证券代码:002819　证券简称:东方中科　公告编号:2023-029

北京东方中科集成科技股份有限公司
2022 年年度报告摘要

一、重要提示

本年度报告摘要来自年度报告全文,为全面了解本公司的经营成果、财务状况及未来发展规划,投资者应当到证监会指定媒体仔细阅读年度报告全文。

所有董事均已出席了审议本报告的董事会会议。

非标准审计意见提示

□适用 ☑ 不适用

董事会审议的报告期利润分配预案或公积金转增股本预案

☑ 适用 □不适用

是否以公积金转增股本

□是 ☑ 否

公司经本次董事会审议通过的利润分配预案为:以 305,795,002 为基数,向全体股东每 10 股派发现金红利 0.6 元(含税),送红股 0 股(含税),不以公积金转增股本。

董事会决议通过的本报告期优先股利润分配预案

□适用 □不适用

二、公司基本情况

1、公司简介

股票简称	东方中科	股票代码	002819
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	常虹	邓狄	
办公地址	北京市海淀区阜成路 67 号银都大厦 15 层	北京市海淀区阜成路 67 号银都大厦 15 层	
传真	010-68727993	010-68727993	
电话	010-68727993(公司业务联系:010-68715566)	010-68727993(公司业务联系:010-68715566)	
电子信箱	dfjc@oimec.com.cn	dfjc@oimec.com.cn	

2、报告期主要业务或产品简介

(一)测试技术与服务领域

公司的测试技术与服务业务源自电子测试测量仪器行业。电子测试测量仪器在传统制造及高科技制造等行业都是至关重要的设备,在研发、生产、维护及其他服务提供等环节都拥有无可替代的地位。电测仪器目前广泛应用于各个行业及各大领域,包括但不限于半导体、大数据、无线通信、国防与航空航天、消费电子、汽车、工业电子、医疗设备以及其他诸多行业。

电子测试测量仪器的需求贯穿电子产品全产业链与全生命周期。测试技术与测试仪器是电子产业链中重要的一环,渗透于通信芯片、模块、终端、基站、无线网络等几乎所有的产业链环节,同时贯穿于设计研发、认证验收、生产、网络建设与优化等几乎完整的产业生命周期。其中设计与研发是使用测试仪器种类最多最广的阶段。例如通信测试,验证通信新技术的可靠性与可行性,确定了产业链各环节的衡量基准,协调了产业链的完整性,帮助运营商构建新一轮网络建设。随着 5G 的全面铺开,除了通信网络的测试需求,测试设备和业务也将率先反馈在未来端的创新和应用场景中。

1、宏观背景:研发投入持续增加

党的十八大以来,习近平总书记高度重视科技创新,把创新摆在我国现代化建设的核心地位,把科技自强自立作为国家发展的战略支撑,围绕实施创新驱动发展战略、加快推进科技创新,提出一系列新思想、新论断、新要求。

在"十四五"期间,中国的科研投入主要倾向于国家提出的科技创新三大方向,对应着 15 个具有国家级战略意义的重大项目。上层方向确定后便逐步向下进行落实,近年科研投入和科研投入强度均有较大程度的增长,同时在重点行业由政府政策和政府引导基金牵头的企业创新扶持均有所提升。其中,需要深入实施的国家重大科研方向包括:核心电子器件、高端通用芯片及基础软件产品,极大规模集成电路制造装备及成套工艺,新一代宽带无线移动通信网,高档数控机床与基础制造装备,大型油气田及煤层气开发,大型先进压水堆及高温气冷堆核电站,水体污染控制与治理,转基因生物新品种培育,重大新药创制,艾滋病和病毒性肝炎等重大传染病防治,大型飞机,高分辨率对地观测系统,载人航天与探月工程。

近年来,我国的研发强度不断增加,研发投入增长率一直高于经济增长率,与之正相关的测试技术与服务领域的投入也相应不断提高。

2、电子测试测量行业持续增长

电子测试测量仪器的下游应用行业极其分散。根据 Frost & Sullivan 的报告统计,通信行业、半导体行业和计算机行业(CS&C)是近年来增长最快且对电测下游市场拉动最大的行业,未来三年的主要市场规模预测来源均基于上述行业的高速增长和广泛应用。另外,新能源汽车、工业自动化(I&A)也将会成为电测仪器的主要下游市场之一。

3、衍生行业机会

(1)国产替代

目前国产电测仪厂家主要集中在全球科教个人及国内工业电子行业的维修下线检测等中低端场景应用。2019 年以来,多家高科技企业和机构被纳入美国出口管制"实体清单",国产电测仪厂家得以进入实体清单企业采购范围,并在部分核心企业开始应用,而后有望加快在其上下游企业子的渗透。目前可以明晰的看到国产品牌主打在教育工业等电子领域积累口碑,打破垄断壁垒并切入中低端市场,形成规模效应后逐步替代进口产品,并通过资金的快速积累积极投入研发向中高端产品迈进。

(2)系统集成

目前行业以非标系统集成为主,供应商整体较为分散,行业内没有形成集中的头部企业,现阶段进口头部品牌的厂商主要在各行业寻找本土的系统集成商进行合作,应用端主要以客户需求为牵引进行定向设计,大部分供应商都未实现通过量变积累质变进而降低边际成本,仍以单对单的定制化合作为主。但是从需求角度来看,终端用户目前对仪器的需求越来越倾向于绑定系统方案进行一站式采购,即"交钥匙"模式。

同时,系统集成商也逐渐倾向于将多项业务整合,为客户提供更多的包括检测服务在内的各项支持,同时依托与供应商的关系提供相应的直销产品销售。

(3)计量检测校准服务

伴随着战略新兴产业的发展,头部企业,直至行业标准开始建立并不断完善、更新,基于测试技术的计量检测服务需求相应保持持续增长,延伸出的后续校准、调整、技术整改等高附加值业务需求将在测试行业形成差异化的竞争格局。

(一)测试技术与服务相关业务:

公司作为中国领先的先进测试技术与科技服务商,专注于为客户提供包括仪器销售、租赁、系统集成,以及保理和招标业务在内的一站式综合服务。

"业务+产品+服务"一站式综合服务模式是公司的核心竞争力所在。公司在不断拓展电子测量仪器产品线的基础上,结合高效的信息管理系统、经验丰富的技术团队和全国营销服务网络,为客户提供仪器销售、租赁、系统集成,以及保理和招标等多种专业服务;同时配套方案设计、产品选型、计量校准、维修维护、升级更新和专业咨询等增值服务,可以有效解决由于仪器的精密性、复杂性和多样性,以及测试要求的复杂性给客户采购、应用和管理等方面带来的难题,从而帮助客户降低商务成本和测试成本、提高工作效率和测试效果,一站式满足客户需求。

公司采取多品牌、多品种的经营模式,配备专业的团队提供本地化的服务支持,辅之以控制资金风险为核心的财务管理制度和以 IT 系统为支撑的运营管理模式,使销售业务能够有效的运转和扩张,收入和利润持续增长。

上市后,公司通过投资和并购拓展了保理和招标业务,进一步从行业供应链金融和仪器设备采购招标代理方面完善了公司的综合服务模式。同时,公司不断加强和拓展既有仪器销售、租赁和系统集成业务,在国家部署产业结构升级,大力发展战略新兴产业的宏观背景下,面向 5G 新一代移动通信、新能源汽车、先进智能制造等高技术、高成长产业的产品研发设计、生产工艺控制、产品质量检测、运行维护升级等应用场景所涉及的各种复杂测试应用需求提供全面解决方案,通过不断加大在各种测试应用系统方面的研发投入和业务拓展,进一步提高了公司营业收入和盈利能力。

1、仪器销售业务

公司仪器销售模式以直销为主、分销业务为辅,其中分销业务客户包括仪器分销商、贸易商及服务商等。公司从事分销业务,一方面由于公司作为仪器厂商的授权代理商,为部分产品的供货平台,需向其他分销商提供现货;同时代理商之间由于库存差异,需要相互调货。另一方面仪器的最终用户分布广泛,通过分销商可形成更广泛的客户覆盖。

(1)主要经营模式

①多品牌、多品种经营

公司采取多品牌、多品种的经营模式,注重分销渠道的品牌建设和服务质量,坚持以市场为导向,选择拥有品牌优势、质量优势和技术优势的仪器制造商作为公司经营产品的供应商,建立战略合作伙伴关系。公司正式代理的仪器品牌近 20 个,业务涉及的仪器品牌超过 200 个,能够提供超过 3,000 种型号的仪器产品。公司客户涉及电子制造、通讯及信息技术、教育科研、航空航天、工业过程控制、交通运输、新能源等众多行业和领域,产品种类越丰富,满足客户需求的程度就越高,这是服务商相对仪器制造商所特有的优势。

