**UMOOC教学系统平台概要设计说明书**

**一、引言**

**1.1 概要简述**

概要设计是用来评价软件整体设计可行性的重要支撑标准，由于每个模块这个阶段已经开始确定，可以很好的检查已有的模块是否已经足够完整，还可以用于评估工作量以及知道下一步的主要计划，这里用合力的具体实现来展示项目的具体业务流程，它是一个纲领。

**1.2 编写目的**

本概要设计文档主要用来指导UMOOC软件教学系统平台的详细设计工作，为详细设计提供统一的参照标准，其中包括系统的总体设计、内外部接口、系统架构、编程模型以及其他各种主要问题的解决方案。

在此文档被经过同行评审后，所有有关本系统的详细设计必须遵照此文档的相关标准和约束来进行。另外，此文档也作为对详细设计文档进行同行评审所依照的标准之一。

在详细设计的过程中，如果发现需要添加新的概要设计标准或者约束来指导详细设计工作，必须在此文档进行更新和评审，以确保各模块详细设计的一致性和正确性。

本文档主要描述的是创新综合线上教育管理系统的概要设计，其中包括定义系统的内外部接口、相关的系统架构和设计标准，不会涉及系统业务逻辑现实的细节。

在对用户进行需求调研的基础上，根据需求分析说明书编写了本概要设计，以作为详细设计及系统实现的依据。本文主要阅读对象为相关技术人员和项目责任人。

**1.3 背景**

**1.3.1 “互联网+线上教育的概念及背景**

随着互联网+时代、全球化、知识化和信息化时代的来临，生活方式逐渐信息化,网络化,逐渐涌现了各种网上教学系统，网上教学近几年逐渐兴盛起来， 是未来教育的一种发展趋势， 网上教学能为教师的“教”和学生的“学“提供更广阔的灵活空间， 能打破地域、资源和时间的限制，让学生真正为自己的学习做主。有专家估计，在线教育将会在各行各业的培训活动中，发挥着越来越大的重要性。在线教育，完全是时代发展进步的产物。无论是从目前政策看，还是技术手段上看，都在推动着教育的变革和创新；同时享受教育升级的用户群体，受教育程度越来越高的80后、90后，互联网原住民00后，对线上教育的接受程度是超乎想象的。未来互联网+线上教育会成为一种趋势

线上教育既解决了传统培训机构的运营成本高、生源较局限、口碑传播率低、营销活动困难等问题，也解决了学员们信息知识不对等、学习场景单一、作业考试反馈慢等问题。

**1.4 基线**

UMOOC教学系统平台技术报告。

**1.5 术语和定义**

**用户：**被授权使用或负责维护应用信息系统的人员。

**用户帐号：**在应用信息系统中设置与保存、用于授予用户合法登陆和使用应用信息系统等权限的用户信息，包括用户名、密码以及用户真实姓名、学校、联系方式等基本信息内容。

**权限：**允许用户操作应用信息系统中某功能点或功能点集合的权力范围。

**角色：**应用信息系统中用于描述用户权限特征的权限类别名称。

**1.6 参考资料**

1. 《UMOOC教学系统技术报告》
2. 《UMOOC教学系统需求规格说明书》
3. 《UMOOC教学系统建设方案》
4. 《UMOOC教学系统开发计划说明书》
5. 《UMOOC教学系统原型设计说明书》

**二、总体设计**

**2.1 设计前提和约束条件**

1. 系统用户登陆通过与认证系统实名认证；
2. 有合理的通知功能；
3. 遵循项目开发文档所制定的规范；
4. 符合系统权限要求。

**2.2 基本设计思想**

UMOOC教学系统平台信息管理涉及各大高校、线上培训机构、等众多参与方，信息量巨大，信息交换复杂。传统培训机构的运营成本高、生源较局限、口碑传播率低、营销活动困难等问题，线上教育既解决了以上问题,也解决了学员们信息知识不对等、学习场景单一、作业考试反馈慢等问题因此，基于UMOOC教学系统平台的信息管理框架的构建思路的核心就是要改变传统的信息传递和共享方式，通过线上将不同阶段、都在推动着教育的变革和创新；真正实现教学系统平台项目全生命周期的线上管理教育。因此，基于教学系统平台的建设项目全生命周期信息管理框架的构建主要从以下三点展开：

**（1）数据问题：**

建设项目信息管理过程中，产生的信息形式多样，各参与方所用的信息管理软件不尽相同，如何实现BIM数据和其他形式数据的共享和利用，保证不同阶段产生的信息能够持续应用，而避免重复输入，就需要建立可以保证不同BIM应用之间的信息提取、关联及扩展的数据库，该数据库也是基于BIM的信息管理框架的基础。

**（2）信息模型：**

数据库是存储信息的地方，而信息模型是承载信息的载体。随着教学系统平台项目的进展，信息数据不断增加，如何保证这些信息分门别类有效地存储并传授给学生群体，需要在全生命周期不同阶段，针对不同的子系统形成子信息模型，由各子信息模型来承载不同专业和类别的功能工作，以保证线上教育的有效进行。子信息模型通过提取上一阶段信息模型中的数据，然后再经过扩展和集成，如此继续反复，最终形成全生命周期信息模型。

**（3）功能实现：**

对信息进行存储和高校教学管理的最终目的就是有效地应用信息，进行建设项目管理，因此，在管理框架的最上层为功能模块层。不同的功能模块对应着不同的BIM应用，也即为一个功能子信息模型。使用多种研发技术、中间件、设备搭建基于互联网环境的轻量化BIM信息管理平台；采用B/S架构构建平台；

具体通过以下技术实现：

1. 基于OpenGL的三维模型引擎，集成BIM+GIS数据；
2. 基于ActiveX的浏览器、移动端APP模型引擎部署；
3. 基于关系型数据库SQL Server的结构化构件数据存储、检索；
4. 基于React的H5前端研发技术；
5. 基于PHP的表单、流程处理功能开发；
6. 基于MySQL的业务表单、流程数据存储；
7. 基于萤石云的视频监控中间件集成。

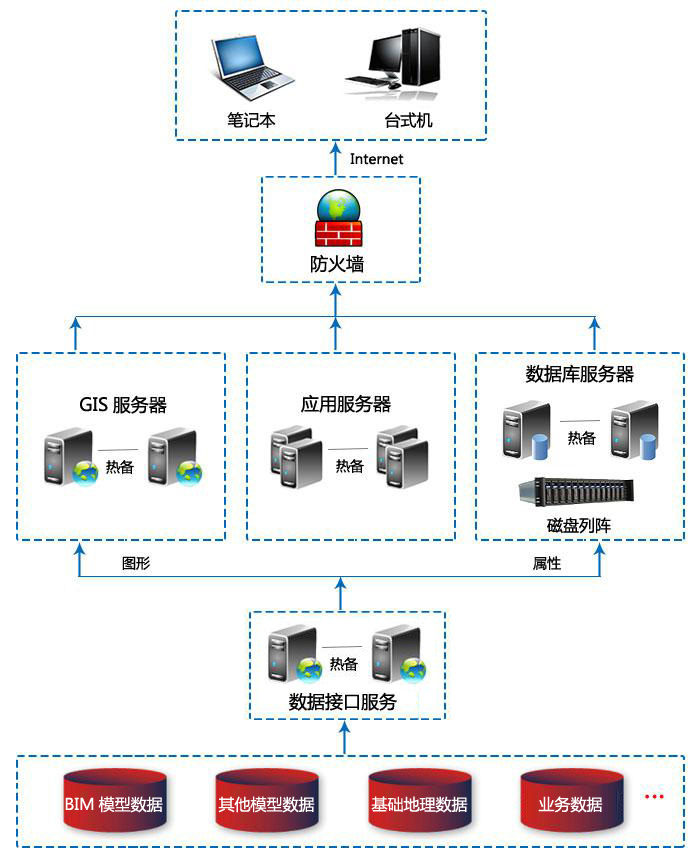
**2.3 系统整体结构设计**

系统整体结构图如下：

系统提供了web门户和移动APP门户两种方式，适用于PC、笔记、和手机等不同终端接入设备。

**2.4 物理部署关系图**

物理部署图如下：



**2.5 平台应用技术路线**

**2.6 需求规定**

* 网站内容建设：工程可视化信息展示子系统、工程设计协同管理子系统、工程建设协同管理子系统、工程运维管理子系统、系统管理平台。
* 安全系统建设：入侵防御系统、网络漏洞扫描、综合过滤网关、网络防病毒系统、网页防篡改及网站恢复系统的采购、集成。
* 硬件与系统软件建设：与网站相关的服务器及系统软件、KVM管理中心设备的采购、集成。

