ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/QGCML XXXX—XXXX

数据中心运维安全防护系统技术规范

Technical specifications for data center operation and maintenance security protection system

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

全国城市工业品贸易中心联合会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由××××提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

数据中心运维安全防护系统技术规范

1 范围

本文件规定了数据中心运维安全防护系统技术规范的术语和定义、医疗机构的安全防护管理监测系统、医院信息化基础设施安全运维、网络隔离和密码编译的门户安全设计、定制化专用系统平台批量自动配置方法。

本文件适用于数据中心运维安全防护系统技术的应用及检验。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 医疗机构的安全防护管理监测系统

4.1 数据采集模块

在安全防护管理监测系统工作时采集的数据总集N，数据总集N包括医务关联数据子集A和医疗机构常规数据子集B，其中，医务关联数据子集A为医务耗材数据、医务人员数据和病人数据，医疗机构常规数据子集B为医疗机构的各项设备、电力线路和安全系统的运行数据。

4.1.1 图像采集单元

实时采集医疗机构各个空间范围的音像数据，并将采集到的音像数据传输至数据分析模板中进行数据分析。

4.1.2 传感器单元

采集医疗机构中设备的运行稳定、空压、电力、流量运行输出数据，以及医务耗材数据的追踪、医疗人员和病人位置追踪。

4.2 数据分析模块

从数据总集N进行各项数据与阈值进行对比，判断数据是否出现异常，分析出异常数据P。

4.3 数据统计模块

统计异常数据P中医务关联数据子集A中的紧急报警次数A1，紧急报警权重系数a，以及医疗机构常规数据子集B中出现的非紧急报警次数B1，非紧急报警权重系数b。

4.4 数据判断模块

根据紧急报警次数A1，紧急报警权重系数a，非紧急报警次数B1，非紧急报警权重系数b，以及投总报警次数F，获取运行安全的紧急程度M；其中，a大于或者等于b。

4.5 运维管理模块

确定运行安全的紧急程度M大于或者等于预设紧急程度E，显示报警提醒并且将报警提醒发送到管理人员。

4.5.1 常规管理单元

通过控制网络对采集医疗机构中各项设备、电力线路和安全系统实时调控。

4.5.2 医务管理单元

通过控制网络在收到权限确认后对医务耗材数据、医务人员数据和病人数据进行更新。

4.6 医务权限模块

根据系统设置的安全规则，规定所述医务人员可以访问对应的所述病人数据。

4.7 可视化模块

实时采集的数据总集N上传至电脑端的网页中进行分类处理后可视化展示，以及报警提醒可视化显示。

4.8 可追踪模块

记录医务人员数据对其对应的病人数据所使用的医务耗材数据。

4.9 三维 GIS 模块和定位模块

含有各项设备、电力线路和安全系统的三维地图，所述定位模块用于在三维GIS模块中标记显示故障点。

4.10 预案存储模块

存储预先输入的紧急处理预案，运维管理模块根据存储的紧急处理预案进行执行。

5 医院信息化基础设施安全运维

5.1 Down 状态

新增的系统或设备尚未开启，向中心认证服务器发送认证请求，进入Register状态。

5.2 Register 状态

认证状态，向中心认证服务器发送Register包，请求认证，若认证成功，则进入Judge状态，若认证失败，则继续处于该状态，并且每30 s发送一次Register包进行再次认证，Register包格式为：名称、类型、IP地址、MAC地址、加密预留密码，若3次后均未认证成功，则进入Dormancy 状态。

5.3 Dormancy 状态

休眠状态，由于连续3次认证失败会进入该状态，进入该状态以下列公式进行计时：180×count，其中每次进入该状态count将增加1，若180 s内未再次进入该状态，则count自动清零。

5.4 Judge 状态

判断状态，该状态主要用于查看是否管理员指定了某运维应用程序，若管理员已经指定，则进入Listen状态，若管理员未指定，则将长期处于该状态下，管理员可以通过该状态判断出自己尚未对该设备指定监控的程序。

