**腾龙芳烃（漳州）有限公司**

**分散控制系统DCS网络安全加固**

**技术规范书**

**编 制：**

**初 审：**

**审 核：**

**批 准 ：**

**腾龙芳烃（漳州）有限公司**

**2023年04月26日**

# 投标人资质和条件

1、投标人应具备独立法人资格且有能力提供招标服务。

2、投标人须为依法注册的独立法人或其他组织，须提供有效的证明文件。

投标人须具有并提供有效的信息安全管理体系认证证书、信息安全等级保护安全建设服务机构能力评估合格证书。并提供有效的书面证明材料。

3、业绩要求

1. 投标方应具有最近3年内已完工的200MW或以上火电机组DCS网络安全防护系统设备供货及现场调试业绩，需提供与最终用户等签订的合同作为业绩证明文件（至少包括合同封面、签字页、供货、工作范围描述相关页及完工证明文件 (如发票、完成验收表、用户证明等)）
2. 未提供业绩证明文件或提供的业绩证明文件无法认定上述业绩要求的，视为无效业绩。
3. 与招标人存在利害关系可能影响招标公正性的法人，不得参加投标。
4. 单位负责人为同一人或者存在控股、管理关系的不同单位，不得同时参加本招标项目投标。
5. 处于被责令停业或投标资格被取消或财产被接管、冻结、查封、破产等权利状态受限状态的投标人，不得参加投标。
6. 本项目不接受联合体投标。

4、投标费用

承包方应承担其编制投标文件与递交文件所涉及的一切费用。

5、投标文件的语言

单位之间来往的通知、函件和文件均使用中文。

6、评标形式

本工程按照国家有关规定，实行公平、公正、公开的原则，建议通过招标形式综合评标，择优选定中标单位。

1. 本次评标采用综合评分法评标，得分最高者中标。

各部分评分分值分布如下：

PT：商务部分评分 满分10分

PB：技术部分评分 满分20分

PF：报价部分评分 满分70分

注:①PT和PB部分的最终得分为各个评标委员会评分的算术平均值，并四舍五入取小数点后2位数。②评标委员会评分取小数点后1位数。

综合得分：P＝PT＋PB＋PF

2. 评分标准见下表。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 |  | 评审项目 | 分值 | 评分细则 | 投标人1 | 投标人2 | …… |
| 1 | 商务部分 | 体系认证 | 2 | 信息安全管理体系认证证书、信息安全等级保护安全建设服务机构能力评估合格证书得5分，不全得2分，没有得0分。 |  |  |  |
| 工作业绩 | 8 | 近3年有类似产品业绩。提供一个合同及发票凭证得1分，最高得8分。 |  |  |  |
| 2 | 技术部分 | 技术方案和人员资质 | 20 | 1、根据响应人的网络安全建设技术方案横向比较综合评审，最高15分，最低得 5 分。  2、项目团队负责人及技术人员资质（CISSP注册信息系统安全专家证书、ISO27001 LA信息安全管理体系主任审核员证书、CISAW信息安全保障人员证、CISP注册信息安全专业人员认证），最高5分，没有最低得 0 分。 |  |  |  |
| 3 | 报价部分 | 投标报价 | 70 | 投标价格得分=( F低/ Fn)×70  式中：①F低为评标基准价=进入报价部分评分的各合格投标人中最低的报价评标价。  ②Fn为进入报价部分评分的各合格投标人的报价评标价。 |  |  |  |
|  | 合计： | | | |  |  |  |

六、答疑及现场勘察

1.开标前：承包方可以通过传真、电话询问方式答疑。

2.勘察现场：

1）承包方勘察现场所发生的费用由承包方自己承担。

2）承包方提出的与投标有关的任何问题须在招标文件规定的时间内以书面形式送至发包方。

七、差异表

投标人要将投标文件和招标文件的差异之处汇集成表。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 招标文件 | | | 投标文件 | |
| 条目 | 简要内容 | 条目 | | 简要内容 |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |

备注：承包方如对本规范书有偏差（无论多少或微小）都必须清楚地表示在本规范书的附件 “差异表”中。否则认为承包方完全接受。

# 一、总则

1.1本技术规范书适用腾龙芳烃（漳州）有限公司热电厂4×670t/h+3×150MW汽轮发电机组的分散控制系统DCS网络安全加固项目的技术要求。

1.2本技术规范书规定的是最低限度的技术协议，并未对一切技术细节作出规定，也未充分引述有关标准和规范的条文，投标方应提供符合本技术协议要求和有关行业标准的服务。

1.3本技术规范书投标方若有异议，则以差异表方式在投标文件中一并提出。如投标方没有以书面形式对本规范的条文提出异议，那么招标方可以认为投标方提供的服务完全满足本规范的要求。

1.4如投标方有除本规范书以外的其他要求，应以书面形式提出，经与招标方讨论、确认后，载于本规范书。

1.5在合同签订后，招标方有权提出因设计、标准、规程、规范和现场实际发生变化而产生的修订要求。投标方应承诺予以配合，具体项目和条件由双方共同商定。

1.6本技术规范书经招标方、投标方双方确认后作为合同的技术附件，与合同正文具有同等效力。

1.7本规范所使用标准如与投标方所执行标准发生矛盾时，按较严格现行标准执行。

1.8投标方对供货范围内的设备负有全部责任，且包括分包(或对外采购)的产品。

1.9在签订合同之后，招标方有权提出因规范标准和规程发生变化而产生的一些补充要求，具体项目由双方共同商定。

1.10本项目要求采用国家最新实行的或将要实行的有关标准、规范和规定。

1.11设备采用的专利涉及到的全部费用均被认为已包含在设备报价中，卖方应保证买方不承担有关设备及软件等专利的一切责任。

1.12为便于评标工作，投标方提交的所有投标文件的电子版应采用可编辑电子文件，使用语言为中文，投标方在投标文件中所提的技术数据应以表格的形式列出。工程联系文件、技术资料、图纸、计算、仪表刻度和文件中的计量单位均采用法定计量单位。

# 二、工程概况

**2.1厂址概况**

热电厂位于漳州古雷港口经济区（位于福建省南端，东经117°30′～117°45′，北纬23°25′～24°），古雷区域东临浮头湾、台湾海峡，西靠东山湾，面对东山县、云霄县，三面环海。水路至厦门77海里，至汕头73海里，至台湾澎湖98海里。陆路至漳州112km，至厦门138km，至汕头146km。沈海高速公路从规划区北面穿过并设有互通口。国道324线、漳州沿海大通道和规划建设的厦深铁路横贯规划区北面，区位和交通条件优越。

**2.2工程概况**

**1）工程简介**

腾龙芳烃热电厂装设4台670t/h超高压煤粉锅炉（670t/h、13.7MPa、540℃）。锅炉采用自然循环、四角切向燃烧方式，单炉膛，无再热，平衡通风，露天布置，固态排渣，全钢架悬吊结构∏型汽包锅炉。过热器出口压力13.7MPa，过热器出口温度540℃。配套3×150MW (12.5MPa,534℃)抽汽凝汽式汽轮发电机组,汽轮机采用南京汽轮机有限公司生产的超高压双缸双排汽抽汽凝汽式汽轮机进行设计,每套汽轮机设计一段可调工业抽汽系统,其抽汽负荷性质为4.3MPa\*382\*282t/h。一段可调工业抽汽一部分直接作为外界供热蒸汽,另一部分经减温减压2.3MPa\*230℃后作为外界供热蒸汽,以满足主厂区的供热蒸汽需求。

**2）气象条件**

本项目所在地属南亚热带季风性气候，冬无严寒，夏无酷暑。年平均气温为21.3℃；年平均降水1327.4mm，雨季集中在5~8月；多年平均湿度为80%；常年主导风向为东北风；7~9月受台风影响频率最高。

* 气温

|  |  |
| --- | --- |
| 年平均大气温度 | 21.3℃ |
| 极端最高气温 | 38.2℃ |
| 极端最低气温 | 4.7℃ |
| 最热月的日最高大气温度的平均值 | 31.6℃ |
| 年最高气温日数 | ≥30℃，平均每年81d |
|  | ≥35℃，平均每年0.65d |
| 无霜期 | 365天/年 |

* 降水

|  |  |
| --- | --- |
| 多年平均年降水量 | 1327.4毫米 |
| 历年最多年降水量 | 2125.6毫米 |
| 历年最少年降水量 | 788.8毫米 |

* 风

|  |  |
| --- | --- |
| 多年平均风速 | 5.5米/秒 |
| 夏季平均风速 | 3.9米/秒（10m高处平均风速） |
| 冬季平均风速 | 6.9米/秒（10m高处平均风速） |
| 主导风向 | 东北，北北东 |

