监测数据中心内的物理威胁

第 102 号白皮书

版本 3

作者　Michael R. Zlatic

> 摘要

用于监测数据中心环境的传统方法已不再足够。随着刀片式服务器等技术推高制冷需求、萨班斯-奥克斯利（Sarbanes-Oxley）法案等规章提高数据安全要求，数据中心内的物理环境必须得到更为密切的监测。尽管已有明确的制度用于监测 UPS 系统、计算机房空调机以及消防系统等物理设备，仍然有一类呈分布式的监测点经常被忽视。本文将介绍此类威胁，提出部署监测设备的方式，并提供利用所采集数据来缩短停机时间的最优方法。

目录

点击内容即可跳转至具体章节

APC 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 43 号白皮书
数据中心和网络机房的动态功率变化

当今常用的数据中心环境监测技术可以追溯到集中式大型机时代，需要 IT 人员携带温度计四处走动等活动，并要依靠 IT 人员来“感知”机房内的环境。但随着数据中心持续发展，分布式处理和服务器技术不断推高供电和制冷需求，必须对其环境进行更为密切的监测。

功率密度提高和功率动态变化是推动 IT 环境监测方法变革的两大主因。刀片式服务器使功率密度大大提升，显著改变了周围环境的供电和制冷动态模式。供电管理技术使服务器和通信设备能够根据计算用负载来改变吸收功率（继而改变热耗散量）。这一问题在第 43 号白皮书《数据中心和网络机房的动态功率变化》中详述。

尽管在 UPS、计算机房空调机（CRAC）及消防系统等物理设备中配备复杂的监测和告警功能已经很常见，物理环境的其它方面却经常被忽视。仅对设备监测并不足够，还必须对周围环境进行全面查看和针对威胁和侵入的主动监视。这些威胁包括服务器进气温度过高、漏水以及未经授权的人员进入数据中心，或者是人员在数据中心内进行不当操作。

分支机构、资料室等远程网络地点以及本地销售点进一步强化了对自动化监测的需求，在这些地方由人来现场检查温度和湿度等条件并非实际和可靠的办法。随着无人值守网络站点的引入，IT 管理员必须有可靠的系统来了解情况。

通过当前技术，监测系统可以被详细配置成满足数据中心具体环境和安保要求的程度：每一台机柜均可被视为具有自身要求的微型“数据中心”，并采用可能包括多个数据采集点的监测策略。

本文将讨论可通过分布式监测策略加以缓解的物理威胁，并给出在数据中心内部署传感器的准则和最优方法。文中还将讨论数据中心设计工具的使用，以简化这些分布式监测系统的规范和设计过程。

什么是分布式物理威胁?

本文针对的是威胁的一个子分类，即分布式物理威胁，这类威胁吸引了人们特别的关注，因为它们需要精心而专业化的设计方可加以防止。为标识该子分类，需对数据中心所受威胁的范围进行简要的归类描述。

数据中心威胁可被归为两个大类，依据是其属于 IT 软件和网络范畴（**数码**威胁）还是数据中心物理基础设施范畴（**物理**威胁）。

数码威胁

资源链接
第 101 号白皮书
网络安全的基本原理

数码威胁是诸如黑客、病毒、网络瓶颈以及其它针对数据安全性或数据流的意外或恶意攻击等问题。数码威胁在业界和媒体上广为人知，且多数数据中心均有健壮且主动维护式的系统，如防火墙和病毒查杀程序，以对其提供保护。第 101 白皮书《网络安全的基本原理》回顾了针对数码威胁的基本保护措施。数码威胁不是本文的主题。

