

广东精诚粤衡律师事务所
关于珠海市鸿瑞信息技术股份有限公司
首次公开发行股票并在创业板上市的

补充法律意见书（三）

广东精诚粤衡律师事务所
广东省珠海市香洲区情侣中路 47 号怡景湾大酒店五层
电话：（0756）889 3339 传真：（0756）889 3336

目录

问题 1. 关于关于产品与业务	5
问题 2. 关于鸿瑞软件股东	26
问题 3. 关于知识产权	30
问题 5. 关于信息披露	36
问题 14. 关于信息披露豁免	39

广东精诚粤衡律师事务所

关于珠海市鸿瑞信息技术股份有限公司

首次公开发行股票并在创业板上市的补充法律意见书（三）

致：珠海市鸿瑞信息技术股份有限公司（以下简称“发行人”）

广东精诚粤衡律师事务所（以下简称“本所”）根据与珠海市鸿瑞信息技术股份有限公司（以下简称“公司”、“发行人”或“珠海鸿瑞”）签订的《专项法律顾问合同》，接受公司的委托，担任其首次公开发行人民币普通股股票并在创业板上市的特聘专项法律顾问。本所已于 2020 年 11 月 20 日出具了《广东精诚粤衡律师事务所关于珠海市鸿瑞信息技术股份有限公司首次公开发行股票并在创业板上市的法律意见书》（以下简称“《法律意见书》”）及《广东精诚粤衡律师事务所关于珠海市鸿瑞信息技术股份有限公司首次公开发行股票并在创业板上市的律师工作报告》（以下简称“《律师工作报告》”），并于 2021 年 2 月 26 日出具了《广东精诚粤衡律师事务所关于珠海市鸿瑞信息技术股份有限公司首次公开发行股票并在创业板上市的补充法律意见书（一）》（以下简称“《补充法律意见书（一）》”），于 2021 年 5 月 10 日出具了《广东精诚粤衡律师事务所关于珠海市鸿瑞信息技术股份有限公司首次公开发行股票并在创业板上市的补充法律意见书（二）》（以下简称“《补充法律意见书（二）》”）。

鉴于深圳证券交易所上市审核中心于 2021 年 5 月 25 日出具了《关于珠海市鸿瑞信息技术股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函》（审核函〔2021〕010588 号，以下简称“问询函”），本所律师现就问询函相关问题所涉及的相关法律事项更新情况出具本补充法律意见书，对《律师工作报告》《法律意见书》《补充法律意见书（一）》《补充法律意见书（二）》的相关内容进行修改、补充或作进一步说明。

对本补充法律意见书，本所声明适用《律师工作报告》《法律意见书》《补充

法律意见书（一）》《补充法律意见书（二）》的相关声明。除本补充法律意见书中另有说明外，本补充法律意见书所用简称与《律师工作报告》《法律意见书》《补充法律意见书（一）》《补充法律意见书（二）》的释义一致。本所同意将本补充法律意见书作为发行人本次发行与上市所必备的法定文件，随同其他材料一同报送监管机构审核及进行相关的信息披露，并依法对本补充法律意见书所出具的法律意见承担相应的责任；本所律师同意发行人在其关于本次发行与上市的报送材料中自行引用或按审核要求引用本补充法律意见书的全部或部分内容，但不得因引用而导致法律上的歧义或曲解；本补充法律意见书仅供发行人作本次发行与上市之目的使用，未经本所书面许可，不得用作任何其他目的或用途。

基于上述声明，本所律师按照律师行业公认的业务标准、道德规范和勤勉尽责精神，就本次发行与上市相关事项出具补充法律意见如下：

第一部分：问询函回复

问题 1. 关于产品与业务

招股说明书披露，发行人业务覆盖“网络安全隔离+加密认证+网络安全审计+网络安全服务”四大业务板块，在电力行业信息安全产品方面已取得显著的成果，并在石油石化、轨道交通、水务等领域已开展长远布局。在招股说明书“第六节 业务与技术”“(二) 发行人主要产品与服务”部分，发行人介绍各类产品的主要功能及用途，未明确披露相关产品在电力行业或其他领域的应用情况。发行人客户主要为电力行业相关用户。

请发行人：

(1) 结合发行人产品具体用途、下游客户行业分布、产品在终端使用者的应用情况等，补充披露报告期各期各类型产品的应用领域（电力、石油石化、轨道交通、水务等）、各应用领域的销售金额及占比；

(2) 说明“工业控制领域”的具体含义及包含的细分行业，并结合前述主要产品的应用情况，在招股说明书中对各类产品的主要应用领域及具体用途进行修订，以通俗易懂的方式披露发行人核心产品的应用场景以及不同产品之间解决的安全问题以及差异，如产品广泛应用于电力行业而在其他领域缺乏相应技术、客户或商业合作的，请在招股说明书中就相关情况进行明确说明；

(3) 结合行业主要法律法规及政策、销售合同的规定，补充披露在终端客户发生网络安全事件时，发行人应承担的具体责任及对生产经营的影响，是否存在因违反法律法规或合同约定而被行政处罚或承担赔偿责任的情形，存在相关风险的请进行重大事项提示。

请保荐人、发行人律师发表明确意见。

回复：

一、结合发行人产品具体用途、下游客户行业分布、产品在终端使用者的

应用情况等，补充披露报告期各期各类型产品的应用领域（电力、石油石化、轨道交通、水务等）、各应用领域的销售金额及占比；

发行人自成立以来专注于电力工业控制信息安全领域，并积极向石油石化、轨道交通、水务等国家重点行业拓展，具体拓展路径、电力工业控制系统与其它工业控制系统关系、发行人产品具体用途等详见本题第二点之回复分析。

按照最终的应用领域统计，报告期内，发行人销售收入分类情况如下：

单位：万元

行业	2020 年度		2019 年度		2018 年度	
	金额	占比	金额	占比	金额	占比
电力	14,328.33	98.19%	17,310.40	99.03%	13,704.07	99.25%
水务及环保	127.43	0.87%	46.40	0.27%	4.47	0.03%
政府及事业单位	39.12	0.27%	3.40	0.02%	37.33	0.27%
金属加工	36.06	0.25%	26.59	0.15%	16.54	0.12%
其他能源	29.95	0.21%	18.37	0.11%	20.57	0.15%
制造业	8.36	0.06%	34.04	0.19%	11.03	0.08%
石油及化工	7.88	0.05%	10.00	0.06%	7.05	0.05%
轨道交通	-	0.00%	31.41	0.18%	-	0.00%
其他	14.87	0.10%	-	0.00%	6.38	0.05%
合计	14,592.00	100.00%	17,480.61	100.00%	13,807.43	100.00%

由上表可知，报告期内，发行人销售收入主要集中在电力行业工业控制领域，但已经逐步实现向其他行业工业控制领域的销售。

报告期内，发行人在各行业销售的产品类型如下：

行业	销售产品类型		
	2020 年度	2019 年度	2018 年度
电力	网络安全隔离产品、加密认证类产品、网络安全审计类产品、网络安全服务	网络安全隔离产品、加密认证类产品、网络安全审计类产品、网络安全服务	网络安全隔离产品、加密认证类产品、网络安全审计类产品、网络安全服务
水务及环保	网络安全隔离产品、加密认证类产品、网络安全审计类产品	网络安全隔离产品、网络安全审计类产品	网络安全隔离产品
政府及事业单位	网络安全隔离产品、网络安全审计类产品	网络安全服务	网络安全隔离产品、网络安全审计类产品
金属加工	网络安全隔离产品、加密	网络安全隔离产品、网络	网络安全隔离产品、加密

	认证类产品、网络安全审计类产品、网络安全服务	安全审计类产品	认证类产品、网络安全审计类产品
其他能源	网络安全隔离产品、加密认证类产品、网络安全审计类产品、网络安全服务	网络安全隔离产品、加密认证类产品、	网络安全隔离产品
制造业	网络安全隔离产品、加密认证类产品、网络安全审计类产品	加密认证类产品、网络安全审计类产品	网络安全隔离产品、加密认证类产品、网络安全审计类产品
石油及化工	网络安全隔离产品、网络安全审计类产品	网络安全隔离产品	网络安全隔离产品
轨道交通	--	加密认证类产品	--
其他	网络安全隔离产品、网络安全审计类产品	-	加密认证类产品

由上表可知，发行人的部分主要产品在部分通用工业控制信息安全领域已有应用，在前述领域中，发行人的产品同样是用于解决上述工业行业生产、运行过程中各种信息传递、交互的网络安全相关问题。

二、说明“工业控制领域”的具体含义及包含的细分行业，并结合前述主要产品的应用情况，在招股说明书中对各类产品的主要应用领域及具体用途进行修订，以通俗易懂的方式披露发行人核心产品的应用场景以及不同产品之间解决的安全问题以及差异，如产品广泛应用于电力行业而在其他领域缺乏相应技术、客户或商业合作的，请在招股说明书中就相关情况进行明确说明；

（一）“工业控制领域”的具体含义及包含的细分行业

1、工业控制领域的具体含义及包含的细分行业

（1）工业控制系统

工业控制系统（Industrial Control System）简称ICS，是由各种自动控制组件以及对实时数据进行采集、监测的过程控制组件共同构成确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统，是用于工业生产过程控制上的多种控制系统以及相关仪器设备总称。工业控制系统可以小到由几个模块型的控制器组成，也可以是大型互联的分布式控制系统。典型工业控制系统有数据采集与监控系统（SCADA）、分散式控制系统（DCS）、可编程逻辑控制器（PLC）、远程终端单元（RTU）等。

（2）工业控制领域

“工业控制领域”是指使用了工业控制系统的范围或区域，涵盖社会经济活

动涉及生产与运营的各个行业。工业控制系统广泛用于各个行业，特别是在关键的基础设施方面更加依赖工业控制系统，比如电力、石化、航天、水利设施、国防工业、通信、应急响应、政府设施、重点制造、能源、公共卫生、水处理、核反应设施、交通系统等支撑现代社会运行的重要行业。

（3）电力工业控制系统与工业控制领域的关系

电力工业控制系统主要指用于监视和控制电力生产及供应过程，基于计算机及网络技术的业务系统及智能设备，以及作为基础支撑的通信及数据网络等设施。其中，“电力一次设备（也称主设备）”是指电力系统中包含的直接生产、输送和分配电能的设备，“电力二次系统”指对电力一次设备进行控制、调节、保护和监测的设备组成的系统。在电力行业中，“电力二次系统”、“电力监控系统”、“电力工业控制系统”三者含义通常是一致的。

依据国家发改委第14号《电力监控系统安全防护规定》第二十三条，对电力监控系统含义或范围定义如下：

1、电力监控系统具体包括电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和安全自动装置、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统、电力调度数据网络等。

2、电力调度数据网络，是指各级电力调度专用广域数据网络、电力生产专用拨号网络等。

国家相关政策明确了电力监控系统属于工业控制系统，依据如下：

中央网信办下发的《关键信息基础设施确定指南(试行)》指出：“关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统”，其中能源行业的工业控制系统明确包括了电力行业。具体如下：

行业		关键业务
能源	电力	电力生产（含火电、水电、核电等）
		电力传输
		电力配送

	石油石化	油气开采
		炼化加工
		油气输送
		油气储存
	煤炭	煤炭开采
		煤化工

工信部协[2011]451号《关于加强工业控制系统信息安全管理的通知》中第二条指出：“加强工业控制系统信息安全的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。”该通知也明确了工业控制系统信息安全管理包括电力行业在内的重点工业控制领域。

因此，综合上述分析，电力工业控制系统是工业控制领域的重要组成部分。除电力行业外，工业控制领域还包括石化、航天、水利设施、国防工业、通信、应急响应、政府设施、重点制造、能源、公共卫生、水处理、核反应设施、交通系统等行业。

（二）各类产品的主要应用领域及具体用途，以通俗易懂的方式披露发行人核心产品的应用场景以及不同产品之间解决的安全问题以及差异

1、发行人的主要产品及服务，应用环节、主要应用领域及具体用途及如下表所示：

一级分类	二级分类	主要产品与服务	产品简介	应用环节	具体作用
网络安全隔离类产品	网络隔离类	单向网络隔离装置	属性：电力监控系统网络安全专用产品。 依据《电力监控系统安全防护规定》第九条要求，产品部署在电力生产控制大区与管理信息大区之间或者安全接入区与电力生产控制大区其他部分的连接处。	电力调度中心、变电站、发电厂等控制系统的网络边界	主要应用于电力工业控制领域的电力生产控制大区与管理信息大区之间或者安全接入区与电力生产控制大区的隔离防护，阻断信息网（外网，即办公网）和控制网（内网，即生产网）之间的入侵途径，实现控制网向信息网实时、连续、安全的单向数据传输。
		OPC 网络隔离装置	属性：通用工业控制领域或发电厂站端产品。 针对控制网与信息网采用 OPC 协议通信的工业控制系统数据传输需求，产品采用网络隔离、单向通信、双机非网、应用代理等技术完成应用数据的单向传	发电厂、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络边界	主要应用于工业控制领域的控制网和信息网之间。产品主要实现控制网和信息网基于 OPC 协议应用的单向网络隔离数据传输，不存在反向数据传输通道。