**三、技术标准**

供货范围和服务所涉及的硬件和软件等应符合相应的标准规范或法规的最新版本或其修正本的要求, 除非另有特别说明，将包括投标期内有效的任何修正和补充。

除非合同另有规定，均须遵守最新的国家标准(GB)、国家电力行业标准(DL)、国际电工委员会(IEC)标准及国际单位制(SI)标准。当上述标准不一致时，按技术条款要求高的标准执行。

GB 17859-1999 计算机信息系统 安全保护等级划分准则

GBT 22239-2019 信息安全技术 网络安全等级保护基本要求

GBT 28448-2019 信息安全技术 网络安全等级保护测评要求

GBT 28449-2018 信息安全技术 网络安全等级保护测评过程指南

GBT 36572-2018 电力监控系统网络安全防护导则

GBT 33009.1-2016 工业自动化和控制系统网络安全 集散控制系统（DCS） 第1部分：防护要求

GBT 33009.2-2016 工业自动化和控制系统网络安全 集散控制系统（DCS） 第2部分：管理要求

GBT 33009.3-2016 工业自动化和控制系统网络安全 集散控制系统（DCS） 第3部分：评估指南

GBT 33009.4-2016 工业自动化和控制系统网络安全 集散控制系统（DCS） 第4部分：风险与脆弱性检测要求

GBT 37933-2019 信息安全技术 工业控制系统专用防火墙技术要求

GBT 37934-2019 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求

GBT 37953-2019 信息安全技术 工业控制网络监测安全技术要求及测试评价方法

GBT 37941-2019 信息安全技术 工业控制系统网络审计产品安全技术要求

GBT 37954-2019 信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法

GBT 40813-2021 信息安全技术 工业控制系统安全防护技术要求和测试评价方法

GAT 1350-2017 信息安全技术 工业控制系统安全管理平台安全技术要求

GAT 1485-2018 信息安全技术 工业控制系统入侵检测产品安全技术要求

GAT 1559-2019 信息安全技术 工业控制系统软件脆弱性扫描产品安全技术要求

GAT 1560-2019 信息安全技术 工业控制系统主机安全防护与审计监控产品安全技术要求

GAT 1562-2019 信息安全技术 工业控制系统边界安全专用网关产品安全技术要求

国家能源局在2015年2月4日印发了《电力监控系统安全防护总体方案》（俗称36号文）

国家发展和改革委员会第14号令《电力监控系统安全防护规定》

以上标准提出了最基本要求， 投标方应执行本技术协议所列标准。有不一致时,按较高标准执行，并及时通告买方。从订货之日至卖方开始制造之日的这段时期内，买方有权提出因规程、规范和标准发生变化而产生的补充要求，卖方应遵守这些要求。且不论买方知道与否，卖方有责任及时书面通知买方有关规程、规范和标准发生的变化。

**四、系统概况**

4.1分散控制系统简介

腾龙芳烃（漳州）有限公司热电厂4×670t/h+3×150MW汽轮发电机组的分散控制系统DCS采用南京科远NT6000，每台锅炉、汽机和公用部分设立独立设备电子间，辅网车间控制系统脱硫区域DCS采用南京科远NT6000,4台锅炉烟气脱硫控制系统在脱硫控制楼电子设备间。除尘除灰区域控制系统采用西门子S7-400，4台锅炉除尘输灰电子设备间设在除尘输灰控制楼。输煤区域控制系统DCS采用南京科远NT6000，电子设备间设在输煤控制楼。采用全厂集中控制布置在汽机房10米层中央控制室内。腾龙芳烃（漳州）有限公司热电厂分散控制系统DCS网络现状如下：

网络拓扑图

1. 4×670t/h+3×150MW汽轮发电机组DCS系统网络采用A/B网冗余配置，每台锅炉、每台汽机和公用系统各设置1对网络控制域，该主机和公用系统共8个域，16个网段。4台锅炉为1-4号控制域、3台汽机为5-7号控制域每个控制域各设置2台操作站、1台工程师站。锅炉、汽机各控制域通过三层交换机接入公用系统的8号控制域，公用系统的8号控制域设置3台工程师站,2台值长站、1台公用操作站、2台历史站，1台接口机。
2. 辅网车间控制系统DCS系统网络采用A/B网冗余配置1对控制域，设置4台脱硫操作站，1台脱硫工程师站，1台脱硫废水工程师站、4台除尘输灰操作站、2台输煤操作站、1台输煤工程师站、2台辅网工程师站、2台历史站。
3. 辅网车间控制系统数据通过辅网工程师站数据转发至8号控制域接口机，接口机连接电力专用隔离装置数据传输至外网MES系统。
4. 海腾码头输煤管廊控制系统数据通过输煤楼输煤工程师站数据采集转发至辅网控制系统。

# 五、技术要求

# 5.1总的要求

依据等保2.0的一个中心,三重防护的思想,针对DCS控制系统面临的主要安全威胁,部署入侵检测、主机安全软件、工业防火墙、工控安全检测与审计、日志审计、统一管理平台等网络安全设备。分别从安全计算环境、安全通信网络、安全区域边界、安全管理中心四个部分使用相应的防护技术以应对安全威胁,提升网络安全防御能力。投标人负责提供满足招标方4×670t/h+3×150MW汽轮发电机组DCS控制系统控制大区网络安全建设满足等保三级要求所需要的全部硬件、软件、系统改造的附件及辅材、相关安全管理文档等。

# 5.2基本要求

1. 本技术规范书对腾龙芳烃（漳州）有限公司热电厂DCS系统网络安全加固项目所采用的硬件、软件提出技术及相关要求。
2. 本规范书涉及网络安全加固项目的软件系统划分为两部分：即系统软件和应用软件，这两部分软件都由投标方提供。
3. 本技术规范书提出的是最低限度的要求，并未对所有技术细节做出规定（如目前所列的各个子系统并不是最终确定的，投标方可根据自身设计提出更完善的设置)，也未完全陈述与之有关的协议和标准。投标方提供符合本技术规范书和有关工业标准要求的经过实践代表当今先进技术的优质工业网络安全系统和有关设备及材料。
4. 应用软件系统包括投标方自行开发和采用的各种软件系统，即直接用于网络安全管理的软件系统，或为使整个系统更为完善而配置的各种功能软件。

应用软件的主体部分应采用投标方自主开发的B/S结构系统，业务流程基于图形化工作流系统驱动，工作流系统完全为自主知识产权产品而不是第三方软件。应用软件所有业务功能模块基于统一平台、统一登录入口。对非投标方开发的应用软件，投标方应在投标书中进行说明。

1. 设备采购的专利涉及到的全部费用均被认为已包含在设备报价中，投标方应保证需方不承担有关设备专利的一切责任和可能的费用。
2. 投标方提供的进口的硬件应是原产地原产国产品,并附有原产地证明书。所提供的软件(包含数据库应用软件、操作系统在内的第三方软件)应保证正版。并在国内同等级机组上有三年以上的成功运行业绩。
3. 投标方随合同提供的供货清单在执行合同期间的任何减少或更换不同型号规格参数应经过招标方认可。
4. 投标方供货范围内所有设备的选型,均应在投标书中详细列出规格型号、数量、品牌等内容。
5. 投标方必须提供包括但不限于招标规范书要求的网络安全建设全套硬、软件设括备，以及相应的规划、迁移、安装、调试等全部服务。
6. 全面负责供货、安装、调试,包括系统内部的接线,负责其供货范围内所有设备的内部及其连线的设计和供货。
7. 根据本招标文件的要求,提供必须的安装详图和安装指导以及施工图设计、安装调试、培训指导、运行维护所需的全部软件、图纸和竣工资料。
8. 投标方根据招标方要求负责网络安全系统软、硬件的安装、调试、最终整合成一个安全网络系统，直至稳定运行。
9. 本技术规范书作为合同的一个附件，与合同文件具有相同的法律效力。双方共同签署的会议纪要、补充文件等也与合同文件一样具有相同的法律效力。
10. 招标方对本规范书拥有最终解释权。

## 5.3硬件要求

1. 投标方必须根据本项目建设和运行的实际需求，提供合理和必需的设备配置和报价，明确说明每个设备的类型和用途。
2. 投标方所提供的各类设备，所有提供的软、硬件（如接口设备、缆线、软件」控制器等，包括本规范中未列出而系统实施又必需的软件、硬件)需配齐以构成一套实用系统，并在投标设备清单中详细的体现。如果投标方在中标并签署合同后，在供货或系统集成时出现软、硬件的任何遗漏，均必须由中标方免费提供，招标方将不再支付任何费用。
3. 投标方所提供的各类设备其性能必须达到或超过需求中技术指标的要求。
4. 投标方应提供所有投标设备的工作环境说明，包括机房要求、供电功率、空间要求、承重要求等。
5. 投标方所提供的各类设备如需使用特别接头、插座、附件等，由投标方免费提供。另外,所投设备的用电保护如果超过一般线路保护,保护设备也由投标方免费提供。如必须产生费用的附件投标方应将与此有关的费用计入投标价中。
6. 投标方必须提供投标设备的详细配置清单及分项细项报价,性能必须与报价中的详细配置一致。
7. 如果投标方已中标并签署合同,所有设备和材料必须具有原制造厂商的授权证署或许可证,具备原制造厂商的铭牌、标志,招标方将向制造商(生产厂商)进行产品验证。投标方所有设备和材料必须通过合法渠道提供给招标方。本系统中出现的任何涉及非法设备和材料的纠纷,均由投标方承担全部法律责任。

