# 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(上) ----- www.ICSISIA.com



#### 联盟动态

4

- 2 数据驱动安全,智能成就未来——2021工业安全大会在京召开
- 3 2021年工业安全系统典型应用案例征集活动开启
- 3 《工业控制系统信息安全产品及服务指南(2021版)》上线
- 3 《工业控制系统信息安全专刊(第七辑)》出版
  - 2020年度优质工业安全服务商揭晓
- 4 ICSISIA策划"两会话安全"专题活动
- ICSISIA 2021上半年新增9家成员单位

#### 政策与规划

- 5 工信部:发布《工业互联网创新发展行动计划(2021-2023年)》
- 5 强制性国家标准《网络关键设备安全通用要求》发布,8月1日起施行
  - 工信部部署启动工业互联网企业网络安全分类分级管理试点工作
- 5 《2021年网络安全国家标准项目申报指南》发布
- 6 《2021年工业和信息化标准工作要点》发布,涉及关键信息基础设施安全保护
- 6 《"双千兆"网络协同发展行动计划(2021-2023年)》要求重点强化安全保障
- 6 国家医保局:《关于加强网络安全和数据保护工作的指导意见》发布
- 7 《"十四五"智能制造发展规划》(征求意见稿)发布,要求加强安全保障
- 7 国家安全部公布《反间谍安全防范工作规定》
- 7 国家网信办:《汽车数据安全管理若干规定(征求意见稿)》发布
- 8 2021年新一代信息技术与制造业融合发展试点示范申报开启,涵盖工业信息安全能力提升
- 8 发改委等:《全国一体化大数据中心协同创新体系算力枢纽实施方案》印发,强调数据安全
- 8 工信部部署推进5G安全工作
- 9 《工业互联网专项工作组2021年工作计划》印发
- 9 工信部、中央网信办印发《关于加快推动区块链技术应用和产业发展的指导意见》
- 9 《中华人民共和国数据安全法》正式颁布,9月1日起施行
- 10 核电 | 生态环境部: 《核动力厂网络安全技术政策》发布
- 10 交通 交通运输部印发《交通运输政务数据共享管理办法》
  - 教育 | 《加强新时代教育管理信息化工作》发布,强调提升安全保障能力
- 10 密码 国家保密局发布《涉密信息系统集成资质管理办法》

#### 产业生态

- 11 中电标协工控安全推进分会成立大会成功召开
- 11 河南省工业控制系统信息安全技术支撑单位(第二批)名单公布
- 11 6部门联合印发《重庆市工业信息安全管理实施办法(试行)》
- 11 《安徽省大数据发展条例》5月1日起施行实行大数据安全责任制明晰责任主体
- 12 山东省网信办等12部门联合发布《关于促进山东省网络安全产业发展的指导意见》
- 12 《我国关键信息基础设施安全保护白皮书》发布
- 12 国内首款"国密算法高抗冲突物联网安全芯片"发布
- 12 首个IETF国密标准正式发布,加速国密算法应用进程
- 13 "网络安全万人培训资助计划"启动,3年培养网安人才超1万名
- 13 《2020年工业信息安全态势报告》发布
- 13 2021年第一届中国工业互联网安全大赛将举办
- 14 国内首个自主可控区块链软硬件技术体系"长安链"发布
- 14 霍尼韦尔发布《USB威胁报告2020》
- 14 美最大的汽油管道遭受勒索软件攻击暂停运营,管道网络安全不容忽视
- 14 以色列"摩萨德"对伊朗核设施进行网络攻击

#### 智库研究

- 15 张晋宾:可信工业自动化和控制系统研发之探讨
- 15 汪义舟: 工业安全标准现状及展望

#### 成员资讯

- 16 和利时牵头的"工控系统安全可信关键技术及应用"项目启动会成功召开
- 16 首批工控安全防护能力贯标技术服务机构发布,电子标准院在列
- 16 公安部三所与中国电信成立数据安全共享和应用联合实验室
  - 6 国家工业信息安全发展研究中心与华为联合发布《数据安全白皮书》
- 17 360政企安全集团新一代智能安全网关产品护航大安全
- 17 启明星辰与河南省电检院达成战略合作,护航工控安全
- 17 奇安信与阿里云达成战略合作
- 17 长扬科技&赛宁联手,工业安全靶场练兵
- 18 绿盟科技发布智慧安全3.0理念体系
- 18 新华三新一代应用交付网关发布
- 18 立思辰安科获中电基金在工控网络安全领域的独家战略投资
- 18 六方云牵手麒麟软件,布局工业互联网安全、信创云领域



官方徵信



## 数据驱动安全,智能成就未来——2021工业安全大会在京召开





2021年5月20日,由工业控制系统信息安全产 业联盟主办,中国自动化学会、智能制造推进合作 创新联盟、边缘计算产业联盟、中国仪器仪表行业 协会支持,控制网(www.kongzhi.net)&《自动 化博览》、OICT学院承办的"2021工业安全大会 (ISSC2021)"在北京召开, 共有来自电力、石油 化工、能源、水利、轨道交通等行业的用户单位、 系统集成商、生产厂商、设计院、大学及科研单位的 160余位来宾出席, 共同探讨数字经济时代下工业安 全领域的前沿技术、创新成果和产业生态。中国科学 院院士、中国自动化学会会士吴宏鑫、中国工程院院 士沈昌祥出席大会。工业控制系统信息安全产业联盟 秘书长、中国电子技术标准化研究院网络安全研究中 心主任姚相振, 工业控制系统信息安全产业联盟副秘 书长孙凝分别担任大会上、下半程主持人。

大会特邀中国工程院院士沈昌祥做题为《用主 动免疫可信计算筑牢工控系统安全防线》的主题报



告,中国电子技术标准化研究院高级工程师李琳, 国家信息技术安全研究中心总工程师王宏, 宁波和 利时信息安全研究院有限公司方案总监穆雷霆,360 政企安全集团助理总裁兼工业安全事业部总经理李 航, 西安交通大学网络空间安全学院副院长、教授 刘烃, 杭州立思辰安科科技有限公司咨询规划部总 经理郭占先, 百通赫思曼网络系统国际贸易(上 海)有限公司产品经理朱杰,北京理工大学教授胡 昌振, 北京网御星云信息技术有限公司副总裁韩明 畅,水利部机电研究所高级工程师李小龙,国家工 业信息安全发展研究中心标准质量处处长陈雪鸿分 别带来精彩报告。

