【软考达人】

软考资料免费获取

1、最新软考题库

2、软考备考资料

3、考前压轴题

微信扫一扫，立马获取

6W+免费题库

免费备考资料

PC版题库：ruankaodaren.com

手机端题库：微信搜索「软考达人」 / PC端题库：www.ruankaodaren.com

论信息系统安全性设计

摘要：

随着国内航空业的高速发展，机场空中交通日趋繁忙，机场空管有必要提前掌握空中态势，做好空中交通管制的准备工作。现阶段各个机场空管系统的信息获取手段单一，依赖本机场雷达提供的信息已不能满足场内空中交通管制的需要。为了改变这种现状，我单位对民航部分系统实施改造，开发了一个空管综合数据定制系统，使得机场空管能够根据业务需要自主定制所需信息，实现资源共享。 在整个项目中，我担任空管综合数据定制系统的主任设计师，负责空管综合数据定制系统分析、设计和开发工作。空管综合数据定制系统是 B/S 结构的 WEB 应用系统，用户登录系统后可以在有限的范围内自主定制飞行情报、气象情报等信息。在项目开发过程中，我们注重系统的安全性。在系统安全方面，我们采用登录控制、授权管理等方法保证用户访问安全；用日志记录加数据备份保障系统数据安全；用双机热备系统保障服务器系统运行安全。

正文：

国内民航空中交通管制按地理区域划分，由各大地区空中交通管理机构通过区域中心管制系统实现对各个机场空管系统的管理工作。机场空管的信息数据通过内部网络或专线等方式汇集到区管中心，运用数据融合等情报处理技术形成多种信息的统一态势，以便于对管制区内的飞行统一实施空中交通管制。 现阶段各个机场空管系统的信息获取手段较为单一，管制所需的数据来源处于一个“被动”状态。为改变这种现状，实现空管信息资源共享，我单位对地区空中交通管制系统进行初步改造，以实现机场对飞行情报、气象情报、飞行计划等信息的按需定制。 在该项目中，我参与项目的需求分析，并担任用户按需定制功能的主任设计师，负责设计和开发“空管综合信息数据定制系统”。该项目于 2010 年 8 月开始启动，历时 7 个月完成项目的开发工作，并于 2011 年 3 月投入试运行。目前系统已交付，运行至今相当稳定。 根据系统的功能需求，空管综合信息数据定制系统按功能分为用户管理，信息定制、数据查询与维护等部分。用户管理分为用户帐户管理、用户基本信息维护、用户定制权限管理。根据用户的类型，系统设置了两种用户的角色，分别是管理员用户和定制用户。信息定制功能根据信息的类型分为飞行情报定制、飞行计划定制、气象情报定制和飞行流量定制等。定制用户根据其定制类型权限可以分别不同类型的信息。数据查询与维护功能包括定制状态查询、日志数据查询、基础数据查询与维护等。 在系统开发初期，我们对系统的层次架构和系统环境进行仔细分析。定制并不限于在用户系统的哪一个席位上进行操作，并考虑到实现用户定制应对用户的客户端影响最小化，所以我们决定采用 B/S 架构，以 WEB 方式实现用户定制功能。这样也使得应用程序都存放在 WEB 服务器上，方便了系统的部署与维护，实现了零客户端。考虑到空管系统中 UNIX 操作系统的 HP 服务器，我们以 JAVA 为主要开发语言。为使系统有更好的可扩充性、灵活性与逻辑性，并实现系统的业务处理与显示相分离，系统采用 MVC 模式，结构分为表示层、业务层（控制层、业务逻辑层、数据访问层和消息发送层）、数据层。在系统中采用 Tomcat 作为 Web 服务器，数据库服务器则使用原来在空中交通管制系统中作为数据库服务器的 Oracle9i。 空管行业是一个比较特殊的行业，他们的系统有一个独立的网络，在物理上与互联网隔离。空管综合信息数据定制系统也是运行在他们内部网络上的 WEB 应用系统，所以在安全问题上，我们重点保证用户访问安全、数据安全以及系统的运行安全。 （一）保障用户的访问安全的措施 虽然系统运行在空管内部