## 5.4软件要求

1. 投标方必须承诺保证提供的所有软件产品为最新正式版本。
2. 投标方必须承诺保证提供的所有软件产品都具有在中国境内的正式合法使用权。所有系统软件必须具有原制造厂商的授权证或许可证，应具有功能、性能参数和使用手册。本系统中出现的任何涉及版权纠纷，均由投标方承担全部法律责任。
3. 投标方必须承诺保证提供的所有软件产品都具有完整的技术资料和介质。
4. 投标方必须给出所有软件产品的价格（或使用权的价格），并给出所有软件产品模块的详细分项报价。如提供的某些技术资料或介质不含在基本报价中，也需另外单独列出报价。
5. 如果投标方已中标并签署合同，所有软件系统必须具有原制造厂商的授权证或许可证，具备原制造厂商的铭牌、标志，招标方将向制造商（生产厂商）进行产品验证。投标方所有软件系统必须通过合法渠道提供给招标方。本系统中出现的任何涉及非法软件系统的纠纷，均由投标方承担全部法律责任。

## 5.5工作范围

投标方提供的网络安全建设必须是成套服务，其范围包括：

* 系统整体规划、方案设计及设备选型;
* 系统工程的施工，包括设备及软件的采购、测试、联调、安装、调测；
* 整个安全系统的测试验收、人员培训、技术支持以及对系统的优化调整;
* 负责进行网络的规划。
* 在现有网络安全环境基础上提出设备升级改造加固方案，并列出报价。
* 完成2022年度集散控制系统DCS等级测评报告所列相关的网络设备加固整改。

## 5.6供货要求

### 5.6.1工控防火墙技术要求

1. 网络层控制

* 包过滤

工控防火墙的包过滤要求如下：

a)安全策略应使用默认禁止原则，即除非明确允许，否则就禁止;

b) 安全策略应包含基于源 IP 地址、目的 IP 地址的访问控制；

c)安全策略应包含基于源端口、目的端口的访问控制；

d)安全策略应包含基于协议类型的访问控制；安全策略应包含基于 MAC 地址的访问控制；

f)应支持用户自定义的安全策略，安全策略可以是 MAC 地址、IP 地址、端口的部分或全部组合。

* NAT

部署域间的工控防火墙应具备NAT功能，具体技术要求如下：

a)应支持双向NAT:SNAT和DNAT:

b)SNAT应至少可实现“多对一”地址转换，使得内部网络主机访问外部网络时，其源IP地址被转换

* 状态检测

工控防火墙应具备状态检测功能，支持基于状态检测技术的访问控制。

a)动态开放端口工控防火墙应具备动态开放端口功能，应至少支持OPC、FTP协议。

b)1P/MAC地址绑定工控防火墙应支持自动或手动绑定IP/MAC地址；应能够检测IP地址盗用事件，拦截盗用IP地址的主机经过工控防火墙的各种访问。

* 抗拒绝服务攻击

工控防火墙应具有抗拒绝服务攻击的能力，具体技术要求如下（包括，但不限于）：

a)ICMP Flood攻击：

b)UDP Flood攻击；

c)SYN Flood攻击：

d)TearDrop攻击；

e)Land攻击；

f)超大ICMP数据攻击。

* 网络扫描防护

工控防火墙应能够检测和记录扫描行为,包括对受保护网络的扫描。

1. 应用层控制

* 应用协议控制工控防火墙应能识别并控制各种应用类型，具体技术要求如下：

a)支持 HTTP、FTP、Telnet 等通用应用层协议；

b)支持常用工业控制协议，如OPC、Modbus TCP、S7协议、Profinet、BACnet、DNP3、IEC104等。

* 工业协议深度内容检测工控防火墙应能对主流工业协议进行深度内容检测，具体技术要求如下：

a)工控协议格式规约检查，禁止不符合协议规约的通信；

b)对工业协议的操作类型、操作对象、操作范围等参数进行控制；

c)至少支持一种主流工控协议。

1. 管理安全

工控防火墙应具备管理安全功能,具体技术要求如下:

a)支持对授权管理员的口令鉴别方式,且口令设置满足安全要求;

b)应在所有授权管理员请求执行任何操作之前,对每个授权管理员进行唯一的身份鉴别;

c)应具有登录失败处理功能,身份鉴别在经过一个可设定的鉴别失败最大次数后,工控防火墙应终止管理主机或用户建立的会话;

d)工控防火墙应为每一位规定的授权管理员提供一套唯一的为执行安全策略所必需的安全属性

1. 管理方式

工控防火墙应具备多种管理方式,具体技术要求如下:

a)应支持进行本地管理工控防火墙;

b)应支持通过网络接口进行远程管理,并可限定可进行远程管理的网络接口;

c)远程管理过程中,管理端与工控防火墙之间的所有通信数据应加密传输。

1. 管理能力

工控防火墙应具备相应的管理能力,具体技术要求如下

a)向授权管理员提供设置和修改安全管理相关的数据参数的功能；

b)向授权管理员提供设置、查询和修改各种安全策略的功能；

c)向授权管理员提供管理审计日志的功能。

1. 安全审计

* 记录事件类型

工控防火墙应具备安全审计功能,记录事件类型要求如下：

a)工控防火墙访间控制策略匹配的访问请求;

b)访问控制策略默认禁止的访问请求,包括试图穿越或到达工控防火墙的访问请求;

c)检测到的攻击行为;

d)试图登录工控防火墙管理端口和管理身份鉴别请求;

e)对工控防火墙系统重要管理配置操作,如增加/删除/修政管理员,保存/删除审计日志,更改安全策略和配置参数等;

f)其他应记录的事件类型。

* 日志内容

工控防火墙应具备安全审计功能,日志内容要求如下

a)事件发生的日期时间,日期应包括年、月、日,时间应包括时,分,秒；

b)访问控制日志应包括数据包的协议类型,源地址、日标地址,源端口、日标端口,允许或禁止；

c)工控协议的深度内容检查信息:

d)管理日志应包括事件主体、事件客体,事件描述

* 日志管理

工控防火墙应具备日志管理功能,具体技术要求如下：

a)应只允许授权审计员对日志进行读取-存档,导出,删除和清空等操作；

b)应提供日志查阅工具,具备对审计事件以时间、旧期、主体标识,客体标识等条件检索的能力；

c)并且只允许授权审计员使用查阅工具;

d)审计事件应存储于掉电非易失性存储介质中,且在存储空间达到阈值时通知授权管理员进行处理。

1. 安全管理

* 工控防火墙的底层支撑系统应满足以下要求:

a)不提供多余的网络服务;

b)不含任何导致产品权限委失,拒绝服务等的安全漏洞。

* 异常处理机制

工控防火墙在非正常关机(比如掉电、强行关机)再重新启动后,应满足如下技术要求：

a)安全策略你复到关机前的状态

b)日志信息不会丢失

c)管理员重新鉴别

1. 高可用性
2. 可用性保障

部署在现场控制层的工控防火墙应具备Bypass功能,当工控防火墙自身出现断电故障时,应使工控防火墙内部接口与外部接口直接物理连通,保持内部网络与外部网络之间的正常通信,并及时告警。

1. 自检功能

工控防火墙应具备一定的自检功能

* 在初始化或启动期间,应能对设备硬件、程序或功能模块、重要配置文件等进行检测,当发现早常时能够及时告警
* 在运行期间,应能在授权管理员的要求下或者周期性的对提供安全功能的模块或进程进行检测,当出现异常时能够及时告警

1. 运行模式

工控防火墙应支持多种运行模式,工控防火墙能够区分部署过程和工作过程,以实现对被防护系统的最小影响,具体技术要求如下：

* 支持学习模式,工控防火墙记录运行过程中经过防火墙的所有策略,资产等信息,形成白名单策略集；
* 支持验证模式或测试模式,该模式下工控防火墙对禁止策略进行告警,但不拦截；
* 支持正常工作模式,工控防火墙的正常工作模式,严格按照防护策略进行过滤等动作保护。

1. 安全策略更新

工控防火墙安全策略应用时不应影响正常的数据通信。

1. 时间同步

工控防火墙应支持与时钟服务器自动同步时间的功能。

1. 电源冗余

部署现场控制层的工控防火墙应提供双电源冗余功能。

1. 散热方式

部署现场控制层的工控防火墙应采用自然散热.无风扇方式设计。

1. 性能要求
2. 吞吐量

工控防火墙在只有一条允许规则和不丢包的情况下，一对相应速率的端口应达到的双向吞吐量指标如下：

部署在域间的工控防火墙：

* + 对64字节短包,百兆工控防火墙应不小于线速的30%,千兆工控防火墙应不小于线速的40%；
  + 对256字节中长包,百兆工控防火墙应不小于线速的70%,千兆工控防火墙应不小于线速的80%；
  + 对512字节长包,百兆工控防火墙应不小于线速的90%,千兆工控防火墙应不小于线速的95%。

部署在现场控制层设备前的工控防火墙:

* 对64字节短包,百兆工控防火墙应不小于线速的10%,千兆工控防火墙应不小于线速的20%;
* 对256字节中长包,百兆工控防火墙应不小于线速的30%,千兆工控防火墙应不小于线速的40%;
* 对512字节长包,百兆工控防火墙应不小于线速的50%,千兆工控防火墙应不小于线速的70%.