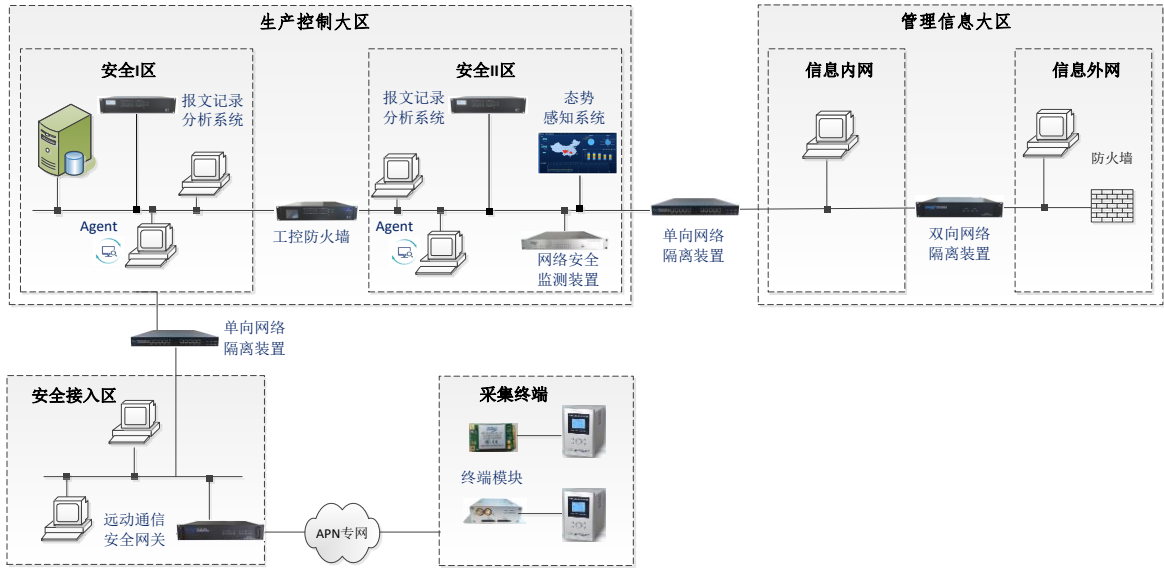
一级分类	二级分类	主要产品与服务	产品简介	应用环节	具体作用
			输,其作用是阻断信息网对控制网中 OPC 服务器的直接访问。		
		双向网络隔离装置	属性: 电力管理信息大区或通用工业控制领域产品。 满足不同系统之间的数据通信需求,产品采用网络隔离、双机非网、身份认证加密、内容过滤等技术阻断病毒木马在信息系统内部的传播途径。	电力管理信息系统、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络边界	主要应用于电力管理信息大区或通用工业控制领域的控制网和信息网之间。产品主要实现控制网和信息网网络隔离,同时满足工业控制双向通信的协议应用要求,并对工控协议特征报文进行过滤审计,反向数据加密认证。产品通信安全约束强度低于单向通信隔离。
	逻辑隔离类	工业控制防火墙	属性: 电力生产控制大区内部或通用工业控制领域产品。 满足内部不同系统之间或通用工业控制领域的网络边界的逻辑隔离,产品支持对 OPC、Modbus、DNP3.0、IEC104 等协议进行深层分析过滤,通过检测可疑行为阻止网络攻击蔓延。	电力、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络边界	主要应用于电力生产控制大区内部或工业控制系统现场控制层与过程监控层网络之间;产品采用逻辑隔离方式,支持对工控协议深层分析过滤,检测可疑的或违反授权的行为,检测已知和未知攻击。
	加密认证类产品	通信加密类	属性: 电力安全接入区或通用工业控制领域产品。 电力多用于配网自动化系统中,通用工业控制系统则用于控制系统与互联网的边界处,产品遵循国密算法和 IPsecVPN 规范,通过对数据加密、认证、完整性检查来保证数据传输的可靠性、私有性和保密性。	电力调度中心、发电厂、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络边界	主要应用于电力安全接入区或工业控制系统数据通信网络环境,部署于控制系统数据中心网络出口和控制终端侧之间;产品实现工业通信数据保密性、数据完整性和不可否认性,降低使用公网通信带来的网络安全风险。
		身份认证类	属性: 通用工业控制领域产品。 主要用于工业控制系统的远程运维,产品遵循国密算法和 IPsecVPN 规范,对接入用户进行身份认证、对操作行为进行记录及安全审计。	石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络边界	主要应用于工业控制系统远程运维的网络环境;对工业控制系统远程维护通道进行加密,识别接入网络用户身份,并对通信及操作行为进行安全审计
网络安全审计类产品	网络安全监测装置		属性: 电力生产控制大区内部或通用工业控制领域产品。 电力系统中必须满足其专用技术规范,通用工业控制系统则与电力规范不同需按行业规范开发,产品提供监测网络安全状况、记录网络数据事件、在线告警以及审计分析追溯等功能。	电力调度中心、发电厂、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络数据监测	主要应用于电力生产控制大区内部或工业控制系统网络安全状况监测,实时完整记录网络数据,及时发现网络运行的潜在风险,减少因网络安全导致的系统故障,提升工业控制系统设备运行的可靠率和抵御网络安全风险的能力。
	Agent 探针		属性: 网络安全监测装置的可选配套前级软件。 安装在现场其他设备上,是监测装置的前级采集软件,产品安装在通用操作系统的服务器、工作	电力调度中心、变电站、石油化工厂、轨道交通调度中心、水控中心、生产线信	主要应用于采集工业控制系统主机运行信息,并上送及接收网络安全监测装置数据及信息。

一级分类	二级分类	主要产品与服务	产品简介	应用环节	具体作用
			站、嵌入式主机中,监测服务器、工作站、嵌入式主机的安全事件,并将数据发送到网络安全监测装置。	信息中心等控制系统的网络数据监测	
	网络安全态势感知系统		属性:电力生产控制大区内部或通用工业控制领域产品,属于网络安全监测装置的后级系统。产品支持接入一台或多台网络安全监测装置的数据,提供数据采集、资产管理、安全监视、安全告警、安全审计、安全分析、安全核查等功能,通过页面可视化方式及时反馈网络中的风险和威胁。	电力调度中心、变电站、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络数据监测	主要应用于监测电力生产控制大区内部或工业控制系统网络安全状况,为工业控制系统提供网络安全预警及网络安全态势分析,提升工业控制系统网络管理员的网络安全决策及网络安全事件处理的有效性。
	网络报文记录分析系统		属性:智能变电站内生产控制大区产品。装置基于 IEC 61850 协议分析技术,通过对智能变电站原始网络报文进行记录与分析,实现通信数据在线监测,对网络通讯故障及异常进行在线告警及数据离线分析。	变电站控制系统的站控层及过程层网络业务数据监测	主要应用于监测变电站工业控制系统的业务运行监测,实时展示电力测量数据,波形图,数据跳变情况,通过关联分析工业控制系统前端运行线路测量数据及动作开关跳变的过程,为继电保护等业务提供网络通信追溯的原始数据,并分析业务逻辑的合法性。
网络安全服务			为客户提供维保服务、安全加固、网络安全培训和网络安全管理咨询服务等全方位的安全服务。	电力调度中心、变电站、石油化工厂、轨道交通调度中心、水控中心、生产线信息中心等控制系统的网络数据监测	对工业企业客户提供专业的信息安全服务,为客户的工业控制系统的网络安全进行评估、网络安全维保、网络安全加固及网络安全培训及管理咨询。

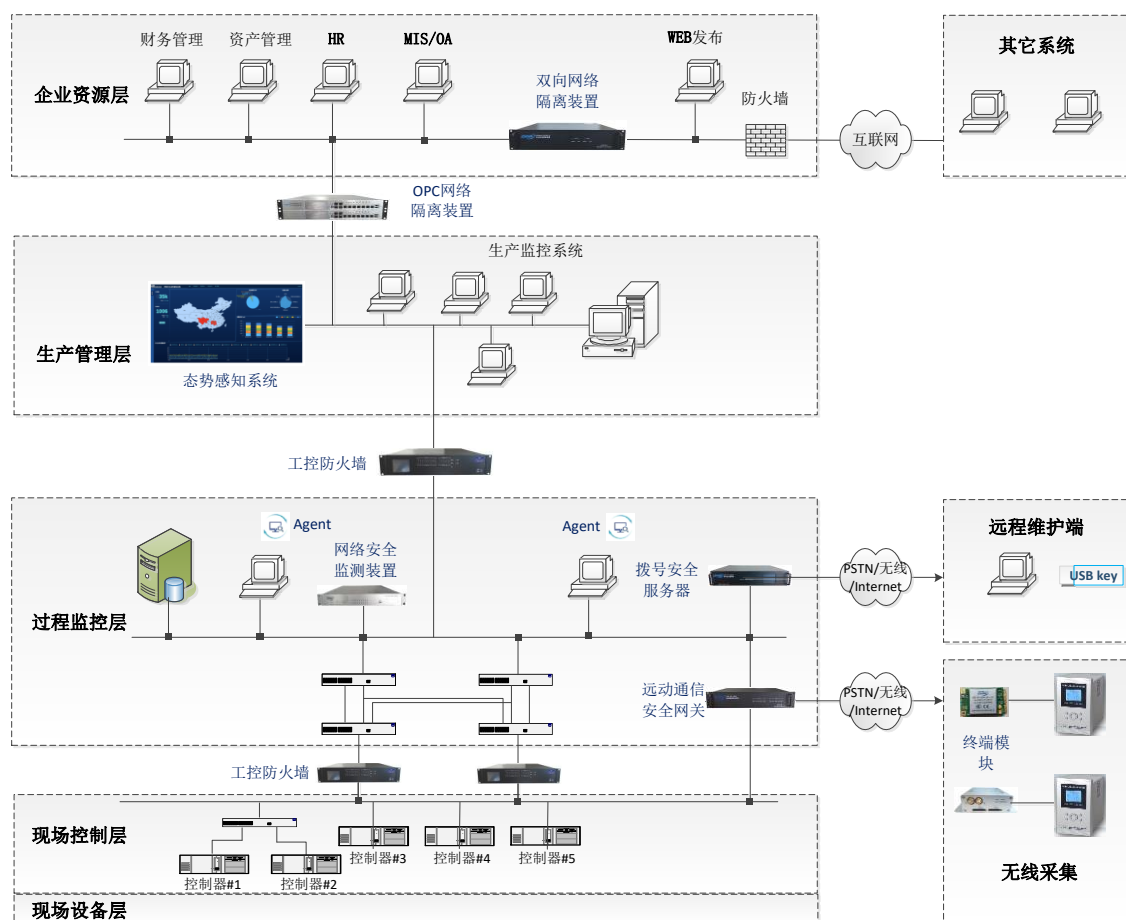
发行人已在招股说明书中将发行人行业属性由“工业控制信息安全”修改为“电力及通用工业控制信息安全”，并在招股说明书“第六节/一/（二）发行人主要产品与服务”中补充披露各产品具体应用综合示意图：

2、发行人各产品具体应用综合示意图如下：

（1）发行人应用于电力工控领域产品的部署示意图



（2）发行人应用于通用工控领域产品的部署示意图



（三）虽然发行人产品目前主要应用于电力行业工业控制领域，但具备向其他行业工业控制领域拓展的技术基础

工业控制领域涵盖支撑现代社会运行的诸多重要行业，而电力行业是我国较早应用工业控制网络信息安全产品和设施的行业之一。发行人电力行业工业控制网络安全技术向其他行业工业控制领域拓展的可行性具体分析如下：

1、电力行业工业控制领域与其他行业工业控制领域政策发布轴线

电力行业工业控制系统网络安全建设起步比较早。2002年，国家经济贸易委员会发布《电网和电厂计算机监控系统及调度数据网络安全防护规定》，电力系统就启动了工业控制系统网络安全的研究建设工作，2006年，电力系统出台了《电力二次系统安全防护总体方案》，规范了省级以上调度中心、地县级调度中心、变电站、发电厂和配电二次系统安全防护工作。而对于其他行业工业控制系统，

2011年，工信部发布451号文《关于加强工业控制系统信息安全管理的通知》，2016年，工信部发布《工业控制系统信息安全防护指南》，可见电力行业工业控制系统网络安全建设的起步时间较其他行业早数年。

2015年，电力系统发布《电力监控系统安全防护总体方案》，上述方案是对2006年版本的进一步完善，通过继续强化纵横边界、内外边界及其在线监视，提高自身安全免疫能力并加强内网安全监控，同时对具体产品进一步细化规范，至此，电力行业工业控制系统网络安全技术产品日趋成熟，电力行业工业控制安全防护进入快速发展阶段。

