**综合监控（ISCS）概要设计说明书**

**集群**

|  |  |  |  |
| --- | --- | --- | --- |
| 文档版本号： | V1.0 | 文档编号： | NG\_TS\_RTDB\_SDS |
| 文档密级： | 内部公开 | 归属部门/项目： | 专业系统部 |
| 编写人： | 阚文第 | 生效日期： | 2017-12-22 |

**版权信息**

本文件涉及之信息，属南京轨道交通系统工程有限公司所有。

未经南京轨道交通系统工程有限公司允许，文件中的任何部分都不能以任何形式向第三方散发。

网址：http://www.nanjingrail.com/

**文档修订记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **版本号** | **修订日期** | **修订人** | **修订说明** | **修订状态** | **审核日期** | **审核人** | **批准人** |
| V1.0 | 2017-12-22 | 阚文第 | 草稿版 | A |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

修订状态：A--增加，M--修改，D--删除

日期格式：YYYY-MM-DD

**目　录**

[1. 引言 1](#_Toc287377107)

[1.1. 编写目的 1](#_Toc287377108)

[1.2. 背景 1](#_Toc287377109)

[1.3. 术语 1](#_Toc287377110)

[1.4. 预期读者与阅读建议 1](#_Toc287377111)

[1.5. 参考资料 1](#_Toc287377112)

[2. 总体设计 2](#_Toc287377113)

[2.1. 设计概述 2](#_Toc287377114)

[2.1.1 设计约束 2](#_Toc287377115)

[2.1.2 设计策略 2](#_Toc287377116)

[2.1.3 设计实现 2](#_Toc287377117)

[2.2. 设计目标 2](#_Toc287377118)

[2.3. 运行环境 2](#_Toc287377119)

[2.4. 平台架构 2](#_Toc287377120)

[2.5. 总体设计思路和处理流程 3](#_Toc287377121)

[2.6. 模块结构设计 3](#_Toc287377122)

[2.7. 功能需求与程序模块的关系（可选） 3](#_Toc287377123)

[2.8. 尚未解决的问题 3](#_Toc287377124)

[3. 接口设计 3](#_Toc287377125)

[3.1. 用户接口 3](#_Toc287377126)

[3.2. 外部接口 4](#_Toc287377127)

[3.3. 内部接口 4](#_Toc287377128)

[4. 界面总体设计 4](#_Toc287377129)

[5. 数据结构设计 4](#_Toc287377130)

[5.1. 设计原则 4](#_Toc287377131)

[5.2. 数据库环境说明 4](#_Toc287377132)

[5.3. 数据库命名规则 4](#_Toc287377133)

[5.4. 逻辑结构 4](#_Toc287377134)

[5.5. 物理存储 4](#_Toc287377135)

[5.6. 数据备份和恢复 4](#_Toc287377136)

[6. 系统出错处理设计[可选] 4](#_Toc287377137)

[6.1. 出错信息 4](#_Toc287377138)

[6.2. 补救措施 5](#_Toc287377139)

[6.3. 系统维护设计 5](#_Toc287377140)

[7. 系统安全设计 5](#_Toc287377141)

[7.1. 数据传输安全性设计 5](#_Toc287377142)

[7.2. 应用系统安全性设计 5](#_Toc287377143)

[7.3. 数据存储安全性设计 5](#_Toc287377144)

[8. 系统部署（可选） 6](#_Toc287377145)

# 引言

* 1. 编写目的

本文为地铁ISCS集群与系统管理概要设计说明书，本部分与ISCS系统总体设计和其他各子系统设计共同组成ISCS概要设计文件。

系统的接口设计遵守《地铁ISCS系统技术规范》的规定，此技术标准与本概要设计作为软件详细设计和程序编制的设计依据。

* 1. 背景

ISCS系统需要提稳定、可靠、持续的监控服务。为了保证系统的关键节点能够有效的持续提供服务，ISCS系统需要采用集群的方式实现系统的设计开发和部署。

* 1. 术语

N/A。

* 1. 预期读者与阅读建议

|  |  |
| --- | --- |
| 预期读者 | 阅读重点 |
| 需求发起者和需求调研人员 | 系统架构和功能模块是否满足需求 |
| 项目负责人 | 系统架构设计是否合理，功能模块划分是否明确 |
| 系统设计人员 | 系统架构设计、功能模块划分是否合理 |
| 代码编写人员 | 根据系统架构、功能模块设计编码实现 |
| 系统测试人员 | 根据模块功能进行测试 |
|  |  |

