5.7. 售后服务

5.7.1. 售后服务措施

5.7.1.1. 售后服务原则

我公司非常重视此次项目，领导要求公司各相关部门为用户提供全面的集成和售后服务。公司将以整体的优势，全面支持本项目。

针对用户系统的特点以及项目的重要性，为了更好的完成技术支持和服务工作，为用户提供最有力的服务保证，我公司将利用完善的支持队伍，成立针对本项目的售后服务队伍。

我们的服务将主要遵循以下原则：

- 以处理问题、故障，保障系统安全畅通为第一原则：

本着我公司“用户至上，用心服务”的一贯宗旨，在施工过程中如果遇到非本项目问题、故障，我公司将尽最大努力帮助客户在最短时间内解决问题、故障。

- 快速响应原则：

我公司的技术服务机构覆盖了本次工程的实施节点，我们的技术支持服务将 24 小时以本地化的快速的现场响应为原则，当系统出现问题、故障时，都将提供快速现场响应。

- 备件先行原则：

当硬件设备出现故障时，我们将提供快速的备件更换服务，保障在最短时间内恢复正常工作。我方将充分调动公司技术支持中心的备件资源，并协调厂商的备件资源，为客户提供快速的备件更换服务。

- “用户至上、用心服务”原则：

我方将遵循“用户至上、用心服务”的原则，时刻把客户满意放在首位。在作好本职支持工作的同时，服从客户的统一安排和调度，协助客户做好其他方面我方力所能及的工作。

5.7.1.2. 售后服务目标

我公司的服务目标是：秉承“用户至上、用心服务”的理念，为客户提供全方位、

全过程、全业务“一站式”服务，全面满足客户通信、增值应用及整体服务的需求，在为客户提供创造价值的服务过程中不断提升企业的价值。

在服务期内，我方及原厂商负责对所提供的设备进行保修，并迅速更换发生故障的产品。

为了保质保量的做好这项工程及技术支持服务,我方承诺配备齐备的技术素质过硬的技术支持队伍,配备的人员都具有类似此项规模工程的经历和必要的经验及必要的服务意识，承诺各项目组的技术支持队伍在售前和售后相对固定，如果进行必要的替补或调离，将会在第一时间与客户协商，征得同意。

5.7.1.3. 售后服务范围

售后服务范围包括网络设备的安装、运行、维护、升级服务系统、故障解决、定期巡检、系统监控、技术支撑服务、技术资料归集、系统培训、用系统运维服务、培训运维服务和平台展示运维等工作。

5.7.1.4. 售后服务形式

我方将为本项目提供 3 种方式的故障排除服务：

➢远程诊断服务

根据客户提供的故障信息,对故障进行诊断，并对故障的处理提出建议。

➢远程处理服务

通过电话指导的方式，或者在客户允许且条件具备的前提下远程来处理客户的故障。

➢按需现场服务

首先通过电话指导或远程登录的方式来诊断和处理故障，如果故障不能够通过远程处理方式解决，指派工程师在规定时间内赶赴客户现场处理故障。

5.7.1.5. 响应时间

（1）故障报修热线服务提供 7×24 小时不间断的电话服务支持，不限次，响应时间不超过 60 分钟。采购人在使用维保范围内硬件或软件如遇到问题，都随时可以拨打 10000 或 03938990012 电话支持与帮助。

（2）远程问题诊断和支持服务提供 7×24 小时远程协助支持，响应时间不超过 60 分钟。若故障不能通过热线支持解决，我公司可使用远程支持服务工具对服务范围内的软件进行远程诊断，或通过其它远程方式为解决问题提供帮助。

（3）现场支持服务对于通过电话支持和远程支持都不能解决的软件故障，我公司提供 7×24 小时现场支持服务，安排经验丰富的技术支持工程师赴现场分析故障原因，制定故障解决方案。现场技术支持完成后，技术支持人员需向采购人提交现场技术服务报告，采购人签字确认，双方各自存档。

5.7.1.6. 运维服务

我公司根据采购人的实际情况，分析现有系统的业务特点和设备运行情况，提供完整的系统服务方案，包括设备巡检计划、维护保养时间计划表、建立各种设备预防性维护保养规程等。提供详尽的技术手册，实施严格的项目管理，成立专门的服务团队，指定维保项目负责人，对服务支持实施严格的服务管理，统筹相关工作，以保证维保服务正常高效运行。

5.7.1.7. 巡检计划服务

我公司会定期对系统进行巡检。巡检服务包括以下内容：

巡检服务包括以下内容：

1、网络设备巡检

（1）网络设备运行情况及资源使用情况；

（2）应用进程；

（3）应用和传送后台日志占用情况；

（4）监控系统性能以及进程；

2、网络运行环境巡检检查网络的运行健康性情况，分析和判断网络的运行情况是否满足系统稳定运行的必要条件。

3、在线运行的应用软件巡检。

4、系统数据的规范性以及备份情况巡检。

5、前一次巡检发现问题的解决情况。

6、根据巡检情况形成巡检报告。

5.7.1.7.1. 日常维护标准

类别	项目	维护标准
管道光缆	标识标牌	1、人孔内的光缆必须绑扎标志牌。2、标志牌标明线路名称、芯数、中继段。3、站在线路路由正上方，确保在路由上的任一点能看清前后标志和路由走向，有碍路由视线的围墙、障碍物上应喷涂醒目“光缆”字样及箭头示意。
	人井	1、人井、井圈无塌损，井盖无丢失，井盖不得被泥土、杂物覆盖,清楚易见。2、手（人）井内积水不淹到管孔及接头盒。
	光缆	1、人孔内光缆接头必须固定在井壁内侧，安装牢固，余留光缆必须捆扎固定在井壁上。2、光缆余留的曲径大于光缆直径的 20 倍。
直埋光缆	标石及宣传牌	1、标石出土出 90±5CM。2、每公里不少于 10 块，必须达到站在线路上方任一点能看通路由的效果。3、宣传牌每公里不少于 4 块。4、标石、宣传牌无损坏、字迹清楚、编写正确。
	光缆位置与埋深	1、 巡检员熟悉光缆位置和埋深。2、埋深符合标准。
	光缆路面维护	光缆路由上 3M 范围内不应有深度大于 30CM 的取土坑、冲刷坑和下陷坑，无严重坑洼及光缆裸露等现象，
其他	备纤	1、线路侧尾纤标记完好无损。2、备纤满足全程平均衰耗≤0.25dB/km（1550nm）且单处损耗台阶≤0.5 dB。
	外力施工	外力施工点现场管理应符合《河南电信线路标准化维

