网信动态周报

第 45 期

2022 年

11月21日-11月26日

网络安全 工业互联网 智能科技

工业控制系统信息安全技术国家工程研究中心

特约顾问：刘廉如

1 安全一周要闻

- 英国与韩国完成脱欧后首个独立数据传输协议
- NHS 寻找国家首席信息安全官以监督整个医疗部门网络安全
- 瑞士要求运营商建立 5G 网络安全中心
- 印度政府发布《2022 年个人数据保护法案》草案
- 罕见操作，Meta 封禁多个美国军方小号
- 日本考虑组建新的网络安全防御机构
- 瑞典推出欧洲最先进的汽车网络安全中心
- 黑客攻击欧盟议会网站长达数小时，导致网络瘫痪
- 2023 年八大网络安全威胁
- 中国电信启动安全能力池建设工程集采：预估总采购规模 561 套
- 谷歌安全团队披露多个 Mali GPU 安全漏洞，三星、小米、OPPO 等均受影响

特别关注：

- 新形势下美欧网络安全应急响应机制对我启示
- 美国防部发布零信任网络战略和路线图的启示建议
- 从战略角度看 2023 年网络安全发展态势

■ 英国与韩国完成脱欧后首个独立数据传输协议

英国已经完成脱欧后的第一个独立数据保护决议，这将允许英国在今年年底之前不受限制地将个人数据安全地转移到韩国。英国政府表示，在 7 月首次达成原则性协议的新立法，将使两国的企业更容易分享数据，增强合作和增长的机会。这一决定是在对韩国的个人数据立法

进行全面评估之后做出的，就评估结果而言，韩国拥有强大的隐私法，将保护数据传输，同时维护英国公民的权利。

英国政府在数字、文化、媒体和体育部的一份新闻稿中表示，一旦生效，新的数据传输协议将消除数据传输的障碍，通过简化协作来促进研究和创新。韩国作为英国增长最快的市场之一，超过三分之二的英国服务出口到韩国。在此之前，各企业需要制定昂贵且耗时的合同保障措施，如标准数据保护条款和有约束力的公司规则。消除这些障碍将为许多中小型企业提供机会，企业可以不为这些负担而担忧。

■ NHS 寻找国家首席信息安全官以监督整个医疗部门网络安全

publictechnology 消息，NHS 拟花费 15 万英镑招聘国家首席信息安全官（NCISO），该职位由卫生和社会保障部发布，年薪为 15 万英镑，位于英国国家医疗服务体系转型理事会内，负责监督整个 NHS、卫生和社会保障部以及整个国家卫生和保健系统的网络安全以及对网络重大事件进行应急响应的指导。另外。NCISO 还将在三年内创建一个新的部门，带头实施全系统网络安全战略，为管理全国网络安全风险提供方法，并向 DHSC 和 NHS 风险管理委员会提供季度风险反馈。

■ 瑞士要求运营商建立 5G 网络安全中心

Telecompaper 消息，瑞士政府发布《电信服务条例》，要求网络运营商建立 5G 服务信息安全管理系统，企业可以选择在瑞士或国外设立相关网络安全中心，《条例》自 2023 年 1 月 1 日起生效。根据最新要求，网络运营商有责任在网络中断影响至少 1 万名客户的情况下与国家紧急行动中心联系，而以前的要求为 3 万名客户。此外，新规定还要求网络运营商主动检测和反击网络攻击，遏制网络恶意活动，如网络钓鱼等。

■ 印度政府发布《2022 年个人数据保护法案》草案

印度政府日前发布了《2022 年个人数据保护法案》草案，这是印度政府自 2018 年 7 月以来第四次修改该草案。

《2022 年个人数据保护法案》草案旨在用户同意的情况下，以收集信息为目的对信息进行分类，确保个人数据安全，该草案将在 2022 年 12 月 17 日之前公开征求公众意见。

印度有超过 7.6 亿活跃的互联网用户，根据该法案要求在线平台产生和使用的数据必须遵守隐私规则，以防止数据滥用。同时该法案要加强问责机制，提高用户信任度。

■ 罕见操作，Meta 封禁多个美国军方小号

近日 Meta 已经封禁了多个美国军方的小号，其中包括 Facebook/Instagram 等社交平台上的账号，并表示这些由美国军方运营的账号一直针对中东、俄罗斯等国家 / 地区，在中东和东亚传播对美国军方有利的内容。

■ 日本考虑组建新的网络安全防御机构

据报道，日本正在考虑建立一个新的组织来保护国家免受网络攻击，在过去几年里，日本遭受了许多重大事件。如果日本着手实施这些计划，这个新部门将在国家安全秘书处 (National Security 秘书处) 内成立。国家安全秘书处是领导日本国家安全委员会 (National Security Council) 的部门，负责提升日本的网络安全能力。

据一名政府消息人士向共同社 (Kyodo News) 透露，如果建立该机构的计划得以实施，该机构将负责整个日本军队和国家警察厅 (National Police Agency) 的网络安全。为了创建新的组织，政府目前正在制定 2024 年的新的安全预算。它将扩大目前国家网络安全事件准备和战略中心 (NISC) 的功能。NISC 负责推动整个政府的网络安全政策，并与各部委、机构和企业共享攻击信息。采取积极主动的网络防御措施通常不在 NISC 的职权范围内，但有人提议赋予这个新机构主动权，在攻击到达日本之前主动先发制人并阻止攻击。新机构的负责人将致

力于加强日本与美欧网络安全机构的跨境合作和情报共享，以加强日本对网络攻击的反应。根据IBM的《x-force威胁情报指数2022》报告，亚洲在2021年成为全球受攻击最多的地区，成为所有网络攻击的26%的目标。日本、澳大利亚和印度是该地区受攻击最严重的三个国家。