本次大会特设企业展示区, 共有广州虹科电子科 技有限公司、北京国泰网信科技有限公司、杭州立思 辰安科科技有限公司、宁波和利时信息安全研究院有 限公司、百通赫思曼网络系统国际贸易(上海)有限 公司、北京网御星云信息技术有限公司、北京简网科

技有限公司7家企业现场展示 各自工业安全领域的最新产 品、创新技术与解决方案。

观看2021工业安全大会精 彩回放,请扫右侧二维码→





#### 2021年工业安全系统典型应用案例征集活动开启

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于2021工业安全大会期间正 式开启2021年工业安全系统典型应用案例征集活动。

扫描右侧二维码,查看征集活动详情并下载申报表格。





## 《工业控制系统信息安全产品及服务指南 (2021版)》上线

2021年2月、ICSISIA出版《工业控制系统信息安全产品及服务指南(2021

版)》(以下简称《指南》),《指南》梳理近一年 (2019-2020年)市场上推出的工控信息安全产品及服 务,加以分类、汇编成册,方便广大用户了解工控信息 安全产业的前沿技术及最新动态、从而方便、快捷地选 择合适的产品及服务。





扫描右侧二维码、即可查看《指南》全部内容。

#### 《工业控制系统信息安全专刊(第七辑)》出版

《工业控制系统信息安全专刊》作为业内第一本聚焦于工控信息安全的文 集,于2014年起连续出版七辑,一经发行,引起了业内的广泛关注。该书集结 了众多行业用户、政府机构、科研院所、大专院校、厂商等业内专家的文章、包 含市场分析、 标准、测试、培训、技术和应用等多个方面, 聚焦国内外工业控 制系统信息安全的现状、面临的紧迫问题,以及国内外工业控制系统信息安全的

技术探讨与解决方案实践分析等热点话题, 致力成为政 府、用户、企业、科研机构、大专院校等相关单位间, 及时、高效、实用的技术交流平台、成为工业控制系统 信息安全领域中独树一帜的风向标。2021年1月, 《工 业控制系统信息安全专刊(第七辑)》出版。









#### 2020年度优质工业安全服务商揭晓

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》承办的2021中国自动化产业年会(CAIAC2021) 以"创新融合,共建数字新生态"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 业如何推动制造业变革创新、引领中国工业的数字化转 型发展之路。经过前期的积极推荐、专家评审、入围公 布、网上投票等阶段,2020中国自动化领域年度优质工 业安全服务商获奖结果揭晓, 共有14家企业获此殊荣。

11		T-1 + + - PD /
712		科技有限公司
オルホノト	// T/1945 / /	

北京惠而特科技有限公司

北京启明星辰信息安全技术有限公司

北京圣博润高新技术股份有限公司

博智安全科技股份有限公司

长扬科技(北京)有限公司

烽台科技(北京)有限公司

杭州安恒信息技术股份有限公司

杭州木链物联网科技有限公司

绿盟科技集团股份有限公司

奇安信科技集团股份有限公司

深圳融安网络科技有限公司

西门子(中国)有限公司

360政企安全集团

#### ICSISIA策划"两会话安全"专题活动

没有网络安全就没有国家安全, 随着新一代信息技术与经济社 会发展各领域深度融合, 网络安全形势日益严峻, 网络安全技术为 维护国家安全、支撑产业转型、服务社会发展、保障公众利益等提 供了重要的技术基础与坚实的安全屏障。2021年两会期间、网络安 全仍然是备受关注的高频词。各界代表汇聚一堂, 纷纷为网络安全 建言献策。ICSISIA推出两会话安全专题,梳理两会代表们涵盖"工 业互联网安全"、"网络安全"、"5G安全"、"信息安全"、 "物联网安全"、"人工智能安全"、"数据安全"等精彩提议提案。



扫描二维码,查看全部安全提议提案

#### ICSISIA 2021上半年新增9家成员单位

2021上半年,工业控制系统信息安全产业联盟新增9家成员单位,现有理事单位共计125家。

北京安点科技有限责任公司	北京简网科技有限公司
北京六方云信息技术有限公司	北京龙祥世纪信息技术有限公司
南京讯石数据科技有限公司	上海孪数科技有限公司
武汉卓尔信息科技有限公司	西安尚易安华信息科技有限责任公司
新华三技术有限公司	

#### MANAY ICSISIA com

#### 工信部:发布《工业互联网创新发展行动计划(2021-2023年)》

2021年1月,工业和信息化部印发《工业互联网创新发展行动计划(2021-2023年)》。在工业互联网安全方面,《行动计划》强调到2023年,我国工业互联网安全保障能力进一步增强的发展目标,明确将开展安全保障强化行动的重点任务,主要行动

内容包括:依法落实企业网络安全主体责任、加强 网络安全供给创新突破、促进网络安全产业发展壮 大、强化网络安全技术保障能力。提出工业互联网 安全综合保障能力提升工程:实施企业网络安全能 力贯标计划、实施技术保障能力提升计划。

## 强制性国家标准《网络关键 设备安全通用要求》发布, 8月1日起施行

2021年2月20日,国家市场监督管理总局(国家标准化管理委员会)发布2021年第1号公告,批准了7项强制性国家标准和1项强制性国家标准修改单,GB 40050-2021《网络关键设备安全通用要求》在列。该标准是工业和信息化部网络安全管理局为落实《中华人民共和国网络安全法》中有关网络关键设备安全的要求,组织相关研究机构编制的一项重要标准,于2021年8月1日正式实施。

网络关键设备和网络安全专用产品目录(第一批)