**2.6.1 服务器配置要求**

服务器系统平台建设要依据实用、先进、可靠、高效、易用、安全、可扩展原则，以满足大量老师,学生用户上网使用服务的要求。

服务器要具有强大的处理能力、快速的磁盘访问和高可靠性、高可用性的特点；同时服务器的体系结构要符合开放性的标准，具有可扩充性，最大范围地支持业界各种优秀的操作系统和服务软件，充分满足持续快速的业务发展需要。

主要服务器设备为：

* WEB服务器：Web服务器提供HTTP服务，是用户访问的接入口，是构造网站群应用的基础，本工程要求设置两台Web服务器，利用Web服务器软件的负载均衡功能，保证不间断对外服务。
* 数据库服务器：数据库服务器是应用系统中所有数据资源的管理中心。
* 应用服务器：应用服务器提供网站应用逻辑和动态服务栏目的功能处理，应用系统对服务器处理速度、内存、存储容量等方面有较高要求。
* 其它服务器：运行网站后台内容管理服务、跨网站检索服务、访问统计分析服务、视频点播服务、网络防病毒服务和网页防篡改发布服务等。

服务器和存储系统配置表如下：



**2.6.2 网络安全建设要求**

网络安全的建设目标要求针对网络在将来实际运行过程中可能遇到的各种安全威胁，采用防护、检测、反应、恢复四方面行之有效的安全措施，建立一个全方位并易于管理的安全体系，保障网络能够安全、稳定、可靠地运行，需要制定出安全体系的具体目标，以保证安全系统工程的实施。

主要体现：

* 提高可靠性：通过冗余措施加以保证，具体包括线路冗余、设备备份措施。
* 防范与Internet互联的安全威胁：在外网与Internet互连区采用安全可靠的防火墙。
* 采用防病毒措施：在两个方面防范。一方面建立完整的网络防毒机制，另一方面建立严格完善的防毒管理规范。
* 防范网络服务的安全威胁：确保必须的网络服务的安全和可靠性。如DNS；对其它网络基本服务，限制使用范围，建立严格的使用管理规定，防止被黑客利用，绝对禁止匿名FTP服务，对需要使用又必须保证安全的场合，要经过身份认证、访问授权和审计记录机制的控制。
* 阻止黑客攻击：在两个方面防护。一方面在Internet互联区域及与内网互连区域设置防火墙。另一方面采用防黑客攻击软件：1）实现安全漏洞的扫描，结合系统管理及时修补安全漏洞；2）提供网络实时入侵检测，在一定程度上实现对内网与外网的入侵阻隔；3）做好攻击的跟踪审计。
* 保障网站内容安全：防止网站数据被非法篡改，并且在被篡改后能及时恢复。

**2.6.3 平台建设目标**

本项目研究将以UMOOC教学系统平台工程建设为背景，将BIM技术应用贯穿设计、建设和运维全阶段，结合GIS、web等技术搭建一个大型线上教育全生命周期协同管理平台，实现信息资源集成、共享、更新和管理，保证信息的一致性，实现各高校与高校,学生与学生,学生与老师的交流交流、信息共享，实现对整个项目的动态控制，为管理和教育提供帮助，解决了学员们信息知识不对等、学习场景单一、作业考试反馈慢等问题,以构建“特大型教学系统基于BIM全生命周期协同管理平台”为核心，建立工程参建各方的信息网络和信息流动机制，结合计算机技术、BIM技术、数据分析技术，通过基于BIM的中心数据库建设及工程协同管理技术的研究，形成一套可在互联网+教育行业内复制推广的成套信息技术管理体系。

具体完成以下目标：

1. 满足施工项目管理过程中对BIM信息化平台的业务需求；
2. 满足业务需求在异构系统下的融合；
3. 满足多种类型终端的功能部署；
4. 形成BIM数据资产；

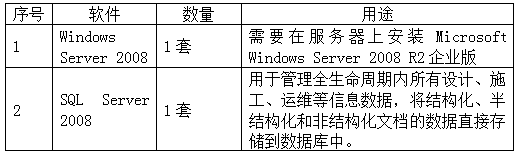
**2.7 运行环境**



**2.8 开发环境**

* 开发系统：CentOS
* 开发环境：Linux
* 开发语言：PHP、html5、javascript
* 数据库：Mysql

软件需求表如下：



**2.9 性能要求**

**2.9.1 处理能力**

系统面对多用户任务并发性，应保证正常的处理运行能力。

**2.9.2 稳定性**

系统资源利用合理，保证系统前后台数据操作效率。

**2.9.3 传输能力**

本系统业务功能包括课程附件视频,和图片传输，应提高文件传输速度。

**2.9.4 管理能力**

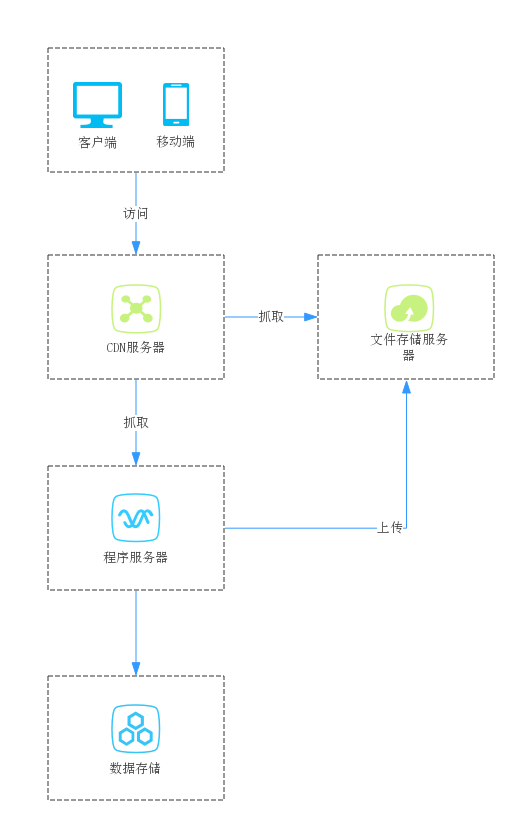
有序的对信息内容和模块进行合理的管理。

**2.10 基本设计概念和处理流程**

**2.10.1 平台结构**

系统的操作界面完全基于浏览器，程序服务系统划分为三种组件，模型 – 视图 – 控制器（MVC）设计定义它们之间的相互作用。

平台结构层次图如下：



系统具有良好的跨平台性，系统采用基于开发语言的一系列标准，使本系统可在各种硬件平台、操作系统、Web Server平台上进行方便的移植。

**模型（Model）**用于封装与应用程序的业务逻辑相关的数据以及对数据的处理方法。“Model”有对数据直接访问的权力，例如对数据库的访问。“Model”不依赖“View”和“Controller”——也就是说，Model 不关心它会被如何显示或是如何被操作。但是 Model 中数据的变化一般会通过一种刷新机制被公布。为了实现这种机制，那些用于监视此 Model 的 View 必须事先在此 Model 上注册，从而，View 可以了解在数据 Model 上发生的改变。

