证券简称：山石网科　　**证券代码：**688030

山石网科通信技术股份有限公司

Hillstone Networks Co., Ltd.

（苏州高新区景润路 181 号）

向不特定对象发行可转换公司债券
募集资金使用可行性分析报告
（修订稿）

二〇二一年八月

一、本次募集资金运用计划

本次向不特定对象发行可转换公司债券拟募集资金不超过 26,743.00 万元（含本数），扣除发行费用后的募集资金净额将全部用于以下项目：

序号	项目名称	项目投资总额（万元）	拟使用募集资金额（万元）
1	苏州安全运营中心建设项目	32,277.00	10,530.00
2	基于工业互联网的安全研发项目	22,393.00	16,213.00
合计		**54,670.00**	**26,743.00**

如本次发行实际募集资金（扣除发行费用后）少于拟投入本次募集资金总额，公司董事会将根据募集资金用途的重要性和紧迫性安排募集资金的具体使用，不足部分将通过自筹方式解决。在不改变本次募集资金投资项目的前提下，公司董事会可根据项目实际需求，对上述项目的募集资金投入顺序和金额进行适当调整。在本次发行可转换公司债券募集资金到位之前，公司将根据募集资金投资项目实施进度的实际情况通过自筹资金先行投入，并在在募集资金到位后按照相关法律、法规规定的程序予以置换。

二、本次募集资金投资项目的实施背景

（一）网络攻击事件频发，行业发展政策持续加码，网络安全的重要性日益提升，网络安全市场前景可观

世界经济论坛《2019 年全球风险报告》中指出，网络攻击已成为目前全球五大风险之一，其威胁主要源于三个方面：第一，软硬件设备安全漏洞频出；第二，行业关键信息基础设施遭受攻击；第三，个人信息与商业数据遭遇大规模泄露及违规利用。随着信息技术在日常生产、生活中的不断渗透，未来全球将可能面临更多类型的网络攻击威胁，其影响的范围亦将更为广泛。

为了应对网络威胁，保障信息技术健康可持续发展，全球各国都在持续加大在网络安全方面的投入，并通过发布相关法律法规将网络安全行业的重要性提升到国家安全的战略高度，中国亦不例外。

一方面，我国网络安全相关立法及重要制度建设持续加快推进。2016 年，

国家互联网信息办公室发布了《国家网络空间安全战略》；2017 年《网络安全法》颁布实施；2019 年 5 月，网络安全等级保护 2.0 系列标准正式发布；2019 年 7 月，《密码法（草案）》向社会公开征求意见；2019 年 12 月，等级保护 2.0 系列新规正式实施；2020 年 6 月，《数据安全法（草案）》初次审议通过。

另一方面，国家在重要行业和新兴领域的安全要求进一步细化明确，以电力、工业互联网、车联网等重要行业领域为例，其网络安全相关顶层设计陆续出台：2018 年 9 月，国家能源局发布了《关于加强电力行业网络安全工作的指导意见》，强调“提升电力系统安全稳定运行和电力可靠供应的能力”；2019 年 9 月，工业和信息化部会同九部门联合印发《加强工业互联网安全工作的指导意见》，要求“加快构建工业互联网安全保障体系，形成覆盖工业互联网全生命周期的事前防范、事中监测和事后应急能力”。

综上，现阶段国内对网络安全的重视程度已经达到了历史高点，行业政策持续加码，为行业后续发展营造了良好的政策环境，市场前景可观。

（二）信息技术快速发展推动各行各业数字化转型，客户的网络安全需求呈现多元化趋势，国内网络安全市场将从安全硬件向安全软件、安全服务加快延伸

与全球相比，中国网络安全市场近几年在国家政策、数字经济、威胁态势等多方需求驱动下，整体的市场规模呈现较快发展。

根据 2021 年 3 月最新发布的《IDC 全球网络安全支出指南,2021V1》，IDC 预测，2021 年中国网络安全市场总体支出将达到 102.2 亿美元，到 2024 年，中国网络安全市场规模将增长至 172.7 亿美元，2020-2024 年预测期内的复合年均增长率为 16.8%，增速继续领跑全球网络安全市场。2020 年，安全硬件在中国整体网络安全支出中仍将继续占据绝对主导地位，占比高达 47.2%；安全软件和安全服务支出比例分别为 20.8%和 32.0%。