而对于包含其它工业控制系统在内的总体工业控制网络安全政策，是在2011年初步提出。2016年后，国家相关部门密集出台了一系列政策规范，力求引导工业控制网络信息安全发展到新的高度。

电力行业工业控制系统与总体工业控制网络安全政策规范发布时间轴线如下：

电力行业工业控制领域政策规范	发布时间	其它行业工业控制领域政策规范
国家经济贸易委员会《电网和电厂计算机监控系统及调度数据网络安全防护规定》	2002 年	-
国家电力监管委员会《电力二次系统安全防护规定》	2004 年	-
《电力二次系统安全防护总体方案》等共计 6 个安全防护配套方案，规范了省级以上调度中心、地县级调度中心、变电站、发电厂和配电二次系统安全防护工作	2006 年	-
《关于开展电力行业信息系统安全等级保护定级工作的通知》电监信息[2007]34 号 《电力行业网络与信息安全监督管理暂行规定》电监信息[2007]50 号	2007 年	-
国家电网〔2011〕168 号《关于加强配电网自动化系统安全防护工作的通知》《中长期电力交易系统安全防护补充技术规定》	2011 年	工信部 451 号文《关于加强工业控制系统信息安全管理的通知》
《核电站二次系统安全防护技术规定（试行）》，《风电、光伏和燃气电厂二次系统安全防护技术规定（试行）》《电力二次系统安全防护评估规范（试行）》	2012 年	国家发改委信息安全专项支持（包含工业控制领域）
电监会《电力工控信息安全专项监管工作方案》（办发〔2013〕50 号）	2013 年	-
《电力监控系统安全防护规定》（国家发改委会令第 14 号）	2014 年	-

国家能源局《电力监控系统安全防护总体方案》	2015 年	-
-	2016 年	中央网信办《国家网络空间安全战略》国务院《关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28 号）工信部《工业控制系统信息安全防护指南》《信息安全技术工业控制系统安全控制应用指南》（GB/T 32919-2016）
-	2017 年	全国人大常委会《中华人民共和国网络安全法》工信部《工业控制系统信息安全防护能力评估工作管理办法》信软〔2017〕188 号
《国家能源局关于加强电力行业网络安全工作的指导意见》国能发安全〔2018〕72 号	2018 年	-
-	2019 年	全国人大常委会《中华人民共和国密码法》市场监督管理总局、国准委《信息安全技术网络安全等级保护基本要求》2.0 版本
-	2020 年	《信息安全技术工业控制系统信息安全防护建设实施规范》（计划号 20173583-T-469）《信息安全技术工业控制系统信息安全防护能力评价方法》
-	2021 年	信息安全技术《工业控制系统信息安全防护能力成熟度模型（报批稿）》

2、电力工业控制网络安全技术向其它工业控制领域拓展的可行性

从前述分析工业控制系统范围、电力工业控制网络安全建设时间等因素，再结合电力监控系统安全防护体系取得的防护效果来看，我国电力监控系统网络安全防护在整个工业控制领域处于领先地位，具备向整个工业控制领域推广的条件和价值。

2016年，《工业控制系统信息安全》专刊第三辑发布了工业控制系统信息安全产业联盟专家委员会委员文章《论电力监控系统安全防护方案在工控系统安全防护建设中的借鉴意义》，文章指出“国家对电力监控系统安全非常重视。在2002年，原经贸委发布了《电网与电厂计算机监控系统及调度数据网络安全防护规定》；原电监会在2006年发布《电力二次系统安全防护方案》。到2015年国家能源局发布36号文，即《电力监控系统安全防护总体方案等安全防护方案和评估规范》，电力监控系统安全成体系的发展，已经走过十个年头，积累了大量的工控系统安全实践经验。国家能源局发布的36号文，在总结以前经验的基础上，对电力监控系统安全防护进行了提升和完善。本文在分析电力监控系统安全实践的基础上，提炼其最佳实践理念、方法、经验、技术，力求为其它行业工控系统安全

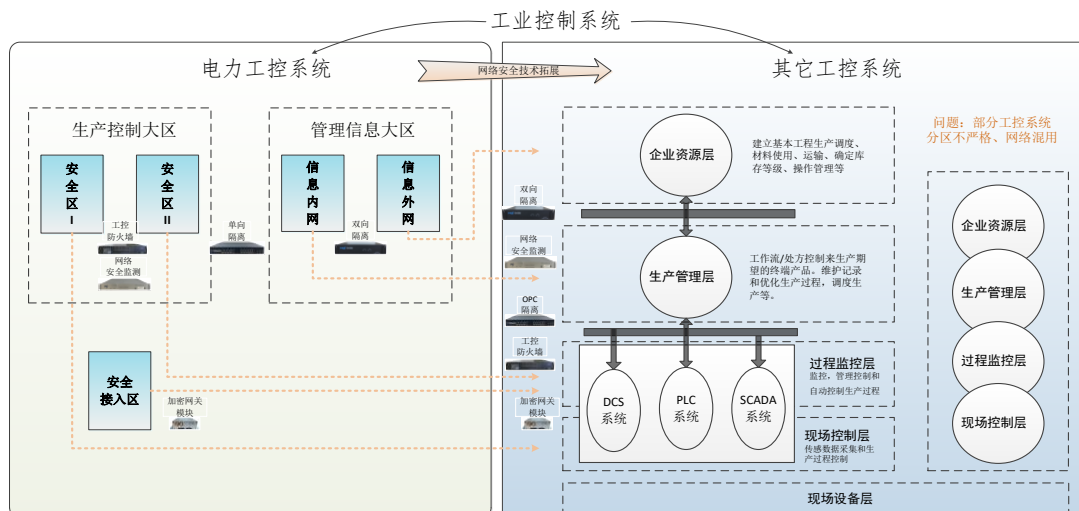
提供有益的指导，以提升其工控系统安全防护水平。”由此可见，工业控制领域对电力工业控制取得的成就高度认同。

2013年，发行人核心成员刘智勇、陈良汉、陈敏超参与发表了期刊文章《电力二次安全防护技术在工业控制系统中的应用》（[J]. 电网技术，2013，20（11）：3227-3232），文中阐述了：“我国电力二次系统安全防护技术已广泛应用并取得了良好的安全防护效果，通用工业控制系统与电力二次系统既有相似性，又存在行业不同的需求差异。该文根据电力二次安全防护技术成果，通过加强工控网络边界的防护强度、对工控通信协议进行深度分析、挖掘工控协议攻击特征模型、建立统一安全管理平台等技术手段，构筑具备纵深防御能力的通用工控信息安全防护系统。”因此，发行人对电力工业控制网络安全防护技术向整个工业控制系统拓展应用早有部署。

3、电力行业工业控制网络安全技术向其它行业工业控制领域的拓展应用情况

电力工业控制系统与其它工业控制系统同属工业控制系统，因此从技术架构上有一定的相似性。同时，由于通用工业控制网络安全政策规范发布时间相对滞后，在政策制订上吸取电力工业控制系统网络安全防护的经验，因此，电力工业控制系统网络安全防护技术向其它工业控制领域拓展有一定先发优势。但同时因为不同领域、不同类型的工业控制系统结构存在差异，而且部分工业控制系统由于建设成本导致的存在分区不严格、网络混用的现象，因而从技术上也需要调整以适应其它工业控制系统。

发行人已有的电力工业控制系统网络安全技术向其它工业控制系统拓展应用的示意图如下：



综合上述分析，虽然发行人产品主要应用于电力行业，但从技术角度，向其他工业控制领域拓展并不存在障碍。报告期内，发行人已有部分产品应用于其他行业工业控制领域，并已与其他行业工业控制领域客户开展合作。因此，虽然发行人产品目前主要应用于电力行业工业控制领域，但向其他行业工业控制领域拓展具有可行性。

(四) 发行人已就下游客户行业集中度较高及未来未能有效向通用工业控制信息安全领域拓展的风险在招股说明书中进行了风险提示

发行人已在招股说明书“重大事项提示”/三/(二)下游客户行业集中度较高及未来未能有效向通用工业控制信息安全领域拓展的风险”补充披露如下：

目前，公司下游客户主要集中于电网、各大能源集团及发电厂，下游客户行业集中度较高。现有电力领域客户的投资需求受政策变动影响较大，若未来由于政策原因导致主要客户需求发生重大变化，或公司产品和服务质量不能持续满足主要客户需求，使得公司与主要客户的合作关系发生不利变化，将对公司的经营业绩带来重大不利影响。

此外，经过十余年的发展，公司已推出了一系列工业控制信息安全领域的产品与服务，在电力行业信息安全产品方面已取得显著的成果，并在石油石化、轨道交通、水务等通用工业控制信息安全领域已开展长远布局。报告期内公司来自电力工业控制信息安全行业的收入占比分别为99.25%、99.03%、98.19%；而来自水务及环保、石油及化工等通用工业控制信息安全行业收入占比仅分别为0.75%、

0.97%、1.81%。若公司未来向通用工业控制信息安全行业拓展策略、营销服务等不能很好适应并引导客户需求，将面临新行业市场开拓风险。

三、结合行业主要法律法规及政策、销售合同的规定，补充披露在终端客户发生网络安全事件时，发行人应承担的具体责任及对生产经营的影响，是否存在因违反法律法规或合同约定而被行政处罚或承担赔偿责任的情形，存在相关风险的请进行重大事项提示。

（一）结合行业主要法律法规及政策、销售合同的规定，补充披露在终端客户发生网络安全事件时，发行人应承担的具体责任及对生产经营的影响，是否存在因违反法律法规或合同约定而被行政处罚或承担赔偿责任的情形

1、《中华人民共和国网络安全法》（以下简称“《网络安全法》”）、《中华人民共和国密码法》（以下简称“《密码法》”）、《中华人民共和国产品质量法》（以下简称“《产品质量法》”）等行业主要法律法规及政策关于终端客户发生网络安全事件时相关责任的规定

鉴于发行人在第二轮反馈回复的同时将招股说明书中发行人主营业务由“从事工业控制信息安全技术软件、硬件的开发与销售，并基于上述产品为客户提供工业控制信息安全技术综合应用的解决方案、技术支持和后续服务等”修改为“从事电力及通用工业控制信息安全技术软件、硬件的开发与销售，并基于上述产品为客户提供电力及通用工业控制信息安全技术综合应用的解决方案、技术支持和后续服务等”，据此，本补充法律意见书对《律师工作报告》《法律意见书》《补充法律意见书（一）》《补充法律意见书（二）》中关于发行人主营业务的相应表述进行同步修改。

根据发行人现行有效的《营业执照》及发行人出具的说明，发行人主营业务为从事电力及通用工业控制信息安全技术软件、硬件的开发与销售，并基于上述产品为客户提供电力及通用工业控制信息安全技术综合应用的解决方案、技术支持和后续服务等。发行人业务领域主要集中在电力行业工业控制领域，并逐步向能源、环保、制造业、石油石化、轨道交通等其他行业工业控制领域拓展。

发行人所处行业主要法律法规及政策的对网络安全责任的相关规定如下：

（1）行业主要法律法规及政策

发行人属于《网络安全法》中所述的“网络产品、服务的提供者”，属于《密码法》中所述的“商用密码从业单位”，根据《网络安全法》《密码法》及其下位法、行业政策的相关规定及法律责任如下：

主要依据文件	相关规定	法律责任
《网络安全法》	第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。	第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款： （一）设置恶意程序的；（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；（三）擅自终止为其产品、服务提供安全维护的。
《密码法》	第二十一条 国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。 各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位（以下统称商用密码从业单位）。国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。 商用密码的科研、生产、销售、服务和进出口，不得损害国家安全、社会公共利益或者他人合法权益。	第四十一条 违反本法规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。
	第二十六条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。 商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。	第三十六条 违反本法第二十六条规定，销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证不合格的商用密码服务的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足

		十万元的，可以并处三万元以上十万元以下罚款。
《计算机信息系统安全专用产品监测和销售许可证管理办法》	第三条 中华人民共和国境内的安全专用产品进入市场销售，实行销售许可证制度。	第二十条 生产企业违反本办法的规定，有下列情形之一的，视为未经许可出售安全专用产品，由公安机关根据《中华人民共和国计算机信息系统安全保护条例》的规定予以处罚： （一）没有申领销售许可证而将生产的安全专用产品进入市场销售的； （二）安全专用产品的功能发生改变，而没有重新申领销售许可证进行销售的； （三）销售许可证有效期满，未办理延期申领手续而继续销售的； （四）提供虚假的安全专用产品检测报告或者虚假的计算机病毒防治研究的备案证明，骗取销售许可证的； （五）销售的安全专用产品与送检样品安全功能不一致的； （六）未在安全专用产品上标明“销售许可”标记而销售的； （七）伪造、变造销售许可证和“销售许可”标记的。
	---	第二十二条 安全专用产品中含有有害数据危害计算机信息系统安全的，依据《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚；构成犯罪的，依法追究刑事责任。
《中华人民共和国计算机信息系统安全保护条例》	第七条 任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。	第二十条 违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿： （一）违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的； （二）违反计算机信息系统国际联网备案制度的； （三）不按照规定时间报告计算机信息系统中发生的案件的； （四）接到公安机关要求改进安全状况的通知后，在限期内拒不改进的； （五）有危害计算机信息系统安全的其他行为的。
		第二十三条 故意输入计算机病毒以及其他有害数据危害计算机信

