测评和认证工作。落实5G网络安全指南性文件，统筹安全与发展，将5G网络安全保障纳入能源领域5G应用的全流程全环节。

工信部印发《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》

2021年7月12日，为加快建设创新能力强、产业结构优、供给质量高、需求释放足、产融合作深、人才队伍专的健康有序产业发展生态，推动网络安全产业实现技术先进、产业发达的高质量发展目标，不断提升网络安全产业综合实力和国家网络安全保障能力，工业和信息化部起草了《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》（以下简称：《计划》）。《计划》提出，到2023年，网络安全技术创新能力明显提高，产品和服务水平不断提升，经济社会网络安全需求加快释放，产融合作精准高效，网络安全人才队伍日益壮大，产业基础能力和综合实力持续增强，产业结构布局更加优化，产业发展生态健康有序。

工信部、网信办、公安部联合印发《网络产品安全漏洞管理规定》

2021年7月12日，工业和信息化部、国家互联网信息办公室、公安部联合印发《网络产品安全漏洞管理规定》（以下简称：《规定》）。《规定》旨在维护国家网络安全，保护网络产品和重要网络系统的安全稳定运行；规范漏洞发现、报告、修补和发布等行为，明确网络产品提供者、网络运营者，以及从事漏洞发现、收集、发布等活动的组织或个人等各类主体的责任和义务；鼓励各类主体发挥各自技术和机制优势开展漏洞发现、收集、发布等相关工作。《规定》已于9月1日起施行。

工信部：印发《新型数据中心发展三年行动计划（2021-2023年）》，提出开展数据中心安全可靠保障行动

2021年7月，工业和信息化部印发《新型数据中心发展三年行动计划（2021-2023年）》，强调统筹发展与安全，进一步强化网络和数据安全管理和能力建设，构建完善的安全保障体系。提出安全可靠保障行动任务，完善新型数据中心安全监测体系。建立政企联动的数据安全风险监测机制和技术手段，围绕数据中心网络汇聚、传输、存储等重要环节，建设数据安全监测技术平台，切实提升数据资源安全保障能力。开展网络安全技术能力评估。数据中心上线前，开展网络安全风险评估、隐患排查和防护能力认证。针对数据中心云化趋势，定期开展镜像安全、进程行为、容器逃逸等安全检测评估。强化新型数据中心可靠性。加强数据中心多活架构的研究与部署，实现跨数据中心的故障转移和恢复。

李克强签署国务院令公布《关键信息基础设施安全保护条例》

2021年7月30日，国务院总理李克强签署第745号国务院令，公布《关键信息基础设施安全保护条例》（以下简称《条例》），《条例》的出台旨在落实《中华人民共和国网络安全法》有关要求，将为我国深入开展关键信息基础设施安全保护工作提供有力法治保障。已于2021年9月1日起施行。

国家互联网信息办公室等五部门发布《汽车数据安全管理若干规定（试行）》

2021年8月16日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》（以下简称《规定》）。《规定》强调，汽车数据处理者开展重要数据处理活动，应当遵守依法在境内存储的规定，加强重要数据安全保护；落实风险评估报告制度要求，积极防范数据安全风险；落实年度报告制度要求，按时主动报送年度汽车数据安全管理情况。因业务需要确需向境外提供重要数据的，汽车数据处理者应当落实数据出境安全评估制度要求，不得超出出境安全评估结论违规向境外提供重要数据，并在年度报告中补充报告相关情况。《规定》已于2021年10月1日起施行。

八部门印发《物联网新型基础设施建设三年行动计划（2021—2023年）》

2021年9月，工业和信息化部、中央网络安全和信息化委员会办公室、科学技术部、生态环境部、住房和城乡建设部、农业农村部、国家卫生健康委员会、国家能源局等八部门联合印发《物联网新型基础设施建设三年行动计划（2021-2023年）》。《行动计划》提出四大行动12项重点任务，明确到2023年底，构建一套健全完善的物联网标准和安全保障体系。提出依托科研机构与联盟协会，从加强物联网卡安全管理、建设面向物联网密码应用检测平台以及安全公共服务平台、打造“物联网安心产品”等方面发力，提升物联网安全技术应用水平和安全公共服务能力。

