数据中心容灾和灾备实用指南

第 5 号白皮书

版本 0

> 摘要

对于需要维持系统 24/7/365 全天候运行的机构来说，容灾和灾备计划是必不可少的。管理层必须设定 100% 可用性的目标，认真评估支持关键任务设施的物理基础设施并降低其风险。业务连续性计划通常针对信息技术（IT），本文则主要关注和探讨基础设施要求，作为广义上业务连续性容灾和灾备计划的一部分。如果没有为基础设施制订适合的容灾和灾备计划，那么整个业务连续性计划就建立在一个充满风险的基础平台之上。如果设施遭遇自然灾害、人为或技术失误，基础设施是否做好万全的准备？企业是否已制订了应对暴风雪、地震、雷雨、飓风或其它灾难的准备？要想安然度过未来灾难，就必须未雨绸缪，立即计划。

目录

点击内容即可跳转至具体章节

施耐德电气旗下 APC 的白皮书现收录于施耐德电气白皮书资料库
由施耐德电气**数据中心科研中心**发表，
DCSC@Schneider-Electric.com

Schneider Electric

简介

资源链接
第 7 号白皮书
优化关键任务设施和数据中心的正常运行时间

什么是灾难？

灾难是无法预测的，可能会对人员、财产、信息或环境造成伤害的意外事件。灾难的形式包括紧急事件或意外事故：火灾、洪水、雷雨或恐怖活动、飓风、危险物质泄露或人为错误、地震、设备故障、断电、暴风雪等。在很多情况下，这些原本可以避免的小问题如果累积起来，会造成大灾难。请参见第 7 号白皮书《优化关键任务设施和数据中心的正常运行时间》。

故障

灾难在一开始的表现形式可能是各种类型的故障。为了有效应对和计划，首先需要了解有可能发生的故障类型，这非常重要。关键任务设施中的设备宕机可以归因于四种主要故障类型：

- 设计缺陷引发的故障
- 灾难引发的故障
- 复合并发故障
- 人为失误故障

每种类型的故障都需要不同的预防方法。如果能从根源上解决潜在故障问题，就有可能避免大规模灾难的发生。

设计缺陷引发的故障
为防止设计缺陷引发的故障，应从制订全面的概念设计开始。选择在特定应用方面有丰富经验的设计公司，积极参与设计流程。让组件供应商集思广益，反复审查设计方案。从一开始就要思维清晰、目的明确。

灾难引发的故障
制订一个全面的维护计划并采用预测分析方法可以有助于防止灾难引发的故障。评估发生故障的可能性、故障结果，并检查防御故障的步骤。此外，实施正式的“总结经验教训”计划，来防止故障再次发生。

人为失误故障
使用详细的规程实施办法(MOP)。在开关操作过程中运用双保险的方法，在正式部署前验证 MOP 的正确性。全面培训内部人员和供货商对降低人为错误风险非常重要。

容灾和灾备计划

做好最充分的规划与准备，意味着采取所有可行措施来预防、准备、响应、减轻危机并从危机中恢复。准备分为四个重要方面：

1. 准备和预防：旨在预防危机、降低发生危机的可能性或减轻危机造成的破坏性影响的所有行动。
2. 发现事故并分类：旨在发现、评估危机并根据危机的严重度进行分类的所有行动。
3. 响应和缓解：旨在拯救生命、防止进一步伤害发生并缩小危机影响的所有行动。
4. 恢复正常：旨在发生危机后恢复到正常甚或更安全状态的所有活动。

信息

在发生危机期间，能否访问重要信息很关键。这些信息应该持续备份并存储在多个地点。许多公司在世贸中心坍塌后完全丢失了资产，包括其恢复计划。有很多公司因为失去重要信息而无法继续经营下去。

紧急事件联系人列表
在发生紧急事件时应联系的员工和供货商列表应不断更新，且保证在发生灾难时随时都能访问。

设施门禁准入列表
确保设施门禁准入列表处于最新状态。在发生紧急事件时，员工将需要通过门禁系统进入备份站点，但却不被允许。被拒绝进入或延迟进入会损失宝贵的恢复时间。

检验恢复能力

随着数据和应用的迅速增长，确保容灾和灾备站点拥有足够的资源来存储数据。一般来说，人们常常将关注的焦点集中在保证主站点采用最新技术上，经常忽略备份站点，导致备份站点仍使用过时技术。