		护手册》中相关标准。
	图纸资料	一、二干“五图”齐全，图纸和实际相符。
	护线宣传	护线宣传应符合《河南电信线路标准化维护手册》中相关标准。

序号	周期	项目	内容及要求
1	天	巡检	查看平台系统、前端抓拍设备、干线巡检情况，抽查上传照片，发现问题及时通知巡检人员整改，并根据线路现场情况适当调整巡检人员配置、区域。
2	周	现场检查	至少对本辖区内所有干线光缆检查一次；对本辖区内所有外线外力施工点进行一次逐点检查，并汇总更新各外力施工点施工进展、线路影响情况、施工计划、后续看护工作布置。
3	月	维护业计划	主要内容包含：平台系统、前端抓拍设备、线路巡检、管道人井检查（含进局通道、进线室）、月度护线宣传（巡检过程中开展防盗、防火、防外力施工和人为破坏的宣传）、图纸资料完善。
4	月	分析总结	对上月维护质量进行总结分析，并组织召开月度干线维护质量分析会，主要内容：本月障碍、割接情况、巡检情况、线路检修整治、月度工作计划完成情况及后期重点工作安排。
5	季	纤芯测试	对光缆冗余纤芯通道后向散射信号曲线检查、应急倒代系统纤芯测试，汇总分析测试情况，列入年度整治计划。
6	年	制定维护作业计划	主要内容包含：线路巡检、线路路面维护、杆路维护、护线宣传计划、年度纤芯整治计划等全年工作计划。

7	年	线路整治	主要整治内容：直埋线路路由整修、杆路检修、纤芯质量修复、路由探测、人孔检修、人孔抽水。
8	年	护线宣传	组织开展“5.17 世界电信日”干线宣传，并向省公司上报宣传总结。
9	年	资料更新	对线路图纸资料完成更新工作，主要对线路维护图、线序图、路由图、拓扑图、框架图进行审核修订。
10	年	年度总结与计划	总结全年平台系统、前端抓拍设备及网络运行情况、隐患整治情况、考核指标完成情况；制订下一年度重点工作计划、考核办法、培训计划等。

巡检的要求

巡检时应携带必要工具和材料：日记本、笔、锹或砍刀等。巡检工作要有巡检记录、发现问题及处理过程记录、巡线宣传工作记录等。遇到以下情况时应适当增加巡检次数：大雨过后易塌方山（沟坎）、河（水）沟；执行特殊（如通信保障）任务的线路。

直埋线路的巡检

发现线路边有划线测量、堆放管线及电杆等施工准备的迹象时，应详细了解施工规模、施工时间、施工方案、施工负责人及其联系电话等信息，对相关单位及人员做好护线宣传、进行线路路由交底，并立即汇报。

发现线路边有钻探、机械挖掘、推土或机械顶管、打桩、打洞、挖塘、打井爆破；近距离敷设管（杆）线、公路改造或扩建施工等危害线路安全的施工时，应立即制止，并向乙方维护负责人汇报。情况严重的，应中止巡检，负责“三盯”工作。

发现线路路由有塌方、滑坡、洪水冲刷等危害线路安全情况时，应立即处理和汇报。

管道沿线的巡检

维护人员沿管道路由进行定期检查,查看自来水部门、燃气公司、电力公司、热力公司、市政建设局、电业局、园林局、铁路及其他单位等在管道附近施工或零星作业,危及或可能危及管道安全,应及时与该现场负责人取得联系,研究防护办法和注意事项。

在巡检过程中如发现有单位在人(手)孔上覆或堆放大量物资,应立即洽商,请该单位及时迁移,以免一旦发生事故,影响线务人员进入该人(手)孔及时检修光缆。

在巡检过程中如园林部门未按规定间距或在管道上方栽花种树,应及时与该部门洽商请其

移植。

做好管道路由沿线的宣传工作，严禁在人（手）孔附近放火，严禁往人（手）孔中倾倒垃圾和其他废料。

交接分线设备的巡检

发现交接设备盖上出现破损、箱体锈蚀、破损，门体变形，门锁失效等情况，应及时进行临时处理，避免设备损毁并及时联系维护班组维修。

发现分线（纤）设备箱盖（门）未关闭，要及时关闭箱盖（门）。

发现分线设备壳体松动、脱落、锈蚀等现象，要临时进行固定和密封，避免坠物伤人或设备进水发生故障。

5.7.1.7.2. 线路检修

确保线路的附属设施、标石、宣传牌无丢失，无严重损坏。标识、标牌的字迹清晰、号码正确 、整洁美观。

管道线路的维护工作

定期检查人孔内的托架、托板是否完好，标志是否清晰醒目，光缆的外护层及接头盒有无腐蚀、损坏或变形等异常情况，发现问题及时处理。

定期检查人孔内的走线排列是否整齐、预留光缆和接头盒固定是否可靠。

发现管道或人孔沉陷、破损及井盖丢失等情况，及时采取措施进行修复。

清除人孔内缆上的污垢，配合管道维护人员抽取人孔内的积水。

直埋线路的维护工作

检查线路标识、宣传牌是否有损坏、移位现象，字迹是否清晰，发现缺损及时更换或重新涂刷。

检查线路路面是否存在塌陷、积水等影响线路安全的隐患，及时回填或排除积水。

检查护坡、护坎是否存在滑坡、垮塌、开裂现象，缆线有无外露现象，遇到险情及时进行临时防护，并及时向上级反映，采取措施，排除险情。

交接分线设备的维护工作

检查箱体基础是否破损、下沉，壳体有无锈蚀，门锁是否有效，接地线是否牢固，箱体内

是否有露水，进线孔洞封堵是否严密。

检查分线设备固定是否牢靠、壳体是否有锈蚀、门（盖）是否关闭、尾缆是否有脱落现象，发现异常情况要及时处理。

5.7.1.7.3. 障碍抢修

接到障碍通知后，乙方抢修人员应在半个小时内集合人员，携带工具仪表、联络工具迅速出发。到达故障地点时限一般应控制在 10 分钟以内，整体抢修时限不超过 4 小时。

障碍抢修应遵循 “先干线，后支线，先抢通、后修复”的原则，不分白天黑夜、不分天气好坏、不分维护界限，用最快的方法临时抢通高比特率的传输系统，然后再尽快修复，障碍排除之前，查修不得中止。

