技术方案

第一章 项目概述

一、项目背景概述

面对新型网络攻击手段的出现和高安全网络对安全的特殊需求，全新安全防护防范理念的网络安全技术——“网络隔离技术”应运而生。网络隔离技术的目标是确保把有害的攻击和病毒进行隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。网络隔离技术是在原有安全技术的基础上发展起来的，它弥补了原有安全技术的不足，突出了自己的优势。

电视台着眼未来安全技术的发展方向，针对广电行业对网络安全要求的特殊性并结合自身需求，启动大数据安全交互平台建设项目。

二、项目特点介绍

对于外来数据的导入，我们采用了独有的 USB 数据隧道技术，通过“两层防毒过滤+两层防攻击+一次统一认证”设计，确保了数据能安全的从外网导入业务网络中，该技术已在国内多家大型电视台得以广泛应用，同时在《电视台数字化网络化建设白皮书（2007）》中被列为推荐使用安全措施之一。

1、一次统一认证

外网安全交互软件仍然需要登录认证才能使用，且外网的登录认证与内网的统一认证绑定在一起，未在内网登记注册的用户，无法将

数据交互到内网，确保外来内容在内网的数据流向，又增加了个人素材的隐私性。

2、两层防毒过滤

- 两个服务端装有不同的杀毒软件

安全交互软件能与包括：Kaspersky、ESET Nod32、Avira 在内的多家杀毒软件生产厂商进行底层的深度耦合。

- 指定格式的数据迁移

指定格式做数据迁移后，软件能自动的识别传输文件的类型，屏蔽指定传输文件以外的格式，只将经过安全认定的格式进行传输。

- 软件深层检测：

安全交互软件能自动判断识别将更改后的病毒文件，能自动识别二级后缀的文件，能将隐藏病毒文件进行排除。

3、两层防攻击

- 两个服务端通过专用 USB 线进行连接：

两台传输设备使用 USB 进行连接，而非以太网线进行连接，避免了 IP 链路的链接，没有了 IP 地址的链接就防止了网络攻击，起到了防火墙的作用。

- 服务端采用私有交互指令：

两个服务端采用私有的交互指令，严格指令校验，防止在外网端被恶意控制的情况下，无法对内网造成任何威胁。

第二章 设计参考标准

一、相关国际标准

- BS743 接地规范
- ISO/IEC 11801:2002 Ed2.0 建筑及建筑群结构化综合布线系统国际标准
- EN50173 关于 ClassE 六类布线的最新要求
- CCITT 有关标准
- ISO/IEC17799 信息安全管理操作规则

二、国家相关标准

- GB/T 12365-1990 广播电视短程光缆传输技术参数
- GB/T 50311－2000 建筑与建筑群综合布线系统工程设计规范
- GB/T 50312－2000 建筑与建筑群综合布线系统工程施工与验收规范
- GB/T 18018-1999 路由器安全技术要求
- GB/T 18019-1999 信息技术 包过滤防火墙安全技术要求
- GB/T 18020-1999 信息技术 应用级防火墙安全技术要求

三、行业标准

- GY/T 134-1998 数字电视图像质量主观评价方法
- GY/T 155-2000 高清晰度电视节目制作及交换用视频参数值
- GY/T 187-2002 多通路音频数字串行接口

- GY/T 192-2003　数字音频设备的满度电平
- GY/T 193-2003　数字音频系统同步
- GD/J038-2011 广播电视相关信息系统安全等级保护基本要求

四、项目设计参考标准

- 播出系统与其他信息系统之间进行数据交换时，应对文件类型及格式进行限定；
- 应限定可以通过移动介质交换数据的主机，所有通过移动介质上载的内容应经过两种以上的防恶意代码产品进行恶意代码检查后，方可正式上载到内容网络；对蓝光、P2 等专业移动介质通过特定的防护机制进行上载；
- 信息系统与外部网络进行数据交换时，应通过数据交换区或专用数据交换设备完成内外网数据的安全交换；
- 数据交换区对外应通过访问控制设备与外部网络进行安全隔离，对内应采用安全的方式进行数据交换，必要时可通过协议转换的手段，以信息摆渡的方式实现数据交换；

文件安全交互平台的各项软、硬件技术必须遵循现有的（或通用的）中国标准，若无相应的中国标准，则必须遵循国际有关技术标准。主要可分为多媒体方面、传统系统、建筑施工综合布线等。

五、总体设计原则

所提供的文件安全交互平台解决方案及软硬件设备配置，能高质

量地满足用户对数据安全快速交互的需要。本解决方案项目设计原则概括起来，主要是：全局性、实用性、易用性、先进性、开放性、可扩展性、可靠性等。

可靠性

采用安全、稳定的系统结构是文件安全交互平台系统建设中的关键。在其日后的节目录制、编辑、播出、存储以及内容数据管理等方面安全性表现更加突出。系统应具有极高的运行可靠性，具有检错、纠错能力，并具备完善的应急方案，且应急操作安全、快捷。备份系统（包括通道）要有独立性，防止主系统出故障时对备份系统造成影响。同时，系统运行过程中的各关键因素要有严格的监控和管理手段。

此外，我们在硬件选型方面，均采用国际知名品牌产品，产品的稳定性、成熟性及先进性都有所保障，其售后服务及备品备件供应也能够满足用户的需求，为整个系统正常运行保驾护航。

实用性

所提供的文件安全交互平台系统方案及软硬件设备配置，选用成熟的技术和先进的设备、软硬平台建设，整个系统易于管理和维护。能满足网络高安全隔离的需要；同时也能满足高效数据交互的需要。

易用性

■ **运行维护**

所设计和提供的文件安全交互平台具备优秀的可用性能，同时也提供了良好的检错、纠错能力，具有完善的备份措施。在系统出现故障时，能够在较短的时间内恢复系统运行。

■ **网络管理**

所设计的文件安全交互平台具备完善的网络管理功能，网络管理操作简单、直观、维护管理方便。所有日常维护工作要求能实现在线式操作，同时所有的主要设备必须支持在线热插拔。

■ **操作界面**

同时根据用户的实际需求，我们设计了美观便捷的操作界面，用户可以自定义工作模版和快捷键，最大限度符合使用者的工作习惯，便于工作效率的提高。

开放性

文件安全交互平台按照国际、国内相关标准设计建设，采用开放式平台，允许多品牌设备、异构设备在本系统中运行。

采用标准平台、运用标准规范、实施规范设计与开发，是任何 IT 应用系统建设的一个关键因素，在文件安全交互平台系统设计中也必须始终重视开放性原则。

全局性

文件安全交互平台中采取整体规划，整体设计的建设思路，构建整个安全交互平台的系统架构。系统建设从全局出发，综合考虑现有系统建设、其它子系统以及将来与新建设的系统之间的互联互通。

先进性

文件安全交互平台除了保证功能齐全之外，对技术的前瞻性要求更是技术实力的体现。在保证安全性和高效性的前提下，先进的技术对整体网络来说如虎添翼，所以对产品技术前瞻性的考虑，应该更加充分，才能确保系统的可持续发展能力。系统的先进性涉及多方面的因素，例如：整体架构、系统平台、网络构件、技术实现手段等，需要综合全面的设计。

关于系统的先进性，贯穿整个项目系统的设计理念、设备选型及工程施工的全过程，不仅完全符合我国电视广播规范和有关标准，符合国际广播电视技术发展潮流，完全适应视音频编辑技术、计算机技术、网络通信技术及系统中其他技术发展的要求，同时，借鉴和发展了国际领先的理念，实现先进、高效的自动化流程，以保证系统的先进性。

可扩展性

长远考虑、分步实施，使系统具有良好的可扩展性。随着功能需求和系统规模需求的增加，具备良好的升级、扩容能力，并在升级、扩容的同时应尽可能保护先期投资。整个系统可以从系统架构、系统规模、应用业务以及新技术应用等四个方面按需扩展。