		息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 1.5 万元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。
《电力监控系统安全防护规定》	第十八条 电力监控系统相关设备及系统的开发单位、供应商应当以合同条款或者保密协议的方式保证其所提供的设备及系统符合本规定的要求，并在设备及系统的全生命周期内对其负责。 电力监控系统专用安全产品的开发单位、使用单位及供应商，应当按国家有关要求做好保密工作，禁止关键技术和设备的扩散。	第二十二条 对于因违反本规定，造成电力监控系统故障的，由其上级单位按相关规程规定进行处理；发生电力设备事故或者造成电力安全事故（事件）的，按国家有关事故（事件）调查规定进行处理。
《网络安全等级保护条例》（征求意见稿）	第二十七条【网络服务机构要求】 网络服务提供者应为第三级以上网络提供网络建设、运行维护、安全监测、数据分析等网络服务，应当符合国家有关法律、法规和技术标准的要求。 网络安全等级测评机构等网络服务提供者应当保守服务过程中知悉的国家秘密、个人信息和重要数据。不得非法使用或擅自发布、披露在提供服务中收集掌握的数据信息和系统漏洞、恶意代码、网络入侵攻击等网络安全信息。	第六十六条【网络安全服务责任】 违反本条例第二十六条第三款，第二十七条第二款规定的，由公安机关责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿，直至通知发证机关吊销相关业务许可证或者吊销营业执照。 违反本条例第二十七条第二款规定，泄露、非法出售或者向他人提供个人信息的，依照《中华人民共和国网络安全法》第六十四条第二款的规定处罚。

（2）其他法律法规

此外，发行人亦属于《产品质量法》中描述的“生产者、销售者”，相关规定如下：

相关义务	法律权责
第四条 生产者、销售者依照本法规定承担产品质量责任。	—
第二十六条 生产者应当对其生产的产品质量负责。 产品质量应当符合下列要求： （一）不存在危及人身、财产安全的不合理的危险，有保障人体健康和人身、财产安全的国家标准、行业标准的，应当符合该标准； （二）具备产品应当具备的使用性能，但是，对产品存	第四十九条 生产、销售不符合保障人体健康和人身、财产安全的国家标准、行业标准的产品的，责令停止生产、销售，没收违法生产、销售的产品，并处违法生产、销售产品（包括已售出和

在使用性能的瑕疵作出说明的除外； (三)符合在产品或者其包装上注明采用的产品标准，符合以产品说明、实物样品等方式表明的质量状况。	未售出的产品，下同)货值金额等值以上三倍以下的罚款；有违法所得的，并处没收违法所得；情节严重的，吊销营业执照；构成犯罪的，依法追究刑事责任。
第二十七条 产品或者其包装上的标识必须真实，并符合下列要求： (一)有产品质量检验合格证明； (二)有中文标明的产品名称、生产厂厂名和厂址； (三)根据产品的特点和使用要求，需要标明产品规格、等级、所含主要成份的名称和含量的，用中文相应予以标明；需要事先让消费者知晓的，应当在外包装上标明，或者预先向消费者提供有关资料； (四)限期使用的产品，应当在显著位置清晰地标明生产日期和安全使用期或者失效日期； (五)使用不当，容易造成产品本身损坏或者可能危及人身、财产安全的产品，应当有警示标志或者中文警示说明。 裸装的食品和其他根据产品的特点难以附加标识的裸装产品，可以不附加产品标识。	第五十四条 产品标识不符合本法第二十七条规定的，责令改正；有包装的产品标识不符合本法第二十七条第(四)项、第(五)项规定，情节严重的，责令停止生产、销售，并处违法生产、销售产品货值金额百分之三十以下的罚款；有违法所得的，并处没收违法所得。
第三十四条 销售者应当采取措施，保持销售产品的质量。	—
第三十六条 销售者销售的产品的标识应当符合本法第二十七条的规定。	第五十四条 产品标识不符合本法第二十七条规定的，责令改正；有包装的产品标识不符合本法第二十七条第(四)项、第(五)项规定，情节严重的，责令停止生产、销售，并处违法生产、销售产品货值金额百分之三十以下的罚款；有违法所得的，并处没收违法所得。
第四十条 售出的产品有下列情形之一的，销售者应当负责修理、更换、退货；给购买产品的消费者造成损失的，销售者应当赔偿损失： (一)不具备产品应当具备的使用性能而事先未作说明的； (二)不符合在产品或者其包装上注明采用的产品标准的； (三)不符合以产品说明、实物样品等方式表明的质量状况的。 销售者依照前款规定负责修理、更换、退货、赔偿损失后，属于生产者的责任或者属于向销售者提供产品的其他销售者(以下简称供货者)的责任的，销售者有权向生产者、供货者追偿。 销售者未按照第一款规定给予修理、更换、退货或者赔偿损失的，由市场监督管理部门责令改正。 生产者之间，销售者之间，生产者与销售者之间订立的买卖合同、承揽合同有不同约定的，合同当事人按照合同约定执行。	根据第四十条规定进行修理、更换、退货，或承担损失赔偿责任
第四十一条 因产品存在缺陷造成人身、缺陷产品以	根据第四十一条规定承担损失

外的其他财产(以下简称他人财产)损害的,生产者应当承担赔偿责任。 生产者能够证明有下列情形之一的,不承担赔偿责任: (一)未将产品投入流通的; (二)产品投入流通时,引起损害的缺陷尚不存在的; (三)将产品投入流通时的科学技术水平尚不能发现缺陷的存在的。	赔偿责任
---	------

根据前述内容,《网络安全法》《密码法》《产品质量法》等相关法律法规、政策对发生网络安全事件时的责任未进行明确规定,相关法律法规主要系对销售许可资质、行为约束、产品质量等方面进行规范,如违反上述规定,发行人将可能依法依约承担刑事责任、面临行政处罚风险外,还将承担相关违约、损失赔偿责任。

2、发行人与客户签订的销售合同的约定

网络安全责任是层层压实的架构,即:设备生产厂家承担严格按照国家法律法规研发、设计、生产、运维并通过相关机构检测,以及为终端客户提供足够的培训,确保设备运行稳定、可靠等责任;运营管理者承担严格按照技术规范管理、执行的责任;终端客户的日常管理对网络安全防护尤为重要,即使终端客户已装备工业控制网络安全防护设备,也可能会因终端客户或其管理者的安全策略不当,从而导致网络安全事件发生。

基于上述原因,发行人与客户的业务合同中通常仅会对产品质量进行约定,而不会对终端客户发生网络安全事件时的责任承担进行约定。若因发行人及其产品质量问题违反合同约定的,则发行人将需承担相应的违约赔偿责任。

3、是否存在因违反法律法规或合同约定而被行政处罚或承担赔偿责任的情形

根据发行人提供的公司内部《售后服务管理制度》及相关产品说明,并经保荐机构、发行人律师访谈发行人相关负责人,发行人已建立并执行相关《售后服务管理制度》,能够确保其销售的产品符合相关法律法规的规定,以及业务合同的约定(如有),并按照发行人售后服务政策的标准提供维护服务。

根据发行人出具的说明,并经本所律师查询国家企业信用信息公示系统(网址:<http://www.gsxt.gov.cn/index.html>)、信用中国网(网址:<https://www.creditchina.gov.cn/>)、中共中央网络安全和信息化委员会办公室

官网（网址：<http://www.cac.gov.cn/index.htm>）、中华人民共和国公安部官网（网址：<https://www.mps.gov.cn/>）、中华人民共和国工业和信息化部官网（网址：<http://www.miit.gov.cn/>）、中国裁判文书网（网址：<http://wenshu.court.gov.cn/>）、中国执行信息公开网（网址：<http://zxgk.court.gov.cn/>）等网站以及对发行人主要客户的访谈，报告期内，发行人不存在因违反《网络安全法》《密码法》《产品质量法》等相关法律法规、政策而受到行政处罚的情形，亦不存在因终端客户发生网络安全事件引起合同纠纷而承担赔偿责任的情形。

综上，工业控制信息安全行业主要法律法规及政策未对发生网络安全事件责任进行明确规定，在发行人销售合同通常亦不会对终端客户发生网络安全事件时的责任承担进行约定。发生网络安全事件的原因应由相关专业机构判断分析而不是仅仅依赖终端用户判定，只有在设备生产厂家未合法合规或未按合同约定提供设备与服务时，才需按照法律法规承担刑事责任、受到行政处罚或承担赔偿责任。

（二）风险提示

基于谨慎性，发行人已在招股说明书“重大事项提示”/三/（二）/3、因产品质量问题引起网络安全事件导致需要承担法律责任的风险”进行如下风险提示：

3、因产品质量问题引起网络安全事件导致需要承担法律责任的风险

发行人业务主要集中在电力及通用工业控制信息安全领域，其中电力行业客户较多。由于电力行业工业控制信息安全直接关系到国家安全，一旦电力系统受到攻击，可能会对国民经济造成重大损失。因此，电力行业工业控制信息安全领域的参与方均需严格履行各自职责，共同维护电力系统安全运行。

鉴于电力行业工业控制信息安全是体系性防护，政策制定、资质发放、产品生产、设备安装运行、设备安装后的日常管理等各个环节对电力系统安全运行均具有重要意义。发行人仅在未合法合规或未按合同约定提供设备与服务时，才需按照相关法律法规的规定，承担相应刑事责任、受到行政处罚或承担赔偿责任。

虽然发行人在电力及通用工业控制信息安全领域深耕多年，生产经营资质

完备，技术水平较高，其产品可靠性、稳定性获得客户广泛认可，但若发行人的产品因质量问题导致终端客户发生网络安全事件，则可能导致发行人需承担相应法律责任或赔偿责任，进而对生产经营造成不利影响。

四、请保荐人、发行人律师发表明确意见。

（一）核查程序

保荐人、发行人律师履行了如下核查程序：

- 1、获取并分析发行人下游客户及最终用户的行业分类收入及占比情况；
- 2、获取并查阅工业控制领域相关政策法规，以及《关键信息基础设施确定指南（试行）》《关于加强工业控制系统信息安全管理的通知》等行业规范文件；
- 3、访谈发行人业务负责人，了解报告期内各主要产品的应用环节、主要应用领域及具体用途；
- 4、查阅《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国产品质量法》等行业主要法律法规及政策中是否存在关于终端客户发生网络安全事件时相关责任的规定；
- 5、抽取部分发行人与客户签订的销售合同，查阅销售合同中是否存在关于终端客户发生网络安全事件时相关责任的约定；
- 6、取得并查阅发行人内部《售后服务管理制度》《售后服务承诺》等，并就发行人执行的与网络安全和信息安全方面的内控管理制度访谈了相关负责人员；
- 7、检索国家企业信用信息公示系统（网址：<http://www.gsxt.gov.cn/index.html>）、信用中国网（网址：<https://www.creditchina.gov.cn/>）、中共中央网络安全和信息化委员会办公室官网（网址：<http://www.cac.gov.cn/index.htm>）、中华人民共和国公安部官网（网址：<https://www.mps.gov.cn/>）、中华人民共和国工业和信息化部官网（网址：<http://www.miit.gov.cn/>）、中国裁判文书网（网址：<http://wenshu.court.gov.cn/>）、中国执行信息公开网（网址：<http://zxgk.court.gov.cn/>）等网站，对发行人报告期内是否存在重大行政处罚的情形以及合同纠纷进行核查；

8、取得发行人行政主管部门关于发行人报告期内合规经营的证明文件。

（二）核查意见

经核查，保荐人、发行人律师认为：

1、报告期内，虽然发行人产品主要应用于电力行业工业控制领域，但在能源、环保、制造业、石油石化、轨道交通等其他行业工业控制领域也已有应用并已实现销售；

2、除电力行业外，工业控制领域还包括石化、航天、水利设施、国防工业、通信、应急响应、政府设施、重点制造、能源、公共卫生、水处理、核反应设施、交通系统等行业。发行人已在招股说明书中对各类产品的主要应用领域及具体用途进行修订，并以通俗易懂的方式披露发行人核心产品的应用场景以及不同产品之间解决的安全问题以及差异。虽然发行人产品目前主要应用于电力行业工业控制领域，但具备向其他行业工业控制领域拓展的技术基础，具有可行性；

