**微波成像重点实验室SAR综合处理软件（MSARPro）**

**总体设计说明书**

**版本：V1.0**

北京超图软件股份有限公司

2016年12月

# 引言

本文是微波成像重点实验室SAR综合处理软件（MSARPro）总体设计说明书。

## 编写目的

本文档作为中国科学院电子学研究所与北京超图软件股份有限公司之间就建设“微波成像重点实验室SAR综合处理软件（MSARPro）”系统需求理解达成一致共识的基础文件，作为双方界定项目范围、签定合同的主要基础，也作为本项目验收的主要依据。同时，本文档也作为系统后继工作开展的基础，供双方项目主管负责人、项目经理、技术开发人员、测试人员等理解需求之用。

## 预期读者

本文档适用于所有与本项目有关的软件开发阶段及其相关人员，其中：中国科学院电子学研究所项目负责人、公司方项目经理、技术开发人员（包括分析人员、设计人员、程序人员）、测试人员应重点阅读本文档各部分，其他人员可选择性阅读本文档。

## 文档概述

本文档主要描述了“微波成像重点实验室SAR综合处理软件（MSARPro）”系统项目的软件总体设计思路。 本文档首先从业务背景、系统功能、运行环境等方面概要描述系统，其次从设计原则、功能设计、数据结构设计等方面描述系统的总体设计情况，然后进一步详细描述系统技术实现策略、项目实施以及待确定的问题。

## 引用文件

《微波成像重点实验室SAR综合处理软件（MSARPro）-开发合同书》

《微波成像重点实验室SAR综合处理软件（MSARPro）－系统建设需求》

# 项目背景

## 项目背景

项目名称：微波成像重点实验室SAR综合处理软件（MSARPro）

提出者：中国科学院电子学研究所

开发者：北京超图软件股份有限公司

用户：中国科学院电子学研究所

## 项目目标

“微波成像重点实验室SAR综合处理软件（MSARPro）”在前期建设的成果基础上，增加通用图像处理、遥感图像处理以及基于SAR图像处理的GIS功能。

# 用户需求成果分析

## 功能需求

“微波成像重点实验室SAR综合处理软件（MSARPro）”系统主要在原有系统基础上新增通用图像处理、遥感图像处理以及基于SAR图像处理的GIS功能。

在功能调整及重组过程中，保障“微波成像重点实验室SAR综合处理软件（MSARPro）”原有功能的正常使用。

### 通用图像处理功能

#### 通用图像加载

1. 可以打开不同格式的数据：包括float complex、float、double、int、char等常见的数据类型
2. 集成电子所开发的快视控件，支持大副摇杆数据的快速显示。
3. RGB三通道图像显示：每个通道可单独灰度显示。
4. 单通道图像显示彩色、灰度可选：可以对打开的单通道图像进行灰度或彩色显示，采用彩色显示时调色板可选。

#### 通用图像显示与浏览

1. 图像加载列表：显示所有加载到显示窗口的文件，双击每个文件可在窗口内打开。
2. 图像停靠模式多样化：并列显示（同时拖动）、选项卡显示等。
3. 图像放大、缩小、拖动。
4. 图像卷帘显示或者关联和交替显示：比较两幅图像的差异。
5. 增加局部放大窗口（在全景图之外单独显示）。

#### 像素定位与信息显示

像素定位与信息显示：增加“+”形光标，在适当位置显示“+”瞄准像素的行、列、经度、纬度、海拔、像素值等信息。

#### 通用图像保存

图像格式转换：可以将打开的图像导出为不同格式，如：jpg、tiff等，导出时格式由用户选择。

### 遥感图像处理功能

#### 感兴趣区域（ROI）处理

1. 线的选取：根据鼠标
2. 多边形（矩形、圆、任意多边形）的选取：矩形、圆通过鼠标确定起始点，并按住鼠标进行缩放，放开鼠标时固定多边形的大小，任意多边形通过鼠标点击的顺序依次连接并闭合。
3. ROI显示：对每个选取的对象进行彩色显示，颜色可选，多边形对闭合圈内的面进行颜色显示。
4. ROI统计：对每个对象包含的所有的像元进行统计，包含最大值、最小值、均值、方差及直方图显示。
5. ROI存储：选择的对象可存储为文本及.shp（常用矢量格式）

#### 图像裁剪

1. 基于行列号：输入左上角、右下角行列号裁剪图像，并修改参数文件（未地理编码的图像）和geotiff包头（地理编码的图像）相应的参数。
2. 基于地理位置：输入左上角、右下角经纬度裁剪图像，并修改geotiff包头（地理编码的图像）相应的参数。
3. 基于ROI：根据选取的多边形裁剪图像，并修改参数文件（未地理编码的图像）和geotiff包头（地理编码的图像）相应的参数。外接矩形内非ROI区域的值可默认为0，也可手动输入）

### 基于SAR图像的GIS处理功能

#### SAR图像加载与性能优化

针对SAR数据的特性，优化地图加载与显示性能。

#### 符号资源设计

针对SAR领域关注的特定目标，如灌木丛，沙漠，水等进行设计；符号的类型，大小，颜色，图标等相关信息定制符号。

#### 多通道的显示

支持RGB通道、R通道、G通道、B通道独立显示。

#### 图层控制

提供添加图层、删除图层、图层显示与否、图层顺序的调整功能。

#### 支持对图层进行编辑的功能

修改当前比例尺、添加数据、添加文字等相关信息，编辑信息快速查找功能。

#### 常用地图模版的保存，地图保存，打开等相关功能

地图的相关信息可以通过状态栏进行查看

## 性能需求

### 数据精确度

在精度需求上，根据实际需要，数据在输入、输出及传输的过程中要满足各种精度的需求根据关键字精度的不同。如：查找可分为精确查找和泛型查找，精确查找可精确匹配与输入完全一致的查询结果，泛型查找，只要满足与输入的关键字相匹配的输入即输出，可供查找。

### 时间特性

系统响应时间应在人的感觉和视觉范围内(<1 s)，系统响应时间足够迅速(<5 s)，当数据大时，以最短的时间进行响应，最大化满足用户要求。

### 适应性

在操作方式、运行环境、软件接口或开发计划等发生变化时，应具有适应能力。 可使用性

操作界面简单明了，易于操作，对格式和数据类型限制的数据，进行验证，包括客户端验证和服务器验证，并采用错误提醒机制，提示用户输入正确数据和正确的操作系统。

### 安全保密性

只有合法用户才能登录使用系统，对每个用户都有权限设置。对登录名、密码、以及用户重要信息进行加密，保证账号信息安全。

### 可维护性

系统采用了记录日志，用于记录用户的操作及故障信息，结构清晰，便于维护人员进行维护。

# 总体设计

## 设计目标、依据和方法

系统开发的最终目的是面向最终用户，因此，系统的开发应以最终用户的需求为出发点，充分考虑他们的要求：

1. 使用部门的负责人和开发项目的负责人密切配合，保证项目开发的顺利进行。

2. 各职能部门的领导和有关业务人员应该积极参与系统设计和试运行。

3. 开发过程中，系统开发人员和最终用户应随时沟通，共同研究、互相督促。

### 设计目标

本系统的设计目标是：

1、完整的体系架构

应具备从数据入库到数据分析及展示的一系列完整的系统功能，可以满足不同用户、不同应用场景下的需求。

2、跨平台

要求能够运行在多种操作系统、数据库平台和浏览器平台下，具备良好的跨平台性。

3、专业化的地图展示平台

在具备强大的通用地理信息平台功能的前提下，还需要进一步结合科技情报所专业需求，在数据模型支持、数据引擎扩展、数据显示、算法分析等方面都要突出系统在地理信息方面的专业特性，同时，在性能、安全性等方面都针对专业应用场景作出有针对性的设计。

4、高效、稳定

系统需要具有良好的稳定性，要求具备7\*24小时不间断运行的能力。

MSARPro系统业务系统属于计算密集型的数据处理系统，一般的分析模型都需要复杂的计算过程才能完成；从每日需要处理的数据量和请求量来看，系统在数据输入和输出（I/O）方面的压力也不小。因此MSARPro平台自身的效率必须达到一定的水平，然后辅以相对强大的硬件设备，从整体上保证应用业务系统的高效性。

5、高扩展性

MSARPro平台的开发是一个长期的过程，需要在实际应用的过程中不断加以完善。同时，业务需求的变化也要求平台具备方便的扩充功能，这些都要求系统具有较好的可扩展性。

这种可扩展性一方面要求平台本身具备可扩展能力，依靠该能力可以逐渐完善和增强平台所具有的基础功能；另一方面是平台应能实现和集成专业数据处理逻辑的支持，应用开发人员要求可以在平台所提出的基础功能模块之上实现专业数据分析模型。

这种可扩展性需求具体包括数据的可扩展性、功能的可扩展性和可视化可扩展性。

### 依据

#### 4.1.2.1测绘类标准

1、《基础地理信息要素分类与代码》GB/T 13923-2006

2、《公共信息标志用图形符号》 GB 1001—1994

#### 4.1.2.2公共服务平台类标准

1、《基础地理信息标准数据基本规定》（GB 21139―2007）

2、《国家地理信息公共服务平台技术设计指南》

#### 4.1.2.3软件信息化相关标准

1、《电子政务系统总体设计要求》GB/T 21064-2007

2、《政务信息资源目录体系》GB/T 21063-2007

3、《政务信息资源交换体系》GB/T 21062-2007

4、《计算机软件文档编制规范》GBT8567-2006

5、《计算机软件需求说明编制指南》GB/T 9385-2008

6、《计算机软件测试文档编制规范》GB/T 9386-2008

7、《计算机软件可靠性和可维护性管理》GB/T 14394-2008

#### 4.1.2.4地理信息公共服务规范文档

1、GB/T 28584-2012《城市坐标系统建设规范》；

2、GB/T 13923-2006《基础地理信息要素分类与代码》；

3、GB/T 20258.1-2007《基础地理信息要素数据字典 第1部分：1:500 1:1000 1:2000基础地理信息要素数据字典》；

4、GB/T 14912-2005《1:500 1:1000 1:2000外业数字测图技术规程》；

5、CH/T 9008.1-2010《基础地理信息数字成果1:500、1:1000、1:2000数字线划图》；

6、CH/T 9008.2-2010《基础地理信息数字成果1:500、1:1000、1:2000数字高程模型》；

7、GB/T 17797-1999《地形数据库与地名数据库接口技术规程》；

## 设计原则

### 统一设计原则

统筹规划和统一设计系统结构。尤其是应用系统建设结构、数据模型结构、数据存储结构以及系统扩展规划等内容，均需从全局出发、从长远的角度考虑。

### 标准化原则

设计和实施过程严格遵循国家和京津冀科技资源数字地图的相关标准规范。

基础支撑环境采用通用、标准、成熟的设备及软件。

数据库设计在依据现行规范的同时，补充制定一系列规范，来约束、指导数据的提供者与管理者按照统一的标准来集成整合分散、异构、异源的空间信息资源。

### 先进性原则

在确保能够满足系统可靠、稳定运行要求的情况下，尽量采用领先的、适合当前的主流趋势的IT技术，新技术要有一定的成熟度、开放度和成功案例，符合工程项目使用要求。

### 易用性原则

在达到预定的目标、具备所需要的功能前提下，应用系统的使用操作要简单、方便，易于向同类行业及服务机构推广使用，这样可减少处理费用，提高系统效益，便于实现和管理。

设计上需要具有足够的灵活性，能够实现对应用的快速调整，以适应各类业务流程的多变特性和不同应用场景的工作差异。

考虑基层的信息化水平和IT维护能力，系统设计上简化系统节点，并采用自动化的更新维护手段。

### 可靠性原则

基础支撑环境通过采用高可靠的硬件和网络环境及系统运行环境，满足虚拟化、热备、镜像等技术提高可靠性。在出现严重突发故障时，不会造成应用服务的长时间中断和数据的丢失。