六、信息技术软件质量标准

- GB/T 17544-1998《信息技术 软件包 质量要求和测试》
- GB/T 16260-1996《信息技术 软件产品评价 质量特性及其使用指南》

七、安全要求标准

- 广电总局 GD/J038-2011

第三章 项目总体设计

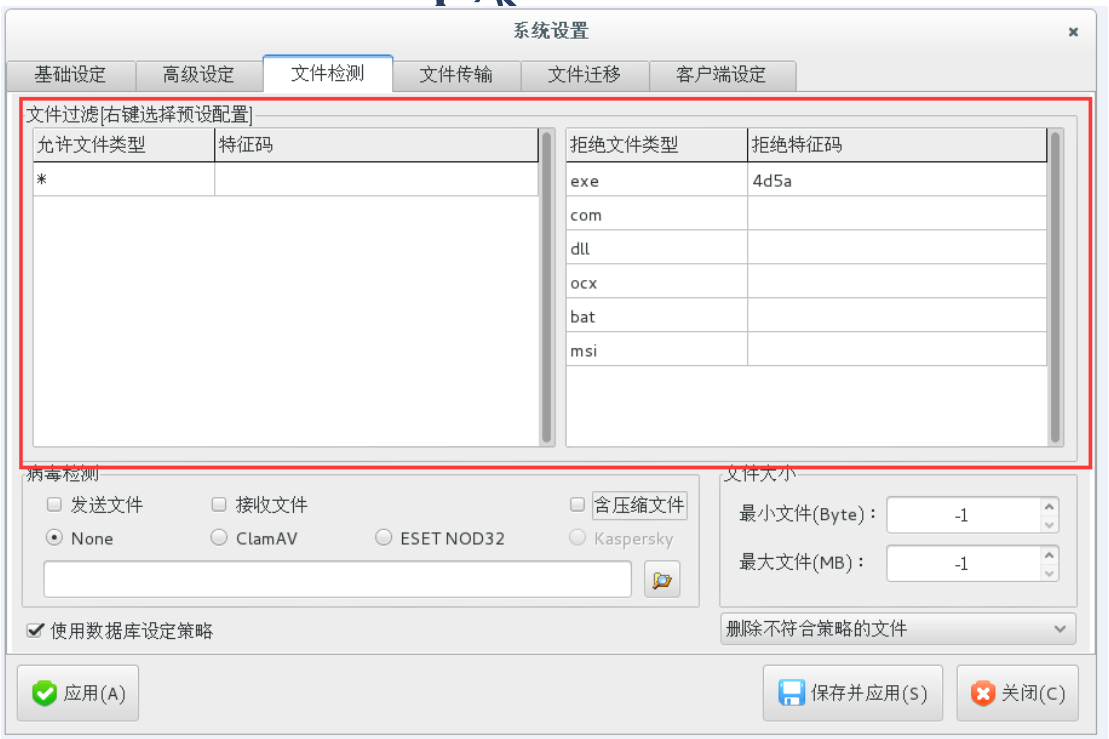
本设计方案专门针对电视台制作网、媒资网、演播室及播出机房，意在通过这种安全、高效，便捷的方式，将来至于非安全网络的文档、图片、字幕模板、视音频素材、节目单等数据安全的交互到高安全网

络指定的缓存区存储，以供相关人员使用。

一、系统特点

基于 USB 的安全隔离和信息交换，由 2 个拥有操作系统的独立主机系统（内网服务器和外网服务器）和连接硬件组成。连接硬件是与以太网异构的介质组成（USB 线缆），连接硬件通过主机上的程序和硬件上独立的芯片来对两个网络中需要交换的信息数据采用不同于 TCP/IP 的私有协议进行封包、摆渡、解包，从而实现内外网之间数据的交换。这种架构抛弃了较为脆弱的基于 TCP/IP 协议的内外网安全隔离机制，从真正意义上达到内外网连接时的安全隔离。