**视图（View）**能够实现数据有目的的显示（理论上，这不是必需的）。在 View 中一般没有程序上的逻辑。为了实现 View 上的刷新功能，View 需要访问它监视的数据模型（Model），因此应该事先在被它监视的数据那里注册。

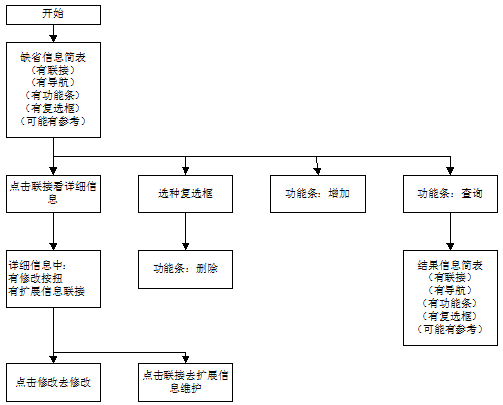
**控制器（Controller）**起到不同层面间的组织作用，用于控制应用程序的流程。它处理事件并作出响应。“事件”包括用户的行为和数据 Model 上的改变。

**2.10.2 系统软件设计模式的基本描述**

1. 用户在登录界面，输入操作员号，密码后，提交。
2. 用户有效性检查：客户密码有效性检查，用户状态检查。
3. 根据用户端提供的客户名称、口令，取出对应的加密后的口令，检查客户口令的正确性
4. 若用户登录不合法，则返回客户登录不成功界面
5. 若用户登录合法，进入客户登录后界面生成模块
6. 进入用户登录后界面，组织并生成客户登录后页面
7. 根据用户在页面上的操作分别进入不同处理流程
8. 用户点击通知信息条目，则在新窗口显示此通知信息内容
9. 用户点击指向课程的菜单条目，则再进入用户选择业务列表界面，界面中显示用户的专业课程列表。

**2.10.3 模块的标准流程**

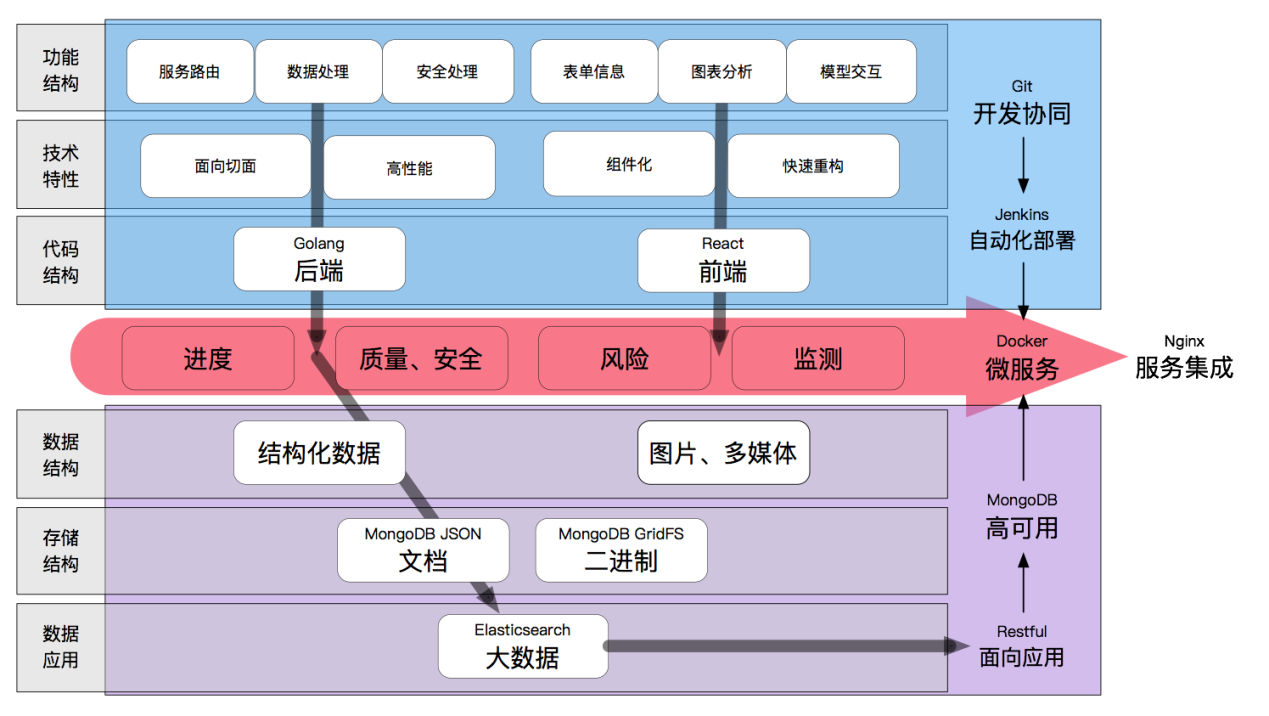
模块标准流程图如下：



**2.11 平台技术架构**

平台开发采用B/S架构，集成多种异构系统，结合代码协同工具Git，帮助研发人员完成协作开发，使用自动化运维工具，简化部署发布流程；

平台技术架构图：



**2.12 功能需求与程序的关系**

**2.12.1 概述**

网站群的应用系统功能主要分为三大类，网站前台发布展现功能、网站内容管理功能、网站其它应用系统后台管理功能。

* 网站前台发布展现功能主要提供给Internet用户，一般是网站浏览者，网站注册用户（个人和企业用户）。
* 网站内容管理功能、网站其它应用系统后台管理功能主要提供给系统管理员、网站管理员及相关单位网站信息管理员等。

**2.12.2 分配关系**

网站群主要功能模块与网站群应用系统的矩阵关系如下：



交互功能栏目包括：用户注册、用户登录。

其它应用子系统：资源中心系统、我的课程系统、随堂教学系统、个人中心系统。

**2.13 关键技术要点**

**2.13.1 多元异构模型融合**

将BIM模型导入GIS场景时，读取BIM模型的坐标系信息，自动计算与GIS坐标系的转换公式，并依据公式将BIM模型的所有坐标转换为GIS投影坐标，完成GIS与BIM的集成。针对Revit模型、GIS数据、测绘院模型等，通过分析格式之间的差异，在保证模型信息不丢失的前提下，基于格式扩展与转换技术，实现多模型无缝融合。

BIM与GIS应用领域的不同导致其具有不同的数据标准，数据模型上两者采用了不同的对象几何表达方式和语义描述方法。

前者是针对建筑设计和分析应用的几何表达，具有丰富的建筑构造、建筑设施的几何语义信息；后者更加强调对空间对象的多尺度表达，并顾及对象几何、拓扑和语义表达的一致性。

在几何表达方面，BIM模型通常采用的表达方式有三种：

边界表示法（B-rep），扫描体以及构造实体几何模型（CSG）。

在边界模型中，通过多个组成面拼接来呈现整个模型。扫描体是通过将平面对象沿路径拉伸或者绕轴旋转拉伸而得到。

结构实体几何模型（CSG）通常是通过将立方体、球体、圆柱体、圆锥体等基本体素作为基元实体类型，然后通过对这些基本实体进行几何变换、布尔运算以及剖割、局部修改等操作形成更加复杂的几何实体。而GIS中的三维几何主要采用边界表示法。