软考达人：软考专业备考平台，免费提供6w+软考题库，1TB免费专业备考资料

手机端题库：微信搜索「软考达人」 / PC端题库：www.ruankaodaren.com

网络上，但是也必须保证只有合法用户才能访问系统。我们采用登录页面作为用户访问系统的首页，这也是 WEB 应用系统的通用模式。在这个页面上需要输入用户名与口令，系统验证正确后，用户才能进行下一步操作。用户名与密码需要从用户使用的客户端传输到 WEB 服务器上进行验证。如果是定制用户，则用户使用的计算机很可能与 WEB 服务器不在一个网段中，那么必须考虑对用户名与密码信息进行保护，防止数据的机密性的破坏。我们查找相关的 HTTP 安全技术，决定使用 HTTPS 安全技术保护用户名和密码信息在网络中的传输。TOMCAT 对 HTTPS 提供了直接的支持，实现起来也不复杂，但由于 HTTPS 连接过程比一般的 HTTP 连接要慢，所以我们也只在登录页面使用了 HTTPS 连接。 用户名和密码被保存在服务器端的数据库相关的用户信息表中，所以具有相应权限的数据库用户可以通过 oracle 客户端或者 Sql Plus 工具直接查看用户信息表的内容。为了防止用户密码的泄露，我们对密码字段的内容进行加密，然后再存储到数据库的表格中。我们编写了一个中间转换类实现对密码字段的转换，方便了系统对密码的读写操作。 在开发需求中，系统用户分为管理员用户和定制用户，这两种用户对系统有不同的访问范围和操作方式，而定制用户对定制情报数据也有不同的地理范围权限。因此，对用户进行操作权限控制也是我们必须考虑的安全性问题。 我们在用户登录时就根据用户名对用户的身份进行判断，针对不同类型的用户设计不同的访问界面和菜单，这也就使管理员和定制用户对应不同的功能。对于定制用户不同的定制地理范围权限，我们设计了一个类似定制界面中的 ActiveX 地图控件，管理员用户在授权管理时，在这个地图控件中绘制出一个地理区域，并将结果保存到定制用户的权限表中。这样在定制用户实施定制操作时，系统将他的地理范围权限显示在定制界面中的地图控件上，他所绘制的定制区域不能超出其地理范围权限，否则告警并要求他重新输入。 （二）数据安全的保护措施 对于系统的数据安全问题，我们通过两个方面的措施，一个是记录用户操作的日志；二是定时备份系统数据。 我们对定制用户的每一个定制操作及取消定制操作都进行了日志记录，以便于查找定制用户是否正常使用系统，和检查用户的定制范围是否在授权范围内。管理员需要对用户信息进行维护，对用户权限进行管理，以及对系统基础数据维护。我们对管理员的每一个操作也进行了日志记录。日志记录不但可以用于查询管理员和定制用户的操作历史记录，还有助于分析系统其它的功能问题，防止用户的误操作。 我们在 UNIX 服务器设置了一个定时任务，每天对系统的关键数据进行了备份；每周自动进行一次数据全备份。定时任务是个服务器上的 SHELL 脚本，执行数据库表格数据的备份，和一些运行数据文件的备份。对于系统自动产生的备份文件，我们采用人工的方式按期拷贝出来，转存到备份盘上，以释放服务器上的磁盘空间。 （三）系统运行安全机制 为保证系统的运行安全，我们采用了双机热备的方式。在服务器端运行着一主一备的服务器。服务器上运行着集群软件，主备服务器用“心跳”来检测对方的状态。这些状态包括数据库状态、WEB 服务器状态以及其它子进程的状态。备机一旦发现主机的某个子进程的状态失效，立即自动切换。这两台服务器上 oracle 数据库搭建了高级复制，以保证数据库中表格数据的同步。 从系统的实际运行效果上看，系统在安全性方面很好地符合了用户的需求。安全性是一个 WEB 应用系统必须重视的问题，不管系统运行在内网还是互联网。用户登录、用户权限、数据安全，以及系统运行安全等方面是 WEB 系统重要安全问题。我们在系统运行安全方面还有个异地备份需要考虑。现在状况是只在一个区域中心的系统运行综合数据定制系统，如果本地的系统出现故障，还需要一个异地和备中心来接替运行。但在主备中心的数据同步和状态通信上还存在不少需要解决的问题。

软考达人：软考专业备考平台，免费提供6w+软考题库，1TB免费专业备考资料