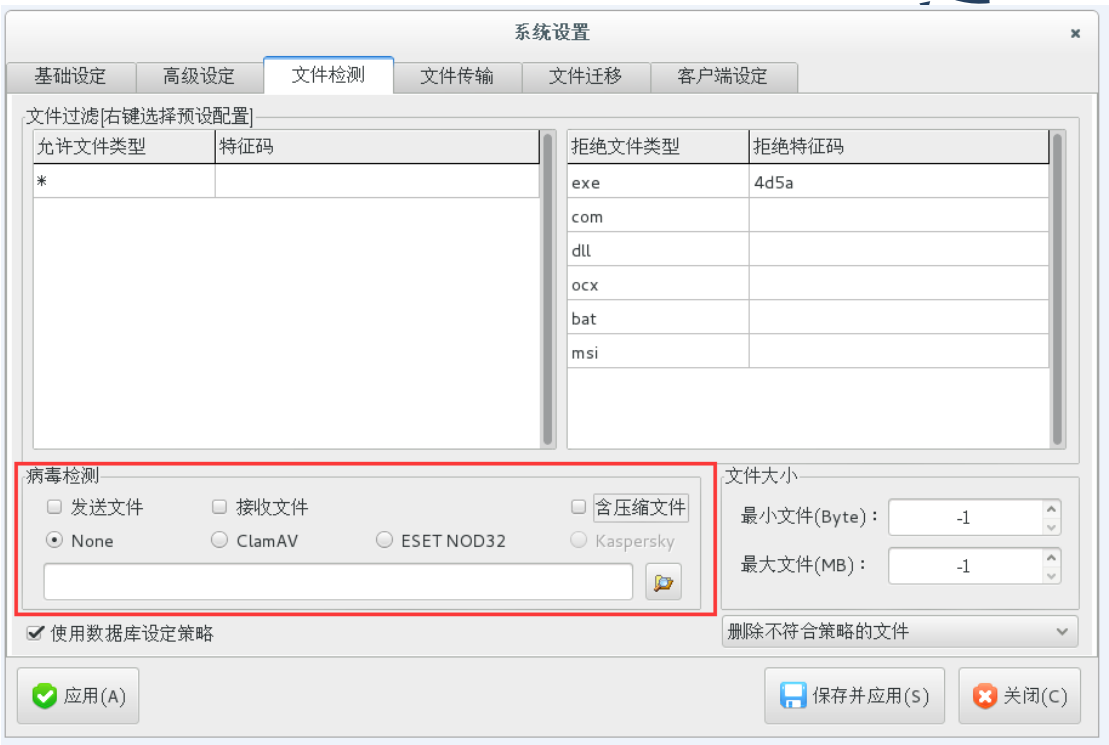
1、严格的文件类型检查



用户可自定义文件传输类型，可允许传输和拒绝传输某些类型文

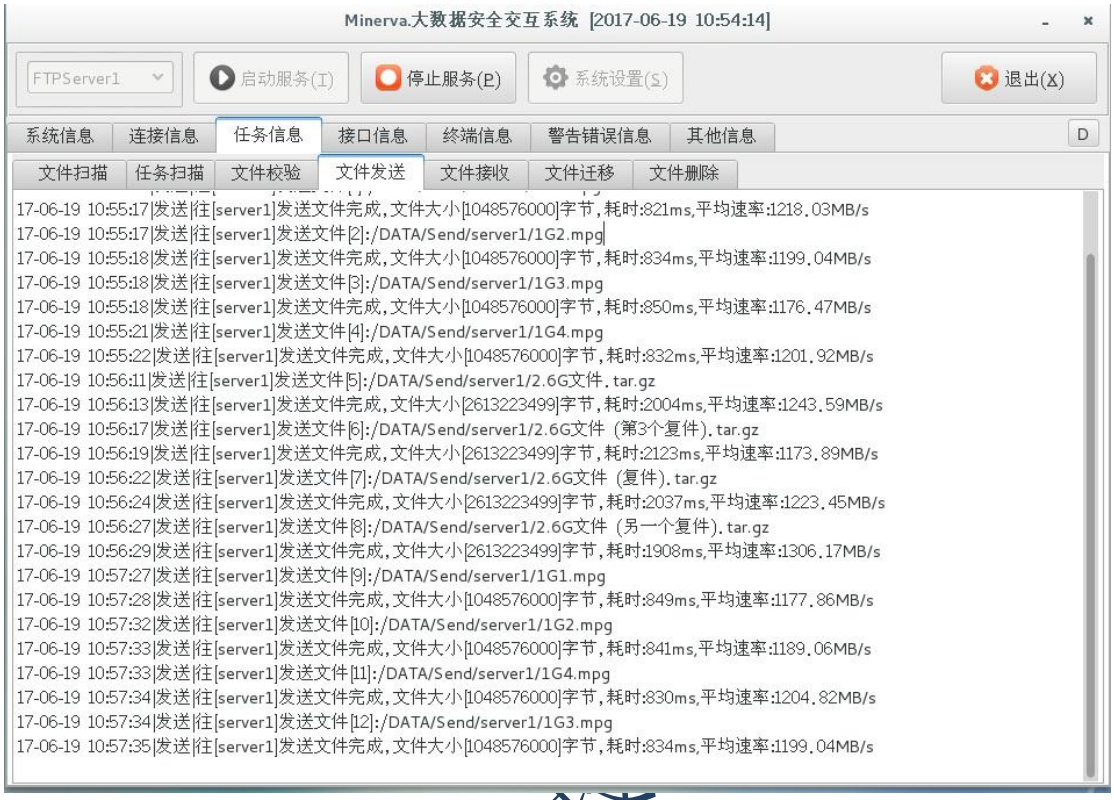
件，可根据配置检测问题内部格式是否是相对应的文件类型，防止某些恶意的文件类型修改欺骗（如将 EXE 执行程序更改为 AVI 类型）。从传输文件的类型上进行又一次过滤，确保进入内网的文件没有被病毒感染的可能。

2、高效的病毒查杀



采用国外著名的杀毒软件（卡巴斯基，ESET NOD32，Avira，BitDefender，Avast 等），拥有强大的杀毒引擎和完善的病毒库，使用内嵌式后台杀毒模式，快速高效的扫描所有传输的文件，从根本上解决病毒木马等问题。并且采用双独立主机系统异种杀毒软件的查杀，几乎可以清除掉所有的病毒威胁。

3、高速传输速率



InfiniBand 的传输速度理论可以达到 100Gbps 以上，实际测试速度能达到 10Gpbs 以上(与服务器硬件平台性能相关)，支持双向同步传输，完全能满足各行业用户的传输速率需求。支持超大文件的稳定传输，能稳定传输 100G 以上的大文件。

4、智能的传输控制

自动检测任务并控制传输，采用 MD5 文件完整性效验，保证传输到内网的所有文件完整。自动检测现有文件，并根据设定规则进行重命名，防止重复传输同名文件被覆盖。可根据文件类型自动分类保存，方便在内网进行文件的检索。

当系统遇到小文件进入系统后，会自动把它的优先级设为最高，

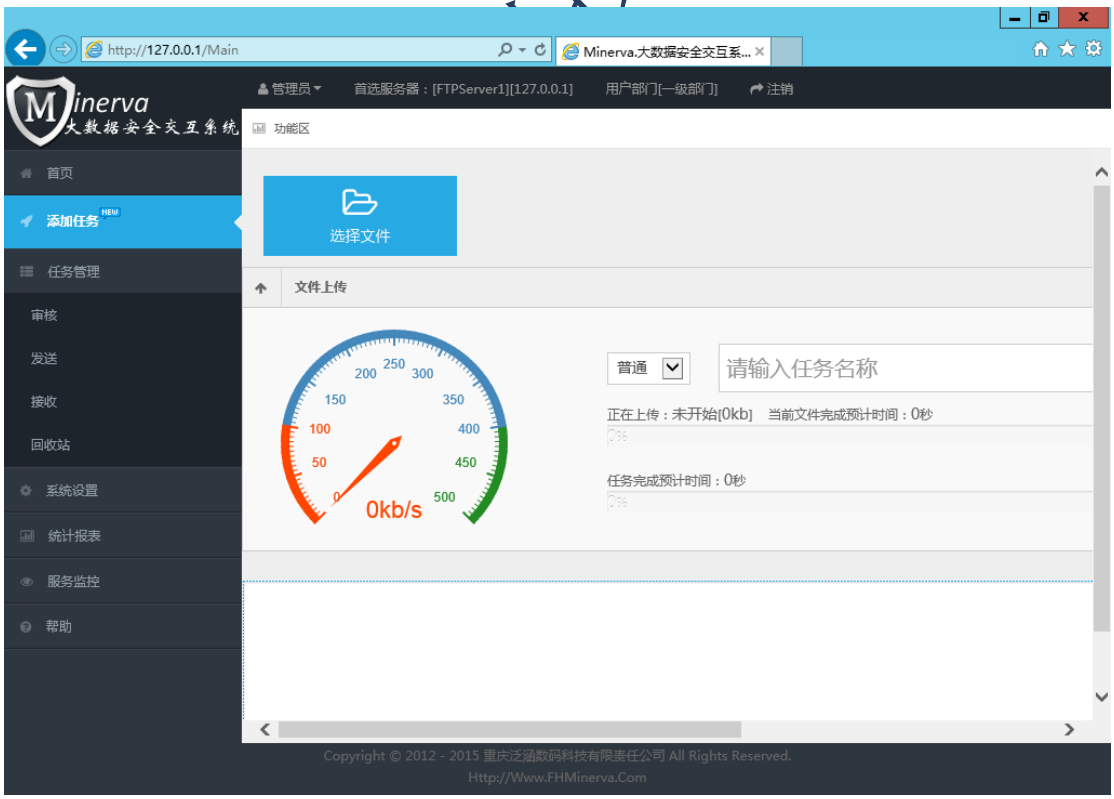
使系统优先处理它。

并且可根据实际的运用场景，对系统的端口进行限定，比如只开启 20、21、80、3306 等端口，这样可进一步保障系统的安全。

5、简单易用的操作方式

可根据实际使用情况配置多种文件传输的方式。CIFS（文件共享式），按 WINDOWS 权限进行共享权限设定，操作简单方便，即日常的文件复制粘贴操作。WEB 网页上传（支持断点续传）、共享方式上传可按设定用户可传输的文件类型，支持在带路由的办公网或英特网进行远程传输。并且支持 Windows,Linux,MacOS 等操作系统环境。