应用软件设计时考虑全面的容错机制，开发和测试采用科学有效的技术和手段，确保能够长期稳定、可靠的运行。

提高系统可靠性的途径主要有：

1、选取可靠性较高的主机和外部设备；

2、硬件结构的冗余设计，即在高可靠性的应用场合，应采取双机或双工的结构方案；

3、对故障的检测处理和系统安全方面的措施，如对输入数据进行校检，建立运行记录和监督跟踪，规定用户的文件使用级别，对重要文件的拷贝等。

### 安全性原则

按照GB/T 22239-2008《信息安全技术信息系统安全等级保护基本要求》，结合本项目安全需求，从物理安全、网络安全、数据安全、应用安全四方面进行全面的设计，并采取一定的安全审计措施，对系统安全情况进行跟踪记录。

### 一致性原则

一致性是指系统中信息编码、采集、信息通信要具备一致性设计规范应标准。

### 完整性原则

完整性是指系统作为一个统一的整体而存在，系统功能应尽量完整。

### 健壮性原则

是指软件对于规范要求以外的输入能够判断出这个输入不符合规范要求，并能有合理的处理方式。软件设计的健壮与否直接反应了分析设计和编码人员的水平。

### 扩展性原则

基础支撑环境和应用软件的设计要有足够的通用性、余量和扩展能力，能够有效的集成、兼容已有设备和专用业务系统，并能够实现在未来较长时间内，简单、方便、低成本的资源扩展。

## 系统总体架构

### 总体架构设计

#### 4.3.1.1配置项划分原则

1、系统配置项依据《需求规格说明书》进行划分，并在范围定义上与需求规格说明书保持一致；

2、系统配置项的划分将严格按照国家软件工程的对配置项的定义，配置项间功能相对独立，配置项内部高内聚；

3、系统配置项的划分粒度将依据《需求规格说明书》中的子系统级别进行定义，不同配置项间通过数据接口实现动态交互；

4、系统配置项按照配置项、部件、单元三级层次结构进行系统设计功能的细分。

### 总体架构

系统建设要充分利用现有的软硬件基础设施，既要考虑系统的扩展性，还要能够基于此系统扩展数据和业务应用系统。根据系统的应用需求，按照系统软件工程的思想和方法，将整个系统结构化、模块化，采用分层构架方式进行设计。

系统总体架构如下图：



#### 4.3.2.1基础设施层

传统的基础设施层是系统高效、稳定、安全运行的重要保障。根据系统运行的实际需求，系统基础设施包括网络设施、硬件设施、软件设施等。网络设施包括防火墙、路由器、交换机等，硬件设施包括应用服务器、数据库服务器、文件服务器、产品分发服务器等，软件设施包括操作系统、数据库系统等。

防火墙、路由器以及交换机则是在部署系统局域网以及为增强系统安全所必需的基础设施。

操作系统为本系统提供了良好的操作、交互平台；

#### 4.3.2.2数据存储层

数据存储层包括空间数据库和非空间数据库，空间数据层采用SDX+空间数据库引擎来存储和管理空间矢量数据、空间栅格数据（包括影像）和DEM数字高程数据，非空间数据采用Oracle或SQL Server来存储和管理。

空间数据库主要由SAR影像库、光学影像库和基础地理数据库构成。SAR影像库主要提供SAR数据的存储和管理，该数据库是本应用的核心。光学影像库主要提供光学遥感数据的存储和管理。基础地理数据库主要提供各种基础地理数据的存储和管理。

#### 4.3.2.3数据访问层

数据访问层主要提供空间数据库和非空间数据库的数据访问接口，空间数据访问主要通过空间数据访问引擎来完成。

数据访问层提供插件机制可以实现数据访问引擎的扩展能力，来满足对各种数据格式的支持。

#### 4.3.2.4应用服务层

应用服务层主要提供标准空间信息处理服务功能，包括数据管理、数据转换、数据编辑、空间查询、二维浏览、三维浏览、空间分析等。

#### 4.3.2.5平台层

应用支撑平台提供标准可视化交互界面，有机集成应用服务层功能接口，并且提供功能扩展接口以及可视化界面定制机制。

#### 4.3.2.6应用层

提供专业的SAR影像及光学影像遥感处理、分析、解译一站式服务平台。

## 系统软、硬件配置方案

### 性能设计指标

待定

### 开发环境

#### 4.4.2.1软件环境

系统开发的软件环境如下表所示：

表 4‑1 系统开发软件环境

| 平台软件 | SuperMap iDesktop .Net 8C |
| --- | --- |
| 开发工具 | Visual Studio 2008 简体中文专业版 |
| 开发语言 | C#.Net |
| 操作系统 | Windows XP、Windows 2003 Server、Windows 7 |

#### 4.4.2.2硬件环境

系统开发的硬件环境如下表所示：

表 4‑2 系统开发硬件环境

| 服务器类型 | Windows工作站 |
| --- | --- |
| 内存 | 128GB |
| 硬盘 | 1TB及以上 |
| CPU | 24核心以上 |
| 图形显卡 | 专业图形化 |

### 系统运行环境

#### 4.4.3.1软件环境

系统运行的软件环境如下表所示：

表 4‑3 系统运行软件环境

| 软件环境类型 | 版本/型号 |
| --- | --- |
| GIS软件 |  |
| 操作系统 | WindowsXP/2003 Server及Windows 7 |
| .Net Framework | 4.0及以上版本 |
| GIS软件 |  |
| 操作系统 | Windows XP、Windows 2003 Server、Windows 7 |

#### 4.4.3.2硬件环境

系统运行的硬件环境如下表所示：

表 4‑4 系统运行硬件环境

| 服务器类型 | Windows工作站 |
| --- | --- |
| 内存 | 128GB |
| 硬盘 | 1TB及以上 |
| CPU | 24核心以上 |
| 图形显卡 | 专业图形化 |

### 系统测试环境

#### 4.4.4.1软件环境

系统测试的软件环境如下表所示：

表 4‑5 系统测试软件环境

| 软件环境类型 | 版本/型号 |
| --- | --- |
| GIS软件 |  |
| 操作系统 | WindowsXP/2003 Server及Windows 7 |
| .Net Framework | 4.0及以上版本 |
| GIS软件 |  |
| 操作系统 | Windows XP、Windows 2003 Server、Windows 7 |

#### 4.4.4.2硬件环境

系统测试的硬件环境如下表所示：

表 4‑6 系统测试硬件环境

| 服务器类型 | Windows工作站 |
| --- | --- |
| 内存 | 128GB |
| 硬盘 | 1TB及以上 |
| CPU | 24核心以上 |
| 图形显卡 | 专业图形化 |

## 核心业务流程

系统最核心的业务流程有影像数据可视化设置和影像数据解译流程。

* 影像数据可视化设置：

数据导入→通道控制→调色板设置→可视化浏览→通道计算→数据统计→成果输出

* 影像数据解译流程：

数据导入→可视化浏览→解译制图→专题地图展示→成果输出

## 系统划分

结构化系统分析与设计的基本思想就是自顶向下地将整个系统划分为若干个子系统，子系统再分子系统（或模块），层层划分，然后在自上而下地逐步设计。

### 系统划分原则

#### 4.6.1.1子系统要具有相对独立性

子系统的划分必须使得子系统的内部功能、信息等各方面的凝聚性较好。在实际中我们都希望每个子系统或模块相对独立，尽量减少各种不必要的数据、调用和控制联系。并将联系比较密切、功能近似的模块相对集中，这样对于以后的搜索、查询、调试、调用都比较方便。

#### 4.6.1.2子系统之间数据的依赖性尽量小

子系统之间的联系要尽量减少，接口简单、明确。一个内部联系强的子系统对外部的联系必然是相对很少。所以划分时应将联系较多的都划入子系统内部。这样划分的子系统，将来调试、维护、运行都是非常方便的。

#### 4.6.1.3子系统划分的结果应使数据冗余最小

如果我们忽视这个问题，则可能引起相关的功能数据分布在各个不同的子系统中，大量的原始数据需要调用，大量的中间结果需要保存和传递，大量计算工作将要重复进行。从而使得程序结构紊乱，数据冗余，不但给软件编制工作带来很大的困难，而且系统的工作效率也大大降低了。

#### 4.6.1.4子系统的设置应考虑今后管理发展的需要

子系统的设置光靠上述系统分析的结果是不够的，因为现存的系统由于这样或那样的原因，很可能都没有考虑到一些高层次管理决策的要求。为了适应现代管理的发展，对于老系统的这些缺陷，在新系统的研制过程中应设法将它补上。只有这样才能使系统实现以后不但能够更准确、更合理地完成现存系统的业务，而且可以支持更高层次、更深一步的管理决策。

#### 4.6.1.5子系统的划分应便于系统分阶段实现

信息系统的开发是一项较大的工程，它的实现一般都要分期分步进行。所以子系统的划分应该考虑到这种要求，适应这种分期分步的实施。另外，子系统的划分还必须兼顾组织机构的要求（但又不能完全依赖于组织，因为目前正在进行体制改革，组织结构相对来说是不稳定的），以便系统实现后能够符合现有的情况和人们的习惯，更好地运行。

# 接口设计

## 用户接口

用户接口又称人机界面、人机交互，是计算机和使用者之间进行信息交换的通道。用户接口是为方便用户使用计算机资源所建立的用户和计算机之间的联系。

系统暂无用户接口需求。

## 外部接口

系统暂无外部接口需求。

## 内部接口

系统暂无内部接口需求。

# 系统功能设计

MSARPro（二期）根据业务需求应用共分为：通用图像处理、遥感影像处理和基于SAR影像GIS处理功能。

以下仅列出本期即二期所需要的功能。

## 通用图像处理功能

### 通用图像加载

提供Tiff、裸数据等格式的影像数据加载功能。具体包括数据格式解析、数据导入、多通道处理、金字塔建立、调色板设定环节。

**数据解析**，通过读取头文件（tiff）或者元数据（裸数据）等文件内容描述信息，从二进制数据中依次读取每一个像素的数值，写入内存数组中。

**数据导入**，将数据解析成果保存到数据集中。根据像素的数值类型不同，可以分为浮点型、整形、无符号整形等类型，对应生成不同像素类型的数据集。根据数据的通道数不同，分为灰度和RGB两类数据集，对应生成栅格数据集和影像数据集。

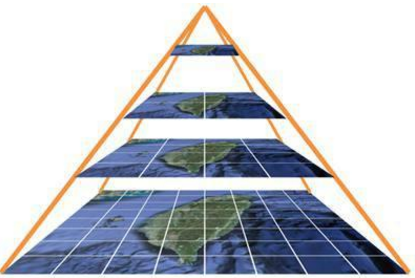
**多通道处理**，将RGB数据拆分为三个灰度数据集，并将拆分结果和原始RGB数据作为一个群组，统一管理。