切勿低估恢复时长

几乎没有规划人员能够准确预测大规模灾难中的时间延误，如确保生命安全阶段、损失评估阶段以及到达热备份站点、建立远程运营等所需的时间。

应对压力

大规模灾难可能会使机构瘫痪。在巨大压力下仍能运作的关键是做好充分的准备并不断练习。发生灾难时，员工需要先和家人取得联系，之后才能全身心投入恢复计划。还需关注并评估应急人员在换班前能连续工作多少小时，以及确定伤者状态需要多长时间等因素。目前的大多数计划都未能从现实角度出发，来准确估计从灾难中恢复所需的时间。

了解撤离疏散的问题

大规模撤离疏散引起的复杂局面也经常被错误估计。容灾和灾备计划应评估与撤离疏散相关的问题，如灾难发生后设施内人员应在多长时间内完成撤离疏散，以及主要和备用撤离疏散路线等。此外，还应指定一个备份紧急事件指挥中心(EOC)，它应距离主要办公地点有一段合理的距离。

消除通信瓶颈

因为“单故障点”问题，多种通信都会出现故障。许多公司的计划是以公共网络保持正常运行为前提的。但不幸的是，在大型灾难中，公共网络也可能瘫痪。机构需要安排备用通信方式。

了解保险责任范围

了解保险责任范围。确保有足够的保险，能够为继续业务运营而提供必要资源。

评估状况

正如在个人医疗方面，定期进行体检可以尽早发现疾病，能有效预防重症发生。同样，这一做法也适用于灾难防御，当代表建筑物业主或保险公司对建筑物或设施进行物理风险评估，也有助于预防灾难性损失。

危险评估

危险评估流程旨在确定危险区域。这其中，危险包括森林大火、泥石流、雷雨、飓风和洪水，以及附近的铁路、天然气管道等。危险评估会估计发生危险的可能性和严重性，以及当前的防御措施。危险评估还应确定危险可能发生的地点和地区范围、某一事件可能会发生的次数以及发生的概率。

易损性评估

易损性评估流程旨在估计灾难有可能造成的损害。一次彻底全面的易损性评估应该评估处于风险中的人数、处于风险中的资产价值、处于风险中的重要系统的数目和功能，以及发生的次生危险等重要问题

风险评估

风险评估旨在综合衡量危险事件发生的可能性和可能造成的危害程度。这其中也应将间接或次生危险考虑在内。

容灾和灾备评估

容灾和灾备评估包括备份资源的充足性、设备更换优先次序、供货商列表、紧急事件响应规划、恢复计划演习和其它能增强容灾和灾备的流程。

消防评估

最常见的灾难起因就是火灾。建筑物消防规范旨在确保建筑物能为住户提供安全消防措施，并提供安全撤离疏散路线。但是，仅遵从消防规范是远远不够的。各种规范是最低标准，根据风险和易遭受危险的程度，还应采取其它措施。消防评估是“消防注意事项”的重要组成部分，重点关注消防系统（如火灾探测器的间隔和正确使用等）、危险品（如纸张和易燃物等）、撤离疏散流程、灭火措施以及消防队相关信息（如响应时间、门禁和对设施的熟悉程度等）。

