

[供电服务]

供电服务指挥系统中数据集成需求与技术方法研究

文/国网甘肃省电力公司、北京中恒博瑞数字电力科技有限公司 李 策 刘克发 李方军 白文远 韩世飞

为了解决供电服务指挥系统中营、配、调协同不足和业务融合不够的问题，提出一种多源端数据的集成方案。分析多源输入数据的来源、内容与结构特征，根据其信息交互需求，提出数据接口需要实现的技术目标。通过对Web Service接口、数据库接口等多源系统集成技术的研究，得到与技术目标相适应的接口方案。

当前，电网公司在配用电数据采集与应用方面有一定的基础，但是面向客户的服务中，数据来源众多，不同方面的信息由不同的系统提供，如图1所示。由于数据模型有可能不一致，而且管理模式为“分散式”，不同来源的数据难以实现深度融合，导致客户诉求的处理链条长、矛盾协调困难、最终响应过慢。而且营、配、调系统运行在“孤岛状态”，限制了配、用电大数据的利用，缺乏“一站式”管理，缺乏对过程的管控。传统的营、配、调业务各自为政的模式日益暴露出不适应电力系统发展的不足，因此供电服务指挥系统的建设变得极为迫切。为解决这一问题，电网企业决定建设供电服务指挥系统，改善响应速度，强化专业协同，缩短管控链条，提高管理能力。

为了破除各个信息源呈现“信息孤岛”的现状，使数据能够被交换和共享，需要首先解决数据集成的问题。多源信息数据由于来自于不同的业务部门而显得孤立，然而，这些数据中同时也包含着相互关系，将这些数据集链接起来，就构成了颇有价值的数据网络。网络的背后是其共性以及信息系统的整体特征。

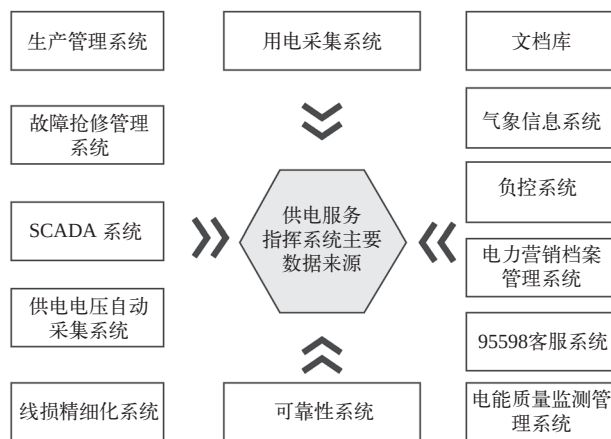


图1 供电服务指挥系统数据来源和类别

输入数据分析及接口技术目标

1. 主要数据源分析

电力系统传统的管理模式为竖井式，在这一模式下建立了多个为配用电业务服务的信息来源。对主要数据源分析如下。

1) 电网拓扑数据。电网拓扑数据来源于配电网中的生产管理系统，其中包括了表征电气连接关系的电气拓扑和表征地理连接关系的地理拓扑。它们是网络分析，故障范围划分等的重要依据。

2) 一次设备台账数据。一次设备台账数据来源于配电网中的生产管理系统。数据格式主要有xml和xls。

3) 配电网调度运行数据。配电网调度运行数据来源于数据采集与监视控制(SCADA)系统,系统同时提供了各项遥感量及非电量数据。数据文件格式为E格式文件。

4) 分布式电源数据。来源于用户信息采集系统。分布式电源位于用户附近,所发电能方便就地利用。数据格式为dmp格式文件。

5) 对节点电压的运行监测数据。对节点电压的运行监测数据来源于供电电压自动采集系统。数据格式为dmp格式文件。

6) 配电网线损数据。配电网线损数据来源于线损精细化系统,线损精细化系统开放数据库,提供大数据平台可读用户名密码,权限。配电网线损数据包含理论线损和统计线损。

7) 可靠性数据。可靠性数据来源于可靠性系统,物理实体可描述可靠性运行事件、可靠性设备操作记录、可靠性运行事件统计数据 and 事件影响相关用户记录表,实体类型为业务表的形式。