■ 瑞典推出欧洲最先进的汽车网络安全中心

瑞典国有研究机构RISE正在启动欧洲最先进的专门用于车辆测试的网络安全计划。RISE Cyber Test Lab for Automotive使汽车行业能够使用最新的网络技术和世界上最严格的测试方法来测试车辆。

网络测试实验室将与世界领先的电信专家和道德黑客合作，提供一系列前所未有的见解、方法和测试平台。该合作伙伴关系在解决竞争制造联网汽车的制造商所关注的关键问题方面是独一无二的。

在世界各地发生多起备受瞩目的汽车网络攻击事件后，RISE于2021年开始规划专门的汽车网络安全测试实验室。网络测试实验室将测试关键领域的漏洞——虚拟测试/数字双胞胎、车辆单元(ECU)中的嵌入式软件、基于车辆云的软件。Cyber Test Lab提供的测试服务包括模拟/虚拟化、子系统测试、在受控环境中的半虚拟和整车测试。它通过将我们现有的Cyber Range与汽车测试台AWITAR和Asta Zero互连，提供完整的测试能力链。这使得制造商可以在整个研发过程中对新技术和产品进行压力测试。欧盟网络安全组织ENISA已经在准备欧盟网络安全标准和认证。

随着Cyber Test Lab的启动，RISE将成为支持该认证流程的测试方法和研究的领先欧洲供应商。RISE已经在哥德堡郊外的AstaZero和AWITAR拥有世界领先的道路系统和自动驾驶车辆研究试验场。这两个试验场都被纳入了网络测试实验室。RISE网络测试实验室将于2023年初开始高级测试。在准备过程中，试点项目已经全面展开，模拟对车辆和电动汽车充电基础设施的网络攻击。

■ 黑客攻击欧盟议会网站长达数小时，导致网络瘫痪

外媒称，欧洲议会研究所所长表示，欧洲议会网站（European Parliament's website）在当地时间周三遭到“亲克里姆林宫”黑客的拒绝服务攻击，导致网站瘫痪数小时。据了解，大约在该机构报告故障两小时后，议会网站再次启动。欧洲议会主席梅特索拉（European Parliament President Roberta Metsola）在网站瘫痪后不久发推文称，“欧洲议会正遭受复杂的网络攻击。一个亲克里姆林宫的组织（pro-Kremlin group）声称对此负责。我们的IT专家正在反击，保护我们的系统。”

■ 2023年八大网络安全威胁

2023年即将到来，网络安全仍是首席信息官最关心的问题。这不足为奇。在2022年上半年，全球共发生28亿次恶意软件攻击和2.361亿次勒索软件攻击。到2022年底，预计将有60亿次网络钓鱼攻击。以下是2023年IT行业可能面临的八大安全威胁。1. 恶意软件；2. 勒索软件；3. 网络钓鱼；4. 物联网；5. 内部员工；6. 数据中毒；7. 新技术；8. 多层安全。

■ 谷歌安全团队披露多个Mali GPU安全漏洞，三星、小米、OPPO等均受影响

谷歌ProjectZero团队近日发现了存在于三星Exynos芯片组Mali GPU的多个安全漏洞。其中一个漏洞可能导致内核内存损坏，另一个漏洞可能泄露物理内存地址，还有三个漏洞涉及use-after-free。ProjectZero团队表示这些漏洞可以让攻击者返回系统后继续读写物理页。或者换句话说，在应用程序中执行原生代码的攻击者可以获得对系统的完全访问权，并绕过安卓操作系统的权限模型。目前包括三星、小米和OPPO在内的诸多厂商都在使用ARM设计的Mali GPU。而这些漏洞最初是在调查Pixel 6设备时发现的。虽然Project Zero团队曝光了这些漏洞，但是谷歌目前也没有修复这些漏洞。采用骁龙处理器的Galaxy S22等三星设备并不受这些漏洞的影响。

■ 中国电信启动安全能力池建设工程集采：预估总采购规模 561 套

来自中国电信官方消息，中国电信安全能力池建设工程已批准。本项目共划分 5 个标包，分别为网页防篡改安全原子能力软件标包、防火墙安全原子能力软件标包、入侵防护安全原子能力软件标包、堡垒机安全原子能力软件标包、Web 漏洞扫描和系统漏洞扫描安全原子能力软件标包。预估总采购规模 561 套。

中国电信安全能力池建设工程集采项目

标包	产品名称	产品分档	数量（套）
1	网页防篡改安全原子能力软件	A类	6
		B类	44
2	防火墙安全原子能力软件	A类	23
		B类	9
		C类	72
3	入侵防护安全原子能力软件	A类	45
		B类	8
		C类	74
4	堡垒机安全原子能力软件	A类	34
		B类	10
5	Web漏洞扫描安全原子能力软件	/	45
	系统漏洞扫描安全原子能力软件	/	191