3、行业主要法律法规及政策及销售合同中未对终端客户发生网络安全事件时的责任承担进行规定或约定，若发生网络安全事件，将根据相关法律法规、部门规章及政策，由专业机构或调查部门或司法机构进行调查、判断、分析、裁定，认定相关责任人，由责任人依法承担相应刑事、行政或民事责任。发行人主要产品技术水平较高，可靠性及稳定性较好，报告期内，不存在因违反法律法规或合同约定而被行政处罚或承担赔偿责任的情形。

4、经核查，上述事项发行人已在《招股说明书》相应章节中进行了修改及补充披露。

问题 2. 关于鸿瑞软件股东

根据申报材料，朱玉珍、张子爱、徐晓骊、刘智勇作为鸿瑞软件的股东，签署《一致行动人协议》。

请发行人说明朱玉珍、张子爱的背景及履历，入股鸿瑞软件的原因，是否与鸿瑞软件、发行人的客户、供应商等存在关联关系或为发行人的前客户、前

供应商等，对鸿瑞软件、发行人的业务开拓及商务拓展等的影响。

请保荐人、发行人律师发表明确意见。

回复：

一、朱玉珍、张子爱的背景、履历，以及入股鸿瑞软件的原因

（一）朱玉珍的背景、履历，以及入股鸿瑞软件的原因

朱玉珍，1946 年 4 月出生，中国国籍，无境外永久居留权，高中学历。1963 年 10 月至 1992 年 3 月，在大连第七塑料厂先后担任车间工人，加工组组长及车间主任，并于 1992 年 4 月退休。

根据鸿瑞软件的工商档案资料以及对朱玉珍及其女儿余梅的访谈确认，朱玉珍于 2007 年 4 月 10 日受让了鸿瑞软件原股东阮杰雄持有的鸿瑞软件 18.5% 股权，股权转让时阮杰雄为朱玉珍的女婿，本次股权转让属于阮杰雄与朱玉珍家庭内部债权债务的处理结果，朱玉珍在受让上述股权后，作为财务投资人一直持有鸿瑞软件股权至今，不参与鸿瑞软件的实际经营、决策，也无股权争议或纠纷。

阮杰雄是通过朋友介绍认识刘智勇，当时双方的办公地点相近，且当时都从事计算机、IT 行业并对行业前景看好（阮杰雄当时投资并经营贸易类公司，主要批发零售电子产品、电子线路板、五金等），经协商一致，阮杰雄于 2003 年 2 月 18 日从鸿瑞软件股东刘智勇、徐晓骊处受让了鸿瑞软件合计 18.5% 的股权。

（二）张子爱的背景、履历，以及入股鸿瑞软件的原因

张子爱，1966 年 5 月出生，中国国籍，无境外永久居留权，硕士研究生学历。1991 年 7 月至 1993 年 7 月，任佳能珠海有限公司制造部职工；1993 年 7 月至 1995 年 11 月，任珠海八达株式会社业务经理职务；1995 年 11 月至 2002 年 12 月，任珠海爱城电脑设备有限公司总经理职务；2003 年至今，任珠海诚欣计算机系统有限公司总经理职务。

根据鸿瑞软件的工商档案资料以及对张子爱的访谈确认，张子爱主要从事与计算机销售相关的工作，在鸿瑞软件成立初期，双方的办公地点均在珠海市香洲区湾仔沙电脑城海城大厦办公，且鸿瑞软件成立初期还通过张子爱采购过少量的电脑及配件等办公设备，双方逐渐成为朋友关系，后来了解到当时鸿瑞软件股东有资金需求，同时张子爱也对 IT 软件信息技术行业有一定了解，经协商一致，于 2003 年 2 月 18 日从鸿瑞软件股东刘智勇、原股东徐梅处受让了鸿瑞软件合计 18.5% 的股权，并作为财务投资人持有鸿瑞软件股权，不参与鸿瑞软件的实际经营、决策。

二、是否与鸿瑞软件、发行人的客户、供应商等存在关联关系或为发行人的前客户、前供应商等

根据对朱玉珍的访谈确认，朱玉珍与鸿瑞软件、珠海鸿瑞的客户、供应商不存在关联关系，也不是珠海鸿瑞的前客户、前供应商。

根据对张子爱的访谈确认，鸿瑞软件成立初期曾通过张子爱采购过少量的电脑及配件等办公设备，金额大概在十万元左右；

2017 年 7 月以及 2018 年 3 月，张子爱控股的珠海诚欣计算机系统有限公司曾分别向发行人采购过远动通讯安全网关设备，金额分别为 1.71 万元以及 9.78 万元。2019 年，发行人曾向张子爱配偶的姐姐控制的公司珠海市思贝特贸易发展有限公司采购过安装调试服务，采购金额为 27.77 万元。

除上述事项外，张子爱与鸿瑞软件、珠海鸿瑞的客户、供应商不存在关联关系。

三、对鸿瑞软件、发行人的业务开拓及商务拓展等的影响

根据对朱玉珍及张子爱的访谈确认，自上述人员入股鸿瑞软件以来，上述人员只是作为鸿瑞软件的股东，享受鸿瑞软件向股东进行的分红，并不直接参与鸿瑞软件的日常经营、决策，并不对鸿瑞软件或者珠海鸿瑞的业务开拓、商务拓展提供帮助或产生其他影响，属于财务投资人。

四、请保荐人、发行人律师发表明确意见

（一）核查程序

保荐人、发行人律师履行了如下核查程序：

1、查阅并取得了鸿瑞软件的现行有效的营业执照、公司章程以及工商登记资料；

2、查阅并取得了朱玉珍、张子爱签署的《关联关系自查表》；

3、对朱玉珍及其女儿余梅、张子爱进行访谈，取得并查阅上述人员签字确认的访谈文件；

4、检索国家企业信用信息公示系统（<http://www.gsxt.gov.cn/index.html>）、天眼查（<https://www.tianyancha.com>）等网站对朱玉珍、张子爱的关联关系进行核查、比对。

（二）核查意见

经核查，保荐人、发行人律师认为：

1、发行人已补充说明朱玉珍、张子爱的背景、履历以及入股鸿瑞软件的原因，是否与鸿瑞软件、发行人的客户、供应商等存在关联关系或为发行人的前客户、前供应商等，对鸿瑞软件、发行人的业务开拓及商务拓展等的影响情况。

2、除上述说明的张子爱的关联方曾为鸿瑞软件、发行人的客户、供应商外，朱玉珍、张子爱与鸿瑞软件、发行人的客户、供应商不存在关联关系或为发行人的前客户、前供应商

3、朱玉珍、张子爱为鸿瑞软件的财务投资人，不对鸿瑞软件、发行人的业务开拓及商务拓展提供重大帮助或产生其他重大影响。

问题 3. 关于知识产权

招股说明书显示，发行人拥有的专利中，部分专利为发行人与其他专利权人共有。

请发行人补充披露相关专利与他人共有的背景、原因，相关发明、实用新型是否系商业合作、项目实施过程中形成，发行人就此类专利与其他专利权人就相关权利归属、技术运用是否存在特别约定，是否存在纠纷或潜在纠纷。

请保荐人、发行人律师发表明确意见。

回复：

一、共有专利的情况

截至报告期末，发行人与第三方共有专利情况如下：

序号	专利名称	专利权人	类型	取得方式	专利号	申请日	权利期限	权利状态
1	电力专用公网通信安全网关	发行人、中国南方电网有限责任公司	发明	原始取得	ZL200810218549.2	2008-10-22	20 年	专利权维持
2	电力专用公网通信数据安全防护方法	发行人、中国南方电网有限责任公司	发明	原始取得	ZL200910041892.9	2009-8-17	20 年	专利权维持
3	电力专用 3G 公网通信安全网关	发行人、广东电网公司东莞供电局	实用新型	原始取得	ZL201220160089.4	2012-4-17	10 年	专利权维持
4	一种应用于 TD-LTE 无线专用通信的安全网关	发行人、广东电网公司东莞供电局	实用新型	原始取得	ZL201220369645.9	2012-7-27	10 年	专利权维持
5	一种配网微型加密终端	发行人、国网上海市电力公司	实用新型	原始取得	ZL201621235082.9	2016-11-17	10 年	专利权维持
6	电力数据公网安全通信系统	发行人、云南电网有限责任公司	实用新型	原始取得	ZL201820633938.0	2018-4-29	10 年	专利权维持

序号	专利名称	专利权人	类型	取得方式	专利号	申请日	权利期限	权利状态
7	电力专用加密通信安全模块	发行人、云南电网有限责任公司	实用新型	原始取得	ZL201820633932.3	2018-4-29	10 年	专利权维持
8	具有远程准入控制功能的变电站自动化系统在线监控装置	发行人、国家电网有限公司、国网湖南省电力有限公司、国网湖南省电力有限公司检修公司	实用新型	继受取得	ZL201621091236.1	2016-9-29	10 年	专利权维持

其中 2 项系与中国南方电网有限责任公司共有，2 项系发行人与广东电网公司东莞供电局共有，2 项系与云南电网有限责任公司共有，1 项系与国网上海市电力公司共有，1 项系与国家电网有限公司、国网湖南省电力有限公司、国网湖南省电力有限公司检修公司共有。

二、相关专利与他人共有的背景、原因，相关发明、实用新型是否系商业合作、项目实施过程中形成

根据发行人出具的说明，并经保荐人、发行人律师对发行人相关专利研发负责人的访谈，发行人共有专利形成的背景、原因及形成情况如下：

（一）与中国南方电网有限责任公司共有的专利

发行人与中国南方电网有限责任公司共有的专利合计 2 项，即“电力专用公网通信安全网关”以及“电力专用公网通信数据安全防护方法”。上述共有专利形成的背景是基于发行人的技术及其运用恰逢 2008 年南方大面积冻灾，贵州省电网公司都匀供电局麻尾变电力通信中断，发行人参与对贵州省电网公司都匀供电局麻尾变的远动通讯恢复工作，通过采用“HR YD-3000 远动通信安全网关”以公用移动通讯网为基础建立安全数据传输通道恢复了实时运行信息的采集，为调度自动化系统安全、连续运行提供技术支持，提高了电网应急情况下的安全水平。借助中国南方电网有限责任公司下属贵州电网都匀供电局的工作环境条件，对发行人本次应用技术、设备安全、可靠性进行了检验。

根据贵州省电网公司都匀供电局出具的《远动通信安全网关用户报告》，发行人装置运行安全可靠、性能稳定、功能齐全、使用方便，提供的应急通道对都匀调度自动化系统联系、安全、稳定运行提供了有力保障。实践表明该装置具有实用性和有效性。

根据中国南方电网电力调度通信中心出具的《关于远动通信安全网关在南方电网的应用情况》，发行人此次采用的设备运行安全可靠、性能稳定，该装置在应对电力通信灾害、电网调度自动化运行维护等方面具有较强实用性和有效性，使用该装置提供的应急远动通道可以缩短通道故障情况下电网实时信息中断的时间，为调度自动化系统安全、连续运行提供了有力的应急支持手段，提高了电网紧急情况下的安全水平。

据此，中国南方电网有限责任公司与发行人共同申请了专利，该专利为发行人与共有人救灾合作实施过程中形成的，但并未就产品合作或技术开发签订书面协议。

（二）与广东电网东莞供电局共有的专利

发行人与广东电网东莞供电局共有的专利合计 2 项，即“电力专用 3G 公网通信安全网关”以及“一种应用于 TD-LTE 无线专用通信的安全网关”，上述共有专利形成是基于发行人与广东电网东莞供电局就当时 3G 网络应用逐步推广背景下对网络安全设计进行技术研讨与实施过程中形成的，但并未就项目合作或技术开发签订书面协议。

（三）与国网上海市电力公司共有的专利

发行人与国网上海市电力公司共有的专利 1 项，即“一种配网微型加密终端”专利，上述共有专利是基于发行人前身鸿瑞有限与国网上海市电力公司对配电网络通讯安全一体化关键技术的研讨，并根据双方签署《科学技术项目合同》（项目名称“配电网络通讯安全一体化关键技术的研究及典型装置的研发”），共同申请专利，属于发行人与共有人商业合作、项目实施过程中形成的。

（四）与云南电网有限责任公司共有的专利

发行人与云南电网有限责任公司共有的专利合计 2 项，即“电力数据公网安全通信系统”以及“电力专用加密通信安全模块”2 项专利，上述共有专利是基

于发行人与云南电网有限责任公司对公网通信系统安全技术以及电力专用安全加密技术研讨，并根据双方签署的《技术服务合同》（项目名称为“多特性小水电群大规模接入消纳关键技术研究与应用”）共同申请的专利，属于发行人与共有人商业合作、项目实施过程中形成的。

（五）与国家电网有限公司、国网湖南省电力有限公司、国网湖南省电力有限公司检修公司共同共有的专利

发行人与国家电网有限公司、国网湖南省电力有限公司、国网湖南省电力有限公司检修公司共同共有的专利 1 项，即“具有远程准入控制功能的变电站自动化系统在线监控装置”专利，该专利原为控股股东鸿瑞软件与上述共有人共同共有，鸿瑞软件为了进一步避免与发行人产生同业竞争的嫌疑，将“具有远程准入控制功能的变电站自动化系统在线监控装置”专利无偿转让给发行人。