1. 延退

延迟视不同速率的工控防火墙有所不同,在吞吐量90%条件下,应满足如下要求：

a)部署在域间的工控防火墙:

* 对64字节短包、256字节中长包、512字节长包,百兆工控防火墙平均延退不应超过1 ms；
* 对64字节短包、256字节中长包、512字节长包,千兆工控防火墙平均延迟不应超过200μs。

b)部署在现场控制层设备前的工控防火墙：

* 对64字节短包、256字节中长包,512字节长包,百兆工控防火墙平均延退不应超过500μs；
* 对64字节短包、256字节中长包、512字节长包,千兆工控防火墙平均延迟不应超过2OOμs。

1. 最大并发连接数

最大并发连接数视不同速率的工控防火墙有所不同,具体指标要求如下：

* 百兆工控防火墙的最大并发连接数应不小于60000个;
* 千兆工控防火墙的最大并发连接数应不小于300000个。

1. 最大连接速率

最大连接速率视不同速率的工控防火墙有所不同,具体指标要求如下：

* + 百兆工控防火墙的最大连接速率应不小于1500个/s;
  + 干兆工控防火墙的最大连接速率应不小于5000个/s。

### 5.6.2入侵检测系统技术要求

1. 数据探测功能
2. 数据收集

应具有实时获取受保护网段内的数据包的能力

1. 协议识别

至少应识别基于以下协议的事件:

* 网络层协议;TCP/IP;
* 应用层协议;ModBus TCP,OPC,S7 等

1. 行为监测

至少应监视以下行为,端口扫描、工程师站组态变更、操作站数据与操作指令变更,以及资产变更通信行为等。

1. 流量监测

应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量,特别是异常流量的监测

1. 协议定义

除支持默认的工控协议集外,支持基于应用的协议自动识别,还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

1. 入侵分析功能
2. 数据分析

应对收集的数据包进行分析,发现攻击事件。

1. 分析方式

应以模式匹配、协议分析等一种或多种方式进行人侵分析。

1. 参数分析

应具备过程状态参数、控制信号的阙值检查功能。

1. 恶意代码识别

应支持恶意代码识别的功能,如对木马、蜗虫等的识别。

1. 防躲避能力

应能发现躲避或欺骗检测的行为,如 TCP流重组、协议端口重定位等。

1. 事件合并

应具有对高频度发生的相同安全事件进行合并告警的功能。

1. 事件关联

应具有将不同的事件关联起来,发现低危害事件中隐含的高危害攻击的能力。

1. 入侵响应功能
2. 安全告警

当检测到人侵时,应自动采取相应动作以发出安全告警。

1. 告警方式

告警方式可以采取界面实时提示、声音告警等方式中一种或多种方式。

1. 报文留存

在监测到网络上的攻击行为时,应具有自动保存攻击报文的能力。

1. 排除响应

应允许管理员定义对被检测网段中指定的主机或特定的事件不予告警。

1. 定制响应

应允许管理员对被检测网段中指定的主机或特定的事件定制不同的响应方式,以对特定的事件突发告警。

1. 管理控制功能
2. 事件数据库

应提供事件数据库,包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

1. 事件分级

应按照事件的严重程度将事件分级,以使授权管理员能从大量信息中捕捉到危险的事件。

1. 策略配置

应提供安全策略配置功能,并支持:

* 对安全策略进行添加、删除、修改和分发；
* 对安全策略进行的导人和导出。

1. 产品升级

应具有及时更新、升级产品和事件库的能力,支持离线升级并保证升级安全。

1. 分布式部署

应具有本地或异地分布式部署、远程管理的能力。

1. 端口分离

探测器应配备不同的端口分别用于产品管理和网络数据监听。

1. 检测结果处理
2. 事件记录

应记录并保存检测到的人侵事件。入侵事件信息应至少包含以下内容:

事件发生时间-源地址、目的地址、危害等级等。

1. 报告生成

应能生成检测结果报告。报告应至少包含事件详细描述、解决方案建议等。

1. 报告模板定制

应具有自定义报告模板的功能。

1. 报告查阅

应具有查询检测结果报告的功能。

1. 报告导出

应具有支持检测结果报告导出的功能。

1. 安全审计
2. 审计日志生成

应对与自身安全相关的下列事件生成审计日志:

* 用户登录成功和失败;
* 对安全策略进行更改;
* 对用户进行增加、删除和属性修改;
* 因鉴别失败的次数超出设定值而导致的会话连接终止；
* 对事件记录,审计日志的操作。

1. 审计日志内容

审计日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果等。若采用远程登录方式对产品进行管理,还应记录管理主机的地址

1. 审计日志查阅

应支持按照一定条件对审计日志进行查阅。

1. 审计日志存储

审计日志应存储于掉电非易失性存储介质中,并满足以下要求:

* 当审计日志存储空间超过阙值时,应能通知用户;
* 当审计日志存储空间将要耗尽时,应采取相应的防止审计数据丢失的技术措施。

### 5.6.3安全管理平台技术要求

1. 安全管理
2. 设备管理

产品应能对运行于工业控制系统中的安全产品进行统一管理,并建立设备清单。设备清单应至少包括设备名称、设备类型、重要程度,所处位置和安全责任人等内容。

1. 状态监测

产品应能够对工业控制系统安全产品的运行状态进行监测,并满足以下要求：

* + 监测频率支持自定义；
  + 监测的运行状态.包括在线状态、系统资源(CPU、内存和硬盘)使用情况等,网络流量等；
  + 支持工业控制系统安全产品网络拓扑图的绘制。

1. 信息收集

产品应能对工业控制系统安全产品的信息进行收集,具体包括;

* + 硬件型号；
  + 软件版本；
  + 审计日志；
  + 安全策略.如工业控制系统人侵检测系统报警策略、工业控制系统防火墙的数据包过滤规则；
  + 工业控制系统网络隔离产品访问控制策略、工业控制系统安全审计产品的审计策略等；
  + 安全配置；
  + 硬件序列号。

1. 策略配置

产品应能够对工业控制系统安全产品的安全策略进行设置,比如工业控制人侵检测系统报警策略、工业控制防火墙的数据包过滤规则、工业控制网络隔离产品访问控制策略、工业控制安全审计产品的审计策略等.并支持以下功能:

* + 对安全策略进行添加、删除,修改和分发；
  + 对安全策略进行导人和导出。

1. 身份鉴别

产品应保证要通过鉴别才能够对工业控制系统安全产品进行管理,并且应保证存储在产品中的鉴别数据不被未授权查阅或修改。

1. 统计分析
2. 安全事件库维护

产品应建立安全事件库,并提供安全事件库的维护功能,具体包括:

* + 安全事件库内容应包括:事件名称,事件类型,事件级别,事件描述和事件特征；
  + 安全事件库支持工业控制协议(MODBUS.OPC等)和工业控制系统的安全事件；
  + 提供开放接口.允许用户自定义安全事件；
  + 应提供安全事件库升级功能

1. 安全事件分析

产品应能对收集的审计日志进行分析,从中提取安全事件。

1. 统计分析报表
   * 产品应能够对安全事件进行统计.并生成汇总报表,并满足报表应能够以通用格式(例如html.pdf或doc)导出;
   * 报表应包含文字、图、表等表现形式。
2. 潜在危害分析

