









Product Application Guide

Threat	Definition	Types of Sensors	Impact on Industry
Temperature/ Air Flow	Room, rack, and equipment ambient temperature	Temperature sensors	Equipment failure and reduced equipment life span from temperature above specification and/or drastic temperature changes Spoilage on refrigerated inventory
Air Flow/ Humidity	Room and rack humidity and refrigerated airflow	Humidity sensors Air Flow sensors	Equipment failure from static electricity buildup at low humidity points Condensation formation at high humidity points Air flow reduction can lead to higher cooling costs
Power Outages	Power outages due to overloaded circuits or fuses	Third party PDU Control (RS-232) sensor	Equipment failure from power loss Corrupt data from sudden power loss
Liquid leaks	Water or coolant leaks	Liquid sensors	Liquid damage to floors, cabling and equipment Indication of CRAC problems
Human error and personnel access	Unintentional wrongdoing by personnel Unauthorized and/or forced entry into the data center with malicious intent	Digital video cameras Motion sensors Security sensor	Equipment damage and data loss Equipment downtime Theft and sabotage of equipment
Smoke / Fire	Electrical or material fire	Smoke sensors	Equipment failure Loss of assets and data

Guidelines for Basic Sensors

Sensor Type	Location	General Best Practice	Examples	Comments	Applicable Industry Guidelines
Temperature and Airflow sensors	Rack and Room	At top, middle, and bottom of the front door of each IT rack, to monitor inlet temperature of devices in rack		In wiring closets or other open rack environments, temperature monitoring should be as close as possible to equipment inlets	ASHRAE Guidelines ¹
Humidity sensors	Room and Rack	One per cold aisle, at the front of a rack in the middle of the row		Since CRAC units provide humidity readings, location of row-based humidity sensors may need to be adjusted if too close to CRAC output	ASHRAE Guidelines
Third Party PDU Control RS-232 sensors	Row	RS-232 sensor placed next to PDU		Single point monitoring of PDUs better controls power consumption levels	HIPPA and Sarbanes-Oxley ²
Water sensors	Room and Floor	Water sensor placement around each CRAC system, around cooling distribution units, and under raised floors, and any other leak source (such as pipes)		Water sensors for monitoring fluid overflows in drip pans, monitoring in smaller rooms/closets and at any low spots	No industry standard
Digital video cameras	Room and Row	Strategically placed according to data center layout covering entry / exit points and a good view of all hot and cold aisles; ensure complete required field of view is covered		Monitoring and recording of normal access as well as unauthorized or after-hours access with video surveillance software	No industry standard
Security sensor	Room and Cabinet Doors	Security sensor at every entry door to provide audit trail of room access, and to limit access to specific people at specific times		Integrating room switches into the facility system may be desirable and can be achieved through a communications interface	HIPPA and Sarbanes-Oxley ²
Smoke sensors	Rack	Rack level "very early smoke detection" (VESD) to provide advanced warning of problems in highly critical areas or areas without dedicated smoke sensors ³		When rack-level smoke detection exceeds budget, placing VESD on the input of each CRAC provides some degree of early warning	No industry standards
Motion sensors	Room and Row	Used when budget constraints don't allow for digital camera installation, which is best practice		Motion sensors are a lower cost alternative to digital video cameras for monitoring human activity	No industry standards

¹ ASHRAE TC9.9 Mission Critical Facilities, "Thermal Guidelines for Data Processing Environments," 2004.

² CSO Fiona Williams, Deloitte & Touche security services, says "Physical security does fall under the Sarbanes-Oxley requirements. It is a critical component of the infosec program as well as general computer controls. It falls within sections 302 and 404, which require that management evaluate and assert that the internal controls are operating effectively." <http://www.csoonline.com/read/100103/counsel.html> (accessed on April 20, 2006)

³ Assumes the existence of a separate fire detection system to meet building codes