	设备或产品类别	范围	
网络关键设备	1. 路由器	整系统吞吐量(双向)≥12Tbps 整系统路由表容量≥55万条	
	2. 交换机	整系統吞吐量(双向)≥30Tbps 整系統包转发率≥10Gpps	
	3. 服务器(机架式)	CPU 数量≥8 个 单 CPU 内核数≥14 个 内存容量≥256GB	
	4. 可编程逻辑控制器(PLC设备)	控制器指令执行时间≤0.08 微秒	
	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1 小时	
	6. 防火墙(硬件)	整机吞吐量≥80Gbps 最大并发连接数≥300万 每秒新建连接数≥25万	
	7. WEB 应用防火墙(WAF)	整机应用吞吐量≥6Gbps 最大 HTTP 并发连接数≥200 万	
	8. 人侵检测系统(IDS)	満检速率≥15Gbps 最大并发连接数≥500 万	
网络安全	9. 人侵防御系统(IPS)	満检速率≥20Gbps 最大并发连接数≥500 万	
专用产品	10. 安全隔离与信息交换产品(网闸)	吞吐量≥1Gbps 系统延时≤5ms	
	11. 反垃圾邮件产品	连接处理速率(连接/秒)>100 平均延迟时间<100ms	
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5万条/秒	
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个	
	14. 安全数据库系统	TPC-E tpsE(每秒可交易数量)≥ 4500 个	
	15. 网站恢复产品(硬件)	恢复时间≤2ms 站点的最长路径≥10 级	

抄送:中央国家机关有关部门。 国家互联网信息办公室秘书局 2017 年 6 月 1 日印发

## 工信部部署启动工业互联网 企业网络安全分类分级管理 试点工作

2021年2月24日,工业和信息化部网络安全管理局部署启动工业互联网企业网络安全分类分级管理试点工作。会议对《工业互联网企业网络安全分类分级管理指南(试行)》及系列安全防护规范进行了解读,要求地方工信和通信主管部门要加强组织领导,加强对试点企业的指导督促,开展企业试点进展情况评估;同时要求地方工信和通信主管部门、第三方专业机构及试点企业要发挥各自优势,加强协同对接,扎实推进试点工作落地见效。

## 《2021年网络安全国家标准 项目申报指南》发布

2021年3月12日,为全面贯彻落实中央关于网络安全工作"四个坚持"的重要指示,以及《网络安全法》《标准化法》《密码法》《关于加强国家网络安全标准化工作的若干意见》相关要求,优化网络安全标准体系,提升立项质量,全国信息安全标准化技术委员会组织编制并发布《2021年网络安全国家标准项目申报指南》。

#### 《2021年工业和信息化标准工作要点》发布, 涉及关键信息基础设施安全保护

2021年3月16日,工业和信息化部发布《2021年 工业和信息化标准工作要点》,重点涉及网络和数据 安全、关键信息基础设施安全保护、个人信息保护 等。要点提出,在强制性标准整合精简工作基础上, 围绕产品安全、生态环境安全、网络和数据安全,船舶、飞机、民爆和通信行业的安全生产等编制工业和信息化强制性国家标准体系建设指南,统筹推进全产业链的标准工作。

#### 《"双千兆"网络协同发展行动计划(2021-2023年)》 要求重点强化安全保障

2021年3月25日,工业和信息化部发布《"双千兆"网络协同发展行动计划(2021-2023年)》(以下称"行动计划")。该"行动计划"是为贯彻落实《政府工作报告》部署要求,推进"双千兆"网络建设互促、应用优势互补、创新业务融合,进一步发挥"双千兆"网络在拉动有效投资、促进信息消费

和助力制造业数字化转型等方面的重要作用,加快推动构建新发展格局。

作为该"行动计划"的重点任务,工信部要求从 提升网络安全防护能力,构筑安全可信的新型信息基 础设施,做好跨行业网络安全保障等3个方面落实安 全保障强化行动。

#### 国家医保局:《关于加强网络安全和数据保护工作的指导 意见》发布

医疗保障信息化是医疗保障事业高质量发展的基础,是医保治理体系和治理能力现代化的重要支撑。为全面落实中央关于网络强国战略、大数据战略、数字经济的重要指示批示精神,防范化解医疗保障系统数据安全风险,促进数据合理安全开发利用,国家医保局于2021年4月6日印发《关于加强网络安全和数据保护工作的指导意见》。意见提出到

2022年,基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到"十四五"期末,医疗保障系统网络安全和数据安全保护制度体系更加健全,智慧医保和安全医保建设达到新水平。实现网络安全水平显著提升、数据安全管理有效实施、数据共享使用安全有序。

#### 《"十四五"智能制造发展规划》(征求意见稿)发布, 要求加强安全保障

2021年4月14日,为加快推动智能制造发展,工业和信息化部会同有关部门起草了《"十四五"智能制造发展规划》(征求意见稿)(下称"《规划》"),面向社会公开征求意见。其中,在安全保障方面,《规划》里明确提出要围绕智能制造安全需求,协同推进网络安全、信息安全和功能安全建设,推动密码技术深入应用。强化网络安全和工

业数据分类分级管理,推进工业数据治理。完善覆盖国家、地方、企业的多级工控信息安全监测预警网络。加大网络安全产业供给,推动专用产品试点应用。培育工业安全服务机构,提升诊断、咨询、设计、实施等服务能力。落实企业安全防护主体责任,引导企业建立符合政策标准要求的技术防护体系和安全管理制度。

#### 国家安全部公布《反间谍安全防范工作规定》

2021年4月26日,国家安全部公布《反间谍安全 防范工作规定》,规定指出关键信息基础设施运营者 应当落实反间谍安全防范主体责任,开展反间谍安全 防范教育、培训,提高本单位人员的安全防范意识和 应对能力,加强本单位反间谍安全防范管理,落实有 关安全防范措施等;此外,还应履行采取反间谍技术安全防范措施,防范、制止境外网络攻击、网络入侵、网络窃密等间谍行为,保障网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全等义务。

#### 国家网信办:

#### 《汽车数据安全管理若干规定(征求意见稿)》发布

2021年5月,为加强个人信息和重要数据保护,规范汽车数据处理活动,根据《中华人民共和国网络安全法》等法律法规,国家互联网信息办公室会同有关部门起草了《汽车数据安全管理若干规定(征求意见稿)》,意见明确运营者应当落实网络安全等级保护制度,加强个人信息和重要数据保护,依法履行

网络安全义务。科研和商业合作伙伴需要查询利用境 内存储的个人信息和重要数据的,运营者应当采取有 效措施保证数据安全,防止流失;严格限制对重要数 据以及车辆位置、生物特征、驾驶人或者乘车人音视 频,以及可以用于判断违法违规驾驶的数据等敏感数 据的查询利用。