总体上，随着信息技术的快速发展，数据成为了新型生产要素，推动各行各业数字化转型，作为支撑信息化建设的重要组成部分——网络安全的产品形态正在加速由传统的安全硬件逐步向安全软件、安全服务等模式演变，从而满足新技术、新场景下的客户新需求。

（三）作为专注于网络安全行业技术创新的厂商，公司仍处于成长阶段，需要持续扩充产品线并加大安全服务投入，从而不断提升整体安全解决方案能力

公司是中国网络安全行业的技术创新型厂商，自成立以来一直专注于企业级网络安全产品的研发与创新。公司于 2007 年在国内率先自主研发出基于多核处理器的网络安全产品，具备了自主软硬件设计能力，确立了产品的高性能优势。2010 年，公司自主研发出分布式防火墙产品，通过多个处理器集成到一个设备中，大幅提高了单设备的处理性能，进一步奠定了公司在边界安全产品线的竞争优势。

近年来，公司一直在加强网络安全产品线的性能优化与品类扩充，从安全硬件逐步扩展至安全软件及安全服务。目前，公司的产品线已涵盖边界安全、云安全、其他安全（主要包括：Web 安全、内网安全、数据安全、应用交付、态势感知）等领域。

2018 年至 2020 年，公司营业收入从 5.62 亿元增长到 7.25 亿元，年均复合增长率为 13.58%；公司归母净利润从 6,891.17 万元降至到 6,023.52 万元，年均复合增长率为-6.51%；同时，过去三年，公司边界安全产品收入年均复合增长率为 2.71%，云安全产品收入年均复合增长率为 39.37%，其他安全产品收入年均复合增长率为 134.45%，公司核心业务保持了较为稳健的发展。2018 年至 2020 年，公司研发费用分别为 15,646.14 万元、18,674.72 万元及 21，221.62 万元，占同期营业收入比例分别为 27.83%、27.68%及 29.26%，长期保持了较高的研发投入。截至 2021 年 3 月末，公司拥有研发人员 490 名，占员工总人数比例 34.58%。

新技术、新场景应用推广是网络安全行业发展的重要驱动力。近年来，苏州实施制造强市战略，以创建“中国制造 2025”国家级示范区为突破，在坚实的制造业基础上，实现“苏州制造”向“苏州智造”的转变。作为总部在苏州的网络安全企业，公司将充分发挥苏州的区域优势，在前期产品线持续扩充的基础上，加大对智能制造企业的需求挖掘，研发针对工业互联网场景下的安全产品。此外，结合客户实际需求及市场发展趋势，公司于 2020 年构建了“安全产品+安全服务”模式，将产品与服务深度融合形成合力，进一步提升安全整体解决方案能力与安全运营效率。

在未来的一段时间内，公司仍处在快速成长阶段，需要持续加大在产品端及服务端的投入，吸引更多优秀的人才加入，把握行业发展的机会，努力将公司在传统安全产品线上的竞争优势拓展至其他产品线及安全服务领域，从而逐步提升公司的核心竞争力和市场占有率。