在语义信息表达上，从宏观上GIS模型包含有多尺度的语义描述，而BIM模型虽然具有丰富的语义信息却不具有多尺度表达的特点。

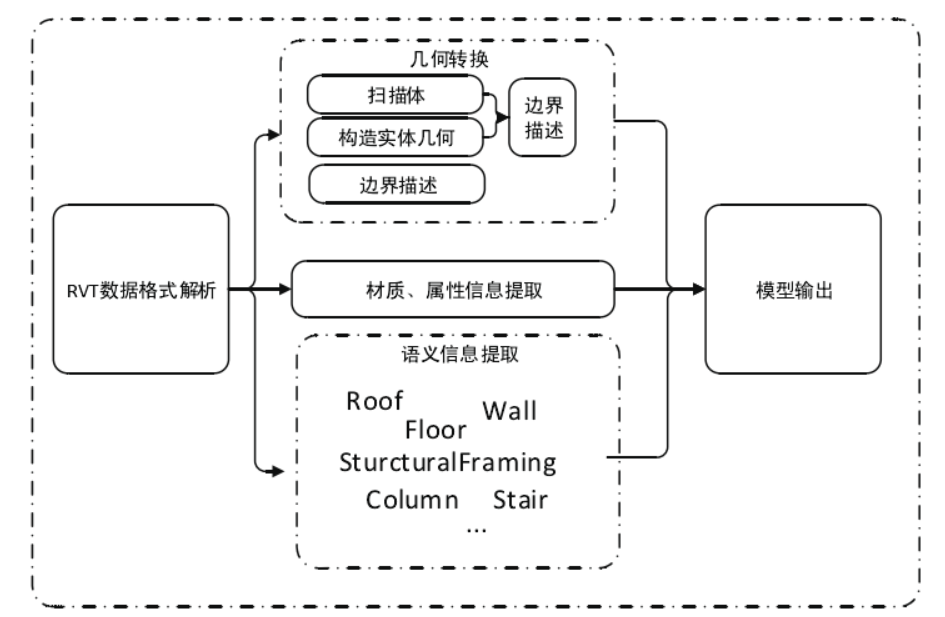
具体来讲，BIM模型包含有大量的建筑物细节描述，包括构件语义信息和部件间的语义连接关系，而GIS中语义信息采用多细节层次表达（LOD）技术，如CityGML标准将三维对象的精细程度分为五个细节层次。

LOD0在本质上就是2.5维的数字地形图，表达了建筑物的底面平面和屋顶平面；LOD1表达了平屋顶的棱状建筑，为块模型；LOD2表达了有分化的建筑物屋顶及其附属结构；LOD3在此基础上增加了墙体、屋顶、凹陷和突出部分等外观信息的细节性描述，可以将高分辨率的纹理映射到这些结构中；LOD4在LOD3的基础上增加了对内部结构的描述，如房间，内部门，楼梯和家具等，具有详细的几何和语义信息表达。

在BIM与GIS集成的过程中，数据模型的一致性转换成为当下急需解决的问题，Revit模型中包含了丰富的几何信息和语义信息；然而，在GIS系统中，不同的应用对数据模型的详细程度要求不一致，所以在数据转换的过程中，需要针对不同的应用需求进行相应的转换，涉及到几何简化，语义映射及语义输出的问题。

整体数据转换思路如下图所示：

整体转换流程图：



首先，获取模型语义信息，Revit模型中定义了从建筑、结构到暖通、机械、电气，管道等室内外建筑元素的语义类别信息。除此之外，每种建筑元素都包含有特定的属性信息，如建筑墙体会有是否为承重墙等标识属性。

其次，以这些类语义信息作为约束条件，构建过滤器，获取构件元素实体的几何信息和属性信息，并通过元素的ID标识将属性和几何信息关联。

最后，提取材质信息，Revit模型单独定义了材质元素，可以通过构建材质过滤器的方式，获取实际模型中所用的所有材质信息，并通过材质的ID标识和几何信息中相应材质关联起来。

Revit模型中包含了丰富的语义信息，涉及到建筑设计、建筑结构工程设计和暖通、电气、给排水工程设计等众多建筑学领域。选取Revit中常用的建筑元素，按照建筑、结构、管道和卫浴、机械设备、暖通（HVAC）等进行分块，定义了从室外到室内各类型建筑构件，见表1所列。

可根据GIS中不同LOD的表达需要，做相应的语义信息映射。

除此之外，RVT模型中还包含了建筑元素的建造阶段、拆除阶段、防火等级，成本，功能、制造商、结构用途以及物理性能等属性信息。

RVT模型中常用构建类别表如下：



**2.13.2 网络环境下的模型轻量化浏览**

对数据自动分层分块，内部用bsp树组织场景，客户端按需要请求必要的数据，保证每次请求的数据量不会太大，加快客户端加载速度。数据下载与模型渲染采用多线程方式并行处理，但模型渲染的优先级高，从而保证用户在浏览操作时不会因为数据下载而卡顿。数据下载模块同样采用多线程技术，同时采用异步机制，利用下载队列进行数据下载管理。

（1）模型优化

BIM模型数据内部存在很多冗余数据或者不必要的点面，导致数据量非常庞大。平台在进行BIM数据处理时，增加了多种优化数据选项供用户选择，包括：构件按族、类型、类别合并；构件自动生成LOD数据；抽取关键点坐标重构构件；平滑组优化等。

（2）渲染优化

① LOD技术：

能根据用户视角自动对模型简化生成不同精度的模型，从而对于距离摄像机比较远的模型采用其对应的粗模，这样就能保证用户体验效果的情况下大大减少了提交给显卡的数据量，减小了系统的渲染压力，提高了系统渲染速度。

② 多种场景剔除技术：

* 层剔除按摄像机在不同高度对相应的图层模型进行剔除；
* 投影面积剔除则是针对非常小的模型肉眼几乎无法识别的时候做隐藏处理；
* 子场景剔除可通过设定子场景范围，当摄像机位于子场景之外时，将子场景内部的模型做剔除处理。一般适用于包含室内场景及室外场景的场合。

③ 内存动态合并技术：

三维展现的基本机制是将三维模型数据提交给显卡，由显卡进行绘制渲染。由于显卡显存与计算机总线进行数据交换的数据通道宽度有限，过多的模型个数会造成数据通道的阻塞，形成IO瓶颈。

Q-MAP引擎采用内存动态合并的技术，将模型文件中的多个构件在内存中自动合并成一个模型，一次性推送给显卡，从而降低的渲染的批次，在不提升硬件水平的情况下提升展示的流畅度，同时又不影响对单个构件的查询定位。