根据鸿瑞软件与国网湖南省电力有限公司检修公司签署的《技术服务合同》（项目名称为“智能变电站自动化系统远程在线监控与测试验证平台关键技术研究及应用”），鸿瑞软件与国网湖南省电力有限公司检修公司及其上级单位国家电网有限公司、国网湖南省电力有限公司共同申请专利，上述专利属于鸿瑞软件与共有人商业合作过程中形成的，不属于发行人与共有人商业合作、项目实施过程中形成的。

三、发行人就此类专利与其他专利权人就相关权利归属、技术运用是否存在特别约定，是否存在纠纷或潜在纠纷。

（一）共有专利权归属、技术运用方面的特别约定等情况

1、除发行人与过往上海市电力公司共有的专利外，发行人未就共有专利与共有专利权人进行特别约定。发行人根据《中华人民共和国专利法》（以下简称“《专利法》”）行使专利权。根据《专利法》，发行人和共有人均可以单独实施或者以普通许可方式许可他人实施该类专利（如收取许可使用费，应当与共有人进行分配），但未经其他共有人同意，任意一方均不得将该类共有专利转让给第三方。

2、根据发行人前身鸿瑞有限与国网上海市电力公司签署的《科学技术项目合同》，协议双方就共有专利的申请权、使用权、转让及申请奖励等事项特别约

定如下：

“（1）合同项下的研究成果申请专利的权利归甲方（国网上海市电力公司）享有，未经甲方许可，乙方（鸿瑞有限）不得单独申请或向第三方转让专利申请权。乙方取得专利权的，未经甲方许可，不得转让专利权或许可第三方实施该权利。

（2）甲乙双方均享有本合同项下研究成果的使用权，但乙方仅能在甲方许可的范围内使用该研究成果。因使用该研究成果所产生的效益，由甲乙双方共同协商确定分配方式。

（3）合同项下的研究成果的转让权属于甲方，乙方不得向第三方转让，亦不得许可第三方实施使用，乙方擅自转让所产生的利益归甲方所有。

（4）合同项下的研究成果申请奖励的权利归甲方享有。未经甲方许可，乙方不得单方申请奖励。

（5）合同项下的研究成果的发表权由甲乙双方共同享有。未经一方许可，另一方不得单方发表。根据项目研究成果发表论文须注明“国网上海市电力公司科技项目资助”；项目参加人员个人发表有关项目研究内容的论文须征得甲乙双方的同意。

（6）使用履行本合同产生的研究成果参与国际标准、国家标准或行业标准等的制定或修订工作的权利属于甲方所有，未经甲方许可，乙方不得单独参与此类工作。”

根据《科学技术项目合同》的约定，上述专利的申请权归国网上海市电力公司所有，国网上海市电力公司申请上述专利时与发行人共同申请了上述专利，据此，该专利为国网上海市电力公司与发行人共有。但根据《科学技术项目合同》的约定，发行人取得专利权的，未经国网上海市电力公司许可，不得转让专利权或许可第三方实施该权利。

综上所述，发行人按照相关法律法规或合同约定使用共有专利，共有专利不存在诉讼、仲裁，未产生过相关纠纷。

四、请保荐人、发行人律师发表明确意见

（一）核查程序

保荐人、发行人律师履行了如下核查程序

- 1、访谈发行人及研发部门负责人，了解共有专利的取得过程、使用情况及重要程度等；
- 2、取得发行人专利证书及相关资料；
- 3、查询国家知识产权局专利局网站，了解专利状态及发行人与其他方共有专利情况；
- 4、前往国家知识产权局专利局调取专利查册文件，核查专利法律状态；
- 5、查阅并取得共有人就共有专利出具的确认文件，了解了相关专利的权属纠纷情况；
- 6、查阅并取得了发行人与共有人之间签署的项目合同、相关专利申请表等材料，了解共有专利的产生背景、原因；
- 7、通过中国裁判文书网（<http://wenshu.court.gov.cn>）、中国执行信息公开网（<http://zxgk.court.gov.cn/>）、中国法院网（<https://www.chinacourt.org/index.shtml>）、天眼查（<https://www.tianyancha.com/>）网站进行查询。

（二）核查意见

经核查，保荐人、发行人律师认为：

发行人已补充披露相关专利与他人共有的背景、原因。“具有远程准入控制功能的变电站自动化系统在线监控装置”专利系发行人自控股股东鸿瑞软件处无偿受让，其他共有专利均系发行人与共有人商业合作或项目实施过程中形成的。根据发行人与国网上海市电力公司签署《科学技术项目合同》约定，发行人未经国网上海市电力公司许可，不得转让专利权或许可第三方实施该权利。除此以外，发行人未就其他共有专利与共有专利权人进行特别约定。发行人按照相关法律法规或合同约定使用共有专利，共有专利不存在诉讼、仲裁，未产生过相关纠纷。

问题 5. 关于信息披露

招股说明书显示，发行人于 2016 年 9 月在全国中小企业股份转让系统挂牌并公开转让。

请发行人说明本次申报文件与股转系统挂牌期间在业务和技术、会计估计和会计政策、关联关系及关联方、主要财务数据等方面的信息披露是否存在差异，主要的差异内容及产生差异的原因，本次信息披露的准确性、完整性。

请保荐人、发行人律师、申报会计师发表明确意见。

回复：

一、本次申报文件与股转系统挂牌期间在业务和技术、会计估计和会计政策、关联关系及关联方、主要财务数据等方面的信息披露是否存在差异，主要的差异内容及产生的原因

（一）与财务相关的信息披露是否存在差异，主要的差异内容及产生差异的原因

发行人挂牌期间的财务信息主要披露于《公开转让说明书》以及 2017 年至报告期末的定期报告等公告文件。其中，发行人对挂牌期间的 2017 年年报、2018 年年报、2017 年半年报、2018 年半年报、2019 年半年报的财务信息（原始财务报表）进行了更正和重新披露。

立信会计师事务所（特殊普通合伙）已对发行人原始财务报表与申报财务报表的差异进行了专项审核，并先后出具编号为信会师报字[2020]第 ZC10551 号、

信会师报字[2021]第 ZM10034 号《关于珠海市鸿瑞信息技术股份有限公司原始财务报表与申报财务报表的差异情况的专项审核报告》。发行人本次申报财务报表与原始财务报表（挂牌期间对外公告的财务报表）存在差异的原因主要为：

（1）对应收票据-应收商业承兑汇票按照账龄连续计算并根据应收账款坏账准备政策计提坏账准备，调整 2018 年度财务报表；

（2）根据《企业会计准则第十三号—或有事项》规定，并结合发行人合同中关于产品质量保证的约定，公司决定由原来产品质量售后服务实际发生时计入当期损益，变更为在产品实现销售收入时根据公司历史发生的售后服务情况计提“预计负债-售后服务”，根据《企业会计准则第二十八号—会计政策、会计估计变更及差错更正》的规定调整 2017 年度、2018 年度财务报表；

（3）因公司原委托第三方技术服务成本结算不及时，根据权责发生制及匹配原则，对委托第三方发生的技术服务成本进行核实并调整 2017 年度、2018 年度财务报表；

（4）公司对发出商品、委托加工物资核算不准确，公司对发出商品、委托加工物资进行核实并调整 2017 年度、2018 年度财务报表；

（5）对报告期内进行往来重分类调整、成本费用重分类调整。

发行人已在本次申报前对前期会计差错进行核实及更正，相关会计政策的变更、会计差错更正已经公司 2019 年年度股东大会对《关于公司前期会计差错更正的议案》《关于珠海市鸿瑞信息技术股份有限公司会计政策变更的议案》等议案审议通过，发行人已经履行了必要的审批程序。更正后的财务报表已在股转系统披露，申报文件中的财务数据与发行人挂牌期间已经披露的更正后财务报表和定期报告不存在差异。

（二）其他非财务相关的信息披露是否存在差异，主要的差异内容及产生差异的原因

经查验，发行人本次申报文件与股转系统挂牌期间在其他非财务相关的信息披露存在的主要差异、原因以及发行人发行人在新三板挂牌期间更正或补充披露，具体情况如下：

序	差异事	挂牌期间的信息	本次发行与上市申请文件的	差异原因	发行人采取的更
---	-----	---------	--------------	------	---------

号	项	披露	披露信息		正或补充披露措施（如适用）
1	业务和技术	公司致力于工控信息安全行业十几年，专注于提供工控信息安全技术综合应用解决方案与服务，包括工控信息安全技术软硬件的开发与销售、技术支持和后续服务等，在工控信息安全行业具有较高的认可度。	原披露一致，本次拟修订为：“珠海鸿瑞是一家提供电力及通用工业控制信息安全技术综合应用解决方案与服务的高新技术企业，自成立以来专注于电力工业控制信息安全领域并逐步向通用工业控制信息安全领域拓展，主营业务为从事工业控制信息安全技术软件、硬件的开发与销售，并基于上述产品为客户提供工业控制信息安全技术综合应用的解决方案、技术支持和后续服务等。”	修订后的内容更准确地描述了公司产品目前的应用领域。	--
2	关联方及关联关系	根据当时生效的《全国中小企业股份转让系统挂牌公司信息披露细则（试行）》《企业会计准则第 36 号》认定并披露了发行人的实际控制人、控股股东及发行人董监高等主要关联方	按照《公司法》《企业会计准则第 36 号》《深圳证券交易所创业板股票上市规则》等规定对发行人的关联方进行认定，并对发行人实际控制人、董监高、5%以上股东及其重要家庭密切成员投资/具有重大影响，或担任董事、高管等的关联方进行了披露。	因报告期和关联方认定依据不同，以及因部分董事、监事、高级管理人员变更等原因导致关联方发生变化等	--
3	实际控制人及一致行动人	实际控制人为刘智勇	实际控制人为刘智勇，一致行动人为徐梅、刘芝秀、陈良汉、占小斌	1、刘智勇、徐梅、刘芝秀系参考《上市公司收购管理办法》认定的一致行动关系 2、刘智勇、陈良汉、占小斌系基于各方签署一致行动协议认定的一致行动关系。	1、就刘智勇及徐梅、刘芝秀之间的一致行动关系，发行人履行了相应的内部审批程序，并于 2020 年 8 月 21 日发布了《关于报告期内所涉年度报告、半年度报告的更正公告》。 2、就刘智勇及鸿瑞软件、陈良汉、占小斌之间的一致行动协议，发行人于 2020 年 11 月 3 日披露了《关于实际控制人签订一致行动人协议公告》
4	2017 年 2018 年的关联交易	--	2017 年、2018 年发行人向珠海诚欣计算机系统有限公司销售产品，上述关联交易经过 2017 年第四次总经理办公会议决议、2018 年第三次总经理办公会议审批通过。	履行了相应的内部审批程序但未及时披露	发行人履行了相应的内部审批程序，并于 2020 年 8 月 21 日发布了《关于补发偶发性关联交易的声明公告》《关于补发偶发性关联交易的公告（补发）》及更正后的定期报告。
5	2019 年的关联	--	2019 年发行人委托关联方珠海市思贝特贸易发展有限公	因关联方未及时报备相关关	发行人履行了相应的内部审批程

	交易		司为发行人客户提供现场技术服务。	联关系,发行人未能及时披露该关联交易公告。	序,于2020年9月28日发布了《关于补发偶发性关联交易的声明公告》《关于补发偶发性关联交易的公告》及更正后的定期报告。
--	----	--	------------------	-----------------------	--

综上所述,本次申报文件与新三板挂牌期间的信息无重大差异,且已采取了相应更正披露或补充披露措施,本次申报信息披露准确、完整。

二、请保荐人、发行人律师、申报会计师发表明确意见。

(一) 核查程序

保荐人、发行人律师、申报会计师履行了如下核查程序:

1、查阅发行人报告期内在全国中小企业股份转让系统发布的历次公告,就其中披露的信息与本次发行上市申请文件的内容进行了比对,核实了《招股说明书》披露的信息与新三板挂牌期间信息披露,核实存在的差异原因及并予以分析;

2、取得并查阅了上述披露事项相关工商登记资料、关联关系调查表以及发行人股东大会、董事会、监事会以及总经理办公会议等内部决策文件。

(二) 核查意见

经核查,保荐人、发行人律师、申报会计师认为:

1、发行人已就本次申报文件与新三板挂牌期间信息披露的差异内容及原因进行了相关说明;

2、本次申报文件与新三板挂牌期间的信息及其修订已无重大差异,且公司已采取了相应更正披露或补充披露措施,本次申报信息披露准确、完整。

问题 14. 关于信息披露豁免

请保荐人、发行人律师、申报会计师针对下列情况进行说明,并进一步论证所涉相关信息披露豁免的合理性、必要性:

(1) “发行人未取得纵向加密认证装置、反向隔离装置生产资质并未对公司

经营活动产生不利影响”的原因及其充分性，发行人需要向行业其他公司购买纵向加密认证装置、反向隔离装置等履行相关合同义务对客户合作、业务获取、招投标要求、相关产品毛利率的影响，相关外采销售与贴牌业务的差异，各期所涉金额，相关所涉项目中纵向加密认证装置、反向隔离装置的供应是否为必要或为合同中不可分割的内容；

(2) “相关生产资质的主要内容、相关装置的应用环节和具体作用”是否属于所涉国家秘密等相关信息，发行人对该生产资质的内容及影响进行豁免披露对投资者判断的影响；

(3) “发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的主要产品的毛利率”与发行人招股说明书所称发行人对相关产品进行改造和优化、体现了发行人技术优势等是否相互矛盾，发行人对相关原材料的实际改造情况，发行人披露主要原材料的平均采购价格并不涉及到单一型号的采购价格，相关信息需要豁免披露的合理性。

回复：

一、“发行人未取得纵向加密认证装置、反向隔离装置生产资质并未对公司经营活动产生不利影响”的原因及其充分性，发行人需要向行业其他公司购买纵向加密认证装置、反向隔离装置等履行相关合同义务对客户合作、业务获取、招投标要求、相关产品毛利率的影响，相关外采销售与贴牌业务的差异，各期所涉金额，相关所涉项目中纵向加密认证装置、反向隔离装置的供应是否为必要或为合同中不可分割的内容

(一) 发行人未取得纵向加密认证装置、反向隔离装置生产资质并未对公司经营活动产生不利影响”的原因及其充分性

1、纵向加密认证装置、反向隔离装置并非发行人主要产品，仅在客户存在需求时才会销售

报告期内，发行人销售的主要产品为单向网络隔离装置、双向网络隔离装置、

OPC 网络隔离装置、工业控制防火墙、远动通信安全网关及终端模块、拨号安全服务器、网络安全监测装置、Agent 探针、网络安全态势感知系统、网络报文记录分析系统等多款自主研发的电力及通用工业控制信息安全防护产品。纵向加密认证装置、反向隔离装置并非发行人的核心产品，也不属于发行人未来业务重点发展方向，仅在下游客户存在相关需求时，发行人才会向具备相应生产资质厂商或其代理商购买相关产品，再向客户销售该等产品。

2、纵向加密认证装置、反向隔离装置销售占比较低，与发行人自主研发的产品独立销售，对发行人经营活动影响较小

由于纵向加密认证装置、反向隔离装置并非发行人业务发展重点，纵向加密认证装置销售收入占比已由 2018 年的 21.37%下降至 2019 年的 5.24%及 2020 年的 6.58%，反向隔离装置在报告期内的销售收入占比分别为 1.36%、2.38%、1.33%，占比较低。纵向加密认证装置、反向隔离装置销售占比降低主要系发行人业务发展侧重点、市场开拓力度等因素所致，并非由于未取得生产资质导致。

发行人拥有多款自主研发的电力及通用工业控制信息安全防护产品，该部分产品均与纵向加密认证装置、反向隔离装置独立销售，未取得纵向加密认证装置、反向隔离装置生产资质并不会影响发行人其他产品的销售。

综上，未取得纵向加密认证装置、反向隔离装置资质不会对公司经营活动产生不利影响。

（二）发行人需要向行业其他公司购买纵向加密认证装置、反向隔离装置等履行相关合同义务对客户合作、业务获取、招投标要求、相关产品毛利率的影响

由前述分析可知，销售纵向加密认证装置、反向隔离装置并不影响发行人其他产品的销售。

由于发行人下游的电网公司搭建信息安全防护体系时，需要采购各类工业控制信息安全防护产品，客户综合考虑便利性、供应商调试技术水平等因素后，会向发行人提出纵向加密认证装置、反向隔离装置的采购需求，在此情况下，发行人向生产厂商或其代理商采购相关产品。该业务模式在电力工业控制信息安全领

域较为常见，具有其合理性。发行人过往也未曾出现无法从生产厂商或其代理商采购纵向加密认证装置、反向隔离装置的情形，因此，发行人需要向行业其他公司购买纵向加密认证装置、反向隔离装置并不会对客户合作、业务获取、满足招投标要求等产生不利影响。

发行人销售自主研发生产的正向隔离装置（属于单向网络隔离装置）时，部分客户会向发行人采购反向隔离装置，但该情况并不影响发行人正向隔离装置销售及毛利率。报告期内，发行人销售的正向隔离装置主要为百兆安全隔离装置和千兆安全隔离装置产品，2018 年至 2020 年，百兆安全隔离装置毛利率分别为 76.20%、80.16%、80.60%，千兆安全隔离装置毛利率分别为 81.51%、83.85%、78.87%，毛利率水平较为稳定。纵向加密认证装置则通常单独销售，报告期内，该类产品毛利率分别为 28.12%、34.94%、34.54%，毛利率水平同样较为稳定。因此，发行人需要向行业其他公司购买纵向加密认证装置、反向隔离装置对相关产品毛利率不存在重大影响。

（三）相关外采销售与贴牌业务的差异，各期所涉金额，相关所涉项目中纵向加密认证装置、反向隔离装置的供应是否为必要或为合同中不可分割的内容

发行人向下游客户销售纵向加密认证装置、反向隔离装置系客户需求所致，并非采购上游生产厂商的相关产品后进行的贴牌销售。

纵向加密认证装置、反向隔离装置的供应不属于必要或为合同中不可分割的内容，具体原因如下：

1、根据《电力监控系统安全防护规定》第一条的规定“为了加强电力监控系统的信息安全管理，防范黑客及恶意代码等对电力监控系统的攻击及侵害，保障电力系统的安全稳定运行，……制定本规定”。电力监控系统安全防护是在统一安全策略下保护重要系统免受黑客、病毒、恶意代码等侵害的安全防护体系，该系统是一个可从多个角度、多个层面实现保护功能的体系，系统搭建遵守整体规划、分步实施的原则，并且随着网络安全攻防技术的演变在后续实施过程中不断完善。

因此，电力监控系统安全防护项目建设中，除全新厂站建设中可能需采购防护体系中所有部件外，大部分项目并非需要采购所有安全防护设备。

2、报告期内，部分下游客户在采购发行人核心产品的同时，综合考虑便利性、技术团队专业水平等因素，向发行人采购部分纵向加密认证装置、反向隔离装置，其不是与发行人自主研发生产的产品捆绑采购，亦不是发行人的核心产品。

3、报告期内，不存在因纵向加密认证装置、反向隔离装置供应影响发行人其他产品销售的情形。

综上所述，纵向加密认证装置、反向隔离装置的供应不属于必要或为合同中不可分割的内容。

二、“相关生产资质的主要内容、相关装置的应用环节和具体作用”是否属于所涉国家秘密等相关信息，发行人对该生产资质的内容及影响进行豁免披露对投资者判断的影响

（一）对“相关生产资质的主要内容、相关装置的应用环节和具体作用”进行豁免披露不影响投资者判断

1、披露相关生产资质的主要内容、相关装置的应用环节和具体作用可能会对电力系统安全带来一定不利影响

电力系统安全运行意义重大，世界上很多国家都发生过大面积停电事故，例如 2003 年美国东北部和加拿大东部大停电事故使得 5,000 万人受到影响；2012 年印度北部大停电事故使得印度超过 22 个邦的 6.2 亿人受到影响；2019 年阿根廷和乌拉圭大规模停电事故有超过 4,800 万人受到影响。电力系统瘫痪呈现波及面较广，经济损失重大的特点，因此，电力行业工业控制信息安全直接关系到国家安全，若电力系统受到攻击，将会对国民经济和人民正常生活秩序产生重大不利影响。

电力监控系统安全防护是与国计民生密切相关的电力系统安全运行的重要保障，如对生产资质、应用环境和具体作用进行详细披露会泄露电力系统相关技

术方案与实施细节，降低电力监控系统安全防护强度，进而影响到国家电力系统安全。同时，这也可能引发公众不必要的猜测或误读，可能带来负面影响。

2、对“相关生产资质的主要内容、相关装置的应用环节和具体作用”进行豁免披露符合《电力监控系统安全防护规定》对保密管理的规定

根据《电力监控系统安全防护规定》第四章保密管理第十八条规定：“电力监控系统相关设备及系统的开发单位、供应商应当以合同条款或者保密协议的方式保证其所提供的设备及系统符合本规定的要求，并在设备及系统的全生命周期内对其负责。电力监控系统专用安全产品的开发单位、使用单位及供应商，应当按国家有关要求做好保密工作，禁止关键技术和设备的扩散”，以及第十九条规定：“对生产控制大区安全评估的所有评估资料和评估结果，应当按国家有关要求做好保密工作”。

同时，发行人与国家电网有限公司签订了《电力监控系统专用网络安全防护设备供应商承诺书》，承诺“健全保密机制，明确涉密范围，将专用设备关键技术细节（包括但不限于涉及图纸、密码算法、密码芯片、核心软件等）纳入保密管理范畴，严格控制接触人员”。

因此，申请豁免详细披露“相关生产资质的主要内容、相关装置的应用环节和具体作用”，符合《电力监控系统安全防护规定》对保密管理的规定。

综上，发行人申请在审核问询函回复和招股说明书等申请文件中豁免或简化披露纵向加密认证装置、反向隔离装置生产资质的具体内容、应用环境和具体作用具有必要性。

（二）发行人对该生产资质的内容及影响进行豁免披露不影响投资者实质判断

纵向加密认证装置、反向隔离装置并非发行人核心产品，仅在下游客户有需求时，发行人才会向上游有生产资质的供应商或其代理商采购相应产品。2019年及2020年，纵向加密认证装置、反向隔离装置合计销售金额占发行人当年营

业收入的比重不到 10%，占比较低，未取得纵向加密认证装置、反向隔离装置生产资质不会对发行人主营业务产生实质性影响。

综上，发行人对纵向加密认证装置、反向隔离装置生产资质的内容及影响进行豁免披露不影响投资者实质判断。

三、“发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的主要产品的毛利率”与发行人招股说明书所称发行人对相关产品进行改造和优化、体现了发行人技术优势等是否相互矛盾，发行人对相关原材料的实际改造情况，发行人披露主要原材料的平均采购价格并不涉及到单一型号的采购价格，相关信息需要豁免披露的合理性。

（一）“发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的主要产品的毛利率”与发行人招股说明书所称发行人对相关产品进行改造和优化、体现了发行人技术优势等是否相互矛盾

1、“发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的主要产品的毛利率”主要是指纵向加密认证装置、反向隔离装置两类产品

发行人不具备纵向加密认证装置和反向隔离装置的生产资质。上述两种产品非发行人的核心产品，只有在最终客户项目现场应用环境、产品参数、与原系统的适配性、整体解决方案的防护效果等存在需求时采购纵向加密认证装置和反向隔离装置的整机，若披露上述整机的采购单价，则发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的纵向加密认证装置和反向隔离装置等相关产品的毛利率。

2、相关说法不相互矛盾

发行人各主要产品的营业成本中占比较高的均为直接材料，若剔除技术服务费影响，报告期内各主要产品直接材料占比在 90%以上，发行人的核心技术主要体现在产品前期的研发设计环节，而相关的研发支出均计入研发费用而非营业成本中。发行人高度重视研发投入，设立以来投入大量精力和人员用于产品研发，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，持续研发，提

升市场竞争力，发行人出于谨慎性原则，相关研发支出未确认无形资产，均费用化处理计入研发费用。因此，发行人的主要产品的营业成本中直接材料占比较高，“发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的主要产品的毛利率”与发行人的相关产品体现了发行人技术优势等不存在矛盾。

（二）发行人对相关原材料的实际改造情况

发行人根据客户需求以及销售合同的签订情况制定生产计划，并根据生产计划提交原材料采购需求，公司采购部对相应原材料进行采购并对购回的材料进行检测。对于需要外协加工的主板，由公司提供设计图纸和关键技术参数，同时采购加密芯片、主控芯片等关键元器件及部分零配件发予外协厂商进行贴片处理。外协厂商完成加工后，由公司对半成品进行测试，测试合格后将外协生产的主板与其他零部件进行成品组装，此过程需严格遵循研发设计定型的硬件图纸与工艺说明。在各类电子元器件及其辅料组装调试后，将自主研发的软件灌装入硬件设备中，最后经烤机测试、产品质量检验、入库等环节完成生产。

发行人采购原材料后，主要对其进行检测、组装、灌装软件、拷机测试和产品质量检验等生产步骤，对原材料本身未进行改造。

（三）发行人披露主要原材料的平均采购价格并不涉及到单一型号的采购价格，相关信息需要豁免披露的合理性

1、网关类装置、元器件、工控机等原材料采购价格的公允性

发行人原材料种类、型号繁多，且部分产品系电力行业专用装置，不存在公开活跃市场价格。报告期内，发行人原材料采购价格主要通过第三方询价、比价等方式确定。发行人的原材料按大类主要分为网关类装置、元器件、工控机等。其中，各个大类原材料又分为不同的细分原材料，不同细分原材料在规格、型号、品牌等方面也存在差异，且部分材料发行人需根据客户实际需求进行定制，导致价格存在差异。

