电力监控系统多重可靠冗余配置设计

王海峰，丁 杰
（国电南瑞科技股份有限公司， 江苏 南京 210003）

摘要：电力监控系统的可靠性是电网安全运行的保证，很多企业对此进行了长期研究，并提出了一些方案。最常见方案是双服务器、双前置机、多值班员机的可靠冗余运行配置。由于服务器和前置机是系统的关键设备，如果它们出现单机运行状况，则不能满足安全运行要求。该文主要描述了在双服务器、双前置机的可靠冗余配置基础上，进行服务器和前置机的多重可靠冗余的设计与实现方案。该方案已在全国多个集控中心和调度中心监控系统中实现。

关键词：多重可靠冗余；监控系统；电网

A design of multi-layered reliable redundant supervisory and control system for power network

WANG Hai-feng，DING Jie
（NARI Technology Development Limited Company，Nanjing 210003，China）

Abstract: The reliability of supervisory and control system guarantees the power network secure operation. Many vendors have researched reliability for a long time and put forward various solutions. Dual servers, dual communication controllers and multiple LMIs redundant configuration are the common solution. As servers and communication computers are key equipments, they cannot meet secure operation needs if they work alone. Based on dual servers, dual communication controllers redundant configuration, the paper mainly deals with the design and implementation of multi-layered reliable redundance. This solution has been already used in many Integrated Control Centers and Dispatching Centers.

Key words: multi-layer reliabl; redundance; supervisory and control system; power network

中图分类号： TM76 文献标识码： A 文章编号： 1003-4897(2006)24-0056-04

0 引言

随着现代科技尤其是分布式远动技术、通讯技术、信息技术的飞速发展，越来越多的变电站包括高压变电站开始实现无人值守，多个变电站内的监控功能被放到远方集中管理，电力运行人员只能通过电力监控系统对变电站进行管理，电力监控系统任何一个环节出现问题都会使变电站处于失去监控的危险状态。系统故障期间变电站脱离了调度、运行人员的监控，如果这时变电站设备发生故障，集控站和调度得不到任何信息，极有可能造成事故扩大或延误事故分析处理，对电网的安全运行、经济调度都会造成威胁和损失，社会影响更难以估计[1, 2]。因此电力监控系统的可靠运行得到越来越多的重视。

双服务器、双前置机可靠冗余运行是电力监控系统中最常见的运行方式。由于它们是监控系统的关键设备，当其中一台出现故障，立刻就不能满足安全运行要求。在维护人员维修故障机器时，如果另外一台机器再出现故障，值班员将不能监视无人值守变电站状况。为了解决该问题，多重可靠冗余的电力监控系统被提出。

1 系统工作模型

1.1 常规电力监控系统的工作模型

常规电力监控系统主要由 3 个部分组成：服务器、前置机和值班员机，有的系统还会有若干个应用机（如 VQC 机、Web 机等），他们在功能上相互独立。

服务器主要负责整个系统的协调和管理，并存储工程配置数据和历史数据，同时保证双服务器中数据的一致性；前置机主要负责外部数据的采集和处理；值班员机完成对电网的实时监视和操作功能，它为操作员提供了系统所有功能的入口[3,4]。系统工