②配备专业的团队提供本地化的服务支持

仪器的精密性、复杂性和多样性使得仪器综合服务商必须贴近客户、快速响应,这就要求跨地域经营的仪器综合服务商必须通过建立分支机构,并配备专业的团队为客户提供本地化服务。公司作为全国性综合服务商,除北京总部外,在上海、南京、苏州、杭州、深圳、西安、武汉、成都等地设立了分公司或办事处,服务范围覆盖了全国三十多个大中城市,形成了全国性的营销网络,能及时迅速的响应客户需求。在此基础上,公司还持续投入资源,完善全国布局,在产业发展相对聚集的地区增设营业机构,进一步加强了公司贴近服务客户的能力。同时,公司采用"销售工程师+产品经理+应用工程师"的团队合作方式,为客户提供专业的服务。其中,销售工程师主要负责日常拜访、信息交互、价格谈判、合同签订等商务沟通内容;产品经理主要负责根据客户的应用需求和预算,设计、推荐测试系统方案和具体产品搭配;应用工程师负责测试系统的展示介绍、系统搭建、日常维护和使用培训等应用技术问题。团队分工合作的方式,有效保证了一站式服务的高效执行。

③以 IT 系统为支撑的运营管理模式

产品和服务的不断丰富、业务规模的扩张对公司运营管理能力提出了更高的要求。公司利用先进的 IT 系统,如 ERP 系统、CRM 系统、BPM 系统、OA 系统等,统一管理公司的物流、资金流、业务流和信息流,最大限度的提高公司的管理和决策效率。

(2)业务流程

公司的销售业务主要采用订单销售模式,即通过收集客户信息、市场推广等活动,由销售人员获取客户订单,在综合考虑交货期、客户信用、销售利润率并经审核通过后,通过 IT 系统将订单汇总到公司。公司仓库无备货或不足部分由公司集中向供应商采购,供应商根据指令将货物发运给公司仓库。此后,公司仓库根据销售订单,将货物发运客户所在地的分公司,以客户自提、上门送货、专业运输公司配送等形式移交货物。销售完成后,视客户需求,公司向其提供仪器使用培训、计量校准、维护维修、技术咨询等服务。

2、(新能源)汽车测试业务

公司上市后在基于测试应用系统集成业务及团队,面向新兴的(新能源)汽车产业高速增长的测试系统集成需求,设立了新能源汽车事业部。经过 4 年多的发展,(新能源)汽车测试业务已经进入行业第一梯队,建立了完整的研发、生产和销售体系。在此基础上,公司于 2022 年控股收购了北汇信息,从而形成了包括为整车厂和零部件企业提供从测试工具、专用测试设备、测试应用方案到实车测试服务的(新能源)汽车全产业链测试应用服务能力,成为行业专业测试服务头部企业之一。

(新能源)汽车测试业务包括专业测试工具代理、测试应用系统集成,以及测试服务外包和第三方测试认证。

专业测试工具代理主要从事德国 Vector 公司产品的代理业务,目前已经成为其在中国区域最主要的代理商之一。Vector 公司是一家专门从事现场总线的研究、开发和应用的高科技公司,在 Controller Area Networks 总线领域内提供了一系列强有力的软硬件工具,能够支持 CAN 总线网络节点以及整个系统的建模、仿真等开发过程,为工业领域特别是汽车电子领域的客户在 CAN 总线需求研发中提供完善全面的解决方案。

测试应用系统集成主要针对客户在汽车电子的复杂测试需求,提供包括技术咨询、测试方案设计、软硬件选型与集成、软件系统开发在内的全面测试应用解决方案,目前已推出的成熟方案主要面对三大方向:主要针对燃油车的网络总线测试、主要针对电动车的新能源测试,以及包括 V2X、ADAS、HIL 测试等在内的智能网联测试。

测试服务外包和第三方测试认证主要分为针对汽车电子、软件运行等方面的功能性测试外包服务,以及作为第三方专业认证的 Test House 测试认证服务。其中 Test House 测试认证服务主要通过与整车厂达成的合作,对整车厂的供应商所提供的汽车零部件产品进行一系列标准化测试,通过第三方测试来提高测试置信度和一致性,减少 OEM 部件级测试验证工作量,同时提高其产品质量。

3、专业服务业务

公司在测试技术与服务领域的专业服务业务包括仪器租赁、商业保理和招标代理。

(1)仪器租赁业务

作为国内仪器租赁的先行者,公司于 2006 年开始面向国内半导体、通信和电子信息相关企业开展仪器租赁服务,建立了专业化的技术支持团队和覆盖全国的营销服务网络体系,各行业主要头部企业均有覆盖,并与部分重要产业客户建立了长期、稳定和深入的业务合作关系。

公司通过综合分析客户的测试目标、应用方式、现有仪器状况以及预算情况,为客户提供电子测量仪器的经营性租赁服务,以满足客户的弹性需求、降低客户综合投入以及规避技术风险。比如,由于市场订单的不确定性,制造商在生产过程中需要根据订单的变化调整产能,在生产高峰时期,通过租赁相关仪器,可以解决高峰期生产的实际需求。此外,对于一些中短期项目,特别是一些有较高不确定因素的研发生产项目,通过租赁仪器的方式,可以快速获得研发、生产必备设备,有效避免财务风险。

公司仪器租赁业务属于经营性租赁。公司用于出租的仪器主要来源于自营租赁仪器和从第三方租入的仪器。自营租赁仪器主要选择市场需求量大,出租率和回收率高,市场流通性好的仪器,在资产风险可控的前提下,确保较高的利润率。公司对自营租赁仪器的选购标准十分严格,一方面分析相关产业测试应用情况,了解租赁客户对仪器类型的偏好,挑选市场需求量稳定的仪器;另一方面高度关注仪器的生命周期与技术走向,选择生命周期较长、更新换代较慢、稳定性较高的产品。考虑到公司客户覆盖面较为广泛,客户需求所涉及仪器种类繁多,其中有很多的应用频次低、数量少,公司在以自营租赁为主的情况下,通过向第三方租入仪器的方式满足客户需求,既控制了整体经营风险,又最大程度满足了客户需求,同时也增加了租赁收入和利润。

(2)商业保理业务

公司通过控股子公司东科保理开展商业保理业务,致力于创新金融解决方案,为生产、贸易领域优质客户提供贸易融资、账户管理等综合性服务。

保理全称保付代理,卖方将其现在或将来的基于其与买方订立的货物销售/服务合同所产生的应收账款转让给保理公司,由保理公司向其提供资金融通、买方资信评估、销售账户管理、信用风险担保、账款催收等一系列服务的综合金融服务方式。它是商业贸易中以托收、赊账方式结算货款时,卖方为了强化应收账款管理、增强流动性而采用的一种委托第三者(保理商)管理应收账款的做法。

东科保理拥有一只具备专业金融知识和长期从业经验的供应链金融服务团队,建立了高效的业务运营能力和较为完善的风险控制体系,能够为行业内的上游仪器生产厂商和下游中间商提供较为完备的商业渠道融资服务,与公司其他主要业务形成良性的互动和补充。一方面公司对行业全面深入的了解能够协助保理业务在有效控制风险的前提下,快速挖掘优质目标客户,合理控制尽调、收款等运营成本,另一方面保理业务为上下游合作伙伴提供的融资支持也进一步加强了公司在产业链中的地位,形成更为明显的竞争优势。

(3)招标代理业务

公司通过控股子公司东方招标开展招标代理业务,具体包括向客户提供招投标法律政策咨询、策划招标方案、编制招标过程相关文件、组织和实施招标、开标、评标、定标等服务。

东方招标是国内较早开展招标代理业务的企业之一,一直专注于科研仪器设备的招标代理业务,在该领域积累了较强的技术实力与丰富的行业经验,可以为招标方提供专业的技术咨询和招标代理服务,在业内具有较高的知名度。

招标代理业务主要服务对象包括中科院下属研究所、国家政府机构、高校、大型企业、医院等,与公司其他主要业务在服务内容和客户群体方面具有互补性,能够优化公司现有业务结构,加强业务协同,确保多条业务线优势互补,共同发展,从而进一步提升公司在行业内的知名度和综合服务能力。

4、公司主要产品

电子测量是测量领域的主要组成部分,泛指以电子技术为基本手段的一种测量技术。利用电子技术实现测量的仪器,统称为电子测量仪器。电子测量仪器种类众多,按照其基础测试功能,可划分为以下几大类:

序号	种类	具体内容	公司提供的主要产品
1	信号发生器	用来提供各种测量所需的信号,根据用途不同,又有不同波形、不同频率范围和各种功率的信号发生器,如低频信号发生器、高频信号发生器、函数信号发生器、脉冲信号发生器、任意波形信号发生器和射频合成信号发生器。	信号发生器
2	电压测量仪器	用来测量电信号的电压、电流、电平等参量,如电流表、电压表(包括模拟电压表和数字电压表)、电平表、多用表等。	万用表
3	频率、时间测量仪器	用来测量电信号的频率、时间间隔和相位等参量,如各种频率计、相位计、波长表等。	频率计
4	信号分析仪器	用来观测、分析和记录各种电信号的变化,如各种示波器(包括模拟示波器和数字示波器)、波形分析仪、失真度分析仪、谐波分析仪、频谱分析仪和逻辑分析仪等。	示波器、综合测试仪、视频分析仪、音视频测试仪、逻辑分析仪、频谱分析仪、温度测试仪
5	电子元器件测试仪器	用来测量各种电子元器件的电参数,检测其是否符合要求。根据测试对象的不同,可分为晶体管测试仪(如晶体管特性图示仪)、集成电路(模拟、数字)测试仪和电路元件测试仪(如万用电桥和高频 Q 表)等。	元器件测试仪器
6	电波特性测试仪器	用来测量电波传播、干扰强度等参量,如测试接收机、场强计、干扰测试仪等。	场强仪、功率计
7	网络特性测试仪器	用来测量电气网络的频率特性、阻抗特性、功率特性等,如阻抗测试仪、频率特性测试仪(又称扫描仪)、网络分析仪和噪声系数分析仪等。	网络分析仪、电气测试仪
8	辅助仪器	与上述各种仪器配合使用的仪器,如各类放大器、衰减器、滤波器、记录器,以及各种交直流稳压电源。	电源、数据采集/开关、电子负载

数字安全与保密相关业务:

(一)报告期内公司所从事的主要业务、主要产品及其用途、经营模式等内容

1、主要业务

万里红业务涵盖信息安全保密、虹膜识别以及政务集成,主要业务流程覆盖项目咨询、设计、开发、实施、运维全过程,具体产品及服务包括软件产品、硬件产品及解决方案。万里红软件类产品主要根据客户需求提出解决方案,设计系统架构,进行软件及系统设计、开发和编程;硬件类产品则通过对采购硬件进行装配、检测和调试,并根据客户需求将完成自主开发软件进行嵌入和灌装,完成对硬件产品的高技术含量工序加工;对于解决方案类产品,万里红根据用户应用需求,设计解决方案,对解决方案涉及的硬件设备和软件产品进行选用,实施解决方案,通过检测后为客户进行现场安装调试,并根据客户要求定期在现场或远程完成系统维护、检查、调试升级等工作。

2、主要产品及用途

万里红主要产品及服务包括信息安全保密产品和解决方案、虹膜识别产品和解决方案,以及政务集成解决方案。

1)信息安全保密

信息安全保密产品及服务应用单位的网络环境包括互联网、外网及内网,一般由服务器、终端(笔记本、台式机、通信设备等)、信息安全保密产品及其他功能设备组成。

万里红信息安全保密产品线适配主流国产 CPU、国产操作系统、国产数据库及国产中间件,围绕数据安全监管、数据安全防护、安全应用、信息检查清除、通用电磁防护、网络安全防护等方面打造了完整的产品体系,覆盖了安全监管防护、安全综合管理、信息保密检查、网络安全审计、主机监控审计、人员行为审计、访问控制、运维审计、综合日志审计、电磁泄漏发射防护、移动通信防护与安全检查、电磁屏蔽、人员管理、业务应用等方面。基于完善的信息安全保密产品线,万里红能够根据客户的不同需求,从数据安全、网络安全、终端安全、行为安全、应用安全、电磁防护、通信安全等方面为客户提供防泄漏、防入侵、可溯源的解决方案,以满足单位数据安全防护要求,从多个维度切实增强应用单位数据安全防护监管能力。

① 安全监管类产品

安全监管类产品包含安全运行监管平台、数据安全管控系统、安全态势感知系统、运维安全管理系统、敏感信息监控分析平台、微信群(含公众号)内容监测软件、用户实体行为分析系统、互联网接入口监测平台等产品。聚焦数据安全防护和监管,以提升机关单位用户数据安全管控、安全态势感知、风险监测预警和事件应急处置能力为目的,融合大数据、人工智能和数据可视化技术,汇聚整合网络资产信息、日志、告警、故障、人员行为、风险、应用等各类数据,通过对海量数据和告警信息进行的聚合收敛和关联分析,深度挖掘安全事件链条便于追踪溯源,实现对机关单位网络安全风险的及时发现、实时数据安全和网络安全监管和态势感知能力,支撑单位网络向主动防御和动态监管转型。

② 安全防护类产品

安全防护类产品包含计算机及移动存储介质保密管理系统(三合一)、专用配置管理及三合一管理融合系统、服务器安全授权管理融合系统、主机监控与审计系统、打印刻录安全监控与审计系统、服务器审计系统、终端安全登录系统、电子文件密级标志管理系统、电子文档安全管理系统、文档发文信息隐写溯源系统、敏感信息监控管理系统、移动存储介质管理系统、违规外联监控报警系统、软件升级发布平台系统和 WIFI 热点设备控制系统等产品,以重要数据和敏感数据的防泄漏、防窃取、可追溯为目标,围绕介质管控、主机审计、打刻审计、安全登录、密级标志、文档管理、隐写溯源、违规外联报警等方面构建数据安全防护能力体系,实现对网络环境的立体化全方位安全防护,确保内网环境达到预定程度的信息安全,实现对重要数据资产和人员行为的可知、可见、可管控。

③ 安全应用类产品

安全应用类产品包含信息综合管理系统和综合办公应用管理系统,以信息安全管理为核心,对信息安全管理涉及到的各项工作进行综合管理,为单位日常信息安全管理工作提供综合应用平台。

④ 信息检查清除类产品

信息检查清除类产品包含计算机终端保密检查系统、移动存储介质信息消除工具、电子邮件系统内容检查系统和智能移动终端检查系统,用于对终端设备、存储介质、电子邮件等存储、处理的敏感信息进行安全检查,并对违规存储的敏感数据进行彻底清除,以避免终端设备在转移、弃置时导致的信息泄露,加强数据泄露防护能力。

⑤ 通用电磁防护类产品

通用电磁防护类产品包含屏蔽机柜、微机视频信息保护系统、笔记本视频信息保护系统、红黑电源滤波隔离插座、网络隔离传导干扰器和手机屏蔽柜,用于防止重要数据通过电磁辐射、网络传导、通讯设备等方式被窃取泄漏。

⑥ 网络安全防护类产品

网络安全防护类产品包含网络敏感信息检测器系统、网络接入控制系统、防火墙、入侵检测系统、网络安全审计系统、网络光单向传输系统、安全隔离与信息交换系统(双向网闸)和日志采集与分析系统,从网络出入口、网络流量、接入设备、网络行为、数据传输、网络隔离等维度构建基于通信网络的安全防护能力体系,确保设备接入可控、网络流量可检测、网络行为可审计、数据传输可管控。

信息安全保密主要产品:

产品类别	主要产品名称	产品简介
安全监管类	安全运行监管平台	通过接入汇聚网络日志信息、告警数据、网络流量、威胁情报、资产信息等数据,对海量数据进行关联分析,对安全事件进行聚合收敛,有效减少大量告警日志和误报,提供资产运维管理、网络安全管理、保密监管等能力,实时监测网络安全风险,及时发现数据窃取、数据泄露、设备故障、攻击威胁、风险行为等安全事件,全面掌握网络安全态势,提高风险管控和安全事件处置响应能力,切实提升整体网络、数据和资产的安全运行监管水平。
	数据安全管控系统	对单位内网进行实时在线监测,及时发现、处置配置合规性、网络安全、数据安全、行为异常等方面的安全事件,有效监督管理网络安全风险,强化网络运行期间的监管工作,有效发现并降低网络中存在的数据窃密风险和运行管理风险,实时掌握网络安全态势,提高威胁响应能力,提高风险管控和数据安全治理能力,支撑单位确切落实数据安全管理主体责任。
	安全态势感知系统	汇聚整合日志和告警信息进行分析挖掘,并提供行政区划地图轮播,多级联动,整体态势展示,将结果进行数据可视化集成展示,对存储介质、密级文件、接入登录、刻录打印情况、主机审计等情况进行分项事件管理和监测告警,实现事件告警和态势感知,全面掌握违规行为及网络安全风险。
	运维安全管理系统	对系统设备软硬件进行监控,从终端、网络和应用等不同层次,收集各种信息和实时运行数据,对故障指标进行告警,并对信息进行关联分析、集中展示,实现对网络资源综合运维管理,全面掌握计算机网络资源利用情况、诊断服务瓶颈,为运维服务提供依据。
	敏感信息监控分析平台	由敏感信息监控分析系统、敏感信息监控配置管理系统、以及邮件内容监测、数据库(含共享存储)内容监测、门户网站(含微博)内容监测、微信群(含公众号)内容监测和互联网流量内容监测等软件组成,用于终端、网络、数据库、应用等多个网络节点敏感信息进行实时监测,发现和告警,对多个来源的敏感信息进行智能聚合、分类和重组,将分散的敏感信息和告警信息进行关联分析,聚焦事件管理链条,提供智能处置指引和快速处置通道,消除敏感信息泄露风险,并通过泄露源趋势、泄露形态分布等分析手段对敏感信息检测策略进行有针对性调整,全面优化提升敏感信息安全管理水平。
	微信群(含公众号)内容监测软件	实时检测单位微信群组、公众号内容,对单位一个或多个工作微信群或官方公众号发送、发布的聊天文字、图片、文件、语音、视频等敏感信息内容进行识别和提取,对微信群内所有成员发出的信息进行实时检测分析,对监测到的敏感内容通过微信"@ 当事人撤回"的形式进行处理,有效解决敏感信息随意发送、敏感文章内容随意发布等问题,避免泄密事件的发生。
	用户实体行为分析系统	通过探针对人员违规操作、设备异常等日志数据进行采集汇聚和关联分析,根据规则和策略对单位、人员行为、资产三大核心实体进行行为风险画像,对人员异常行为、违规操作和泄密事件进行监控、分析和研判,及时准确发现内部威胁和潜在风险隐患,保障行为可控、风险可见。
	互联网接入口监测平台	由互联网接入口检测器、互联网接入口检测器管理系统等部分组成,用于对互联网接入口流出的信息进行深度检查,检测、分析、处置网络攻击窃密及传输敏感信息行为,并基于数据模型自动检索违规发布的敏感信息,精确定位信息泄露源头,提升单位互联网失窃泄密事件的发现与防范能力。
安全防护类	计算机及移动存储介质保密管理系统(三合一)	具备阻断内网计算机违规外联、防止移动存储介质交叉使用、外部信息单向导入内网计算机等功能,能够切实解决和防范内网计算机违规连接互联网和移动存储介质在内网计算机与外网计算机之间交叉使用引起的安全问题,防止信息泄露。
	专用配置管理及三合一管理融合系统	具备对内网计算机和服务器自身系统补丁、适配软件程序及应用安装管理功能,对计算机网络注册及信息进行管理,具备违规外联告警、移动存储介质管理功能,能够对计算机的输入输出接口进行管控和策略配置。
	服务器安全授权管理融合系统	具备服务器登录控制、移动存储介质管理、端口控制、磁盘控制等管理功能,用于对内网信创服务器的安全授权进行全面保护和远程管理,有效提高专用服务器使用和管理的安全性。
	主机监控与审计系统	能够对计算机的账户变更、进程、服务、打印、刻录、软件、硬件、目录等方面的用户操作进行监控和审计,实时监控单位内部用户对计算机的操作使用行为,发现计算机异常违规行为并产生告警,防止内部主机发生异常违规行为。
	打印刻录安全监控与审计系统	用于对内网计算机用户的打印与刻录行为进行控制与审计,通过权限管理对用户行为进行实时监控并产生日志信息,规范计算机日常打印刻录行为,实现对文档输出过程的有效监管和事后行为追溯,有效解决打印刻录的授权审核和安全监管难题。
	服务器审计系统	对专用服务器的账户、进程、服务、软件和硬件等模块的操作行为进行监控和审计,基于安全策略实现服务器异常违规行为发现并产生告警,为服务器安全提供保障,降低数据泄露风险。
	终端安全登录系统	具备基于 USB Key、虹膜识别等多重身份验证方式,对登录计算机操作系统的用户进行身份鉴别,可采用虹膜识别技术有效防止非授权用户登录,确保计算机终端登录安全。
	电子文件密级标志管理系统	用于对电子文件添加唯一、不可分离、不可篡改的密级标志,实现电子文件的访问控制、流转管控、读写管控和监控审计等管控措施,规范和加强电子文件安全管理。
	电子文档安全管理系统	提供文件分级集中存储、流转管控(内部流转管控)、操作管控、安全共享协作、文件查询检索、文档隐写、身份鉴别、安全审计等功能,可基于密标对电子文档集中进行管理,保证密级信息与信息主体不可分离、不可篡改,并通过密级信息实现对文档流转、文档操作的管控。
	文档发文信息隐写溯源系统	采用先进的图形水印变换技术,在流版式文档嵌入人眼不可识别的信息,当发生文档泄露后,可从泄露的电子或纸质文档中提取隐写信息进行解析,以实现文档泄露后的追踪溯源。
	敏感信息监控管理系统	实时检测监控计算机存储、处理的敏感文件信息内容,及时发现违规存储敏感文件的信息并自动告警上报至监控中心,管理员通过信息的统计分析,随时了解并处理所辖范围内网计算机和互联网计算机上的违规存储、处理敏感信息的行为,为敏感数据安全监管提供保障。
	移动存储介质管理系统	采用移动存储介质读写控制技术,对优盘、移动硬盘等移动存储介质在计算机上的使用进行管控,对计算机间数据传输行为进行监管,实现对移动存储介质使用的严格管控和使用人员管理,防止移动存储介质交叉使用。
	违规外联监控报警系统	监控网络内主机及存储介质违规接入互联网或其它公共网络的系统,对用户的违规外联行为进行实时监测,记录日志信息并产生报警,能够自动切断违规计算机的网络连接,避免重要信息泄露。
	软件升级发布平台系统	系统服务端与客户端协同使用,服务端主要对系统整体信息进行管理,能够上传升级包并通过消息通讯与客户端进行信息交互;客户端主要执行服务端相关策略和任务,自动下载、运行软件和升级包。
	WIFI 热点设备控制系统	通过系统下发策略对计算机终端无线网卡的联网功能和热点分享功能进行控制,可以控制指定范围内的无线网卡联网功能和 WIFI 热点分享功能的启用和禁用。
	桌面型光单向导入系统	自动将移动存储介质中指定文件夹中存储的文件单向导入到专用主机中,有效阻止数据从高密区向低密区传输,从而降低数据泄露风险。
	智能光单向导入系统	实现从不同种类、品牌、型号的设备中,安全、方便、快速地将数据单向导入到内网中,提高数据传输效率,保证重要数据安全。
安全应用类	信息综合管理系统	对单位业务数据进行统一汇总和融合分析,为单位提供信息安全自查自评、信息安全宣传教育、内部人员、核心设备、信息系统等综合管理功能,实现信息安全融合管理,全面提升信息安全管理工作质量和水平。
	综合办公应用管理系统	提供信息安全管理、人员管理、信息安全教育考试等能力,用于集中处理和查询统计保密机关在工作中产生的大量信息,对信息安全管理工作中涉及到的各项工作进行统一综合管理。
信息检查清除类	计算机终端保密检查系统	通过主机检查、终端自查、违规判定等,进行全方位、多角度的分析识别,采用自动判定和人工手动判定相结合的方式对终端进行违规检查,及时发现违规行为、失泄密漏洞和安全隐患,从而提高系统检查的全面性、高效性和准确性,降低数据泄露隐患。
	移动存储介质信息消除工具	提供对文件、目录和整个磁盘的数据彻底销毁功能,彻底清除存储介质上的数据,解决数据被删除及格式化后可通过特殊技术或工具恢复的问题。
	电子邮件系统内容保密检查系统	用于对电子邮箱、邮件客户端及邮件服务器中存储的邮件内容进行敏感性检查,及时发现违规传递行为和安全隐患,有效避免电子邮件处理、存储敏感数据的行为。
	智能移动终端保密检查系统	用于对移动终端存储、处理的文件、图片等内容进行全面、高效检查,及时发现敏感数据,确保移动终端的使用符合信息安全管理规定。
通用电磁防护类	屏蔽机柜	根据国家关于电磁泄漏发射屏蔽机柜相关技术要求进行设计,用于存放服务器、交换机、路由器、防火墙等专用网络设备,提供电磁防泄漏安全防护能力。
	微机视频信息保护系统	采用计算机视频信息干扰技术,有效防止计算机视频信息被窃取。
	笔记本视频信息保护系统	具有较强的抗侦收技术,有效防止笔记本视频信息被窃收截获。
	红黑电源滤波隔离插座	具备普通的电源插座功能,采用滤波和屏蔽技术,防止所连接信息设备电源线的信息传导泄露。
	网络隔离传导干扰器(线路传导干扰器)	采用传导干扰技术,保护网线中传输的敏感信息。
	手机屏蔽柜	用于临时储存手机,能够有效屏蔽手机信号。
网络安全防护类	网络敏感信息检测器系统	由检测器和客户端两部分组成,检测器采用旁路监听方式接入网络,结合客户端上报数据信息,快速发现网络中主动传输敏感信息的行为和通过网络攻击被动传输敏感信息的行为,并产生告警,实现对网络出入口流量和计算机操作行为的实时监控,降低泄密风险。
	网络接入控制系统	以终端计算机和网络设备作为准入控制对象,对入网终端和网络设备进行合规审查、安全检查等,防止未授权、不合规、不健康的终端和网络设备接入内部网络,杜绝通过私接乱接设备构建网中网的行为,保证合法终端的网络畅通,避免非法终端接入带来的安全隐患。
	防火墙	具备应用快速、智能识别能力,具有防病毒、异常流量、DDOS、非法外联、防暴力破解能力,提供基于应用层的用户行为监听和防护能力,通过安全检测引擎和应用识别,实现对应用、URL、入侵防御、病毒查杀等内容的统一管控。
	入侵检测系统	对缓冲区溢出、SQL 注入、暴力猜测、DoS 攻击、扫描探测、蠕虫病毒、木马后门等各类黑客攻击和恶意流量进行实时检测、报警和动态防御。
	网络安全审计系统	采用智能流控、智能阻断、智能路由等技术,通过分析网络流量,对用户行为和网络安全事件进行全面审计,对重要安全事件或行为进行风险分析、追查取证,为单位全面了解网络资源和风险趋势提供有效数据支撑。
	网络光单向传输系统	在保证信号绝对单向的情况下,实现可靠的数据单向传输,确保内网数据不被泄漏。
	安全隔离与信息交换系统(双向网闸)	基于网络隔离技术,分别连接安全和非安全的网络,切断不同网络域之的 TCP/IP 通讯,实现内网和外网之间安全隔离、适度可控的数据交换。
	日志采集与分析系统	实时采集网络中安全设备、网络设备、服务器资源和应用系统的日志,可对多数据源日志进行分析并生成告警,并通过集中存储和分布式集群存储方式对海量日志进行存储管理,通过存储、备份、查询、实时汇总分析和报表汇总,实现对海量日志全生命周期管理。