**2.14 需要人工处理过程**

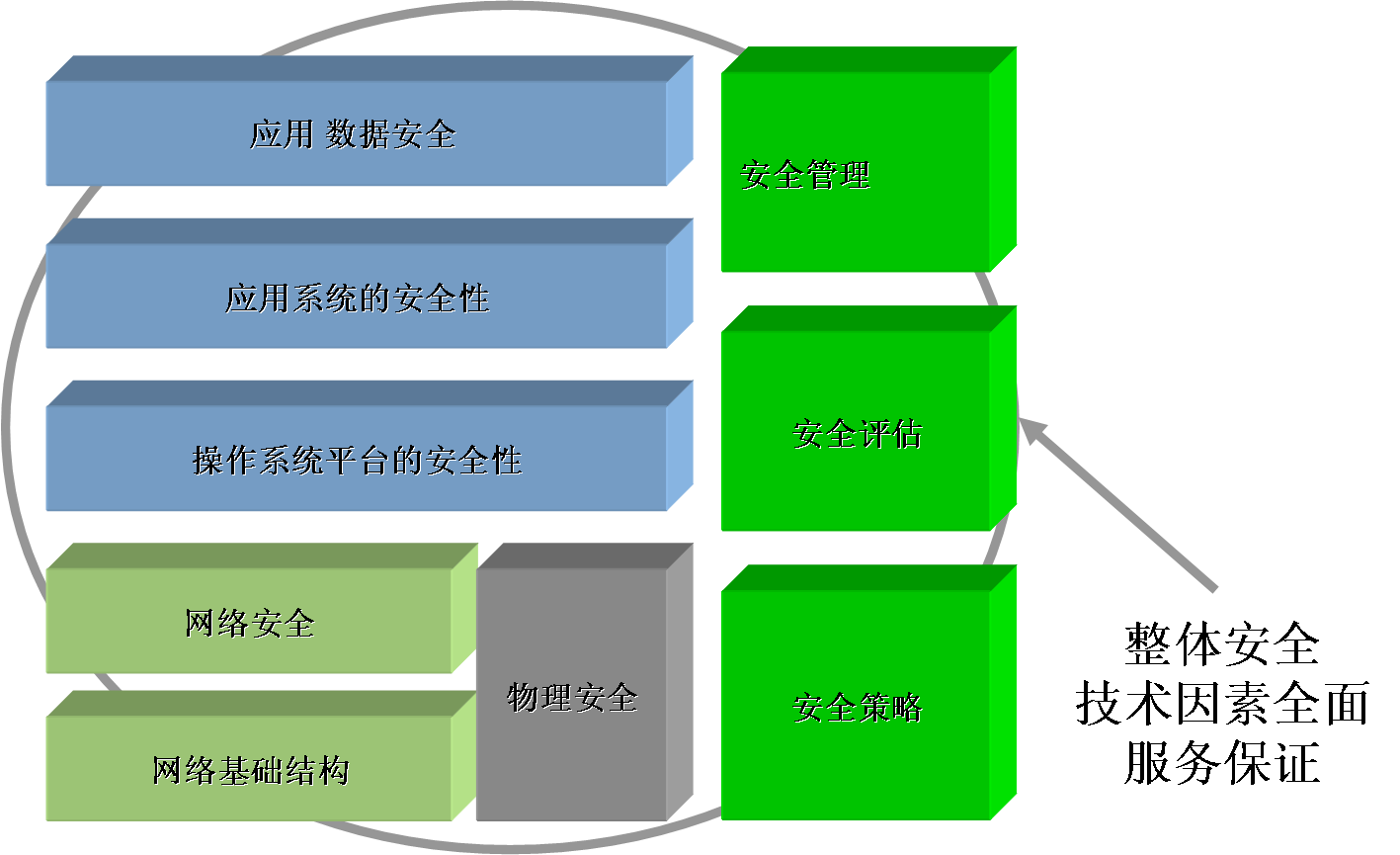
各种表单填制等需要填制的信息。

数据权限和功能权限需要管理员进行人工操作。

**三、安全设计**

**3.1 系统安全体系**

系统的安全体系可用下图表示：



整个系统的安全取决于系统运行物理环境的安全性、服务器及网络的安全性、操作系统的安全性、应用系统的安全性及应用数据的安全性等，通过设计实施整体的安全策略，对安全策略的实施结果进行评估，及时采取修复补救措施，调整安全预防策略，综合动态地进行系统安全管理。

创新综合管理系统的信息数据安全主要实现在业务流程控制和代码的详细设计中，对系统权限设计应充分考虑整体策略安全性。

由于本系统建立在我行现有的物理环境和网络环境中，环境安全性很好，并将不断完善优化，因此，有关本系统的安全设计的主要对象是系统自身的应用安全、数据安全、服务器操作系统和数据库的安全管理维护。

**3.2 系统面临的安全威胁**

本系统需要考虑系统及数据可能面临的以下安全威胁：

* 非人为因素：服务器意外断电、损坏、硬盘出错或损坏，网络中断等；
* 人为因素：操作失误，恶意攻击，病毒破坏等；
* 信息泄露、信息窃取、假冒、抵赖等；
* 系统软件安全漏洞。

**3.3 访问控制**

对于网络资源保持有限访问的原则，信息流向可根据安全需求实现单向或双向控制。采用防火墙进行访问控制，安置在不同安全区域出入口，对进出网络的IP信息包进行过滤并按设定的安全策略进行信息流控制。

**3.4 容错机制**

利用RAID提供的磁盘存储产品，可以在硬盘故障的情况下不影响数据的有效和使用。

采用RAID（0+1）模式，利用RAID1的数据镜像实现数据冗余，同时与RAID0一起增加数据读取速度。

**3.5 系统安全方案**

针对上述安全威胁，系统的安全运行依赖网络和服务器系统的安全，系统本身需要设计相应的安全监控功能。

**3.6 服务器及客户端系统安全**

对于数据库系统，进行相应的安全配置维护管理，根据实际情况及时进行安全策略调整，定期进行数据库系统的有关备份。

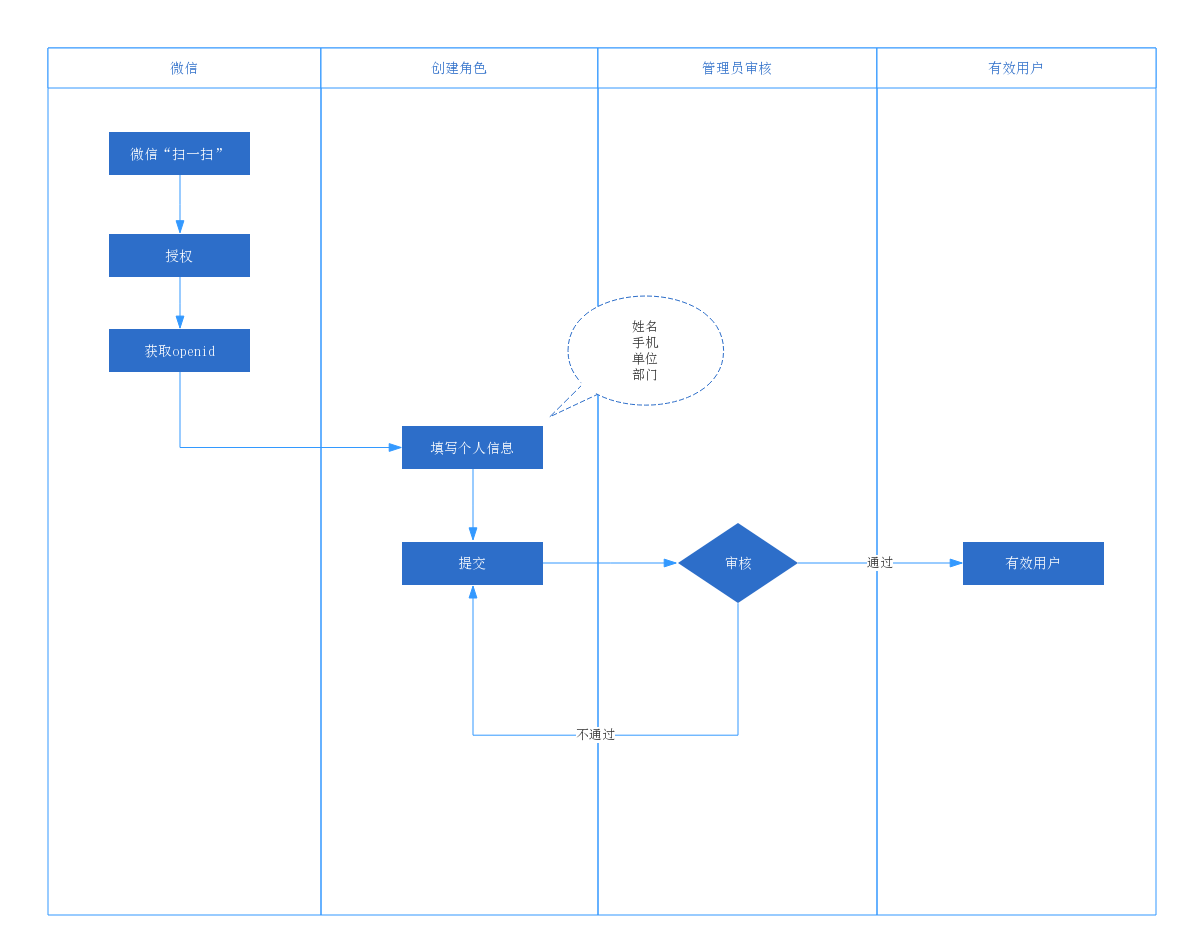
由于客户端计算机用途很开放，很容易受到病毒感染、恶意攻击等，可能会进一步影响到服务器，因此，对客户端计算机也要采取安全措施，进行相应的安全配置管理，如设置有效的系统密码，设置较高的浏览器级别，及时打补丁，安装反病毒程序，定期查杀病毒，根据实际情况及时采取安全措施。