#### 2021年新一代信息技术与制造业融合发展试点示范申报 开启,涵盖工业信息安全能力提升

工业和信息化部于2021年5月印发通知,启动2021年新一代信息技术与制造业融合发展试点示范申报工作。通知提出,将围绕深化新一代信息技术与制造业融合发展,聚焦两化融合管理体系贯标、特色专业型工业互联网平台、工业信息安

全能力提升、中德智能制造合作等方向,遴选一批试点示范项目,试点示范期为2年,将探索形成可复制、可推广的新业态和新模式,增强工业信息安全产业发展支撑,为制造业高质量发展注入新动能。

## 发改委等:《全国一体化大数据中心协同创新体系算力枢纽 实施方案》印发,强调数据安全

2021年5月24日,国家发展改革委、中央网信办、 工业和信息化部、国家能源局印发《全国一体化大数 据中心协同创新体系算力枢纽实施方案》,明确"加 强统筹、绿色集约、自主创新、安全可靠"四项基本 原则,提出九项国家枢纽节点重点任务,数据安全保 障工作在列。

方案提出,要加强对基础网络、数据中心、云平 台、数据和应用的一体化安全保障,提高大数据安全 可靠水平。加强对个人隐私等敏感信息的保护,确保 基础设施和数据的安全。完善海量数据汇聚融合的风 险识别与防护技术、数据脱敏技术、数据安全合规性 评估认证、数据加密保护机制及相关技术监测手段, 同步规划、同步建设、同步使用安全技术措施,保障 业务稳定和数据安全。加快推进全国互联网数据中 心、云平台等数据安全技术监测手段建设,提升敏感 数据泄露监测、数据异常流动分析等技术保障能力。

#### 工信部部署推进5G安全工作

近日,工信部在北京召开全国电视电话会议,部署推进5G安全工作。会议要求,各单位要认真贯彻落实信息通信行业"1+2+9"规划部署,统筹5G安全供给与安全需求,在供需两侧同步发力;统筹企业主体与行业监管两个责任,促进一体落实;统筹当前实践与长远谋划,持续提升5G安全保障水平。一是加强组织领导,系统规划本领域、本地区5G网络安全工作,明确工作目标、推进路径和工作

机制。二是加强协同联动,推动上下游企业深度协同配合,打好5G安全"团体赛"。三是加强责任落实,政府和企业两侧发力,共同促进5G安全工作各项措施落地实施。四是加强示范引领,积极推动"绽放杯"5G应用安全专题赛,引导创建5G应用安全创新示范中心,加大5G安全实践的示范推广。五是促进产业发展,借助5G赛道促进网络安全产业发展,提升5G安全产业供给能力和水平。

#### www.ICSISIA.com

#### 《工业互联网专项工作组2021年工作计划》印发

2021年6月,《工业互联网专项工作组2021年工作计划》印发。《计划》从依法落实企业网络安全主体责任、加强网络安全供给创新突破、促进网络安全产业发展壮大、强化网络安全技术保障能力、开展企业网络安全能力贯标五个方面对安全保障强化行动任务进行了介绍。

任务类别	重点工作	具体举措	年度目标成果	完成时间	牵头部门	配合部门
十、安全保障 强化行动	(一)依 (一) (本 (本 (本 (本 (本 (本 (本 (本 (本 (本	55. 实施工业互 联网企业网络安 全分类分级管理 制度。	开展工业互联网企业网络安全分类分级管理指南及系列安全防护规范宣贯,在15个省份开展工业互联网企业网络安全分类分级管理试点工作。	2021年12月	工业和信息化 部(网安局、原 材料司、装备二 司、装备司、 消费品司、电子 司)	
		56. 鹽化逐級负责的監督管理制度,加强供应链安全管理。	督促企业完善网络安全管理体系,以 电力行业横向隔离装置升级加固为抓 手,加强网络产品供应链安全管理。	2021年12月	能源局(电力安 全监管司)	
			印发行业网络安全监督管理办法。	2021年12月	国防科工局(安 全生产与保密 司、系统工程三 司)	
	(二)加 强网络安 全供给创 新突破	57. 强化工业互 联网安全优秀解 决方案等宣传推 广。	举办网络安全宣传周、产业峰会等活动,加强宣传推广与供需对接。	2021年12月	工业和信息化 部(网安局)	
		58. 鼓励重点网络安全企业和工业企业联合攻关。	在"十四五"国防基础科研规划中布局 军工网络安全重点方向,论证相关科 研项目。	2021年12月	国防科工局(系 统工程三司、科 技与质量司)	
	(三)促安 (三)格业 (三)格业 (全) (基)	59. 强化先进引领, 开展实验, 连点智能, 连进级各全全额, 不见用外面,连续全全球的工厂, 网络进广最低, 是是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一	开展工业互联网安全试点示范、遴选 一批试点示范项目,推动工业互联网 安全最佳实践推广应用。	2021年12月	工业和信息化 部(网安局)	

任务类别	重点工作	具体举措	年度目标成果	完成时间	牵头部门	配合部门
	(四)强 化网络安 全技术保 障能力	格安 提升网络和数据 术保 安全技术能力。	推动一批企业建设完善安全态势感知、安全防护、数据保护等技术手段, 提升网络和数据安全技术能力。	2021年12月	工业和信息化 部(网安局)	
			完成能源工业互联网安全态势感知平 台技术和管理规范的优化和升级,完 成国家级能源工控安全实验室的申 报。	2021年12月	国资委(办公厅)	
		61. 打造多方联 动、运行高效的技 术服务保障体系。	指导省级平台完善功能建设,推动31 个省级平台实现与国家平台完成对 接,实现工业互联网安全监测服务能 力全国覆盖。	2021年12月	工业和信息化 部(网安局)	
			依托工业互联网创新发展工程, 加快 完善工业互联网安全测试验证环境、 攻防演练靶场、安全漏洞库、基础资 源库等能力建设。	2021年12月	工业和信息化 部(网安局)	
		62. 搭建一批网络安全测试环境和攻防演练靶场。	突破新一代工控系统全生命周期的内 生安全的涉收水等关键核心技术名 项,开发那一代工程系统心技术名 传与装备10 套。研制工业互联网系统 旅游志势略出后迄南临底统,构建 大型工业装置数字孪生模型,建设新 一代工业互联网系统安全大型试验 床、	2021年12月	教育部(科技司)	
		63. 健全完善监 测预警、信息共 享、协同处置等闭 环工作机制。	定期发布工业互联网安全态势报告, 打造协同联动的通报处置机制。	2021年12月	工业和信息化 部(网安局)	
	(五)开 展企业网 络安全能 力贯标	64. 针对重点行业、企业开展宣标 业、企业开展宣标、培训等。企业实施达收销等自识域 企业实施达收销标自识域 选一批贯标示范 企业。	实施工业互联网企业网络安全分类分级管理试点,同步在试点企业开展分级防护规范宣贯和落实。	2021年12月	工业和信息化 部(网安局)	

