核电站计算机应急辅助决策系统设计

郑 儿[1,3],由玉伟[2],石桂连[2]

(1.华北计算机系统工程研究所,北京 100083;
2.北京广利核系统工程有限公司,北京 100084)

摘 要:对核电站计算机应急辅助决策系统的使用环境、目标以及功能进行了分析,并给出了采用 C/S 和 B/S 混合结构的设计方案。系统包含数据采集处理、辅助判断、应急响应支持、应急演习四大功能,该系统对核电站应急事故处理有重大意义。

关键词:应急辅助决策系统;客户端/服务端结构;浏览器/服务器结构;分布式控制系统;动态服务器页面

中图分类号:TP319 **文献标识码**:A **文章编号**:1674-7720(2010)12-0052-05

The analysis and design for emergency decision-making support system of the nuclear power plant

ZHENG Er[1,2], YOU Yu Wei[2], SHI Gui Lian[2]

(1.National Computer System Engineering Research Institute of China, Beijing 100083, China;
2.China Techenergy Co., Ltd., Beijing 100084, China)

Abstract: This paper analyzes the environment, purpose and function for the computer based emergency decision-making support system of the nuclear power plant, and gives a design proposal based on C/S and B/S structure. System consists of data acquisition and processing, auxiliary judge, emergency response support, emergency drills four functions, the system has great significance to deal with nuclear power plant emergency.

Key words: emergency decision-making support system; C/S; B/S; DCS; ASP

核电无小事,核电站的任何事故,如果不能妥善应对,都有可能对厂区人员、公众以及环境造成具大影响,核电站应急计划必须贯穿于核电站始终。核电站的应急状态包含应急待命、厂房应急、厂区应急、场外应急四种[1]。

核事故发生时,往往面临时间紧、责任大、变化多的难题。在这种情况下,只有采用科学的决策理论,并利用计算机实时在线支持决策系统,才有可能满足核事故应急决策的要求。

目前,国外欧共体联合东欧和前苏联部分国家开发了实时在线事故应急决策支持系统。国内诸如秦山、田湾、大亚湾等核电站也建立了计算机应急指挥系统,但其功能相对单一,大多只满足数据监视功能及资料查询功能,不能很好地对应急过程起到支持作用。

本文介绍的核电站计算机应急辅助决策系统(以下简称系统)紧密贴合应急计划,能够有效接收、存储、分析、处理和发布来自不同区域的核电站信息,并在事故突发期间快速形成准确的应急指挥指令,为应急管理和指挥决策提供强有力的技术支持,提高应急管理和指挥决策的科学性和时效性[2]。

1 系统功能分析

为了满足核电站应急准备以及应急响应的需求,系统应当具备数据采集和处理功能、辅助决策功能、应急响应支持功能以及应急演习功能[3]。

1.1 数据采集和处理功能

1.1.1 数据交换

应急辅助决策系统主要通过网络实现与电站专业系统、办公系统网络、集团网络系统的数据通信。通信的数据包括文本信息、数据和多媒体等类型。

系统通信内容包括:机组数据、厂区出入监督数据、控制区出入检测系统 KZC 数据、模拟机数据、应急中心

通信数据、后果评价辐射监测数据、堆芯损伤评价、计算机源项通信数据、气象数据等。

1.1.2 数据存储和服务

在与各个数据源进行数据交换后，系统将收到的数据以通用数据库的形式保存起来，并可以随时备份。这样做有助于将来系统的扩展，并且通用数据库支持的工具众多，有利于数据分析。例如查找最大值、最小值、生成表格趋势图等。

1.1.3 人机界面

人机界面支持流程图画面、日志、表格、辅助判断画面、GIS 系统画面、各种专家系统信息画面等的显示，且界面上的图形应该可以动态变化，并支持操作人员制作和修改自己的画面。