物理威胁

IT 设备的物理威胁包括供电和制冷问题、人为错误或恶意破坏、火灾、泄漏及空气质量等问题。其中包括涉及供电的一些威胁以及涉及制冷和火灾的威胁由内建的供电、制冷和消防设备功能加以例行监测。例如，UPS 系统将监测供电质量、负载和蓄电池健康程度；PDU 将监测电路负载；制冷机组将监测输入和输出温度以及过滤器状态；消防系统（楼宇规范所要求的）将监测有无烟或过热。这些监测通常会遵循自动进行汇集、记录、解释并显示信息的软件系统的广为人知的协议。由设计在设备中的预设功能以此方式监测的威胁无需用户具有任何专门技能或进行任何规划即可获得有效的管理，只要监测和解释系统经过良好的工程设计即可。*这些被自动监测的物理威胁是全面管理系统所针对的关键部分，但不是本文的主题。*

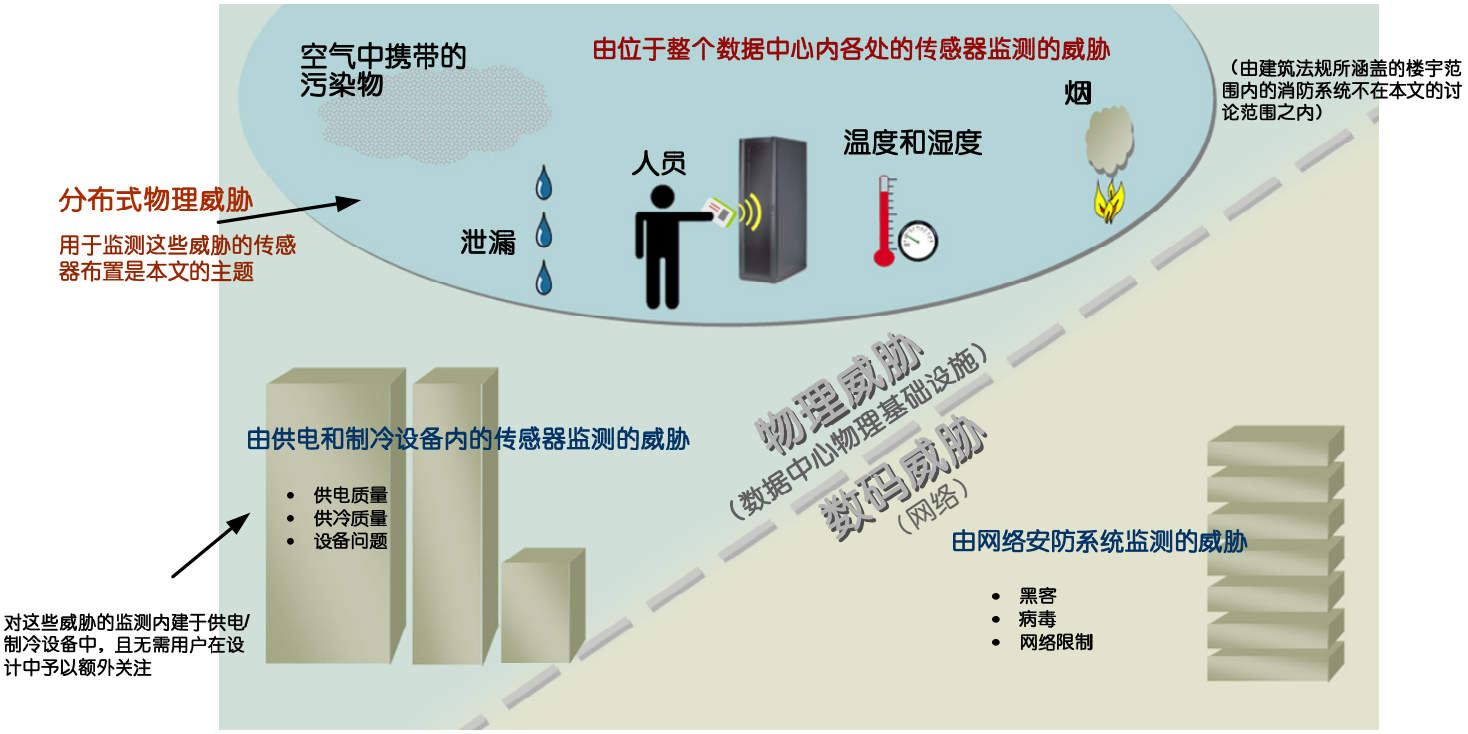
然而，对于数据中心内某些类型的物理威胁，特别是严重的威胁，用户并不能获得预先设计的嵌入式监测解决方案。例如，湿度水平不佳的威胁可以存在于数据中心内的任何地方，因此在对此威胁的管理中，湿度传感器的数量和位置将是重要的考虑因素。这样的威胁可能**潜在分布于整个数据中心的任何地方，位于特定于机房布局和设备定位的可变位置。**本文所涉及的分布式物理威胁分为以下大类：