5.5 Listen 状态

监听状态，用于监听指定端口的运维数据，为各种运维系统的指定端口，若某些运维软件使用随机端口发送运维数据，则监听指定应用程序，在该状态下，被监听端口或应用程序发送的运维数据，可以正常与运维服务器进行通信，并且将运维数据复制到数据备份与审计服务器中以供后期对数据的审计。

5.6 中心认证服务器

5.6.1 Down 状态下的系统或设备向中心认证服务器发送认证请求，进入 Register 状态。

5.6.2 中心认证服务器接收认证请求后，将自身公钥返回给 Register 状态下的系统或设备。

5.6.3 Register 状态下的系统或设备收到中心认证服务器返回的公钥后，管理员将中心认证服务器预留密码使用公钥加密放入 Register 包中并将 Register 包发送给中心认证服务器。

5.6.4 中心认证服务器收到 Register 包后，使用私钥将 Register 包中加密预留密码进行解密并与原始预留密码进行比对，若比对一致，则将 Register 包中信息存入本地并返回认证成功信息，若比对不一致，则返回认证失败信息。

5.6.5 Register 状态下的系统或设备收到中心认证服务器返回的认证信息后，若认证成功，进入 Judge 状态，若认证失败，则再次进行认证，若 3 次认证失败后，则进入 Dormancy 状态。

6 网络隔离和密码编译的门户安全设计

6.1 使用微服务架构建立安全管理中心，并将用户注册、登录信息保存在内部加密数据库中。

6.1.1 安全管理中心的微服务架构设计时采用具有服务自治的轻量级通讯协议，实现系统功能模块化，功能模块包括认证服务、配置服务、文件服务、通信服务、接口服务和监控服务。

6.1.2 认证服务采用 Spring Security 框架进行搭建，对用户账号密码进行管理、JWT 身份验证、权限控制，通过生成 token 令牌并返回给客户端验证用户身份。

6.1.3 配置服务使用 Spring Cloud Config 实现，负责对系统配置文件的管理、存储和调用，让管理员可以动态更改系统的配置信息。

6.1.4 文件服务采用 FastDFS 对象存储技术来实现文件的分布式存储，同时管理系统中的文件上传、下载和存储，并使用 CDN 加速技术提高文件传输效率，减轻网络负载。

6.1.5 通信服务通过第三方平台进行发送和接收信息消息通知，同时使用 Twilio 平台发送短信验证码。

6.1.6 接口服务采用 Spring Boot 技术搭建微服务架构，并使用 Swagger 工具生成 API 文档，通过架构接口接收并处理用户客户端发送的请求并响应相应的数据。

6.1.7 监控服务对整个系统的运行状态进行监控和警告，然后使用 Prometheus/Grafana 技术对监控的数据进行统计和分析，生成系统日志、性能指标、异常警报，还能够使用第三方平台对异常情况进行及时通知。

6.1.8 安全管理中心是先让用户通过 API Service 服务向系统发送请求，API Service 完成相关操作，将操作结果返回给请求方，并记录操作日志，在更改系统配置时，管理员通过 Configuration Service 进行配置文件修改，并向 API Service 同步更新，当系统需要进行升级、部署和扩容时，管理员通过 API Service 接口服务来进行操作，API Service 会将操作传递给其他微服务来完成对应的功能。

6.1.9 请求包括用户身份认证、配置文件获取、文件上传下载、消息通知，若是请求为用户进行身份验证，API Service 会将请求传递给 Authentication Servic 进行身份验证，验证成功后，Authentication Service 会生成 token 令牌，并返回给 API Service；若是请求为配置文件获取，API Service 根据请求的内容，调用 Configuration Service 服务获取相应的系统配置文件；若是请求为文件上传下载，API Service 会将请求转发给 File Service 进行操作；若是请求为消息通知，则会将请求传递给 Mail Service 来发送消息。

6.1.10 安全管理中心在检测发现异常情况时，API Service 会将异常信息发送给 Monitoring Service，Monitoring Service 会进行统计和分析，对系统日志、性能指标、异常警报等进行监控和警告，并通过第三方通知软件实时通知相关负责人员处理。