信安标委：发布TC260-001《汽车采集数据处理安全指南》

2021年10月8日，全国信息安全标准化技术委员会发布了我国首个汽车数据安全技术文件TC260-001《汽车采集数据处理安全指南》（以下简称：《指南》），《指南》规定了汽车制造商对汽车采集数据的传输、存储和出境等处理活动的安全要求，为汽车制造商开展汽车的设计、生产、销售、使用、运维提供数据保护实施规范，同时也为主管监管部门、第三方评估机构等对汽车采集数据处理活动进行监督、管理和评估提供依据。

工信部组织开展2021年工业互联网试点示范项目申报工作，涵盖安全集成创新

为深入实施工业互联网创新发展战略，促进工业互联网融合应用，工信部于2021年10月21日印发通知，组织开展2021年工业互联网试点示范项目申报工作。通知提出，将围绕网络集成创新、平台集成创新、安全集成创新、园区集成创新4大类17个具体方向，遴选一批工业互联网试点示范项目，试点示范期为2年。

工信部印发《物联网基础安全标准体系建设指南（2021版）》

2021年10月，工信部印发《物联网基础安全标准体系建设指南（2021版）》。提出到2022年，初步建立物联网基础安全标准体系，研制重点行业标准10项以上，明确物联网终端、网关、平台等关键基础环节安全要求，满足物联网基础安全保障需要，促进物联网基础安全能力提升。到2025年，推动形成较为完善的物联网基础安全标准体系，研制行业标准30项以上，提升标准在细分行业及领域的覆盖程度，提高跨行业物联网应用安全水平，保障消费者安全使用。

国家互联网信息办公室印发《网络数据安全管理条例（征求意见稿）》

为规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，根据国务院2021年立法计划，国家互联网信息办公室会同相关部门研究起草《网络数据安全管理条例（征求意见稿）》，于2021年11月发布。

工信部发布《“十四五”软件和信息技术服务业发展规划》，强调安全可控、安全服务保障

2021年11月30日，工信部印发《“十四五”软件和信息技术服务业发展规划》（以下简称：《规划》）。《规划》强调坚持发展和安全并重，实现质量、规模、效益、安全相统一，提出强化安全服务保障，开展软件数据安全、内容安全评估审查，加强软件源代码检测和安全漏洞管理能力，提升开源代码、第三方代码使用的安全风险防控能力。鼓励第三方服务机构，积极提升软件安全咨询、培训、测试、认证、审计、运维等服务能力。开展工业信息安全防护能力贯标，持续完善国家工业控制系统信息安全态势感知网络，鼓励产业链开展典型工业控制系统的联合攻关和集成应用，提升工业控制系统本质安全水平。

工信部组织开展工业领域数据安全管理试点工作

为探索构建工业领域数据安全管理体系，有效保障数据安全，推动数字经济高质量发展，工信部于2021年12月14日印发通知，组织开展工业领域数据安全管理试点工作。将贯彻落实《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规，指导省级工业和信息化主管部门组织开展数据安全管理试点，督促企业落实数据安全主体责任，加强数据分类分级管理、安全防护、安全评估、安全监测等工作，提升数据安全防护能力。加强试点成果转化应用，完善工业领域数据安全制度规范和工作机制，遴选一批示范企业、优秀产品和典型解决方案，形成可复制可推广的管理模式，促进提升行业数据安全保护水平。

《智能网联汽车数据安全共享参考架构》（T/TIAA 020—2021）团体标准发布

6月4日，《智能网联汽车数据安全共享参考架构》（T/TIAA 020—2021）团体标准正式发布，该标准由电子科技大学牵头联合国家工业信息安全发展研究中心、中国第一汽车集团有限公司、中国汽车技术研究中心有限公司、吉利汽车研究院（宁波）有限公司等二十余家机构共同编制。