* 1. 参考资料

N/A。

# 总体设计

* 1. 设计概述

### 2.1.1 设计约束

本部分的设计必须以《综合监控系统软件需求规格说明书》定义的需求为依据，按照需求文档的要求设计系统集群的系统架构和定义系统的功能模块。如果设计的功能是需求文档未做要求的情况，该功能不能影响或改变需求定义的功能。

### 2.1.2 设计策略

系统架构设计按照功能和业务逻辑关系进行模块化划分，不同的模块实现不同的功能，不允许夸模块的功能。模块与模块要低耦合高内聚，模块与模块通过接口交换数据。

### 2.1.3 设计实现

#### 2.1.3.1 集群架构设计

集群由管理节点和数据节点组成（图1）。



图1. 集群架构图

管理节点，集群的控制节点，主要用于集群管理和控制。例如集群启动时、集群节点故障时、集群节点故障恢复时，对应的集群节点的角色决策和切换；集群状态的查询、手动切换集群节点角色等。

数据节点，集群的服务节点，主要提供ISCS业务服务。例如RTDB节点等。

集群中的节点设计。在一个独立的集群当中，管理节点有两个，一个主管理节点和一个备管理节点；数据节点至少有一个，每一个主数据节点至少有一个备数据节点（最多3个）。

#### 2.1.3.2 节点角色决策

##### 2.1.3.2.1 决策原则

集群节点的角色裁定通过节点注册机制实现集群中的节点启动后，节点首先向它的管理者节点发起注册请求，管理者节点接收到注册请求后，根据请求注册的节点的注册先后和节点优先级，来决定注册者的集群角色是主节点还是备节点。然后把决策的结果通知给注册者节点，注册者节点接收到自己的角色信息后，启动角色对应的服务。

角色决策的原则。在没有配置优先级的情况下，先注册的为主节点，后注册的为备节点。在有优先级的情况下，优先级最高的节点为主节点，其它为备节点。如果优先级相同时，先注册的为主节点，后注册的为备节点。

特殊情况处理。集群中一个节点有多个对等节点存在时，优先级低的先注册，优先级高的后注册的情况。管理者节点应该在收到该节点的全部对等节点的注册后或等待超时后（例如10秒），在对该对等节点的注册进行主备决策。 以保证优先级高的节点作为主节点，同时防止节点角色抖动。

##### 2.1.3.2.2节点注册

节点注册分为两种情况：管理节点之间的注册和数据节点向管理节点的注册。

管理节点之间的注册。管理节点启动后，检查对等的管理节点是否存在。如果对等的管理节点不存，在则本节点作为主节点运行。如果对等节点存在则本节点以对等节点返回的角色运行。

数据节点的注册。数据节点启动后，向本集群内的所有管理节点进行注册，只有管理节点返回注册的角色信息，备管理节点仅返回注册收到信息。如果有一个管理节点返回了注册的角色信息，则数据节点以返回的角色运行并启动服务。同时，本数据节点需要继续向其它管理节点继续注册，直至所有的管理节点都注册成功。

数据节点在没有收到注册返回的节点角色之前，节点不允许启动节点的数据服务；只有收到注册返回的角色之后，节点以注册返回的角色运行，并启动角色允许的服务。

#### 2.1.3.3 集群模型

ISCS系统集群由多个独立的小集群构成的系统整体集群。独立的小集群分为车站集群和中央集群。

##### 2.1.3.3.1 车站集群

集群中管理节点有两个，每一类型的数据节点有两个，每一个节点在集群中都有一个对等的节点与之对应。

车站集群的管理节点。管理节点有两个，分别以主管理节点与备管理节点运行。管理节点具有相同的优先级，节点主备角色由注册机制裁定。只有主管理节点提供节点角色裁定和角色切换功能，备管理节点仅提供节点管理功能。

车站集群的数据节点。每一类型的数据节点有两个，分别以主数据节点与备数据节点运行。对等的同类数据节点具有相同的优先级，节点主备状态由注册机制裁定。只有主数据节点提供数据服务，备数据节点不提供数据服务。

##### 2.1.3.3.2 中央集群

集群中的管理节点有有四个，每一类型的数据节点有四个，即每一个节点在集群中存在三个对等的节点与之对应。

中央集群的管理节点。管理节点有四个，两个位于主中心，两个位于备中心。一个作为主节点运行，其它作为备节点运行。节点的主备角色由注册机制决定。管理节点具有不同的优先级，位于中心的两个管理节点具有相同的优先级，且优先级高于备中心的管理节点；位于备中心的两个管理节点具有相同的优先级，且优先级低于主中心的管理节点。管理节点的主备角色由注册机制裁定。只有主管理节点提供节点角色裁定和角色切换功能，备管理节点仅通过节点管理功能。