三、本次募集资金投资项目的具体情况

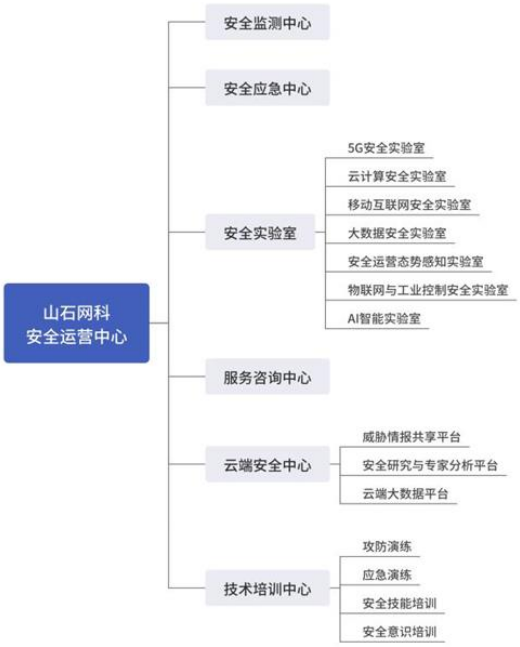
（一）苏州安全运营中心建设项目

1、项目概述

苏州安全运营中心建设项目拟通过整合公司在安全行业内的各项优势资源，组建安全服务专家团队并成立安全服务咨询中心，提供风险评估、等保咨询、管理咨询等安全咨询服务；同时，结合公司在安全漏洞、弱口令、网马暗链、远控后门等网络脆弱性扫描和高危流行漏洞渗透测试方面的服务能力，以及在威胁检测和防御、威胁情报等方面的技术积累，公司还将建立安全监测中心和安全应急中心，实现安全运营能力的输出，以应对不断变化的网络威胁形式，从而满足下游客户群体对各类网络安全的要求。

2、项目建设内容

安全运营中心建设内容如下图所示：



2、项目可行性分析

（1）安全运营市场份额快速增长，优于传统安全产品市场增速

国家重视行业地方信息安全建设的表现为加大对信息化产值的投入及利用。信息安全建设涉及我国国家重点行业（电力、能源、制造、能源、运营商、金融、医疗、政府等）以及关键信息基础设施分布产业、国家、地方政府重点扶持产业等多领域建设。近年来由于国家对安全建设的重视，各行业在传统安全建设、安全设备建设方面已形成建设规模及目标设备构建，由于传统安全产品市场竞争优势差异化缩小，多行业随新技术领域、国家安全政策扶持风向，逐步关注于新技术、新场景。安全运营已逐渐成为网络安全行业投资新风向。

（2）公司优质的客户资源及高端的品牌形象为发展安全运营服务奠定坚实基础

经过行业内十余年的耕耘及积累，公司目前已累计为 20,000 余家客户提供了稳定、高效的网络安全解决方案。凭借突出的研发创新能力、出色的产品品质以及高效的响应速度等多维综合实力，公司得到了金融、政府、运营商、互联网、教育、医疗卫生、能源交通等优质行业客户群体的广泛认可，在国内市场已普遍形成高品质、技术领先的高端品牌形象。广泛优质的客户群体为公司多元产品线格局的建立创造了良好的成长环境，同时也为公司从传统安全产品向安全服务的延伸奠定了坚实的客户基础。

（3）公司具备安全运营所需技术能力、资源能力及本地化安全能力

安全运营平台建设作为核心建设，其技术能力、坐标定位、人员能力及人员规模将作为安全运营建设可行性的重要保障。安全运营中枢核心位于公司总部苏州山石网科大厦，目前公司具备安全运营平台建设所需云端资源环境、高精尖的人员研发能力、云安全服务资源支持保障能力及相关配套服务等前提条件，可为客户提供安全运营所需的高质量、高价值的安全技能交付等能力。此外，安全运营平台资源支持中，最重要的技术核心为云安全技术；在云安全技术领域，公司是国内最早进行云计算数据中心安全领域研发的厂商之一，2020 年公司成功入选 Gartner 云工作负载安全防护平台市场指南（CWPP），成为国内首家获得该指南推荐的“微隔离与可视化云安全产品”全球供应商。同时，在威胁检测和响应领域，公司已连续 3 年入选 Gartner IDPS（入侵检测和防御系统）市场指南&