本标准提出了智能网联汽车的数据安全共享参考架构，明确了智能网联汽车数据共享架构的参与方（数据提供方、使用方、共享运营方），定义了数据服务接口、数据共享交换流程以及具体业务流程中涉及的安全要素，如密码算法的应用、身份管理、审计控制等。标准以数据不出库为基本原则，提出了应对数据提供方的源数据进行预处理、针对共享架构设计安全机制等多项要求，以保障数据共享交换的安全合规及数据权益，实现数据资产的有序管理和流通。适用于具有智能网联汽车数据收集能力的车厂和需要汽车数据进行数据支撑的服务方，能够为智能网联汽车数据产业链上的各相关方安全合规使用数据提供参考和借鉴。

工信部部署推进2021年基础电信企业行业数据安全标准贯标工作

为督促指导基础电信企业贯彻落实《数据安全法》，加强数据安全管理工作，7月9日，工业和信息化部网络安全管理局组织召开全国视频会议，部署开展2021年基础电信企业行业数据安全标准贯标工作，并对《基础电信企业数据分类分级方法 》《基础电信企业重要数据识别指南》《电信和互联网数据安全评估规范》三项标准进行宣贯讲解。

会议强调，数据已成为关键性生产要素，数据安全事关国家安全和社会经济发展。基础电信企业是信息通信行业数据安全的“基本盘”，扎实做好数据安全标准贯标工作，既是深入贯彻落实习近平总书记重要批示指示精神和党中央国务院决策部署的根本要求，也是全面落实《数据安全法》的具体实践。

中国信通院发布《数据安全治理实践指南（1.0）》

2021年7月14日，中国信通院云计算与大数据研究所所长何宝宏发布了《数据安全治理实践指南（1.0）》（以下简称“指南”）。《指南》参考数据安全领域的相关标准，重点以中国互联网协会T/ISC-0011-2021《数据安全治理能力评估方法》为基础，阐述了数据安全治理的内涵；从组织如何落实数据安全治理要求的角度出发，提出数据安全治理总体视图；按照数据安全治理目标、治理框架、治理实践路径分别提出落地建议，并对未来发展进行展望。此外，指南还收录了部分企业开展数据安全治理的实践经验。

工信部：车联网身份认证和安全信任试点项目名单公示

2021年8月20日，根据《关于开展车联网身份认证和安全信任试点工作的通知》，经单位申报、专家评审、网上公示等环节，工信部确定了车联网身份认证和安全信任试点项目名单并予以公布。新能源和智能网联汽车车联网身份认证和安全信任体系建设项目等61个试点项目上榜，同时要求各入选项目申报单位按照试点实施方案、相关安全标准和技术指南要求，扎实推进试点工作，加速车联网安全技术创新研发，高质量建设车联网身份认证技术系统和设施，积极接入车联网安全信任行业根和区域根、工业和信息化部车联网安全信任根管理平台，推动提升我国车云、车车、车路、车设备等场景安全通信保障能力，形成车联网安全通信优秀解决方案，加快全国规模化应用推广。

中电标协印发《信息安全技术 石油炼化工业控制系统信息安全防护能力要求》团体标准征求意见稿

2021年8月，中国电子工业标准化技术协会团体标准促进工作委员会印发通知，《信息安全技术 石油炼化工业控制系统信息安全防护能力要求》团体标准（项目号：CESA-2021-2-035）征求意见稿的编制工作已完成。本标准规定了石油炼化工业控制系统信息安全防护能力要求，包括安全管理要求、安全技术要求和安全运维要求，适用于石油炼化行业开展工业控制系统信息安全防护设计、建设、运维等工作。

工信部网络安全威胁和漏洞信息共享平台正式上线运行

为落实《网络产品安全漏洞管理规定》有关要求，工业和信息化部网络安全管理局组织建设的工业和信息化部网络安全威胁和漏洞信息共享平台（以下简称：平台）（https://www.nvdb.org.cn）于2021年9月1日正式上线运行。

根据《网络产品安全漏洞管理规定》，网络产品提供者应当及时向平台报送相关漏洞信息，鼓励漏洞收集平台和其他发现漏洞的组织或个人向平台报送漏洞信息。平台包括通用网络产品安全漏洞专业库（https://www.cnvdb.org.cn）、工业控制产品安全漏洞专业库（https://www.cics-vd.org.cn）、移动互联网APP产品安全漏洞专业库（https://cappvd.cstc.org.cn）、车联网产品安全漏洞专业库（https://cavd.org.cn）等，支持开展网络产品安全漏洞技术评估，督促网络产品提供者及时修补和合理发布自身产品安全漏洞。