系统应当支持趋势组态工具，以提供简单灵活的趋势分组和组态功能，实现实时和历史趋势查看、对比分析功能，同时还能极其直观地实现对多点多时间段的数据对比分析。

1.1.4 日志和报表

系统应当支持日志和报表功能，以方便应急人员记录和分析数据。

1.2 辅助判断功能

1.2.1 应急状态辅助判断

应急行动水平辅助判断功能依据《核电站应急计划》生成。

系统在接收到来自电厂各个区域的信息后，与应急行动水平进行比较，经逻辑判断后得出当前的状态，如果发现应当进入应急状态，则通过应急信息平台自动将结果发给相关应急人员，在获得具有权限的应急人员批准后，系统将进入应急状态。

1.2.2 机组关键安全功能判断

系统选取可以反映核电站关键安全功能的机组参数与运行技术规格书中的安全限值进行比较，对各机组的核功率水平、堆芯冷却、通过二回路系统对反应堆冷却剂的热量排出、反应堆冷却剂的装载量、安全壳的完整性参数进行监视，实现反应性控制、堆芯冷却、主回路完整性、主回路冷却失效、安全壳完整性的辅助判断。

1.2.3 参数超限报警功能

系统提供的实时报警功能，可以把电厂各状态重要数据参数录入报警程序，当参数的实时数据超出了预先设定的高高限、高限、低限、低低限的限值时，系统的报警数据信息会不断闪烁同时伴有报警声音，自动打印报警信息，并在系统中记录报警的时间和报警信息。

系统提供的报警类型有实时数据报警、变化率报警、偏差报警等多种类型；并提供手动确认和自动确认两种报警确认方式。

1.2.4 堆芯损伤评价

应急辅助决策系统向堆芯损伤评价软件输入数据，并提供单独的画面进行相应评价参数以及评价结果的显示和调用。

1.2.5 环境事故后果评价

环境事故后果评价计算机通过数据检索，实现从应急辅助决策系统的数据库直接获取气象数据和堆芯损伤评价计算得到的源项数据进行评价，评价结果以图片和文本文件的方式输出，应急决策系统直接调用这些图片和文本文件通过特定方式进行显示。

1.3 应急响应支持功能

系统提供应急响应行动支持功能以协助应急人员执行应急行动。应急响应行动支持功能如下：

(1)自动通知功能

系统提供自动通知功能，包括两种情况：①系统自动判定发生应急相关事故和事件，通过手机短信的方式自动通知应急值班人员；②当系统判定进入相应的应急状态(应急待命、厂房应急、场区应急、场外应急)时，应急人员手动录入通知内容并选定通知的相关应急组或人员，系统通过手机短信的方式向指定人员发送事件通知。

(2)到岗确认功能

应急相关人员就位后通过应急决策系统报告到岗就位，系统根据反馈情况自动填充应急组织状态图。未到岗人员或组织白色显示，全部就位的个人或组织灰色显示，如图 1 所示。

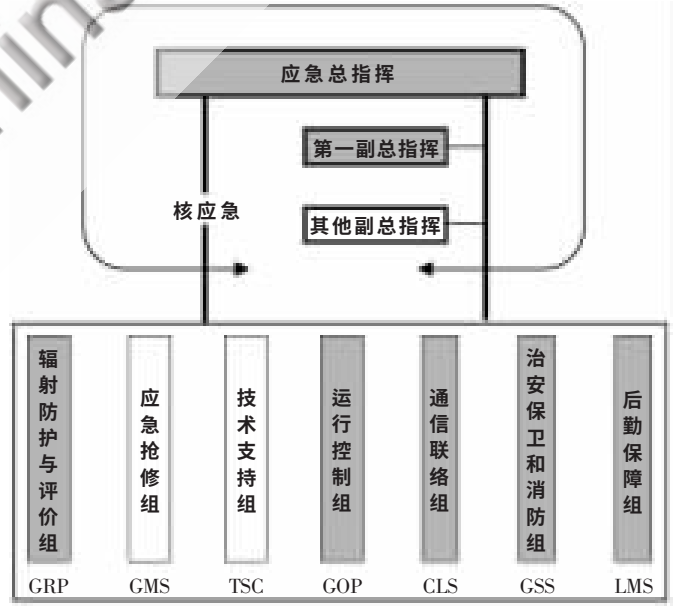

图 1 到岗状态图

通过点击相应应急小组(如技术支持组)，可以查看该组内人员的详细信息。

(3)应急任务单发放

应急决策系统为每个应急人员设定用户名和权限，

当发生报警并进入应急状态时，系统根据应急行动计划的规定自动或手工给每个应急人员发送任务单。相应的应急人员使用自己的用户名登录系统自动获取任务单。当应急状态变化时，应急指令也应相应地变化。