图表制作：C114通信网 2022.11.23

■ 本期特别关注

新形势下美欧网络安全应急响应机制对我启示

背景概述

11 月 23 日消息，美网络安全与基础设施安全局（CISA）针对全国基础设施发布更新版指导文件，旨在为各州、及地区级网络安全保卫者提供最新指引。

《基础设施弹性规划框架》（IRPF，下文简称《框架》）早在 2021 年发布第一版，以强化网络攻击应对规划编制、提升关键基础设施网络安全保护水平为目的。

主要内容

新版《框架》为政府机构和私营部门提供了指导，以提升关键基础设施服务的安全性和弹性为目的。具体包括：

1. 沟通并了解并相关州、及地区所辖范围关键基础设施的安全弹性，提高其网络安全保护能力；

2. 明确影响各州、及地区关键基础设施正常运行可能存在的安全威胁；

3. 为政府和运营商等提供抵御和适应网络安全威胁的能力；

4. 在规划和投资决策中将关键基础设施安全和考虑在内；

5. 对各州、及地区关键基础设施快速恢复到正常功能的指导。

新版《框架》还附带一份新指南，里边概述了相关风险可能对基础设施系统产生的直接或间接影响及示例，还有可用于评估和缓解相关风险的联邦资源。

另外，本次指南更新，也是 CISA 为解决影响关键基础设施的各项网络安全问题而做出的整体努力的一部分。专家们认为 CISA 此举将提高政府机构和私营企业加强关键基础设施网络安全的认识。

启示建议

总的来看，此次美 CISA 发布的《基础设施弹性规划框架》意在持续改进关键基础设施安全。建议我可从以下几方面进行及时调整应对：一是优化关键信息基础设施识别数据集，持续提升关键信息基础设施运行弹性。二是定期对关键信息基础设施进行安全评估，加强相关安全风险的应急响应能力。三是全面提高政府机构和私营企业对关键信息基础设施的安全认识，提升相关行业网络安全标准。

美国防部发布零信任网络战略和路线图的启示建议

一、背景概述

11 月 22 日，美国防部正式公布零信任战略和路线图，旨在保护相关部门敏感信息免遭窥探等。文件详细介绍实现零信任所需的 100 多项措施和能力，另外该战略和路线图拟定一个信息体系，该体系将由零信任网络安全框架进行保护，该框架在减少攻击面，数据共享，遏制对手活动等风险管理方面十分有效。

二、主要内容

战略概述了四项综合战略目标：

一是零信任文化采纳，通过零信任安全框架和思维方式指导美军零信任生态系统中信息技术的设计、开发、集成和部署；

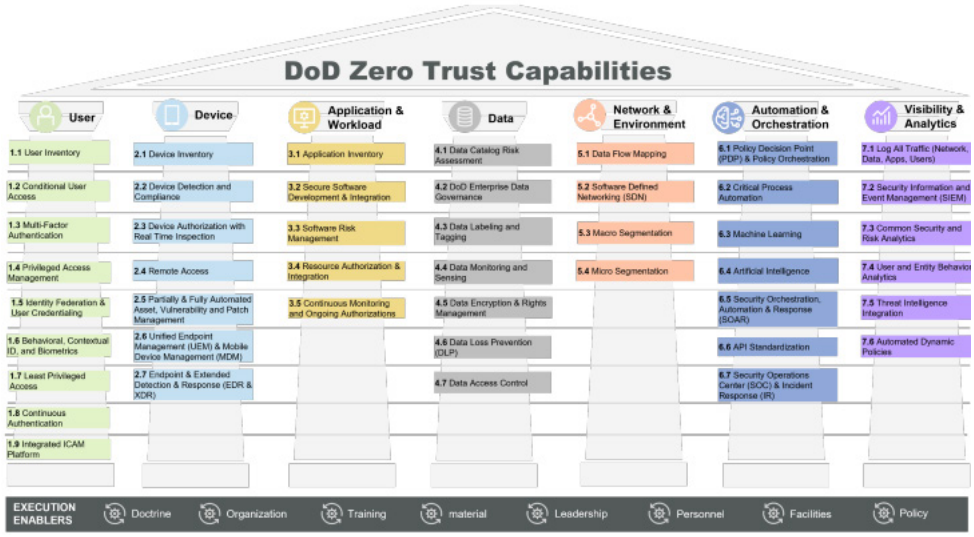
二是整合实施新旧系统零信任，美国防部要求在网络安全实践中在合并实施新旧系统零信任，以实现国防部信息系统的整体安全弹性。

三是零信任技术加速，以等于或超过行业进步的速度加快零信任技术升级，以保持其在威胁环境中始终处于领先地位；

四是零信任启动，美国防部启动零信任应与相关机构启动零信任的流程、政策和资金同步，从而实现无缝衔接的零信任启动。

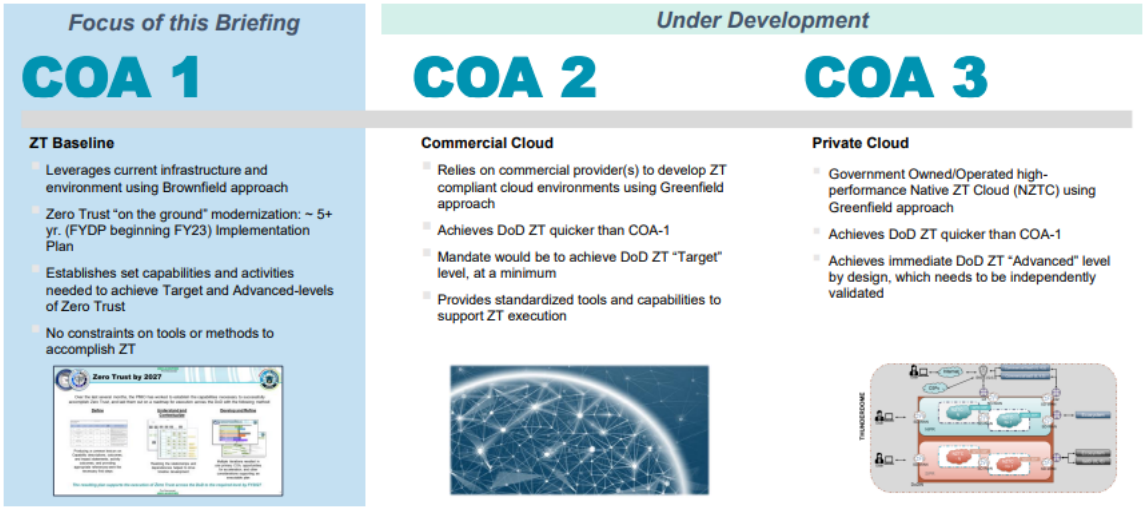
美国防部零信任战略指出，面对当前快速发展的网络威胁和攻击，基于传统身份验证和授权模型的传统边界防护方法已不能有效地阻止当前和未来的网络攻击，需要采取更具适应性、灵活性和敏捷性的响应方法。美国防部首席信息官约翰·谢尔曼在战略中指出，该战略的目的是通过从外围防御模式转变为零信任模式来应对快速增长的网络威胁。