- 对 IT 设备的空气质量威胁（温度、湿度）
- 液体泄漏
- 人员出现或异常活动
- 空气质量对人员的威胁（空气中携带的杂质）
- 因数据中心事故产生的烟和火 [1]

图 1 显示了数码威胁与物理威胁之间的区别，以及在物理威胁中，基于预工程化设备的供电/制冷监测的物理威胁与本文主题——分布式物理威胁之间的区别，后者需要评估、决策和规划以确定监测用传感器的类型、位置和数量。后一种物理威胁可能因为在有效监测策略的设计方面缺乏知识和专业技能而有疏漏的风险。

图 1

对数据中心的威胁



[1] 楼宇规范所要求的基本机房烟/火检测受特定的法律和安全规章管辖，不是本文的主题。本文所涉及的是除楼宇规范要求之外、特定于数据中心内危险的补充烟感检测。

表 1 归纳了分布式物理威胁、其对数据中心的影响以及用于对其监测的传感器类型。

表 1

分布式物理威胁

威胁	定义	对数据中心的影响	传感器类型
空气温度	机房、机柜和设备空气温度	因温度高于规范和/或温度剧烈变化而导致设备故障和设备寿命缩短	温度传感器
湿度	特定温度下的机房和机柜相对湿度	在低湿度点下因静电累积而导致设备故障 在高湿度点下结露形成	湿度传感器
液体泄漏	水或制冷剂泄漏	液体对地板、电缆和设备造成破坏 告警 CRAC 问题	点状泄漏传感器 绳状泄漏传感器
人为错误和人员进入	人员无意中不当操作 未经授权和/或强行恶意进入数据中心	设备损坏和数据损失 设备停机 设备失窃和破坏	数字摄像机 运动传感器 门禁触点 玻璃破裂传感器 振动传感器
烟/火	电气或材料火灾	设备故障 资产和数据损失	辅助烟感传感器
空气中危险污染物	空气中携带的化学物质，如来自电池的氢，以及灰尘等颗粒	因氢的释放而造成的人员危险情况和/或 UPS 不可靠及故障 静电和过滤器/风机积尘导致的设备故障	化学/可燃气体传感器

传感器布置

可采用多种类型的传感器来实现对上述威胁所致问题的预警。尽管传感器的具体类型和数量可能根据预算、威胁风险和破坏所致企业成本而有不同，但对多数数据中心而言，仍有一个可保证有效的最少的基本传感器组。**表 2** 给出了这一基本推荐传感器组的准则。

表 2

基本传感器准则

传感器类型	位置	常规最优方法	备注	适用的行业准则	举例
温度传感器	机柜	在每一 IT 机柜前门的顶部、中部和底部，用以监测机柜内设备的入口温度	在布线室或其它开放式机柜环境中，温度监测应尽可能接近设备入口	ASHRAE准则 [2]	
湿度传感器	行	每个冷空气通道一个，位于排中部一机柜的前方	由于 CRAC 机组可提供湿度读数，基于排的湿度传感器的位置如果过于接近 CRAC 输出，可能需要调整	ASHRAE 准则	
绳状泄漏传感器 点状泄漏传感器	机房	围绕每一 CRAC 系统、围绕制冷分配单元，以及在活动地板下方及其它任何泄漏源（如管道）处进行泄漏绳布置	点状泄漏传感器用于监测滴盘内液体流量过大，在较小机房/隔室和任何低点处进行监测	无行业标准	
数字摄像机	机房和行	根据数据中心布局策略性布置，覆盖入口/出口点，并对所有热、冷空气通道有良好的视野；确保覆盖所需的完整视场	采用视频监控软件监测并记录正常的进入以及未经授权或工作时间之外的进入	无行业标准	
机房门禁	机房	电子开关位于每一入口门上，用以提供机房门禁的检查索引，并在特定时间限制特定人员进入	将机房开关集成到设施系统中可能较为理想，并可通过通信接口实现	HIPPA 和萨班斯-奥克斯利法案 [3]	