图6 – 1 SAR数据多通道显示

****

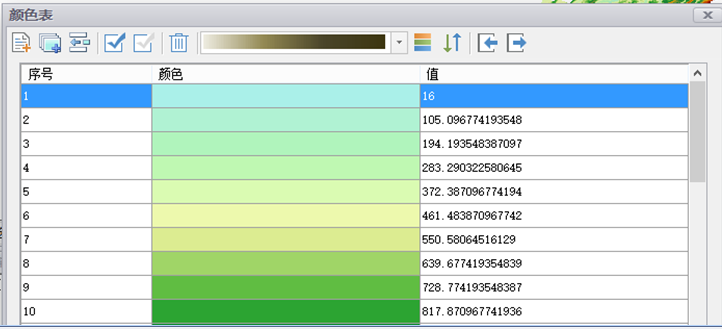
**金字塔建立**，将所有的灰度和RGB数据建立影像金字塔，提高后续影像显示效率。

图6 – 2 金字塔示意图



**调色板设定**，提供单通道影像调色板设置功能。支持色带批量设置功能。

图6 – 3 调色板设定

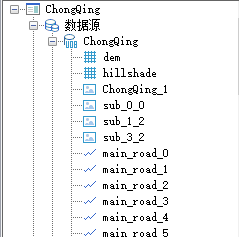


### 通用图像显示与浏览

提供数据管理面板，实现数据加载、图像显示、多窗口任务、卷帘浏览、图层控制和局部放大功能。

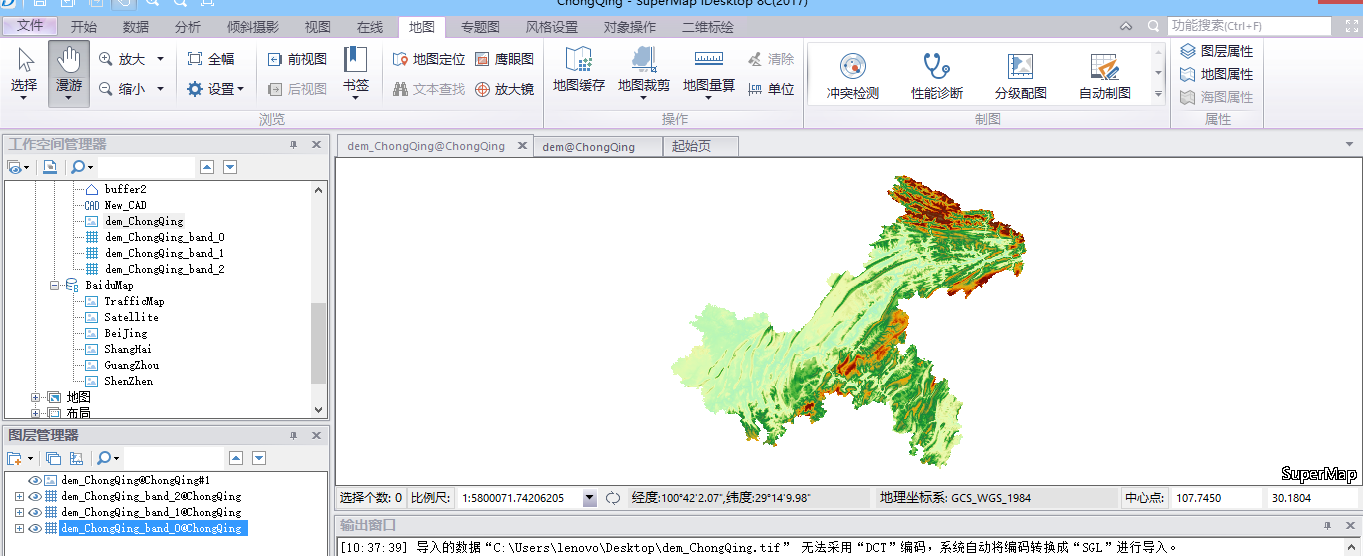
**数据加载**，提供数据管理面板，将系统中所有加载的影像、矢量数据以列表形式在面板中显示。

图6 – 4 数据管理面板



**图像显示**，通过双击数据列表记录，或者在右击菜单中选择“添加到当前图像窗口”、“添加到新图像窗口”的方式，将目标影像添加到图像窗口中。通过“放大”、“缩小”、“平移”、“全局”等工具实现图像的浏览控制。

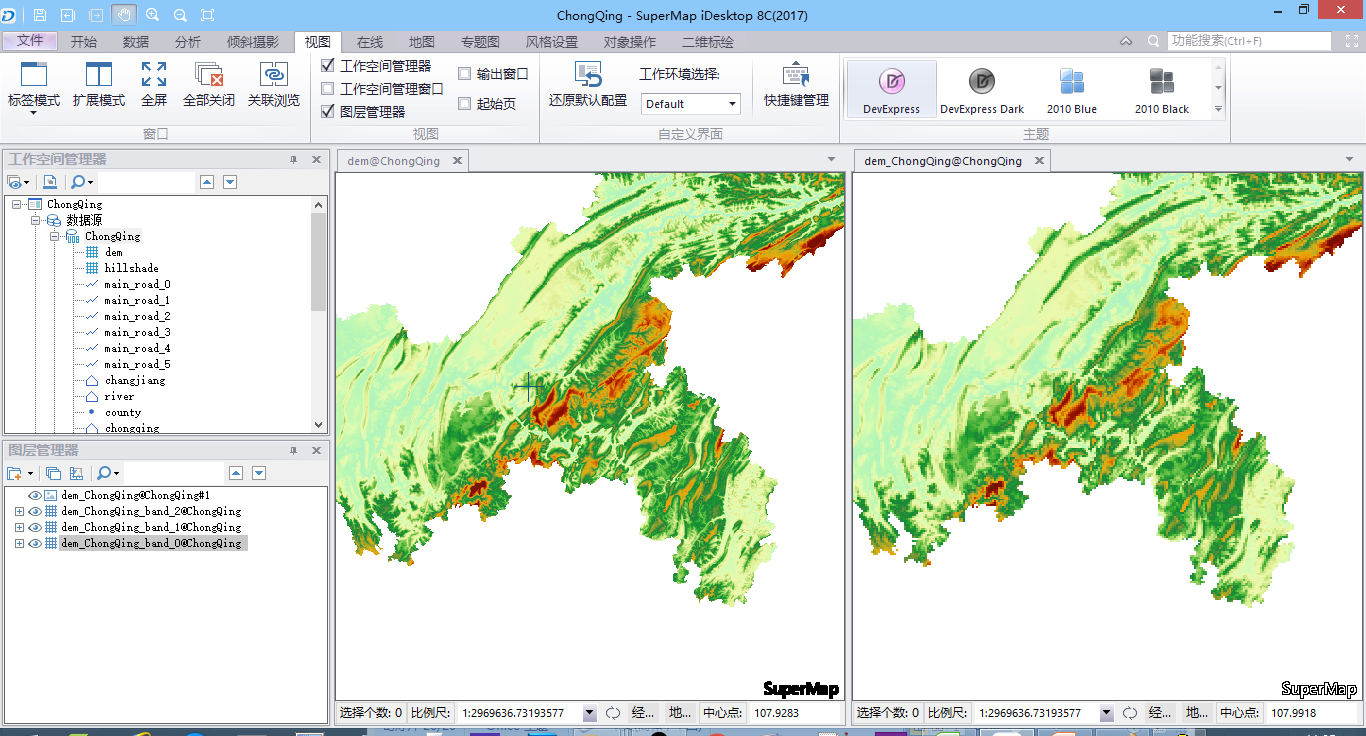
图6 – 5 图像显示



**多窗口任务**，当有多个图像窗口的情况下，提供多窗口布局设置选项。可以实现“选项卡布局”、“水平平铺”、“垂直平铺”窗口模式切换。

并提供窗口间视野范围同步功能。

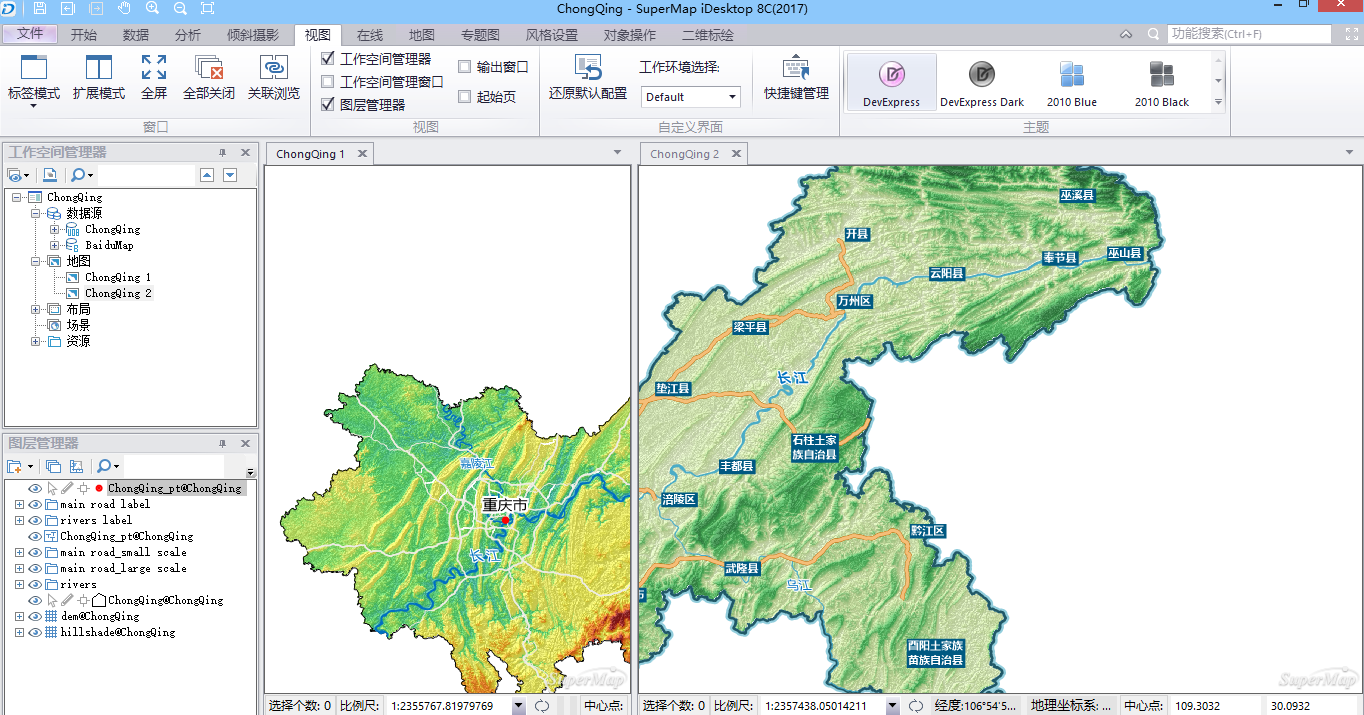
图6 – 6 多窗口任务



**卷帘浏览**，通过设置同一图像窗口中两景关联影像，进入卷帘浏览模式。

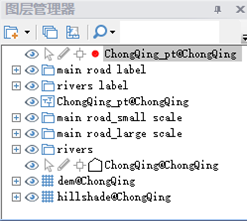
模式中，图像窗口将一分为二（提供“左右”和“上下”两种结构），设置的关联影像将分别显示在两个窗口中，中间有卷帘控制手柄，可以调节两个窗口的所占的比例关系。两景图像空间位置是重叠的，所以调整卷帘手柄的时候，可以观察两景影像在同一区域的变化。