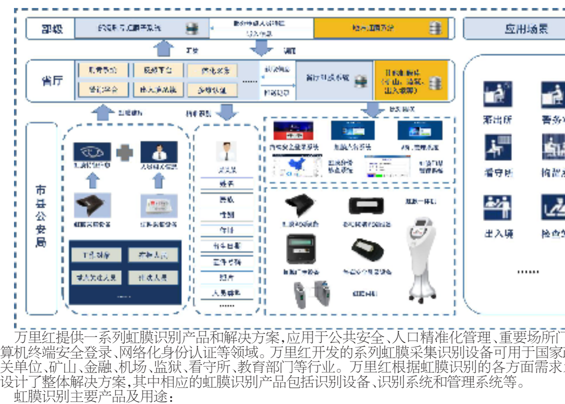
信息安全保密主要解决方案:

方案名称	方案简介
数据安全综合解决方案	通过数据分类分级服务,提高数据识别精准度;动态监控敏感数据流转趋势,评估数据安全风险;建立数据安全防护措施,增强数据安全防护能力;追溯数据传输过程及关键节点信息并可视化呈现,提高溯源效率,实现全场景、全链路、全生命周期的数据综合安全管理。
商用密码应用解决方案	针对单位的重要信息系统,从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全,以及密钥管理、安全管理等方面,进行商用密码应用技术方案、安全管理方案和实施保障方案的设计,合规、正确、有效采用密码技术进行保护,并使用符合相关要求的密码产品和服务,在系统规划、建设和运行阶段,开展密码应用安全性评估。
位终端网络协同安全解决方案	通过安全信息收集、自动关联分析、快速威胁检测和事件响应等能力,实现精准威胁发现、聚合告警数量、多种威胁检测、快速响应处置等终端网络协同联动、联防联控的主动防御目标。
敏感信息监控管理解决方案	通过对终端、网络流量、数据库、微信群、邮件、网站等节点的重要文件和敏感信息进行检测、识别,分析敏感信息泄露风险隐患,并依据敏感信息安全管理策略进行风险处置,提升敏感信息安全防护水平。
网络安全接入控制解决方案	采用扫描探测、流量监听、特征匹配等方式,在不改变网络结构的情况下,对各类入网设备进行接入控制,实现合法用户、授权设备才能入网,隔离非法、不安全的用户和设备,提升网络空间安全防护能力。
安全综合管理解决方案	为推动单位综合安全管理能力,针对单位信息安全管理工作中存在的流程不规范、管理不精细等突出问题,提供自查自评业务模块、信息安全宣传教育、重要人员、核心设备、敏感载体、信息系统等安全管理能力,旨在用信息化手段帮助单位全面提升信息安全管理工作质量和水平。
立体化数据安全防控方案	聚焦数据安全,利用大数据和人工智能技术,围绕"事前入侵防范、事中检测监控、事后追踪溯源"等安全能力板块,构建"终端–边界–应用–数据"立体化数据安全防控体系,打造数字安全屏障,切实增强数据和网络安全防控能力,有效解决外部攻击窃密和内部违规泄密问题。
人员行为分析解决方案	基于人员行为日志汇聚和分析,围绕单位、人员、资产三大核心实体刻画行为风险画像,基于安全基线,对人员异常行为、违规操作和泄密事件进行监控、分析和研判,及时准确发现内部威胁和潜在风险隐患,精准定位单位中安全意识淡薄的人员、潜在的窃密分子和单位安全管理薄弱地带,使安全管理核心力量更有效的靶向打击和治理,保障行为可控、风险可见。
安全运行监管解决方案	采用大数据分析和智能建模技术,关联日志、流量、告警、漏洞、资产等数据,集安全监管、运维管理、安全管理和态势展示等能力为一体,构建安全运行监管一体化平台,从安全配置合规性、网络安全、数据安全、行为异常等维度进行全面监管,对事件进行上报处置,有效提升网络安全运行防护监管能力。
电子文档安全管理解决方案	根据预设权限对电子文档流转、阅读、打印和传输、纸质文档借阅等环节进行全流程、可视化闭环管理,能够对重要文档嵌入人眼不可见的隐写信息,一旦由于截屏、拍照、录像、传阅等行为导致信息泄露,可快速精准定位到文件分发泄密的源头,确保文档流转过程中的事前防护、事中管控和事后溯源,实现对文档全生命周期的安全管理。

2)虹膜识别

虹膜是位于人眼表面黑色瞳孔和白色巩膜之间的圆环状区域,具有丰富的纹理信息。虹膜识别技术是使用图像处理、模式识别等技术对虹膜纹理信息进行提取、编码,形成虹膜特征并存入数据库,并将现场捕捉到的虹膜特征与数据库进行快速匹配,实现对个人身份的精准识别。相较于指纹识别、人脸识别和语音识别等其他生物识别技术,虹膜识别在精确度、安全性、采集方式等方面具有明显的优势。

万里红能够为客户建设功能强大、覆盖广泛的虹膜身份核查系统,使用虹膜采集设备、证件采集设备针对重点关注人员,将虹膜特征与身份信息进行绑定,并通过虹膜识别设备(虹膜识别设备、移动终端识别设备、虹膜门禁设备、终端安全登录设备、虹膜闸机、虹膜一体机等)、虹膜识别及管理系统(虹膜身份核查系统、虹膜门禁管理系统、虹膜点名系统、终端安全登录系统、AB 门管理系统等)等产品,为国家政法机关单位、矿山、出入境等行业客户提供比对服务,实现虹膜采集、虹膜识别、轨迹跟踪与监控、人证合一验证等功能,具体架构如下:



万里红提供一系列虹膜识别产品和解决方案,应用于公共安全、人口精准化管理、重要场所门禁、计算机终端安全登录、网络化身份认证等领域。万里红开发的系列虹膜采集识别设备可用于国家政法机关单位、矿山、金融、机场、监狱、看守所、教育部门等行业。万里红根据虹膜识别的各方面需求为客户设计了整体解决方案,其中相应的虹膜识别产品包括识别设备、识别系统和管理系统等。

虹膜识别主要产品及用途:

产品名称	代表产品图	产品用途	客户群体	具体形式
基于虹膜的终端安全登录系统		通过虹膜识别控制人员登录计算机系统,用于对存储涉密信息、敏感信息或个人隐私数据的计算机的登录人员进行高强度的身份认证,防止信息被非授权查看,充分保证系统及数据的安全性	政府机关、军工单位、国企单位、金融机构及教育机构	软件产品,用于登录计算机时进行虹膜身份识别
在押人员虹膜点名系统		在无需人工介入的情况下,为监管部门对在押人员进行自动化虹膜点名,用于杜绝人工巡查点名可能出现的误差,减少人力、物力投入,且对所有在押人员进行全面的监控管理	监管部门	软件产品,用于对在押人员点名时进行虹膜识别
监所 AB 门管理系统		通过建设高度信息化、高安全性的虹膜 AB 门禁系统,为出入管理提供智能化手段,用于对人员出入情况进行实时、在线、全面有效的监控和管理,达到安全出入、维护次序、预防入侵、防止胁迫尾随等目的	监管部门	软件产品,通过虹膜识别开启 AB 门,对通行人员进行管控
虹膜身份核查系统		对各类采集点流动人员的虹膜信息进行采集和识别,建立虹膜特征数据资源,并与身份证信息或护照信息进行绑定,联动进行校验,用于快速实现各类人员的身份鉴别,根据系统提供的定级模型进行人员安全级别定级,查出可疑人员	政府机关、军工单位、国企单位、金融机构及教育机构	软件产品,采用虹膜识别对被核查人身份进行精准确认
虹膜门禁管控系统		精准核实人员的真实身份,用于对人员的出入情况进行全面、实时、防伪性高、非接触的网络化管理与监控	政府机关、军工单位、国企单位、金融机构及教育机构	软件产品,通过虹膜识别对进入重点场所的人员身份进行精准识别
虹膜采集设备		将虹膜采集与识别功能合一,用于大规模虹膜采集,为虹膜精准识别奠定基础	政府机关、军工单位、国企单位、金融机构及教育机构	软硬结合产品,用于大规模虹膜信息采集和识别
虹膜门禁设备		同时支持虹膜采集、虹膜识别和人像照片采集,用于重要场所门禁系统、监管场所 AB 门管理系统、监室自动点名系统等	政府机关、军工单位、国企单位、金融机构、教育机构及监管部门	软硬结合产品,用于门禁系统,对出入重点区域的人员进行识别和通行管控
移动虹膜设备		民警通过安装在警用手机上的虹膜识别 APP,用于随时随地对可疑人员进行虹膜身份核查,精准确定其真实身份	公安系统	软硬结合产品,用于民警移动执法中通过虹膜识别对可疑人员身份信息进行确认
虹膜终端安全登录设备		设备具有高适配性,可搭载多种安全防护领域的登录系统,用于用户的计算机操作系统登录、应用系统登录的身份认证	公安系统	软硬结合产品,用于对登录计算机的人员身份进行识别
虹膜一体机		将虹膜生物特征识别与身份证件核验合为一体,自动对接后台虹膜比对算法集群,用于对通行人员进行身份精准核查与管控,实现无证自助通关	出入境管理部门	软硬结合产品,用于远距离实现虹膜采集识别
虹膜闸机		同时支持虹膜采集、虹膜识别和人像照片采集,自动对接后台虹膜比对算法集群,用于对通行人员进行身份精准核查与管控,实现无证自助通关	出入境管理部门	软硬结合产品,用于在重要区域入口对通行人员进行虹膜识别和出入管控