中央集群的数据节点。数据节点有四个，两个位于主中心，两个位于备中心。一个作为主节点运行，其它作为备节点运行。节点的主备角色由注册机制决定。数据节点具有不同的优先级，位于中心的两个数据节点具有相同的优先级，且优先级高于备中心的数据节点；位于备中心的两个数据节点具有相同的优先级，且优先级低于主中心的数据节点。数据节点的主备角色由注册机制裁定。只有主数据节点提供数据服务，备数据节点不提供数据服务。

#### 2.1.3.4 数据同步

集群节点数据同步分为启动时数据同步和运行时数据同步。

启动时数据同步。同步原则是新启动的节点向已经运行的对等节点召唤数据。

运行时数据同步。同步原则是主节点主动推送发送变化的数据给对等的备节点。

节点是否需要数据同步，由各个数据节点根据实际的业务需要自己决定。

#### 2.1.3.5 集群启动

集群启动原则是先启动管理节点，后启动数据节点。相同节点之间先启动优先级高的节点，后启动优先级低的节点。优先级相同的节点启动顺序不做要求。

##### 2.1.3.5.1 管理节点的启动

管理节点启动后，向本集群的其它管理节点注册。如果第一个启动的管理节点优先级大于等于其它管理节点，本节的以主管理节点运行；否则等待其它管理节点返回注册的角色信息，并以返回的角色运行。如果在超时时间内没有注册成功，则本节的以主管理节点运行。本集群内的管理节点必须相互注册，如果注册失败管理节点必须重复尝试注册直至成功。

##### 2.1.3.5.2 数据节点的启动

数据节点启动后，向本集群的所有管理节点注册。只有主管理节点会返回数据节点的角色信息，所有的备管理节点返回注册状态信息。数据节点在收到管理节点返回的角色信息后，以返回的角色运行，并提供服务。数据节点需要保证向所有的管理节点都注册成功，即使数据节点已经拥有角色并提供服务了，也是重复尝试向注册失败的管理节点去注册直至成功。

#### 2.1.3.6 节点角色切换

集群中节点的角色切换分为节点故障切换和人工切换。节点故障切换指当节点发生故障时，集群中的一个对等节点自动接替故障节点的角色动作。人工切换指操作员通过工具，手动为一个节点强制一个角色，集群中的对等节点自动作出相应角色调整。

##### 2.1.3.6.1 管理节点故障切换

管理节点的故障切换分为两种情况：主管理节点故障与备管理节点故障。

主管理节点故障。当前主管理节点发生故障时，备管理节点之间通过选举，选出一个优先级最高的节点升级为主管理节点运行。

备管理节点故障。当备管理节点发生故障时，管理节点之间不执行节点角色切换。

##### 2.1.3.6.2 管理节点故障恢复切换

管理节点故障恢复后，如果本管理节点的优先级比当前正在运行的主管理节点高，则本管理节点抢夺“主”角色，备抢夺的管理节点自动降为备节点。其它情况执行系统启动裁决流程。

##### 2.1.3.6.3 管理节点人工切换

人工指定一个节点为主节点，当前集群中的如果已经存在主节点，则当前的主节点自动降为备节点，被指定的节点升级为主节点。

人工指定当前主节点为备节点，集群中它的所有对等节点之间，选择一个优先级高的节点为主节点。

##### 2.1.3.6.4 数据节点故障切换

备数据节点发生故障，管理节点不对集群中发生故障的节点的对等节点做角色切换。

主数据节点发生故障，主管理节点在集群中的故障节点的对等节点中，选择一个优先级最高的数据节点作为主数据节点。

##### 2.1.3.6.5 数据节点故障恢复切换

数据节点故障回复后，如果节点优先级比集群中当前主数据节点的低，则不做节点故障切换；否则主管理节点把故障恢复的节点作为主数据节点运行，优先级低的主数据节点降为备节点运行。其它情况执行启动时裁决流程。