平台由中国信息通信研究院会同国家工业信息安全发展研究中心、中国软件评测中心、中国汽车技术研究中心等国家网络安全专业机构共同建设。

工信部：第一批网络关键设备安全检测结果公布

根据《中华人民共和国网络安全法》《关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测认证机构名录（第一批）的公告》（国家认监委、工业和信息化部、公安部、国家互联网信息办公室公告2018年第12号），2021年9月，工信部公布由具备资格的机构按照《网络关键设备安全通用要求》（GB40050-2021）强制性国家标准，经安全检测符合要求的网络关键设备（第1批）名单。

序号	设备名称	型号	生产企业	检测报告编号	有效期	检测机构
1	路由器	NE5000E-X16A	华为技术有限公司	01-21-N00001	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室
2	路由器	NE5000E-20	华为技术有限公司	01-21-N00002	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室
3	交换机	CE16804	华为技术有限公司	01-21-N00003	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室
4	交换机	CE16808	华为技术有限公司	01-21-N00004	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室
5	交换机	S12508F-AF	新华三技术有限公司	01-21-N00005	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室
6	交换机	S12516F-AF	新华三技术有限公司	01-21-N00006	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室
7	服务器	TS860M5	浪潮电子信息产业股份有限公司	01-21-N00007	2021年8月5日至2024年8月4日	中国信息通信研究院泰尔实验室

风电行业首个工控安全自动核查系统在国家能源集团研发成功

现今在发电企业的网络安全核查中，业内机构普遍采用手动人机接口输入方式，获取和核查企业信息系统的访问控制权限、审计信息、防病毒措施、漏洞存量和系统版本的安全等级，存在核查效率低、核查信息遗漏、核查结果不准确等现象，严重影响核查质量，也为企业网络安全埋下隐患。2021年10月，国家能源集团龙源中能公司成功研发行业内首个工控安全自动化核查系统，该系统可快速实现网络安全核查并统计结果，极大提高工作效率，利于电力行业网络安全核查的标准化作业，推动工控网络安全核查的自动化进程。

国家等保办撤销等保测评机构推荐证书

2021年11月19日，国家网络安全等级保护工作协调小组办公室发布公告，为贯彻落实国务院“放管服”改革要求，不断提升网络安全等级测评机构管理工作的规范化、专业化和社会化水平，经研究决定，自即日起，国家网络安全等级保护工作协调小组办公室撤销网络安全等级测评机构推荐证书，不再发布《全国网络安全等级测评机构推荐目录》，相关工作纳入国家认证体系。

《湖南省网络安全和信息化条例》通过，2022年1月1日起施行

为了保障网络安全，促进信息化发展，提高数字化水平，推进经济社会高质量发展，根据有关法律、行政法规，结合湖南省实际，制定《湖南省网络安全和信息化条例》（以下简称：《条例》）。《条例》于2021年12月3日湖南省第十三届人民代表大会常务委员会第二十七次会议通过，自2022年1月1日起施行。

2021年工业互联网安全标准体系正式发布

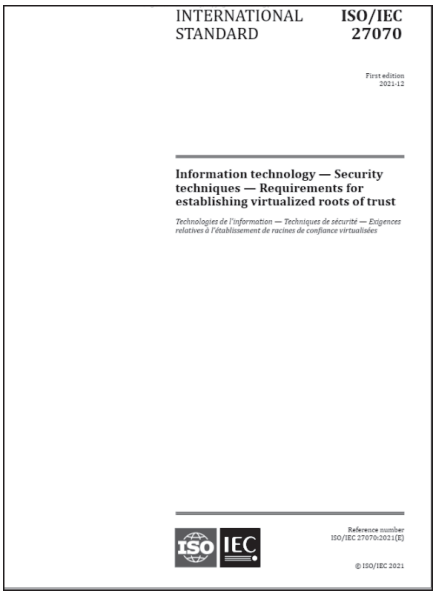
为系统推进工业互联网安全标准体系研究，加快基础共性、关键技术、典型应用等产业亟需标准制定，2021年12月，在工业和信息化部网络安全管理局指导下，工业互联网产业联盟、工业信息安全产业发展联盟、工业和信息化部商用密码应用推进标准工作组共同发布《工业互联网安全标准体系（2021年）》。