## 工信部、中央网信办印发《关于加快推动区块链技术应用 和产业发展的指导意见》

2021年6月,为发挥区块链在产业变革中的重要作用,促进区块链和经济社会深度融合,加快推动区块链技术应用和产业发展,工信部、中央网信办联合印发《关于加快推动区块链技术应用和产业发展的指导意

见》,意见提出要强化网络安全,加强区块链基础设施和服务安全防护能力建设,常态化开展区块链技术对重点领域安全风险的评估分析。引导企业加强行业自律,建立风险防控机制和技术防范措施,落实安全主体责任。

#### 《中华人民共和国数据安全法》正式颁布,9月1日起施行

2021年6月10日, 《中华人民共和国数据安全 法》(以下简称《数据安全法》)由第十三届全国人 民代表大会常务委员会第二十九次会议通过, 自2021 年9月1日起施行。

针对数据安全保护义务,《数据安全法》中有关规定如下:第二十七条,开展数据处理活动应当依照法律、法规的规定,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。利用互联网等信息网络开展数据处理活动,应当在网络安全等级保

护制度的基础上,履行上述数据安全保护义务。第二十九条,开展数据处理活动应当加强风险监测,发现数据安全缺陷、漏洞等风险时,应当立即采取补救措施;发生数据安全事件时,应当立即采取处置措施,按照规定及时告知用户并向有关主管部门报告。第三十条,重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估,并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量,开展数据处理活动的情况,面临的数据安全风险及其应对措施等。

#### 核电 | 生态环境部: 《核动力厂网络安全技术政策》发布

为提高核电厂网络安全监管的有效性,国家核安全局和国家原子能机构联合编制了《核动力厂网络安全技术政策》(试行),用于指导核电厂营运单位通过建立、实施和维护网络安全大纲,对核电厂网络安全风险进行监测和管理,以保证核电厂安

全水平得以维持或得到提升。其他核设施营运单位 可参照执行。鉴于维护核电厂网络安全是一项复杂 的持续性工作,需要长期不断优化完善,国家核安 全局和国家原子能机构鼓励各核电厂采用试点的方 式逐步开展相关工作。

#### 交通 | 交通运输部印发《交通运输政务数据共享管理办法》

2021年4月6日,为规范交通运输政务数据共享, 推动交通运输数字政府建设,加快建设交通强国,交 通运输部印发《交通运输政务数据共享管理办法》, 《办法》提出建立机制,保障安全。建立健全政务数据共享管理机制。加强对政务数据共享全过程的身份 鉴别、授权管理和安全保障,确保政务数据安全。

## 教育 | 《加强新时代教育管理信息化工作》发布,强调提升安全保障能力

2021年3月10日,教育部印发《加强新时代教育管理信息化工作》的通知,通知提出要全面落实《中华人民共和国网络安全法》等法律法规和政策要求,建立健全网络安全责任体系,明晰各方职责。落实网络安全等级保护制度,重点保障关键信息基础设施。开展网络安全监测预警通报,提升网

络安全态势感知能力。建立供应链安全管理体系, 定期组织审计,优先选用具有自主核心技术以及安 全性达到要求的国产化产品。全面加强数据安全保 障,建立覆盖全生命周期的数据安全保障机制,重 点保护广大师生和家长,特别是未成年人的个人隐 私信息。

#### 密码 | 国家保密局发布《涉密信息系统集成资质管理办法》

为了加强涉密信息系统集成资质管理,确保国家秘密安全,根据《中华人民共和国保守国家秘密法》等有关法律法规,国家保密局发布《涉密信息系统集成资质管理办法》,办法介绍涉密集成资质包括总体集成、系统咨询、软件开发、安防监控、

屏蔽室建设、运行维护、数据恢复、工程监理,以及国家保密行政管理部门许可的其他涉密集成业务。取得总体集成业务种类许可的,除从事系统集成业务外,还可从事软件开发、安防监控和所承建系统的运行维护业务。





#### 中电标协工控安全推进分会成立大会成功召开

2021年1月19日,由中国电子工业标准化技术协会主办,中国电子技术标准化研究院等承办的工业控制系统信息安全防护能力推进分会成立大会以线上形式成功召开。工业和信息化部信息技术发展司副司长王建伟,中国电子工业标准化技术协会副理事长韩

俊,中国科学院院士何积丰,中国电子技术标准化研 究院副院长程多福等出席会议。

大会公开发布了工控安全防护能力贯标公共服务 平台(www.iiscpb.cn),该平台将为贯标工作开展 提供基础技术支撑。

#### 河南省工业控制系统信息安全技术支撑单位(第二批)名单公布

2021年4月6日,根据《河南省工业和信息 化厅办公室关于组织开展河南省工业控制系统信息安全技术支撑单位(第二批)遴选工作的通知》,经相关单位自主申报、地方工信部门初审推荐、河南省工业和信息化厅组织专家评审,公

布认定北京天融信网络安全技术有限公司、长扬 科技有限公司、北京威努特技术有限公司、北京 鸿腾智能科技有限公司、杭州立思辰安科科技有 限公司等12家单位为河南省工业控制系统信息安 全技术支撑单位。

#### 6部门联合印发《重庆市工业信息安全管理实施办法(试行)》

为贯彻落实《中华人民共和国网络安全法》、《加强工业互联网安全工作的指导意见》,建立健全工业信息安全工作机制,加强工业信息安全指导、监督和管理工作2021年2月8日,重庆市经济和信息化委员会、中共重庆市委网络安全和信息化委员会办公室、重庆市公安局等6部门联合印发《重庆市工业信息安全管理实施办法(试行)》,办法提