魔力象限；2019 年和 2020 年连续两年成为中国唯一入选《网络威胁检测及响应全球市场指南》的网络安全厂商。经过多年的研发投入，目前公司能够为云计算数据中心提供覆盖网络层、应用层、数据层等全面的安全防护，云计算安全技术在全球范围内处于先进水平，为安全运营平台搭建提供强有力的支持及保障。

3、项目必要性分析

（1）安全运营中心的建设有利于提升公司整体安全服务能力

传统安全设备一般基于网站防护、威胁预警层面，多以行为识别、网站特征库比对等方式实现网站安全风险识别及威胁预警。然而，受限于情报库静态化、数据基础及更新频率、无法联动获取全网环境网站风险、误报高、高价值威胁数据提取筛选能力差等因素，依靠单一传统安全设备无法达到实时性、有效性网站安全分析监测及预警等功效，并且对未知威胁防御、检出及预判能力存在一定的滞后性。

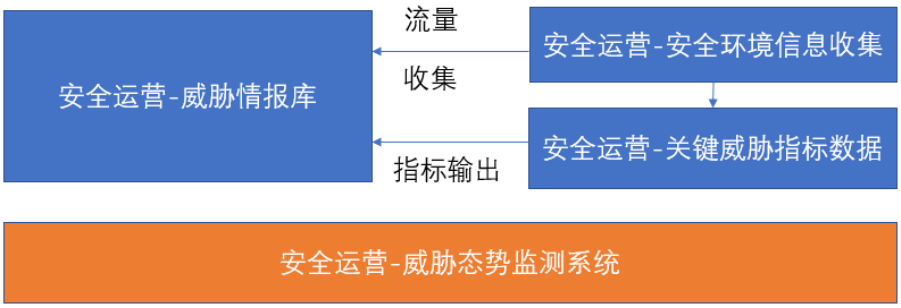
基于此，公司安全运营中心建设将针对关键信息基础设施建设过程中的安全痛点，解决当下传统安全产品仅针对单点防护或专项安全建设、无法相互联动及高效利用、安全建设过程中价值发挥能力不足等问题，构建安全运营环节的威胁检测、威胁防御及威胁综合研判能力，提升整体安全建设过程中威胁防御及事件处置能力。

此次公司安全运营中心的建设核心，源于自身海量级安全运营-威胁情报库的实时数据获取、采集、积累及更新，并引用大数据+AI 技术设定网站安全基线、风险预警参数等，从而实现网站安全风险的动态化检出、网站安全风险行为分析及安全预警。同时，公司将通过与安全服务、安全产品建设高效联动，满足安全威胁防御过程中所需的实时性、溯源性、针对性，打通安全威胁防御闭环，从而提升公司整体安全服务能力。

（2）安全运营中心的建设有利于构建城市级安全运营中枢，有助于公司进一步开拓新市场、新客户

安全运营中心建设将不局限于单个行业监管机构、行业单位及内部组织，而是以服务资源模式构建国家级、城市级安全运营中枢，为国家、城市安全中的行业监管、行业单位及组织的安全建设能力进行孵化及循环赋能，全面实现安全建设价值化。

地方单位海量信息流量数据，通过汇总于上级监管单位安全运营平台中心，安全运营平台又以监管机构、市级、省级安全运营中心为基点，高效收集、量化筛选、精准提炼安全威胁指标数据，实现构建城市级安全运营中枢的目标。构建城市级安全运营中心建设过程中，数据获取、威胁情报库建设、全时段安全运营威胁态势监测组件流转示意图如下：



如图，安全运营中心通过基于平台化构建，通过底端“安全运营-威胁态势监测系统”进行全面化安全威胁监控、环境信息收集及安全指标信息收集，使安全威胁形成量级化“安全运营-威胁情报库”。通过数据价值化关联、分析、呈现、输出、运用，使威胁指标价值化落地服务于国家级、城市级安全运营。