安保和告警评估

安保和告警评估旨在评估安全政策和设备告警是否足够、设施是否方便进入、安保措施破坏率、告警中心路线以及告警响应流程问题

环境评估

环境评估旨在评估土壤和大气污染、空气过滤、环境对设备的影响、住户舒适程度和设施整体清洁度，以及室外空气来源和通风率、HVAC（暖通空调）等支持系统的易损性。

电力评估

确定是否具有足够的备份电力系统、浪涌抑制、主电源可靠性、配电路径、连接器系统和其它许多供电可靠性因素

测试灾难恢复计划

一旦计划制订完成，就必须进行严格的测试。测试流程本身也必须正确规划，应在能够模拟真实情况的环境中，由在发生紧急事件时实际负责采取这些行动的人员执行。测试容灾和灾备计划、告警和流程、执行建筑物检测并查看建筑物问题报告，有助于有效衡量。无论选择哪些衡量措施，关键是管理层能够实际地评估衡量结果。在现实中，有忽略不良结果，从同情心出发对已付出的努力给予过高评价的倾向。但是，现在正是采取纠正行动的时候。现在的每一步都能在将来节约时间、金钱并挽救生命。例如，为预消防灾，需要定期对设施中的所有电气设备进行检查。如果管理层决定不按规定，将实际检查次数减少到每年一次，将会发生什么情况？建筑物问题评估报告能够揭示，过去三个月中有两个设备曾发生轻微火灾。如果每年只评估一次，那么就可能太晚了，问题已“积少成多”。一旦计划已通过测试并更新，测试流程和结果都应记录下来。所有需要参与计划实施的人员都必须不断接受正规培训。

灾难缓解

灾难缓解是紧急事件管理的基石。它旨在采取长期措施，减轻灾难对于人员和房产的影响。例如，灾难缓解措施包括保持住宅选择远离洪泛平原的地区、设计能够抗地震的桥梁，以及创建并实施有效的建筑物规范，来保护建筑物不会受到飓风影响。灾难缓解措施被定义为“能够减少或消除人员和房产遭受自然灾害的长期风险及影响的可持续措施”。它包括联邦、州、地方和个人等各个层次、旨在减轻灾难对家庭、住宅、社区及经济的影响的长期措施。

更新容灾和灾备计划

获得反馈信息，在测试后精确调整计划是非常重要的。它是一个动态文件，必须随时更新，适用于当前业务环境。应指派专人负责保证该计划定期维护与更新。此计划如有改动或增补，都必须进行全面测试。相关人员也应随时了解这些改动对其职责有何影响。

成功恢复计划的九个要素

制订计划的理由

列出机构制订容灾和灾备计划的理由。部分常见理由包括：保护人身安全；恢复关键运营；保护竞争地位；保持客户信任与好评；以及避免法律诉讼。

识别

人员必须通过培训，能够识别告警信号。如果在清晨三点有水从门缝流入设备室，将会发生什么？保安、清扫人员和其它合同工是否知道应致电谁、如何报告所遇到的麻烦？以下问题应该在识别阶段得到解决：执行初始应对流程；报告灾难的发生；通知警察、消防部门和医护人员；以及通知管理层。

应对

听到告警后应采取什么措施？谁来负责安保？谁负责向媒体发言？如何区分授权紧急救援人员和入侵者及借机浑水摸鱼者？通过仔细规划来解决这些问题。动员行政管理团队(EMT)；向 EMT 提交初始损失评估报告；帮助 EMT 准备对外声明；进行关键事件记录，以便审计等，这些仅是应对阶段应采取的大量措施中的一小部分。

响应

对灾难的响应举措将很大程度上决定着企业运营受灾难的影响程度。如果已部署恰当的通知系统，将加速恢复过程。建立一个专门的紧急事件指挥中心(EOC)或“指挥室”，有助于集中精力开展恢复工作，而不是忙着寻找和安排所需资源。在执行损失评估时，保护人员和设备资源是十分重要的。安全应是首要考虑因素。

恢复

确立恢复阶段的运营流程。所涉及的问题包括更改购置设备的签字权、获取现金的流程、保持物理安全的流程、在受破坏站点和恢复中心安排安保的流程，以及找到并抵达恢复中心的流程等。

重建

重建流程包括协调原办公地点的重建和电子设备的复位；重装软件；重新部署供电、UPS 和普通建筑物系统；更换灭火系统；建筑物重布线；恢复局域网；以及恢复广域网连接等。

回归正常

在此阶段，建立测试流程，来测试将要部署的新硬件和软件；培训或再次培训运营人员和其他员工；计划并安排实施系统迁移回原工作地点。

休息和放松

确保安排补偿式休假时间，使员工充分休息，能够身心愉悦地迎接未来。确保安排计划，去看望正在接受治疗的员工。

再评估和再记录

安然度过一次灾难之后，应该对恢复措施进行分析，减少未来风险，提高未来恢复能力。浏览重要事件记录，评估供货商表现，表彰表现突出的人员，准备最终评估报告，并帮助评估讼诉责任。