Web 客户端操作界面：

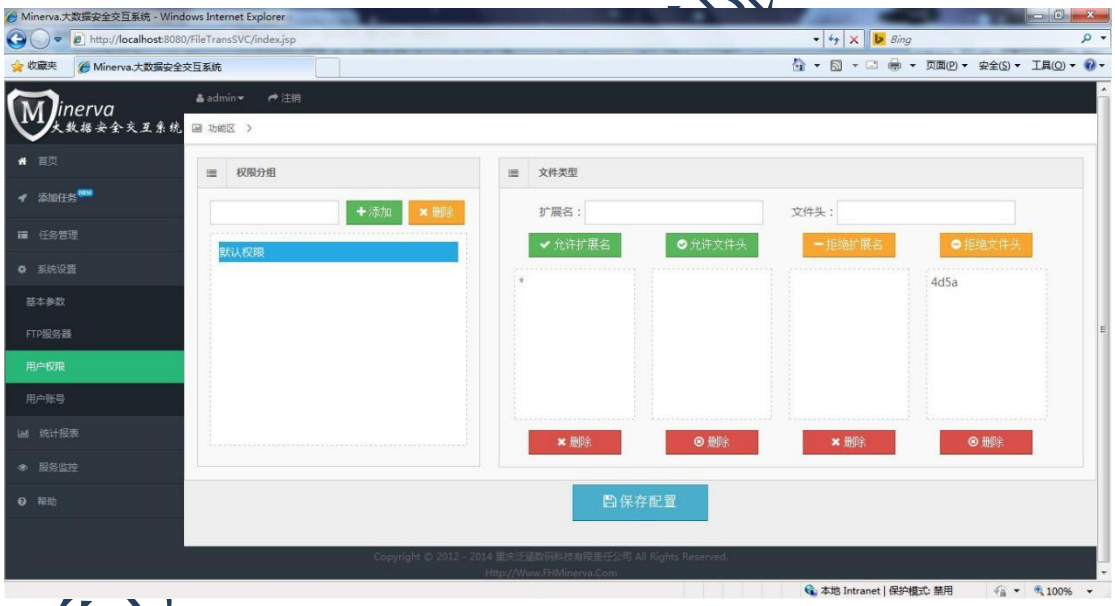


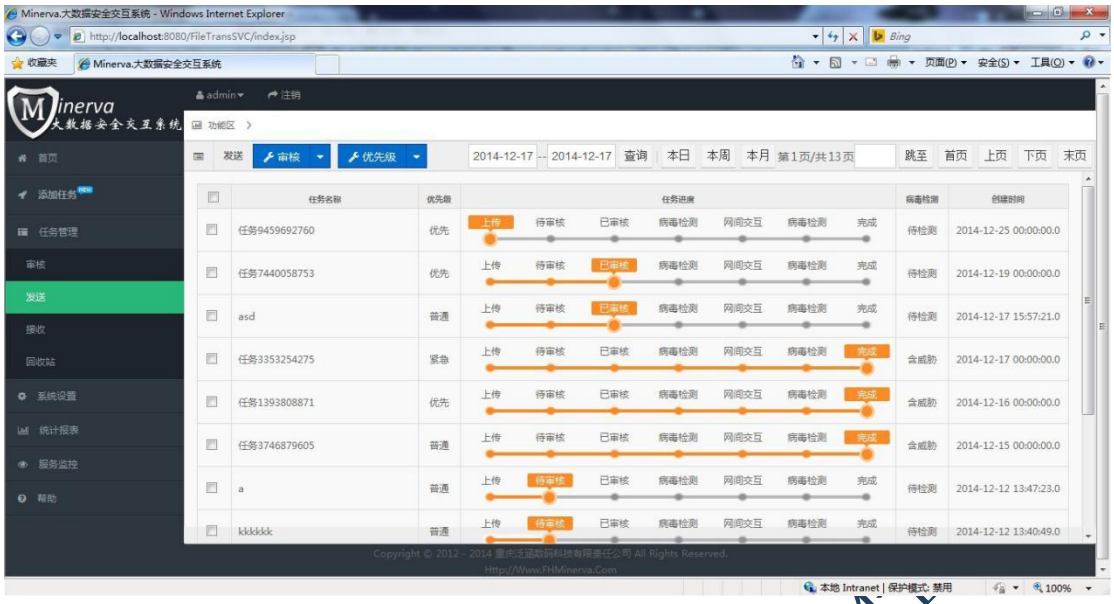
根据用户指定的检索方式扫描素材，可选择的预览素材并进行上传。

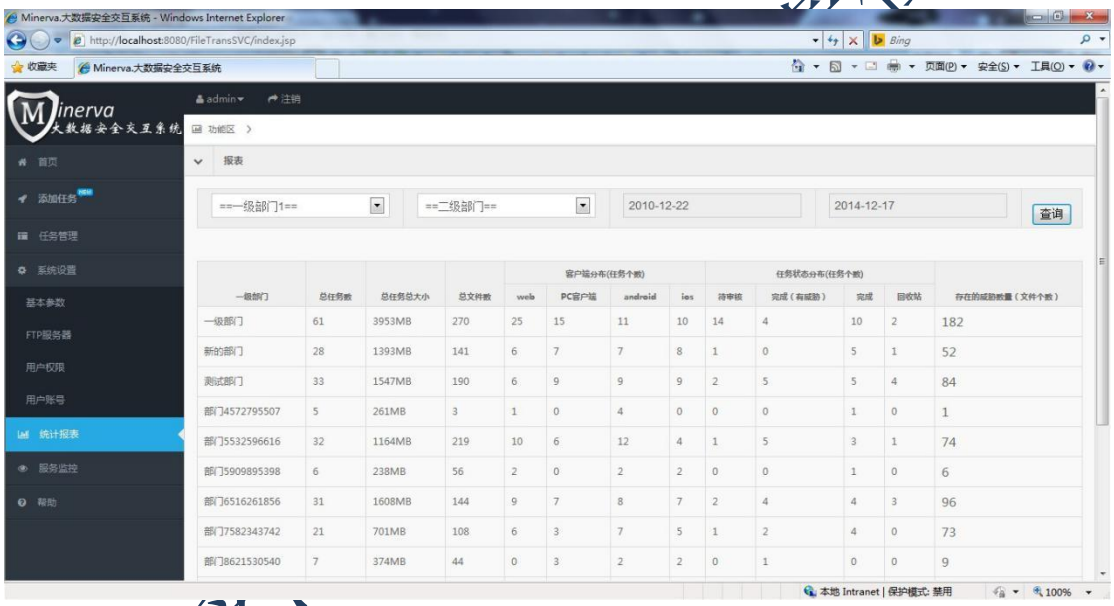
如果是移动介质，比如蓝光。这时你可以选择普通文件旁边的移动介质这个选项。

在选择完设备种类，和设备对应盘符后，点击扫描就能自动读出设备里面的文件。然后点击添加已选或者添加全部。输入任务名，在点添加任务即开始文件传输。

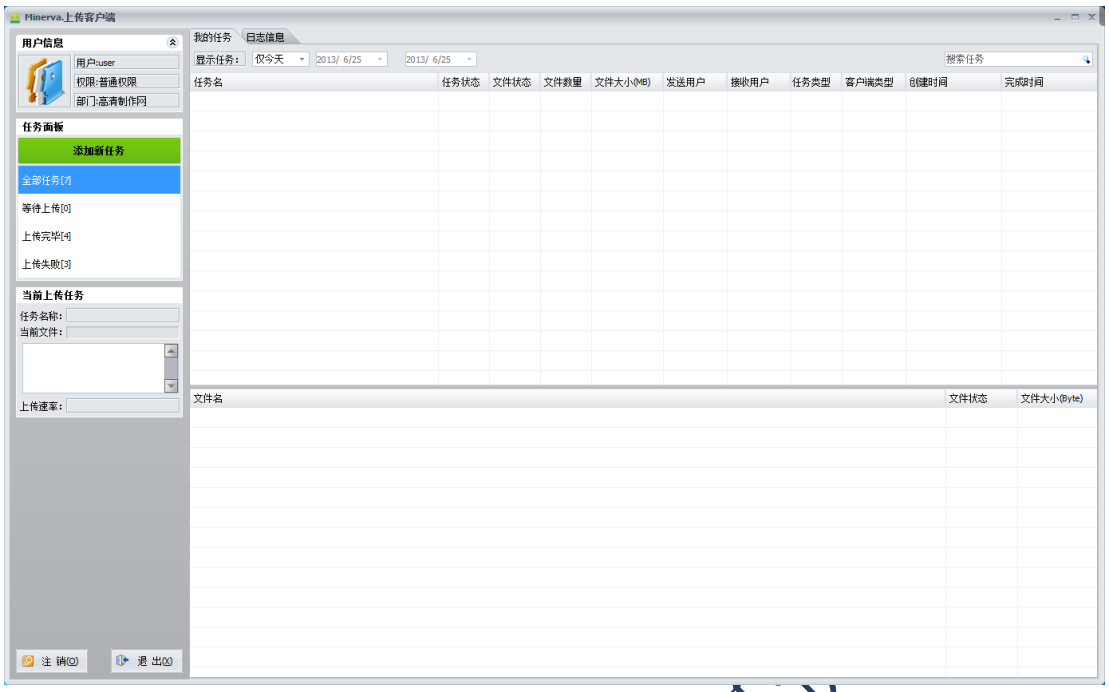
WEB 方式除了提供了方便的浏览器使用模式以外，还提供了其他强大的功能，其中包括了 WEB 远程进行系统配置、数据库相关配置，可读取数据库实时跟踪任务状态，并且可统计各部门各用户的使用情况，并形成相应报表。