6.2 采用离线部署方式，在使用之前将所需的数据和程序部署在本地，使用非对称加密算法对内部加密数据库进行加密。

6.2.1 内部加密数据库加密采用 RSA 算法，通过 RSA 算法对配置信息和账号数据的加密存储，先由安全管理中心生成一对 RSA 密钥，RSA 密钥分为公钥和私钥，密钥位数长度较长，将公钥发送给用户客户端进行使用，用户客户端将配置信息和账号数据使用公钥进行加密，并将密文传递给安全管理中心进行

存储，后续使用时，安全管理中心通过私钥进行解密，获取明文数据并进行相应处理。

6.2.2　内部加密数据库加密同时采用密钥轮换技术，定期更换密钥。

6.3　将配置数据保存在内部加密数据库中，只有掌握解密私钥的人才能解密该数据，确保数据的机密性和完整性。

6.4　利用虚拟化技术进行网络隔离，使系统与外网隔离，同时选择强类型语言进行编程开发使源码难以被逆向破解。

6.4.1　虚拟化技术进行网络隔离是先综合考虑安全性、可靠性、性能和易用性，根据实际情况进行权衡和选择，确定虚拟化技术；再针对需要隔离的客户端，在虚拟化平台上使用类 Unix 系统搭建虚拟机，并配置相应的操作系统和应用程序；使用虚拟化平台提供的桥接模式，将虚拟机与本地网络直接连通，对虚拟机的网络进行配置，将其与客户端所在的网络隔离开来，并使用虚拟化平台提供的网络过滤技术和防火墙对其进行保护；针对需要向外网提供服务的虚拟机，对虚拟机进行安全加固保护虚拟机的安全性，进行系统补丁更新、防病毒软件安装和网络过滤；使用虚拟化平台提供的监控和审计工具对虚拟机进行监控和审计，发现并处理安全问题。

6.4.2　选择强类型语言进行编程开发是先使用代码混淆工具采用控制流混淆法对源码进行混淆处理，使反编译者难以理解和推断代码的实际含义；选择 DES 算法将源码分块进行加密处理，将加密后的代码与原有代码整合，以二进制格式安全存储，防止黑客通过访问文件系统获取源码，进行防盗链处理，防止恶意程序员将代码复制到其他地方；使用安全审计工具定期对源码进行安全审核和漏洞扫描，寻找并修复代码中存在的漏洞和弱点；使用针对软件和数据的保护芯片 Secure Element 和嵌入式安全模块 Trusted Platform Module 对源码进行保护；对访问代码的用户进行权限控制，只有经过授权才能访问相关代码文件，同时对需要运行代码的用户，采用数字签名和安全沙箱保护系统的安全性。

7　定制化专用系统平台批量自动配置方法

7.1　使用设备检测工具对硬件设备进行检测，获取硬件型号信息并储存。设备检测工具内设置有硬件数据库，硬件数据库存储有当前硬件设备的各项硬件参数信息，同时存储有硬件设备启动时的各项数据，以及通过联网检索该硬件设备在标准环境下启动时的各项数据，每次系统启动加载时，设备检测工具进行硬件自检，确定当前硬件是否出现故障，是否与存储硬件型号信息相匹配，当硬件出现变动时，对硬件设备进行重新检测，更新存储的硬件型号信息。