数据中心设计元素

从一开始就要思维清晰、目的明确。现实情况是，设计意图要么模糊不清，要么涵盖不全。全面的设计意图，对于相关各方能够在关键任务设施中实现最长正常运行时间非常重要。并没有一个理想的设施设计配置，而是根据不同的目的，每种设计类型都各有优缺点。与经验丰富的专家一起，精心设计功能、灵活性和经济性，来满足机构的目标。请参见第 145 号白皮书《数据中心规划中的九大错误》。

资源链接
第 145 号白皮书
数据中心规划中的九大错误

设施选址

有很多因素影响着设施的地点。除了业务因素外，还需了解当地危险因素（洪泛区/洪泛平原、地役权和建筑物外墙阶梯式缩入等）会产生什么影响。当灾难降临，是否有可用的资源？确保公用事业能随着业务的发展，继续支持需求，且该地点有足够的空间和冗余性。如需了解有关设施选址的更多信息，请参见第 81 号白皮书《数据中心设施选址》。

资源链接
第 81 号白皮书
数据中心设施选址

建筑物外观设计

当地环境是影响建筑物外观设计的最重要因素之一。危险评估将详细说明所有当地危险因素。在设计建筑物外观时，采用针对这些危险的必要保护措施。危险因素可能包括森林大火、泥石流、雷雨、飓风、恐怖分子袭击、洪水，以及附近的铁路、天然气管道等。

例如，通过采用防火阻燃屋顶材料、适当的外墙阶梯式缩入并保证建筑物周围没有易燃植物等，来降低发生火灾的风险。应修剪树木和高灌木丛，以使它们不会妨碍到电线。保持其它重要系统（如发电机排气系统、冷却塔、变压器和冷凝器等）周围没有树木和灌木丛。如果处于地震带，应使设施做好抗震准备。

屋顶和墙壁的设计应该高度安全，能够防御附近的危险。应考虑地板和屋顶的承重能力，以便不仅能承受预期部署设备的重量，而且能支持未来的扩展。UPS 系统的电池重量有时较高，需要特殊的支撑结构或地板才能承载。数据中心应该位于设施的中心，不与外墙相邻。在恐怖袭击危险不断增加的情况下，防弹措施能确保正确保护设施。防弹措施包括控制建筑物门禁、在建筑中采用外墙大幅阶梯式缩入，为建筑物外墙和窗户选择特殊材料和特殊建筑方案。例如，现在玻璃越来越多地作为建筑材料，而且用量激增。通常来说，玻璃处于遭受冲击的第一线，而且经常在易损性评估中被忽视。运用安全膜，一种非常先进的聚酯和金属化涂层的层压膜，能够大幅减少因自然和人为灾难造成的损失和人身伤害。

设备选择

在为关键任务设施选择设备时，确保生产商提供的设备参数符合设计工程师提出的规格要求。此外，大多数设备都有一系列可用配件和选项。和设计工程师一起来确定这些选项的价值，以及在未来用到它们的可能性。

有时可能不需要一开始就具备某一选项，但随着发展，将来可能需要在现场添加此选项。由此造成的设备宕机和额外支出，可能远比在初始购买时就订购此选项要多得多。专业的系统集成商能为制订未来计划提供帮助，发现并避免设备缺陷，并最大程度地实现投资回报。

公用事业

现在就要为未来公用事业供应中断做好准备。电力常常是首要考虑的因素，而水、天然气、下水道服务或电信等公用事业的中断，也会对关键任务设施构成严重影响。需要考虑的公用事业举例如下：

电
电线埋线铺设有助于保证服务、保护重要连线，特别是发生大风和冰暴时，其作用更为明显。但是，如果发生地下施工和洪水泛滥，埋线面临的风险就加大了。选择由不同变电站进行冗余馈电提供了最高保护水平，但成本常常过高，完全抵消甚或超过了其带来的保护优势。

水
如果设施使用带冷却塔的冷水机，就需要持续供水，才能保证制冷系统正常运行。使用水冷冷水机相对于风冷冷水机的优缺点，以及保证可靠备份供水的能力，都需要认真评估。

下水系统
如果对下水系统有较高要求，评估一旦中断会对运营有何影响，以及在下水中断时提供备份的安排情况。

天然气
如果制冷系统、锅炉或发电机需要天然气，应安排冗余供气源，或安装使用其它燃料类型的冗余设备。

电信接入
在设计设施时，使用通过不同路由进入设施的冗余电信服务。

柴油发电机燃料
在发生大范围停电，如 2003 年 8 月东北部地区停电事件时，柴油发电机燃料供应量会很有限。确定所需的燃料量是一项很难的挑战。在普通情况下，只需提前几小时告知，即可获得燃料。但是在停电时，燃料供应商甚至无法从储备箱中抽出燃料。