Figure 5. DoD Zero Trust Capabilities



该战略围绕七个支柱设定了 45 项网络安全独立能力。这七个支柱包括：用户；设备；网络和环境；应用程序和工作负载；数据；洞察和分析；自动化和编排。

此外，该战略为美国防部定义了三个行动方案，以最终实现其设想的零信任目标：一是建立零信任“基线”；二是依靠商业供应商开发符合零信任的云环境；三是利用政府拥有的私有云，通过这三项措施制定未来零信任路线图。



三、启示建议

总的来看，此次美国防部公布的零信任战略和路线图旨在通过从外围防御模式转变为零信任模式来应对攻击性网络威胁的“快速增长”。建议我国持续关注美在网络安全领域的最新动态，及时调整方针政策有效应对，具体可从以下几方面进行应对：一是继续优化调整零信任安全框架，指导相关零信任生态系统中信息技术的设计、开发、集成和部署。二是强化零信任网络安全实践，加强相关信息通信系统的整体弹性。三是加快零信任技术部署，统筹协调相关部门实现零信任执行。

从战略角度看 2023 年网络安全发展态势

在过去几个月，包括 Uber、思科、Twilio 和 Rockstar Games 在内的大型企业组织均不幸沦为了网络攻击的受害者。由此可以看出，对各种类型的企业而言，想做好网络安全建设工作都并非易事。最近，德勤公司的多位资深网络安全分析师在接受专业媒体 VentureBeat 采访时，对 2023 年网络安全领域的发展态势进行了战略性预测。分析师们认为，针对安全威胁的长远准备和增强组织网络安全弹性，将会成为帮助组织有效防范潜在威胁的关键性因素。

1. 安全防护将从董事会开始

保障网络安全并不是简单的技术性问题，2023 年的网络威胁形势将会更加复杂，这将促进企业董事会在网络风险监管方面发挥更加重要的作用。获得客户信任与业务持续增长之间有高度的关联性，董事会的参与有助于将网络安全定位于组织数字化发展战略赋能者，以加强客户、供应商、员工和股东之

间的关系。

只有认识到稳健的网络安全态势对业务发展有直接影响，董事会才能更有效地监督网络安全风险管理活动。美国证券交易委员会（SEC）最近的提案中再次强调了应该加风险治理和管理，并及时通知投资者，董事会则是实现这些网络安全风险控制目标的核心。

2. 攻击面管理得到更多重视

很多组织目前已部署了与物联网相连的设备，但往往缺乏足够的安全治理。随着联网设备数量日益增加，与它们相连的网络和生态系统的攻击面也随之扩大，从而导致了安全、数据和隐私风险激增。

在 2023 年，领先的组织将致力于各种联网设备和资产的网络安全实践，为此制定或更新相关的管理政策和程序，更充分清点当前的网络资产，监控和修补设备，在注重安全的情况下完善设备采购和处置实践，将物联网和 IT 网络深度融合关联，实现更密切地监控联网设备，以进一步确保这些端点的安全和事件响应。

3. 安全性成为新兴技术能否落地的挑战

随着物联网、区块链、5G、量子及其他技术的应用继续加快，与这些技术相关的网络安全风险继续凸显出来。尽管采用这些技术将有助于推动组织的数字化转型，实现更快的战略增长计划，然而如何确保这些技术的可靠应用，将有赖于组织能否实施与之匹配的安全管理措施。

4. 隐私保护成为赢得客户信任的前提

组织与客户之间的数字化互动已是一种发展常态，调查数据显示，目前企业组织平均有近 72% 的客户沟通连接活动是通过数字化方式来实现。因此，客户需要对其数据拥有更大控制权，同时希望企业在数据处理方面增加透明度。只有组织可以证明自己值得信任，客户才更愿意共享数据，并购买其服务产品。因此，组织需要有一种紧迫感以赢得客户信任，将数据隐私、安全和合规视为不可或缺的有效机制，不断加强客户的沟通体验和品牌认知。

5. 网络安全需要长远的规划和准备

通过研究过去几年的网络安全变化，可以发现组织需要尽快为未来做好长远规划和准备。组织需要在不断变化中，持续性地完善网络风险管理实践，并寻求创新。由于更多的技术突破和不断变化的威胁趋势，组织应该充分利用网络技术为客户带来更多的价值和竞争差异化优势，同时抢先一步探究新兴风险和威胁。无论是针对近期的市场应用创新进行规划，还是遵守日益严格的监管要求，组织都需要积极评估并制定统一的网络战略，确保数字化业务足够灵活，积极抓住未来机会。

6. 保障网络安全弹性仍然是重点

随着数字化发展的深入，企业的网络攻击面也在进一步加大，因此会面临众多的供应链、地缘政治、网络环境和攻击事件可能，这将带来监管部门越来越严的审查，也给传统的风险防御计划提出了挑战。只有全面分析对核心业务运营构成威胁的场景，组织才能采用合适的方法和技术，以打造安全风险态势