作模型如图 1 所示。

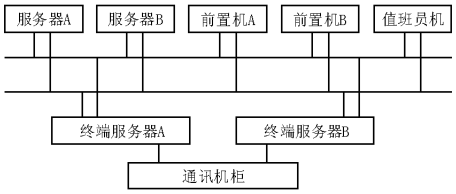

图 1 常规电力监控系统框图

Fig.1　Architecture of general system

1.2 多重可靠冗余电力监控系统的工作模型

1）如果服务器和前置机工作都正常，多重可靠冗余电力监控系统的工作模型与常规电力监控系统的工作模型相同。

2）如果双服务器发生故障，系统工作模型自动切换到如图 2 所示。

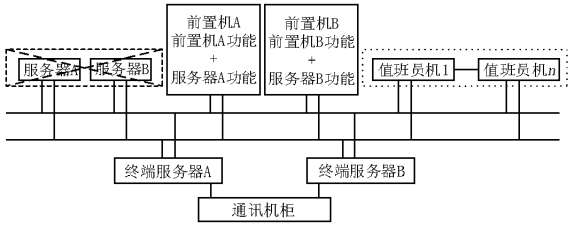

图 2 多重可靠冗余电力监控系统框图

Fig.2　Architecture of multi-layer reliable redundant system

3）如果双前置机发生故障，系统工作模型自动切换到如图 3 所示。

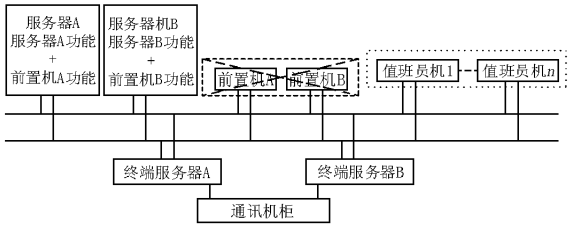

图 3 多重可靠冗余电力监控系统框图

Fig.3　Architecture of multi-layered reliable redundant system

4）如果双服务器或双前置机从故障中恢复，系统工作模型自动从图 2 或图 3 切换到如图 1 所示。

2　切换原理

在多重可靠冗余电力监控系统中，服务器与前置机相互冗余,他们除了要实现自身双机之间的冗余切换，还要实现服务器与前置机之间的多重冗余切换。

2.1 服务器切换原理

服务器是整个系统的核心，为了实现切换功能，它每秒向网上发送一包反映自身运行状态的心跳报文。当服务器发生故障时，如果其网络通讯模块运行正常，则向网上发送故障报文，否则停止发送所有通讯报文。前置机通过心跳报文来判断服务器的运行状态。

如果前置机发现双服务器都发生故障，则激活本机的服务器功能，同时向网上发送服务器功能模块心跳报文。前置机上的服务器功能模块与前置功能模块相互独立，它们之间的数据依然通过网络来交互。

当前置机检测到服务器故障恢复后，立刻停止本机的服务器功能模块。为避免服务器恢复时，服务器和前置机上的服务器功能模块发生冲突，服务器恢复后首先检查前置机上是否有服务器功能模块在运行，如果有发出请求报文，请求前置机上的服务器功能模块停止运行，等前置机上的服务器功能模块完全停止后，再启动本机的服务器功能模块。通过运行测试，这个过程可以控制在毫秒级时间内。

服务器功能模块在服务器和前置机上提供的服务完全相同，因此当值班员机请求服务器功能模块服务时（如查看曲线等），只需要通过心跳报文判断服务器功能模块运行的目标机，而不需要关心目标机是服务器还是前置机。

2.2 前置机切换原理

前置机切换原理与服务器切换原理大部分相同。为了使前置机与服务器实现快速切换，前置机上的前置功能模块与服务器上的前置功能模块必须同时接收通道数据，保证前置功能模块内的数据始终都是最新的，这样无论前置功能模块在哪台机器上工作，都能够及时地向后台转发通道数据。

当前置机工作正常时，服务器上的前置功能模块处在热备状态，它只接收通道数据，但不向后台转发数据。当双前置机都发生故障时，服务器上的前置功能模块才被真正激活。

3　数据的一致性保证

电力监控系统中的数据主要分为工程配置数据、实时数据和历史数据。他们存放在服务器的工程配置数据库和历史数据库中。由于采用多重冗余技术，系统中的数据需要存储在多台机器中，它们的一致性是系统可靠运行的重要前提。

工程配置数据是整个系统运行的基础。电力监控系统启动时，首先读取工程配置数据，然后根据

系统的配置要求，在不同的机器上激活相应的服务和功能。在多重可靠冗余电力监控系统中，为了保证服务器功能在双服务器都发生故障时能实时地迁移到前置机中，工程配置数据必须同时存储在服务器和前置机中。

实时数据是系统实时采集的各类监控信息，多重可靠冗余电力监控系统采用分布式实时监控结构，每台机器都包含实时数据以及相应的实时数据处理服务，这样能有效地提高数据的处理时间和效率。