图6 – 7 卷帘显示



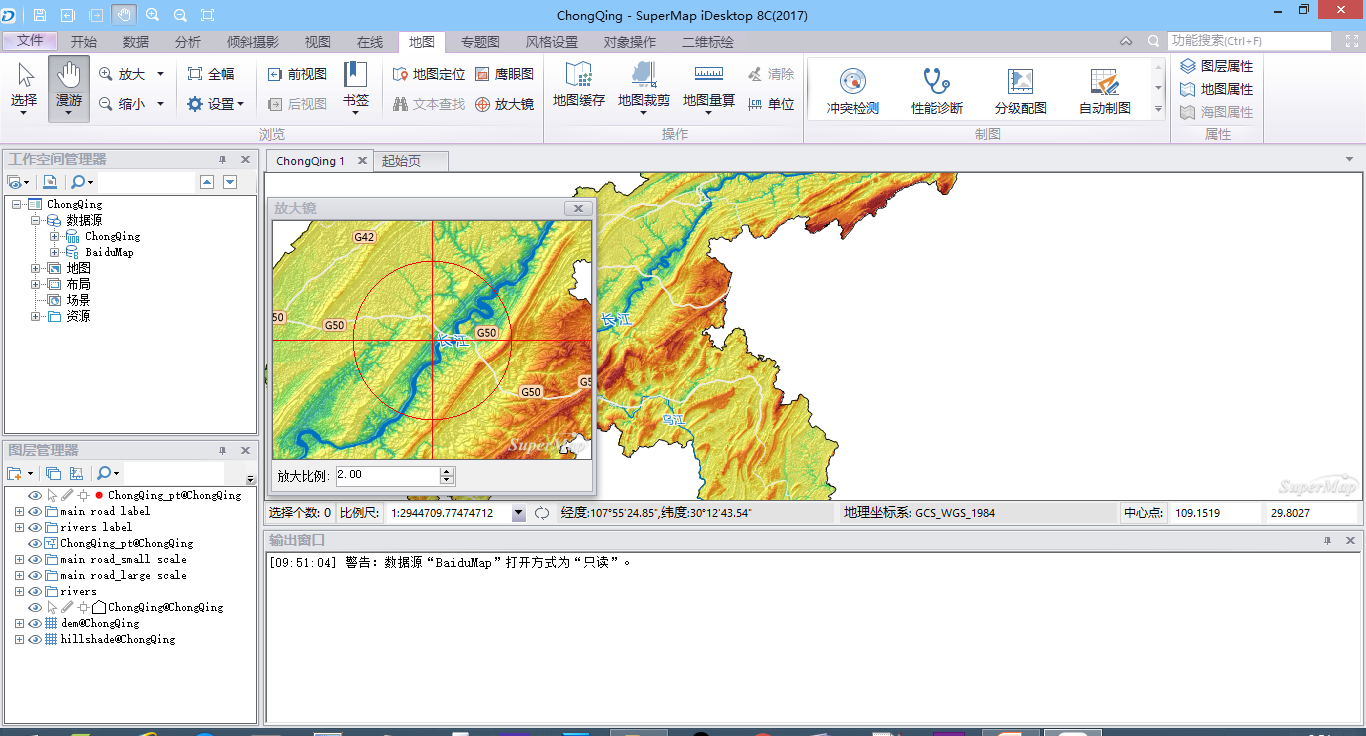
**图层控制**，提供图像窗口中所有加载影像或者矢量信息的控制面板。通过面板可以控制叠加顺序，修改影像的显隐功能。

图6 – 8 图层控制面板



**局部放大**，提供放大镜功能。在新弹出的监视窗口中实时显示光标移动区域的放大影像，放大倍数可以进行切换。

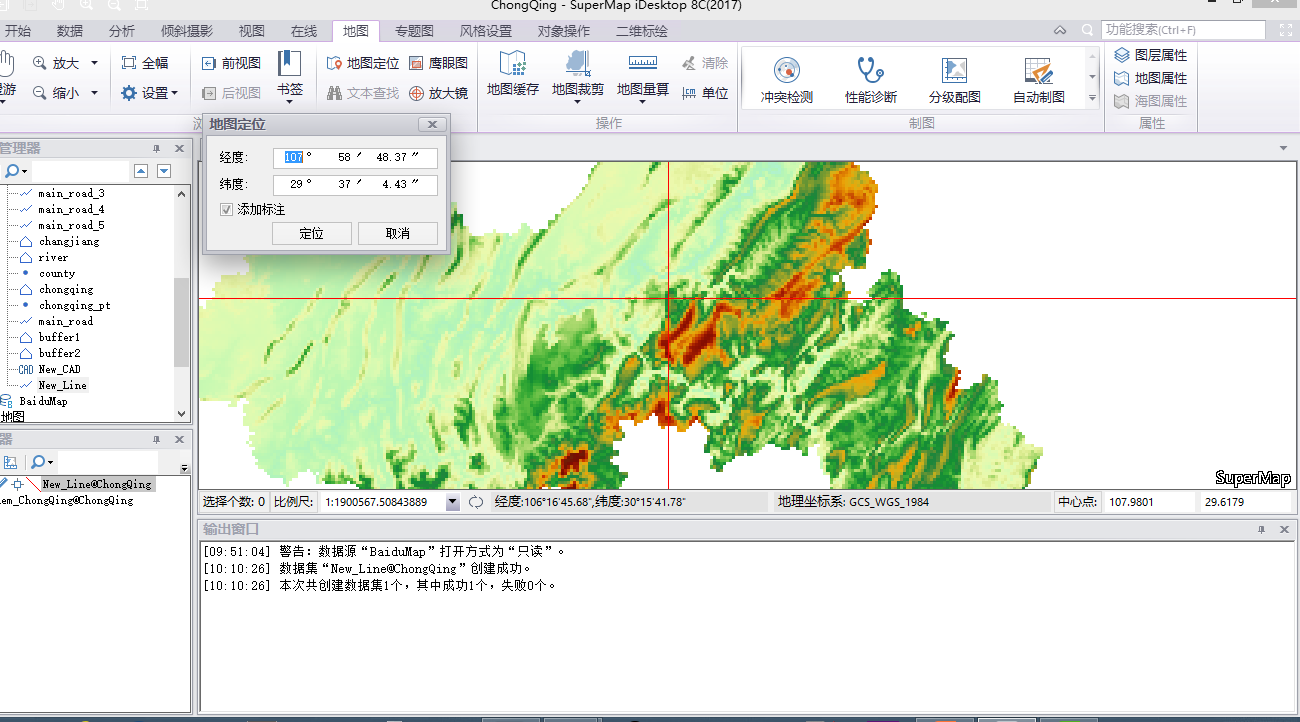
图6 – 9 局部放大功能



### 像素定位与信息显示

**提供像素定位窗口**，通过设置行列号或者经纬度信息，可以在图像窗口中快速定位显示指定目标，并且在图像窗口中以十字丝的形式标记查询的位置，并且在信息栏中显示目标点信息（包括：行列号，经纬度，像元值）。

图6 – 10 定位窗口



**提供像素信息实施查询状态栏**，当鼠标在图像窗体中移动的时，查询状态栏同步显示鼠标所在位置的详细信息（包括：行列号，经纬度，像元值）。

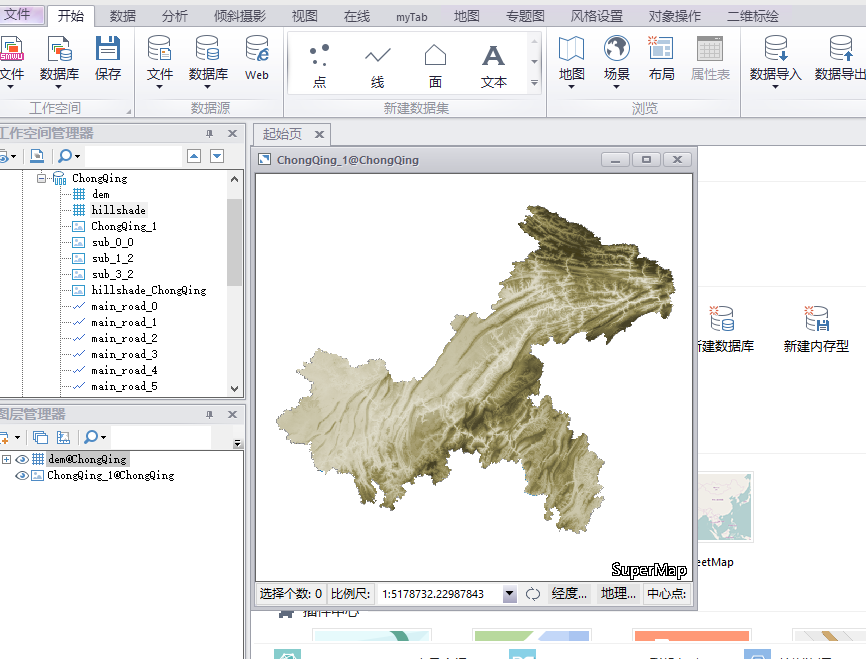
图6 – 11 查询状态栏



### 通用图像保存

**图像格式转换**，可以将打开的图像导出为不同格式，如：jpg、tiff等，导出时格式由用户选择。

### 快视数据显示

**快速浏览可视化** 通过SuperMap iDesktop扩展一个IForm窗体，将SAR数据快速浏览控件嵌入到扩展窗体中，实现快速浏览控件的集成。快速浏览控件需要提供基本的放大、缩小、平移、复位等浏览功能。 

需要快速浏览模块提供的接口：

1. 数据加载接口，输入一个数据文件存放路径，实现数据加载显示功能。
2. 提供放大功能接口。切换一种鼠标交互模式
3. 提供缩小功能接口。切换一种鼠标交互模式
4. 提供平移功能接口。切换一种鼠标交互模式
5. 提供复位功能接口。