**3.7 应用系统安全**

**3.7.1 用户系统**

该平台拥有灵活的用户体系，根据项目的实际需求，可创建不同的用户多用户角色，同时该角色可分配相应的操作权限。

用户登录方式图如下：



**3.7.2 权限系统**

权限系统一直以来是我们应用系统不可缺少的一个部分，若每个应用系统都重新对系统的权限进行设计，以满足不同系统用户的需求，将会浪费我们不少宝贵时间，所以花时间来设计一个相对通用的权限系统是很有意义的。

本系统的设计目标是对应用系统的所有资源进行权限控制，比如应用系统的功能菜单、各个界面的按钮控件等进行权限的操控。

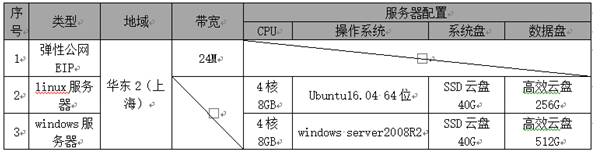
权限颗粒、节点权限、模块入口权限、添加、删除、修改。

**3.8 服务器设备配置规划**

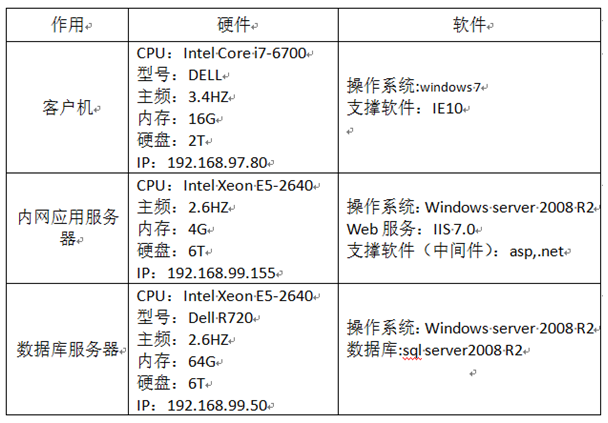
**3.8.1 需求规定**

XXXX管理平台主要为阿里云服务器。

**3.8.2 服务配置表**



**3.8.3 部署配置说明**



**3.9 网络安全设置**

**3.9.1 需求规定**

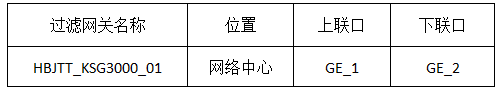
Internet 是自由开放的信息载体，对于网站群的建设不可避免的带来信息安全隐患。如果不设安全保护系统，Internet上的黑客很容易利用已存在的网络漏洞攻击系统内网的服务器，Internet上的病毒也会伺机入侵网站系统。

为了彻底解决网站群的安全性，确保其内网敏感信息不被泄漏、删除及篡改，要求网站群整体部署入侵防御系统、漏洞扫描系统、综合过滤网关系统、防病毒系统、网页防篡改及网站恢复系统，并制订相应的安全策略设计,在实际运行中最大程度上杜绝Internet带来的安全风险。

**3.9.2 网络安全规划设计**

3.9.2.1 综合过滤网关

综合过滤网关的连接方式如下图所示，安装在网络中心互联网出口，防火墙之后。采用透明模式，需要分配一个内网的管理地址进行管理配置，GE\_1口上连H3C防火墙，GE\_2口下连IPS的GE\_1口，管理端口连接在H3C核心交换机上。



综合过滤网关实现以下主要功能：

1. 防病毒引擎。过滤网关采用自有防病毒引擎，以保证防病毒网关在使用过程中病毒库、蠕虫库等的可持续性升级和病毒库数量和质量的持续保障。
2. 病毒过滤。全面过滤网页访问（http）、文件下载（ftp）、电子邮件（smtp、pop3）等形式的病毒和恶意代码，智能识别处理可疑病毒和伪装形式病毒，防止多种传播方式的病毒入侵破坏。
3. 蠕虫过滤。可以实现蠕虫过滤（过滤静态蠕虫扩散、阻断蠕虫动态攻击）。为修复漏洞和改进网络安全状况赢得宝贵时间。
4. 垃圾邮件过滤。通过垃圾邮件特征分析、规则库、黑白名单等技术，全面实现垃圾邮件双向过滤。
5. 非法内容过滤。通过关键字识别方法，对邮件头、正文、附件进行内容过滤，并支持URL过滤和网页脚本过滤。
6. 网络防御保护。可根据IP地址、端口、协议、连接频率和速率等对网络数据包进行控制，防止非法的网络访问活动。
7. 自动更新。根据预定义的更新频率与策略，可通过Internet自动实时更新特征码，并可实现系统内核的在线升级。

3.9.2.2 入侵防御系统

入侵防御系统的连接方式如上图（网络安全设备连接图）所示，安装在网络中心的互联网出口，过滤网关之后。采用透明模式，需要分配一个内网的管理地址进行管理配置，GE\_1口上连过滤网关的GE\_2口，GE\_2口下连光电转换器的千兆电口，管理端口连接在H3C核心交换机上。



入侵防御系统入侵检测就是对发生在计算机系统或者网络上的事件进行监视、分析是否出现入侵的过程。

入侵防御系统按照检测目标环境可分为两类：网络型入侵检测系统和主机型入侵检测系统，二者可独立应用也可协同作战。

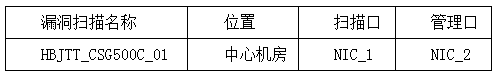
网络型入侵检测系统主要用于实时监控网络关键路径的信息，如同大楼内无处不在的电子监控系统，它采用旁路方式全面侦听网上信息流，动态监视网络上流过的所有数据包，进行检测和实时分析，从而实时甚至提前发现非法或异常行为，并且执行报警、阻断等功能，对事件的响应提供在线帮助，以最快的方式阻止入侵事件的发生。

并且能够全面的记录和管理日志，进行离线分析，对特殊事件提供智能判断和回放功能。

主机入侵检测系统是基于对主机的审计系统的信息进行监测，及时发现系统级用户的非法操作行为，可以用来实时监视可疑的连接、系统日志检查、非法访问的闯入等，并且提供对典型应用的监视，如Web服务器，电子邮件服务器等。

3.9.2.3 网络漏洞扫描系统

网络漏洞扫描系统的连接方式如上图（网络安全设备连接图）所示，该设备与核心交换机H3C 9500相连，其中NIC\_1端口作为扫描端口，NIC\_2端口作为网管端口。



网络漏洞扫描系统对整个网络进行安全扫描，以发现网络潜在的安全漏洞和薄弱环节，为整体的网络安全作出评估和测试。

另外，当网络的配置发生变化或者有其它的升级操作时，也应该进行同样的操作，防止网络发生变化时产生安全漏洞，给非法入侵者造成机会。

通常包括功能相对独立的三部分：

* 全面地扫描每个网络设备的安全漏洞并自动推荐合适的校正措施，呈现一张所有网络设备安全漏洞的全方位视图；
* 从操作系统的角度检测专用主机的整个安全性，允许管理员任意从远程自动更正分散网络上的安全漏洞；
* 通过网络快速、方便地扫描数据库，去检查数据库特有的安全漏洞，全面评估所有的安全漏洞和认证、授权、完整性方面的问题。