除**表 2** 中所示的基本传感器之外，根据具体的机房配置、威胁程度以及可用性要求，还有其它传感器可作为备选。**表 3** 列出了这些附加传感器以及最优方法准则。

[2] ASHRAE TC9.9 任务关键设施，“数据处理环境的热学准则”，2004。

[3]德勤安保服务（Deloitte & Touche security services）CSO Fiona Williams 说：“物理安保确实需满足萨班斯-奥克斯利法案要求。它是 infosec 计划以及常规计算机控制的一个关键组件。它归于 302 和 404 节，要求管理层评估并确认内部控制有效运行。” http://www.csoonline.com/read/100103/counsel.html（2006 年 4 月 20 日访问）

表 3

附加与情况相关的传感器的准则

传感器类型	位置	常规最优方法	备注	适用的行业准则	示例
辅助烟感传感器	机柜	机柜级“非常早的烟检测”（VESD），用以在高度关键区域或无专用烟感传感器区域提供高级问题警告 [4]	当机柜级补充烟检测超出预算时，在每一 CRAC 的输入上安置 VESD 可提供某种程度的预警	无行业标准	
化学/氢传感器	机房	当 VRLA 电池位于数据中心中时，不需要在机房中放置氢传感器，因为它们在正常运行中不会释放氢（与湿式电池一样）	单独电池室内的湿式电池须满足特定规范要求	IEEE / ASHRAE 指引草案 [5]	
运动传感器	机房和行	当预算约束不允许安装数字摄像机时（最优方法，见**表 2**）使用	运动传感器是用于监测人员活动的数字摄像机的低成本替代方案	无行业标准	
机柜触点	机柜	在高流量数据中心中，每一机柜前门和后门上的电子开关用以提供机柜门禁的检查索引，并在特定时间限制特定人员对关键设备的使用	将机柜开关集成到设施系统中可能较为理想，并可通过通信接口实现	HIPPA 和萨班斯 - 奥克斯利法案	
振动传感器	机柜	在高流量数据中心中，每一机柜内的振动传感器用以检测对关键设备的未经授权的安装或拆卸	每一机柜内的振动传感器也可用于在人挪动机柜时进行检测	无行业标准	
玻璃破裂传感器	机房	位于每一数据中心窗口上的玻璃破裂传感器（在走廊或机房外部或内部）	最好与视频监控摄像机配合使用	无行业标准	

[4] 假设有单独的火灾检测系统以满足楼宇规范

[5] IEEE/ASHRAE，“固定式蓄电池设施的通风和热学管理指引”，提交 2006 年末投票草案

汇集传感器数据

在选择并布置了传感器之后，下一步是对传感器接收到的数据进行收集和分析。通常并不是将所有传感器数据直接发送至一个中央收集点，而是采用更好的方式，即让汇集点分布于整个数据中心内，每一汇集点具备告警和通知功能。这不仅可以消除单一中央汇集点的单点故障风险，而且还支持对远程服务器机房和电信室的使用点监测[6]。汇集器通过IP网络与中央监测系统通信（图 2）。