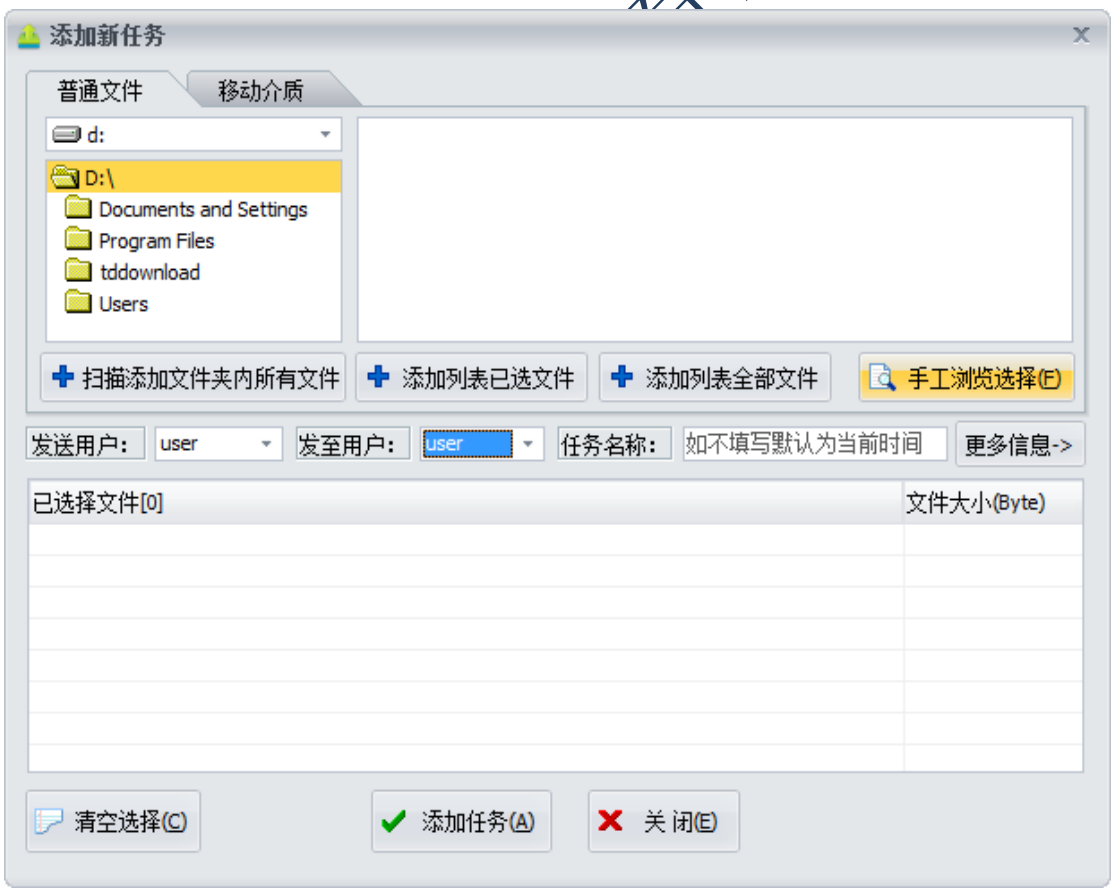

Minerva.大数据安全交互系统 - Windows Internet Explorer
http://localhost:8080/FileTransSVC/index.jsp
Minerva.大数据安全交互系统
admin
注销
功能区
首页
添加任务
任务管理
审核
发送
接收
回收站
系统设置
统计报表
服务监控
帮助
发送
审核
优先级
2014-12-17
2014-12-17
查询
本日
本周
本月
第1页/共13页
跳至
首页
上页
下页
末页
任务名称
优先级
任务进度
病毒检测
创建时间
任务9459692760
任务7440058753
asd
任务3353254275
任务1393808871
任务3746879605
a
kkkkkk
上传
待审核
已审核
病毒检测
网间交互
完成
待检测
2014-12-25 00:00:00.0
2014-12-19 00:00:00.0
2014-12-17 15:57:21.0
2014-12-17 00:00:00.0
2014-12-16 00:00:00.0
2014-12-15 00:00:00.0
2014-12-12 13:47:23.0
2014-12-12 13:40:49.0
Copyright © 2012 - 2014 重庆泛涵数码科技有限责任公司 All Rights Reserved.
Http://Www.FHMinerva.Com
本地 Intranet | 保护模式: 禁用
100%


Minerva.大数据安全交互系统 - Windows Internet Explorer
http://localhost:8080/FileTransSVC/index.jsp
Minerva.大数据安全交互系统
admin
注销
功能区
首页
添加任务
任务管理
系统设置
基本参数
FTP服务器
用户权限
用户账号
统计报表
服务监控
帮助
报表
==一级部门1==
==二级部门==
2010-12-22
2014-12-17
查询
一级部门
总任务数
总任务总大小
总文件数
客户端分布(任务个数)
web
PC客户端
android
ios
任务状态分布(任务个数)
待审核
完成（有威胁）
完成
回收站
存在的威胁数量（文件个数）
一级部门 61 3953MB 270 25 15 11 10 14 4 10 2 182
新的部门 28 1393MB 141 6 7 7 8 1 0 5 1 52
测试部门 33 1547MB 190 6 9 9 9 2 5 5 4 84
部门4572795507 5 261MB 3 1 0 4 0 0 0 1 0 1
部门5532596616 32 1164MB 219 10 6 12 4 1 5 3 1 74
部门5909895398 6 238MB 56 2 0 2 2 0 0 1 0 6
部门6516261856 31 1608MB 144 9 7 8 7 2 4 4 3 96
部门7582343742 21 701MB 108 6 3 7 5 1 2 4 0 73
部门8621530540 7 374MB 44 0 3 2 2 0 1 0 0 9
本地 Intranet | 保护模式: 禁用
100%