3.9.2.4 网络防病毒系统

网络防病毒系统部署在服务器（应用服务器）上。

网络防病毒系统能实现以下主要功能：

（1）网络防病毒集中管理和部署

* 强大、灵活的管理和任务调度手段，允许管理员通过中心控制台，集中地实现全网范围内防毒策略的定制、分发和执行；
* 管理员通过控制台，集中地实现所有节点上防毒软件的监控、配置、查询等管理工作；
* 病毒扫描引擎和代码库的更新，并能将此扫描引擎和代码库自动提供给各种服务器和工作站；
* 提供出色的事件报警、汇总、统计等辅助决策功能，可以随时对网络中病毒发生的情况进行查询统计，能按时间（日、周或任意时间段）、按IP地址、机器名、按病毒名称、病毒类型进行统计查询；使管理人员随时了解网络及病毒的宏观概况；
* 灵活的管理方式，可以支持集中和分布式管理，分布式管理可以跨越广域网，跨广域网时需要有效地利用带宽；
* 提供对手提电脑移动用户离开办公室后病毒防治的方案，包括病毒库的升级。

（2）网络防病毒处理能力

* 发现病毒后，有多种处理方法，例如清除、删除或隔离，以清除为主；采用伪指令技术，杀毒无需专杀工具。
* 支持邮件客户端防病毒，如：Outlook、foxmail邮件客户端；对SMTP、POP3进出邮件进程病毒监控；
* 全面监控所有病毒入口，对来自Internet、E-mail或是光盘、软盘移动存储、网络这些病毒入口，无论是宏病毒、特洛伊木马、黑客程序和有害程序全面进行实时监控；
* 支持查杀多种压缩格式的文件，同时不限压缩层数，能清除常见格式的压缩文件中的病毒。

（3）及时更新和响应

* 提供占用网络通讯流量最小的增量病毒定义码、引擎的更新升级方式；
* 提供多种方式的更新升级方法。

3.9.2.5 网页防篡改及恢复系统

网页防篡改及恢复软件系统部署在服务器（应用服务器）上。

网页防篡改及恢复系统能够完全保护网站不发送被篡改的页面，主要功能目标如下：

（1）动态网页脚本保护

采用核心内嵌技术的系统，可以直接从Web服务器上得到动态网页脚本，不受变化的内容影响，因而能够象静态网页一样保护动态网页脚本。

（2）连续篡改攻击保护

有意进行恶意攻击的黑客可以利用外挂轮询技术的扫描间隔来进行连续的篡改攻击，即在网页被恢复后立即重新篡改网页。而系统在每次输出网页时都进行完整性检查，如有变化则阻断发送。无论连续攻击多么迅速，保证不让公众看到被篡改的网页。

**四、功能设计**

**4.1 功能总体设计**

本平台共分为6个应用系统：资源中心子系统、我的课程管理子系统、随堂教学管理子系统、个人中心子系统、课程活动子系统、课程资源子系统、。

**4.1.1 需求规定**

基于BIM全生命周期线上教育管理平台整个系统分为资源中心子系统、我的课程管理子系统、随堂教学管理子系统、个人中心子系统、课程活动子系统、课程资源子系统、六个子系统。

**4.1.2 基本设计**

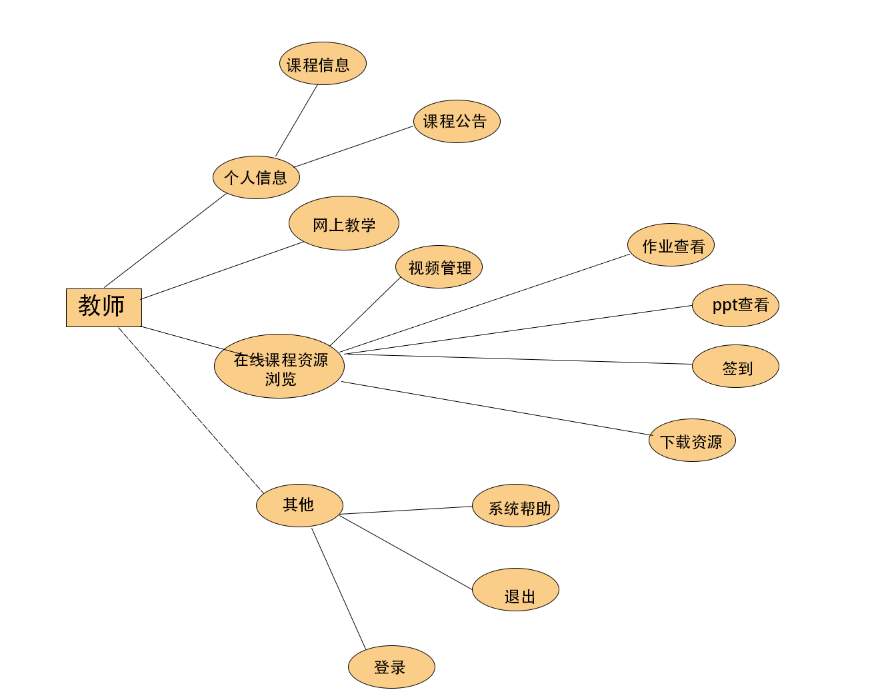
4.1.2.1 总体内容设计

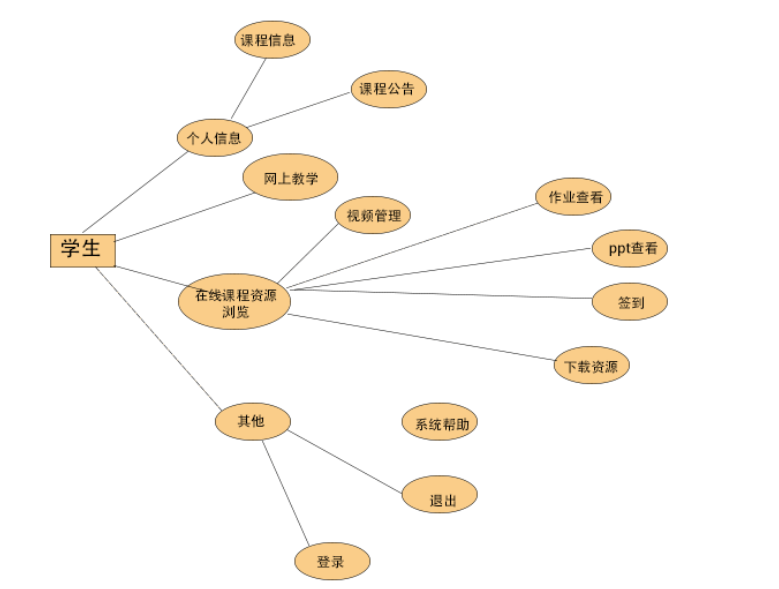
平台整体结构设计如下：

* 用户管理
* 用户列表
* 用户组列表
* 课程中心
* 个人中心
* 资源中心
* 课程活动
* 学习统计分析
* 学生学习进度管理
* 学生课程进度查看
* 计划维护
* 进度报告
* 计划变更
* 课程管理
* 时间统计
* 视频列表