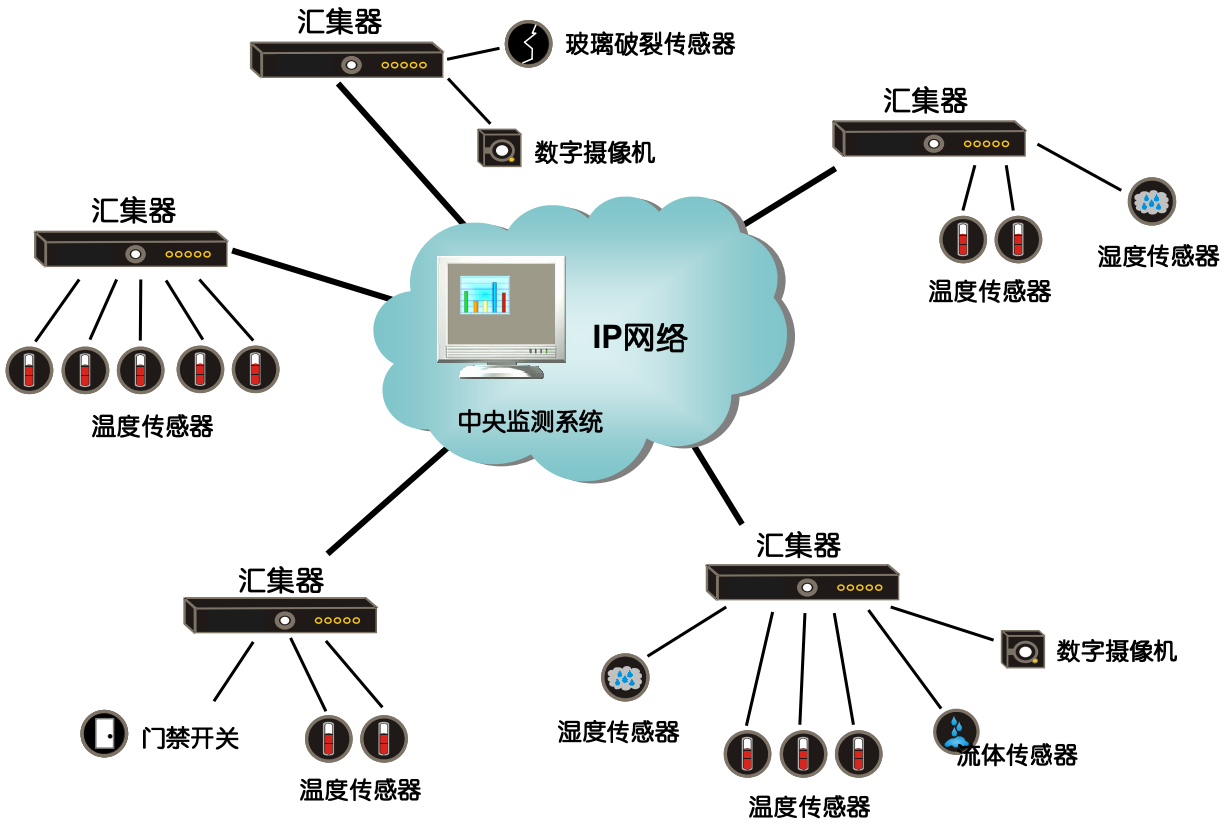


图 2

汇集传感器数据

单个传感器通常不会独自连接至 IP 网络，而是由汇集器解释传感器数据，并向中央系统发送告警，并/或直接发送至通知列表（见下一节）。这一分布式监测体系结构显著减少了所需网络分接口的数量，并可降低系统总体成本和管理负担。汇集器通常被分配至数据中心内的各个物理区域，对有限区域内的传感器进行汇集，以限制传感器连线复杂程度。

“智能”操作

传感器提供原始数据，但同样重要的是对该数据进行解释，以进行通知、告警和校正。随着监测策略日益变得复杂，以及传感器遍布整个有良好监测的数据中心，对这种潜在的大量数据的“智能”处理至关重要。收集和分析传感器数据并触发适当操作的最有效且最高效的方式就是采用前一节所述的“汇集器”。