**关联浏览**

2.1十字丝关联显示

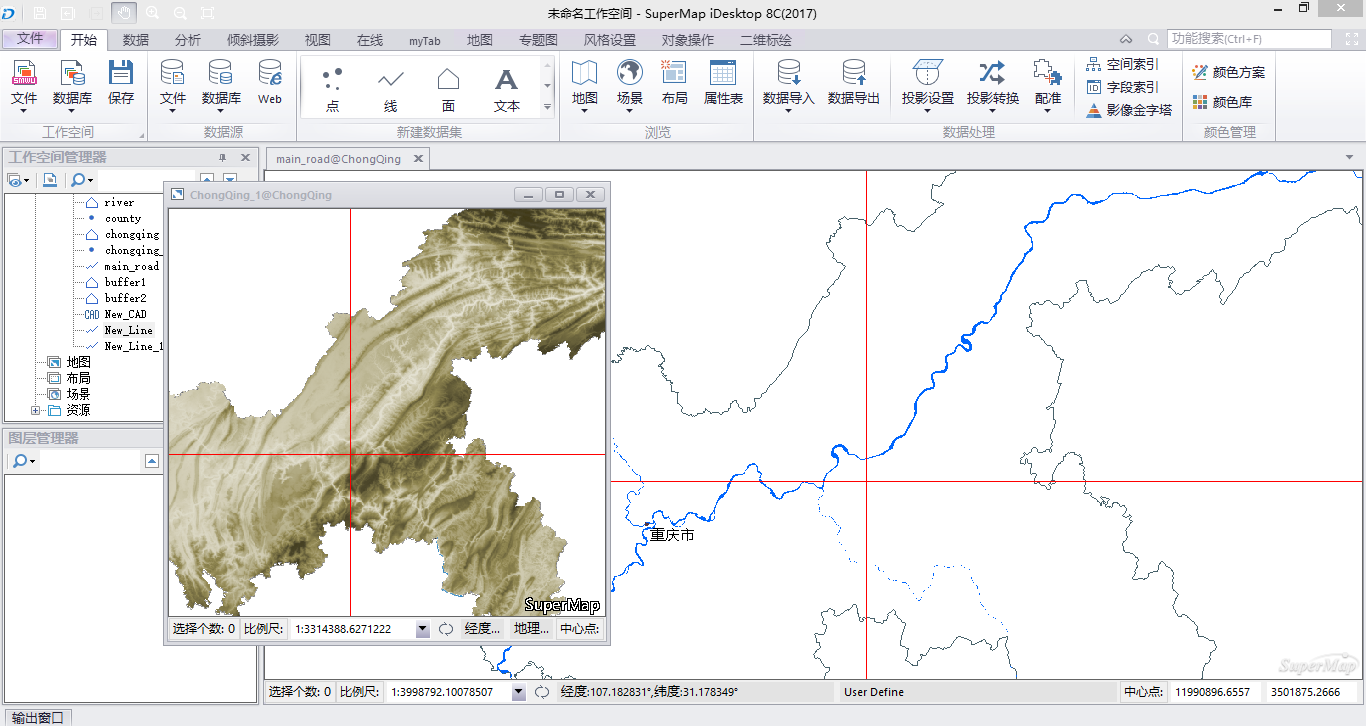
同时打开快速浏览窗口和常规浏览窗口。常规浏览窗口可以加载显示基础地理数据。快速浏览和常规浏览窗口之间可以通过十字丝来进行关联定位。十字丝可以随鼠标移动实时变化更新，也可以通过点击鼠标将十字丝固定到浏览窗口实现相对定位。

2.2同步缩放功能

提供同步缩放按钮，实现快速显示窗口和常规显示窗口之间的同步放大和缩小。

2.3同步浏览功能

提供同步平移按钮，实现快速显示窗口和常规显示窗口之间的同步平移。

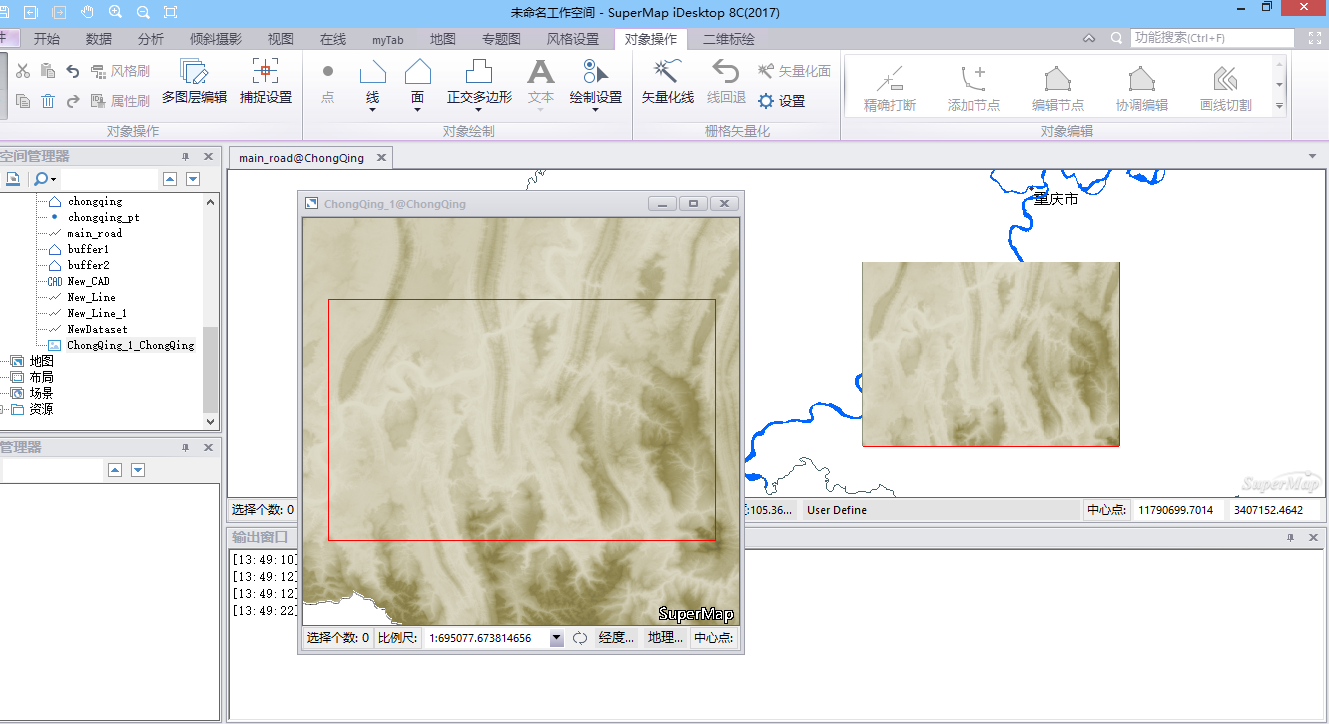


需要快速浏览模块提供的接口：

1. 提供任意光标位置的地理坐标接口。
2. 提供直线的绘制和清除接口。

**兴趣区域同步提取**

通过绘制兴趣区域可以提取区域内的影像数据并导入到常规影像窗口中，与常规窗口中的基础地理数据进行叠加显示。



需要快速浏览模块提供的接口：

1. 提供像素坐标转换为地理坐标接口。
2. 提供地理坐标转换为像素坐标接口。

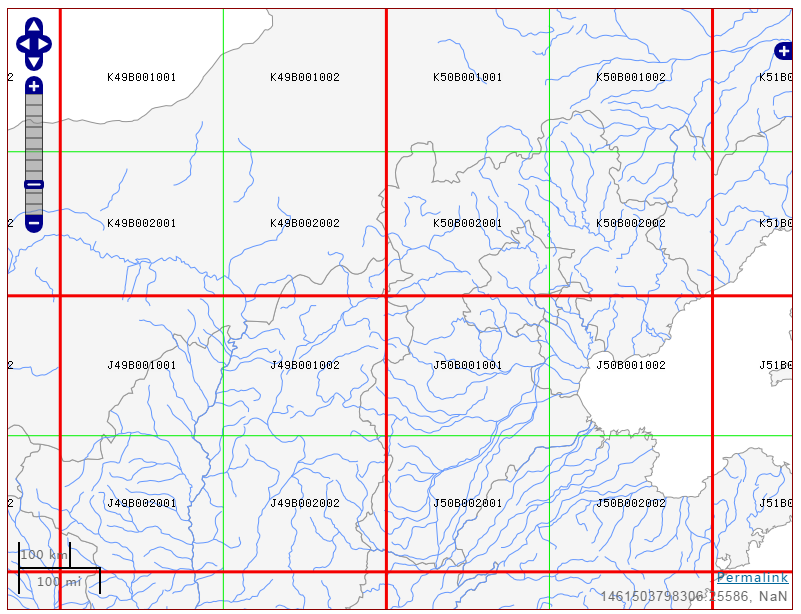
c．提供通过像素坐标获取栅格值接口。

### 地图分幅功能

**地图分幅数据创建：**用户点击对应功能按钮，弹出地图分幅创建对话框，用户在对话框中输入地图比例尺、范围、目标影像，确认后，系统自动根据选中的比例尺，根据影像大小创建地图分幅，并根据生成的分幅号对目标影像进行分幅裁剪。将裁剪后的数据保存到一个目标位置。

注：支持新编地图分幅算法。

**地图分幅数据显示：**用户点击对应按钮，打开地图分幅显示对话框，用户选取对话框中的分幅号，确认后，在主视图中添加与分幅号匹配的影像数据。



## 遥感图像处理功能

### 感兴趣区域（ROI）处理

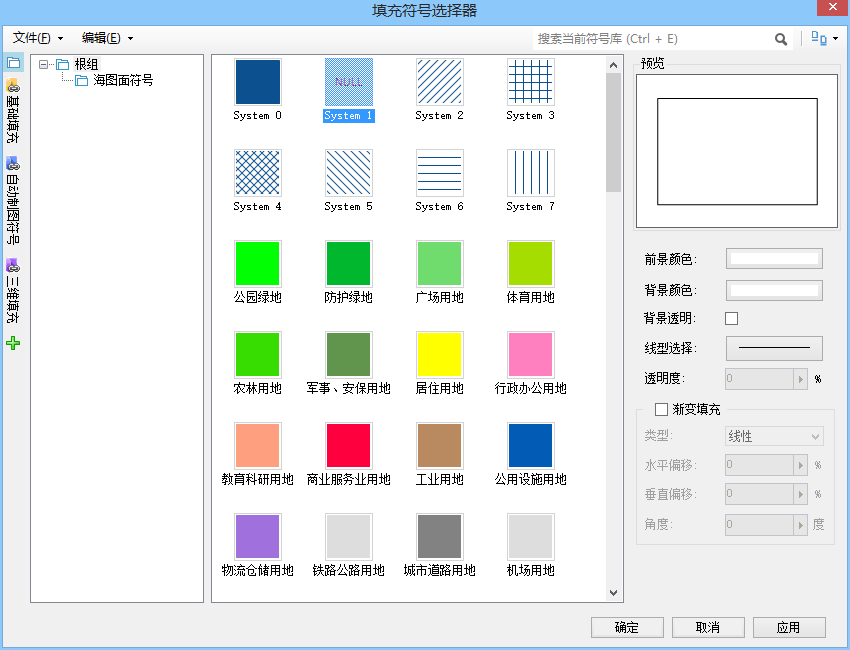
**绘制兴趣区域**，提供创建ROI功能。启动绘制ROI模式后，可以通过：鼠标交互在图形窗口，手动绘制矩形、圆形、任意多边形等ROI。