##### 2.1.3.6.6 数据节点人工切换

人工指定一个节点为主节点，当前集群中的如果已经存在主节点，则当前的主节点自动降为备节点，被指定的节点升级为主节点。

人工指定当前主节点为备节点，集群中它的其它对等节点之间，选择一个优先级高的节点为主节点。

* 1. 设计目标

集群能够为ISCS系统提供稳定、安全、可靠、可扩展的系统管理服务。能够保证集群中的一个节点故障后，ISCS系统能够最大成都的正常运行。

* 1. 运行环境

OS版本。实时数据库支持的OS版本有RHEL7\_x64、CentOS7\_x64、Ubuntu\_Server14\_x64、Linux主流发行版x64（内核2.8及以上）。

硬件要求。处理器8核（及以上），单核频率3.0 GHZ（及以上），内存32 GB（及以上），磁盘1 TB（及以上），1000M以太网卡，1000M网络带宽。

* 1. 平台架构



图2.ISCS集群平台架构

ISCS系统集群是一个由中心集群与多个车站集群功能构成的分布式集群系统。其中，车站集群是可以独立部署和独立运行集群。中心集群是一个可独立部署和独立运行的集群。车站集群与中心集群通过中心骨干网互联。

车站集群。部署一主一备两个管理节点，管理节点的优先级相同。部署多个不同类型的数据节点，每一类型的数据节点部署一主一备两个且优先级相同。所有车站集群采用相同的部署。

中心集群。部署一主三备四个管理节点，两个在主中心（优先级高且相同），两个在备中心（优先级低且相同）。部署多个不同类型的数据节点，每一类型的数据节点部署一主三备四个节点，两个在主中心（优先级高且相同），两个在备中心（优先级低且相同）。

* 1. 总体设计思路和处理流程

集群以管理节点作为集群处理的核心模块，通过管理节点实现集群的节点的注册、节点角色切换、集群状态查询，以及集群节点的控制等。

### 2.5.1 节点注册

集群内管理节点的注册。集群内的所有管理节点之间必须相互注册，且裁决出主管理节点。如果注册失败，即使已经裁决出主管理节点，管理节点也需要重复尝试注册直至成功。

集群内数据节点的注册。集群内的数据节点必须向集群内的所有管理节点进行注册，并且由主管理节点裁决那个数据节点作为主节点或备节点。即使数据节点以及备裁决了主备角色且正常提供数据服务了，也要保证向所有管理节点都成功注册。

### 2.5.2 控制处理

集群的主/备管理节点都可以提供集群状态查询，但仅限主管理节点提供集群控制功能。

### 2.5.3 数据同步

管理节点的数据同步，仅限于集群内部管理节点之间。车站集群之间、车站集群与中心集群之间不存在同步。

数据节点的同步，仅限于集群内部同类型的节点之间，车站集群之间、车站集群与中心集群之间不存在同步。且节点的数据同步由数据节点自己根据需要裁定。

* 1. 制作购买或复用的分析

N/A。

* 1. 模块结构设计

集群系统设计为两个部分：集群接口和系统管理。集群接口是以开发包的形式提供的API（动态库、静态库），系统管理是可独立运行的进程（对应集群的管理节点）。按照集群的功能要求，集群的系统的功能模块主要有客户端接口模块、注册管理模块、集群管理模块、心跳模块和通信接口模块。（图3）。



图3. ISCS集群模块层次结构图

### 2.7.1 客户端接口

客户端接口主要提供集群查询和控制接口。外部系统通过客户端接口来查询集群节点状态和切换集群节点运行角色。

查询接口。集群的查询接口主要提供集群管理的节点查询、节点状态查询，以及其它查询。

控制接口。主要提供节点角色切换控制，以及其它控制。

### 2.7.2 注册管理

注册管理模块，主要实现对集群中节点的注册请求进行处理，并根据系统配置的节点信息进行裁决，选择出主节点和备节点。并把裁决的结果通知给注册者节点。

### 2.7.3 集群管理

集群管理，分为两个部分：集群内部管理和外部集群管理。

集群内部管理，主要管理本集群内（车站集群或中心集群）部的节点。对节点的故障处理、故障恢复处理、人工切换节点角色处理等。

外部集群管理，主要是管理维护外部集群的信息。与集群内部管理的差别是它仅维护一些简单的外部集群信息，客户端通过本集群进行查询时，通过本集群查询到外部集群的状态等信息。