基本要求是要能够过滤、关联并评价数据，以确定超限事件出现时的最佳操作过程。有效操作指向正确的人员通过正确的方式提示正确的信息。操作采用以下三种方式之一：

[6] 这种多汇集器体系结构有时被称为“边缘分布式智能”，其中每一汇集器均具有针对其所支持传感器的提示和通知功能。

- **告警**可能威胁特定设备、机柜或整个数据中心的超限情况
- 基于规定告警和阈值的自动**操作**
- **分析和报告**，以方便改进、优化和错误/故障测量

告警

在设置告警时需要确定三方面事项：**告警阈值** — 在何值处应触发告警；**告警方法** — 告警应如何发送、发送给谁；以及**逐步升级** — 特定类型的告警是否需要不同级别的逐步升级来加以解决？

告警阈值 – 对于每一传感器，应确定可接受的工作条件，并配置阈值，以便在读数超出这些工作条件时生成告警。理想情况下，监测系统应具备对每一传感器配置多个阈值的灵活性，以便给出信息告警、告警、临界及故障级别的各种告警。除单值阈值之外，还应有诸如超出阈值持续规定时间量、增长率和下降率等触发条件。对于温度，就变化率的告警可提供比快照温度值更快的故障告警。

阈值必须谨慎设置以确保最大的有效性。根据事件的严重程度，可能有导致不同告警的不同阈值。例如，湿度阈值事件可能导致向 IT 管理员发送电子邮件，而烟感传感器则可能触发自动拨打消防电话。类似地，不同的阈值水平将确保不同的逐步升级路径。例如，未经授权进入机柜的事件可能逐步升级至 IT 管理员处，而强行进入事件则可能逐步升级至 IT 主管。

阈值应以全局方式设置为缺省值，然后根据IP设备规范以及传感器相对设备位置的安装位置进行个别调整（例如，靠近服务器电源的传感器应比靠近服务器进风口的传感器设置较高的阈值）。**表 4** 列出了根据ASHRAE TC9.9 的温度和湿度的推荐缺省阈值。除这些阈值之外，监测温度变化率也很重要。在 5 分钟内温度改变 5.6 °C（10 °F）可能告警CRAC故障。[7]

表 4

推荐温度和湿度传感器阈值

传感器	上限阈值	下限阈值
空气温度	25 °C（77 °F）	20 °C（68 °F）
湿度	相对湿度 55%	相对湿度 40%

告警方法 — 告警信息可采用多种不同方式发送，如电子邮件、SMS 文本消息、SNMP trap 以及发布至 HTTP 服务器。重要的是，告警系统应灵活且可定制，以使正确的信息量可以被成功地传递至预定接收方。告警通知应包含用户定义的传感器名、传感器位置以及告警日期/时间等信息。

告警逐步升级 — 某些告警可能需要立即引起注意。如果在规定时间内问题未被解决，智能监测系统应能够将特定的告警逐步升级至更高的权限水平。告警逐步升级有助于确保在小问题升级成大问题之前对其进行及时处理。

以下是有用的和不太有用的告警的示例：

温度传感器#48 超出阈值 — 不太有用，因为它没有提示传感器#48 所处的位置

Web 服务器 X 存在过热危险 — 较为有用，因为确定了具体的服务器

[7] ASHRAE TC9.9 1 类环境建议，它受到最严格的控制，且可能最适合于从事任务关键作业的数据中心。

门传感器被激活 — 不太有用，因为没有确定具体的门

位置 Y 处的门 X 被打开，并拍摄了一张开门人的照片 — 非常有用，因为它包括了门的标识、门的位置以及事件照片

对数据的操作

收集传感器数据只是第一步，如果数据中心管理员单纯依靠手动响应，数据将不会发挥最大优势。可采用根据用户指定告警和阈值进行自动操作的系统。为实现这种“智能”自动化，必须对以下方面进行评估：

告警操作 — 根据告警的严重程度，应采取何种自动化操作？这些自动化操作可以是人员通知，也可以是矫正操作，如触发干式触点以接通或断开风机或泵等设备。

传感器数据持续实时可见 — 查看个别传感器“快照”读数的能力是一项基本要求，而实时查看个别传感器趋势的能力则可提供对情况的更好的了解。对这些趋势的解释让管理员可以检测更广范围的问题，并对来自多个传感器的数据进行相关处理。