虹膜识别主要解决方案及用途:

方案名称	方案用途	客户群体	具体形式
身份核查解决方案	将身份证件信息与虹膜特征绑定,实现快速精准的识别	政府机关、军工单位、国企单位、金融机构及教育机构	整合虹膜识别的软硬件产品,用于大规模虹膜身份核查系统的建立和比对
矿山虹膜识别考勤解决方案	结合定位技术与虹膜技术实时显示井下人员信息,用于矿山安全管理	矿山	整合虹膜识别的软硬件产品,用于矿山应用场景下的虹膜身份核查系统的建立和比对
出入境管理解决方案	采集入境人员虹膜特征,一方面与犯罪人员进行比对,另一方面在入境闸机前进行信息验证,用于识别和比对出入境人员真实身份与所持护照信息	出入境管理部门	整合虹膜识别的软硬件产品,用于出入境应用场景下的虹膜身份核查系统的建立和比对
看守所虹膜身份识别解决方案	通过虹膜识别技术对出入看守所的在干警和在押人员核实,提高看守所安全防范能力	看守所	整合虹膜识别的软硬件产品,用于看守所应用场景下的虹膜身份核查系统的建立和比对
大型活动会议安保解决方案	通过虹膜识别技术对授权准入人员进行身份验证,阻止可疑人员、非授权人员进入会场,确保活动会议顺利完成	大型活动场所的重点区域	整合虹膜识别的软硬件产品,用于大型活动场所应用场景下的虹膜身份核查系统的建立和比对
金融行业虹膜应用解决方案	建设金融行业的虹膜识别身份核查系统,将形成金融行业相关人员、银行客户的完整虹膜特征数据资源,为金融行业的各类人员身份认证提供高精度的核查服务,还能够与公安机关已经建设完成的各类重点关注人员虹膜特征数据进行交叉比对,从而经过多重身份认证,确保相关人员身份信息的安全性与真实性	金融行业	整合虹膜识别的软硬件产品,用于金融行业的虹膜身份核查系统的建立和比对

3)政务集成

传统政务集成

万里红为党政机关、大型国有企业提供计算机网络系统、网络安全系统以及电子政务应用系统的规划、设计、实施、运维、技术支持等全面服务。万里红承担了大量国家级及省部级涉密信息系统建设项目、信息系统安全等级保护项目,为用户建设了安全、可靠、高效、稳定的网络系统,实现了业务系统的信息化、网络化、电子化。

万里红传统政务集成解决方案及用途如下:

业务描述	方案用途	客户群体
涉密计算机信息系统建设	为用户提供涉密计算机信息系统建设的咨询顾问、规划设计、建设实施、保密检查和维护保障等服务	党政机关、大型国有企业
信息系统安全等级保护	为用户提供重要信息系统的等级保护整体解决方案、风险评估和工程建设等服务	党政机关、大型国有企业
政务应用系统开发	为党政机关的应用系统提供需求分析、系统设计、系统开发和测试服务	党政机关、大型国有企业
计算机信息系统运行维护	为用户的信息系统相关的机房、主机、网络、安全等设备和业务系统提供运行维护服务	党政机关、大型国有企业

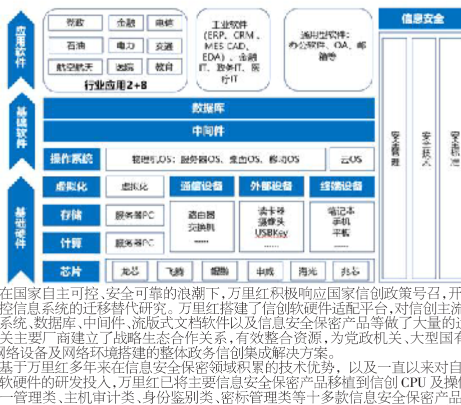
万里红主要政务应用系统如下:

产品名称	产品用途	客户群体
党务管理信息系统	建立一套适合基层使用的、功能多样的党务信息化系统,用于统计各类信息,进行多样化的党建活动	党政机关及组织工作部门
干部人事管理信息系统	实现干部信息管理业务的计算机处理和网格化管理,用于组织部门对干部信息进行统计及管理	党政机关及组织工作部门
干部任免审批表编辑器	用于编辑、打印干部任免表等干部管理的日常工作	党政机关及组织工作部门
PDA 领导干部查询系统	用于领导干部在移动设备上浏览、查询干部信息	党政机关及组织工作部门
干部任免管理信息系统	实现上会前干部任免人员名单相关信息的维护,为干部任免上会系统提供上会演示辅助材料	党政机关及组织工作部门
公务员管理信息系统	按照统一标准建设和完善公务员信息,为公务员管理和公务员队伍建设工作提供信息服务和辅助决策支持	党政机关及组织工作部门
人才管理信息系统	建立本级人才信息,实现对人才的基本信息、学历、职称、专业技术水平、科技成果、主要业绩等信息的动态管理,为人才管理工作提供信息服务和辅助决策支持	党政机关及组织工作部门
非公有制经济代表人士综合评价系统	用于及时对相关人士进行评价操作	中央及地方统战部经济处
共青团管理信息系统	将数据采集、信息管理、统计分析等功能合为一体,用于各级团组织进一步了解基层团组织各项情况	共青团系统

政务信创集成:

信创行业,即信息技术应用创新行业,其主要内涵为基于自有 IT 底层架构和标准建立起来的 IT 产业生态,而党政领域安全可控体系的建立即为政务信创。

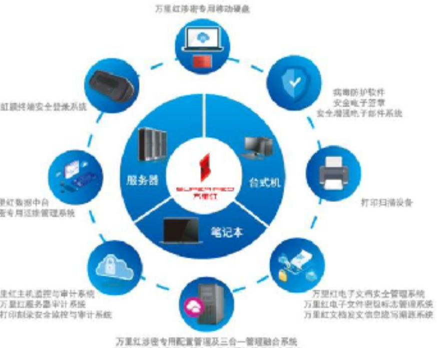
我国信创行业的全景图如下:



在国家自主可控、安全可靠的浪潮下,万里红积极响应国家信创政策号召,开展国家关键领域自主可控信息系统的迁移替代研究。万里红搭建了信创软硬件适配平台,对信创主流服务器、桌面终端、操作系统、数据库、中间件、流版式文档软件以及信息安全保密产品等做了大量的适配工作,与信创产品相关主要厂商建立了战略生态合作关系,有效整合资源,为党政机关、大型国有企业提供软件、整机、网络设备及网络环境搭建的整体政务信创集成解决方案。

基于万里红多年来在信息安全保密领域积累的技术优势,以及一直以来对自主可控信息设备及配套软硬件的研发投入,万里红已将主要信息安全保密产品移植到信创 CPU 及操作系统平台上,其中三合一管理类、主机审计类、身份鉴别类、密标管理类等十多款信息安全保密产品已经进入了国家信创名录。万里红能够在为客户构建自主可控信息系统的基础上,提供适配的信息安全保密产品,以保障自主可控信息系统的安全、可靠。

万里红已与多家信创企业建立战略合作关系,与国内多家主流 CPU、基础软件、办公软件、应用软件及云平台等信创企业完成产品联合认证测试,在产品的功能、性能等方面完全兼容,运行稳定高效,逐步构建起万里红信创生态,具体如下:


万里红涉密专用移动硬盘
病毒防护软件
安全电子签章
安全增强电子邮件系统
打印扫描设备
万里红电子文档安全管理系统
万里红电子文件密级标志管理系统
万里红文档发文信息隐写溯源系统
万里红涉密专用配置管理及三合一管理融合系统
万里红涉密专用服务器安全授权管理融合系统
万里红主机监控与审计系统
万里红服务器审计系统
万里红打印刻录安全监控与审计系统
万里红数据中台
万里红涉密专用运维管理系统
万里红虹膜终端安全登录系统
服务器
台式机
笔记本
SUPERRED
万里红

