**招标文件**

**项目名称：** 工控网络安全建设

**计划令号：** GJ2023073-LS

**招标单位**： 贵州航天林泉电机有限公司

**第一部分投标邀请**

**贵州航天林泉电机有限公司**（以下称“招标人”）对**工控网络安全建设**项目进行招标。招标情况如下：

1. 招标货物名称：工控网络安全建设
2. 数量：1
3. 主要技术规格：见本招标文件第二部分
4. 交货地点：招标人指定
5. 商务材料：营业执照、纳税证明、相关资质证明、业绩证明材料、交货周期、售后服务等
6. 投标截止时间：2023年12月20日下午2：00时（北京时间），逾期收

到或不符合规定的投标文件恕不接受

1. 开标时间、地点：投标截止后一周于贵州航天林泉电机有限公司会议室
2. 设备付款方式

本次招标对中标价的设备款付款方式原则上为招标方预付款30%，设备到位安装调试合格后付款60%，设备质保期一年满后10日内付10%的余款。

1. 企业名称及地址

企业名称：贵州航天林泉电机有限公司

单位地址：贵州省贵阳市观山湖区长岭南路89号林泉科技园区

10、投标书**一正二副**用快递投寄或其他方式传递到我公司，务必在标书密封条外写明项目名称！以免影响开标前的资料整理！供应商不到现场参加开标。

11、联系方式：

单位名称：贵州航天林泉电机有限公司

通信地址：贵州省贵阳市观山湖区长岭南路89号林泉科技园区

联系人：龙孟伟

电话：18085598229

招标机构：贵州航天林泉电机有限公司

2023年12月13日

**第二部分 技术规格及要求**

# 工控安全设计

## 工控安全建设思路

在保证系统可用性前提下，对工业控制系统进行防护，实现“垂直分层，水平分区。边界控制，内部监测”。

“垂直分层、水平分区”即对工业控制系统垂直方向化分为三层：现场设备层、现场控制层、监督控制层。水平分区指各工业控制系统之间应该从网络上隔离开，处于不同的安全区。

“边界控制，内部监测”即对系统边界即各操作站、工业控制系统连接处、无线网络等要进行边界防护和准入控制等。对工业控制系统内部要监测网络流量数据以发现入侵、业务异常、访问关系异常和流量异常等问题。

系统面临的主要安全威胁来自于黑客攻击、恶意代码（病毒蠕虫）、越权访问（非授权接入、移动介质、弱口令、操作系统漏洞、误操作和业务异常等，因此，其安全防护应在以下方面予以重点完善和强化：

(1)入侵检测及防御；

(2)恶意代码防护。

(3)内部网络异常行为的检测；

(4)边界访问控制和系统访问控制策略；

(5)工业控制系统开发与维护的安全；

(6)身份认证和行为审计；

(7)账号唯一性和口令安全，尤其是管理员账号和口令的管理；

(8)操作站操作系统安全。

## 第二代防火墙设计效果

本方案中，在核心交换区和四楼汇聚交换机边界处部署了第二代防火墙系统，在实现细粒度访问控制的同时，实现入侵防御、恶意代码防范和抗DDOS攻击功能，进行多维度的安全防护。

第二代防火墙主要实现效果如下：

* 可以在蠕虫、后门、木马、间谍软件、拒绝服务等攻击的防御方面具备了检测、阻断、限流、审计报警等防御手段，满足各种应用需要。
* 可以检测和阻断RedCode、Slammer、sober，Zotob、nimda等多种国内外流行的蠕虫病毒，并可通过会话数管理防御未知蠕虫病毒的攻击。
* 可检测和阻断Sub7、netbus、bandook、Doly、GateCrasher等多种国内外主流的后门程序。
* 可以检测和阻断灰鸽子、Storm、Duntek等多达200多种国内外主流的木马。
* 可以检测和阻断IECodec、Spybuddy等多达400多种国内外主流的间谍软件。
* 可以检测和阻断CGI、Unicode等间谍软件。
* 可以检测和阻断ARP攻击、UDPFlooding、SynFlooding 等网络层拒绝服务攻击，以及处理CC，DNS Query Flooding等多种应用拒绝服务攻击。
* 网络访问控制兼顾病毒防御