产品应能设定单类事件累计发生次数或发生频率的闽值,当统计分析表明此类事件超出闽值时，则表明工业控制系统出现了潜在的危害。

1. 异常行为分析

产品应能对工业控制系统中的异常行为进行分析

1. 关联事件分析

产品应能制定关联分析规则.并基于不同的规则对不同设备上报的审计日志进行关联分析。

1. 管理安全
2. 安全角色管理

产品应能通过对授权管理员给以不同的管理角色.赋予授权管理员不同的管理权限。

1. 管理方式

产品应支持本地管理。若提供远程管理方式,产品应能满足以下要求：

* 对可远程管理主机的IP地址进行限制；
* 对可远程管理主机的MAC地址进行限制；
* 远程管理接口可由管理员关闭。

1. 数据保护
2. 数据存储保护

产品应能对存储的重要数据进行保护,以免被非授权访问。这些重要数据至少包括：

* 用户及工业控制系统安全产品的鉴别信息;
* 工业控制系统安全产品的审计日志,安全配置和安全策略等。

1. 数据传输保护

产品应采取安全措施保护重要数据在传输过程中不被泄露和窃取。这些重要数据至少包括：

* 用户及工业控制系统安全产品的鉴划信息；
* 工业控制系统安全产品的安全配置和安全策略等。

1. 数据备份和恢复

产品应提供重要数据的备份和恢复功能,这些重要数据包括:

* 工业控制系统安全产品的安全配置；
* 安全策略和审计日志等。

1. 端口分离

产品应配备不同的端口分别用于产品管理和信息收集。

1. 安全审计
2. 系统日志生成

产品应对与自身安全相关的下列事件生成审计日志:

* 用户登录成功和失败；
* 对安全策略进行更改；
* 对用户进行增加、删除和属性修政；
* 因鉴别失败的次数超出了设定值.导致的会话连接终小；
* 对事件记录,审计日志的操作。

1. 系统日志内容

产品的系统日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果、若采用远程登录方式对产品进行管理.还应记录管理主机的地址。

1. 审计日志查阅

产品应提供多条件查阅工具,对系统日志和收集的审计日志进行查询

1. 审计日志存储

产品的审计日志应存储于掉电非易失性存储介质中.并满足以下要求：

a)当审计日志存储空间超过阈值时,应能通知用户;

b)当审计日志存储空间将要耗尽时,应采取相应的防小审计数据丢失的技术措施。

### 5.6.4网络监测审计系统技术要求

1. 安全功能要求
2. 审计数据采集

产品应支持基于策略的数据采集;

* 支持基于网络层要素的数据采集策略;至少包括源目的MAC或源目的IP,传输层协议、目的端口；
* 支持基于工业控制协议的数据采集策略。

1. 审计数据生成

产品应在实际的系统环境和网络带宽下及时生成审计数据

1. 审计数据还原

* 网络层通信协议还原

产品应支持对网络层通信协议的数据进行还原,至少包括源目的 MAC,源目的IP,传输层协议,源目的端口,应用层协议。

* 应用协议还原

产品应支持对HTTP、FTP-TELNET协议的应用数据还原：

HTTP通信,目标URL；

FTP通信,使用的账号,输人命令；

TELNET通信:使用的账号,输人命令。

* 工业控制协议还原

产品应支持对工业控制协议应用数据进行分析和还原,支持至少一种工业控制协议。至少支持组态变更,包括上传,下载，指令变更,包括写指令及相关参数,如控制点位地址、控制值等。

1. 审计事件识别和分析

基于白名单规则分析

1. 白名单规则定义

产品应支持白名单规则的定义;

* 网络通信白名单:支持基于1P或MAC等要求进行规制定义
* 工业控制协议通信白名单:支持基于控制命令,控制点位,控制值等要素进行规则定义。

1. 白名单方式识别

产品应支持基于白名单机制对审计信息的识别。

1. 异常事件识别

产品应支持对以下异常事件的识别

* 网络中出现IP或MAC白名单之外的设备;
* 工业控制协议通信出现异常的控制命令、控制点位,控制值。

1. 审计记录
2. 记录内容

产品应按照事件的分类和级别,生成包含以下内容的审计记录

* 事件主体;
* 事件客体;
* 事件发生的日期和时间;
* 事件类型；
* 事件的级别。
* 审计源身份(分布式产品);
* 事件的描述;
* 工业控制协议的深度解析内容,至少包括控制命令,控制点位,控制值

1. 事件分类

产品应对事件按用户可理解的方式进行分类,方便用户浏览和策略定制。如按事件的潜在风险分类,正常事件,异常事件;按协议类型分类等。

1. 事件分级

产品应将异常事件可能的潜在危害程度划分为不同的级别,对不同级别的事件采取不同的处理方式。

1. 数据库支持

产品应支持一种数据库管理软件,用于存储审计记录,方便用户查阅,检索和统计分析。

1. 事件响应和报警
2. 事件告警

产品应能对系统安全策略定义的不同等级的事件采取不同方式进行告警。

1. 告警方式

产品应产生报警,响应报警方式至少包含以下方式中的一种：

* 管理界面告警；
* 向网管中心发送SNMP Trap报警消息；
* 向声光电发生装置发送启动信号；
* 向网管人员发送SMS报警短消息。

1. 审计查阅和报表
2. 常规查阅

产品应提供查阅审计记录的工具,查阅的结果应以用户易于理解的方式和格式提供,并且能支持导出及打印。

1. 有限查阅

产品应确保除授权管理员之外,其他用户无权对审计记录进行查阅。

1. 可选查阅

产品应为授权管理员提供将审计记录按一定的条件进行选择,搜索,分类和排序的功能,所得结果应以用户友好的、便于理解的形式提供报告或打印。

1. 审计报表

报表生成器将审计分析器传来的分析结果进行数据汇总报表输出,对报表至少有以下要求：

* 产品应提供审计报表模板,能够基于模板生成审计报表；
* 报告内容应至少支持文字、图像两种描述方式；
* 审计数据报告生成格式应至少支持txt\html\doc\xls\pdf等通用文件格式中的一种。

1. 审计记录存储
2. 存储安全

产品应提供安全机制保护审计记录数据免遭未经授权的删除或修改,如采取严格的身份鉴别机制和适合的文件读写权限等。任何对审计记录数据的删除或修改都应生成系统自身安全审计记录。应对审计记录进行完整性保护。

1. 存储空间耗尽处理

产品应提供数据存储空间耗尽处理功能,当剩余存储空间达到预定义的阈值时进行告警。

1. 安全管理
2. 接口及管理安全

产品应保证业务接口,管理接口-管理界面的安全:

* 业务接口和管理接口采用不同的网络接口；
* 业务接口采取被动收包方式工作,不得外发数据包；
* 管理接口及管理界面不存在中高风阶安全漏洞。

1. 管理信息传输安全

产品需要通过网络进行管理时,产品应能对管理信息进行保密传输

1. 安全状态监测

产品应能够监测产品自身及组件状态,包括对产品 CPU,内存,存储空间等系统资源使用状态进行监测。

1. 时间同步

产品及组件应支持以下时间同步功能：

1. 若由多个组件组成,各组件支持与审计中心进行时间同步；
2. 审计中心支持与外部时间服务器进行时间同步。
3. 审计日志
4. 审计日志生成

产品应对与自身安全相关的以下事件生成审计日志：

* 身份鉴别.包括成功和失败；
* 因鉴别失败次数超过了阈值而采取的禁止进一步尝试的措施；
* 审计策略的增加、删除-修改。

1. 审计日志内容

审计日志内容至少应包括日期,时间、事件主体、事件客体、事件描述等

1. 审计日志存储

产品应将自身审计日志与审计记录分开保存到不同的记录文件或数据库(或同一数据库的不同表)中.方便用户查阅和分析。应保证自身审计日志存储的最短期限不少于6个月。

### 5.6.5日志审计与分析技术要求

1. 日志采集和存储
2. 日志数据源

日志分析产品应能对日志数据源进行添加、修改和删除等管理操作，并且日志数据源的类型应至少包含以下范围:

* 网络设备，如交换机、路由器、防火墙；
* 操作系统；
* 数据库系统；
* 其他应用系统。

1. 日志数据采集

数据采集

日志分析产品应能通过一定的方式采集日志数据源的日志数据，至少包括以下一种采集方式：

* 日志代理；
* 标准协议；
* 文件导入；
* 其他。

1. 日志采集及时性

日志分析产品应能及时采集日志数据源的日志数据。

1. 日志数据的预处理
2. 数据筛选

日志分析产品应能基于既定策略对采集的日志数据进行过滤，有选择地生成日志记录。

1. 数据转换

日志分析产品应能将各种不同格式的原始日志数据转换为统一的数据格式,且转换时不能造成关键

数据项丢失和损坏

1. 日志记录生成

日志分析产品应在对采集的日志数据进行预处理和事件分析之后，生成相应的日志记录，日志记录内容应为管理员可理解，并且包含以下信息:

* 事件发生的日期和时间；
* 事件主体；
* 事件客体；
* 事件描述；
* 事件类型；
* 事件级别；
* 日志数据源的D地址、MAC或名称。

1. 日志记录存储

安全保护

日志分析产品应采取安全机制，保护日志记录免遭未经授权的读取、删除或修改。

1. 防止日志记录丢失

日志分析产品应提供以下措施防止日志记录丢失:

* 日志记录应存储于掉电非易失性存储介质中；
* 当日志记录的存储容量达到闽值时，发出报警信息；
* 在月末记录的存储空间择足前自动将较早日末记录转存到其他设备上。

1. 日志记录备份

日志分析产品应提供以下日志记录备份功能

1. 支持可定制的自动化备份功能及策略;
2. 通过自动方式对日志记录进行转存，实现异地备份。
3. 日志记录处理
4. 数据整合

日志分析产品应能检查日志记录是否重复或无效，并进行数据的整合

1. 数据拆分

若日志记录的单一字段包含多种信息并且这多种信息间具有分隔符,日志分析产品应能将此单一字段拆分成便于分析的若干字段存储。

1. 日志记录分析
2. 事件辨别

日志分析产品应能动态地维护一个事件库，对网络中的各种事件根据一定的特征进行分类，并且应能对采集的日志数据进行分析，判断日志数据所属的事件类型。

1. 事件定级

日志分析产品应为不同类型的事件设定其级别,以表明事件的性质或揭示此类事件的发生给信息系统所带来危险程度。

1. 事件统计

日志分析产品应能够根据事件的以下属性进行统计：

* 事件主体；
* 事件客体；
* 事件类型；
* 事件级别；
* 事件发生的日期和时间；
* 日志数据源的IP地址或名称；
* 事件的其他属性或属性的组合。

1. 潜在危害分析

日志分析产品应能设定单类事件累计发生次数或发生频率的阈值,当统计分析表明此类事件超出阈值时则表明信息系统出现了潜在的危害。

1. 异常行为分析

日志分析产品应维护一个与信息系统相关的合法用户的正常行为集合,以此区分入侵者的行为和合法用户的异常行为。

1. 关联事件分析

日志分析产品应提供以下关联分析功能：

* 根据事件的级别、事件的累计发生次数等指标进行综合分析，从而对信息系统或信息系统中单个资源的风险等级进行评估；
* 通过对多个日志数据源进行关联事件分析应能分析到多步访问行为，并能根据已知的事件序列以图示方法模拟出完整的访问路径。

1. 日志记录数据挖掘

日志分析产品应能够从大量的日志数据中提取隐育的、事先未知的、具有潜在价值的有用信息和知识，具体要求如下：

* 提取同一类型的事件的共同性质，如事件频繁发生的时间段等；
* 想取单个事件和其他事件之间依赖或关联的知识。如事件发生的因果关系等；
* 提取反映相关事件共同性质的特征和不同事件之间的差异型特征，揭示隐含事件的发生；
* 发现其他类型的知识，揭示偏离常规的异常现象;
* 根据数据的时间序列，由历史的和当前的数据去推测未来的数据，比如分析某一目标系统的用户访问目志，从中寻找用户普遍访问的规律。

1. 日志查询

日志分析产品应能够根据事件的以下属性进行日志记录查询:

1. 事件主体；
2. 事件客体；
3. 事件类型；
4. 事件级制；
5. 事件发生的日期和时间；
6. 日志数据源的地址或名称；
7. 事件的其他属性或属性的组合。
8. 统计报表

日志分析产品应能够根据事件统计结果生成统计报表，并能以通用格式输出。

1. 分析报告

日志分析产品应能根据日志记录分析结果生成分析报告，并能够以通用格式输出，分析报告应包含以下内容:

1. 日志记录分析结果；
2. 对信息系统或信息系统中单个资源的风险等级提供评估结果；
3. 对日志记录分析结果提供补救建议；
4. 根据日志数据挖倔收集到的知识、提供预测性的信息。
5. 报警机制

日志分析产品应能针对以下事件，进行报警：

1. 用户指定的事件，如高危险级别的事件等；
2. 在危害分析结果表明信息系统存在潜在危害；
3. 异常行为分析结果表明信息系统存在入侵者的行为或合法用户的异常行为；
4. 日志记录分析结果表明信息系统或信息系统中某一资源存在风险。

### 5.6.6主机安全防护技术要求

1. 访问控制

针对主体、客体以及主客体之间的所有操作，产品应能够执行以下访问控制策略:

1. 支持根据主体 (如:访问用户等) 、客体 (如:被防护主机等)、访问权限设置访问控制策略;
2. 主客体之间发送和接收的信息流均经过安全策略允许后传输;
3. 主体访问权限至少包括:被防护主机管理权限、审计数据查询、访问控制策略等
4. 操作行为审计与监控
5. 操作行为审计

产品应记录操作行为，包括但不限于:

* 提供工业控制系统主机图形化实时监视功能；
* 记录工业控制系统主机通过键盘、鼠标进行输入的操作行为；
* 记录工业控制系统主体通过移动存储交换介质进行数据交换的操作行为；
* 记录工业控制系统主机通过网络进行运维管理的操作行为。

1. 操作行为响应

产品应对违反访问控制策略的操作行为进行响应，如日志审计、对话框报警等响应策略。

1. 操作事件回溯

产品应支持操作事件回溯，包括：

* 支持回溯用户通过移动存储交换介质进行数据交换的过程；
* 支持选择指定节点进行回溯操作，并可按事件发生时间、审计事件类别、主体、客体等进行查询。

1. 实时监控

产品应支持实时监控功能，包括:

* 对被防护主机当前登录状态进行实时监控，当有访问人员登录时，能及时发现;
* 对安全防护装置进行实时监控，当出现故障时断开时，能及时发现。

1. 数据安全交换
2. 摆渡式数据安全交换

产品应支持摆渡式数据安全交换，在主体执行数据拷贝操作时，应通过身份鉴别，利用移动存储介质和安全防护装置进行数据摆渡操作。

1. 数据封装

产品应支持对拷入移动存储介质中的数据进行数据封装操作。

1. 恶意代码防御

产品应支持恶意代码防御功能,对外部拷入的数据进行恶意代码查杀,支持恶意代码库的手动升级。

1. 安全审计
2. 自身审计数据生成

产品应对下列可审计事件生成一个审计记录:

* 管理员的登录和退出；
* 对安全策略进行更改的操作；
* 对管理员进行增加、删除和属性修改的操作；
* 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；
* 安全防护装置与安全防护平台状态日志；
* 对其他安全功能配置参数的修改 (设置和更新)，无论成功与否；
* 对于每一个审计记录，产品应至少记录以下信息:事件发生的日期和时间、事件类型、主体身份和事件结果 (成功或失败) 等。

1. 安全管理功能

如果产品支持远程管理，应能通过加密的方式来保护远程管理会话内容不被非授权获取。

1. 网络性能要求

产品不能影响工业控制系统原有网络设备和主机的功能，并且不能对原网络系统产生明显的影响。

### 5.6.7漏洞检测产品技术要求

1. 工业控制设备识别

漏洞检测产品应能自动识别工业控制设备。

漏洞检测产品应支持手动添加工业控制设备。

1. 工业控制设备端口扫描

漏洞检测产品应能扫描所有TCP端口,检查其是否开启。

漏洞检测产品应能扫描所有UDP端口,检查其是否开启。

对于已开启的TCP、UDP端口,漏洞检测产品应能判断出与之对应的公开的工业控制通信协议。

1. 工业控制设备通信协议漏洞检测

漏洞检测产品应能检测体用(包括但不限于)以下通信协议的工业控制设各的已知漏洞：

1. 工业以太网协议:Modbus/TCP协议,OPC协议,DNPS.0协议、IEC-60870-5-104 协议、IEC61850 MMS协议,Siemens S7Comm 协议,PROFINET协议,IEC-61850 GOOSE协议,IEC61850 SV协议,EtherNet/IP协议；
2. 互联网协议,HTTP协议,FTP协议,TELNET协议,SNMP协议；
3. 串口协议.Modbus RTU协议,IEC-60870-5-101协议；
4. 私有协议(包括行业专业协议)。
5. 工业控制组态软件漏洞检测

漏洞检测产品应能检测工业控制组态软件的已知漏洞。

1. 工业控制设备操作系统检测

漏洞检测产品应能检测工业控制设备操作系统的安全问题,检测项目应包括但不限于以下内容：

1. 操作系统类型和版本号识别
2. 操作系统登录弱口令检测:
3. 操作系统已知安全漏洞检测
4. 工业控制数据库漏洞检测

漏洞检测产品应能检测工业控制数据库的已知漏洞

1. 工业控制网络通信设备漏洞检测

漏洞检测产品应能检测工业控制网络通信设备(例如,工业交换机等)的已知漏洞。

1. 检测结果处理要求

漏洞检测产品应能满足以下要求;

1. 漏洞检测产品应能实时查看检测进度
2. 漏洞检测产品应能实时查看测试用例的执行方法和每一方法的结果
3. 漏洞检测产品应能监测工业控制设备的实时响应
4. 检测任务应能随时暂停或者终止.
5. 漏洞检测产品应能保存检测结果
6. 漏洞检测产品应能记录并追溯导致工业控制设备异常的数据报文,
7. 漏洞检测产品应能根据检测结果自动生成检测报告。检测报告应包括但不限于以下内容：