3、主要经营模式

公司盈利模式、采购模式、生产开发及服务模式、销售模式、结算模式如下:

1)盈利模式

万里红目前产品类型较多,客户群体涵盖政府机关、军工单位、国企单位、金融机构及教育机构等。其中,信息安全保密业务为客户提供信息保密产品及需求解决方案,虹膜识别业务为客户提供虹膜采集识别设备和安全保障解决方案,政务集成业务为客户提供信息系统的规划、设计、实施、运维、技术支持等服务以及自主可控信息系统的适配。万里红通过提供高技术水平的产品及综合解决方案实现盈利。

2)采购模式

万里红对外采购主要包括软硬件产品(专用 U 盘、光单导、虹膜镜头、操作系统、计算机、服务器、应用软件等)及技术服务(安装调试、技术培训、技术支持、系统运维、非核心功能的开发测试以及其他服务等)。其中,软硬件产品由业务部门根据清单情况以及生产和销售计划,结合现有库存情况,拟定采购计划,收到采购产品后,由质量检验部门按照合同及万里红相关规定进行验收入库。万里红建立了较为完善的供应商管理制度,对供应商进行考核评价,以保证采购渠道的稳定性和采购成本的可控性。

3)生产、开发及服务模式

万里红业务涵盖信息安全保密、虹膜识别以及政务集成,主要业务流程覆盖项目咨询、设计、开发、实施、运维全过程,具体产品及服务包括软件产品、硬件产品及解决方案。万里红软件类产品主要根据客户需求提出解决方案,设计系统架构,进行软件及系统设计、开发和编程;硬件类产品则通过对采购硬件进行装配、检测和调试,并根据客户需求将完成自主开发软件进行嵌入和灌装,完成对硬件产品的高技术含量工序加工;对于解决方案类产品,万里红根据用户应用需求,设计解决方案,对解决方案涉及的硬件设备和软件产品进行选用,实施解决方案,通过检测后为客户进行现场安装调试,并根据客户要求定期在现场或远程完成系统维护、检查、调试升级等工作。

4)销售模式

万里红的销售模式以直销为主,主要产品涉及信息安全保密、虹膜识别以及政务集成相关产品及整体解决方案。销售部门整体负责市场开发、需求反馈、产品销售、客户管理和维护、对接售后服务等工作。销售价格考虑生产成本、市场需求、竞争情况等因素,与客户协商定价。对于党政机关、国有企业等客户,万里红一般通过参与公开招标、邀请招标、竞争性谈判、单一来源采购等政府购买方式取得订单。此外,对于虹膜识别业务,万里红为加速虹膜识别业务市场推广和提高市场占有率,通过自主推广和代理商推广相结合的模式进行市场开拓。

5)结算模式

报告期内,万里红分别与供应商、客户约定不同的结算模式:

供应商方面,万里红综合考虑采购内容以及与供应商的合作关系等因素确定与供应商的结算方式。一般而言,在软硬件采购入库、技术服务商提供完技术服务并开具发票后一定期间(1-3 个月)内支付货款。

客户方面,万里红通常与客户在合同约定达到项目各阶段付款条件后即付款,在实际执行过程中,由于万里红客户主要为政府机关、军工单位、国企单位、金融机构及教育机构等,项目付款流程需要一定的审批时间,且主要客户遵循预算管理制度,采购资金的支付集中在第四季度,所以万里红收到回款的时间与合同约定时间或存在一定差异。

(二)报告期内公司产品市场地位、竞争优势与劣势、主要的业绩驱动因素、业绩变化是否符合行业发展状况等内容

1、公司产品市场地位

2021 年 6 月,国内数字化产业第三方调研与咨询机构数世咨询发布《中国网络安全百强报告(2021)》,公司凭借技术经验积累和业务实力,成功入选"2021 中国网络安全百强",位于综合实力百强竞争者类别。

2022 年 11 月 15 日,由中国计算机学会抗恶劣环境计算机专委会、信息产业信息安全测评中心、安全牛联合发起的第十版《中国网络安全企业 100 强》(基于 2021 年度数据)正式发布,公司凭借出色的经营能力、产品能力以及广泛的行业应用从 300 余家参选企业中脱颖而出,位列榜单第 16 名,排名较第九版上升 7 位。

2022 年 3 月,行业安全咨询机构"安全牛"发布《中国网络安全行业全景图(第九版)》,全面展现当前我国网络安全行业整体概况。公司凭借多年的技术积累及创新服务优势,多款产品入选 2022《中国网络安全全景图(第九版)》数字办公安全、保密安全、主机安全、身份认证、文档安全、网络访问控制、上网行为管理、网络准入控制、物理环境安全 9 项细分领域,覆盖计算环境安全、身份与访问安全、数据安全、网络与通信安全、物理环境安全五项一级安全分类。成功入选安全牛网络安全行业全景图,充分体现了业界对公司在网络安全领域成果表现的高度认可,肯定了公司过硬的技术创新能力和卓越的产品服务能力,奠定了公司在网络安全行业领先品牌的地位。

2、竞争优势与劣势

公司凭借多年深耕行业形成的对客户需求的深度了解和技术积累,且已经回归中科院,在技术、产品、人才、客户等方面建立起了自身的竞争优势。

1)国资和中科院体系双重赋能

在网络安全被日益重视的情况下,万里红回归国资体系,为万里红的业务拓展打开了长足的发展空间,在国资和中科院体系的双重赋能下,万里红品牌形象及资源渠道将得到进一步增强,加速业务的快速增长。中科院是全球在科研领域国立科研机构的代表、是咱们国家的战略科技力量。万里红背靠中科院基础研究力量,可以实现天然结合,助力科研成果转移转化。

2)技术优势

万里红自 2001 年成立之初即开展基础软件和政务信息化相关研究,2002 年开始涉足信息安全保密领域,2005 年进入虹膜识别领域。20 年来,万里红一直深耕信息安全保密相关的基础技术自主研发和国产化,具备丰富的技术积累和技术储备。

万里红坚持自主创新,专注于技术研发,拥有多项核心资质,是信息安全保密领域资质较全的企业之一,主要资质包括高新技术企业等。

万里红具备较强的大型研发项目承担能力,先后承担国家 863 计划 1 项,成果获得国家科技进步二等奖;承担"核高基"项目 1 项,"火炬计划"1 项,"电子信息产业发展基金"项目 2 项;"创新基金"2 项;发改委信息安全产品产业化项目 1 项;中国科学院知识创新工程重大项目 1 项。

3)产品优势

在信息安全保密领域,万里红掌握多项核心技术和软件著作权,建立起了完善的信息安全保密产品线,覆盖了综合保密管理系统、网络保密检查、网络安全审计、主机监控审计、数据库审计、访问控制、运维审计、综合日志审计、电磁泄漏发射防护、移动通信防护与保密检查、电磁屏蔽、涉密人员管理、保密工作管理、保密工作应用等方面。万里红通过多年对行业客户的需求深度了解和技术积累,形成了功能覆盖全面、产品安全可靠的核心产品优势和产品形象。

在虹膜识别领域,万里红建造光学实验室打磨高端虹膜设备,为公安、矿山、金融、教育、司法、出入境等领域提供全面的虹膜识别产品及综合解决方案。万里红开发的系列虹膜采集识别设备(包括:手持型、移动型、桌面型、壁挂型)质量过硬,更是在远距离(三米)及行进中虹膜采集识别技术方面取得突破。

在政务集成领域,万里红一直大力投入对国产化专用信息设备及配套软硬件的研发,对信创主流服务器、桌面终端、操作系统、数据库、中间件、流版式文档软件以及信息安全保密产品等做了大量的适配工作。万里红已将主要信息安全保密产品移植到信创 CPU 及操作系统平台上,三合一管理类、主机审计类、身份鉴别类、密标管理类等十多款产品已进入国家信创名录,系入围信创三期名录安全保密产品最多的厂商之一。

4)人才优势

万里红业务骨干大多来自于清华大学、国防科技大学、中科院等知名学府和科研机构,且拥有多年信息技术行业从业经验,70%以上的员工取得本科学历。万里红技术总监张小亮博士入选 2019 年度"国家百千万人才工程",被人力资源和社会保障部授予"有突出贡献中青年专家"荣誉称号,同时入选"北京市科技创业领军人才。同时,万里红拥有强有力的技术支撑和坚实的技术后盾,通过国家级的科研项目、良好的成长环境和优厚的回报吸引高素质人才。

5)客户优势

万里红依托于产品的安全可靠及技术优势,通过良好服务积累了良好的客户口碑和客户资源。主要客户包括公安部、中组部、教育部、中国人民银行、检察院等政府机关、军工单位、国企单位、金融机构及教育机构等,该类型客户对产品性能、质量、安全性均有较高要求,与安全可信赖的供应商建立良好合作关系后,具备长期较为稳定的合作意愿。