第二代防火墙可以部署在Internet和内部网络之间，执行网络访问控制功能，防止外部用户对内部核心资源的非法访问，同时，也可以阻挡来自Internet的病毒、蠕虫、木马、间谍软件、恶意软件。第二代防火墙还支持HTTP协议和FTP协议，对于Web浏览、下载、Web邮件及FTP文件传输过程中携带的病毒均可进行拦截。

* 入侵防御功能

第二代防火墙主要目的是防御来自于外网针对内网的攻击。普通防火墙仅具有四层封包解析的功能，对于利用七层的黑客攻击手法或是利用合法掩护非法的网络行为便无法有效管控。通过第二代防火墙中入侵防御模块的保护，除了对于来自外网针对内网的暴力攻击能够有效阻挡之外，对于所有进出的封包均进行详细的七层分析，黑客利用合法方式进行的非法攻击将无所遁形。

## 高级威胁检测系统设计效果

高级威胁检测系统（Advanced Threat Detection System，ATD），将人工智能、大数据技术与安全技术相结合，实时分析网络流量，监控可疑威胁行为，内置多种检测技术，可对APT攻击链进行交叉检测和交叉验证。

ATD除了具备常规的入侵检测功能外，还可以从网络流量中还原出文件（HTTP、SMTP、POP3、IMAP、FTP、SMB等协议）并通过多病毒检测引擎有效识别出病毒、木马等已知威胁；通过基因图谱检测技术检测恶意代码变种； 还可以通过沙箱（Sandbox）行为检测技术发现未知威胁；对抽取的网络流量元数据，进行情报检测、异常检测、流量基因检测；最后将所有安全威胁进行关联分析，输出检测结果，对检测及防御APT攻击起到关键作用。

* 文件基因图谱人工智能检测

如今病毒木马变种层出不穷，攻击者通过改变病毒木马的某一部分特征，实现对传统杀毒软件检测的绕过。

ATD采用业界独特的基因检测技术，可以利用恶意代码在变种过程中的遗传学特征，即基因在遗传过程中的复制特性及部分基因突变特性，对恶意代码进行检测。通过基因比对，可以很轻易的识别出恶意代码变种，目前基因库恶意病毒基因高达数10亿样本，覆盖5000个以上家族，且在不断更新，检测的时间粒度在毫秒级别。

* 流量基因图谱人工智能检测

网络流量的规模和密度逐年增长，协议的类型和应用服务的类型更是多样化,更有恶意流量利用非标准协议进行数据的伪装或加密，以实现数据隐蔽传输。因此，如何准确识别网络流量的是网络安全中的重要问题。

这些都是同一恶意代码家族的不同变种的外联通讯会话，不同会话的特征均存在差异，现有的基于特征的检测技术如果未曾更新到特征库，就无法识别。ATD采用业界独特的基因检测技术，将流量会话映射成基因图谱，通过海量恶意样本家族产生的流量训练形成未知协议通讯检测模型，结合系统实时获取的网络会话基因特征，进行基因比对，实现精确的流量基因检测。

* 加密流量人工智能检测分析

恶意加密流量人工智能检测

ATD支持恶意加密流量人工智能检测，通过提取恶意代码家族的加密网络会话基因特征（DNS特征、TLS元数据、HTTP特征、包特征信息等）训练形成恶意代码加密通讯检测模型。

在现网中，ATD系统获取实时网络会话元数据，构建特征向量，使用检测模型对网络流量进行恶意代码加密通讯检测。

* Tor流量人工智能检测

ATD支持Tor（暗网）流量人工智能检测，采用构建Tor流量/非Tor流量捕获环境进行同类应用的数据传输（包括但不局限于浏览器、邮件、聊天工具、视频流、音频流、文件传输、P2P、VoIP等），分别提取步态指纹特征数据集训练建立暗网检测模型。