此外，安全运营中心建设将基于城市安全运营进行覆盖，还可服务于政府、医疗、运营商、教育等多行业领域安全运营建设，形成行业安全风险问题检测发现、信息收集、风险处置、指标量化的全维度、高精度、可视化的综合呈现，为多行业领域安全运营提供保障，从而有助于公司进一步加大新市场、新客户的开拓

4、项目投资概算

项目总投资额为 32,277.00 万元，主要用于安全运营中心所需办公场所购置及装修、研发设备及软件购置以及支付研发人员和安全运维人员的工资。安全运营中心建设项目计划在苏州市高新区实施。公司已召开第一届董事会第二十一次会议，审议通过《关于拟购买资产的议案》，拟竞买公司目前租赁使用的苏州高新区景润路 181 号房地产，作为苏州安全运营中心建设项目的实施场所。截至本可行性报告出具之日，相关不动产权变更登记手续已办理完毕。

具体资金运用情况见下表：

单位：万元

序号	类别	投资额	投资额占该项目总投资比	拟使用募集资金投入金额
1	办公场所购置及装修	22,100.00	68.47%	1,020.00
2	研发设备及软件购置	4,370.00	13.54%	4,370.00
3	研发投入	1,227.00	3.80%	920.00
3.1	研发投入-资本化部分	641.40	1.99%	641.40
3.2	研发投入-费用化部分	585.60	1.81%	278.60
4	安全运维人员投入	4,220.00	13.07%	4,220.00
5	其他	360.00	1.12%	-
合计		**32,277.00**	**100%**	**10,530.00**

5、项目备案手续

2020 年 12 月 21 日，苏州安全运营中心建设项目已完成备案，并取得苏州高新区（虎丘区）行政审批局颁发的《江苏省投资项目备案证》（苏高新项备（2020）519 号）。

（二）基于工业互联网的安全研发项目

1、项目概述

工业互联网在提高工业企业生产和管理效率的同时，也会带来全新的网络安全挑战。随着工业互联网的不断发展，工业系统中的关键信息基础设施正逐步暴露于攻击者的视野之中，近年来针对工业互联网实施的高持续性威胁事件频发，造成的影响和损失与日俱增。

公司在网络安全领域耕耘十多年，积累了防火墙、入侵检测、智能威胁检测技术、云安全技术、态势感知等领域丰富的安全技术与产品经验。同时，工业互联网安全与 IT 网络安全在协议解析、访问控制上有很大的相似性，公司积累的技术、产品与工业互联网结合，可应用于工业互联网安全领域。同时，在工业互联网安全的典型行业，如电力、能源、交通、制造业等，公司已积累了大量的优质客户，依托公司的技术、产品和客户资源，可以进一步拓展覆盖的市场，并提升公司盈利能力。

2、项目建设内容

围绕工业互联网安全保障的内在要求，为实现从“被动防御”到“主动防御”的

演进发展，基于工业互联网的安全产品研发项目涵盖工业互联网终端、网络、平台三大层级，涉及设备安全、控制安全、网络安全、数据安全、平台安全和应用程序安全六个方面。本次募投项目具体建设内容包括：关键技术研究、产品研发、重点行业解决方案三个部分。

（1）工业互联网安全关键技术研究

工业互联网安全关键技术研究，具体技术包括：

序号	关键技术名称
1	工业设备指纹采集与分析技术
2	工业协议识别技术
3	工业系统漏洞识别与管理技术
4	工业系统威胁检测与攻防对抗技术
5	工业系统异常行为检测技术
6	工业互联网与物联网结合的安全关键技术研究
7	工业互联网与 5G 结合的安全关键技术研究

（2）工业互联网安全产品研发

工业互联网安全产品研发，计划开发的具体产品如下：

序号	计划开发的产品名称
1	工业防火墙
2	工业入侵检测与防御系统
3	工业漏洞扫描与管理系统
4	工业安全审计系统
5	工业态势感知系统
6	工业互联网虚拟化安全系统

