

[数据中心]

# 以重庆某数据中心为例探讨数据中心电气系统风险

文/爱玛客服务产业(中国)有限公司重庆分公司 钟建兵

数据的大集中,对很多公司或者机构来说,数据中心就变成了其业务运转的心脏,一旦出现问题,将造成无法估量的金钱、形象和声誉的损失。这给数据中心运维工作带来了巨大的挑战,而电气系统作为数据中心非常重要的组成要素之一,其重要性不言而喻。

随着数据中心日渐趋向大型化和复杂化,技术管理人员也面临着艰巨的挑战。根据一项针对数据中心的调查结果显示,在过去5年中,超过75%的公司都曾经历过业务中断,而电力系统的故障发生率在机房总体各类故障发生率的占比达到72.2%。因此,供配电作为数据中心最重要的系统,其安全可靠运行是保障数据中心业务连续运行关键的要素之一。本文以某数据中心为例,深入分析数据中心电气系统存在的常见风险,并以一个运维人员的角度,提出风险防范的思路与对策。

## 项目概况

本项目位于重庆市F区,按照A级电子信息系统机房标准建设,部署有1 059个机柜,具备10 000台服务器运营能力。数据中心为两栋建筑,一栋为数据机房(含动力中心),一栋为运维楼,总建筑面积为12 336 m<sup>2</sup>。

## 电气系统架构

数据中心电气系统供电电源由10 kV市电作为主供电源,柴油发电机组作为应急电源,UPS用于数据中心信息设备的不间断供电。本工程引入两路市电,每路市电容量为11 500 kV·A,分段运行,互为备用,当一路电源故障时,另一路电源

能保证其所有负荷的供电。同时,系统设置7台10 kV柴油发电机(2 000 kW/台,6+1冗余)作为应急电源。系统在10 kV母联柜上设自投自复装置,两路市电都有电时,负荷由两路市电供电。当任一市电停电时,另一路市电自动投入,当市电恢复时,自动断开。当两路市电停电时,柴油发电机组自动起动,并机成功后向两段10 kV母线供电,任一市电恢复后,市电电源自动投入。备用电源自动投入(以下简称备自投)装置满足自投自复的同时带手动功能。

系统采用4台2 000 kV·A(暖通、建筑和消防等动力负荷)和6台2 500 kV·A(IT负荷)干式变压器,每段母线挂5台变压器,两段母线下边各5台变压器互为备份。每两台变压器(400 V侧)之间设ATMT自投装置,当任一变压器失电时,母联自动投入,恢复时,母联自动断开,分合闸时间按避开高压备自投装置动作时间设置。

本工程的IT负荷不间断电源系统均采用2N(N=2)系统保障,每组由两台600 kV·A UPS并机运行,蓄电池组单路后备时间15 min,选用静态交流高频UPS,电池室和主机物理隔离。共计有7个机房,其中4个机房采用列头柜向机柜供电,3个机房采用始端箱+密集母线槽向机柜供电。

## 电气系统风险案例

风险分析一：10 kV系统两路市电、应急电源之间，设备自投装置进行自投自复，但仅设置一套备自投装置，一旦备自投装置发生故障，将导致电源切换失败。不满足A级电子信息系统机房内的场地设施应按容错系统配置的要求。

风险分析二：10 kV系统所有手车开关位置、继电保护装置和二次回路电源开关状态等均未接入DCIM系统监视，完全依靠人工巡视，合母（储能）电源为例，本项目高压柜体上仅有一个很小的指示灯来指示开关是否储能，人工巡视极易被疏漏。为了确保可靠性，备自投装置动作时需要开关等设备发送众多动作信号，并需要复杂的反馈作为是否满足动作条件的逻辑判定，而手车开关位置等未受到DCIM系统监视，一旦任一设备的位置或状态错误，动作或反馈失败均会导致备自投装置逻辑中断，操作失败。继电保护装置更是10 kV系统可靠运行的核心，不接入DCIM系统监视，保护与告警信息将不能被及时发现，存在带故障持续运行甚至故障扩大的风险。

风险分析三：柴油发电机采用快速起动机组，6+1并机运行，但并机母线为单母线。另并机系统控制电源为双路交流市电转DC 24 V供电，应急电源为系统自配2节12 V蓄电池，蓄电池内阻、电压等参数未受到监视，电池老化容量下降无法及时发现，存在较大的双路市电停电后柴油发电机无法启动并机风险。市电转DC 24 V开关电源也无冗余备份，存在单点故障风险。

风险分析四：本项目部分机房采用始端箱+密集母线槽供电，此种供电方式将配电设备设计在了机柜顶部，减少了列头柜，确实节约了机房空间。但因始端箱内空间狭窄，而电源电缆型号为 $4 \times 120 + 1 \times 70 \text{ mm}^2$ ，电缆直径大，转弯半径小，施工时极易留下缺陷。且这种设计方式在带电状态下不能打开箱门，无法进行巡视测温。本项目目前在前期负载率较低情况下，已经发生一次因发热导致机柜断电的情况，后进行的风险排查中又发现了其他几处同类隐患，后期运行风险极大。

风险分析五：本项目弱电系统仅设置1台UPS主机，主机容量75 kV·A，后备时间15 min，蓄电池与UPS在同一物理空间，UPS供电电源来自运维楼建筑电源配电箱，非单独供电回路。一旦发生故障供电中断，将导致BA、DCIM、门禁和监控等弱电系统供电中断。达不到国标A级机房不间断