出主体企业负有本单位工业信息安全的主体责任, 应结合实际做好本单位工业信息安全防护,建立健 全工业信息安全责任制,负责本单位工业信息安全 保障和应急管理工作,落实人、财、物保障。主体 企业负责依法落实网络安全等级保护制度,开展定 级备案、等级测评、商用密码应用安全性评估和安 全建设整改等工作。

#### 《安徽省大数据发展条例》5月1日起施行 实行大数据安全 责任制明晰责任主体

《安徽省大数据发展条例》近日获得通过,于5 月1日起施行。对于社会普遍关注的数据盗用、泄露 等问题,《条例》明确要求实行大数据安全责任制, 并清晰界定大数据安全的各方责任主体和责任范围, 为数据信息加上"保险锁"。

《条例》分别对推动大数据与制造业、服务业和农业

的融合发展作出规定,要求县级以上人民政府及其有关部门应当推动大数据与制造业的融合,支持制造企业、互联网企业、信息技术服务企业跨界联合,建设数据驱动的智能车间、智能工厂,提升制造业数字化、网络化、智能化水平。推动大数据在服务业广泛应用,支持云计算、物联网、人工智能、区块链等新一代信息技术产业发展。



www.ICSISIA.com

#### 山东省网信办等12部门联合发布 《关于促进山东省网络安全产业发展的指导意见》

为贯彻落实网络强国的重要思想,推动山东省网络安全产业高质量发展,山东省网信办、发展改革委等12部门联合发布《关于促进山东省网络安全产业发展的指导意见》,意见提出坚持规划引领、创新驱动、协同发展、应用牵引,着力突破关键核心技术,着力推动服务创新升级,着力加快产品推广应用,着力打造良好产业生态,网络安全业务收入年均增速达到20%以上。到2025年,全省网络

安全产业规模突破300亿元,带动聚集网络安全上下游企业超过1000家,引进和培育年业务收入过亿元的企业超过50家,推动形成一批年业务收入超过10亿、具有国际竞争力的网络安全骨干企业,初步建成全国领先网络安全产业基地,全面加强网络安全保障体系和保障能力建设,为全省网络强国战略实施和数字强省建设提供核心产业保障和关键技术支撑。

#### 《我国关键信息基础设施安全保护白皮书》发布

近期赛迪发布了《我国关键信息基础设施安全保护白皮书》,白皮书从关键信息基础设施概述、重点国家和地区关键信息基础设施安全保护的做法与启示、我国关键信息基础设施安全保护现状及问题、提升我国关键信息基础设施安全保护水平的对策建议等方面对国内外关键信息基础设施保护策略进行了系统性梳理,旨在为我国关键信息基础设施安全防护提供参考意见。



扫描右侧二维码, 查看白皮书全文→

#### 国内首款"国密算法高抗冲突物联网安全芯片"发布

山东航天人工智能安全芯片研究院于2021年5月28 日正式发布了国内首款"国密算法高抗冲突物联网安全 芯片"。这款具有完全自主知识产权、支持国密算法 SM7的安全芯片,有效实现了防破解、防篡改、防克 隆、防窃听、防转移等五防安全防护作用,填补了我国 物联网安全芯片精准识读的技术空白。

#### 首个IETF国密标准正式发布,加速国密算法应用进程

近日,《商密算法在TLS 1.3中的应用》标准 (RFC 8998)在IETF发布,将国密算法应用到TLS (传输层安全协议)1.3中。这也是我国首次正式将国 密算法推进到IETF国际标准中,使得我国的国密算法 第一次在TLS协议中被认可使用而无需担心互操作性和 冲突问题。本次发布的RFC 8998标准中定义了两个TLS 1.3中的国密加密套件,一个SM2椭圆曲线ID,以及一个SM2-SM3的签名方法。该标准的发布有效解决了国密算法在TLS 1.3协议中应用的互联互通问题,将大力促进国密算法的应用。

#### "网络安全万人培训资助计划"启动,3年培养网安人才超1万名

2021年3月20日, "网络安全万人培训资助计划"启动仪式在位于武汉的国家网安基地举行。据悉,该计划面向党政机关、企事业单位工作人员,大中院校在校学生等开展网络安全培训的机构进行资助,并对优秀学员进行奖励,未来三年内将培养国家网络安全人才超1万名。

"网络安全万人培训资助计划"是在中央网信办

指导下,由武汉市人民政府、中国互联网发展基金会、中国信息安全测评中心、中国信息安全认证中心、国家计算机网络应急技术处理协调中心共同发起。为推动"网络安全万人培训资助计划"顺利开展,武汉市及东西湖区人民政府各出资2000万元、中国互联网发展基金会网络安全专项基金出资2000万元支持"网络安全万人培训资助计划"。

#### 《2020年工业信息安全态势报告》发布

2021年2月5日,国家工业信息安全发展研究中心发布了《2020年工业信息安全态势报告》。报告指出,2020年,全球工业信息安全呈现技术应用化发展、事件爆发式增长、政策多维度深化、风险弥漫性扩散等特征,危机中孕育希望,机遇与挑战并存。放眼技术趋势,围绕威胁诱捕、数据保护、供应链安全、人工智能等的技术应用从理论走向实践;回顾安

全事件,新型冠状病毒全球大流行致使利用疫情实施的网络攻击层出不穷,针对工业领域的勒索攻击频发;跟踪政策进展,主要国家围绕工业控制系统安全、工业数据安全、智能制造安全等领域出台一系列法规标准,推动各项措施走向深耕;追溯风险威胁,低防护联网工业控制系统数量激增,高危漏洞占比居高不下,重点行业面临严峻的安全挑战。

#### 2021年第一届中国工业互联网安全大赛将举办

为深入实施工业互联网创新发展战略,大力培育高素质网络安全技术技能人才队伍,加快推进工业互联网安全保障体系建设,做好庆祝中国共产党成立100周年工业互联网安全保障工作,服务新型网络基础设施建设,推动制造强国和网络强国建设,2021年中国信息通信研究院将主办"第一届中国工业互联网安全大赛"。