另一方面，存储大量燃料也会产生问题，如环保限制、所存储燃料的“保质期”有限等。随着时间的推移，燃料开始分解，将会形成胶质和清漆，生长出某些藻类。燃料添加剂能延长可用存储期限。在发电机维护期间，让服务供应商对燃料进行分析是很重要的。过滤系统和妥善规划的燃料循环计划将有助于降低这些风险。

电气设计考虑因素

电力是关键任务设施运营的基本要素。通常认为，电力服务非常容易受到大量危险的威胁，中断经常发生。以下是一系列电力设计考虑因素，有助于降低断电带来的风险。

发电机
发电机在市电中断时提供备份电力。无论是简单的单一发电机和自动转换开关(ATS)，还是复杂的多机组发电厂，对发电机的支持和维护是设施生存的关键。在每周测试中启动一台无负载的应急发电机，能够确保发电机运行正常。但是，每周测试有可能会导致“积碳”现象。当发电机多次重复无负载或轻负载运行时，会发生这种现象。当要求发电机联网，为所有设备负载供电时，在无负载测试期间累积的沉淀物就使其无法在满负载情况下供电。因此，应在可能情况下，让发电机带负载测试，以便将沉淀物清除出系统。应定期安排执行 2-4 小时的满负载测试。请咨询发电机生产商或基础设施专家，听取他们对于带负载测试的频率和时长的建议。发电机在长时间运行时会消耗曲轴箱润滑油。了解发电机的曲轴箱润滑油消耗速度，在发电机因无曲轴箱润滑油骤停前及时补给。一些发电机需要安装润滑油系统，在运行时添加润滑油。请咨询发电机生产商或服务供应商，确定润滑油消耗速度。此外，大多数发电机都有冷却液过少告警并自动关停，以防发电机在冷却液较少时启动（关键任务设施中因发电机冷却液过少而停机的现象相当普遍，很令人惊讶）。定期维护是避免因小问题疏忽而导致大故障出现的关键。储备足够的冷却液和润滑油，储备量至少要足够设施持续运营一周。如可能，安装外部曲轴箱和冷却液储存器，以便无需终止发电机的运行，就能检查润滑油和冷却液的液位。电动机组加热器使电动机能快速启动联网。但一直加热的水和发电机振动会给水管和接头造成压力。在电动机组和加热器间安装独立阀门，就可随时更换水管和接头，而无需中断发电机运行。

自动转换开关
自动转换开关(ATS)用于在市电断电时自动提供紧急供电。ATS 能够检测到市电断电，启动发电机并使其联网。当市电恢复，大多数转换开关会比较谨慎，等待一段时间后，再自动切换回市电。这些转换开关的部件和连线也肯定会发生故障，因此持续维护很重要。尽可能缠绕包好馈电线，或使用独立回路，以便即使在 ATS 无法工作时，仍能保证为设施供电。

不间断电源
不间断电源(UPS)是关键任务设施中的重要设备。从插接个人电脑插座的小型 UPS，到为大型计算机中心供电的大型并联系统，所有 UPS 都有一个共同的组件——电池。UPS 电池寿命有限，必须定期测试。市场上有很多类型的 UPS 系统（双转换、磁饱和式或 delta 转换型）和多种配置（如单模块、并联模块、串联冗余、定位器系统、双系统冗余等）。每个系统和配置都有优缺点。和设计工程师、厂商及基础设施专家一起，确定最适合基础设施解决方案。有两种基本类型的 UPS 电池，即富液湿电池和排气式阀控铅酸电池（VRLA），它们各有优缺点。富液电池初始成本较高，但比 VRLA 可靠且寿命较长（富液电池的典型寿命为 15 到 20 年，而 VRLA 只能使用 3 到 5 年）。如果选择 VRLA，请让 UPS 厂商使用他们自己的直流断路器和机柜将电池配置为独立电池组。藉此，电池组与 UPS 系统隔离，在电池维护与更换期间，UPS 系统仍能保持在线。随着新技术的推出，UPS 系统和电池监控器性能更出色、价格更廉宜。电池是 UPS 系统的核心，电池监控器则有助于延长电池寿命，并提高电池组可靠性。同时，不要忽视设施中其它电池的维护。从发电机启动电池、可编程逻辑控制器(PLC)、监控和管理系统，到断路器和脱扣器，一块价值 2.00 美元的电池就可能使发电机无法联机。即使 UPS 系统也不能避免故障。应在设计时提