(4)应急资料查询

应急人员可以通过系统快速查询到所需的机组画面、应急指南等各种资料，从而根据这些资料和程序进行有效的响应；给每个应急指挥人员作一个简洁的应急响应指南，以便于在最短的时间内查询相关的资料和文件，做出快速有效的指挥和响应。

(5)应急文件流转

应急系统的一个重要作用就是要实现应急过程报告、报表的电子化，提高应急过程的工作效率。

文件的发起人指定了流转顺序，每一个处于流转环节的应急人员分别处理自己的部分，在加盖电子签章后，流转到下一部分或退回给上一个环节，每个人员可以随时查看文件当前所处位置、处理状态以及各个历时版本，最大限度地保证文档处理及时、准确。

(6)电子签名功能

系统集成电子签名功能。在核应急情况下，有些专业组与应急指挥室不在同一物理地点，报告由网络传递，通过电子签名功能可以实现报告的起草、审核、批准的流转传递，并确保文件不被修改。

(7)文件拟制签字功能

应急决策系统根据不同的事件依据应急计划预先制定相关的应急报告和文件，系统通过 Microsoft Excel 实现相关的应急报告，应急人员在需要的时候可以登录系统，手动调出相应的报告和文件(如初始通知、后续通知)，通过指定时间系统可以自动地在报告中添加该时间机组、气象、环境等参数数值，方便应急人员快速准确地生成报告。系统集成文件电子签名功能，电子签名与手写签名有同样的法律效力和不可更改功能。

系统配备专门的动态数据定义组态平台，将实时/历史数据库获得数据转移到 Excel 中，从而利用 Excel 强大的分析和数据处理能力。报表打印包括自动打印和请求打印两种。自动打印是由报表组态工具定义报表格式和事件触发功能块定义报表打印时间的报表，可以按周期触发或按事件触发来启动自动打印；请求打印则由应急人员触发打印功能。

(8)应急信息显示、绘图功能

应急辅助决策系统提供数字地图、应急计划区、主要应急设施、各应急集合点、应急撤离路线、气象与环境监测设施、医疗救护设施、消防设施等应急相关图纸的查询和显示。

系统提供交互式电子白板，计算机画面(地图)内容通过投影机投影在白板上，计算机与电子白板通过网线建立连接，应急人员在电子白板上手绘应急撤离路线等内容，会自动体现到计算机相应的文件中，实现系统的绘图功能。

1.4 应急演习功能

在核电站实际运行过程中，可能直到退役也不会出现真的事故，而应急人员应当可以随时熟悉应急流程，以便在事故情况下快速实施，因此，应急演习功能就是应急系统最重要的功能之一。

为了达到高仿真，应急系统要求能够接收机组模拟数据，并且可以自定义气象、环境、KKK、辐射监测等信息，并通过对模拟数据的判断，启动相应的应急响应流程，同时系统还应该在没有模拟数据的情况下，直接启动应急响应演习，以方便应急人员练习。

系统提供事故工况画面和演习工况画面，在事故工况下系统显示数据为真实的机组工况数据、气象数据、厂区出入监督系统数据、控制区出入检测系统数据；在模拟工况下(应急演习)系统显示的机组数据从模拟机获取，气象数据、厂区出入监督系统数据、控制区出入检测系统数据根据应急情景编制，通过文本文件输入到应急决策系统。

2 系统技术分析

由于各种原因，国内现役及在建的核电站所用仪控系统各有不同，甚至同一电站不同机组所用的仪控系统也不相同，再加上种类繁多的专家系统，应急系统与其进行数据交换时，往往需要同时面对 Modbus、TCP、OPC 以及各种自定义的通信协议，而对外部传输的参数也可能随着情况而变化，这就要求数据通信功能在保证稳定性、准确性的同时，还要具有最大的兼容性。