告警系统应不仅仅提供基本的违反阈值通知。例如，某些监测系统允许管理员将附加数据放在告警中。该附加数据可能是拍摄的视频、录制的音频、图片以及地图。此类内容丰富型告警系统由于在告警中包含了背景数据，使管理员可以在掌握更多信息的条件下做出决策。在某些情况下，过多的信息可能需要加以过滤方可得出有用内容。例如，在一个高流量数据中心内，如果每次一有运动都给出告警，将是非常麻烦的事情。可能存在为安全起见而将特定信息阻塞或“掩盖”的情况。例如，包含键盘图像的视频可能会阻塞个人键入密码的内容。

以下是“智能”解释和操作的示例：

- 在触及温度阈值时，自动开启风机或 CRAC
- 根据哪一面在进行实时视频监控，远程提供对带电子门锁的特定机柜的门禁控制
- 当在一远程数据中心内检测到有水时，自动开启污水泵
- 当在正常工作时间之后检测到数据中心内有运动时，自动拍摄视频并提示保安人员
- 当在工作时间以外检测到玻璃破裂时，通知保安人员并发出告警提示音
- 当一个门开关告警机柜门已开启超过 30 分钟（告警门未正常关闭）时，向管理员发出检查门的告警

分析和报告

智能监测系统不仅应包含传感器数据的短期趋势，还应有长期历史数据。最好的监测系统应能访问以往数周、数月乃至数年的传感器读数，并能按此数据生成图象和报告。该图象应能在同一份报告上呈现多种类型传感器，以供比较和分析。报告应能够对各组传感器在所选时段内提供最低、最高和平均传感器读数。

传感器长期历史信息可以多种方式使用，例如，用以显示数据中心达到容量极限并非由于物理空间，而是由于制冷不足。此类信息可在越来越多的设备加装到数据中心时用于推断未来趋势，并可协助预测数据中心何时将达到容量极限。长期趋势分析可在机柜级用于比较不同机柜中不同制造商的设备如何产生更多的热量或达到更凉的效果，比较结果将可能影响未来的采购。

监测系统所采集的传感器读数应可导出为业界标准格式，使得数据以及定制报告和分析程序可以现成使用。

设计方法

尽管威胁监测系统的规范和设计可能看起来很复杂，该过程可采用数据中心设计工具加以自动化，如的 InfraStruXure Designer。此类设计工具让用户可以输入一个简单的偏好列表，并可自动布置相应数量的传感器和汇集设备。汇总报告将提供推荐传感器的零件列表和安装说明。这些数据中心设计工具采用基于最优方法和行业标准的算法和成规，按照密度、机房布局、机房门禁策略以及用户特定的监测要求来提供具体的配置建议。