历史数据及其提供的服务是报表、曲线、事故重演等应用的基础。它不仅向 SCADA 提供遥信、遥测采样数据提供存取服务，也向其它各个应用提供历史数据的读写功能。在整个系统运行正常时，历史数据只存储在服务器中。当双服务器都发生故障时，在此期间的历史数据存储到前置机中。如果双服务器都从故障中恢复，需要将故障期间的历史数据从前置机中同步到服务器。

当双服务器发生故障时，前置机取代了服务器功能，如果此时工程配置数据、实时数据和历史数据发生了变化，这些变化只会存储在前置机中，为了使服务器故障恢复后，服务器中的数据保持与前置机中的数据一致，服务器启动后必需进行如下操作：

1) 通过心跳报文检测前置机中的服务器功能模块是否运行。

2) 请求前置机中的工程配置数据库的数据版本号，并与本机的工程配置数据库的数据版本号进行比较，判断数据是否一致，如果不一致进行数据同步。因为工程配置数据容量有限，建议按表全部同步，以提高同步时间。

3) 读取更新的工程配置数据，进行系统初始化。

4) 检查前置机中的历史数据存储时间范围，并与本机的历史数据最后存储时间进行比较，同步本机在故障期间丢失的历史数据。

5) 同步实时数据库。

6) 发送报文，停止前置机上的服务器功能模块。

7) 激活服务器中相应的服务和功能。

4 数据通讯算法

前置机向所有后台转发通道数据时，存在双网的冗余、双机的冗余、前置机和服务器的冗余。由于存在这些冗余，监控后台可能收到来自 8 个 IP 地址的前置数据，为了避免前置数据因冗余而造成的重复，系统设计了如下数据通讯算法。

4.1 双网冗余

双网同时冗余发送数据。当发送数据包时，将一个带序列号的报头加入数据包并将其从双网同时发送，每次发送数据包时将序列号加 1。后台收到数据包后，比较其序列号（假设为 X）和上一个已处理数据包的序列号（假设为 Y）大小。X = Y，当前数据包无效，丢弃当前数据包，当前数据包已从另一网络接收。X = Y+1，当前数据包有效，继续处理。Y+1 ＜ X ≤ Y+17,当前数据包有效，继续处理，同时判定 Y+1≈X-1 数据丢失。X ＞ Y+17，当前数据包有效，继续处理。此种情况可能是网络发生长时间中断或发送设备重新启动。Y-16 ≤X ＜ Y，当前数据包无效，丢弃当前数据包。X＜Y-16，当前数据包有效，继续处理，此种情况可能是网络发生长时间中断或发送设备重新启动。

4.2 双机冗余

主机工作模式；双机中只有主机向后台转发通道数据，备机处于热备状态，只向后台发送心跳报文，反应自身运行状态，而不转发通道数据。如果因为某种错误的原因，备机也向后台转发通道数据，后台可以根据它的运行状态将其转发的通道数据丢弃。

双机工作模式；双机并行处理数据，切换方式细化到通道，根据机器性能动态调整双前置机的工作量（部分通道数据由前置 A 机转发，另一部分通道数据由前置 B 机转发）。后台收到通道数据后，首先判断通道状态，确定为主通道后，再接收该通道转发的数据。

4.3 前置机和服务器的冗余（前置功能模块）

前置机工作正常时，服务器上的前置功能模块处于热备状态，它们只接收通道数据，但不向后台转发。当双前置机都发生故障时，服务器上的前置功能模块被激活，它的所有功能与前置机上的前置功能模块相同。后台只有在检测到双前置机都发生故障时才允许接收服务器上的前置功能模块转发的通道数据，如果前置机运行正常，即使服务器上的前置功能模块转发了通道数据，这些数据也将会被后台丢弃。