系统提供的辅助决策功能同样不能太过僵化。当机组传入的参数发生变化时，系统应该能够通过简单的修改即可支持这种变化，同样，当要监视的报警信息增加或者减少时，系统也应当只需进行简单修改。

应急响应支持的功能平时并不运行，只是在演习或者事故发生时才启用，因此，其关注的重点应当是在易用性上，对稳定性的要求则没有数据通信功能高。

此外，上述 3 个功能都应当支持应急演习功能，也就是既要能保证演习数据与真实数据的处理方式相同，同时还要将两者在记录时加以区分，以保证查询时不会混淆。3 个功能的特点分析如表 1 所示。

表 1 功能特点分析

名称	使用人员	特点	要求
数据采集和处理	操作人员	一旦确定，则长时间不会变更	稳定性高，兼容性好，能够长时间运行
辅助判断	操作人员 应急组员	运行后根据实际情况可能会微调，但不会大变	可靠性高，准确性好，能够长时间运行
应急响应支持	应急指挥人员 应急组员	随着应急流程及文件的升版，可能随时变化	易用性好，贴近应急流程

综上可以看出，由于使用人员以及运行情况的不同，数据通信和辅助判断部分更强调稳定性和准确性，而应急响应支持部分则更偏重易用性，应急演习功能则贯穿于整个系统。

3 设计方案

3.1 体系结构

应急系统在核电站中往往部署在专网中，以保证事故情况下应急系统能够独立运行。系统如果采用单一的C/S或者B/S结构，很可能为了满足某一部分的功能而造成大幅增加软件复杂度的情况。因此，这里采用C/S和B/S的混合结构来实现系统，从而合理利用两种方式的优点[4]。

应急系统体系结构如图2所示，系统中共部署3台服务器，其中1台为C/S结构中的通信服务器，1台是B/S结构中的Web服务器，还有1台作为数据服务器，里面安装有微软SQL2005数据库，用于存储通信服务器以及Web服务器的数据。通信服务器和Web服务器通过数据服务器进行数据交换。

系统中的设备通过核心交换机连接。应急系统客户端可以部署在厂区的各个位置，如果需要实时监视数据，并且对过程进行控制，则需要安装C/S的客户端，否则直接通过浏览器访问Web服务器即可实现浏览功能。

系统通过网关与外部通信系统相连接。各种不同格式的数据在经过网关处理后，转换为通信服务器能够识别的格式，并传入通信服务器，通信服务器对其进行分析，如果有报警或者应急状态的变化，则通过HMI部分显示出来。并实时地将数据存入数据服务器，供Web服务器和专家系统使用。

各个专家系统通过交换机直接连接数据服务器，获取各自所需要的数据，经过分析处理后，再将结果保存到数据服务器，供客户端查看。

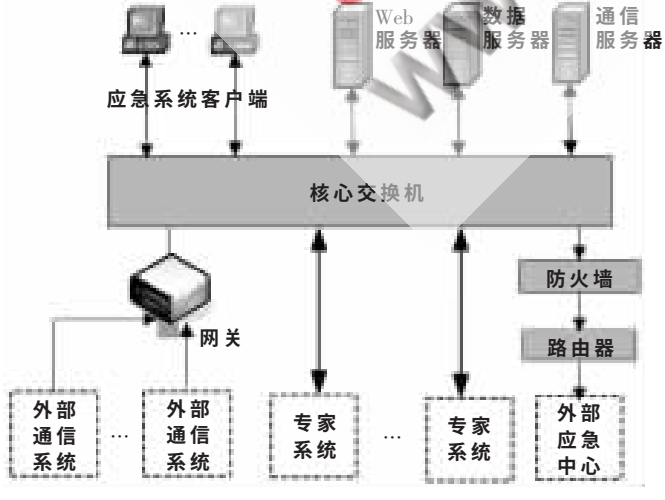

图2 应急系统体系结构示意图

最后，应急系统通过防火墙和路由器，定时将数据传输到外部的应急中心。

3.2 软件结构设计

如图3所示，应急决策系统软件体系结构分为数据接入、数据处理层、数据应用3个层次，该系统适用于数据采集显示、数据存储、工艺流程模拟、趋势分析，应急辅助判断、应急资料查询、应急演习数据模拟等功能。