建立完善的抢修组织，制定切实可行的抢修调度预案。仪表、机具保持性能良好，材料、资料齐全。

干线光缆抢修所需材料必须使用由甲方提供的专用材料，不得与其他光缆维护材料混用。

障碍抢修过程中，必须有专人在近端机房监控光纤熔接衰耗，熔接衰耗≤0.2dB。

障碍排除并经网管监控部门严格测试纤芯衰耗质量，确认无误后，抢修人员方可离开现场。

障碍排除后，维护单位应按规定时间填写《障碍登记表》上报甲方各市分公司主管部门，并对障碍原因进行分析，整理技术资料，总结经验教训，提出改进措施。一周内向甲方省公司提交书面报告。

如故障发生在引接点之内（引接点到甲方机房间）由乙方组织抢修。如障碍发生在引接点之外由甲方相关部门通知当地联通长线维护部门抢修，乙方按照甲方要求协助配合。抢修线路障碍时，乙方人员要听从甲方机务人员指挥，在线路障碍没有恢复之前，不得离开抢修现场。如与联通长线维护部门沟通不畅时，及时上报甲方解决。

5.7.1.7.4. 线路割接

割接前应整理割接所涉及的光电路资料、用户资料，并进行资源的核查与备份。甲方负责制定详细割接方案。

乙方要在割接工作开始前准备好割接所需材料、仪表、工具等相关物料。在割接过程中必

须严格按照割接方案中规定的割接步骤和操作执行。如果割接后业务不能恢复正常，并且不能在割接方案规定的时间内解决，应按割接方案启动恢复方案。

割接中要进行接续点监测，控制接续质量指标，避免割接产生大损耗及断纤。如发现漏割、错割现象要及时纠正。应检查新系统的工作情况，做到标识清楚，系统正常运转无隐患。

割接实施完成后，应在 24 小时内加强监控，密切注意网络运行情况，进行网络质量分析，比对割接（调整）前后系统、网络运行指标，确保割接后业务正常运行。

每次割接后 2 个工作日内汇报割接情况，并将线路割接完成表上传，进行回单。

5.7.1.7.5. 外力现场管理

光缆路由沿途出现外力施工隐患时，由乙方进行三盯作业。

干线光缆外力施工影响实行三级管理。一级：对线路安全有严重威胁必须立即处理。如光缆外露，路由滑坡、塌陷；光缆沿线 10 米范围内的开挖、回填土、顶管等施工；在光缆附近打桩、挖沙、炸鱼、放炮作业等。二级：对线路安全有较大威胁，如不及时处理，可能导致上升为一级外力隐患。如光缆沿线 10-20 米之间的开挖、回填土、顶管等施工；在三级：对线路安全有潜在威胁。如在光缆沿线 20-50 米之间的施工和堆放堆积腐蚀物品。

在确定外力影响等级后，必须于 24 小时内完成看护现场设置。

外力影响现场必须设置以下警示标志：在醒目位置张贴《关于保护通信线路安全的通告》；在光缆路由上方增加临时标石、插小红旗、立临时警示牌等，确保光缆路由醒目;采用打石灰线、拉警戒带、挂宣传横幅等方式设置警示范围，有条件的必须拉警戒带。临时标石和宣传牌的密度不低于 1 块/25 米（每处不低于 2 块），小红旗的密度不低于 1 面/2 米，现场必须采用两种以上的警示标志。外力影响现场的各类标志标记一旦丢失或缺损，要及时补齐。

一级外力影响点的施工现场，实施 7×24 小时轮班看护。要严格盯防区域内的重型机械施工，必要时做到“一机一人”。二级外力影响点施工时，必须确保现场有人值守、看护。三级外力影响点的施工现场原则上设置 1 名看护人员。

看护人员要向施工单位提供相关技术及宣传资料，包括光缆路由走向及埋深资料 1 份，看护人员与施工现场机械操作人员交换联系电话。

现场看护人员要按照“三盯四有”的要求（即：盯紧、盯死、盯到底，有协议、有标志、有专人、有检查），确保施工现场通信光缆的安全畅通。及时掌握施工进度及机械动向，一经

发现危及线路安全的施工，要主动与施工单位联系，想方设法予以制止，并立即向上级部门报告。

现场看护人员（三盯人员）要求

三盯人员熟悉线路路径、埋深，尤其是涉及大型机械作业的区域内线路基本情况。

三盯人员需了解掌握施工方案和实时变动情况，能准确及时掌握施工动向和进度，三盯人员需在当日施工开始前 20 分钟到达施工现场，当日施工结束并明确施工方次日施工计划后方可离开施工现场，并做好三盯日志记录。