供适当冗余性，确保万一 UPS 发生故障，关键负载仍能运行。需要在这里再次重申，主动维护计划是降低故障风险的关键。部分维护任务必须使 UPS 系统离线。这就需要配备一个完全冗余的系统，如双系统冗余设计或外部维护旁路等。这些系统很重要，能在必要性关键负载的情况下，进行维护。

配电

一旦确定了需要的正确 UPS 配置，现在就可以进行配电。这通过配电柜(PDU)、远程电源板(RPP)、配电盘和某类电源线和电源板完成。许多设施的设计中都采用了最新技术，如双路市电、大型发电机组和冗余双系统冗余 UPS。但如果与负载的最终连接采用了不适当的布线、断路器和配电方法，所有这些技术都无法发挥其应有作用。支持服务器的 20 A 断路器应该是一个经过测试的螺栓插入型断路器。住宅应用中使用的嵌入式断路器较为便宜，使用和安装也比较简单，但相比较而言，不太安全、未经充分测试且可靠性低很多（故障率大概在 20%到 50%之间）。廉价的断路器会使其前面线路中所有内置冗余性失效。请不要将数百万美元的基础设施交由采用 10 美分断路器和 20 美分开关、价值 4 美元的电源插排控制。

模拟负载

模拟负载是维护关键任务设施的一个重要工具。它用于测试备份供电系统，以确保该系统在发生紧急事件时能支持必要负载。可安装永久模拟负载，也可请服务供应商带来临时模拟负载，以供维护使用。无论如何，都须确保在开关设备中进行了配置，将模拟负载连接到 UPS 系统和发电机。这个额外的模拟负载断路器将在未来使用中受益良多。

机械设计考虑因素

如果温度过高，人员和设备都会崩溃。对关键任务设施来说，充足、清洁、凉爽、干燥、无污染的空气是至关重要的。但如果处于高层建筑之中，可能没有自己的空调系统。许多建筑物不提供备份空调，也没有可靠的维护支持。最佳保护就是在租约中明确定义有关空调的条款。增加自己的备份系统虽然昂贵，但如果所在建筑物空调不可靠或没有备份空调，这是个相当重要的战略。

和 UPS 系统及其配置一样，主用和备份空调系统也有很多选择，如采用水冷或风冷冷水机的大型中央空调，或采用风冷、乙二醇制冷或其它制冷方式的直接膨胀空调等。

在选择风冷或水冷冷水机时，确保拥有为其提供支持的必要资源，包括冗余供电供水等。此外，可与应急便携式空调租赁公司事先签订应急暖通空调(HVAC)合同，只需拨打电话就能上门服务。这可将系统停运时间缩短几小时甚至几天。请谨记，现在就要为未来灾难做好充分准备。确保知道发生紧急事件时，应致电谁、需要什么设备，而且已拥有连接此设备的配置。

控制系统设计

关键任务设施的控制核心是控制发电机、开关设备、UPS 系统、制冷系统、火灾告警系统、安保以及其它机械和电气系统的多个系统。确保这些系统具有冗余性和容错性，且软件的可加载（包括密码）拷贝安全可用。在发生紧急事件时，要确保在不依靠外部人员的情况下，自行重装并恢复密钥系统。

临时系统配置

灾难来临时，可能需要临时设备来支持设施。如果事先没有计划，那么可能需要完全关闭设施，而且花费很长时间，才能连接临时设备。有可能在某个时刻需要用到临时发电机、燃料贮藏库、UPS 系统、电池、模拟负载、制冷系统甚至供水系统。立即检查设施，确定为支持临时设备，可能需要的断路器、接头、检修门、临时供电、空间和通道，以及隔离阀等。