8) 配电设备运维数据。配电设备运维数据来源于故障抢修管理系统。系统同时提供了抢修资源信息和专家库,数据格式主要为E格式文件。

9) 实时的电能质量数据。电能质量数据来源于电能质量检测管理系统。除了实时的电能质量数据,系统同时提供了最值、均值及95%概率值等统计数据,实体类型为业务表。

10) 用户档案数据。用户档案数据来源于电力营销档案管理系统。

11) 用户用电数据。用户用电数据包含100 kW以上用户用电数据、50~100 kW用户用电数据和50 kW以下用户用电数据。

12) 气象信息数据。气象信息数据来源于气象信息系统,气象信息数据是按照日期命名的数据文件,一个气象站一份文件,信息数据组织成E格式文件。

13) 客户服务数据。包括通过电话的服务数据、通过多媒体的服务数据、客服受理数据集和客户档案信息留存,来自95598客服系统。

2. 接口设计目标

数据接口是多源数据和供电服务指挥系统的数据平台交互的通路,因此实用高效的接口设计是稳定的供电服务指挥系统的前提。一方面,接

口的设计需要实现多源信息的集成;另一方面,要满足在不同网络下的传输需求。接口设计有如下几个目标。

1) 开放性。接口能够满足不同的计算机环境和不同的网络系统。即不依赖于特定的编程语言和特殊的计算机硬件结构及操作系统。

2) 高效性。通过优良技术快速实现既定目标。

3) 可靠性。接口应该能够适应长时间的、复杂的使用条件,系统的可靠性和数据传输、数据交互的稳定性不受到工作量增加的影响而降低。

4) 保密性。接口应配备保证安全的防护措施和保密措施,保障数据安全性。

5) 通用性和发展性。接口技术可以通过简单移植而应用于其他新加入的数据源系统。

接口方案研究

基于多源数据特点及接口设计目标,数据集成采用以下几种接口方式进行。

1. Web Services接口

Web Services是一种与平台无关的接口技术,它基于XML,主要用来促进跨平台的程序对程序的服务。经Web Services接口的操作,通过XML的标准化消息传递机制,得以借助网络访问任意节点的服务。它的重要特点体现在多个系统同平台运行时的功能整合上。Web Services可以用来使分散于不同节点上的功能集成起来。它提供的简单且廉价的信息整合方式,适合用于整合新系统和遗留系统之间的业务流程。

2. 基于IEC 61970的CIM XML接口方式

基于IEC 61970标准的电力应用系统能够以XML的格式进行数据传输。这种传输方案基于共同的CIM进行,因此很大程度上简化了格式转换的步骤,通过XML的信息传输快捷而又能被交互的双方正确接收。一方面可以传递表征网络模型的信息;另一方面可以传递遥信和遥测数据。

3. 基于SVG的图形传递

表征网络模型的信息可以通过CIM/XML的接口方式获取,但是图形界面的传递仍然存在问题。在图形格式方面,通过标准SVG的图形交换方式,将系统单线图、监控图像等转换为SVG格式,可以简化第三方系统/应用模块的图形处理,大大减少工作量,方便了图像的交互。

4. 基于数据库的信息交互

通过JDBC接口,把不同数据库连接起来,

可以使数据集中到一个实时库里，便于统一的流程管理和应用调度。库的数据结构由双方先约定好，在一次写和读的操作中，由一方先写入内容，完毕后由另一方读出。这里涉及时间配合的问题，因此双方对于读和写的时间应做好约定和标识，写入完毕后再发信号提示读取，或者是信息交互定时进行，以免发生收信方在信号为输入完毕时进行读取的情况。如果是实时的数据在不断发展中，则不涉及此种时间配合的问题。