4.1.2.2 系统功能模块图

4.1.2.3 系统业务流程图





4.1.2.4 用户接口设计

Internet用户在客户端IE地址栏输入站点URL“beiheng.suadi.com.cn”即可访问到首页。

**（1）轻量化访问：**

将平台整体进行轻量化处理，用户可以使用手机、平板灯移动设备高效、快速、随时随地查询浏览模型。

**（2）信息推送：**

用户可以通过手机、平板等各种移动设备随时随地记录与推送包括文字、声音、图片、视频等各类信息，实现在线实时沟通和信息共享。

**五、接口设计**

上海市地下空间设计研究总院系统是B/S结构的，它提供友好的浏览页面，利用HTTP协议交互与用户之间的操作指令、数据信息。用户各种操作都是通过浏览器来实现的，数据格式是以字符串的形式传到服务器，同时使用Ftp协议完成附件的上传和文件的下载。

**5.1 用户接口**

本系统有两种类型的用户接口，一般用户接口和管理员用户接口。

1. 一般用户的接口关系图：



网站注册用户登录后进入个人中心，使用网站服务功能。

系统管理员和网站管理员的接口关系图：

系统管理员或网站管理员登录管理中心，对特定功能模块进行管理。

系统管理员或者网站管理员登录CMS管理系统，对网站结构、网站内容、模板样式等进行管理。

**5.2 外部接口**

**5.3 内部接口**

内部接口方面，各模块之间采用函数调用、参数传递、返回值的方式进行信息传递。具体参数的结构将在数据结构设计的内容中说明。接口传递的信息将是以数据结构封装了的数据，以参数传递或返回值的形式在各模块间传输。

**六、运行设计**

**6.1 运行模块组合**

客户端在有输入时启动接收数据模块，通过各模块之间的调用，读入并对输入进行格式化。

在接收数据模块得到充分的数据时，将调用网络传输模块，将数据通过网络送到服务器，并等待接收服务器返回的信息。接收到返回信息后随即调用数据输出模块，对信息进行处理，产生相应的输出。

服务器程序的接收网络数据模块必须始终处于活动状态。接收到数据后，调用数据处理/查询模块对数据库进行访问，完成后调用网络发送模块，将信息返回客户机。

**6.2 运行控制**

运行控制将严格按照各模块间函数调用关系来实现。在各事务中心模块中，需对运行控制进行正确的判断，选择正确的运行控制路径。

在网络传方面，客户端在发送数据后，将等待服务器的确认收到反馈，收到后，再次等待服务器发送回答数据，然后对数据进行确认。服务器在接到数据后发送确认信号，在对数据处理、访问数据库后，将返回信息送回客户端，并等待确认。

**七、系统数据结构设计**

**7.1 逻辑结构设计要点**

设计遵循的标准：

（1）表名定义标准:

类型：指定该表属于什么类型的哪一部分，长度是6。

描述：该表的简单描述，长度是8。

所有表名长度是14。

例如：

prms\_resourceprms

指该表是一个资源权限表。

（2）域名的定义标准：

<Field data >\_<Field one>

域的数据类别+域的描述

域的数据类型:特定的域数据类型,长度是1.

域的描述1该域的简单描述.

例如：

prms\_id

指该域名是资源权限类别ID.

（3）索引名定义标准：

XK\_<Table name >\_<Other symbol>

X—用’X’表明该对象是一个索引.

索引类型:

* P：主键索引
* U：唯一的索引
* R：通常索引

表名描述：

最好用表明描述作为索引名的一部分。

其他字符：可以加域名描述或其他作为索引名的一部分。

**7.2 部分数据结构**

这部分是数据字典方面的内容，由于牵扯到数据的问题，在这里就不一一展示，就用一张表来作为案例：

**八、容灾设计**

**8.1 出错情况**

本设计要考虑的出错情况主要是指软件运行、系统部署时可能出现的异常,包括：

* 用户不规范的输入导致的程序错误；
* 系统运行时容器崩溃；
* 用户环境和开发时环境不一致造成的程序错误；
* 编码中的逻辑错误或者漏洞导致系统报错；

不包括由于硬件损伤、网络中断等情况的容错处理。

**8.2 异常处理**

本系统将采用如下的一般性设计原则减少程序和用户交互过程中可能出现的错误：

**（1）一致性**

* 菜单选择、数据显示以及其它功能都应使用一致的格式；
* 提供有意义的反馈信息；
* 执行有较大破坏性的动作前要求确认；
* 在数据录入上进行尽可能严格的合法性检测；
* 减少在动作间必须记忆的信息数量；
* 允许用户非恶意错误，系统应保护自己不受致命的破坏；
* 提供和运行环境相关的帮助机制。

**（2）本系统对于出错信息和警告应该遵循以下原则**

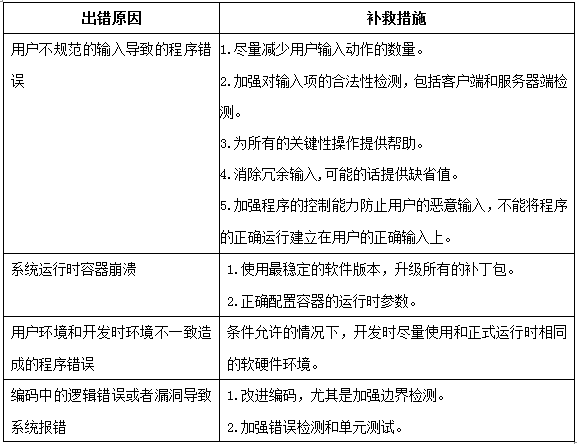
* 信息以用户可以理解的术语描述；
* 信息应提供如何从错误中恢复的建设性意见；
* 信息应指出错误可能导致哪些不良后果，以便用户检查是否出现了这些情况或帮助用户进行改正；
* 信息应伴随着视觉上的提示，如特殊的图像、颜色或信息闪烁；
* 信息不能带有判断色彩，即任何情况下不能指责用户。

系统采用统一的异常捕获和处理机制，为了便于团队开发的一致性，统一定义错误代码和友好显示信息。开发过程中根据具体情况可以扩展错误信息，制定更加详细的错误分类和信息显示。

为规范、统一各类系统错误或业务提示信息，统一定义公共信息列表。根据信息的性质与应用范围，将公共信息分类列表如下：



**8.3 补救措施**



**8.4 容灾备份**

利用RAID5数据存储解决方案，实现实时数据备份,保障了系统的安全稳定运行。

**8.5 系统维护设计**

**8.5.1 设备运行维护**

* 设备运行维护指对网站群网络、服务器硬件设备、网络安全设备的运行管理维护，保证硬件设备正常运行。
* 设备运行维护由专业的硬件工程师进行，处理日常的设备管理、运行配置等操作。
* 设备运行维护按照设备操作手册与要求执行。

**8.5.2 应用系统运行维护**

主要负责对网站群所有应用系统软件的运行维护管理工作，一般由网站群系统管理员负责，处理应用系统日常数据维护、运行配置、软件应用异常处理等。

系统管理员将根据日志信息记录对系统进行维护处理。在该系统中，将规范统一系统日志管理，系统日志的信息级别分为一般信息、调试信息、警告信息、严重错误信息。

**8.5.3 系统安全与数据备份恢复维护**

由网站群系统安全管理员负责网络硬件、软件安全管理，同时，按照规范处理日常的数据备份工作，对系统安全异常情况，立即进行恢复应急处理。

日常数据备份内容一般包括数据库数据备份和网站用户上传的文件数据备份。

系统安全管理员严格按照安全管理制度进行日常管理工作。

**8.5.4 网站信息内容管理维护**

由专业的内容信息维护人员负责网站内容信息管理、策划，按照网站日常运行需求，策划网页内容建设。

**结语**

概要设计是一个将用户目标与需求转换成具体界面设计方案的重要阶段，在这里我们将要由前一阶段的需求分析得到软件（包括移动应用和网站等）的设计和数据结构。

概要设计通常是将复杂的系统按照不同的功能进行模块化，理清模块之间的层次关系以及调用关系、确定模块间的接口以及用户界面。而数据结构部分则是要根据数据的特征来确定数据的结构并设计出相应的数据库。