在现网中，ATD系统获取实时网络会话元数据，构建实时步态指纹特征，使用暗网检测模型对网络流量进行暗网通讯检测。

* VPN流量人工智能检测

ATD支持VPN流量人工智能检测，采用构建流量捕获环境进行同类应用的数据传输（包括但不局限于浏览器、邮件、聊天工具、视频流、音频流、文件传输、P2P、VoIP等），分别提取步态指纹特征数据集训练建立VPN流量检测模型，VPN流量检测模型框架。

在现网中，ATD获取实时步态指纹特征，使用VPN流量检测模型对网络流量进行VPN流量检测。

* ShadowSocks流量人工智能检测

ATD支持ShadowSocks流量人工智能检测，构建流量捕获环境进行同类应用的数据传输（包括但不局限于浏览器、邮件、聊天工具、视频流、音频流、文件传输、P2P、VoIP等），分别提取步态指纹特征数据集，通过Shadowsocks步态指纹检测结果生成Shadowsocks的服务端黑名单和客户端黑名单，经训练建立ShadowSocks流量检测模型，ShadowSocks流量检测模型框架。ATD获取实时步态指纹特征，使用ShadowSocks流量检测模型有效精准的定位存在ShadowSocks流量的主机。

* 移动应用加密流量人工智能检测

对手机APP应用程序流量检测整体检测，分为静态指纹检测和动态AI检测。静态指纹检测主要依赖SSL通信中Hello数据包生成方式与相应的客户端关联，构建JA3和JA3S的指纹引擎。动态指纹检测分为通信特征AI模型和步态指纹AI模型。

分别刻画不同手机APP通信流量特征，通过AI大数据和机器学习集成模型算法来识别手机APP流量，三个模型输出的最终结果到达关联引擎，综合判定APP流量类型。

* WEB攻击人工智能检测

SQL注入攻击人工智能检测

ATD支持SQL注入攻击人工智能检测，利用机器学习、集成学习和强化学习技术构建SQL注入攻击检测模型。

通过提取Web的URI、POST内容、User-Agent等其他HTTP头部信息，递归解码后，提取参数键值内容，基于SQL关键字泛化后生成word embedding特征后进入模型检测，判断是否存在SQL注入。

* XSS跨站攻击人工智能检测

ATD支持XSS跨站攻击人工智能检测，利用机器学习、集成学习和强化学习技术构建XSS检测模型。

通过提取Web的URI、POST内容、User-Agent等其他HTTP头部信息，递归解码后，提取参数键值内容，基于JavaScript/HTML等其他关键字泛化后生成word embedding特征后进入模型检测，判断是否存在XSS。

* WebShell网页后门人工智能检测

ATD支持Webshell网页后门人工智能检测，通过搭建Webshell运行环境，利用词袋与TF-IDF技术提取特征，同时利用uri/request body/response body，URI中的资源文件名称和动作建立静态AI检测模型；通过php动态脚本opcode提取N-Gram特征建立动态AI检测模型；通过异常特征统计、异常流量会话构建动态AI异常检测模型。

* 隐蔽隧道人工智能检测

DNS隐蔽隧道人工智能检测

DNS Tunneling，是隐蔽信道的一种，通过将其他协议或数据封装在DNS协议中传输建立通信。

ATD支持DNS隐蔽隧道人工智能检测，通过渗透环境搭建收集黑数据和白数据，生成用于分类DNS隧道和正常DNS数据的样本集合，利用基于窗口的DNS隐蔽隧道特征向量（DNS隧道空间、回应包的长度、qname 中数字字符占比等），构建DNS隐蔽隧道检测模型。

在现网中使用DNS隐蔽隧道检测模型对网络流量进行DNS隐蔽隧道检测。

* HTTP隐蔽隧道人工智能检测

ATD支持HTTP隐蔽隧道人工智能检测，通过提取原始流量HTTP流量特征，规则引擎用来打标和清洗过滤HTTP流量，经标注的正常流量和HTTP隧道流量分别经过自动化特征提取引擎，提取出重要特征，异常检测模型根据特征建立HTTP隐蔽隧道流量识别模型。