对集群的节点进行人工控制时，必须通过节点所在的集群的管理节点实现。

### 2.7.4 心跳管理

心跳管理，主要负责管理维护集群节点之间的心跳。心跳失败后需要重复尝试建立心跳连接，并发送心跳。

管理节点之间的心跳。管理节点之间要互相发送心跳包数据包，心跳包的数据内容包括本节的角色、以及管理的节点信息等。

管理节点与数据节点之间的心跳。数据节点需要向管理节点发送自己的角色信息等数据，管理节点需要向数据节点发送自己的角色信息等数据。

### 2.7.5 通信接口

通信接口，主要实现网络连接创建、连接有效性检查、数据的发送和接收，以及数据的编组和解组等。

* 1. 功能需求与程序模块的关系（可选）

本条用一张如下的矩阵图说明各项功能需求的实现同各块程序模块的分配关系，本表可用需求跟踪距阵替代：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 程序1 | 程序2 | …… | 程序m |
| 功能需求1 | √ |  |  |  |
| 功能需求2 |  | √ |  |  |
| …… |  |  |  |  |
| 功能需求n |  | √ |  | √ |

* 1. 尚未解决的问题

说明在概要设计过程中尚未解决而设计者认为在系统完成之前必须解决的各个问题。

# 接口设计

* 1. 用户接口

说明与用户接口的输入输出关系，以及将向用户接口提供的命令和它们的语法结构，以及软件的回答信息。

* 1. 外部接口

说明本系统同外界的所有接口的安排包括软件与硬件之间的接口、本系统与各支持软件之间的接口关系、协议要求等。

* 1. 内部接口

说明本系统之内的各个系统元素（各层模块、子程序、公用程序等）之间的接口的安排，包括设计用关系、输入输出要求、语法结构等。

# 界面总体设计

说明界面总体布局和风格设计。

# 数据结构设计

可以在本文说明也可以单独使用数据库设计说明书描述

* 1. 设计原则

给出系统数据库的设计原则。

* 1. 数据库环境说明

简单介绍一些数据库直接有关的支持软件，如数据库管理系统、存储定位程序和用于装入、生成、修改、更新数据库的程序等。说明这些软件的名称、版本号和主要功能特性。

* 1. 数据库命名规则

联系用途，详细说明用于唯一地标识该数据库的代码、名称或标识符，附加的描述性信息亦要给出。

* 1. 逻辑结构

数据库设计人员根据需求文档，利用数据建模技术来描述逻辑数据库结构。要求使用PowerDesigner或Visio创建数据库PDM模型。此处只需列出PDM模型名称。

* 1. 物理存储

描述整个逻辑数据模型是如何被转换为数据文件（物理模式）。文件结构类型在这里应清楚的体现。

* 1. 数据备份和恢复

描述数据库的备份和恢复策略。

# 系统出错处理设计[可选]

* 1. 出错信息

用一览表的方式说明出错的类型，以及每种可能的出错或故障情况出现时，系统输出信息的形式、含意及处理方法。例如：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **错误分类** | **子项及其编码** | **错误名称** | **错误代码** | **备注** |
| 数据库错误 | 连接 | 连接超时 | 100001001 |  |
| 连接断开 | 100001002 |  |
| 数据库本身错误代码 | 数据库本身错误代码 | 100002+数据库错误代码 |  |
| TCP连接错误 | 连接 | 连接超时 | 101001001 |  |
| 连接断开 | 101001002 |  |
| 其它TCP连接错误(socket自身错误代码) |  | 101002+ socket错误代码 |  |
| 配置信息错误 | 未配置输入参数 |  | 102001 |  |
| 未配置输出参数 |  | 102002 |  |

* 1. 补救措施

说明故障出现后可能采取的变通措施，包括：

a．后备技术 说明准备采用的后图示技术，当原始系统数据万一丢失时启用的副本的建立和启动的技术，例如周期性地把磁盘信息记录到磁带上去就是对于磁盘媒体的一种后备技术；

b．降效技术 说明准备采用的后备技术，使用另一个效率稍低的系统或方法来求得所需结果的某些部分，例如一个自动系统的降效技术可以是手工操作和数据的人工记录；

c.恢复及再启动技术 说明将使用的恢复再启动技术，使软件从故障点恢复执行或使软件从头开始重新运行的方法。

* 1. 系统维护设计

说明为了系统维护的方便而在程序内部设计中作出安排，包括在程序中专门安排用于系统的检查与维护的检测点和专用模块。

# 系统安全设计

* 1. 数据传输安全性设计

说明在数据通信和传输过程中安全性设计。

* 1. 应用系统安全性设计

说明在访问应用系统过程中用户以及访问权限、操作等安全性设计。

* 1. 数据存储安全性设计

说明在数据和文件在存储过程中的安全性设计。

# 系统部署（可选）

给出系统部署方案，尽量使用图表的形式，并辅以必要的文字说明。