三盯人员需加强现场的巡检。发现警戒线内动土应及时制止并上报，注重施工高峰、工程复工、收尾等时段的防护工作。

三盯人员除做好跟盯工作外，需做好相关防控设施的保护工作。

三盯人员应按要求坚守岗位、佩带明显标志，做好交接班和记录工作。

5.7.1.7.6. 线路安全作业

贯彻执行“安全第一，预防为主”的方针，加强线路施工和维护安全管理，规范作业人员的操作行为，确保人身安全和设施与设备安全。

维护单位必须为作业人员提供符合国家或行业标准的劳动防护用品、用具；作业人员在作业中必须按规定正确穿戴和使用。

维护作业的人员，必须经过安全知识教育和安全操作技能的专业培训与考核，成绩合格后持证上岗。

维护作业中所使用的各类工具、用具、设备及防护用品等在作业前必须进行检查。

维护作业前，必须对作业现场和周围环境进行必要的检查。

维护单位对安全重点地段应根据安全施工方案，经实地勘察后提出保障作业人员安全和预防事故的具体措施，施工作业前应逐级进行安全技术交底并签字。

5.7.2. 售后服务制度

服务制度由售后服务制度、售后服务组织、售后服务队伍以及运行维护对象组成，涉及制度、人、技术、对象四类因素。制度是规范运维管理工作的基本保障，也是流程建立的基础。

售后服务组织中的相关人员遵照制度要求和标准化的流程，采用先进的运维管理技术对各类运维对象进行规范化的运行管理和技术操作。

5.7.2.1. 建立运维体系架构

建立系统项目运维组织和管理机制，明确运维管理职责，建立沟通机制，制定应急处理预案，进行运维管理培训。

5.7.2.2. 制定运维管理规范

制定运维管理过程中各参与要素的行为准则和工作程序，提供制度化、规范化、高质量售后服务。例如：制定数据库管理、备份、恢复管理制度，系统管理制度、突发应急事件处理流程等。

5.7.2.3. 梳理运维管理流程

梳理运维管理流程，实现对网络设备、主机设备、存储设备，以及基础软件、应用软件等资源的综合管理和运行状态监控，支持售后服务流程标准化管理。

5.7.2.4. 形成运维技术管理

采购人运维的内容涉及到服务器、应用模块、用户信息等内容，如果仅靠人工来运维监控，将不能满足安全稳定运行的要求，因此，系统运行监控技术需要应用到运维中，利用运行监控系统对信息系统运行环境、运行状况等进行实时监控和事后分析，不仅可以对系统出现异常情况进行及时报警，并辅助快速定位故障点，而且还可以根据监控日志提供的线索，来检查系统的健康状况，做到防患于未然。

5.7.2.5. 建立考核评价体系

建立完整的考核管理制度，制定详细的考核标准。细分考核指标，通过提取关键指标实现系统的自动考核，根据每月的考核信息和监控情况，形成有数据、有分析、有建议的报告，对于考核中出现的问题，抓紧落实和整改，促进系统的 应用，持续性提升售后服务水平，推动

执行与管理水平的提升。

5.7.2.6. 服务流程

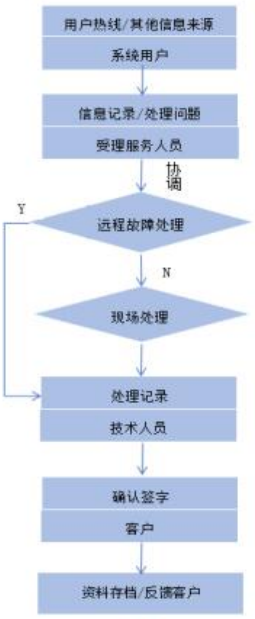


图 维护流程图

流程说明：

1、用户通过客服热线电话或其他渠道等沟通方式向售后服务团队咨询、反应与平台系统维护有关的相关信息。

2、受理技术人员受理，明确用户需求，并认真记录。

3、受理技术人员请示相关领导，并协调技术人员先进性远程受理排除故障，若远程受理无法排除故障，则联系工程师进行现场受理，排除故障。

4、处理完成后，对所排除的故障、解决方案等内容进行记录，以便在之后更好的排除故障，及时处理。

5、故障处理工程师将故障处理结果反馈给用户。

6、我公司手里技术人员将相关资料进行归档。

5.7.3. 故障响应计划

省公司网管中心负责全省通信设备故障处理的指挥、协调、协助与督促工作。地市级本地故障 市公司网管中心负责全市通信设备故障处理的指挥、协调、协助与督促工作。

省网络运营部下设的网络监控与维护中心（NOC）负责全省通网络运行情况的管控，及时发现告警并协调、督促故障归属分公司处理，提高维护效率，缩短故障历时；响应集团的故障调度，负责对跨区域故障的协调处理和管控；负责定期提交故障处理各项考核指标的完成情况；负责 7＊24 小时统一受理前端部门转派的公众客户、政企客户的业务申告。

市网络监控与维护中心（NOC）负责全市通信网络运行情况的管控，及时发现告警并协调、督促故障归属县区公司处理，提高维护效率，缩短故障历时；响应省公司的故障调度，负责对本地区故障的协调处理和管控；负责定期提交故障处理各项考核指标的完成情况；负责 7＊24 小时统一受理前端部门转派的公众客户、政企客户的业务申告。

网络监控与维护中心（NOC）各专业班组负责在规定的时间内派发、接收各类故障工单，协调、协助诊断并修复相关的网络故障；负责故障处理过程中根据不同故障等级以不同时间间隔（最长不超过 1 个小时报告一次）向市公司相关领导及专业负责人以短信形式广播报告故障处理进度，对于重特大故障至少 30 分钟报告一次处理进度情况。

网管监控与维护中心（NOC）对严重、重大故障负责在故障处理完毕后及时组织相关维护单位及专业负责人等相关人员整理故障分析报告，按要求上报相关部门与领导。

市分公司网络维护部门负责在规定的时间内接收、派发各类故障工单，诊断、修复相关通信设备（包括用户端）故障（包括线路故障），在修复故障后及时回复故障工单；根据不同故障等级，在故障处理中按不同时间间隔（最长不超过 1 个小时报告一次）向省网络监控与维护中心报告故障处理进度。遇有重大故障，至少每 30 分钟向网络监控与维护中心报告一次故障处理进度，并在处理完毕后负责提交处理报告；负责故障处理后对涉及的相关资源进行及时更新；负责根据与客户签订的 SLA 协议要求，向大客户提供差异化的故障处理等级服务；负责制订本地通信网应急调度方案，并将应急演练纳入日常维护工作。

故障处理流程起点由省网络监控与维护中心或地市网络监控与维护中心受理前端及后端维护部门申告开始，经过测试、预处理、派修、修障、测试恢复确认等环节后回复前端确认销障（有必要时在测试恢复确认过程中直接与用户确认）止。同时对前端的受理归口及派修流程作出规范。