* DGA域名人工智能检测

DGA (Domain Generation Algorithm，域名生成算法)的设计思想是，malware代码里不写入域名字符串，而是使用一个私有的随机字符串生成算法，按照日期或者其他随机种子，每天生成一些随机字符串然后用其中的一些当作C&C域名。

ATD支持DGA域名人工智能检测，通过建立针对DGA生成域名的长短期记忆神经网络LSTM深度学习模型，用海量DGA生成域名和正常域名对深度学习模型进行训练，使深度学习模型具备识别能力。在捕捉到网络流量中的域名信息后，将之输入深度学习模型进行识别，深度学习模型输出该域名是否为DGA生成的域名，进而准确定位受控主机。

## 安全监管平台设计效果

部署安全监管平台，实现对各个单元网络的性能采集、安全监控和必要的日志收集。

信息安全管理系统给用户带来的一个关键价值就是可以提供一个总体安全监控平台，并通过该平台集中展示整个网络中的安全信息和攻击威胁。为了达到直观易用并且符合用户使用习惯的高效监控能力，信息安全管理系统应提供专业的安全监控拓扑。该拓扑可根据实际的环境自由定义，直观展现信息网站的物理部署拓扑，可使用户从全局视角了解整体生产环境的信息控制安全。

安全监控拓扑提供了各种风格的展现效果，可通过丰富的设备类型和网络表现形式展现生产制造等不同领域的环境。通过该拓扑用户犹如直接面对全环境的各类控制和运行设备，并且该拓扑是安全的晴雨表，如果网络中那台设备出现安全告警或故障问题，将实时在拓扑图标上闪烁告警，提醒监控运维人员尽快处理。

安全监控拓扑同时是安全监控的信息展示入口，可任意点击拓扑上的设备快捷的获得设备的基础信息和监控概要信息，如果需要对设备进行重点关注的话，可进一步进入该设备的详细监控视图，可完整监视与这台设备相关的各类安全信息，包括漏洞信息、安全事件信息、告警信息、性能状态信息等等。

安全监控拓扑是信息安全管理系统综合全部安全监控能力，直观展现威胁，提升用户监视与运维效率的有力体现。

* 设备管理

生产的信息控制网络中包含有大量的管理信息类、控制类、调度优化类、生产执行类设备，企业或者工厂的规模越大则设备数量和种类就越多越复杂，无疑管理的难度就更高。而对于工控安全来说，本质上就是保障各类工控设备及通信链路正常稳定运行。因此安全防护以及集中监控的首要工作就是识别并梳理全网环境中的设备资产，并以此为基础关联全部的安全信息进行展示和威胁分析。

设备管理可以维护从监控层、控制层到生产层各类工控设备的信息维护管理，设备基础信息除了手动创建，还支持自动发现和批量导入以应对设备数量庞大的工控用户。设备资产可以以资产树的形式和对用工控动态拓扑的方式进行

系统在资产管理功能中，除了记录资产的基本属性，还维护着资产的安全属性，包括CIA（Confidentiality/Integrality/Availability，私密性、完整性、可用性）三种属性。系统能够根据资产的安全属性遭受破坏后对所属业务系统的影响性程度计算出资产的价值，并进而计算出安全域和业务系统的价值。软件界面显示更友好的展示用户设备信息，用户可对资产信息进行编辑设置，配置与实际生产环境一直的资产显示环境界面。

* 事件管理

信息安全管理系统提供了强大的事件采集与集中展现功能，可采集环境中全部设备的运行日志、告警信息，以及全网部署的安全设备所产生的威胁事件。系统支持海量日志的本地存储或分布式存储，并利用最先进的分布式检索技术实现海量信息的秒级检索。在展现方面信息安全管理系统提供有丰富多样的展示方式，提供了面向数据特点和人员操作习惯的最佳数据可视化体验，包括展现数据对比关系的视图、反映事件访问关系的视网膜图、反映事件发展历程的追溯视图，直观表现事件起始位置的定位地图等。