C/S 客户端上传模式：

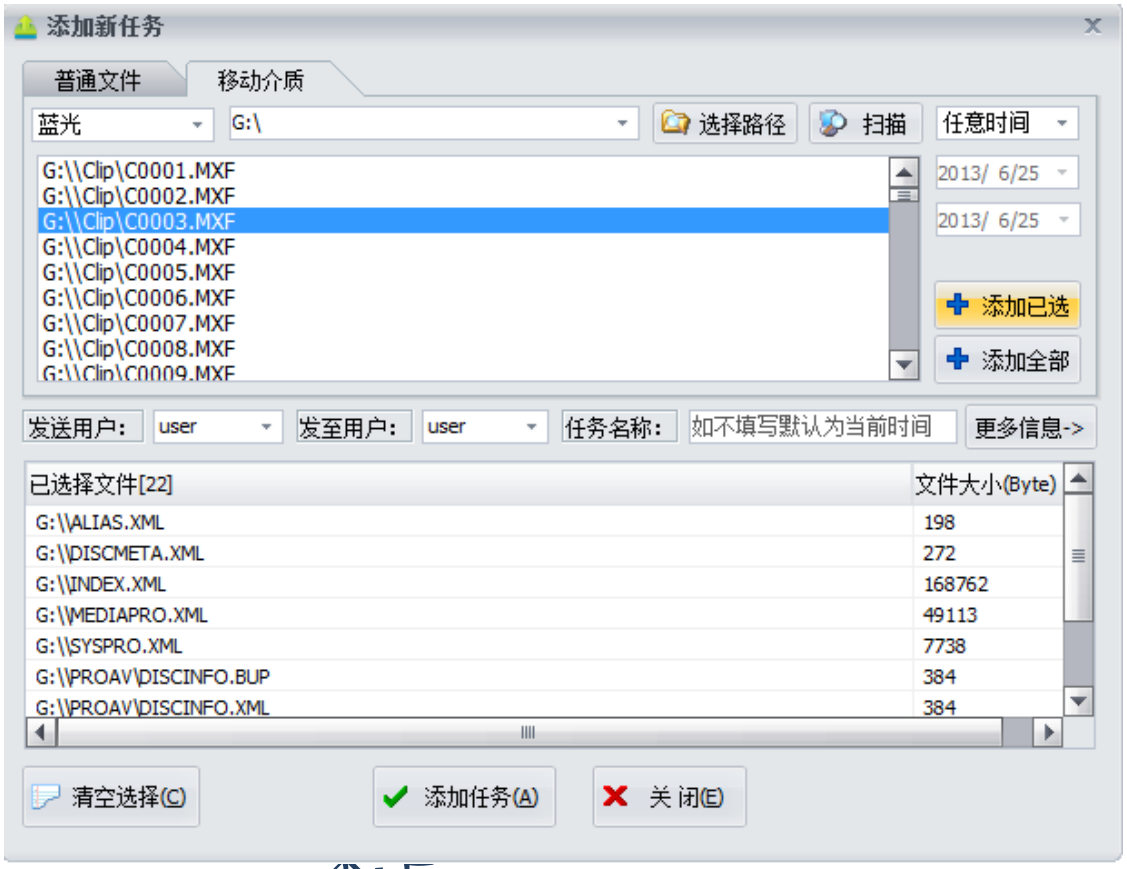


根据用户指定的检索方式扫描素材，可选择的预览素材并进行上传。



如果是移动介质，比如蓝光。这时你可以选择普通文件旁边的移动介质这个选项。

在选择完设备种类，和设备对应盘符后，点击扫描就能自动读出设备里面的文件。然后点击添加已选或者添加全部。输入任务名，在点添加任务即开始文件传输。

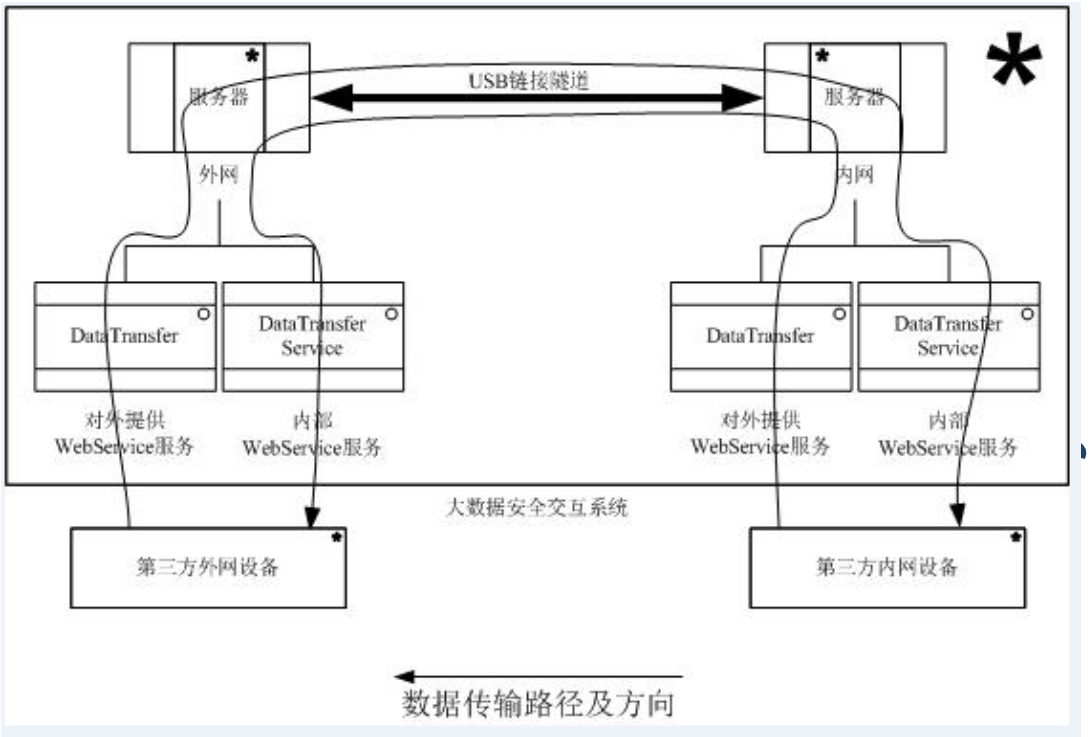


6、完善的运行状态监控

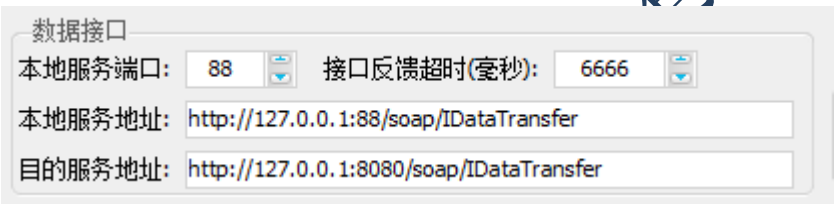
软件开启后，当前系统的通道状态、正在摆渡传输任务列表、待传输队列、已处理的任务数量等相关信息均显示在主程序界面的醒目位置。

7、丰富的对外接口支持

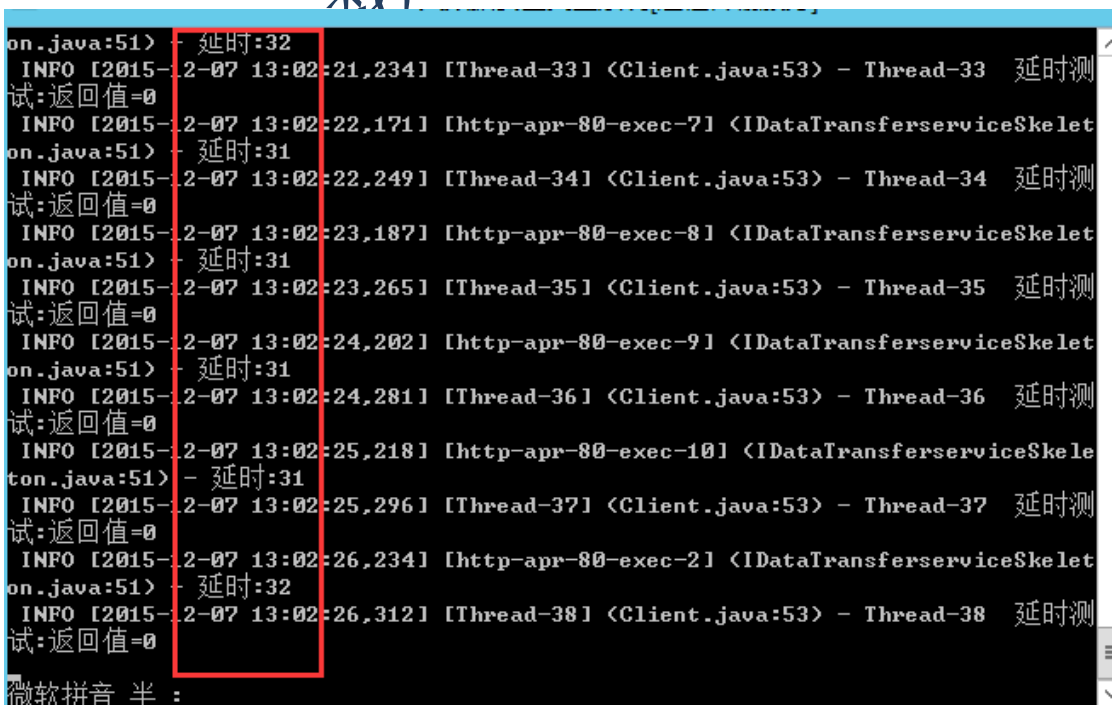
接口流程图：


服务器
USB链接隧道
服务器
外网
内网
DataTransfer
DataTransfer Service
DataTransfer
DataTransfer Service
对外提供WebService服务
内部WebService服务
对外提供WebService服务
内部WebService服务
大数据安全交互系统
第三方外网设备
第三方内网设备
数据传输路径及方向