10000+9 客服热线及 0393-8990012 是客户 7*24 小时保障热线电话。网管监控与维护中心是一点受理部门，负责受理公众客户、政企客户的各种需求及业务申告。负责客户申告的受理，根据申告类型向各专业负责人或相应的地市分公司派发工单，负责在接到维护部门故障修复回单后，向用户回复。

客户保障后要在 10 分钟内积极响应并做相应转派与督促，根据客户等级按照集团相关规定的修复时限要求，修复故障恢复业务。

网络监控与维护中心（NOC）各专业班组负责在规定的时间内派发、接收各类故障工单，协调、协助诊断并修复相关的网络故障；负责故障处理过程中根据不同故障等级以不同时间间隔（最长不超过 1 个小时报告一次）向市公司相关领导及专业负责人以短信形式广播报告故障处理进度，对于重特大故障至少 30 分钟报告一次处理进度情况。

网管监控与维护中心（NOC）对严重、重大故障负责在故障处理完毕后及时组织相关维护单位及专业负责人等相关人员整理故障分析报告，按要求上报相关部门与领导。

业务名称（电路维护等级）	电路维护等级简称	网络等级	网络质量要求	故障修复时限
SLA 质量保证承诺服务 AAA 级（优质标准）	AAA 级	A	端到端电路可用率不低于 99.999%。同一障碍重复率小于 1 次/3 个月。	60 分钟
SLA 质量保证承诺服务 AA 级（优质标准）	AA 级	B	到端电路可用率不低于 99.95%。同一障碍重复率小于 1 次/2 个月。	90 分钟
SLA 质量保证承诺服务 A 级（优质标准）	A 级	C	到端电路可用率不低于 99.95%。同一障碍重复率小于 1 次/2 个月。	180 分钟
维护质量保证服务 I 级	I 级	C		240 分钟
维护质量保证服务 II 级	II 级	N		240 分钟
维护质量保证服务III级	III级	N		240 分钟

质量水平承诺服务	普通	无具体要求针对质量水平承诺服务的业务，由于各省向用户承诺的修复故障时限不同，因此各省在大客户售后服务管理系统派单时要注明承诺的修复时限，且承诺修复时限不应小于 240 分钟。
网络等级A、B、C、N则是由政企客户业务处理系统根据电路维护等级自动匹配。省内跨地市政企客户电路按电路维护等级 N 级进行管理。市内本地重要政企客户电路等级按照 N 级进行管理。		

5.7.4. 应急保障措施

我公司已经针对本项目制定了详尽的设计、应急处理预案，整个流程严谨而有序。但是，在服务维护过程中，意外情况将难以完全避免。下面，我们将对项目实施的突发风险进行详细分析，并且针对各类突发事件，设计了相应的预防与解决措施，同时提供了完整的应急处理流程。

5.7.4.1. 预防措施

针对上门服务过程中可能遇到的各种各样的风险，我公司总结多年维护服务 经验，针对一些可能出现的情况，制定了一系列预防处理措施，举例如下：

类型	事件	预防措施	处理
应用软件	无法启动软件可执行文件	上门人员提前准备好各类需维护软件安装程序	将应用软件数据文件备份后，重新安装
	软件打开过程中或运行中异常错误关闭	上门人员准备好安装程序，操作系统优化和修补软件，查杀病毒软件	判断出错原因，备份数据，采取相关修复措施
网络设备	B/S 结构系统网络流量异常或服务器登	判断服务器是否异常，否则准备杀毒软件	检查网络流量，流量异常小则报修网络服务商，流量异常大则查

	录异常		杀病毒

5.7.4.2. 突发事件应急策略

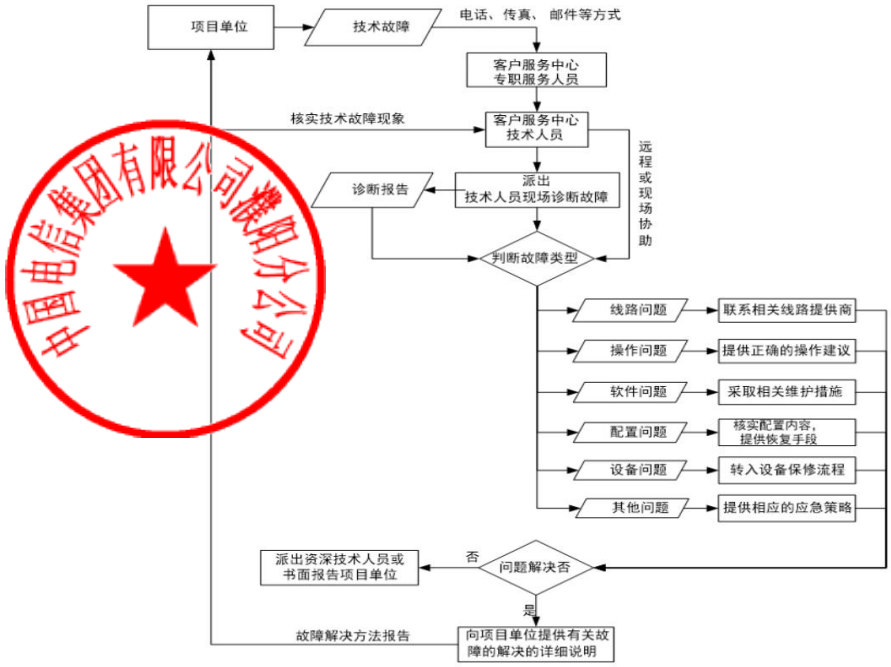
系统运维应急方案是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，我公司设计了完善的突发事件应急策略。

系统巡检人员要定期规范检查各系统的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

对发现的问题在报负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

我公司不但拥有经验丰富的技术支持工程师，而且根据长期以来的客户服务工作经验，建立了常用知识库，其中包括多种常见技术故障和突发事件的应急策略。当获悉出现突发事件时，技术支持人员可以立即从知识库中获取相应的应急策略，并综合用户方的具体情况，给出相关解决方案，然后在第一时间以电话、邮件支持或现场服务的方式帮助用户解决问题，尽最大努力减小突发事件对用户日常应用的影响。