3、主要的业绩驱动因素

(1)信息安全保密行业

①国家产业政策的积极支持

信息安全保密是国家安全战略的重要组成部分,国家秘密事关国家安全和利益,国家秘密一旦泄露,必将直接危害国家的政治、经济、科技和文化安全,更会危害广大人民群众的利益,是国家的重要战略资源。近年来国际贸易摩擦事件频发,核心技术受制于人会带来极大的风险,而由于信息安全保密领域具有涉密性,信息安全保密领域的关键技术一旦受到限制,会对国家信息的安全造成威胁,因此是自主可控的重中之重。

近年来,党中央、国务院高度重视信息安全保密工作,出台了一系列的与信息安全保密紧密相关的法规和规划,从而为我国信息安全保密相关领域的发展提供了强有力的政策支持和良好的政策环境。全国人大常委会发布的《中华人民共和国网络安全法》强化了网络运行安全,为网络安全行业明确了治理目标和战略;公安部发布的《网络安全等级保护条例(征求意见稿)》提出了对网络和信息系统按照重要性等级分级别保护的要求,都为行业发展提供有力的政策保障与推动。

②市场需求旺盛,未来空间广阔

信息安全保密产品的服务对象较为广泛,涉及的行业、领域、人员范围越来越大。随着信息技术的不断进步,信息安全保密的应用空间进一步扩大。另外随着各企业保密意识的增强,信息安全保密检查、信息安全保密防护、安全审计以及安全风险评估与分析等信息安全保密产品的市场需求持续增加。

(2)虹膜识别行业

①国家产业政策的积极支持

我国生物识别行业虽然起步较晚,但后发优势显著,产业势头强劲,应用需求旺盛。近年来,我国相继出台了《"互联网+"人工智能三年行动实施方案》、《新一代人工智能发展规划》、《促进新一代人工智能产业发展三年行动计划(2018-2020 年)》、《关于促进网络安全产业发展的指导意见》(征求意见稿)》等政策文件,推进生物特征识别等关键技术的研发和产业化,拓展在安防、金融、网络安全等领域的应用,支持生物识别行业的发展。

②虹膜识别应用广泛,市场空间广阔

利用生物识别技术进行身份认证、人机交互已经成为消费级和企业级市场的重要趋势,而相比当下流行的指纹识别与人脸识别,虹膜识别在准确性、稳定性、可复制性、活体检测等综合安全性能上占据绝对优势,有望在金融、医疗、安检、安防、特种行业考勤与门禁、工业控制等领域实现广泛运用,市场空间广阔。

③进军消费电子领域,或将驶入快车道

当前无论是硬件还是虹膜识别算法,均已比较成熟,可以支持虹膜识别在智能手机、平板等消费电子上应用。目前,智能手机上应用虹膜识别技术的趋势已经显现。2015 年 3 月,富士通为智能手机带来了虹膜识别技术,可以直接通过眨眼就能解锁手机。2016 年 8 月,三星发布旗舰机 Note7,这是虹膜识别技术首次出现在主流手机厂商的旗舰机。未来随着虹膜识别技术在消费电子市场的空间被打开,虹膜识别有望在更多智能手机、平板电脑上得到应用。

(3)政务集成行业

①国家产业政策的积极支持

信创行业事关国家安全,近年来国家多次出台相关政策法规,并将其部署为国家重要战略。《国家信息化发展战略纲要》、《软件和信息技术服务业发展规划(2016-2020 年)》、《关于实施涉密领域国产化替代工程的通知》、《国家政务信息化项目建设管理办法》、《关于新时期促进集成电路产业和软件产业高质量发展若干政策的通知》等政策法规均大力支持信创产业的发展,推动自主可控进程。

②信创放量在即,打开广阔市场空间

信创行业涵盖从底层到应用层,包括基础硬件、基础软件、应用软件以及系统集成。基础信创在国家"2+8"安全可控体系的推动下放量在即,2020-2022 年是国家安全可控体系推广最重要的 3 年,中国 IT 产业有望迎来自主可控浪潮,2020 年将成为信创产业全面推广的起点,政务信创成为规模化推广的首要目标,未来在行业应用和民用商用领域铺开后,信创市场空间将进一步扩大。

报告期内,公司净利润较同期有所下降的主要原因是公司持续加大产品及解决方案的研发投入,提升产品竞争力,研发费用约 1.39 亿元,研发人员数量增长约 6%。公司成本费用的增速,影响了公司利润水平。同时,由于不可抗力因素等方面影响,万里红部分订单延期,导致部分收入确认递延。这两项因素在一定程度上影响了利润与上年同期比较水平。

3、主要会计数据和财务指标

(1)近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据

□是 ☑ 否

单位:元

	2022 年末	2021 年末	本年末比上年末增减	2020 年末
总资产	5,154,039,762.40	5,273,831,637.82	-2.27%	1,066,541,854.58
归属于上市公司股东的净资产	3,353,237,106.99	3,852,869,981.60	-12.97%	549,115,674.83
	2022 年	2021 年	本年比上年增减	2020 年
营业收入	3,022,814,268.86	1,848,389,467.26	63.54%	1,129,966,213.42
归属于上市公司股东的净利润	888,840,608.20	171,858,699.94	417.19%	55,044,402.33
归属于上市公司股东的扣除非经常性损益的净利润	-120,972,233.67	172,418,229.68	-170.16%	55,640,536.55
经营活动产生的现金流量净额	-130,715,792.30	244,473,998.14	-153.47%	90,769,525.10
基本每股收益(元/股)	2.8712	1.0116	183.83%	0.3513
稀释每股收益(元/股)	2.8601	1.0058	184.36%	0.3500
加权平均净资产收益率	20.79%	18.50%	2.29%	10.03%

(2)分季度主要会计数据

单位:元

	第一季度	第二季度	第三季度	第四季度
营业收入	575,407,115.00	577,431,455.52	597,019,859.74	1,272,955,838.60
归属于上市公司股东的净利润	-8,878,144.75	6,340,109.83	-15,756,008.99	907,134,652.11
归属于上市公司股东的扣除非经常性损益的净利润	-9,944,036.76	3,229,342.88	-16,661,433.48	-97,596,106.31
经营活动产生的现金流量净额	-231,354,219.53	113,353,216.65	-96,991,219.50	84,276,430.08

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□是 ☑ 否

4、股本及股东情况

(1)普通股股东和表决权恢复的优先股股东数量及前 10 名股东持股情况表

单位:股

报告期末普通股股东总数	13,667	年度报告披露日前一个月末普通股股东总数	17,166	报告期末表决权恢复的优先股股东总数	0	年度报告披露日前一个月末表决权恢复的优先股股东总数	0

前 10 名股东持股情况

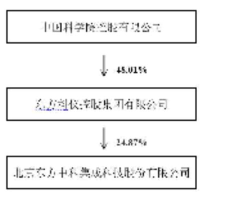
股东名称	股东性质	持股比例	持股数量	持有有限售条件的股份数量	质押、标记或冻结情况	
					股份状态	数量
东方科仪控股集团有限公司	国有法人	24.87%	76,064,719	36,959,846		
万里锦程创业投资有限公司	境内非国有法人	13.03%	39,850,238	32,803,687		
大连金融产业投资集团有限公司	境内非国有法人	12.29%	37,570,000	0		
刘达	境内自然人	3.54%	10,837,363	5,205,610		
金泰富资本管理有限责任公司	境内非国有法人	3.05%	9,319,328	2,099,090		
王戈	境内自然人	2.58%	7,903,743	7,802,807	质押	5,425,000
杭州明颉企业管理有限公司	境内非国有法人	2.50%	7,651,948	3,608,406		
珠海格力创业投资有限公司	境内非国有法人	2.03%	6,212,884	1,399,393		
青岛精确力升资产管理有限公司-青岛精确智芯股权投资合伙企业(有限合伙)	其他	1.85%	5,659,472	1,399,393		
张林林	境内自然人	1.46%	4,452,256	2,099,537		
上述股东关联关系或一致行动的说明	上述股东中,刘达与张林林构成一致行动关系,其他股东并未向公司报告一致行动人关系。					
参与融资融券业务股东情况说明(如有)	不适用					

(2)公司优先股股东总数及前 10 名优先股股东持股情况表

□适用 ☑ 不适用

公司报告期无优先股股东持股情况。

(3)以方框图形式披露公司与实际控制人之间的产权及控制关系



5、在年度报告批准报出日存续的债券情况

□适用 ☑ 不适用

三、重要事项

受不可抗力因素的影响,万里红所处信创市场环境及其生产经营活动均受到不可抗力的冲击,万里红在研发市场投入也大幅增加,导致万里红 2020 年、2021 年和 2022 年承诺扣除非经常性损益后归属于母公司股东的净利润(以下简称"净利润")分别为 0.71 亿元、2.1 亿元和 3.1 亿元,三年累积承诺净利润为 5.91 亿元;2020 年、2021 年和 2022 年万里红实现的实际净利润分别为 7,311.35 万元、11,164.25 万元和-11,406.22 万元,三年累积实现净利润为 7,069.38 万元,交易对手方存在业绩不及承诺,未来进行业绩补偿的可能,还请投资者注意相关风险。