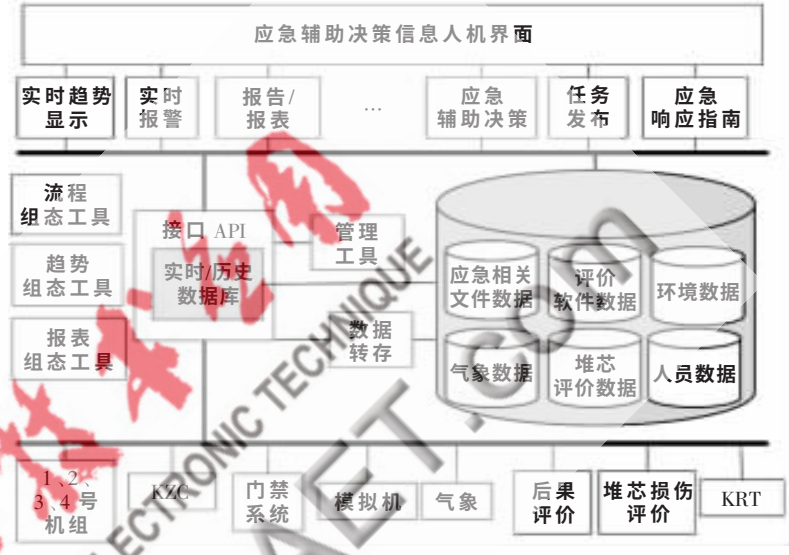

图3 核电站应急系统软件体系结构示意图

3.2.1 C/S结构设计

由于C/S方式的稳定和可靠的特性，可以用于实现与各种外部系统通信，对接收到的数据进行分析处理，并提供给流程图页面和辅助判断功能进行显示，最后将数据传入数据服务器保存。

与应急系统通信的主要部分是核电站的仪控系统（DCS）系统，虽然各个电厂以及各个机组的DCS系统均有可能不同，但都支持标准的工业传输协议（如MODBUS、OPC等）。另外，气象、环境信息以及KKK等信息的提供系统也大都支持这些协议，因此，C/S部分功能实现方式直接采用DCS系统。

3.2.2 B/S结构设计

系统采用HTTP协议为标准通信协议，以SQL Server 2005（部署在数据服务器上）作为后台数据库，共分三层：

（1）客户端（即浏览器），主要完成客户与后台的交互及最终查询结果的输出功能。客户通过浏览器向服务层发起请求，服务层将结果以及相关文档传回给客户端并显示。

（2）部署在Web服务器上的服务层，其作用是响应客户端的请求，并与数据库进行通信，获取所需要的数据，再将结果传回给客户端，或根据客户端的操作修改数据库中的数据。

服务层也分为三层，分别是表现层、业务逻辑层和数据访问层。表现层采用 C#、ASP.NET、AJAX、HTML、CSS 等技术来实现，用于控制界面的显示。业务逻辑层采用 C# 语言实现，用于处理应急响应过程中的各种逻辑操作。数据访问层采用 C# 和 ADO.NET 实现，用于处理 SQL Server 的相关操作。

服务层的三层架构方式具有如下优点：结构清晰，易维护；代码功能抽象，易重用；实现了功能、职责的独立，扩展性高；程序员可以并行开发，互不干扰，提高了开发效率。

(3)数据库层，采用 SQL Server2005，部署在数据服务器上，用于存储应急响应系统所有相关数据(如用户信息、文档信息、日志等)。

3.3 硬件构成

系统硬件主要包括网络系统、计算机系统、通信系统、会议室系统。网络系统包括交换机、路由器、防火墙；会议室系统包括显示系统、扩声系统、会议系统、摄像系统、集中控制系统、视频会议设备、音频系统。结构如图 4 所示。