竞赛内容紧密结合相关行业实际生产场景和工业互联网安全技术应用发展情况,将安全评估、测试、应急处置以及新技术应用防护等内容同步融合设计到竞赛中,重点考察参赛选手在工业互联网网络、设备、控制、平台、应用、数据等方面的安全测试、评估、运维、保障以及完成指定任务的理论和技术水平。



#### 国内首个自主可控区块链软硬件技术体系"长安链"发布

2021年1月27日,国内首个自主可控区块链软硬件 技术体系"长安链"发布,同时推出首批应用场景。软件方面,"长安链"独创深度模块化、可装配、高性能 并行执行的区块链底层技术架构,实现抗量子加密算 法、可治理流水线共识、混合式分片存储等十余个核心 模块全部自主研发,交易处理能力达到10万TPS,位居 全球领先水平。"长安链"软件平台可实现根据不同的业务场景自动选取和装配适当组件,满足资产交易、数据共享、可信存证等不同需求。硬件方面,全球首创基于RISC-V开源指令集的96核区块链芯片架构,构建物理安全隔离的高效可信运行环境,实现智能合约的并行加速处理、大幅提升超大规模区块链网络交易性能。

#### 霍尼韦尔发布《USB威胁报告2020》

2021年4月1日,霍尼韦尔发布《USB威胁报告 2020》,报告提出专门针对操作技术(OT)系统的网络 安全威胁数量从2019年针对工业系统的所有网络威胁 的16%增长到2020年的28%。在同一时期,能够对OT 系统造成重大干扰的威胁数量增加了一倍多,从26%增加 到59%。报告显示,所有威胁中有五分之一(19%)专门利用USB可移动媒体作为攻击媒介,一半以上的威胁用于打开后门,建立持久的远程访问或下载其他恶意负载。这些发现表明,可能存在更多的协同攻击针对大多数工业控制环境和关键基础设施中使用的物理隔离系统。

## 美最大的汽油管道遭受勒索软件攻击暂停运营,管道网络 安全不容忽视

2021年5月7日,美国最大的成品油管道运营商 Colonial Pipeline受到勒索软件攻击,黑客通过非 法软件控制其电脑系统或数据,Colonial Pipeline 被迫关闭其美国东部沿海各州供油的关键燃油网络。知情人士称,该起事件黑客索要的赎金或高达数百万美元虚拟币。

尽管Colonial Pipeline管道运输公司按照黑客的要求交了赎金,出于安全也仍然需要关停运营实施维护,依然会造成巨大的损失。有网络专家表示,如今网络自动化攻击工具逐渐兴起,犯罪分子利用加密货币要求受害者支付赎金的做法,加大了执法部门追踪犯罪者的难度,这也加剧了此类病毒的攻击。

#### 以色列"摩萨德"对伊朗核设施进行网络攻击

当地时间4月11日晚,以色列《耶路撒冷邮报》等媒体援引西方国家情报人士的话称,伊朗纳坦兹核设施当天凌晨发生的断电事故,是以色列国安机构"摩萨德"实施的网络攻击。据报

道,伊朗纳坦兹核设施一直是以色列网络攻击的目标。2010年,以色列和美国联合行动,利用Stuxnet电脑病毒攻击伊朗纳坦兹核设施,造成重大破坏。

#### 张晋宾:可信工业自动化和控制系统研发之探讨

常规网络安全机制防护下的工控系统已不能满足新形势下(如网络作战域)关键基础设施的需求,新一代可信工控系统的研发势在必行。本文阐述了可信工控系统的概念及关键特性,分析了包括最高层、数据防护层和安全模型&策略层等3层结构的可信工控系统安全框架,提出了包括7个环节的可信工控系统的可信链,描述了SL2~SL4安全等级的端点设备的网

络安全结构。

扫描二维码、查看全文精彩内容。



#### 汪义舟: 工业安全标准现状及展望

2021年3月14日,长扬科技(北京)有限公司副总裁汪义舟在OICT学院公益直播分享《工业安全标准现状及展望》,从梳理工业安全的标准体系出发,首先从狭义上梳理工业控制安全产品、安全评估的体系标准,结合等级保护建设和安保,进一步介绍了各标准在各工业行业领域的实际指导,实施和落地,最后,结合我国十四五规划中的工业互联网,广义上对未来的工业安全的相关标准进行了展望,以望对业内

人士相关工作提供参考。

扫描二维码,查看全文精彩内容。





#### www.ICSISIA.com

#### 和利时牵头的"工控系统安全可信关键技术及应用"项目 启动会成功召开

2021年4月14日,由北京和利时系统工程有限公司牵头的国家重点研发计划"制造基础技术与关键部件"重点专项"工控系统安全可信关键技术及应用"项目启动会在和利时北京基地成功召开。

"工控系统安全可信关键技术及应用"项目由北京和利时系统工程有限公司牵头,联合哈尔滨工业大学、国家工业信息安全发展研究中心、机械工业仪器仪表综合技术经济研究所、中国科学院沈阳自动化研

究所、中国石油集团安全环保技术研究院有限公司等 共同研制。项目下设5个课题,以和利时工业控制系 统的内生信息安全为核心,结合现有防护手段和全生 命周期安全管控理念,融合主动免疫技术、安全态势 感知技术、协同防护技术、风险评估技术,构造云-工 控边-工控端协同场景下态势感知系统与协同防护系统 构建智能网联安全架构下的一体化工控安全风险评估 体系,并在典型流程工业开展应用验证。

#### 首批工控安全防护能力贯标技术服务机构发布,电子标准院在列

2021年4月,中国电子工业标准化技术协会工业 控制系统信息安全防护能力推进分会在京组织召开 了首批工控安全防护能力贯标技术服务机构遴选评 审会,经专家组评选,同意推荐中国电子技术标准 化研究院等4家单位为工控安全防护能力贯标一级核 验机构。

#### 公安部三所与中国电信成立数据安全共享和应用联合实验室

2021年4月24日,公安部第三研究所与中国电信股份有限公司举行了"数据安全共享和应用联合实验室"揭牌仪式。双方将充分发挥各自的科研和产业资源优势,针对数据安全共享和应用领域的去标识化处理、可控重标识和隐私计算等专项技术进行共同研

