电力企业数据恢复中心的建设

徐晓伟，李也白，张明乐

（国网浙江长兴县供电公司，浙江 长兴 313100）

摘 要：电力企业的相关生产、营销、财务、劳资等数据都具有保密性，数据一旦发生丢失或损坏，必须第一时间进行数据恢复。为此，搭建了一个数据恢复中心实验室，使这些丢失的保密数据能在内部环境中得以恢复。同时，通过加强对内部人员的培训、建立一套数据恢复规章制度和恢复流程，有效提升了企业的信息安全和数据保密能力。

关键词：电力；信息化；数据；恢复

中图分类号：TN919.5 **文献标志码**：B **文章编号**：1007-1881(2014)09-0059-03

Construction on Data Recovery Center of Power Enterprises

XU Xiaowei, *LI Yebai*, *ZHANG Mingle*

(State Grid Changxing Power Supply Company, Changxing Zhejiang 313100, China)

Abstract: Data of production, marketing, finance, human resources are confidential in power enterprises. In case lost or damaged, the data must be recovered as quickly as possible. Therefore, a central laboratory for data recovery was built so that the lost data can be recovered in the internal environment. In the meantime, by personnel training, establishment of rules and regulations for data recovery, information security and data secrecy of power enterprises are effectively enhanced.

Key words: power; information-based; data; recovery

随着信息化建设步伐不断加快，计算机、网络设施等信息化设备在电力企业得到了大范围的普及。设备中数据如果一旦发生丢失或损坏，必须第一时间进行数据恢复。由于受到数据恢复人员、技术及工具的局限性，目前县级供电公司还不具备独立进行数据恢复的能力，需要求助于外界机构进行数据恢复，但又可能面临更严重的数据泄密问题，可能会给企业造成更大的危害和损失。因此，内部人员在内部环境恢复设备的内部数据，对企业有效地加强信息安全具有重大意义。

1 数据恢复的基本方式

目前在数据丢失后，通常采取的方式有 2 种：

(1)选择一家外部数据恢复机构。虽然可以通过签订保密协议等方法确保一定的数据安全，但仍然存在数据泄密的风险；

(2)建设自己的数据恢复中心。在中心建设前期，限于操作人员的技术水平，对高难度数据恢复操作可能还不具备操作能力，仍然需要向外界求助，这时可要求外界数据恢复公司不带任何设备上门操作，用内部设备进行数据恢复，完成后也不能带任何设备离开，可保证相关数据的绝对安全。后期内部人员掌握了一定的数据恢复技能之后，就可以实现内部人员在内部环境恢复设备内部数据的目标。

为此，国网长兴县供电公司将数据恢复中心实验室的技术首次引入电力企业中，以增强企业的信息安全和数据安全防护水平。同时由于目前国家电网公司内部统一采用的是加密移动介质，对加密后的移动存储介质出现物理或逻辑故障后，数据的恢复方法[1]也进行研究。

2 数据恢复中心的建设

2.1 数据恢复中心建设的基础

信息运维技术人员通过采购硬盘数据恢复原理、数据恢复方法的相关书籍，网上查阅相关资料和典型案例，与专业技术厂商进行技术交流和分享等多种渠道，积累了一定的数据恢复知识。

目前的数据恢复技术可解决市面主流品牌硬盘、闪存(U 盘、SD 卡等)的机械故障维修，包括

硬盘固件信息丢失的修复、逻辑层面(如误删、误格等)数据恢复、硬盘盘体故障(如磁头坏、磁头卡死、电机卡死、电路板坏等)引发数据丢失后的数据恢复。数据恢复技术的研究是在以上基础上进一步研究服务器阵列丢失、服务器重组等问题，以及针对国家电网公司加密的专用存储介质在发生故障造成数据损坏或数据丢失的情况下，进行数据恢复的研究和探索[2]。

2.2 数据恢复中心建设的实施方案

数据恢复中心需要建立 1 个数据恢复和硬件维修平台。这个平台设施分 2 大类，即硬件层面类和逻辑层面类，见图 1。硬件层面的设备主要用于存储介质的硬件维修、固件维修、计算机硬件维修，能够针对硬盘不被电脑主板识别、原厂固件区(驱动)出错、硬盘 ATA 加密解密、SMART 分区表故障、硬盘数据区只读等情况进行硬盘原厂工业级修复；逻辑层面的设备主要针对硬盘分区丢失、误删除、误格式化、误克隆、黑客破坏等情况下的数据直接提取，解决数据区坏道多、硬盘固件区损坏、电机及磁头不稳定的数据提取，及磁盘阵列数据重组和数据提取[3]。