接口配置：

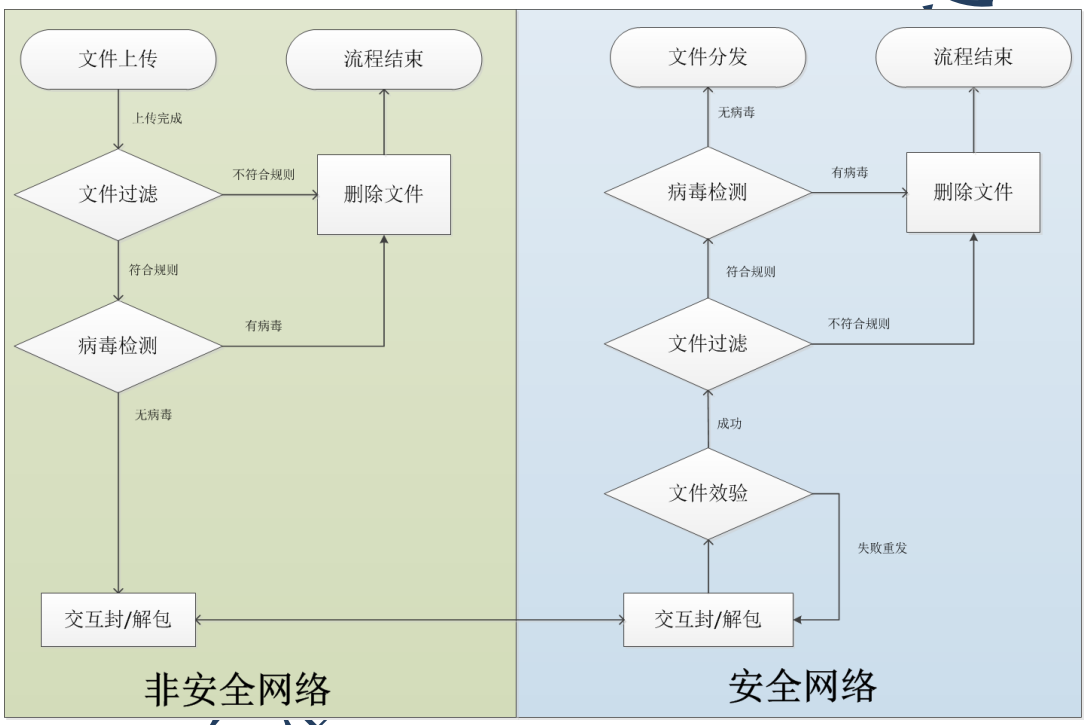

数据接口
本地服务端口: 88
接口反馈超时(毫秒): 6666
本地服务地址: http://127.0.0.1:88/soap/IDataTransfer
目的服务地址: http://127.0.0.1:8080/soap/IDataTransfer

测试延时：

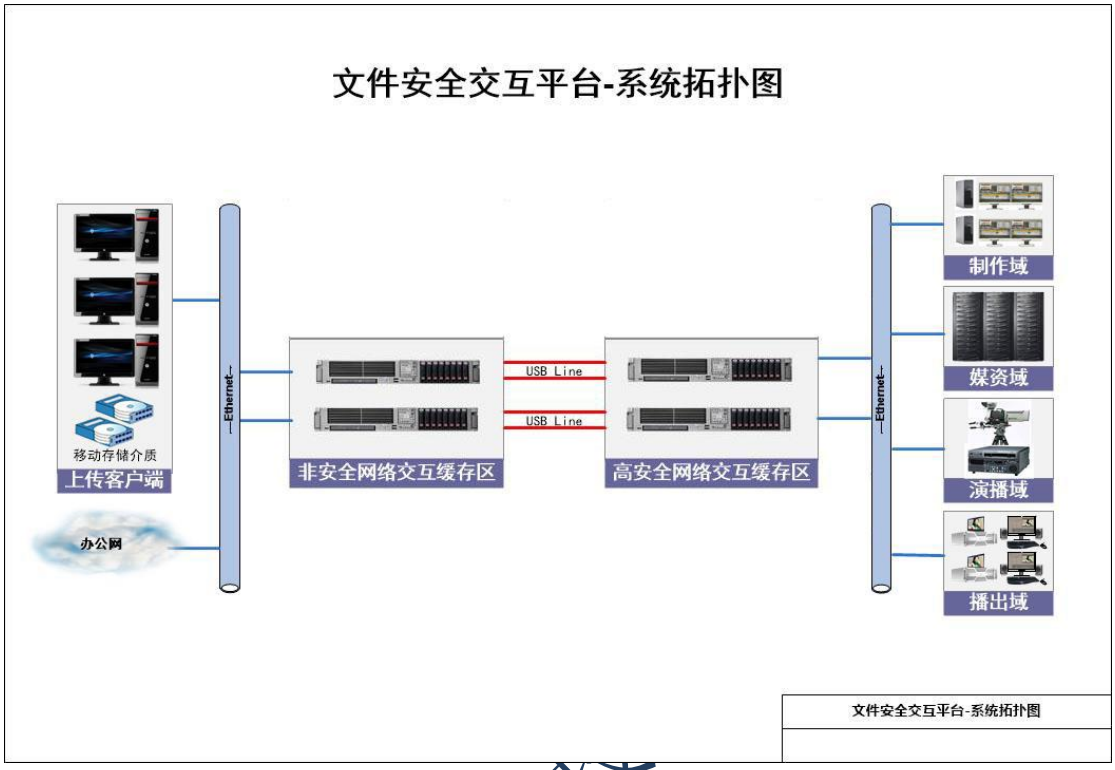

on.java:51) - 延时:32
INFO [2015-12-07 13:02:21,234] [Thread-33] (Client.java:53) - Thread-33 延时测试:返回值=0
INFO [2015-12-07 13:02:22,171] [http-apr-80-exec-7] (IDataTransferserviceSkeleton.java:51) - 延时:31
INFO [2015-12-07 13:02:22,249] [Thread-34] (Client.java:53) - Thread-34 延时测试:返回值=0
INFO [2015-12-07 13:02:23,187] [http-apr-80-exec-8] (IDataTransferserviceSkeleton.java:51) - 延时:31
INFO [2015-12-07 13:02:23,265] [Thread-35] (Client.java:53) - Thread-35 延时测试:返回值=0
INFO [2015-12-07 13:02:24,202] [http-apr-80-exec-9] (IDataTransferserviceSkeleton.java:51) - 延时:31
INFO [2015-12-07 13:02:24,281] [Thread-36] (Client.java:53) - Thread-36 延时测试:返回值=0
INFO [2015-12-07 13:02:25,218] [http-apr-80-exec-10] (IDataTransferserviceSkeleton.java:51) - 延时:31
INFO [2015-12-07 13:02:25,296] [Thread-37] (Client.java:53) - Thread-37 延时测试:返回值=0
INFO [2015-12-07 13:02:26,234] [http-apr-80-exec-2] (IDataTransferserviceSkeleton.java:51) - 延时:32
INFO [2015-12-07 13:02:26,312] [Thread-38] (Client.java:53) - Thread-38 延时测试:返回值=0
微软拼音 半 :

本系统支持通过接口（WebService、RESTful）的方式进行文件传输，也可以定制开发针对第三方业务系统的消息透传。通过系统开放的接口可以创建迁移任务、查询任务信息和状态、查询待传输队列、查询已完成列表等。可以将本系统纳入流程化管理。