感知能力，及时发现新兴威胁，并提升应对威胁的能力。

7. 复杂的供应链攻击或将出现

今天的组织严重依赖供应链，这种高度的依赖性也使得供应链安全和风险成为现代企业组织必须面对的重要挑战。2023 年，引入到供应链中的安全威胁在复杂性、规模和频率上都将会持续加大，因此组织需要继续创新并完善其供应链安全和风险转变能力，以保持良好的发展势头。

企业应该部署更加全面的供应链安全防护工具，从基于时间点的第三方评估转向实时监控外来软件以及相关固件、组件中的第三方风险和安全漏洞。

此外，企业还应该积极部署和使用身份及访问管理（IAM）和零信任功能，这些功能可以更有效地确保只有授权的第三方才能访问系统和数据，并减小第三方受攻击导致的后果。

8. 网络安全专业人才缺口继续扩大

随着网络安全风险的广度、复杂性和频率急剧加大，利益相关者（监管机构、董事会和业务人员）对管理网络安全风险的要求越来越大，因此企业组织对技能娴熟、经验丰富的网络人才有着巨大的需求。

由于这种需求加上网络人才短缺（尤其是训练有素的专业技能），组织通常很难快速找到合适的人才，这将严重影响它们管理网络风险的能力。随着这种人才短缺现象越来越严峻，更多的组织会考虑其他出路，比如选择专业的外包服务。不过，为了保持灵活、有效的安全运营流程，组织需要在采用外包策略的同时致力于招募和留住专业网络安全人才。

9. 云安全技术将加快成熟

云服务的普及和 DevOps 等新型开发方法的出现推动更多组织将业务迁移到云端，这为企业组织业务增长创造了新的发展机会。随着云计算技术日趋成熟，更多的数据和业务职能被托管在云端，组织需要意识到：如果不将安全纳入到转型过程中，代价高昂的数据泄漏和破坏性网络攻击可能会让云计算的好处荡然无存。只有同时积极拥抱安全和数字化转型，并采用零信任原则，组织才能实现云化敏捷安全发展的转型。

10. 工业互联网应用面临不断变化的威胁

随着物联网、大数据、人工智能等先进 IT 技术的快速发展，制造业为重塑企业核心竞争力，正加速推动 IT 与 OT 的融合，改造传统的生产关系与业务流程，从产品研发、业务管理到生产车间全方位推动企业的数字化转型与智能制造。当工业网络从封闭走向开放，工控安全问题也逐渐显现，由于很多关键生产与运营数据属于企业的核心商业机密和资产，一旦泄露，将会给企业带来巨大损失。更重要的是，工控系统承载着事关社会经济乃至国家安全的重要工业数据，一旦被窃取、篡改或流动至境外，将对国家安全造成严重威胁。

工业企业必须要应对好 OT 安全风险，为此可以采取诸多措施，包括加强设备可见性、实施 OT 网络分段、部署先进安全工具等。同时，在新的威胁形势下，以大数据分析、AI 技术为基础的工控安全

统一管理平台将得到更多应用。通过平台化的管控模式，不仅能够实现对多种安全设备的集中监控、系统分析、统一运营，还可以有效提升工业企业的安全风险响应速度与未知威胁感知能力，全面提升工业企业的安全防护能力。

2 工业互联网行业一周要闻

- 我国智能制造应用规模全球领先，中国制造业机器人密度增长约 13 倍
- 工信部等三部门：深化“5G+ 工业互联网”融合应用 加快 5G 全连接工厂建设
- 工业互联与数字孪生的关键技术与发展趋势
- 中国移动战略布局“5G 全连接工厂”
- 美的集团联合中国移动和华为等公司共同打造的 5G 智能制造标杆工厂
- 工信部：我国工业互联网标识解析体系国家顶级节点全面建成
- 工业互联网标识解析国家顶级节点（重庆）累计标识注册 143 亿
- 湖北标识注册量 87.52 亿个
- 科大讯飞发布“工业六感”产品

■ 我国智能制造应用规模全球领先，中国制造业机器人密度增长约 13 倍

据消息，在 2022 世界智能制造大会上，工业和信息化部相关负责人表示，十年来，我国智能制造应用规模和水平进入全球领先行列。据介绍，制造业机器人密度增长约 13 倍，达到每万名工人 322 台；5G、人工智能等智能制造关键技术的应用规模稳居全球前列。我国目前已有 110 家工厂达到国际智能制造先进水平，建成了近 2000 家引领行业发展的高水平数字化车间和智能工厂。十年来，我国智能制造装备产业规模已接近 3 万亿元，工业软件产品收入突破 2400 亿元。主营业务收入超 10 亿元的智能制造系统解决方案供应商达到近百家，服务范围覆盖 90% 以上的制造业领域。随着智能制造标准体系不断完善，我国已建成近 200 个标准试验验证平台，制定发布了近 340 项国家标准，在顶层设计、互联互通、新模式应用等领域实现国际标准突破。

■ 工信部等三部门：深化“5G+ 工业互联网”融合应用 加快 5G 全连接工厂建设

11 月 21 日，工业和信息化部、国家发展改革委、国务院国资委联合印发《关于巩固回升向好趋势加力振作工业经济的通知》（以下简称《通知》）。同日，工业和信息化部、国家发展改革委、国务院国资委召开全国加力振作工业经济电视电话会议，对巩固回升向好趋势、