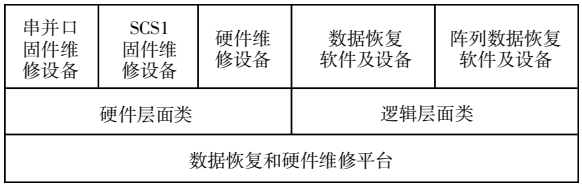

图 1 数据恢复和硬件维修平台

在拥有了硬件恢复和逻辑恢复平台之后，为故障硬盘的拆装、维修和数据恢复提供一个良好的物理环境，还应配置 1 套硬盘物理拆卸工具和 1 个无尘洁净工作平台。在拆卸硬盘盘体的过程中，硬盘拆卸工具可以将可能会发生的手误减少到最低，保障更换工作的安全可靠，提高数据恢复成功率。如果随意打开硬盘，因为硬盘内部的盘片在高速旋转时无法经受细小颗粒尘埃的冲击，极有可能使硬盘报废，无尘洁净工作平台能够确保硬盘拆卸环境达到原厂级标准，确保硬盘的安全性。

另外，还需要加强相关技术人员的培养和技术交流，使内部人员能在较短时间内掌握数据恢复的原理和方法，实现关键技术为我掌握。

2.3 数据恢复中心建设的具体实施

确定数据恢复中心实验室的实施方案后，根据需求将数据恢复软/硬件设备进行集成，主要包括逻辑层数据恢复、物理层数据恢复、固件层数据恢复、开盘数据恢复、服务器及 RAID(磁盘阵列)数据恢复等设备，以及闪存数据恢复等软硬件数据恢复工具，并进行相应的调试。

数据恢复中心实验室选用了 1 套软硬相结合的专业数据工具，主要由控制器、底层控制软件和上层数据恢复软件 3 部分组成。该数据恢复工具在设计上更具人性化，其最大的特点是不需要进行强力复制并创建镜像盘，只是在读数据成功时才建立相应的影子，对不能成功读取的数据做相应的特殊处理。所以恢复数据的速度更快、效率更高，也对源盘起到了一定的保护。其控制器设计合理、可直接通过 USB 接口连接 PC 机、快捷方便，支持硬盘热拔查，体积小、重量轻、移动携带方便，控制程序和上层数据恢复软件做到操作尽可能方便、快捷，满足不同层次用户的使用要求。图 2 为恢复工具的执行流程。

目前最为流行的是 SATA(串行高级技术附件，一种基于行业标准的串行硬件驱动器接口)、IDE(电子仿成驱动器)接口的硬盘，为了尽最大可能

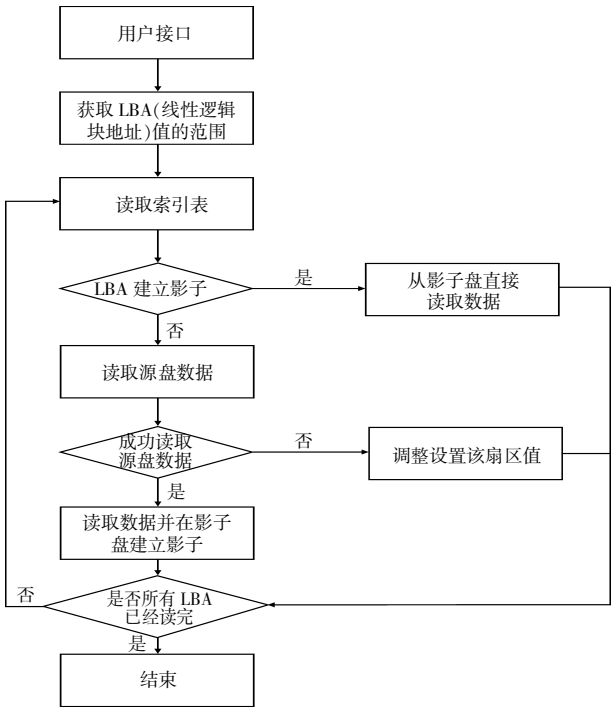

图 2 数据恢复工具执行流程

满足这部分的用户群体，该恢复工具的连接接口支持不同厂家生产的不同型号的 SATA 与 IDE 等标准通用接口硬盘。面对其他标准通用接口的连接，也可以通过硬盘接口转换卡和控制器相连接，如与 SCSI(小型计算机系统接口)硬盘的连接，就可以考虑采用硬盘接口转换卡来连接[4]。