二、系统工作流程



三、系统拓扑图



大数据安全交互平台：实现对所有数据的安全交互

第四章 需求分析

一、高安全区

随着电视台高清制播网建设的进一步展开，电视节目制作多元化及三网融合、IPTV、网络电视台建设的实际需要，生产网向办公网的业务延伸和拓展及办公网向生产网提供的服务也越来越多。目前只具备单一以太网通道，仅支持基于 WEB 方式的节目生产管理系统的高安全区，已经不能满足实际发展的需求。需要对现有高安全区进行扩容和改造。由于借助高安全区传输链路来实现的业务功能越来越多，每个参与业务交互的系统，单独建设服务系统和传输链路既浪费资源，又不利于维护。需要建设一个综合性的生产业务支撑平台，来统一为办公网与生产网间的交互业务提供服务。高安全区的扩容和改造，就是为综合性生产业务支撑平台提供基础传输链路。

1. 高安全区建设要求

对高安全区的建设，要充分考虑目前已建成的传输链路及在此上运行的业务。并且，高安全区作为综合性生产业务支撑平台的基础传输链路，要根据不同的需求设计不同的网络通道，不同的通道都要考虑以后的业务扩展，当相关业务大规模增加时，在不改变网络架构的同时，只需增加相应设备即可满足系统扩容。

- 优先确保生产网的安全性和业务连续性：

高安全区的建设打通了办公网与生产网之间的通道，极大的方便了业务交互。但这种便利性是以不损害生产网的安全性为前提的，生产网是电视台制播业务系统的核心，因此高安全区要采取多种

措施以确保生产网的安全性。高安全区的设计将通过多条通道实现，分别传输普通文件、控制信息和数据流文件，但这些数据的特点不同，其安全防护需求也不同，要对不同数据进行针对性的防护。综合分析在办公网和生产网间需要实现的交互业务，发现各类业务对安全的要求是不一致的，如从办公网向生产网传输数据，可以认为是从安全级别低的网络向安全级别高的网络传输数据，是需要重点防范的；而从生产网向办公网传输数据，则可认为是从安全级别高的网络向安全级别低的网络传输数据，重点是网络隔离的问题。考虑到数据类型的不同，以及数据传输的方向不同，需要分别建设以下两类传输通道。

- 控制信息、元数据传输通道：

  该通道传输控制信息及元数据，数据交互方向为双向，该通道主要考虑数据流的传输并且与其它系统的对接。所以考虑建设一条专门走数据流的通道。

- 办公网与生产网之间数据传输通道：

  该通道业务需求为双向传输通道，主要传输内容为媒体文件以及文稿等文件由办公网传入生产网。由于该通道数据来源是不可靠的，因此，对该通道的安全防护尤为重点。从办公网到生产网的数据为普通素材数据，只需建立一个文件传输通道来进行素材的传输即可。

二、数据安全交换系统

1、数据安全交换系统现有功能

数据安全交换系统，主要部署的异构杀毒，服务器之间由 USB 共享线缆相连，实现网络安全隔离传输。

- 数据分析功能

数据在被导入数据安全交换系统时，系统会对文件类型进行分析，判断文件类型的真实性（真实文件类型是否和后缀名一致）以及是否在允许导入文件类型的范围内，如发现异常将终止导入流程，提示人为干预执行。

- 数据自动杀毒传输功能

数据可以在三级杀毒传输服务器间，实现自动传输和自动触发杀毒程序进行病毒的扫描和查杀，运用 MD5 码校验功能，通过专用线缆私有协议，实现文件的高安全、高效率传输。对一次性触发的大量数据文件也具有良好的处理能力，具备较高的传输杀毒效率。

- 任务流程监控管理

所有通过数据安全交换系统导入到制播网络系统中的数据，都会以任务的形式存在于整个导入流程中。通过自动杀毒传输功能，实时地反映任务及任务中包含的数据在流程中的状态。

- 与其他系统进行无缝链接

所有通过数据安全交换系统的数据文件，都可以通过本系统的分发功能，到达诸如转码（视频格式转换）、文件高速技审、媒资管理

等业务系统中。同时，也可以通过本系统与转码、文件高速技审、媒资管理等业务系统等进行接口进行对接，向他们提供高安全区的服务。

三、客户端功能

1、数据导入导出客户端

- 用户登录。
- 能够同时导入多组数据，每组数据可包含多个同类型文件。
- 能够选择导入栏目组，默认为登录时候选择的栏目组。
- 能够判断文件类型。
- 能够实时反馈文件杀毒、传输状态。
- 能够导出本系统公共存储中本人的数据。
- 能够保存和管理历史传输记录。
- 能够实现制播网分数据的导出。

2、数据共享交换客户端

- 能够访问本系统公共存储中的全部数据文件，进行数据的管理。包括数据导出、栏目数据交换等。

四、服务端功能

1、数据库服务器

- 提供整个系统数据信息的后台管理服务。主要存放管理人员信息，

系统配置信息，数据传输通道信息等。

第五章 安全性设计

一、系统总体安全

安全数据交互业务支撑平台系统在广播电视信息系统中属于业务支撑系统，系统的总体安全性设计符合广电系统等保中所指定的二级要求。整个系统包含“硬件设施”和“软件应用”两个层面，保证基础设施层和应用上层的安全、稳定是系统稳定的必要条件。

整个系统中的核心设备采用冗余或集群的部署方式，关键链路采用双链路连接方式，对重要数据实施定期或实时备份的机制，对系统中各层制定相应的安全策略，提高系统的安全级别。

安全数据交互业务支撑平台系统中要保证业务的连续性，必须保证基础设施层、服务端。具体的方法有：

- **基础设施层的安全**

在基础设施层，所有的 PC 硬件均采用国内、外知名厂商的原装机，其 PC 服务器均采用校验（如:内存使用 ECC 校验）、冗余（如：电源、硬盘）等措施，极大降低硬件自身的故障，与此同时自身的硬件检测系统，能快速定位到故障点，提高排除故障的效率。

- **服务端系统安全**

在服务端的系统层面上，应用系统、数据库采用用户名使用唯一性、定期更换、禁止口令和用户名相同、启用登录失败处理等安全策略，防止用户被冒用和篡改；同时启用访问控制功能，依据安全策略控制用户对资源的访问，根据需要禁止通过 USB、光驱等外设进行数

据交换，关闭不必要的服务和端口；部署具有统一管理功能的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库，提高系统层面的安全级别。

- **网络数据库的数据安全**

网络数据库自身支持的集群部署方式，提高多点负载均衡、高可用性、提高事务的相应时间，实现故障容错和无缝切换。

系统为网络数据提供数据有效性检验功能，保证通过人机接口输入或通信接口输入的数据长度、格式、范围、数据类型等符合设定要求，防止诸如 SQL 注入、跨站攻击、溢出攻击等恶意行为，对非法输入进行明确的错误提示并报警。

二、系统数据备份

由于计算机系统的故障(硬件故障、网络故障、进程故障和系统故障)影响数据库系统的操作，使数据库中全部或部分数据丢失，造成业务间断或终止。为了尽快恢复业务，将对数据库进行恢复操作，但恢复的前提条件是备份。

数据库的备份的方式有多种，可采用数据库级的定时完全或增量备份，数据导出备份、最小备份系统等不同手段完成。安全数据交互业务支撑平台系统，数据是整个系统的核心，在各子系统中数据保证安全的情况下，安全数据交互业务支撑平台系统也必须对自己的数据做相应的安全策略。

系统数据库采用 RAC 的部署方式，避免了单点故障，为防止人为

对数据的误操作，系统的数据必须信息进行本地备份和恢复，完全数据备份至少每周一次，增量备份或差分备份至少每天一次，备份介质应在数据执行所在场地外存放。如果对进行异地备份，利用通信网络将关键数据定时批量传送至备用场地。