我公司应急事件处理流程：



应急事件处理流程

我公司紧急事件应急响应策略清单：

紧急情况	预防措施	应急策略
硬件损坏	项目单位操作用电脑硬件损坏	在磁盘数据未丢失情况下，保证数据安全性，建议项目单位替换相关硬件。
操作失误	加强培训力度，掌握培训效果，检验操作人员操作水准，提示注意事项。	操作失误未造成即成结果或数据未丢失情况下，保障数据安全，反之，协调相关部门，进行补救。对操作人员强调注意事项
配置丢失	培训时强调使用前配置方法和步骤，并特别提示需在使用前按要求操作	派出上门维护、培训人员重新配置，并耐心讲解。
数据丢失	培训时强调使用过程中注意定期备份重要数据，日常维护过程中，上门服务人员实时备份数据并告知用户	协调有关部门，进行补救，无法补救，提交报告说明原因。

5.7.4.3. 应急响应等级

我公司针对用户系统不同的问题和故障服务请求，提供多种服务响应。

1、应急响应一级、二级故障，系统出现影响客户的业务使用。得到用户通知后，工程师

在第一时间响应；同时上报公司负责售后技术维护服务的副总经理，调度相关技术力量进行配合。

2、重要故障响应三级、四级故障。得到用户通知后，我们将通过电话、邮件、远程访问等方式进行诊断、指导，为您的运维工程师解决响应的故障。

3、一般故障响应五级故障，用户提出安装、配置、产品、技术等方面的信息咨询，或因政策变更而进行系统调整等业务要求。得到用户通知后，通过电话、邮件等方式进行支持。对于已经发生的故障建立评定标准，对故障进行动态评定，充分响应用户的反馈信息，保障运维服务效果。

评定项	降级标准	升级标准
响应时间	第一时间响应，包括故障的通知，处理，善后等事宜	相关人员一再催促下，责任人仍没有及时对故障进行处理
准备度	对故障发生的原因已有充分的预防机制	对已有发生的问题，或低级错误没有进行预防或规避
处理态度与能力	在最快时间内处理故障，并积极配合其他相关人员的故障处理工作；遇到技术问题积极寻求解决办法和资源支持；	对故障不重视，态度怠慢，敷衍；或没有足够技能进行故障处理
处理结果	系统在最短时间内完全恢复正常运作，故障影响降到最低	故障没有完全解决；或由于处理过程不及时不妥善导致故障影响（范围，金额，投诉量，恶性舆论等）有所扩大
后续措施	对故障发生的原因进行总结，制定同类故障的预防规避措施	拒绝对故障原因（除不可抗力因素以外）进行总结和制定预防/规避

		措施

5.7.4.4. 应急保障预警

我公司已经针对本项目制定了详尽的设计、应急处理预案，整个流程严谨而有序。但是，在服务维护过程中，意外情况难以完全避免。

发现信息安全突发事件的工作人员，应当对异常情况进行调查核实、保存相关证据，并向领导小组报告。领导小组接到异常情况报告，应立即组织力量排查摸底、专题研究、提出方案、及时解决。

积极推行信息安全和抗灾害登记保护，逐步实行信息安全风险评估。对基础业务信息建立应急备份与灾难恢复，并进行制度化管理。

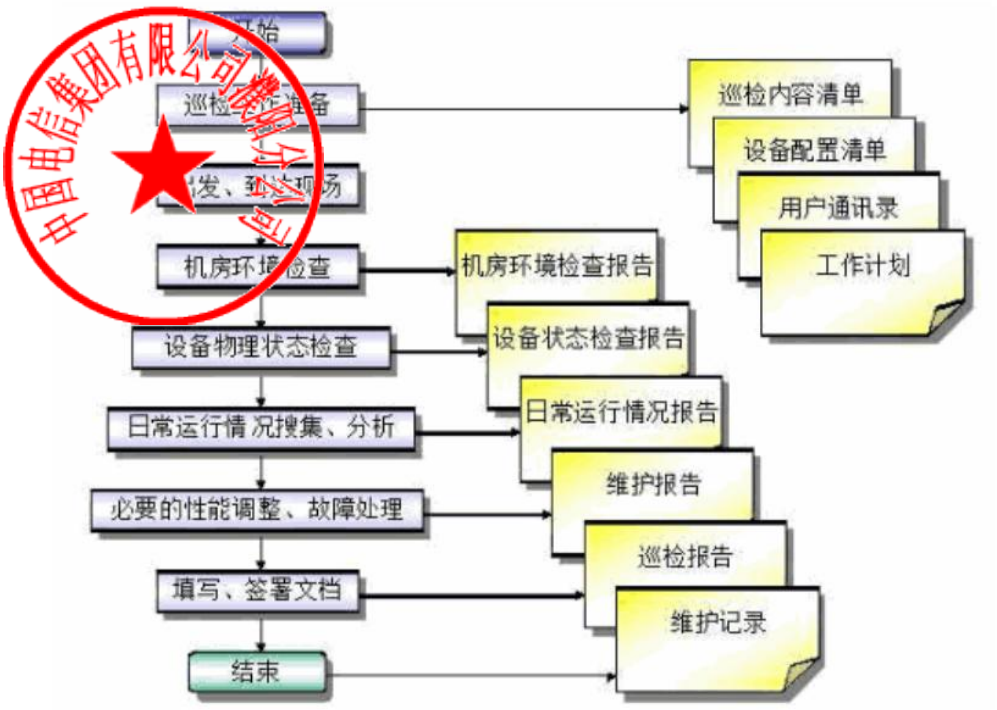
5.7.4.5. 应急保障机制

系统运维应急方案是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，我公司设计了完善的突发事件应急策略。

系统巡检人员要定期规范检查各系统的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

我公司不但拥有经验丰富的技术支持工程师，而且根据长期以来的客户服务工作经验，建立了常用知识库，其中包括多种常见技术故障和突发事件的应急策略。当获悉出现突发事件时，技术支持人员可以立即从知识库中获取相应的应急策略，并综合建设方的具体情况，给出相关解决方案，然后在第一时间以电话、邮件支持或现场服务的方式帮助建设方解决问题，尽最大努力减小突发事件对建设方日常应用的影响。