图6 – 15 ROI工具



**ROI风格设置**，ROI绘制完成后，可以设定ROI的显示风格，包括边框线型、填充颜色、透明度等设置参数。

图6 – 16 ROI风格设置

****

**基于ROI统计**，提供ROI区域统计信息，包括最大值、最小值、均值、方差及直方图。

**ROI存储和加载**，选择的对象可存储为文本及.shp（常用矢量格式）并且可以通过导入接口直接加载导出后的ROI文件。

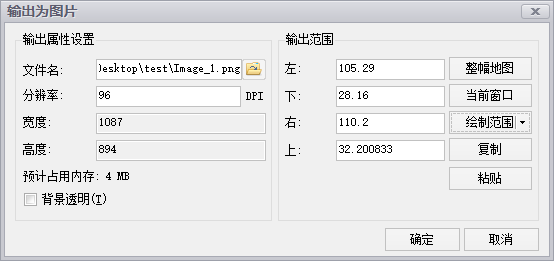
* 图像裁剪

**基于行列号裁剪**，通过输入左上和右下的行列号，设定图像裁剪范围来生成新的图像。

**基于地理位置裁剪**，通过输入左上和右下的经纬度信息，设定图像裁剪范围来生成新的图像。

**基于ROI裁剪**，通过指定导出的ROI文件，依据ROI空间分布信息，进行图像裁剪。

图6 – 17 图像裁剪

****

## 基于SAR图像的GIS处理功能

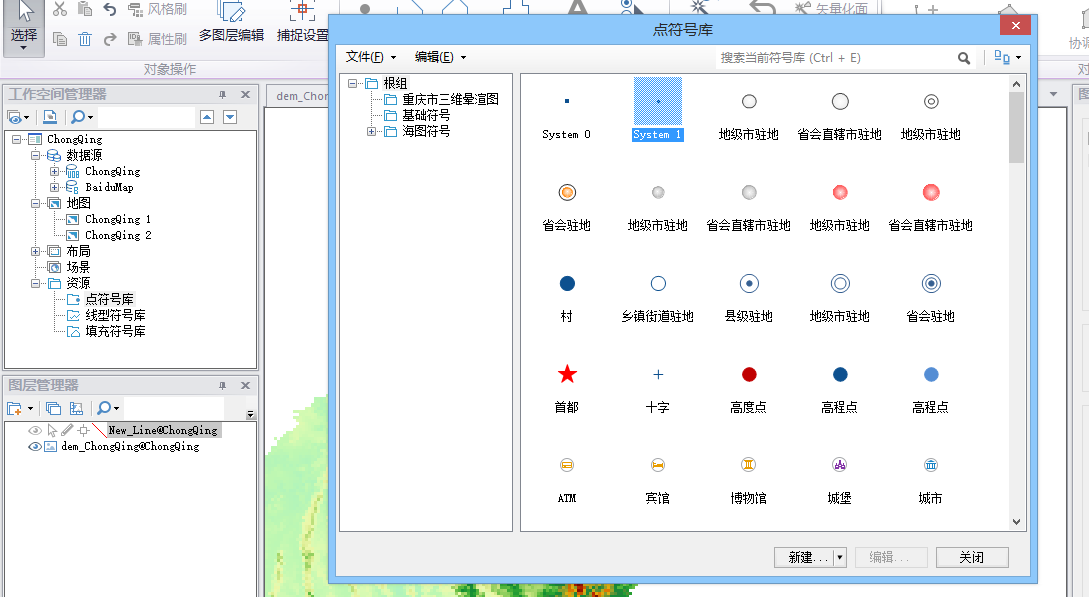
### SAR图像加载与性能优化

SAR数据转换为tiff文件格式，进行图像加载。

### 符号资源设计

针对SAR领域关注的特定目标，如灌木丛，沙漠，水等进行设计；符号的类型，大小，颜色，图标等相关信息定制符号。

图6 – 20 符号资源设计



### 多通道的显示

支持RGB通道、R通道、G通道、B通道独立显示。

### 图层控制

提供添加图层、删除图层、图层显示与否、图层顺序的调整功能。

### 支持对图层进行编辑的功能

修改当前比例尺、添加数据、添加文字等相关信息，编辑信息快速查找功能。

### 常用地图模版的保存

* 地图保存，打开等相关功能

保存常用地图模版，实现背景地图的快速加载与显示。

图6 – 21 地图模版



# 数据库设计

## 数据库设计原则

### 命名规范

所有的库名、表名、域名必须遵循统一的命名规则，并进行必要说明，以方便设计、维护、查询。

### 控制字段的引用

在设计时，可以选择适当的数据库设计管理工具，以方便开发人员的分布式设计和数据小组的集中审核管理。采用统一的命名规则，如果设计的字段已经存在，可直接引用；否则，应重新设计。

### 库表重复控制

在设计过程中，如果发现大部分字段都已存在，开发人员应怀疑所设计的库表是否已存在。通过对字段所在库表及相应设计人员的查询，可以确认库表是否确实重复。

# 运行设计

## 运行模块的组合

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下面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。

## 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，电脑在发送数据后，将等待数据库的确认收到信息，收到后，在对数据处理将返回信息送回电脑，并等待确认。

## 运行时间

在软体的需求分析中，对运行时间的要求为必须对作出的操作有较快的反应。服务器的性能，这将影响对数据库访问时间即操作时间的长短，影响加大客户机操作的等待时间，所以必须使用高性能的服务器。硬件对本系统的速度影响将会大于软件的影响。

# 用户界面设计

系统界面是系统提供给最终用户访问系统功能和数据的界面，一个系统是否容易使用主要取决于系统的界面对最终用户是否友好、是否操作简便。

## 用户界面设计思路

在人和机器的互动过程中，有一个层面，即我们所说的界面（interface）。界面是人与机之间交流、沟通的层面，是系统的重要组成部分。用户界面设计的主要思路是：置界面于用户的控制之下，减少用户的记忆负担，保持界面的一致性；界面设计是以人为中心，使产品达到简单使用和愉悦使用的设计。

界面设计从流程上分为结构设计、交互设计和视觉设计三部分。

1、结构设计Structure Design

结构设计也称概念设计（Conceptual Design），是界面设计的骨架。通过对用户需求研究和任务分析，制定出产品的整体架构。基于纸质的的低保真原型（Paper Prototype）可提供用户测试并进行完善。在结构设计中，目录体系的逻辑分类和语词定义是用户易于理解和操作的重要前提。

2、交互设计Interactive Design

交互设计的目的是使产品让用户能简单使用。任何产品功能的实现都是通过人和机器的交互来完成的。因此，人的因素应作为设计的核心被体现出来。

3、视觉设计Visual Design

在结构设计的基础上，参照目标群体的心理模型和任务达成进行视觉设计。包括色彩、字体、页面等。视觉设计要达到用户愉悦使用的目的。

## 用户界面设计原则

### 易用性原则

按钮名称应该易懂，用词准确，没有模棱两可的字眼，要与同一界面上的其他按钮易于区分，如能望文知意最好。理想的情况是用户不用查阅帮助就能知道该界面的功能并进行相关的正确操作。

### 规范性原则

界面遵循规范化的程度越高，则易用性相应的就越好。

### 帮助设施原则

系统应该提供详尽而可靠的帮助文档，在用户使用产生迷惑时可以自己寻求解决方法。帮助文档中的性能介绍与说明要与系统性能配套一致。最好提供目前流行的联机帮助格式或HTML 帮助格式。

### 合理性原则

1. 重要的命令按钮与使用较频繁的按钮要放在界面上注目的位置。
2. 错误使用容易引起界面退出或关闭的按钮不应该放在易点位置。
3. 横排开头或最后与竖排最后为易点位置。
4. 与正在进行的操作无关的按钮应该加以屏蔽。
5. 对可能造成数据无法恢复的操作必须提供确认信息，给用户放弃选择的机会。
6. 非法的输入或操作应有足够的提示说明。
7. 对运行过程中出现问题而引起错误的地方要有提示，让用户明白错误出处，避免形成无限期的等待。
8. 提示、警告、或错误说明应该清楚、明了、恰当并且应避免英文提示的出现。

### 美观与协调性原则

界面应该大小适合美学观点，感觉协调舒适，能在有效的范围内吸引用户的注意力。布局要合理，不宜过于密集，也不能过于空旷，合理的利用空间。按钮的大小要与界面的大小和空间要协调。避免空旷的界面上放置很大的按钮。

### 排错性考虑原则

在界面上通过下列方式来控制出错几率，会大大减少系统因用户人为的错误引起的破坏。开发者应当尽量周全地考虑到各种可能发生的问题，使出错的可能降至最小。如应用出现保护性错误而退出系统，这种错误最容易使用户对软件失去信心。因为这意味着用户要中断思路，并费时费力地重新登录，而且已进行的操作也会因没有存盘而全部丢失。

1. 应当注意尽可能避免用户无意录入无效的数据。
2. 对可能引起致命错误或系统出错的输入字符或动作要加限制或屏蔽。

### 窗口的应用与系统资源原则

设计良好的软件不仅要有完备的功能，而且要尽可能的占用最低限度的资源。

在多窗口系统中，有些界面要求必须保持在最顶层，避免用户在打开多个窗口时，不停的切换甚至最小化其他窗口来显示该窗口。

## 用户界面需求

### 减少不必要的重复交互

1、减少不必要的各种操作，能够点一次鼠标或敲一次键盘完成的绝不做两次或多次。

2、提示信息要适度，不要太多或太少。系统再进行删除、保存、审核等操作时，系统要有相应友好的提示信息。

3、数据项在进行完整性校验，发现错误时光标焦点自动定位到错误处。

4、完整业务功能尽量在一个表单内完成。

5、相同的信息不要在系统中多处或多次录入，保证入口的唯一性。

6、系统要尽可能根据用户已经录入的信息自动获取其它附属信息，而不需要用户重复的选择或录入。

### 系统性能和健壮性

1、系统耗时操作超过30秒的最好能够提供给用户相关的进度条功能。

2、系统耗时功能超过2分钟的最好能够设计为异步多线程的方式进行处理。

3、系统应用有友好的完整性和约束校验的提示信息，方便用户修改录入数据。

4、在系统出现异常情况下应该有友好的统一的提示信息，同时后台应该记录详细的异常日志。

### 保持界面友好性和易用性

1、表单应该能够根据屏幕分辩率自动适应，让用户一次能够看到足够多的信息。

2、表单应该支持Tab键功能，顺序为从左到右，从上到下。

3、表单上控件的布局应该间距适当，标签和控件对齐，有适当的录入提示信息。

4、界面的配色应该尽量简单，尽量少使用各种刺眼的颜色。

5、表单要尽量自我解释，不要设计过多的隐含在表单里面的功能。

### 数据录入和检索

1、根据业务需要选择适合的数据录入控件。

2、系统应该提供给用户暂时保存录入数据的功能。

3、数据检索条件应该适中，不应太多也不应太少。检索支持组合条件检索。

4、为了满足不同需求检索可以提供简单检索和高级检索多种方式。

5、应该在第一时间提供给用户检索数据，因此检索功能存在性能问题时候要考虑分页。

# 系统安全设计

系统必须保证信息的安全性，数据的丢失，信息的不安全将会给企业带来巨大的损失。故为了防止数据外泄、丢失或遭破坏，系统需有安全性方面的措施。这在技术上采用物理保护与数据加密相结合的方法。考虑到本系统的实际需要，本系统将从以下八个方面实施安全和加密保护：

1. 为中心服务器系统加密；
2. 为存储在媒体上的文件加密；
3. 为系统开发组的专业文件加密；
4. 数据库加密；
5. 网络安全措施；
6. 数据备份；
7. 配置防火、防水、防高温、防震、防电磁场、防静电及防盗的设备，并定期予以检查维护；
8. 制定安全策略、建立安全保护机构、限定用户访问范围。