* 工业控制设备的信息列表,包括设备类型、固件版本-操作系统版本等。
* 漏洞的名称、漏洞编号、发布日期等。
* 潜在的漏洞。
* 被测设备的危险等级评估,明确标出扫描出的漏洞的危险等级。

1. 检测报告应以通用文档格式(例如,WPS,DOC,TXT,RTF,PDF,HTML等)输出。
2. 测试过程异常终止时,漏洞检测产品应能生成已检测部分的报告,并说明测试过程异常终止。
3. 管理控制功能要求

漏洞粉测产品应能满足以下要求，

1. 漏洞检测产品应能针对不同的工业控制设备和系统设置相应的检测参数(例如,扫描地址范围,端口范围,漏洞类型,测试报文、测试次数,测试时间间隔等)。
2. 漏洞检测产品应支持以下测试方式:

* 依据工业控制通信协议将测试用例进行归类:
* 支持测试用例随机组合;
* 支持测试集合随机组合:
* 支持用户编写测试用例;
* 根据设备类型向用户推荐某类或某几类测试用例。

1. 漏洞粉测产品方内皆工业控制设备信息库并允许更新。
2. 漏洞检测产品应内置漏洞库。
3. 漏洞检测产品应能通过产品升级等方式更新漏洞库,添加新发现的安全漏洞。
4. 漏洞检测产品应内置测试用例库,包含测试用例和测试集合,用于检测已知漏洞和发现未知漏洞。

## 5.7工程量清单

不限以下产品和数量要求，需满足现场设备使用要求。（须在近3年电力行业中有5家以上单位应用过的成熟产品），完全满足第三方等保测评要求（2022年度测评情况如附件）。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 规格型号  （或内容描述） | 单位 | 数量 | 备注 |
| 1 | 工控（边界）防火墙 |  | 台 | 4 | 其中一台防火墙提供辅网控制系统的网络地址转换接入安全管理平台 |
| 2 | 入侵检测系统 |  | 套 | 1 |  |
| 3 | 安全管理平台 |  | 套 | 1 |  |
| 4 | 网络监测审计系统 |  | 套 | 1 |  |
| 5 | 日志审计与分析系统 |  | 套 | 1 |  |
| 6 | 主机安全防护产品 |  | 套 | 52 | 含主机加固及漏洞修复。 |
| 7 | 漏洞检测系统 |  | 套 | 1 |  |
| 8 | 电力专用网络安全隔离装置 | 正向单比特版 | 套 | 1 | 经福建省电力检测认证 |
| 9 | 调试计算机 | i7/32GB/512GB/T600/14英寸LED显示屏/鼠标 | 台 | 1 |  |
| 10 | 机柜 | 含PDU电源分配单元等 | 个 | 1 | 所有安全设备进行统一安装部署在机柜内。 |
| 11 | 彩色激光打印机 | A4 | 台 | 1 |  |
| 12 | 网络辅材 | 网线、水晶头RJ45等安装附件 | 批 | 1 |  |
| 13 | 安全认证U盘 | 32GB | 个 | 6 |  |
| 14 | 工程师站玻璃门电子门禁系统 | 支持IC、NFC等。 | 项 | 1 | 含安装、调试。 |
| 15 | 安全管理体系建设 |  | 项 | 1 |  |

## 5.8项目资料

### 5.8.1一般要求

1. 卖方提供的资料应使用国际单位制，语言为中文。其中提供的图纸须同时提供AUTOCAD电子版本。
2. 资料的组织结构清晰、逻辑性强。资料内容要正确、准确、一致、清晰完整，满足工程要求。
3. 卖方资料的提交及时充分，满足工程进度要求。在接到预中标通知后2周内提供满足设计要求的技术资料。
4. 卖方提供的技术资料一般可分类为1）配合工程设计资料；2）设备监造检验资料；3）施工、调试、试运、性能验收试验资料；4）运行维护资料等4类。卖方所提供的资料须满足工程各阶段的具体要求。本工程采用国家标准《电厂标识系统编码标准》（GB 50549-2010）标识系统。卖方在中标后提供的技术资料都应采用标识编码。具体标识要求由买卖双方讨论确定。
5. 对于其它没有列入合同技术资料清单，却是工程所必需的文件和资料，一经发现，卖方也应及时免费提供。
6. 卖方要及时提供与合同设备设计制造有关的资料。
7. 卖方提供的技术资料的数量双方沟通确定。
8. 卖方必须确保以上条款所确定的图纸资料的交付进度,卖方对买方来往信函、确认文件必须在3个工作日内作出反应,对确认文件在3个工作日内未作出确认，逾期视为自然确认。

### 5.8.2资料提交的基本要求

1. 配合工程设计的资料图纸

卖方应及时提供满足工程设计、安装和调试所需的资料和图纸，

1. 设备监造检查所需要的技术资料

卖方应提供满足合同设备监造检查/见证所需要的全部技术资料。

1. 施工、调试、试运、机组性能试验和运行维护所需要的技术资料（包括但不限于此）
2. 提供设备安装、运行、调试和试运说明书，以及组装、拆卸时所需要的技术资料。
3. 安装、运行、维护、检修所需的详尽图纸和技术资料（包括设备总图、部件总图、分图和必要的零件图、计算资料）。
4. 设备安装、运行、维护、检修说明书（包括设备结构特点、安装程序和工艺要求、启动调试要领、运行操作规定和控制数据、定期校验和维护说明等）。
5. 卖方须提供备品备件清单和易损零件图。
6. 卖方提供的其它技术资料（包括但不限于此）
7. 检查记录、试验报告及质量合格等出厂报告。
8. 卖方提供在设计、制造时所遵循的规范、标准和规定清单。
9. 设备和备品管理资料文件（包括设备和备品发运和装箱的详细资料，设备和备品存放与保管技术要求，运输超重超大件的明细表和外形图）。
10. 详细的产品质量文件（包括材质、材质检查、焊接、热处理、加工质量、外形尺寸和性能试验等）。
11. 进口设备、部件的原产地证明。

## 5.9项目实施要求

### 5.9.1项目计划以及实施方法

投标人需要编制明确的里程碑计划，制定实能计划，明确项目范围、项目实

施方案、项目进度、项目质量标准、项目投入的人天数以及调研时间，作为评标的重要依据。

投标人应建立实施组织架构，结合项目团队和时间表在要求的时间框架下完成项目，具体应包括:

1. 详细阐述本项目的组织机构、职责，投标人拟派出的人员，以及对招标人组织和人员构成的建议；
2. 项目的实施步骤、阶段性成果及最终成果；
3. 项目计划的执行和推进所需的手段及保障措施；
4. 对变更的处理机制；
5. 项目文档管理机制；
6. 项目采用的系统上线策略、方案的详细说明；
7. 对争议的处理机制。

### 5.9.2项目人员要求

1. 投标方服务人员的一切费用己包含在合同总价中，它包括请如服务人员的工资及各种补助、交通费、通讯费、食宿费、医疗费、各种保险费、各种税费等
2. 现场服务人员的工作时间满足现场运行的要求。招标方不再因投标方现场服务人员的加班和节假日而另付费用。
3. 未经招标方同意，投标方不随意更换现场服务人员。同时，投标方及时更换招标方认为不合格的投标方现场服务人员。
4. 下述现场服务表中的天数均为现场服务人员人天数
5. 现场服务计划表 (投标方填写)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目内容 | 计划天数/人 | 人员职称 | 人数 | 备注 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 5.10技术服务和培训

1. 为使设备能正常安装和运行，卖方有责任提供相应的技术培训。培训内容应与工程进度相一致。
2. 培训计划和内容由卖方在技术协议中列出。
3. 培训的时间、人数、地点等具体内容由买卖双方商定。
4. 卖方为买方培训人员提供设备、场地、资料等培训条件。

**六、保密要求**

任何一方未经许可禁止泄露本协议、合同所涉及商业、技术、业务等秘密，

本协议、合同条款之时效不受本协议有效期的影响，本协议有效期年满5年

后该保密条款仍然有效。

**七、工期要求**

合同签订后，投标方应在60日内完成。

**八、差异表**

投标方要将投标文件和招标文件的差异之处汇集成表。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 招标文件 | | | 投标文件 | |
| 条目 | 简要内容 | 条目 | | 简要内容 |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |

备注：投标方如对本规范书有偏差（无论多少或微小）都必须清楚地表示在本规范书的附件“差异表”中。否则招标方将认为投标方完全接受和同意本招标文件的要求，擅自修改招标文件而为清除表示差异的条款均视为无效。