7.1.1　使用高斯窗函数对历史软件进程资源数据进行转换，得到分析转换后的资源波形图，对波形图进行快速傅里叶变换和希尔伯特变换，得到频谱数据和包络波形数据。

7.1.2　根据频谱数据和包络波形数据得到软件进程运行时资源占比突降、突升、谐波以及波形扰动类型，对不同波形扰动类型进行特征提取，得到扰动特征。

7.1.3　根据提取的扰动特征进行训练分类，对资源占比扰动进行检测与判断。

7.1.4　设置调节卷积神经网络模型的参数，搭建扰动分析模型。

7.1.5　使用扰动分析模型对资源波形图的数据进行分析计算和预测，根据分析计算结果。

7.1.6　得到软件进程运行时最佳的资源占比，同时设置、屏蔽、控制会造成资源占比扰动的干扰。

7.2　使用配置管理工具根据硬件型号信息对系统组件和硬件设备进行各项属性配置。属性配置包括：存储空间和交换空间进行分区处理，配置系统缓存所占比例，处理器核心是否屏蔽，各个硬件的电压、功耗和频率，设置各个硬件设备的固件更新版本；用户进行各项属性配置时，可以选择默认配置、手动配置和自动配置，默认设置是按照硬件数据库内通过联网检索硬件设备在标准环境下启动时的各项数据，将硬件设备按照标准情况下各项参数进行属性配置；手动配置是用户根据设备的专项用途和资源的实际运行需求对硬件设备的各项参数进行属性配置；自动配置是硬件设备初次启动时，按照默认设置的各项参数进行属性配置，之后每次硬件设备启动时，启动时的各项参数保存至硬件数据库内，根据这些参数

信息建立硬件属性自动配置模型，通过硬件属性自动配置模型计算出硬件设备启动时最佳的参数信息，并根据最佳的参数信息对硬件设备进行自动属性配置。

7.2.1 使用 LPP 算法从历史参数特征集中提取具有判别性的特征进行降维，生成历史参数特征子集。

7.2.2 使用 Boosting 框架算法对历史参数特征子集进行训练计算，得到训练样本子集，再用训练样本子集训练生成基分类器，进行多轮训练，生成多个基分类器，在将这多个基分类器进行加权融合，生成参数调整分类器。

7.2.3 按照数据存储时的时间戳，从硬件数据库内提取系统近期启动时硬件设备的各项属性参数，将硬件设备近期的属性参数作为待检测参数样本，对待检测参数样本进行预处理，统计分析并计算待检测参数样本的参数特征，生成待检测参数特征集。

7.2.4 使用 LPP 算法从待检测参数特征集中提取具有判别性的特征进行降维，生成待检测参数特征子集，使用参数调整分类器对待待检测参数特征子集进行预测判断，获取待检测参数样本的分析结果。

7.2.5 根据分析结果判断系统近期启动时，各个硬件设备的运行效率，结合参数调整分类器，对硬件设备的属性参数进行设置，使硬件设备在满足系统使用的情况下达到最佳的运行效率。

7.2.6 待检测参数样本在分析完成后，会将自身的待检测参数特征子集根据分析结果存储至历史参数特征子集，达到预设时间时，根据历史参数特征子集数据的更新对参数调整分类器进行更新。

7.3 使用自动化安装工具安装和更新应用软件进程，获取软件版本并存储，同时设置软件进程的权限。自动化安装工具内设置有软件数据库，每次安装和更新应用软件进程都会获取软件版本并存储，通过联网检索软件当前储存使用的版本的各项参数以及当前软件的最新版本和各项参数，每次启动软件进程时都会通过软件数据库检测软件版本，判断与存储的版本号和软件当前最新版的版本号是否匹配，若是与存储的版本号不匹配，则限制该软件进程的启动，若是与软件当前最新版的版本号不匹配，则发送更新请求。若是无法检索到软件当前版本和最新版本的各项参数数据时，使用容器编排工具通过容器化技术打包应用程序和依赖项并运行，进行应用程序部署和管理容器化，使用容器编排工具对各个应用程序进程运行时需要的硬件资源数据储存至软件数据库内，根据软件数据库内存储的历史软件进程资源数据进行分析。

7.4 使用控制部署工具对系统组件进行初始化和兼容性设置，通过标记配置初始化数据约束系统自执行逻辑。

7.5 使用安全规范工具编写安全规则建立防火墙，设置管理者账号和权限，对软件进程和接收的数据进行安全扫描，对发送的数据进行安全数据加密，部署风险策略。

7.5.1 安全规范工具部署风险策略是对软件进程的原始数据进行重构，获得重构数据；根据软件进程历史数据判断原始数据是否存在风险，以此将数据标记为不同的样本，获取数据标签，结合重构数据计算出重构数据各个特征的信息价值指标值；根据信息价值指标值从重构数据中筛选出有效特征；根据数据标签和有效特征，采用等频分箱法对重构数据进行分箱处理，计算出各个分箱对应的风险指标；使用有效特征和风险指标生成风险策略。

7.5.2 对原始数据进行重构是采用自编码器进行重构，先使用编码器对数据降维压缩，然后使用解码器对数据进行升维解压，以此达到数据重构的效果。