（3）重点行业解决方案

本项目主要针对行业包括电力能源、石油化工、轨道交通、智能制造、水利水务五个重点行业。公司拟针对上述行业推出解决方案，并根据客户的特定需求进行产品的定制化开发与优化，满足重点行业在安全方面的需求。

3、项目可行性分析

（1）国家战略扶持为项目实施提供良好的政策环境

工业互联网是信息通信技术与先进制造业深度融合所形成的新兴业态，是大国之间产业竞争的关键。美国提出了基于先进传感与控制、信息与数字制造等技术的先进制造业战略以吸引制造业回流与复兴；德国重点发展融合物理信息系统，打造工业 4.0 战略，以强化制造业国际竞争力；日本基于机器人、物联网方面的优势打造高附加值工业价值链，以工业支持社会转型；中国为了从制造业大国升级为制造业强国，提出制造 2025 计划，以期深化融合信息通信技术与传统制造业。

2018 年，工业互联网产业联盟编制了《中国工业互联网安全态势报告（2018 年）》。报告指出，当前我国工业互联网平台网络安全防护发展尚处起步阶段，工业互联网应用环境也出现了较多安全问题，工业互联网平台较多采用传统网络安全防护技术、设备构建安全防护体系架构，整体安全解决方案还不成熟，我国工业互联网发展所面临众多挑战。

2019 年 8 月，工业和信息化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》，针对当前工业互联网安全面临的问题，提出促进企业提高工业互联网安全防护水平，推动工业互联网安全科技创新与产业发展的意见，以到 2025 年基本建立起较为完备可靠的工业互联网安全保障体系。

（2）市场快速扩容，为项目实施提供良好的市场环境

工业互联网作为“新基建”重要支点，随着智能制造和工业互联网推进政策的不断出台，政府及企业越来越重视对工业互联网安全的投入，工业互联网安全市场必然会快速增长，驶入发展的黄金时期。根据中商产业研究院的报告数据显示，2018 年、2019 年我国工业互联网产业规模分别为 1.42 万亿元、2.13 万亿元，增长率 50%。在工业互联网安全方面，2019 年国内市场规模在 125 亿元左右，同比增长 30%以上。2020 年工业互联网安全市场规模预估 161 亿，到 2021 年，工业互联网安全规模将达到 230 亿元，两年的复合增长率超 35%。根据中国信通院的研究报告显示，工业互联网安全在未来数年的市场规模将持续高速增长。

从目前的市场来看，工业互联网的安全需求快速上升，由于工业数据主要用于工控设备的运转，对精准的要求高，出现偏差将影响到工业制造流程。所以，

工业互联网的防护，是传统工业企业拥抱互联网的前置保障，其市场增长速度与工业互联网总体增长速度同步。随着工业企业安全意识的提高，工业互联网安全产业也将从以“应急响应”为代表的单点防御向以“持续响应”为代表的纵深防御转变。使工业互联网安全防护体系既覆盖传统的边界防护、流量监测，也会产生新的需求，如态势感知，威胁感知，以对各种未知威胁、高级威胁进行有效预防、发现、防御和回溯。上述情况均为项目的实施提供了良好的市场环境。

（3）公司拥有完善的技术及产品储备，良好的客户口碑，为项目实施提供有效的技术及客户支撑

公司在传统网络安全方面有多年的技术积累，研发了包括高性能防火墙、安全审计、安全运维、入侵检测、态势感知，漏洞扫描、数据库审计与防护、数据泄露防护、云安全防护等多型产品，并在能源、交通、制造等相关的多个行业的众多客户中赢得了良好的口碑，并与众多优质客户形成了稳定的合作关系。针对工业互联网高可靠性及高可用性特征，公司将依托在传统网络安全领域积累的技术，对软硬件进行升级改造，重点研发适应工业互联网场景需求的工业防火墙，工业入侵检测与防御系统，工业漏洞扫描与管理系统，工业安全审计系统，工业态势感知系统，工业互联网虚拟化安全系统，并重点针对电力能源、石油化工、轨道交通，智能制造，水利水务等行业特点，将研发的产品组织成行业解决方案，满足行业用户的安全需求。