**附件一：2022年三级等保测评报告主要问题摘要**

主要安全问题及整改建议经过单项测评结果判定和整体测评发现，23个中风险和1个低风险。集散控制系统DCS存在的主要问题及整改建议如下：

**1、安全物理环境**

1）**中风险，不具备自动灭火的能力。**

建议对机房设置火灾自动消防系统，实现自动检测火情、自动报警，并自动灭火。涉及测评对象:脱硫电子间、公用电子间、#4炉电子间、#3炉电子间、#3机电子间、#2炉电子间、#2机电子间、#1炉电子间、#1机电子间。

2）**中风险，机房内未部署机房专用精密空调，使用家用空调进行温度控制，不具备恒温恒湿功能。**

建议更换机房中的家用空调为机房专用恒温恒湿精密空调，以保证各区域内温湿度恒定。涉及测评对象:脱硫电子间、公用电子间、#4炉电子间、#3炉电子间、#3机电子间、#2炉电子间、#2机电子间、#1炉电子间、#1机电子间。

**2、安全通信网络**

**1）中风险，未采用密码技术保证通信过程中数据的完整性。**

建议对重要数据采用密码技术保证通信过程中数据的完整性。涉及测评对象：安全通信网络。

**2）中风险，未采用密码技术保证通信过程中数据的保密性。**

建议对重要数据采用密码技术保证通信过程中数据的保密性。涉及测评对象：安全通信网络。

**3）低风险，未基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证。**

建议基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警。涉及测评对象:安全通信网络。

**3、安全区域边界**

1）**中风险，未采用技术手段对非授权设备私自联到内部网络的行为进行检查或限制。**

建议部署准入控制系统防范非法内联行为。涉及测评对象:安全区域边界。

2）**中风险，未采用技术手段对内部用户非授权联到外部网络的行为进行检查或限制。**

建议部署终端安全管控系统对非法外联行为进行检查和限制。涉及测评对象：安全区域边界。

**3）中风险，未部署应用层访问控制设备，未能对进出网络的数据流实现基于应用协议和应用内容的访问控制。**

建议在网络边界处部署应用层防护设备，并开启内容过滤策略防范应用层面的攻击。涉及测评对象:安全区域边界。

4）**中风险，无法对内部发起的网络攻击行为进行检测限制。**

建议在网络中部署入侵防御系统，对从内部发起的网络攻击行为进行检测、防止或限制。涉及测评对象:安全区域边界。

**5）中风险，网络中未部署相关安全防范设备，无法对新型网络攻击行为进行分析和检查。**

建议部署抗APT攻击的系统或设备对高级持续威胁进行防范。涉及测评对象：安全区域边界。

**6）中风险，网络中未部署恶意代码防范系统，无法对恶意代码进行检测和清除。**

建议部署恶意代码防范设备对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。涉及测评对象:安全区域边界。

**4、安全计算环境**

**1）中风险，未配置口令复杂度策略和口令有效期策略。**

建议配置口令的复杂度策略及有效期策略，防止口令被轻易破解(建议口令长度不小于8位，至少包含小写字母、大写字母、数字、特殊符号中的3种，口令有效期不超过90天）。涉及测评对象:公用交换机B网、汽机交换机A网-1、汽机交换机A网-2、汽机交换机A网-3、汽机交换机B网-1、汽机交换机B网-2、汽机交换机B网-3、辅网交换机-1、辅网交换机-2、锅炉交换机A网-1、锅炉交换机A网-2、锅炉交换机A网-3、锅炉交换机A网-4、锅炉交换机B网-1、锅炉交换机B网-2、锅炉交换机B网-3、锅炉交换机B网-4、NT6000分散控制系统、正向隔离装置、DCS交换机-1、DCS交换机-2、公用交换机 A 网。

**2）中风险，登录连接超时策略时间过长，且未配置登录失败锁定策略。**

建议配置登录失败处理策略，防止恶意人员暴力破解账户口令；并配置登录连接超时策略，降低设备被非授权访问的风险(建议登录连接超时时间不超过30分钟）。涉及测评对象：锅炉交换机A 网-3、锅炉交换机A网-2、锅炉交换机A网-1、辅网交换机-2、辅网交换机-1、汽机交换机B网-3、汽机交换机B网-2、汽机交换机B网-1、汽机交换机A网-3、汽机交换机A网-2、汽机交换机A网-1、公用交换机B网、公用交换机A网、DCS交换机-2、DCS交换机-1、锅炉交换机B网-4、锅炉交换机B网-3、锅炉交换机B网-2、锅炉交换机 B网-1、锅炉交换机A 网-4。

**3）中风险，未配置登录失败处理策略及登录连接超时策略。**

建议配置登录失败处理策略，防止恶意人员暴力破解账户口令;并配置登录连接超时策略，降低设备被非授权访问的风险(建议登录连接超时时间不超过30分钟）。涉及测评对象:正向隔离装置、NT6000分散控制系统。

**4）中风险，未严格限制系统默认账户的访问权限。**

建议严格限制默认账户访问权限，或锁定系统无用默认账户。涉及测评对象:辅网历史站-2、辅网历史站-1、汽机工程师站3(3号汽机）、汽机工程师站2(2号汽机）、汽机工程师站1 (1号汽机）、内网接口机、DCS工程师站2、 DCS工程师站-1、DCS历史站-2、DCS历史站-1、DCS值长站-2、DCS值长站-1、锅炉工程师站4 (4号炉）、锅炉工程师站3 (3号炉）、锅炉工程师站2(2号炉）、锅炉工程师站1(1号炉）、辅网工程师站-3、辅网工程师站-2、辅网工程师站-1。

**5）中风险，未对登录的用户分配合理的账户和权限。**

建议对登录的用户分配合理的账户和权限。涉及测评对象：正向隔离装置。

**6）中风险，存在默认账户。**

建议锁定或删除默认账户。涉及测评对象:DCS交换机-2、公用交换机A网、公用交换机 B 网、汽机交换机 A 网-1、汽机交换机 A 网-2、汽机交换机 A网-3、汽机交换机B网-1、汽机交换机B网-2、汽机交换机B网-3、辅网交换机-1、辅网交换机-2、锅炉交换机A网-1、锅炉交换机A网-2、锅炉交换机A网-3、锅炉交换机A网-4、锅炉交换机B网-1、锅炉交换机B网-2、锅炉交换机B网-3、锅炉交换机B网-4、DCS值长站-1、DCS值长站-2、DCS历史站1、DCS历史站-2、DCS工程师站-1、DCS工程师站-2、公用操作员站、内网接口机、汽机工程师站1(1号汽机）、汽机工程师站2(2号汽机）、汽机工程师1站3(3 号汽机）、汽机操作员站1(1号汽机）、汽机操作员站6(3号汽机）、辅网历史站-1、辅网历史站-2、辅网工程师站-1、辅网工程师站-2、辅网工程师站-3、辅网操作员站-1、辅网操作员站-2、锅炉工程师站1(1号炉）、锅炉工程师站2(2号炉）、锅炉工程师站3(3号炉）、锅炉工程师站4 (4号炉）、锅炉操作员站8(4号炉）、锅炉操作员站(1号炉）、DCS交换机-1。

**5、安全管理中心**

**1）中风险，未部署集中管理设备，无法实现只允许系统管理员通过集中管理设备进行系统管理操作**。

建议部署集中管理设备，所有设备均配置系统管理员，且只允许系统管理员通过集中管理设备进行系统管理操作。涉及测评对象:安全管理中心。

**2）中风险，未部署集中管理设备，无法实现只允许审计管理员通过集中管理设备进行系统审计操作。**

建议部署集中管理设备，所有设备均配置审计管理员，且只允许审计管理员通过集中管理设备进行系统审计操作。涉及测评对象:安全管理中心。

**3）中风险，未部署集中管理设备，无法实现只允许安全管理员通过集中管理设备进行安全管理操作。**

建议部署集中管理设备，所有设备均配置安全管理员，且只允许安全管理员通过集中管理设备进行安全管理操作。涉及测评对象：安全管理中心。

**4）中风险，未划分安全管理区，未实现对安全设备及安全组件的统一管控。**

建议划分出安全管理区域对设备进行集中管理。涉及测评对象：安全管理中心。

**5）中风险，未部署综合网管系统，无法对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。**

建议部署综合网管系统对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测，当网络链路、安全设备、网络设备和服务器等的工作状态超过阈值时实时报警。涉及测评对象：安全管理中心。

**6）中风险，未能实现所有设备审计日志的集中分析。**

建议部署综合安全审计系统对各个设备的审计数据进行收集和分析，审计数据保存时间满足6个月以上。涉及测评对象：安全管理中心。

6、**安全建设管理**

**1）中风险，系统上线前测试中未包含安全性测试内容，同时也未实施过密码应用安全性测评工作。**

建议系统在系统上线前依据测试方案对系统进行安全性测试验收。涉及测评对象：安全建设管理。