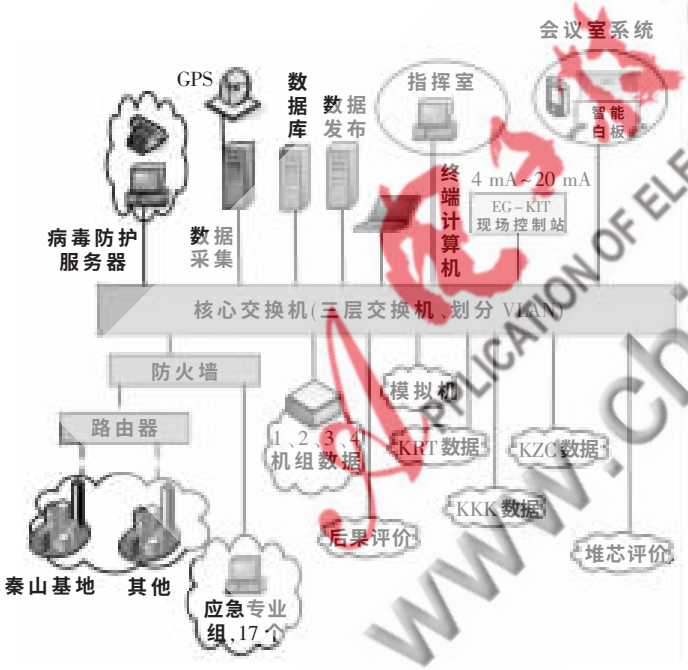

图 4 应急系统硬件结构图

3.4 网络结构设计

应急决策系统包括外部网络、EG 楼网络、厂内网络。

(1)外部网络

与核安全局、中核总等单位建立通信网络，此网络由 2 M 专线或 ISDN 组成。此网络用于与相关单位建立视频会议和数据通信。

(2)EG 楼网络

应急决策系统的专用网络，网络连接系统的服务器、台式工作站、笔记本工作站、后果评价计算机和机组网关、KKK、KZC 等系统。

应急专网采用单一核心交换机，支持路由和防火墙功能，双路交流电源供电，该交换机采用模块化结构提供高性能的数据处理能力和高可靠性。交换机连接系统的服务器、工作站和数据通信源系统，为保证数据源系统的安全性，在交换机上应用 VLAN、访问列表等功能，以保证应急网和数据源网络的安全。

(3)厂内网络

核电站的办公网络，部分应急专业组通过该网与 EG 楼网络连接进入应急决策系统，堆芯损伤计算机也在该网络上。该网络与应急专网的路由连接实现路由，通过应急专网的防火墙进行网络安全防护。防止从办公网络对应急专网的网络攻击。

3.5 方案总结

通过以上设计，应急辅助决策系统最终可以实现应急数据监视、辅助判断决策、响应流程支持等功能。

另外，系统还具有如下优点：

(1)提供开放的、平台级的设备和管理工具，可根据业务需要进行扩展；

(2)具有开放性、可扩展性、易用性、实时性、安全性以及高可靠性的特点；

(3)具有优良的性能价格比和较低的开发、维护和运营成本；

(4)有利于保护原来的信息化建设的成果和投资。

本文设计的核电站应急辅助决策系统具有功能明确、运行环境稳定、软件成本适中、管理界面友好、灵活性强和操作简便的优点。该系统已经应用于秦山二期核电站，为应急状态下应急管理以及指挥决策提供了有力的支持。

参考文献

[1] 国家核安全局.核电站营运单位的应急准备和应急响应(HAF002/01)[S].1998.5.12.

[2] 国家核安全局.核电站设计安全规定(HAF102)[S].1991.7.27.

[3] 国务院.核电站核事故应急管理条例(HAF002)[S].1993.8.4.

[4] 刘璐，汪传生.基于 Web 的 DCS 数据监控系统设计与实现[J].橡胶工业，2005(52)：102.

(收稿日期：2010-03-29)

作者简介：

郑儿，女，1984年生，在读硕士研究生，主要研究方向：计算机应用技术。