电源系统配置应为 $2N$ 或 $M(N+1)$ 冗余（ $M=2、3、4、\dots$ ）的标准。

风险分析六：人为操作风险，从历次数据中心电气故障事件分析来看，有相当部分的风险来自运维人员的操作不当或操作失误。本项目是当地首个数据中心项目，大部分运维人员无数据中心运维工作经验。运维人员技术覆盖面不全，缺乏能够处理综合性、复杂性问题的能力，当面临问题时，技术上的不全面导致误操作的可能性增大。

## 电气系统运行安全思路与对策

### 1. 跟踪落实供配电系统风险改造

供配电系统作为数据中心的基础支撑平台，供配电系统的电能质量稳定性直接影响数据中心的安全运行。因此，推动数据中心电气系统安全风险整改，从根源上解决隐患，将数据中心的可用性等级提升，是本项目电气风险防范工作的首选。但考虑项目已投入运行，改造受到各种条件的限制，且必须在保证机房负荷不停电的情况下进行。因此，每项改造必须要深入分析改造的风险，从设计、施工、调试和运行等角度提出风险控制的策略后，才允许实施，不能因为改造带来更大的风险。另外，改造费用投资也是一项必须要综合考量的因素，项目前期建设已经投入大量资金，如果再投资大笔资金进行改造，就会对项目带来很大的资金压力。因此风险改造的思路还必须综合权衡改造投入与风险等级，资金投入低的，不管风险高低，能改尽量改；而资金投入大的则要仔细评估风险等级，确实存在高风险才按容错系统配置改造。暂不具备改造条件的风险可采取持续探索优化途径，逐步降低风险等级的方式解决。以本文中的风险四为例，如果要从根源上解决此风险，必须要改变原有的供电方式，而无论从现场情况还是资金投入来说，这都不太现实。因此，项目运维团队将风险改造的思路放在了在始端箱及各分支箱内增加温度探头，这样既能降低风险，在改造资金上也不会对项目带来压力。

### 2. 培养高素质、专业化的运维人才队伍

什么是数据中心最宝贵的财富？是“人”。因为无论设备是否设置冗余，都有故障的可能，更何况现有的风险也不具备100%改造的可行性，这时就需要人员进行快速有效的处置来保障运行安全，如果人员的技术不全就好比埋藏的“不定

（下转第71页）

最为常用的安全保密手段之一。

#### 4. 数据交换网技术

数据交换以网络方式进行，通过缓冲区隔离，防止网络数据泄密。数据交换网相比其他边界安全技术有明显优势：综合应用多种安全网关，增加安全保障；专家和监控者可在缓冲空间内对付黑客入侵；业务代理使得来访人不能进入内网，保证数据的完整性。

#### 5. 数据完整性防护与自愈方法

数据完整性保护可包括防护、检测和恢复三个阶段。在明确需要保护的数据后，三个阶段是一个顺序发生的过程，首先利用完整性防护模型对数据进行防护，防止外界的恶意入侵，非法篡改数据等行为，这也是目前用的主要防护方法。

然后通过完整性检测和评估来检测数据目前所处的安全状态。对已经发生的入侵，则需要对相应的数据进行完整性的恢复即数据自愈。

### 结束语

本文根据供电服务指挥系统的信息交互需求，分析了多源输入数据的内容与结构特征，总结出了数据接口需要实现的技术目标。通过对Web Services接口、数据库接口等多源系统集成技术的研究，总结与技术目标相适应的接口方案。并且为了有效避免恶意攻击，提出了保证数据交互安全可靠的防护标准。EA

(收稿日期：2019.12.01)

(编辑：朱金凤)

(上接第67页)

时炸弹”，不但不能确保运行安全，甚至有误操作导致事故扩大的可能。因此数据中心的安全运行还必须培养一支高素质、专业化的数据中心电气运维技术和管理团队。为了早日达到这一目标，本项目在避免人为失误操作和电气专业化培养方面做了大量工作，制定了各电气设备图文并茂的操作手册，完善了操作流程，每周开展岗位技能提升培训等。同时配套建立了完善的引进、考核、培训管理和知识库管理体系。

#### 3. 不断开展风险排查分析

没有意识到风险是最大的风险，风险意识对数据中心的安全运行有着重要意义。本项目在风险排查上不断探索，建立问题记录表，每班进行风险排查；针对行业其他的数据中心发生的事故进行举一反三专项风险排查；开展风险排查月活动，从市电电缆到高压柜、变压器、低压柜、UPS和列头柜；从电缆沟到电缆井、桥架、吊顶和夹层等进行全方位无死角的风险排查，并将风险分析能力作为员工绩效考核的重要依据。

#### 4. 不断完善运维制度体系

优化日常运维工作，完善应急管理流程，强化风险把控。合理安排运维工作，确保设备巡视无遗漏，设备维护保养无疏忽。健全运维督导工

作体系，确保运维工作7×24 h管理无漏洞，运维质量检查无盲点。加强运维应急处置能力建设，分析其他灾难事件处置经验，丰富应急演练层次。以双路市电中断故障为例，针对本项目可能存在的风险及结合其他数据中心同类灾难处置经验，目前已经制定了双路市电停电，柴油发电机不能自启动（备自投系统故障）；双路市电停电，柴油发电机不能自启动（并机柜蓄电池电压低）；双路市电停电，柴油发电机不能自启动（发电机故障）；发电机油路故障等场景的应急预案，并逐步实现演练的作业化、常态化。

### 结束语

数据中心与一般建筑相比，是一项复杂的系统工程，而电气系统在数据中心各个系统中的相对复杂度更是非常高，设计、建设期需要考虑的问题太多，因此难免留下一些不完美的地方。本文以某数据中心为例，介绍了数据中心电气系统架构，电气系统风险分析，以及风险应对思路与策略，希望能实现经验的交流与共享。EA

(收稿日期：2019.11.28)

(编辑：朱金凤)