加力振作工业经济进一步作出部署。《通知》从多措并举夯实工业经济回稳基础、分业施策强化重点产业稳定发展、分区施策促进各地区工业经济协同发展、分企施策持续提升企业活力、保障措施五方面提出了 17 项具体举措。深入实施智能制造工程，开展智能制造试点示范行动，加快推进装备数字化，遴选发布新一批服务型制造示范，加快向智能化、绿色化和服务化转型；深入开展工业互联网创新发展工程，实施 5G 行业应用“十百千”工程，深化“5G+ 工业互联网”融合应用，加快 5G 全连接工厂建设，推动各地高质量建设工业互联网示范区和“5G+ 工业互联网”融合应用先导区；落实 5G 应用“扬帆”行动计划，深入推进 5G 规模化应用。

■ 工业互联与数字孪生的关键技术与发展趋势

围绕工业互联网有五项关键技术在电力行业可以得到应用，一是人机交互技术，二是工况感知技术，三是数据挖掘技术，四是自主学习技术，五是自主决策技术。工业互联主要是做硬件互联、软件共享、数据集成，从而实现市场互联、设备互联、资源互联。而目前来看，数字化、网络化、智能化技术在电力行业有十大应用。一是智能电网。通过利用智能化手段与先进传感测量技术、先进的设备、先进的控制方法和先进的决策支持系统来进行智能化输变电，实现电网的可靠、安全、经济、高效、环境友好以及使用安全。二是无人机巡检。过去，电网需要人工巡检，现在是无人机巡检，可以保证线路的安全、可靠、畅通。三是维修、操作机器人。变电站变压器温度很高，电磁场非常大，人工操作对于身体有较大危害。现在可以利用机器人进行巡检、维修、操作。四是用电大数据分析。利用大数据分析用电总量是否降低，哪些行业用电量发生起伏等。此外，还有智能化电表，电力系统数字孪生，电网安全、设备安全远程预测、预报与预警，电力设备操作、维修人员上岗培训，电网、发电设备输变电系统的协同优化以及电力工程预设备设计、制造、施工企业的数字化转型。数字孪生有八项关键技术在电力行业内可以得到充分应用：复杂装备多元异构数据转换与集成技术、复杂装备几何物理行为工况建模技术、复杂状态数字孪生多性能耦合分析技术、大数据驱动下的数字孪生行为仿真技术、复杂装备全生命周期作业过程仿真技术、智能车间布局规划与生产调度优化技术、运行状态可视分析与故障智能预测技术、基于增强现实的维修维护操作导航技术。

■ 中国移动战略布局“5G 全连接工厂”

中国移动五维推进 5G 全连接工厂建设，5G 全连接工厂不仅限于工厂，还包括像钢铁、矿山、港口等更多的行业。从内涵看，5G 全连接工厂是三个“全”：一是流程 5G 全覆盖；二是场景 5G 全应用；三是生产要素 5G 全连接。中国移动从五个维度着手，锻造了 5G 全连接工厂“1+1+1+N”能力体系，并在 26 个省落地 OnePower 工业互联网平台，全面支撑 5G 全连接工厂建设。一是方案一体化，提供 5G 全连接工厂建设端到端解决方案。二是云网服务化，既有公网、也有 5G 专网，还有工业边缘云中心，可打包为企业服务。三是路径流程化，从诊断、规划、交付到运营，中国移动提供全流程支撑。四是协同开放化，与政产学研各界合作、与行业龙头合作，提炼 5G 场景、打磨完善方案，形成共赢局面。五是产品迭代化，不断沉淀行业产品，打造端网边云用一体化产品体系，全面覆盖十大重点行业痛点需求。，中国移动已经形成了“1+1+1+N”能力体系，即 1 个工业互联网平台、1 张 5G 工业专网、1 类 5G 工业终端和 N 个全连接场景应用。

■ 美的集团联合中国移动和华为等公司共同打造的 5G 智能制造标杆工厂

通过 5G 贯通各流程环节，实现了每 15 秒下线一台洗衣机的能力，下线直发率提升 1 倍，库存降低 50%，单台人工成本下降 30%。在品质管理领域，基于 5G 大带宽的优势，结合美的自研的 AI 平台，实现 AI 质检等场景的落地和推广，提升坏件检出率 10%，实现品质在线化，全方位品质刚性，智能检验、品质透明，去人为化、可视化。在柔性生产领域，依托 5G 的低时延优势，通过 5G+MEC 边缘云对生产区域的机器人生产过程数据进行采集和预测性维护，同时也可以进行机器人的控制工艺模型加载来调整机器人生产动作。基于 5G 专网和 AI 工业大脑，通过 5G+MES 联机，5G+ 工控机联机等应用，实现业务数据的抽取与智能分析和预测，对整个制造过程的闭环优化控制。在工厂物流领域，依托 5G 低时延和高可靠性优势，搭建智能物流平台，拉通物流场景，有效整合供方、生产、配送、成品仓储及发运等流程，实现 5G+AGV 调度，5G+ 叉车调度等应用。在园区管理方面，充分发挥 5G 的区域覆盖能力，在设备改造、能源管理、安全生产、环保监控以及园区安防等场景，承载了大量环保设备、仪器仪表、摄像头等连接。5G 技术的引入，减少了布线工作量，加快项目上线速度，也在一定程度上降低了成本。

■ 工信部：我国工业互联网标识解析体系国家顶级节点全面建成

在近日举行的 2022 中国 5G+ 工业互联网大会开幕式上，工业和信息化部信息通信管理局举行了工业互联网标识解析体系——国家顶级节点全面建成发布仪式，标志着“5+2”国家顶级节点全面建成。该体系累计注册量突破 2139 亿，日解析量 1.2 亿，服务企业超 20 万家，覆盖 29 个省、自治区、直辖市和 38 个重点行业，已成为推动数字经济创新发展、产业优化升级、生产力整体跃升的重要驱动力量。