事件管理中包含实时监视、实时统计、历史统计、历史查询、历史关联五项功能。

实时监测，实时解析日志信息，实时动态展示。用户可以通过丰富的事件分析策略对全网的安全事件进行全方位、多视角、大跨度、细粒度的实时监测、统计分析、查询、调查、追溯、地图定位、可视化分析展示等等。

实时监控提供多种可视化功能，帮助熟练的使用者第一时间发现网络异常，及时采取措施，

历史查询、历史关联等功能，针对历史数据，本系统提供用户细粒度分析功能。

对于事件的查询，系统自动分类，提供详细事件信息，事件查询中提供关联分析功能，帮助使用者进行深度关联分析，方便查找故障原由。

* 性能监测

该解决方案采集网络中数据包信息中包含各主机的性能日志信息，如cpu利用率，内存使用率等可用性信息。性能监控包括安全设备性能监控、主机监控、数据库监控、中间件监控等，同时也对解决方案自身系统状态进行监控。

系统应自带性能信息采集功能，同时也支持在用户网络中分布式部署多个性能采集器，就近采集管理对象的性能信息，包括可用性信息、运行状态信息、性能信息等，并汇聚到管理中心，从而实现对分散管理对象的性能信息采集，同时提高性能监测的并行性，进而提升性能监测的性能。

# 终端安全设计

## 主机卫士防护效果

工业卫士是专门为工控主机提供的一款防护产品，实现对工控上位机与工控服务器全面的安全防护。

工业卫士能够监控工控主机的进程状态、网络端口状态、USB端口状态，以白名单的技术方式，全方位地保护主机的资源使用。根据白名单的配置，工业卫士会禁止非法进程的运行，禁止非法网络端口的打开与服务，禁止非法USB设备的接入，从而切断病毒和木马的传播与破坏路径。

工业卫士提供严格的USB存储设备管理，U盘、USB硬盘等存储设备在接入工控主机使用前，必须先经过使用授权。未经授权的USB存储设备不能使用，经过授权的设备，也不能进行超越其权限的操作。通过授权管理，工业卫士能够有效防止文件泄密。同时，工业卫士还会审计USB存储设备的文件操作行为，为事后追责提供依据。