工业互联网安全标准体系包括分类分级安全防护、安全管理、安全应用服务等3个类别、16个细分领域以及76个具体方向，对切实发挥标准规范引领作用、加快建立网络安全分类分级管理制度、强化工业互联网企业安全防护能力、推动网络安全产业高质量发展具有重要支撑作用。

信安标委：我国主导提出的国际标准ISO/IEC 27070《信息技术 安全技术 虚拟信任根建立要求》正式发布

2021年12月，我国主导提出的国际标准ISO/IEC 27070《信息技术 安全技术 虚拟信任根建立要求》正式发布，该标准通过功能视图和活动视图两种视角规定了建立虚拟信任根的要求。

ISO/IEC 27070用于解决云计算服务应用和发展中信任的核心问题，可以指导企业与研究机构增强云服务基础设施的安全性，提升用户信心，也可以规范企业安全增强开发的技术架构、协议、接口，促进不同企业间的互联互通和行业间的规范发展，有助于可信计算产业的积极落地和实施。


INTERNATIONAL STANDARD
ISO/IEC 27070
First edition 2021-12
Information technology — Security techniques — Requirements for establishing virtualized roots of trust
Technologies de l'information — Techniques de sécurité — Exigences relatives à l'établissement de racines de confiance virtualisées
ISO IEC
Reference number ISO/IEC 27070:2021(E)
© ISO/IEC 2021

电子四院：物联网领域商用密码应用分析与展望

当前，物联网、人工智能、大数据等新一代信息技术不断发展，推动人类社会从“信息化”向“网络化”“智能化”转变，开启了万物互联新时代。与此同时，复杂的万物互联环境使得网络空间面临迥异以往的严峻安全挑战。密码作为国家重要战略资源，是保障网络空间安全的核心技术和基础支撑，是解决物联网环境下网络安全问题的重要手段。本文针对物联网领域密码应用情况开展了集中研究，系统梳理了物联网领域密码应用现状，深入分析了存在的问题和困难，并研究提出了下一步建议。

扫描二维码，查看全文精彩内容。

沈昌祥院士：打造工业控制安全可信主动免疫新生态（附PPT全文）

2021年12月7日，以“‘十四五’加持 共建工业安全生态”为主题的2021世界智能制造大会智能制造安全保障论坛在南京隆重举办。中国工程院院士沈昌祥带来题为《打造工业控制安全可信主动免疫新生态》的报告。作为中央网信办专家咨询委员会顾问、国家集成电路产业发展咨询委员会委员、国家三网融合专家组成员，沈院士从构筑网络主动免疫保障体系、筑牢关键信息基础设施网络安全防线，以及构建等保2.0与可信计算3.0新型产业空间几个方面，分析了我国工控安全的整体现状和发展趋势。

扫描二维码，查看全文精彩内容。

长扬科技完成E2轮1亿元战略融资，E轮合计2.75亿元

2021年7月，长扬科技完成E2轮1亿元战略融资，本轮由青岛国投、中航基金、国新南方、联创永宣、国君资本联合投资，其中，联创永宣为原股东持续加持。至此，长扬科技E轮融资已全部到位， E1+E2合计2.75亿元。在国有资本的持续加持下，长扬科技股东中的国有资本股权比例已近50%。

绿盟科技联合腾讯安全发布《2021上半年全球DDoS威胁报告》

2021年9月，绿盟科技联合腾讯安全发布《2021上半年全球DDoS威胁报告》（以下简称：《报告》），基于对2021上半年监测到的数据情况进行统计分析，全面盘点了过去半年中DDoS攻击的发展态势。《报告》指出，在疫情影响下，各类企业业务持续线上迁移，DDoS攻击次数已连续4年高速增长，且量级强度、手段方式、攻击来源相较以往都有明显的升级变化。针对越发复杂的网络安全环境，《报告》还结合实际案例为企业DDoS攻击防护提供了实用性建议。