安保设计

在为设施设计安保系统时，重要的是，应使用多种安保措施，来应对安全威胁，防止未授权人员进入建筑物和设施中的各个房间。物理安保由三个基本元素组成：机械、组织和环境安保。

物理安保
物理（电子系统）安保指对安保硬件的使用，包括门禁控制、闭路电视(CCTV)、门锁、监控系统、紧急呼叫系统和入侵告警。

- 门禁控制系统 – 门禁控制系统通过电子读卡器和电子门锁等设备，规定了哪些人有进入建筑物的权限。
- 入侵检测器 – 入侵检测器使用传感器来检测受保护门的开关状态。它们还能确定是否有人进入某一区域，以及不会引起告警的安全区。
- 监视系统 – 监视系统使用摄像头和显示屏来提醒人们事件的发生。监视设备一般由摄像头和电视显示屏、视频放大器、视频开关、录像机、录音机以及相关连线、接头和配件组成。
- 车流量控制 – 应控制车流量和停车场，以防未授权车辆进入建筑物。可以使用护栏、大门、水泥路障和路桩来控制车辆进入。

组织安保
组织（安保人员和流程）安保提供管理人员、安保人员、租户和员工都参与的安保计划。

环境安保
环境（建筑物基本元素）安保提供有关建筑物定义、环境监视和门禁控制的基本安保理念。值得注意的是，关键任务设施的核心是数据中心，而数据中心的核心则是设备间和机房。常常发生这种情况：数据中心得到了妥善保护，但为数据中心供电和提供保护的设备室却完全没有保护措施。应对通往电气和机械室的通道进行保护，用闭路电视监控关键系统。

EPO 开关
各种安全、消防和电气规范都要求设施具有一个紧急断电(EPO)系统，能在发生紧急事件时关闭设施的电源。虽然这些系统是必须的，但很少有人注重它们的设计。EPO 系统的设计应允许该系统在需要时运行，同时还确保此系统不会在升级和维护期间意外激活。EPO 系统应需要一种双重激活方法，如接到告警后，一个按钮激活摄像头或其它安保设备等。

监控系统设计

现在，技术极为先进，能够现场或远程监控任意类型的基础设施设备和环境状况。利用这些信息，就能收集趋势信息，有助于预测设备故障，当某个设备改变了运行模式或告警时，就会通知。

从多个地点获得趋势数据的能力，使管理层能够收集足够的数据，进行预测分析。借助这些数据，可确定应该何时更换泵轴承、保养电池或轮换设备。从发电机振动到制冷系统性能，正确监控数据能够节约时间和资金，并提高系统可靠性。

安全注意事项

安全与可靠性息息相关，能够节省时间、资金，甚至挽救生命。不安全的设施不可能可靠。先不计算人员成本，如果员工受伤、发生灾难，都会导致设备宕机。而救援和调查则会将宕机时间大大延长。确保安全计划处于最新状态且易于执行。在外部供货商在设施中开展工作之前，先索取一份他们的安全计划，确保它保持最新并得以贯彻执行。为设施中所需完成的工作制订一份相应的安全计划，并就此对员工进行培训。这其中应包括个人防护设备(PPE)的使用和维护、上锁挂牌流程以及高温作业安全要求等。在发生灾难前、灾难期间和发生灾难后，都要确保员工安全。在要求员工撤离疏散建筑物、再次进入受损建筑物或在受影响地点作业前，雇主应确保不会将员工置于危险之中。

设施运营

设施运营是保证关键任务设施可靠性的一个重要组成部分。大量故障的起因都是人为错误。提高可靠性应从了解设备运行状况，以及如果设备发生故障，会对设施有何影响开始。公布和运用详细的运行、维护及恢复流程非常关键。必须为关键任务设施的基础设施制订一个全面、详细的开关级别流程方法(MOP)，测试、确信并使用它们。通过试用/联合试用方法，来严格遵循 MOP。无论决定如何运行设施，都要保证员工得到充分培训。为在发生灾难时，维持设施运行并恢复，需要定期安排涵盖所有运行和通信功能的演习。特别要注意，因通信或信息拥塞或效率低下，需要进行哪些相应改动。每次测试后更新计划。保存记录也对设施运行很重要。应具备一个能保存记录并供随时查看的系统。