* 智能识别应用并生成白名单

应用软件安装、升级智能识别。

应用程序签名、证书、特征值等多元素匹配。

生成自定义集合的安全基线。

工业卫士通过机器学习的模式，全盘扫描，智能分析主机程序、进程，对于可以进程放置到隔离沙箱，保护主机的安全。

* 独有的应用程序检查机制

采取“暂停-检查-启动”三步过程，任何程序在启动前，都必须暂停下来接受检查，从而在恶意程序启动前即将其中止。

* 完善的外设安全控制

限制未经授权的USB外设在特定的主机上运行

完善的移动存储介质安全策略，可细分为允许读写、禁止等。

* 周全的工控网络攻击防护

采用独有的工控网络防护方法，能有效阻止Havex、沙虫等最新工控病毒、BadUSB等最新针对工控网络的攻击方法。

* 通过完整性保护来实现本体安全性

通过应用程序完整性保护和操作系统完整性保护来实现本体安全性。

有效保护计算环境和进程空间的运行安全。

有效防止计算环境被篡改和后门、缓冲区溢出等传统攻击方法。

* 专门针对工控上位机和服务器的操作系统防护技术

在不影响正常业务的运行下，采用白名单策略来实现对进程、外设、网络的防护，实现可持续的行为安全性。

## 移动终端安全防护效果

移动终端安全管理系统主要针对移动终端设备，如PDA等手持设备，对终端违规外联控制（外设端口管理控制及连接外网控制），功能支持以下：

1. 端口管理控制: 拨号上网、USB大容量存储设备、无线网卡、WiFi热点、红外/蓝牙、双网卡、串/并/1394/PCMCIA口；

2. 用户自定义的设备类型；

3. 禁止光驱刻录；

4、网络连接审计与控制功能。

# 2.3设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 单位 | 备注 |
| 1 | 第二代防火墙 | 2 | 台 |  |
| 2 | 高级威胁检测 | 1 | 台 |  |
| 3 | 安全管理平台系统 | 1 | 台 | 日志收集、主机卫士控制台 |
| 4 | 移动终端安全管理 | 若干 | 套 | 复用现有移动安全管理系统 |
| 5 | 网闸信息推送接口定制 | 1 | 套 |  |
| 6 | 文件检测与告警 | 1000 | 台 | 文件检测与告警（关键字检测） |
| 7 | 终端安全管理软件 | 1000 | 台 | 含进程白名单防护、外设管控 |

**3.设备操作培训、验收等要求。**

3.1需负责对招标方操作人员进行技术培训指导，直至操作人员能够安装、调试及处理简单常见故障，培训在招标人指定地点进行。

3.2使用过程中如发现质量问题，投标人接到通知后必须迅速解决。需要派遣技术人员到现场的，在得到招标人许可后，迅速派技术人员到现场对应。

3.3招标人为进行维修而要求生产并供应的设备零部件 (以下简称「维修零部件」)，投标人应尽可能满足该要求。维修零部件的价格和数量由双方协商决定。

3.4设备质量保证期为最终交付验收合格之日算起1年或一年以上。质保期内设备免费维修，由此发生的所有相关费用（包括更换零部件等内容）由投标人承担。

3.5 设备运行效率≥80%

3.6 标准件能耗等级：不低于国家及相关行业等标准规定的二级要求。

3.7 需标明产品能耗等级，并提供相关证明或测试报告。

**4.设备交付需提供的相关资料、附件。**

验收资料纸质版及电子版各一份，资料需双方进行签署确认，具体清单如下：

1. 设备操作规程；
2. 附件清单；
3. 设备使用维护说明书（含配件的型号、规格）。

**投标书（格式）**

致：贵州航天林泉电机有限公司

根据贵方为项目招标采购货物及服务的投标邀请，签字代表（全名、职务）经正式授权并代表投标人（投标人名称、地址）提交下述正本一份和副本二份。

1. 投标书；
2. 投标价格表；
3. 投标设备技术性能指标的详细描述；
4. 商务资料；
5. 规格、技术参数偏离表；
6. 其他材料。

据此函，签字代表宣布同意如下：

1、附投标价格中规定的应提供和交付的货物投标总价为

（注明币种），即（文字表述）。

2、我们将按招标文件的规定履行合同责任和义务。

3、我们已详细审查全部招标文件，包括修改文件（如有的话）以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

4、本投标自开标日起有效期为个日历日。

5、我们同意提供按照贵方可能要求的与本投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到的任何投标。

6、与本投标有关的一切正式往来通讯请寄：

地址： 邮编：

电话： 传真：

投标人代表姓名、职务（印刷体）：

投标人名称：

（公 章）：

日 期：年月日

授权代表签字：

**投标价格表（格式）**

货币单位：

|  |  |  |
| --- | --- | --- |
| 1 | 投标货物序号 |  |
| 2 | 货物名称 |  |
| 3 | 原产地 |  |
| 4 | 数量 |  |
| 5 | 主机和标准附件单价 |  |
| 6 | 备品备件价 |  |
| 7 | 易损件价 |  |
| 8 | 专用工具价 |  |
| 9 | 技术服务价 |  |
| 10 | 安装价（单独报价） |  |
| 11 | 检验培训费 |  |
| 12 | 运输（至目的地） |  |
| 13 | 保险 |  |
| 14 | 其它 |  |
| 15 | 投标总价 |  |

投标人代表签字: 日期：

**商务、技术参数偏离表（格式）**

|  |  |  |
| --- | --- | --- |
| 招标文件条款 | 投标文件对标情况及条款号（请逐项填写） | 偏差说明（正偏离、负偏离、无偏离或其他情况叙述） |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

投标人代表签字: 日期：

**除商务和技术偏差表里列出的偏差外，投标人响应招标文件的全部要求。**