报告期内，发行人主要原材料的采购单价的具体情况如下：

所属 大类	典型 原材 料	典型 规格 型号	单 位	2020 年度	2019 年度	2018 年度	市场价格/第三方价格区 间
网关	产品一		元/	5,065.22	10,408.90	9,652.42	2,200.00-42,000.00

所属 大类	典型 原材料	典型 规格 型号	单 位	2020 年度	2019 年度	2018 年度	市场价格/第三方价格区 间
类装 置			套				
	产品二		元/ 套	30,454.39	31,557.71	29,823.84	24,000.00-48,000.00
	内网监测 设备		元/ 套	4,994.61	4,973.56	4,980.73	5,224.82
元器 件	通信模块		元/ 个	115.06	125.44	139.42	145.00-270.00
	芯片		元/ 片	34.53	34.31	32.07	4.35-84.07
	电源		元/ 个	136.82	113.34	123.74	72.00-320.00
	交换机		元/ 台	2,799.99	3,051.52	3,476.72	2,100.00-5,400.00
工控 机	低端机型		元/ 套	4,448.74	4,552.73	4,049.82	1,060.00-8,940.00
	高端机型		元/ 套	13,874.55	15,728.80	15,948.28	13,000.00-18,500.00

注：发行人用以比较的市场可比价格的选择依据依次为：（1）同类产品的市场公开价格或者其他企业采购的同类产品交易价格的公开数据；（2）发行人询价的供应商报价区间。

由上表可见，发行人在采购过程中执行询价、比价流程，采购的原材料基本在市场价格/第三方价格区间之内。公司采购的网关类装置中的产品一和产品二有多种型号，报告期内各年度采购型号的结构不同导致各年度的采购单价有所波动；公司采购的通信模块，报告期内公司与不同通信模块厂商之间进行合作，最终选取了通信模块产品性价比最高的通信模块厂商，该产品询价时以小批量询价，与供应商建立了长期稳定的合作关系后，公司采购数量较多，供应商给予了优惠，因此实际采购平均单价低于市场询价价格。报告期内，公司各类主要细分原材料单价较为稳定，不存在重大变化，上述部分细分原材料单价存在一定波动，平均价格的差异主要系由于采购品牌差异、具体规格差异、定制内容差异、采购数量变化等原因所致。

综上所述，报告期内，公司各类主要细分原材料单价较为稳定，各类主要细分原材料的采购价格与市场价格或第三方价格不存在明显差异，采购价格公允合理。

2、报告期内向前五大和新增供应商的采购单价及公允性

发行人选取报告期内向前五大供应商和前五十大新增供应商采购的主要产品种类或型号，与市场可比价格进行对比，确定采购单价的公允性。发行人用以比较的市场可比价格的选择依据依次为：（1）同类产品的市场公开价格或者其他企业采购的同类产品交易价格的公开数据；（2）发行人询价的供应商报价区间；（3）当年发行人向其他供应商采购同类产品的单价。报告期内，发行人向前五大供应商和前五十大新增供应商采购单价及市场可比价格情况如下：

单位：元/套，元/台，元/件

2020 年度前五大供应商					
序号	供应商名称	采购内容	采购单价	市场可比价格	差异情况
1	兴唐通信科技有限公司	纵向加密认证装置	/	/	长期稳定合作关系供应商给予一定折扣导致略低于市场可比价格
2	南京合为电气科技有限公司	内网监测设备	4,973.45	5,224.82	无重大差异，由于规格型号及批量采购的原因导致与市场可比价格存在差异
3	广州兴森快捷电路科技有限公司	贴片加工	115.88	-	-
4	深圳市安腾达科技有限公司	交换机	3,676.11	2,100.00-5,400.00	在市场可比价格区间内
5	研祥智能科技股份有限公司	工控机	13,875.02	13,000.00-18,500.00	在市场可比价格区间内
2020 年度前五大新增供应商					
序号	供应商名称	采购内容	采购单价	市场可比价格	差异情况
1	深圳市畅康电子科技有限公司	电脑	8,355.01	2,793.00-11,308.00	在市场可比价格区间内
2	广州市明锐电器有限公司	辅助系统	117,319.85	-	-
3	广州市正道润同科技有限公司	电脑	3,628.32	2,793.00-11,308.00	在市场可比价格区间内
4	山西友利华科技有限公司	电脑	7,079.65	2,793.00-11,308.00	在市场可比价格区间内
5	广西兴成科技有限公司	辅助系统	221,238.94	-	-
2019 年度前五大供应商					
序号	供应商名称	采购内容	采购单价	市场可比价格	差异情况
1	南京合为电气科技有限公司	内网监测设备	4,973.56	5,224.82	无重大差异，由于规格型号及批量采购的原因导致与市场可比价格存在差异

2	兴唐通信科技有限公司	纵向加密认证装置	/	/	在市场可比价格区间内
3	英伟捷科技（深圳）有限公司	通信模块	125.38	145.00-270.00	长期稳定合作关系供应商给予一定折扣导致略低于市场可比价格
4	国家电网有限公司	纵向加密认证装置	/	/	在市场可比价格区间内
		反向隔离装置	/	/	在市场可比价格区间内
		安全芯片	84.07	84.07	无差异
5	广州兴森快捷电路科技有限公司	贴片加工	93.42	-	-

2019 年度前五大新增供应商

序号	供应商名称	采购内容	采购单价	市场可比价格	差异情况
1	北京旭泓科技有限公司	纵向加密认证装置	/	/	在市场可比价格区间内
		反向隔离装置	/	/	在市场可比价格区间内
2	云南恒佳建设工程有限公司	技术服务	-	-	-
3	云浮市知行电力科技有限公司	技术服务	-	-	-
4	乌鲁木齐九州凌云电子科技有限公司	交换机	3,451.33	2,100.00-5,400.00	在市场可比价格区间内
		工作站	6,194.69	5,299.00-8,069.00	在市场可比价格区间内
		机柜	7,964.60	6,159.29	无重大差异，由于该供应商的机柜含空气开关等配件，且其包含偏远地区的运费导致高于市场可比价格
5	桂林龙传通信技术有限公司	内存	398.06	279.00-549.00	在市场可比价格区间内
		CPU	648.54	774.34	无重大差异，规格型号不同导致差异

2018 年度前五大供应商

序号	供应商名称	采购内容	采购单价	市场可比价格	差异情况
1	国家电网有限公司	纵向加密认证装置	/	/	在市场可比价格区间内
		反向隔离装置	/	/	在市场可比价格区间内
		安全芯片	81.79	84.07	无重大差异
2	兴唐通信科技有限公司	纵向加密认证装置	/	/	长期稳定合作关系供应商给予一定折扣导致略低于市场可比价格
3	南京合为电气科技有限公司	内网监测设备	4,980.73	5,224.82	无重大差异，由于规格型号及批量采购的原因导致

					与市场可比价格存在差异
4	北京中电昱邦技术有限公司	纵向加密认证装置	/	/	在市场可比价格区间内
5	深圳市思诺康科技有限公司	芯片	30.59	6.65-45.00	在市场可比价格区间内
		天线	3.85	4.58	无重大差异

2018 年度前五大新增供应商

序号	供应商名称	采购内容	采购单价	市场可比价格	差异情况
1	南京合为电气科技有限公司	内网监测设备	4,980.73	5,224.82	无重大差异，由于规格型号及批量采购的原因导致与市场可比价格存在差异
2	北京中电昱邦技术有限公司	纵向加密认证装置	/	/	在市场可比价格区间内
3	广州奥存计算机科技有限公司	主板	554.17	578.85	无重大差异
4	海南金海翔网络科技有限公司	电源	110.79	72.00-320.00	在市场可比价格区间内
5	杭州乾坤科技有限公司	技术服务	-	-	-

发行人采购的辅助系统和贴片服务定制化程度较高，无市场报价，价格根据公司对产品的要求与供应商协商确定。除此之外，经比较，发行人向前五大供应商或者前五大新增供应商采购的主要产品的单价与市场可比价格不存在显著差异，存在差异的主要原因系：1、发行人采购的产品细分型号众多，基于客户对产品和应用的相应要求，发行人使用的主要原材料也存在品牌、规格、型号以及技术参数等方面的差异，因此用以比较的产品的品牌、规格型号等并非完全相同；2、发行人与供应商建立了长期稳定合作关系或采购数量较大，供应商给予一定折扣导致略低于市场可比价格。发行人采购的技术服务内容不固定，会根据客户的具体需求情况，结合调试时间、施工地点、交通方式、服务周期以及服务内容等确定采购价格，难以在公开市场直接查到一致服务的价格标准，发行人主要是通过询价的方式确定最终的供应商及采购价格，按市场性价比原则，价格公允。

综上所述，发行人向前五大供应商与前五大新增供应商采购的主要产品的单价具有公允性。

3、相关信息需要豁免披露的合理性

依据《电力监控系统安全防护规定》第四章保密管理第十八条的相关规定，“电力监控系统相关设备及系统的开发单位、供应商应当以合同条款或者保密协

议的方式保证其所提供的设备及系统符合本规定的要求，并在设备及系统的全生命周期内对其负责。电力监控系统专用安全产品的开发单位、使用单位及供应商，应当按国家有关要求做好保密工作，禁止关键技术和设备的扩散”。以及第十九条“对生产控制大区安全评估的所有评估资料和评估结果，应当按国家有关要求做好保密工作”。

电力行业工业控制信息安全直接关系到国家安全，一旦电力系统受到攻击，可能会对国民经济造成重大损失，对人民生活秩序产生波及面较广的重大不利影响，并可能危害国家安全。

披露相关厂商和产品的销售信息可能会对国家电力系统安全带来一定不利影响。因此，发行人申请豁免相关信息具有合理性。

四、核查程序及核查意见

（一）核查程序

保荐人、发行人律师、申报会计师履行了如下核查程序：

1、查阅相关法律法规，以及发行人业务开展情况，分析发行人未取得纵向加密认证装置、反向隔离装置的生产资质对其经营活动的影响；

2、取得并查阅发行人销售明细表，分析纵向加密认证装置、反向隔离装置销售收入及占比；

3、访谈了发行人董事长，了解发行人未取得纵向加密认证装置、反向隔离装置的生产资质的原因，向行业其他公司购买纵向加密认证装置、反向隔离装置对客户合作、业务获取、招投标要求的影响，并获取相关产品毛利率进行分析；

4、查阅《电力监控系统安全防护规定》，了解电力行业对产品、技术的保密要求；

5、访谈了发行人生产负责人，了解发行人主要产品的生产流程。

（二）核查意见

经核查，保荐人、发行人律师、申报会计师认为：

1、发行人未取得纵向加密认证装置、反向隔离装置生产资质具有合理性，

未取得相关资质并未对公司经营活动产生不利影响。发行人需要向行业其他公司购买纵向加密认证装置、反向隔离装置对客户合作、业务获取、招投标要求、相关产品毛利率不存在重大影响。报告期内，发行人不存在贴牌销售的情形，产品销售中纵向加密认证装置、反向隔离装置的供应不属于合同中不可分割的内容；

2、若对生产资质、应用环境和具体作用进行详细披露会泄露电力系统相关技术方案与实施细节，降低电力监控系统安全防护强度，进而影响到国家电力系统安全，故豁免披露相关生产资质的主要内容、相关装置的应用环节和具体作用具有必要性，符合《电力监控系统安全防护规定》对保密管理的规定。由于纵向加密认证装置、反向隔离装置报告期内销售收入占比相对较低，发行人对该生产资质的内容及影响进行豁免披露不影响投资者对企业价值及业务开展情况等方面进行实质性判断；

3、“发行人的部分客户及竞争对手可能通过主要原材料的采购单价推算发行人的主要产品的毛利率”与发行人招股说明书所称体现了发行人技术优势等不存在矛盾。发行人采购原材料后，主要对其进行检测、组装、灌装软件、拷机测试和产品质量检验等生产步骤，对原材料本身未进行改造。发行人对元器件、工控机等原材料采购单价进行了补充披露，仅豁免披露涉及商业秘密的部分网关类专用设备的采购单价，相关信息豁免披露具有合理性。

本补充法律意见书正本一式六份，无副本。

（此页无正文，为广东精诚粤衡律师事务所《关于珠海市鸿瑞信息技术股份有限公司首次公开发行股票并在创业板上市的补充法律意见书（三）》之签署页）



负责人：罗 刚 罗刚

经办律师：罗 刚 罗刚

李勇虎 李勇虎

唐伟振 唐伟振

日期：2021年 6 月 6 日