4、项目必要性分析

（1）工业互联网安全是支撑工业智能的重要基础，公司布局工业互联网安全项目具有重要战略意义

从工业信息化的发展趋势上看，数字化、网络化、智能化，是工业发展的必然趋势，工业互联网作为工业智能化的重要基础，结合业务智能、智能产品、物联网等技术的发展，工业智能才能真正落地发生，因此，工业互联网是工业智能的基础，而工业互联网安全则是保障工业互联网健康可持续运转的基础。

2019 年，全球工控安全事件的报告数量达到 329 件，各地工控安全问题事件数量呈逐年上升趋势。在这些工控安全事件中，细分领域涉及超过 15 个行业，如制造、石油、电力、供水、交通、医疗、核工业等等。

2020 年上半年，在新的国际形势下，网络战风险加大，高持续威胁（APT）团体正在利用 COVID-19 大流行实施更加广泛的网络攻击。2020 年 2 月，美国一家天然气公司因遭受勒索软件攻击后被迫关闭设施两天，攻击从钓鱼邮件内的恶意链接发起，从其 IT 网络渗透到 OT（Operation Technology）网络，勒索软件对 IT 和 OT 资产都造成了影响。2020 年 4 月，黑客攻击了以色列的水利设施，该国的废水处理厂、泵站、污水处理设施的 SCADA 系统多次遭受了网络攻击。2020 年 5 月，台湾石油、汽油和天然气公司 CPC 及其竞争对手台塑石化公司 FPCC 都受到了网络攻击，导致其 IT 和计算机系统关闭，加油站数字平台无法访问。2020 年 6 月，本田汽车位于美国、欧洲及日本分公司的服务器，遭到网络攻击，攻击传播到本田的整个网络，影响了本田的计算机服务器、电子邮件以及其它内网功能，该攻击事件影响了本田在全球的业务，导致电脑和其他装置无法作业，造成部分工厂停工，损失十分严重。

在新基建浪潮下，中国的工业互联网以及工业互联网安全受到更多关注。工业互联网发展提速，也面临着传统网络安全防护手段在复杂环境下捉襟见肘的问题。2020 年 5 月，工信部发布的《关于工业大数据发展的指导意见》中提到，我国 34%的联网工业设备存在高危漏洞，仅在 2019 年上半年嗅探事件就高达 5,151 万起。指导意见指出，目前工业信息安全责任体系建设还是空白，技术上尚无法有效防护工业数据安全，进而导致工业互联网安全防护能力滞后于工业融合发展进程。

在新冠肺炎疫情爆发之后，中国的制造业与供应链承受着巨大的压力。为了抗击疫情，关键原材料和零部件的供给受到影响，运输业被限制，生产和分销途径受严重影响。而工业互联网，可以实现，全要素、全产业链、全价值链的全面连接，对各类数据进行采集、传输、存储、分析并形成智能反馈，推动形成全新的生产制造和服务体系，优化资源要素配置效率，充分发挥制造装备、工艺和材料的潜能，提高企业生产效率，创造差异化的产品并提供增值服务。工业互联网将成为实体经济各个领域的转型升级提供具体的实现方式和推进抓手，为产业变革赋能，因此，公司布局工业互联网安全具有重要的战略意义。