5.7.4.6. 巡检规范



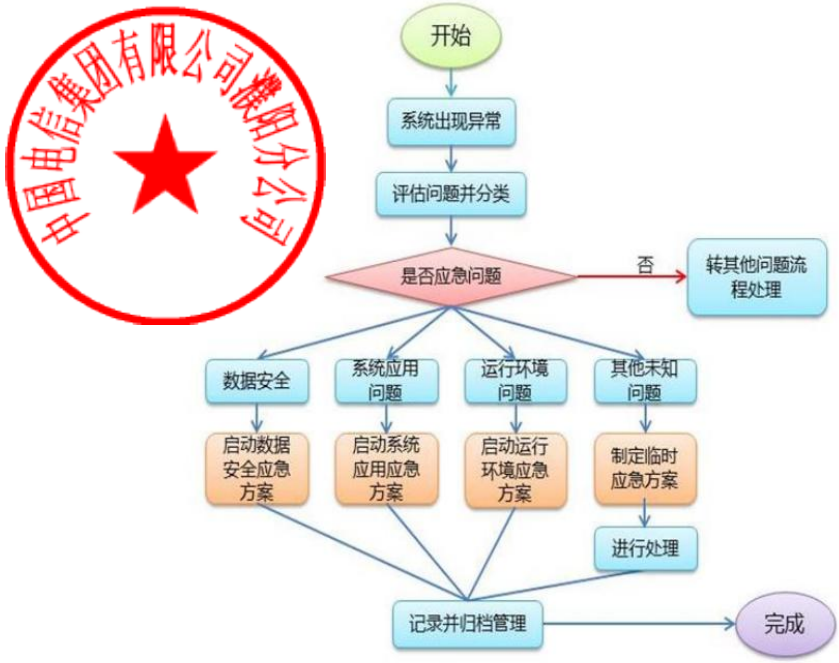
巡检工作流程图

5.7.4.7. 巡检方式

1、电话远程巡检：选择每月业务相对空闲期，每月两次的远程电话巡检，电话巡检通过最终用户授权后，用专用工具远程巡检。

2、现场巡检：在质保期内，根据客户要求提供现场巡检服务，现场巡检需经最终用户签字盖章认可。

5.7.4.8. 应急响应流程



应急响应流程示意图

1、系统出现异常当各业务系统的使用人员或维护人员发现系统在使用中出现问题和隐患时，应第一时间通知采购方负责人以及项目经理，有必要时可以以书面形式汇报。

2、评估问题和划分项目维护人员及时并快速分析系统出现问题的原因，并将问题进行大体的分类，判断是否启动应急处理流程方案和启动那一类应急处理方案和流程。

3、数据安全应急 如果经过分析确定出现的故障是数据安全问题引起，对问题进行具体的定位，执行数据安全应急处理方案，并对故障发生问题进一步描述，问题已经处理，并对处理过程进行详细记录。

4、系统应用应急如果经过分析确定出现的故障是系统应用问题，对问题进行具体的定位，执行系统应用应急处理方案，并对故障发生问题进一步描述，问题已经处理，并对处理过程进行详细记录。

5、运行环境应急如果经过分析确定出现的故障是由于运行环境问题，对问题进行具体的

定位，立即执行运行环境应急处理方案，并对故障发生问题进一步描述，问题已经处理，并对处理过程进行详细记录。

6、其他情况问题：当系统出现意外的紧急问题时，即本应急方案未制定该问题的事先应急方案时，项目维护人员应对本问题划分为“其他未知问题”，并上报相关采购方负责人以及项目经理。由项目经理牵头组织人员，针对出现的意外问题制定相应的应急方案，并执行意外问题应急方案，并对故障发生问题进一步描述，问题已经处理，并对处理过程进行详细记录。

7、处理结果记录归档管理维护人员对故障问题出现到问题处理整个的记录进行归集，对处理结果进行记录并归档管理。

8、事件报警与确认维护人员对数据库服务器、应用系统的运行状况以及网络情况进行监测，及时发现系统的异常和网络故障，一旦发现异常情况需及时通知相关人员进行原因的排查和故障的处理。

9、对系统进行检查

1）检查网络连接：需要相关网络管理人员配合检查；

2）检查应用服务器性能指标，检查的内容包括：web 中间件进程是否正常、CPU 使用率、内存使用率；

3）检查后台数据库服务器性能指标，检查内容包括：数据库服务器双机状态、数据库进程是否正常、数据库服务是否启动、CPU 使用率、内存使用率。

10、安全审计及事故分析通过系统日志、网络设备日志、数据库访问日志等，对事件进行审计，对损失进行评估，追查事件的发生原因。

11、消除隐患、恢复正常运行根据审计结果，排除系统隐患，恢复系统正常运行。

12、安全报告、归档提供故障分析报告，分析故障原因，修正预案处理流程并归档。

5.7.4.9. 应急处理措施

5.7.4.9.1. 数据安全应急方案

（1）非法入侵情况描述：网络管理员或系统管理员发现有非法用户登录系统，登录系统后非法执行系统功能，并篡改系统数据时，视为紧急情况。

应对方案：

1）如果系统管理员处理此情况有困难，可要求应用软件实施商帮助处理；

2）如果能够根据系统的相关日志进行针对性恢复，则属上策；

3）否则，将系统恢复到最近的一个备份点；

4）注意：尽量不要整库恢复，一定要将损失降到最低，至少要能定位到数据表进行恢复；

5）注意：必须将系统数据恢复到应用系统认可的数据同步状态，即恢复后要进行相关的功能测试。

（2）数据崩溃恢复

情况描述：网络管理员或系统管理员发现网络数据及配置系统遭到严重破坏时，并且试图进行各种技术处理无法恢复时，视为本紧急情况。

应对方案：

如果系统管理员处理此情况有困难，可要求应用软件实施商帮助处理；重新安装和配置数据库服务器；将系统恢复到最近的一个备份点。

5.7.4.9.2. 系统应用应急方案

（1）非法入侵 情况描述：网络管理员或系统管理员发现有非法用户登录系统，或者登录系统后非法执行系统功能，视为本紧急情况。

应对方案：

网络管理员或系统管理员应及时保护操作系统、数据库系统、中间件系统和应用软件系统的相关日志；检查系统重要数据是否被非法篡改；及时邀请项目的应用软件实施商到现场，进行评估和处理；24 评估安全问题出现在那个环节，判断问题的严重行，决定是否需要咨询信息安全专家，并进行处理；评估应用软件实施商应该进行那些系统安全方面的改进；应制定一个临时应对措施。