## 系统安全原则

根据防范安全攻击的安全需求、需要达到的安全目标、对应安全机制所需的安全服务等因素，参照SSE-CMM("系统安全工程能力成熟模型")和ISO17799(信息安全管理标准)等国际标准，综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面，网络安全防范体系在整体设计过程中应遵循以下7项原则：

### 网络信息安全的整体性原则

要求在网络发生被攻击、破坏事件的情况下，必须尽可能地快速恢复网络信息中心的服务，减少损失。因此，信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全威胁采取的相应的防护措施，避免非法攻击的进行。安全检测机制是检测系统的运行情况，及时发现和制止对系统进行的各种攻击。安全恢复机制是在安全防护机制失效的情况下，进行应急处理和尽量、及时地恢复信息，减少供给的破坏程度。

### 安全性评价与平衡原则

对任何网络，绝对安全难以达到，也不一定是必要的，所以需要建立合理的实用安全性与用户需求评价与平衡体系。安全体系设计要正确处理需求、风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。评价信息是否安全，没有绝对的评判标准和衡量指标，只能决定于系统的用户需求和具体的应用环境，具体取决于系统的规模和范围，系统的性质和信息的重要程度。

### 标准化与一致性原则

本系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互联互通、信息共享。

### 技术与管理相结合原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

### 等级性原则

等级性原则是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的，本系统采用信息系统等级二级（需要根据项目情况自行修改）来进行相关设计，对用户操作权限分级，对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

### 动态发展原则

系统安全设计时，要根据（最终用户单位名称）网络安全的变化不断调整安全措施，适应新的网络环境，系统设计要满足新的网络安全需求。

因此，根据系统安全性原则要求，我们从物理安全、主机安全、网络安全、应用系统安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理八个方面来进行对系统的安全性设计。

### 易操作性原则

首先，安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。因此，本系统采用操作简便。

## 系统安全机制

### 应用程序安全

应用安全主要指同系统软件相关的系列安全机制，这些安全机制直接通过呼叫中心平台系统自身实现，主要包括以下三方面：

1、程序代码安全：

(1)系统程序进行严格的权限控制，禁止没有访问权限的用户访问。

(2)杜绝文件上传漏洞，禁止非法上传文件。

(3)对用户输入数据进行验证，过滤SQL语句，禁止SQL注入和跨站脚本攻击。

(4)程序运行中严格保护系统的关键信息。

2、登录与资源访问控制：系统应做到用户统一身份认证、统一权限配置。主要包括以下四点：

(1)凡是系统页面采均用HTTPS进行通信；

(2)所有Web服务访问，都要经过授权，并且交互信息都要进行加密。

(3)账户密码采用高强度的密码，如数字+字母+大小写+特殊符号，不低于8个字符的要求。密码不得明文保存在数据库中。

(4)对于用户访问的时间及IP进行限制。

3、系统日志：对所有的业务模块记录访问者的操作日志，并提供详细的操作日志和审计数据，包括用户登录日志、模块业务应用日志、应用服务调用日志、管理操作日志、系统运行日志及系统异常日志等。

### 数据安全

1、数据备份与恢复：为了防止硬盘突然损坏、数据误操作、病毒攻击等事件发生，要求对系统重要信息进行备份，备份要做到异地存放，妥善管理。备份范围包括：业务数据库、运行程序等，备份周期为每天晚上0:00，系统自动备份。.

2、数据的加密与传输：系统数据通讯与传输，需要对数据进行特殊的安全处理，包括数据的加密存储和数据的加密传输（使用SSL）等。

### 系统安全

要求系统运行的应用服务器及数据库服务器，及时下载最新的安全补丁，安装防火墙及杀毒软件，并实时更新病毒库。

### 硬件及网络安全

因为系统部署在Internet上，所以需要使用防火墙进行维护，考虑使用VPN设备对代理店本地的物理设备行维护；同时要求指派专人进行网络监控与入侵防范、网络安全检测等。

## 应用系统安全

应用系统安全从身份鉴别、访问控制、安全审计、通信保密性、系统容错性、应用系统加密进行安全设计。

### 身份鉴别

1、系统提供专用的登录控制模块对登录用户进行身份标识和鉴别；

2、提供用户身份标识唯一和鉴别信息复杂度检查功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

3、提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

4、启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

### 访问控制

1、提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

2、访问控制的覆盖范围包括与资源访问相关的主体、客体及它们之间的操作；

3、由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；

4、授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

### 安全审计

1、提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

2、保证无法删除、修改或覆盖审计记录；

3、审计记录的内容至少包括事件日期、时间、发起者信息、类型、描述和结果等。

### 通信保密性

1、在通信双方建立连接之前，应用系统必须进行用户名、密码和检验码进行初始化验证；

2、对通信过程中的敏感信息进行加密，如气象部门与国土部门在进行会商时，对会商文件进行加密处理后上传与下载，以防止密级高的数据被他人截获与恶意使用。

### 系统容错性

对于数据容错性：一是对数据异常情况（如数据未到）进行提示；二是对未到数据提供补调功能；三可以采取候补数据替换的方式；四是加强数据的质量控制，以保证获取数据的质量。

对于功能容错性，提供人性化的错误提示，提供撤销恢复操作等。

1、提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

2、在故障发生时，应用系统能够继续提供一部分功能，确保能够实施必要的措施。

### 应用系统加密

为了保护软件不被非法复制，确保（最终用户单位名称）对软件的正当权益，系统设计采用两种软件保护机制：一种是“软”许可方式，二种是“硬”加密锁许可方式。“软”许可方式是指根据用户的机器ID号为用户生成许可文件。“硬”加密锁是指采用USB接口的加密锁将软件的许可信息写入到加密锁中，加密锁的安全防护等级较高，破解的难度较大。在“软”许可方式中，还支持限时试用的软件许可方式。在本系统中，将预留一部分（取决于加密锁的容量）许可空间，可以为专业模块提供软件许可服务。

为了保证产品发布与共享子系统的应用安全，系统提供了服务管理证书验证和基于角色的服务器权限安全管理。

WEB服务器启动采用证书验证机制进行验证，没有证书或证书时间到期，则服务启动失败并将失败信息写入系统日志。

WEB服务器安全管理采用基于角色的权限管理，系统支持自定义角色，并支持基于角色进行权限的控制，下图展示了基于角色的权限管理的设计：

系统的应用安全主要通过用户权限进行控制，通过子系统安全管理员进行业务模块的权限分配，只有获得权限的用户才可以访问相关子系统数据，且只有有权限的用户才可以进行数据的分析等工作。

## 数据安全及备份恢复

数据安全及备份恢复从数据完整性、数据保密性、数据备份和恢复进行安全设计。

### 数据完整性

建议采用共享存储（磁盘阵列，英文缩写RAID）的双机热备方式，为数据完整性提供保障。共享存储方式主要通过磁盘阵列提供切换后，对数据完整性和连续性进行保障。用户数据一般会放在磁盘阵列上，当主机宕机后，备机继续从磁盘阵列上取得原有数据。这种方式一般来讲存储的安全性较高。所以如果忽略存储设备故障的情况下，这种方式也是业内采用最多的热备方式。

### 数据保密性

由于系统运行于复杂的网络环境下，因此需要保证地理信息数据和业务数据的安全问题，使子系统客户端或者没有数据密码的客户端不能获取保密数据，我们设计了三种安全机制，数据图片化的安全机制、基于数据密码的验证机制和基于RSA的安全验证制。

数据图片化的安全机制是指：在进行地图数据发布时，将地图数据事先生成图片缓存，在数据浏览数据时，不直接去访问真正的空间数据，而是根据用户的访问请求直接将图片缓存发到客户端。客户端得到的只是不带任何地理信息的图片数据。这种方式即提高了数据的访问效率，也保证了用户数据的安全。

基于数据密码的验证机制和基于RSA的安全验证机制是指：已有数据密码的客户端可以直接通过密码验证进行登录访问，没有数据密码的客户端则需要通过RSA验证，才能进行数据访问和下载。这两种验证方式相结合，使得通过验证的客户端，才都能获得数据下载和使用的密码，而没有通过验证的客户端则不能获得数据密码，从而保证了业务数据的安全。

在本系统中，所有空间对象的存储采用大二进制方式进行存储，每种对象类型的二进制存储方式只有通过本系统才能进行解译。如果有人非法复制了数据库内容，也无法获得空间数据的内容。

在本系统中，所有数据源支持（DataSource）支持密码设定。在数据引擎中，只有在输入正确密码的情况下，才能在系统中打开该数据源。

所有数据库型数据源（Oracle、SQL Server、MySQL）都支持数据库级的安全机制，如数据访问权限的设定、数据库审计机制、日志跟踪机机制、备份和恢复机制等安全措施。

### 数据备份和恢复

数据库是系统运行的基础，需要高效安全运行，因此系统需要提供完善的数据恢复与备份机制。在发生紧急事件时，能够迅速恢复系统需要的数据，可以指定要恢复的文件，系统提供手工备份、恢复和定时备份两种操作。

## 主机安全

### 数据库系统选择

本系统采用Oracle数据库存储数据，我们通过数据库本身提供的安全机制，来提供系统安全，主要体现在以下方面：

1、身份验证：通过数据库验证的用户才能登录并使用数据库；

2、访问控制：拒绝非授权访问，防止信息泄密；

3、可审计性：建议使用Oracle数据库提供的audit审计，把对数据库的操作记录下来。建议使用使 SQL\_TRACE设置 SQL跟踪非常简单，SQL\_TRACE 是一个参数，只需要在会话层将它设置为TRUE，就开启了 SQL跟踪，Oracle将会把 SQL 语句的执行过程记录到跟踪文件中。通过查阅跟踪文件，将有利于了解SQL语句的执行过程，有助于对SQL语句进行调优、排故，非法用户的入侵行为和破坏时也能跟踪，并能及时恢复数据；

4、语义保密性：数据库的数据以某种加密的形式存储，这样非法用户即使得到数据文件也无法利用。

### 身份鉴别

1、系统启动时，必须进行用户登录；每个用户只提供三次登录机会，每个用户登录失败，锁定xxx天（项目组应自行确定限制标准）；

2、操作系统和数据库系统管理用户身份标识具有不易被冒用的特点，口令有复杂度要求并定期更换；

3、启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

4、建议对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听。

### 访问控制

1、建议启用访问控制功能，依据安全策略控制用户对资源的访问；

2、建议实现操作系统和数据库系统特权用户的权限分离；

3、限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

4、建议及时删除多余的、过期的帐户，避免共享帐户的存在。

### 入侵防范

操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

### 资源控制

1、系统通过绑定用户IP和MAC，记录用户登录情况；

2、根据安全策略设置登录终端的操作超时锁定；

3、限制单个用户对系统资源的最大或最小使用限度。

## 网络安全

网络安全从网络结构安全、访问控制、安全审计、边界完整性检查、防火墙技术、入侵防范、网络设备防护进行安全设计。

### 网络结构安全

1、充分考虑京津冀科技资源数字地图系统现有的网络环境，保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；