究,为建设多方数据安全融合计算平台、隐私计算与安全共享平台以及数据共享安全评估平台奠定良好基础,推进各领域挖掘大数据的经济价值,释放各类数据的应用潜力,共同构建可信、有效、稳定的数据流通应用技术和安全环境。

#### 国家工业信息安全发展研究中心与华为联合发布《数据安 全白皮书》

2021年5月27日,国家工业信息安全发展研究中心与华为技术有限公司联合发布了《数据安全白皮书》。白皮书剖析了数据安全在新产业生态中的需求与挑战,提出了数据安全总体策略及治理思路。在此基础上,深入分析了我国数据安全产业、

技术、法律法规现状,从提升数据安全产业基础能力、加快研究和应用数据安全防护技术、强化法律法规在数据安全主权的支撑保障作用三方面,提出数据安全发展建议,助力产业数字化和数字产业化安全发展。

#### www.icsisia.com

#### 360政企安全集团新一代智能安全网关产品护航大安全

当前,数字化时代悄然而至,虚拟世界与物理世界的边界越来越模糊,随着数字化转型升级的不断加码,新的安全威胁不断产生,网络安全面临着前所未有的全新挑战。360政企安全集团新一代智能安全网关产品——360下一代安全防火墙系统和360网络入侵防御系统,针对数字时代花样百出的网络攻击和威胁问题,在360安全大脑的赋能下,全方位护航政府、企业乃至国家的网络安全。

360下一代安全防火墙系统是一款可以全面应对

应用层威胁的高性能防火墙,通过融合360安全大脑专业威胁对抗能力,深入洞察网络流量中的用户、应用和威胁,并借助全新的高性能单路径异构并行处理引擎,为用户提供有效的应用层一体化安全防护。360网络入侵防御系统围绕精准识别、精准打击、有效阻断的设计理念。通过对网络流量的深层次解析,精准识别各类网络攻击破坏、非法入侵的威胁行为,执行实时阻断防御,高效保护客户网络的IT基础设施。

#### 启明星辰与河南省电检院达成战略合作,护航工控安全

2021年3月,郑州启明星辰信息安全技术有限公司与河南省电子信息产品质量监督检验院达成战略合作,成为河南省工业控制系统技术服务战略合作伙伴。本次双方合作旨在推动河南省工控系统信息安全

监测平台、工控系统安全研究实验室及实用技能型人才培训建设,双方通过优势互补、资源共享,实现"1+1>2"的共赢效果,为河南省工控安全保障体系建设提供有力技术支撑。

#### 奇安信与阿里云达成战略合作

2021年3月4日, 奇安信与阿里云宣布达成战略 合作, 双方将围绕重点行业的云安全领域进行自主研 发, 同时将在工业物联网、应急与攻防演练等场景, 展开技术、产品、市场、资本等领域全面深入合作。 根据协议,阿里云与奇安信将共同打造适配主流云计 算平台的云+安全解决方案。同时,奇安信与阿里云 整合双方在产业资源、技术生态、人才培养、安全运 营等方面的优势,共同拓展新的业务合作。

## 长扬科技&赛宁联手,工业安全靶场练兵

2021年3月30日,长扬科技(北京)有限公司与南京赛宁信息技术有限公司在北京宣布达成战略合作,并联合举办了主题为"融合发展共建工业安全新生态--成立合资公司暨工业安全靶场产品发布会"活动。双方将

针对工业互联网安全领域不断发展变化的网络作战训练和人员能力需求展开合作,通过攻防实战演练、系统装备测试、赛事全程保障和人员能力提升,提高工业互联网安全整体建设和策略水平、建设网络强国贡献力量。



#### 绿盟科技发布智慧安全3.0理念体系

2021年3月19日,绿盟科技在其合作伙伴大会上 正式发布了智慧安全3.0理念体系。该理念提出在新时 代下,需要以体系化建设为指引,构建"全场景、可 信任、实战化"的安全运营能力,达到"全面防护, 智能分析,自动响应"的防护效果。

"全场景"是指绿盟科技致力于面向全部数字

化应用场景,针对全部安全要素,提供全方位的安全能力;"可信任"是指绿盟科技要支撑客户构建可信任的能力,可信任的访问与可信任的供应链;"实战化"是指绿盟科技以实战化安全运营为目标,为客户构建按需调度能力,以及响应高效的安全运营体系。

#### 新华三新一代应用交付网关发布

2021年4月,新华三集团正式发布新一代应用交付网关(ADC)。新产品采用2U高度紧凑设计,具备电信级性能,主打"高效交付"、"云动智能"、"灵活简洁"、"强劲安全"等特性,助力企业在数字化转型过程中高效地应对应用部署及应用交付带来的挑战,进一步践行"云智原生"的技术战略。

该产品支持最新TLSv1.3协议,具备SSL协议转换功能,并支持丰富的SSL对称、非对称加解密算法,可实现对数据传输的安全防护。新产品还提供网络层和应用层的DDoS防护能力,保障服务器免受DDoS攻击,并确保HTTP、HTTPS、DNS等重要协议的安全,提升服务可用性。

#### 立思辰安科获中电基金在工控网络安全领域的独家战略投资

2021年4月13日,杭州立思辰安科科技有限公司(简称"立思辰安科")获得了网络安全"国家队"——中国电子科技集团有限公司所属中电基金在工控网络安全领域的独家数千万级战略投资。目前,立思辰安科拥有"立思辰"、"谷神星"两大产品品牌,产

品涵盖安全审计、边界防护、安全管理、终端防护、云安全五大类二十多条产品线。立思辰安科表示将通过不断提升产品的技术实力,与中国电科在业务、资源等方面开展深度合作、优势互补,持续领跑工控网络安全产业发展,为国家关键信息基础设施建设贡献力量。

#### 六方云牵手麒麟软件,布局工业互联网安全、信创云领域

2021年2月8日, 六方云携手麒麟软件有限公司签署战略合作协议。双方将基于银河麒麟操作系统在工业互联网安全、信创云领域展开合作, 共同打造国产化生态, 最终实现"信创强国"的战略使命。双方将

在工控安全、网络安全、IT和OT融合安全、云计算/虚拟化安全等方面,展开全面合作,共同提供满足信创标准、安全需求的联合产品、解决方案,为双方客户提供更优质的服务。



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