（2）系统崩溃恢复

情况描述：

网络管理员或系统管理员发现应用系统遭到严重破坏时，并且试图进行各种技术处理无法恢复时，视为紧急情况。

应对方案：

如果系统管理员处理此情况有困难，可要求应用软件实施商帮助处理。重新安装中间件系统；重新配置安装中间件系统；安装和配置应用系统的中间层组建；对系统进行全面测试。

5.7.4.9.3. 运行环境应急方案

（1）网络紧急情况情况描述：网络系统，包括保障系统运行的信息专网的网络设备出现故障或可靠性严重下降时，视为紧急情况。

应对方案：

网络方面如下应急方案：

1）当客户端连接服务器时，经过长时间等待后，报服务连接失败的错误。此时有可能是网络不通。请安如下步骤操作：首先尝试 ping 本地局域网的其它计算机，如果没有响应，联系技术服务部门及时处理；如果能正常响应，则 ping 应用服务器，如果能通，则可能属于软件系统的故障，寻求软件技术工程师处理。如果不通，可能是网络故障。请联系网络管理员解决，并启用备用网络连接。

2）当客户端连接时，出现了数据库连接失败的提示时，则 ping 数据库服务器，如果不通，可能是数据库群集的网络出现故障，请联系网络系统管理员解决。如果能连通，可能是数据库故障，联系数据库管理员处理。

3）要考虑对网络设备的冗余，对网络设备进行备份，主要是对交换机、防火墙、路由器等设备采用备份策略，解决网络设备的单点故障，保证网络可靠的运行。

4）根据网络设备的售后服务协议，及时进行维修。

5）如果是线路故障，也要及时通知有关部门进行维修。

（2）机房环境紧急情况

情况描述：发生水害、火害等自然灾害。

应对方案：

报警措施：

1）关闭机房外的供电总闸；

2）启用灭火设备进行灭火，并打火警电话 119；

3）在 UPS 的支持时间内，关闭相关服务器；

4）全力保护重要的数据备份，并转移到安全地点；

5）完全熄掉各种明火；

6）尽量保护好火灾现场，协助有关方面勘察分析火灾发生的原因、造成的损失、提出批评防范措施和需要改进的地方；

7）对发生火灾造成的损失、原因等做好记录，经部门负责人、联社领导审阅后，向上级主管部门全面汇报。

数据及设备撤离措施：

1）将数据备份磁带、操作系统、数据库系统等软件转移到安全地方，或者多做一些拷贝；

2）将服务器、阵列、集线器转移到安全地方；

3）将前置机及远程数据通讯器转移到安全地方；将有关外部设备转移到安全地方。

5.7.4.9.4. 病毒安全紧急处置措施

当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。

对该设备的硬盘进行数据备份。

启用反病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。

如发现反病毒软件无法清楚该病毒，应立即向安全小组负责人报告。

信息安全小组相关负责人员在接到通报后，应在十分钟内赶到现场。

经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即向信息安全领导小组副组长报，并迅速联系有关产品商研究解决。

安全领导小组经会商后，认为情况极为严重，应立即向公安部门或上级机关报告。

如果感染病毒的设备是服务器或者主机系统，经领导小组组长同意，应立即告知各下属单位做好相应的清查工作。

5.7.4.9.5. 数据库安全紧急处置措施

数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。

一旦数据库崩溃，应立即向网络安全员报告，同时通知各下属单位暂缓上传上报数据。

信息安全员应对主机系统进行维修，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。

系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

5.7.4.9.6. 局域网中断紧急处置措施

局域网中断后，网络管理员和网络安全员应立即判断故障节点，查明故障原因，并向网络安全领导小组副组长汇报。

如属线路故障，应重新安装线路。

如属防火墙、交换机等网络设备故障，应立即与设备提供商联系更换设备，并调试畅通。

如属防火墙、交换机配置文件破坏，应迅速按照要求重新配置，并调试畅通。

如遇无法解决的技术问题，立即向上级单位或有关厂商请求支援。

如有必要，应向安全领导小组组长汇报。

5.7.4.9.7. 设备安全紧急处置措施

服务器、磁盘阵列等关键设备损坏后，有关人员应立即向网络管理员和网络安全员汇报。网络管理员和网络安全员应立即查明原因。

如果能够自行恢复，应立即用备件替换受损部件。

如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。

如果设备一时不能修复，应向安全领导小组领导汇报，并告知各下属单位，暂缓上传上报数据。

5.7.4.9.8. 机房发生火灾紧急处置措施

应遵照下列原则：首先保人员安全；其次保关键设备、数据安全；三是保一般设备安全。

人员疏散的程序是：机房值班人员立即按响火警警报，并通过 119 电话向公 安消防请求支援，所有人员戴上防毒面具，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出。

人员灭火的程序是：首先切断所有电源，启动自动喷淋系统，灭火值班人员戴好防毒面具，从指定位置取出泡沫灭火器进行灭火。

5.7.4.9.9. 外电中断后的设备

外电中断后，机房值班人员应立即切换到备用电源。

机房值班人员应立即查明原因，并向值班领导汇报。

如因机关内部线路故障，请机关服务部门迅速恢复。

如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

如果供电局告知需长时间停电，应做如下安排：

预计停电 1 小时以内，由 UPS 供电。预计停电 2 小时，关掉非关键设备，确保各主机、防火墙、交换机供电。

预计停电超过 2 小时，应联系小型发电机自行发电。

5.7.4.9.10. 关键人员不在岗的紧急处置措施

对于关键岗位平时应做好人员储备，确保一项工作有两人能操作。

一旦发生关键人员不在岗的情况，首先应向值班领导汇报情况。经值班领导批准后，由备用人员上岗操作。

如果备用人员无法上岗，请求上级单位支援。上级单位在接到请求后，应立即派遣人员进行支援。