2、保证接入网络和核心网络的带宽满足业务高峰期需要；

3、绘制与当前运行情况相符的网络拓扑结构图；

4、根据北京市科学技术情报研究所的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

### 访问控制

1、建议在网络边界部署访问控制设备，启用访问控制功能；

2、建议能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级；

3、建议按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

### 安全审计

1、建议对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

2、审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

### 边界完整性检查

建议能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

### 防火墙技术

防火墙是目前保护网络免遭黑客袭击的有效手段，利用防火墙，用户可以防止站点的任意连接，并且还能建立跟踪工具，它可以根据日志摘要帮助用户，因为日志中记载着连接的起点，服务器提供的服务量，甚至还包含是否有攻击进入等信息。防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。

通常网络环境下一般使用软件防火墙，但软件防火墙只有包过滤的功能，因此，我们建议采购硬件防火墙提升网络安全性，硬件防火墙除软件防火墙的功能外，还有CF（内容过滤）、IDS（入侵侦测）、IPS（入侵防护）以及VPN等等的功能。

### 入侵防范

在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。

### 网络设备防护

1、建议对登录网络设备的用户进行身份鉴别；

2、建议对网络设备的管理员登录地址进行限制；

3、网络设备用户的标识唯一；

4、身份鉴别信息具有不易被冒用的特点，口令复杂度要求并定期更换；

5、具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

## 物理安全

物理安全设计我们建议从物理位置的选择、物理访问控制、硬件设备安全、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、供电安全、电磁防护来进行设计。

### 物理位置的选择

建议（最终用户单位名称）的机房和办公场地选择在具有防震、防风和防雨等能力的建筑内。

### 物理访问控制

1、建议机房出入口安排专人值守，控制、鉴别和记录进入的人员；

2、建议进入机房的来访人员经过申请和审批流程，并限制和监控其活动范围。

### 硬件设备安全

建议（最终用户单位名称）选择性能较高的服务器和网络设备，并考虑设备本身稳定可靠。设备对环境条件的要求尽可能低，能抗震防潮；本身电磁辐射小，抗电磁辐射干扰和抗静电能力强；有过压、欠压、过流等电冲击的自动防护能力；有良好的安全接地等。

### 防盗窃和防破坏

1、建议将主要设备放置在机房内；

2、建议将设备或主要部件进行固定，并设置明显的不易除去的标记；

3、建议将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

4、建议对介质分类标识，存储在介质库或档案室中；

5、建议主机房安装必要的防盗报警设施。

### 防雷击

1、建议机房建筑设置避雷装置；

2、建议机房设置交流电源地线。

### 防火

建议机房设置灭火设备和火灾自动报警系统。

### 防水和防潮

1、建议水管安装时，不得穿过机房屋顶和活动地板下；

2、建议采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

3、采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

### 防静电

建议关键设备采用必要的接地防静电措施。

### 温湿度控制

建议机房设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

### 供电安全

1、建议在机房供电线路上配置稳压器和过电压防护设备；

2、建议提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。

### 电磁防护

建议电源线和通信线缆隔离铺设，避免互相干扰。

## 安全管理制度

安全管理制度建议从管理制度、制定和发布、评审和修订三个方面进行安全设计。

### 管理制度

1、建议制定本系统建设的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

2、建议对安全管理活动中重要的管理内容建立安全管理制度；

3、建议对安全管理人员或操作人员执行的重要管理操作建立操作规程。

### 制定和发布

1、建议指定或授权专门的部门或人员负责安全管理制度的制定；

2、建议组织相关人员对制定的安全管理制度进行论证和审定。

### 评审和修订

建议定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

## 安全管理机构

安全管理机构设计我们建议从岗位设置、人员配备、授权和审批、沟通和合作、审核和检查五个方面来进行机构管理。

### 岗位设置

1、建议设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

2、建议设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

### 人员配备

1、建议配备一定数量的系统管理员、网络管理员、安全管理员等；

2、建议安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

### 授权和审批

1、建议根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；

2、建议针对关键活动建立审批流程，并由批准人签字确认。

### 沟通和合作

1、建议加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通；

2、建议加强与兄弟单位、公安机关、电信公司的合作与沟通。

### 审核和检查

建议安全管理员负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

## 人员安全管理

人员安全管理设计我们建议从人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理五个方面来进行人员管理。

### 人员录用

1、建议指定或授权专门的部门或人员负责人员录用；

2、建议规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；

3、建议与从事关键岗位的人员签署保密协议。

### 人员离岗

1、建议规范人员离岗过程，及时终止离岗员工的所有访问权限；

2、建议取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

3、建议办理严格的调离手续。

### 人员考核

建议定期对各个岗位的人员进行安全技能及安全认知的考核。

### 安全意识教育和培训

1、建议对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；

2、建议告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；

3、建议制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。

### 外部人员访问管理

建议确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

# 防错与出错处理

## 系统的出错信息及处理方法

### 出错信息

程序在运行时主要会出现两种错误：

1. 由于输入信息，或无法满足要求时产生的错误，称为软错误。

2、由于其他问题，如网络传输超时等，产生的问题，称为硬错误。

对于软错误，须在用户发出的请求操作是否合法及输入的数据验证模块由数据进行数据分析，判断错误类型，并将错误记录到系统错误日志中再返回给用户友好的错误提示信息。

对于硬错误，可在出错的相应模块中输出简单的出错语句，并将程序重置。返回输入阶段。

### 出错处理对策

所有的客户机及服务器都必须安装不间断电源以防止停电或电压不稳造成的数据丢失的损失。

在网络传输方面，可考虑建立一条成本较低的后备网络，以保证当主网络断路时，还能继续保证数据的正常通信。

在硬件方面要选择较可靠、稳定的服务器机种，保证系统运行时的可靠性。

### 出错信息与处理对策表

|  |  |  |
| --- | --- | --- |
| 出错名称 | 系统输出信息 | 处理方法 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 补救措施

由于数据在数据库中已经有备份，故在系统出错后可以依靠数据库的恢复功能，并且依靠日志文件使系统再启动，就算系统崩溃用户数据也不会丢失或遭到破坏。但有可能占用更多的数据存储空间，权衡措施由用户来决定。

1. 对一般错误给用户提示信息，用户重新输入或退出。
2. 对于严重错误，启动备份文件恢复，建议使用帮助文件。

# 系统维护设计

系统的可维护性设计主要包括应用系统的可维护性和代码的可维护性。

应用系统的可维护性包括两个方面的含义：一是指系统在向下级单位推广时，便于系统管理和维护人员快速完成系统的本地化部署工作；二是指系统在运行的过程中，如果业务发生变化，能够方便灵活的进行系统的维护和升级。代码的可维护性是指方便系统开发人员进行代码的升级和完善。

## 应用系统的本地化和升级

通过提供数据、模型、功能、产品的本地化维护，实现系统的数据、模型、功能、产品在国家级-省级之间的无缝衔接，赋予该系统本地化应用的功能可扩展和使用灵活性，充分发挥该系统在各级单位业务中的作用。

### 数据的本地化维护

在系统的实际应用中，对数据的需求是不断发生变化的，除了系统中主体业务数据的定期正常更新外，还有许多数据需要进行不定期的更新，或随环境或业务的变化而进行调整，以及数据内容的增加、数据结构的调整。因此系统提供了数据的可扩展性，主要包括以下方面：

1、提供数据转换功能；

2、只要业务空间数据遵循数据库设计规范，则可以方便的将xxxxx数据导入系统；

3、提供地图整饰功能，能够进行地图风格的配置，以满足本地化地图整饰需求；

4、系统支持导出常规业务数据的功能，从而能够与其他常用业务系统很好的集成；

5、系统预留与其他系统的数据接口。

### 功能的本地化维护

功能设计上，本系统除实现现有的业务功能外，充分考虑将来可能进行的功能扩充，提供可扩展的应用接口，进行模块化、参数化和组件化设计，避免因增加新功能而大规模修改程序，影响其他功能模块。

1、系统基础功能的本地化移植

系统基础功能的移植是指在系统数据本地化后，与本地数据进行绑定，驱动本系统在当地的稳定运行。系统在本地安装完成后将进行初始化配置，包括：

（1）默认加载的基础地理数据范围

（2）模板文件

（3）资源文件的路径配置

此外，系统还提供可视化的参数配置界面，便于系统管理员进行参数配置和系统管理，从而实现良好的本地化支持。系统提供的参数配置功能包括：

（1）服务器IP配置

（2）数据库连接配置

（3）参考资料配置

（4）产品存储设置

（5）数据备份设置等。

2、系统业务功能的本地化配置

系统功能应能够结合本地化需求进行灵活配置，以满足本地化业务服务需求。包括：

用户、角色与权限设置：每种角色赋予不同的权限，每个用户赋予不同的角色，一个用户可以拥有多种角色，从而满足不同的系统用户的需求等。

3、本地化特色功能的扩展开发

本系统按照国家软件工程的对配置项的定义将系统功能划分为若干配置项，各配置项间功能相对独立，配置项高内聚。各配置项基于插件式开发框架。基于该框架，可以扩展相关的业务插件。只要遵循一定的接口标准和二进制可执行文件规范，用户就可以自由开发新的功能插件。新的功能插件通常以动态链接库的形态存在，通过简单的注册就可以与系统连通起来。

### 系统升级

由于本项目需要全国进行推广，因此在系统的升级上尽可能使用自动升级功能，降低系统维护的费用。对于C/S系统，自动升级软件的基本功能是对软件进行升级，通过将软件各组件的最新版本信息保存为一定格式的文件，放置到网络上固定的地址。用户在使用软件的过程中，C/S系统自动通过网络从指定的服务器获得软件最新版本的信息，并和本地保存的最新版本进行比较，对更新版本自动下载相应的升级文件来实现C/S系统版本的更新。对于B/S系统，则只需要在服务器端进行系统更新和省级，客户端启动浏览器即可看到更新后的系统。

## 代码的可维护性

代码的可维护性主要通过规范代码编写过程来实现。

### 代码的规范性

C/S系统采用C#.Net编程语言，采用插件设计，模块结构良好，高内聚，松耦合。系统代码编写遵循代码编写规范，保持风格一致，不使用令人捉摸不定或含糊不清的代码，使用有意义的数据名和过程名，具备完整性（对输入数据进行完整性检查）等，添加代码注释，从而使代码易于理解。

### 代码的可测试性

系统从功能上划分为相对独立的配置项、部件和单元，各个模块高内聚低耦合，有明确的输入输出和操作流程；性能上，定义了量化的性能指标。此外，系统提供测试方案并根据各个模块编写了测试用例，使系统代码具备良好的可测试性。

### 系统运行日志

系统提供两大类日志：系统日志和业务日志。通过日志管理能够查询到系统运行时记录的日志，主要的日志类型有：数据输入检查日志、数据交换日志、数据接入日志、数据备份日志、数据格式转换日志、系统监控日志等信息。

日志查询的条件为时间段以及日志类型。能够将查询到的日志信息导出成文本文件。

对于异常情况，系统在要求稳定的同时，对于系统出现的运行时错误全部写入系统日志。系统运行日志有助于维护人员对系统运行状况进行监控，对系统出现的问题进行快速定位。

### 程序文档

程序文档是对程序总目标、程序各组成部分之间的关系、程序设计策略、程序实现过程的历史数据等的说明和补充。程序文档对提高程序的可理解性有着重要作用。系统提供各阶段程序文档（用户手册、联机帮助、系统开发日志、系统缺陷及维护记录等）（项目组需自行修改可提供的文档），在软件维护阶段，利用程序文档，可以大大简化维护工作。