■ 工业互联网标识解析国家顶级节点（重庆）累计标识注册 143 亿

工业互联网标识解析国家顶级节点（重庆）已形成以重庆为核心、成渝联动、辐射西部省市的工业互联网标识解析体系网络。在西部十省联动方面，重庆顶级节点已覆盖重庆、四川、贵州、陕西等西部九省（市），累计标识注册 143 亿，标识解析 83.5 亿次，接入企业节点 5225 家，服务于电子、石化、汽车等 19 个行业。

■ 湖北标识注册量 87.52 亿个

截至今年 11 月 17 日，武汉顶级节点接入二级节点 31 个（其中湖北省 13 个），累计标识注册量 87.52 亿个，累计标识解析量 80.59 亿次，累计接入企业节点 6720 家，初步实现了湖北、河南、湖南、江西中部四省标识解析“有体系、有流量、有应用”的目标。

■ 科大讯飞发布“工业六感”产品

据官方介绍，工业六感模拟人的视听嗅味触思六感在工业场景的应用，基于听觉、视觉、嗅觉、味觉、触觉及工业大脑，融合 AI 技术让工业生产过程具备一系列智能感知能力，并逐步拥有运动、认知能力，支持智能决策。

3 科技行业一周要闻

- SA：2022 年 Q3 三星重回西班牙智能手机市场榜首，小米苹果位列二三位
- 让声音被“看见” 中国移动数智人手语主播弋瑭首次亮相世界杯
- 四大根技术构建个人化操作系统，荣耀正式发布 MagicOS 7.0
- Counterpoint Research：Q3 东南亚市场高端智能手机出货量同比增长 29%
- 报告：到 2035 年元宇宙每年为中国内地 GDP 将贡献 4560-8620 亿美元
- 网易数帆中标安徽电信，低代码助跑通信行业高效运营
- 日韩最大电信运营商宣布达成深度战略合作：瞄准元宇宙和 6G 领域发展
- 2023 年中国智能终端市场洞察：不确定性加剧

■ SA：2022 年 Q3 三星重回西班牙智能手机市场榜首，小米苹果位列二三位

Strategy Analytics 机构报告称，2022 年第三季度，西班牙智能手机市场年增长率为 7%，环比增长率为 3%。这已经是四个季度后，该市场出现积极的年度势头。三星、小米和苹果是前三名供应商，市场份额分别为 30%、29% 和 13%。除 OPPO 外，前五名供应商都有所增长。苹果在该季度录得 60% 的强劲年度增长。对于三星来说，其 Galaxy A 和 Galaxy S 系列是主要的销量驱动力。本季度的中国供应商占了近一半的智能手机销量。

■ 让声音被“看见” 中国移动数智人手语主播弋瑭首次亮相世界杯

2022 卡塔尔世界杯激战正酣，作为世界顶级体育赛事，此次卡塔尔世界杯在全球掀起了足球观赛热潮。在这场足球盛宴中，中国移动作为本届世界杯持权转播商，为“科技观赛”注入了“人文情怀”。据悉，全球有超 4 亿人听力受损，被“听不清、听不真”所困扰，为了打破“无声的世界”，让更多人同频感受到体育赛事的激情，中国移动推出首个数智人手语主播弋瑭，为听障人士打通“信息无障碍”的桥梁。

■ 四大根技术构建个人化操作系统，荣耀正式发布 MagicOS 7.0

在“荣耀 MagicOS 发布会暨首届开发者大会”上，荣耀正式发布 AI 使能的个人化全场景智慧操作系统荣耀 MagicOS 7.0，其四大根技术 MagicRing 信任环、Magic Live 智慧引擎、Turbo X 系统引擎、MagicGuard 荣耀安全同步揭晓。MagicRing 信任环，是基于身份认证体系，实现跨系统多设备可信互联，使服务在设备间智慧流转和共享的技术解决方案。Magic Live 智慧引擎，是基于场景感知、用户理解和意图决策三大核心能力的平台型 AI 解决方案。Turbo X 系统引擎，从内核出发，围绕对应用场景计算特征的感知，实现资源层、调控层和表现层能力深度提升的内核级资源调度方案，为用户带来操作响应和网络传输上的灵敏感、平稳感、优雅感，完成全面的感知流畅和认知流畅的体验跃升。MagicGuard 荣耀安全，是基于“两锁一芯”纵深防御体系，实现应用权限、行为、内容的可知可控，让用户可以轻松掌控自己隐私的技术解决方案，通过芯片、系统、应用三层安全服务带来“信任、纯净、可靠”的体验。

■ Counterpoint Research：Q3 东南亚市场高端智能手机出货量同比增长 29%

根据 Counterpoint Research 东南亚月度智能手机渠道份额追踪报告，东南亚主要市场的高端智能手机出货量 2022 年第三季度年同比增长 29%。但另一方面，本季度智能手机总出货量年同比下降了 10%。数据指出，2022 年第三季度，东南亚主要市场 400 美元以上（约合人民币 2800 元）的高端智能手机出货量年同比增长 29%，但 200 美元以下（约合人民币 1400 元）的普通智能手机出货量则下降 24%。面对宏观经济困境，东南亚的商业和消费情绪低迷，投资放缓，且部分国家的外商直接投资乏力，共同导致智能手机品牌厂商在 2022 年第四季度前出现库存过剩。然而，在困难时期高端智能手机出货量仍实现年同比大增，凸显出这个细分市场消费者的消费力韧性。从手机品牌来看，第三季度东南亚手机市场三星的出货量年同比下降 13%，但苹果公司在各主要国家的出货量则年同比增长 63%，其中在越南市场的增速高于各邻国。