4.4 前置机和服务器的冗余（服务器功能模块）

服务器功能模块占用系统资源较多，为了在整个监控系统运行正常时，前置机工作效率不受影

响，前置机上的服务器功能模块平常不工作，处于冷备状态。当它通过心跳报文发现双服务器都发生故障时，才开始激活自身服务功能。

4.5　算法效率

1）双网冗余；由于双网同时冗余发送数据，所以切换时间等效于数据编号的比较时间。

2）双机冗余；由于双机同时在工作，处于热备状态，切换时间等效于心跳报文发送和处理周期。

3）前置机和服务器的冗余（前置功能模块）；前置功能模块处于热备状态，切换时间等效于心跳报文发送和处理周期。

4）前置机和服务器的冗余（服务器功能模块）；服务器功能模块处于冷备状态，切换时间等效于心跳报文发送和处理周期 + 服务器功能模块激活时间。

5　系统与通道的接口

前置通道主要分为串行通道和网络通道，串行通道和网络通道一般通过终端服务器和路由器接入计算机。由于双前置机和双服务器上的前置功能模块处于工作和热备状态，所以它们需要同时接收通道数据。

终端服务器通过网络与双前置机和双服务器相连，因此在物理连接上与常规电力监控系统完全一样，但常规的终端服务器内置控制软件只允许与一台机器相连。我们根据多重可靠冗余电力监控系统的设计需求，向终端服务器生产厂家（如 MOXA 等）提出建议，现在已可以通过升级终端服务器内置控制软件，实现终端服务器与多台机器相连。这样双前置机和双服务器就可以同时从网络上接收一个串行通道的数据。

路由器可以将不同网络中的远方设备直接接入双前置机和双服务器，但远方设备需要建立多个网络连接。

6　多重可靠冗余技术的发展

为了进一步提高监控系统可靠性，“1+*N*” 技术被提出。“1+*N*”的功能要求监控系统按照分布式信息处理系统的特点来实现监控系统的整体功能，该功能突破功能分散式处理系统的局限性，使监控系统各个功能处理模块实现动态分布和自动平衡，确保监控系统可靠性不完全依赖某个功能节点的可靠性，即使在极端情况下单个节点也能具备基本的监控功能，并在其它节点故障恢复时保持信息的连续性。“1+*N*”技术是监控系统发展的方向。

7　结语

目前要完全实现理论上严格意义的“1+*N*”功能是相当困难的。多重可靠冗余电力监控系统在不增加硬件设备的情况下，在服务器和前置机上实现了“1+*N*”功能，为监控系统的可靠运行提供了简单、快速、实用的可行方案。

参考文献

[1] 韩英铎,姜齐荣,谢小荣,等. 从美加大停电事故看我国电网安全稳定对策的研究[J]. 电力设备, 2004, 5(3):8-12.
HAN Ying-duo, JIANG Qi-rong, XIE Xiao-rong, et al.August 14th Blackout in the US and Propose for Chinese Power System to Improving Stability and Secutity [J]. Electrical Equipment, 2004,5 (3) :8-12.

[2] 印永华,郭剑波,赵建军,等. 美加"8·14'、大停电事故初步分析以及应吸取的教训[J]. 电网技术, 2003, 27(10):8-11.
YIN Yong-hua, GUO Jian-bo, ZHAO Jian-jun, et al. Preliminary Analysis of Large Scale Blackout in Interconnected North America Power Grid on August 14 and Lessons to be Drawn [J]. Power System Technology, 2003,27(10) :8-11.

[3] 蔡春元. 电网调度自动化系统的安全运行问题探讨[J]. 继电器，2005，33(7)：66-69.
CAI Chun-yun. Choosing Internal Communication Network of Digital Substation Integrated Automation System[J]. Relay，2005，33(7)：66-69.

[4] 胡炎,谢小荣,韩英铎,等. 电力信息系统安全体系设计方法综述[J]. 电网技术, 2005, 29(1):35-39.
HU Yan, XIE Xiao-rong, HAN Ying-duo, et al. A Survey to Design Method of Security Architecture for Power Information Systems [J]. Power System Technology, 2005, 29(1):35-39.

收稿日期：2006-07-26；　修回日期：2006-09-19

作者简介

王海峰（1973-），男，工程师，长期从事电力系统自动化方面的工作;E-mail:wanghf@naritech.cn

丁　杰（1966-），男，高级工程师，长期从事电力系统自动化方面的工作。