（2）响应工业互联网安全产业发展需求，有利于公司进一步提升整体解决方案能力并扩大市场机会空间

公司进入工业互联网安全产业，是在工业智能化大趋势与政策支持大环境下，响应工业互联网安全产业的发展需求。同时，目前公司主要为金融、政府、运营商、互联网、医疗、教育、能源、交通、制造业等行业客户提供安全产品、技术、方案和服务，作为国内技术创新型的网络安全厂商，一直走在安全行业创新的前列。目前的公司行业客户，尤其是在能源（如电力、石油）、交通、制造业领域，对公司提出了更多的更高的安全要求，这些行业是典型的工业互联网行业，这些需求本身就是工业互联网安全领域的需求，为了全面响应这些行业客户的需求，公司需要对原有安全产品进行升级和完善。

在产品与方案上，公司将在网络安全、应用安全、虚拟化安全、数据安全、5G 安全、安全审计与管理方面已经积累的大量相关技术与经验，转化为更适合工业互联网场景的安全产品，以满足工业控制协议、工业通信协议、工业运行环境的要求，从而促进公司的产品与方案更加完整。通过对现有行业客户需求的满足，可以充分挖掘客户机会潜力，并增强客户粘性。此外，在工业互联网安全领域的技术具有通用性，在响应现有客户需求的情况下，还可扩展至同行业其他客户，为行业客户提供优质的解决方案，进一步扩大公司的市场机会空间。

5、项目投资概算

项目总投资额为 22,393.00 万元，主要用于项目所需研发设备及软件的购置、支付研发人员工资等。具体资金运用情况见下表：

单位：万元

序号	类别	投资额	投资额占该项目总投资比	拟使用募集资金投入金额
1	研发设备购置	2,630.00	11.75%	2,630.00
2	软件购置	3,850.00	17.19%	3,850.00
3	研发投入	15,613.00	69.72%	9,733.00
3.1	研发投入-资本化部分	6,245.20	27.89%	6,245.20
3.2	研发投入-费用化部分	9,367.80	41.83%	3,487.80
3	其他	300.00	1.34%	-
合计		**22,393.00**	**100.00%**	**16,213.00**

6、项目备案手续

经与苏州高新区（虎丘区）行政审批局沟通确认，基于工业互联网的安全研发项目不属于固定资产投资，因此无需备案。

四、本次募集资金对公司经营管理和财务状况的影响

（一）本次发行可转换债券对公司经营管理的影响

自创立以来，公司一直专注于网络安全领域前沿技术的创新与开拓，经过十余年的发展，公司目前的产品线已涵盖边界安全、内网安全、云计算安全、数据安全、智能分析管理、安全服务等方面。本次募集资金投资项目围绕公司主营业务展开，在现有产品线的基础上进行品类的扩充及品质的提升，同时结合国内网络安全行业的发展趋势与下游客户群体的需求偏好，加强在核心业务领域及新兴市场的投入力度，符合国家相关产业政策及产业发展方向，具有较好的发展前景和经济效益。本次发行有利于加快公司营收多元化，进一步提高公司的盈利能力与规模效应，从而巩固公司的行业领先地位，保持并增强市场竞争力，为公司的可持续发展奠定坚实的基础。

（二）本次发行可转换债券对公司财务状况的影响

本次募集资金到位后，公司的资产规模有所提高，资金实力得到提升，为公司的后续发展提供有力保障。本次可转换公司债券转股前，公司使用募集资金的财务成本较低，利息偿付风险较小。本次可转换公司债券的转股期开始后，若本次发行的可转换公司债券大部分转换为公司股票，公司的净资产将有所增加，资本结构将得到改善。

五、结论

综上所述，本次向不特定对象发行可转换公司债券募集资金投资项目围绕公司主营业务展开，符合国家产业政策以及公司的战略发展规划方向，具有较好的发展前景和经济效益。本次募集资金投资项目的实施，将进一步扩大公司业务规模，增强公司竞争力，有利于公司可持续发展，符合全体股东与可转换债券投资

者的利益。因此，本次募集资金投资项目具备较强的可行性。

山石网科通信技术股份有限公司董事会

二〇二一年八月十三日