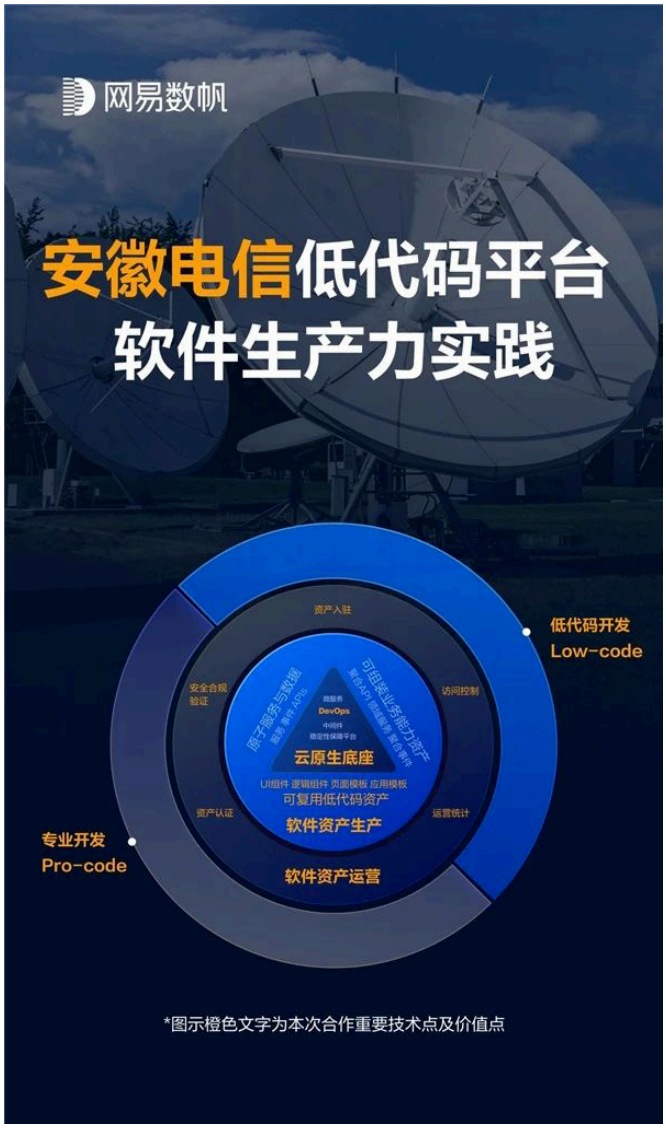
■ 报告：到 2035 年元宇宙每年为中国内地 GDP 将贡献 4560-8620 亿美元

日前，德勤（Deloitte）发布报告《亚洲的元宇宙：加速经济影响的战略》，研究元宇宙对 12 个亚洲经济体的潜在影响。报告显示，到 2035 年，元宇宙每年对 GDP 的贡献情况——中国内地 4560-8620 亿美元，日本 870-1650 亿美元，印度 790-1480 亿美元，韩国 360-670 亿美元。报告称，虚拟现实可能对亚洲经济产生“变革性影响”，并预测到 2035 年，元宇宙对亚洲 GDP 的贡献可能在每年 8000 亿至 1.4 万亿美元之间。假设“在未来五到十年内进行持续的技术投资”，这将占到整体 GDP 的大约 1.3% 到 2.4%。

■ 网易数帆中标安徽电信，低代码助跑通信行业高效运营

近日，网易数帆成功中标中国电信股份有限公司安徽分公司（以下简称“安徽电信”），双方将携手在低代码

领域展开合作，基于网易数帆轻舟低代码应用开发平台（以下简称“轻舟低代码平台”）共同探索通信行业数字化转型升级新模式。轻舟低代码平台，作为一款企业级应用开发工具，轻低代码平台具备快速开发和敏捷发布等特性，自研的可视化编程语言——NASL 语言让平台具备强大的编程表达能力，帮助企业构建中高复杂度的业务系统。



■ 日韩最大电信运营商宣布达成深度战略合作：瞄准元宇宙和 6G 领域发展

近日，韩国最大的移动运营商 SK 电讯（SKT）与日本最大的移动运营商 NTT DOCOMO 宣布签署了一份谅解备忘录，双方将在 ICT 领域展开深入合作。根据这份谅解备忘录，两家公司将在三个关键领域建立战略合作伙伴关系：元宇宙、移动网络基础设施和媒体业务。他们还将通过与 SK 海力士（SK hynix）和 Contents Wavve 等其他 SK ICT 附属公司合作，创造更大的协同效应。

■ 2023 年中国智能终端市场洞察：不确定性加剧

2022 年中国智能终端市场经历了消费环境、渠道结构和行业市场等多方面的变化和调整，在多重挑战和压力下负重前行。对于未来的生态交互、用户消费和重点行业等方面，IDC 总结出 2023 年中国智能终端市场的十大洞察：

洞察一：智能终端市场硬件、软件和服务走向一体化

洞察二：国内消费终端平台各自为阵的状态将持续

洞察三：从“手机 +X”到“人 +X”

洞察四：传感技术将成为交互中的重中之重

洞察五：长期消费升级与短期的消费 K 型化并存

洞察六：消费人群分布逐渐向理性自主型偏移

洞察七：汽车市场在各方角力中加速电动化和智能化，将迎来商业模式变革

洞察八：云终端技术进一步应用与落地

洞察九：混合办公将加速渗透

洞察十：不确定性加剧

声 明

周报内容均来自网络和微信公众号公开信息，在此仅做摘编和转述，编制机构并不对内容真实性和可靠性负责，读者可根据自身需要做进一步核实。

本期编辑：于寅虎

排版设计：赵景平

出　　品：中国电子信息产业集团有限公司第六研究所信息服务部