5. 基于专用通信协议的信息交互

和基于数据库的信息交互不同，基于通信协议的信息交互方式通过一整套的协议约定解决读写配合问题。协议对于数据包写入、加密、识别和读取都作了详细规定，因此具有良好的适用范围，可用于不断发送的实时数据，也适用于不定时的信息交互。

6. 基于E语言的信息交互

为了电网各类非实时信息的高效、便捷交互，国调制定了E语言技术规范，进行文本类信息传输。传输非结构化文件如配电设备运维数据、配电网调度运行数据等更为高效。

保证安全的防护标准

在供电服务指挥系统中的大数据层、大数据调度以及大数据访问和存储中，都需要检测网络入侵，避免恶意攻击。为使供电服务指挥系统与多源端系统集成数据流交互得到有效的检测和控制数据的安全性，有必要编写供电服务指挥系统与多源端系统集成安全标准。

本标准的制定可以有效地避免恶意攻击，提高数据交互过程中的安全性和可靠性。电力信息系统安全防护标准的提出，不仅可以指导电力信息系统安全工作的开展，还可以保证供电服务指挥系统系统运行的安全、稳定、经济和优质运行。

供电服务指挥系统与多源端系统集成安全标准内容如图2所示，主要包含了：防火墙、安全隔离网闸、信息加密算法、数据交换网技术、数据完整性防护与自愈方法。

1. 防火墙

防火墙是一种将局域网和广域网分开的方法，一个具备包过滤功能的简单路由器。它能限制被保护的网与外网之间的信息存取和交换操作。

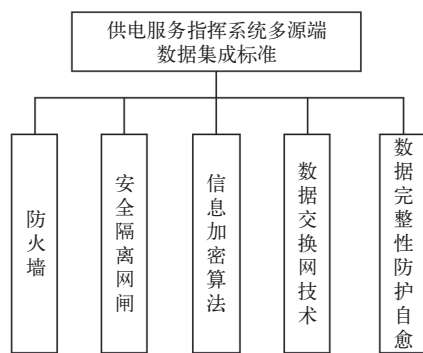


图2 安全标准的构成

包过滤技术：包过滤板块工作在网络层，功能是在端口区分包和限制包。具有包过滤功能的路由器逐一审查包头信息，包括TCP/UDP的源及目的端口号、通信协议的类型、源地址和目的地址、数据包的入接口和出接口，并根据匹配和规则决定包的前行或被舍弃。如果数据包中的信息与某条过滤规则匹配，同时该规则对数据包通过表示允许，则该数据包会被转发；如果信息与某条过滤规则匹配，但是该规则拒绝数据包的通过，则数据包被丢弃。当没有可与该数据包信息匹配的规则时，缺省规则会决定数据包是被转发还是被丢弃。

代理：代理是套有特定功能的应用层代码，功能上是网络信息的中转站。它对网络上的信息进行监听和检查，对访问内网的数据进行过滤，所有通信都必须经应用层代理软件转发，从而起到隔断内网与外网直接通信的作用。代理方式下，内网用户对外网的访问变成代理对外网的访问。

2. 安全隔离网闸

安全隔离网闸是采用SU-Gap安全隔离技术，用于不同安全级别网络之间的安全隔离，创建一个内、外网物理断开的环境，并且提供适度的数据交换的系统，由内网处理单元、外网处理单元、隔离与交换控制单元组成。内网处理单元包括内网接口单元和内网数据缓冲区，对数据进行检测、剥离和存放。外网处理单元与内网处理单元功能相同。隔离与交换控制单元是数据交换的摆渡船，控制交换通道开启和关闭。

3. 信息加密算法

该项标准内容是解决了网络安全问题的主要保密安全措施。信息加密算法在一定程度上提高信息传输的安全性，保证传输信息的完整性，是

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)