珞安科技连续完成B+、B++两轮融资，金额1亿元

2021年8月，珞安科技连续完成B+、B++两轮战略融资，合计融资金额1亿元人民币。B+轮融资由容腾5G产业基金、上汽产业基金联合投资，B++轮融资由背靠苏州工业园区的品牌基金元禾重元独家投资。继获得深信服旗下琥珀资本领投，加盛投资、同创伟业追投的B轮融资后，再次引入多家产业战略投资方。

浙江大学-安恒信息前沿技术联合研究中心正式成立

2021年8月9日，浙江大学-安恒信息前沿技术联合研究中心（以下简称：联合研究中心）在浙江大学紫金港校区正式成立。中国科学院院士、浙江大学校长吴朝晖和安恒信息董事长范渊出席仪式并发表致辞。未来，联合研究中心将依托浙江大学雄厚的科研实力和安恒信息丰富的行业实践，聚焦于大数据安全、云安全、物联网安全、AI安全等前沿领域，持续开展前沿信息技术研究，形成对学术界与产业界的引领性影响力，并将科研成果转化为国家安全力量，共筑网络安全防线，为网络信息安全行业发展添砖加瓦，为推动数字化改革浪潮贡献力量，助力安全中国。

共建车联网安全生态，360发布“车联网安全守护计划”

随着国家相关部委接连出台车联网安全相关标准体系以及法规条例，对健全车辆全生命周期的网络安全防护体系提出了明确要求。为助力车企应对安全新挑战，化解车企转型中遇到的安全难题，2021年8月23日，360政企安全集团正式发布“车联网安全守护计划”，“计划”将逐步开放车端IDPS能力及相关源码，并免费提供SaaS化VSoC监测服务，以满足国内外法规标准要求和车企的安全监测需求，提升企业对汽车的安全监测及资产管理能力、网络安全响应与防护能力，助力车企建立自有的汽车安全运营体系。

威努特与中国电子技术标准化研究院共建联合实验室

2021年10月21至22日，由中国电子技术标准化研究院、中国电子工业标准化技术协会主办的“2021 新一代信息技术标准化论坛”在深圳举行。论坛期间举办了举行了电子信息产品标准化国家工程实验室首批联合实验室落地深圳的揭牌仪式。威努特与中国电子技术标准化研究院合作，依托电子信息产品标准化国家工程实验室，共建工业控制设备漏洞检测联合实验室。双方将加快落实国家《关键信息基础设施保护条例》等重要政策文件，促进工业领域网络安全和工业互联网网络安全生态体系建设，依托各自优势资源，在工控网络安全和工业互联网网络安全政策法规与技术研究、标准研制与示范验证、科技项目合作、资源共享、市场宣传和人才培养等方面展开全面深入合作，促进双方科技创新和成果转化。

奇安信发布业内首个“数据安全能力框架”

大数据DT时代，数据应用场景和参与主体的日益多样化，数据安全体系建设必须抛弃传统的单点防御模式，而要采用全局治理的体系化建设思路。为此，奇安信集团于2021年8月30日正式发布“数据安全能力框架”，以及“数据安全运行构想图”（数据安全ConOps），旨在为数字化转型不断深入的大型政企客户以及业内伙伴，提供基于甲方视角的数据安全全面图景，以及一条构建大数据安全体系的可行道路。

启明星辰蓝鲸实验室正式揭牌

2021年9月27日，启明星辰蓝鲸实验室揭牌仪式在启明星辰大厦成功举办。蓝鲸实验室由启明星辰专业攻防技术专家组成，聚焦网络安全实战化攻防技术研究和场景化创新应用，以场景模拟、实战靶场、红蓝对抗、人才培养、远程托管、应急演练和安全保障七大核心能力为支撑，打造基于实战的场景化解决方案，提升用户网络安全防护能力。同时，针对当前攻防对抗的复杂性和动态性，蓝鲸实验室将不断完善和开创新的攻防策略和技术战法，并通过实战化场景模拟演练环境，进一步融合创新场景应用和最佳实践，结合场景模拟沙盘推演和实战演练，以达到提升攻防核心技术能力和企业安全保障方案的实用性，实现国内企业网络安全防护能力目标。