例如，以下由用户指定的偏好可能根据数据中心流量和访问水平来影响威胁监测系统的设计：

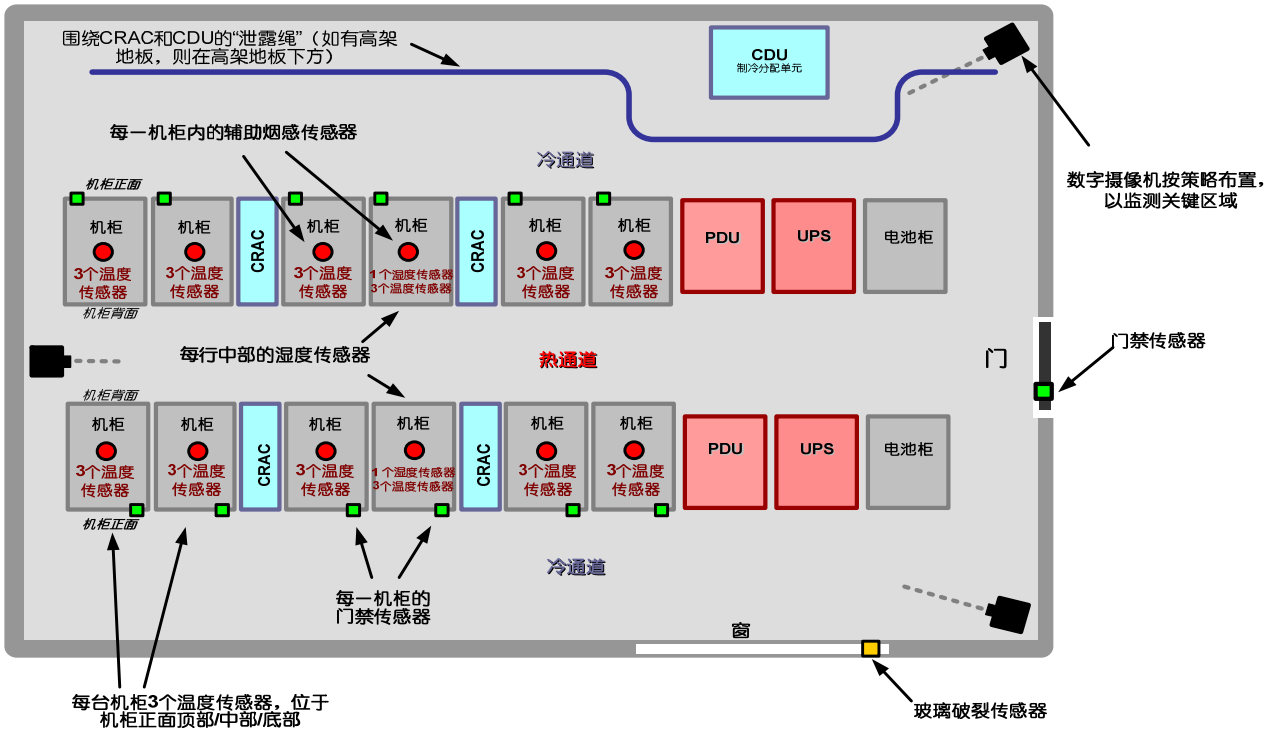
- **高流量/访问** – 如果数据中心有许多个人进入，每个人在数据中心内都有不同的应用和职能，则设计工具会建议每一机柜上的机柜开关仅向需要进入相应机柜的个人赋予准入权。
- **低流量/访问** – 如果数据中心仅有经选择的少数个人进入，每个人均对所有数据中心功能负责，则设计工具将不会建议机柜开关来控制对单个机柜的准入权；一个机房门开关将足以限制其它人员进入机房。

传感器布置示例

图 3 中给出了一个数据中心布置示例，其中根据本文所述最优方法示出了监测设备的位置。

图 3

传感器布置示例



结论

针对分布式物理威胁的保护对于全面安保策略至关重要。尽管传感设备的布置和方法需要评估、决策和设计，仍有最优方法和设计工具可以协助进行有效的传感器部署。

除了传感器的类型、位置和数量要合适之外，还必须有软件系统来管理所收集的数据，并提供日志记录、趋势分析、智能告警通知以及可能场合下的自动化矫正操作。

理解监测分布式物理威胁的技术将使 IT 管理员们填补数据中心总体安保方面的关键鸿沟，并使物理安保措施与变化中的数据中心基础设施和可用性目标保持一致。

关于作者

Michael R. Zlatic 是施耐德电气信息技术事业部的安防与环境监测部门的高级产品经理。Michael 在哈利伯顿能源服务集团和 Magnetic Power Systems 公司担任过工程、销售和管理等多项职务。在加入施耐德电气之前，他是智能视频和分析设备和软件产品套件生产商 Arteco Vision Systems 公司的产品经理。Michael 拥有密苏里大学罗拉分校（University of Missouri-Rolla）机械工程专业的学士学位。

资源

点击图标打开相应参考资源链接

数据中心和网络机房的动态功率变化
第 43 号白皮书

网络安全的基本原理
第 101 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

如果您是我们的客户并对数据中心项目有任何疑问：

请与您的 **施耐德电气**销售代表联系