现场维护

为保证最高可靠性，正确维护势在必行。如果不能进行适当的维护，系统将不可避免出现故障。在维护期间，应详细记录发现的问题和开展的修复措施，这是很重要的。

预测性维护

全面的预防性维护计划能够通过及早发现设备问题，提高设施安全性和可靠性。一个成功的预防性维护检测计划具有极大优势。预防性维护能够在潜在问题浮出水面之前，就预测出故障点。预测性维护具有一定预见性，提供了坚实平台，来管理已测试和未测试的数据、发现的问题以及它们是否被修复等，将有助于长期预计投资回报的实现。为制订世界一流的预防性维护计划，只需确保其简单易行，并谨记其目的就是为了提高设施中设备的可靠性，将此作为制订计划的指导原则。

场地试运行

制订书面计划固然重要，但基础设施既涵盖虚拟环境，也涉及实际的机械和环境因素。它不仅包括位和字节，还包括具体物理细节。通过试运行，可以看出设计者的期望和生产商的承诺在实际环境中的实现情况。试运行是通过实际测试，验证并记录设施设备性能的系统化流程。

基础设施是由不同厂商的机械、电气和控制组件及系统构成的，由各专业公司安装。试运行流程对每个系统进行全方位的测试和均衡，以确保它能按照设想，正确安装和运行。

场地试运行机构必须确保系统从一开始就以最高水平运行。资历丰富的试运行专家会坚持执行全面彻底的质量管理流程，来验证和记录设施及系统的性能。试运行方法由大量流程组成，旨在验证关键任务设施的基础设施完整性与性能，这些流程包括：

- 试运行计划准备
- 开机前筹备和开机流程
- 集成系统测试(IST)
- 操作培训和防止员工离职，包括制订标准操作流程(SOP)和流程方法(MOP)等
- 系统（竣工）文件记录

培训

应针对关键任务设施的全体员工，制订一个全面的培训计划。尽早定期培训员工，对于保证设施的可靠性很重要。构建阶段和试运行阶段是让操作人员快速熟悉设备的理想时间。一旦设施投入运行，就应该持续开展有关安全操作，以及设备运行和维护的培训。在培训方面投入的时间和资金，将来都会收获丰厚回报。

结论

确保良好的公司氛围至关重要。归根结底，关键任务设施的运行依靠的是先进技术、信任和团队合作。高度可用的基础设施是电工、工程师、规划人员、管道工、CIO、保洁人员、技术人员、管理人员和维护团队精诚合作的结晶。基础设施供应商致力于协调所有这些团队的工作，确保关键任务设施能够提供出色性能和可用性，满足需求。对于像关键任务设施的基础设施这样重要的资产，应该投入充分时间来选择一家值得信赖的公司，这个公司应具备丰富经验和充足资源，能帮助延长正常运行时间，降低风险。在理想状态下，关键任务设施的基础设施专家将为提供所有必要的产品、人员、服务和战略，来帮助完成设施的设计、集成、试运行、人员培训、维护和监控。从一家公司获得所有这些重要服务，能够大大减少将来的问题，避免采用多供货商时出现的相互推诿责任的现象。当然，并非所有灾难都能避免，但通过正确的计划和维护，许多本该发生的灾难都能化解于无形。而对于不可避免的灾难，如飓风等，战略性灾难规划能够将其影响降至最低，以最快速度实现恢复。通过不断积累经验，我们能够更好应对下一次挑战。正如福特汽车的创始人亨利•福特曾说过的那样：“失败恰恰是重新开始的机会，吃一堑长一智” 。

资源

点击图标打开相应参考资源链接

优化关键任务设施和数据中心的正常运行时间
第 7 号白皮书

数据中心设施选址
第 81 号白皮书

数据中心规划中存在的九大误区
第 145 号白皮书

浏览所有 白皮书
whitepapers.apc.com

浏览所有 TradeOff Tools™ 权衡工具
tools.apc.com

联系我们

关于本白皮书内容的反馈和建议请联系：

数据中心科研中心
DCSC@Schneider-Electric.com

如果您作为我们的客户需要咨询数据中心项目相关信息：

请与所在地区或行业的 **施耐德电气** 销售代表联系，或登陆：
www.apc.com/support/contact/index.cfm