神州龙芯成功挂牌

2021年11月9日，神州龙芯智能科技有限公司正式在江苏股权交易中心官网科创板（俗称“四板”）成功挂牌。证券简称：神州龙芯，企业代码：651567。江苏“科创板”的挂牌是公司成长道路上的一个里程碑，是公司正式踏入中国资本市场的第一步，公司将充分利用资本市场打造国家级自主可控工业芯片龙头企业，加大自主可控核心技术研发力度，打造具有市场竞争力的产品，满足国内外市场需求。同时，进一步完善公司法人治理结构，规范企业的经营管理，增强企业核心竞争力，努力实现公司的高速健康发展。

国家工业信息安全发展研究中心发起成立关键软件密码应用研究中心

为进一步推动产业发展，更好地汇聚产学研用各方力量，聚焦关键软件领域密码应用核心问题，不断夯实软件产业发展基础，共同推动软件产业和密码技术融合发展，2021年12月18日，“2021年商用密码应用创新高端研讨会”在经开区国家信创园成功召开。会上，国家工业信息安全发展研究中心联合北京理工大学、北京电子科技学院、龙芯中科技术股份有限公司、麒麟软件有限公司、北京炼石网络技术有限公司等18家首批成员单位等共同组建成立“关键软件密码应用研究中心”。该中心将充分发挥行业的桥梁纽带作用，动员社会力量参与国家商用密码与关键软件的融合应用工作，为我国软件产业发展提供安全保障。

后续，国家工业信息安全发展研究中心将联合产业界相关单位，利用好关键软件密码应用研究中心这个平台，围绕关键软件密码应用技术研究、国产密码和关键软件的兼容适配攻关、重点行业试点示范应用、密码应用人才培养等方面开展相关工作，推动我国软件密码应用生态体系建设，助力软件产业高质量发展。

烽台科技与首自信签署战略合作协议 融合双方优势共创钢铁行业协调发展新模式

2021年10月，烽台科技（北京）有限公司与北京首钢自动化信息技术有限公司签署战略合作协议。根据《协议》，双方将充分发挥各自在钢铁行业自动化、信息化与工控安全领域的优势，打造钢铁行业工业互联网+安全生产解决方案创新模式，形成优势互补、各具特色、共建共享的协同发展格局，共同助力钢铁行业工业互联网安全生产更高质量、一体化发展。

此次战略签约，双方将共同打造钢铁行业工业互联网安全生产产业生态，以“本质安全+业务智能”为核心，赋能钢铁行业工业互联网安全生产建设。作为战略合作伙伴，烽台科技将不断发挥合作优势，拓展合作领域，深化合作内容，为钢铁行业智能制造快速健康稳定发展作出更大贡献。

国利网安联合宁波水务环境集团开展工控网络安全防护平台项目培训

2021年8月9日，国利网安与宁波市水务环境集团有限公司联合组织开展的工控网络安全防护平台项目培训顺利举行。此次培训主要围绕国利网安工控系统网络安全设备的功能、操作和运维等相关内容展开，旨在提升合作伙伴运维人员的网络安全防范意识和安全防护技术水平。培训由国利网安产品工程师主讲，集中介绍了工业安全态势感知平台、控制器防护系统、控制器监测与恢复系统、工业防火墙等工控网络安全产品的主要功能、操作规范、运维细则等内容。

工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

出 品

使命与责任 提升核心技术能力 服务工业用户

微信：ICSISIA

网站：www.ICSISIA.com

秘书处

中国电子技术标准化研究院信息安全研究中心

电 话：010-64102378，010-64102379

邮 箱：ICSISIA_CESI@kongzhi.net

地 址：北京市安定门东大街1号

邮 编：100007

常务秘书处

中国自动化学会《自动化博览》杂志社

电 话：010-62669087

邮 箱：ICSISIA@kongzhi.net

地 址：北京市海淀区上地十街辉煌国际5号楼1416

邮 编：100085