数据恢复是实践性很强的技术操作，在具有数据恢复工作环境及相关使用工具的前提下，还需要加强相关技术人员的培养和技术交流，能够对故障做出准确的判断、采取正确的解决方法及具备灵活的操作能力，能在较短时间内掌握数据恢复的原理和方法，实现关键技术为我掌握。培训内容主要包括硬盘数据丢失故障判断、软件级数据恢复、硬件级数据恢复、存储产品维修等。

3　数据恢复中心的工作流程

在完成数据恢复中心实验室建设的同时，还通过制定相关配套的规章制度和工作流程来加强对数据恢复工作的监控和管理，确保数据恢复工作合理、合规，以进一步保障数据的安全。

国网长兴县供电公司制定了《数据恢复中心实验室管理规定》，从实验室的运行管理、设备使用、设备保管、清洁卫生等方面来规范实验室的使用。科学、合理的业务操作流程规范是数据恢复成功的重要前提，也是数据安全的重要保证：

(1)数据恢复保密协议。数据恢复中心实验室在数据恢复前，先与用户签署“数据恢复保密协议”，保证磁介质中的任何数据不向第三方透露以及磁介质在滞留期间保证不丢失；

(2)硬盘数据检测报告。说明经过技术检测，已经确认存储介质存在的问题，并且找到了相应的解决方法，经过用户授权可以将相关数据恢复，同时应该注明导致数据丢失的原因；

(3)开盘授权书。在开盘前必须签署“开盘授权书”，在得到用户授权后方可进行开盘修复操作。由于开盘修复过程中受到诸多不确定因素的影响，因此对于开盘操作的风险也必须事先做出声明；

(4)数据恢复授权书。必须在用户签署了“数据恢复授权书”后，才能开始下一步的数据恢复工作。

数据恢复中心于 2014 年开始工作，真正实现了企业内部人员掌控数据恢复技术，在企业的硬盘、U 盘等存储介质发生故障后，可以及时处理各种硬盘损坏和数据丢失状况，并且可以提前演练制定各种数据修复应急方案，以便及时响应。调整相应的硬盘数据修复策略，防范硬盘数据丢失带来的危害，保障企业安全生产、防止企业的重大利益流失。数据恢复中心解决了各种敏感及涉密性强的数据遗失和恢复问题，大大减轻了相关部门和人员涉密数据安全的管理压力，提高了工作效率。

4　结语

通过分析和调研，搭建了 1 套电力企业内部的数据恢复中心，可以为由于物理或逻辑原因造成数据损坏的普通硬盘、U 盘等设备完成数据恢复工作，根据今后的需求亦可考虑增加服务器硬盘数据销毁功能，保障企业数据安全。后期还可增加服务器硬盘修复、数据库修复，以及服务器阵列重组模块等功能。数据恢复中心实验室的建设，不仅提高了相关技术人员的数据恢复技术水平，更能进一步提高企业内部人员数据保密和信息安全意识，保护企业的内部数据，提升企业的信息安全和数据安全防护水平。

参考文献：

[1] 刘伟.数据恢复技术深度揭秘[M].北京：电子工业出版社，2010.

[2] 王晓海，张曦，袁建国.涉密数据恢复安全管理初探[J].信息技术与标准化，2011(5):41-44.

[3] 陶永红.数据恢复实践与研究[J].信息网络安全，2013(4):72-74.

[4] 王海文，黄小龙，黄瑞政.软件层面上的硬盘主引导记录数据恢复[J].大众科技，2012(6):3-5.

[5] 华莺.磁盘的数据恢复系统研究与设计[D].四川：电子科技大学，2012.

收稿日期：2014-04-23

作者简介：徐晓伟(1981-)，男，浙江长兴人，工程师，从事电力企业信息设备运行维护工作。

（本文编辑：陆　莹）